Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Кафедра Технического и программного обеспечения вычислительных и информационных систем
(название кафедры)

ПРЕЗЕНТАЦИЯ К КУРСОВОЙ РАБОТЕ

Разработка локальной сети двух зданий с исрользваонием технологиии Firewall

09.03.02 Информационные системы и технологии
(код и наименование направления подготовки)

По дисциплине: Инфокоммуникационные системы и сети

Выполнил: студент группы: ИС2-201-ОБ Провоторов Д.С.

Проверил: руководитель, к.т.н., доцент: Заревич А.И.

Воронеж 2022

Определение «Firewall»

Межсетевой экран (МЭ, брандмауэр или Firewall) представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты, блокирует или разрешает их прохождение. В фильтрации трафика брандмауэр опирается на установленные параметры — чаще всего их называют правилами МЭ.

Современные межсетевые экраны располагаются на периферии сети, ограничивают транзит трафика, установку нежелательных соединений и подобные действия за счет средств фильтрации и аутентификации.

Для чего нужен МЭ и как он работает

Главная задача МЭ – это фильтрация трафика между зонами сети. Он может использоваться для разграничения прав доступа в сеть, защиты от сканирования сети компании, проведения сетевых атак. Проще говоря, межсетевой экран – это одно из устройств, при помощи которого обеспечивается сетевая безопасность компании.

Функции «Firewall»

Брандмауэр может:

- **Остановить подмену трафика**. Представим, что ваша компания обменивается данными с одним их своих подразделений, при этом ваши IP-адреса известны. Злоумышленник может попытаться замаскировать свой трафик под данные офиса, но отправить его с другого IP. Брандмауэр обнаружит подмену и не даст ему попасть внутрь вашей сети.
- **Защитить корпоративную сеть от DDoS-атак**. То есть ситуаций, когда злоумышленники пытаются вывести из строя ресурсы компании, отправляя им множество запросов с зараженных устройств. Если система умеет распознавать такие атаки, она формирует определенную закономерность и передает ее брандмауэру для дальнейшей фильтрации злонамеренного трафика.
- **Заблокировать передачу данных на неизвестный IP-адрес**. Допустим, сотрудник фирмы скачал вредоносный файл и заразил свой компьютер, что привело к утечке корпоративной информации. При попытке вируса передать информацию на неизвестный IP-адрес брандмауэр автоматически остановит это.

Правила МЭ

Сетевой трафик, проходящий через брандмауэр, сопоставляется с правилами, чтобы определить, пропускать его или нет.

Правило межсетевого экрана состоит из условия (IP-адрес, порт) и действия, которое необходимо применить к пакетами, подходящим под заданное условие. К действиям относятся команды **разрешить** (accept), **отклонить** (reject) и **отбросить** (drop). Эти условия указывают МЭ, что именно нужно совершить с трафиком:

- разрешить — пропустить трафик;
- отклонить — не пропускать трафик, а пользователю выдать сообщение-ошибку «недоступно»;
- отбросить — заблокировать передачу и не выдавать ответного сообщения.

Для лучшего понимания рассмотрим пример. Допустим, у нас есть три правила:

1. Разрешить доступ всем IP-адресам, которые принадлежат отделу маркетинга, на 80-й порт.
2. Разрешить доступ всем IP-адресам, которые принадлежат отделу системного администрирования.
3. Отклонить доступ всем остальным.

Если к сети попытается подключиться сотрудник отдела технической поддержки, он получит сообщение об ошибке соединения (см. правило 3). При этом если сотрудник отдела маркетинга попробует подключиться по SSH, то также получит сообщение об ошибке, поскольку использует 22-й порт (см. правило 1).

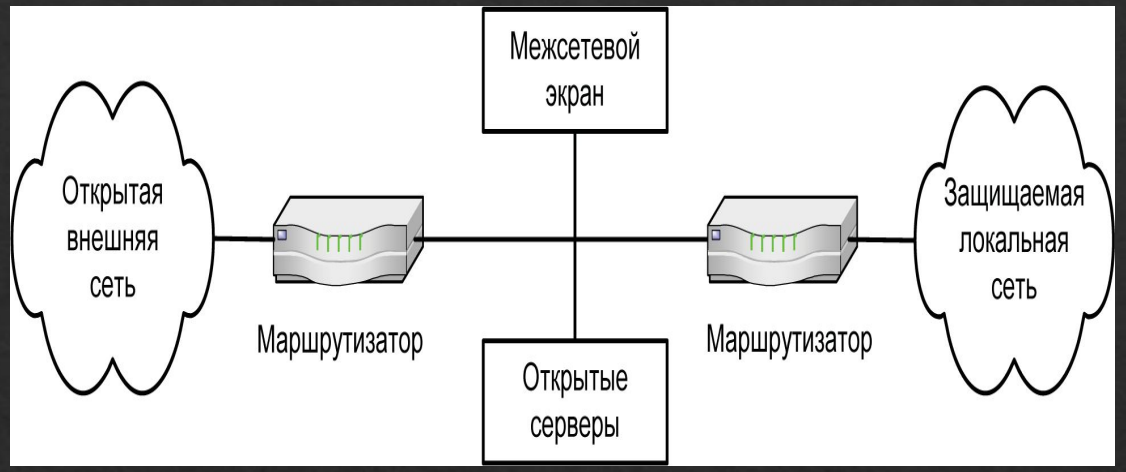
```
FortiGate # show firewall address marketing
config firewall address
    edit "marketing"
        set uuid 728e3f24-3e29-51ec-ad86-7fd7638fda4b
        set type iprange
        set start-ip 10.0.3.1
        set end-ip 10.0.3.254
    next
end

FortiGate # show firewall policy 7
config firewall policy
    edit 7
        set name "acsess to marketing department"
        set uuid 387225d4-ac61-51ec-784d-3adea05aeba7
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "marketing"
        set dstaddr "all"
        set schedule "always"
        set service "HTTP"
        set logtraffic disable
    next
end

FortiGate #
```

Контроль состояния сеансов на уровне МЭ

Межсетевой экран с контролем состояния сеансов анализирует всю активность пользователей от начала и до конца — каждой установленной пользовательской сессии. На основе этих данных он определяет типичное и нетипичное поведение пользователя. Если поведение в рамках сессии показалась ему нетипичной, МЭ может заблокировать трафик.



Получается, решение об одобрении или блокировке входящего трафика принимается не только на основании заданных администратором правил, но и с учетом контекста — сведений, полученных из предыдущих сессий. Брандмауэры с отслеживанием состояния сеансов считаются гораздо более гибкими, чем классические межсетевые экраны.

Типы «Firewall»

Аппаратный межсетевой экран

Аппаратный МЭ – это, как правило, специальное оборудование, составляющие которого (процессоры, платы и т.п.) спроектированы специально для обработки трафика.

Работает они на специальном ПО — это необходимо для увеличения производительности оборудования. Примерами аппаратного межсетевого экрана выступают такие устройства, как Cisco ASA, FortiGate, Cisco FirePower, UserGate и другие.

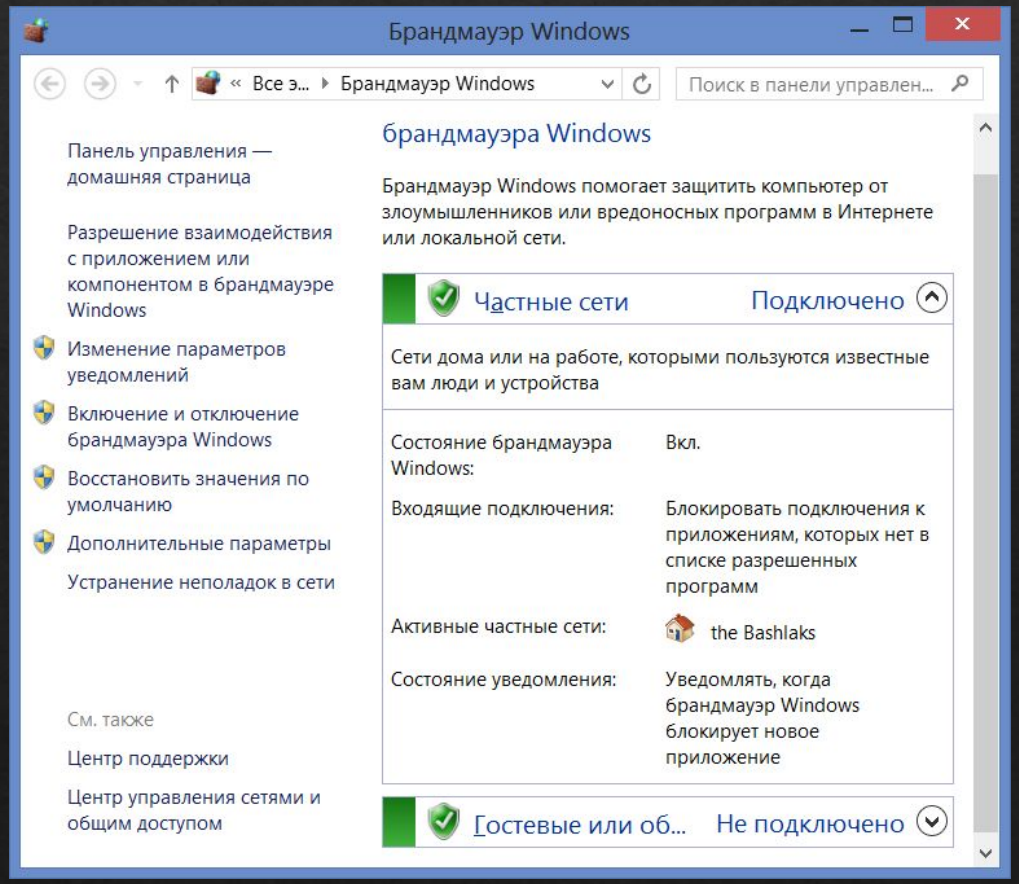
Аппаратные МЭ более мощные по сравнению с программными, однако это влияет на стоимость решений. Нередко она в разы выше, чем у программных аналогов.

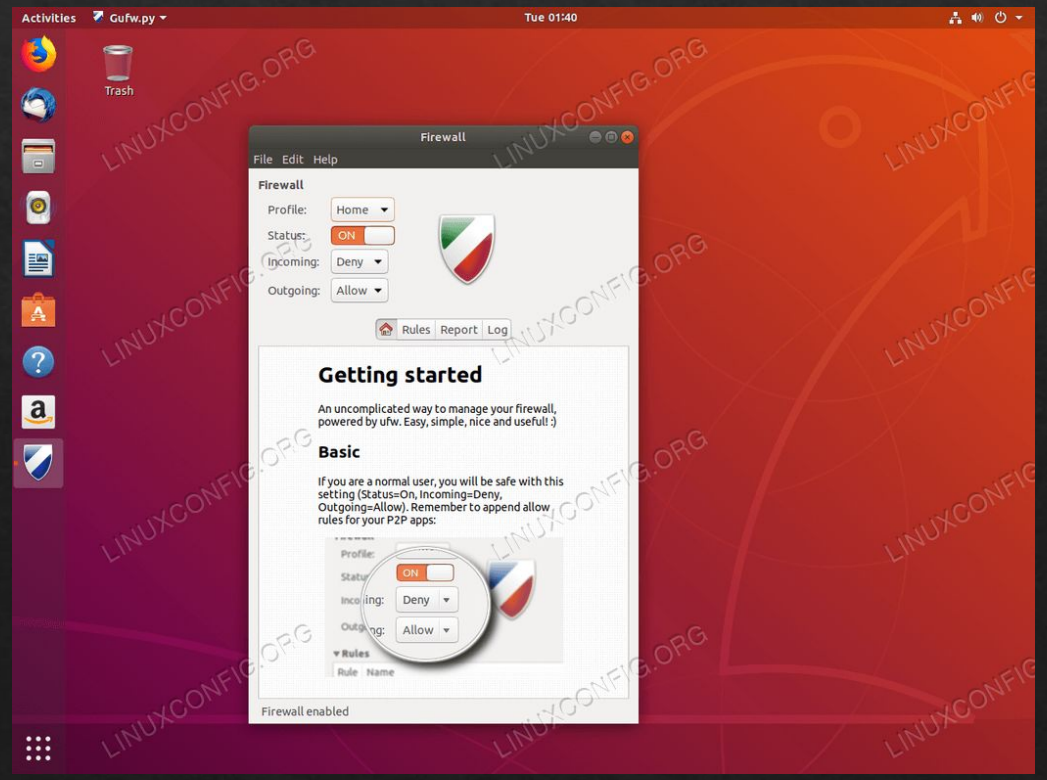
Программный межсетевой экран

Программный МЭ – это программное обеспечение, которое устанавливается на устройств, реальное или виртуальное.

Через такой межсетевой экран перенаправляется весь трафик внутрь рабочей сети. К программным относятся брандмауэр в Windows и iptables в Linux.

Программные МЭ, как правило, дешевле и могут устанавливаться не только на границах сети, но и на рабочих станциях пользователей. Из основных недостатков — более низкая пропускная способность и сложность настройки в ряде случаев.





Unified threat management, или универсальный шлюз безопасности

Такие межсетевые экраны включают в себя антивирус, брандмауэр, спамфильтр, VPN и систему IDS/IPS (системы обнаружения и предотвращения вторжений), контроль сеансов.

Основное преимущество данной технологии в том, что администратор работает не с парком различных устройств, а использует единое решение. Это удобно, так как производитель предусматривает централизованный интерфейс управления службами, политиками, правилами, а также дает возможность более «тонкой» настройки оборудования.

Архитектура UTM

В UTM-устройство входят несколько видов процессоров:

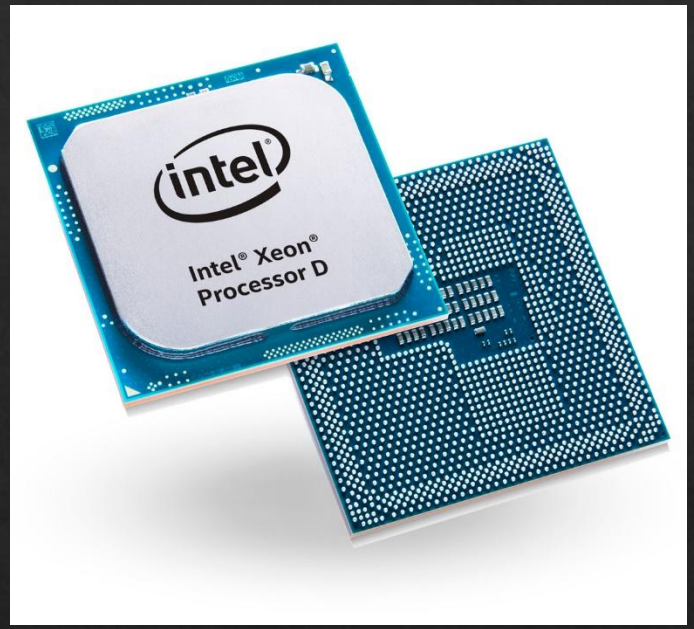
- процессор общего назначения, или центральный процессор,
- процессор обработки данных,
- сетевой процессор,
- процессор обработки политик безопасности.

Процессор общего назначения

Похож на процессор, установленный в обычном ПК. Он выполняет основные операции на межсетевом экране. Остальные виды процессоров призваны снизить нагрузку на него.

Сетевой процессор

Предназначен для высокоскоростной обработки сетевых потоков. Основная задача заключается в анализе пакетов и блоков данных, трансляции сетевых адресов, маршрутизации сетевого трафика и его шифровании.



Процессор данных

Отвечает за обработку подозрительного трафика и сравнения его с изученными угрозами. Он ускоряет вычисления, происходящие на уровне приложений, а также выполняет задачи антивируса и служб предотвращения вторжений.

Процессор обработки политик безопасности

Отвечает за выполнение задач антивируса и служб предотвращения вторжений. Также он разгружает процессор общего назначения, обрабатывая сложные вычислительные задачи.

Межсетевой экран следующего поколения (NGFW)

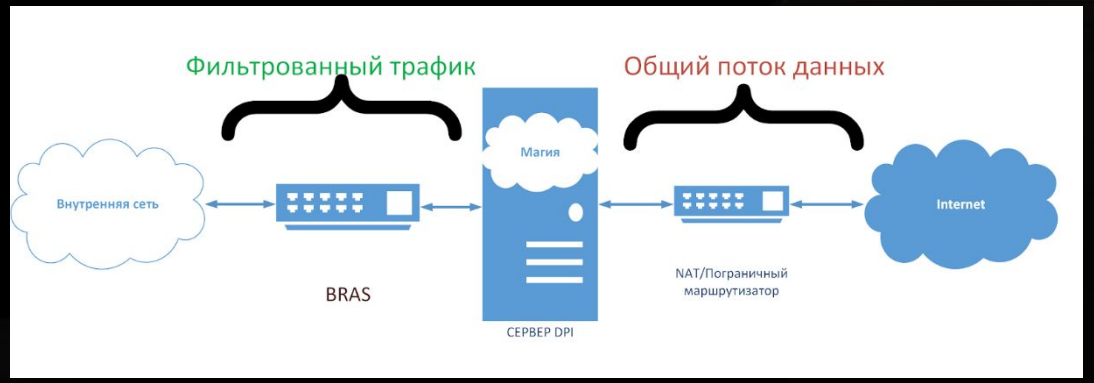
Next-generation firewall (NGFW) – файрвол следующего поколения. Его ключевая особенность в том, что он может производить фильтрацию не только на уровне протоколов и портов, но и на уровне приложений и их функций. Это позволяет успешнее отражать атаки и блокировать вредоносную активность.

Также, в отличие от межсетевого экрана типа Unified threat management, у NGFW есть более детальная настройка политик безопасности и решения для крупного бизнеса.

Основные функции Next-generation firewall

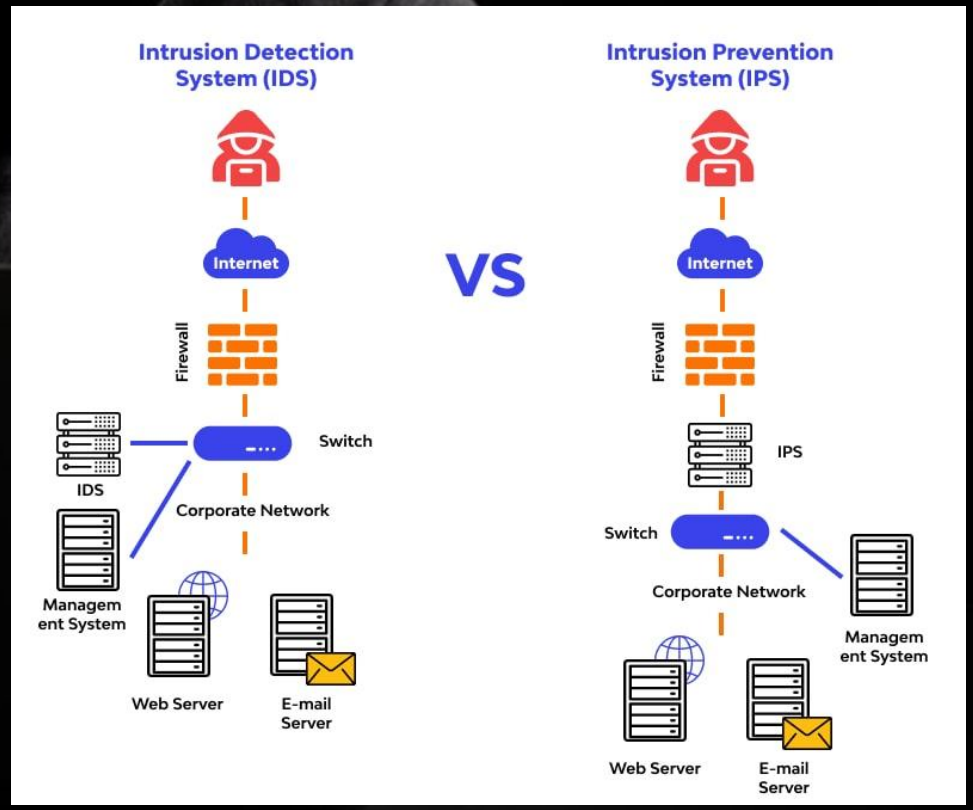
Deep Packet Inspection (DPI)

Технология, выполняющая детальный анализ пакетов. В отличие от правил классического межсетевого экрана данная технология позволяет выполнять анализ пакета на верхних уровнях модели OSI. Помимо этого, DPI выполняет поведенческий анализ трафика, что позволяет распознавать приложения, которые не используют заранее известные заголовки и структуры данных.



Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)

Система обнаружения и предотвращения вторжений. Межсетевой экран блокирует и фильтрует трафик, в то время как IPS/IDS обнаруживает вторжение и предупреждает системного администратора или предотвращает атаку в соответствии с конфигурацией.



Антивирус

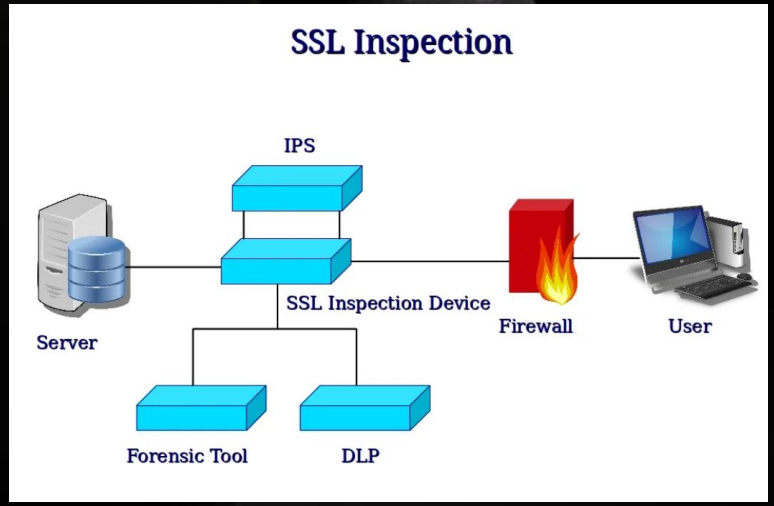
Обеспечивает защиту от вирусов и шпионского ПО в реальном времени, определяет и нейтрализует вредонос на различных платформах.

Фильтрация по URL, или веб-фильтр

Возможность блокировки доступа к сайтам или другим веб-приложениям по ключевому слову в адресе.

Инспектирование SSL

Позволяет межсетевому экрану нового поколения устанавливать SSL-сессию с клиентом и сервером. Благодаря этому существует возможность просматривать шифрованный трафик и применять к нему политики безопасности.

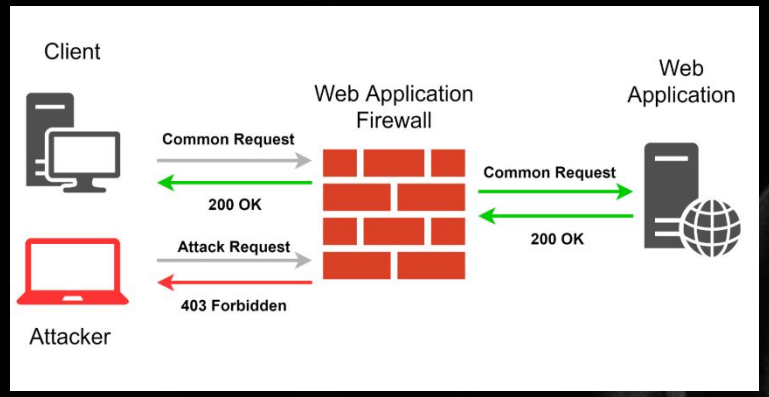


Антиспам

Функция, которая позволяет защитить корпоративных пользователей от фишинговых и нежелательных писем.

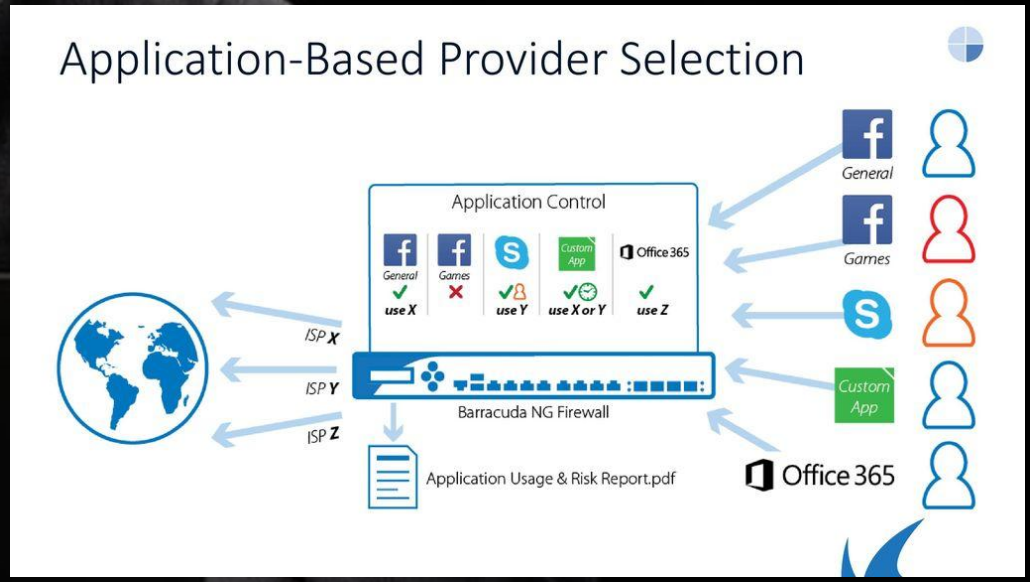
Web Application Firewall

Совокупность правил и политик, направленных на предотвращение атак на веб-приложения.



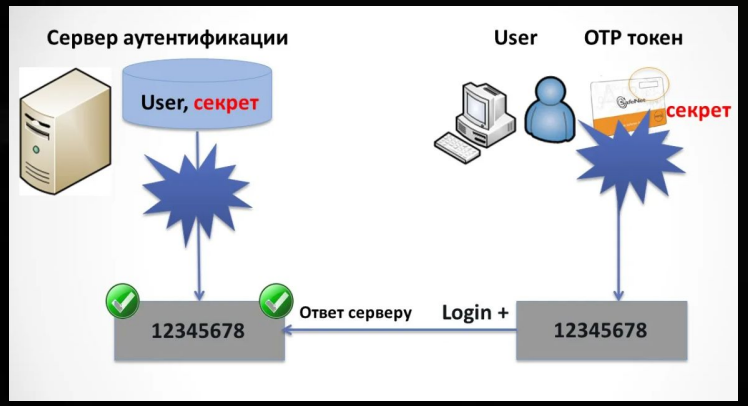
Application Control

Используется для ограничения доступа к приложениям, их функциям или к целым категориям приложений. Все это задействует функции отслеживания состояния приложений, запущенных пользователем, в режиме реального времени.



Аутентификация пользователей

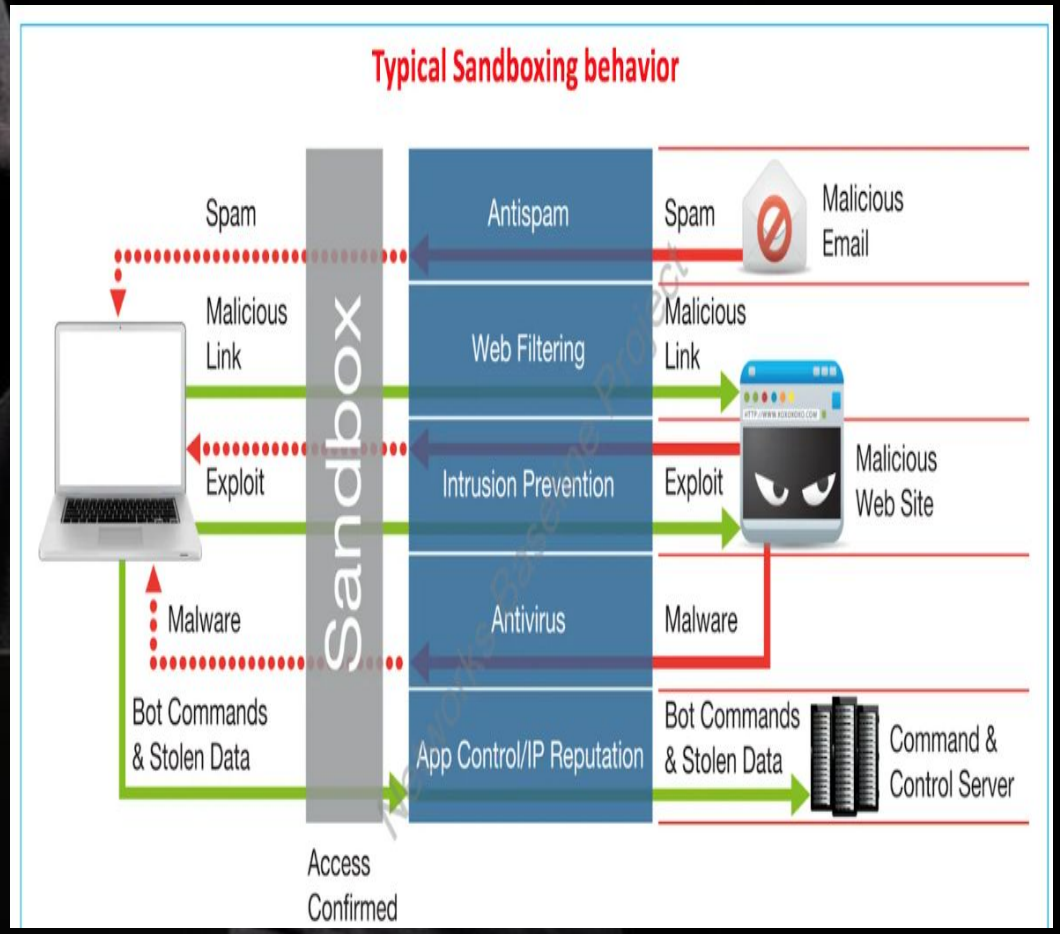
Возможность настраивать индивидуальные правила под каждого пользователя или группу.



Sandboxing

Метод, при котором файл автоматически помещается в изолированную среду для тестирования, или так называемую песочницу. В ней можно инициализировать выполнение подозрительной программы или переход по URL, который злоумышленник может прикрепить к письму. Песочница создает безопасное место для установки и выполнения программы, не подвергая опасности остальную часть системы.

Изолированная защита очень эффективна в работе с так называемыми угрозами нулевого дня. Это угрозы, которые ранее не были замечены или не соответствуют ни одному известному вредоносному ПО. Несмотря на то, что обычные фильтры электронной почты могут сканировать электронные письма для обнаружения вредоносных отправителей, типов файлов и URL-адресов, угрозы нулевого дня появляются постоянно. Традиционные средства фильтрации могут их пропустить.



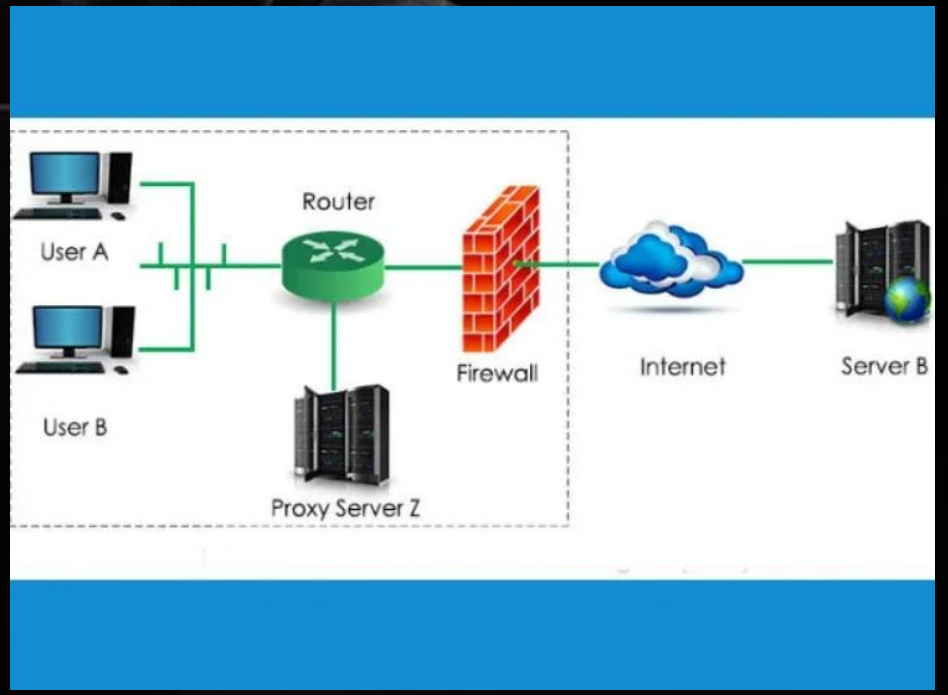
Использование прокси в качестве межсетевого экрана

Прокси-сервер контролирует трафик на последнем уровне стека TCP\IP, поэтому иногда его называют шлюзом приложений. Принцип работы заключается в фильтрации данных на основании полей заголовков, содержимого поля полезной нагрузки и их размеров (помимо этого, задаются дополнительные параметры фильтрации).

Прокси-серверы осуществляют фильтрацию одного или нескольких протоколов. Например, наиболее распространенным прокси-сервером является веб-прокси, предназначенный для обработки веб-трафика.

Такие серверы используются для следующих целей:

- обеспечение безопасности — например, для защиты вашего веб-сайта или пользователей от посещения сторонних сайтов,
- повышение производительности сети,
- ускорение доступа к некоторым ресурсам в интернете и др.



Поскольку прокси-серверы предназначены для определенных протоколов/портов, они, как правило, имеют более глубокие и сложные средства управления, чем общие правила безопасности межсетевого экрана.

Помимо веб-прокси, существуют такие прокси-серверы, как DNS, FTP, telnet, SSH, SSL, и другие протоколы.

Основной функцией классического брандмауэра является отслеживание и фильтрация трафика на сетевом и транспортном уровнях модели OSI. В отличие от него прокси-сервер устанавливает связь между клиентом и сервером, тем самым позволяя производить проверку на прикладном уровне, фильтровать запросы на подключение и так далее.

Чаще всего прокси-сервер является дополнением к стандартному межсетевому экрану, а межсетевые экраны нового поколения уже включают в себя все функции прокси-сервера.

Контрольные вопросы:

1. Дайте определение понятию «Firewall»
2. Назовите типы Firewall.
3. Опишите принцип работы Firewall.
4. Назовите функции Firewall.
5. Для чего нужны правила Firewall.