Политики межсетевого экрана

- Политики, основанные на IP-адресах и протоколах
  - IP-адреса и другие характеристики IP
  - IPv6
  - Протоколы TCP и UDP
  - Политики, основанные на приложениях
- Политики, основанные на идентификации пользователя
- Политики, основанные на сетевой активности

Политики, основанные на IP-адресах и протоколах

- Политика межсетевого экрана определяет, как межсетевой экран будет обрабатывать сетевой трафик для определенных IP-адресов и диапазонов адресов, протоколов, приложений и типов содержимого (например, активного содержимого). Перед разработкой политики межсетевого экрана следует проанализировать риски и определить типы трафика, которые необходимы организации. Анализ риска должен основываться на оценки угроз и уязвимостей.
- Обычно межсетевой экран должен блокировать весь входящий и исходящий трафик, который явно не разрешен политикой межсетевого экрана. Такая практика, называемая ***deny by default***, уменьшает риск атак и может уменьшить объем трафика в локальной сети. В силу динамичной природы хостов, сетей, протоколов и приложений по умолчанию все запретить является более безопасным подходом, чем разрешить весь трафик, который явно не запрещен.

- Рассмотрим детально какие типы трафика должны блокироваться. Сначала обсудим политику пакетных фильтров и анализ состояний на основе IP-адресов и других характеристиках IP. Потом рассмотрим политики, относящиеся к прикладному уровню. Далее рассмотрим доступ, основанный на идентификации пользователя и политики, которые запускаются в результате определенной сетевой активности.

Политики, основанные на IP-адресах и протоколах

- Политика межсетевого экрана должна разрешать прохождение только необходимых IP-протоколов, например, ICMP, TCP и UDP. Другими примерами являются протоколы IPsec (ESP и AH) и протоколы маршрутизации, которым тоже может быть необходимо проходить межсетевой экран. Все остальные IP-протоколы по умолчанию запрещены.
- Некоторые IP-протоколы **редко используются между внешней сетью и локальной**, и, следовательно, на межсетевом экране могут быть блокированы в обоих направлениях. Например, IGMP является протоколом, который используется для управления групповой передачей данных и использует широковещательные сообщения. Но широковещательные сообщения редко используются, и если они и используются, то не проходят через маршрутизаторы. Следовательно, можно блокировать IGMP трафик в обоих направлениях, если не используются широковещательные сообщения.

IP-адреса и другие характеристики IP

Политика межсетевого экрана должна разрешать прохождение пакетов, в которых адрес принадлежит используемым **в локальной сети диапазонам IP-адресов**. Конкретные рекомендации для IP-адресов следующие:

- Трафик с недействительными IP-адресами источника и получателя должен всегда блокироваться, независимо от расположения межсетевого экрана. Например, недействительными IPv4-адресами являются адреса с 127.0.0.0 по 127.255.255.255 (также известные как *localhost* адреса) и 0.0.0.0 (интерпретируемый некоторыми ОС как локальный или широковещательный (broadcast) адрес). Эти адреса не должны использоваться в сети.
- На сетевом периметре должен блокироваться трафик с недействительным адресом источника для входящего трафика и недействительным адресом получателя для исходящего трафика. Данный трафик часто связан с вредоносным ПО, spoofing и DoS-атаками или попытками переконфигурировать оборудование. Большинство типов недействительных внешних адресов являются IPv4-адреса в диапазоне, определенном в RFC 1918 как адреса для частных сетей. Этими диапазонами являются с 10.0.0.0 по 10.255.255.255 (10.0.0.0/8 в CIDR нотации), с 172.16.0.0 по 172.31.255.255 (172.16.0.0/12) и с 192.168.0.0 по 192.168.255.255 (192.168.0.0/16).

IP-адреса и другие характеристики IP

- На границы сетевого периметра должен блокироваться входящий трафик, если у него адрес источника принадлежит внутренней сети. Может выполняться преобразование адресов, чтобы разрешить внутренним хостам с частными адресами взаимодействовать с внешними хостами, но частные адреса не должны проходить через сетевой периметр.
- Исходящий трафик с недействительными адресами источника должен блокироваться (это часто называется *выходным фильтрованием*), так как скомпрометированные системы могут использоваться для выполнения атак на другие системы в интернете. Атаки, которые используют недействительные адреса источника, остановить гораздо труднее. Блокирование межсетевым экраном данного типа трафика снижает эффективность подобных атак.
- Входящий трафик, адресом получателя в котором является сам межсетевой экран, должен блокироваться, если только межсетевой экран не предоставляет сервисы для входящего трафика, которые требуют прямого соединения – например, если межсетевой экран действует как прикладной прокси.

IP-адреса и другие характеристики IP

- На границы сетевого периметра следует также блокировать трафик из внешней сети, содержащий **широковещательные адреса**, которые предназначены для внутренней сети. Любая система, которая отвечает на широковещательные сообщения, посылает **свой ответ системе, указанной в качестве источника**, а не самой системе источника. Такие пакеты могут быть использованы для создания огромного «шторма» сетевого трафика, что приведет к **DoS-атаке**. Обычные широковещательные адреса, а также адреса, используемые для multicast IP, могут как блокироваться межсетевым экраном, так и не блокироваться. Широковещательные и multicast-сообщения редко используются в обычных сетевых окружениях, но если они используются как внутри, так и вне организации, им следует разрешить прохождение через межсетевой экран.
- Межсетевые экраны, расположенные на границе сетевого периметра, должны блокировать весь входящий трафик к сетям и хостам, которые не должны быть доступны для внешних сетей. Решение о том, какие адреса должны блокироваться, часто является наиболее трудоемкой задачей при разработке политики межсетевого экрана.

IP-адреса и другие характеристики IP

- Некоторые производители выделяют в отдельную группу правила, проверяющие **доступность IP-адреса источника в пакете с интерфейса**, на который пришел данный пакет. Это так называемые правила доступа – **Access Rules**. Эти правила позволяют предотвратить одну из наиболее распространенных атак – атаку подделки IP-адреса источника (IP Spoofing). В подобных атаках нарушитель изменяет IP-адрес источника на IP-адрес доверенного хоста, что может позволить пакету соответствовать правилам фильтрования для доверенных хостов. Хотя в этом случае источник не может получать возвращаемые пакеты и завершить установление соединения, возникает потенциальная угроза DoS-атак.
- Перед проверкой нового соединения правилами фильтрования, выполняется проверка IP-адреса источника правилами доступа. Эти правила доступа используются для того, чтобы проверить, что трафик на конкретном интерфейсе получен с доступных для данного интерфейса сетей, а также для блокировки пакетов, полученных с конкретных сетей/хостов источников. Правила доступа обеспечивают эффективную и целенаправленную фильтрацию попыток установления новых соединения.

IP-адреса и другие характеристики IP

- В подобных системах обычно бывает определено так называемое *Правило доступа по умолчанию*. Данное правило обычно выполняет проверку входящего запроса на создание соединения, выполняя так называемый ***поиск обратного маршрута (reverse lookup)*** в таблицах маршрутизации. Данный поиск выполняется для подтверждения того, что запрос на создание входящего соединения идет от источника, который доступен с данного интерфейса. В случае неудачного поиска обратного маршрута соединение не устанавливается.

IPv6

- IPv6 является следующей версией протокола IP, развертывание которой в настоящее время возрастает. Хотя внутренний формат IPv6 и длина адреса отличаются от IPv4, многие другие возможности остаются теми же самыми – и это же относится к межсетевым экранам. Для возможностей, которые остались такими же в IPv6, поведение межсетевого экрана не меняется. Например, блокирование всего входящего и исходящего трафика, который не был явно разрешен, должно выполняться независимо от того, трафик имеет адрес IPv4 или IPv6.
- Некоторые межсетевые экраны не могут обрабатывать трафик IPv6; другие имеют ограниченные возможности фильтрования трафика IPv6. Если во внутренней сети необходим трафик IPv6, то межсетевой экран также должен иметь возможности в фильтровании этого трафика. Такие межсетевые экраны должны обладать следующими возможностями:

- Межсетевой экран должен иметь возможность **указывать IPv6 адреса в правилах фильтрования**.
- Для облегчения администрирования интерфейс администратора должен позволять **клонировать IPv4 правила в IPv6 правила**.
- Межсетевой экран должен иметь возможность **фильтровать протокол ICMPv6**, как описано в RFC 4890.

IPv6

- Межсетевой экран должен иметь возможность **блокировать** относящиеся к IPv6 протоколы, такие как **v6-to-v4 туннелирование**, Teredo и ISATAP, если они не требуются.
- Многие сайты туннелируют IPv6 пакеты в IPv4 пакеты. Это чаще всего используется сайтами, которые экспериментируют с IPv6, потому что в настоящий момент легче получать IPv6 от туннелирующего брокера с помощью v6-to-v4 туннеля, чем получать исходный IPv6 от ISP. Существует большое число способов сделать это, при этом стандарты туннелирования только разрабатываются. Если межсетевой экран умеет анализировать содержимое IPv4 пакетов, ему необходимо знать, как анализировать трафик, который туннелирован каким-либо из способов. Следствием этого является то, что если межсетевой экран используется для запрещения прохождения IPv6 в сеть, то он должен распознавать и блокировать все формы v6-to-v4 туннелирования.

  - Заметим, что приведенный выше список является достаточно коротким, и не все правила относятся к безопасности. Так как развертывание IPv6 находится еще на достаточно ранней стадии, еще не существует всеобъемлющего соглашения относительно операций IPv6, которые должен выполнять межсетевой экран, и чем он должен отличаться от межсетевых экранов IPv4.

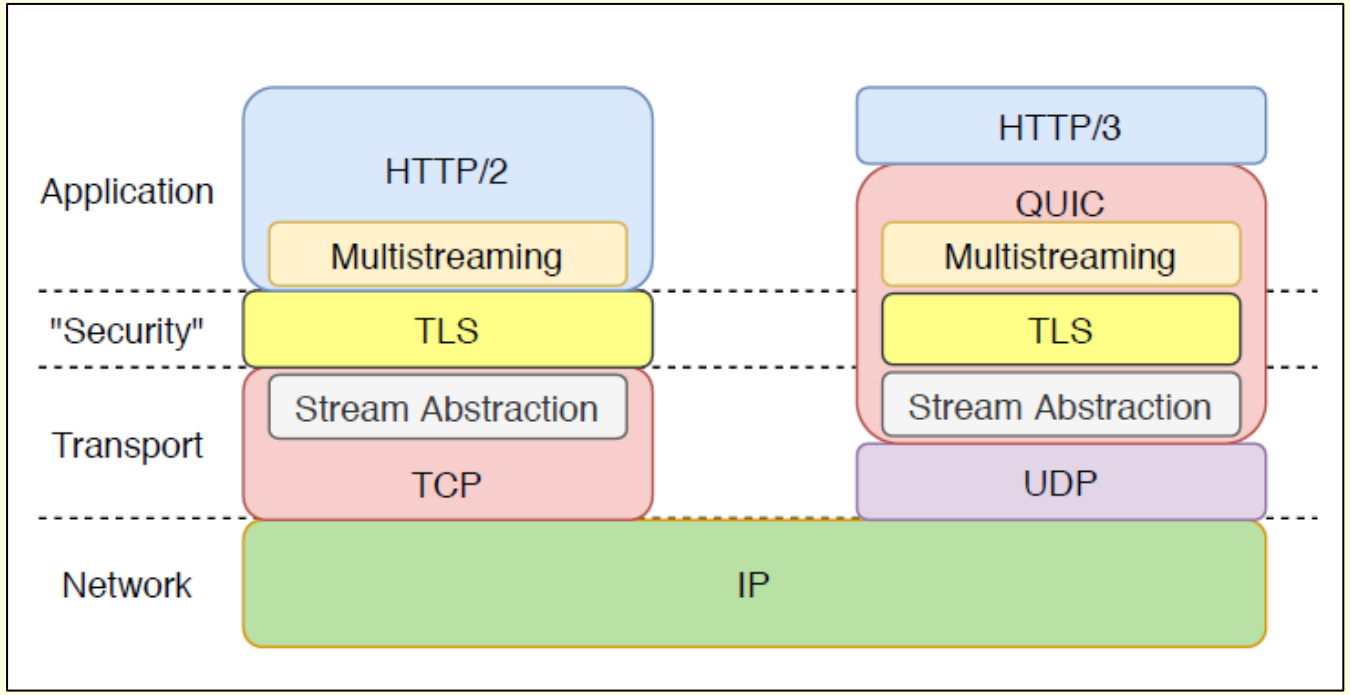
IPv6

- Для межсетевых экранов, которые допускают использование IPv6, **трафик с недействительным IPv6 адресами источника и получателя должен блокироваться** – аналогично блокированию трафика с недействительными IPv4 адресами. Следует заметить, **что определить список недействительных IPv6 адресов гораздо сложнее**. Также IPv6 позволяет администратору назначать адреса различными способами. Это означает, что конкретный диапазон адресов, связанный с организацией, может иметь огромное число недействительных представлений, и только несколько представлений будут действительными. Перечисление всех недействительных IPv6 адресов является более сложной задачей, чем перечисление недействительных IPv4 адресов.
- Организации, которые еще не используют IPv6, должны блокировать весь исходный и туннелированный IPv6-трафик. Заметим, что такое блокирование ограничивает возможности тестирования и оценки IPv6 и технологий туннелирования IPv6. Чтобы обойти это, следует выборочно разблокировать IPv6 или определенные технологии туннелирования.

Протоколы TCP и UDP

- Прикладные протоколы могут использовать TCP, UDP или оба протокола. **Прикладной сервер обычно слушает один или несколько фиксированных TCP- или UDP-портов.** Некоторые приложения используют один порт, но многие приложения используют несколько портов. Например, хотя SMTP использует TCP-порт 25 для отправки почты, он использует также порт 587 для передачи почты. Аналогично, FTP использует по крайней мере два порта, один из которых не предсказуем. Большинство веб-серверов используют TCP порт 80, но часто также используются дополнительные порты, такие как TCP-порт 8080. Некоторые приложения используют как TCP, так и UDP; например, поиск (lookup) DNS может происходить и через UDP порт 53, и через TCP порт 53. Прикладные клиенты обычно используют любой порт из широкого диапазона портов.
- С учетом этого в наборе правил для межсетевого экрана для входящего TCP и UDP трафика по умолчанию должна использоваться запрещающая политика (**`Drop`**). Для исходящего TCP- и UDP-трафика обычно используется менее строгая политика, потому что в большинстве случаев локальным пользователям разрешается доступ ко внешним приложениям.

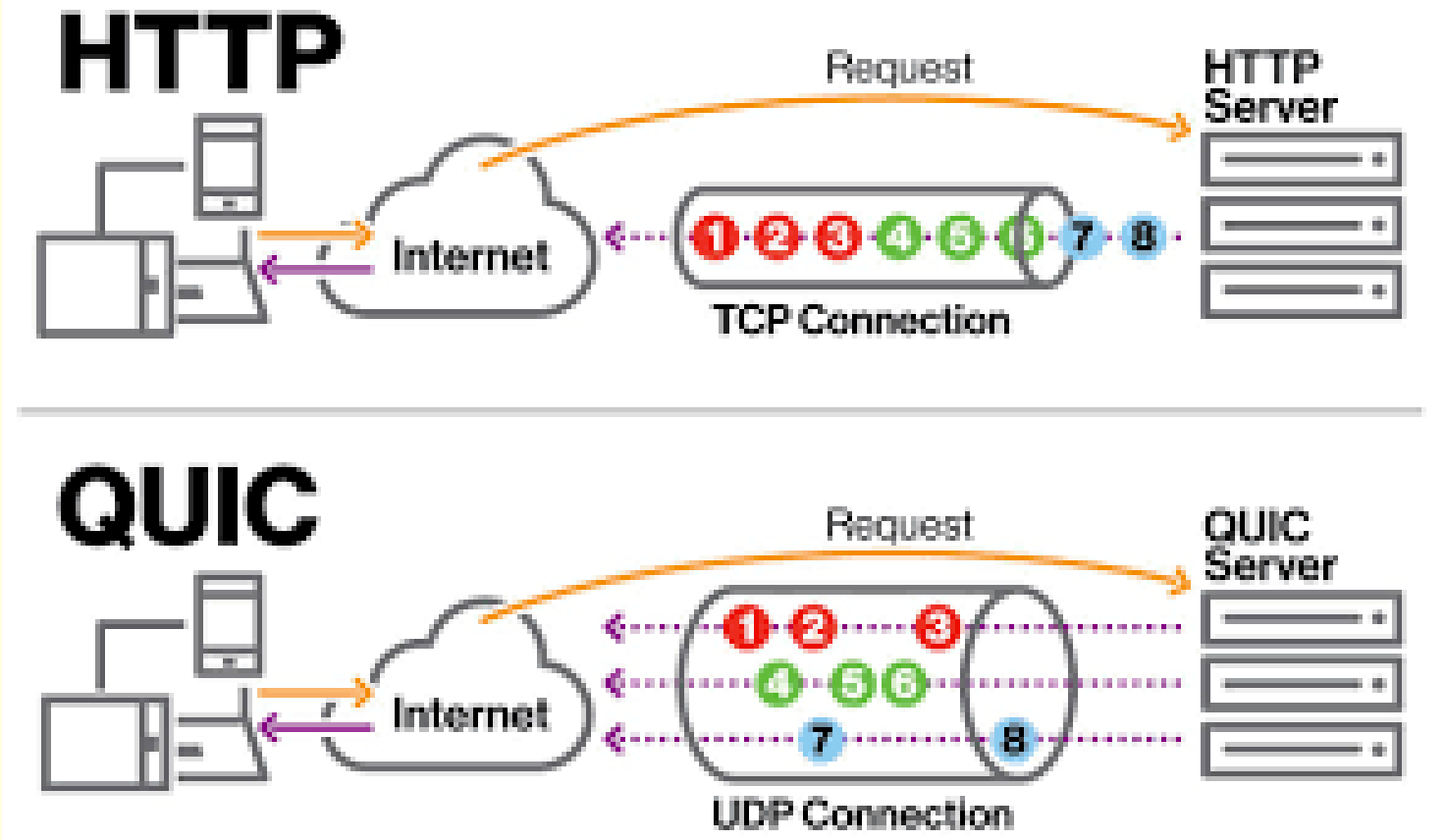
Протокол QIUC



Протокол QIUC

- QUIC (Quick UDP Internet Connections) разработан Google в 2012г., стандартизован IETF в 2021г.
- HTTP/2 использует одно TCP-соединение с сервером вместо отдельных соединений для каждой страницы.
- Это единое соединение может быть использовано для независимых запросов и получения отдельных ресурсов.
- Преимущества QUIC:
  - Сокращение трехстороннего рукопожатия до запуска одного пакета (нулевое рукопожатие)
  - Уменьшение количества повторно передаваемых пакетов, необходимых для передачи данных
  - Уменьшение блокировки заголовка между несколькими потоками данных в пределах одного потока TCP, вызванной потерей пакетов

Протокол QIUC



Протокол QIUC

- МЭ сталкиваются с серьёзными проблемами при использовании QUIC, поскольку его зашифрованный протокол, основанный на протоколе UDP, обходит традиционные методы проверки, такие как HTTPS DPI и расшифровка TLS.
- Эта недостаточная прозрачность может создавать «слепые зоны» безопасности, что приводит к тому, что некоторые предприятия блокируют QUIC или принудительно переходят на TLS поверх TCP, в то время как производители и пользователи изучают экспериментальные функции и альтернативные методы фильтрации трафика.
- Google разработал QUIC таким образом, чтобы он был гибким и легко обновляемым, в отличие от жёсткой и устаревшей инфраструктуры TCP. Хотя такой подход способствует быстрому внедрению инноваций, он также требует от МЭ и инструментов безопасности быстрой адаптации к изменениям на уровне протокола. Постоянная необходимость в обновлениях может стать серьёзной нагрузкой на ИТ-отделы и инфраструктуру.

Протокол QIUC

- МЭ, пропускающие QUIC, могут быть подвержены проникновению по протоколу UDP, который хорошо известен и документирован, но до сих пор имел ограниченное применение для веб-серверов, защищенных межсетевыми экранами.
- Существуют угрозы, связанные с проникновением по UDP, посредством создания обратного shell, который был бы невозможен в сценарии TCP/TLS.

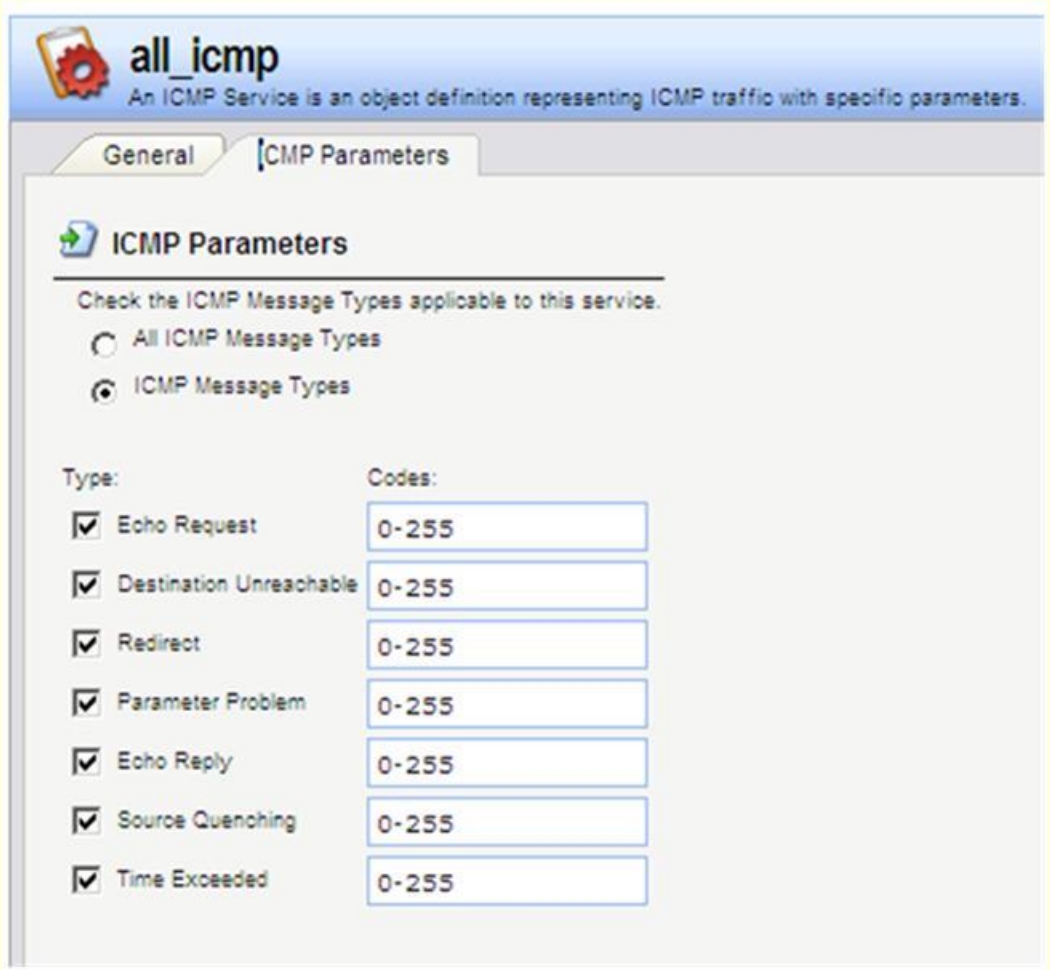
Протокол ICMP

- Атакующие могут использовать различные типы и коды ICMP **для разведки или манипулирования потоком сетевого трафика**.
- Однако ICMP также необходимо для выполнения многих **полезных функций**, таких как определение производительности сети.
- Некоторые политики межсетевых экранов блокируют весь ICMP-трафик, но это часто ведет к проблемам, связанным с **диагностикой** и производительностью.
- Часто политика **разрешает весь исходящий ICMP-трафик**, но **ограничивает входящий ICMP** по типам и кодам, которые необходимы для обнаружения PMTU (ICMP код 3) и достижения получателя.
- Для предотвращения вредоносной деятельности межсетевые экраны, расположенные на границе сетевого периметра, должны **запрещать весь входящий и исходящий ICMP-трафик**, **за исключением отдельных типов и кодов**, которые должны быть специально разрешены.

Протокол ICMP

- Для ICMP IPv4 сообщения типа 3 не должны фильтроваться, потому что они используются для **сетевой диагностики**.
- Команды **`ping`** (ICMP код 8) является важной диагностикой сети, но входящие **`ping`** часто блокируются политикой межсетевого экрана, чтобы предотвратить изучение внутренней топологии сети атакующим.
- Для ICMP в IPv6 многие типы сообщений должны быть разрешены.
- ICMP часто используется **другими протоколами для увеличения скорости и надежности сети**.
- Следовательно, **ICMP внутри сети организации не должно блокироваться** межсетевыми экранами, которые не расположены на границы сетевого периметра, если только это не перевешивается необходимостью обеспечения безопасности.
- Аналогично, если в организации существует более одной сети, то ICMP из этих сетей не должен блокироваться.

Протокол ICMP



Протоколы IPSec

- Необходимо иметь политику, **явно разрешающую или запрещающую IPSec-трафик**, который начинается или заканчивается внутри сетевого периметра. В IPSec используются протоколы ESP и AH; межсетевой экран, который блокирует эти протоколы, не будет разрешать IPSec.
- Блокирование ESP предотвращает использование шифрования для защиты чувствительных данных. Это может позволить межсетевому экрану с поддержкой состояния или шлюзу прикладного уровня анализировать данные, которые в противном случае были бы зашифрованы.
- Организации, которые разрешают использование IPSec, **должны блокировать ESP и AH за исключением определенных адресов во внутренней сети – это адреса шлюзов IPSec**, которые будут являться конечными точками VPN. Реализация такой политики будет требовать от сотрудников организации получить соответствующее разрешение на доступ к маршрутизаторам IPSec. Это также уменьшит количество зашифрованного трафика во внутренней сети, который не может быть проанализирован.

Политики, основанные на приложениях

- Изначально большинство межсетевых экранов просто блокировало нежелательный или подозрительный трафик на границе сетевого периметра.
- Прикладные межсетевые экраны, анализирующие входящий трафик, используют другой подход – они анализируют трафик, только после этого пропуская его к серверу.
- Подход, основанный **на приложении**, обеспечивает дополнительный уровень безопасности для входящего трафика, проверяя корректность этого трафика перед тем, как он достигнет нужного сервера.
- Теоретически входящий прикладной межсетевой экран может защитить сервер лучше, чем это может сделать сам сервер – например, может удалить вредоносный трафик до того, как он достигнет сервера.
- Входящий прикладной межсетевой экран должен использоваться перед любым сервером, который не имеет достаточных возможностей обеспечения собственной безопасности от атак прикладного уровня.

Политики, основанные на приложениях

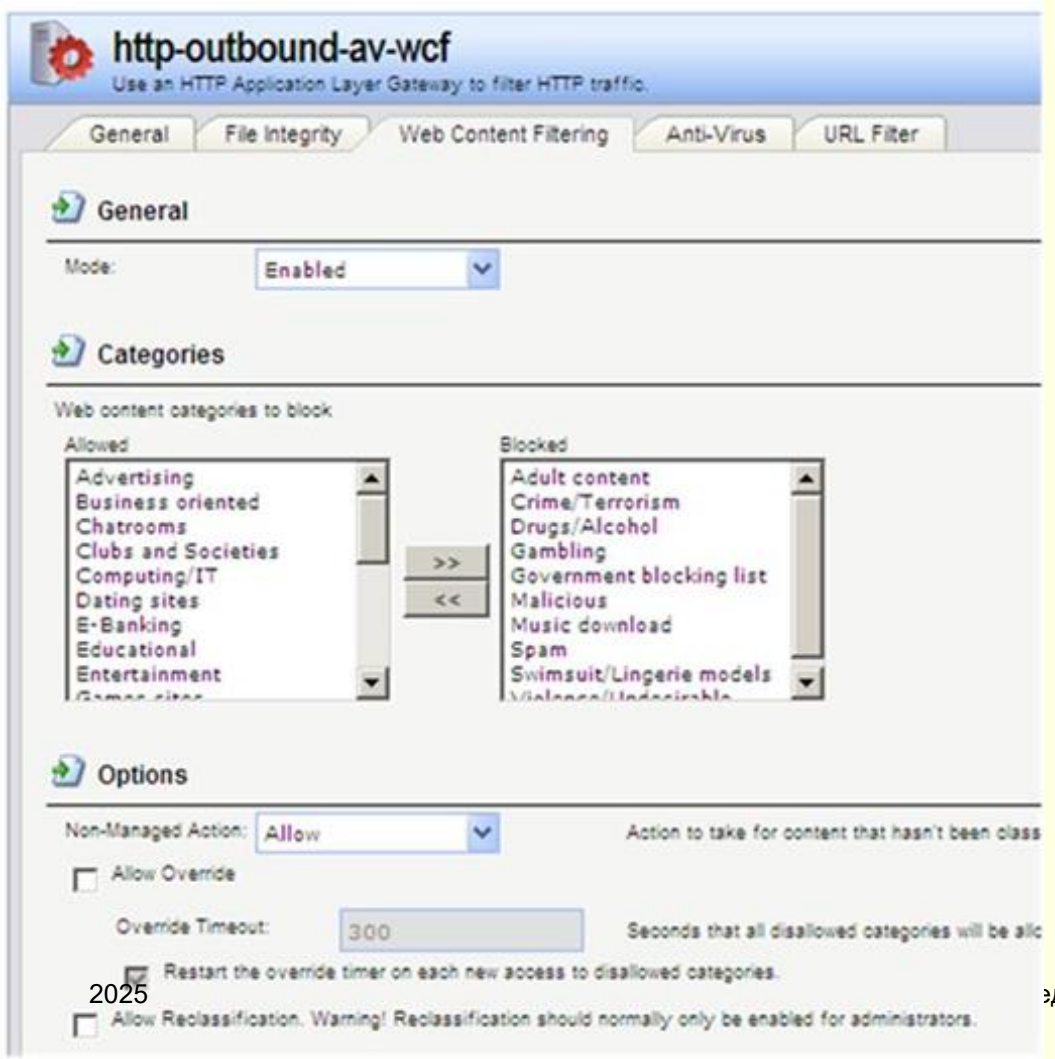
Главное, что необходимо рассмотреть при принятии решения об использовании входящего прикладного межсетевого экрана:

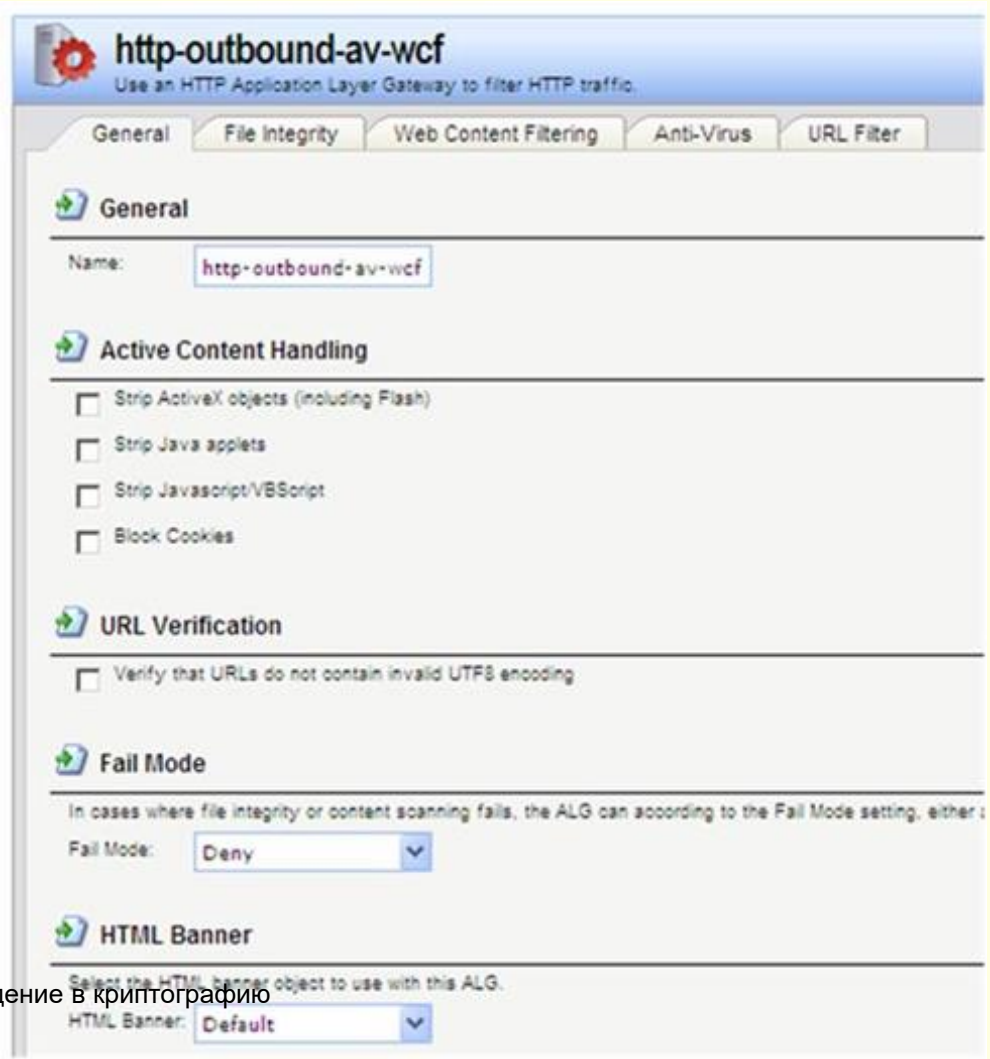
- Существует ли подходящий прикладной межсетевой экран.
- Достаточно ли защищен сервер существующими межсетевыми экранами.
- Может ли основной сервер удалить вредоносное содержимое также эффективно, как и прикладной межсетевой экран.
- Легко ли изменять правила фильтрования на основном сервере и на прикладном межсетевом экране для предотвращения новых угроз.

Политики, основанные на приложениях

- Прикладной межсетевой экран может внести **дополнительные проблемы, если он недостаточно быстрый для обработки трафика, предназначенного серверу**. Важно также проанализировать ресурсы сервера – если сервер не имеет достаточных ресурсов, чтобы отражать атаки, в качестве щита можно использовать прикладной межсетевой экран.
- Если **входящий прикладной межсетевой экран расположен позади пакетного фильтра на границе периметра** или межсетевого экрана в DMZ, пакетный фильтр должен блокировать трафик на основе IP-адресов, чтобы **снизить нагрузку на прикладной межсетевой экран**. При этом уменьшается количество трафика, которое видит прикладной межсетевой экран, тем самым у него остается больше ресурсов для фильтрования содержимого.
- **Исходящий прикладной прокси** полезен для определения систем, которые устанавливают не разрешенные политикой соединения изнутри защищаемой сети. В большинстве случаев это относится к HTTP. Исходящие HTTP-прокси **позволяют фильтровать опасное содержимое**. Также преимуществом HTTP-прокси, не относящимся к безопасности, является возможность **кэширования веб-страниц** для увеличения скорости загрузки и уменьшения нагрузки на сеть.

Политики, основанные на приложениях





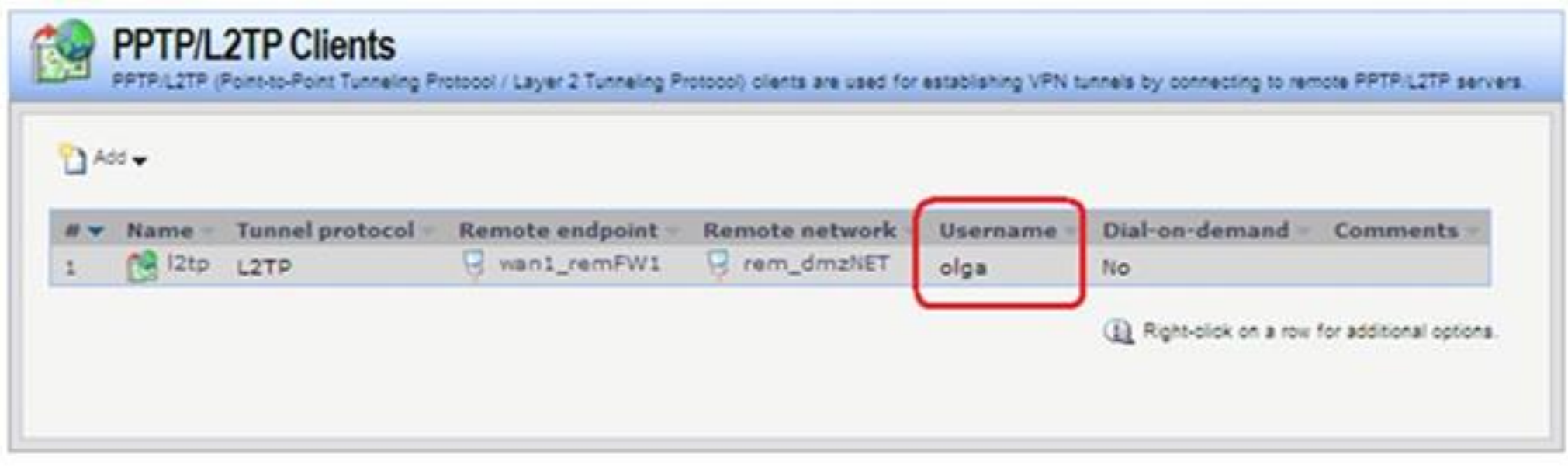
Примеры конфигурирования параметров HTTP-протокола

Политики, основанные на идентификации пользователя

- Традиционное фильтрование пакетов не знает идентификацию пользователя, который устанавливает соединение, поэтому без дополнительных возможностей технологии межсетевых экранов не могут иметь политики, которые разрешают или запрещают доступ на основе этих идентификаций.
- Однако существуют технологии межсетевых экранов, которые могут видеть эти идентификации и, следовательно, устанавливать политики, основанные на аутентификации пользователя.
- Одним из наиболее общих способов использовать на межсетевом экране политику, основанную на **идентификации пользователя**, является использование **VPN**.
- Как **IPSec VPN**, так и **TLS VPN** имеют много способов аутентификации пользователей, такие как секреты, определяемые для каждого пользователя, многофакторная аутентификация (например, криптографические токены, основанные на времени и защищенные PIN-кодом) или цифровые сертификаты, выданные каждому пользователю.
- Популярным методом для межсетевых экранов также становится NAC (**Network Access Control**), с помощью которого разрешается или запрещается доступ пользователей к отдельным сетевым ресурсам.
- Кроме того, прикладные межсетевые экраны могут разрешать или запрещать доступ, основываясь на аутентификации пользователя самим приложением.

Политики, основанные на идентификации пользователя

- Межсетевые экраны, которые реализуют политики, основанные на идентификации пользователя, должны иметь возможность отображать эти политики в своих логах. Это означает, что в логах для каждого пользователя должен записываться не только IP-адрес, но и идентификация пользователя.



Политики, основанные на сетевой активности

- Многие межсетевые экраны позволяют блокировать соединения после некоторого периода **активности или простоя**.
- Например, если пользователь с внешней стороны межсетевого экрана вошел на файловый сервер, но не сделал никаких запросов в течение последних 15 минут, политика может блокировать весь последующий трафик по этому соединению.
- Политики, зависящие от времени, используются для защиты от атак, которые выполняются, используя установленное соединение вошедшего пользователя и, следовательно, его креденциалы.
- Некоторые межсетевые экраны могут блокировать соединения, которые с их точки зрения являются активными, но с точки зрения приложения они уже не являются активными.

Политики, основанные на сетевой активности

- Другой тип политики межсетевого экрана, основанной на сетевой активности, является **перенаправление трафика, если количество трафика превысило значение**, установленное в политике.
- Например, межсетевой экран может перенаправлять соединения, сделанные с конкретного внутреннего адреса, по более медленному маршруту, если уровень превысит определенный порог.
- Другой пример политики – можно отбрасывать входящие ICMP-пакеты, если трафик превысил некоторое значение. Разработка таких политик является достаточно сложной, потому что перенаправление может приводить к потерям и трудно диагностируемым сбоям.