Межсетевые экраны

- Основные принципы использования межсетевых экранов
- Технологии межсетевых экранов
  - Стек протоколов
  - Состояния TCP-соединения
  - Фильтрование пакетов
  - Пакетные фильтры с анализом состояния
  - DMZ-сеть
  - МЭ прикладного уровня
  - Прокси-шлюзы прикладного уровня
  - Выделенные прокси-сервера
  - Конечные точки VPN
  - Гибридные технологии МЭ
  - Расширенное управление доступом в сеть
  - Унифицированное управление угрозами
  - МЭ для веб-приложений
  - МЭ для виртуальных инфраструктур
  - МЭ для отдельных хостов и домашних сетей
  - Устройства персональных МЭ
- Ограниченность анализа межсетевого экрана
- Политики межсетевого экрана
- Межсетевые экраны с возможностями NAT
- Топология сети при использовании межсетевых экранов

Основные принципы использования межсетевых экранов

- Будем предполагать, что локальная сеть имеет **четкие границы**, т.е. про любой хост можно сказать, находится ли он в локальной сети или нет. Эти границы будем называть **сетевым периметром**. Также будем предполагать, что существуют явные **точки входа в локальную сеть**.
- Основной задачей межсетевого экрана является **предотвращение нежелательного доступа** в локальную сеть. Примером нежелательного доступа является нарушитель, который пытается осуществить незаконное проникновение в системы, доступные по сети. Он может просто получать удовольствие от взлома, а может стараться повредить информационную систему или внедрить в нее что-нибудь для своих целей. Например, целью хакера может быть получение номеров кредитных карточек, хранящихся в системе. Другим примером нежелательного доступа является размещение в вычислительной системе чего-либо, что воздействует на прикладные программы и сервисы, которые вычислительная система предоставляет своим пользователям.

Основные принципы использования межсетевых экранов

Рассмотрим технологии предотвращения нежелательного доступа в локальную сеть и к информационным системам.

Сервисы безопасности, которые предотвращают нежелательный доступ, можно разбить на две категории:

- Первая категория состоит из **процедур входа**, основанных на использовании разного рода **аутентификаторов** (паролей, аппаратных ключей, сертификатов и т.п.). Это позволяет разрешить доступ только законным пользователям. К этой категории относятся также различные межсетевые экраны (firewall), которые предотвращают атаки, основанные на использовании уязвимостей на различных уровнях стека протоколов TCP/IP.
- Вторая категория состоит из различных **мониторов**, **анализирующих доступ и деятельность пользователей**.

Основные принципы использования межсетевых экранов

- Межсетевые экраны защищают компьютеры и сети от попыток **несанкционированного доступа с использованием уязвимых мест**, существующих в семействе протоколов TCP/IP. Дополнительно они помогают решать проблемы безопасности, связанные с наличием уязвимостей в другом ПО, которое установлено на компьютерах в сети.
- Межсетевые экраны являются **аппаратно-программными устройствами или программами**, которые **регулируют поток сетевого трафика** между сетями или хостами, имеющими **разные требования к безопасности**. Большинство межсетевых экранов расположено на границы сетевого периметра, и в первую очередь они предназначены для защиты внутренних хостов от внешних атак.
- Однако **атаки могут также начинаться и с хостов, расположенных в локальной сети**, при этом они могут не проходить через межсетевые экраны на границе сетевого периметра. Поэтому в настоящее время межсетевые экраны размещают не только на границы сетевого периметра, но и **между различными сегментами сети**. Это обеспечивает дополнительный уровень безопасности.

Основные принципы использования межсетевых экранов

- Межсетевые экраны **пропускают или запрещают трафик, сравнивая его характеристики с шаблонами, заданными в политике межсетевого экрана**.
- Возможности фильтрования, выполняемого межсетевыми экранами, с начала 90-х годов существенно увеличились. Чаще всего возможности межсетевых экранов сравнивают **по количеству уровней в стеке TCP/IP**, которые они могут анализировать.
- Кроме этого, межсетевые экраны можно сравнивать **по возможностям совместного функционирования с другими инструментальными средствами**, такими как системы обнаружения проникновений и сканеры содержимого e-mail или веб с целью нахождения вирусов или опасного прикладного кода. Использование исключительно только межсетевых экранов не обеспечивает полной защиты от всех проблем, порожденных интернетом. Как результат, межсетевые экраны являются только одной из частей архитектуры информационной безопасности.

Основные принципы использования межсетевых экранов

- Для обеспечения максимально эффективной работы межсетевых экранов следует придерживаться следующих принципов:

Определить все требования, которые накладывает внешнее окружение на функционирование межсетевого экрана.

- Необходимо определить топологию защищаемой сети, используемые транспортные протоколы (IPv4 или IPv6) и специфику защищаемых сервисов и типы технологий межсетевых экранов, которые наиболее эффективны в данном случае. Также следует помнить о производительности и об интеграции межсетевого экрана в существующую сетевую инфраструктуру и инфраструктуру безопасности. Необходимо учитывать требования к физическому окружению и к квалификации персонала, а также требования, которые могут возникнуть в дальнейшем, такие как переход на технологии IPv6 или внедрение VPN.

Основные принципы использования межсетевых экранов

Создать политику межсетевого экрана, в которой определено, как следует обрабатывать входящий и исходящий трафик.

- Необходимо выполнить анализ рисков и определить при каких условиях какому типу трафика разрешено проходить через межсетевой экран. Обычно весь входящий и исходящий трафик, который явно не разрешен политикой межсетевого экрана, должен быть запрещен. Это снижает риск атак и может уменьшить объем трафика в сети. В политике должно быть определено, как межсетевой экран обрабатывает входящий и исходящий трафик для конкретных IP-адресов, диапазонов адресов, протоколов, приложений и типов содержимого.

Основные принципы использования межсетевых экранов

Разработать набор правил межсетевого экрана, которые реализуют политику безопасности в организации и обеспечивают максимальную производительность межсетевого экрана. Проанализировать производительность межсетевого экрана.

- Набор политик должен максимально эффективно обрабатывать трафик. При создании набора правил следует определить типы разрешенного трафика, включая протоколы, которые необходимы для управления самим межсетевым экраном. Детали создания набора правил зависят от типа межсетевого экрана и конкретного производителя, но часто производительность межсетевого экрана зависит от оптимизации набора правил. Например, большинство межсетевых экранов последовательно сравнивают трафик с правилами до тех пор, пока не будет найдено соответствие. Для таких межсетевых экранов правила, которые чаще всего будут соответствовать шаблонам трафика, должны быть размещены вверху списка.

Основные принципы использования межсетевых экранов

Управлять архитектурой, политиками, ПО и другими компонентами межсетевого экран следует в течение всего времени его функционирования.

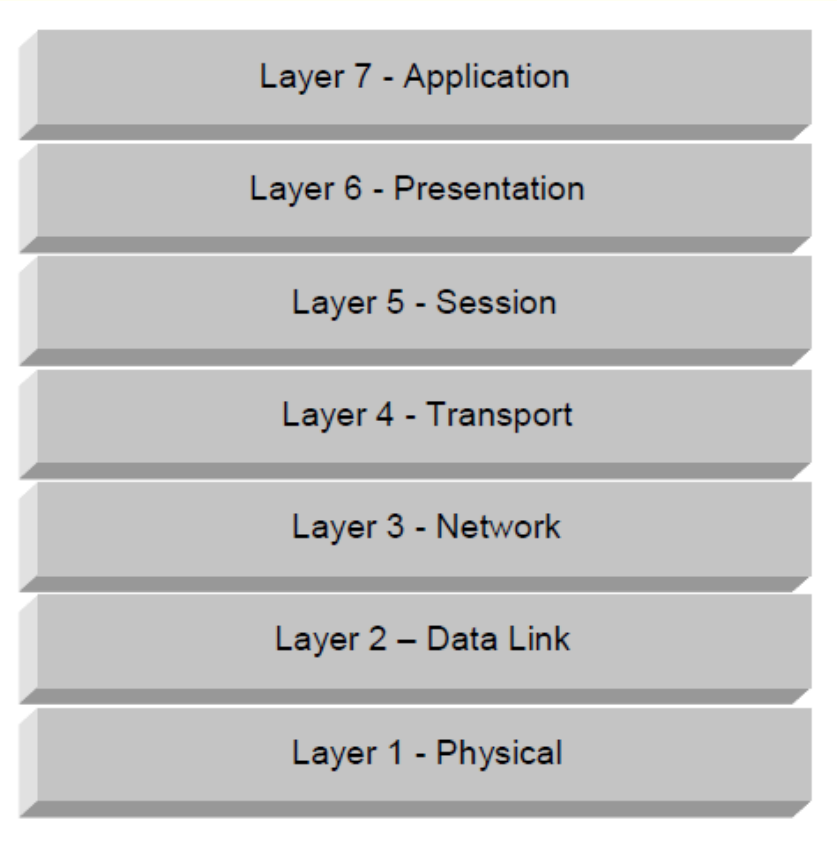
Существует много аспектов, касающихся управления межсетевым экраном. Например, выбор одного или нескольких типов межсетевых экранов и их расположение в сети может существенно влиять на политику безопасности, которую смогут реализовывать эти межсетевые экраны. При изменении требований в организации может потребоваться изменить набор правил, чтобы в сети могли функционировать новые приложения или хосты. Необходимо также следить за производительностью компонент межсетевого экрана, чтобы потенциальные проблемы с ресурсами были своевременно определены. Также должны постоянно просматриваться логи и оповещения для определения угроз, как осуществленных, так и не осуществленных.

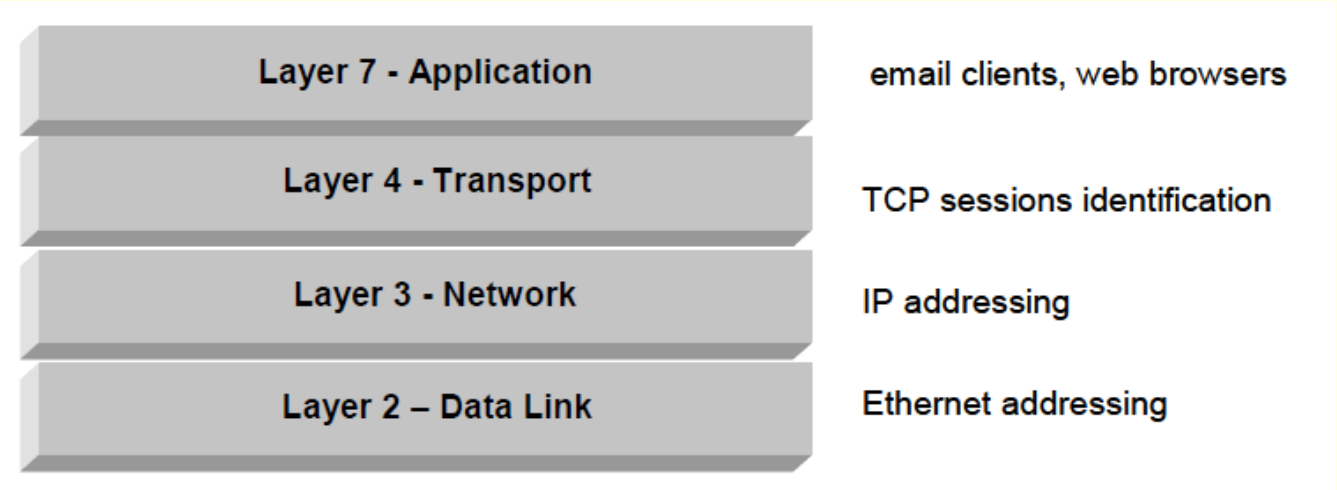
Технологии межсетевых экранов

Стек протоколов TCP/IP состоит из четырех уровней.

Уровень стека протоколов	**Примеры протоколов**
Прикладной уровень	Обеспечивает взаимодействие пользовательских приложений с сетью. Протоколы: HTTP, FTP, TFTP. DNS, SMTP, Telnet, SNMP и т.п.
Транспортный уровень	Обеспечивает передачу данных и коррекцию ошибок. Протоколы: TCP, UDP и т.п.
Сетевой уровень	Выполняет адресацию и маршрутизацию. Протоколы: IP, OSPF, ICMP, IGMP и т.п.
Канальный уровень	Упаковывает данные в стандартные кадры для передачи через физический уровень и обеспечивает проверку и коррекцию ошибок. Протоколы: Ethernet, PPP и т.п. На этом уровне работает ARP.

Стек протоколов





Стек протоколов

- **Канальный уровень** (также называемый **Data Link** уровень) обеспечивает взаимодействие компонентов физической сети. Канальный уровень представляет собой реальную аппаратуру физического соединения и физическую среду, такую как Ethernet. Это уровень, который обычно называется локальной сетью или LAN. Это первый уровень, обладающей возможностью адресации, с помощью которой можно идентифицировать отдельный хост. Адреса назначаются на сетевые интерфейсы и называются MAC (Media Access Control) адресами. Ethernet-адрес, принадлежащий Ethernet-карте, является примером MAC-адреса. Межсетевые экраны редко имеют дело с данными на этом уровне. Блок данных, передаваемый на канальном уровне, называют кадром.

Стек протоколов

- **Сетевой уровень** (также называемый **IP-уровнем**) маршрутизирует пакеты между локальными сетями. IPv4 является основным протоколом сетевого уровня для TCP/IP. Другими часто используемыми протоколами сетевого уровня являются IPv6 и IGMP. Данный уровень отвечает за доставку пакетов между отдельными локальными сетями, соединенными маршрутизаторами. Такие сети часто обозначаются WAN (Wide Area Network). Адреса данного уровня называются IP-адресами; они обычно являются уникальными, но при определенных обстоятельствах, например, при трансляции сетевых адресов (Network Address Translation – NAT), возможны ситуации, когда различные физические системы имеют один и тот же IP-адрес. Блок данных, передаваемый на сетевом уровне, называют дейтаграммой.

Стек протоколов

- **Транспортный уровень** предоставляет сервисы, ориентированные на соединение, которые используются для передачи данных между сетями. Часть протоколов (а именно TCP) могут гарантировать надежность соединения. Примерами протоколов транспортного уровня являются TCP и UDP. На транспортном уровне возникает понятие *сессии* как потока данных между двумя приложениями. Для сессии определено понятие *портов*, которые являются конечными точками сессии: номер порта *источника* определяет конечную точку коммуникационной сессии на исходной системе; номер порта *назначения* определяет конечную точку коммуникационной сессии на системе назначения. Хост может иметь с другими хостами практически любое число сессий на транспортном уровне.

Стек протоколов

- **Прикладной уровень** посылает и получает данные конкретных приложений, таких как DNS, HTTP, SMTP. Прикладной уровень сам может состоять из нескольких подуровней. Например, SMTP или HTTP могут инкапсулировать другие форматы, такие как HTML.

Межсетевые экраны анализируют данные одного или нескольких уровней. Считается, что чем больше уровней анализирует межсетевой экран, тем более совершенным и эффективным он является. Чем большее число уровней может быть проанализировано, тем более точная и тщательная проверка может быть выполнена. Межсетевые экраны, которые понимают прикладной уровень, потенциально могут анализировать уязвимости на уровне приложения и предоставлять сервисы, ориентированные на конечного пользователя, например, выполнять аутентификацию пользователя и записывать в логи события, касающиеся конкретного пользователя.

Стек протоколов

- Независимо от архитектуры, межсетевой экран может **предоставлять дополнительные сервисы**. Эти сервисы включают трансляцию сетевых адресов (NAT), поддержку протокола динамической конфигурации хоста (DHCP), функции шифрования, тем самым являясь конечной точкой VPN-шлюза.
- Многие межсетевые экраны также включают различные технологии фильтрации так называемого **активного содержимого**. Содержимое называется активным, потому что оно является кодом, который может быть выполнен на конечной системе. Например, при использовании таких технологий может быть выполнено сканирование файлов на наличие вирусов. Межсетевые экраны также применяются для фильтрации наиболее опасного активного содержимого, такого как Java, JavaScript и ActiveX. Или они могут быть использованы для фильтрации содержимого, соответствующего определенному образцу, или поиска ключевых слов с целью ограничения доступа к запрещенным сайтам или доменам.

Состояния TCP-соединения

- **IP-протокол** обеспечивает **способ адресации источника и получателя**. IP-протокол также имеет дело с **фрагментацией** и **реассемблированием пакетов**, которые затем передаются на транспортный уровень.
- **TCP является надежным протоколом** в сетях, основанных на коммутации пакетов, обеспечивая гарантированную доставку пакетов. Так как пакетные фильтры анализируют параметры TCP-протокола, рассмотрим подробно этот протокол.
- Каждый октет данных, передаваемый по соединению, имеет последовательный номер. В пакете указывается номер первого передаваемого октета. Пакет также содержит номер октета, который был получен отправителем данного пакета. При отправке пакет на стороне отправителя не отбрасывается, а помещается в очередь для возможной повторной передачи, если в течение определенного времени не будет получено подтверждение от противоположной стороны о получении данного пакета. Если подтверждение не получено при истечении этого времени, пакет передается повторно. Тем самым обеспечивается надежность соединения, т.е. гарантирование того, что все пакеты будут доставлены получателю.

Состояния TCP-соединения

- Для идентификации начальной и конечной точек TCP-соединения вводится понятие **номера порта**. Номера портов выбираются независимо для каждого TCP-соединения, при этом они не обязательно должны быть уникальными. **Пара (IP-адрес, порт) называется сокетом**.
- Каждый конец TCP-соединения является **либо клиентом, либо сервером**. **Соединение инициируется клиентом**. Сервер ждет установления соединения от клиента, в этом случае говорят, что сервер слушает порт. TCP-соединение может быть открыто либо в пассивном – сервером, либо в активном режиме – клиентом.
- Сервер может использовать любые номера портов. Тем не менее определены некоторые базовые принципы назначения номеров портов. **Существуют «хорошо известные» номера портов**, которые обычно соответствуют определенным приложениям. При инициализации TCP-сессии на стороне клиента открывается порт, номер которого в соответствии со спецификацией протокола TCP должен быть в диапазоне от 1023 до 65535. **Номер порта на стороне клиента может быть каждый раз разным**.

Состояния TCP-соединения

- Приложение, которое хочет предоставлять сервис, доступный по сети другим приложениям, открывает порт в пассивном режиме. Для получения сервиса приложение, называемое клиентом, должно открыть порт в активном режиме и инициировать создание соединения с сервером.
- Установление TCP-соединения происходит с использованием так называемого **«тройного рукопожатия»**. Соединение инициирует клиент, посылая пакет с установленным битом **`SYN`**. Сервер отвечает клиенту пакетом с установленными битами **`SYN`** и **`ACK`**. Сервер также передает начальный порядковый номер в поле **`Sequence Number`**. Наконец, клиент посылает серверу сообщение с установленным битом **`ACK`**, в поле **`Sequence Number`** указывает свой начальный номер, в поле **`Acknowledgement Number`** указывает полученный от сервера начальный порядковый номер, увеличенный на единицу.

Состояния TCP-соединения

В течение своего жизненного цикла соединение проходит через несколько состояний.

Состояния на стороне клиента:	Состояния на стороне сервера:
CLOSED	CLOSED
SYN-SENT	LISTEN
ESTABLISHED	SYN-RESEIVED
FIN-WAIT-1	ESTABLISHED
CLOSE-WAIT	FIN-WAIT-1
FIN-WAIT-2	CLOSE-WAIT
CLOSING	FIN-WAIT-2
LAST-ACK	CLOSING
CLOSED	TIME-WAIT
	CLOSED

Состояния TCP-соединения

- Состояние **CLOSED** является фиктивным, потому что оно представляет собой состояние, для которого не существует структур данных на стороне клиента и сервера, и, следовательно, не может существовать соединения.
- **LISTEN** – состояние сервера, в котором он ожидает запрос от клиента на создание соединения.
- **SYN-SENT** – состояние клиента, в котором он ожидает ответа от сервера после посылки запроса на создание соединения.
- **SYN-RECEIVED** – состояние сервера, в котором он ожидает подтверждения после того, как и клиент, и сервер получили и послали запрос на создание соединения.
- **ESTABLISHED** – состояние как клиента, так и сервера, которое представляет собой открытое соединение: полученные данные доставляются на прикладной уровень. Обычное состояние при пересылке данных по соединению.

Состояния TCP-соединения

Инициатором закрытия соединения может быть как клиент, так и сервер.

- **FIN-WAIT-1** – состояние инициатора закрытия соединения, при котором данной стороной был послан пакет с флагом **FIN**. Инициатор закрытия соединения ожидает подтверждения на запрос закрытия.
- **CLOSE-WAIT** – состояние отвечающей стороны закрытия соединения, при котором было послано подтверждение **ACK** на запрос закрытия (**FIN**). При этом канал становится симплексным: передача возможна только в одном направлении – от отвечающей стороны закрытия соединения, т.е. от того, кто послал подтверждение **ACK**.
- **FIN-WAIT-2** – состояние инициатора закрытия соединения, при котором было получено подтверждение **ACK** запроса закрытия соединения от удаленной стороны. После этого данная сторона ждет получения пакета с установленным флагом **FIN**. При получении пакета с флагом **FIN** канал считается окончательно разрушенным.

Состояния TCP-соединения

- **LAST-ACK** – состояние отвечающей стороны закрытия соединения, при котором послано подтверждение (пакет с установленным флагом **FIN**) завершения соединения, ранее посланного удаленной стороне.
- **CLOSING** – обе стороны инициировали закрытие соединения одновременно: после отправки пакета с флагом **FIN** инициатор закрытия получает пакет с флагом **FIN**.
- **TIME-WAIT** – представляет собой ожидание в течение определенного времени, чтобы быть уверенным, что удаленная сторона получила подтверждение запроса на закрытие соединения.
- TCP-соединение переходит из одного состояния в другое в результате возникновения событий. Событиями являются вызовы функций **OPEN**, **SEND**, **RECEIVE**, **CLOSE**, **ABORT** и **STATUS**, входящие пакеты, содержащие флаги **SYN**, **ACK**, **RST** и **FIN**, а также таймауты.

Классификация межсетевых экранов

Межсетевое экранирование часто совмещают с **другими технологиями**:

- Маршрутизация (ACL)
- **NAT**
- Другие политики организации (не только безопасность)
- IDS

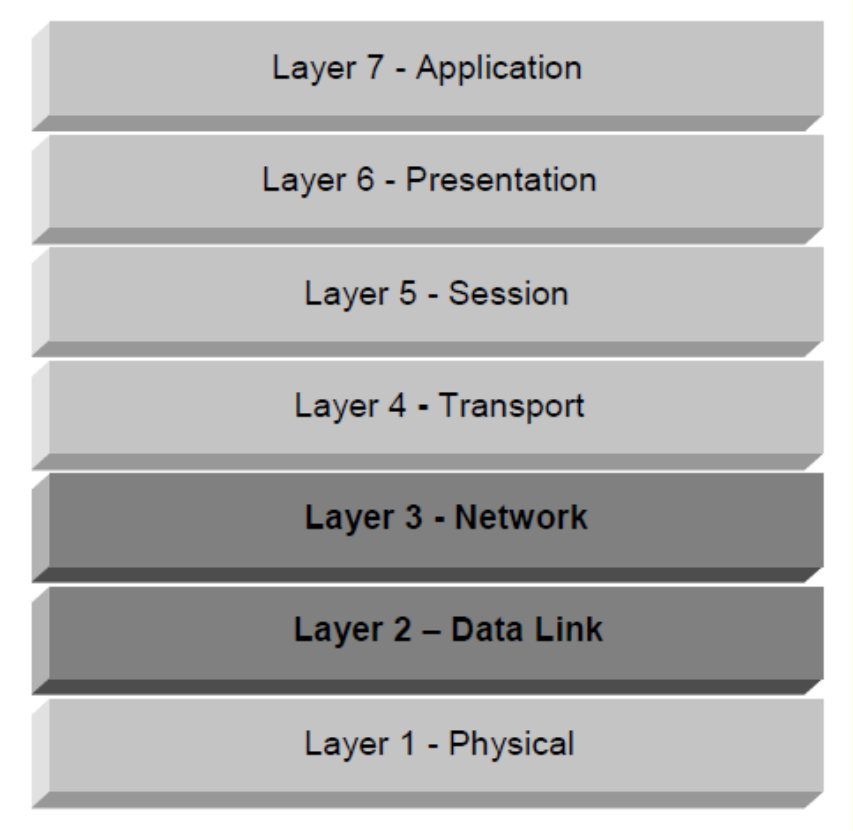
Если МСЭ на границе сетевого периметра:

- **внешний** интерфейс
- **внутренний** интерфейс

Фильтрование пакетов

Межсетевые экраны **без анализа состояния**
Управление трафиком определяется **упорядоченным** набором директив, которые называются **ruleset**.

- **IP-адрес источника** в пакете – адрес хоста, с которого пришел пакет.
- **IP-адрес получателя** в пакете – адрес хоста, которому предназначен пакет.
- **Транспортный протокол**, используемый для взаимодействия хостов отправителя и получателя, такой как TCP, UDP или ICMP.
- Некоторые характеристики коммуникационной сессии транспортного уровня, такие как **порты источника и получателя**, отдельные флаги сессии (наличие **SYN**, отсутствие **ACK**).
- **Интерфейс**, через который проходит пакет, и направление (**входящий** или **исходящий**).



Фильтрование пакетов

Для пакетов, которые соответствуют правилу, выполняется одно из следующих действий (action):

- **`Accept`** (**`FwdFast, pass, permit, accept`**): пакет пропускается через МСЭ, в зависимости от настроек могут выполняться дополнительные действия (создание логов, преобразование NAT и т.п.)
- **`Drop`** (**`Discard`**): пакет отбрасывается, никакого ответа отправителю не посылается. Данное действие используется для реализации методики «черной дыры»
- **`Deny`** (**`Reject`**): пакет отбрасывается, отправителю посылается ICMP-сообщение об ошибке

Фильтрование пакетов

- Базовой возможностью межсетевого экрана является ***фильтрование пакетов***. Первоначально межсетевые экраны были частью маршрутизаторов, обеспечивая управление доступом на основе адресов хостов и коммуникационных сессий. Эти устройства, также называемые *межсетевыми экранами без анализа состояния*, не поддерживали информацию о состоянии потока трафика, который проходит через межсетевой экран. Это означает, что они не могут определить, что несколько запросов принадлежат одной сессии. Фильтрование пакетов является основой большинства современных межсетевых экранов, хотя осталось немного пакетных фильтров, которые выполняют фильтрование без поддержки состояния. В отличие от более мощных фильтров, пакетные фильтры анализируют только заголовки сетевого и транспортного уровней, а не содержимое пакетов. Управление трафиком определяется набором директив, которые называются ***ruleset***. Возможности фильтрования пакетов встроены в большинство ОС и устройств, выполняющих маршрутизацию. Самым типичным примером является маршрутизатор, в котором определены списки управления доступом.

Фильтрование пакетов

Управление трафиком осуществляется на основе анализа следующей информации, содержащейся в пакете:

- IP-адрес источника в пакете – адрес хоста, с которого пришел пакет.
- IP-адрес получателя в пакете – адрес хоста, которому предназначен пакет.
- Транспортный протокол, используемый для взаимодействия хостов отправителя и получателя, такой как TCP, UDP или ICMP.
- Возможно некоторые характеристики коммуникационной сессии транспортного уровня, такие как порты источника и получателя (например, TCP 80 для порта получателя и TCP 1320 для порта источника).
- Интерфейс, через который проходит пакет, и направление (входящий или исходящий).

Фильтрование пакетов

- Фильтрование *входящего трафика* еще называют *входящим фильтрованием*. *Исходящий трафик* также может фильтроваться, этот процесс называется *исходящим фильтрованием*. Исходящее фильтрование дает возможность ограничить внутренний трафик, например, блокируя использование внешних FTP-серверов или предотвращая атаки, которые могут запускаться изнутри на внешние цели.
- **Фильтры пакетов без поддержки состояния уязвимы для атак**, связанных с особенностями TCP/IP. Например, многие такие пакетные фильтры не могут определить, что **информация в сетевом адресе подделана или каким-то образом изменена**, или что присутствует комбинация параметров, разрешенная стандартами, но которая использует уязвимости в конкретном приложении или ОС. Атаки подделки, такие как использование некорректных адресов в заголовках пакетов, могут дать возможность атакующему обойти контроль, выполняемый межсетевым экраном. Межсетевые экраны, которые выполняются на более высоких уровнях, могут препятствовать некоторым атакам, связанным с подделкой адресов, проверяя, что сессия установлена, или аутентифицируя пользователей перед тем, как разрешить прохождение трафика. В силу этого большинство межсетевых экранов, которые реализуют фильтрацию пакетов, также поддерживают некоторую информацию о состоянии для пакетов, проходящих через межсетевой экран.

Фильтрование пакетов

- В некоторых случаях полезно **фильтровать фрагментированные пакеты**. Фрагментация пакетов допускается спецификациями TCP/IP и в некоторых ситуациях бывает необходима. Однако фрагментация пакетов делает определение некоторых атак более трудной, так как атака размещается во фрагментированных пакетах. Например, некоторые сетевые атаки используют пакеты, которые в нормальных ситуациях не могут появиться, например, посылая определенные фрагменты пакета, но не посылая первый фрагмент, или посылая фрагменты пакета, которые перекрывают друг друга. Чтобы предотвратить использование фрагментированных пакетов для выполнения атак, межсетевой экран можно сконфигурировать таким образом, чтобы блокировать фрагментированные пакеты.
- В настоящий момент фрагментированные пакеты часто появляются не потому, что являются атакой, а **вследствие использования технологий VPN**, которые инкапсулируют пакеты внутрь других пакетов. Если инкапсуляция пакета приводит к тому, что новый пакет превышает максимально допустимый размер, пакет будет фрагментирован.

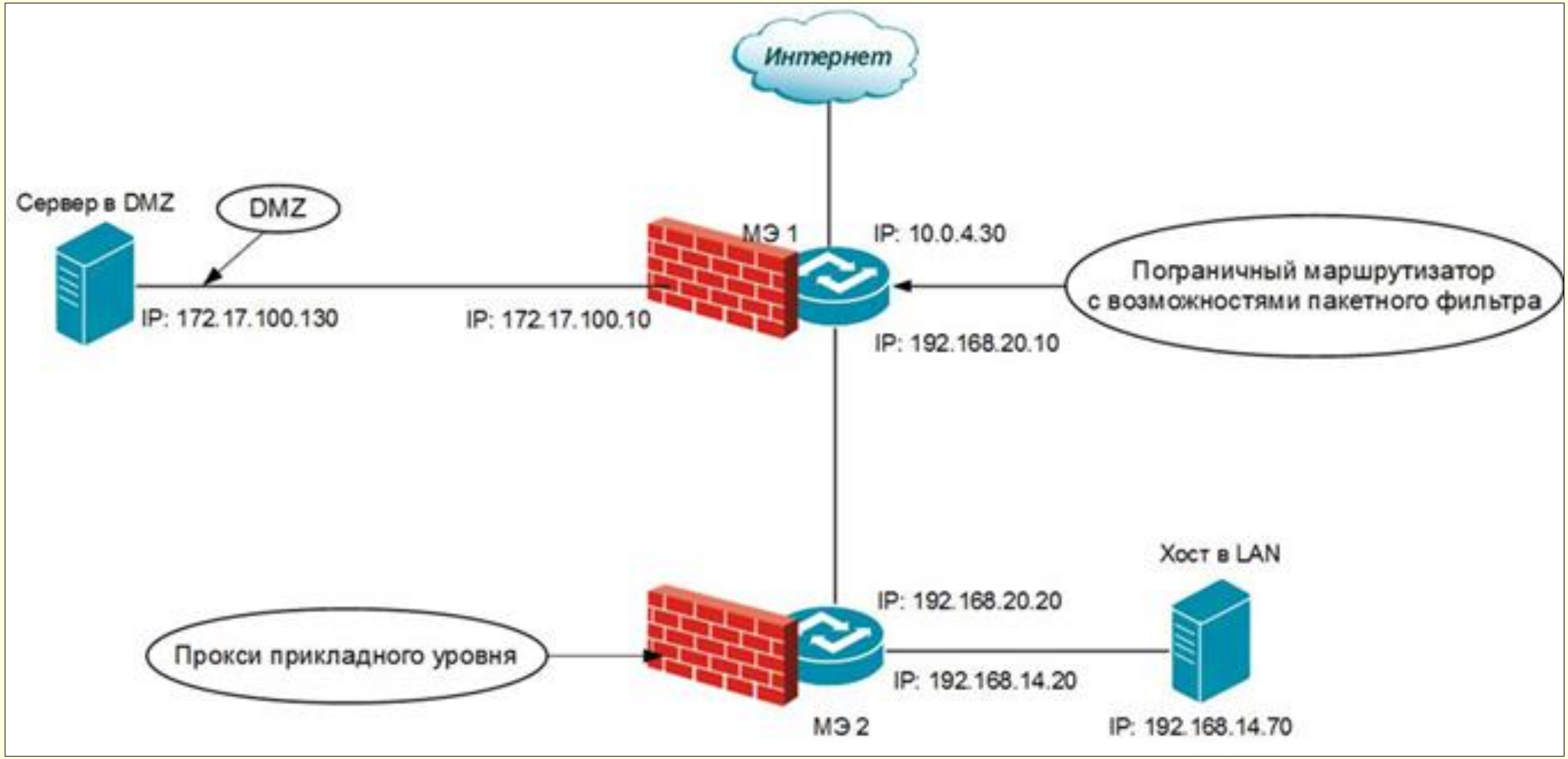
Фильтрование пакетов

- Фрагментированные пакеты, которые блокируются межсетевыми экранами, являются **типичной проблемой**, связанной с использованием VPN.
- Некоторые межсетевые экраны могут **дефрагментировать пакеты** перед тем, как пересылать их во внутреннюю сеть. Следует понимать, что это требует дополнительных ресурсов самого межсетевого экрана, особенно памяти. Такая функциональность должна использоваться очень обоснованно, иначе **межсетевой экран легко может стать объектом DoS-атаки**. Выбор того, что делать с фрагментированным пакетом: отбросить, реассемблировать или пропустить, должен являться компромиссом между необходимой интероперабельностью и полной безопасностью сети.

Фильтрование пакетов

- Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры:
  - Пограничные маршрутизаторы
  - ОС
  - Персональные межсетевые экраны
- Основным **преимуществом пакетных фильтров** является их **скорость**. Так как пакетные фильтры обычно проверяют данные только в заголовках сетевого и транспортного уровней, они могут выполнять это очень быстро. По этим причинам пакетные фильтры, встроенные в *пограничные маршрутизаторы*, идеальны для размещения на границе с сетью с невысокой степенью доверия. Пакетные фильтры, встроенные в пограничные маршрутизаторы, могут блокировать основные атаки, фильтруя нежелательные протоколы, выполняя простейший контроль доступа на уровне сессий и затем передавая трафик другим межсетевым экранам для проверки данных на более высоких уровнях стека протоколов.

Фильтрование пакетов



Фильтрование пакетов

- На рисунке показана топология сети, в которой пограничный маршрутизатор с возможностями пакетного фильтра используется в качестве первой линии обороны. Маршрутизатор принимает пакеты от недоверяемой сети, например, интернет, выполняет контроль доступа в соответствии со своей политикой, например, блокирует SNMP, разрешает HTTP и т.п. Затем он передает пакеты более мощному межсетевому экрану для дальнейшего управления доступом и фильтрования данных на более высоких уровнях стека протоколов. На рисунке также показана промежуточная сеть между пограничным маршрутизатором и внутреннем межсетевым экраном, называемая *DMZ-сетью*.
- Порт на стороне сервера имеет фиксированный номер. На стороне клиента открывается порт, номер которого может быть каждый раз разным.

Фильтрование пакетов

- В этом случае пакетный фильтр **должен разрешать входящий трафик** для всех таких **портов «с большими номерами»**, чтобы клиент, инициализировавший соединение, мог получать возвращаемые сервером пакеты. Открытие портов создает риск несанкционированного проникновения в локальную сеть.

Преимущества пакетных фильтров:

- Основным преимуществом пакетных фильтров является их **скорость**.
- Пакетный фильтр **прозрачен для клиентов и серверов**, так как не разрывает TCP-соединение.

Фильтрование пакетов

Недостатки пакетных фильтров:

- Так как пакетные фильтры не анализируют данные более высоких уровней, они **не могут предотвратить атаки**, которые используют уязвимости, **специфичные для приложения**. Например, пакетный фильтр не может блокировать конкретные команды приложения; если пакетный фильтр разрешает данный трафик для приложения, то все операции, определенные в данном приложении, будут разрешены.
- **В логах** пакетного фильтра содержится информация только о **параметрах сетевого и транспортного уровней**. Логи пакетного фильтра обычно содержат ту же информацию, которая использовалась при принятии решения о возможности доступа (адрес источника, адрес назначения, тип трафика и т.п.).
- Большинство пакетных фильтров **не поддерживают** возможность **аутентификации пользователя**. Данная возможность обеспечивается межсетевыми экранами, анализирующими более высокие уровни.

Фильтрование пакетов

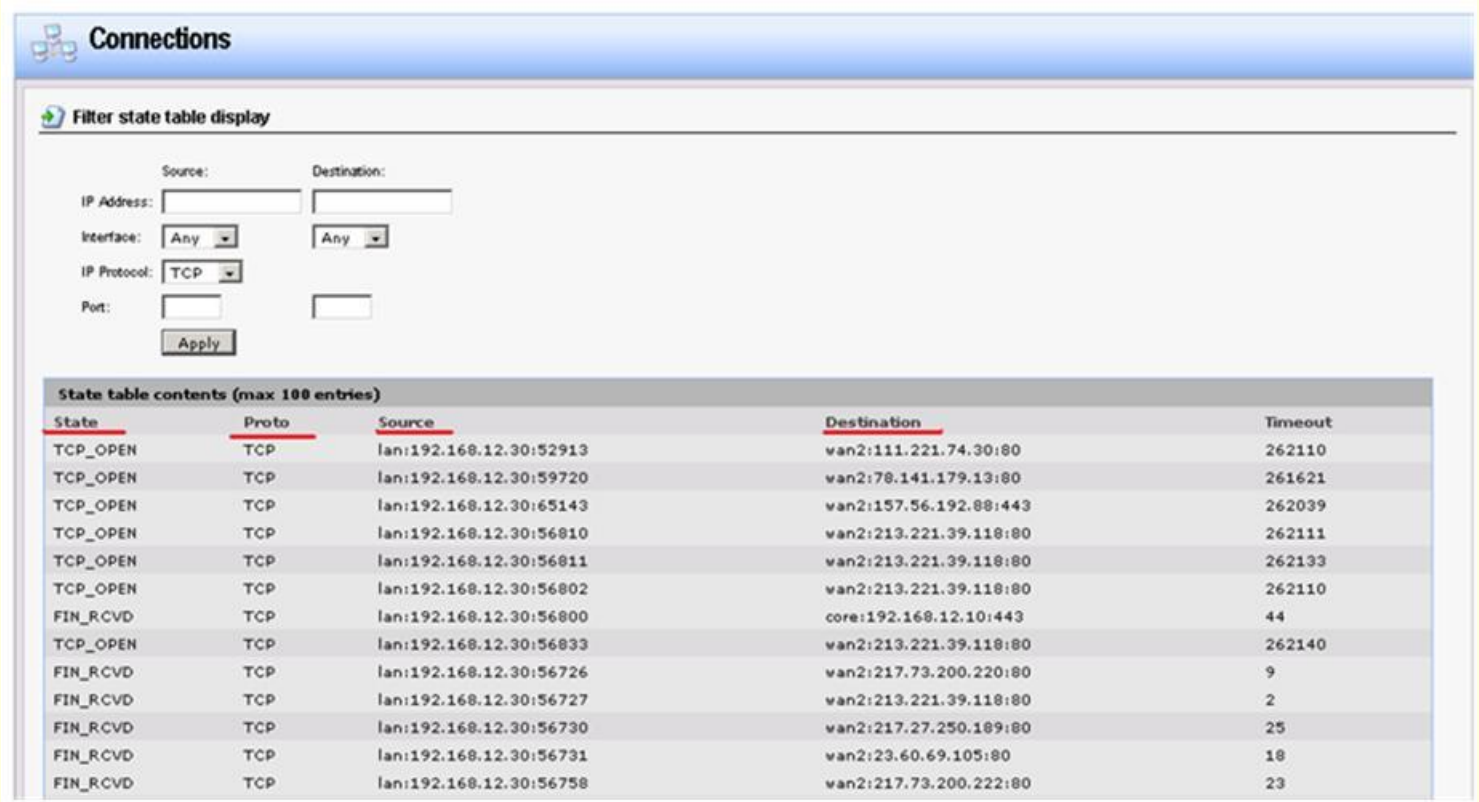
- Пакетные фильтры обычно **уязвимы для атак**, которые используют такие уязвимости TCP/IP, как **подделка (spoofing) сетевого адреса**. Многие пакетные фильтры не могут определить, что в сетевом пакете изменена адресная информация транспортного уровня. Spoofing-атаки обычно выполняются для обхода управления доступом, осуществляемого межсетевым экраном.
- Пакетные фильтры **трудно конфигурировать**. Можно случайно переконфигурировать пакетный фильтр для разрешения типов трафика, источников и назначений, которые должны быть запрещены.
- Так как номер порта клиента может быть любым, так называемым «большим номером» (с 1023 до 65535), то на межсетевом экране приходится **открывать все порты с номерами больше 1023**.

Фильтрование пакетов

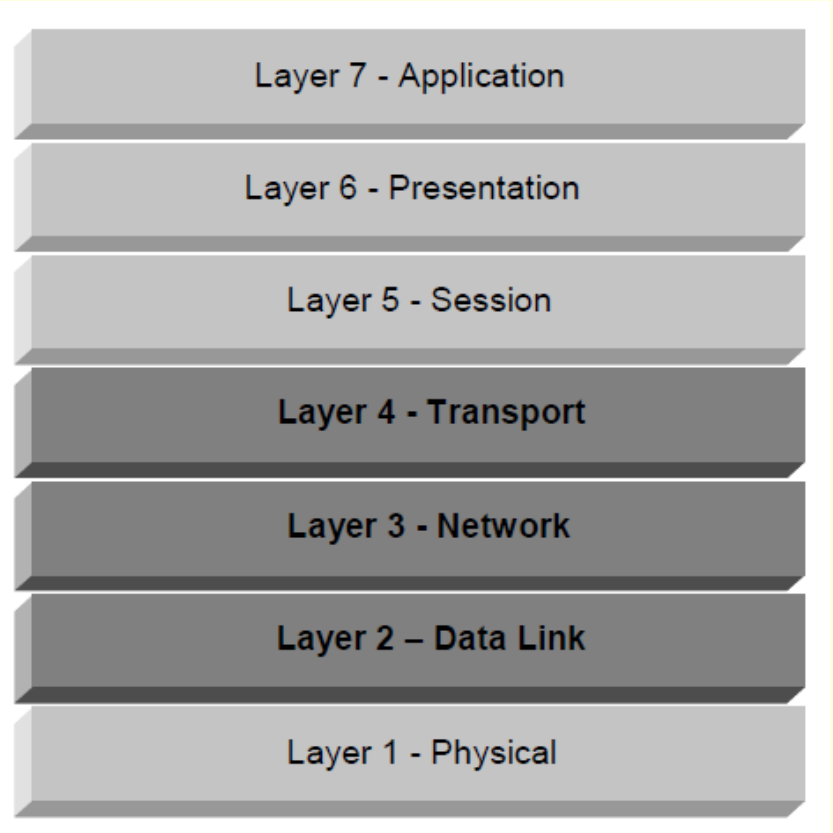
- Следовательно, пакетные фильтры больше всего подходят, если **требуется большая пропускная способность**, а создание подробных логов и аутентификация пользователя не столь важны.
- Практически все современные межсетевые экраны включают большее количество возможностей, сейчас трудно найти межсетевой экран, который имеет возможности только пакетного фильтра. Примером может являться маршрутизатор, осуществляющий проверку списка контроля доступа для управления сетевым трафиком. Высокая производительность пакетных фильтров также способствует тому, что они реализуются в устройствах, обеспечивающих высокую доступность и особую надежность; некоторые производители предлагают аппаратные и программные решения как высоко доступные, так и особо надежные. Также большинство SOHO (Small Office Home Office) устройств межсетевых экранов и межсетевых экранов, встроенных по умолчанию в ОС, предоставляют возможности пакетных фильтров.

Пакетные фильтры с анализом состояния

- Добавляет возможность отслеживания состояния соединения и блокировку пакетов, которые не соответствуют ожидаемому состоянию (анализ данных транспортного уровня) - **таблица состояний**



State	Proto	Source	Destination	Timeout
TCP_OPEN	TCP	lan:192.168.12.30:52913	wan2:111.221.74.30:80	262110
TCP_OPEN	TCP	lan:192.168.12.30:59720	wan2:78.141.179.13:80	261621
TCP_OPEN	TCP	lan:192.168.12.30:65143	wan2:157.56.192.88:443	262039
TCP_OPEN	TCP	lan:192.168.12.30:56810	wan2:213.221.39.118:80	262111
TCP_OPEN	TCP	lan:192.168.12.30:56811	wan2:213.221.39.118:80	262133
TCP_OPEN	TCP	lan:192.168.12.30:56802	wan2:213.221.39.118:80	262110
FIN_RCVD	TCP	lan:192.168.12.30:56800	core:192.168.12.10:443	44
TCP_OPEN	TCP	lan:192.168.12.30:56833	wan2:213.221.39.118:80	262140
FIN_RCVD	TCP	lan:192.168.12.30:56726	wan2:217.73.200.220:80	9
FIN_RCVD	TCP	lan:192.168.12.30:56727	wan2:213.221.39.118:80	2
FIN_RCVD	TCP	lan:192.168.12.30:56730	wan2:217.27.250.189:80	25
FIN_RCVD	TCP	lan:192.168.12.30:56731	wan2:23.60.69.105:80	18
FIN_RCVD	TCP	lan:192.168.12.30:56758	wan2:217.73.200.222:80	23



Пакетные фильтры с анализом состояния

- Анализ состояния **добавляет возможность отслеживания состояния соединения и блокировку пакетов, которые не соответствуют ожидаемому состоянию**. Для этого выполняется анализ данных **транспортного** уровня. Также как и при простом фильтровании пакетов межсетевой экран анализирует содержимое сетевого уровня на соответствие правилам. Но в отличие от фильтрации пакетов, инспекция состояния **отслеживает историю каждого соединения**, используя для этого таблицу состояний. Хотя детали записей таблицы состояний во многом зависят от конкретной реализации межсетевого экрана, обычно они содержат IP-адрес источника, IP-адрес получателя и информацию о состоянии соединения.
- В TCP-протоколе существуют **три** основных состояния – **соединение устанавливается, используется и завершается**. Причем в последнем случае любая из конечных точек может запросить завершение соединения. При анализе состояния межсетевой экран проверяет определенные значения в TCP-заголовках. Для каждого полученного пакета ищется запись в таблице состояний и определяется, что флаги в заголовках пакета соответствует ожидаемому состоянию. Например, атакующий может создать пакет, в заголовке которого указано, что он является частью установленного соединения, в надежде, что он пройдет через межсетевой экран. Если межсетевой экран использует анализ состояний, то он поймет, что пакет не является частью установленного соединения, так как в таблице отсутствует соответствующая запись, и отбросит такой пакет.

Пакетные фильтры с анализом состояния

- В простейшем случае межсетевой экран пропускает любой пакет, если он считает, что пакет является частью открытого соединения (или соединения, которое еще не полностью установлено). Многие межсетевые экраны точно могут определить состояние таких протоколов, как TCP и UDP, и они могут блокировать пакеты, которые не соответствуют состоянию протокола. Например, часто межсетевой экран проверяет такие параметры, как последовательные номера TCP, и отбрасывает пакеты, номера которых вне ожидаемого диапазона. Если межсетевой экран предоставляет сервис NAT, то информация NAT часто также содержится в таблице состояний.

Пакетные фильтры с анализом состояния

- Так как некоторые протоколы, в частности UDP, не поддерживают состояния, и для них не существует инициализации, установления и завершения соединения, то для них невозможно определить состояние на транспортном уровне как для TCP. Для этих протоколов межсетевые экраны с поддержкой состояния имеют возможность только отслеживать IP-адреса и порты источника и получателя. Так, например, ответ DNS от внешнего источника будет пропускаться только в том случае, если межсетевой экран до этого видел соответствующий DNS-запрос от внутреннего хоста. Так как межсетевой экран не имеет возможности определить завершение сессии, запись удаляется из таблицы состояний после заранее сконфигурированного таймаута. Межсетевые экраны прикладного уровня, которые умеют распознавать DNS поверх UDP, завершают сессию после того, как получен DNS-ответ.

Пакетные фильтры с анализом состояния

- В сущности, межсетевые экраны с анализом состояния добавляют в пакетный фильтр понимание логики протокола транспортного уровня. Межсетевые экраны с анализом состояния разделяют сильные и слабые стороны пакетных фильтров, но всё же межсетевые экраны с анализом состояния обычно считаются более безопасными, чем пакетные фильтры.

  Преимущества межсетевых экранов с анализом состояния:

- Разрешают прохождение пакетов только для установленных соединений;
- Прозрачны для клиентов и серверов, так как не разрывают TCP-соединение.

  Недостатки межсетевых экранов с анализом состояния:

- Реально используются только в сетевой инфраструктуре TCP/IP. Хотя надо отметить, что межсетевые экраны с анализом состояния можно реализовать в других сетевых протоколах тем же способом, что и пакетные фильтры.

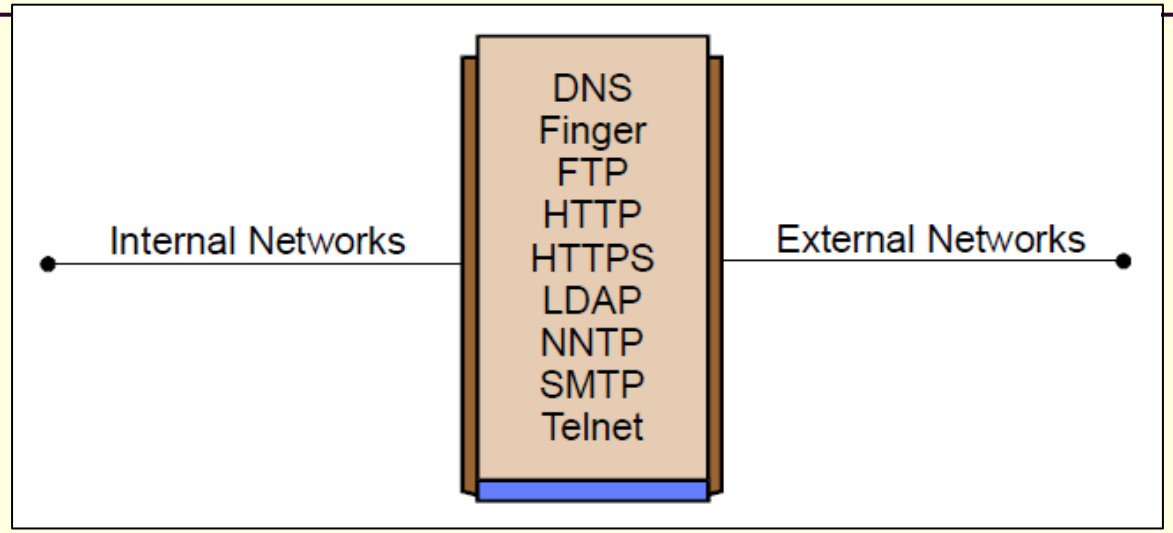
Пакетные фильтры с анализом состояния

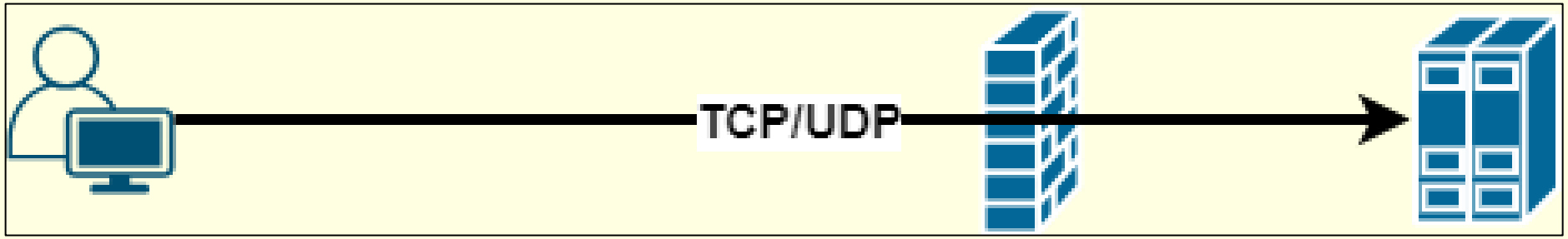
Правила пакетного фильтра с анализом состояний

Межсетевые экраны прикладного уровня

- Современная тенденция анализа состояний состоит в добавлении возможностей *анализа состояний протокола*, которое некоторыми производителя называется *глубоким анализом пакета* (*deep packet inspection*). Анализ состояния протокола добавляет в стандартный анализ состояния базовую технологию обнаружения вторжения, которая анализирует протокол на прикладном уровне, сравнивая поведение протокола с определенными производителем профилями и определяя отклонения в поведении. Это позволяет межсетевому экрану разрешать или запрещать доступ, основываясь на том, как выполняется приложение. Например, межсетевой экран прикладного уровня может определить, что почтовое сообщение содержит неразрешенный тип присоединенного файла (такой как выполняемый файл). Другая возможность состоит в том, что он может блокировать соединения, в которых выполняются определенные действия (например, присутствуют команды **`put`** в FTP). Данная возможность также позволяет разрешать или запрещать передавать веб-страницы в зависимости от конкретных типов содержимого, такого как Java или ActiveX, или проверять, что TLS-сертификаты подписаны конкретным CA.

Межсетевые экраны прикладного уровня





Межсетевые экраны прикладного уровня

- Межсетевые экраны прикладного уровня могут предоставлять возможность определять **нежелательную последовательность команд**, такую как некоторые повторяющиеся команды или команда, которой не предшествует другая команда, от которой зависит данная команда. Такие подозрительные команды часто означают атаки переполнения буфера, DoS-атаки или другие атаки, связанные с прикладными протоколами, таким как HTTP.
- Другая возможность состоит в проверке входных данных для отдельных команд, такой как **минимальная и максимальная длина аргументов**. Например, аргумент имени пользователя длиной в 1000 символов является подозрительным или если он содержит бинарные данные. Межсетевые экраны прикладного уровня доступны для многих протоколов, включая HTTP, БД (SQL), почтовые (SMTP, POP, IMAP), VoIP и XML.

Межсетевые экраны прикладного уровня

- Другая возможность, которая встречается в некоторых межсетевых экранах прикладного уровня, состоит в **отслеживании состояний приложения**, при этом проверяется, что **трафик соответствует шаблонам, определенным в спецификациях протокола**.
- Межсетевые экраны с возможностями анализа состояний и анализа состояний протокола не являются полной заменой IDPS, которые обычно имеют более обширные возможности определения проникновения. Например, IDPS используют сигнатурный и аномальный анализ для определения проблем, связанных с сетевым трафиком.

Преимущества межсетевых экранов прикладного уровня:

- Межсетевой экран прикладного уровня имеет возможность выполнять **аутентификацию пользователя**. Часто существует возможность указывать тип аутентификации, который считается необходимым для данной инфраструктуры.
- Благодаря возможности аутентифицировать пользователя они считаются **менее уязвимыми для атак подделки адреса**.

Межсетевые экраны прикладного уровня

- Межсетевые экраны прикладного уровня обычно имеют больше возможностей **анализировать весь сетевой пакет**, а не только сетевые адреса и номера портов. Например, они могут определять команды и данные, специфичные для каждого приложения.
- Как правило, межсетевые экраны прикладного уровня создают **более подробные логи**.

Недостатки межсетевых экранов прикладного уровня:

- Так как межсетевые экраны прикладного уровня «знают о пакете все», межсетевой экран вынужден тратить много времени на анализ каждого пакета. По этой причине они обычно **не подходят** для приложений, которым необходима **высокая пропускная способность**, или **приложений реального времени**. Чтобы уменьшить нагрузку на межсетевой экран, можно использовать выделенный прокси-сервер для обеспечения безопасности менее чувствительных ко времени сервисов, таких как e-mail и большинство веб-трафика.

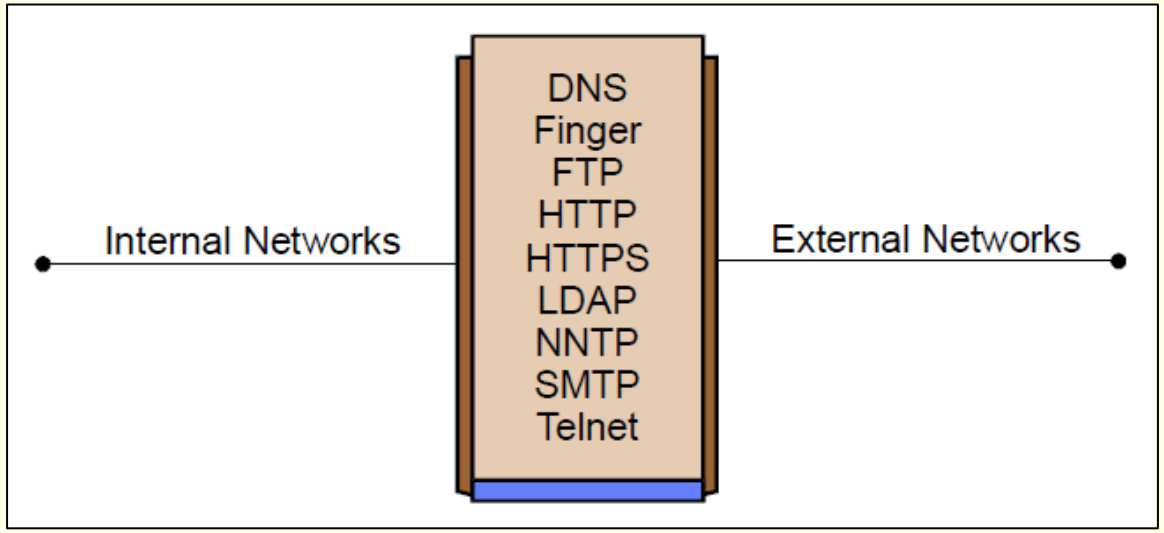
Межсетевые экраны прикладного уровня

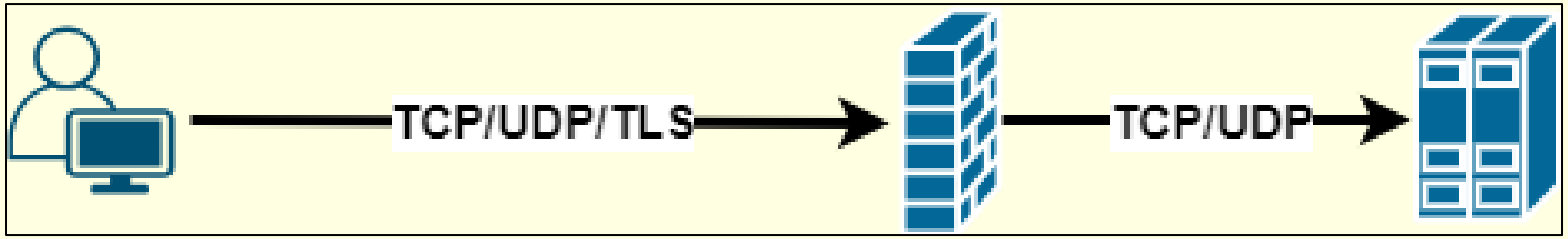
- Другим недостатком является то, что они обрабатывают **ограниченное количество сетевых приложений и протоколов** и не могут автоматически поддерживать новые сетевые приложения и протоколы. Для каждого прикладного протокола, который должен проходить через межсетевой экран, необходим **свой агент**. Большинство производителей предоставляют общих агентов для поддержки неизвестных сетевых приложений или протоколов. Однако эти общие агенты не имеют большинства преимуществ межсетевых экранов прикладного уровня: как правило, они просто туннелируют трафик через межсетевой экран.

Прокси-шлюзы прикладного уровня

- *Прокси-шлюзы прикладного уровня* являются межсетевыми экранами, которые **комбинируют управление доступом на нижнем уровне с функциональностью верхнего уровня**. Эти межсетевые экраны имеют прокси-агента, действующего как посредник между двумя хостами, которые хотят взаимодействовать друг с другом, и никогда не допускает прямого взаимодействия между ними. Результатом успешной попытки установления соединения является **создание двух отдельных соединений – одно между клиентом и прокси-агентом, другое – между прокси-агентом и реальным сервером**. Так как внешние хосты взаимодействуют только с прокси-агентом, внутренние IP-адреса не видны вовне. Прокси-агент использует набор правил межсетевого экрана, чтобы определить, что данному сетевому трафику разрешено проходить через межсетевой экран.
- В дополнение к набору правил некоторые прокси-агенты могут выполнять аутентификацию пользователя. Такая аутентификация может иметь много форм, включая ID пользователя и пароль, аппаратный или программный токен, адрес источника и биометрические параметры.

Прокси-шлюзы прикладного уровня





Прокси-шлюзы прикладного уровня

- Подобно межсетевым экранам прикладного уровня прокси-шлюзы могут анализировать содержимое трафика. Они также устанавливают TCP-соединение с системой источника и могут защитить от различных вредоносных вставок на каждом шаге взаимодействия. Кроме того, шлюзы могут принимать решение о разрешении или запрещении трафика, основываясь на информации заголовков или содержимого прикладного протокола. После того, как шлюз определил, что данные корректные, он отправляет их хосту получателя.
- Прокси-шлюзы прикладного уровня отличаются от межсетевых экранов прикладного уровня. **Во-первых**, прокси-шлюзы прикладного уровня **не допускают прямые соединения между двумя хостами, а не только анализируют содержимое трафика**. Другим возможным преимуществом является то, что **некоторые прокси-шлюзы прикладного уровня могут расшифровывать пакеты** (т.е. защищенное TLS-содержимое), проверять его и затем повторно шифровать перед тем, как послать получателю. Данные, которые шлюз не может расшифровать, передаются непосредственно приложению. При выборе типа развертываемого межсетевого экрана важно решить, действительно ли необходимо межсетевому экрану функционировать в качестве прокси.

Прокси-шлюзы прикладного уровня

- Межсетевые экраны с возможностями прокси-шлюза могут также иметь и определенные недостатки по сравнению с пакетными фильтрами и с инспекцией состояния. Во-первых, так как прикладные прокси-шлюзы «знают о пакете все», то межсетевой экран **тратит больше времени на анализ каждого пакета**. Это плохо сказывается и на пропускной способность сети, и на приложениях реального времени. Чтобы уменьшить нагрузку на межсетевой экран, можно использовать выделенный прокси-сервер для обеспечения безопасности менее чувствительных ко времени сервисов, таких как почта и большинство веб-трафика. Другим недостатком является то, что прикладные прокси-шлюзы имеют **ограниченную возможность в поддержке новых приложений и протоколов** – требуется прокси-агент для каждого конкретного приложения, которому необходимо передавать данные по сети.

Прокси-шлюзы прикладного уровня

Преимущества прокси-серверов прикладного уровня:

- Прокси имеет возможность запросить **аутентификацию пользователя**. Часто существует возможность указывать тип аутентификации, который считается необходимым для данной инфраструктуры. Прикладные прокси имеют возможность аутентифицировать самих пользователей, в противоположность пакетным фильтрам как с анализом состояний, так и без, обычно проверяющим только адрес сетевого уровня, с которого пришел пользователь. Эти адреса сетевого уровня могут быть легко подменены без обнаружения подмены пакетным фильтром.
- Благодаря возможности аутентифицировать пользователя прикладные прокси считаются **менее уязвимыми для атак подделки адреса**.
- Межсетевые экраны прикладного уровня обычно имеют больше возможностей **анализировать весь сетевой пакет**, а не только сетевые адреса и номера портов. Например, они могут определять команды и данные, специфичные для каждого приложения.
- Как правило прокси прикладного уровня создают **более подробные логи**.

Прокси-шлюзы прикладного уровня

Недостатки прокси-серверов прикладного уровня:

- Так как прикладные прокси «знают о пакете все», межсетевой экран вынужден **тратить много времени** на анализ каждого пакета. По этой причине прикладные прокси обычно не подходят для приложений, которым необходима высокая пропускная способность, или приложений реального времени. Чтобы уменьшить нагрузку на межсетевой экран, можно использовать выделенный прокси сервер для обеспечения безопасности менее чувствительных ко времени сервисов, таких как e-mail и большинство веб-трафика.
- Другим недостатком является то, что прикладные прокси обрабатывают ограниченное количество сетевых приложений и протоколов и не могут автоматически поддерживать новые сетевые приложения и протоколы. Для каждого прикладного протокола, который должен проходить через межсетевой экран, необходим свой агент прокси. Большинство производителей прикладных прокси предоставляют общих агентов прокси для поддержки неизвестных сетевых приложений или протоколов. Однако эти общие агенты не имеют большинства преимуществ прикладных прокси: как правило, они просто туннелируют трафик через межсетевой экран.

Выделенные прокси-сервера

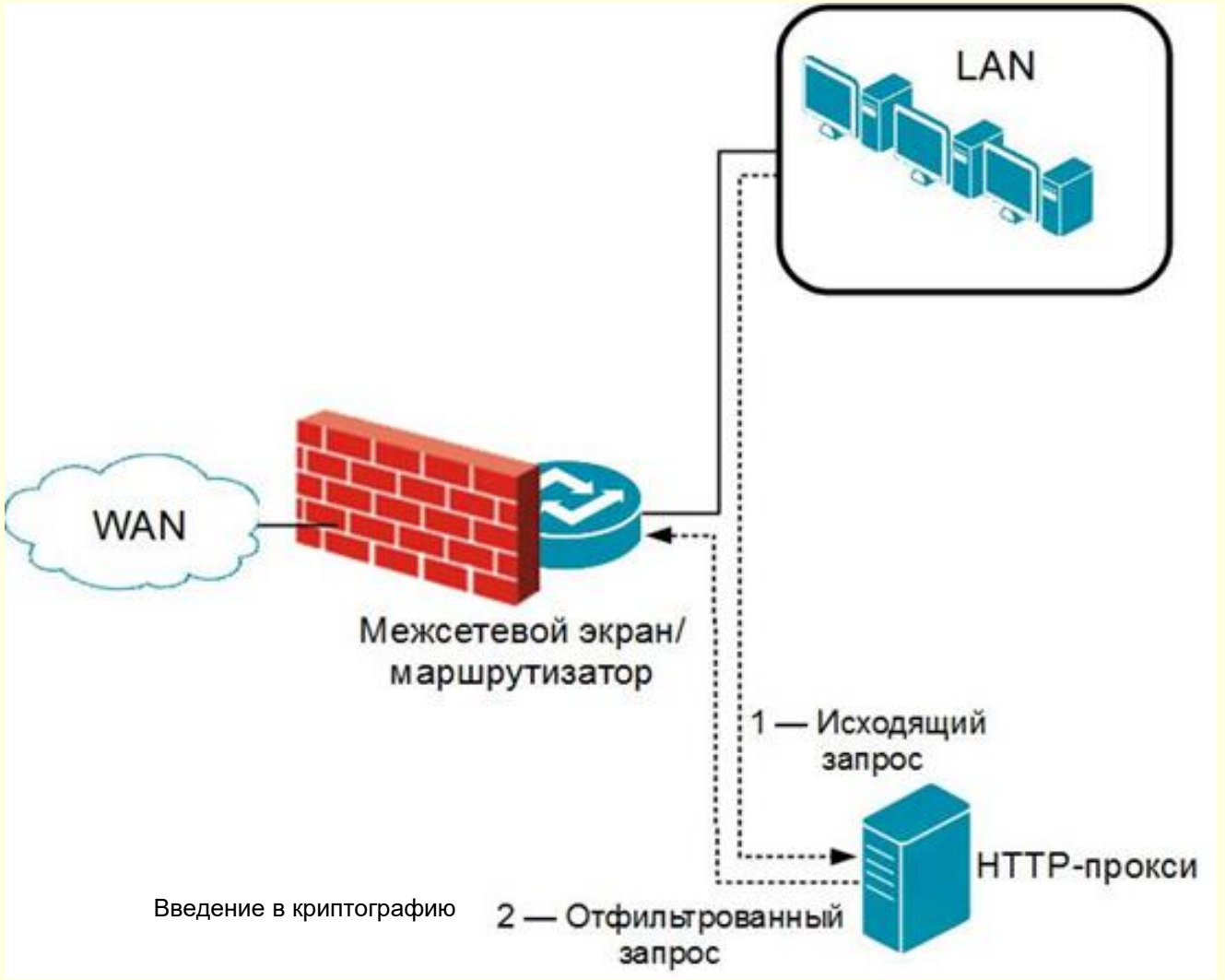
- *Выделенные прокси-сервера* отличаются от прикладных прокси-шлюзов тем, что, хотя они и остаются посредниками по управлению трафиком, **они имеют более ограниченные возможности межсетевого экранирования**. Мы рассматриваем их, потому что они связаны с прикладными прокси-шлюзами. Многие выделенные прокси-сервера специфичны для каждого приложения, некоторые выполняют анализ и проверку корректности прикладных протоколов, таких как HTTP. Так как эти сервера имеют ограниченные возможности межсетевого экранирования, такие как простое блокирование трафика, основанное на источнике или получателе, они обычно развертываются позади традиционных межсетевых экранов. Обычно основной межсетевой экран получает трафик, определяет, какому приложению он предназначен, и пересылает трафик соответствующему прокси-серверу. Этот сервер уже выполняет фильтрование или создание логов трафика и перенаправляет его внутренним системам. Прокси-сервер может также принимать исходящий трафик непосредственно от внутренних систем, фильтровать его или создавать логи и передавать межсетевому экрану для дальнейшей доставки. Примером этого является HTTP-прокси, развернутый позади межсетевого экрана – пользователи должны подключаться к этому прокси, чтобы получить доступ к веб-серверам. Выделенные прокси-сервера обычно используются для уменьшения нагрузки на межсетевой экран и выполнения специализированного фильтрования и создания логов, которое может быть трудно выполнить самому межсетевому экрану.

Выделенные прокси-сервера

- В последние годы использование *входящих* прокси-серверов существенно уменьшается. Это связано с тем, что входящий прокси-сервер должен выглядеть максимально похожим на реальный сервер, который он защищает. Использование прокси-сервера с меньшими возможностями, чем защищаемый им сервер, приводит к тому, что отсутствующие в прокси-сервере возможности не используются. Кроме того, специальные возможности, которые могут иметь входящие прокси-сервера (создание логов, управление доступом и т.п.), обычно встроены в реальные сервера. Большинство прокси-серверов теперь используются в качестве *исходящих* прокси-серверов, при этом наиболее часто используются HTTP-прокси.

Выделенные прокси-сервера

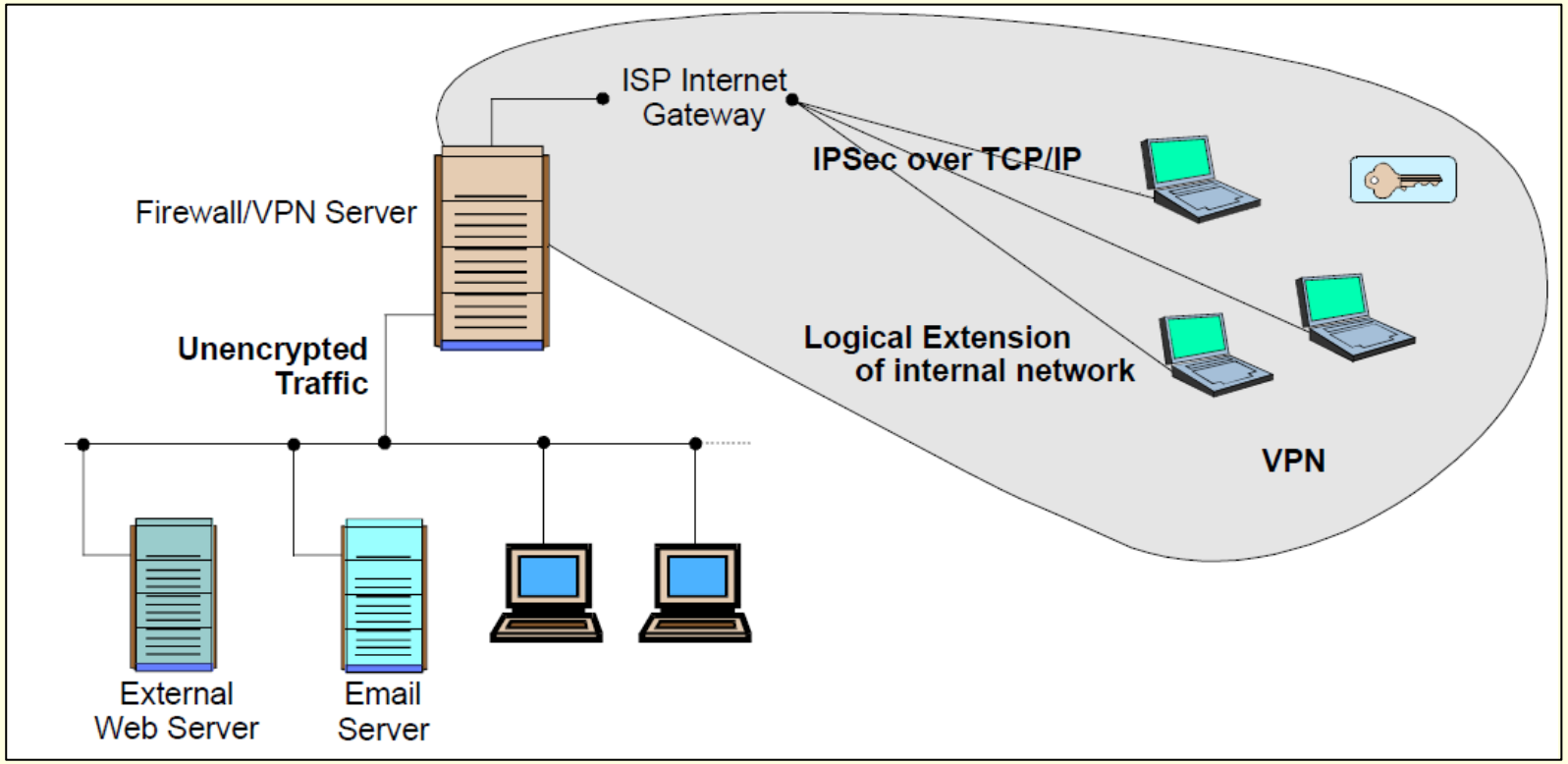
Показана простая сеть, в которой развернут выделенный прокси-сервер, расположенный позади другого межсетевого экрана. **HTTP-прокси обрабатывает исходящие соединения** ко внешним веб-серверам и возможно фильтрует активное содержимое. Запросы первым делом приходят на прокси, затем прокси пересылает запрос (возможно измененный) к внешнему веб-серверу. Ответ от этого веб-сервера приходит обратно к прокси, который пересылает его пользователю. В этом случае можно выполнить кэширование на прокси часто используемых веб-страниц, чтобы уменьшить сетевой трафик и улучшить время ответа.



Конечные точки VPN

- От межсетевых экранов, которые расположены на границы сетевого периметра, иногда требуется нечто большее, чем простое блокирование нежелательного трафика. От них часто требуется **шифрование определенного трафика между защищаемой сетью и внешними сетями**. Это означает создание **VPN**, которые используют дополнительные протоколы для шифрования трафика, аутентификации пользователя и проверки целостности. VPN используется для обеспечения безопасных сетевых взаимодействий по небезопасным сетям. Технология VPN широко применяется для создания защищенной сети, состоящей из нескольких локальных сетей, соединенных через интернет, или предоставления безопасного удаленного доступа ко внутренней сети через интернет.
- Двумя наиболее часто используемыми **архитектурами VPN** являются **шлюз-шлюз и хост-шлюз**. Архитектура **шлюз-шлюз** соединяет несколько локальных сетей через публичную сеть, используя VPN-шлюзы. VPN-шлюз обычно является частью сетевого устройства, такого как межсетевой экран или маршрутизатор. Когда VPN-соединение устанавливается между двумя шлюзами, пользователи, находящиеся в удаленных локальных сетях, ничего не знают о существовании VPN-соединения, и никаких специальных установок на их компьютерах не требуется.

Конечные точки VPN



Конечные точки VPN

- Второй тип архитектуры, **хост-шлюз**, предоставляет индивидуальным пользователям, обычно называемым *удаленными пользователями*, которые находятся вне организации, безопасное соединение с локальной сетью. В этом случае клиент на пользовательской машине устанавливает безопасное соединение с VPN-шлюзом организации. Как в случае шлюз-шлюз, так и в случае хост-шлюз функциональность VPN часто является частью самого межсетевого экрана. При расположении его позади межсетевого экрана VPN-трафик будет проходить через межсетевой экран зашифрованным, что не позволит межсетевому экрану анализировать его.
  - VPN удаленного доступа (хост-шлюз) должны позволять администратору межсетевого экрана указывать, каким пользователям разрешить доступ к сетевым ресурсам. Такое управление доступом обычно выполняется на уровне пользователя или группы. Это означает, что политика VPN позволяет указать, каким пользователям и группам разрешен доступ к каким ресурсам. Для этого обычно используются такие протоколы аутентификации, как RADIUS и LDAP. RADIUS позволяет использовать различные пользовательские креденциалы, примерами которых являются имя пользователя и пароль, цифровые подписи и аппаратные токены. Другим аутентификационным протоколом, часто используемым VPN, является LDAP.

Конечные точки VPN

- Если функциональность VPN поддерживается межсетевым экраном, то требуются дополнительные ресурсы, которые зависят от количества трафика, проходящего по VPN, и типа используемого шифрования. В некоторых случаях дополнительный трафик, связанный с VPN, может потребовать дополнительных ресурсов. Многие межсетевые экраны имеют аппаратные ускорители шифрования, чтобы минимизировать влияние VPN на производительность.

Гибридные технологии межсетевых экранов

- Дальнейшее развитие сетевой инфраструктуры и информационной безопасности привели к стиранию границ между различными типами межсетевых экранов, которые обсуждались выше. Как результат, многие межсетевые экраны **соединяют функциональности нескольких различных типов межсетевых экранов**. Например, многие производители прикладных прокси реализуют базовую функциональность пакетных фильтров.
- Также многие разработчики пакетных фильтров как с анализом состояний, так и без, реализуют базовую функциональность прикладных прокси для ликвидации слабых мест, связанных с пакетными фильтрами. В большинстве случаев производители реализуют прикладные прокси для улучшения создания логов и аутентификации пользователя.

- В результате этого не всегда просто решить, какой продукт наиболее подходит для данного приложения или данной инфраструктуры. Гибридные свойства платформ межсетевых экранов делают особенно важной фазу оценки межсетевого экрана. При выборе продукта важнее оценить поддерживаемые возможности, чем смотреть на формально заявленный тип межсетевого экрана.

Расширенное управление доступом в сеть

- Часто требованием к межсетевым экранам, которые расположены на границы сетевого периметра, является необходимость разрешения входящих соединений не только после выполнения аутентификации удаленного пользователя, но и проверки параметров безопасности пользовательского компьютера. Такая проверка, называемая обычно *управлением доступом в сеть* (*network access control – NAC*) или *защитой доступа в сеть* (*network access protection – NAP*) разрешает доступ не только на основе пользовательских креденциалов, но и на проверке «жизнеспособности» пользовательского компьютера. **Проверка жизнеспособности** обычно состоит из проверки того, что выполнены определенные условия организационной политики:
  - Выполнены последние обновления, защищающие удаленный компьютер от вредоносного ПО.
  - Время, прошедшее с последнего сканирования вредоносного ПО, соответствует политике безопасности.
  - Проверен уровень внесения исправлений в ОС и отдельные приложения.
  - Проверена конфигурация безопасности ОС и отдельных приложений.
- Такая проверка жизнеспособности требуется для ПО на пользовательском компьютере, с которого осуществляется доступ. Если у пользователя есть действительный креденциал, но система не прошла проверки жизнеспособности, пользователь может получить лишь ограниченный доступ ко внутренней сети до тех пор, пока не будет восстановлена жизнеспособность его компьютера.

Унифицированное управление угрозами

Многие межсетевые экраны имеют возможность централизованного управления несколькими сетевыми устройствами. Идея состоит в том, что установить и поддерживать политику в единственной системе легче, чем на нескольких системах, которые развернуты в разных местах в сети. Типичная система унифицированного управления угрозами (**Unified Threat Management – UTM**) включает межсетевой экран с возможностями определения и удаления вредоносного ПО на находящихся под его управлением хостах, определения сетевых проблем, блокирования нежелательного трафика и т.п. **Существуют аргументы за и против совмещения нескольких функций в одной системе.** Например, развертывание UTM уменьшает сложность, так как в этом случае единственная система отвечает за политику безопасности нескольких сетевых устройств. Но при этом может существенно ухудшиться производительность: единственная система, решающая несколько задач, должна иметь достаточное количество ресурсов, таких как ЦП и память, для выполнения каждой задачи. В одном случае можно найти определенный баланс для использования UTM, в другом случае лучше использовать несколько межсетевых экранов в одном сегменте сети.

Межсетевые экраны для веб-приложений

- Веб-сервер может быть атакован различными способами, с помощью размещения вредоносного ПО или обмана пользователя, пытаясь получить от него частную информацию или заставить перейти по ссылке на сервер нарушителя. Многие подобные атаки могут быть определены специализированными межсетевыми экранами прикладного уровня, называемыми *межсетевыми экранами веб-приложений*, которые размещают перед веб-сервером.
- Межсетевые экраны веб-приложений являются относительно новой технологий по сравнению с другими технологиями межсетевых экранов, поэтому их возможности достаточно быстро развиваются. Так как для предотвращения атак на веб-сервера они должны понимать особенности HTTP-протокола, они существенно отличаются от традиционных межсетевых экранов.

Межсетевые экраны для виртуальных инфраструктур

- Виртуализация позволяет нескольким ОС одновременно выполняться на одной машине, при этом каждая ОС считает, что она выполняется на реальном компьютере. Это стало очень популярным, потому что позволяет более эффективно использовать аппаратуру. Большинство типов систем виртуализации имеют *виртуализированные сетевые инфраструктуры*, которые позволяют нескольким ОС взаимодействовать точно также, как если бы у них был стандартный Ethernet, даже если у них нет стандартной сетевой аппаратуры.
- Сетевая активность, которая происходит непосредственно между виртуализированными ОС внутри хоста, не может просматриваться внешним межсетевым экраном. Тем не менее некоторые системы виртуализации предлагают встроенные межсетевые экраны или разрешают добавлять ПО межсетевых экранов третьих фирм. Использование межсетевых экранов для мониторинга виртуализированных сетевых инфраструктур является относительно новой областью технологий межсетевых экранов.

Межсетевые экраны для отдельных хостов и домашних сетей

- Хотя межсетевые экраны, установленные на границе сетевого периметра, обеспечивают определенную защиту внутренних хостов, во многих случаях требуется дополнительная защита сети. Межсетевые экраны, установленные на границы сети, не имеют возможности распознать все варианты и формы атак, позволяя некоторым атакам достигнуть внутренних хостов – после чего атака начинается с одного внутреннего хоста на другой возможно даже не проходя через межсетевой экран, установленный на границы сети. По этой причине разработчики сетевой архитектуры часто добавляют функциональность межсетевого экрана не только в сетевой периметр, что обеспечивает дополнительный уровень безопасности. Рассмотрим межсетевые экраны, специально разработанные для развертывания на отдельных хостах и в домашних сетях.
- Межсетевые экраны для серверов и персональные межсетевые экраны для настольных компьютеров и ноутбуков обеспечивают дополнительный уровень безопасности от сетевых атак. **Эти межсетевые экраны являются программными и устанавливаются на хостах, которые они защищают** – каждый из них просматривает и управляет входящим и исходящим сетевым трафиком для отдельного хоста. Они обеспечивают более точную защиту, чем межсетевые экраны, расположенные в сети, учитывая конкретные потребности отдельных хостов.

Межсетевые экраны для отдельных хостов и домашних сетей

- Межсетевые экраны для хостов доступны **как часть серверных ОС**, таких как Linux, Windows, BSD, Mac OS X Server, они также могут быть установлены в качестве дополнительного компонента от третьих фирм. Политика безопасности межсетевого экрана для отдельного хоста разрешает только необходимый трафик, защищая сервер от вредоносной деятельности всех хостов, включая тех, которые расположены в той же самой подсети или в подсетях, которые не отделены межсетевым экраном. Может быть также полезно ограничение исходящего трафика для предотвращения распространения вредоносного ПО, которым может быть инфицирован хост. Межсетевые экраны для отдельного хоста обычно создают достаточно подробные логи и могут быть сконфигурированы для выполнения управления доступом на основе адреса и на основе приложения. Многие межсетевые экраны для отдельного хоста также функционируют как системы предотвращения вторжения (**IPS**), т.е. после определения атаки предпринимают действия по остановке атакующего и предотвращению нанесения вреда защищаемому хосту.

Межсетевые экраны для отдельных хостов и домашних сетей

- **Персональным межсетевым экраном называется ПО, которое выполняется на настольном компьютере или ноутбуке** с установленной на нем пользовательской ОС, такой как Windows Vista/7, Macintosh OS X или Linux. Персональный межсетевой экран аналогичен межсетевому экрану для отдельного хоста, но компьютер защищается в интересах конечного пользователя, интерфейс обычно более дружественный. Персональный межсетевой экран предоставляет дополнительный уровень безопасности для персонального компьютера, расположенного как внутри, так и за пределами сетевого периметра (например, для мобильных пользователей), так как он может ограничивать входящие соединения и часто может также ограничивать исходящие соединения. Это позволяет не только защитить персональный компьютер от внешних атак, но и ограничить распространение вредоносного ПО с инфицированного компьютера и использование нелицензионного ПО.

Межсетевые экраны для отдельных хостов и домашних сетей

- Некоторые персональные межсетевые экраны позволяют **создавать разные профили на основе местоположения**, например, один профиль для использования внутри сети организации и другой профиль для использования вне локальной сети. Это особенно важно, если компьютер используется в недоверяемой внешней сети, так как, имея отдельный профиль межсетевого экрана для использования в таких сетях, можно тщательнее ограничить сетевую активность и обеспечить более строгую защиту, чем в случае единственного профиля для всех вариантов расположения.
- В дополнение к традиционному фильтрованию с учетом состояния многие персональные межсетевые экраны **могут быть сконфигурированы для разрешения взаимодействия на основе списка допустимых приложений** – таких как веб-браузеры, соединяющиеся с веб-серверами, и почтовые клиенты, посылающие и получающие почтовые сообщения – и могут запрещать взаимодействие с использованием других приложений. Это часто называется *межсетевым экраном на основе приложения*. Управление доступом в этом случае основано на запуске приложений или сервисов, а не на доступе к портам или сервисам.
- Управление персональными межсетевыми экранами должно быть централизовано, если это помогает эффективному созданию, распространению и внедрению политики для всех пользователей и групп. Это будет гарантировать выполнение политики безопасности при получении пользователем доступа к вычислительным ресурсам. Но не зависимо от способа управления любые уведомления, которые создаются межсетевым экраном, должны быть показаны пользователю персонального компьютера, чтобы помочь ему решить обнаруженные проблемы.

Устройства персональных межсетевых экранов

- В дополнение к использованию персонального межсетевого экрана можно использовать **небольшое недорогое устройство**, называемое устройством межсетевого экранирования или маршрутизатором с функциями межсетевого экрана, для защиты компьютеров в домашней сети. Персональное устройство межсетевого экранирования выполняет функции, аналогичные персональному межсетевому экрану, включая некоторые дополнительные возможности, такие как VPN. Даже если на каждом компьютере в домашней сети используется персональный межсетевой экран, устройство межсетевого экранирования все-таки добавляет определенный уровень безопасности. Если персональный межсетевой экран на компьютере будет отключен или неправильно сконфигурирован, устройство межсетевого экранирования будет продолжать защищать компьютер от неавторизованного сетевого взаимодействия. Персональные устройства межсетевого экранирования аналогичны небольшим межсетевым экранам, развертываемым в организации, поэтому возможность централизованного управления и администрирования является важной для устройств персонального межсетевого экранирования.

Устройства персональных межсетевых экранов

- Некоторые персональные устройства межсетевого экранирования могут частично конфигурироваться с использованием технологии UPnP, которое **позволяет приложению, установленному на компьютере за межсетевым экраном, автоматически запрашивать у межсетевого экрана открытие определенных портов, чтобы приложение могло нормально взаимодействовать с внешней системой**. На большинстве персональных межсетевых экранах, которые поддерживают динамическое переконфигурирование посредством UPnP, по умолчанию данная возможность отключена, так как это существенно увеличивает риск безопасности, позволяя недоверяемым приложениям изменять политику безопасности межсетевого экрана.

Устройства персональных межсетевых экранов

Преимущества межсетевых экранов для отдельного хоста:

- Сервер защищен лучше, чем если бы он выполнялся на ОС, не имеющей межсетевого экрана, защищающего этот хост. Серверы должны иметь свою собственную защиту. Не следует предполагать, что они не могут быть атакованы только потому, что они расположены позади основного межсетевого экрана.
- Функционирование межсетевого экрана на отдельном хосте не всегда оправдано. Межсетевой экран, защищающий отдельный хост, достаточно хорошо выполняет функции обеспечения безопасности этого хоста.
- ПО, реализующее межсетевой экран для хоста, обычно обеспечивает возможности достаточно точного управления доступом и возможности ограничения трафика для серверов, выполняющихся на том же хосте. Обычно существуют достаточно хорошие возможности создания логов. Хотя межсетевые экраны, защищающие отдельный хост, менее предпочтительны в случае большого трафика и в окружениях с высокими требованиями к безопасности, для внутренних сетей небольших офисов они обеспечивают адекватную безопасность при меньшей цене.

Недостаток межсетевых экранов для отдельного хоста:

- Каждый такой межсетевой экран необходимо администрировать самостоятельно, и после определенного количества серверов с межсетевыми экранами для отдельного хоста легче и дешевле просто разместить все серверы позади выделенного межсетевого экрана.

Ограниченность анализа межсетевого экрана

- Межсетевые экраны **эффективны только для трафика, который они могут анализировать**. Независимо от выбранной технологии межсетевого экрана, если он не может понимать проходящий через него трафик, он не может осмысленно разрешить или запретить его. Много сетевые протоколы используют криптографию, чтобы скрыть содержимое. Примерами таких протоколов являются IPsec, TLS, SSH и SRTP (Secure Real-time Transport Protocol). **Межсетевые экраны не могут также читать зашифрованные прикладные данные**, например, если почтовое сообщение зашифровано с помощью протоколов S/MIME или OpenPGP. Другим примером ограничения является то, что многие межсетевые экраны **не понимают туннелированный трафик, даже если он не зашифрован**. Например, IPv6 трафик может быть туннелирован в IPv4 многими различными способами. Содержимое даже может быть не зашифровано, но если межсетевой экран не понимает используемый механизм туннелирования, трафик не может быть проинтерпретирован.
- Во всех этих случаях правила межсетевого экрана должны определить, что делать с трафиком, если они не могут его понять.