

A thick, solid blue vertical bar with rounded ends, positioned to the left of the main text block.

Сервисные маршрутизаторы серии ESR

**ESR-10, ESR-12V, ESR-12VF, ESR-14VF, ESR-20,
ESR-21, ESR-100, ESR-200, ESR-1000, ESR-1200,
ESR-1500, ESR-1510, ESR-1700**

Руководство по эксплуатации, Описание функционала (02.04.2020)
Версия ПО 1.8.5

Содержание

| | | |
|-------|---|----|
| 1 | Примеры настройки маршрутизатора | 8 |
| 1.1 | Настройка VLAN | 8 |
| 1.1.1 | Алгоритм настройки..... | 8 |
| 1.1.2 | Пример настройки 1. Удаление VLAN с интерфейса..... | 10 |
| 1.1.3 | Пример настройки 2. Разрешение обработки VLAN в тегированном режиме..... | 10 |
| 1.1.4 | Пример настройки 3. Разрешение обработки VLAN в тегированном и не тегированном режиме | 11 |
| 1.2 | Настройка LLDP | 11 |
| 1.2.1 | Алгоритм настройки..... | 12 |
| 1.2.2 | Пример настройки..... | 12 |
| 1.3 | Настройка LLDP MED | 13 |
| 1.3.1 | Алгоритм настройки..... | 14 |
| 1.3.2 | Пример настройки Voice VLAN..... | 15 |
| 1.4 | Настройка терминации на саб-интерфейсе | 16 |
| 1.4.1 | Алгоритм настройки..... | 16 |
| 1.4.2 | Пример настройки саб-интерфейса..... | 17 |
| 1.5 | Настройка терминации на Q-in-Q интерфейсе | 18 |
| 1.5.1 | Алгоритм настройки..... | 18 |
| 1.5.2 | Пример настройки Q-in-Q интерфейса..... | 19 |
| 1.6 | Настройка USB модемов | 20 |
| 1.6.1 | Алгоритм настройки USB-модемов | 20 |
| 1.6.2 | Пример настройки..... | 22 |
| 1.7 | Настройка AAA | 22 |
| 1.7.1 | Алгоритм настройки локальной аутентификации..... | 23 |
| 1.7.2 | Алгоритм настройки AAA по протоколу RADIUS | 26 |
| 1.7.3 | Алгоритм настройки AAA по протоколу TACACS | 30 |
| 1.7.4 | Алгоритм настройки AAA по протоколу LDAP | 33 |
| 1.7.5 | Пример настройки аутентификации по telnet через RADIUS-сервер | 37 |
| 1.8 | Настройка привилегий команд | 38 |
| 1.8.1 | Алгоритм настройки..... | 38 |
| 1.8.2 | Пример настройки привилегий команд | 38 |
| 1.9 | Настройка DHCP-сервера | 39 |
| 1.9.1 | Алгоритм настройки..... | 39 |
| 1.9.2 | Пример настройки DHCP-сервера | 42 |
| 1.10 | Конфигурирование Destination NAT | 44 |

| | | |
|--------|---|----|
| 1.10.1 | Алгоритм настройки..... | 44 |
| 1.10.2 | Пример настройки Destination NAT | 47 |
| 1.11 | Конфигурирование Source NAT..... | 49 |
| 1.11.1 | Алгоритм настройки..... | 49 |
| 1.11.2 | Пример настройки 1..... | 52 |
| 1.11.3 | Пример настройки 2..... | 54 |
| 1.12 | Конфигурирование Static NAT..... | 55 |
| 1.12.1 | Алгоритм настройки..... | 55 |
| 1.12.2 | Пример настройки Static NAT..... | 56 |
| 1.12.3 | Пример настройки фильтрации приложений (DPI)..... | 57 |
| 1.13 | Проксирование HTTP/HTTPS-трафика..... | 59 |
| 1.13.1 | Алгоритм настройки..... | 59 |
| 1.13.2 | Пример настройки HTTP-прокси..... | 61 |
| 1.14 | Настройка логирования и защиты от сетевых атак..... | 62 |
| 1.14.1 | Алгоритм настройки..... | 62 |
| 1.14.2 | Описание механизмов защиты от атак..... | 65 |
| 1.14.3 | Пример настройки логирования и защиты от сетевых атак..... | 68 |
| 1.15 | Конфигурирование Firewall..... | 69 |
| 1.15.1 | Алгоритм настройки..... | 70 |
| 1.15.2 | Пример настройки Firewall..... | 77 |
| 1.16 | Настройка списков доступа (ACL)..... | 79 |
| 1.16.1 | Алгоритм настройки..... | 79 |
| 1.16.2 | Пример настройки списка доступа..... | 81 |
| 1.17 | Конфигурирование статических маршрутов..... | 82 |
| 1.17.1 | Процесс настройки..... | 82 |
| 1.17.2 | Пример настройки статических маршрутов..... | 83 |
| 1.18 | Настройка PPP через E1..... | 85 |
| 1.18.1 | Процесс настройки..... | 85 |
| 1.18.2 | Пример конфигурации..... | 88 |
| 1.19 | Настройка MLPPP..... | 89 |
| 1.19.1 | Алгоритм настройки..... | 89 |
| 1.19.2 | Пример настройки..... | 91 |
| 1.20 | Настройка Bridge..... | 92 |
| 1.20.1 | Алгоритм настройки..... | 92 |
| 1.20.2 | Пример настройки bridge для VLAN и L2TPv3-туннеля..... | 94 |
| 1.20.3 | Пример настройки bridge для VLAN..... | 95 |
| 1.20.4 | Пример настройки добавления/удаления второго VLAN-тега..... | 97 |

| | | |
|--------|---|-----|
| 1.21 | Настройка RIP | 97 |
| 1.21.1 | Алгоритм настройки..... | 98 |
| 1.21.2 | Пример настройки RIP | 102 |
| 1.22 | Настройка OSPF | 103 |
| 1.22.1 | Алгоритм настройки..... | 104 |
| 1.22.2 | Пример настройки OSPF | 113 |
| 1.22.3 | Пример настройки OSPF stub area..... | 115 |
| 1.22.4 | Пример настройки Virtual link | 115 |
| 1.23 | Настройка BGP..... | 117 |
| 1.23.1 | Алгоритм настройки..... | 117 |
| 1.23.2 | Пример настройки..... | 124 |
| 1.24 | Настройка BFD..... | 126 |
| 1.24.1 | Алгоритм настройки..... | 126 |
| 1.24.2 | Пример настройки BFD с BGP..... | 130 |
| 1.25 | Настройка политики маршрутизации PBR..... | 131 |
| 1.25.1 | Настройка Route-мар для BGP..... | 131 |
| 1.25.2 | Route-мар на основе списков доступа (Policy-based routing)..... | 138 |
| 1.26 | Настройка GRE-туннелей | 140 |
| 1.26.1 | Алгоритм настройки..... | 141 |
| 1.26.2 | Пример настройки IP-GRE-туннеля | 144 |
| 1.27 | Настройка DMVPN..... | 146 |
| 1.27.1 | Алгоритм настройки..... | 146 |
| 1.27.2 | Пример настройки..... | 148 |
| 1.28 | Настройка L2TPv3-туннелей..... | 153 |
| 1.28.1 | Алгоритм настройки..... | 153 |
| 1.28.2 | Пример настройки L2TPv3-туннеля..... | 155 |
| 1.29 | Настройка IPsec VPN | 157 |
| 1.29.1 | Настройка Route-based IPsec VPN..... | 157 |
| 1.29.2 | Настройка Policy-based IPsec VPN..... | 167 |
| 1.29.3 | Настройка Remote Access IPsec VPN..... | 176 |
| 1.30 | Настройка LT-туннелей | 188 |
| 1.30.1 | Алгоритм настройки..... | 188 |
| 1.30.2 | Пример настройки..... | 189 |
| 1.31 | Настройка удаленного доступа к корпоративной сети по PPTP-протоколу..... | 190 |
| 1.31.1 | Алгоритм настройки..... | 190 |
| 1.31.2 | Пример настройки PPTP-сервера..... | 193 |
| 1.32 | Настройка удаленного доступа к корпоративной сети по L2TP over IPsec протоколу..... | 195 |

| | | |
|--------|--|-----|
| 1.32.1 | Алгоритм настройки..... | 195 |
| 1.32.2 | Пример настройки..... | 197 |
| 1.33 | Настройка удаленного доступа к корпоративной сети по OpenVPN протоколу | 199 |
| 1.33.1 | Алгоритм настройки..... | 200 |
| 1.33.2 | Пример настройки..... | 203 |
| 1.34 | Настройка клиента удаленного доступа по протоколу PPPoE..... | 205 |
| 1.34.1 | Алгоритм настройки..... | 205 |
| 1.34.2 | Пример настройки PPPoE-клиента | 207 |
| 1.35 | Настройка клиента удаленного доступа по протоколу PPTP | 208 |
| 1.35.1 | Алгоритм настройки..... | 208 |
| 1.35.2 | Пример настройки удаленного подключения по PPTP-протоколу | 210 |
| 1.36 | Настройка клиента удаленного доступа по протоколу L2TP | 211 |
| 1.36.1 | Пример настройки удаленного подключения по L2TP-протоколу | 213 |
| 1.37 | Настройка Dual-Homing | 215 |
| 1.37.1 | Алгоритм настройки..... | 215 |
| 1.37.2 | Пример настройки..... | 215 |
| 1.38 | Настройка QoS..... | 216 |
| 1.38.1 | Базовый QoS | 217 |
| 1.38.2 | Расширенный QoS..... | 221 |
| 1.39 | Настройка зеркалирования | 228 |
| 1.39.1 | Алгоритм настройки..... | 228 |
| 1.39.2 | Пример настройки..... | 229 |
| 1.40 | Настройка Netflow..... | 230 |
| 1.40.1 | Алгоритм настройки..... | 230 |
| 1.40.2 | Пример настройки..... | 231 |
| 1.41 | Настройка sFlow | 232 |
| 1.41.1 | Алгоритм настройки..... | 232 |
| 1.41.2 | Пример настройки..... | 233 |
| 1.42 | Настройка LACP | 234 |
| 1.42.1 | Алгоритм настройки..... | 234 |
| 1.42.2 | Пример настройки..... | 236 |
| 1.43 | Настройка VRRP | 237 |
| 1.43.1 | Алгоритм настройки..... | 237 |
| 1.43.2 | Пример настройки 1..... | 240 |
| 1.43.3 | Пример настройки 2..... | 241 |
| 1.44 | Настройка VRRP tracking..... | 243 |
| 1.44.1 | Алгоритм настройки..... | 243 |

| | | |
|--------|---|-----|
| 1.44.2 | Пример настройки..... | 245 |
| 1.45 | Настройка VRF Lite..... | 247 |
| 1.45.1 | Алгоритм настройки..... | 248 |
| 1.45.2 | Пример настройки..... | 249 |
| 1.46 | Настройка MultiWAN..... | 250 |
| 1.46.1 | Алгоритм настройки..... | 251 |
| 1.46.2 | Пример настройки..... | 253 |
| 1.47 | Настройка SNMP..... | 255 |
| 1.47.1 | Алгоритм настройки..... | 255 |
| 1.47.2 | Пример настройки..... | 259 |
| 1.48 | Настройка Zabbix-agent/proxy..... | 261 |
| 1.48.1 | Алгоритм настройки..... | 261 |
| 1.48.2 | Пример настройки zabbix-agent/proxy..... | 262 |
| 1.48.3 | Пример настройки zabbix-server..... | 263 |
| 1.49 | Настройка Syslog..... | 266 |
| 1.49.1 | Алгоритм настройки..... | 267 |
| 1.49.2 | Пример настройки Syslog..... | 269 |
| 1.50 | Настройка BRAS (Broadband Remote Access Server)..... | 271 |
| 1.50.1 | Алгоритм настройки..... | 271 |
| 1.50.2 | Пример настройки с SoftWLC..... | 276 |
| 1.50.3 | Пример настройки без SoftWLC..... | 282 |
| 1.51 | Настройка IPS/IDS..... | 287 |
| 1.51.1 | Алгоритм базовой настройки..... | 288 |
| 1.51.2 | Алгоритм настройки автообновления правил IPS/IDS из внешних источников | 289 |
| 1.51.3 | Рекомендуемые открытые источники обновления правил..... | 289 |
| 1.51.4 | Пример настройки IPS/IDS с автообновлением правил..... | 292 |
| 1.51.5 | Алгоритм настройки базовых пользовательских правил..... | 294 |
| 1.51.6 | Пример настройки базовых пользовательских правил..... | 304 |
| 1.51.7 | Алгоритм настройки расширенных пользовательских правил..... | 305 |
| 1.51.8 | Пример настройки расширенных пользовательских правил..... | 306 |
| 1.52 | Настройка VoIP..... | 307 |
| 1.52.1 | Процесс настройки SIP-профиля..... | 307 |
| 1.52.2 | Процесс настройки FXS/FXO-портов..... | 308 |
| 1.52.3 | Процесс настройки плана нумерации..... | 310 |
| 1.52.4 | Процесс настройки PBX-сервера..... | 310 |
| 1.52.5 | Процесс создания транка регистрации..... | 312 |
| 1.52.6 | Пример настройки VoIP..... | 313 |

| | | |
|--------|---|-----|
| 1.52.7 | Пример настройки плана нумерации..... | 315 |
| 1.52.8 | Настройка FXO-порта..... | 317 |
| 1.53 | Проверка целостности | 319 |
| 1.53.1 | Процесс настройки | 319 |
| 1.53.2 | Пример конфигурации..... | 319 |
| 1.54 | Настройка архивации конфигурации маршрутизатора | 319 |
| 1.54.1 | Процесс настройки | 319 |
| 1.54.2 | Пример конфигурации..... | 320 |
| 2 | Часто задаваемые вопросы | 322 |
| 3 | Техническая поддержка | 324 |

1 Примеры настройки маршрутизатора

1.1 Настройка VLAN

VLAN (Virtual Local Area Network) – логическая («виртуальная») локальная сеть, представляет собой группу устройств, которые взаимодействуют между собой на канальном уровне независимо от их физического местонахождения. Работа VLAN основана на использовании дополнительных полей Ethernet-заголовка согласно стандарту 802.1q. По сути, VLAN изолирует широковещательный домен путем ограничения коммутации Ethernet-фреймов только с одинаковым VLAN-ID в Ethernet-заголовке.

1.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 1 | Создать VLAN. | esr(config)# vlan <VID> | <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис). |
| 2 | Задать имя vlan (не обязательно). | esr(config-vlan)# name <vlan-name> | <vlan-name> – до 255 символов. |
| 3 | Отключить отслеживание состояния интерфейсов, на которых разрешена обработка Ethernet-фреймов данного VLAN (не обязательно) | esr(config-vlan)# force-up | |
| 4 | Отключить обработку входящих не тегированных Ethernet-фреймов на основе таблицы коммутации VLAN'a по умолчанию (VLAN-ID – 1) (не обязательно) | esr(config-if-gi)# no switchport forbidden default-vlan | |
| 5 | Установить режим работы физического интерфейса в L2-режим | esr(config-if-gi)# mode switchport | |
| 6 | Задать режим работы L2 интерфейса. | esr(config-if-gi)# switchport access | Только для ESR-10/12V(F)/14VF/20/21/100/200. Данный режим является режимом по умолчанию и не отображается в конфигурации. |
| | | esr(config-if-gi)# switchport trunk | Только для ESR-10/12V(F)/14VF/20/21/100/200. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| | | esr(config-gi)# switchport general | Только для ESR-1000/1200/1500/1510/1700. Данный режим является режимом по умолчанию и не отображается в конфигурации. |
| 7 | Настроить список VLAN на интерфейсе в тегированном режиме. | esr(config-if-gi)# switchport trunk allowed vlan add <VID> | Для ESR-10/12V(F)/14VF/20/21/100/200. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис). |
| | | esr(config-if-gi)# switchport general allowed vlan add <VID> tagged | Для ESR-1000/1200/1500/1510/1700. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис). |
| 8 | Настроить VLAN на интерфейсе в нетегированном режиме (не обязательно). | esr(config-if-gi)# switchport trunk native-vlan <VID> | Для ESR-10/12V(F)/14VF/20/21/100/200. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. |
| | | esr(config-if-gi)# switchport general allowed vlan add <VID> untagged | Для ESR-1000/1200/1500/1510/1700. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. |
| 9 | Разрешить на интерфейсе обработку Ethernet-фреймов всех созданных на маршрутизаторе VLAN (не обязательно). | esr(config-if-gi)# switchport trunk allowed vlan auto-all | Только для ESR-10/12V(F)/14VF/20/21/100/200. |
| | | esr(config-if-gi)# switchport general allowed vlan auto-all | Только для ESR-1000/1200/1500/1510/1700. |

1.1.2 Пример настройки 1. Удаление VLAN с интерфейса

Задача:

На основе заводской конфигурации удалить из VLAN 2 порт gi1/0/1.



Рисунок 1 – Схема сети

Решение:

Удалим VLAN 2 с порта gi1/0/1:

```
esr(config)# interface gi 1/0/1
esr(config-if-gi)# switchport general allowed vlan remove 2 untagged
esr(config-if-gi)# no switchport general pvid
```

1.1.3 Пример настройки 2. Разрешение обработки VLAN в тегированном режиме

Задача:

Настроить порты gi1/0/1 и gi1/0/2 для передачи и приема пакетов в VLAN 2, VLAN 64, VLAN 2000.

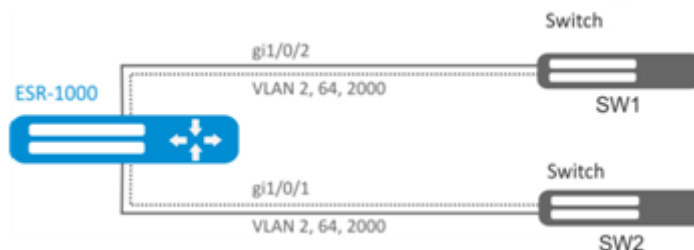


Рисунок 2 – Схема сети

Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000 на ESR-1000:

```
esr-1000(config)# vlan 2,64,2000
```

Пропишем VLAN 2, VLAN 64, VLAN 2000 на порт gi1/0/1-2:

```
esr-1000(config)# interface gi1/0/1
esr-1000(config-if-gi)# mode switchport
esr-1000(config-if-gi)# switchport forbidden default-vlan
esr-1000(config-if-gi)# switchport general allowed vlan add 2,64,2000 tagged
```

1.1.4 Пример настройки 3. Разрешение обработки VLAN в тегированном и не тегированном режиме

Задача:

Настроить порты gi1/0/1 для передачи и приема пакетов в VLAN 2, VLAN 64, VLAN 2000 в режиме trunk, настроить порт gi1/0/2 в режиме access для VLAN 2 на ESR-100/ESR-200.

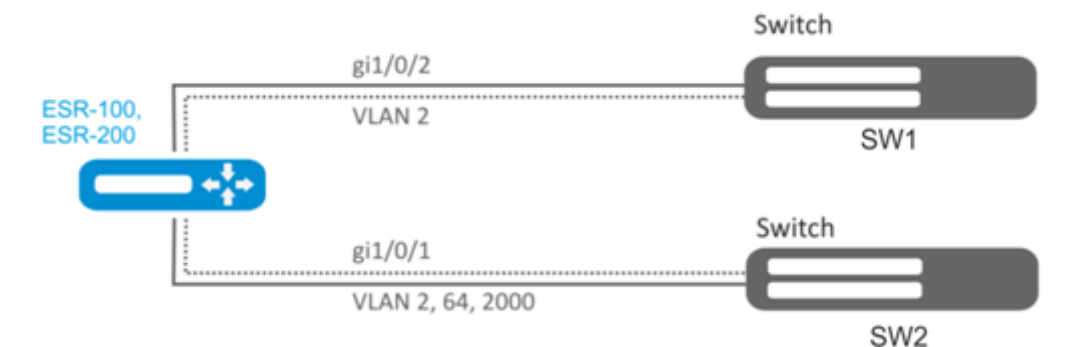


Рисунок 3 – Схема сети

Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000 на ESR-100/ ESR-200:

```
esr(config)# vlan 2,64,2000
```

Пропишем VLAN 2, VLAN 64, VLAN 2000 на порт gi1/0/1:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 2,64,2000
```

Пропишем VLAN 2 на порт gi1/0/2:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport access vlan 2
```

1.2 Настройка LLDP

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

1.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Активировать LLDP на маршрутизаторе | esr(config)# lldp enable | |
| 2 | Установить период, в течение которого маршрутизатор хранит информацию, полученную по LLDP (не обязательно). | esr(config)# lldp hold-multiplier <SEC> | <SEC> – период времени в секундах, принимает значение [1..10]. |
| 3 | Установить IP-адрес, который будет передаваться в LLDP TLV в качестве management-address (не обязательно). | esr(config)# lldp management-address <ADDR> | <ADDR> – IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. По умолчанию задается один из существующих |
| 4 | Установить поле system-description, которое будет передаваться в LLDP TLV в качестве system-description (не обязательно). | esr(config)# lldp system-description <DESCRIPTION> | <DESCRIPTION> – описание системы, задается строкой до 255 символов. По умолчанию содержит информацию о модели и версии ПО маршрутизатора. |
| 5 | Установить поле system-name, которое будет передаваться в LLDP TLV в качестве system-name (не обязательно). | esr(config)# lldp system-name <NAME> | <NAME> – имя системы, задается строкой до 255 символов. По умолчанию совпадает с заданным hostname |
| 6 | Установить период отправки LLDPDU (не обязательно). | esr(config)# lldp timer <SEC> | <SEC> – период времени в секундах, принимает значение [1..32768]. |
| 7 | Включить прием и обработку LLDPDU на физическом интерфейсе. | esr(config-if-gi)# lldp receive | |
| 8 | Включить отправку LLDPDU на физическом интерфейсе. | esr(config-if-gi)# lldp transmit | |

1.2.2 Пример настройки

Задача:

Организовать обмен и обработку LLDPDU между маршрутизаторами ESR-1 и ESR-2.



Рисунок 4 – Схема сети

Решение:

1. Конфигурирование R1

Включим LLDP глобально на маршрутизаторе:

```
esr(config)# lldp enable
```

Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp transmit
```

2. Конфигурирование R2

Включим LLDP глобально на маршрутизаторе:

```
esr(config)# lldp enable
```

Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp transmit
```

Общую информацию по LLDP соседям можно посмотреть командой:

```
esr# show lldp neighbors
```

Подробную информацию по соседу конкретного интерфейса можно посмотреть командой:

```
esr# show lldp neighbors gigabitethernet 1/0/1
```

Общую статистику по LLDP можно посмотреть командой:

```
esr# show lldp statistics
```

1.3 Настройка LLDP MED

LLDP MED – расширение стандарта LLDP, которое позволяет передавать сетевые политики: VLAN ID, DSCP, priority.

1.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 1 | Активировать LLDP на маршрутизаторе | esr(config)# lldp enable | |
| 2 | Активировать расширение MED LLDP на маршрутизаторе | esr(config)# lldp med fast-start enable | |
| 3 | Создать сетевую политику | esr(config)# network-policy <NAME> | <NAME> – имя network-policy, задается строкой до 31 символа. |
| 4 | Указать тип приложения | esr(config-net-policy)# application <APP_TYPE> | <APP-TYPE> – тип приложения, для которого будет срабатывать network-policy. Принимает значения: <ul style="list-style-type: none"> • voice, • voice-signaling, • guest-voice, • guest-voice-signaling, • softphone-voice, • video-conferencing, • streaming-video, • video-signaling. |
| 5 | Установить значение DSCP | esr(config-net-policy)# dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. |
| 6 | Установить значение COS | esr(config-net-policy)# priority <PRIORITY> | <COS> – значение приоритета, принимает значения: <ul style="list-style-type: none"> • best-effort – COS0; • background – COS1; • excellent-effort – COS2; • critical-applications – COS3; • video – COS4; • voice – COS5; • internetwork-control – COS6; • network-control – COS7. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 7 | Установить значение VLAN ID | esr(config-net-policy)# vlan <VID> [tagged] | <VID> – идентификационный номер VLAN, принимает значения [1...4094]; • tagged – ключ, при установке которого абонентское устройство будет отправлять Ethernet-фреймы указанного приложения в тегированном виде. |
| 8 | Установить сетевую политику на интерфейс | esr(config-if-gi)# lldp network-policy <NAME> | <NAME> – имя network-policy, задается строкой до 31 символа. |
| 9 | Включить отправку LLDPDU на физическом интерфейсе. | esr(config-if-gi)# lldp transmit | |

1.3.2 Пример настройки Voice VLAN

Voice VLAN – VLAN ID, при получении которого IP-телефон переходит в режим trunk с заданным VLAN ID для приема и отправки VoIP-трафика. Передача VLAN ID осуществляется посредством расширения MED протокола LLDP.

Задача:

Необходимо разделить трафик телефонии и данных по разным VLAN, vid 10 для данных и vid 20 для телефонии, и настроить отправку Voice VLAN с порта gi 1/0/1 ESR. При этом на IP-телефоне должен поддерживаться и быть включен Voice VLAN.



Рисунок 5 – Схема сети

Решение:

Предварительно необходимо создать VLAN 10 и 20 и настроить интерфейс gi 1/0/1 в режиме trunk:

```
esr(config)# vlan 10,20
esr(config-vlan)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 10,30
esr(config-if-gi)# exit
```

Включим LLDP и поддержку MED в LLDP глобально на маршрутизаторе:

```
esr(config)# lldp enable
esr(config)# lldp med fast-start enable
```

Создадим и настроим сетевую политику таким образом, чтобы для приложения voice указывался VLAN ID 20:

```
esr(config)# network-policy VOICE_VLAN
esr(config-net-policy)# application voice
esr(config-net-policy)# vlan 20 tagged
esr(config-net-policy)# exit
```

Настроим LLDP на интерфейсе и установим на него сетевую политику:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp transmit
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp network-policy VOICE_VLAN
esr(config-if-gi)# exit
```

1.4 Настройка терминации на саб-интерфейсе

Для терминирования Ethernet-фреймов конкретного VLAN на определенном физическом интерфейсе необходимо создать саб-интерфейс с указанием номера VLAN, фреймы которого будут терминироваться. При создании двух саб-интерфейсов с одинаковыми VLAN, но на разных физических/агрегированных интерфейсах, коммутация Ethernet-фреймов между данными саб-интерфейсами будет невозможна т.к. сегменты за пределами саб-интерфейсов будут являться отдельными широковещательными доменами. Для обмена данными между абонентами разных саб-интерфейсов (даже с одинаковым VLAN-ID) будет использоваться маршрутизация, т.е. обмен данными будет происходить на третьем уровне модели OSI.

1.4.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 1 | Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routeport). | <pre>esr(config)# interface gigabitethernet <PORT>.<S- VLAN></pre> <p>или</p> <pre>interface tengigabitetherne t <PORT>.<S- VLAN></pre> <p>или</p> <pre>interface port- channel <CH>.<S- VLAN></pre> | <p><PORT> – номер физического интерфейса.</p> <p><CH> – номер агрегированного интерфейса.</p> <p><S-VLAN> – идентификатор создаваемого S-VLAN.</p> <p>Если физический интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 2 | Задать описание саб-интерфейса (не обязательно). | esr(config-subif)# description <DESCRIPTION> | <DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов. |
| 3 | Указать экземпляр VRF, в котором будет работать данный саб-интерфейс (не обязательно). | esr(config-subif) # ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (не обязательно). | esr(config-subif)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. |
| 5 | Включить саб-интерфейс bridge-group (не обязательно). | esr(config-subif)#bridge-group <BRIDGE-ID> | <BRIDGE-ID> – идентификационный номер моста. |
| 6 | Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (не обязательно). | esr(config-subif)# ip arp reachable-time <TIME> или ipv6 nd reachable-time <TIME> | <TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>. |

1.4.2 Пример настройки саб-интерфейса

Задача:

Настроить терминацию подсети 192.168.3.1/24 в VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.

Решение:

Создадим саб-интерфейс для VLAN: 828

```
esr(config)# interface gigabitethernet 1/0/1.828
```

Настроим IP-адрес из необходимой подсети:

```
esr(config)# interface gigabitethernet 1/0/1.828
esr(config-subif)# ip address 192.168.3.1/24
esr(config-subif)# exit
```

⚠ Помимо назначения IP-адреса, на саб-интерфейсе необходимо либо отключить firewall, либо настроить соответствующую зону безопасности.

1.5 Настройка терминации на Q-in-Q интерфейсе

Q-in-Q – технология передачи пакетов с двумя 802.1q тегами. Данная технология используется для расширения количества используемых VLAN в сети передачи данных. Внутренним тегом (InnerTag) называется 802.1q заголовок ближе к payload. Так же внутренний тег называют C-VLAN (Customer VLAN). Внешний тег (OuterTag) – это 802.1q заголовок, добавленный к изначальному 802.1q пакетом, так же называется S-VLAN (Service VLAN). Использование двойных меток в Ethernet фреймах описывается протоколом 802.1ad.

1.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 1 | Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routeport). | <pre>esr(config)# interface gigabitethernet <PORT>.<S- VLAN></pre> <p>или</p> <pre>interface tengigabitethernet <PORT>.<S-VLAN></pre> <p>или</p> <pre>interface port-channel <CH>.<S-VLAN></pre> | <p><PORT> – номер физического интерфейса.</p> <p><CH> – номер агрегированного интерфейса.</p> <p><S-VLAN> – идентификатор создаваемого S-VLAN.</p> |
| 2 | Создать Q-in-Q интерфейс. | <pre>esr(config)# interface gigabitethernet <PORT>.<S- VLAN>.<C-VLAN></pre> <p>или</p> <pre>esr(config)# interface tengigabitethernet <PORT>.<S-VLAN>.<C-VLAN></pre> <p>или</p> <pre>esr(config)# interface port- channel <CH>.<S-VLAN>.<C- VLAN></pre> | <p><PORT> – номер физического интерфейса.</p> <p><CH> – номер агрегированного интерфейса.</p> <p><S-VLAN> – идентификатор создаваемого S-VLAN.</p> <p><C-VLAN> – идентификатор создаваемого C-VLAN.</p> <p>Если физический или саб-интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 3 | Задать описание Q-in-Q интерфейса (не обязательно). | esr(config-qinq-if)# description <DESCRIPTION> | <DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов. |
| 4 | Указать экземпляр VRF, в котором будет работать данный Q-in-Q интерфейс (не обязательно). | esr(config-qinq-if) # ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 5 | Установить интервал времени, в течение которого собирается статистика о нагрузке на Q-in-Q интерфейс (не обязательно). | esr(config-qinq-if)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. |
| 6 | Включить Q-in-Q интерфейс bridge-group (не обязательно). | esr(config-qinq-if)#bridge-group <BRIDGE-ID> | <BRIDGE-ID> – идентификационный номер моста. |
| 7 | Установить время жизни IPv4/IPv6 записей в ARP-таблице изученных на данном Q-in-Q интерфейсе (не обязательно). | esr(config-qinq-if)# ip arp reachable-time <TIME> или ipv6 nd reachable-time <TIME> | |

1.5.2 Пример настройки Q-in-Q интерфейса

Задача:

Настроить терминацию подсети 192.168.1.1/24 комбинации C-VLAN: 741, S-VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.

Решение:

Создадим саб-интерфейс для S-VLAN: 828

```
esr(config)# interface gigabitethernet 1/0/1.828
esr(config-subif)# exit
```

Создадим Q-in-Q саб-интерфейс для S-VLAN: 741 и настроим IP-адрес из необходимой подсети.

```
esr(config)# interface gigabitethernet 1/0/1.828.741
esr(config-qinq-if)# ip address 192.168.1.1/24
esr(config-qinq-if)# exit
```

⚠ Помимо назначения IP-адреса, на Q-in-Q саб-интерфейсе необходимо либо отключить firewall, либо настроить соответствующую зону безопасности.

1.6 Настройка USB модемов

Использование USB-модемов позволяет организовать дополнительный канал связи для работы маршрутизатора. При подключении USB-модемов возможно использовать USB-концентраторы. Одновременно в системе может быть сконфигурировано до 10-ти USB-модемов.

1.6.1 Алгоритм настройки USB-модемов

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 1 | После подключения USB-модема дождаться, когда система обнаружит подключенное устройство | | |
| 2 | Определить, какой номер устройства назначен на подключенный USB-модем | <code>esr# show cellulars status modem</code> | В поле "USB port" будет указан идентификатор подключенного устройства. |
| 3 | Создать профиль настроек для USB-модема и перейти в режим конфигурирования профиля | <code>esr(config)# cellular profile <ID></code> | <ID> – идентификатор профиля настроек для USB-модема в системе [1..10]. |
| 4 | Задать описание профиля настроек (не обязательно) | <code>esr(config-cellular-profile)# description <DESCRIPTION></code> | <DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов. |
| 5 | Задать точку доступа мобильной сети | <code>esr(config-cellular-profile)# apn <NAME></code> | <NAME> – точка доступа мобильной сети, задаётся строкой до 31 символа. |
| 6 | Задать имя пользователя мобильной сети (если мобильный оператор требует данное поле) | <code>esr(config-cellular-profile)# user <NAME></code> | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 7 | Установить пароля для пользователя мобильной сети (если мобильный оператор требует данное поле) | <code>esr(config-user)# password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code> | <CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F]; <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов. |
| 8 | Установить номер дозвона для подключения к мобильной сети | <code>esr(config-cellular-profile)# number <WORD></code> | <WORD> – номер дозвона для подключения к мобильной сети, задаётся строкой до 15 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 9 | Задать метод аутентификации пользователя в мобильной сети (не обязательно) | <code>esr(config-cellular-profile)# allowed-auth <TYPE></code> | <TYPE> – метод аутентификации пользователя в мобильной сети [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP]. |
| 10 | Ограничить возможность использования семейств IP-адресов в мобильной сети. | <code>esr(config-cellular-profile)# ip-version { ipv4 ipv6 }</code> | <ul style="list-style-type: none"> • ipv4 – семейство IPv4; • ipv6 – семейство IPv6; |
| 11 | Создать USB-модем в конфигурации маршрутизатора и перейти в режим конфигурирования модема | <code>esr(config)# cellular modem <ID></code> | <ID> – идентификатор USB-модема в системе [1..10]. |
| 12 | Указать экземпляр VRF, в котором будет работать данный модем (не обязательно). | <code>esr(config-cellular-modem)# ip vrf forwarding <VRF></code> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 13 | Задать идентификатор USB-модема, назначенного системой (определен в пункте 2.) | <code>esr(config-cellular-modem)# device <WORD></code> | <WORD> – идентификатор USB-порта подключенного модема [1..12]. |
| 14 | Назначить ранее созданный профиль настроек для USB-модема | <code>esr(config-cellular-modem)# profile <ID></code> | <ID> – идентификатор профиля настроек для USB-модема в системе [1..10]. |
| 15 | Задать код разблокировки SIM-карты (в случае необходимости) | <code>esr(config-cellular-modem)# pin <WORD></code> | <WORD> – код разблокировки SIM-карты [4..8]. Возможно использование только цифр. |
| 16 | Разрешить использование того или иного режима работы USB-модема (не обязательно) | <code>esr(config-cellular-modem)# allowed-mode <MODE></code> | <p><MODE> – допустимый режим работы USB-модема [2g, 3g, 4g].</p> <p>По умолчанию: разрешены все режимы, поддерживаемые модемом.</p> |
| 17 | Задать размер максимального принимаемого пакета (не обязательно) | <code>esr(config-cellular-modem)# mru { <MRU> }</code> | <MRU> – значение MRU, принимает значения в диапазоне [128..16383]. |
| 18 | Задать предпочтительный режим работы USB-модема в мобильной сети (не обязательно) | <code>esr(config-cellular-modem)# preferred-mode { <MODE> }</code> | <MODE> – предпочтительный режим работы USB-модема [2g, 3g, 4g] |
| 19 | Активировать USB-модем | <code>esr(config-cellular-modem)# enable</code> | |

1.6.2 Пример настройки

Задача:

Настроить подключение к сети Интернет, используя USB-модем.

Решение:

Для примера разберём подключение к сотовому оператору МТС.

После подключения модема необходимо дождаться, когда система обнаружит устройство. Определим порт устройства, который был назначен на подключённый USB-модем:

```
esr# show cellular status modem
Number
device  USB port      Manufacturer  Model  Current state  Interface  Link  state
1      1-2 huawei E3372   Disabled  -- Down
```

Создадим профиль настроек для USB-модема:

```
esr(config)# cellular profile 1
```

Зададим APN, который требует провайдер, или иной необходимый адрес. Ниже показан пример подключения к APN МТС:

```
esr(config-cellular-profile)# apn internet.mts.ru
```

При необходимости задаём имя пользователя, пароль, номер дозвона и метод аутентификации:

```
esr(config-cellular-profile)# user mts
esr(config-cellular-profile)# password ascii-text mts
esr(config-cellular-profile)# number *99#
esr(config-cellular-profile)# allowed-auth PAP
```

Перейдём к конфигурированию USB-модема и зададим идентификатор, соответствующий порту устройства, который был определён в начале:

```
esr(config)# cellular modem 1
esr(config-cellular-modem)# device 1-2
```

Назначим соответствующий профиль настроек и активируем модем:

```
esr(config-cellular-modem)# profile 1
esr(config-cellular-modem)# enable
```

1.7 Настройка AAA

AAA (Authentication, Authorization, Accounting) – используется для описания процесса предоставления доступа и контроля над ним.

- Authentication (аутентификация) – сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю.
- Authorization (авторизация, проверка полномочий, проверка уровня доступа) – сопоставление учётной записи в системе и определённых полномочий.
- Accounting (учёт) – слежение за подключением пользователя или внесенным им изменениям.

1.7.1 Алгоритм настройки локальной аутентификации

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 1 | Указать local в качестве метода аутентификации. | esr(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: <ul style="list-style-type: none"> • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов. |
| 2 | Указать enable в качестве способа аутентификации повышения привилегий пользователей. | esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: <ul style="list-style-type: none"> • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 3 | Указать способ перебора методов аутентификации в случае отказа (не обязательно). | esr(config)# aaa authentication mode <MODE> | <p><MODE> – способы перебора методов:</p> <ul style="list-style-type: none"> • chain – если сервер вернул FAIL, перейти к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. <p>Значение по умолчанию: chain.</p> |
| 4 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно) | esr(config)# aaa authentication attempts max-fail <COUNT> <TIME> | <p><COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];</p> <p><TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535].</p> <p>Значение по умолчанию: <COUNT> – 5; <TIME> – 300</p> |
| 5 | Включить запрос на смену пароля по умолчанию для пользователя admin (не обязательно) | esr(config)# security passwords default-expired | |
| 6 | Включить режим запрета на использование ранее установленных паролей локальных пользователей (не обязательно) | esr(config)# security passwords history <COUNT> | <p><COUNT> – количество паролей сохраняемых в памяти маршрутизатора. Принимает значение в диапазоне [1..15].</p> <p>Значение по умолчанию: 0</p> |
| 7 | Установить время действия пароля локального пользователя (не обязательно) | esr(config)# security passwords lifetime <TIME> | <p><TIME> – интервал времени действия пароля в днях. Принимает значение в диапазоне [1..365].</p> <p>По умолчанию: Время действия пароля локального пользователя неограниченно.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 8 | Установить ограничение на минимальную длину пароля локального пользователя и ENABLE-пароля (не обязательно) | esr(config)# security passwords min-length <NUM> | <NUM> – минимальное количество символов в пароле. Принимает значение в диапазоне [8..128]. Значение по умолчанию: 0 |
| 9 | Установить ограничение на максимальную длину пароля локального пользователя и ENABLE-пароля (не обязательно) | esr(config)# security passwords max-length <NUM> | <NUM> – максимальное количество символов в пароле. Принимает значение в диапазоне [8..128]. Значение по умолчанию: не ограничено. |
| 10 | Установить минимальное количество типов символов, которые должны присутствовать в пароле локального пользователя и ENABLE-пароле (не обязательно) | esr(config)# security passwords symbol-types <COUNT> | <COUNT> – минимальное количество типов символов в пароле. Принимает значение в диапазоне [1..4]. Значение по умолчанию: 1 |
| 11 | Установить минимальное количество строчных букв в пароле локального пользователя и ENABLE-пароле (не обязательно) | esr(config)# security passwords lower-case <COUNT> | <COUNT> – минимальное количество строчных букв в пароле локального пользователя и ENABLE-пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0 |
| 12 | Установить минимальное количество прописных (заглавных) букв в пароле локального пользователя и ENABLE-пароле (не обязательно) | esr(config)# security passwords upper-case <COUNT> | <COUNT> – минимальное количество прописных (заглавных) букв в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0 |
| 13 | Установить минимальное количество цифр в пароле локального пользователя и ENABLE-пароле (не обязательно) | esr(config)# security passwords numeric-count <COUNT> | <COUNT> – минимальное количество цифр в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0 |
| 14 | Установить минимальное количество специальных символов в пароле локального пользователя и ENABLE-пароле (не обязательно) | esr(config)# security passwords special-case <COUNT> | <COUNT> – минимальное количество специальных символов в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0 |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 15 | Добавить пользователя в локальную базу и перейти в режим настройки параметров пользователя | esr(config)# username <NAME> | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 16 | Установить пароль пользователя | esr(config-user)# password { <CLEAR-TEXT> encrypted <HASH_SHA512> } | <CLEAR-TEXT> – пароль, задаётся строкой [8 .. 32] символов, принимает значения [0-9a-fA-F]; <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой из 110 символов. |
| 17 | Установить уровень привилегий пользователя | esr(config-user)# privilege <PRIV> | <PRIV> – необходимый уровень привилегий. Принимает значение [1..15]. |
| 18 | Перейти в режим конфигурирования соответствующего терминала | esr(config)# line console или esr(config)# line telnet или esr(config)# line ssh | |
| 19 | Активировать список аутентификации входа пользователей в систему | esr(config-line-ssh)# login authentication <NAME> | <NAME> – имя списка, задаётся строкой до 31 символа. |
| 20 | Активировать список аутентификации повышения привилегий пользователей | esr(config-line-ssh)# enable authentication <NAME> | <NAME> – имя списка, задаётся строкой до 31 символа. |
| 21 | Задать интервал, по истечении которого будет разрываться бездействующая сессия | esr(config-line-ssh)# exec-timeout <SEC> | <SEC> – период времени в минутах, принимает значения [1..65535]. |

1.7.2 Алгоритм настройки AAA по протоколу RADIUS

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 1 | Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов RADIUS-сервера (не обязательно). | esr(config)# radius-server dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 2 | Задать глобальное значение количества перезапросов к последнему активному RADIUS-серверу (не обязательно). | esr(config)# radius-server retransmit <COUNT> | <COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10]. Значение по умолчанию: 1. |
| 3 | Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что RADIUS-сервер недоступен (не обязательно). | esr(config)# radius-server timeout <SEC> | <SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды. |
| 4 | Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования. | esr(config)# radius-server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>] esr(config-radius-server)# | <IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 5 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и времени блокировки (не обязательно). | aaa authentication attempts max-fail <COUNT> <TIME> | <COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в секундах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300 |
| 6 | Задать пароль для аутентификации на удаленном RADIUS-сервере. | esr(config-radius-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } | <TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 7 | Задать приоритет использования удаленного RADIUS-сервера (не обязательно). | esr(config-radius-server)# priority <PRIORITY> | <PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1. |
| 8 | Задать интервал, по истечении которого маршрутизатор считает, что данный RADIUS-сервер недоступен (не обязательно). | esr(config-radius-server)# timeout <SEC> | <SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: используется значение глобального таймера. |
| 9 | Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых RADIUS-пакетах. | esr(config-radius-server)# source-address { <ADDR> <IPV6- ADDR> } | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 10 | Указать radius в качестве метода аутентификации. | esr(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: <ul style="list-style-type: none"> • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 11 | Указать radius в качестве способа аутентификации повышения привилегий пользователей. | esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <p><NAME> – имя списка строка до 31 символа;</p> <ul style="list-style-type: none"> • default – имя списка по умолчанию. <p><METHOD> – способы аутентификации:</p> <ul style="list-style-type: none"> • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP. |
| 12 | Указать способ перебора методов аутентификации в случае отказа (не обязательно). | esr(config)# aaa authentication mode <MODE> | <p><MODE> – способы перебора методов:</p> <ul style="list-style-type: none"> • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. <p>Значение по умолчанию: chain.</p> |
| 13 | Сконфигурировать radius в списке способов учета сессий пользователей (не обязательно). | esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>] | <p><METHOD> – способы учета:</p> <ul style="list-style-type: none"> • tacacs – учет сессий по протоколу TACACS; • radius – учет сессий по протоколу RADIUS. |
| 14 | Перейти в режим конфигурирования соответствующего терминала. | esr(config)# line <TYPE> | <p><TYPE> – тип консоли:</p> <ul style="list-style-type: none"> • console – локальная консоль; • ssh – защищенная удаленная консоль. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 15 | Активировать список аутентификации входа пользователей в систему. | esr(config-line-console)# login authentication <NAME> | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8. |
| 16 | Активировать список аутентификации повышения привилегий пользователей. | esr(config-line-console)# enable authentication <NAME> | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 9. |

1.7.3 Алгоритм настройки AAA по протоколу TACACS

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов TACACS-сервера (не обязательно). | esr(config)# tacacs-server dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63. |
| 2 | Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что TACACS-сервер недоступен (не обязательно). | esr(config)# tacacs-server timeout <SEC> | <SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды. |
| 3 | Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования. | esr(config)# tacacs -server host { <IP-ADDR> <IPv6-ADDR> } [vrf <VRF>] esr(config- tacacs -server)# | <IP-ADDR> – IP-адрес TACACS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] <IPv6-ADDR> – IPv6-адрес TACACS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 4 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно) | aaa authentication attempts max-fail <COUNT> <TIME> | <p><COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];</p> <p><TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535].</p> <p>Значение по умолчанию: <COUNT> – 5; <TIME> – 300</p> |
| 5 | Задать пароль для аутентификации на удаленном TACACS-сервере | esr(config-tacacs-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } | <p><TEXT> – строка [8..16] ASCII-символов;</p> <p><ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задается строкой [16..32] символов.</p> |
| 6 | Задать номер порта для обмена данными с удаленным TACACS-сервером (не обязательно). | esr(config-tacacs-server)# port <PORT> | <p><PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].</p> <p>Значение по умолчанию: 49 для TACACS-сервера.</p> |
| 7 | Задать приоритет использования удаленного TACACS сервера (не обязательно). | esr(config-tacacs-server)# priority <PRIORITY> | <p><PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535].</p> <p>Чем ниже значение, тем приоритетнее сервер.</p> <p>Значение по умолчанию: 1.</p> |
| 8 | Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых TACACS-пакетах. | esr(config-radius-tacacs)# source-address { <ADDR> <IPV6-ADDR> } | <p><ADDR> – IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 9 | Указать TACACS в качестве способа аутентификации повышения привилегий пользователей. | esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <p><NAME> – имя списка строка до 31 символа;</p> <ul style="list-style-type: none"> • default – имя списка по умолчанию. <p><METHOD> – способы аутентификации:</p> <ul style="list-style-type: none"> • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP. |
| 10 | Указать способ перебора методов аутентификации в случае отказа (не обязательно). | esr(config)# aaa authentication mode <MODE> | <p><MODE> – способы перебора методов:</p> <ul style="list-style-type: none"> • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. <p>Значение по умолчанию: chain.</p> |
| 11 | Сконфигуровать список способов учета команд, введенных в CLI (не обязательно). | esr(config)# aaa accounting commands stop-only tacacs | |
| 12 | Сконфигурировать tacacs в списке способов учета сессий пользователей (не обязательно). | esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>] | <p><METHOD> – способы учета:</p> <ul style="list-style-type: none"> • tacacs – учет сессий по протоколу TACACS; • radius – учет сессий по протоколу RADIUS. |
| 13 | Перейти в режим конфигурирования соответствующего терминала. | esr(config)# line <TYPE> | <p><TYPE> – тип консоли:</p> <ul style="list-style-type: none"> • console – локальная консоль; • ssh – защищенная удаленная консоль. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 14 | Активировать список аутентификации входа пользователей в систему. | esr(config-line-console)# login authentication <NAME> | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 7. |
| 15 | Активировать список аутентификации повышения привилегий пользователей. | esr(config-line-console)# enable authentication <NAME> | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8. |

1.7.4 Алгоритм настройки AAA по протоколу LDAP

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 1 | Задать базовый DN (Distinguished name), который будет использоваться при поиске пользователей. | esr(config)# ldap-server base-dn <NAME> | <NAME> – базовый DN, задается строкой до 255 символов. |
| 2 | Задать интервал, по истечении которого устройство считает, что LDAP-сервер недоступен (не обязательно). | esr(config)# ldap-server bind timeout <SEC> | <SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды. |
| 3 | Задать DN (Distinguished name) пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей. | esr(config)# ldap-server bind authenticate root-dn <NAME> | <NAME> – DN пользователя с правами администратора, задается строкой до 255 символов. |
| 4 | Задать пароль пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей. | esr(config)# ldap-server bind authenticate root-password ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } | <TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 5 | Задать имя класса объектов, среди которых необходимо выполнять поиск пользователей на LDAP-сервере (не обязательно). | esr(config)# ldap-server search filter user-object-class <NAME> | <NAME> – имя класса объектов, задаётся строкой до 127 символов. Значение по умолчанию: posixAccount. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 6 | Задать область поиска пользователей в дереве LDAP-сервера (не обязательно). | esr(config)# ldap-server search scope <SCOPE> | <p><SCOPE> – область поиска пользователей на LDAP-сервере, принимает следующие значения:</p> <ul style="list-style-type: none"> • onelevel – выполнять поиск в объектах на следующем уровне после базового DN в дереве LDAP-сервера; • subtree – выполнять поиск во всех объектах поддерева базового DN в дереве LDAP сервера. <p>Значение по умолчанию: subtree.</p> |
| 7 | Задать интервал, по истечении которого устройство считает, что LDAP-сервер не нашел записей пользователей, подходящих под условие поиска (не обязательно). | esr(config)# ldap-server search timeout <SEC> | <p><SEC> – период времени в секундах, принимает значения [0..30]</p> <p>Значение по умолчанию: 0 – устройство ожидает завершения поиска и получения ответа от LDAP-сервера.</p> |
| 8 | Задать имя атрибута объекта, со значением которого идет сравнение имени искомого пользователя на LDAP-сервере (не обязательно). | esr(config)# ldap-server naming-attribute <NAME> | <p><NAME> – имя атрибута объекта, задаётся строкой до 127 символов.</p> <p>Значение по умолчанию: uid.</p> |
| 9 | Задать имя атрибута объекта, значение которого будет определять начальные привилегии пользователя на устройстве (не обязательно). | esr(config)# ldap-server privilege-level-attribute <NAME> | <p><NAME> – имя атрибута объекта, задаётся строкой до 127 символов.</p> <p>Значение по умолчанию: priv-lvl</p> |
| 10 | Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов LDAP-сервера (не обязательно). | esr(config)# ldap-server dscp <DSCP> | <p><DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].</p> <p>Значение по умолчанию: 63</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 11 | Добавить LDAP-сервер в список используемых серверов и перейти в режим его конфигурирования. | <pre>esr(config)# ldap -server host { <IP-ADDR> <IPv6-ADDR> } [vrf <VRF>] esr(config-tacacs-server)#</pre> | <p><IP-ADDR> – IP-адрес LDAP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]</p> <p><IPv6-ADDR> – IPv6-адрес TACACS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]</p> <p><VRF> – имя экземпляра VRF, задается строкой до 31 символа.</p> |
| 12 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно) | <pre>aaa authentication attempts max-fail <COUNT> <TIME></pre> | <p><COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];</p> <p><TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535].</p> <p>Значение по умолчанию: <COUNT> – 5; <TIME> – 300</p> |
| 13 | Задать номер порта для обмена данными с удаленным LDAP-сервером (не обязательно). | <pre>esr(config-ldap-server)# port <PORT></pre> | <p><PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].</p> <p>Значение по умолчанию: 389 для LDAP-сервера.</p> |
| 14 | Задать приоритет использования удаленного LDAP-сервера (не обязательно). | <pre>esr(config-ldap-server)# priority <PRIORITY></pre> | <p><PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535].</p> <p>Чем ниже значение, тем приоритетнее сервер.</p> <p>Значение по умолчанию: 1.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 15 | Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых LDAP-пакетах. | esr(config-ldap-server)# source-address { <ADDR> <IPv6-ADDR> } | <p><ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><IPv6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].</p> |
| 16 | Указать LDAP в качестве метода аутентификации. | esr(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <p><NAME> – имя списка, задаётся строкой до 31 символа.</p> <p>Способы аутентификации:</p> <ul style="list-style-type: none"> • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов. |
| 17 | Указать LDAP в качестве способа аутентификации повышения привилегий пользователей. | esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>] | <p><NAME> – имя списка строка до 31 символа;</p> <ul style="list-style-type: none"> • default – имя списка по умолчанию. <p><METHOD> – способы аутентификации:</p> <ul style="list-style-type: none"> • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 18 | Указать способ перебора методов аутентификации в случае отказа. | esr(config)# aaa authentication mode <MODE> | <p><MODE> – способы перебора методов:</p> <ul style="list-style-type: none"> • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. <p>Значение по умолчанию: chain.</p> |
| 19 | Перейти в режим конфигурирования соответствующего терминала. | esr(config)# line <TYPE> | <p><TYPE> – тип консоли:</p> <ul style="list-style-type: none"> • console – локальная консоль; • ssh – защищенная удаленная консоль. |
| 20 | Активировать список аутентификации входа пользователей в систему. | esr(config-line-console)# login authentication <NAME> | <p><NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 14.</p> |
| 21 | Активировать список аутентификации повышения привилегий пользователей. | esr(config-line-console)# enable authentication <NAME> | <p><NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 15.</p> |

1.7.5 Пример настройки аутентификации по telnet через RADIUS-сервер

Задача:

Настроить аутентификацию пользователей, подключающихся по Telnet, через RADIUS (192.168.16.1/24).

Решение:

Настроим подключение к RADIUS-серверу и укажем ключ (password):

```
esr# configure
esr(config)# radius-server host 192.168.16.1
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# exit
```

Создадим профиль аутентификации:

```
esr(config)# aaa authentication login log radius
```

Укажем режим аутентификации, используемый при подключении по Telnet-протоколу:

```
esr(config)# line telnet
esr(config-line-telnet)# login authentication log
esr(config-line-telnet)# exit
esr(config)# exit
```

Посмотреть информацию по настройкам подключения к RADIUS-серверу можно командой:

```
esr# show aaa radius-servers
```

Посмотреть профили аутентификации можно командой:

```
esr# show aaa authentication
```

1.8 Настройка привилегий команд

Настройка привилегий команд является гибким инструментом, который позволяет назначить набору команд минимально необходимый уровень пользовательских привилегий (1-15). В дальнейшем при создании пользователя можно задать уровень привилегий, определяя ему доступный набор команд.

- *1-9 уровни* – позволяют использовать все команды мониторинга (show ...);
- *10-14 уровни* – позволяют использовать все команды кроме команд перезагрузки устройства, управления пользователями и ряда других;
- *15 уровень* – позволяет использовать все команды.

1.8.1 Алгоритм настройки

Для изменения минимального уровня привилегий необходимого для выполнения команды CLI используется команда:

```
esr(config)# privilege <COMMAND-MODE> level <PRIV><COMMAND>
```

<COMMAND-MODE> – командный режим;

<PRIV> – необходимый уровень привилегий поддерева команд, принимает значение [1..15];

<COMMAND> – поддерево команд, задается строкой до 255 символов.

1.8.2 Пример настройки привилегий команд

Задача:

Перевести все команды просмотра информации об интерфейсах на уровень привилегий 10, кроме команды «show interfaces bridges». Команду «show interfaces bridges» перевести на уровень привилегий 3.

Решение:

В режиме конфигурирования определим команды, разрешенные на использование с уровнем привилегий 10 и уровнем привилегий 3:

```

esr(config)# privilege root level 3 "show interfaces bridge"
esr(config)# privilege root level 10 "show interfaces"

```

1.9 Настройка DHCP-сервера

Встроенный DHCP-сервер маршрутизатора может быть использован для настройки сетевых параметров устройств в локальной сети. DHCP-сервер маршрутизаторов способен передавать дополнительные опции на сетевые устройства, например:

- `default-router` – IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию;
- `domain-name` – доменное имя, которое должен будет использовать клиент при разрешении имен хостов через Систему Доменных Имен (DNS);
- `dns-server` – список адресов серверов доменных имен в данной сети, о которых должен знать клиент. Адреса серверов в списке располагаются в порядке убывания предпочтения.

1.9.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Включить IPv4/IPv6 DHCP-сервер. | esr(config)# ip dhcp-server [vrf <VRF>] | <VRF> – имя экземпляра VRF, в рамках которого будет работать DHCP-сервер. Задаётся строкой до 31 символа. |
| | | esr(config)# ipv6 dhcp-server [vrf <VRF>] | |
| 2 | Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера (не обязательно). | esr(config)# ip dhcp-server dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 61. |
| 3 | Создать пул IPv4/IPv6-адресов DHCP-сервера и перейти в режим его конфигурирования. | esr(config)# ip dhcp-server pool <NAME> [vrf <VRF>] | <NAME> – имя пула IPv4/IPv6-адресов DHCP-сервера, задаётся строка до 31 символа. <VRF> – имя экземпляра VRF, в рамках которого будет работать данный пул IP-адресов DHCP-сервера. Задаётся строкой до 31 символа |
| | | esr(config)# ipv6 dhcp-server pool <NAME> [vrf <VRF>] | |
| 4 | Задать IPv4/IPv6-адрес и маску для подсети, из которой будет выделен пул IPv4/IPv6-адресов. | esr(config-dhcp-server)# network <ADDR/LEN> | <ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| | | esr(config-ipv6-dhcp-server)# network <IPV6-ADDR/LEN> | <IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 5 | Добавить диапазон IPv4/IPv6-адресов к пулу адресов, конфигурируемого DHCP-сервера. | esr(config-dhcp-server)# address-range <FROM-ADDR>- <TO-ADDR> | <p><FROM-ADDR> – начальный IP-адрес диапазона;</p> <p><TO-ADDR> – конечный IP-адрес диапазона,</p> <p>Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> <p>Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую.</p> |
| | | esr(config-ipv6-dhcp-server)# address-range <FROM-ADDR>- <TO-ADDR> | <p><FROM-ADDR> – начальный IPv6-адрес диапазона;</p> <p><TO-ADDR> – конечный IP-адрес диапазона;</p> <p>Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].</p> |
| 6 | Добавить IPv4/IPv6-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера (не обязательно). | esr(config-dhcp-server)# address <ADDR> {mac-address <MAC> client-identifier <CI>} | <p><ADDR> – IP-адрес клиента, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><MAC> – MAC-адрес клиента, которому будет выдан IP-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].</p> <p><CI> – идентификатор клиента согласно DHCPOption61. Может быть задан в одном из следующих видов:</p> <ul style="list-style-type: none"> • HH:HH:HH:HH:HH:HH:HH: – идентификатор клиента в шестнадцатеричной форме и mac-адрес клиента; • STRING – текстовая строка длиной от 1 до 64 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| | | esr(config-ipv6-dhcp-server)# address <ADDR> mac-address <MAC> | <p><IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];</p> <p><MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]</p> |
| 7 | Задать список IPv4-адресов шлюзов по умолчанию, которые DHCP-сервер будет сообщать клиентам, используя DHCP-опцию 3. | esr(config-dhcp-server)# default-router <ADDR> | <ADDR> – IP-адрес шлюза по умолчанию, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую. |
| 8 | Задать DNS-имя сетевого домена. Имя домена передаётся клиентам в составе DHCP-опции 15 (не обязательно). | esr(config-dhcp-server)# domain-name <NAME> esr(config-ipv6-dhcp-server)# domain-name <NAME> | <NAME> – DNS-имя домена клиента, задаётся строкой до 255 символов. |
| 9 | Задать список IPv4/IPv6-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опции 6 (не обязательно). | esr(config-dhcp-server)# dns-server <ADDR> esr(config-ipv6-dhcp-server)# dns-server <IPV6-ADDR> | <p><ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую.</p> <p><IPV6-ADDR> – IPv6-адрес DNS-сервера, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов, список задаётся через запятую.</p> |
| 10 | Задать максимальное время аренды IP-адресов (не обязательно). Если DHCP-клиент запрашивает время аренды, превосходящее максимальное значение, то будет установлено время, заданное этой командой. | esr(config-dhcp-server)# max-lease-time <TIME> esr(config-ipv6-dhcp-server)# max-lease-time <TIME> | <p><TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где:</p> <ul style="list-style-type: none"> • DD – количество дней, принимает значения [0..364]; • HH – количество часов, принимает значения [0..23]; • MM – количество минут, принимает значения [0..59] <p>Значение по умолчанию: 1 день</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 11 | Задать время аренды, на которое клиенту будет выдан IP-адрес (не обязательно). Данное время будет использоваться если клиент не запрашивал определенное время аренды. | esr(config-dhcp-server)# default-lease-time <TIME> | <TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: <ul style="list-style-type: none"> • DD – количество дней, принимает значения [0..364]; • HH – количество часов, принимает значения [0..23]; • MM – количество минут, принимает значения [0..59] Значение по умолчанию: 12 часов. |
| | | esr(config-ipv6-dhcp-server)# default-lease-time <TIME> | |
| 12 | Создать идентификатор класса поставщика (DHCP Опция 60) (не обязательно). | esr(config)# ip dhcp-server vendor-class-id <NAME> | <NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа. |
| | | esr(config)# ipv6 dhcp-server vendor-class-id <NAME> | |
| 13 | Задать специфическую информацию поставщика (DHCP Опция 43). | esr(config-dhcp-vendor-id)# vendor-specific-options <HEX> | <HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 128 символов. |
| | | esr(config-ipv6-dhcp-vendor-id)# vendor-specific-options <HEX> | |
| 14 | Задать IP-адрес NetBIOS-сервера (DHCP опция 44) (не обязательно). | esr(config-dhcp-server)# netbios-name-server <ADDR> | <ADDR> – IP-адрес NetBIOS-сервера задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно задать до 4 IP-адресов. |
| 15 | Задать IP-адрес tftp-сервера (DHCP Option 150) (не обязательно). | esr(config-dhcp-server)# tftp-server <ADDR> | <ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

1.9.2 Пример настройки DHCP-сервера

Задача :

Настроить работу DHCP-сервера в локальной сети, относящейся к зоне безопасности «trusted». Задать пул IP-адресов из подсети 192.168.1.0/24 для раздачи клиентам. Задать время аренды адресов 1 день. Настроить передачу клиентам маршрута по умолчанию, доменного имени и адресов DNS-серверов с помощью DHCP-опций.

Решение:

Создадим зону безопасности «**trusted**» и установим принадлежность используемых сетевых интерфейсов к зонам:

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
```

Создадим пул адресов с именем «**Simple**» и добавим в данный пул адресов диапазон IP-адресов для выдачи в аренду клиентам сервера. Укажем параметры подсети, к которой принадлежит данный пул, и время аренды для выдаваемых адресов:

```
esr# configure
esr(config)# ip dhcp-server pool Simple
esr(config-dhcp-server)# network 192.168.1.0/24
esr(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
esr(config-dhcp-server)# default-lease-time 1:00:00
```

Сконфигурируем передачу клиентам дополнительных сетевых параметров:

- маршрут по умолчанию: 192.168.1.1;
- имя домена: eltex.loc;
- список DNS-серверов: DNS1: 172.16.0.1, DNS2: 8.8.8.8.

```
esr(config-dhcp-server)# domain-name "eltex.loc"
esr(config-dhcp-server)# default-router 192.168.1.1
esr(config-dhcp-server)# dns-server 172.16.0.1 8.8.8.8
esr(config-dhcp-server)# exit
```

Для того чтобы DHCP-сервер мог раздавать IP-адреса из конфигурируемого пула, на маршрутизаторе должен быть создан IP-интерфейс, принадлежащий к той же подсети, что и адреса пула.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone trusted
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit
```

Для разрешения прохождения сообщений протокола DHCP к серверу необходимо создать соответствующие профили портов, включающие порт источника 68 и порт назначения 67, используемые протоколом DHCP, и создать разрешающее правило в политике безопасности для прохождения пакетов протокола UDP:

```

esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 30
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port dhcp_client
esr(config-zone-rule)# match destination-port dhcp_server
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit

```

Разрешим работу сервера:

```

esr(config)# ip dhcp-server
esr(config)# exit

```

Просмотреть список арендованных адресов можно с помощью команды:

```

esr# show ip dhcp binding

```

Просмотреть сконфигурированные пулы адресов можно командами:

```

esr# show ip dhcp server pool
esr# show ip dhcp server pool Simple

```

 Конфигурирование настроек для IPv6 производится по аналогии с IPv4.

1.10 Конфигурирование Destination NAT

Функция Destination NAT (DNAT) состоит в преобразовании IP-адреса назначения у пакетов, проходящих через сетевой шлюз.

DNAT используется для перенаправления трафика, идущего на некоторый «виртуальный» адрес в публичной сети, на «реальный» сервер в локальной сети, находящийся за сетевым шлюзом. Эту функцию можно использовать для организации публичного доступа к серверам, находящимся в частной сети и не имеющим публичного сетевого адреса.

1.10.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|-------------------------------------|-------|
| 1 | Перейти в режим настройки сервиса трансляции адресов получателя. | esr(config)# nat destination | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 2 | Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно). | esr(config-dnat)# pool <NAME> | <NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа. |
| 3 | Установить внутренний IP-адрес, на который будет заменяться IP-адрес получателя. | esr(config-dnat-pool)# ip address <ADDR> | <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 4 | Установить внутренний TCP/UDP порт, на который будет заменяться TCP/UDP порт получателя. | esr(config-dnat-pool)# ip port <PORT> | <PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 5 | Создать группу правил с определённым именем. | esr(config-dnat)# ruleset <NAME> | <NAME> – имя группы правил, задаётся строкой до 31 символа. |
| 6 | Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно). | esr(config-dnat-ruleset)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 7 | Задать область применения группы правил. Правила будут применяться только для трафика, идущего из определенной зоны или интерфейса. | esr(config-dnat-ruleset)# from { zone <NAME> interface <IF> tunnel <TUN> default } | <NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; <TUN> – имя туннеля устройства; default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил. |
| 8 | Задать правило с определённым номером. Правила обрабатываются в порядке возрастания. | esr(config-dnat-ruleset)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1..10000]. |
| 9 | Задать профиль IP-адресов {отправителя получателя}, для которых должно срабатывать правило. | esr(config-dnat-rule)# match [not] ¹ {source destination}- address <OBJ-GROUP- NETWORK-NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. Значение «any» указывает на любой IP-адрес отправителя. |
| 10 | Задать профиль сервисов (tcp/udp-портов) {отправителя получателя}, для которых должно срабатывать правило (не обязательно). | esr(config-dnat-rule)# match [not] ¹ {source destination}- port <PORT-SET-NAME> | <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. Значение «any» указывает на любой TCP/UDP-порт отправителя. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 11 | Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно). | esr(config-dnat-rule)# match [not] ¹ {protocol <TYPE> protocol-id <ID> } | <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола. <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 12 | Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно). | esr(config-dnat-rule)# match [not] ¹ icmp {<ICMP_TYPE><ICMP_CODE> <TYPE-NAME>} | <ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]. <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения. <TYPE-NAME> – имя типа ICMP сообщения. |
| 13 | Задать действие «трансляция адреса и порта получателя» для трафика, удовлетворяющего критериям, заданным командами «match». | esr(config-dnat-rule)# action destination-nat { off pool <NAME> netmap <ADDR/LEN> } | off – трансляция отключена; pool <NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP портов; netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции. Параметр задается в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| 14 | Активировать конфигурируемое правило. | esr(config-dnat-rule)# enable | |

¹ При использовании ключа *not*, правило будет срабатывать для значений, которые не входят в указанный профиль

Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

Более подробная информация о командах для настройки маршрутизатора содержится в «Справочнике команд CLI».

1.10.2 Пример настройки Destination NAT

Задача:

Организовать доступ из публичной сети, относящейся к зоне «UNTRUST», к серверу локальной сети в зоне «TRUST». Адрес сервера в локальной сети – 10.1.1.100. Сервер должен быть доступным извне по адресу 1.2.3.4, доступный порт 80.



Рисунок 6 – Схема сети

Решение:

Создадим зоны безопасности «UNTRUST» и «TRUST». Установим принадлежность используемых сетевых интерфейсов к зонам. Одновременно назначим IP-адреса интерфейсам.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
```

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# ip address 10.1.1.1/25
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 1.2.3.4/29
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Создадим профили IP-адресов и портов, которые потребуются для настройки правил Firewall и правил DNAT.

- NET_UPLINK – профиль адресов публичной сети;
- SERVER_IP – профиль адресов локальной сети;
- SRV_HTTP – профиль портов.

```
esr(config)# object-group network NET_UPLINK
esr(config-object-group-network)# ip address 1.2.3.4
esr(config-object-group-network)# exit
```

```

esr(config)# object-group service SRV_HTTP
esr(config-object-group-service)# port 80
esr(config-object-group-service)# exit

```

```

esr(config)# object-group network SERVER_IP
esr(config-object-group-network)# ip address 10.1.1.100
esr(config-object-group-network)# exit

```

Войдем в режим конфигурирования функции DNAT и создадим пул адресов и портов назначения, в которые будут транслироваться адреса пакетов, поступающие на адрес 1.2.3.4 из внешней сети.

```

esr(config)# nat destination
esr(config-dnat)# pool SERVER_POOL
esr(config-dnat-pool)# ip address 10.1.1.100
esr(config-dnat-pool)# ip port 80
esr(config-dnat-pool)# exit

```

Создадим набор правил «DNAT», в соответствии с которыми будет производиться трансляция адресов. В атрибутах набора укажем, что правила применяются только для пакетов, пришедших из зоны «UNTRUST». Набор правил включает в себя требования соответствия данных по адресу и порту назначения (match destination-address, match destination-port) и по протоколу. Кроме этого в наборе задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat). Набор правил вводится в действие командой «enable».

```

esr(config-dnat)# ruleset DNAT
esr(config-dnat-ruleset)# from zone UNTRUST
esr(config-dnat-ruleset)# rule 1
esr(config-dnat-rule)# match destination-address NET_UPLINK
esr(config-dnat-rule)# match protocol tcp
esr(config-dnat-rule)# match destination-port SRV_HTTP
esr(config-dnat-rule)# action destination-nat pool SERVER_POOL
esr(config-dnat-rule)# enable
esr(config-dnat-rule)# exit
esr(config-dnat-ruleset)# exit
esr(config-dnat)# exit

```

Для пропуска трафика, идущего из зоны «UNTRUST» в «TRUST», создадим соответствующую пару зон. Пропускать следует только трафик с адресом назначения, соответствующим заданному в профиле «SERVER_IP» и прошедший преобразование DNAT.

```

esr(config)# security zone-pair UNTRUST TRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match destination-address SERVER_IP
esr(config-zone-pair-rule)# match destination-nat
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit

```

Произведенные настройки можно посмотреть с помощью команд:


```

esr# show ip nat destination pools
esr# show ip nat destination rulesets
esr# show ip nat proxy-arp
esr# show ip nat translations

```

1.11 Конфигурирование Source NAT

Функция Source NAT (SNAT) используется для подмены адреса источника у пакетов, проходящих через сетевой шлюз. При прохождении пакетов из локальной сети в публичную сеть, адрес источника заменяется на один из публичных адресов шлюза. Дополнительно к адресу источника может применяться замена порта источника. При прохождении пакетов из публичной сети в локальную происходит обратная подмена адреса и порта.

Функция SNAT может быть использована для предоставления доступа в Интернет компьютерам, находящимся в локальной сети. При этом не требуется назначения публичных IP-адресов этим компьютерам.

1.11.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 1 | Перейти в режим настройки сервиса трансляции адресов отправителя. | esr(config)# nat source | |
| 2 | Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно). | esr(config-snat)# pool <NAME> | <NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа. |
| 3 | Установить диапазон IP-адресов, для которых будет заменяться IP-адрес отправителя. | esr(config-snat-pool)# ip address-range <IP>[-<ENDIP>] | <IP> – IP-адрес начала диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ENDIP> – IP-адрес конца диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для трансляции используется только IP-адрес начала диапазона. |
| 4 | Задать диапазон внешних TCP/UDP портов, на которые будет заменяться TCP/UDP порт отправителя. | esr(config-snat-pool)# ip port-range <PORT>[-<ENDPORT>] | <PORT> – TCP/UDP порт начала диапазона, принимает значения [1..65535]; <ENDPORT> – TCP/UDP порт конца диапазона, принимает значения [1..65535]. Если не указывать TCP/UDP порт конца диапазона, то в качестве TCP/UDP порта для трансляции используется только TCP/UDP порт начала диапазона. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 5 | Установить внутренний TCP/UDP порт, на который будет заменяться TCP/UDP порт отправителя. | esr(config-snat-pool)# ip port <PORT> | <PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 6 | Включить функции NAT persistent. | esr(config-snat-pool)# persistent | |
| 7 | Создать группу правил с определённым именем. | esr(config-snat)# ruleset <NAME> | <NAME> – имя группы правил, задаётся строкой до 31 символа. |
| 8 | Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно). | esr(config-snat-ruleset)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 9 | Задать область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс. | esr(config-snat-ruleset)# to { zone <NAME> interface <IF> tunnel <TUN> default } | <NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; <TUN> – имя туннеля устройства default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил. |
| 10 | Задать правило с определённым номером. Правила обрабатываются в порядке возрастания. | esr(config-snat-ruleset)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1..10000]. |
| 11 | Задать профиль IP-адресов {отправителя получателя}, для которых должно срабатывать правило. | esr(config-snat-rule)# match [not] ¹ {source destination}-address <OBJ-GROUP-NETWORK-NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. Значение «any» указывает на любой IP-адрес отправителя. |
| 12 | Задать профиль IP-адресов {отправителя получателя}, для которых должно срабатывать правило (не обязательно). | esr(config-snat-rule)# match [not] ¹ {source destination}-port <PORT-SET-NAME> | <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. Значение «any» указывает на любой TCP/UDP-порт отправителя. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 13 | Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно). | esr(config-snat-rule)# match [not] ¹ {protocol protocol-id} <TYPE> | <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола; <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 14 | Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно). | esr(config-snat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> <TYPE-NAME>} | <ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения; <TYPE-NAME> – имя типа ICMP сообщения |
| 15 | Задать действие «трансляция адреса и порта отправителя» для трафика, удовлетворяющего критериям, заданным командами «match» | esr(config-snat-rule)# action source-nat { off pool <NAME> netmap <ADDR/LEN> [static] interface [FIRST_PORT – LAST_PORT] } | off – трансляция отключена; pool<NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP портов; netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции; static – опция для организации статического NAT. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. interface [FIRST_PORT – LAST_PORT] – задаёт трансляцию в IP-адрес интерфейса. Если дополнительно задан диапазон TCP/UDP-портов, то трансляция будет происходить только для TCP/UDP- портов отправителя, входящих в указанный диапазон. |
| 16 | Активировать конфигурируемое правило. | esr(config-snat-rule)# enable | |

¹ При использовании ключа not, правило будет срабатывать для значений, которые не входят в указанный профиль

Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

Более подробная информация о командах для настройки маршрутизатора содержится в «Справочнике команд CLI».

1.11.2 Пример настройки 1

Задача:

Настроить доступ пользователей локальной сети 10.1.2.0/24 к публичной сети с использованием функции Source NAT. Задать диапазон адресов публичной сети для использования SNAT 100.0.0.100-100.0.0.249.



Рисунок 7 – Схема сети

Решение :

Конфигурирование начнем с создания зон безопасности, настройки сетевых интерфейсов и определения их принадлежности к зонам безопасности. Создадим доверенную зону «TRUST» для локальной сети и зону «UNTRUST» для публичной сети.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
```

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 10.1.2.1/24
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 100.0.0.99/24
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Для конфигурирования функции SNAT и настройки правил зон безопасности потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL».

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
esr(config-object-group-network)# exit
```

```

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 100.0.0.100-100.0.0.249
esr(config-object-group-network)# exit

```

Для пропуска трафика из зоны «TRUST» в зону «UNTRUST» создадим пару зон и добавим правила, разрешающие проходить трафику в этом направлении. Дополнительно включена проверка адреса источника данных на принадлежность к диапазону адресов «LOCAL_NET» для соблюдения ограничения на выход в публичную сеть. Действие правил разрешается командой *enable*.

```

esr(config)# security zone-pair TRUST UNTRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match source-address LOCAL_NET
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

Конфигурируем сервис SNAT. Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT.

```

esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 100.0.0.100-100.0.0.249
esr(config-snat-pool)# exit

```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть – в зону «UNTRUST». Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET».

```

esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to zone UNTRUST
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit

```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL».

```

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL

```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 10.1.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды.

```
esr(config)# ip route 0.0.0.0/0 100.0.0.1
esr(config)# exit
```

1.11.3 Пример настройки 2

Задача:

Настроить доступ пользователей локальной сети 21.12.2.0/24 к публичной сети с использованием функции Source NAT без использования межсетевого экрана (firewall). Диапазон адресов публичной сети для использования SNAT 200.10.0.100-200.10.0.249.



Рисунок 8 – Схема сети

Решение:

Конфигурирование начнем с настройки сетевых интерфейсов и отключения межсетевого:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования функции SNAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 21.12.2.2-21.12.2.254
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.249
esr(config-object-group-network)# exit
```

Конфигурируем сервис SNAT.

Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT:

```

esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 200.10.0.100-200.10.0.249
esr(config-snat-pool)# exit

```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1. Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET»:

```

esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit

```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL»:

```

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL

```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды:

```

esr(config)# ip route 0.0.0.0/0 200.10.0.254
esr(config)# exit

```

1.12 Конфигурирование Static NAT

Static NAT – статический NAT задает однозначное соответствие одного адреса другому. Иными словами, при прохождении через маршрутизатор, адрес меняется на другой строго заданный адрес, один-к-одному. Запись о такой трансляции хранится неограниченно долго, пока не будет произведена перенастройка NAT на маршрутизаторе.

1.12.1 Алгоритм настройки

Настройка Static NAT осуществляется средствами Source NAT, алгоритм настройки которой описан в разделе [Конфигурирование Source NAT, алгоритм настройки](#) настоящего руководства.

1.12.2 Пример настройки Static NAT

Задача:

Настроить двухстороннюю и постоянную трансляцию из локальной сети для диапазона адресов 21.12.2.100-21.12.2.150 в публичную сеть 200.10.0.0/24. Диапазон адресов публичной сети для использования трансляции – 200.10.0.100-200.10.0.150.



Рисунок 9 – Схема сети

Решение :

Начнем конфигурирование с настройки сетевых интерфейсов и отключения межсетевого экрана:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования Static NAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий локальную подсеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip prefix 21.12.2.0/24
esr(config-object-group-network)# exit
```

```
esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip prefix 200.10.0.0/24
esr(config-object-group-network)# exit
```

Диапазон адресов публичной сети для использования Static NAT задаем в профиле «PROXY»:

```
esr(config)# object-group network PROXY
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.150
esr(config-object-group-network)# exit
```

Конфигурируем сервис Static NAT в режиме конфигурирования SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1.

Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET» и проверку адресов назначения на принадлежность к пулу «PUBLIC_POOL».

```
esr(config)# nat source
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# match destination-address PUBLIC_POOL
esr(config-snat-rule)# action source-nat netmap 200.10.0.0/24 static
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в пул трансляции «PROXY», необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов «PROXY».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PROXY
```

Для того чтобы устройства локальной сети могли получить доступ к сети 200.10.0.0/24, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

Изменения конфигурации вступают в действие по команде применения.

```
esr# commit
Configuration has been successfully committed
esr# confirm
Configuration has been successfully confirmed
```

Посмотреть активные трансляции можно с помощью команды:

```
esr# show ip nat translations
```

1.12.3 Пример настройки фильтрации приложений (DPI)

- ⚠ Использование механизма фильтрации приложений многократно снижает производительность маршрутизатора из-за необходимости проверки каждого пакета. Производительность снижается с ростом количества выбранных приложений для фильтрации.

Задача:

Блокировать доступ к ресурсам youtube, bittorrent и facebook.



Рисунок 10 – Схема сети

Решение:

Для каждой сети ESR создадим свою зону безопасности:

```
esr# configure
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-te)# ip address 192.168.0.1/24
esr(config-if-te)# security-zone LAN
esr(config-if-te)# exit
```

Для настройки правил зон безопасности потребуется создать профиль приложений, которые необходимо будет блокировать.

```
esr(config)# object-group application APP
esr(config-object-group-application)# application youtube
esr(config-object-group-application)# application bittorrent
esr(config-object-group-application)# application facebook
esr(config-object-group-application)# exit
```

Для установки правил прохождения трафика из зоны «WAN» в зону «LAN» создадим пару зон и добавим правило, запрещающее проходить трафику приложений, и правило, разрешающее проходить остальному трафику. Действие правил разрешается командой *enable*:

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action deny
esr(config-zone-pair-rule)# match application APP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit
```

Для установки правил прохождения трафика из зоны «LAN» в зону «WAN» создадим пару зон и добавим правило, разрешающее прохождение всего трафика. Действие правил разрешается командой *enable*:

```

esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit

```

Посмотреть членство портов в зонах можно с помощью команды:

```
esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```

esr# show security zone-pair
esr# show security zone-pair configuration

```

Посмотреть активные сессии можно с помощью команд:

```
esr# show ip firewall sessions
```

1.13 Проксирование HTTP/HTTPS-трафика

1.13.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Создать объект с URL | esr(config)# object-group url <NAME> | |
| 2 | Указать набор | esr(config-object-group-url)# url <URL> | <URL> – адрес веб страницы, сайта. |
| 3 | Создать профиль проксирования | esr(config)# ip http profile <NAME> | <NAME> – название профиля. |
| 4 | Выбрать действие по умолчанию | esr(config-profile)# default action {deny permit redirect} [redirect-url <URL>] | <URL> – адрес хоста, на который будут передаваться запросы. |
| 5 | Указать описание (не обязательно) | esr(config-profile)# description <description> | <description> – до 255 символов. |
| 6 | Указать удаленный или локальный список URL и тип операции (блокировка/ пропуск трафика/ перенаправление) (не обязательно) | esr(config-profile)# urls {local remote} <URL_OBJ_GROUP_NAME> action {deny permit redirect} [redirect-url <URL>] | <URL_OBJ_GROUP_NAME> – указать название объекта, содержащего набор URL. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 7 | Указать удаленный сервер, где лежат необходимые списки URL (не обязательно) | esr(config)# ip http proxy server-url <URL> | <URL> – адрес сервера, откуда будут брать удалённые списки url. |
| 8 | Указать прослушиваемый порт для проксирования (не обязательно) | esr(config)# ip http proxy listen-ports <OBJ_GROUP_NAME> | <OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа. |
| 9 | Указать прослушиваемый порт для проксирования (не обязательно) | esr(config)# ip https proxy listen-ports <OBJ_GROUP_NAME> | <OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа. |
| 10 | Включить проксирование на интерфейсе на основе выбранного HTTP-профиля | esr(config-if)# ip http proxy <PROFILE_NAME> | <PROFILE_NAME> – название профиля |
| 11 | Включить проксирование на интерфейсе на основе выбранного HTTPS-профиля | esr(config-if)# ip https proxy <PROFILE_NAME> | <PROFILE_NAME> – название профиля |
| 12 | Создать списки сервисов, которые будут использоваться при фильтрации. | esr(config)# object-group service <obj-group-name> | <obj-group-name> – имя профиля сервисов, задается строкой до 31 символа. |
| 13 | Задать описание списка сервисов (не обязательно). | esr(config-object-group-service)# description <description> | <description> – описание профиля, задается строкой до 255 символов. |
| 14 | Внести необходимые сервисы (tcp/udp порты) в список. | esr(config-object-group-service)# port-range 3129-3134 | Прокси-сервер ESR использует для своей работы порты 3129, 3130, 3133 и 3134. |
| 15 | Создать набор правил межзонового взаимодействия. | esr(config)# security zone-pair <src-zone-name1> self | <src-zone-name> – зона безопасности, в которой находятся интерфейсы с функцией ip http проху или ip https проху. self – предопределенная зона безопасности для трафика, поступающего на сам ESR. |
| 16 | Создать правило межзонового взаимодействия. | esr(config-zone-pair)# rule <rule-number> | <rule-number> – 1..10000. |
| 17 | Задать описание правила (не обязательно). | esr(config-zone-rule)# description <description> | <description> – до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 18 | Указать действие данного правила. | esr(config-zone-rule)# action <action> [log] | <action> – permit log – ключ для активации логирования сессий, которые устанавливаются согласно данному правилу. |
| 19 | Установить имя IP-протокола, для которого должно срабатывать правило | esr(config-zone-rule)# match protocol <protocol-type> | <protocol-type> – tcp Прокси-сервер ESR работает по протоколу ESR. |
| 20 | Установить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило (если указан протокол). | esr(config-zone-rule)# match [not]¹ destination-port <obj-group-name> | <obj-group-name> – имя профиля сервисов, созданного на шаге №12 |
| 21 | Включить правило межзонавого взаимодействия. | esr(config-zone-rule)# enable | |

⚠ Если функция Firewall на ESR принудительно не отключена, необходимо создать разрешающее правило для зоны Self.

1.13.2 Пример настройки HTTP-прокси

Задача:

Организовать фильтрацию по URL для ряда адресов посредством прокси.

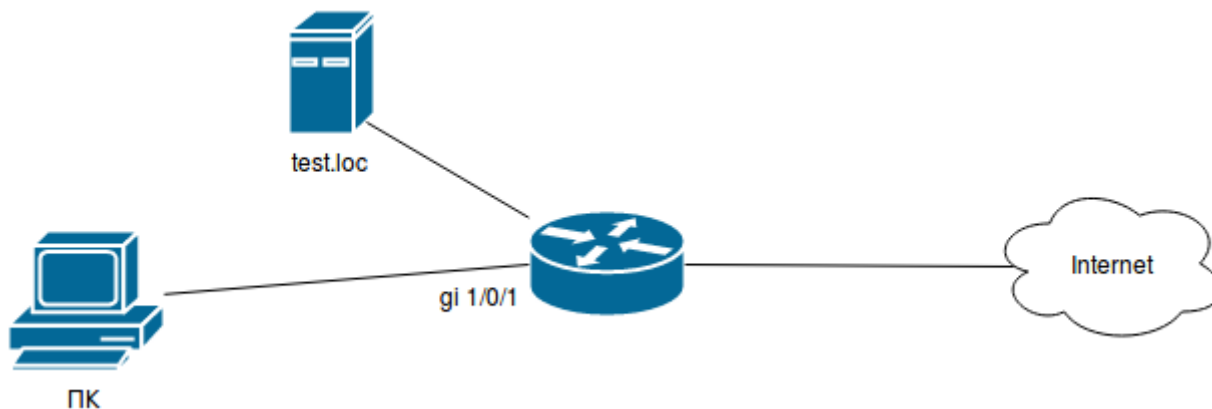


Рисунок 11 – Схема сети

Решение:

Создадим набор URL, по которым будет осуществляться фильтрация. Настроим прокси-фильтр и укажем действия для созданного набора URL:

```

esr# configure
esr(config)# object-group url test1
esr(config-object-group-url)# url http://speedtest.net/
esr(config-object-group-url)# url http://www.speedtest.net/
esr(config-object-group-url)# exit

```

Создаем профиль:

```

esr(config)# ip http profile list1
esr(config-profile)# default action permit
esr(config-profile)# urls local test1 action redirect redirect-url http://test.loc
esr(config-profile)# exit

```

Включим проксирование на интерфейсе по профилю 'list':

```

esr(config)# interface gi 1/0/1
esr(config-if)# ip http proxy list1

```

Если используется Firewall, создадим для него разрешающие правила:

Создаем профиль портов Прокси-сервера:

```

esr(config)# object-group service proxy
esr(config-object-group-service)# port-range 3129-3134
esr(config-object-group-service)# exit

```

Создаем разрешающее правило межзонового взаимодействия:

```

esr(config)# security zone-pair LAN self
esr(config-zone-pair)# rule 50
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match destination-port proxy
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

1.14 Настройка логирования и защиты от сетевых атак

1.14.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|-------------------------------------|---|--|
| 1 | Включить защиту от ICMP flood атак. | esr(config)# ip firewall screen dos-defense icmp-threshold { <NUM> } | <NUM> – количество ICMP-пакетов в секунду задается в диапазоне [1..10000]. |
| 2 | Включить защиту от land атак. | esr(config)# firewall screen dos-defense land | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 3 | Включить ограничение количества одновременных сессий на основании адреса назначения. | esr(config)# ip firewall screen dos-defense limit-session-destination { <NUM> } | <NUM> – ограничение количества IP-сессий задается в диапазоне [1..10000]. |
| 4 | Включить ограничение количества одновременных сессий на основании адреса источника, которое смягчает DoS-атаки. | esr(config)# ip firewall screen dos-defense limit-session-source { <NUM> } | <NUM> – ограничение количества IP-сессий задается в диапазоне [1..10000]. |
| 5 | Включить защиту от SYN flood атак. | esr(config)# ip firewall screen dos-defense syn-flood { <NUM> } [src-dsr] | <NUM> – максимальное количество TCP пакетов с установленным флагом SYN в секунду задается в диапазоне [1..10000]. src-dst – ограничение количества TCP пакетов с установленным флагом SYN на основании адреса источника и адреса назначения. |
| 6 | Включить защиту от UDP flood атак. | esr(config)# ip firewall screen dos-defense udp-threshold { <NUM> } | <NUM> – максимальное количество UDP пакетов в секунду задается в диапазоне [1..10000]. |
| 7 | Включить защиту от winnuke-атак. | esr(config)# ip firewall screen dos-defense winnuke | |
| 8 | Включить блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK. | esr(config)# ip firewall screen spy-blocking fin-no-ack | |
| 9 | Включить блокировку ICMP-пакетов различных типов. | esr(config)# ip firewall screen spy-blocking icmp-type | <TYPE> – тип ICMP, может принимать значения: <ul style="list-style-type: none"> • destination-unreachable • echo-request • reserved • source-quench • time-exceeded |
| 10 | Включить защиту от IP-sweep атак. | esr(config)# ip firewall screen spy-blocking ip-sweep { <NUM> } | <NUM> – интервал выявления ip sweep атаки, задается в миллисекундах [1..1000000]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 11 | Включить защиту от port scan атак. | esr(config)# ip firewall screen spy-blocking port-scan { <threshold> } [<TIME>] | <threshold> – интервал в миллисекундах, в течении которого будет фиксироваться port scan атака [1..1000000]. <TIME> – время блокировки в миллисекундах [1..1000000]. |
| 12 | Включить защиту от IP spoofing атак. | esr(config)# ip firewall screen spy-blocking spoofing | |
| 13 | Включить блокировку TCP-пакетов, с установленными флагами SYN и FIN. | esr(config)# ip firewall screen spy-blocking syn-fin | |
| 14 | Включить блокировку TCP-пакетов, со всеми флагами или с набором флагов: FIN, PSH, URG. Данной командой обеспечивается защита от атаки XMAS. | esr(config)# ip firewall screen spy-blocking tcp-all-flag | |
| 15 | Включить блокировку TCP-пакетов, с нулевым полем flags. | esr(config)# ip firewall screen spy-blocking tcp-no-flag | |
| 16 | Включить блокировку фрагментированных ICMP-пакетов. | esr(config)# ip firewall screen suspicious-packets icmp-fragment | |
| 17 | Включить блокировку фрагментированных IP пакетов. | esr(config)# ip firewall screen suspicious-packets ip-fragment | |
| 18 | Включить блокировку ICMP-пакетов длиной более 1024 байт. | esr(config)# ip firewall screen suspicious-packets icmp-fragment | |
| 19 | Включить блокировку фрагментированных TCP-пакетов, с флагом SYN. | esr(config)# ip firewall screen suspicious-packets syn-fragment | |
| 20 | Включить блокировку фрагментированных UDP-пакетов. | esr(config)# ip firewall screen suspicious-packets udp-fragment | |
| 21 | Включить блокировку пакетов, с ID протокола в заголовке IP равном 137 и более. | esr(config)# ip firewall screen suspicious-packets unknown-protocols | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 22 | Установить частоту оповещения (по SNMP, syslog и в CLI) об обнаруженных и отраженных сетевых атаках. | esr(config)# ip firewall logging interval <NUM> | <NUM> – интервал времени в секундах [30 .. 2147483647] |
| 23 | Включить более детальный вывод сообщений по обнаруженным и отраженным сетевым атакам в CLI. | esr(config)# logging firewall screen detailed | |
| 24 | Включить механизм обнаружения и логирования DoS атак через CLI, syslog и по SNMP. | esr(config)# logging firewall screen dos-defense <ATAK_TYPE> | <ATAK_TYPE> – тип DoS атаки, принимает значения: icmp-threshold, land, limit-session-destination, limit-session-source, syn-flood, udp-threshold, winnuke. |
| 25 | Включить механизм обнаружения и логирования шпионской активности через CLI, syslog и по SNMP | esr(config)# logging firewall screen spy-blocking { <ATAK_TYPE> icmp-type <ICMP_TYPE> } | <ATAK_TYPE> – тип шпионской активности, принимает значения: fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag. <ICMP_TYPE> – тип ICMP, принимает значения: destination-unreachable, echo-request, reserved, source-quench, time-exceeded. |
| 26 | Включить механизм обнаружения нестандартных пакетов и логирования через CLI, syslog и по SNMP | esr(config)# logging firewall screen suspicious-packets <PACKET_TYPE> | < PACKET_TYPE> – тип нестандартных пакетов, принимает значения: icmp-fragment, ip-fragment, large-icmp, syn-fragment, udp-fragment, unknown-protocols. |

1.14.2 Описание механизмов защиты от атак

| Команда | Описание |
|--|--|
| ip firewall screen dos-defense icmp-threshold | Данная команда включает защиту от ICMP flood атак. При включенной защите ограничивается количество ICMP-пакетов всех типов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый запрос и отвечать на него. |
| firewall screen dos-defense land | Данная команда включает защиту от land атак. При включенной защите блокируются пакеты с одинаковыми source и destination IP-адресами, и флагом SYN в заголовке TCP. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток хоста установить TCP сессию с самим собой. |

| Команда | Описание |
|--|---|
| ip firewall screen dos-defense limit-session-destination | Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение количества одновременных сессий на основании адреса назначения, которое смягчает DoS-атаки. |
| ip firewall screen dos-defense limit-session-source | Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение количества одновременных сессий на основании адреса источника, которое смягчает DoS-атаки. |
| ip firewall screen dos-defense syn-flood | Данная команда включает защиту от SYN flood атак. При включенной защите ограничивается количество TCP-пакетов с установленным флагом SYN в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток установить TCP-сессии. |
| ip firewall screen dos-defense udp-threshold | Данная команда включает защиту от UDP flood атак. При включенной защите ограничивается количество UDP пакетов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за массивного UDP-трафика. |
| ip firewall screen dos-defense winnuke | Данная команда включает защиту от winnuke атак. При включенной защите блокируются TCP-пакеты с установленным флагом URG и 139 портом назначения. Атака приводит к выходу из строя старых версий Windows (до 95 версии). |
| ip firewall screen spy-blocking fin-no-ack | Данная команда включает блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы. |
| ip firewall screen spy-blocking icmp-type destination-unreachable | Данная команда включает блокировку всех ICMP-пакетов 3 типа (destination-unreachable), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type echo-request | Данная команда включает блокировку всех ICMP-пакетов 8 типа (echo-request), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type reserved | Данная команда включает блокировку всех ICMP-пакетов 2 и 7 типов (reserved), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type source-quench | Данная команда включает блокировку всех ICMP-пакетов 4 типа (source quench), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type time-exceeded | Данная команда включает блокировку всех ICMP-пакетов 11 типа (time exceeded), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |

| Команда | Описание |
|--|---|
| ip firewall screen spy-blocking ip-sweep | Данная команда включает защиту от IP-sweep атак. При включенной защите, если в течение заданного в параметрах интервала приходит более 10 ICMP-запросов от одного источника, первые 10 запросов пропускаются маршрутизатором, а 11 и последующие отбрасываются на оставшееся время интервала. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов. |
| ip firewall screen spy-blocking port-scan | Данная команда включает защиту от port scan атак. Если в течение первого заданного интервала времени (<threshold>) на один источник приходит более 10 TCP-пакетов с флагом SYN на разные TCP-порты, то такое поведение фиксируется как port scan атака и все последующие пакеты такого рода от источника блокируются на второй заданный интервал времени (<TIME>). Злоумышленник не сможет быстро просканировать открытые порты на устройстве. |
| ip firewall screen spy-blocking spoofing | Данная команда включает защиту от ip spoofing атак. При включенной защите маршрутизатор проверяет пакеты на соответствие адреса источника и записей в таблице маршрутизации и в случае несоответствия пакет отбрасывается. Например, если пакет с адресом источника 10.0.0.1/24 приходит на интерфейс Gi1/0/1, а в таблице маршрутизации данная подсеть располагается за интерфейсом Gi1/0/2, то считается, что адрес источника был подменен. Защищает от вторжений в сеть с подмененными source IP-адресами. |
| ip firewall screen spy-blocking syn-fin | Данная команда включает блокировку TCP-пакетов с установленными флагами SYN и FIN. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы. |
| ip firewall screen spy-blocking tcp-all-flag | Данная команда включает блокировку TCP-пакетов со всеми флагами или с набором флагов: FIN, PSH, URG. Обеспечивается защита от атаки XMAS. |
| ip firewall screen spy-blocking tcp-no-flag | Данная команда включает блокировку TCP-пакетов с нулевым полем flags. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы. |
| ip firewall screen suspicious-packets icmp-fragment | Данная команда включает блокировку фрагментированных ICMP-пакетов. ICMP-пакеты обычно небольшого размера и необходимости в их фрагментации нет. |
| ip firewall screen suspicious-packets ip-fragment | Данная команда включает блокировку фрагментированных пакетов. |
| ip firewall screen suspicious-packets large-icmp | Данная команда включает блокировку ICMP-пакетов длиной более 1024 байт. |
| ip firewall screen suspicious-packets syn-fragment | Данная команда включает блокировку фрагментированных TCP-пакетов с флагом SYN. TCP пакеты с SYN флагом обычно небольшого размера и необходимости в их фрагментации нет. Защита предотвращает накопление фрагментированных пакетов в буфере. |

| Команда | Описание |
|--|---|
| <code>ip firewall screen suspicious-packets udp-fragment</code> | Данная команда включает блокировку фрагментированных UDP-пакетов. |
| <code>ip firewall screen suspicious-packets unknown-protocols</code> | Данная команда включает блокировку пакетов, с ID протокола в заголовке IP равном 137 и более. |

1.14.3 Пример настройки логирования и защиты от сетевых атак

Задача:

Необходимо защитить LAN сеть и маршрутизатор ESR от сетевых атак land, syn-flood, ICMP flood и настроить оповещение об атаках по SNMP на SNMP-сервер 192.168.0.10.



Рисунок 12 – Схема сети

Решение:

Предварительно необходимо настроить интерфейсы и firewall (настройка firewall или ее отсутствие не повлияют на работу защиты от сетевых атак):

```

esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit

```

Настроим защиту от land, syn-flood, ICMP flood атак:

```

esr(config)# ip firewall screen dos-defense land
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dst
esr(config)# ip firewall screen dos-defense icmp-threshold 100

```

Настроим логирование обнаруженных атак:

```

esr(config)# ip firewall logging screen dos-defense land
esr(config)# ip firewall logging screen dos-defense syn-flood
esr(config)# ip firewall logging screen dos-defense icmp-threshold

```

Настроим SNMP-сервер, на который будут отправляться трапы:

```

esr(config)# snmp-server
esr(config)# snmp-server host 192.168.0.10

```

Посмотреть статистику по зафиксированным сетевым атакам можно командой:

```

esr# show ip firewall screen counters

```

1.15 Конфигурирование Firewall

Firewall – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

1.15.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 1 | Создать зоны безопасности. | esr(config)# security zone <zone-name1> esr(config)# security zone <zone-name2> | <zone-name> – до 12 символов. |
| 2 | Задать описание зоны безопасности. | esr(config-zone)# description <description> | <description> – до 255 символов. |
| 3 | Указать экземпляр VRF, в котором будет работать данная зона безопасности (не обязательно). | esr(config- zone)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Включить счетчики сессий для NAT и Firewall (не обязательно, снижает производительность). | esr(config)# ip firewall sessions counters | |
| 5 | Отключить фильтрацию пакетов, для которых не удалось определить принадлежность к какому-либо известному соединению и которые не являются началом нового соединения (не обязательно, снижает производительность). | esr(config)# ip firewall sessions allow-unknown | |
| 6 | Выбрать режима работы межсетевого экрана (не обязательно) | esr(config)# ip firewall mode <MODE> | <MODE> – режим работы межсетевого экрана, может принимать значения: stateful, stateless. Значение по умолчанию: stateful |
| 7 | Определить время жизни сессии для неподдерживаемых протоколов (не обязательно). | esr(config)# ip firewall sessions generic-timeout <TIME> | <TIME> – время жизни сессии для неподдерживаемых протоколов, принимает значения в секундах [1..8553600]. По умолчанию: 60 секунд. |
| 8 | Определить время жизни ICMP-сессии, по истечении которого она считается устаревшей (не обязательно). | esr(config)# ip firewall sessions icmp-timeout <TIME> | <TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд. |
| 9 | Определить время жизни ICMPv6-сессии, по истечении которого она считается устаревшей (не обязательно). | esr(config)# ip firewall sessions icmpv6-timeout <TIME> | <TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 10 | Определить размер таблицы сессий ожидающих обработки (не обязательно). | esr(config)# ip firewall sessions max-expect <COUNT> | <COUNT> – размер таблицы, принимает значения [1..8553600]. По умолчанию: 256. |
| 11 | Определить размер таблицы отслеживаемых сессий (не обязательно). | esr(config)# ip firewall sessions max-tracking <COUNT> | <COUNT> – размер таблицы, принимает значения [1..8553600]. По умолчанию: 512000. |
| 12 | Определить время жизни TCP-сессии в состоянии «соединение устанавливается», по истечении которого она считается устаревшей (не обязательно). | esr(config)# ip firewall sessions tcp-connect-timeout <TIME> | <TIME> – время жизни TCP-сессии в состоянии "соединение устанавливается", принимает значения в секундах [1..8553600]. По умолчанию: 60 секунд. |
| 13 | Определить время жизни TCP-сессии в состоянии "соединение закрывается", по истечении которого она считается устаревшей (не обязательно). | esr(config)# ip firewall sessions tcp-disconnect-timeout <TIME> | <TIME> – время жизни TCP-сессии в состоянии "соединение закрывается", принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд. |
| 14 | Определить время жизни TCP-сессии в состоянии "соединение установлено", по истечении которого она считается устаревшей (не обязательно). | esr(config)# ip firewall sessions tcp-established-timeout <TIME> | <TIME> – время жизни TCP-сессии в состоянии "соединение установлено", принимает значения в секундах [1..8553600]. По умолчанию: 120 секунд. |
| 15 | Определить время ожидания, по истечении которого происходит фактическое удаление закрытой TCP-сессии из таблицы отслеживаемых сессий (не обязательно). | esr(config)# ip firewall sessions tcp-latecome-timeout <TIME> | <TIME> – время ожидания, принимает значения в секундах [1..8553600]. По умолчанию: 120 секунд. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 16 | Включить функцию отслеживания сессий уровня приложений для отдельных протоколов (не обязательно). | esr(config)# ip firewall sessions tracking e; | <p><PROTOCOL> – протокол уровня приложений [ftp, h323, pptp, netbios-ns, tftp], сессии которого должны отслеживаться.</p> <p><ОБЪЕКТ-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.</p> <p>Вместо имени отдельного протокола можно использовать ключ "all", который включает функцию отслеживания сессий уровня приложений для всех доступных протоколов.</p> <p>По умолчанию – отключено для всех протоколов.</p> |
| 17 | Определить время жизни UDP-сессии в состоянии "соединение подтверждено", по истечении которого она считается устаревшей (не обязательно). | esr(config)# ip firewall sessions udp-assured-timeout <TIME> | <p><TIME> – время жизни UDP-сессии в состоянии "соединение подтверждено", принимает значения в секундах [1..8553600].</p> <p>По умолчанию: 180 секунд.</p> |
| 18 | Определить время жизни UDP-сессии в состоянии «соединение не подтверждено», по истечении которого она считается устаревшей. | esr(config)# ip firewall sessions udp-wait-timeout <TIME> | <p><TIME> – время жизни UDP-сессии в состоянии «соединение не подтверждено», принимает значения в секундах [1..8553600].</p> <p>По умолчанию: 30 секунд.</p> |
| 19 | Создать списки IP-адресов, которые будут использоваться при фильтрации. | esr(config)# object-group network <obj-group-name> | <obj-group-name> – до 31 символа. |
| 20 | Задать описание списка IP-адресов (не обязательно). | esr(config-object-group-network)# description <description> | <description> – описание профиля, задаётся строкой до 255 символов. |
| 21 | Внести необходимые IPv4/IPv6-адреса в список. | esr(config-object-group-network)# ip prefix <ADDR/LEN> | <ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| | | esr(config-object-group-network)# ip address-range <FROM-ADDR>-<TO-ADDR> | <p><FROM-ADDR> – начальный IP-адрес диапазона адресов;</p> <p><TO-ADDR> – конечный IP-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IP-адрес.</p> <p>Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> |
| | | esr(config-object-group-network)# ipv6 prefix <IPV6-ADDR/LEN> | <p><IPV6-ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].</p> |
| | | esr(config-object-group-network)# ipv6 address-range <FROM-ADDR>-<TO-ADDR> | <p><FROM-ADDR> – начальный IPv6-адрес диапазона адресов;</p> <p><TO-ADDR> – конечный IPv6-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IPv6-адрес.</p> <p>Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].</p> |
| 22 | Создать списки сервисов, которые будут использоваться при фильтрации. | esr(config)# object-group service <obj-group-name> | <obj-group-name> – имя профиля сервисов, задаётся строкой до 31 символа. |
| 23 | Задать описание списка сервисов (не обязательно). | esr(config-object-group-service)# description <description> | <description> – описание профиля, задаётся строкой до 255 символов. |
| 24 | Внести необходимые сервисы (tcp/udp порты) в список. | esr(config-object-group-service)# port-range <port> | <p><port> – принимает значение [1..65535].</p> <p>Можно указать несколько портов перечислением через запятую «,» либо указать диапазон портов через «-».</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 25 | Создать списки приложений, которые будут использоваться в механизме DPI. | esr(config)# object-group application <NAME> | <NAME> – имя профиля приложений, задается строкой до 31 символа. |
| 26 | Задать описание списка приложений (не обязательно). | esr(config-object-group application)# description <description> | <description> – описание профиля, задается строкой до 255 символов. |
| 27 | Внести необходимые приложения в списки. | esr(config-object-group application)# application <APPLICATION > | < APPLICATION > – указывает приложение подпадающее под действие данного профиля |
| 28 | Включить интерфейсы (физические, логические, E1/Multilink и подключаемые), сервер удаленного доступа (l2tp, openvpn, pptp) или туннели (gre, ip4ip4, l2tp, lt, pppoe, pptp) в зоны безопасности (если необходимо). | esr(config-if-gi)# security-zone <zone-name> | <zone-name> – до 12 символов. |
| | Отключить функции Firewall на сетевом интерфейсе (физические, логические, E1/Multilink и подключаемые), сервере удаленного доступа (l2tp, openvpn, pptp) или туннели (gre, ip4ip4, l2tp, lt, pppoe, pptp) (если необходимо) | esr(config-if-gi)# ip firewall disable | |
| 29 | Создать набор правил межзонового взаимодействия. | esr(config)# security zone-pair <src-zone-name1> <dst-zone-name2> | <src-zone-name> – до 12 символов. <dst-zone-name> – до 12 символов. |
| 30 | Создать правило межзонового взаимодействия. | esr(config-zone-pair)# rule <rule-number> | <rule-number> – 1..10000. |
| 31 | Задать описание правила (не обязательно). | esr(config-zone-rule)# description <description> | <description> – до 255 символов. |
| 32 | Указать действие данного правила. | esr(config-zone-rule)# action <action> [log] | <action> – permit/deny/reject/netflow-sample/sflow-sample log – ключ для активации логирования сессий, устанавливаемым согласно данному правилу. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 33 | Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно). | esr(config-zone-rule)# match [not] ¹ protocol <protocol-type> | <protocol-type> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов. |
| | | esr(config-zone-rule)# match [not] ¹ protocol-id <protocol-id> | <protocol-id> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 34 | Установить профиль IP-адресов отправителя, для которых должно срабатывать правило (не обязательно). | esr(config-zone-rule)# match [not] ¹ source-address <OBJ-GROUP-NETWORK-NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя. |
| 35 | Установить профиль IP-адресов получателя, для которых должно срабатывать правило (не обязательно). | esr(config-zone-rule)# match [not] ¹ destination-address <OBJ-GROUP-NETWORK-NAME> | |
| 36 | Установить MAC-адрес отправителя, для которого должно срабатывать правило (не обязательно). | esr(config-zone-rule)# match [not] ¹ source-mac <mac-addr> | <mac-addr> – задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. |
| 37 | Установить MAC-адрес получателя, для которого должно срабатывать правило (не обязательно). | esr(config-zone-rule)# match [not] ¹ destination-mac <mac-addr> | |
| 38 | Установить профиль TCP/UDP-портов отправителя, для которых должно срабатывать правило (если указан протокол). | esr(config-zone-rule)# match [not] ¹ source-port <PORT-SET-NAME> | <PORT-SET-NAME> – задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя/получателя. |
| 39 | Установить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило (если указан протокол). | esr(config-zone-rule)# match [not] ¹ destination-port <PORT-SET-NAME> | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 40 | Установить тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно). | esr(config-zone-rule)# match [not] ¹ icmp <ICMP_TYPE> <ICMP_CODE> | <ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP. |
| 41 | Установить ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя. | esr(config-zone-rule)# match [not] ¹ destination-nat | |
| 42 | Установить максимальную скорость прохождения пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any). | esr(config-zone-pair-rule)# rate-limit pps <rate-pps> | <rate-pps> – максимальное количество пакетов, которое может быть передано. Принимает значения [1..10000]. |
| 43 | Установить фильтрацию только для фрагментированных IP-пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any). | esr(config-zone-pair-rule)# match [not] ¹ fragment | |
| 44 | Установить фильтрацию для IP-пакетов, содержащих ip-option (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any). | esr(config-zone-pair-rule)# match [not] ¹ ip-option | |
| 45 | Включить правило межзонового взаимодействия. | esr(config-zone-rule)# enable | |
| 46 | Активировать фильтрацию и режим отслеживания сессий при прохождении пакетов между участниками одной Bridge-группы (не обязательно, доступно только на ESR-1000/1200/1500/1510/1700) | esr(config-bridge)# ports firewall enable | |

¹ При использовании ключа not, правило будет срабатывать для значений, которые не входят в указанный профиль.

Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

Более подробная информация о командах для настройки межсетевого экрана содержится в «Справочнике команд CLI».

1.15.2 Пример настройки Firewall

Задача:

Разрешить обмен сообщениями по протоколу ICMP между устройствами R1, R2 и маршрутизатором ESR.

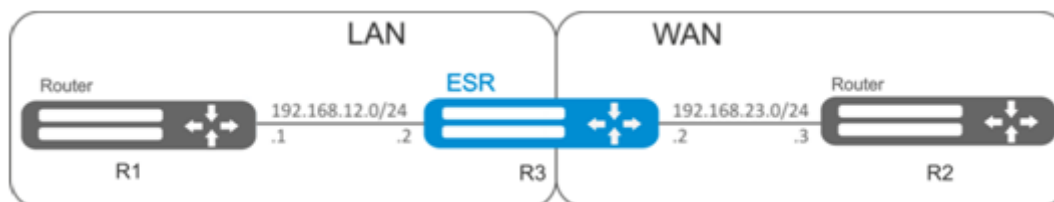


Рисунок 13 – Схема сети

Решение:

Для каждой сети ESR создадим свою зону безопасности:

```
esr# configure
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# ip address 192.168.12.2/24
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# exit
esr(config)# interface gi1/0/3
esr(config-if-gi)# ip address 192.168.23.2/24
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# exit
```

Для настройки правил зон безопасности потребуется создать профиль адресов сети «LAN», включающий адреса, которым разрешен выход в сеть «WAN», и профиль адресов сети «WAN».

```

esr(config)# object-group network WAN
esr(config-object-group-network)# ip address-range 192.168.23.2
esr(config-object-group-network)# exit
esr(config)# object-group network LAN
esr(config-object-group-network)# ip address-range 192.168.12.2
esr(config-object-group-network)# exit
esr(config)# object-group network LAN_GATEWAY
esr(config-object-group-network)# ip address-range 192.168.12.1
esr(config-object-group-network)# exit
esr(config)# object-group network WAN_GATEWAY
esr(config-object-group-network)# ip address-range 192.168.23.3
esr(config-object-group-network)# exit

```

Для пропуска трафика из зоны «LAN» в зону «WAN» создадим пару зон и добавим правило, разрешающее проходить ICMP-трафику от R1 к R2. Действие правил разрешается командой *enable*:

```

esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN_GATEWAY
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit

```

Для пропуска трафика из зоны «WAN» в зону «LAN» создадим пару зон и добавим правило, разрешающее проходить ICMP-трафику от R2 к R1. Действие правил разрешается командой *enable*:

```

esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN_GATEWAY
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

На маршрутизаторе всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам маршрутизатор, то есть трафик не является транзитным, то в качестве параметра указывается зона «self». Создадим пару зон для трафика, идущего из зоны «WAN» в зону «self». Добавим правило, разрешающее проходить ICMP-трафику между R2 и маршрутизатором ESR, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «WAN»:

```

esr(config)# security zone-pair WAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

Создадим пару зон для трафика, идущего из зоны «LAN» в зону «self». Добавим правило, разрешающее проходить ICMP-трафику между R1 и ESR, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «LAN»:

```
esr(config)# security zone-pair LAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

Посмотреть членство портов в зонах можно с помощью команды:

```
esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```
esr# show security zone-pair
esr# show security zone-pair configuration
```

Посмотреть активные сессии можно с помощью команд:

```
esr# show ip firewall sessions
```

1.16 Настройка списков доступа (ACL)

Access Control List или ACL – список контроля доступа, содержит правила, определяющие прохождение трафика через интерфейс.

1.16.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Создать список контроля доступа и перейти в режим его конфигурирования. | esr(config)# ip access-list extended <NAME> | <NAME> – имя создаваемого списка контроля доступа, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигурируемого списка контроля доступа (не обязательно). | esr(config-acl)# description <DESCRIPTION> | <DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов. |
| 3 | Создать правило и перейти в режим его конфигурирования. Правила обрабатываются маршрутизатором в порядке возрастания их номеров. | esr(config-acl)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1..4094]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 4 | Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям. | esr(config-acl-rule)# action <ACT> | <ACT> – назначаемое действие: <ul style="list-style-type: none"> • permit – прохождение трафика разрешается; • deny – прохождение трафика запрещается. |
| 5 | Установить имя/номер протокола, для которого должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match protocol <TYPE> | <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов; |
| | | esr(config-acl-rule)# match protocol-id <ID> | <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 6 | Установить IP-адреса отправителя, для которых должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match source-address { <ADDR> <MASK> any } | <ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; |
| 7 | Установить IP-адреса получателя, для которых должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match destination-address { <ADDR> <MASK> any } | <MASK> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя. |
| 8 | Установить MAC-адреса отправителя, для которых должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match source-mac <ADDR><WILDCARD> | <ADDR> – MAC-адрес отправителя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]; |
| 9 | Установить MAC-адреса получателя, для которых должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match destination-mac <ADDR><WILDCARD> | <WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске. |
| 10 | Установить номер TCP/UDP-порта отправителя, для которого должно срабатывать правило (если указан протокол). | esr(config-acl-rule)# match source-port { <PORT> any } | <PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 11 | Установить номер TCP/UDP-порта получателя, для которого должно срабатывать правило (если указан протокол). | esr(config-acl-rule)# match destination-port { <PORT> any } | |
| 12 | Установить значение 802.1p приоритета, для которого должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match cos <COS> | <COS> – значение 802.1p приоритета, принимает значения [0..7]. |
| 13 | Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с IP Precedence. | esr(config-acl-rule)# match dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения [0..63]. |
| 14 | Установить значение кода IP Precedence, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с DSCP. | esr(config-acl-rule)# match ip-precedence <IPP> | <IPP> – значение кода IP Precedence, принимает значения [0..7]. |
| 15 | Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (не обязательно). | esr(config-acl-rule)# match vlan <VID> | <VID> – идентификационный номер VLAN, принимает значения [1..4094]. |
| 16 | Активировать правило. | esr(config-acl-rule)# enable | |
| 17 | Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика. | esr(config-if-gi)# service-acl input <NAME> | <NAME> – имя списка контроля доступа, задаётся строкой до 31 символа. |

Также списки доступа могут использоваться для организации политик QoS.

1.16.2 Пример настройки списка доступа

Задача:

Разрешить прохождения трафика только из подсети 192.168.20.0/24.

Решение:

Настроим список доступа для фильтрации по подсетям:

```

esr# configure
esr(config)# ip access-list extended white
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match source-address 192.168.20.0 255.255.255.0
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit

```

Применим список доступа на интерфейс Gi1/0/19 для входящего трафика:

```

esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# service-acl input white

```

Посмотреть детальную информацию о списке доступа возможно через команду:

```

esr# show ip access-list white

```

1.17 Конфигурирование статических маршрутов

Статическая маршрутизация – вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора без использования протоколов динамической маршрутизации.

1.17.1 Процесс настройки

Добавить статический маршрут возможно командой в режиме глобальной конфигурации:

```

esr(config)# ip route [ vrf <VRF> ] <SUBNET> { <NEXTHop> | interface <IF> | tunnel <TUN> | wan load-balance rule <RULE> [ <METRIC> ] | blackhole | unreachable | prohibit } [ <METRIC> ] [ track <TRACK-ID> ] [ bfd ]

```

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующем формате:
 - AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];
 - AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].
- <NEXTHop> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
- <IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе [Типы и порядок именования интерфейсов маршрутизатора](#);
- <TUN> – имя туннеля, задаётся в виде, описанном в разделе [Типы и порядок именования туннелей маршрутизатора](#);
- <RULE> – номер правила wan, задаётся в диапазоне [1..50];
- blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop.

Для добавления статического IPv6-маршрута к указанной подсети используется команда:

```
ipv6 route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> [ resolve ] | interface <IF> | wan load-balance rule <RULE> |
blackhole | unreachable | prohibit } [ <METRIC> ] [ bfd ]
```

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующих видах:
 - X:X:X:X – IPv6-адрес хоста, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
 - X:X:X:X/EE – IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
- <NEXTHOP> – IPv6-адрес шлюза, задается в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
- resolve – при указании данного параметра IPv6-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;
- <IF> – имя IP-интерфейса, задается в виде, описанном в разделе [Типы и порядок именования интерфейсов маршрутизатора](#);
- blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- [METRIC] – метрика маршрута, принимает значения [0..255].
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop.

1.17.2 Пример настройки статических маршрутов

Задача:

Настроить доступ к сети Internet для пользователей локальных сетей 192.168.1.0/24 и 10.0.0.0/8, используя статическую маршрутизацию. На устройстве R1 создать шлюз для доступа к сети Internet. Трафик внутри локальной сети должен маршрутизироваться внутри зоны LAN, трафик из сети Internet должен относиться к зоне WAN.

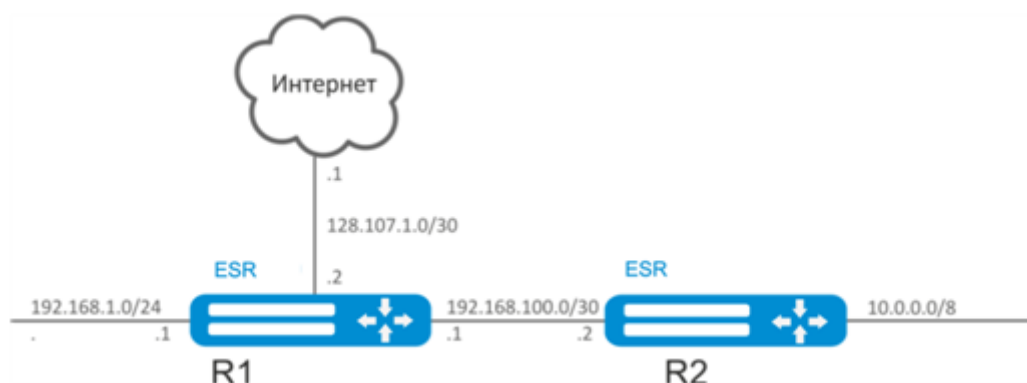


Рисунок 14 – Схема сети

Решение:

Зададим имя устройства для маршрутизатора R1:

```
esr# hostname R1
```

Для интерфейса gi1/0/1 укажем адрес 192.168.1.1/24 и зону «LAN». Через данный интерфейс R1 будет подключен к сети 192.168.1.0/24:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit
```

Для интерфейса gi1/0/2 укажем адрес 192.168.100.1/30 и зону «LAN». Через данный интерфейс R1 будет подключен к устройству R2 для последующей маршрутизации трафика:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.100.1/30
esr(config-if-gi)# exit
```

Для интерфейса gi1/0/3 укажем адрес 128.107.1.2/30 и зону «WAN». Через данный интерфейс R1 будет подключен к сети Internet:

```
esr(config)# interface gi1/0/3
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 128.107.1.2/30
esr(config-if-gi)# exit
```

Создадим маршрут для взаимодействия с сетью 10.0.0.0/8, используя в качестве шлюза устройство R2 (192.168.100.2):

```
esr(config)# ip route 10.0.0.0/8 192.168.100.2
```

Создадим маршрут для взаимодействия с сетью Internet, используя в качестве nexthop шлюз провайдера (128.107.1.1):

```
esr(config)# ip route 0.0.0.0/0 128.107.1.1
```

Зададим имя устройства для маршрутизатора R2:

```
esr# hostname R2
```

Для интерфейса gi1/0/1 укажем адрес 10.0.0.1/8 и зону «LAN». Через данный интерфейс R2 будет подключен к сети 10.0.0.0/8:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 10.0.0.1/8
esr(config-if-gi)# exit
```

Для интерфейса gi1/0/2 укажем адрес 192.168.100.2/30 и зону «LAN». Через данный интерфейс R2 будет подключен к устройству R1 для последующей маршрутизации трафика:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.100.2/30
esr(config-if-gi)# exit
```

Создадим маршрут по умолчанию, указав в качестве nexthop IP-адрес интерфейса gi1/0/2 маршрутизатора R1 (192.168.100.1):

```
esr(config)# ip route 0.0.0.0/0 192.168.100.1
```

Проверить таблицу маршрутов можно командой:

```
esr# show ip route
```

1.18 Настройка PPP через E1

PPP (Point-to-Point Protocol) – двухточечный протокол канального уровня, используется для установления прямой связи между двумя узлами сети. Может обеспечить аутентификацию соединения, шифрование и сжатие данных.

Для установления PPP-соединения через поток E1, необходимо наличие медиаконвертера ToPGATE-SFP в маршрутизаторе ESR.

1.18.1 Процесс настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 1 | Перевести физический интерфейс в режим коммутации | esr(config-if-gi)# mode switchport | |
| 2 | Задать режим работы интерфейса e1 | esr(config-if-gi)# switchport mode e1 | |
| 3 | Задать источник синхронизации | esr(config-if-gi)# switchport e1 clock source <SOURCE> | <SOURCE> – источник синхронизации: <ul style="list-style-type: none"> • Internal (по умолчанию) – синхронизироваться с внутренним источником; • line – синхронизироваться с линейным сигналом. |
| 4 | Указать размер MTU (Maximum Transmission Unit) для физических интерфейсов | esr(config-if-gi)# mtu <MTU> | <MTU> – значение MTU, для E1 и Multilink интерфейсов принимает значения в диапазоне [128..1500]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 5 | Задать хэш-алгоритм проверки кадра (не обязательно) | esr(config-if-gi)# switchport e1 crc <FCS> | <FCS> – последовательность проверки кадра: <ul style="list-style-type: none"> • 16 (по умолчанию) – FCS16; • 32 – FCS32. |
| 6 | Задать проверку на наличие ошибок при передаче (не обязательно) | esr(config-if-gi)# switchport e1 framing <CRC> | <CRC> – проверка циклической избыточности: <ul style="list-style-type: none"> • crc-4 – использовать алгоритм CRC-4; • no-crc4 (по умолчанию) – не использовать проверку. |
| 7 | Задать инвертацию передаваемых бит (не обязательно) | esr(config-if-gi)# switchport e1 invert data | |
| 8 | Задать тип линейного кодирования (не обязательно) | esr(config-if-gi)# switchport e1 linecode <CODE> | <CODE> – тип линейного кодирования; <ul style="list-style-type: none"> • ami – чередующейся полярностью импульсов; • hdb3 (по умолчанию) – двухполярный код высокой плотности порядка 3. |
| 9 | Задать количество тайм слотов | esr(config-if-gi)# switchport e1 timeslots <RANGE> | <RANGE> – количество тайм-слотов |
| 10 | Использовать E1 как единую сущность, без таймслотов (не обязательно) | esr(config-if-gi)# switchport e1 unframed | |
| 11 | Конфигурируем E1 | esr(config)# interface e1 1/ <SLOT>/1 | <SLOT> – номер слота. |
| 12 | Включаем CHAP-аутентификацию для PPP (не обязательно) | esr(config-e1)# ppp authentication chap | |
| 13 | Задается имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации (не обязательно) | esr(config-e1)# ppp chap hostname <NAME> | <NAME> – имя маршрутизатора |
| 14 | Задать пароль для аутентификации (не обязательно) | esr(config-e1)# ppp chap password ascii-text <CLEAR-TEXT> | <CLEAR-TEXT> – пароль в открытой форме, задается строкой [1 .. 64] символов, может включать символы [0-9a-fA-F] |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|------------------------------------|
| 15 | Включить игнорирование аутентификации (не обязательно) | esr(config-e1)# ppp chap refuse | |
| 16 | Задать имя пользователя для аутентификации (не обязательно) | esr(config-e1)# ppp chap username <NAME> | <NAME> – имя пользователя |
| 17 | Разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно) | esr(config-e1)# ppp ipcp accept-address | |
| 18 | Задать IP-адрес, который отправляется удаленной стороне для последующего его присвоения (не обязательно) | esr(config-e1)# ppp ipcp remote-address <ADDR> | <ADDR> – IP-адрес удаленного шлюза |
| 19 | Задать количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно) | esr(config-e1)# ppp max-configure <VALUE> | <VALUE> – количество попыток |
| 20 | Задать количество попыток отправки Configure-NAK пакетов, прежде чем будут подтверждены все опции (не обязательно) | esr(config-e1)# ppp max-failure <VALUE> | <VALUE> – количество попыток |
| 21 | Задать количество попыток отправки Terminate-Request пакетов, прежде чем сессия будет прервана (не обязательно) | esr(config-e1)# ppp max-terminate <VALUE> | <VALUE> – количество попыток |
| 22 | Задать размер MRU (Maximum Receive Unit) для интерфейса (не обязательно) | esr(config-e1)# ppp mru <MRU> | <MRU> – значение MRU |
| 23 | Включение режима MLPPP (не обязательно) | esr(config-e1)# ppp multilink | |
| 24 | Добавить в MLPPP группу (не обязательно) | esr(config-e1)# ppp multilink-group <GROUP-ID> | <GROUP-ID> – номер группы |
| 25 | Задается интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно) | esr(config-e1)# ppp timeout keepalive <TIME> | <TIME> – время в секундах |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---------------------------|
| 26 | Задается интервал, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно) | esr(config-e1)# ppp timeout retry <TIME> | <TIME> – время в секундах |

1.18.2 Пример конфигурации

Задача:

Настроить PPP-соединение со встречной стороной с IP-адресом 10.77.0.1/24 через ToPGATE-SFP, используя 1-8 канальные интервалы для передачи данных; источник синхросигнала – встречная сторона.



Рисунок 15 – Схема сети

Решение:

Переключаем интерфейс, в котором установлен ToPGATE-SFP, gigabitethernet 1/0/3 в режим работы E1:

```

esr# configure
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# description "*** ToPGATE ***"
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 timeslots 1-8
esr(config-if-gi)# switchport e1 clock source line
esr(config-if-gi)# switchport e1 slot 3
esr(config-if-gi)# exit
  
```

Включим interface e1 1/3/1:

```

esr(config)# interface e1 1/3/1
esr(config-e1)# security-zone trusted
esr(config-e1)# ip address 10.77.0.1/24
esr(config-e1)# exit
  
```

Изменения конфигурации вступят в действие по следующим командам:

```

esr# commit
Configuration has been successfully committed
esr# confirm
Configuration has been successfully confirmed
  
```


1.19 Настройка MLPPP

Multilink PPP (MLPPP) предоставляет собой агрегированный канал, включающий в себя методы для распространения трафика через несколько физических каналов, имея одно логическое соединение. Этот вариант позволяет расширить пропускную способность и обеспечивает балансировку нагрузки.



Рисунок 16 – Схема сети

1.19.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 1 | Настроить группу агрегации. | esr(config)# interface multilink <IF> | <IF> – наименование интерфейса. |
| 2 | Указать описание конфигурируемой группы агрегации (не обязательно). | esr(config- multilink)# description <DESCRIPTION> | <DESCRIPTION> – описание группы агрегации, задаётся строкой до 255 символов. |
| 3 | Задать интервал времени, за который усредняется статистика о нагрузке на группе агрегации (не обязательно). | esr(config- multilink)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5. |
| 4 | Указать размер MTU (Maximum Transmission Unit) для группы агрегации (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames". | esr(config- multilink)# mtu <MTU> | <MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500. |
| 5 | Включить CHAP-аутентификацию. | esr(config-multilink)# ppp authentication chap | |
| 6 | Включить игнорирование аутентификации (не обязательно). | esr(config-multilink)# ppp chap refuse | |
| 7 | Указать имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации. | esr(config-multilink)# ppp chap hostname <NAME> | <NAME> – имя маршрутизатора, задаётся строкой до 31 символа |
| 8 | Указать пароль, который отправляется удаленной стороне вместе с именем маршрутизатора для прохождения CHAP-аутентификации. | esr(config-multilink)# ppp chap password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F]. <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 9 | Разрешить принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно). | esr(config-multilink)# ppp ipcp accept-address | |
| 10 | Установить IP-адрес, который отправляется удаленной стороне для последующего его присвоения. | esr(config-multilink)# ppp iccp remote-address <ADDR> | <ADDR> – IP-адрес удаленного шлюза. |
| 11 | Указать пользователя для аутентификации удаленной стороны и перейти в режим конфигурирования указанного пользователя. | esr(config-multilink)# chap username <NAME> | <NAME> – имя пользователя, задается строкой до 31 символа. |
| 12 | Установить пароль в открытой или зашифрованной форме определенному пользователю для аутентификации удаленной стороны. | esr(config-ppp-user)# password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль в открытой форме, задается строкой [8 .. 64] символов, может включать символы [0-9a-fA-F]. <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задается строкой [16..128] символов. |
| 13 | Установить количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно). | esr(config-multilink)# ppp max-configure <VALUE> | <VALUE> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 10. |
| 14 | Установить количество попыток выслать Configure-NAK пакеты, прежде чем будут подтверждены все опции (не обязательно). | esr(config-multilink)# ppp max-failure <VALUE> | <VALUE> – время в секундах, принимает значения [1..255]. |
| 15 | Установить количество попыток выслать Terminate-Request пакеты, прежде чем сессия будет прервана (не обязательно). | esr(config-multilink)# ppp max-terminate <VALUE> | <VALUE> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 2. |
| 16 | Указать размер MRU (Maximum Receive Unit) для интерфейса. | esr(config-multilink)# ppp mru <MRU> | <MRU> – значение MRU, принимает значения в диапазоне [128..1485]. Значение по умолчанию: 1500. |
| 17 | Указать интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно). | esr(config-multilink)# ppp timeout keepalive <TIME> | <TIME> – время в секундах, принимает значения [1..32767]. Значение по умолчанию: 10. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 18 | Установить интервал времени в секундах, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно). | esr(config-multilink)# ppp timeout retry <TIME> | <TIME> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 3. |
| 19 | Определить максимальный размер пакета для MLPP интерфейса. | esr(config-multilink)# mrru <MRRU> | <MRRU> – максимальный размер принимаемого пакета для MLPP интерфейса, принимает значение в диапазоне [1500..10000]. |
| 20 | Привязать порт e1 к физическому интерфейсу. | esr(config-if-gi)# switchport e1 <SLOT> | <SLOT> – идентификатор слота, принимает значение в диапазоне [0..3]. |
| 21 | Перевести физический порт в режим работы с SFPe1 модулем. | esr(config-if-gi)# switchport mode e1 | |
| 22 | Включить режим MLPPP на E1-интерфейсе. | esr(config-e1)# ppp multilink | |
| 23 | Включить E1-интерфейс в группу агрегации. | esr(config-e1)# ppp multilink-group <GROUP-ID> | <GROUP-ID> – идентификатор группы, принимает значение [1..4]. |

1.19.2 Пример настройки

Задача:

Настроить MLPPP-соединение с встречной стороной с IP-адресом 10.77.0.1/24 через устройство MXE.



Рисунок 17 – Схема сети

Решение:

Переключаем интерфейс gigabitethernet 1/0/10 в режим работы E1:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 0
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 1
esr(config-if-gi)# exit
```

Настроим MLPPP 3:

```

esr(config)# interface multilink 3
esr(config-multilink)# ip address 10.77.0.2/24
esr(config-multilink)# security-zone trusted
esr(config-multilink)# exit
esr(config)# exit

```

Включим interface e1 1/0/1, interface e1 1/0/2 в группу агрегации MLPPP 3:

```

esr(config)# interface e1 1/0/1
esr(config-e1)# ppp multilink
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# exit
esr(config)# interface e1 1/0/2
esr(config-e1)# ppp multilink
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# exit

```

1.20 Настройка Bridge

Bridge (мост) – это способ соединения двух сегментов Ethernet на канальном уровне без использования протоколов более высокого уровня, таких как IP. Пакеты передаются на основе Ethernet-адресов, а не IP-адресов. Поскольку передача выполняется на канальном уровне (уровень 2 модели OSI), трафик протоколов более высокого уровня прозрачно проходит через мост.

1.20.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 1 | Добавить сетевой мост (bridge) в систему и перейти в режим настройки его параметров. | esr(config)# bridge <BRIDGE-ID> | <BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1..50]; • для ESR-20/21/100/200 – [1..250]; • для ESR-1000/1200/1500/1510/1700 – [1..500]. |
| 2 | Активировать сетевой мост. | esr (config - bridge)# enable | |
| 3 | Указать экземпляр VRF, в котором будет работать данный интерфейс (не обязательно). | esr(config- bridge)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Назначить описание конфигурируемому сетевому мосту (не обязательно). | esr(config-bridge)# description <DESCRIPTION> | <DESCRIPTION> – описание сетевого моста, задается строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 5 | Указать размер MTU (Maximum Transmission Unit) пакетов, которые может пропускать данный bridge (не обязательно; возможно, если в bridge включен только VLAN). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | esr(config-bridge)# mtu <MTU> | <MTU> – значение MTU, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [552..9600]; • для ESR-20/21 – [552..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 – [552..10000]. Значение по умолчанию: 1500 |
| 6 | Задать интервал времени, за который усредняется статистика о нагрузке на bridge (не обязательно) | esr(config-bridge)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5 |
| 7 | Связать текущий сетевой мост с VLAN. Все интерфейсы и L2-туннели, являющиеся членами назначаемого VLAN, автоматически включаются в сетевой мост и становятся участниками общего L2 домена (не обязательно) | esr(config-bridge)# vlan <VID> | <VID> – идентификатор VLAN, задаётся в диапазоне [1..4094]. |
| 8 | Задать MAC-адрес сетевого моста, отличный от системного (не обязательно). | esr(config-bridge)# mac-address <ADDR> | <ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. |
| 9 | Связать суб-интерфейс, QinQ-интерфейс, L2GRE туннель или L2TPv3 туннель с сетевым мостом. Связанные интерфейсы/туннели и сетевые мосты автоматически становятся участниками общего L2 домена (не обязательно). | esr(config-if-gi)# bridge-group <BRIDGE-ID> esr(config-if-l2tpv3)# bridge-group <BRIDGE-ID> | <BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1..50]; • для ESR-20/21/100/200 – [1..250]; • для ESR-1000/1200/1500/1510/1700 – [1..500]. |
| 10 | Включить на bridge режим изоляции интерфейсов. В данном режиме обмен трафиком между членами сетевого моста запрещен. (не обязательно; применимо только на ESR-1000/1200/1500/1510/1700) | esr(config-bridge)# protected-ports [exclude vlan] | exclude vlan – при указании данного ключа, VLAN (связанный с bridge) исключается из списка изолируемых интерфейсов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 11 | Запретить коммутацию unknown-unicast трафика (когда MAC-адрес назначения не содержится в таблице коммутации) в данном bridge. (не обязательно; применимо только на ESR-1000/1200/1500/1510/1700) | esr(config-bridge)# unknown-unicast-forwarding disable | |
| 12 | Установить время жизни IPv4/IPv6-записей в ARP-таблице, изученных на данном bridge (не обязательно). | esr(config- bridge)# ip arp reachable-time <TIME> или ipv6 nd reachable-time <TIME> | <TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>. |

1.20.2 Пример настройки bridge для VLAN и L2TPv3-туннеля

Задача:

Объединить в единый L2 домен интерфейсы маршрутизатора, относящиеся к локальной сети, и L2TPv3-туннель, проходящий по публичной сети. Для объединения использовать VLAN 333.



Рисунок 18 – Схема сети

Решение :

Создадим VLAN 333:

```
esr(config)# vlan 333
esr(config-vlan)# exit
```

Создадим зону безопасности «trusted»:

```
esr(config)# security-zone trusted
esr(config-zone)# exit
```

Добавим интерфейсы gi1/0/11, gi1/0/12 в VLAN 333:

```

esr(config)# interface gigabitethernet 1/0/11-12
esr(config-if)# mode switchport
esr(config-if)# switchport general allowed vlan add 333 tagged

```

Создадим bridge 333, привяжем к нему VLAN 333 и укажем членство в зоне «trusted»:

```

esr(config)# bridge 333
esr(config-bridge)# vlan 333
esr(config-bridge)# security-zone trusted
esr(config-bridge)# enable

```

Установим принадлежность L2TPv3-туннеля к мосту, который связан с локальной сетью (настройка L2TPv3-туннеля рассматривается в разделе [Настройка L2TPv3-туннелей](#)). В общем случае идентификаторы моста и туннеля не должны совпадать с VID как в данном примере.

```

esr(config)# tunnel l2tpv3 333
esr(config-l2tpv3)# bridge-group 333

```

1.20.3 Пример настройки bridge для VLAN

Задача:

Настроить маршрутизацию между VLAN 50 (10.0.50.0/24) и VLAN 60 (10.0.60.0/24). VLAN 50 должен относиться к зоне «LAN1», VLAN 60 – к зоне «LAN2», разрешить свободную передачу трафика между зонами.

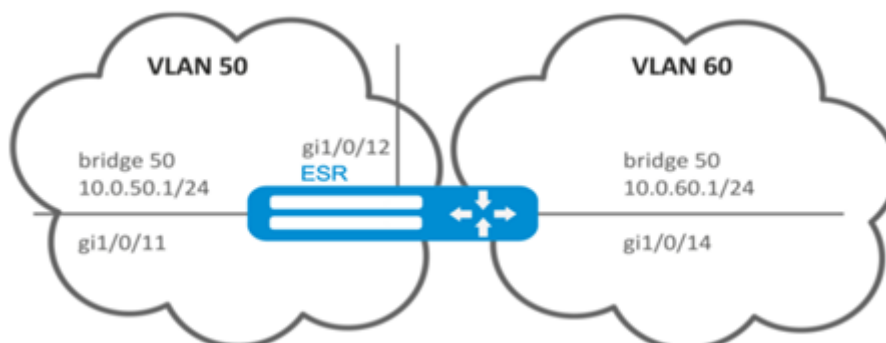


Рисунок 19 – Схема сети

Решение:

Создадим VLAN 50, 60:

```

esr(config)# vlan 50,60
esr(config-vlan)# exit

```

Создадим зоны безопасности «LAN1» и «LAN2»:

```

esr(config)# security-zone LAN1
esr(config-zone)# exit
esr(config)# security-zone LAN2
esr(config-zone)# exit

```

Назначим интерфейсам gi1/0/11, gi1/0/12 VLAN 50:

```

esr(config)# interface gigabitethernet 1/0/11-12
esr(config-if-gi)# switchport general allowed vlan add 50 tagged

```

Назначим интерфейсу gi1/0/14 VLAN 60:

```

esr(config)# interface gigabitethernet 1/0/14
esr(config-if-gi)# switchport general allowed vlan add 60 tagged

```

Создадим bridge 50, привяжем VLAN 50, укажем IP-адрес 10.0.50.1/24 и членство в зоне «LAN1»:

```

esr(config)# bridge 50
esr(config-bridge)# vlan 50
esr(config-bridge)# ip address 10.0.50.1/24
esr(config-bridge)# security-zone LAN1
esr(config-bridge)# enable

```

Создадим bridge 60, привяжем VLAN 60, укажем IP-адрес 10.0.60.1/24 и членство в зоне «LAN2»:

```

esr(config)# bridge 60
esr(config-bridge)# vlan 60
esr(config-bridge)# ip address 10.0.60.1/24
esr(config-bridge)# security-zone LAN2
esr(config-bridge)# enable

```

Создадим правила в Firewall, разрешающие свободное прохождение трафика между зонами:

```

esr(config)# security zone-pair LAN1 LAN2
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair LAN2 LAN1
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit

```

Посмотреть членство интерфейсов в мосте можно командой:

```

esr# show interfaces bridge

```


1.20.4 Пример настройки добавления/удаления второго VLAN-тега

Задача:

На интерфейс `gigabitethernet 1/0/1` поступают Ethernet-кадры с различными VLAN-тегами. Необходимо перенаправить их в интерфейс `gigabitethernet 1/0/2`, добавив второй VLAN-ID 828. При поступлении на интерфейс `gigabitethernet 1/0/2` Ethernet-кадров с VLAN-ID 828, данный тег должен быть удален и отправлен в интерфейс `gigabitethernet 1/0/1`.

Решение:

Создадим на маршрутизаторе bridge без VLAN и без IP-адреса.

```
esr(config)# bridge 1
esr(config-bridge)# enable
esr(config-bridge)# exit
```

Включим интерфейс `gigabitethernet 1/0/1` в bridge 1.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# bridge-group 1
esr(config-if-gi)# exit
```

Включим суб-интерфейс `gigabitethernet 1/0/2.828` в bridge 1.

```
esr(config)# interface gigabitethernet 1/0/2.828
esr(config-subif)# bridge-group 1
esr(config-subif)# exit
```

⚠ При добавлении второго VLAN-тега в Ethernet-кадр, его размер увеличивается на 4 байта. На интерфейсе маршрутизатора `gigabitethernet 1/0/2` и на всем оборудовании передающем Q-in-Q кадры необходимо увеличить MTU на 4 байта или более.

1.21 Настройка RIP

RIP — дистанционно-векторный протокол динамической маршрутизации, который использует количество транзитных участков в качестве метрики маршрута. Максимальное количество транзитных участков (hop), разрешенное в RIP, равно 15. Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации один раз в 30 секунд. RIP работает на 3-м уровне стека TCP/IP, используя UDP-порт 520.

1.21.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 1 | Настроить приоритетность протокола RIP маршрутизации для основной таблицы маршрутизации (не обязательно). | esr(config)# ip protocols rip preference <VALUE> | <VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: RIP (100). |
| 2 | Настроить емкость таблиц маршрутизации протокола RIP (не обязательно). | esr(config)# ip protocols rip max-routes <VALUE> | <VALUE> – количество маршрутов протокола RIP в маршрутной таблице, принимает значения в диапазоне [1..10000]; Значение по умолчанию: 10000. |
| 3 | Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | esr(config)# ip prefix-list <NAME> | <NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа. |
| 4 | Разрешить (permit) или запретить (deny) списки префиксов. | esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP -адресов, задаётся строкой до 31 символа; <LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов; <ul style="list-style-type: none"> • eq – при указании команды длина префикса должна соответствовать указанной; • le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • ge – при указании команды длина префикса должна быть больше либо соответствовать указанной; • default - route – фильтрация маршрута по умолчанию. |
| 5 | Перейти в режим настройки параметров RIP-процесса. | esr(config)# router rip esr(config-rip)# | |
| 6 | Включить RIP-протокол. | esr(config-rip)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 7 | Определить алгоритм аутентификации протокола RIP (не обязательно). | esr(config-rip)# authentication algorithm { cleartext md5 } | <ul style="list-style-type: none"> • cleartext – пароль, передается открытым текстом; • md5 – пароль хешируется по алгоритму md5. |
| 8 | Установить пароль для аутентификации с соседом (не обязательно). | esr(config-rip)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <p><CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;</p> <p><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).</p> |
| 9 | Определить список паролей для аутентификации через алгоритм хеширования md5 (не обязательно). | esr(config-rip)# authentication key-chain <KEYCHAIN> | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 10 | Выключить анонсирование маршрутов на интерфейсах/ туннелях/bridge, где это не нужно (не обязательно). | esr(config-rip)# passive-interface {<IF> <TUN> } | <p><IF> – интерфейс и идентификатор;</p> <p><TUN> – имя и номер туннеля.</p> |
| 11 | Установить временной интервал, по истечении которого производится анонсирование (не обязательно). | esr(config-rip)# timers update <TIME> | <p><TIME> – время в секундах, принимает значения [1..65535].</p> <p>Значение по умолчанию: 180 секунд.</p> |
| 12 | Установить временной интервал корректности маршрутной записи без обновления (не обязательно). | esr(config-rip)# timers invalid <TIME> | <p><TIME> – время в секундах, принимает значения [1..65535].</p> <p>Значение по умолчанию: 180 секунд.</p> |
| 13 | Установить временной интервал, по истечении которого производится удаление маршрута (не обязательно). | esr(config-rip)# timers flush <TIME> | <p><TIME> – время в секундах, принимает значения [1..65535].</p> <p>При установке значения нужно учитывать следующее правило: «timersinvalid + 60»</p> <p>Значение по умолчанию: 240 секунд.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 14 | Включить анонсирование подсетей. | esr(config-rip)# network <ADDR/LEN> | <p><ADDR/LEN> – адрес подсети, указывается в следующем формате:</p> <p>AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].</p> |
| 15 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно). | esr(config-rip)# prefix-list <PREFIX-LIST-NAME> { in out } | <p><PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа.</p> <ul style="list-style-type: none"> • in – фильтрация входящих маршрутов; • out – фильтрация анонсируемых маршрутов. |
| 16 | Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно). | esr(config-rip)# redistribute static [route-map <NAME>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа. |
| | | esr(config-rip)# redistribute connected [route-map <NAME>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| | | esr(config-rip)# redistribute ospf <ID><ROUTE-TYPE> [route-map <NAME>] | <p><ID> – номер процесса, может принимать значение [1..65535];</p> <p><ROUTE-TYPE> – тип маршрута:</p> <ul style="list-style-type: none"> • intra - area – анонсирование маршрутов OSPF-процесса в пределах зоны; • inter - area – анонсирование маршрутов OSPF-процесса между зонами; • external 1 – анонсирование внешних маршрутов OSPF-формата 1; • external 2 – анонсирование внешних маршрутов OSPF-формата 2; <p><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа.</p> |
| | | esr(config-rip)# redistribute bgp <AS> [route-map <NAME>] | <p><AS> – номер автономной системы, может принимать значения [1..4294967295];</p> <p><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.</p> |
| 17 | Перейти в режим конфигурирования интерфейса/ туннеля/ сетевого моста. | esr(config)# interface <IF-TYPE><IF-NUM> | <p><IF-TYPE> тип интерфейса;</p> <p><IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.</p> |
| | | esr(config)# tunnel <TUN-TYPE><TUN-NUM> | <p><TUN-TYPE> тип туннеля;</p> <p><TUN-NUM> номер туннеля.</p> |
| | | esr(config)# bridge <BR-NUM> | <BR-NUM> – номер bridge. |
| 18 | Установить величину метрики RIP-маршрутов на интерфейсе (не обязательно). | esr(config-if-gi)# ip rip metric <VALUE> | <p><VALUE> – величина метрики, задаётся в размере [0..32767].</p> <p>Значение по умолчанию: 5.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 19 | Установить режим анонсирования маршрутов по протоколу RIP (не обязательно). | esr(config-if-gi)# ip rip mode <MODE> | <MODE> – режим анонсирования маршрутов: <ul style="list-style-type: none"> • multicast – маршруты анонсируются в многоадресном режиме; • broadcast – маршруты анонсируются в широковещательном режиме; • unicast – маршруты анонсируются в unicast-режиме соседям. Значение по умолчанию: multicast. |
| 20 | Задать IP-адрес соседа для установления отношения в unicast-режиме анонсирования маршрутов (не обязательно). | esr(config-if-gi)# ip rip neighbor <ADDR> | <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 21 | Включить суммаризацию подсетей (не обязательно). | esr(config-if-gi)# ip rip summary-address <ADDR/LEN> | <ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |

1.21.2 Пример настройки RIP

Задача:

Настроить на маршрутизаторе протокол RIP для обмена маршрутной информацией с соседними маршрутизаторами. Маршрутизатор должен анонсировать статические маршруты и подсети 115.0.0.0/24, 14.0.0.0/24, 10.0.0.0/24. Анонсирование маршрутов должно происходить каждые 25 секунд.

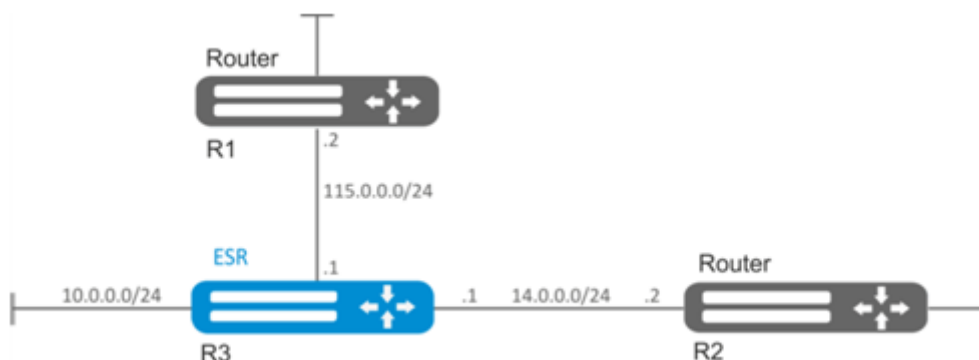


Рисунок 20 – Схема сети

Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке 20.

Перейдём в режим конфигурирования протокола RIP:

```
esr(config)# router rip
```

Укажем подсети, которые будут анонсироваться протоколом: 115.0.0.0/24, 14.0.0.0/24 и 10.0.0.0/24:

```
esr(config-rip)# network 115.0.0.0/24
esr(config-rip)# network 14.0.0.0/24
esr(config-rip)# network 10.0.0.0/24
```

Для анонсирования протоколом статических маршрутов выполним команду:

```
esr(config-rip)# redistribute static
```

Настроим таймер, отвечающий за отправку маршрутной информации:


```
esr(config-rip)# timers update 25
```

После установки всех требуемых настроек включаем протокол:

```
esr(config-rip)# enable
```

Для того чтобы посмотреть таблицу маршрутов RIP воспользуемся командой:

```
esr# show ip rip
```

 Помимо настройки протокола RIP, необходимо в firewall разрешить UDP-порт 520.

1.22 Настройка OSPF

OSPF – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

1.22.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 1 | Настроить приоритетность протокола OSPF маршрутизации для основной таблицы маршрутизации (не обязательно). | esr(config)# ip protocols ospf preference <VALUE> | <VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. |
| | | esr(config-vrf)# ip protocols ospf preference <VALUE> | Значение по умолчанию: 150. |
| 2 | Настроить емкость таблиц маршрутизации протокола OSPF (не обязательно). | esr(config)# ip protocols ospf max-routes <VALUE> | <VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне: |
| | | esr(config)# ipv6 protocols ospf max-routes <VALUE> | <ul style="list-style-type: none"> • для ESR-1000/1200/1500/1510/1700 [1..500000]; • для ESR-20/21/100/200 [1..300000]; • для ESR-10/12V(F)/14VF [1..30000] Значение по умолчанию для глобального режима: <ul style="list-style-type: none"> • для ESR-1000/1200/1500/1510/1700 – (500000); • для ESR-20/21/100/200 – (300000); • для ESR-10/12V(F)/14VF – (30000). Значение по умолчанию для VRF: 0 |
| 3 | Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPF (не обязательно). | esr(config)# router ospf log-adjacency-changes | |
| | | esr(config)# ipv6 router ospf log-adjacency-changes | |
| 4 | Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | esr(config)# ip prefix-list <NAME> | <NAME> – имя конфигулируемого списка подсетей, задаётся строкой до 31 символа. |
| | | esr(config)# ipv6 prefix-list <NAME> | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 5 | Разрешить (permit) или запретить (deny) списки префиксов. | esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP -адресов, задаётся строкой до 31 символа; <LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов; <ul style="list-style-type: none"> • eq – при указании команды длина префикса должна соответствовать указанной; • le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • ge – при указании команды длина префикса должна быть больше либо соответствовать указанной; • default - route – фильтрация маршрута по умолчанию. |
| | | esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} | |
| | | esr(config-ipv6-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} | |
| | | esr(config-ipv6-pl)# deny object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} | |
| 6 | Добавить OSPF-процесс в систему и осуществить переход в режим настройки параметров OSPF-процесса. | esr(config)# router ospf <ID> [vrf <VRF>] | <ID> – номер автономной системы процесса, принимает значения [1..65535] <VRF> – имя экземпляра VRF, задаётся строкой до 31 символа, в рамках которого будет работать протокол маршрутизации. |
| | | esr(config)# ipv6 router ospf <ID> [vrf <VRF>] | |
| 7 | Установить идентификатор маршрутизатора для данного OSPF-процесса. | esr(config-ospf)# router-id <ID> | <ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-ipv6-ospf)# router-id <ID> | |
| 8 | Определить приоритетность маршрутов процесса OSPF. | esr(config-ospf)# preference <VALUE> | <VALUE> – приоритетность маршрутов процесса OSPF, принимает значения в диапазоне [1..255]. Значение по умолчанию: 10. |
| | | esr(config-ipv6-ospf)# preference <VALUE> | |
| 9 | Включить совместимость с RFC 1583 (не обязательно). | esr(config-ospf)# compatible rfc1583 | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| | | esr(config-ipv6-ospf)# compatible rfc1583 | |
| 11 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно). | esr(config-ospf)# prefix-list <PREFIX-LIST-NAME> { in out } esr(config-ipv6-ospf)# prefix-list <PREFIX-LIST-NAME> { in out } | <p><PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа.</p> <ul style="list-style-type: none"> • in – фильтрация входящих маршрутов; • out – фильтрация анонсируемых маршрутов. |
| 12 | Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно). | esr(config-ospf)# redistribute static [route-map <NAME>] esr(config-ipv6-ospf)# redistribute static [route-map <NAME>] | <p><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.</p> |
| | | esr(config-ospf)# redistribute connected [route-map <NAME>] esr(config-ipv6-ospf)# redistribute connected [route-map <NAME>] | <p><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.</p> |
| | | esr(config-ospf)# redistribute rip [route-map <NAME>] | <p><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа.</p> |
| | | esr(config-ospf)# redistribute bgp <AS> [route-map <NAME>] esr(config-ipv6-ospf)# redistribute bgp <AS> [route-map <NAME>] | <p><AS> – номер автономной системы, может принимать значения [1..4294967295];</p> <p><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.</p> |
| 13 | Активировать OSPF-процесс. | esr(config-ospf)# enable esr(config-ipv6-ospf)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 14 | Создать OSPF-область и перейти в режим конфигурирования области. | esr(config-ospf)# area <AREA_ID> | <AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-ipv6-ospf)# area <AREA_ID> | |
| 15 | Включить анонсирование подсетей. | esr(config-ospf-area)# network <ADDR/LEN> | <p><ADDR/LEN> – адрес подсети, указывается в следующем формате:</p> <p>AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].</p> |
| | | esr(config-ipv6-ospf-area)# network <IPV6-ADDR/LEN> | <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |
| 16 | Определить тип области | esr(config-ospf-area)# area-type <TYPE> [no-summary] | <p><TYPE> – тип области:</p> <ul style="list-style-type: none"> • stub – устанавливает значение stub (тупиковая область); no-summary – команда в связке с параметром «stub» образует область «totallystubby» (для передачи информации за пределы области используется только маршрут по умолчанию). • nssa – устанавливает значение nssa (область NSSA); no-summary – в связке с параметром nssa образует область totallynssa (автоматически генерирует маршрут по умолчанию как межобластной). |
| | | esr(config-ipv6-ospf-area)# area-type <TYPE> [no-summary] | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 17 | Включить генерацию маршрута по умолчанию для NSSA-области и анонсирование его в качестве NSSA-LSA. | esr(config-ospf-area)# default-information-originate | |
| | | esr(config-ipv6-ospf-area)# default-information-originate | |
| 18 | Включить суммаризацию или скрытие подсетей. | esr(config-ospf-area)# summary-address <ADDR/LEN> { advertise not-advertise } | <p><ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];</p> <ul style="list-style-type: none"> • advertise – при указании команды вместо указанных подсетей будет анонсироваться суммарная подсеть; • not - advertise – при указании команды подсети, входящие в указанную подсеть, анонсироваться не будут. |
| | | esr(config-ipv6-ospf-area)# summary-address <IPV6-ADDR/LEN> { advertise not-advertise } | <p><IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];</p> <ul style="list-style-type: none"> • advertise – при указании команды вместо подсетей, входящих в указанную подсеть, будет анонсироваться суммарная подсеть; • not-advertise – подсети, входящие в указанную подсеть анонсироваться не будут. |
| 19 | Активировать OSPF-область. | esr(config-ospf-area)# enable | |
| | | esr(config-ipv6-ospf-area)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 20 | Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей. | esr(config-ospf-area)# virtual-link <ID> | <ID> – идентификатор маршрутизатора, с которым устанавливается виртуальное соединение, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-ipv6-ospf-area)# virtual-link <ID> | |
| 21 | Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, который не получил подтверждения о получении (например, DatabaseDescription пакет или LinkStateRequest пакеты). | esr(config-ospf- vlink)# retransmit-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд. |
| | | esr(config-ipv6-ospf- vlink)# retransmit-interval <TIME> | |
| 22 | Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет. | esr(config-ospf- vlink)# hello-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд. |
| | | esr(config-ipv6-ospf- vlink)# hello-interval <TIME> | |
| 23 | Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению «hello-interval». | esr(config-ospf- vlink)# dead-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд. |
| | | esr(config-ipv6-ospf- vlink)# dead-interval <TIME> | |
| 24 | Определяется интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети | esr(config-ospf- vlink)# wait-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд |
| | | esr(config-ipv6-ospf- vlink)# wait-interval <TIME> | |
| 25 | Определить алгоритм аутентификации | esr(config-ospf- vlink)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации: <ul style="list-style-type: none"> • cleartext – пароль, передается открытым текстом (доступно только для RIP и OSPF-VLINK); • md 5 – пароль хешируется по алгоритму md5. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 26 | Установить пароль для аутентификации с соседом. | esr(config-ospf- vlink)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов. <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYYY...) или (YYYYY...). |
| 27 | Определить список паролей для аутентификации через алгоритм хеширования md5. | esr(config-ospf- vlink)# authentication key chain <KEYCHAIN> | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 28 | Активировать виртуальное соединение. | esr(config-ospf- vlink)# enable | |
| 29 | Перейти в режим конфигурирования интерфейса/ туннеля/ сетевого моста. | esr(config)# interface <IF-TYPE><IF-NUM> | <IF-TYPE> тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт. |
| | | esr(config)# tunnel <TUN-TYPE><TUN-NUM> | <TUN-TYPE> тип туннеля; <TUN-NUM> номер туннеля. |
| | | esr(config)# bridge <BR-NUM> | <BR-NUM> – номер bridge. |
| 30 | Определить принадлежность интерфейса/туннеля/ сетевого моста к определенному OSPF-процессу. | esr(config-if-gi)# ip ospf instance <ID> | <ID> – номер процесса, принимает значения [1..65535]. |
| | | esr(config-if-gi)# ipv6 ospf instance <ID> | |
| 31 | Определить принадлежность интерфейса к определенной области OSPF-процесса. | esr(config-if-gi)# ip ospf area <AREA_ID> | <AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-if-gi)# ipv6 ospf area <AREA_ID> | |
| 32 | Включить маршрутизацию по протоколу OSPF на интерфейсе. | esr(config-if-gi)# ip ospf | |
| | | esr(config-if-gi)# ipv6 ospf | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 33 | Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах. | esr(config-if-gi)# ip ospf mtu-ignore esr(config-if-gi)# ipv6 ospf mtu-ignore | |
| 34 | Определить алгоритм аутентификации протокола OSPF. | esr(config-if-gi)# ip ospf authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации: <ul style="list-style-type: none"> • cleartext – пароль, передается открытым текстом; • md 5 – пароль хешируется по алгоритму md5. |
| 35 | Установить пароль для аутентификации с OSPF-соседом при передаче пароля открытым текстом. | esr(config-if-gi)# ip ospf authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 36 | Определить список паролей для аутентификации по алгоритму хеширования md5 с соседом. | esr(config-if-gi)# ip ospf authentication key-chain <KEYCHAIN> | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 37 | Определить интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети. | esr(config-if-gi)# ip ospf wait-interval <TIME> esr(config-if-gi)# ipv6 ospf wait-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд. |
| 38 | Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, DatabaseDescription пакет или LinkStateRequest пакеты). | esr(config-if-gi)# ip ospf retransmit-interval <TIME> esr(config-if-gi)# ipv6 ospf retransmit-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд. |
| 39 | Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет. | esr(config-if-gi)# ip ospf hello-interval <TIME> esr(config-if-gi)# ipv6 ospf hello-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 40 | Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval. | esr(config-if-gi)# ip dead-interval <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| | | esr(config-if-gi)# ipv6 dead-interval <TIME> | Значение по умолчанию: 40 секунд. |
| 41 | Установить интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить HELLO-пакет соседу, даже в случае, если сосед неактивен. | esr(config-if-gi)# ip poll-interval <TIME> | <TIME> – время в секундах, принимает значения [1 .. 65535]. |
| | | esr(config-if-gi)# ipv6 poll-interval <TIME> | Значение по умолчанию: 120 секунд. |
| 42 | Задать статический IP-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях. | esr(config-if-gi)# ip ospf neighbor <IP> [eligible] | <IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. eligible – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля. |
| | | esr(config-if-gi)# ip ospf neighbor <IPV6-ADDR> [eligible] | <IPV6-ADDR> – IPv6-адрес соседа, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; eligible – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 43 | Определить тип сети для установления OSPF соседства. | esr(config-if-gi)# ip ospf network <TYPE> | <TYPE> – тип сети: <ul style="list-style-type: none"> • broadcast – тип соединения широковещательный; • non - broadcast – тип соединения NBMA; • point - to - multipoint – тип соединения точка-многоточие; • point-to-multipoint non-broadcast – тип соединения NBMA точка-многоточие; • point - to - point – тип соединения точка-точка. Значение по умолчанию: broadcast. |
| | | esr(config-if-gi)# ipv6 ospf network <TYPE> | |
| 44 | Установить приоритет маршрутизатора, который используется для выбора DR и BDR. | esr(config-if-gi)# ip ospf priority <VALUE> | <VALUE> – приоритет интерфейса, принимает значения [1..65535]. Значение по умолчанию: 120. |
| | | esr(config-if-gi)# ipv6 ospf priority <VALUE> | |
| 45 | Установить величину метрики на интерфейсе или туннеле. | esr(config-if-gi)# ip ospf cost <VALUE> | <VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 150. |
| | | esr(config-if-gi)# ipv6 ospf cost <VALUE> | |
| 47 | Включить протокол BFD для протокола OSPF | esr(config-if-gi)# ip ospf bfd-enable | |
| | | esr(config-if-gi)# ipv6 ospf bfd-enable | |

1.22.2 Пример настройки OSPF

Задача:

Настроить протокол OSPF на маршрутизаторе для обмена маршрутной информацией с соседними маршрутизаторами. Маршрутизатор должен находиться в области с идентификатором 1.1.1.1 и анонсировать маршруты, полученные по протоколу RIP.

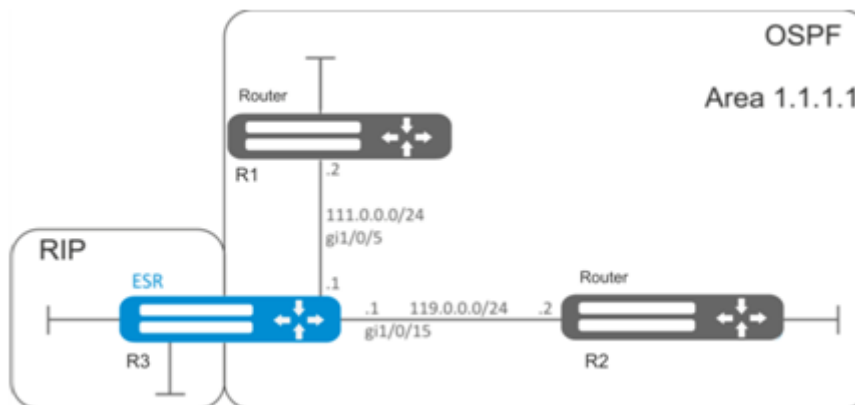


Рисунок 21 – Схема сети

Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 21.

Создадим OSPF-процесс с идентификатором 10 и перейдём в режим конфигурирования протокола OSPF:

```
esr(config)# router ospf 10
```

Создадим и включим требуемую область.

```
esr(config-ospf)# area 1.1.1.1
esr(config-ospf-area)# enable
esr(config-ospf-area)# exit
```

Включим анонсирование маршрутной информации из протокола RIP:

```
esr(config-ospf)# redistribute rip
```

Включим OSPF-процесс:

```
esr(config-ospf)# enable
esr(config-ospf)# exit
```

Соседние маршрутизаторы подключены к интерфейсам gi1/0/5 и gi1/0/15. Для установления соседства с другими маршрутизаторами привяжем их к OSPF-процессу и области. Далее включим на интерфейсе маршрутизацию по протоколу OSPF:

```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
```

```

esr(config)# interface gigabitethernet 1/0/15
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
esr(config)# exit

```

1.22.3 Пример настройки OSPF stub area

Задача:

Изменить тип области 1.1.1.1, область должна быть тупиковой. Тупиковый маршрутизатор должен анонсировать маршруты, полученные по протоколу RIP.

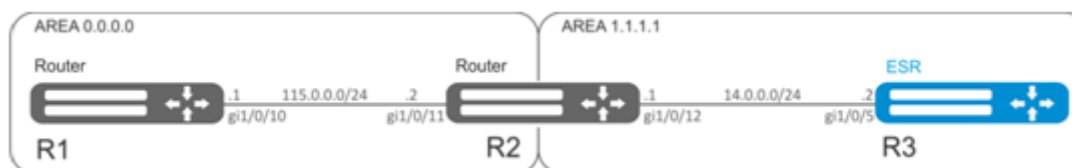


Рисунок 22 – Схема сети

Решение:

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 22.

Изменим тип области на тупиковый. На каждом маршрутизаторе из области 1.1.1.1 в режиме конфигурирования области выполним команду:

```

esr(config-ospf-area)# area-type stub

```

На тупиковом маршрутизаторе R3 включим анонсирование маршрутной информации из протокола RIP:

```

esr(config-ospf)# redistribute rip

```

1.22.4 Пример настройки Virtual link

Задача:

Объединить две магистральные области в одну с помощью virtual link.

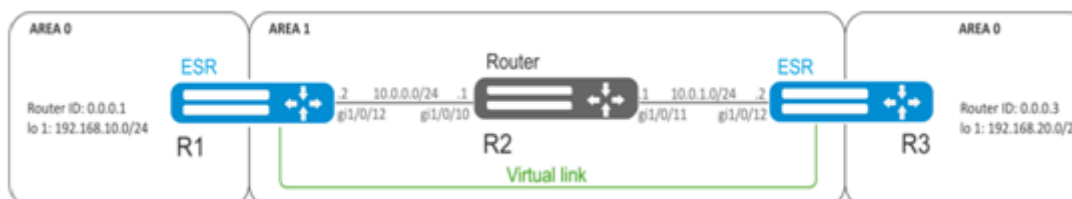


Рисунок 23 – Схема сети

Решение:

Virtual link — это специальное соединение, которое позволяет соединять разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя пограничными маршрутизаторами зоны (Area Border Router, ABR).

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 23.

На маршрутизаторе R1 перейдем в режим конфигурирования области 1.1.1.1:

```
esr(config-ospf)# area 1.1.1.1
```

Создадим virtual link с идентификатором 0.0.0.3 и включим его:

```
esr(config-ospf-area)# virtual-link 0.0.0.3
esr(config-ospf-vlink)# enable
```

На маршрутизаторе R3 перейдем в режим конфигурирования области 1.1.1.1:

```
esr(config-ospf)# area 1.1.1.1
```

Создадим virtual link с идентификатором 0.0.0.1 и включим его:

```
esr(config-ospf-area)# virtual-link 0.0.0.1
esr(config-ospf-vlink)# enable
```

Рассмотрим таблицу маршрутизации на маршрутизаторе R1:

```
esr# show ip route
C    * 10.0.0.0/24      [0/0]   dev gi1/0/12,                [direct 00:49:34]
O    * 10.0.1.0/24     [150/20] via 10.0.0.1 on gi1/0/12,    [ospf1 00:49:53] (0.0.0.3)
O    * 192.168.20.0/24 [150/30] via 10.0.0.1 on gi1/0/12,    [ospf1 00:50:15] (0.0.0.3)
C    * 192.168.10.0/24 [0/0]   dev lo1,                    [direct 21:32:01]
```

Рассмотрим таблицу маршрутизации на маршрутизаторе R3:

```
esr# show ip route
O    * 10.0.0.0/24     [150/20] via 10.0.1.1 on gi1/0/12,    [ospf1 14:38:35] (0.0.0.2)
C    * 10.0.1.0/24     [0/0]   dev gi1/0/12,                [direct 14:35:34]
C    * 192.168.20.0/24 [0/0]   dev lo1,                    [direct 14:32:58]
O    * 192.168.10.0/24 [150/30] via 10.0.1.1 on gi1/0/12,    [ospf1 14:39:54] (0.0.0.1)
```

Так как OSPF считает виртуальный канал частью области, в таблице маршрутизации R1 маршруты, полученные от R3, отмечены как внутризональные и наоборот.

Для просмотра соседей можно воспользоваться следующей командой:

```
esr# show ip ospf neighbors 10
```

Таблицу маршрутов протокола OSPF можно посмотреть командой:

```
esr# show ip ospf 10
```

⚠ В firewall необходимо разрешить протокол OSPF (89).

1.23 Настройка BGP

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (далее АС), то есть группами маршрутизаторов под единым техническим управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляется исходя из правил, принятых в сети.

1.23.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 1 | Настроить приоритетность протокола BGP маршрутизации для основной таблицы маршрутизации (не обязательно). | esr(config)# ip protocols bgp preference <VALUE> | <VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: BGP (170). |
| 2 | Настроить емкость таблиц маршрутизации протокола BGP (не обязательно). | esr(config)# ip protocols bgp max-routes <VALUE> | <VALUE> – количество маршрутов протокола BGP в маршрутной таблице, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-1700 [1..5000000]; • для ESR-1000/1200/1500/1510 [1..3000000]; • для ESR-20/21/100/200 [1..1500000]; • для ESR-10/12V(F)/14VF [1..800000] Значение по умолчанию: <ul style="list-style-type: none"> • для ESR-1700 (5000000); • для ESR-1000/1200/1500/1510/1700 (3000000); • для ESR-20/21/100/200 (1500000); • для ESR-10/12V/12VF/14VF (800000). |
| | | esr(config)# ipv6 protocols bgp max-routes <VALUE> | |
| | | esr(config-vrf)# ip protocols bgp max-routes <VALUE> | |
| | | esr(config-vrf)# ipv6 protocols bgp max-routes <VALUE> | |
| 3 | Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации BGP (не обязательно). | esr(config)# router bgp log-neighbor-changes | |
| | | esr(config)# ipv6 router bgp log-neighbor-changes | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 4 | Включить ESRP и определяется максимальное количество равноценных маршрутов до цели. | esr(config)# router bgp maximum-paths <VALUE> | <VALUE> – количество допустимых равноценных маршрутов до цели, принимает значения [1..16]. |
| 5 | Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | esr(config)# ip prefix-list <NAME> esr(config)# ipv6 prefix-list <NAME> | <NAME> – имя конфигулируемого списка подсетей, задаётся строкой до 31 символа. |
| 6 | Разрешить (permit) или запретить (deny) списки префиксов. | esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route} | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов; <ul style="list-style-type: none"> • eq – при указании команды длина префикса должна соответствовать указанной; • le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • ge – при указании команды длина префикса должна быть больше либо соответствовать указанной; • default - route – фильтрация маршрута по умолчанию. |
| 7 | Добавить BGP-процесс в систему и осуществить переход в режим настройки параметров BGP-процесса. | esr(config)# router bgp <AS> | <AS> – номер автономной системы процесса, принимает значения [1..4294967295]. |
| 8 | Определить тип конфигулируемой маршрутной информации и перейти в данный режим настройки. | esr(config-bgp)# address-family { ipv4 ipv6 } [vrf <VRF>] | <ul style="list-style-type: none"> • ipv 4 – семейство IPv4; • ipv 6 – семейство IPv6; <VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации. |
| 9 | Установить идентификатор маршрутизатора. | esr(config-bgp-af)# router-id <ID> esr(config-ipv6-bgp-af)# router-id <ID> | <ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 10 | Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной. | esr(config-bgp-af)# timers keepalive <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| | | esr(config-ipv6-bgp-af)# timers keepalive <TIME> | Значение по умолчанию: 60 секунд. |
| 11 | Установить временной интервал, по истечении которого встречная сторона считается недоступной. | esr(config-bgp-af)# timers holdtime <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| | | esr(config-ipv6-bgp-af)# timers holdtime <TIME> | Значение по умолчанию: 180 секунд. |
| 12 | Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения | esr(config-bgp-af)# timers error-wait <TIME1> <TIME2> | <TIME1> – время минимальной задержки в секундах, принимает значения [1..65535]; |
| | | esr(config-ipv6-bgp-af)# timers error-wait <TIME1> <TIME2> | <TIME2> – время максимальной задержки в секундах, принимает значения [1..65535]. |
| 13 | Установить идентификатор Route-Reflector кластера, которому принадлежит BGP-процесс маршрутизатора. | esr(config-bgp-af)# cluster-id <ID> | <ID> – идентификатор Route-Reflector кластера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-ipv6-bgp-af)# cluster-id <ID> | |
| 14 | Определить глобальный алгоритм аутентификации с соседями. | esr(config-bgp-af)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм шифрования: |
| | | esr(config-ipv6-bgp-af)# authentication algorithm <ALGORITHM> | md5 – пароль шифруется по алгоритму md5. |
| 15 | Установить глобальный пароль для аутентификации с соседями. | esr(config-bgp-af)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; |
| | | esr(config-ipv6-bgp-af)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 16 | Активировать BGP-процесс. | esr(config-bgp-af)# enable | |
| | | esr(config-ipv6-bgp-af)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 17 | Включить анонсирование статических маршрутов полученных альтернативным образом. | esr(config-bgp-af)# redistribute static [route-map <NAME>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа. |
| | | esr(config-ipv6-bgp-af)# redistribute static [route-map <NAME>] | |
| | | esr(config-bgp-af)# redistribute connected [route-map <NAME>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа. |
| | | esr(config-ipv6-bgp-af)# redistribute connected [route-map <NAME>] | |
| | | esr(config-bgp-af)# redistribute rip [route-map <NAME>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа. |
| | | esr(config-ipv6-bgp-af)# redistribute rip [route-map <NAME>] | |
| | | esr(config-bgp-af)# redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>] | <ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: |
| | | esr(config-ipv6-bgp-af)# redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>] | |
| | | <ul style="list-style-type: none"> • intra - area – анонсирование маршрутов OSPF-процесса в пределах зоны; • inter - area – анонсирование маршрутов OSPF-процесса между зонами; • external 1 – анонсирование внешних маршрутов OSPF-формата 1; • external 2 – анонсирование внешних маршрутов OSPF-формата 2; | |
| | | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа. | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| | esr(config-bgp-af)# redistribute bgp <AS> [route-map <NAME>] | <AS> – номер автономной системы, может принимать значения [1..4294967295]; | |
| | esr(config-ipv6-bgp-af)# redistribute bgp <AS> [route-map <NAME>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа. | |
| 18 | Включить анонсирование подсетей. | esr(config-bgp-af)# network <ADDR/LEN> | <ADDR/LEN> – адрес подсети, указывается в следующем формате: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]. |
| | | esr(config-ipv6-bgp-af)# network <ADDR/LEN> | X:X:X:X/EE – IPv6-адрес и маска подсети, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |
| 19 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно). | esr(config-bgp-af)# prefix-list <PREFIX-LIST-NAME> { in out } | <PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. <ul style="list-style-type: none"> • in – фильтрация входящих маршрутов; • out – фильтрация анонсируемых маршрутов. |
| 20 | Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа. | esr(config-bgp-af)# neighbor <ADDR> | <ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-ipv6-bgp-af)# neighbor <IPV6-ADDR> | <IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 21 | Задать описание соседа (не обязательно). | esr(config-bgp-neighbor)# description <DESCRIPTION> | <DESCRIPTION> – описание соседа, задаётся строкой до 255 символов. |
| 22 | Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной. (не обязательно) | esr(config-bgp-neighbor)# timers keepalive <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| | | esr(config-ipv6-bgp-neighbor)# timers keepalive <TIME> | Значение по умолчанию: 60 секунд. |
| 23 | Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно). | esr(config-bgp-neighbor)# timers holdtime <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| | | esr(config-ipv6-bgp-neighbor)# timers holdtime <TIME> | Значение по умолчанию: 180 секунд. |
| 24 | Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения (не обязательно). | esr(config-bgp-af)# timers error-wait <TIME1> <TIME2> | <TIME1> – время минимальной задержки в секундах, принимает значения [1..65535]; |
| | | esr(config-ipv6-bgp-af)# timers error-wait <TIME1> <TIME2> | <TIME2> – время максимальной задержки в секундах, принимает значения [1..65535]. |
| 25 | Установить номер автономной системы BGP-соседа. | esr(config-bgp-neighbor)# remote-as <AS> | <AS> – номер автономной системы, принимает значения [1..4294967295]. |
| | | esr(config-ipv6-bgp-neighbor)# remote-as <AS> | |
| 26 | Разрешить подключение к соседям, которые находятся не в напрямую подключенных подсетях. (не обязательно) | esr(config-bgp-neighbor)# ebgp-multihop <NUM> | <NUM> – Максимальное количество хопов при установке EBGП (используется для TTL). |
| | | esr(config-ipv6-bgp-neighbor)# ebgp-multihop <NUM> | |
| 27 | Задать режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального маршрутизатора. (не обязательно) | esr(config-bgp-neighbor)# next-hop-self | |
| | | esr(config-ipv6-bgp-neighbor)# next-hop-self | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 28 | Задать режим, в котором перед отправлением обновления из BGP-атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996). (не обязательно) | esr(config-bgp- neighbor)# remove-private-as | |
| | | esr(config-ipv6-bgp- neighbor)# remove-private-as | |
| 29 | Задать режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами всегда отправляется маршрут по умолчанию. (не обязательно) | esr(config-bgp- neighbor)# default-originate | |
| | | esr(config-ipv6-bgp- neighbor)# default-originate | |
| 30 | Включить генерацию и отправку маршрута по умолчанию, если маршрут по умолчанию есть в таблице маршрутизации FIB. (не обязательно) | esr(config-bgp-af)# default- information-originate | |
| 31 | Указать, что BGP-сосед является Route-Reflector клиентом. (не обязательно) | esr(config-bgp- neighbor)# route- reflector-client | |
| | | esr(config-ipv6-bgp- neighbor)# route-reflector-client | |
| 32 | Определить приоритетность маршрутов, получаемых от соседа. (не обязательно) | esr(config-bgp- neighbor)# preference <VALUE> | <VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255]. |
| | | esr(config-ipv6-bgp- neighbor)# preference <VALUE> | Значение по умолчанию: 170. |
| 33 | Задать IP/IPv6-адрес маршрутизатора, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых обновлениях маршрутной информации BGP. (не обязательно) | esr(config-bgp- neighbor)# update-source { <ADDR> <IPV6- ADDR> } | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; |
| | | esr(config-ipv6-bgp- neighbor)# update-source <ADDR> | <IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 34 | Включить режим, в котором разрешен приём маршрутов в BGP-атрибуте, AS Path которых содержит номера автономной системы процесса. (не обязательно) | esr(config-bgp- neighbor)# allow-local-as <NUMBER> | <NUMBER> – пороговое число вхождений номера автономной системы процесса в атрибуте AS Path, при которых маршрут будет принят, диапазон допустимых значений [1..10]. |
| | | esr(config-bgp- neighbor)# allow-local-as <NUMBER> | |
| 35 | Включить BFD-протокол на конфигурируемом BGP-соседе. (не обязательно) | esr(config-bgp- neighbor)# bfd-enable | |
| | | esr(config-ipv6-bgp- neighbor)# bfd-enable | |
| 36 | Определить алгоритм аутентификации с соседом. (не обязательно) | esr(config-bgp- neighbor)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5. |
| | | esr(config-ipv6-bgp- neighbor)# authentication algorithm <ALGORITHM> | |
| 37 | Установить пароль для аутентификации с соседом. (не обязательно) | esr(config-bgp- neighbor)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| | | esr(config-ipv6-bgp- neighbor)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | |

Часто бывает, особенно при конфигурировании iBGP, что в одном `bgp address-family` необходимо настроить несколько `bgp neighbor` с одинаковыми параметрами. Во избежание избыточности конфигурации рекомендуется использовать `bgp peer-group`, в которой возможно описать общие параметры, а в конфигурации `bgp neighbor` просто указать причастность к `bgp peer-group`.

1.23.2 Пример настройки

Задача:

Настроить BGP-протокол на маршрутизаторе со следующими параметрами:

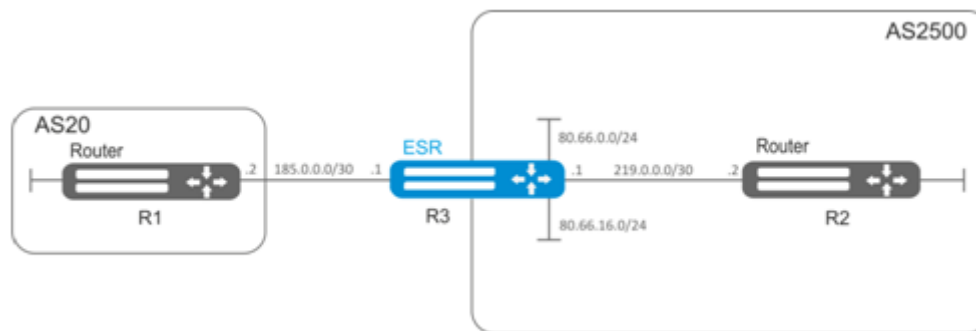


Рисунок 24 – Схема сети

- собственные подсети: 80.66.0.0/24, 80.66.16.0/24;
- анонсирование подсетей, подключенных напрямую;
- собственная AS 2500;
- первое соседство – подсеть 219.0.0.0/30, собственный IP-адрес 219.0.0.1, IP-адрес соседа 219.0.0.2, AS 2500;
- второе соседство – подсеть 185.0.0.0/30, собственный IP-адрес 185.0.0.1, IP-адрес соседа 185.0.0.2, AS 20.

Решение:

Сконфигурируем необходимые сетевые параметры:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 185.0.0.1/30
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip address 219.0.0.1/30
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# ip address 80.66.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/4
esr(config-if-gi)# ip address 80.66.16.1/24
esr(config-if-gi)# exit
```

Создадим BGP процесс для AS 2500 и войдем в режим конфигурирования параметров процесса:

```
esr(config)# router bgp 2500
```

Входим в режим конфигурирования маршрутной информации для IPv4:

```
esr(config-bgp)# address-family ipv4
```

Объявим подсети, подключённые напрямую:

```
esr(config-bgp-af)# redistribute connected
```

Создадим соседства с 185.0.0.2, 219.0.0.2 с указанием автономных систем и включим их:

```

esr(config-bgp-af)# neighbor 185.0.0.2
esr(config-bgp-neighbor)# remote-as 20
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# neighbor 219.0.0.2
esr(config-bgp-neighbor)# remote-as 2500
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit

```

Включим работу протокола:

```

esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
esr(config)# exit

```

Информацию о BGP-пирах можно посмотреть командой:

```

esr# show ip bgp 2500 neighbors


```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```

esr# show ip bgp

```

 Необходимо в firewall разрешить TCP-порт 179.

1.24 Настройка BFD

BFD (Bidirectional Forwarding Detection) — это протокол, работающий поверх других протоколов, позволяющий сократить время обнаружения проблемы до 50 мс. BFD является двусторонним протоколом, т.е. требует настройки обоих маршрутизаторов (оба маршрутизатора генерируют BFD-пакеты и отвечают друг-другу).

1.24.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|-------|
| 1 | Активировать BFD для протокола OSPF на интерфейсе | esr(config-if-gi)# ip ospf bfd-enable | |
| 2 | Активировать BFD для протокола BGP neighbor на интерфейсе | esr(config-bgp-neighbor)# bfd-enable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 3 | Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно) | esr(config)# ip bfd idle-tx-interval <TIMEOUT> | <TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1510/1700 и [300..65535] для ESR-10/12V(F)/14VF/20/21/100/200 По умолчанию 1 секунда |
| 4 | Включить логирование изменений состояния BFD-протокола (не обязательно) | esr(config)# ip bfd log-adjacency-changes | |
| 5 | Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. Глобально (не обязательно) | esr(config)# ip bfd min-rx-interval <TIMEOUT> | <TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1510/1700 и [300..65535] для ESR-10/12V(F)/14VF/20/21/100/200 По умолчанию: <ul style="list-style-type: none"> • 300 миллисекунд на ESR-10/12V(F)/14VF/20/21/100/200 • 200 миллисекунд на ESR-1000/1200/1500/1510/1700 |
| 6 | Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно) | esr(config)# ip bfd min-tx-interval <TIMEOUT> | <TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1510/1700 и [300..65535] для ESR-10/12V(F)/14VF/20/21/100/200 По умолчанию: <ul style="list-style-type: none"> • 300 миллисекунд на ESR-10/12V(F)/14VF/20/21/100/200 • 200 миллисекунд на ESR-1000/1200/1500/1510/1700 |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 7 | Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. Глобально | esr(config)# ip bfd multiplier <COUNT> | <COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100]. По умолчанию: 5 |
| 8 | Запустить работу механизма BFD с определенным IP-адресом. | esr(config)# ip bfd neighbor <ADDR> [{ interface <IF> tunnel <TUN> }] [local-address <ADDR> [multihop]] [vrf <VRF>] | <ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – интерфейс или группы интерфейсов; <TUN> – тип и номер туннеля; <VRF> – имя экземпляра VRF, задается строкой до 31 символа; multihop – ключ для установки TTL=255, для работы механизма BFD через маршрутизируемую сеть. |
| 9 | Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. Глобально (не обязательно) | esr(config)# ip bfd passive | |
| 10 | Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно) | esr(config-if-gi)# ip bfd idle-tx-interval <TIMEOUT> | <TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1510/1700 и [300..65535] для ESR-10/12V(F)/14VF/20/21/100/200. По умолчанию: 1 секунда |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 11 | <p>Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. На интерфейсе (не обязательно)</p> | esr(config-if-gi)# ip bfd min-rx-interval <TIMEOUT> | <p><TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1510/1700 и [300..65535] для ESR-10/12V(F)/14VF/20/21/100/200</p> <p>По умолчанию:</p> <ul style="list-style-type: none"> • 300 миллисекунд на ESR-10/12V(F)/14VF/20/21/100/200 • 200 миллисекунд на ESR-1000/1200/1500/1510/1700 |
| 12 | <p>Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно)</p> | esr(config-if-gi)# ip bfd min-tx-interval <TIMEOUT> | <p><TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1510/1700 и [300..65535] для ESR-10/12V(F)/14VF/20/21/100/200</p> <p>По умолчанию:</p> <ul style="list-style-type: none"> • 300 миллисекунд на ESR-10/12V(F)/14VF/20/21/100/200 • 200 миллисекунд на ESR-1000/1200/1500/1510/1700 |
| 13 | <p>Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. На интерфейсе (не обязательно)</p> | esr(config-if-gi)# ip bfd multiplier <COUNT> | <p><COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100].</p> <p>По умолчанию: 5</p> |
| 14 | <p>Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. На интерфейсе (не обязательно)</p> | esr(config-if-gi)# ip bfd passive | |

1.24.2 Пример настройки BFD с BGP

Задача:

Необходимо настроить eBGP между ESR R1 и R2 и включить BFD.



Рисунок 25 – Схема сети

Решение:

1. Конфигурирование R1

Предварительно необходимо настроить интерфейс Gi1/0/1:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 10.0.0.1/24
```

Настроим eBGP с BFD:

```
esr(config)# router bgp 100
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.0.0.2
esr(config-bgp-neighbor)# remote-as 200
esr(config-bgp-neighbor)# update-source 10.0.0.1
esr(config-bgp-neighbor)# bfd-enable
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
```

2. Конфигурирование R2

Предварительно необходимо настроить интерфейс Gi1/0/1:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 10.0.0.2/24
```

Настроим eBGP с BFD:

```

esr(config)# router bgp 200
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.0.0.1
esr(config-bgp-neighbor)# remote-as 100
esr(config-bgp-neighbor)# update-source 10.0.0.2
esr(config-bgp-neighbor)# bfd-enable
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit

```

1.25 Настройка политики маршрутизации PBR

1.25.1 Настройка Route-map для BGP

Route-map могут служить фильтрами, позволяющими обрабатывать маршрутную информацию при приеме этой информации от соседа либо при ее передаче соседу. Обработка может включать в себя фильтрацию на основании различных признаков маршрута, а также установку атрибутов (MED, AS-PATH, community, LocalPreference и другое) на соответствующие маршруты.

Также Route-map может назначать маршруты на основе списков доступа (ACL).

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 1 | Создать маршрутную карту для фильтрации и модификации IP-маршрутов. | esr(config)# route-map <NAME> | <NAME> – имя маршрутной карты, задается строкой до 31 символа. |
| 2 | Создать правило маршрутной карты. | esr(config-route-map)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1 .. 10000]. |
| 3 | Указать действие, которое должно быть применено для маршрутной информации. | esr(config-route-map-rule)# action <ACT> | <ACT> – назначаемое действие: <ul style="list-style-type: none"> • permit – прием или анонсирование маршрутной информации разрешено; • deny – запрещено. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 4 | Задать значение атрибута BGPAS-Path в маршруте, для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match as-path [begin end contain] <AS-PATH> | <AS-PATH> – список номеров автономных систем, задается в виде AS,AS,AS, принимает значения [1..4294967295]. Оptionальные параметры: <ul style="list-style-type: none"> • begin – значение атрибута начинается с указанных номеров AS; • end – значение атрибута заканчивается указанными номерами AS; • contain – значение атрибута содержит указанный список номеров AS. |
| 5 | Задать значение атрибута BGPCommunity, для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match community <COMMUNITY-LIST> | <COMMUNITY-LIST> – список community, задается в виде AS:N,AS:N, принимает значения [1..4294967295]. Можно указать до 64 community. |
| 6 | Задать значение атрибута BGPExtendedCommunity, для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match extcommunity <EXTCOMMUNITY-LIST> | <EXTCOMMUNITY-LIST> – список extcommunity, задается в виде KIND:AS:N, KIND:AS:N, где KIND – тип extcommunity: <ul style="list-style-type: none"> • RT (Route Target); • RO (Route Origin); N – номер extcommunity, принимает значения [1..65535]. |
| 7 | Задать профиль IP-адресов, содержащий значения подсетей назначения в маршруте (не обязательно). | esr(config-route-map-rule)# match ip address object-group <OBJ-GROUP- NETWORK -NAME> esr(config-route-map-rule)# match ipv6 address object-group <OBJ-GROUP- NETWORK -NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задается строкой до 31 символа. |
| 8 | Задать профиль IP-адресов, содержащий значения атрибута BGPNext-Hop в маршруте для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match ip next-hop object-group <OBJ-GROUP- NETWORK -NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| | | esr(config-route-map-rule)# match ipv6 next-hop object- group <OBJ-GROUP- NETWORK -NAME> | |
| 9 | Задать профиль, содержащий IP-адреса маршрутизатора, анонсировавшего маршрут, для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match ip route-source object- group <OBJ-GROUP- NETWORK -NAME> esr(config-route-map-rule)# match ipv6 route-source object- group <OBJ-GROUP- NETWORK -NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задается строкой до 31 символа. |
| 10 | Задать ACL группу, для которой должно срабатывать правило. | esr(config-route-map-rule)# match access-group <NAME> | <NAME> – имя списка контроля доступа, задается строкой до 31 символа. |
| 11 | Задать значение атрибута BGP MED в маршруте для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match metric bgp <METRIC> | <METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]. |
| 12 | Задать значение атрибута OSPF Metric в маршруте, для которого должно срабатывать правило. | esr(config-route-map-rule)# match metric ospf <TYPE> <METRIC> | <TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535]. |
| 13 | Задать значение атрибута RIP Metric в маршруте, для которого должно срабатывать правило. | esr(config-route-map-rule)# match metric rip <METRIC> | <METRIC> – значение атрибута RIP Metric, принимает значения [0..16]. |
| 14 | Задать значение атрибута OSPF Tag в маршруте, для которого должно срабатывать правило. | esr(config-route-map-rule)# match tag ospf <TAG> | <TAG> – значение атрибута OSPF Tag, принимает значения [0..4294967295]. |
| 15 | Задать значение атрибута RIP Tag в маршруте, для которого должно срабатывать правило. | esr(config-route-map-rule)# match tag rip <TAG> | <RIP> – значение атрибута RIP Tag, принимает значения [0..65535]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 16 | Задать значение атрибута BGP AS-Path, которое будет добавляться в начало списка AS-Path (не обязательно). | esr(config-route-map-rule)# action set as-path prepend <AS-PATH> {track <TRACK-ID>} | <AS-PATH> – список номеров автономных систем, который будет добавлен к текущему значению в маршруте. Задаётся в виде AS,AS,AS, принимает значения [1..4294967295]. <TRACK-ID> – идентификатор vrrp-tracking, при котором будет исполняться указанное действие. Изменяется в диапазоне [1..60]. |
| 17 | Задать значение атрибута BGP Community, которое будет установлено в маршруте (не обязательно) | esr(config-route-map-rule)# action set community {COMMUNITY-LIST} no-advertise no-export } | <COMMUNITY-LIST> – список community, задается в виде AS:N,AS:N, где каждая часть принимает значения [1..65535]; <ul style="list-style-type: none"> • no - advertise – маршруты, передаваемые с данным community, не должны анонсироваться другим BGP-соседям; • no - export – маршруты, передаваемые с таким community, не должны анонсироваться eBGP-соседям, но анонсируются внешним соседям в конфедерации. |
| 18 | Задать значение атрибута BGP ExtCommunity, которое будет установлено в маршруте (не обязательно). | esr(config-route-map-rule)# action set extcommunity <EXTCOMMUNITY-LIST> | <EXTCOMMUNITY-LIST> – список extcommunity, задается в виде KIND:AS:N, KIND:AS:N, где KIND – тип extcommunity: <ul style="list-style-type: none"> • RT (Route Target); • RO (Route Origin); N – номер extcommunity, принимает значения [1..65535]. |
| 19 | Задать атрибут BGP Next-Hop, который будет установлен в маршруте при анонсировании (не обязательно). | esr(config-route-map-rule)# action set ip bgp-next-hop <ADDR> | <ADDR> – IP-адрес шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-route-map-rule)# action set ipv6 bgp-next-hop <IPV6-ADDR> | <IPV6-ADDR> – IPv6-адрес шлюза, задается в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 20 | Задать значение Next-Hop, которое будет установлено в маршруте, полученном по BGP (не обязательно). | esr(config-route-map-rule)# action set ip next-hop {NEXTHOP} blackhole unreachable prohibit} | <p><NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <ul style="list-style-type: none"> • blackhole – пакеты до данной подсети будут удаляться без отправки уведомлений отправителю; • unreachable – пакеты до данной подсети будут удаляться, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1); • prohibit – пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited code 13). |
| | | esr(config-route-map-rule)# action set ipv6 next-hop <IPv6- NEXTHOP> | <IPv6-NEXTHOP> – IPv6-адрес шлюза, задается в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 21 | Задать значение атрибута BGP Local Preference, который будет установлен в маршруте (не обязательно). | esr(config-route-map-rule)# action set local-preference <PREFERENCE> | <PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [0..255]. |
| 22 | Задать значение атрибута BGP Origin, которое будет установлено в маршруте (не обязательно). | esr(config-route-map-rule)# action set origin <ORIGIN> | <p><ORIGIN> – значение атрибута BGP Origin:</p> <ul style="list-style-type: none"> • egp – маршрут выучен по протоколу EGP; • igp – маршрут получен внутри исходной AS; • incomplete – маршрут выучен другим образом. |
| 23 | Задать значение BGP MED, которое будет установлено в маршруте (не обязательно). | esr(config-route-map-rule)# action set metric bgp <METRIC> | <METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 24 | Добавить фильтрацию и модификацию маршрутов во входящих или исходящих направлениях. | <pre>esr(config-bgp-neighbor)# route-map <NAME><DIRECTION></pre> <pre>esr(config-ipv6-bgp-neighbor)# route-map <NAME><DIRECTION></pre> | <p><NAME> – имя сконфигурированной маршрутной карты;</p> <p><DIRECTION> – направление:</p> <ul style="list-style-type: none"> • in – фильтрация и модификация получаемых маршрутов; • out – фильтрация и модификация анонсируемых маршрутов. |

Пример настройки 1

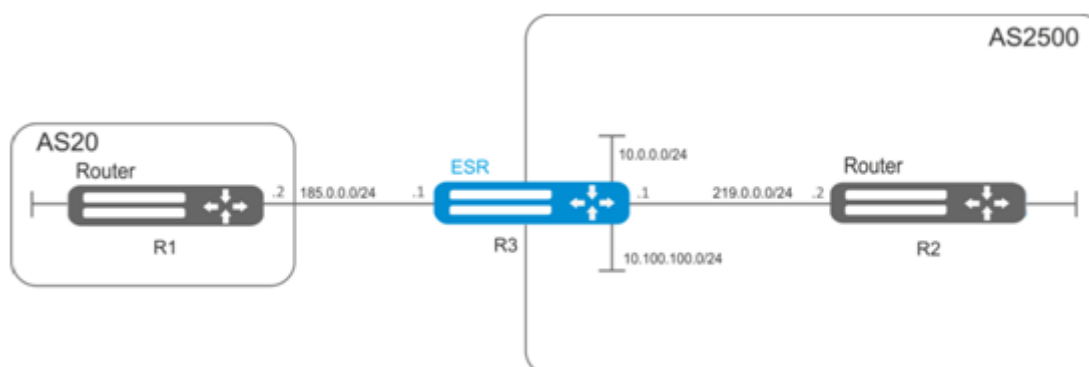


Рисунок 26 – Схема сети

Задача:

Назначить community для маршрутной информации, приходящей из AS 20:

Предварительно нужно выполнить следующие действия:

- Настроить BGP с AS 2500 на маршрутизаторе ESR;
- Установить соседство с AS20.

Решение :

Создаем политику:

```
esr# configure
esr(config)# route-map from-as20
```

Создаем правило 1:

```
esr(config-route-map)# rule 1
```

Если AS PATH содержит AS 20, то назначаем ему community 20:2020 и выходим:


```

esr(config-route-map-rule)# match as-path contain 20
esr(config-route-map-rule)# action set community 20:2020
esr(config-route-map-rule)# exit
esr(config-route-map)# exit

```

В BGP процессе AS 2500 заходим в настройки параметров соседа:

```

esr(config)# router bgp 2500
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 185.0.0.2

```

Привязываем политику к принимаемой маршрутной информации:

```

esr(config-bgp-neighbor)# route-map from-as20 in

```

Пример настройки 2

Задача:

Для всей передаваемой маршрутной информации (с community 2500:25) назначить MED, равный 240, и указать источник маршрутной информации EGP:

Предварительно:

Настроить BGP с AS 2500 на ESR

Решение:

Создаем политику:

```

esr(config)# route-map to-as20

```

Создаем правило:

```

esr(config-route-map)# rule 1

```

Если community содержит 2500:25, то назначаем ему MED 240 и Origin EGP:

```

esr(config-route-map-rule)# match community 2500:25
esr(config-route-map-rule)# action set metric bgp 240
esr(config-route-map-rule)# action set origin egp
esr(config-route-map-rule)# exit
esr(config-route-map)# exit

```

В BGP процессе AS 2500 заходим в настройки параметров соседа:

```

esr(config)# router bgp 2500
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 185.0.0.2

```

Привязываем политику к анонсируемой маршрутной информации:

```

esr(config-bgp-neighbor)# route-map to-as20 out
esr(config-bgp-neighbor)# exit
esr(config-bgp)# exit
esr(config)# exit

```

1.25.2 Route-map на основе списков доступа (Policy-based routing)

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 1 | Создать маршрутную карту для фильтрации и модификации IP-маршрутов. | esr(config)# route-map <NAME> | <NAME> – имя маршрутной карты, задаётся строкой до 31 символа. |
| 2 | Создать правило маршрутной карты | esr(config-route-map)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1 .. 10000]. |
| 3 | Указать действие, которое должно быть применено для маршрутной информации. | esr(config-route-map-rule)# action <ACT> | <ACT> – назначаемое действие: <ul style="list-style-type: none"> • permit – прием или анонсирование маршрутной информации разрешено; • deny – запрещено. |
| 4 | Задать ACL, для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)# match ip access-group <NAME> | <NAME> – имя списка контроля доступа, задаётся строкой до 31 символа. |
| 5 | Задать Next-Hop для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (не обязательно). | esr(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP><METRIC> | <NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <METRIC> – метрика маршрута, принимает значения [0..255]. |
| 6 | Назначить политику маршрутизации на основе списков доступа (ACL). | esr(config-if-gi)# ip policy route-map <NAME> | <NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа. |

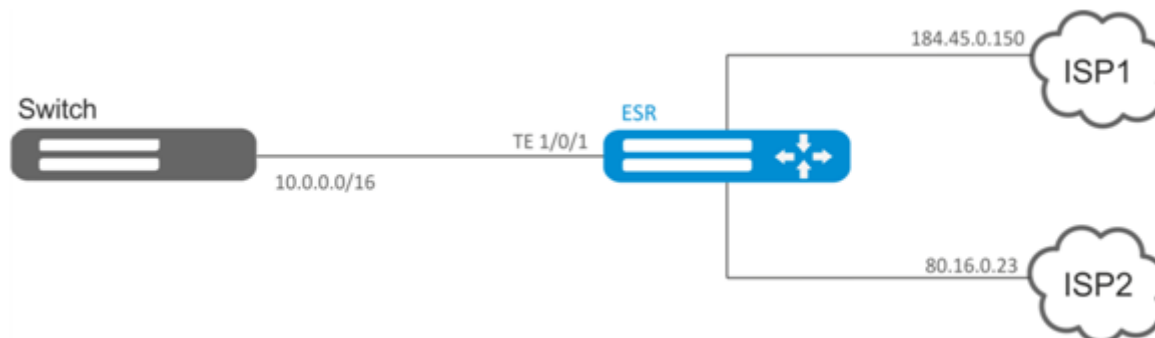
Пример настройки

Рисунок 27 – Схема сети

Задача:

Распределить трафик между Интернет провайдерами на основе подсетей пользователей.

Предварительно нужно назначить IP-адреса на интерфейсы.

Требуется направлять трафик с адресов 10.0.20.0/24 через ISP1 (184.45.0.150), а трафик с адресов 10.0.30.0/24 – через ISP2 (80.16.0.23). Требуется контролировать доступность адресов провайдеров (работоспособность подключений к ISP), и при неработоспособности одного из подключений переводить с него на рабочее подключение весь трафик.

Решение :

Создаем ACL:

```

esr# configure
esr(config)# ip access-list extended sub20
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.20.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended sub30
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.30.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit

```

Создаем политику:

```

esr(config)# route-map PBR

```

Создаем правило 1:

```
esr(config-route-map)# rule 1
```

Указываем список доступа (ACL) в качестве фильтра:

```
esr(config-route-map-rule)# match ip access-group sub20
```

Указываем next-hop для sub20:

```
esr(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 10
esr(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 30
esr(config-route-map-rule)# exit
esr(config-route-map)# exit
```

Правилom 1 будет обеспечена маршрутизация трафика из сети 10.0.20.0/24 на адрес 184.45.0.150, а при его недоступности – на адрес 80.16.0.23. Приоритетность шлюзов задается значениями метрик – 10 и 30.

Создаем правило 2:

```
esr(config-route-map)# rule 2
```

Указываем список доступа (ACL) в качестве фильтра:

```
esr(config-route-map-rule)# match ip access-group sub30
```

Указываем nexthop для sub30 и выходим:

```
esr(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 10
esr(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 30
esr(config-route-map-rule)# exit
esr(config-route-map)# exit
```

Правилom 2 будет обеспечена маршрутизация трафика из сети 10.0.30.0/24 на адрес 80.16.0.23, а при его недоступности – на адрес 184.45.0.150. Приоритетность задается значениями метрик.

Заходим на интерфейс TE 1/0/1:

```
esr(config)# interface tengigabitethernet 1/0/1
```

Привязываем политику на соответствующий интерфейс:

```
esr(config-if-te)# ip policy route-map PBR
```

1.26 Настройка GRE-туннелей

GRE (англ. Generic Routing Encapsulation – общая инкапсуляция маршрутов) – протокол туннелирования сетевых пакетов. Его основное назначение – инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты. GRE может использоваться для организации VPN на 3-м уровне модели OSI. В маршрутизаторе ESR реализованы статические неуправляемые GRE-туннели, то есть туннели создаются

вручную путем конфигурирования на локальном и удаленном узлах. Параметры туннеля для каждой из сторон должны быть взаимосогласованными или переносимые данные не будут декапсулироваться партнером.

1.26.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 1 | Сконфигурировать L3-интерфейс, от которого будет строиться GRE-туннель. | | |
| 2 | Создать GRE-туннель и перейти в режим его конфигурирования. | esr(config)# tunnel gre <INDEX> | <p><INDEX> – идентификатор туннеля в диапазоне:</p> <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1..10]; • для ESR-20/21/100/200 – [1..250]; • для ESR-1000/1200/1500/1510/1700 – [1..500]. |
| 3 | Указать экземпляр VRF, в котором будет работать данный GRE-туннель (не обязательно). | esr(config- bridge)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Указать описание конфигурируемого туннеля (не обязательно). | esr(config-gre)# description <DESCRIPTION> | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 5 | Установить локальный IP-адрес для установки туннеля. | esr(config-gre)# local address <ADDR> | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-gre)# interface <IF> | <IF> – интерфейс, от IP-адреса которого устанавливается туннель. |
| 6 | Установить удаленный IP-адрес для установки туннеля. | esr(config-gre)# remote address <ADDR> | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 7 | Указать режим инкапсуляции для GRE туннеля. | esr(config-gre)# mode <MODE> | <p><MODE> – режим инкапсуляции для GRE туннеля:</p> <ul style="list-style-type: none"> • ip – инкапсуляция IP-пакетов в GRE; • ethernet – инкапсуляция Ethernet-фреймов в GRE. <p>Значение по умолчанию: ip</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 8 | Установить IP-адрес локальной стороны туннеля (только в режиме ip). | esr(config-gre)# ip address <ADDR/LEN> | <p><ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].</p> <p>Можно указать до 8 IP-адресов перечислением через запятую.</p> |
| 9 | Назначить широковещательный домен для инкапсуляции в GRE-пакеты данного туннеля (только в режиме ethernet). | esr(config-gre)# bridge-group <BRIDGE-ID> | <p><BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне:</p> <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1..50]; • для ESR-20/21/100/200 – [1..250]; • для ESR-1000/1200/1500/1510/1700 – [1..500] |
| 10 | Указать размер MTU (MaximumTransmissionUnit) для туннеля (не обязательно). MTU более 1500 будет активно только если применена команда "system jumbo-frames" | esr(config-gre)# mtu <MTU> | <p><MTU> – значение MTU, принимает значения в диапазоне:</p> <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1280..9600]; • для ESR-20/21 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 [1280..10000]. <p>Значение по умолчанию: 1500.</p> |
| 11 | Указать значение времени жизни TTL для туннельных пакетов (не обязательно). | esr(config-gre)# ttl <TTL> | <p><TTL> – значение TTL, принимает значения в диапазоне [1..255].</p> <p>Значение по умолчанию: Наследуется от инкапсулируемого пакета.</p> |
| 12 | Указать DSCP для использования в IP-заголовке инкапсулирующего пакета (не обязательно). | esr(config-gre)# dscp <DSCP> | <p><DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].</p> <p>Значение по умолчанию: наследуется от инкапсулируемого пакета.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 13 | Разрешить передачу ключа (Key) в туннельном заголовке GRE (в соответствии с RFC 2890) и установить значение ключа. Настраивается с обеих сторон туннеля. (не обязательно). | esr(config-gre)# key <KEY> | <KEY> – значение KEY, принимает значения в диапазоне [1..2000000]. Значение по умолчанию: ключ не передаётся. |
| 14 | Включить вычисление контрольной суммы и занесение её в GRE-заголовок отправляемых пакетов. При этом на удаленной стороне необходимо включить проверку контрольной суммы. (не обязательно) | esr(config-gre)# local checksum | |
| 15 | Включить проверку наличия и соответствия значений контрольной суммы в заголовках принимаемых GRE-пакетов. При этом на удаленной стороне необходимо включить вычисление контрольной суммы. (не обязательно) | esr(config-gre)# remote checksum | |
| 16 | Включить проверку доступности удаленного шлюза туннеля (не обязательно) | esr(config-gre)# keepalive enable | |
| 17 | Задать время ожидания keepalive пакетов от встречной стороны (не обязательно) | esr(config-gre)# keepalive timeout <TIME> | <TIME> – время в секундах, принимает значения в диапазоне [1..32767]. Значение по умолчанию: 10 |
| 18 | Задать количество попыток проверки доступности удаленного шлюза туннеля (не обязательно) | esr(config-gre)# keepalive retries <VALUE> | <VALUE> – количество попыток, принимает значения в диапазоне [1..255]. Значение по умолчанию: 5 |
| 19 | Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно) | esr(config-gre)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5 |
| 20 | Включить отправку snmp-trap о включении/отключении туннеля. | esr(config-gre)# snmp init-trap | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 21 | Включить механизм перезапроса IP-адресов по протоколу DHCP на указанных интерфейсах при отключении GRE-туннеля по keepalive (не обязательно) | esr(config-gre)# keepalive dhcp dependent-interface <IF> | <IF> – физический/логический интерфейс, на котором включено получение IP-адреса по DHCP |
| 22 | Задать интервал времени между отключением GRE-туннеля и перезапросом IP-адреса на интерфейсе/интерфейсах, указанных командой keepalive dhcp dependent-interface (не обязательно) | esr(config-gre)# keepalive dhcp link-timeout <SEC> | <SEC> – интервал между отключением GRE-туннеля и перезапросом IP-адреса по DHCP на интерфейсах |
| 23 | Активировать туннель. | esr(config-gre)# enable | |

1.26.2 Пример настройки IP-GRE-туннеля

Задача:

Организовать L3-VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол GRE.

- в качестве локального шлюза для туннеля используется IP-адрес 115.0.0.1;
- в качестве удаленного шлюза для туннеля используется IP-адрес 114.0.0.10;
- IP-адрес туннеля на локальной стороне 25.0.0.1/24.



Рисунок 28 – Схема сети

Решение:

Предварительно на маршрутизаторах должны быть настроены интерфейсы для связи с сетью WAN разрешено получение пакетов протокола GRE из зоны безопасности, в которой работают интерфейсы, подключенные к сети WAN.

Создадим туннель GRE 10:

```
esr(config)# tunnel gre 10
```

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

```
esr(config-gre)# local address 115.0.0.1
esr(config-gre)# remote address 114.0.0.10
```


Укажем IP-адрес туннеля 25.0.0.1/24:

```
esr(config-gre)# ip address 25.0.0.1/24
```

Также туннель должен принадлежать к зоне безопасности, для того чтобы можно было создать правила, разрешающие прохождение трафика в firewall. Принадлежность туннеля к зоне задается следующей командой:

```
esr(config-gre)# security-zone untrusted
```

Включим туннель:

```
esr(config-gre)# enable
esr(config-gre)# exit
```

На маршрутизаторе должен быть создан маршрут до локальной сети партнера. В качестве интерфейса назначения указываем ранее созданный туннель GRE:

```
esr(config)# ip route 172.16.0.0/16 tunnel gre 10
```

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партнеру, независимо от наличия GRE-туннеля и правильности настроек с его стороны.

Опционально для GRE-туннеля можно указать следующие параметры:

- Включить вычисление и включение в пакет контрольной суммы заголовка GRE и инкапсулированного пакета для исходящего трафика:

```
esr(config-gre)# local checksum
```

- Включить проверку наличия и корректности контрольной суммы GRE для входящего трафика:

```
esr(config-gre)# remote checksum
```

- Указать уникальный идентификатор:

```
esr(config-gre)# key 15808
```

- Указать значение DSCP, MTU, TTL:

```
esr(config-gre)# dscp 44
esr(config-gre)# mtu 1426
esr(config-gre)# ttl 18
```

- Включить и настроить механизм keepalive:

```
esr(config-gre)# keepalive enable
esr(config-gre)# keepalive timeout <TIME>
esr(config-gre)# keepalive retries <VALUE>
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status gre 10
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters gre 10
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration gre 10
```

Настройка туннеля IPv4-over-IPv4 производится аналогичным образом.

⚠ При создании туннеля необходимо в firewall разрешить протокол GRE(47).

1.27 Настройка DMVPN

DMVPN (*Dynamic Multipoint Virtual Private Network*) – технология для создания виртуальных частных сетей, с возможностью динамического создания туннелей между узлами. Преимуществом данного решения является высокая масштабируемость и легкость настройки при подключении филиалов к головному офису. DMVPN используется в топологии Hub-and-Spoke, и позволяет строить прямые VPN туннели Spoke-to-Spoke в дополнение к обычным Spoke-to-Hub туннелям. Это означает, что филиалы смогут общаться друг с другом напрямую, без необходимости прохождения трафика через Hub.

Чтобы установить такое соединение, клиенты (NHS) по зашифрованному IPsec-туннелю отправляют соответствие своего внутреннего (туннельного) адреса и внешнего (NBMA) адреса на NHRP-сервер (NHS). Когда клиент захочет соединиться с другим NHS, он посылает на сервер запрос, чтобы узнать его внешний адрес. Получив ответ от сервера, клиент теперь самостоятельно может устанавливать соединение с удалённым филиалом.

1.27.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 1 | Проверить доступность “внешних” IP-адресов, находящихся на физических интерфейсах. | | |
| 2 | Подготовить IPsec-туннели для работы совместно с динамическими GRE-туннелями. | | См. раздел Настройка Policy-based IPsec VPN . |
| 3 | Перейти в режим конфигурирования GRE-туннеля и перевести GRE-туннель в режим multipoint. | esr (config - gre)# multipoint | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 4 | Установить открытый пароль для NHRP пакетов (не обязательно). | esr(config-gre)# ip nhrp authentication <WORD> | <WORD> – пароль в открытой форме, задается строкой [1..8] символов, может включать символы [0-9a-fA-F]. |
| 5 | Указать время, в течении которого на NHS будет существовать запись о данном клиенте (не обязательно). | esr(config-gre)# ip nhrp holding-time <TIME> | <TIME> – время в секундах, в течении которого на сервере будет существовать запись о данном клиенте, принимает значения [1..65535]. Значение по умолчанию: 7200 |
| 6 | Задать «логический(туннельный)» адрес NHRP сервера. | esr(config-gre)# ip nhrp nhs <ADDR> [no-registration] | <ADDR/LEN> – адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; • no - registration – не регистрироваться на NHRP сервере. |
| 7 | Задать соответствие «внутреннего» туннельного адреса с «внешним» NBMA адресом. | esr(config-gre)# ip nhrp map <ADDR> <ADDR> | <ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 8 | Определить адресата мультикастного трафика. | esr(config-gre)# ip nhrp multicast { dynamic nhs <ADDR> } | • dynamic – отправлять на все пиры, с которыми есть соединение; • nhs – отправлять на все статические сконфигурированные сервера; <ADDR> – отправлять на специфически сконфигурированный адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 9 | Включить возможность отправки NHRP Traffic Indication пакетов. Выполняется на NHS (не обязательно). | esr(config-gre)# ip nhrp redirect | |
| 10 | Включить возможность создания кратчайших маршрутов. Выполняется на NHS(не обязательно). | esr(config-gre)# ip nhrp shortcut | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 11 | Привязать IPsec-VPN к mGRE туннелю (не обязательно). | esr(config-gre)# ip nhrp ipsec <WORD> { static dynamic } | <p><WORD> – имя VPN, задаётся строкой до 31 символа;</p> <ul style="list-style-type: none"> • static – статическое соединение, применяется для связи с NHS; • dynamic – динамически устанавливаемое соединение, конфигурируется для связи между NHS. |
| 12 | Включить работу протокола NHRP. | esr(config-gre)# ip nhrp enable | |
| 13 | Организовать IP-связность посредством протокола динамической маршрутизации. | | |

1.27.2 Пример настройки

Задача:

Организовать DMVPN между офисами компании, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (BGP), Ipsec. В нашем примере у нас будет HUB маршрутизатор и два филиала. HUB – это DMVPN сервер (NHS), а филиалы – DMVPN клиенты (NHC).

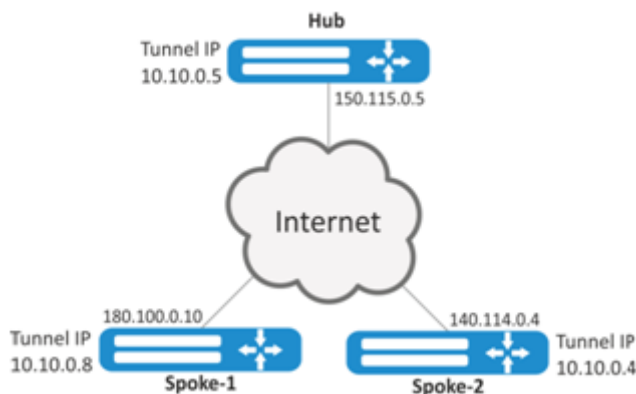


Рисунок 29 – Схема сети

Hub внешний IP-адрес – 150.115.0.5;

Spoke-1 внешний IP-адрес – 180.100.0.10;

Spoke-2 внешний IP-адрес – 140.114.0.4.

Параметры IPsec VPN:

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: SHA1.

IPsec:

- алгоритм шифрования: AES128;
- алгоритм аутентификации: SHA1.

Решение:

1. Конфигурирование Hub
Создадим туннель GRE:

```
esr# configure
esr(config)# tunnel gre 5
```

Укажем IP-адрес интерфейса, граничащего с ISP:

```
esr(config-gre)# local address 150.115.0.5
```

Зададим значение MTU:

```
esr(config-gre)# mtu 1416
```

Установим значение ttl:

```
esr(config-gre)# ttl 16
```

Зададим IP-адрес GRE туннеля:

```
esr(config-gre)# ip address 10.10.0.5/24
```

Переведём GRE-туннель в multipoint режим для возможности соединения с несколькими точками:

```
esr(config-gre)# multipoint
```

Перейдём к настройке NHRP. Настроим отправку мультикастовых рассылок в динамически узнаваемые адреса:

```
esr(config-gre)# ip nhrp multicast dynamic
```

Произведём настройку протокола динамической маршрутизации для Hub. В нашем примере это будет BGP:

```
esr(config)# router bgp 65005
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.8
esr(config-bgp-neighbor)# remote-as 65008
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# neighbor 10.10.0.4
esr(config-bgp-neighbor)# remote-as 65004
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

Произведём настройку IPsec для Hub:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 150.115.0.5
esr(config-ike-gw)# local network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

Привяжем IPsec к GRE туннелю, чтобы клиенты могли устанавливать шифрованное соединение:

```
esr(config-gre)# ip nhrp ipsec IPSECVPN dynamic
```

Включим работу NHRP и сам туннель:

```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

2. Конфигурирование Spoke

Проведём стандартную настройку DMVPN на туннеле:

```

esr# configure
esr(config-gre)# tunnel gre 8
esr(config-gre)# mtu 1416
esr(config-gre)# ttl 16
esr(config-gre)# multipoint
esr(config-gre)# local address 180.100.0.10
esr(config-gre)# ip address 10.10.0.8/24

```

Указываем сколько времени будет храниться запись о клиенте на сервере:

```

esr(config-gre)# ip nhrp holding-time 300

```

Указываем туннельный адрес NHS:

```

esr(config-gre)# ip nhrp nhs 10.10.0.5/24

```

Зададим соответствие туннельному адресу – реальный:

```

esr(config-gre)# ip nhrp map 10.10.0.5 150.115.0.5

```

Настроим мультикастовую рассылку на NHRP сервер:

```

esr(config)# ip nhrp multicast nhs

```

Произведём настройку BGP для spoke:

```

esr(config)# router bgp 65008
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.5
esr(config-bgp-neighbor)# remote-as 65005
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable

```

Произведём настройку IPsec. При создании шлюза протокола IKE для NHS, укажем конкретные адреса назначения. А при создании шлюза IKE для NHC – адрес назначения будет any:

```

esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit

```

```

esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit

```

```

esr(config)# security ike gateway IKEGW_HUB
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address 150.115.0.5
esr(config-ike-gw)# remote network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit

```

```

esr(config)# security ike gateway IKEGW_SPOKE
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit

```

```

esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit

```

```

esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit

```

```

esr(config)# security ipsec vpn IPSECVPN_HUB
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_HUB
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable

```

```

esr(config)# security ipsec vpn IPSECVPN_SPOKE
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_SPOKE
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable

```

Привяжем IPsec к GRE туннелю, для возможности установления зашифрованного соединения с сервером и с другими клиентами сети:

```

esr(config-gre)# ip nhrp ipsec IPSECVPN_HUB static
esr(config-gre)# ip nhrp ipsec IPSECVPN_SPOKE dynamic

```

Включим работу NHRP и сам туннель:


```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

Состояние NHRP записей можно посмотреть командой:

```
esr# show ip nhrp
```

Очистить NHRP записи можно командой:

```
esr# clear ip nhrp
```

1.28 Настройка L2TPv3-туннелей

L2TPv3 (Layer 2 Tunneling Protocol Version 3) – протокол для туннелирования пакетов 2-го уровня модели OSI между двумя IP-узлами. В качестве инкапсулирующего протокола используется IP или UDP. L2TPv3 может использоваться как альтернатива MPLS P2P L2VPN (VLL) для организации VPN уровня L2. В маршрутизаторе ESR реализованы статические неуправляемые L2TPv3-туннели, то есть туннели создаются вручную путем конфигурирования на локальном и удаленном узлах. Параметры туннеля на каждой из сторон должны быть взаимосогласованными или переносимые данные не будут декапсулироваться партнером.

1.28.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Сконфигурировать L3-интерфейс, от которого будет строиться L2TPv3-туннель. | | |
| 2 | Создать L2TPv3-туннель и перейти в режим его конфигурирования. | esr(config)# tunnel l2tpv3 <INDEX> | <INDEX> – идентификатор туннеля в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1..10]; • для ESR-20/21/100/200 – [1..250]; • для ESR-1000/1200/1500/1510/1700 – [1..500]. |
| 3 | Указать описание конфигурируемого туннеля (не обязательно). | esr(config-l2tpv3)# description <DESCRIPTION> | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 4 | Указать экземпляр VRF, в котором будет работать данный L2TPv3-туннель (не обязательно). | esr(config-l2tpv3)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 5 | Установить локальный IP-адрес для установки туннеля. | esr(config-l2tpv3)# local address <ADDR> | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 6 | Установить удаленный IP-адрес для установки туннеля. | esr(config-l2tpv3)# remote address <ADDR> | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 7 | Выбрать метод инкапсуляции для туннеля L2TPv3. | esr(config-l2tpv3)# protocol <TYPE> | <TYPE> – тип инкапсуляции, возможные значения: <ul style="list-style-type: none"> • ip - инкапсуляция в IP-пакет; • udp инкапсуляция в UDP-дейтаграммы. |
| 8 | Установить локальный идентификатор сессии. | esr(config-l2tpv3)# local session-id <SESSION-ID> | <SESSION-ID> – идентификатор сессии, принимает значения [1..200000]. |
| 9 | Установить удаленный идентификатор сессии. | esr(config-l2tpv3)# remote session-id <SESSION-ID> | <SESSION-ID> – идентификатор сессии, принимает значения [1..200000]. |
| 10 | Определить локальный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол). | esr(config-l2tpv3)# local port <UDP> | <UDP> – номер UDP-порта в диапазоне [1..65535]. |
| 11 | Определить удаленный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол). | esr(config-l2tpv3)# remote port <UDP> | <UDP> – номер UDP-порта в диапазоне [1..65535]. |
| 12 | Назначить широковещательный домен для инкапсуляции в L2TPv3-пакеты данного туннеля. | esr(config-l2tpv3)# bridge-group <BRIDGE-ID> | <BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1..50]; • для ESR-20/21/100/200 – [1..250]; • для ESR-1000/1200/1500/1510/1700 – [1..500] |
| 13 | Активировать туннель. | esr(config-l2tpv3)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 14 | Указать размер MTU (MaximumTransmissionUnit) для туннелей (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | esr(config-l2tpv3)# mtu <MTU> | <MTU> – значение MTU, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1280..9600]; • для ESR-20/21 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 [1280..10000]. Значение по умолчанию: 1500. |
| 15 | Определить локальное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно). | esr(config-l2tpv3)# local cookie <COOKIE> | <COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде. |
| 16 | Определить удаленное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно). | esr(config-l2tpv3)# remote cookie <COOKIE> | <COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде. |
| 17 | Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно). | esr(config-l2tpv3)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5. |

1.28.2 Пример настройки L2TPv3-туннеля

Задача:

Организовать L2 VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол L2TPv3.

- в качестве инкапсулирующего протокола используется UDP, номер порта на локальной стороне и номер порта на стороне партнера 519;
- в качестве локального шлюза для туннеля используется IP-адрес 21.0.0.1;
- в качестве удаленного шлюза для туннеля используется IP-адрес 183.0.0.10;
- идентификатор туннеля на локальной стороне равен 2, на стороне партнера 3;
- идентификатор сессии внутри туннеля равен 100, на стороне партнера 200;
- в туннель направим трафик из bridge с идентификатором 333.



Рисунок 30 – Схема сети

Решение:

Создадим туннель L2TPv3 333:

```
esr# configure
esr(config)# tunnel l2tpv3 333
```

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

```
esr(config-l2tpv3)# local address 21.0.0.1
esr(config-l2tpv3)# remote address 183.0.0.10
```

Укажем тип инкапсулирующего протокола и номера UDP-портов:

```
esr(config-l2tpv3)# protocol udp
esr(config-l2tpv3)# local port 519
esr(config-l2tpv3)# remote port 519
```

Укажем идентификаторы сессии внутри туннеля для локальной и удаленной сторон:

```
esr(config-l2tpv3)# local session-id 100
esr(config-l2tpv3)# remote session-id 200
```

Установим принадлежность L2TPv3-туннеля к мосту, который должен быть связан с сетью удаленного офиса (настройка моста рассматривается в пункте [Пример настройки bridge для VLAN и L2TPv3-туннеля](#)):

```
esr(config-l2tpv3)# bridge-group 333
```

Включим ранее созданный туннель и выйдем:

```
esr(config-l2tpv3)# enable
esr(config-l2tpv3)# exit
```

Создадим суб-интерфейс для коммутации трафика, поступающего из туннеля, в локальную сеть с тегом VLAN id 333:

```
esr(config)# interface gi 1/0/2.333
```

Установим принадлежность суб-интерфейса к мосту, который должен быть связан с локальной сетью (настройка моста рассматривается в пункте [Настройка PPP через E1](#)):

```
esr(config-subif)# bridge-group 333
esr(config-subif)# exit
```

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партнеру, независимо от наличия L2TPv3 туннеля и правильности настроек с его стороны.

Настройки туннеля в удаленном офисе должны быть зеркальными локальным. В качестве локального шлюза должен использоваться IP-адрес 183.0.0.10. В качестве удаленного шлюза должен использоваться IP-адрес 21.0.0.1. Номер порта инкапсулирующего протокола на локальной стороне и стороне партнера 519. Идентификатор сессии внутри туннеля должен быть равным 200, на стороне партнера 100. Также туннель должен принадлежать мосту, который необходимо соединить с сетью партнера.

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status l2tpv3 333
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters l2tpv3 333
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration l2tpv3 333
```

⚠ Помимо создания туннеля необходимо в firewall разрешить входящий трафик по протоколу UDP с портом отправителя 519 и портом назначения 519.

1.29 Настройка IPsec VPN

IPsec – это набор протоколов, которые обеспечивают защиту передаваемых с помощью IP-протокола данных. Данный набор протоколов позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

1.29.1 Настройка Route-based IPsec VPN

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Создать VTI-туннель и перейти в режим его конфигурирования. | esr(config)# tunnel vti <TUN> | <TUN> – имя туннеля устройства. |
| 2 | Указать локальный IP-адрес VTI-туннеля. | esr(config-vti)#local address <ADDR> | <ADDR> – IP-адрес локального шлюза. |
| 3 | Указать удаленный IP-адрес VTI-туннеля. | esr(config-vti)#remote address <ADDR> | <ADDR> – IP-адрес удаленного шлюза. |
| 4 | Установить IP-адрес локальной стороны VTI-туннеля | esr(config-vti)# ip address <ADDR/LEN> | <ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 5 | Включить VTI-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для VTI-туннеля. | esr(config-vti)# security-zone<NAME> esr(config-vti)# ip firewall disable | <NAME> – имя зоны безопасности, задаётся строкой до 12 символов. |
| 6 | Включить туннель. | esr(config-vti)#enable | |
| 7 | Создать IKE-профиль и перейти в режим его конфигурирования. | esr(config)# security ike proposal <NAME> | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 8 | Указать описание конфигулируемого IKE-профиля (не обязательно). | esr(config-ike- proposal)# description<DESCRIPTION> | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 9 | Определить алгоритм аутентификации для IKE. (не обязательно) | esr(config-ike- proposal)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1 |
| 10 | Определить алгоритм шифрования для IKE. (не обязательно) | esr(config-ike- proposal)# encryption algorithm <ALGORITHM> | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des |
| 11 | Определить номер группы Диффи-Хеллмана. (не обязательно) | esr(config-ike- proposal)# dh-group <DH-GROUP> | <DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1 |
| 12 | Определить режим аутентификации IKE. (не обязательно) | esr(config-ike- proposal)# authentication method <METHOD> | <METHOD> – метод аутентификации ключа. Может принимать значения: <ul style="list-style-type: none"> • pre - shared - key – метод аутентификации, использующий предварительно полученные ключи шифрования; • rsa - public - key – метод аутентификации, использующий RSA-сертификат. Значение по умолчанию: pre-shared-key |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 13 | Создать ike-политику и перейти в режим её конфигурирования. | esr(config)# security ike policy <NAME> | <NAME> – имя политики IKE, задаётся строкой до 31 символа. |
| 14 | Задать время жизни соединения протокола IKE (не обязательно). | esr(config-ike- proposal)# lifetime seconds <SEC> | <SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 3600 |
| 15 | Привязать IKE-профиль к IKE-политике. | esr(config-ike-policy)# proposal <NAME> | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 16 | Указать ключ аутентификации. (обязательно, если в качестве режима аутентификации выбран pre-shared-key) | esr(config-ike-policy)# pre-shared-key ascii-text<TEXT> | <TEXT> – строка [1..64] ASCII символов. |
| 17 | Создать IKE-шлюз и перейти в режим его конфигурирования. | esr(config)# security ike gateway <NAME> | <NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. |
| 18 | Привязать IKE-политику к IKE-шлюзу. | esr(config-ike-gw)# ike-policy <NAME> | <NAME> – имя политики протокола IKE, задаётся строкой до 31 символа. |
| 19 | Указать версию IKE (не обязательно). | esr(config-ike-gw)# version <VERSION> | <version> – версия IKE-протокола: v1-only или v2-only. Значение по умолчанию: v1-only |
| 20 | Установить режим перенаправления трафика в туннель – route-based. | esr(config-ike-gw)# mode route-based | |
| 21 | Указать действие для DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection action <MODE> | <MODE> – режим работы DPD: <ul style="list-style-type: none"> • restart – соединение переустанавливается; • clear – соединение останавливается; • hold – соединение поддерживается; • none – механизм выключен, никаких действий не предпринимается. Значение по умолчанию: none |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 22 | Указать интервал между отправкой сообщений механизмом DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection interval <SEC> | <SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. Значение по умолчанию: 2 |
| 23 | Указать период времени для ответа на сообщения механизма DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection timeout <SEC> | <SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд |
| 24 | Привязать VTI-туннель к IKE-шлюзу. | esr(config-ike-gw)# bind-interface vti <VTI> | <VTI> – идентификационный номер интерфейса VTI. |
| 25 | Создать в IPsec-профиль. | esr(config)# security ipsec proposal <NAME> | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |
| 26 | Определить алгоритм аутентификации для IPsec. (не обязательно) | esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1 |
| 27 | Определить алгоритм шифрования для IPsec. (не обязательно) | esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM> | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des |
| 28 | Указать протокол инкапсуляции для IPsec (не обязательно). | esr(config-ipsec- proposal)# protocol <PROTOCOL> | <PROTOCOL> – инкапсулирующий протокол, принимает значения Значение по умолчанию: esp |
| 29 | Создать IPsec-политику и перейти в режим её конфигурирования. | esr(config)# security ipsec policy <NAME> | <NAME> – имя политики IPsec, задаётся строкой до 31 символа. |
| 30 | Привязать IPsec-профиль к IPsec-политике | esr(config-ipsec-policy)# proposal <NAME> | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 31 | Задать время жизни IPsec-туннеля (не обязательно). | esr(config-ipsec-policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> } | <p><SEC> – период времени жизни IPsec-туннеля, по истечении происходит пересогласование. Принимает значения [1140..86400] секунд.</p> <p><PACKETS> – количество пакетов, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400].</p> <p><KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд.</p> <p>Значение по умолчанию: 28800 секунд</p> |
| 32 | Создать IPsec VPN и перейти в режим конфигурирования. | esr(config)# security ipsec vpn <NAME> | <NAME> – имя VPN, задаётся строкой до 31 символа. |
| 33 | Определить режим согласования данных, необходимых для активации VPN. | esr(config-ipsec-vpn)# mode <MODE> | <MODE> – режим работы VPN. |
| 34 | Привязать IPsec-политику к IPsec-VPN. | esr(config-ipsec-vpn)# ike ipsec-policy <NAME> | <NAME> – имя IPsec-политики, задаётся строка до 31 символа. |
| 35 | Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно). | esr(config-ipsec-vpn)# ike dscp <DSCP> | <p>DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].</p> <p>Значение по умолчанию: 63</p> |
| 36 | Установить режим активации VPN. | esr(config-ipsec-vpn)# ike establish-tunnel <MODE> | <p><MODE> – режим активации VPN:</p> <ul style="list-style-type: none"> • by - request – соединение активируется встречной стороной; • route – соединение активируется при появлении трафика, маршрутизируемого в туннель; • immediate – туннель активируется автоматически после применения конфигурации. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 37 | Осуществить привязку IKE-шлюза к IPsec-VPN. | esr(config-ipsec-vpn)# ike gateway <NAME> | <NAME> – имя IKE-шлюза, задаётся строкой до 31 символа. |
| 38 | Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно). | esr(config-ipsec-vpn)# ike idle-time <TIME> | <TIME> – интервал в секундах, принимает значения [4..86400]. |
| 39 | Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (не обязательно). | esr(config-ipsec-vpn)# ike rekey disable | |
| 40 | Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (не обязательно). | esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> } | <p><SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой <code>lifetimeseconds</code>, см. 22.2.13). Принимает значения [4..86400].</p> <p><PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой <code>lifetimepackets</code>). Принимает значения [4..86400]</p> <p><KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой <code>lifetimekilobytes</code>). Принимает значения [4..86400]</p> <p>Значение по умолчанию:</p> <ul style="list-style-type: none"> • Пересогласование ключей до истечения времени – за 540 секунд. • Пересогласование ключей до истечения объема трафика и количества пакетов – отключено. |
| 41 | Установить уровень случайного разброса значений параметров <code>margin seconds</code> , <code>margin packets</code> , <code>margin kilobytes</code> (не обязательно). | esr(config-ipsec-vpn)# ike rekey randomization <VALUE> | <p><VALUE> – максимальный процент разброса значений, принимает значения [1..100].</p> <p>Значение по умолчанию: 100%</p> |
| 42 | Указать описание для IPsec-VPN (не обязательно). | esr(config-ipsec-vpn)# description <DESCRIPTION> | <DESCRIPTION> – описание профиля, задаётся строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|-------------------------|--------------------------------------|-------|
| 43 | Активировать IPsec VPN. | esr(config-ipsec-vpn)# enable | |

Пример настройки

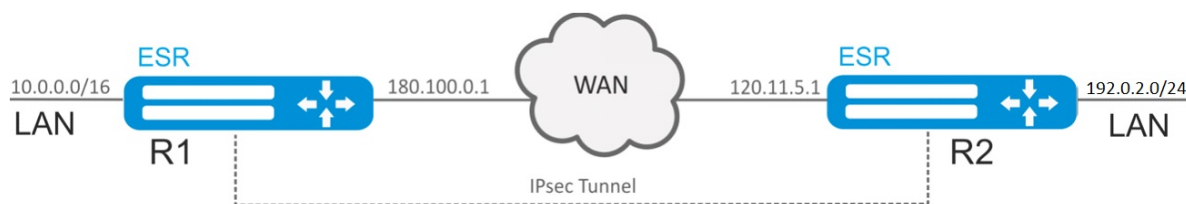


Рисунок 31 – Схема сети

Задача:

Настроить IPsec-туннель между R1 и R2.

- R1 IP-адрес – 120.11.5.1;
- R2 IP-адрес – 180.100.0.1;

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

IP sec:

- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

Решение:

1. Конфигурирование R1

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

Создадим туннель VTI. Трафик будет перенаправляться через VTI в IPsec-туннель. В качестве локального и удаленного шлюза указываются IP-адреса интерфейсов, граничащих с WAN:

```
esr(config)# tunnel vti 1
esr(config-vti)# local address 180.100.0.1
esr(config-vti)# remote address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit

```

Создадим статический маршрут до удаленной LAN-сети. Для каждой подсети, которая находится за IPsec-туннелем, нужно указать маршрут через VTI-туннель:

```

esr(config)# ip route 192.0.2.0/24 tunnel vti 1

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэлла 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```

esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```

esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit

```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```

esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Создадим туннель VTI. Трафик будет перенаправляться через VTI в IPsec-туннель. В качестве локального и удаленного шлюза указываются IP-адреса интерфейсов, граничащих с WAN:

```
esr(config)# tunnel vti 1
esr(config-vti)# remote address 180.100.0.1
esr(config-vti)# local address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

Создадим статический маршрут до удаленной LAN-сети. Для каждой подсети, которая находится за IPsec-туннелем, нужно указать маршрут через VTI-туннель:

```
esr(config)# ip route 10.0.0.0/16 tunnel vti 1
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration ipsec1
```

⚠ В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500).

1.29.2 Настройка Policy-based IPsec VPN

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Создать IKE-экземпляр и перейти в режим его конфигурирования. | esr(config)# security ike proposal <NAME> | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигулируемого туннеля (не обязательно). | esr(config-ike- proposal)# description<DESCRIPTION> | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 3 | Определить алгоритм аутентификации для IKE. | esr(config-ike- proposal)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. |
| 4 | Определить алгоритм шифрования для IKE. | esr(config-ike- proposal)# encryption algorithm <ALGORITHM> | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. |
| 5 | Определить номер группы Диффи-Хеллмана. | esr(config-ike- proposal)# dh-group <DH-GROUP> | <DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. |
| 6 | Определить режим аутентификации. | esr(config-ike- proposal)# authentication method <METHOD> | <METHOD> – метод аутентификации ключа. Может принимать значения: <ul style="list-style-type: none"> • pre - shared - key – метод аутентификации, использующий предварительно полученные ключи шифрования; • rsa - public - key – метод аутентификации, использующий RSA-сертификат. |
| 7 | Создать политику для профиля IKE и перейти в режим её конфигурирования. | esr(config)# security ike policy <NAME> | <NAME> – имя политики IKE, задаётся строкой до 31 символа. |
| 8 | Задать время жизни соединения протокола IKE (не обязательно). | esr(config-ike- proposal)# lifetime seconds <SEC> | <SEC> – период времени, принимает значения [4 ..86400] секунд. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 9 | Привязать политику к профилю. | esr(config-ike-policy)# proposal <NAME> | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 10 | Указать ключ аутентификации. | esr(config-ike-policy)#pre-shared-key ascii-text<TEXT> | <TEXT> – строка [1..64] ASCII символов. |
| 11 | Создать шлюз для IKE и перейти в режим его конфигурирования. | esr(config)# security ike gateway <NAME> | <NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. |
| 12 | Привязать политику IKE. | esr(config-ike-gw)# ike-policy <NAME> | <NAME> – имя политики протокола IKE, задаётся строкой до 31 символа. |
| 13 | Указать версию IKE (не обязательно). | esr(config-ike-gw)# version <VERSION> | <version> – версия IKE-протокола: v1-only или v2-only . |
| 14 | Установить режим перенаправления трафика в туннель. | esr(config-ike-gw)#mode<MODE> | <MODE> – режим перенаправления трафика в туннель, принимает значения: <ul style="list-style-type: none"> • policy - based – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям; • route - based – трафик перенаправляется на основе маршрутов, шлюзом у которых является туннельный интерфейс. |
| 15 | Указать действие для DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection action <MODE> | <MODE> – режим работы DPD: <ul style="list-style-type: none"> • restart – соединение переустанавливается; • clear – соединение останавливается; • hold – соединение поддерживается; • none – механизм выключен, никаких действий не предпринимается. |
| 16 | Указать интервал между отправкой сообщений механизмом DPD (не обязательно). | esr(config-ike-gw)#dead-peer-detection interval <SEC> | <SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. |
| 17 | Указать период времени для ответа на сообщения механизма DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection timeout <SEC> | <SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд. |
| 18 | Указать версию IKE (не обязательно). | esr(config-ike-gw)# version <VERSION> | <version> – версия IKE-протокола: v1-only или v2-only . |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 19 | Установить IP подсети отправителя. | esr(config-ike-gw)# local network <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]] | <p><ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];</p> <p><TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;</p> <p><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];</p> <p><PORT> – TCP/UDP порт, принимает значения [1..65535].</p> |
| 20 | Установить IP-адрес локального шлюза IPsec-туннеля. | esr(config-ike-gw)#local address <ADDR> | <ADDR> – IP-адрес локального шлюза. |
| 21 | Установить IP-адрес удаленного шлюза IPsec-туннеля. | esr(config-ike-gw)#remote address <ADDR> | <ADDR> – IP-адрес удаленного шлюза. |
| 22 | Установить IP-адрес подсети получателя, а также IP-протокол и порт. | esr(config-ike-gw)# remote network <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]] | <p><ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];</p> <p><TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;</p> <p><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];</p> <p><PORT> – TCP/UDP порт, принимает значения [1..65535].</p> |
| 23 | Создать в профиль IPsec. | esr(config)# security ipsec proposal <NAME> | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 24 | Определить алгоритм аутентификации для IPsec. | esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2.384, sha2-512. |
| 26 | Определить алгоритм шифрования для IPsec. | esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM> | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. |
| 26 | Указать протокол (не обязательно). | esr(config-ipsec- proposal)#protocol <PROTOCOL> | <PROTOCOL> – инкапсулирующий протокол, принимает значения |
| 27 | Создать политику для профиля IPsec и перейти в режим её конфигурирования | esr(config)# security ipsec policy <NAME> | <NAME> – имя политики IPsec, задаётся строкой до 31 символа. |
| 28 | Привяжем политику к профилю | esr(config-ipsec-policy)# proposal <NAME> | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |
| 29 | Задать время жизни IPsec туннеля (не обязательно). | esr(config-ipsec- policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> } | <SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд. <PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд. |
| 30 | Создать IPsec VPN и перейти в режим конфигурирования. | esr(config)# security ipsecvpn <NAME> | <NAME> – имя VPN, задаётся строкой до 31 символа. |
| 31 | Определить режим согласования данных, необходимых для активации VPN. | esr(config-ipsec-vpn)# mode <MODE> | <MODE> – режим работы VPN. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 32 | Привязать IPsec политику к VPN. | esr(config-ipsec-vpn)#ike ipsec-policy <NAME> | <NAME> – имя IPsec-политики, задаётся строка до 31 символа. |
| 33 | Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно). | esr(config-ipsec-vpn)#ike dscp <DSCP> | DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. |
| 34 | Устанавливается режим активации VPN. | esr(config-ipsec-vpn)#ike establish-tunnel <MODE> | <MODE> – режим активации VPN: <ul style="list-style-type: none"> • by - request – соединение активируется встречной стороной; • route – соединение активируется при появлении трафика, маршрутизируемого в туннель; • immediate – туннель активируется автоматически после применения конфигурации. |
| 35 | Осуществить привязка IKE-шлюза к VPN. | esr(config-ipsec-vpn)# ike gateway <NAME> | <NAME> – имя IKE-шлюза, задаётся строкой до 31 символа. |
| 36 | Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно). | esr(config-ipsec-vpn)# ike idle-time <TIME> | <TIME> – интервал в секундах, принимает значения [4..86400]. |
| 37 | Отключить пересогласование ключей до разрыва IKE соединения по истечению времени, количеству переданных пакетов или байт (не обязательно). | esr(config-ipsec-vpn)#ike rekey disable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 38 | Настроить начало пересогласования ключей IKE соединения до истечения времени жизни (не обязательно). | esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> } | <SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой <code>lifetimeseconds</code>). Принимает значения [4..86400]. <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой <code>lifetimerackets</code>). Принимает значения [4..86400]. <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой <code>lifetimekilobytes</code>). Принимает значения [4..86400] |
| 39 | Установить уровень случайного разброса значений параметров <code>marginseconds</code> , <code>marginpackets</code> , <code>marginkilobytes</code> (не обязательно). | esr(config-ipsec-vpn)# ike rekey randomization <VALUE> | <VALUE> – максимальный процент разброса значений, принимает значения [1..100]. |
| 40 | Описать VPN (не обязательно). | esr(config-ipsec-vpn)# description <DESCRIPTION> | <DESCRIPTION> – описание профиля, задается строкой до 255 символов. |
| 41 | Активировать IPsec VPN. | esr(config-ipsec-vpn)# enable | |

Пример настройки

Задача:

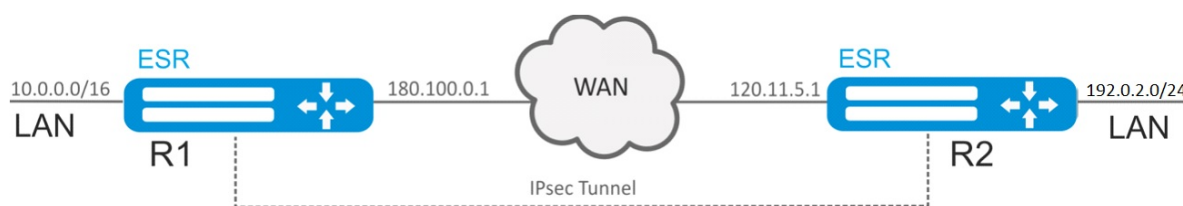


Рисунок 32 – Схема сети

Настроить IPsec-туннель между R1 и R2.

R1 IP-адрес – 120.11.5.1;

R2 IP-адрес – 180.100.0.1;

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

IPsec:

- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

Решение:

1. Конфигурирование R1

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 120.11.5.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 120.11.5.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```

esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit

```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```

esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit

```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500
esr(config-addr-set)# exit

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```

esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```

esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit

```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```

esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```

esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit

```

Состояние туннеля можно посмотреть командой:

```

esr# show security ipsec vpn status ipsec1

```

Конфигурацию туннеля можно посмотреть командой:

```

esr# show security ipsec vpn configuration ipsec1

```

⚠ В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500).

1.29.3 Настройка Remote Access IPsec VPN

Remote Access IPsec VPN – сценарий организации временных VPN-подключений, в котором сервер IPsec VPN находится в режиме ожидания входящих подключений, а клиенты осуществляют временные подключения к серверу для получения доступа к сетевым ресурсам.

Дополнительной особенностью RA IPsec VPN является возможность использования второго фактора аутентификации IPsec – Extended Authentication (XAUTH), вторым фактором аутентификации является пара логин-пароль для клиента IPsec VPN.

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Создать IKE-экземпляр и перейти в режим его конфигурирования. | esr(config)# security ike proposal <NAME> | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигулируемого туннеля (не обязательно). | esr(config-ike- proposal)# description <DESCRIPTION> | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 3 | Определить алгоритм аутентификации для IKE (не обязательно). | esr(config-ike- proposal)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. Значение по умолчанию: sha1 |
| 4 | Установить IP-адрес локальной стороны VTI-туннеля (не обязательно). | esr(config-vti)# ip address <ADDR/LEN> | <ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..31]. |
| 5 | Определить номер группы Диффи-Хеллмана (не обязательно). | esr(config-ike- proposal)# dh-group <DH-GROUP> | <DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1 |
| 6 | Создать политику для профиля IKE и перейти в режим её конфигурирования. | esr(config)# security ike policy <NAME> | <NAME> – имя политики IKE, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 7 | Определить режим аутентификации. | esr(config-ike- policy)# authentication method <METHOD> | <METHOD> – метод аутентификации ключа. Может принимать значения: <ul style="list-style-type: none"> xauth - psk - key – метод двухфакторной аутентификации, использующий пару логин-пароль и предварительно полученные ключи шифрования. |
| 8 | Задать режим клиента (только для клиента). | esr(config-ike- policy)# authentication mode client | |
| 9 | Задать время жизни соединения протокола IKE (не обязательно). | esr(config-ike- policy)# lifetime seconds <SEC> | <SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 3600 |
| 10 | Привязать политику к профилю. | esr(config-ike-policy)# proposal <NAME> | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 11 | Указать ключ аутентификации. | esr(config-ike-policy)#pre-shared-key ascii-text <TEXT> | <TEXT> – строка [1..64] ASCII символов. |
| 12 | Создать профиль доступа. | esr(config)# access profile <NAME> | <NAME> – имя профиля доступа, задаётся строкой до 31 символа. |
| 13 | Создать имя пользователя. | esr(config-access-profile)# user <LOGIN> | <LOGIN> – логин клиента, задаётся строкой до 31 символа. |
| 14 | Задать пароль пользователя. | esr(config-profile)# password ascii-text <TEXT> | <TEXT> – строка [8..32] ASCII символов. |
| 15 | Создать пул адресов назначения (только для сервера). | esr(config)# address-assignment pool <NAME> | <NAME> – имя пула адресов назначения, задаётся строкой до 31 символа. |
| 16 | Задать подсеть, из которой будут выдаваться IP клиентам (только для сервера). | esr(config-pool)# ip prefix <ADDR/LEN> | <ADDR/LEN> – адрес подсети и префикс. |
| 17 | Создать шлюз для IKE и перейти в режим его конфигурирования. | esr(config)# security ike gateway <NAME> | <NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. |
| 18 | Привязать политику IKE. | esr(config-ike-gw)# ike-policy <NAME> | <NAME> – имя политики протокола IKE, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 19 | Установить режим перенаправления трафика в туннель. | esr(config-ike-gw)# mode <MODE> | <p><MODE> – режим перенаправления трафика в туннель, принимает значения:</p> <ul style="list-style-type: none"> • policy - based – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям. |
| 20 | Указать действие для DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection action <MODE> | <p><MODE> – режим работы DPD:</p> <ul style="list-style-type: none"> • restart – соединение переустанавливается; • clear – соединение останавливается; • hold – соединение поддерживается; • none – механизм выключен, никаких действий не предпринимается. <p>Значение по умолчанию: none</p> |
| 21 | Указать интервал между отправкой сообщений механизмом DPD (не обязательно). | esr(config-ike-gw)#dead-peer-detection interval <SEC> | <p><SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд.</p> <p>Значение по умолчанию: 2</p> |
| 22 | Указать период времени для ответа на сообщения механизма DPD (не обязательно). | esr(config-ike-gw)# dead-peer-detection timeout <SEC> | <p><SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд.</p> <p>Значение по умолчанию: 30</p> |
| 23 | Указать версию IKE (не обязательно). | esr(config-ike-gw)# version <VERSION> | <p><VERSION> – версия IKE-протокола: v1-only или v2-only.</p> <p>Значение по умолчанию: v1-only</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 24 | Установить IP подсети отправителя (только для сервера). | esr(config-ike-gw)# local network <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]] | <p><ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];</p> <p><TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;</p> <p><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];</p> <p><PORT> – TCP/UDP порт, принимает значения [1..65535].</p> |
| 25 | Установить IP-адрес локального шлюза IPsec-туннеля. | esr(config-ike-gw)#local address <ADDR> | <ADDR> – IP-адрес локального шлюза. |
| 26 | Установить IP-адрес удаленного шлюза IPsec-туннеля. | esr(config-ike-gw)#remote address [any <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]] | <p>Any – установить в качестве удаленного адреса – любой адрес клиента, в конфигурации сервера;</p> <p><ADDR/LEN> – IP-адрес и маска подсети сервера, в конфигурации клиента.</p> |
| 27 | Задать пул динамического выделения IP-адресов клиентам (только для сервера). | esr(config-ike-gw)# remote network dynamic pool <NAME> | <NAME> – имя пула адресов назначения, задаётся строкой до 31 символа. |
| 28 | Задать режим динамического установления удаленной подсети (только для клиента). | esr(config-ike-gw)# remote network dynamic client | |
| 29 | Задать профиль доступа для XAUTH параметров (только для сервера). | esr(config-ike-gw)# xauth access-profile <NAME> | <NAME> – имя профиля доступа, задаётся строкой до 31 символа. |
| 30 | Задать профиль доступа и логин для XAUTH параметров (только для клиента). | esr(config-ike-gw)# xauth access-profile <NAME> client <LOGIN> | <p><NAME> – имя профиля доступа, задаётся строкой до 31 символа;</p> <p><LOGIN> – логин клиента, задаётся строкой до 31 символа.</p> |
| 31 | Задать интерфейс терминции выделенного IP для построения IPsec VPN (только для клиента). | esr(config-ike-gw)# assign-interface loopback <INDEX> | <INDEX> – индекс интерфейса, принимает значения [1..65535]. |
| 32 | Создать профиль IPsec. | esr(config)# security ipsec proposal <NAME> | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 33 | Определить алгоритм аутентификации для IPsec (не обязательно). | esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1 |
| 34 | Определить алгоритм шифрования для IPsec (не обязательно). | esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM> | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des |
| 35 | Указать протокол (не обязательно). | esr(config-ipsec- proposal)#protocol <PROTOCOL> | <PROTOCOL> – инкапсулирующий протокол, принимает значения. |
| 36 | Создать политику для профиля IPsec и перейти в режим её конфигурирования | esr(config)# security ipsec policy <NAME> | <NAME> – имя политики IPsec, задаётся строкой до 31 символа. |
| 37 | Привяжем политику к профилю | esr(config-ipsec-policy)# proposal <NAME> | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 38 | Задать время жизни IPsec туннеля (не обязательно). | esr(config-ipsec- policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> } | <p><SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование.</p> <p>Принимает значения [1140..86400] секунд.</p> <p>Значение по умолчанию: 540</p> <p><PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля.</p> <p>Принимает значения [4..86400].</p> <p>Значение по умолчанию: отключено.</p> <p><KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд.</p> <p>Значение по умолчанию: отключено.</p> |
| 39 | Создать IPsec VPN и перейти в режим конфигурирования. | esr(config)# security ipsec vpn <NAME> | <NAME> – имя VPN, задаётся строкой до 31 символа. |
| 40 | Определить режим согласования данных, необходимых для активации VPN. | esr(config-ipsec-vpn)# mode <MODE> | <MODE> – режим работы VPN, принимает значения: ike, manual. |
| 41 | Привязать IPsec политику к VPN. | esr(config-ipsec-vpn)#ike ipsec-policy <NAME> | <NAME> – имя IPsec-политики, задаётся строка до 31 символа. |
| 42 | Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно). | esr(config-ipsec-vpn)#ike dscp <DSCP> | <p>DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].</p> <p>Значение по умолчанию: 63</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 43 | Устанавливается режим активации VPN. | esr(config-ipsec-vpn)#ike establish-tunnel <MODE> | <p><MODE> – режим активации VPN:</p> <ul style="list-style-type: none"> • by - request – соединение активируется встречной стороной, доступно для сервера; • route – соединение активируется при появлении трафика, маршрутизируемого в туннель, доступно для сервера; • immediate – туннель активируется автоматически после применения конфигурации, доступно для клиента. |
| 44 | Осуществить привязка IKE-шлюза к VPN. | esr(config-ipsec-vpn)# ike gateway <NAME> | <NAME> – имя IKE-шлюза, задаётся строкой до 31 символа. |
| 45 | Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно). | esr(config-ipsec-vpn)# ike idle-time <TIME> | <p><TIME> – интервал в секундах, принимает значения [4..86400].</p> <p>Значение по умолчанию: 0</p> |
| 46 | Отключить пересогласование ключей до разрыва IKE соединения по истечению времени, количеству переданных пакетов или байт (не обязательно). | esr(config-ipsec-vpn)#ike rekey disable | Значение по умолчанию: включено. |
| 47 | Настроить начало пересогласования ключей IKE соединения до истечения времени жизни (не обязательно). | esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> } | <p><SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой <code>lifetimeseconds</code>) . Принимает значения [4..86400]. Значение по умолчанию: 540</p> <p><PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой <code>lifetimerpackets</code>). Принимает значения [4..86400]. Значение по умолчанию: отключено.</p> <p><KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой <code>lifetimekilobytes</code>). Принимает значения [4..86400] Значение по умолчанию: отключено.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 48 | Установить уровень случайного разброса значений параметров <code>marginseconds</code> , <code>marginpackets</code> , <code>marginkilobytes</code> (не обязательно). | <code>esr(config-ipsec-vpn)# ike rekey randomization <VALUE></code> | <VALUE> – максимальный процент разброса значений, принимает значения [1..100]. Значение по умолчанию: 100 |
| 49 | Описать VPN (не обязательно). | <code>esr(config-ipsec-vpn)# description <DESCRIPTION></code> | <DESCRIPTION> – описание профиля, задаётся строкой до 255 символов. |
| 50 | Активировать IPsec VPN. | <code>esr(config-ipsec-vpn)# enable</code> | |

Пример настройки

Задача:

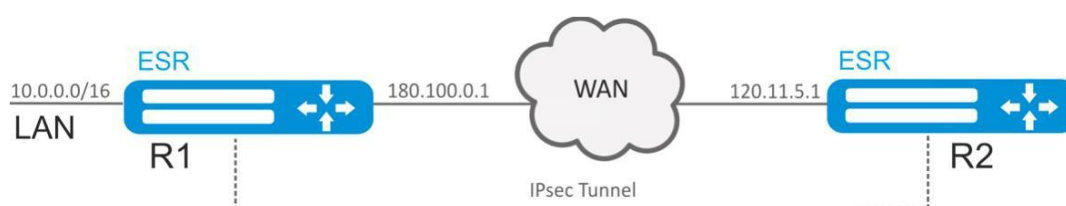


Рисунок 33 – Схема сети

Настроить Remote Access IPsec VPN между R1 и R2 с использованием второго фактора аутентификации IPsec - XAUTH. В качестве сервера IPsec VPN настроить маршрутизатор R1, а маршрутизатор R2 в качестве клиента IPsec VPN.

R2 IP-адрес – 120.11.5.1;

R1 IP-адрес – 180.100.0.1;

Клиентам IPsec VPN:

- выдавать адреса из пула подсети 192.0.2.0/24
- предоставлять доступ до LAN подсети 10.0.0.0/16

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: 3DES;
- алгоритм аутентификации: SHA1.

IPsec:

- алгоритм шифрования: 3DES;
- алгоритм аутентификации: SHA1.

XAUTH:

- логин: client1;
- пароль: password123.

Решение:

1. Конфигурирование R1

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```

esr# configure
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# exit

```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500,4500
esr(config-object-group-service)# exit

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования 3 DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IKE-соединения:

```

esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(config-ike-proposal)# exit

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы, ключ аутентификации и метод аутентификации XAUTH по ключу:

```

esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit

```

Создадим профиль доступа и заведем в нем пару логин и пароль для клиента IPsec VPN:

```

esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit

```

Создадим пул адресов назначения, из которого будут выдаваться IP клиентам IPsec VPN:

```

esr-1000(config)# address-assignment pool CLIENT_POOL
esr-1000(config-pool)# ip prefix 192.0.2.0/24
esr-1000(config-pool)# exit

```

Создадим шлюз протокола IKE. В данном профиле необходимо указать политику протокола IKE, указать локальную подсеть, в качестве удаленной подсети указать пул адресов назначения, задать режим перенаправления трафика в туннель по политике и использование второго фактора аутентификации XAUTH:


```

esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network dynamic pool CLIENT_POOL
esr(config-ike-gw)# dead-peer-detection action clear
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile XAUTH
esr(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования 3DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm sha1
esr(config-ipsec-proposal)# encryption algorithm 3des
esr(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и режим ожидания входящего соединения IPsec – *by-request*. После ввода всех параметров включим туннель командой *enable*.

```

esr(config)# security ipsec IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel by-request
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit

```

Разрешим протокол esp и udp порты 500,4500 в конфигурации firewall для установления IPsec VPN:

```

esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end

```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500,4500
esr(config-addr-set)# exit
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования 3 DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы, ключ аутентификации, метод аутентификации XAUTH по ключу и режим аутентификации – клиент:

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# authentication mode client
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

Создадим профиль доступа и заведем в нем пару логин и пароль:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

Создадим интерфейс loopback для терминации IP адреса, полученного от IPsec VPN сервера:

```
esr(config)# interface loopback 8
esr(config-loopback)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается политика, интерфейс терминации, режим динамического установления удаленной подсети, выбор профиля доступа для XAUTH и режим перенаправления трафика в туннель по политике:

```

esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# assign-interface loopback 8
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network dynamic client
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile xauth client client1
esr(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования 3DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```

esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit

```

Разрешим протокол esp и udp порты 500,4500 в конфигурации firewall для установления IPsec VPN:

```

esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end


```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status IPSECVPN
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration IPSECVPN
```

 В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500,4500).

1.30 Настройка LT-туннелей

LT (англ. Logical Tunnel – логический туннель) – тип туннелей, предназначенный для передачи маршрутной информации и трафика между различными виртуальными маршрутизаторами (VRF Lite), сконфигурированными на одном аппаратном маршрутизаторе. LT-туннель может использоваться для организации взаимодействия между двумя или более VRF с применением ограничений firewall.

1.30.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 1 | Создать LT-туннели для каждого из существующих VRF. | esr(config)# tunnel lt <ID> | <ID> – идентификатор туннеля в диапазоне [1..128]. |
| 2 | Указать описание конфигурируемых туннелей (не обязательно). | esr(config-lt)# description <DESCRIPTION> | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 3 | Включить каждый LT-туннель в соответствующий VRF. | esr(config-lt)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Включить каждый LT-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для LT-туннеля. | esr(config-lt)# security-zone<NAME> | <NAME> – имя зоны безопасности, задаётся строкой до 12 символов. |
| | | esr(config-lt)# ip firewall disable | |
| 5 | Для каждого LT-туннеля задать номер противоположный LT туннель (в другом VRF). | esr(config-lt)# peer lt <ID> | <ID> – идентификатор туннеля в диапазоне [1..128]. |
| 6 | Для каждого LT-туннеля указать IP-адрес для маршрутизации пакетов. Для взаимодействующих LT-туннелей, IP-адреса должны быть из одной IP-подсети. | esr(config-lt)# ip address <ADDR/LEN> | <ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| 7 | Включить туннели. | esr(config-lt)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 8 | Для каждого VRF настроить необходимые протоколы маршрутизации через LT-туннель. | | |
| 9 | Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно) | esr(config-lt)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5 |
| 10 | Указать размер MTU (Maximum Transmission Unit) пакетов, которые может пропускать данный bridge (не обязательно; возможно, если в bridge включен только VLAN). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | esr(config-lt)# mtu <MTU> | <MTU> – значение MTU, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1280..9600]; • для ESR-20/21 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 [1280..10000]. Значение по умолчанию: 1500. |

1.30.2 Пример настройки

Задача:

Организовать взаимодействие между хостами, терминированными в двух VRF vrf_1 и vrf_2.

Исходная конфигурация:

```
hostname esr
ip vrf vrf_1
exit
ip vrf vrf_2
exit
interface gigabitethernet 1/0/1
ip vrf forwarding vrf_1
ip firewall disable
ip address 10.0.0.1/24
exit
interface gigabitethernet 1/0/2
ip vrf forwarding vrf_2
ip firewall disable
ip address 10.0.1.1/24
exit
```

Решение:

Создадим LT-туннели для каждого VRF с указанием IP-адресов из одной подсети:

```

esr(config)# tunnel lt 1
esr(config-lt)# ip vrf forwarding vrf_1
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.1/30
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# ip vrf forwarding vrf_2
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.2/30
esr(config-lt)# exit

```

Укажем для каждого LT-туннеля LT-туннель из VRF, с которым необходимо установить связь, и активируем их:

```

esr(config)# tunnel lt 1
esr(config-lt)# peer lt 2
esr(config-lt)# enable
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# peer lt 1
esr(config-lt)# enable
esr(config-lt)# exit

```

⚠ Если в VRF не работает ни один из протоколов динамической маршрутизации, то необходимо указать статические маршруты для каждого VRF:

```

esr(config)# ip route vrf vrf_1 0.0.0.0/0 192.168.0.2
esr(config)# ip route vrf vrf_2 0.0.0.0/0 192.168.0.1

```

1.31 Настройка удаленного доступа к корпоративной сети по PPTP-протоколу

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

1.31.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|-------------------------------|---|--|
| 1 | Создать профиль PPTP-сервера. | esr(config)# remote-access pptp <NAME> | <NAME> – имя профиля PPTP-сервера, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 2 | Выбрать режим аутентификации РРTP-клиентов. | esr(config-pptp-server)# authentication mode { local radius } | <ul style="list-style-type: none"> • local – аутентификация пользователя по локальной базе. • radius – аутентификация пользователя по базе RADIUS-сервера. |
| 3 | Указать описание конфигулируемого сервера (не обязательно). | esr(config-pptp-server)# description <DESCRIPTION> | <DESCRIPTION> – описание РРTP-сервера, задаётся строкой до 255 символов. |
| 4 | Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно). | esr(config-pptp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME > | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа. |
| 5 | Указать DSCP-приоритет исходящих пакетов (не обязательно). | esr(config-pptp-server)# dscp <DSCP> | <DSCP>– dscp приоритет исходящих пакетов [0..63]. |
| 6 | Включить шифрование MPPE для РРTP-соединений (не обязательно). | esr(config-pptp-server)# encryption mppe | |
| 7 | Указать IP-адрес локального шлюза. | esr(config-pptp-server)# local-address object-group <OBJ-GROUP-NETWORK -NAME > ip-address <ADDR> | <p><OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа;</p> <p><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> |
| 8 | Указать размер MTU (MaximumTransmissionUnit) для сервера (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | esr(config-pptp-server) mtu <MTU> | <p><MTU> – значение MTU, принимает значения в диапазоне [1280..1500].</p> <p>Значение по умолчанию: 1500.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 9 | Указать IP-адрес, который должен обрабатывать PPTP-сервер. | esr(config-pptp-server)# outside-address { object-group <OBJ-GROUP-NETWORK -NAME > ip-address <ADDR> } | <OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать PPTP-сервер, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 10 | Указать список IP-адресов, из которого PPTP выдаются динамические IP-адреса удаленным пользователям. | esr(config-pptp-server)# remote-address { object-group <OBJ-GROUP-NETWORK -NAME > address-range <FROM-ADDR>-<TO-ADDR> } | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа; <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 11 | Включить PPTP-сервер в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall. | esr(config-pptp-server)# security-zone <NAME> | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 12 | Указать имя пользователя (при использовании локальной аутентификации пользователей). | esr(config-pptp-server) username < NAME > | <NAME> – имя пользователя, задаётся строкой до 12 символов. |
| 13 | Указать пароль пользователя. | esr(config-pptp-user) password ascii-text { <PASSWORD> encrypted <PASSWORD> } | <PASSWORD> – пароль пользователя, задается строкой до 32 символов. |
| 14 | Активировать пользователя. | esr(config-pptp-user) enable | |
| 15 | Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно). | esr(config-pptp-server)# wins- servers object-group <OBJ- GROUP-NETWORK -NAME > | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа. |

1.31.2 Пример настройки PPTP-сервера

Задача:

Настроить PPTP-сервер на маршрутизаторе.

- адрес PPTP-сервера – 120.11.5.1;
- шлюз внутри туннеля для подключающихся клиентов – 10.10.10.1;
- пул IP-адресов для выдачи 10.10.10.5-10.10.10.25;
- DNS-серверы: 8.8.8.8, 8.8.8.4;
- учетные записи для подключения – fedor, ivan.

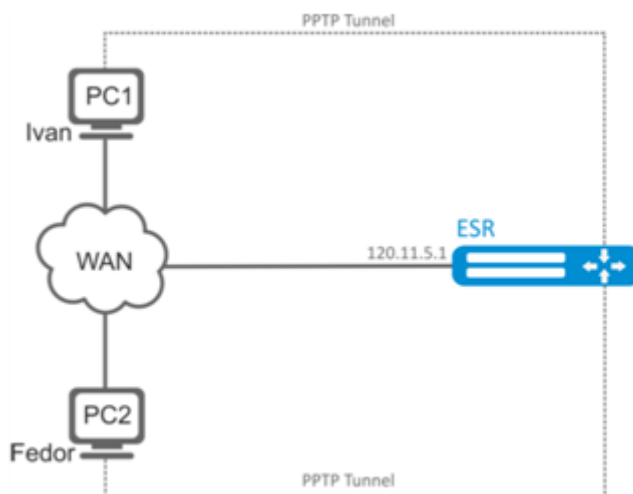


Рисунок 34 – Схема сети

Решение :

Создадим профиль адресов, содержащий адрес, который должен слушать сервер:

```
esr# configure
esr(config)# object-group network pptp_outside
esr(config-object-group-network)# ip address-range 120.11.5.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network pptp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адреса клиентов:

```
esr(config)# object-group network pptp_remote
esr(config-object-group-network)# ip address-range 10.10.10.5-10.10.10.25
esr(config-object-group-network)# exit
```

Создадим PPTP-сервер и привяжем вышеуказанные профили:

```

esr(config)# remote-access pptp remote-workers
esr(config-pptp)# local-address object-group pptp_local
esr(config-pptp)# remote-address object-group pptp_remote
esr(config-pptp)# outside-address object-group pptp_outside
esr(config-pptp)# dns-servers object-group pptp_dns

```

Выберем метод аутентификации пользователей PPTP-сервера:

```

esr(config-pptp)# authentication mode local

```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```

esr(config-pptp)# security-zone VPN

```

Создадим PPTP-пользователей *Ivan* и *Fedor* для PPTP-сервера:

```

esr(config-pptp)# username ivan
esr(config-pptp-user)# password ascii-text password1
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# username fedor
esr(config-pptp-user)# password ascii-text password2
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# exit

```

Включим PPTP-сервер:

```

esr(config-pptp)# enable

```

После применения конфигурации маршрутизатор будет прослушивать 120.11.5.1:1723. Состояние сессий PPTP-сервера можно посмотреть командой:

```

esr# show remote-access status pptp server remote-workers

```

Счетчики сессий PPTP-сервера можно посмотреть командой:

```

esr# show remote-access counters pptp server remote-workers

```

Очистить счетчики сессий PPTP-сервера можно командой:

```

esr# clear remote-access counters pptp server remote-workers

```

Завершить сессию пользователя *fedor* PPTP-сервера можно одной из следующих команд:

```

esr# clear remote-access session pptp username fedor
esr# clear remote-access session pptp server remote-workers username fedor

```

Конфигурацию PPTP-сервера можно посмотреть командой:

```
esr# show remote-access configuration pptp remote-workers
```

⚠ Помимо создания PPTP-сервера необходимо в firewall открыть TCP-порт 1723 для обслуживания соединений и разрешить протокол GRE(47) для туннельного трафика.

1.32 Настройка удаленного доступа к корпоративной сети по L2TP over IPsec протоколу

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) – туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

1.32.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 1 | Создать профиль L2TP-сервера. | esr(config)# remote-access l2tp <NAME> | <NAME> – имя профиля L2TP-сервера, задаётся строкой до 31 символа. |
| 2 | Выбрать режим аутентификации L2TP-клиентов. | esr(config-l2tp-server)# authentication mode { local radius } | local – аутентификация пользователя по локальной базе. radius – аутентификация пользователя по базе RADIUS-сервера. |
| 3 | Указать описание конфигулируемого сервера (не обязательно). | esr(config-l2tp-server)# description <DESCRIPTION> | <DESCRIPTION> – описание L2TP-сервера, задаётся строкой до 255 символов. |
| 4 | Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно). | esr(config-l2tp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME > | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа. |
| 5 | Указать DSCP приоритет исходящих пакетов. | esr(config-l2tp-server)# dscp <DSCP> | <DSCP> – dscp приоритет исходящих пакетов [0..63]. |
| 6 | Включить сервер. | esr(config-l2tp-server)# enable | |
| 7 | Выбрать метод аутентификации по ключу для IKE-соединения. | esr(config-l2tp-server)# ipsec authentication method pre-shared-key | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 8 | Указать общий секретный ключ для аутентификации, который должен совпадать у обеих сторон, устанавливающих туннель. | esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } hexadecimal {<HEX> encrypted <ENCRYPTED-HEX> } } | <p><TEXT> – строка [1..64] ASCII символов;</p> <p><HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...).</p> <p><ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;</p> <p><ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.</p> |
| 9 | Указать IP-адрес локального шлюза | esr(config-l2tp-server)# local-address object-group <OBJ-GROUP-NETWORK -NAME > ip-address <ADDR> | <p><OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа;</p> <p><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> |
| 10 | Указать размер MTU (MaximumTransmissionUnit) для сервера (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | esr(config-l2tp-server) mtu <MTU> | <p><MTU> – значение MTU, принимает значения в диапазоне [1280..1500].</p> <p>Значение по умолчанию: 1500.</p> |
| 11 | Указать IP-адрес, который должен слушать L2TP-сервер. | esr(config-l2tp-server)# outside-address object-group <OBJ-GROUP-NETWORK -NAME > ip-address <ADDR> | <p><OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать L2TP-сервер, задаётся строкой до 31 символа;</p> <p><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 12 | Указать список IP-адресов из которого L2TP выдаются динамические IP-адреса удаленным пользователям. | esr(config-l2tp-server)# remote-address { object-group <OBJ-GROUP-NETWORK -NAME > address-range <FROM-ADDR>-<TO- ADDR > } | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа; <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 13 | Включить L2TP-сервер в зону безопасности и настроить правила взаимодействия между зонами. | esr(config-l2tp-server)# security-zone <NAME> | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 14 | Указать имя пользователя (при использовании локальной базы аутентификации). | esr(config-l2tp-server) username <NAME > | <NAME> – имя пользователя, задаётся строкой до 12 символов. |
| 15 | Указать пароль пользователя (при использовании локальной базы аутентификации). | esr(config-l2tp-user) password ascii-text { <PASSWORD> encrypted <PASSWORD> } | <PASSWORD> – пароль пользователя, задается строкой до 32 символов. |
| 16 | Включить пользователя. | esr(config-l2tp-user) enable | |
| 17 | Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно). | esr(config-l2tp-server)# wins-servers object-group <OBJ-GROUP-NETWORK -NAME > | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа. |

1.32.2 Пример настройки

Задача:

Настроить L2TP-сервер на маршрутизаторе для подключения удаленных пользователей к ЛВС. Аутентификация пользователей проходит на RADIUS-сервере.

- адрес L2TP-сервера – 120.11.5.1;
- шлюз внутри туннеля – 10.10.10.1;
- адрес Radius-сервера – 192.168.1.4;

Для IPsec используется метод аутентификации по ключу: ключ – «password».

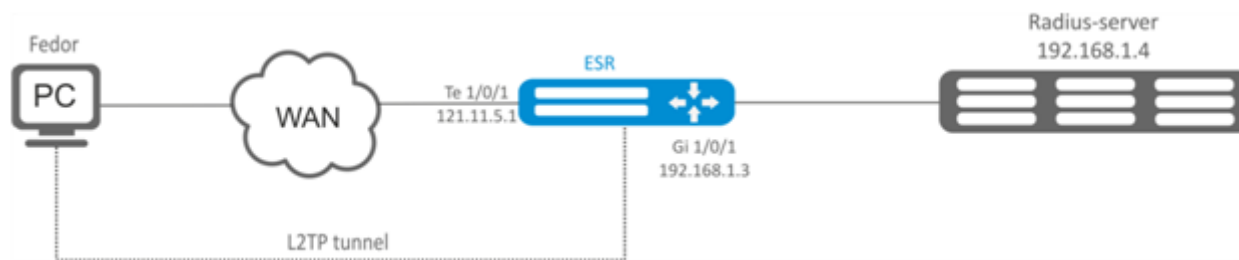


Рисунок 35 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- Настроить подключение к RADIUS-серверу;
- Настроить зоны для интерфейсов te1/0/1 и gi1/0/1;
- Указать IP-адреса для интерфейсов te1/0/1 и te1/0/1.

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network l2tp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий DNS-серверы:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8
esr(config-object-group-network)# ip address-range 8.8.4.4
esr(config-object-group-network)# exit
```

Создадим L2TP-сервер и привяжем к нему вышеуказанные профили:

```
esr(config)# remote-access l2tp remote-workers
esr(config-l2tp)# local-address ip-address 10.10.10.1
esr(config-l2tp)# remote-address address-range 10.10.10.5-10.10.10.15
esr(config-l2tp)# outside-address ip-address 120.11.5.1
esr(config-l2tp)# dns-server object-group l2tp_dns
```

Выберем метод аутентификации пользователей L2TP-сервера:

```
esr(config-l2tp)# authentication mode radius
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-l2tp)# security-zone VPN
```

Выберем метод аутентификации первой фазы IKE и зададим ключ аутентификации:

```
esr(config-l2tp)# ipsec authentication method psk
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим L2TP-сервер:

```
esr(config-l2tp)# enable
```

После применения конфигурации маршрутизатор будет прослушивать IP-адрес 120.11.5.1 и порт 1701. Состояние сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access status l2tp server remote-workers
```

Счетчики сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access counters l2tp server remote-workers
```

Очистить счетчики сессий L2TP-сервера можно командой:

```
esr# clear remote-access counters l2tp server remote-workers
```

Завершить сессию пользователя fedor L2TP-сервера можно одной из следующих команд:

```
esr# clear remote-access session l2tp username fedor
esr# clear remote-access session l2tp server remote-workers username fedor
```

Конфигурацию L2TP-сервера можно посмотреть командой:

```
esr# show remote-access configuration l2tp remote-workers
```

⚠ Помимо создания L2TP-сервера необходимо в firewall открыть UDP-порты 500, 1701, 4500 для обслуживания соединений и разрешить протоколы ESP(50) и GRE(47) для туннельного трафика.

1.33 Настройка удаленного доступа к корпоративной сети по OpenVPN протоколу

OpenVPN – полнофункциональное средство для построения виртуальных частных сетей (Virtual Private Networks, VPN), организации удалённого доступа, и решения ряда других задач, связанных с безопасностью передачи данных, базирующееся на SSL.

1.33.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Создать профиль OpenVPN-сервера. | esr(config)# remote-access openvpn <NAME> | <NAME> – имя профиля OpenVPN-сервера, задаётся строкой до 31 символа. |
| 2 | Указать список IP-адресов, из которого OpenVPN сервером выдаются динамические IP-адреса удаленным пользователям в режиме L2. (только для tunnel ethernet) | esr(config-openvpn-server)# address-range <FROM- ADDR>-<TO-ADDR> | <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 3 | Включить клиентские соединения по OpenVPN в L2 домен (только для tunnel ethernet). | esr(config-openvpn-server)# bridge-group <BRIDGE-ID> | <BRIDGE-ID> – идентификационный номер моста. |
| 4 | Указать сертификаты и ключи. | esr(config-openvpn-server)# certificate <CERTIFICATE- TYPE><NAME> | <CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения: <ul style="list-style-type: none"> • ca – сертификат удостоверяющего сервера; • crl – список отозванных сертификатов; • dh – ключ Диффи-Хеллмана; • server - crt – публичный сертификат сервера; • server - key – приватный ключ сервера; • ta – HMAC ключ. <NAME> – имя сертификата или ключа, задаётся строкой до 31 символа. |
| 5 | Включить блокировку передачи данных между клиентами (не обязательно). | esr(config-openvpn-server)# client-isolation | |
| 6 | Устанавливается максимальное количество одновременных пользовательских сессий (не обязательно). | esr(config-openvpn-server)# client-max <VALUE> | <VALUE> – максимальное количество пользователей, принимает значения [1..65535]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 7 | Включается механизм сжатия передаваемых данных между клиентами и сервером OpenVPN (не обязательно). | esr(config-openvpn-server)# compression | |
| 8 | Указать описание конфигурируемого сервера (не обязательно). | esr(config-openvpn-server)# description <DESCRIPTION> | <DESCRIPTION> – описание OpenVPN-сервера, задаётся строкой до 255 символов. |
| 9 | Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно). | esr(config-openvpn-server)# dns-server <ADDR> | <ADDR> – IP-адрес DNS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; |
| 10 | Выбрать алгоритм шифрования, используемый при передачи данных. | esr(config-openvpn-server)# encryption algorithm <ALGORITHM> | <ALGORITHM> – идентификатор протокола шифрования, принимает значения: 3des,blowfish128, aes128. |
| 11 | Определим подсеть, из которой выдаются IP-адреса пользователям. (только для tunnel ip) | esr(config-openvpn-server)# network <ADDR/LEN> | <ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; |
| 12 | Указать TCP/UDP порт, который будет прослушиваться OpenVPN – сервером (не обязательно). | esr(config-openvpn-server)# port <PORT> | <PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 13 | Указать инкапсулируемый протокол. | esr(config-openvpn-server)# protocol <PROTOCOL> | <PROTOCOL> – тип инкапсуляции, возможные значения: <ul style="list-style-type: none"> • TCP-инкапсуляция в TCP-сегменты; • UDP-инкапсуляция в UDP-дейтаграммы. |
| 14 | Включить анонсирование маршрута по умолчанию для OpenVPN соединений, что приводит к замене маршрута по умолчанию на клиентской стороне (не обязательно). | esr(config-openvpn-server)# redirect-gateway | |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 15 | Включить анонсирование указанных подсетей, шлюзом является IP-адрес OpenVPN-сервера (не обязательно). | esr(config-openvpn-server)# route <ADDR/LEN> | <ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; |
| 16 | Включить OpenVPN-сервер в зону безопасности и настроить правила взаимодействия между зонами. | esr(config-openvpn-server)# security-zone <NAME> | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 17 | Указать временной интервал, по истечению которого встречная сторона считается недоступной (не обязательно). | esr(config-openvpn-server)# timers holdtime <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| 18 | Указать временной интервал, по истечению которого идет проверка соединения со встречной стороной (не обязательно). | esr(config-openvpn-server)# timers keepalive <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. |
| 19 | Определить тип соединения с частной сетью через OpenVPN-сервер. | esr(config-openvpn-server)# tunnel <TYPE> | <TYPE> – инкапсулирующий протокол, принимает значения: <ul style="list-style-type: none"> • ip – соединение точка-точка; • ethernet – подключение к L2 домену. |
| 20 | Определить дополнительные параметры для указанного пользователя OpenVPN-сервера (при использовании локальной базы для аутентификации пользователей). | esr(config-openvpn-server)# username < NAME > | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 21 | Определить подсеть для указанного пользователя OpenVPN-сервера. | esr(config-openvpn-user)# subnet <ADDR/LEN> | <ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]. |
| 22 | Определить статический ip-адрес для указанного пользователя OpenVPN-сервера | esr(config-openvpn-user)# ip address <ADDR> | <ADDR> – адрес имеет следующий формат: AAA.BBB.CCC.DDD – IP-адрес подсети, где AAA-DDD принимают значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 23 | Разрешить подключаться к OpenVPN-серверу нескольким пользователям с одним сертификатом. | esr(config-openvpn-server)# duplicate-cn | |
| 24 | Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно). | esr(config-openvpn-server)# wins-server <ADDR> | <ADDR> – IP-адрес WINS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 25 | Включить профиль OpenVPN-сервера. | esr(config-openvpn-server)# enable | |

1.33.2 Пример настройки

Задача:

Настроить OpenVPN-сервер в режиме L3 на маршрутизаторе для подключения удаленных пользователей к ЛВС.

- подсеть OpenVPN-сервера – 10.10.100.0/24;
- режим – L3;
- аутентификация на основе сертификатов.



Рисунок 36 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- Подготовить сертификаты и ключи:
 - Сертификат Удостоверяющего Центра (CA)
 - Ключ и сертификат для OpenVPN сервера
 - Ключ Диффи-Хелмена и HMAC для TLS
- Настроить зону для интерфейса te1/0/1
- Указать IP-адреса для интерфейса te1/0/1.

Импортируем по tftp сертификаты и ключи:

```

esr# copy tftp://192.168.16.10:/ca.crt certificate:ca/ca.crt
esr# copy tftp://192.168.16.10:/dh.pem certificate:dh/dh.pem
esr# copy tftp://192.168.16.10:/server.key certificate:server-key/server.key
esr# copy tftp://192.168.16.10:/server.crt certificate:server-crt/server.crt
esr# copy tftp://192.168.16.10:/ta.key certificate:ta/ta.key

```

Создадим OpenVPN-сервер и подсеть, в которой он будет работать:

```

esr(config)# remote-access openvpn AP
esr(config-openvpn)# network 10.10.100.0/24

```

Укажем тип соединения L3 и протокол инкапсуляции.

```

esr(config-openvpn)# tunnel ip
esr(config-openvpn)# protocol tcp

```

Объявим подсети ЛВС которые будут доступны через OpenVPN соединение и укажем DNS сервер

```

esr(config-)# route 10.10.0.0/20
esr(config-openvpn)# dns-server 10.10.1.1

```

Укажем ранее импортированные сертификаты и ключи, которые будет использоваться OpenVPN-сервером:

```

esr(config-openvpn)# certificate ca ca.crt
esr(config-openvpn)# certificate dh dh.pem
esr(config-openvpn)# certificate server-key server.key
esr(config-openvpn)# certificate server-crt server.crt
esr(config-openvpn)# certificate ta ta.key

```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```

esr(config-openvpn)# security-zone VPN

```

Выберем алгоритм шифрования aes128:

```

esr(config-openvpn)# encryption algorithm aes128

```

Включим OpenVPN-сервер:

```

esr(config-openvpn)# enable

```

После применения конфигурации маршрутизатор будет прослушивать порт 1194 (используется по умолчанию).

Состояние сессий OpenVPN-сервера можно посмотреть командой:

```

esr# show remote-access status openvpn server AP

```

Счетчики сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access counters openvpn server AP
```

Очистить счетчики сессий OpenVPN-сервера можно командой:


```
esr# clear remote-access counters openvpn server AP
```

Завершить сессию пользователя fedor OpenVPN-сервера можно одной из следующих команд:

```
esr# clear remote-access session openvpn username fedor
esr# clear remote-access session openvpn server AP username fedor
```

Конфигурацию OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access configuration openvpn AP
```

 Помимо создания OpenVPN-сервера необходимо в firewall открыть TCP-порт 1194.

1.34 Настройка клиента удаленного доступа по протоколу PPPoE

PPPoE – это туннелирующий протокол (tunneling protocol), который позволяет инкапсулировать IP PPP через соединения Ethernet и обладает программными возможностями PPP-соединений, что позволяет использовать его для виртуальных соединений на соседнюю Ethernet-машину и устанавливать соединение точка-точка, которое используется для транспортировки IP-пакетов, а также работает с возможностями PPP. Это позволяет применять традиционное PPP-ориентированное ПО для настройки соединения, которое использует не последовательный канал, а пакетно-ориентированную сеть (например, Ethernet), чтобы организовать классическое соединение с логином и паролем для Интернет-соединений. Кроме того, IP-адрес по другую сторону соединения назначается только когда PPPoE-соединение открыто, позволяя динамическое переиспользование IP-адресов.

1.34.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Создать PPPoE-туннель и перейти в режим конфигурирования PPPoE-клиента. | esr(config)# tunnel pppoe <PPPoE> | <PPPoE> – порядковый номер туннеля от 1 до 10. |
| 2 | Указать описание конфигурируемого клиента (не обязательно). | esr(config-pppoe)# description <DESCRIPTION> | <DESCRIPTION> – описание PPPoE-сервера, задаётся строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 3 | Указать метод аутентификации (не обязательно). | esr(config-pptp)# authentication method <METHOD> | <METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap Значение по умолчанию: chap |
| 4 | Включить отказ от получения маршрута по умолчанию от PPPoE-сервера (не обязательно). | esr(config-pppoe)# ignore-default-route | |
| 5 | Указать интерфейс через который будет устанавливаться PPPoE соединение. | esr(config-pppoe)# interface <IF> | <IF> – интерфейс или группа интерфейсов. |
| 6 | Указать интервал времени, за который усредняется статистика о нагрузке (не обязательно). | esr(config-pppoe)# load-average <TIME> | <TIME> – интервал времени в секундах от 5 до 150 (по умолчанию 5 сек) |
| 7 | Указать размер MTU (MaximumTransmissionUnit) для PPPoE-туннеля. MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно). | esr(config-pppoe)# mtu <MTU> | <MTU> – значение MTU, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [1280..9600]; • для ESR-20/21 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 [1280..10000]. Значение по умолчанию: 1500. |
| 8 | Указать имя пользователя и пароль для подключения к PPPoE-серверу | esr(config-pppoe)# username <NAME> password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <name> – имя пользователя, задаётся строкой до 31 символа <CLEAR-TEXT> – пароль, задаётся строкой [8 .. 64] символов; <ENCRYPTED-TEXT> – зашифрованный пароль, задаётся строкой [16..128] символов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 9 | Указать имя экземпляра VRF, в котором будут использоваться указанные сетевой интерфейс, мост, зона безопасности, сервер динамической авторизации (DAS) или группа правил NAT. (не обязательно) | esr(config-pppoe)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 10 | Отключения функции Firewall на сетевом интерфейсе (не обязательно) | esr(config-pppoe)# ip firewall disable | |
| | Настройка зоны безопасности | esr(config-pppoe)#security-zone <NAME> | <NAME>-имя зоны безопасности, задается строкой до 31 символа. |
| 11 | Активировать конфигурируемый профиль | esr(config-pppoe)# enable | |

1.34.2 Пример настройки PPPoE-клиента

Задача:

Настроить PPPoE-клиент на маршрутизаторе.

- Учетные записи для подключения – tester;
- Пароли учетных записей – password;
- Подключение должно осуществляться с интерфейса gigabitethernet 1/0/7.



Рисунок 37 – Схема сети

Решение :

Предварительно настроить PPPoE-сервер с учетными записями.

Зайдем в режим конфигурирования PPPoE-клиента и отключим межсетевой экран:

```
esr# configure
esr(config)# tunnel pppoe 1
esr(config-pppoe)# ip firewall disable
```

Укажем пользователя и пароль для подключения к PPPoE-серверу:

```
esr(config-pppoe)# username tester password ascii-text password
```

Укажем интерфейс через который будет устанавливаться PPPoE-соединение:

```
esr(config-pppoe)# interface gigabitethernet 1/0/7
esr(config-pppoe)# enable
```

Состояние PPPoE-туннеля можно посмотреть командой:

```
esr# show tunnels configuration pppoe 1
```

Счетчики сессий PPPoE-клиента можно посмотреть командой:

```
esr# show tunnels counters pppoe 1
```

1.35 Настройка клиента удаленного доступа по протоколу PPTP

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий устанавливать защищённое соединение за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

1.35.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 1 | Создать PPTP-туннель и перейти в режим его конфигурирования. | esr(config)# tunnel pptp <INDEX> | <INDEX> – идентификатор туннеля в диапазоне: [1..10]. |
| 2 | Указать метод аутентификации (не обязательно). | esr(config-pptp)# authentication method <METHOD> | <METHOD> – метод аутентификации, возможные значения: chap, mschap, mschapv2, eap, pap Значение по умолчанию: chap |
| 3 | Указать экземпляр VRF, в котором будет работать данный PPTP-туннель (не обязательно). | esr(config-pptp)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Указать описание конфигурируемого туннеля (не обязательно). | esr(config-pptp)# description <DESCRIPTION> | <DESCRIPTION> – описание туннеля, задается строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 5 | Установить удаленный IP-адрес для установки туннеля. | esr(config-pptp)# remote address <ADDR> | <ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 6 | Установить размер MTU (MaximumTransmissionUnit) для туннеля (не обязательно) | esr(config-pptp)# mtu <MTU> | <MTU> – значение MTU, принимает значения в диапазоне: <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [552..9600]; • для ESR-20/21 – [552..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 [552..10000]. Значение по умолчанию: 1500. |
| 7 | Игнорировать маршрут по умолчанию через данный PPTP-туннель (не обязательно) | esr(config-pptp)# ignore-default-route | |
| 8 | Задать интервал времени, за который усредняется статистика о нагрузке на туннель (не обязательно). | esr(config-pptp)# load-average <TIME> | <TIME> – интервал в секундах, принимает значения [5..150] Значение по умолчанию: 5 |
| 9 | Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удаленной стороны. | esr(config-pptp)# username <NAME> password ascii-text { <WORD> encrypted <HEX> } | <NAME> – имя пользователя, задается строкой до 31 символа. <WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F]. <HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов. |
| 10 | Включить PPTP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (не обязательно). | esr(config-pptp)# security-zone <NAME> | <NAME> – имя зоны безопасности, задается строкой до 31 символа. |
| 11 | Задать исключение обработки входящего трафика в Firewall (не обязательно). | esr(config-pptp)# ip firewall disable | |

| Шаг | Описание | Команда | Ключи |
|-----|----------------------|-----------------------------------|-------|
| 12 | Активировать туннель | esr(config- pptp)# enable | |

1.35.2 Пример настройки удаленного подключения по PPTP-протоколу

Задача:

Настроить PPTP-туннель на маршрутизаторе:

- адрес PPTP-сервера 20.20.0.1;
- учетная запись для подключения – логин: ivan, пароль: simplepass.



Рисунок 38 – Схема сети

Решение:

Создадим туннель PPTP:

```
esr(config)# tunnel pptp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-pptp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-pptp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-pptp)# security-zone VPN
```

Включим туннель PPTP:

```
esr(config-pptp)# enable
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status pptp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters pptp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration pptp
```

1.36 Настройка клиента удаленного доступа по протоколу L2TP

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) – туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Создать L2TP-туннель и перейти в режим его конфигурирования. | esr(config)# tunnel l2tp <INDEX> | <INDEX> – идентификатор туннеля в диапазоне: [1..10]. |
| 2 | Указать метод аутентификации (не обязательно). | esr(config-pptp)# authentication method <METHOD> | <METHOD> – метод аутентификации, возможные значения: char, mschap, mschap-v2, eap, pap Значение по умолчанию: char |
| 3 | Указать экземпляр VRF, в котором будет работать данный L2TP-туннель (не обязательно). | esr(config-l2tp)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Указать описание конфигурируемого туннеля (не обязательно). | esr(config-l2tp)# description <DESCRIPTION> | <DESCRIPTION> – описание туннеля, задается строкой до 255 символов. |
| 5 | Установить удаленный IP-адрес для установки туннеля. | esr(config-l2tp)# remote address <ADDR> | <ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 6 | Установить размер MTU (MaximumTransmissionUnit) для туннеля (не обязательно) | esr(config-l2tp)# mtu <MTU> | <p><MTU> – значение MTU, принимает значения в диапазоне:</p> <ul style="list-style-type: none"> • для ESR-10/12V(F)/14VF – [552..9600]; • для ESR-20/21 – [552..9500]; • для ESR-100/200/1000/1200/1500/1510/1700 [552..10000]. <p>Значение по умолчанию: 1500.</p> |
| 7 | Игнорировать маршрут по умолчанию через данный L2TP-туннель (не обязательно) | esr(config-l2tp)# ignore-default-route | |
| 8 | Задать интервал времени, за который усредняется статистика о нагрузке на туннель (не обязательно). | esr(config-l2tp)# load-average <TIME> | <p><TIME> – интервал в секундах, принимает значения [5..150]</p> <p>Значение по умолчанию: 5</p> |
| 9 | Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удалённой стороны. | esr(config-l2tp)# username <NAME> password ascii-text { <WORD> encrypted <HEX> } | <p><NAME>– имя пользователя, задается строкой до 31 символа.</p> <p><WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F].</p> <p><HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов.</p> |
| 10 | Выбрать метод аутентификации по ключу для IKE-соединения. | esr(config-l2tp-server)# ipsec authentication method pre-shared-key | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 11 | Указать общий секретный ключ для аутентификации, который должен совпадать у обеих сторон, устанавливающих туннель. | esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } hexadecimal {<HEX> encrypted <ENCRYPTED-HEX> } } | <p><TEXT> – строка [1..64] ASCII символов;</p> <p><HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...).</p> <p><ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;</p> <p><ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.</p> |
| 12 | Включить L2TP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (не обязательно). | esr(config-l2tp)# security-zone <NAME> | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 13 | Задать исключение обработки входящего трафика в Firewall (не обязательно). | esr(config-l2tp)# ip firewall disable | |
| 14 | Активировать туннель | esr(config-l2tp)# enable | |

1.36.1 Пример настройки удаленного подключения по L2TP-протоколу

Задача:

Настроить PPTP-туннель на маршрутизаторе:

- адрес PPTP сервера 20.20.0.1;
- учетная запись для подключения – логин: ivan, пароль: simplepass



Рисунок 39 – Схема сети

Решение:

Создадим туннель L2TP:

```
esr(config)# tunnel l2tp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-l2tp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-l2tp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-l2tp)# security-zone VPN
```

Укажем метод аутентификации ipsec:

```
esr(config-l2tp)# ipsec authentication method pre-shared-key
```

Укажем ключ безопасности для ipsec:

```
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим туннель L2TP:

```
esr(config-l2tp)# enable
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status l2tp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters l2tp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration l2tp
```

1.37 Настройка Dual-Homing

⚠ В текущей версии ПО данный функционал поддерживается только на маршрутизаторе ESR-1000.

Dual-Homing – технология резервирования соединений, позволяет организовать надежное соединение ключевых ресурсов сети на основе наличия резервных линков.

1.37.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Указать резервный интерфейс, на который будет происходить переключение при потере связи на основном. | esr(config-if-gi)# backup interface<IF> vlan <VID> | <IF> – интерфейс, на который будет <VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094]. Можно также задать диапазоном через «-» или перечислением через «,». |
| 2 | Указать количество копий пакетов с одним и тем же MAC-адресом, которые будут отправлены в активный интерфейс при переключении (не обязательно). | esr(config)# backup-interface mac-duplicate <COUNT> | <COUNT> – количество копий пакетов, принимает значение [1..4]. |
| 3 | Указать количество пакетов в секунду, которое будет отправлено в активный интерфейс при переключении (не обязательно). | esr(config)# backup-interfacemac-per-second<COUNT> | <COUNT> – количество MAC-адресов в секунду, принимает значение [50..400]. |
| 4 | Указать, что необходимо осуществить переключение на основной интерфейс при восстановлении связи (не обязательно). | esr(config)# backup-interface preemption | |

1.37.2 Пример настройки

Задача:

Организовать резервирование L2-соединений маршрутизатора ESR для VLAN 50-55 через устройства SW1 и SW2.

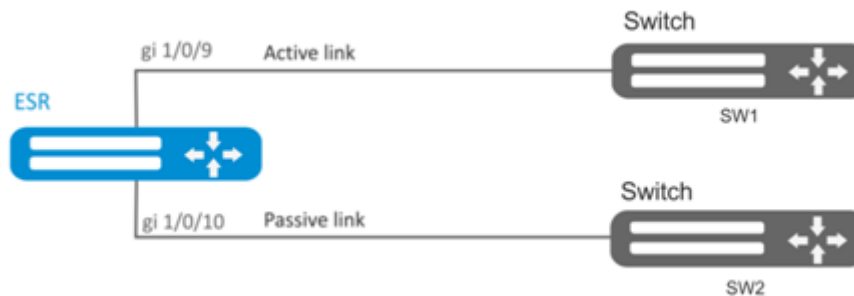


Рисунок 40 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

Создадим VLAN 50-55:

```
esr(config)# vlan 50-55
```

Необходимо отключить STP на интерфейсах gigabitethernet 1/0/9 и gigabitethernet 1/0/10, так как совместная работа данных протоколов невозможна:

```
esr(config)# interface gigabitethernet 1/0/9-10
esr(config-if-gi)# spanning-tree disable
```

Интерфейсы gigabitethernet 1/0/9 и gigabitethernet 1/0/10 добавим в VLAN 50-55 в режиме general.

```
esr(config-if-gi)# switchport general allowed vlan add 50-55
esr(config-if-gi)# exit
```

Основной этап конфигурирования:

Сделаем интерфейс gigabitethernet 1/0/10 резервным для gigabitethernet 1/0/9:

```
esr(config)# interface gigabitethernet 1/0/9
esr(config-if-gi)# backup interface gigabitethernet 1/0/10 vlan 50-55
```

Посмотреть информацию о резервных интерфейсах можно командой:

```
esr# show interfaces backup
```

1.38 Настройка QoS

QoS (Quality of Service) – технология предоставления различным классам трафика различных приоритетов в обслуживании. Использование службы QoS позволяет сетевым приложениям сосуществовать в одной сети, не уменьшая при этом пропускную способность других приложений.

1.38.1 Базовый QoS

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | <p>Включить сервис QoS на интерфейсе/туннеле/сетевом мосту.</p> <p>Если на интерфейсе не назначена политика QoS, то интерфейс работает в режиме BasicQoS.</p> | esr(config-if-gi)# qos enable | |
| 2 | <p>Установить режим доверия к значениям кодов 802.1p и DSCP во входящих пакетах. (не обязательно)</p> | esr(config)# qos trust <MODE> | <p><MODE> – режим доверия к значениям кодов 802.1p и DSCP, принимает одно из следующих значений:</p> <ul style="list-style-type: none"> • dscp – режим доверия значениям кодов DSCP в IP-заголовке. Не IP-пакеты будут направлены в очередь по умолчанию. • cos – режим доверия значениям кодов 802.1p в теге 802.1q. Нетегированные пакеты будут направлены в очередь по умолчанию. • cos - dscp – режим доверия значениям кодов DSCP для IP-пакетов и значениям кодов 802.1p для остальных пакетов. |
| 3 | <p>Установить соответствие между значениями кодов DSCP входящих пакетов и исходящими очередями</p> <p>Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QOS (не обязательно).</p> | esr(config)# qos map dscp-queue <DSCP> to <QUEUE> | <p><DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63];</p> <p><QUEUE> – идентификатор очереди, принимает значения [1..8].</p> <p>Значения по умолчанию:</p> <ul style="list-style-type: none"> • DSCP: (0-7), очередь 1 • DSCP: (8-15), очередь 2 • DSCP: (16-23), очередь 3 • DSCP: (24-31), очередь 4 • DSCP: (32-39), очередь 5 • DSCP: (40-47), очередь 6 • DSCP: (48-55), очередь 7 • DSCP: (56-63), очередь 8 |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 4 | <p>Установить соответствие между значениями кодов 802.1p входящих пакетов и исходящими очередями.</p> <p>Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QoS. (не обязательно)</p> | esr(config)# qos map cos-queue <COS> to <QUEUE> | <p><COS> – классификатор обслуживания в теге 802.1p пакета, принимает значения [0..7];</p> <p><QUEUE> – идентификатор очереди, принимает значения [1..8].</p> <p>Значения по умолчанию:</p> <ul style="list-style-type: none"> • CoS: (0), очередь 1 • CoS: (1), очередь 2 • CoS: (2), очередь 3 • CoS: (3), очередь 4 • CoS: (4), очередь 5 • CoS: (5), очередь 6 • CoS: (6), очередь 7 • CoS: (7), очередь 8 |
| 5 | <p>Установить соответствие между значениями кодов DSCP входящих пакетов и кодов DSCP на выходе из устройства. (в случае необходимости перемаркировки)</p> <p>Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QoS.</p> | esr(config)# qos map dscp-queue <DSCP> to <DSCP> | <DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63]. |
| 6 | Включить изменения кодов DSCP в соответствии с таблицей DSCP-Mutation. (в случае необходимости перемаркировки) | esr(config)# qos dscp mutation | |
| 7 | Установить номер очереди по умолчанию, в которую попадает весь трафик кроме IP в режиме доверия DSCP-приоритетам. | esr(config)# qos queue default <QUEUE> | <QUEUE> – идентификатор очереди, принимает значения [1..8]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 8 | <p>Задать количество приоритетных очередей. Оставшиеся очереди являются взвешенными. (не обязательно)</p> | <p>esr(config)# priority-queue out num-of-queues <VALUE></p> | <p><VALUE> – количество очередей, принимает значение [0..8], где:</p> <ul style="list-style-type: none"> • 0 – все очереди участвуют в WRR (WRR – механизм обработки очередей на основе веса); • 8 – все очереди обслуживаются как «strictpriority» (strictpriority – приоритетная очередь обслуживается сразу, как только появляются пакеты). <p>Приоритетные очереди выделяются, начиная с 8-й, в сторону уменьшения номера очереди.</p> <p>Значение по умолчанию: 8</p> |
| 9 | <p>Определить веса для соответствующих взвешенных очередей.</p> | <p>esr(config)# qos wrr-queue <QUEUE> bandwidth <WEIGHT></p> | <p><QUEUE> – идентификатор очереди, принимает значение [1..8];</p> <p><WEIGHT> – значение веса, принимает значение [1..255].</p> <p>Значение по умолчанию: вес 1 для всех очередей.</p> |
| 10 | <p>Установить ограничение скорости исходящего трафика для определенной очереди или интерфейса в целом.</p> <p>Команда актуальна только для BasicQoS режима интерфейса.</p> <p>Если трафик на входе был классифицирован при помощи расширенного QoS, ограничение не работает. (в случае необходимости ограничения скорости входящего потока)</p> | <p>esr(config-if-gi)# traffic-shape { <BANDWIDTH> [BURST] queue <QUEUE><BANDWIDTH> [BURST] }</p> | <p><QUEUE> – идентификатор очереди, принимает значение [1..8];</p> <p><BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TenggigabitEthernet интерфейсов и [64..1000000] для прочих интерфейсов и туннелей;</p> <p><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.</p> <p>Значение по умолчанию: Отключено.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 11 | Установить ограничение скорости входящего трафика. (в случае необходимости ограничения скорости исходящего потока) | esr(config-if-gi)# rate-limit <BANDWIDTH> [BURST] | <p><BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TenGigabitEthernet интерфейсов и [64..1000000] для прочих интерфейсов и туннелей;</p> <p><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.</p> <p>Значение по умолчанию: Отключено.</p> |

Пример настройки

Задача:

Настроить следующие ограничения на интерфейсе gigabitethernet 1/0/8: передавать трафик с DSCP 22 в первую приоритетную очередь, трафик с DSCP 14 в седьмую взвешенную очередь, установить ограничение по скорости в 60 Мбит/с для седьмой очереди.

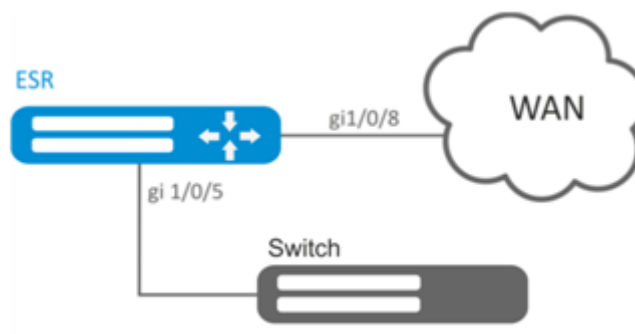


Рисунок 41 – Схема сети

Решение:

Для того чтобы первая очередь осталась приоритетной, а очереди со второй по восьмую стали взвешенными, ограничим количество приоритетных очередей до 1:

```
esr(config)# priority-queue out num-of-queues 1
```

Перенаправим трафик с DSCP 22 в первую приоритетную очередь:

```
esr(config)# qos map dscp-queue 22 to 1
```

Перенаправим трафик с DSCP 14 в седьмую взвешенную очередь:

```
esr(config)# qos map dscp-queue 14 to 7
```

Включим QoS на входящем интерфейсе для корректной классификации трафика и направления в соответствующую очередь со стороны LAN:

```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# qos enable
esr(config-if-gi)# exit
```

Включим QoS на интерфейсе со стороны WAN для правильной обработки очередей и ограничения полосы пропускания:

```
esr(config)# interface gigabitethernet 1/0/8
esr(config-if-gi)# qos enable
```

Установим ограничение по скорости в 60Мбит/с для седьмой очереди:

```
esr(config-if)# traffic-shape queue 7 60000
esr(config-if)# exit
```

Просмотреть статистику по QoS можно командой:

```
esr# show qos statistics gigabitethernet 1/0/8
```

1.38.2 Расширенный QoS

Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 1 | Создать списки доступа для определения трафика, к которому должен быть применен расширенный QoS. | | См. Раздел Настройка списков доступа (ACL) . |
| 2 | Создать класс QoS и перейти в режим настройки параметров класса. | esr(config)# class-map <NAME> | <NAME> – имя создаваемого класса, задается строкой до 31 символа. |
| 3 | Задать описание класса QoS. (не обязательно) | esr(config-class-map)# description <description> | <description> – до 255 символов. |
| 4 | Определить трафик относящийся к конфигурируемому классу по списку контроля доступа (ACL). | esr(config-class-map)# match access-group <NAME> | <NAME> – имя списка контроля доступа, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 5 | <p>Задать значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих конфигулируемому классу</p> <p>(невозможно назначать одновременно с полями IP Precedence и CoS). (при необходимости перемаркировки)</p> | esr(config-class-map)# set dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения [0..63]. |
| 6 | <p>Задать значение кода IP Precedence, которое будет установлено в IP-пакетах, соответствующих конфигулируемому классу (невозможно назначать одновременно с полями DSCP и CoS). (при необходимости перемаркировки)</p> | esr(config-class-map)# set ip-precedence <IPP> | <IPP> – значение кода IP Precedence, принимает значения [0..7]. |
| 7 | <p>Задать значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих конфигулируемому классу (невозможно назначать одновременно с полями DSCP и IP Precedence). (при необходимости перемаркировки)</p> | esr(config-class-map)# set c os <COS> | <COS> – значение 802.1p приоритета, принимает значения [0..7]. |
| 8 | Создать политику QoS и осуществить переход в режим настройки параметров политики. | esr(config)# policy-map <NAME> esr(config-policy-map)# | <NAME> – имя создаваемой политики, задается строкой до 31 символа. |
| 9 | Задать описание политики QoS. (не обязательно) | esr(config-policy-map)# description <description> | <description> – до 255 символов. |
| 10 | Установить гарантированную полосу пропускания исходящего трафика для политики в целом. | esr(config-policy-map)# shape average <BANDWIDTH> [BURST] | <p><BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..1000000];</p> <p><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 11 | Включить автоматическое распределение полосы пропускания между классами, в которых нет настройки полосы пропускания, включая класс по умолчанию. (в случае необходимости) | esr(config-policy-map)# shape auto-distribution | |
| 12 | Включить указанный QoS-класс в политику и осуществить переход в режим настройки параметров класса в рамках политики. | esr(config-policy-map)# class <NAME> esr(config-class-policy-map)# | <NAME> – имя привязываемого класса, задается строкой до 31 символа. При указании значения «class-default» в данный класс попадает трафик неклассифицированный на входе. |
| 13 | Включить политику QoS в класс QoS для создания иерархического QoS. | esr(config-class-policy-map)# service-policy <NAME> | <NAME> – имя политики, задается строкой до 31 символа. Вкладываемая политика должна быть уже создана. |
| 14 | Установить гарантированную полосу пропускания исходящего трафика для класса в рамках политики. (при необходимости) | esr(config-class-policy-map)# shape average <BANDWIDTH> [BURST] | <BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000]; |
| 15 | Установить разделяемую полосу пропускания исходящего трафика для определенного класса. Данную полосу класс может занять, если менее приоритетный класс не занял свою гарантированную полосу. (при необходимости) | esr(config-class-policy-map)# shape peak <BANDWIDTH> [BURST] | <BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт. |
| 16 | Определить режим работы класса. (не обязательно) | esr(config-class-policy-map)# mode <MODE> | <MODE> – режим класса: <ul style="list-style-type: none"> • fifo – режим FIFO (First In, First Out); • gred – режим GRED (Generalized RED); • red – режим RED (Random Early Detection); • sfq – режим SFQ (очередь SFQ распределяет передачу пакетов на базе потоков). Значение по умолчанию: FIFO . |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 17 | Задать приоритет класса в WRR-процессе. (при необходимости) | esr(config-class-policy-map)# priority class <PRIORITY> | <PRIORITY> – приоритет класса в WRR-процессе, принимает значения [1..8]. Классы с наибольшим приоритетом обрабатываются в первую очередь. |
| 18 | Перевести класс в режим StrictPriority и задать приоритет класса. (при необходимости) | esr(config-class-policy-map)# priority level <PRIORITY> | <PRIORITY> – уровень приоритета в StrictPriority-процессе, принимает значения [1..8]. Классы с наибольшим приоритетом обрабатываются в первую очередь. Значение по умолчанию: класс работает в режиме WRR, приоритет не задан. |
| 19 | Определить предельное количество виртуальных очередей. (не обязательно) | esr(config-class-policy-map)# fair-queue <QUEUE-LIMIT> | <QUEUE-LIMIT> – предельное количество виртуальных очередей, принимает значения в диапазоне [16..4096]. Значение по умолчанию: 16. |
| 20 | Определить предельное количество пакетов для виртуальной очереди. (не обязательно) | esr(config-class-policy-map)# queue-limit <QUEUE-LIMIT> | <QUEUE-LIMIT> – предельное количество пакетов в виртуальной очереди, принимает значения в диапазоне [2..4096]. Значение по умолчанию: 127. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 21 | Определить параметры RED (Random Early Detection). (при необходимости) | esr(config-class-policy-map)# random-detect <LIMIT><MAX><MIN><PROBABILITY> | <p><LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000];</p> <p><MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];</p> <p><MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];</p> <p><PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].</p> <p>При указании значений должны выполняться следующие правила:</p> <ul style="list-style-type: none"> • <MAX>> 2 * <MIN> • <LIMIT>> 3 * <MAX> |
| 22 | Определить параметры GRED (Generalized Random Early Detection). (при необходимости) | esr(config-class-policy-map)# random-detect precedence <PRECEDENCE><LIMIT><MAX> <MIN><PROBABILITY> | <p><PRECEDENCE> – значение IPPrecedence [0..7];</p> <p><LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000];</p> <p><MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];</p> <p><MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];</p> <p><PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].</p> <p>При указании значений должны выполняться следующие правила:</p> <ul style="list-style-type: none"> • <MAX>> 2 * <MIN> • <LIMIT>> 3 * <MAX> |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 23 | Включить протокол компрессии tcp заголовков для трафика отдельного класса. (при необходимости) | esr(config-class-policy-map)# compression header ip tcp | |
| 24 | Включить сервис QoS на интерфейсе/туннеле/ сетевом мосту. | esr(config-if-gi)# qos enable | |
| 25 | Назначить политику QoS на сконфигурируемом интерфейсе/ туннеле/сетевом мосту для классификации входящего (input) или приоритезации исходящего (output) трафика. | esr(config-if-gi)# service-policy { input output } <NAME> | <NAME> – имя QoS-политики, задаётся строкой до 31 символа. |

Пример настройки

Задача:

Классифицировать входящий трафик по подсетям (10.0.11.0/24, 10.0.12.0/24), произвести маркировку по DSCP (38 и 42) и произвести разграничение по подсетям (40 Мбит/с и 60 Мбит/с), ограничить общую полосу до 250 Мбит/с, остальной трафик обрабатывать через механизм SFQ.

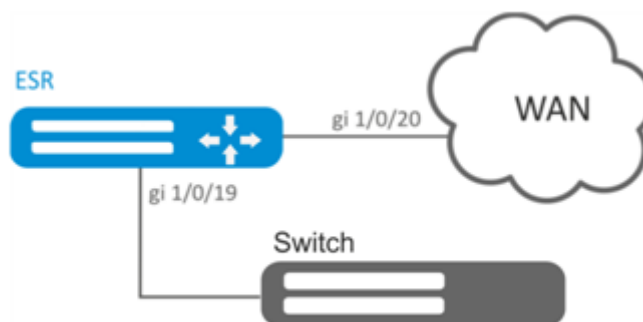


Рисунок 42 – Схема сети

Решение:

Настроим списки доступа для фильтрации по подсетям, выходим в глобальный режим конфигурации:

```

esr(config)# ip access-list extended fl1
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address 10.0.11.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended fl2
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address 10.0.12.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit

```

Создаем классы fl1 и fl2, указываем соответствующие списки доступа, настраиваем маркировку:

```

esr(config)# class-map fl1
esr(config-class-map)# set dscp 38
esr(config-class-map)# match access-group fl1
esr(config-class-map)# exit
esr(config)# class-map fl2
esr(config-class-map)# set dscp 42
esr(config-class-map)# match access-group fl2
esr(config-class-map)# exit

```

Создаём политику и определяем ограничение общей полосы пропускания:

```

esr(config)# policy-map fl
esr(config-policy-map)# shape average 250000

```

Осуществляем привязку класса к политике, настраиваем ограничение полосы пропускания и выходим:

```

esr(config-policy-map)# class fl1
esr(config-class-policy-map)# shape average 40000
esr(config-class-policy-map)# exit
esr(config-policy-map)# class fl2
esr(config-class-policy-map)# shape average 60000
esr(config-class-policy-map)# exit

```

Для другого трафика настраиваем класс с режимом SFQ:

```

esr(config-policy-map)# class class-default
esr(config-class-policy-map)# mode sfq
esr(config-class-policy-map)# fair-queue 800
esr(config-class-policy-map)# exit
esr(config-policy-map)# exit

```

Включаем QoS на интерфейсах, политику на входе интерфейса gi 1/0/19 для классификации и на выходе gi1/0/20 для применения ограничений и режима SFQ для класса по умолчанию:

```

esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy input fl
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/20
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy output fl
esr(config-if-gi)# exit

```

Для просмотра статистики используется команда:

```

esr# do show qos policy statistics gigabitethernet 1/0/20

```

1.39 Настройка зеркалирования

⚠ В текущей версии ПО данный функционал поддерживается только на маршрутизаторе ESR-1000

Зеркалирование трафика — функция маршрутизатора, предназначенная для перенаправления трафика с одного порта маршрутизатора на другой порт этого же маршрутизатора (локальное зеркалирование) или на удаленное устройство (удаленное зеркалирование).

1.39.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 1 | Определить VLAN, по которому будет передаваться отзеркалированный трафик (в случае использования удаленного зеркалирования). | esr(config)# port monitor remote vlan <VID><DIRECTION> | <VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094]; <DIRECTION> – направление трафика: <ul style="list-style-type: none"> • tx – зеркалирование в указанный VLAN только исходящего трафика; • rx – зеркалирование в указанный VLAN только входящего трафика. |
| 2 | Включить режим удаленного зеркалирования (в случае использования удаленного зеркалирования). | esr(config)# port monitor remote | |
| 3 | Определить режим порта передающего отзеркалированный трафик. | esr(config)# port monitor mode <MODE> | <MODE> – режим: <ul style="list-style-type: none"> • network – совмещенный режим передачи данных и зеркалирование; • monitor-only – только зеркалирование. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 4 | В режиме конфигурации интерфейса включить зеркалирование. | esr(config-if-gi)# port monitor interface <IF><DIRECTION> | <p><IF> – интерфейс в который будет осуществляться зеркалирование;</p> <p><DIRECTION> – направление трафика:</p> <ul style="list-style-type: none"> • tx – зеркалирование только исходящего трафика; • rx – зеркалирование только входящего трафика. |

1.39.2 Пример настройки

Задача:

Организовать удаленное зеркалирование трафика по VLAN 50 с интерфейса gi1/0/11 для передачи на сервер для обработки.

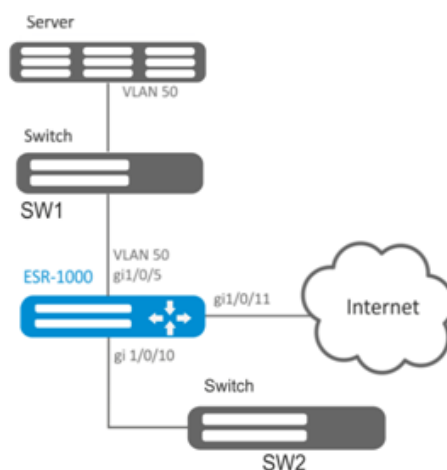


Рисунок 43 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- Создать VLAN 50;
- На интерфейсе gi 1/0/5 добавить VLAN 50 в режиме general.

Основной этап конфигурирования:

Укажем VLAN, по которой будет передаваться зеркалированный трафик:

```
esr1000(config)# port monitor remote vlan 50
```

На интерфейсе gi 1/0/5 укажем порт для зеркалирования:

```
esr1000(config)# interface gigabitethernet 1/0/5
esr1000(config-if-gi)# port monitor interface gigabitethernet 1/0/11
```

Укажем на интерфейсе gi 1/0/5 режим удаленного зеркалирования:

```
esr1000(config-if-gi)# port monitor remote
```

1.40 Настройка Netflow

Netflow – сетевой протокол, предназначенный для учета и анализа трафика. Netflow позволяет передавать данные о трафике (адрес отправителя и получателя, порт, количество информации и др.) с сетевого оборудования (сенсора) на коллектор. В качестве коллектора может использоваться обычный сервер.

1.40.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 1 | Задать версию Netflow-протокола. | esr(config)# netflow version <VERSION> | <VERSION> – версия Netflow-протокола: 5, 9 и 10. |
| 2 | Установить максимальное количество наблюдаемых сессий. | esr(config)# netflow max-flows <COUNT> | <COUNT> – количество наблюдаемых сессий, принимает значение [10000..2000000]. Значение по умолчанию: 512000. |
| 3 | Установить интервал, по истечении которого информация об устаревших сессиях экспортируются на коллектор. | esr(config)# netflow inactive-timeout <TIMEOUT> | <TIMEOUT> – задержка перед отправкой информации об устаревших сессиях, задается в секундах, принимает значение [0..240]. Значение по умолчанию: 15 секунд. |
| 4 | Установить частоту отправки статистики на Netflow-коллектор. | esr(config)# netflow refresh-rate <RATE> | <RATE> – частота отправки статистики, задается в пакетах на поток, принимает значение [1..10000]. Значение по умолчанию: 10. |
| 5 | Активировать Netflow на маршрутизаторе. | esr(config)# netflow enable | |
| 6 | Создать коллектор Netflow и перейти в режим его конфигурирования. | esr(config)# netflow collector <ADDR> | <ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 7 | Установить порт Netflow-сервиса на сервере сбора статистики. | esr(config-netflow-host)# port <PORT> | <PORT> – номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 2055. |
| 8 | Включить отправку статистики на Netflow-сервер в режим конфигурирования интерфейса/ туннеля/ сетевого моста. | esr(config-if-gi)# ip netflow export | |

1.40.2 Пример настройки

Задача:

Организовать учет трафика с интерфейса gi1/0/1 для передачи на сервер через интерфейс gi1/0/8 для обработки.

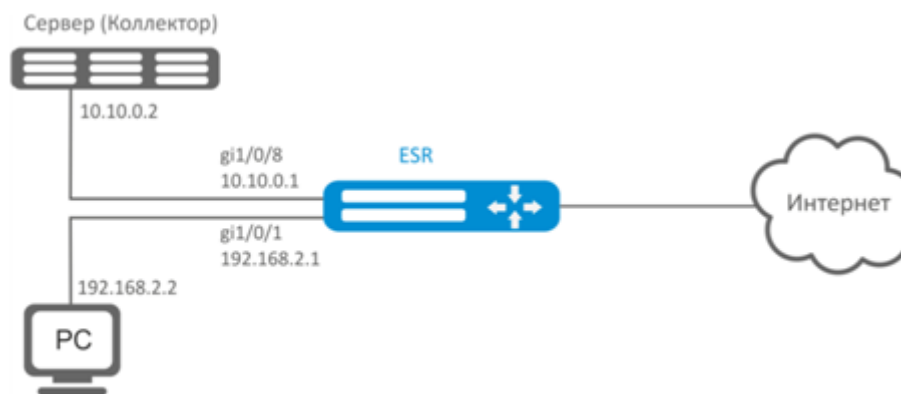


Рисунок 44 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- На интерфейсах gi1/0/1, gi1/0/8 отключить firewall командой «ip firewall disable».
- Назначить IP-адреса на портах.

Основной этап конфигурирования:

Укажем IP-адрес коллектора:

```
esr(config)# netflow collector 10.10.0.2
```

Включим сбор экспорта статистики netflow на сетевом интерфейсе gi1/0/1:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip netflow export
```

Активируем netflow на маршрутизаторе:

```
esr(config)# netflow enable
```

Для просмотра статистики Netflow используется команда:

```
esr# show netflow statistics
```

Настройка Netflow для учета трафика между зонами аналогична настройке sFlow, описание приведено в разделе [Настройка sFlow](#).

1.41 Настройка sFlow

Sflow – стандарт для мониторинга компьютерных сетей, беспроводных сетей и сетевых устройств, предназначенный для учета и анализа трафика.

1.41.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 1 | Установить частоту отправки пакетов пользовательского трафика в неизменном виде на sFlow-коллектор. | esr(config)# sflow sampling-rate <RATE> | <RATE> – частота отправки пакетов пользовательского трафика на коллектор, принимает значение [1..10000000]. При значении частоты 10 на коллектор будет отправлен один пакет из десяти. Значение по умолчанию: 1000. |
| 2 | Установить интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса | esr(config)# sflow poll-interval <TIMEOUT> | <TIMEOUT> – интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса, принимает значение [1..10000]. Значение по умолчанию: 10 секунд. |
| 3 | Активировать sFlow на маршрутизаторе. | esr(config)# sflow enable | |
| 4 | Создать коллектор sFlow и перейти в режим его конфигурирования. | esr(config)# sflow collector <ADDR> | <ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|-------|
| 5 | Включить отправку статистики на sFlow-сервер в режим конфигурирования интерфейса/ туннеля/ сетевого моста. | esr(config-if-gi)# ip sflow export | |

1.41.2 Пример настройки

Задача:

Организовать учет трафика между зонами trusted и untrusted.

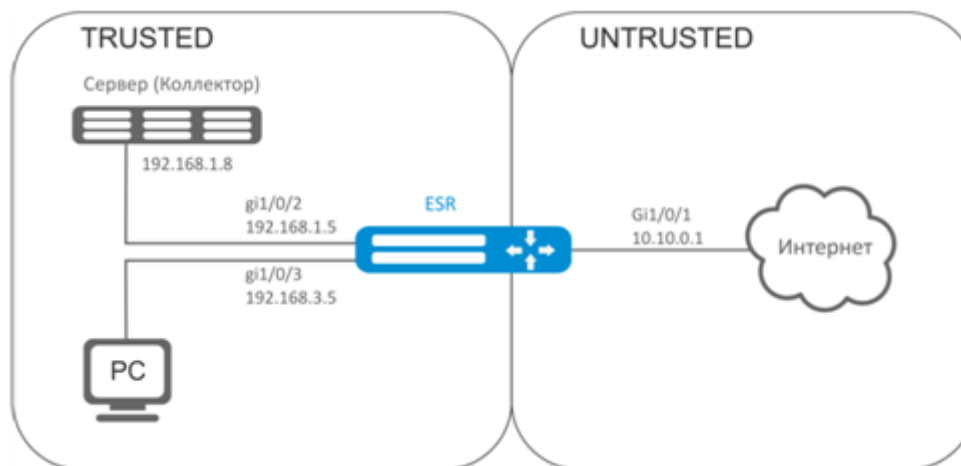


Рисунок 45 – Схема сети

Решение:

Для сетей ESR создадим две зоны безопасности:

```
esr# configure
esr(config)# security zone TRUSTED
esr(config-zone)# exit
esr(config)# security zone UNTRUSTED
esr(config-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```

esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone UNTRUSTED
esr(config-if-gi)# ip address 10.10.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2-3
esr(config-if-gi)# security-zone TRUSTED
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-gi)# ip address 192.168.1.5/24
esr(config-if-gi)# exit
esr(config)# interface gi1/0/3
esr(config-if-gi)# ip address 192.168.3.5/24
esr(config-if-gi)# exit

```

Укажем IP-адрес коллектора:

```

esr(config)# sflow collector 192.168.1.8

```

Включим экспорт статистики по протоколу sFlow для любого трафика в правиле «rule1» для направления TRUSTED-UNTRUSTED:

```

esr(config)# security zone-pair TRUSTED UNTRUSTED
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action sflow-sample
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable

```

Активируем sFlow на маршрутизаторе:

```

esr(config)# sflow enable

```

Настройка sFlow для учета трафика с интерфейса осуществляется аналогично [Настройка Netflow](#).

1.42 Настройка LACP

LACP – протокол для агрегирования каналов, позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала.

1.42.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 1 | Установить приоритет системы для протокола LACP. | esr(config)# lacp system-priority <PRIORITY> | <PRIORITY> – приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 2 | Установить механизм балансировки нагрузки для групп агрегации каналов. | esr(config)# port-channel load-balance {src-dst-mac-ip src-dst-mac src-dst-ip src-dst-mac-ip-port} | <ul style="list-style-type: none"> • src - dst - mac - ip – механизм балансировки основывается на MAC-адресе отправителя и получателя; • src - dst - mac – механизм балансировки основывается на MAC-адресе отправителя и получателя; • src - dst - ip – механизм балансировки основывается на IP-адресе отправителя и получателя; • src - dst - mac - ip - port – механизм балансировки основывается на MAC-адресе, IP-адресе и порте отправителя и получателя. |
| 3 | Установить административный таймаут протокола LACP. | esr(config)# lacp timeout { short long } | <ul style="list-style-type: none"> • long – длительное время таймаута; • short – короткое время таймаута. <p>Значение по умолчанию: long.</p> |
| 4 | Создать и перейти в режим конфигурирования агрегированного интерфейса. | esr(config)# interface port-channel <ID> | <ID> – порядковый номер группы агрегации каналов, принимает значения [1..12]. |
| 5 | Настроить необходимые параметры агрегированного канала. | | |
| 6 | Перейти в режим конфигурирования физического интерфейса. | esr(config)# interface <IF-TYPE><IF-NUM> | <p><IF-TYPE> тип интерфейса (gigabitethernet или tengigabitethernet).</p> <p><IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 7 | Включить физический интерфейс в группу агрегации каналов с указанием режима формирования группы агрегации каналов. | esr(config-if-gi)# channel-group <ID> mode <MODE> | <p><ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].</p> <p><MODE> – режим формирование группы агрегации каналов:</p> <ul style="list-style-type: none"> • auto – добавить интерфейс в динамическую группу агрегации с поддержкой протокола LACP; • on – добавить интерфейс в статическую группу агрегации. |
| 8 | Установить LACP-приоритет интерфейса Ethernet. | esr(config-if-gi)# lacp port-priority <PRIORITY> | <p><PRIORITY> – приоритет, указывается в диапазоне [1..65535].</p> <p>Значение по умолчанию: 1.</p> |

1.42.2 Пример настройки

Задача:

Настроить агрегированный канал между маршрутизатором ESR и коммутатором.



Рисунок 46 – Схема сети

Решение:

Предварительно нужно выполнить следующие настройки:

На интерфейсах gi1/0/1, gi1/0/2 отключить зону безопасности командой «no security-zone».

Основной этап конфигурирования:

Создадим интерфейс port-channel 2:

```
esr(config)# interface port-channel 2
```

Включим физические интерфейсы gi1/0/1, gi1/0/2 в созданную группу агрегации каналов:

```
esr(config)# interface gigabitethernet 1/0/1-2
esr(config-if-gi)# channel-group 2 mode auto
```

Дальнейшая конфигурация port-channel проводится как на обычном физическом интерфейсе.

1.43 Настройка VRRP

VRRP (Virtual Router Redundancy Protocol) – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети.

1.43.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Перейти в режим конфигурирования интерфейса/ туннеля/ сетевого моста, для которого необходимо настроить протокол VRRP | esr(config)# interface <IF-TYPE><IF-NUM> | <IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт. |
| | | esr(config)# tunnel <TUN-TYPE><TUN-NUM> | <TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля. |
| | | esr(config)# bridge <BR-NUM> | <BR-NUM> – номер сетевого моста. |
| 2 | Настроить необходимые параметры на интерфейсе/ туннеле/ сетевом мосту, включая IP-адрес | | |
| 3 | Включить VRRP-процесс на IP-интерфейсе. | esr(config-if-gi)# vrrp | |
| | | esr(config-if-gi)# ipv6 vrrp | |
| 4 | Установить виртуальный IP-адрес VRRP-маршрутизатора. | esr(config-if-gi)# vrrp ip <ADDR/LEN> | <ADDR/LEN> – виртуальный IP-адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 4 IP-адресов на интерфейс. |
| | | esr(config-if-gi)# ipv6 vrrp ip <IPV6-ADDR> | <IPV6-ADDR> – виртуальный IPv6-адрес, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8ми IPv6-адресов перечислением через запятую. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 5 | Установить идентификатор VRRP-маршрутизатора. | esr(config-if-gi)# vrrp id <VRID> | <VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255]. |
| | | esr(config-if-gi)# ipv6 vrrp id <VRID> | |
| 6 | Установить приоритет VRRP-маршрутизатора. | esr(config-if-gi)# vrrp priority <PR> | <PR> – приоритет VRRP-маршрутизатора, принимает значения [1..254]. |
| | | esr(config-if-gi)# ipv6 vrrp priority <PR> | Значение по умолчанию: 100. |
| 7 | Установить принадлежность VRRP-маршрутизатора к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произведется смена ролей. | esr(config-if-gi)# vrrp group <GRID> | <GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32]. |
| | | esr(config-if-gi)# ipv6 vrrp group <GRID> | |
| 8 | Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений. | esr(config-if-gi)# vrrp source-ip <IP> | <IP> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-if-gi)# ipv6 vrrp source-ip <IPV6> | <IPV6> – IPv6-адрес отправителя, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 9 | Установить интервал между отправкой VRRP-сообщений | esr(config-if-gi)# vrrp timers advertise <TIME> | <TIME> – время в секундах, принимает значения [1..40]. |
| | | esr(config-if-gi)# ipv6 vrrp timers advertise <TIME> | Значение по умолчанию: 1 секунда. |
| 10 | Установить интервал, по истечении которого происходит отправка GratuitousARP сообщения(ий) при переходе маршрутизатора в состояние Master. | esr(config-if-gi)# vrrp timers garp delay <TIME> | <TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5 секунд. |
| 11 | Установить количество GratuitousARP сообщений, которые будут отправлены при переходе маршрутизатора в состояние Master. | esr(config-if-gi)# vrrp timers garp repeat <COUNT> | <COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 5. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 12 | Установить интервал, по истечении которого будет происходить периодическая отправка GratuitousARP сообщения(ий), пока маршрутизатор находится в состоянии Master. | esr(config-if-gi)# vrrp timers garp refresh <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: Периодическая отправка отключена. |
| 13 | Установить количество GratuitousARP сообщений, которые будут отправляться с периодом garpprefresh пока маршрутизатор находится в состоянии Master. | esr(config-if-gi)# vrrp timers garp refresh-repeat <COUNT> | <COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 1. |
| 14 | Определить, будет ли Backup-маршрутизатор с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом. | esr(config-if-gi)# vrrp preemption disable esr(config-if-gi)# ipv6 vrrp preemption disable | |
| 15 | Установить временной интервал, по истечении которого Backup-маршрутизатор с более высоким приоритетом будет пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом. | esr(config-if-gi)# vrrp preemption delay <TIME> esr(config-if-gi)# ipv6 vrrp preemption delay <TIME> | <TIME> – время ожидания, определяется в секундах [1..1000]. Значение по умолчанию: 0 |
| 16 | Установить пароль для аутентификации с соседом. | esr(config-if-gi)# vrrp authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 17 | Определить алгоритм аутентификации. | esr(config-if-gi)# vrrp authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм аутентификации: <ul style="list-style-type: none"> • cleartext – пароль, передается открытым текстом; • md 5 – пароль хешируется по алгоритму md5. |
| 18 | Задать версию VRRP-протокола. | esr(config-if-gi)# vrrp version <VERSION> | <VERSION> – версия VRRP-протокола: 2, 3. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 19 | Установить режим, когда vrrp IP-адрес остается в состоянии UP вне зависимости от состояния самого интерфейса. (не обязательно) | esr(config-if-gi)# vrrp force-up | |
| 20 | Определить задержку между установлением ipv6 vrrp состояния MASTER и началом рассылки ND сообщений. | esr(config-if-gi)# ipv6 vrrp timers nd delay <TIME> | <TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5 |
| 21 | Определить период обновления информации протокола ND для ipv6 vrrp в состоянии MASTER. | esr(config-if-gi)# ipv6 vrrp timers nd refresh <TIME> | <TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 |
| 22 | Определить количество ND сообщений отправляемых за период обновления для ipv6 vrrp в состоянии MASTER. | esr(config-if-gi)# ipv6 vrrp timers nd refresh-repeat <NUM> | <NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 0 |
| 23 | Определить количество отправок ND пакетов после установки ipv6 vrrp в состоянии MASTER. | esr(config-if-gi)# ipv6 vrrp timers nd repeat <NUM> | <NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 1 |

1.43.2 Пример настройки 1

Задача:

Организовать виртуальный шлюз для локальной сети в VLAN 50, используя протокол VRRP. В качестве локального виртуального шлюза используется IP-адрес 192.168.1.1.

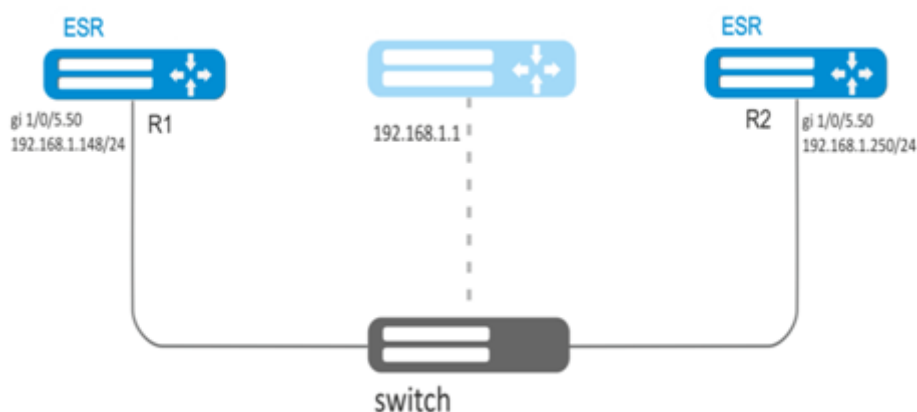


Рисунок 47 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- создать соответствующий саб-интерфейс;
- настроить зону для саб-интерфейса;
- указать IP-адрес для саб-интерфейса.

Основной этап конфигурирования:

Настроим маршрутизатор R1.

В созданном саб-интерфейсе настроим VRRP. Укажем уникальный идентификатор VRRP:

```
R1(config)#interface gi 1/0/5.50
R1(config-subif)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

```
R1(config-subif)# vrrp ip 192.168.1.1
```

Включим VRRP:

```
R1(config-subif)# vrrp
R1(config-subif)# exit
```

Произвести аналогичные настройки на R2.

1.43.3 Пример настройки 2

Задача:

Организовать виртуальные шлюзы для подсети 192.168.1.0/24 в VLAN 50 и подсети 192.168.20.0/24 в VLAN 60, используя протокол VRRP с функцией синхронизации Мастера. Для этого используем объединение VRRP-процессов в группу. В качестве виртуальных шлюзов используются IP-адреса 192.168.1.1 и 192.168.20.1.

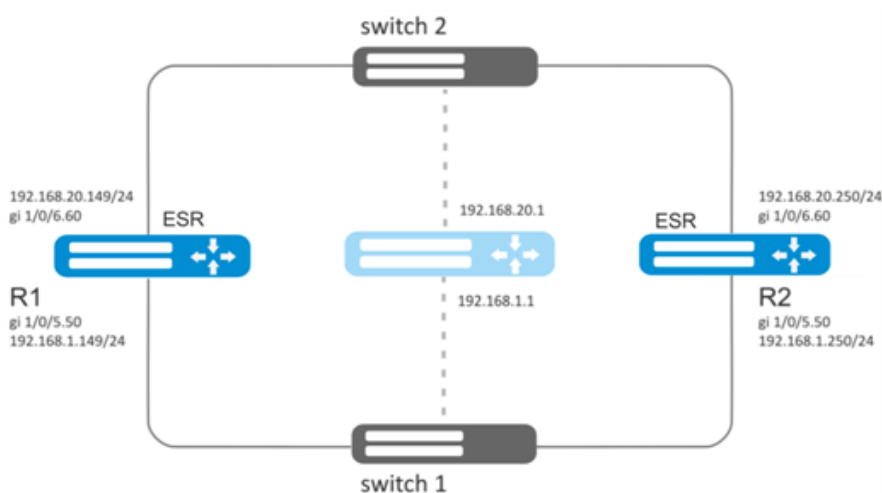


Рисунок 48 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- создать соответствующие саб-интерфейсы;
- настроить зону для саб-интерфейсов;
- указать IP-адреса для саб-интерфейсов.

Основной этап конфигурирования:

Настроим маршрутизатор R1.

Настроим VRRP для подсети 192.168.1.0/24 в созданном саб-интерфейсе.

Укажем уникальный идентификатор VRRP:

```
R1(config-sub)#interface gi 1/0/5.50  
R1(config-subif)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1:

```
R1(config-subif)# vrrp ip 192.168.1.1
```

Укажем идентификатор VRRP-группы:

```
R1(config-subif)# vrrp group 5
```

Включим VRRP:

```
R1(config-subif)# vrrp  
R1(config-subif)# exit
```

Настроим VRRP для подсети 192.168.20.0/24 в созданном саб-интерфейсе.

Укажем уникальный идентификатор VRRP:

```
R1(config-sub)#interface gi 1/0/6.60  
R1(config-subif)# vrrp id 20
```

Укажем IP-адрес виртуального шлюза 192.168.20.1:

```
R1(config-subif)# vrrp ip 192.168.20.1
```


Укажем идентификатор VRRP-группы:

```
R1(config-subif)# vrrp group 5
```

Включим VRRP:

```
R1(config-subif)# vrrp  
R1(config-subif)# exit
```

Произвести аналогичные настройки на R2.

 Помимо создания туннеля необходимо в firewall разрешить протокол VRRP(112).

1.44 Настройка VRRP tracking

VRRP tracking – механизм позволяющий активировать статические маршруты в зависимости от состояния VRRP.

1.44.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Настроить VRRP согласно разделу Алгоритм настройки USB-модемов . | | |
| 2 | Добавить в систему Tracking-объект и перейти в режим настройки параметров Tracking-объекта. | esr(config)#tracking <ID> | <ID> – номер Tracking-объекта, принимает значения [1..60]. |
| 3 | Задать правило слежения за состоянием VRRP-процесса. | esr(config-tracking)# vrrp <VRID> [not] state { master backup fault } | <VRID> – идентификатор отслеживаемого VRRP-маршрутизатора, принимает значения [1..255]. |
| 4 | Включить Tracking-объект. | esr(config-tracking)#enable | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 5 | Создать статический IP-маршрут к указанной подсети с указанием Tracking-объекта. | <pre>esr(config)# ip route [vrf <VRF>] <SUBNET> { <NEXTHOP> [resolve] interface <IF> tunnel <TUN> wan load-balance rule <RULE> blackhole unreachable prohibit } [<METRIC>] [track <TRACK-ID>]</pre> | <p><VRF> – имя экземпляра VRF, задается строкой до 31 символа;</p> <p><SUBNET> – адрес назначения, может быть задан в следующих видах:</p> <p>AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];</p> <p>AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].</p> <p><NEXTHOP> – IP-адрес шлюза задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <ul style="list-style-type: none"> • resolve – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему; <p><IF> – имя IP-интерфейса, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;</p> <p><TUN> – имя туннеля, задается в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;</p> <p><RULE> – номер правила wan, задается в диапазоне [1..50];</p> <ul style="list-style-type: none"> • blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю; |

| Шаг | Описание | Команда | Ключи |
|-----|----------|---------|--|
| | | | <ul style="list-style-type: none"> • unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1); • prohibit – при указании команды, пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13); <p>[METRIC] – метрика маршрута, принимает значения [0..255];</p> <p><TRACK-ID> – идентификатор Tracking объекта. Если маршрут привязан к Tracking объекту, то он появится в системе только при выполнении всех условий, заданных в объекте.</p> |

1.44.2 Пример настройки

Задача:

Для подсети 192.168.0.0/24 организован виртуальный шлюз 192.168.0.1/24 с использованием протокола VRRP на основе аппаратных маршрутизаторов R1 и R2. Так же между маршрутизаторами R1 и R2 есть линк с вырожденной подсетью 192.168.1.0/30. Подсеть 10.0.1.0/24 терминируется только на маршрутизаторе R2. ПК имеет IP-адрес 192.168.0.4/24 и шлюз по умолчанию 192.168.0.1

Когда маршрутизатор R1 находится в состоянии vrrp backup, трафик от ПК в подсеть 10.0.1.0/24 пойдет без дополнительных настроек. Когда маршрутизатор R1 находится в состоянии vrrp master, необходим дополнительный маршрут для подсети 10.0.1.0/24 через интерфейс 192.168.1.2.

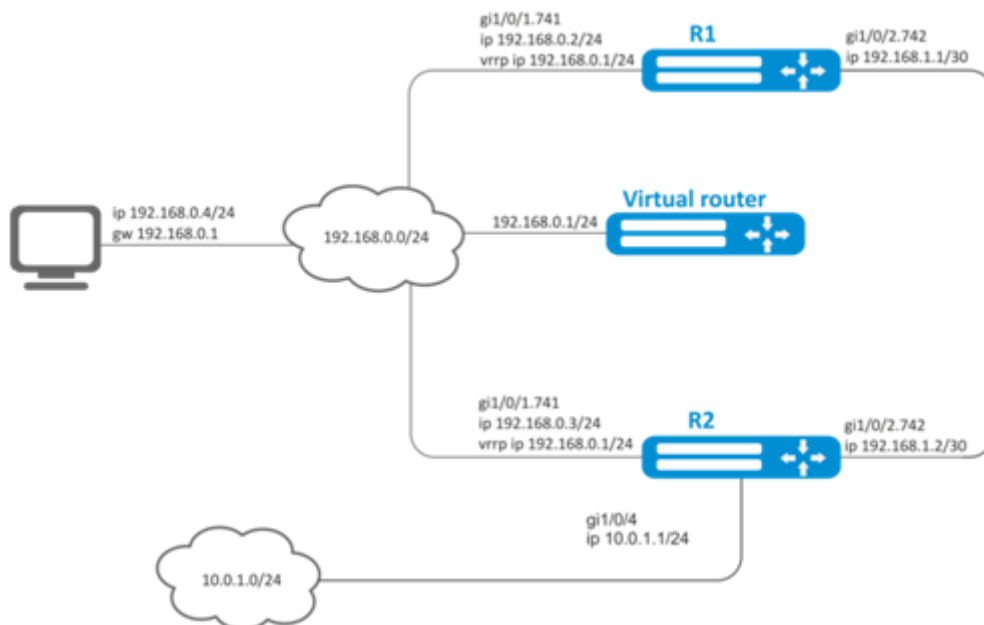


Рисунок 49 – Схема сети

Исходные конфигурации маршрутизаторов:**Маршрутизатор R1**

```

hostname R1
interface gigabitethernet 1/0/1
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
  ip firewall disable
  ip address 192.168.0.2/24
  vrrp id 10
  vrrp ip 192.168.0.1/24
  vrrp
exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.1/30
exit

```

Маршрутизатор R2

```

hostname R2
interface gigabitethernet 1/0/1
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
  ip firewall disable
  ip address 192.168.0.3/24
  vrrp id 10
  vrrp ip 192.168.0.1/24
  vrrp
exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.2/30
exit
interface gigabitethernet 1/0/4
  ip firewall disable
  ip address 10.0.1.1/24
exit

```

Решение :

На маршрутизаторе R2 никаких изменений не требуется так как подсеть 10.0.1.0/24 терминируется на нем, и в момент, когда R2 выступает в роли vrrp master, пакеты будут переданы в соответствующий интерфейс. На маршрутизаторе необходимо создать маршрут для пакетов с IP-адресом назначения из сети 10.0.1.0/24 в момент, когда R1 выступает в роли vrrp master.

Для этого создадим tracking-object с соответствующим условием:

```

R1(config)# tracking 1
R1(config-tracking)# vrrp 10 state master
R1(config-tracking)# enable
R1(config-tracking)# exit

```

Создадим статический маршрут в подсеть 10.0.1.0/24 через 192.168.1.2, который будет работать в случае удовлетворения условия из tracking 1:

```

R1(config)# ip route 10.0.1.0/24 192.168.1.2 track 1

```

1.45 Настройка VRF Lite

VRF (Virtual Routing and Forwarding) – технология, которая позволяет изолировать маршрутную информацию, принадлежащую различным классам (например, маршруты одного клиента).

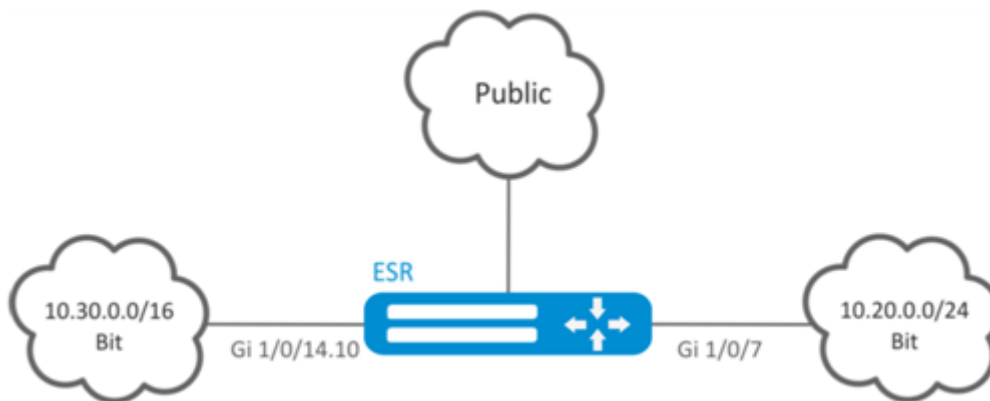


Рисунок 50 – Схема сети

1.45.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Создать экземпляр VRF и перейти в режим настройки параметров экземпляра VRF. | esr(config)# ip vrf <VRF> | <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 2 | Назначить описание конфигурируемого экземпляра VRF. | esr(config-vrf)# description <DESCRIPTION> | <DESCRIPTION> – описание экземпляра VRF, задается строкой до 255 символов. |
| 3 | Настроить емкость таблиц маршрутизации в конфигурируемом VRF для IPv4/IPv6 протоколов маршрутизации (не обязательно). | esr(config-vrf)# ip protocols <PROTOCOL> max-routes <VALUE> esr(config-vrf)#ipv6 protocols <PROTOCOL> max-routes <VALUE> | <PROTOCOL> – вид протокола, принимает значения: ospf, bgp; <VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне: OSPF ESR-1000/1200/1500/1510/1700 [1..500000], ESR-20/21/100/200 [1..300000], ESR-10/12V(F)/14VF [1..30000] BGP ESR-1000/1200/1500/1510/1700 [1..2800000], ESR-20/21/100/200 [1..1500000], ESR-10/12V(F)/14VF [1..800000]. Значение по умолчанию: 0 |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 4 | Включить и настроить протоколы динамической маршрутизации трафика (Static/OSPF/BGP) в экземпляре VRF (не обязательно). См. соответствующий раздел Конфигурирование статических маршрутов , Настройка OSPF и Настройка BGP . | | |
| 5 | В режиме конфигурирования физического/логического интерфейса, туннеля, правила DNAT/SNAT, DAS-сервера или SNMPv3 пользователя указать имя экземпляра VRF для которого будет использоваться (при необходимости). | esr(config-snat-ruleset)# ip vrf forwarding <VRF> | <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 6 | Настроить LT-туннель для передачи трафика в глобальный режим или другие VRF (при необходимости). | | |

1.45.2 Пример настройки

Задача:

К маршрутизатору серии ESR подключены 2 сети, которые необходимо изолировать от остальных сетей.

Решение:

Создадим VRF:

```
esr(config)# ip vrf bit
esr(config-vrf)# exit
```

Создадим зону безопасности:

```
esr(config)# security zone vrf-sec
esr(config-zone)# ip vrf forwarding bit
esr(config-zone)# exit
```

Создадим правило для пары зон и разрешим любой TCP/UDP-трафик:

```

esr(config)# security zone-pair vrf-sec vrf-sec
esr(config-zone-pair)# rule 1
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit

```

Создадим привязку интерфейсов, назначим IP-адреса, укажем принадлежность к зоне:

```

esr(config)# interface gigabitethernet 1/0/7
esr(config-if-gi)# ip vrf forwarding bit
esr(config-if-gi)# ip address 10.20.0.1/24
esr(config-if-gi)# security-zone vrf-sec
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/14.10
esr(config-subif)# ip vrf forwarding bit
esr(config-subif)# ip address 10.30.0.1/16
esr(config-subif)# security-zone vrf-sec
esr(config-subif)# exit
esr(config)# exit

```

Информацию об интерфейсах, привязанных к VRF, можно посмотреть командой:

```
esr# show ip vrf
```

Таблицу маршрутов VRF можно просмотреть с помощью команды:

```
esr# show ip route vrf bit
```

1.46 Настройка MultiWAN

Технология MultiWAN позволяет организовать отказоустойчивое соединение с резервированием линков от нескольких провайдеров, а также решает проблему балансировки трафика между резервными линками.

1.46.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 1 | Сконфигурировать интерфейсы, по которым будет работать MultiWAN: установить ip-адреса и указать security-zone. | | |
| 2 | Прописать статические маршруты через WAN (если необходимо). | esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>] | <ID> – идентификатор создаваемого правила из п.2. [METRIC] – метрика маршрута, принимает значения [0..255]. |
| 3 | Создать правило WAN и перейти в режим настройки параметров правила. | esr(config)# wan load-balance rule <ID> | <ID> – идентификатор создаваемого правила, принимает значения [1..50]. |
| 4 | Задать интерфейсы или туннели, которые являются шлюзами в маршруте, создаваемом службой MultiWAN. | esr(config-wan-rule)# outbound { interface <IF> tunnel <TUN> } [WEIGHT] | <IF>– имя интерфейса устройства; <TUN> – имя туннеля; [WEIGHT] – вес туннеля или интерфейса, определяется в диапазоне [1..255]. Если установить значение 2, то по данному интерфейсу будет передаваться в 2 раза больше трафика, чем по интерфейсу со значением по умолчанию. В режиме резервирования активным будет маршрут с наибольшим весом. Значение по умолчанию 1. |
| 5 | Описать правила (не обязательно). | esr(config-wan-rule)# description <DESCRIPTION> | <DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов. |
| 6 | Данной командой осуществляется переключение из режима балансировки в режим резервирования (если необходимо). | esr(config-wan-rule)# failover | |
| 7 | Включить wan правило. | esr(config-wan-rule)# enable | |
| 8 | Создать список IP-адресов для проверки целостности соединения и осуществить переход в режим настройки параметров списка. | esr(config)# wan load-balance target-list <NAME> | <NAME> – название списка, задаётся строкой до 31 символа. |
| 9 | Задать цель проверки и перейти в режим настройки параметров цели. | esr(config-target-list)# target <ID> | <ID> – идентификатор цели, задаётся в пределах [1..50]. Если при удалении используется значение параметра «all», то будут удалены все цели для конфигулируемого списка целей. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|--|
| 10 | Описать target (не обязательно). | esr(config-wan-target)# description <DESCRIPTION> | <DESCRIPTION> – описание target, задаётся строкой до 255 символов. |
| 11 | Указать время ожидания ответа на запрос по протоколу ICMP (не обязательно). | esr(config-wan-target)# resp- time <TIME> | <TIME> – время ожидания, определяется в секундах [1..30]. |
| 12 | Указать IP-адрес проверки. | esr(config-wan-target)# ip address <ADDR> | <ADDR> – IP-адрес назначения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-wan-target)# ipv6 address <IPV6-ADDR> | <IPV6-ADDR> – IPv6-адрес назначения, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 13 | Включить проверку цели. | esr(config-wan-target)# enable | |
| Команды для пунктов 13-17 необходимо применить на интерфейсах/туннелях в MultiWAN | | | |
| 14 | Включить WAN режим на интерфейсе для IPv4/IPv6 стека. | esr(config-if-gi)# wan load- balance enable | |
| | | esr(config-if-gi)# ipv6 wan load-balance enable | |
| 15 | Задать количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение будет считаться неактивным (не обязательно). | esr(config-if-gi)# wan load- balance failure-count <VALUE> | <VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию 1. |
| | | esr(config-if-gi)# ipv6 wan load-balance failure-count <VALUE> | |
| 16 | Задать количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным (не обязательно). | esr(config-if-gi)# wan load- balance success-count <VALUE> | <VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию 1. |
| | | esr(config-if-gi)# ipv6 wan load-balance success-count <VALUE> | |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 17 | Задать IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN. | esr(config-if-gi)# wan load-balance nexthop { <IP> dhcp enable tunnel enable } | <IP> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. dhcp enable – если на интерфейсе IP-адрес получен через DHCP-клиента, используется шлюз с DHCP-сервера. tunnel enable – использовать в качестве nexthop – p-t-p адрес назначения. Применимо для подключаемых интерфейсов работающих через ppp. |
| | | esr(config-if-gi)# ipv6 wan load-balance nexthop { <IPV6> } | <IPV6> – IPv6-адрес назначения (шлюз), задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 18 | Данной командой будут проверяться IP-адреса из списка проверки целостности. В случае недоступности одного из проверяемых узлов, шлюз будет считаться недоступным. | esr(config-if-gi)# wan load-balance target-list { check-all <NAME> } | <NAME> – проверку производить на основании конкретного target листа (заданного в п.7). |
| | | esr(config-if-gi)# ipv6 wan load-balance target-list { check-all <NAME> } | check-all – проверку производить на основании всех target листа. |
| 19 | Прописать статические маршруты через WAN (если необходимо). | esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>] | <ID> – идентификатор создаваемого правила из п.2. |
| | | esr(config)# ipv6 route <SUBNET> wan load-balance rule <ID> [<METRIC>] | [METRIC] – метрика маршрута, принимает значения [0..255]. |

1.46.2 Пример настройки

Задача:

Настроить маршрут к серверу (108.16.0.1/28) с возможностью балансировки нагрузки.



Рисунок 51 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- настроить зоны для интерфейсов te1/0/1 и te1/0/2;
- указать IP-адреса для интерфейсов te1/0/1 и te1/0/2.

Основной этап конфигурирования:

Настроим маршрутизацию:

```
esr(config)# ip route 108.16.0.0/28 wan load-balance rule 1
```

Создадим правило WAN:

```
esr(config)# wan load-balance rule 1
```

Укажем участвующие интерфейсы:

```
esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/2
esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/1
```

Включим созданное правило балансировки и выйдем из режима конфигурирования правила:

```
esr(config-wan-rule)# enable
esr(config-wan-rule)# exit
```

Создадим список для проверки целостности соединения:

```
esr(config)# wan load-balance target-list google
```

Создадим цель проверки целостности:

```
esr(config-target-list)# target 1
```

Зададим адрес для проверки, включим проверку указанного адреса и выйдем:

```
esr(config-wan-target)# ip address 8.8.8.8
esr(config-wan-target)# enable
esr(config-wan-target)# exit
```

Настроим интерфейсы. В режиме конфигурирования интерфейса te1/0/1 указываем nexthop:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if)# wan load-balance nexthop 203.0.0.1
```

В режиме конфигурирования интерфейса te1/0/1 указываем список целей для проверки соединения:

```
esr(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/1 включаем WAN-режим и выходим:

```
esr(config-if)# wan load-balance enable
esr(config-if)# exit
```

В режиме конфигурирования интерфейса te1/0/2 указываем nexthop:

```
esr(config)# interface tengigabitethernet 1/0/2
esr(config-if)# wan load-balance nexthop 65.6.0.1
```

В режиме конфигурирования интерфейса te1/0/2 указываем список целей для проверки соединения:

```
esr(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/2 включаем WAN-режим и выходим:

```
esr(config-if)# wan load-balance enable
esr(config-if)# exit
```

Для переключения в режим резервирования настроим следующее:

Заходим в режим настройки правила WAN:

```
esr(config)# wan load-balance rule 1
```

Функция MultiWAN также может работать в режиме резервирования, в котором трафик будет направляться в активный интерфейс с наибольшим весом. Включить данный режим можно следующей командой:

```
esr(config-wan-rule)# failover
```

1.47 Настройка SNMP

SNMP (англ. Simple Network Management Protocol – простой протокол сетевого управления) – протокол, предназначенный для управления устройствами в IP-сетях на основе архитектур TCP/UDP. SNMP предоставляет данные для управления в виде переменных, описывающих конфигурацию управляемой системы.

1.47.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|----------------------|---------------------------------|-------|
| 1 | Включить SNMP-сервер | esr(config)# snmp-server | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 2 | Определить community для доступа по протоколу SNMPv2c. | esr(config)# snmp-server community <COMMUNITY> [<TYPE>] [{ <IP-ADDR> <IPV6-ADDR> } [client-list <OBJ-GROUP-NETWORK-NAME>] [<VERSION>] [view <VIEW-NAME>] [vrf <VRF>] | <p><COMMUNITY> – сообщество для доступа по протоколу SNMP;</p> <p><TYPE> – уровень доступа:</p> <ul style="list-style-type: none"> • ro – доступ только для чтения; • rw – доступ для чтения и записи. <p><IP-ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];</p> <p><OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, от которых обрабатываются snmp-запросы, задаётся строкой до 31 символа;</p> <p><VERSION> – версия snmp, поддерживаемая данным community, принимает значения v1 или v2c;</p> <p><VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа;</p> <p><VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа.</p> |
| 3 | Устанавливает значение переменной SNMP, содержащей контактную информацию | esr(config)# snmp-server contact <CONTACT> | <CONTACT> – контактная информация, задается строкой до 255 символов. |
| 4 | Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно). | esr(config)# snmp-server dscp <DSCP> | <p><DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].</p> <p>Значение по умолчанию: 63.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 5 | Разрешить перезагрузку маршрутизатора при помощи snmp-сообщений (не обязательно) | esr(config)# snmp-server system-shutdown | |
| 6 | Создать SNMPv3-пользователь. | esr(config)# snmp-server user <NAME> | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 7 | Устанавливает значение переменной SNMP, содержащей информацию о расположении оборудования | esr(config)# snmp-server location <LOCATION> | <LOCATION> – информация о расположении оборудования, задаётся строкой до 255 символов. |
| 8 | Определить уровень доступа пользователя по протоколу SNMPv3. | esr(config-snmp-user)# access <TYPE> | <TYPE> – уровень доступа: <ul style="list-style-type: none"> • ro – доступ только для чтения; • rw – доступ для чтения и записи. |
| 9 | Определить режим безопасности пользователя по протоколу SNMPv3. | esr(config-snmp-user)# authentication access <TYPE> | <TYPE> – режим безопасности: <ul style="list-style-type: none"> • auth – используется только аутентификация; • priv – используется аутентификация и шифрование данных. |
| 10 | Определить алгоритм аутентификации SNMPv3-запросов. | esr(config-snmp-user)# authentication algorithm <ALGORITHM> | <ALGORITHM> – алгоритм шифрования: <ul style="list-style-type: none"> • md 5 – пароль шифруется по алгоритму md5; • sha 1 – пароль шифруется по алгоритму sha1. |
| 11 | Установить пароль для аутентификации SNMPv3-запросов. | esr(config-snmp-user)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ul style="list-style-type: none"> • encrypted – при указании команды задается зашифрованный пароль: <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 12 | Активировать фильтрацию и установить профиль IP-адресов, с которых могут приниматься SNMPv3 пакеты с данным именем SNMPv3 пользователя. | esr(config-snmp-user)# client-list <NAME> | <NAME> – имя ранее созданной object-group, задается строкой до 31 символа. |
| 13 | Активировать фильтрацию и установить IPv4/IPv6-адрес, которому предоставлен доступ к маршрутизатору под данным SNMPv3-пользователем. | esr(config-snmp-user)# ip address <ADDR> | <ADDR> – IP-адрес клиента, которому предоставлен доступ, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-snmp-user)# ipv6 address <ADDR> | <IPV6-ADDR> – IPv6-адрес клиента, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 14 | Активировать SNMPv3-пользователя. | esr(config-snmp-user)# enable | Значение по умолчанию: процесс выключен. |
| 15 | Определить алгоритм шифрования передаваемых данных. | esr(config-snmp-user)# privacy algorithm <ALGORITHM> | <p><ALGORITHM> – алгоритм шифрования:</p> <ul style="list-style-type: none"> • aes 128 – использовать алгоритм шифрования AES-128; • des – использовать алгоритм шифрования DES. |
| 16 | Установить пароль для шифрования передаваемых данных. | esr(config-snmp-user)# privacy key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> } | <p><CLEAR-TEXT> – пароль, задается строкой от 8 до 16 символов;</p> <p><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).</p> |
| | Установить профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для user. | esr(config-snmp-user)# view <VIEW-NAME> | <VIEW-NAME> – имя SNMP view профиля, на основании которого обеспечивается доступ к OID, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 17 | Включить передачу SNMP уведомлений на указанный IP-адрес и перейти в режим настройки SNMP уведомлений. | esr(config)# snmp-server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>] | <p><IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</p> <p><IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];</p> <p><VRF> – имя экземпляра VRF, в котором находится коллектор SNMP-уведомлений, задается строкой до 31 символа.</p> |
| 18 | Определить порт коллектора SNMP уведомлений на удаленном сервере (не обязательно). | esr(config-snmp-host)# port <PORT> | <p><PORT> – номер UDP-порта, указывается в диапазоне [1..65535].</p> <p>Значение по умолчанию: 162.</p> |
| 19 | Установить фильтрацию на отправляемые SNMP-уведомления. | esr(config)# snmp-server enable traps <TYPE> | <p><TYPE> – тип фильтруемых сообщений. Может принимать значения:</p> <p>config, entry, entry-sensor, environment, envmon, files-operations, flash, flash-operations, interfaces, links, ports, screens, snmp, syslog.</p> <p>Дополнительные параметры зависят от типа фильтра. См. Справочник команд CLI (ESR).</p> |
| 20 | Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3). | esr(config)# snmp-server enable traps <TYPE> | <p><VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа.</p> |

1.47.2 Пример настройки

Задача:

Настроить SNMPv3 сервер с аутентификацией и шифрованием данных для пользователя admin. IP-адрес маршрутизатора esr – 192.168.52.41, IP-адрес сервера – 192.168.52.8.



Рисунок 52 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- указать зону для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

Основной этап конфигурирования:

Включаем SNMP-сервер:

```
esr(config)# snmp-server
```

Создаем пользователя SNMPv3:

```
esr(config)# snmp-server user admin
```

Определим режим безопасности:

```
esr(snmp-user)# authentication access priv
```

Определим алгоритм аутентификации для SNMPv3-запросов:

```
esr(snmp-user)# authentication algorithm md5
```

Установим пароль для аутентификации SNMPv3-запросов:

```
esr(snmp-user)# authentication key ascii-text 123456789
```

Определим алгоритм шифрования передаваемых данных:

```
esr(snmp-user)# privacy algorithm aes128
```

Установим пароль для шифрования передаваемых данных:

```
esr(snmp-user)# privacy key ascii-text 123456789
```

Активируем SNMPv3-пользователя:

```
esr(snmp-user)# enable
```

Определяем сервер-приемник Trap-PDU сообщений:

```
esr(config)# snmp-server host 192.168.52.41
```

1.48 Настройка Zabbix-agent/proxy

Zabbix-agent – агент, предназначенный для мониторинга устройства, а также выполнения удаленных команд с Zabbix-сервера. Агент может работать в двух режимах: пассивный и активный. Для работы в пассивном режиме, по умолчанию, необходимо разрешающее правило в firewall – протокол tcp, порт 10050. Для активного режима – протокол tcp, порт 10051. Zabbix-прокси - это процесс, способный собирать данные мониторинга с одного или нескольких наблюдаемых устройств и отправлять эту информацию Zabbix-серверу.

1.48.1 Алгоритм настройки

| | | | |
|---|---|--|--|
| 1 | Перейти в контекст настройки агента/прокси. | esr(config)# zabbix-agent esr(config)# zabbix-proxy | |
| 2 | Указать имя узла сети (опционально). Для активного режима имя должно совпадать с именем узла сети на zabbix сервере. | esr(config-zabbix)# hostname <WORD> esr(config-zabbix-proxy)# hostname <WORD> | <WORD> – имя узла сети, задается строкой до 255 символов. |
| 3 | Указать адрес zabbix сервера. | esr(config-zabbix)# server <ADDR> esr(config-zabbix-proxy)# server <ADDR> | <ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 4 | Указать адрес сервера для активных проверок (при использовании активного режима). | esr(config-zabbix)# active-server <ADDR> <PORT> esr(config-zabbix-proxy)# active-server <ADDR> <PORT> | <ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <PORT> – Порт сервера, задается в диапазоне [1..65535]. Значение по умолчанию 10051. |
| 5 | Указать порт, который будет слушать агент/прокси (не обязательно) | esr(config-zabbix)# port <PORT> esr(config-zabbix-proxy)# port <PORT> | <PORT> – Порт, который слушает zabbix агент/прокси, задается в диапазоне [1..65535]. Значение по умолчанию: 10050. |
| 6 | Разрешить выполнение удаленных команд zabbix агентом/прокси (при использовании активного режима). | esr(config-zabbix)# remote-commands esr(config-zabbix-proxy)# remote-commands | |

| | | | |
|---|--|--|--|
| 7 | Указать адрес, с которого будет осуществляться взаимодействие с сервером (не обязательно). | <code>esr(config-zabbix)# source-address <ADDR></code> <code>esr(config-zabbix-proxy)# source-address <ADDR></code> | <ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Значение по умолчанию: ближайший адрес по маршрутизации. |
| 8 | Указать время обработки удаленных команд (не обязательно). | <code>esr(config-zabbix)# timeout <TIME></code> <code>esr(config-zabbix-proxy)# timeout <TIME></code> | <TIME> – время ожидания, определяется в секундах [1..30]. Значение по умолчанию 3. Рекомендуется устанавливать максимальное значение, т.к. некоторые команды могут выполняться дольше значения по умолчанию. Если за указанное время команда не будет выполнена, то обработка команды будет прекращена. |
| 9 | Включить функционал агента/прокси | <code>esr(config-zabbix)# enable</code> <code>esr(config-zabbix-proxy)# enable</code> | |

1.48.2 Пример настройки zabbix-agent/proxy



Рисунок 53 – Схема сети

Задача:

Настроить взаимодействие между агентом и сервером для выполнения удаленных команд с сервера.

Решение:

В контексте настройки агента укажем адрес zabbix сервера и адрес, с которого будет осуществляться взаимодействие с сервером:

```
esr(config-zabbix)# server 192.168.32.101
esr(config-zabbix)# source-address 192.168.39.170
```

Для активации активного режима укажем hostname, active-server, а также включим выполнение удаленных команд.

```

esr(config-zabbix)# hostname ESR-agent
esr(config-zabbix)# active-server 192.168.32.101
esr(config-zabbix)# source-address 192.168.39.170
esr(config-zabbix)# remote-commands

```

Зададим время выполнения удаленных команд и активируем функционал агента.

```

esr(config-zabbix)# timeout 30
esr(config-zabbix)# enable

```

1.48.3 Пример настройки zabbix-server

Создадим узел сети:

Узлы сети

Все узлы сети / TEST
Активировано ZBX SNMP JMX IPMI
Группы элементов данных 10
Элементы данных 94
Триггеры 15
Графики 36
Правила обнаружения 2
Веб-сценарии

Узел сети
Шаблоны
IPMI
Макросы
Инвентарные данные узла сети
Шифрование

* Имя узла сети

Видимое имя

* Группы SLA x Выбрать
начните печатать для поиска

* Должен существовать по крайней мере один интерфейс.

| Интерфейсы агента | IP адрес | DNS имя | Подключаться через | Порт | По умолчанию |
|--------------------------|---|----------------------|---|------------------------------------|--|
| | <input type="text" value="192.168.39.170"/> | <input type="text"/> | <input checked="" type="radio"/> IP <input type="radio"/> DNS | <input type="text" value="10050"/> | <input checked="" type="radio"/> Удалить |
| Добавить | | | | | |
| Интерфейсы SNMP | Добавить | | | | |
| Интерфейсы JMX | Добавить | | | | |
| Интерфейсы IPMI | Добавить | | | | |

Описание

Наблюдение через прокси (без прокси)

Активировано

Обновить
Клонировать
Полное клонирование
Удалить
Отмена

Создадим скрипт (Администрирование -> Скрипты-> Создать скрипт)

Общие Прокси Аутентификация Группы пользователей Пользователи Способы оповещений **Скрипты** Очередь

Скрипты

* Имя

Тип IPMI Скрипт

Выполнять на Zabbix агент Zabbix сервер (прокси) Zabbix сервер

* Команды

Описание

Группа пользователей

Группа узлов сети

Требуемые права доступа к узлам сети Чтение Запись

Включить подтверждение

Текст подтверждения

Маршрутизаторы ESR поддерживают выполнение следующих удаленных команд:

- **Ping:**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo ping -c 3 192.168.32.101]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит ping до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Ping в VRF:**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo netns-exec -n backup sudo ping 192.168.32.101 -c 5 -W 2 ]"
```

Вышеупомянутая команда будет выполнена в заданном VRF.

- **Fping**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo fping 192.168.32.101]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит fping до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Fping в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo netns-exec -n backup sudo fping 192.168.32.101 ]"
```


- **Traceroute**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo traceroute 192.168.32.101]
```

Клиент (ESR), получивший данную команду от сервера, выполнит traceroute до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Traceroute в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo netns-exec -n backup sudo traceroute 192.168.32.179]"
```

- **Iperf**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo iperf -c 192.168.32.101 -u -b 100K -i 1 -t 600]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит iperf до заданного сервера (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Iperf в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo netns-exec -n backup sudo iperf -c 192.168.32.101 -u -b 100K -i 1 -t 600]"
```

- **Nslookup**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo nslookup ya.ru ]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит nslookup , и вернет результат серверу.

- **Nslookup в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo netns-exec sudo nslookup ya.ru ]"
```

Пример выполнения команды Iperf:

iperf_agent

x

```
zabbix_get -s 192.168.39.170 -p 10050 -k "system.run[ sudo iperf -c 192.168.32.101]"
```

```
-----  
Client connecting to 192.168.32.101, TCP port 5001
```

```
TCP window size: 49.5 KByte (default)  
-----
```

```
[ 3] local 192.168.39.170 port 52815 connected with 192.168.32.101 port 5001
```

```
[ ID] Interval      Transfer      Bandwidth
```

```
[ 3] 0.0-10.0 sec  1.01 GBytes   864 Mbits/sec
```

[Отмена](#)

1.49 Настройка Syslog

Syslog (англ. system log – системный журнал) – стандарт отправки и регистрации сообщений о происходящих в системе событиях, используется в сетях, работающих по протоколу IP.

1.49.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Задать уровень syslog-сообщений, которые будут передаваться SNMP-Traps сообщениями (не обязательно) | esr(config)# syslog alarms <SEVERITY> | <p><SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности):</p> <ul style="list-style-type: none"> • emerg – в системе произошла критическая ошибка, система неработоспособна; • alert – сигналы тревоги, необходимо немедленное вмешательство персонала; • crit – критическое состояние системы, сообщение о событии; • error – сообщения об ошибках; • warning – предупреждения, неаварийные сообщения; • notice – сообщения о важных системных событиях; • info – информационные сообщения системы; • debug – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы; • none – отключает вывод syslog-сообщений. |
| 2 | Задать уровень syslog-сообщений, которые будут отображаться при удаленных подключениях (Telnet, SSH) (не обязательно) | esr(config)# syslog monitor <SEVERITY> | |
| 3 | Включить процесс логирования введённых команд пользователя на локальный syslog-сервер (не обязательно) | esr(config)# syslog cli-commands | |
| 4 | Включить сохранение сообщений syslog заданного уровня важности в указанный файл журнала | esr(config)# syslog file <NAME> <SEVERITY> | <p><NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа;</p> <p><SEVERITY> описано в команде syslog alarms.</p> |
| 5 | Указать максимальный размер файла журнала (не обязательно) | esr(config)# syslog file-size <SIZE> | <SIZE> – размер файла, принимает значение [10..1000000] кбайт |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 6 | Задать максимальное количество файлов, сохраняемых при ротации (не обязательно) | esr(config)# syslog max-files <NUM> | <NUM> – максимальное количество файлов, принимает значения [1.. 1000] |
| 7 | Включить передачу сообщений syslog заданного уровня важности на удаленный syslog-сервер | esr(config)#syslog host <HOSTNAME> <ADDR> <SEVERITY> <TRANSPORT> <PORT> | <p><HOSTNAME> – наименование syslog-сервера, задаётся строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде no syslog host для удаления всех syslog-серверов;</p> <p><ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><SEVERITY> – уровень важности сообщения, опциональный параметр, возможные значения приведены в разделе Пример настройки Syslog;</p> <p><TRANSPORT> – протокол передачи данных, опциональный параметр, принимает значения:</p> <ul style="list-style-type: none"> • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP; <p><PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514</p> |
| 8 | Включить вывод отладочных сообщений во время загрузки устройства (не обязательно) | esr(config)#syslog reload debugging | |
| 9 | Включить нумерацию сообщений (не обязательно) | esr(config)#syslog sequence-numbers | |
| 10 | Включить точность даты сообщений до миллисекунд (не обязательно). | esr(config)#syslog timestamp msec | |
| 11 | Включить регистрацию неудачных аутентификаций (не обязательно). | esr(config)#logging login on-failure | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|-------|
| 12 | Включить регистрацию изменений настроек системы аудита (не обязательно). | esr(config)#logging syslog configuration | |
| 13 | Включить регистрацию изменений настроек пользователя (не обязательно). | esr(config)#logging userinfo | |

1.49.2 Пример настройки Syslog

Задача:

Настроить отправку сообщений для следующих системных событий:

- неудачная аутентификация пользователя;
- внесены изменения в конфигурацию логирования системных событий;
- старт/остановка системного процесса;
- внесены изменения в профиль пользователей.

IP-адрес маршрутизатора ESR – 192.168.52.8, ip-адрес Syslog сервера – 192.168.52.41. Использовать параметры по умолчанию для отправки сообщений – протокол UDP порт 514.



Рисунок 54 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- указать зону для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

Основной этап конфигурирования:

Создаем файл на маршрутизаторе для системного журнала, уровень сообщений для журналирования – info:

```
esr(config)# syslog file ESR info
```

Указываем IP адрес и параметры удаленного Syslog-сервера:

```
esr(config)# syslog host SERVER 192.168.17.30 info udp 514
```

Задаем логирование неудачных попыток аутентификации:

```
esr(config)# logging login on-failure
```

Задаем логирование изменений конфигурации syslog:

```
esr(config)# logging syslog configuration
```

Задаем логирование старта/остановки системных процессов:

```
esr(config)# logging service start-stop
```

Задаем логирование внесений изменений в профиль пользователей:

```
esr(config)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

```
esr# commit  
Configuration has been successfully committed  
esr# confirm  
Configuration has been successfully confirmed
```

Посмотреть текущую конфигурацию системного журнала:

```
esr# show syslog configuration
```

Посмотреть записи системного журнала:

```
esr# show syslog ESR
```

1.50 Настройка BRAS (Broadband Remote Access Server)

1.50.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования. | esr(config)# radius -server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>]esr(config-radius-server)# | <p><IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><IPV6-ADDR>–IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]</p> <p><VRF> – имя экземпляра VRF, задается строкой до 31 символа.</p> |
| 2 | Задать пароль для аутентификации на удаленном RADIUS-сервере. | esr(config-radius-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } | <TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 3 | Создать профиль AAA. | esr(config)# aaa radius-profile <NAME> | <NAME> – имя профиля сервера, задается строкой до 31 символа. |
| 4 | В профиле AAA указать RADIUS-сервер. | esr(config-aaa-radius-profile)# radius-server host { <IP-ADDR> <IPV6-ADDR> } | <p><IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><IPV6-ADDR>–IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].</p> |
| 5 | Создать DAS-сервер. | esr(config)# das-server <NAME> | <NAME> – имя DAS-сервера, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 6 | Задать пароль для аутентификации на удаленном DAS-сервере. | esr(config-das-server)# key ascii-text {<TEXT> encrypted <ENCRYPTED-TEXT> } | <TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 7 | Создать AAA DAS-профиль. | esr(config)# aaa das-profile <NAME> | <NAME> – имя DAS-профиля, задается строкой до 31 символа. |
| 8 | Указать DAS-сервер в DAS-профиле. | esr(config-aaa-das-profile)# das-server <NAME> | <NAME> – имя DAS-сервера, задается строкой до 31 символа. |
| 9 | Сконфигуровать BRAS. | esr(config)# subscriber-control [vrf <VRF>] | <VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать контроль пользователей. |
| 10 | Выбрать профиль серверов динамической авторизации (DAS), на которые будут приходить CoA-запросы от PCRF | esr(config-subscriber-control)# aaa das-profile <NAME> | <NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа. |
| 11 | Выбрать профиль RADIUS-серверов для получения параметров сервисов пользователя | esr(config-subscriber-control)# aaa services-radius-profile <NAME> | <NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа. |
| 12 | Выбрать профиль RADIUS-серверов для получения параметров сессии пользователя. | esr(config-subscriber-control)# aaa sessions-radius-profile <NAME> | <NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа. |
| 13 | Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS пакетах. | esr(config-subscriber-control)# nas-ip-address <ADDR> | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 14 | Включить аутентификацию сессий по MAC-адресу (не обязательно). | esr(config-subscriber-control)# session mac-authentication | |
| 15 | Организовать прозрачное пропускание служебного трафика (DHCP, DNS и т.д.) на основе фильтров. | esr(config-subscriber-control)# bypass-traffic-a c l <NAME> | <NAME> – имя привязываемого ACL, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 16 | Перейти в режим конфигурирования сервиса по умолчанию. | esr(config-subscriber-control)# default-service | |
| 17 | Привязать указанный QoS-класс к сервису по умолчанию. | esr(config-subscriber-default-service)# class-map <NAME> | <NAME> – имя привязываемого класса, задается строкой до 31 символа. |
| 18 | Указать имя списка URL, который будет использоваться для фильтрации HTTP/HTTPS трафика не аутентифицированных пользователей. | esr(config-subscriber-default-service)# filter-name { local<LOCAL-NAME> remote<REMOTE-NAME> } | <LOCAL-NAME> – имя профиля URL, задается строкой до 31 символа; <REMOTE-NAME> – имя списка URL на удаленном сервере, задается строкой до 31 символа. |
| 19 | Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых входит в список URL, назначенных командой «filter-name». | esr(config-subscriber-default-service)# filter-action<ACT> | <ACT> – назначаемое действие: <ul style="list-style-type: none"> • permit – прохождение трафика разрешается; • deny – прохождение трафика запрещается; redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов. |
| 20 | Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых не входит в список URL, назначенных командой «filter-name». | esr(config-subscriber-default-service)# default-action<ACT> | <ACT> – назначаемое действие: <ul style="list-style-type: none"> • permit – прохождение трафика разрешается; • deny – прохождение трафика запрещается; redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов. |
| 21 | Активировать профиль контроля пользователей. | esr(config-subscriber-control)# enable | |
| 22 | Изменить идентификатор сетевого интерфейса (физического, саб-интерфейса или сетевого моста) (не обязательно). | esr(config-if)# location <ID> | <ID> – идентификатор сетевого интерфейса, задается строкой до 220 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 23 | Включить контроль пользователей на интерфейсе. | esr(config-if-gi)# service-subscriber-control {any object-group <NAME>} | <NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. |
| 24 | Включить перезапрос значения квоты при ее истечении для сервисов пользователя с настроенным ограничением по объему трафика или времени (не обязательно). | esr(config-subscriber-control)# quota-expired-reauth | |
| 25 | Включить аутентификацию сессий по IP-адресу. (не обязательно) | esr(config-subscriber-control)# session ip-authentication | |
| 26 | Включить прозрачное пропускание трафика в состоянии backup для BRAS (не обязательно). | esr(config-subscriber-control)# backup traffic-processing transparent | |
| 27 | Задать интервал, по истечении которого с устройства будут удалены неиспользуемые в текущий момент списки URL (не обязательно). | esr(config)# subscriber-control unused-filters-remove-delay <DELAY> | <DELAY> – временной интервал в секундах, принимает значения [10800..86400]. |
| 28 | Задать интервал, по истечении которого, если не было пакетов от пользователя, сессия считается устаревшей и удаляется с устройства (не обязательно). | esr(config-subscriber-default-service)# session-timeout <SEC> | <SEC> – период времени в секундах, принимает значения [120..3600]. |
| 29 | Определить VRRP-группу, на основе которой определяется состояние сервиса контроля абонентов (основной/резервный) (не обязательно). | esr(config-subscriber-control)# vrrp-group <GRID> | <GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 30 | Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTP Proxy-сервер маршрутизатора (не обязательно). | esr(config-subscriber-control)# ip proxy http listen-ports <NAME> | <NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа. |
| 31 | Определить порт HTTP Proxy-сервера на маршрутизаторе (не обязательно). | esr(config-subscriber-control)# ip proxy http redirect-port <PORT> | <PORT> – номер порта, указывается в диапазоне [1..65535]. |
| 32 | Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTPS Proxy-сервер маршрутизатора (не обязательно). | esr(config-subscriber-control)# ip proxy https listen-ports <NAME> | <NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа. |
| 33 | Определить порт HTTPS Proxy-сервера на маршрутизаторе (не обязательно). | esr(config-subscriber-control)# ip proxy https redirect-port <PORT> | <PORT> – номер порта, указывается в диапазоне [1..65535]. |
| 34 | Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых Proxy-сервером HTTP/HTTPS пакетах (не обязательно). | esr(config-subscriber-control)# ip proxy source-address <ADDR> | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 35 | Задать URL-адрес сервера, предоставляющего списки приложений для фильтрации трафика (не обязательно) | esr(config)# subscriber-control apps-server-url <URL> | <URL> – адрес ссылки, задаётся строкой от 8 до 255 символов. |
| 36 | Включить контроль приложений на интерфейсе (не обязательно) | esr(config-if-gi)# subscriber-control application-filter <NAME> | <NAME> – имя профиля приложений, задаётся строкой до 31 символа. |
| 37 | Установить/ сбросить верхнюю границу количества сессий BRAS (не обязательно) | esr(config-subscriber-control)# thresholds sessions-number high <Threshold> | <Threshold> – количество сессий BRAS, [0-50000] – для ESR-1700 <ul style="list-style-type: none"> • [0-10000] – для ESR-1200/1000 • [0-1000] – для ESR-100/200 |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 38 | Установить/ сбросить нижнюю границу количества сессий BRAS (не обязательно) | esr(config-subscriber-control)# thresholds sessions-number low <Threshold> | <p><Threshold> – количество сессий BRAS, [0-50000] – для ESR-1700</p> <ul style="list-style-type: none"> • [0-10000] – для ESR-1200/1000 • [0-1000] – для ESR-100/200 |

1.50.2 Пример настройки с SoftWLC

Задача:

Предоставлять доступ до ресурсов сети Интернет, только для авторизованных пользователей.

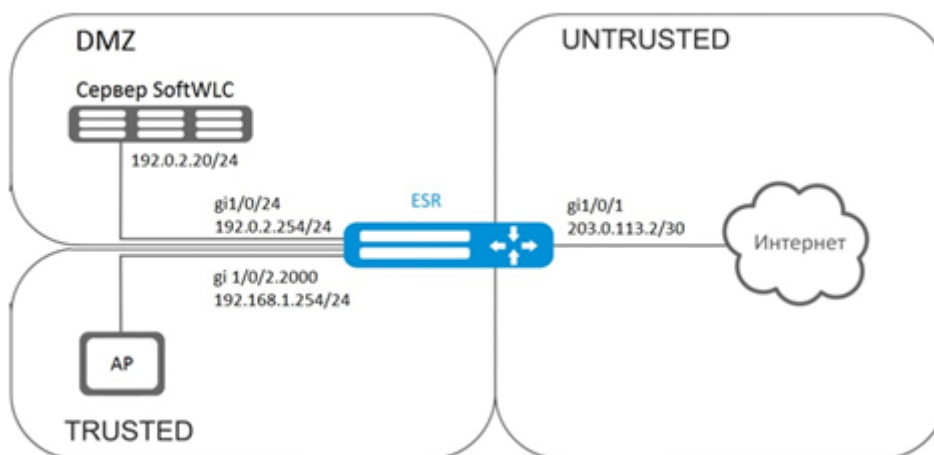


Рисунок 55 – Схема сети

Решение:

За хранение учетных данных пользователей и параметров тарифных планов отвечает сервер SoftWLC. Информацию по установке и настройке сервера SoftWLC можно найти по ссылкам ниже:

<http://kcs.eltex.nsk.ru/articles/960> – общая статья о SoftWLC;

<http://kcs.eltex.nsk.ru/articles/474> – установка SoftWLC из репозитория.

Для маршрутизатора необходимо наличие лицензии BRAS, после ее активации можно переходить к конфигурированию устройства.

Создадим три зоны безопасности на устройстве, согласно схеме сети:

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# security zone dmz
esr(config-zone)# exit
```

Сконфигурируем параметры публичного порта и сразу пропишем шлюз по умолчанию:

```

esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 203.0.113.2/30
esr(config-if-gi)# service-policy dynamic upstream
esr(config-if-gi)# exit
esr(config)# ip route 0.0.0.0/0 203.0.113.1

```

Сконфигурируем порт в сторону сервера SoftWLC:

```

esr (config)# interface gigabitethernet 1/0/24
esr (config-if-gi)# security-zone dmz
esr (config-if-gi)# ip address 192.0.2.1/24
esr (config-if-gi)# exit

```

Сконфигурируем порт для подключения Wi-Fi точки доступа.

```

esr(config)# bridge 2
esr(config-bridge)# security-zone trusted
esr(config-bridge)# ip address 192.168.0.254/24
esr(config-bridge)# ip helper-address 192.0.2.20
esr(config-bridge)# service-subscriber-control object-group users
esr(config-bridge)# location ssid1
esr(config-bridge)# enable
esr(config-bridge)# exit
esr(config)# interface gigabitethernet 1/0/2.2000
esr(config-subif)# bridge-group 1
esr(config-subif)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-policy dynamic downstream
esr (config-if-gi)# exit

```

⚠ Подключать клиентов необходимо через сабинтерфейсы в бриджи, причем от параметра location (смотри конфигурацию bridge 2) зависит выбор тарифного плана.

Модуль, отвечающий за AAA-операции, основан на eltex-radius и доступен по IP-адресу сервера SoftWLC. Номера портов для аутентификации и аккаунтинга в нашем примере – это значения по умолчанию для SoftWLC.

Зададим параметры для взаимодействия с этим модулем:

```

esr(config)# radius-server host 192.0.2.20
esr(config-radius-server)# key ascii-text password
esr(config-radius-server)# auth-port 31812
esr (config-radius-server)# acct-port 31813
esr (config-radius-server)# exit

```

Создадим профиль AAA:

```

esr(config)# aaa radius-profile RADIUS
esr(config-aaa-radius-profile)# radius-server host 192.0.2.20
esr(config-aaa-radius-profile)# exit

```

Укажем параметры доступа к DAS (Direct-attached storage) серверу:

```

esr(config)# object-group network server
esr(config-object-group-network)# ip address-range 192.0.2.20
esr(config-object-group-network)# exit
esr(config)# das-server CoA
esr(config-das-server)# key ascii-text password
esr(config-das-server)# port 3799
esr(config-das-server)# clients object-group server
esr(config-das-server)# exit
esr(config)# aaa das-profile CoA
esr(config-aaa-das-profile)# das-server CoA
esr(config-aaa-das-profile)# exit

```

До аутентификации весь трафик из зоны trusted блокируется, в том числе DHCP и DNS запросы. Необходимо настроить разрешающие правила для пропуска DHCP и DNS запросов:

```

esr(config)# ip access-list extended DHCP
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 11
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit

```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```

esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended INTERNET
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit

```

Зададим web-ресурсы доступные без авторизации:

```
esr(config)# object-group url defaultservice
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# exit
```

Списки фильтрации по URL находятся на сервере SoftWLC (меняется только IP-адрес сервера SoftWLC, если используется адресация отличная от данного примера, все остальное в URL оставить без изменения):

```
esr(config)# subscriber-control filters-server-url http://192.0.2.20:7070/Filters/file/
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с SoftWLC, в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/24:

```
esr(config)# subscriber-control
esr(config-subscriber-control)# aaa das-profile CoA
esr(config-subscriber-control)# aaa sessions-radius-profile RADIUS
esr(config-subscriber-control)# nas-ip-address 192.0.2.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl DHCP
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map INTERNET
esr(config-subscriber-default-service)# filter-name local defaultservice
esr(config-subscriber-default-service)# filter-action permit
esr(config-subscriber-default-service)# default-action redirect http://192.0.2.20:8080/
eltex_portal/
esr(config-subscriber-default-service)# session-timeout 3600
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit
```

Далее необходимо сконфигурировать правила перехода между зонами безопасности.

```
esr(config)# object-group service telnet
esr(config-object-group-service)# port-range 23
esr(config-object-group-service)# exit
esr(config)# object-group service ssh
esr(config-object-group-service)# port-range 22
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# object-group service ntp
esr(config-object-group-service)# port-range 123
esr(config-object-group-service)# exit
```

Разрешим доступ в Интернет из зон trusted и dmz:

```

esr(config)# security zone-pair trusted untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz trusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

Разрешим прохождение DHCP из trusted в dmz:

```

esr (config)# security zone-pair trusted dmz
esr (config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port dhcp_client
esr(config-zone-pair-rule)# match destination-port dhcp_server
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

Разрешим прохождение ICMP к устройству, для работы BRAS необходимо открыть порты для веб-проксирования – TCP 3129/3128 (NetPort Discovery Port/Active API Server Port):


```

esr(config)# object-group service bras
esr(config-object-group-service)# port-range 3129
esr(config-object-group-service)# port-range 3128
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port any
esr(config-zone-pair-rule)# match destination-port bras
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair dmz self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit

```

Активируем DHCP-Relay:

```
esr(config)# ip dhcp-relay
```

Настроим SNAT в порт gigabitethernet 1/0/1:

```

esr(config)# nat source
esr(config-snat)# ruleset inet
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/1
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# end

```

1.50.3 Пример настройки без SoftWLC

Задача:

Настроить BRAS без поддержки SoftWLC.

Дано:

Подсеть с клиентами 10.10.0.0/16, подсеть для работы с FreeRADIUS-сервером 192.168.1.1/24

Решение:

Шаг 1:

Настройка RADIUS-сервера.

Для FreeRADIUS-сервера нужно задать подсеть, из которой могут приходить запросы и добавить список пользователей. Для этого в файл users в директории с файлами конфигурации FreeRADIUS сервера нужно добавить:

Профиль пользователя:

<MACADDR> Cleartext-Password := <MACADDR>

#Имя пользователя

User-Name = <USER_NAME>,

#Максимальное время жизни сессии

Session-Timeout = <SECONDS>,

#Максимальное время жизни сессии при бездействии пользователя

Idle-Timeout = <SECONDS>,

#Время на обновление статистики по сессии

Acct-Interim-Interval = <SECONDS>,

#Имя сервиса для сессии (A – сервис включен, N – сервис выключен)

Cisco-Account-Info = "{A|N}<SERVICE_NAME>"

Профиль сервиса:

<SERVICE_NAME> Cleartext-Password := <MACADDR>

Соответствует имени class-map в настройках ESR

Cisco-AVPair = "subscriber:traffic-class=<CLASS_MAP>,"

Действие, которое применяет ESR к трафику (permit, deny, redirect)

Cisco-AVPair = "subscriber:filter-default-action=<ACTION>,"

Возможность прохождения IP потоков (enabled-uplink, enabled-downlink, enabled, disabled)

Cisco-AVPair = "subscriber:flow-status=<STATUS>"

В файл clients.conf нужно добавить подсеть, в которой находится ESR:

client ESR {

ipaddr = <SUBNET>

```
secret = <RADIUS_KEY>
```

```
}
```

В нашем случае настройка RADIUS-сервера будет выглядеть так:

в файл «clients.conf» добавляем строки:

```
client BRAS {
```

```
ipaddr = 192.168.1.1
```

```
secret = password
```

```
}
```

В файл «users» добавляем строки (вместо <MAC> нужно указать MAC адрес клиента):

```
"54-E1-AD-8F-37-35" Cleartext-Password := "54-E1-AD-8F-37-35"
```

```
User-Name = "Bras_user",
```

```
Session-Timeout = 259200,
```

```
Idle-Timeout = 259200,
```

```
Cisco-AVPair += "subscriber:policer-rate-in=1000",
```

```
Cisco-AVPair += "subscriber:policer-rate-out=1000",
```

```
Cisco-AVPair += "subscriber:policer-burst-in=188",
```

```
Cisco-AVPair += "subscriber:policer-burst-out=188",
```

```
Cisco-Account-Info = "AINTERNET"
```

```
INTERNET Cleartext-Password := "INTERNET"
```

```
User-Name = "INTERNET",
```

```
Cisco-AVPair = "subscriber:traffic-class=INTERNET",
```

```
Cisco-AVPair += "subscriber:filter-default-action=permit"
```

Шаг 2:

Настройка ESR.

Для настройки функционала BRAS необходимо наличие лицензии BRAS.

```
esr(config)# do sh licence
```

```
Licence information
```

```
-----
```

```
Name:    Eltex
```

```
Version: 1.0
```

```
Type:    ESR-X
```

```
S/N:     NP00000000
```

```
MAC:     XX:XX:XX:XX:XX:XX
```

```
Features:
```

```
BRAS - Broadband Remote Access Server
```

Настройка параметров для взаимодействия с RADIUS-сервером:

```
esr(config)# radius-server host 192.168.1.2
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# source-address 192.168.1.1
esr(config-radius-server)# exit
```

Создадим профиль AAA:

```
esr(config)# aaa radius-profile bras_radius
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)# exit
esr(config)# aaa radius-profile bras_radius_servers
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)# exit
```

Укажем параметры к DAS-серверу:

```
esr(config)# das-server das
esr(config-das-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-das-server)# exit
esr(config)# aaa das-profile bras_das
esr(config-aaa-das-profile)# das-server das
esr(config-aaa-das-profile)# exit
esr(config)# vlan 10
esr(config-vlan)# exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
esr(config)# ip access-list extended BYPASS
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 2
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended INTERNET
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 443
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 20
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8443
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 30
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 80
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 40
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
```

```

esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8080
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit

```

Настройка действие фильтрации по URL обязательно, а именно, необходимо настроить фильтрацию http-проxy на BRAS для неавторизованных пользователей:

```

esr(config)# object-group url defaultserv
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# url http://ya.ru
esr(config-object-group-url)# url https://ya.ru
esr(config-object-group-url)# exit

```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с RADIUS-сервером в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/2:

```

esr(config)# subscriber-control
esr(config-subscriber-control)# aaa das-profile bras_das
esr(config-subscriber-control)# aaa sessions-radius-profile bras_radius
esr(config-subscriber-control)# aaa services-radius-profile bras_radius_servers
esr(config-subscriber-control)# nas-ip-address 192.168.1.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl BYPASS
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map BYPASS
esr(config-subscriber-default-service)# filter-name local defaultserv
esr(config-subscriber-default-service)# filter-action permit
esr(config-subscriber-default-service)# default-action redirect http://192.168.1.2:8080/eltex_portal
esr(config-subscriber-default-service)# session-timeout 121
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit

```

На интерфейсах, для которых требуется работа BRAS настроить (для успешного запуска требуется как минимум один интерфейс):

```

esr(config)# bridge 10
esr(config-bridge)# vlan 10
esr(config-bridge)# ip firewall disable
esr(config-bridge)# ip address 10.10.0.1/16
esr(config-bridge)# ip helper-address 192.168.1.2
esr(config-bridge)# service-subscriber-control any
esr(config-bridge)# location USER
esr(config-bridge)# protected-ports
esr(config-bridge)# protected-ports exclude vlan
esr(config-bridge)# enable
esr(config-bridge)# exit

```

Сконфигурируем порт в сторону RADIUS-сервера:

```

esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit

```

Порт в сторону Клиента:

```

esr(config)# interface gigabitethernet 1/0/3.10
esr(config-subif)# bridge-group 10
esr(config-subif)# ip firewall disable
esr(config-subif)# exit

```

Настройка SNAT в порт gigabitethernet 1/0/2:

```

esr(config)# nat source
esr(config-snat)# ruleset factory
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/2
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
esr(config-snat-rule)# match protocol any
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# match destination-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
esr(config-snat)# exit
esr(config)# ip route 0.0.0.0/0 192.168.1.2

```

Изменения конфигурации вступят в действие после применения:

```

esr(config) # do commit
esr(config) # do confirm

```

Для просмотра информации и статистики по сессиям контроля пользователей – можно воспользоваться командой:

```

esr # sh subscriber-control sessions status

```

| Session id | User name | IP address | MAC address | Interface | Domain |
|---------------------|-----------|------------|-------------------|------------|--------|
| 1729382256910270473 | Bras_user | 10.10.0.3 | 54:e1:ad:8f:37:35 | gi1/0/3.10 | -- |

1.51 Настройка IPS/IDS

IPS/IDS (*Intrusion Prevention System / Intrusion Detection System*) – система предотвращения вторжений – программная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Работа системы основана на сигнатурном анализе трафика. Сигнатуры для систем IPS/IDS принято называть правилами. Устройства ESR позволяют скачивать актуальные правила с открытых источников

в сети Интернет или с корпоративного сервера. Так-же с помощью CLI можно создавать свои, специфические правила.

По умолчанию на устройствах ESR установлен базовый набор правил от компании EmergingThreats предназначенный для тестирования и проверки работоспособности системы.

1.51.1 Алгоритм базовой настройки

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 1 | Создать политику безопасности IPS/IDS. | esr(config)# security ips policy <NAME> | <NAME> – имя политики безопасности, задаётся строкой до 32 символов |
| 2 | Задать описание политики (не обязательно). | esr(config-ips-policy)# description <DESCRIPTION> | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 3 | Задать профиль IP-адресов, которые будет защищать IPS/IDS. | esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля защищаемых IP-адресов, задается строкой до 32 символов. |
| 4 | Задать профиль IP- адресов, внешних для IPS/IDS (не обязательно). | esr(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля внешних IP-адресов, задается строкой до 32 символов. |
| 5 | Перейти в режим конфигурирования IPS/IDS. | esr(config)# security ips | |
| 6 | Назначить политику безопасности IPS/IDS. | esr(config-ips)# policy <NAME> | <NAME> – имя политики безопасности, задаётся строкой до 32 символов |
| 7 | Использовать все ресурсы ESR для IPS/IDS. (не обязательно). | esr(config-ips)# perfomance max | По умолчанию для IPS/IDS отдается половина доступных ядер процессора. |
| 8 | Задать USB диск, для записи логов в формате EVE. (не обязательно). | esr(config-ips)# logging storage-device <DEVICE_NAME> | <DEVICE_NAME> имя usb накопителя. |
| 9 | Активировать IPS/IDS. | esr(config- ips)# enable | |
| 10 | Активировать IPS/IDS на интерфейсе. | esr(config-if-gi)# service-ips enable | |

1.51.2 Алгоритм настройки автообновления правил IPS/IDS из внешних источников.

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 1 | Перейти в режим конфигурирования автообновлений. | esr(config-ips)# auto-upgrade | |
| 2 | Задать имя и перейти в режим конфигурирования пользовательского сервера обновлений. | esr(config-ips-auto-upgrade)# user-server <WORD> | <WORD> – имя сервера, задаётся строкой до 32 символов. |
| 3 | Задать описание пользовательского сервера обновлений. (не обязательно). | esr(config-ips-upgrade-user-server)# description <DESCRIPTION> | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 4 | Задать URL. | esr(config-ips-upgrade-user-server)# url <URL> | <URL> – текстовое поле, содержащее URL-ссылку длиной от 8 до 255 символов. В качестве URL-ссылки может быть указан: <ul style="list-style-type: none"> • файл правил с расширением .rule; • файл классификатора правил с именем classification.config; • каталог на сервере содержащий файлы правил и/или файл классификатора правил. |
| 5 | Задать частоту проверки обновлений. (не обязательно). | esr(config-ips-upgrade-user-server)# upgrade interval <HOURS> | <HOURS> – интервал обновлений в часах, от 1 до 240. Значение по умолчанию: 24 часа |

1.51.3 Рекомендуемые открытые источники обновления правил

| | |
|---|--|
| https://sslbl.abuse.ch/ | SSL Blacklist содержит списки «плохих» SSL сертификатов, т.е. сертификатов, в отношении которых установлен факт их использования вредоносным ПО и ботнетами. В списках содержатся SHA1 отпечатки публичных ключей из SSL сертификатов. |
|---|--|

| | |
|---|--|
| https://feodotracker.abuse.ch/ | Feodo Tracker – список управляющих серверов для троянской программы Feodo. Feodo (также известный как Cridex или Bugat) используется злоумышленниками для кражи чувствительной информации в сфере электронного банкинга (данные по кредитным картам, логины/пароли) с компьютеров пользователей. В настоящее время существует четыре версии троянской программы (версии A, B, C и D), главным образом отличающиеся инфраструктурой управляющих серверов. |
| https://rules.emergingthreats.net/open/suricata/rules/botcc.rules | Данные правила описывают известные ботнеты и управляющие сервера. Источники: Shadowserver.org , Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker. |
| https://rules.emergingthreats.net/open/suricata/rules/ciarmy.rules | Данные правила описывают вредоносные хосты по классификации проекта www.cinsarmy.com . |
| https://rules.emergingthreats.net/open/suricata/rules/compromised.rules | Данные правила описывают известные скомпрометированные и вредоносные хосты. Источники: Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects. |
| https://rules.emergingthreats.net/open/suricata/rules/drop.rules | Данные правила описывают спамерские хосты / сети по классификации проекта www.spamhaus.org . |
| https://rules.emergingthreats.net/open/suricata/rules/dshield.rules | Данные правила описывают вредоносные хосты по классификации проекта www.dshield.org . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-activex.rules | Данные правила содержат сигнатуры использования ActiveX-контента. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-attack_response.rules | Правила, детектирующие поведение хоста после успешно проведенных атак. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-chat.rules | Данные правила описывают признаки обращения к популярным чатам. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-current_events.rules | Временные правила, ожидающие возможного включения в постоянные списки правил. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules | Данные правила содержат сигнатуры уязвимостей в протоколе DNS, признаки использования DNS вредоносным ПО, некорректного использования протокола DNS. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-dos.rules | Данные правила содержат сигнатуры DOS-атак. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-exploit.rules | Данные правила содержат сигнатуры эксплойтов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-ftp.rules | Данные правила содержат сигнатуры уязвимостей в протоколе FTP, признаки некорректного использования протокола FTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-games.rules | Данные правила описывают признаки обращения к популярным игровым сайтам: World of Warcraft, Starcraft и т.п. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules | Данные правила содержат сигнатуры некорректного использования протокола ICMP. |

| | |
|---|--|
| https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp_info.rules | Данные правила содержат сигнатуры информационных ICMP-сообщений. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-imap.rules | Данные правила содержат сигнатуры уязвимостей в протоколе IMAP, признаки некорректного использования протокола IMAP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-inappropriate.rules | Данные правила описывают признаки обращения к нежелательным ресурсам. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-info.rules | Данные правила содержат сигнатуры различных уязвимостей. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-malware.rules | Данные правила содержат сигнатуры вредоносного ПО, использующего в своей работе протокол HTTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-misc.rules | Данные правила содержат сигнатуры различных уязвимостей. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-mobile_malware.rules | Данные правила содержат сигнатуры вредоносного ПО для мобильных платформ. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-netbios.rules | Данные правила содержат сигнатуры уязвимостей в протоколе NetBIOS, признаки некорректного использования протокола NetBIOS. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-p2p.rules | Данные правила описывают признаки обращения к P2P-сетям (Bittorrent, Gnutella, Limewire). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-policy.rules | Данные правила описывают нежелательную сетевую активность (обращение к MySpace, Ebay). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-poprules | Данные правила содержат сигнатуры уязвимостей в протоколе POP3, признаки некорректного использования протокола POP3. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-rpc.rules | Данные правила содержат сигнатуры уязвимостей в протоколе RPC, признаки некорректного использования протокола RPC. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-scada.rules | Данные правила содержат сигнатуры уязвимостей для SCADA-систем. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-scan.rules | Данные правила описывают признаки активности, связанной с сетевым сканированием (Nessus, Nikto, portscanning). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-shellcode.rules | Данные правила описывают признаки активности, связанной с попытками получить шелл-доступ в результате выполнения эксплойтов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-smtp.rules | Данные правила содержат сигнатуры уязвимостей в протоколе SMTP, признаки некорректного использования протокола SMTP. |

| | |
|---|---|
| https://rules.emergingthreats.net/open/suricata/rules/emerging-sql.rules | Данные правила содержат сигнатуры уязвимостей для СУБД SQL. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-telnet.rules | Данные правила содержат сигнатуры уязвимостей для протокола telnet, признаки некорректного использования протокола telnet. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-tftp.rules | Данные правила содержат сигнатуры уязвимостей в протоколе TFTP, признаки некорректного использования протокола TFTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-trojan.rules | Данные правила содержат признаки сетевой активности троянских программ. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-user_agents.rules | Данные правила содержат признаки подозрительных и потенциально опасных HTTP-клиентов (идентифицируются по значениям в HTTP-заголовке User-Agent). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-l.rules | Данные правила содержат сигнатуры уязвимостей в VOIP-протокола. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_client.rules | Данные правила содержат сигнатуры уязвимостей для веб-клиентов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_server.rules | Данные правила содержат сигнатуры уязвимостей для веб-серверов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_specific_apps.rules | Данные правила содержат сигнатуры эксплуатации уязвимостей веб-приложений. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules | Данные правила описывают признаки активности сетевых червей. |

1.51.4 Пример настройки IPS/IDS с автообновлением правил

Задача:

Организовать защиту локальной сети с автообновлением правил из открытых источников.

192.168.1.0/24 – локальная сеть

Решение:

Создадим профиль адресов локальной сети, которую будем защищать:

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

Настроим на ESR DNS-клиента для разрешения имен источников обновления правил IPS/IDS

```
esr(config)# domain lookup enable
esr(config)# domain name-server 8.8.8.8
```

Создадим политику безопасности IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

Разрешим работу IPS/IDS на интерфейсе локальной сети bridge 1:

```
esr(config)# bridge 1
esr(config-bridge)# service-ips enable
```

Настроим параметры IPS/IDS:

```
esr(config)# security ips
esr(config-ips)# logging storage-device usb://DATA
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
```

Устройство будет использоваться только как шлюз безопасности, по этому отдадим сервису IPS/IDS все доступные ресурсы:

```
esr(config-ips)# performance max
```

Настроим автообновление правил с сайтов [EmergingThreats.net](https://www.emergingthreats.net), [etnetera.cz](https://www.etnetera.cz) и [Abuse.ch](https://www.abuse.ch):

```
esr(config-ips)# auto-upgrade
esr(config-auto-upgrade)# user-server ET-Open
esr(config-ips-upgrade-user-server)# description «emerging threats open rules»
esr(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/suricata-4.0/rules/
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server Aggressive
esr(config-ips-upgrade-user-server)# description «Etnetera aggressive IP blacklist»
esr(config-ips-upgrade-user-server)# url https://security.etnetera.cz/feeds/etn_aggressive.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server SSL-BlackList
esr(config-ips-upgrade-user-server)# description «Abuse.ch SSL Blacklist»
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server C2-Botnet
esr(config-ips-upgrade-user-server)# description «Abuse.ch Botnet C2 IP Blacklist»
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslipblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
```

1.51.5 Алгоритм настройки базовых пользовательских правил

| Шаг | Описание | Команда | Ключи |
|-----|--|---|--|
| 1 | Задать имя и перейти в режим конфигурирования набора пользовательских правил | esr(config)# security ips-category user-defined <WORD> | <WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов. |
| 2 | Задать описание набора пользовательских правил (не обязательно). | esr(config-ips-category)# description <DESCRIPTION> | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 3 | Создать правило и перейти в режим конфигурирования правила. | esr(config-ips-category)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1..512]. |
| 4 | Задать описание правила (не обязательно) | esr(config-ips-category-rule)# description <DESCRIPTION> | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 5 | Указать действие данного правила | esr(config-ips-category-rule)# action { alert reject pass drop } | <ul style="list-style-type: none"> • alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP трафик отправителю и получателю посылаются пакеты TCP-RESET, для остального типа трафика посылаются пакеты ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение. |
| 6 | Установить имя IP-протокола, для которого должно срабатывать правило | esr(config-ips-category-rule)# protocol <PROTOCOL> | <p><PROTOCOL> – принимает значения any/ip/icmp/http/tcp/udp</p> <p>При указании значения «any» правило будет срабатывать для любых протоколов</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 7 | <p>Установить IP-адреса отправителя для которых должно срабатывать правило</p> | <pre>esr(config-ips-category-rule)# source-address {ip <ADDR> ip-prefix <ADDR/LEN> object-group <OBJ_GR_NAME> policy-object-group { protect external } any }</pre> | <p><<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><ADDR/LEN> – IP-подсеть отправителя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32].</p> <p>< OBJ_GR_NAME> – имя профиля IP-адресов, который содержит ip адреса отправителя, задаётся строкой до 31 символа.</p> <ul style="list-style-type: none"> • protect – устанавливает в качестве адресов отправителя, protect адреса определенные в политике IPS/IDS; • external – устанавливает в качестве адресов отправителя, external адреса определенные в политике IPS/IDS. <p>При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.</p> |
| 8 | <p>Установить номера TCP/UDP-портов отправителя, для которых должно срабатывать правило.</p> <p>Для значения protocol icmp, значение source-port может быть только any</p> | <pre>esr(config-ips-category-rule)# source-port {any <PORT> object-group <OBJ-GR-NAME> }</pre> | <p><PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535].</p> <p><OBJ_GR_NAME> – имя профиля TCP/UDP портов отправителя, задаётся строкой до 31 символа.</p> <p>При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 9 | Установить IP-адреса получателя для которых должно срабатывать правило | esr(config-ips-category-rule)# destination-address {ip <ADDR> ip-prefix <ADDR/LEN> object-group <OBJ_GR_NAME> policy-object-group { protect external } any } | <p><ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];</p> <p><ADDR/LEN> – IP-подсеть получателя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32].</p> <p>< OBJ_GR_NAME> – имя профиля IP-адресов, который содержит ip адреса получателя, задаётся строкой до 31 символа.</p> <ul style="list-style-type: none"> • protect – устанавливает в качестве адресов получателя, protect адреса определенные в политике IPS/IDS; • external -устанавливает в качестве адресов получателя, external адреса определенные в политике IPS/IDS. <p>При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.</p> |
| 10 | Установить номера TCP/UDP-портов получателя, для которых должно срабатывать правило. Для значения protocol icmp, значение destination-port может быть только any | esr(config-ips-category-rule)# destination-port {any <PORT> object-group <OBJ-GR-NAME> } | <p><PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535].</p> <p><OBJ_GR_NAME> – имя профиля TCP/UDP портов получателя, задаётся строкой до 31 символа.</p> <p>При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.</p> |
| 11 | Установить направление потока трафика, для которого должно срабатывать правило | esr(config-ips-category-rule)# direction { one-way round-trip } | <ul style="list-style-type: none"> • one-way – трафик передаётся в одну сторону. • round-trip – трафик передаётся в обе стороны. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 12 | Определить сообщение которое IPS/IDS будет записывать в лог, при срабатывании этого правила | esr(config-ips-category-rule)# meta log-message <MESSAGE> | <MESSAGE> – текстовое сообщение, задаётся строкой до 129 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 13 | <p>Определить классификацию трафика, которая будет записываться в лог, при срабатывании этого правила</p> <p>(не обязательно)</p> | <pre>esr(config-ips-category-rule)# meta classification-type { not-suspicious unknown bad-unknown attempted-recon successful-recon-limited successful- recon-largescale attempted-dos successful-dos attempted-user unsuccessful-user successful-user attempted-admin successful-admin rpc- portmap-decode shellcode-detect string-detect suspicious-filename-detect suspicious-login system-call-detect tcp-connection trojan-activity unusual- client-port-connection network-scan denial-of-service non-standard-protocol protocol-command-decode web- application-activity web-application- attack misc-activity misc-attack icmp- event inappropriate-content policy- violation default-login-attempt }</pre> | <ul style="list-style-type: none"> • not-suspicious – не подозрительный трафик. • unknown – неизвестный трафик. • bad-unknown – потенциально плохой трафик. • attempted-recon – попытка утечки информации. • successful-recon-limited – утечка информации. • successful-recon-largescale – масштабная утечка информации. • attempted-dos – попытка отказа в обслуживании. • successful-dos – отказ в обслуживании. • attempted-user – попытка получения привилегий пользователя. • unsuccessful-user – безуспешная попытка получения привилегий пользователя. • successful-user – успешная попытка получения привилегий пользователя. • attempted-admin – попытка получения привилегий администратора. • successful-admin – успешная попытка получения привилегий администратора. • rpc-portmap-decode – декодирование запроса RPC. • shellcode-detect – обнаружен исполняемый код. • string-detect – обнаружена подозрительная строка. • suspicious-filename-detect – было обнаружено подозрительное имя-файла. |

| Шаг | Описание | Команда | Ключи |
|-----|----------|---------|---|
| | | | <ul style="list-style-type: none"> • suspicious-login – была обнаружена попытка входа с использованием подозрительного имени пользователя. • system-call-detect – обнаружен системный вызов. • tcp-connection – обнаружено TCP-соединение. • trojan-activity – был обнаружен сетевой троян. • unusual-client-port-connection – клиент использовал необычный порт. • network-scan – обнаружение сетевого сканирования. • denial-of-service – обнаружение атаки отказа в обслуживании. • non-standard-protocol – обнаружение нестандартного протокола или события. • protocol-command-decode – обнаружена попытка шифрования. • web-application-activity – доступ к потенциально уязвимому веб-приложению. • web-application-attack – атака на веб-приложение. • misc-activity – прочая активность. • misc-attack – прочие атаки. • icmp-event – общее событие ICMP. • inappropriate-content – обнаружено неприемлемое содержание. • policy-violation – потенциальное нарушение корпоративной конфиденциальности. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| | | | <ul style="list-style-type: none"> • default-login-attempt – попытка входа с помощью стандартного логина/пароля. |
| 14 | Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). | esr(config-ips-category-rule)# ip dscp <DSCP> | <DSCP> – значение кода DSCP, принимает значения [0..63]. |
| 15 | Установить значение времени жизни пакета (TTL), для которого должно срабатывать правило (не обязательно). | esr(config-ips-category-rule)# ip ttl <TTL> | <TTL> – значение TTL, принимает значения в диапазоне [1..255]. |
| 16 | Установить номер IP-протокола, для которого должно срабатывать правило Применимо только для значения protocol any (не обязательно). | esr(config-ips-category-rule)# ip protocol-id <ID> | <ID> – идентификационный номер IP-протокола, принимает значения [1..255]. |
| 17 | Установить значения ICMP CODE, для которого должно срабатывать правило Применимо только для значения protocol icmp (не обязательно). | esr(config-ips-category-rule)# ip icmp code <CODE> | <CODE> – значение CODE протокола ICMP, принимает значение в диапазоне [0..255]. |
| | | esr(config-ips-category-rule)# ip icmp code comparison-operator { greater-than less-than } | Оператор сравнения для значения ip icmp code: <ul style="list-style-type: none"> • greater-than – больше чем.. • less-than – меньше чем.. |
| 18 | Установить значения ICMP ID, для которого должно срабатывать правило Применимо только для значения protocol icmp (не обязательно). | esr(config-ips-category-rule)# ip icmp id <ID> | <ID> – значение ID протокола ICMP, принимает значение в диапазоне [0.. 65535]. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 19 | Установить значения ICMP Sequence-ID, для которого должно срабатывать правило Применимо только для значения protocol icmp (не обязательно). | esr(config-ips-category-rule)# ip icmp sequence-id <SEQ-ID> | <SEQ-ID> – значение Sequence-ID протокола ICMP, принимает значение в диапазоне [0..4294967295]. |
| 20 | Установить значения ICMP TYPE, для которого должно срабатывать правило Применимо только для значения protocol icmp (не обязательно). | esr(config-ips-category-rule)# ip icmp type <TYPE> | <TYPE> – значение TYPE протокола ICMP, принимает значение в диапазоне [0..255]. |
| | | esr(config-ips-category-rule)# ip icmp type comparison-operator { greater-than less-than } | Оператор сравнения для значения ip icmp type: <ul style="list-style-type: none"> • greater-than – больше чем.. • less-than – меньше чем.. |
| 21 | Установить значения TCP Acknowledgment-Number, для которого должно срабатывать правило Применимо только для значения protocol tcp (не обязательно). | esr(config-ips-category-rule)# ip tcp acknowledgment-number <ACK-NUM> | <ACK-NUM> – значение Acknowledgment-Number протокола TCP, принимает значение в диапазоне [0..4294967295]. |
| 22 | Установить значения TCP Sequence-ID, для которого должно срабатывать правило Применимо только для значения protocol tcp (не обязательно). | esr(config-ips-category-rule)# ip tcp sequence-id <SEQ-ID> | <SEQ-ID> – значение Sequence-ID протокола TCP, принимает значение в диапазоне [0..4294967295]. |
| 23 | Установить значения TCP Window-Size, для которого должно срабатывать правило Применимо только для значения protocol tcp (не обязательно). | esr(config-ips-category-rule)# ip tcp window-size <SIZE> | <SIZE> – значение Window-Size протокола TCP, принимает значение в диапазоне [0.. 65535]. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 24 | <p>Установить ключевые слова протокола HTTP, для которых должно срабатывать правило</p> <p>Применимо только для значения protocol http (не обязательно).</p> | esr(config-ips-category-rule)# ip http { accept accept-enc accept-lang client-body connection content-type cookie file-data header header-names host method protocol referer request-line response-line server-body start start-code start-msg uri user-agent } | <p>Значение ключевых слов см в документации Suricata 4.X.</p> <p>https://suricata.readthedocs.io/en/suricata-4.1.4/rules/http-keywords.html</p> |
| 25 | <p>Установить значение ключевого слова URI LEN протокола HTTP, для которых должно срабатывать правило</p> <p>Применимо только для значения protocol http (не обязательно).</p> | esr(config-ips-category-rule)# ip http urilen <LEN> | <LEN> – принимает значение в диапазоне [0.. 65535]. |
| | | esr(config-ips-category-rule)# ip http urilen comparison-operator { greater-than less-than } | <p>Оператор сравнения для значения ip http urilen:</p> <ul style="list-style-type: none"> • greater-than – больше чем.. • less-than – меньше чем.. |
| 26 | <p>Установить значение содержимого пакетов (Payload content), для которых должно срабатывать правило</p> <p>(не обязательно).</p> | esr(config-ips-category-rule)# payload content <CONTENT> | <CONTENT> – текстовое сообщение, задаётся строкой до 1024 символов. |
| 27 | <p>Не различать прописные и заглавные буквы в описании содержимого пакетов.</p> <p>Применимо только совместно с командой payload content (не обязательно).</p> | esr(config-ips-category-rule)# payload no-case | |
| 28 | <p>Установить сколько байтов с начала содержимого пакета будет проверено.</p> <p>Применимо только совместно с командой payload content (не обязательно).</p> | esr(config-ips-category-rule)# payload depth <DEPTH> | <p><DEPTH> – число байт с начала содержимого пакета, принимает значение в диапазоне [1.. 65535].</p> <p>По умолчанию проверяется все содержимое пакета.</p> |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 29 | <p>Установить число байт смещения от начала содержимого пакета для проверки.</p> <p>Применимо только совместно с командой <code>payload content</code> (не обязательно).</p> | esr(config-ips-category-rule)# payload offset <OFFSET> | <p><OFFSET> – число байт смещения от начала содержимого пакета, принимает значение в диапазоне [1.. 65535].</p> <p>По умолчанию проверяется с начала содержимого.</p> |
| 30 | <p>Установить размер содержимого пакетов, для которых должно срабатывать правило.</p> <p>(не обязательно)</p> | esr(config-ips-category-rule)# payload data-size <SIZE> | <SIZE> – размер содержимого пакетов, принимает значение в диапазоне [0.. 65535]. |
| | | esr(config-ips-category-rule)# payload data-size comparison-operator { greater-than less-than } | <p>Оператор сравнения для значения <code>payload data-size</code>:</p> <ul style="list-style-type: none"> • greater-than – больше чем.. • less-than – меньше чем. |
| 31 | <p>Указать пороговое значение количества пакетов, при котором сработает правило</p> <p>(не обязательно)</p> | esr(config-ips-category-rule)# threshold count <COUNT> | <COUNT> – число пакетов, принимает значение в диапазоне [1.. 65535]. |
| 32 | <p>Указать интервал времени, для которого считается пороговое количество пакетов.</p> <p>(Обязательно если включен <code>threshold count</code>)</p> | esr(config-ips-category-rule)# threshold second <SECOND> | <SECOND> – интервал времени в секундах, принимает значение в диапазоне [1.. 65535]. |
| 33 | <p>Указать по адресу отправителя или получателя будут считаться пороги.</p> <p>(Обязательно если включен <code>threshold count</code>)</p> | esr(config-ips-category-rule)# threshold track { by-src by-dst } | <ul style="list-style-type: none"> • by-src – считать пороговое значение для пакетов с одинаковым IP-отправителя. • by-dst – считать пороговое значение для пакетов с одинаковым IP-получателя. |

| Шаг | Описание | Команда | Ключи |
|-----|--|--|--|
| 34 | Указать метод обработки пороговых значений | esr(config-ips-category-rule)# threshold type {threshold limit both } | <ul style="list-style-type: none"> • threshold – выдавать сообщение каждый раз по достижении порога. • limit – выдавать сообщение не чаще <COUNT> раз за интервал времени <SECOND>. • both – комбинация threshold и limit. <p>Сообщение будет генерироваться, если в течении интервала времени <SECOND> было <COUNT> или более пакетов подходящих под условия правила, и сообщение будет отправлено только один раз в течении интервала времени <SECOND></p> |

1.51.6 Пример настройки базовых пользовательских правил

Задача:

Написать правило для защиты сервера с IP 192.168.1.10 от DOS-атаки ICMP-пакетами большого размера.

Решение:

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined USER
```

Создадим правило для защиты от атаки:

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)# description «Big ICMP DoS»
```

Мы будем отбрасывать пакеты:

```
esr(config-ips-category-rule)# action drop
```

Настроим сообщение об атаке:

```
esr(config-ips-category-rule)# meta log-message «Big ICMP DoS»
esr(config-ips-category-rule)# meta classification-type successful-dos
```

Укажем тип протокола для правила:


```
esr(config-ips-category-rule)# protocol icmp
```

Так как мы указали протокол icmp, то в качестве порта отправителя и получателя требуется указать any:

```
esr(config-ips-category-rule)# source-port any
esr(config-ips-category-rule)# destination-port any
```

В качестве адреса получателя укажем наш сервер:

```
esr(config-ips-category-rule)# destination-address ip 192.168.1.10
```

Атакующий может отправлять пакеты с любого адреса:

```
esr(config-ips-category-rule)# source-address any
```

Зададим направление трафика:

```
esr(config-ips-category-rule)# direction one-way
```

Правило будет срабатывать на пакеты размером больше 1024байт:

```
esr(config-ips-category-rule)# payload data-size 1024
esr(config-ips-category-rule)# payload data-size comparison-operator greater-than
```

Правило будет срабатывать если нагрузка на сервер будет превышать 3Мб/с, при этом сообщение об атаке будет генерироваться не чаще одного раза в минуту:

```
3 Мб/с = 3145728 бит в сек
Пакет размером 1Кбайт = 8192 бита
3145728 / 8192 = 384 пакета в сек
384 * 60 = 23040 пакетов в минуту
```

```
esr(config-ips-category-rule)# threshold count 2340
esr(config-ips-category-rule)# threshold second 60
esr(config-ips-category-rule)# threshold track by-dst
esr(config-ips-category-rule)# threshold type both
```

1.51.7 Алгоритм настройки расширенных пользовательских правил

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 1 | Задать имя и перейти в режим конфигурирования набора пользовательских правил. | esr(config)# security ips-category user-defined <WORD> | <WORD> –имя набора пользовательских правил, задаётся строкой до 32 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 2 | Задать описание набора пользовательских правил (не обязательно). | esr(config-ips-category)# description <DESCRIPTION> | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 3 | Создать расширенное правило и перейти в режим его конфигурирования. | esr(config-ips-category)# rule-advanced <SID> | <SID> – номер правила, принимает значения [1.. 4294967295] |
| 4 | Задать описание правила (не обязательно) | esr(config-ips-category-rule-advanced)# description <DESCRIPTION> | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 5 | Указать действие данного правила | esr(config-ips-category-rule-advanced)# rule-text <LINE> | <CONTENT> -текстовое сообщение в формате SNORT 2.X / Suricata 4.X, задаётся строкой до 1024 символов. <i>При написании правил символ " требуется заменить на символ '</i> |

1.51.8 Пример настройки расширенных пользовательских правил

Задача:

Написать правило детектирующее атаку типа Slowloris.

Решение:

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined ADV
```

Создадим расширенное правило:

```
esr(config-ips-category)# rule-advanced 1
esr(config-ips-category-rule-advanced)# description «Slow Loris rule 1»
esr(config-ips-category-rule-advanced)# rule-text "alert tcp any any -> any 80 (msg:'Possible Slowloris Attack Detected';
flow:to_server,established; content:'X-a|3a|'; distance:0; pcre:'/\d\d\d\d/'; distance:0;
content:'|0d 0a|'; sid:10000001;)"
```

Создадим ещё одно расширенное правило, работающее по схожему алгоритму, чтобы определить какое из правил будет эффективнее:

```

esr(config-ips-category)# rule-advanced 2
esr(config-ips-category-rule-advanced)# description «Slow Loris rule 2»
esr(config-ips-category-rule-advanced)# rule-text «alert tcp $EXTERNAL_NET any -> $HOME_NET
$HTTP_PORTS (msg:'SlowLoris.py DoS attempt'; flow:established,to_server,no_stream; content:'X-
a: '; dsize:<15; detection_filter:track by_dst, count 3, seconds 30; classtype:denial-of-
service; sid: 10000002; rev:1; )

```

1.52 Настройка VoIP

VoIP (англ. Voice over IP) – набор протоколов, которые позволяют передавать речевую информацию посредством IP-сетей. В рамках данного устройства VoIP используется для подключения аналоговых телефонных аппаратов к IP-сети с возможностью совершения телефонных вызовов.

1.52.1 Процесс настройки SIP-профиля

| Шаг | Описание | Команда | Ключи |
|-----|---|--|---|
| 1 | Настройка SIP-профиля | esr(config)# sip profile <NUM> | <NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5. |
| 2 | Настройка основного SIP проху-сервера и сервера регистрации | esr(config-sip-profile)# proxy primary | |
| 3 | Настройка адреса SIP проху-сервера | esr(config-voip-sip-proxy)# ip address proxy-server <IP> | <IP> – IP-адрес проху-сервера |
| 4 | Настройка порта SIP проху-сервера | esr(config-voip-sip-proxy)# ip port proxy-server <PORT> | <PORT> – номер UDP-порта проху-сервера, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 5 | Настройка адреса сервера регистрации | esr(config-voip-sip-proxy)# ip address registration-server <IP> | <IP> – IP-адрес сервера регистрации. |
| 6 | Настройка порта сервера регистрации: | esr(config-voip-sip-proxy)# ip portregistration-server <PORT> | <PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 7 | Активация регистрации | esr(config-voip-sip-proxy)# registration | |
| 8 | Активация проху-сервера и сервера регистрации: | esr(config-voip-sip-proxy)# enable | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 9 | Настройка адреса сервера регистрации | esr(config-voip-sip-proxy)# ip address registration-server <IP> | <IP> – IP-адрес сервера регистрации. |
| 10 | Настройка порта сервера регистрации: | esr(config-voip-sip-proxy)# ip portregistration-server <PORT> | <PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 11 | Указание SIP-домена, в котором находится устройство | esr(config-sip-profile)# sip-domain address <ADDRESS> | <ADDRESS> – SIP-домен, в котором находится устройство, задается ipv4-адресом или доменным именем. |
| 12 | Активация использования SIP domain при регистрации | esr(config-sip-profile)# sip-domain registration enable | |
| 13 | Настройка SIP-профиля | esr(config)# sip profile <NUM> | <NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5. |
| 14 | Назначение плана нумерации текущему SIP-профилю | esr(config-sip-profile)# dialplan pattern <DNAME> | <DNAME> – имя план нумерации, задается строкой до 31 символа. |
| 15 | Активация SIP-профиля | esr(config-sip-profile)# enable | |

1.52.2 Процесс настройки FXS/FXO-портов

| Шаг | Описание | Команда | Ключи |
|-----|--|--|---|
| 1 | Переход в режим конфигурирования FXO/FXS-портов | esr(config)# interface voice-port <NUM> | <NUM> – номер порта, принимает значение от 1 до 4. |
| 2 | Назначение абонентского номера, закрепленного за телефонным портом | esr(config-voice-port-fxs)# sip user phone <PHONE> | <PHONE> – абонентский номер, закрепленный за телефонным портом, задается до 50 символов. |
| 3 | Назначение имя пользователя, сопоставленное с портом | esr-12v(config-voice-port-fxs)# sip user display-name <LOGIN> | <LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается строкой до 31 символа. |
| 4 | Выбор SIP-профиля для конкретного порта. | esr(config-voice-port-fxs)# profile sip <PROFILE> | <PROFILE> – номер SIP-профиля, задается от 1 до 5. |

| Шаг | Описание | Команда | Ключи |
|-----|---|---|---|
| 5 | Настройка логина для аутентификации | esr(config-voice-port-fxs)# authentication name <LOGIN> | <LOGIN> – логин для аутентификации, задается строкой до 31 символа |
| 6 | Настройка пароля для аутентификации | esr(config-voice-port-fxs)# authentication password <PASS> | <PASS> – пароль для аутентификации, задается строкой до 16 символов. |
| 7 | Активация FXO-порта | esr(config)# interface voice-port <NUM> | <NUM> – номер FXO-порта принимает значение от 1 до 4. |
| 8 | Назначение абонентского номера, закрепленного за телефонным портом | esr(config-voice-port-fxo)# sip user phone <PHONE> | <PHONE> – абонентский номер, закрепленный за телефонным портом. |
| 9 | Указание UDP-порта, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения | esr(config-voice-port-fxo)# sip port <PORT> | <PORT> – номер UDP-порта. |
| 10 | Назначение имени пользователя, сопоставленное с портом | esr(config-voice-port-fxo)# sip user display-name <LOGIN> | <LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается строкой до 31 символа. |
| 11 | Настройка логина для аутентификации | esr(config-voice-port-fxo)# authentication name <LOGIN> | <LOGIN> – логин для аутентификации, задается строкой до 31 символа. |
| 12 | Настройка пароля для аутентификации | esr(config-voice-port-fxo)# authentication password <PASS> | <PASS> – пароль для аутентификации, задается строкой до 16 символов. |
| 13 | Разрешение передачи номера в ТфОП | esr(config-voice-port-fxo)# pstn transmit-number | |
| 14 | Запретить передачу префикса | esr(config-voice-port-fxo)# no pstn transmit-prefix | |
| 15 | Активация услуги «Hostline PSTN to IP» | esr(config-voice-port-fxo)# hotline ipt | |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 16 | Номер абонента, который будет получать вызовы с ТфОП | esr(config-voice-port-fxo)# hotline number ipt <PHONE> | <PHONE> – номер телефона, на который осуществляется вызов при использовании услуги, принимает значение от 1 до 50. «Горячая/Теплая линия» в направлении из аналоговой телефонной линии в VoIP. |

1.52.3 Процесс настройки плана нумерации

| Шаг | Описание | Команда | Ключи |
|-----|-----------------------------|---|--|
| 1 | Создание плана нумерации | esr(config)# dialplan pattern <DNAME> | <DNAME> – имя плана нумерации, задается строкой до 31 символа. |
| 2 | Добавление правил нумерации | esr(config-dial-ruleset)# pattern <REGEXP> | <REGEXP> – регулярное выражение, задающее план нумерации. Задаётся строкой до 1024 символов. Правила составления регулярных выражений описаны в разделе Пример настройки плана нумерации . |
| 3 | Активация плана нумерации | esr(config-dial-ruleset)# enable | |

1.52.4 Процесс настройки PBX-сервера

| Шаг | Описание | Команда | Ключи |
|-----|--------------------------------|---|--|
| 1 | Настройка PBX-сервера | esr(config)# pbx | |
| 2 | Включение PBX-сервера | esr(config-pbx)# enable | |
| 3 | Создание плана маршрутизации | esr(config-pbx)# ruleset <rule_name> | <rule_name> – имя плана маршрутизации, задается строкой до 31 символа. |
| 4 | Создание правила маршрутизации | esr(config-pbx-ruleset)# rule <rule_index> | <rule_index> – номер правила в плане маршрутизации, принимает значение от 1 до 1000. |

| Шаг | Описание | Команда | Ключи |
|-----|--|---|---|
| 5 | Создание паттерна в правиле маршрутизации | esr(config-pbx-rule)# pattern <REGEXP> | <REGEXP> – регулярное выражение, задающее правило маршрутизации. Задаётся строкой до 256 символов. Правила составления регулярных выражений описаны в разделе Пример настройки плана нумерации . |
| 6 | Применение правила маршрутизации | esr(config-pbx-rule)# enable | |
| 7 | Создание SIP - профиля на PBX – сервере | esr(config-pbx)# profile <PROFILE> | <PROFILE> – имя SIP профиля, используемого PBX – сервером, задается строкой до 31 символа. |
| 8 | Выбор кодека, поддерживаемого SIP - профилем | esr(config-pbx-profile)# codec allow { G711A(alaw) G711U(ulaw) G722 G726 } | |
| 9 | Выбор типа SIP - профиля | esr(config-pbx-profile)# client { peer user friend } | <ul style="list-style-type: none"> • peer – входящие и исходящие звонки разрешены без авторизации. • user – разрешены только входящие звонки. • friend – комбинирует типы профилей peer и user. |
| 10 | Выбор политики взаимодействия с NAT (не обязательно) | esr(config-pbx-profile)# nat { comedia force-port both } | <ul style="list-style-type: none"> • comedia – отправить медиа поток на порт PBX, независимо от указаний SDP. • force-port – использовать rport, даже если его нет. • both – объединяет comedia и force-port. |
| 11 | Выбор плана маршрутизации, связанного с SIP - профилем | esr(config-pbx-profile)# ruleset <NAME> | <NAME> – Имя плана маршрутизации, задается строкой до 31 символа. |
| 12 | Создание абонента | esr(config-pbx)# user <user> | <user> – номер телефона или имя пользователя, задается строкой до 31 символа. |
| 13 | Создание пароля для абонента (не обязательно) | esr(config-pbx-user)# password <password> | <password> – пароль, который будет использоваться пользователем для аутентификации, задается строкой до 16 символов. |

| Шаг | Описание | Команда | Ключи |
|-----|---------------------------------------|---|--|
| 14 | Применение SIP - профиля для абонента | esr(config-pbx-user)# profile <SIPPROFILE> | <SIPPROFILE> – SIP - профиль, используемый для данного абонента, задается строкой до 31 символа. |

1.52.5 Процесс создания транка регистрации

| Шаг | Описание | Команда | Ключи |
|-----|---|---|--|
| 1 | Настройка PBX-сервера | esr(config)# pbx | |
| 2 | Создание транка | esr(config-pbx)# register-server <name> | <name> – имя транка, задается строкой до 31 символа. |
| 3 | Настройка адреса сервера регистрации | esr(config-pbx-reg-server)# ip address <IP> | <IP> – адрес сервера, на котором происходит регистрация, может принимать значение IP адреса или задаваться строкой до 31 символа. |
| 4 | Настройка порта сервера регистрации | esr(config-pbx-reg-server)# ip port <PORT> | <PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 5 | Задание аутентификационного имени | esr(config-pbx-reg-server)# username <user> | <user> – имя пользователя для этого транка на вышестоящем домене, задается строкой до 31 символа. |
| 6 | Задание аутентификационного пароля | esr(config-pbx-reg-server)# authentication password <password> | <password> – пароль для этого транка на вышестоящем домене, задается строкой до 16 символов. |
| 7 | Применение SIP - профиля для транка | esr(config-pbx-reg-server)# profile <PROFILE> | <PROFILE> – имя SIP профиля, используемое для данного транка, задается строкой до 31 символа. |
| 8 | Выбор транспортного протокола (не обязательно) | esr(config-pbx-reg-server)# protocol {tcp udp } | По умолчанию используется udp. |
| 9 | Активация транка | esr(config-pbx-reg-server)# enable | |

1.52.6 Пример настройки VoIP

Задача:

Подключить аналоговые телефонные аппараты и факс-модемы к IP-сети посредством маршрутизатора ESR. В качестве проху-сервера и сервера регистрации выступает SIP-сервер, находящийся на ESR.

Решение:



Рисунок 56 – Схема сети

Настройка SIP-профиля:

```
esr(config)# sip profile 1
```

Настройка основного SIP проху-сервера и сервера регистрации:

```
esr(config-sip-profile)# proxy primary
```

Настройка адреса SIP проху-сервера (в качестве SIP проху-сервера использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address proxy-server 192.0.2.5
```

Настройка порта SIP проху-сервера:

```
esr(config-voip-sip-proxy)# ip port proxy-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Если необходимо использовать регистрацию, то необходимо выполнить следующие пункты:

Настройка адреса сервера регистрации (в качестве сервера регистрации использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address registration-server 192.0.2.5
```

Настройка порта сервера регистрации:

```
esr(config-voip-sip-proxy)# ip port registration-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Активация регистрации:

```
esr(config-voip-sip-proxy)# registration
```

Активация проху-сервера и сервера регистрации:

```
esr(config-voip-sip-proxy)# enable
```

На этом конфигурация SIP проху-сервера и сервера регистрации закончена:

```
esr(config-voip-sip-proxy)# exit
```

Далее продолжается настройка SIP-профиля.

⚠ Если в качестве SIP проху и сервера регистрации используется встроенный SIP-сервер, необходимо произвести его настройку согласно документу «Настройка SIP-сервера на маршрутизаторах серии ESR: ESR-12V, ESR-12VF, ESR-14VF».

Настройка SIP-домена:

```
esr(config-sip-profile)# sip-domain address sipdomain.com
```

Если необходимо использовать SIP Domain для регистрации:

```
esr(config-sip-profile)# sip-domain registration enable
```

В такой конфигурации все вызовы будут направлены SIP проху-серверу. Если необходимо указать другое направление для исходящих вызовов, то необходимо проделать следующее:

Создать план нумерации, см. раздел [Пример настройки плана нумерации](#).

Далее созданный план маршрутизации, необходимо присвоить SIP-профилю:

```
esr(config)# sip profile 1
esr(config-sip-profile)# dialplan pattern firstDialplan
```

На этом настройка плана нумерации для SIP-профиля закончена.

Активация SIP-профиля:

```
esr-12v(config-sip-profile)# enable
```

На этом минимально необходимая настройка SIP-профиля закончена:

```
esr(config-sip-profile)# exit
```

Следующим этапом является настройка абонентских портов:

```
esr(config)# interface voice-port 1
```

Указать абонентский номер:

```
esr(config-voice-port-fxs)# sip user phone 4101
```

Указать отображаемое имя:

```
esr(config-voice-port-fxs)# sip user display-name user-one
```

Используемый SIP-профиль:

```
esr(config-voice-port-fxs)# profile sip 1
```

Настройка логина и пароля для аутентификации:

```
esr(config-voice-port-fxs)# authentication name login-4101
esr(config-voice-port-fxs)# authentication password superpassword
```

На этом минимальная настройка абонентского порта закончена:

```
esr(config-voice-port-fxs)# exit
```

1.52.7 Пример настройки плана нумерации

Задача:

Настроить план нумерации так, чтобы вызовы на локальных (подключенных к данному ESR-12V) коммутировались локально, а вызовы на все остальные направления через SIP-proxy.

Решение:

Создать план нумерации:

```
esr(config)# dialplan pattern firstDialplan
```

План нумерации задается при помощи регулярных выражений:

```
esr(config-dial-ruleset)# pattern "<regular expressions>"
```

Для задачи, обозначенной выше "<regular expressions>" будет иметь вид:

"S5, L5 (410[1-3]@{local} | [xABCD*#].S)"

где:

410[1-3]@{ local} – вызовы на номера 4101, 4102, 4103 будут коммутироваться локально;

[xABCD*#]. S – вызовы на все остальные номера будут направлены к SIP-прокси.

Активировать план нумерации:

```
esr(config-dial-ruleset)# enable
```

Настройка плана нумерации закончена.

```
esr(config-dial-ruleset)# exit
```

Структура регулярного выражения:

Sxx, Lxx (),

где:

xx – произвольные значения таймеров S и L;

() – границы плана нумерации.

Основой являются обозначения для записи последовательности набранных цифр. Последовательность цифр записывается с помощью нескольких обозначений: цифры, набираемые с клавиатуры телефона: 0, 1, 2, 3, ..., 9, # и *.

❗ Использование символа # в плане нумерации может блокировать завершение набора с помощью этой клавиши!

Последовательность цифр, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символу.

- Пример: ([1239]) – соответствует любой из цифр 1, 2, 3 или 9.
Через тире может быть указан диапазон символов. Чаще всего используется внутри квадратных скобок.
- Пример 1: (1-5) – любая цифра от 1 до 5.
- Пример 2: ([1-39]) – пример из предыдущего пункта с иной формой записи.
Символ X соответствует любой цифре от 0 до 9.
- Пример: (1XX) – любой трёхзначный номер, начинающийся на 1.
«.» – повторение предыдущего символа от 0 до бесконечности раз.
«+» – повторение предыдущего символа от 1 до бесконечности раз.
{a,b} – повторение предыдущего символа от a до b раз;
{a,} – повторение предыдущего символа не меньше a раз;
{,b} – повторение предыдущего символа не больше b раз.
- Пример: (810X.) – международный номер с любым количеством цифр.
Настройки, влияющие на обработку плана нумерации:
- Interdigit Long Timer (буква «L» в записи плана нумерации) – время ожидания ввода следующей цифры в том случае, если нет шаблонов, подходящих под набранную комбинацию;
- Interdigit Short Timer (буква «S» в записи плана нумерации) – время ожидания ввода следующей цифры, если с набранной комбинацией полностью совпадает хотя бы один шаблон и при этом имеется еще хотя бы один шаблон, до полного совпадения с которым необходимо осуществить донабор номера.

Дополнительные возможности:

1. Замена набранной последовательности

Синтаксис: `<arg1:arg2>`

Данная возможность позволяет заменить набранную последовательность на любую последовательность набираемых символов. При этом второй аргумент должен быть указан определённым значением, оба аргумента могут быть пустыми.

- Пример: (<83812:> XXXXXX) – данная запись будет соответствовать набранным цифрам 83812, но эта последовательность будет опущена и не будет передана на SIP-сервер.

2. Вставка тона в набор

При выходе на межгород (в офисных станциях – на город) привычно слышать ответ станции, что можно реализовать вставкой запятой в нужную позицию последовательности цифр.

- Пример: (8, 770) – при наборе номера 8770 после цифры 8 будет выдан непрерывный тон.

3. Запрет набора номера

Если в конце шаблона номера добавить восклицательный знак '!', то набор номеров, соответствующих шаблону, будет заблокирован.

- Пример: (8 10X xxxxxxx ! | 8 xxx xxxxxxx) – выражение разрешает набор только междугородних номеров и исключает международные вызовы.

4. Замена значений таймеров набора номера

Значения таймеров могут быть назначены как для всего плана нумерации, так и для определённого шаблона. Буква «S» отвечает за установку «*Interdigit Short Timer*», а «L» – за «*Interdigit Long Timer*». Значения таймеров может быть указано для всех шаблонов в плане нумерации, если значения перечислены до открывающейся круглой скобки.

- Пример: S4 (8XXX.) или S4,L8 (XXX)

Если эти значения указаны только в одной из последовательностей, то действуют только для неё. Также в этом случае не надо ставить двоеточие между ключом и значением таймаута, значение может быть расположено в любом месте шаблона.

- Пример: (S4 8XXX. | XXX) или ([1-5] XX S0) – запись вызовет мгновенную передачу вызова при наборе трехзначного номера, начинающегося на 1,2, ..., 5.

5. Набор по прямому адресу (IP Dialing)

Символ «@», поставленный после номера, означает, что далее будет указан адрес сервера, на который будет отправлен вызов на набранный номер. Рекомендуется использовать «*IP Dialing*», а также приём и передачу вызовов без регистрации («*Call Without Reg*», «*Answer Without Reg*»). Это может помочь в случае отказа сервера.

Кроме того, формат адреса с IP Dialing может быть использован в номерах, предназначенных для переадресации звонков.

- Пример 1: (8 xxx xxxxxxx) – 11-значный номер, начинающийся на 8.
- Пример 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) – 11-значный номер, начинающийся на 8, если введён семизначный, то добавить к передаваемому номеру 8495.
- Пример 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) – набор номеров экстренных служб, а так же некоторого странного набора междугородних номеров.
- Пример 4: (S0 <:82125551234>) – быстрый набор указанного номера, аналог режима «Hotline» на других шлюзах.
- Пример 5: (S5 <:1000> | xxxx) – данный план нумерации позволяет набрать любой номер, состоящий из цифр, а если ничего не введено в течение 5 секунд, вызвать номер 1000 (допустим, это секретарь).
- Пример 6: (8, 10x.|1xx@10.110.60.51:5060) – данный план нумерации позволяет набирать номера начинающиеся на 810 и содержащие как минимум одну цифру после "810". После ввода 8 будет выдан сигнал "ответ станции". А также набор трехзначных номеров, начинающихся на "1", Invite на которые будет отправлен на IP-адрес 10.110.60.51 и порт 5060.
- Пример 7: (S3 *xx#|#xx#|#xx#|#xx*x+#) – управление и использование ДВО. Иногда может потребоваться совершать звонки локально внутри устройства. При этом, если IP-адрес устройства не известен или периодически изменяется, удобно использовать в качестве адреса сервера зарезервированное слово «{local}», что означает отправку соответствующей последовательности цифр на собственный адрес устройства.
- Пример: (123@{local}) – вызов на номер 123 будет обработан локально внутри устройства.

1.52.8 Настройка FXO-порта

Задача:

Добавить возможность совершения вызова абонента ТфОП через FXO-порт ESR-12V.

Решение :

Активировать FXO-порт:

```
esr(config)# interface voice-port 4
```

Указать номер FXO-порта, он же префикс выхода на ТфОП:

```
esr(config-voice-port-fxo)# sip user phone 9
```

Указать UDP-порт, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения:

```
esr(config-voice-port-fxo)# sip port 5064
```

Указать отображаемое имя:

```
esr(config-voice-port-fxo)# sip user display-name user-one
```

Настройка логина и пароля для аутентификации:

```
esr(config-voice-port-fxo)# authentication name login-9
esr(config-voice-port-fxo)# authentication password superpassword
```

Назначить SIP-профиль FXO-порту:

```
esr(config-voice-port-fxo)# profile sip 1
```

Разрешить передачу номера в ТфОП:

```
esr(config-voice-port-fxo)# pstn transmit-number
```

Запретить передачу префикса:

```
esr(config-voice-port-fxo)# no pstn transmit-prefix
```

Для работы исходящих вызовов необходимо в настройках плана нумерации указать следующее правило, которое означает, что исходящие вызовы на номера имеющие префикс 9, маршрутизируются локально на FXO-комплект:

9x.#{@local}:5064

На этом минимальная настройка исходящих вызовов на ТфОП закончена. Для того чтобы совершить вызов в ТфОП, нужно набрать номер вызываемого абонента с указанным префиксом (телефонный номер FXO-комплекта).

Для того чтобы принимать вызовы с ТфОП необходимо выбрать абонента, на которого будут поступать все вызовы их ТфОП, допустим, это будет абонент с номером 305.

Активировать услугу «Hostline PSTN to IP»:

```
esr(config-voice-port-fxo)# hotline ipt
```

Указать номер абонента, который будет получать вызовы с ТфОП:

```
esr(config-voice-port-fxo)# hotline number ipt 305
```

1.53 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

1.53.1 Процесс настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|------------------------|---|
| 1 | Запустить проверку целостности системы | esr# verify filesystem | detailed – детальный вывод информации в консоль. |

1.53.2 Пример конфигурации

Задача:

Проверить целостность файловой системы:

Решение:

Основной этап конфигурирования:

Запускаем проверку целостности:

```
esr# verify filesystem
Filesystem Successfully Verified
```

1.54 Настройка архивации конфигурации маршрутизатора

На маршрутизаторах ESR предусмотрена функция локального и/или удаленного копирования конфигурации по таймеру или при применении конфигурации.

1.54.1 Процесс настройки

| Шаг | Описание | Команда | Ключи |
|-----|--|-----------------------------|-------|
| 1 | Перейти в режим настройки параметров резервирования конфигурации | esr(config)# archive | |

| Шаг | Описание | Команда | Ключи |
|-----|---|--|--|
| 2 | Установить тип сохранения резервных конфигураций маршрутизатора (не обязательно) | esr(config-ahchive)# type <TYPE> | <TYPE> – тип сохранения резервных конфигураций маршрутизатора. Принимает значения: <ul style="list-style-type: none"> • local; • remote; • both. Значение по умолчанию: remote |
| 3 | Включить режим резервирования конфигурации по таймеру (не обязательно) | esr(config-ahchive)# auto | |
| 4 | Включить режим резервирования конфигурации после каждого успешного применения конфигурации (не обязательно) | esr(config-ahchive)# by-commit | |
| 5 | Указать путь для удаленного копирования конфигураций маршрутизатора (обязательно для типов remote и both) | esr(config-ahchive)# path <PATH> | <PATH> - определяет протокол, адрес сервера, расположение и префикс имени файла на сервере |
| 6 | Задать период времени для автоматического резервирования конфигурации (не обязательно, актуально только для режима auto) | esr(config-ahchive)# time-period <TIME> | <TIME> – периодичность автоматического резервирования конфигурации, принимает значение в минутах [1..35791394]. Значение по умолчанию: 720 минут |
| 7 | Задать максимальное количество локально сохраняемых резервных копий конфигураций (не обязательно, актуально при типах local и both) | esr(config-ahchive)# count-backup <NUM> | <NUM> – максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100]. Значение по умолчанию: 1 |

1.54.2 Пример конфигурации

Задача:

Настроить локальное и удаленное резервное копирование конфигурации маршрутизатора 1 раз в сутки и при успешном изменении конфигурации. Удаленные копии необходимо отправлять на tftp-сервер 172.16.252.77 в подпапку esr-examp1e. Максимальное количество локальных копий – 30.

Решение:

Для успешной работы удаленной архивации конфигураций, между маршрутизатором и сервером должна быть организована IP-связность, настроены разрешения на прохождение tftp-трафика по сети и сохранения файлов на сервере.

Основной этап конфигурирования:

Перейти в режим конфигурирования резервного копирования конфигураций:

```
esr# configure
esr(config)# archive
```

Задать режим локального и удаленного резервного копирования конфигурации:

```
esr(config)# type both
```

Настроить путь для удаленного копирования конфигураций и максимальное количество локальных резервных копий:

```
esr(config-archive)# path tftp://172.16.252.77:/esr-example/esr-example.cfg
esr(config-archive)# count-backup 30
```

Задать интервал резервного копирования конфигурации в случае отсутствия изменений:

```
esr(config-archive)# time-period 1440
```

Включить режимы архивации конфигурации маршрутизатора по таймеру и при успешном изменении конфигурации:

```
esr(config-archive)# auto
esr(config-archive)# by-commit
```

После применения данной конфигурации 1 раз в сутки и при каждом успешном изменении конфигурации маршрутизатора на tftp-сервер будет отправляться конфигурационный файл с именем вида "esr-exampleYYYYMMDD_HHMMSS.cfg". Также, на самом маршрутизаторе в разделе flash:backup/ будет создаваться файл с именем вида "config_YYYYMMDD_HHMMSS". Когда в разделе flash:backup/ накопится 30 таких файлов, при создании нового будет удаляться наиболее старый.

2 Часто задаваемые вопросы

- **Не удалось получить маршруты по BGP и/или OSPF , сконфигурированных в VRF . Соседство успешно устанавливается, но в записи маршрутов в RIB отказано %ROUTING-W-KERNEL: Can not install route. Reached the maximum number of BGP routes in the RIB**
Необходимо выделить ресурс RIB для VRF, по умолчанию он равен нулю. Делаем это в режиме конфигурирования VRF:

```
esr(config)# ip vrf <NAME>
esr(config-vrf)# ip protocols ospf max-routes 12000
esr(config-vrf)# ip protocols bgp max-routes 1200000
esr(config-vrf)# end
```

- **Закрываются сессии SSH/Telnet проходящие через маршрутизатор ESR.**
Для поддержания сессии активной необходимо настроить передачу keepalive пакетов. Опция отправки keepalive настраивается в клиенте SSH, например, для клиента PuTTY раздел "Соединение".
В свою очередь, на маршрутизаторе можно выставить время ожидания до закрытия неактивных сессий TCP (в примере выставлен 1 час):

```
esr(config)# ip firewall sessions tcp-established-timeout 3600
```

- **На интерфейсе был отключен firewall (ip firewall disable), после внесения этого интерфейса в security zone , удаления из конфигурации ip firewall disable и применения изменений – доступ для активных сессий с данного порта не закрылся, согласно правилам security zone - pair .**
Изменения в конфигурации Firewall будут действовать только для новых сессий, сброса активных сессий в Firewall не происходит. Отчистить активные сессии в firewall можно командой:

```
esr# clear ip firewall session
```

- **Не поднимается LACP на портах XG ESR-1000/1200/1500/1510/1700**
По умолчанию на port-channel режим speed 1000M, необходимо выставить speed 10G.

```
esr(config)# interface port-channel 1
esr(config-port-channel)# speed 10G
```

- **Как полностью очистить конфигурация ESR, и как сбросить на заводскую конфигурацию?**
Очистка конфигурации происходит путем копирования пустой конфигурации в candidate-config и применения его в running-config.

```
esr# copy system:default-config system:candidate-config
```

Процесс сброса на заводскую конфигурацию аналогичен.

```
esr# copy system:factory-config system:candidate-config
```

- **Как привязать subinterface к созданным VLAN ?**
При создании саб-интерфейса, VLAN создается и привязывается автоматически (прямая зависимость индекс sub – VID).

```
esr(config)# interface gigabitethernet 1/0/1.100
```

После применения можно наблюдать информационные сообщения:

```
2016-07-14T012:46:24+00:00 %VLAN: creating VLAN 100
```

- **Есть ли функционал в маршрутизаторах серии ESR для анализа трафика?**

В маршрутизаторах серии ESR реализована возможность анализировать трафик на интерфейсах из CLI. Сниффер запускается командой monitor.

```
esr# monitor gigabitethernet 1/0/1
```

- **Как настроить ip prefix-list 0.0.0.0/0?**

Ниже приведен пример конфигурации префикс листа, разрешающего прием маршрута по умолчанию.

```
esr(config)# ip prefix-list eltex
esr(config-pl)# permit default-route
```

- **Проблема прохождения асинхронного трафика .**

В случае организации сети с асинхронной маршрутизацией, Firewall будет запрещать "неправильный (ошибочный)" входящий трафик (не открывающий новое соединение и не принадлежащий никакому установленному соединению) из соображений безопасности. Разрешающее правило в Firewall не решит поставленную задачу для подобных схем. Решить задачу можно, отключив Firewall на входном интерфейсе:

```
esr(config-if-gi)# ip firewall disable
```

- **Как можно сохранить локальную копию конфигурации маршрутизатора?**

Если необходимо скопировать текущую running или candidate -конфигурацию на самом маршрутизаторе – можно воспользоваться командой copy с указанием в качестве источника копирования "system:running-config" или " system:candidate-config", а в качестве назначения – файл в разделе "flash:data/"

```
esr# copy system:candidate-config flash:data/temp.txt
```

Также, существует возможность копирования ранее сохраненных конфигурационных файлов (автоматически из раздела flash:backup/ или вручную из раздела flash:data/) в candidate-конфигурацию:

```
esr# copy flash:data/temp.txt system:candidate-config
esr# copy flash:backup/config_20190918_164455 system:candidate-config
```

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ТОО «ЭлтексАлатау» Вы можете обратиться в Сервисный центр компании:

050032, Республика Казахстан, г. Алматы, мкр-н. Алатау, ул. Ибрагимова 9

Телефон:

+7(727) 220-76-10, +7 (727) 220-76-07

E-mail: post@eltexalatau.kz

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ТОО «ЭлтексАлатау», обратиться к базе знаний, проконсультироваться у инженеров Сервисного центра на техническом форуме.

Официальный сайт компании: <http://eltexalatau.kz>