- **Работа с трафиком в режимах IDS и IPS**
- **Работа с транзитным и зеркалированным трафиком**
- **Выгрузка результатов анализа трафика в SIEM по протоколу Syslog**
- **Гибкое управление подключаемыми категориями IDS/IPS-правил**
- **Регулярные обновления IDS/IPS-правил от коммерческих поставщиков**
- **Возможность загрузки IDS/IPS-правил из пользовательских источников**
- **Создание пользовательских IDS/IPS-правил через встроенный в ESR конструктор**

Intrusion Detection System (IDS, система обнаружения вторжений) — программная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности. Её логическим развитием является **Intrusion Prevention System (IPS, система предотвращения вторжений)** — программная система сетевой и компьютерной безопасности, принимающая меры к выявленным нарушениям безопасности защищаемого сегмента сети.

Устройства серии ESR — это сервисные маршрутизаторы, способные выполнять широкий круг задач, связанных с сетевой защитой. Ключевыми элементами являются средства аппаратного ускорения обработки данных, позволяющие достичь высокого уровня производительности. Линейка устройств серии ESR включает в себя широкий ассортимент моделей с разной производительностью, что позволяет использовать их как в автономных решениях для малого и среднего бизнеса, так и в крупных распределённых сетях.

Решение IDS/IPS в ESR позволяет установить на границе сети маршрутизатор, способный определять и предотвращать атаки на защищаемые сети. Также он может быть установлен внутри сети в качестве межсетевого экрана, что позволяет уменьшить накладные расходы на маршрутизацию. Объединение функциональностей граничного маршрутизатора и межсетевого экрана в ESR позволяет предотвращать атаки на самом раннем этапе и защищать все элементы сети.

Технологии Kaspersky SafeStream II

Powered by kaspersky

Kaspersky SafeStream II — это технология потокового сканирования на уровне сетевого шлюза, предназначенная для обнаружения наиболее опасных и широко распространённых угроз в режиме реального времени. Данная технология обеспечивает достаточно эффективную нейтрализацию угроз в сочетании с максимальной производительностью решения.

Благодаря использованию инфраструктуры безопасности «Лаборатории Касперского», в том числе облачного «коллективного разума» Kaspersky Security Network, ESR с поддержкой Kaspersky SafeStream II способен обнаруживать вредоносное ПО во всех типах трафика (web, email, P2P, сервисы мгновенного обмена сообщениями и т.п.). В результате обеспечивается защита пользователей от самых опасных киберугроз, в том числе угроз нулевого дня, программ-шифровальщиков, заражённых сайтов и других типов угроз.

Наборы правил

Для системы IDS/IPS сервисных маршрутизаторов ESR предложены следующие категории правил:

- **Данные о репутации IP-адресов** — набор IP-адресов с контекстной информацией, сообщающей о подозрительных и вредоносных узлах;
- **URL-адреса вредоносных ссылок** — набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам;
- **URL-адреса фишинговых ссылок** — набор URL-адресов, распознаваемых «Лабораторией Касперского» как фишинговые. Доступны записи с масками и без масок;
- **URL-адреса командных серверов ботнетов** — набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов;

Наборы правил (продолжение)

- **URL-адреса шифровальщиков** — набор URL-адресов шифровальщиков;
- **Хэши вредоносных объектов** — набор файловых хэшей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы;
- **Хэши вредоносных объектов для мобильных устройств** — набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства;
- **Данные о троянцах P-SMS** — набор хэшей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать SMS-сообщения, отвечать на них и удалять их;
- **URL-адреса командных серверов ботнетов для мобильных устройств** — набор URL-адресов с контекстной информацией для выявления командных серверов ботнетов, использующих мобильные устройства;
- **URL-адреса веб-сайтов, используемых для размещения вредоносных программ, заражающих устройства Internet of Things (IoT).**

IDS/IPS правила от PT Search Security Center

positive technologies

Команда специалистов экспертного центра кибербезопасности Positive Technologies Expert Security Center (PT ESC) создала набор уникальных правил для выявления киберугроз, написанных с помощью синтаксиса языка Suricata. Набор включает более 6000 правил. Эксперты PT ESC регулярно обновляют и дополняют его по итогам расследований реальных атак и в ходе изучения деятельности и инструментов хакерских группировок.

Использование сервисных маршрутизаторов ESR с правилами PT ESC дает компаниям возможность выявлять источники подозрительного трафика, вредоносную активность и аномалии в сети, а также обнаруживать эксплуатацию уязвимостей и предотвращать атаки хакеров.

Наборы правил

Для системы IDS/IPS сервисных маршрутизаторов ESR предложены следующие категории правил:

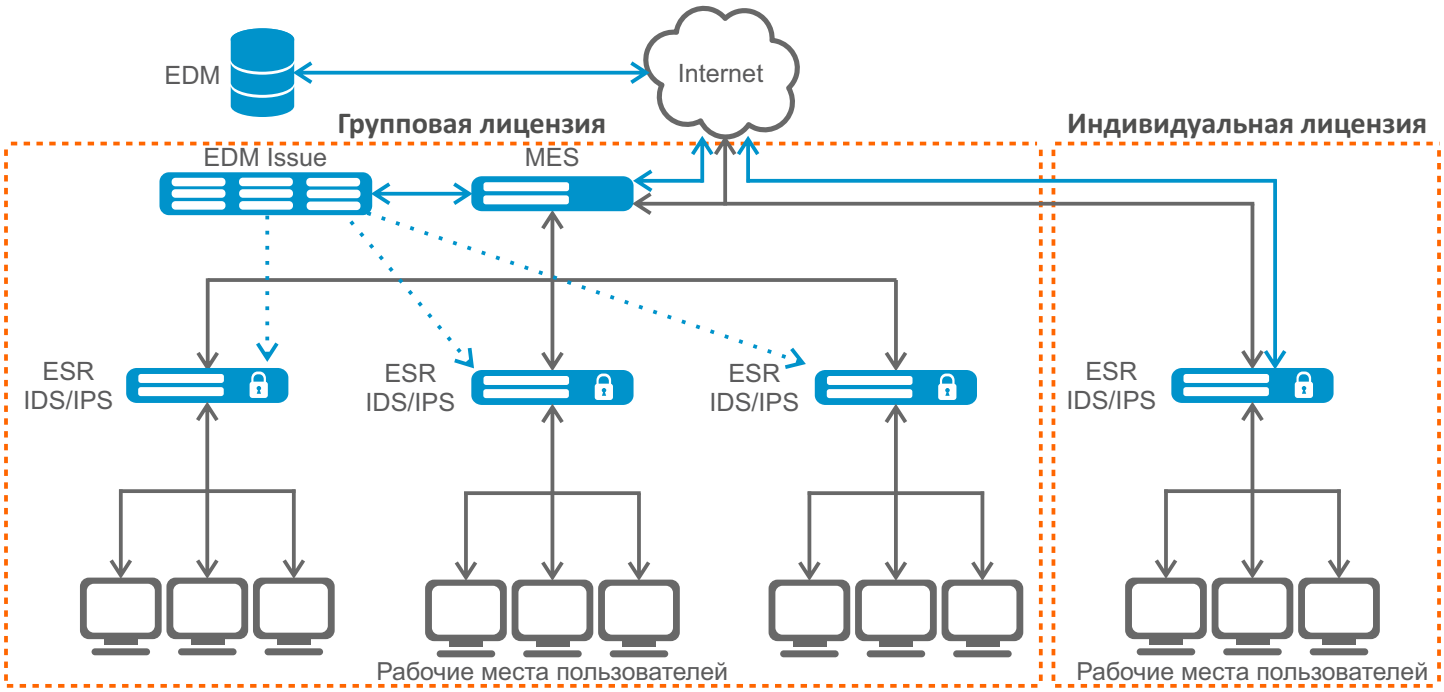
- **Атаки на инфраструктуру** — набор сигнатур для обнаружения атак на внутреннюю инфраструктуру компании, например, разведку внутри домена, подбор учетных записей и паролей, удаленное выполнение команд на узле и горизонтальное перемещение по сети;
- **Вредоносное программное обеспечение** — набор сигнатур для детектирования действия вредоносных программ в сети компании;
- **Доступ изнутри** — набор сигнатур для обнаружения использования скрытых каналов передачи данных от взломанной инфраструктуры к серверу атакующего: различные reverse shell, в том числе использующие шифрование, DNS-туннели, а также различные самописные протоколы.
- **Инструменты выполнения атак** — набор сигнатур для обнаружения использования инструментов атакующих. Правила позволяют детектировать применение всех популярных хакерских инструментов, включая Cobalt Strike, Impacket, Koadic, CrackMapExec, Empire, Powerspoit, Metasploit, ldapper и BloodHound.

Лицензирование

Все перечисленные наборы правил предоставляются по лицензии с ограниченным сроком действия. Минимальный срок действия лицензии один год, в дальнейшем её можно продлить или расширить. Лицензия может быть двух типов — индивидуальная и групповая. Индивидуальная лицензия позволяет получать коммерческие IDS/IPS-правила для одного конкретного устройства ESR, а групповая — сразу для нескольких устройств ESR.

Для работы по групповой лицензии предоставляется ПО EDM Issue, позволяющее автоматически включать в работу новый ESR в рамках действующей лицензии. Таким образом, администратор может сам выбирать устройства ESR, которым будет доступна загрузка IDS/IPS-правил в рамках своей организации.

Пример работы различных вариантов лицензирования



+7 (727) 220-76-10
post@eltexalatau.kz
www.eltexalatau.kz

Компания "ЭлтексАлатау" - один из первых казахстанских производителей IT и телекоммуникационного оборудования. Одним из направлений компании является локализация производства в Республике Казахстан. Создавая новые возможности, мы разрабатываем совокупность решений, а также возможность их бесшовного соединения в инфраструктуру Заказчика.