В ответе на комментарий к 3 заданию.

**Межсетевой экран следующего поколения (NGFW)**

NGFW – это межсетевой экран, который фильтрует трафик как внешний, так и внутренний, в нем есть проверка состояния, есть поддержка фильтрации пакетов, поддержка IPsec и SSL VPN, мониторинг сети и сопоставления IP адресов. NGFW имеет возможность более глубокого проверки содержимого. Он умеет выявлять различные атаки зловредное ПО (Трояны и Черви), а так же блокировать все эти угрозы. Есть поддержка SSL, контроль вторжений и предотвращения вторжений. Для расширения NGFW необходимо применять облачные решения. Решения NGFW не только блокируют вредоносные программы, но и включают возможности для будущих обновлений, обеспечивая гибкость развития при расширении спектра угроз и защищая сеть при возникновении новых угроз.

### Примеры NGFW FortiGate: модели и характеристики межсетевых экранов следующего поколения

## Примеры использования NGFW от FortiGate

### УПРАВЛЕНИЕ РИСКАМИ ВНЕШНИХ СИСТЕМ БЕЗОПАСНОСТИ

С ростом объема HTTPS-трафика в организациях, не использующих стратегии дешифрования TLS, отсутствует проверка почти 90% зашифрованного HTTPS-трафика, а значит, такие организации подвергаются риску целевых атак вредоносных программ и потери данных. NGFW от FortiGate предоставляют сетевые решения обеспечения безопасности, отслеживающие данные приложений, угрозы и сети, защищая любое периферийное устройство с помощью проверенных и лучших в отрасли средств защиты для бесперебойной работы и достижения непрерывности бизнес-процессов

### УПРАВЛЕНИЕ РИСКАМИ ВНУТРЕННИХ СИСТЕМ БЕЗОПАСНОСТИ

Плоские сети хуже выдерживают атаки, потому что в них отсутствует расширенная проверка безопасности. Решения NGFW от FortiGate обеспечивают сегментацию сети, уменьшают поверхность атаки и препятствуют перемещению и распространению атаки внутри сети, гарантируя безопасность сегмента любого уровня (микро, макро, портов и приложений) с помощью автоматизированных рабочих процессов, адаптивной системы доверенных групп и высокопроизводительной защиты от угроз для глубоко интегрированной обороны, соблюдения требований соответствия и доверенного доступа к приложениям.

### УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Большинство вредоносных программ распространяются с использованием известных уязвимостей, и это является основным средством атак. Решения NGFW от FortiGate предлагают консолидированную систему сетевой безопасности с IPS без снижения производительности, обеспечивая виртуальное исправление и предотвращение известных атак и атак нулевого дня, а также снижение затрат и упрощение системы.

Где IPS – система Система предотвращения вторжений

Функциональные возможности и назначение WAF Особенности HTTP-трафика Вкратце, WAF служит для защиты конкретных экземпляров веб-приложений / сервисов, использующих в качестве транспорта семейство протоколов HTTP. В реализациях некоторых производителей также присутствует поддержка других протоколов, таких как SMTP и FTP, но данная возможность не является определяющей для WAF и в данной статье не рассматривается. Основным «полем битвы» для WAF является трафик протоколов семейства HTTP. Рассказ об области применения WAF будет неполным без понимания особенностей трафика, с которым приходится иметь дело, и того, каким угрозам необходимо противодействовать. За тридцатилетнюю историю своего существования HTTP превратился из протокола для передачи содержимого статичных HTML-документов и изображений в транспортный протокол, не только поддерживающий инкапсуляцию различных структур данных, но и способный быть «подложкой» для других протоколов.

Широкие возможности протокола HTTP породили не менее разнообразный набор атак на веб-приложения и сервисы. Наиболее значимые типы атак описываются в перечнях «OWASP Top Ten Web Application Security Risk» (для веб-приложений) и «OWASP API Security Top Ten» (для API-сервисов) от OWASP Foundation. Противодействие таким атакам прежде всего требует декомпозиции HTTP-запроса до отдельных примитивов (заголовки, URI, параметры и их значения, составляющие многокомпонентных запросов) и анализа содержимого структур данных, вложенность которых не имеет теоретических ограничений, а также последующего анализа их элементов, что требует ресурсоёмких вычислений. Наглядным примером является передача данных в форматах JSON или XML. Особо стоит выделить: атаки на бизнес-логику приложения, для противодействия которым требуется понимать нормальные поведенческие паттерны легитимного пользователя при работе с приложением; нелегитимные автоматизированные действия при помощи ботов по сбору информации, подбору паролей, обходу CAPTCHA и т. п.; распределённые атаки типа «отказ в обслуживании» на уровне приложения (L7 DDOS), в результате которых происходит исчерпание ресурсов инфраструктурных компонентов приложения.

Материал взят с <https://www.fortinet.com/ru/products/next-generation-firewall>