ТЕМА 3. ТЕХНОЛОГИИ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

ОСНОВНЫЕ ПОНЯТИЯ

Документ "Оранжевая книга" к основным понятиям информационной безопасности относит понятие **Доверенной вычислительной базы** (лекция "Проблемы информационной безопасности").

Доверенная вычислительная база

Совокупность защитных механизмов информационной системы, реализующих ***политику безопасности*** (включая аппаратное и программное обеспечение).

Периметр безопасности — граница **доверенной вычислительной базы.**

Где проходит **периметр безопасности**?

С развитием распределенных систем понятие **периметр безопасности** приобретает смысл — граница владений определенной организации.

То, что внутри владений, считается надежным, то, что вне — нет.

Связь между внутренним и внешним мирами осуществляют посредством шлюзовой системы, которая должна противостоять потенциально ненадежному или даже враждебному окружению.

Межсетевой экран (**МЭ**) — это комплекс программно-аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов.

Межсетевой экран позволяет разделить общую сеть на две части и задать правила, определяющие условия прохождения пакетов данных через границу из одной части общей сети в другую.

Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет

Межсетевые экраны применяются и в сетевых окружениях, которые не требуют обязательного подключения к Интернету, например во внутренних сетях для обеспечения дополнительного уровня безопасности с целью предотвращения неавторизованного доступа к «чувствительным» ресурсам.

МЭ = брандмауэр = файервол = firewall

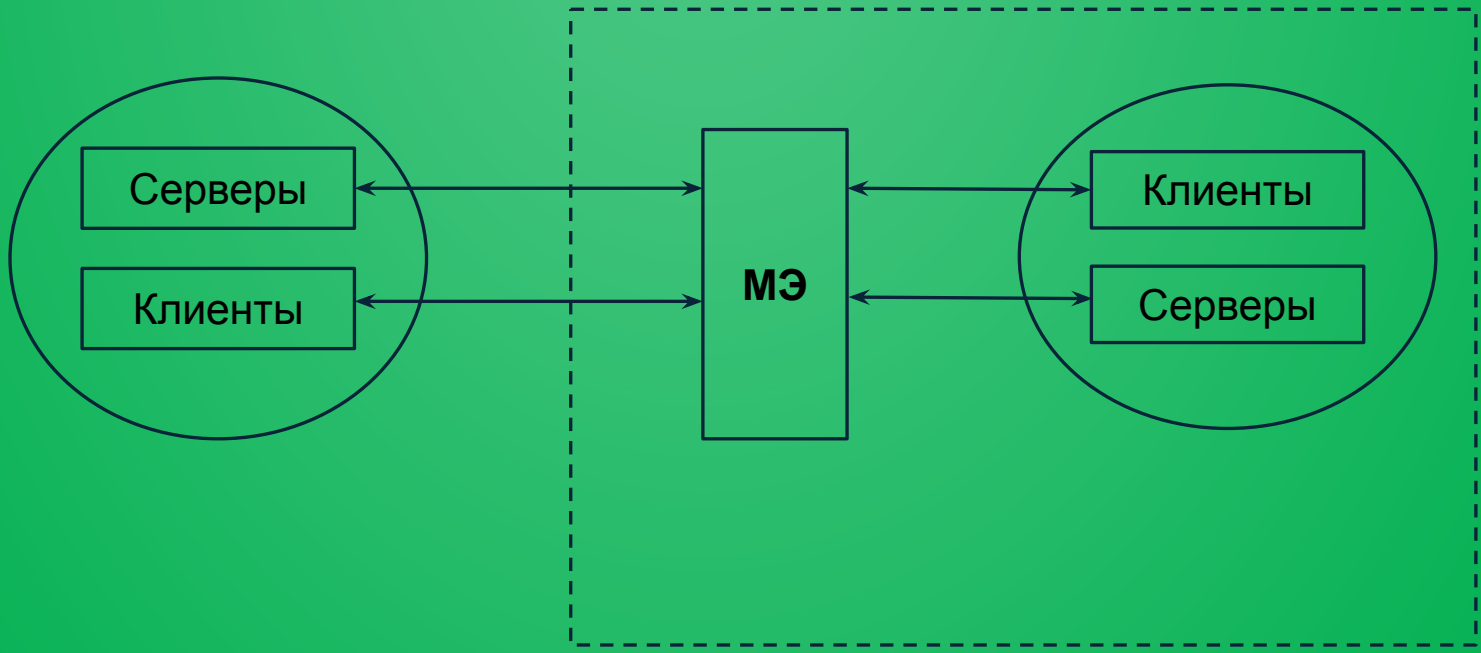
СХЕМА ПОДКЛЮЧЕНИЯ МЕЖСЕТЕВОГО ЭКРАНА

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, явля ющейся внутренней, и потенциально враждебной внешней сетью.

Все взаимодействия между этими сетями должны осуществляться только через межсетевой экран.

Открытая внешняя сеть

Защищаемая внутренняя сеть



ЗАДАЧИ МЭ

Межсетевой экран должен решать две основные задачи:

1) ***ограничение*** доступа внешних пользователей к внутренним ресурсам корпоративной сети.
2) ***разграничение*** доступа пользователей защищаемой сети к внешним ресурсам.

Межсетевые экраны и системы обнаружения вторжений

Межсетевой экран ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и ***не*** отслеживает вторжения, происходящие внутри сети.

Помимо межсетевых экранов существуют также *системы обнаружения вторжений* (Intrusion Detection System, ***IDS***).

IDS, напротив, пропускает трафик, анализирует его и сигнализирует при обнаружении подозрительной активности [Пример — Comodo].

Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил.

Типы МЭ

Существует несколько типов МЭ, которые можно классифицировать по разным признакам, например, **по функционированию на уровнях модели OSI**, которые данный тип МЭ может анализировать.

Современные МЭ функционируют на нескольких уровнях модели OSI.

Более совершенными и эффективными являются те МЭ, которые имеют возможность анализировать большее число уровней.

Возможность анализировать более высокие уровни позволяет межсетевому экрану предоставлять сервисы, которые ориентированы на пользователя, например, аутентификация пользователя.

Задание: Необходимо вспомнить сетевую модель OSI.

Исторически первый межсетевой экран — **сетевой фильтр**, который ставился между доверенной внутренней сетью и внешним Интернетом с целью блокировать подозрительные сетевые пакеты на основе критериев низких уровней модели OSI — сетевом и канальном.

При простой (stateless) фильтрации поток данных фильтруется на основе статических правил, а состояние (state) текущих соединений (например, TCP) не отслеживается.

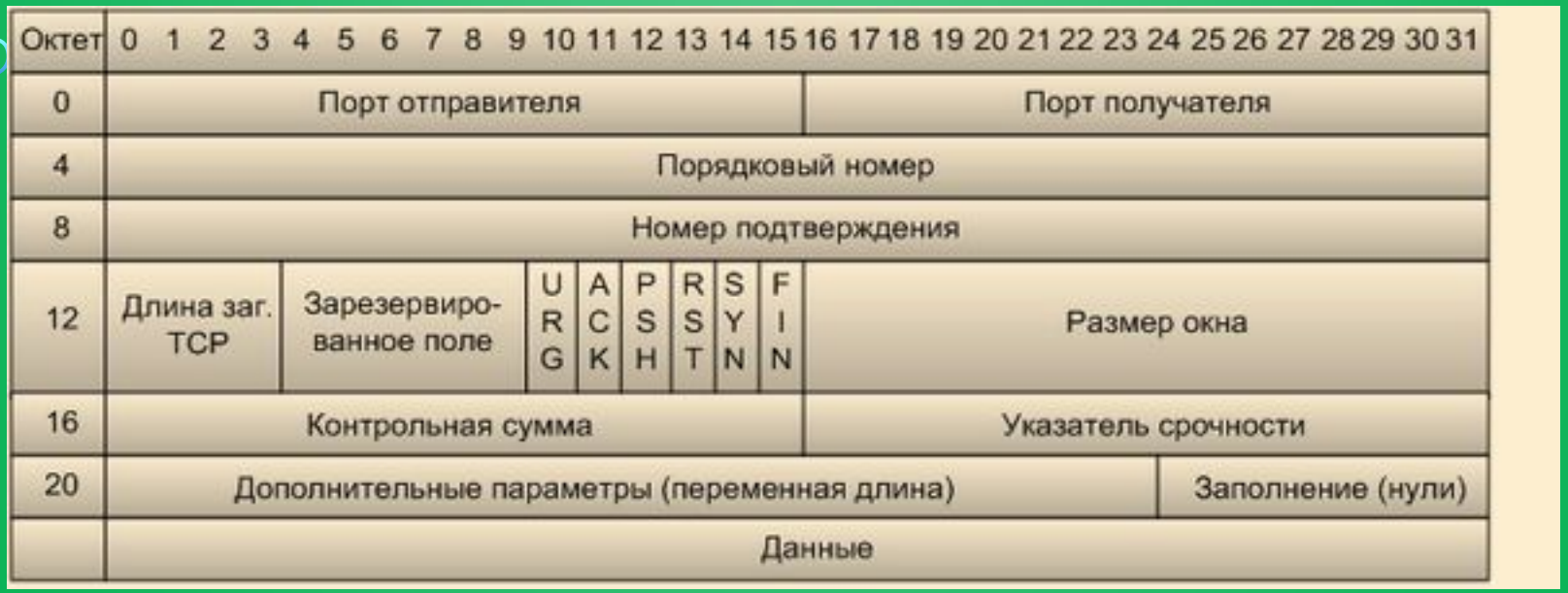
Задание: Необходимо вспомнить структуру

ФОРМАТ IP-ЗАГОЛОВКА

32 бита

Версия (VERS) 4 бита	Длина заголовка (HLEN)	Тип службы (TOS) 8 битов	Общая длина пакета в байтах (Total length) 16 битов
Идентификатор пакета (Identification) 16 битов		Флаги (Flags) 3 бита	Смещение фрагмента (Fragment offset) 13 битов
Время жизни (TTL) 8 битов	Протокол (Protocol) 8 битов	Контрольная сумма заголовка (Header checksum) 16 битов	
IP – адрес источника (Source address) 32 бита			
IP – адрес получателя (Destination address) 32 бита			
Опции (если они есть) (Options)		Заполнение (если нужно) (Padding)	
Данные (Data)			

ЗАГОЛОВОК TCP



Критически важные компоненты заголовка TCP:

1. Флаги TCP.
2. Порядковый номер (**Sequence Number**).
3. Порт отправителя и порт получателя.

Типы МЭ

МЭ второго поколения (stateful firewall) повысили качество и производительность фильтрации за счет контроля принадлежности пакетов к активным TCP-сеансам.

Отслеживается состояние сеансов между приложениями.

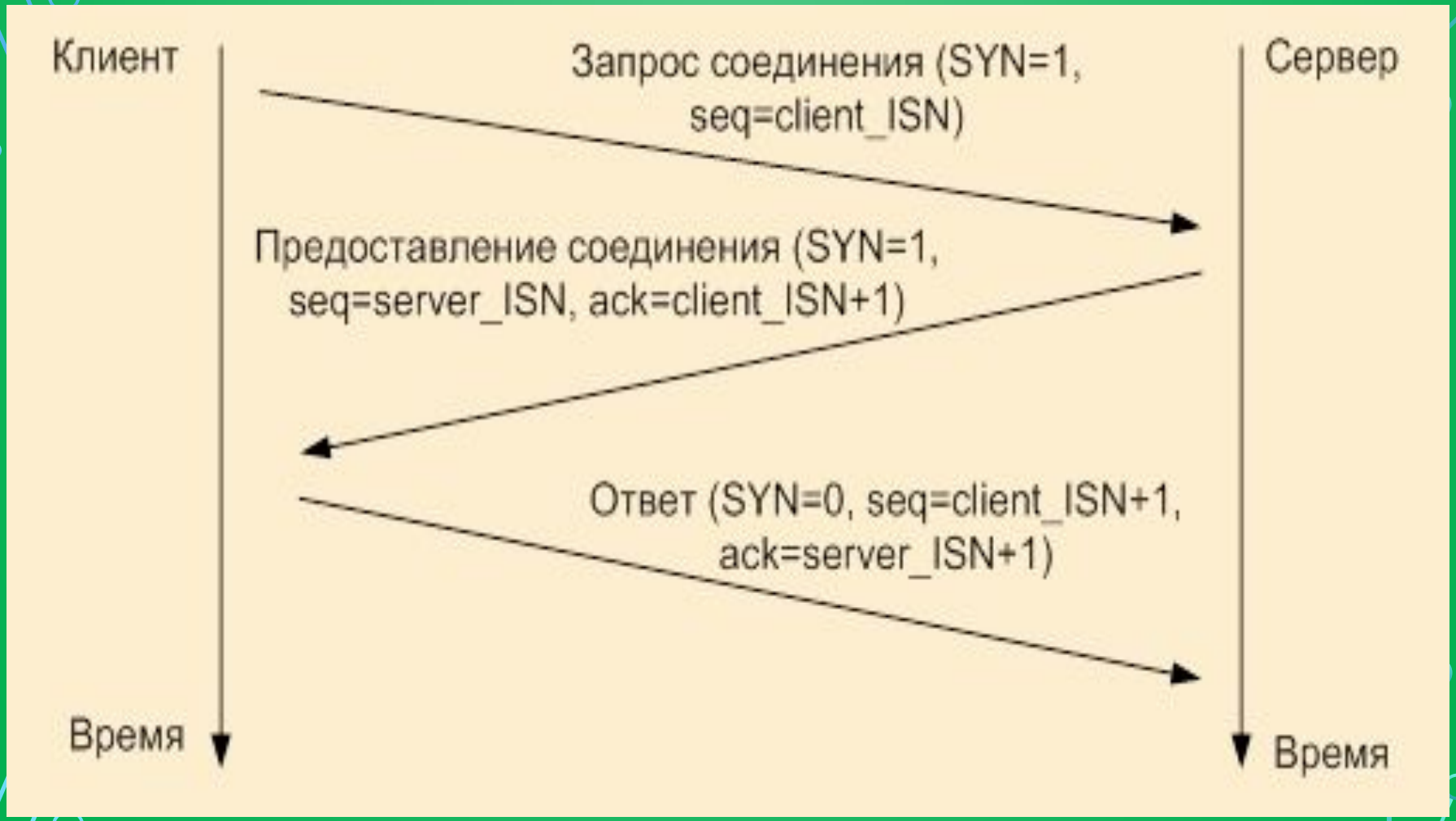
Пакеты, нарушающие спецификации TCP/IP, часто используемые в злонамеренных операциях т.е. сканирование ресурсов, взломы через

Установка соединения TCP (вспомним)

Клиент, желающий установить соединение с некоторым портом сервера, посылает серверу TCP-пакет с флагом SYN.

Если служба, связанная с портом-получателем, принимает соединение, она посылает в ответ запросившему клиенту TCP-пакет с двумя флагами SYN и ACK.

Клиент, запросивший соединение, посылает в ответ TCP-пакет с флагом ACK; соединение устанавливается.


Клиент
Запрос соединения (SYN=1, seq=client_ISN)
Сервер
Предоставление соединения (SYN=1, seq=server_ISN, ack=client_ISN+1)
Ответ (SYN=0, seq=client_ISN+1, ack=server_ISN+1)
Время
Время

Типы МЭ

МЭ следующего поколения способны на уровне приложения изучать в TCP-пакетах поле данных и осуществлять фильтрацию на основании анализа данных приложения, передаваемых внутри пакета.

Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Появление новых сервисов и технологий, например, использование беспроводных сегментов сети, усложняет задачу обеспечения безопасности защищаемой сети.

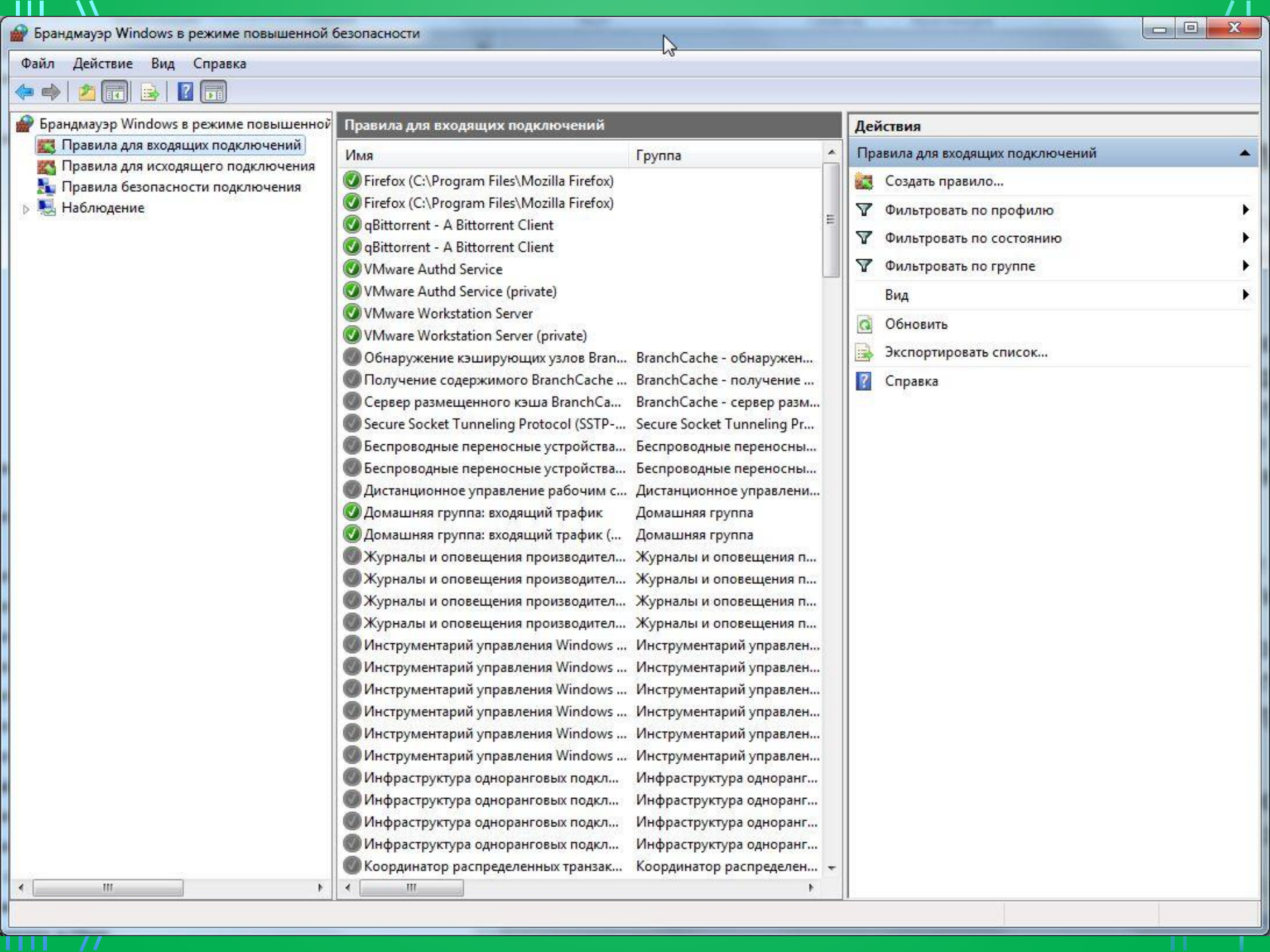
Традиционные межсетевые экраны:

1) защищаемые пользователи и ресурсы находятся под их защитой с внутренней стороны корпоративной или локальной сети;
2) рабочие станции конечных пользователей, находящиеся за пределами защищаемого периметра, являются наиболее уязвимым местом корпоративной сети;
3) не помогают защитить от угроз, возникающих внутри защищаемой сети.

Персональный сетевой экран — программное обеспечение, осуществляющее контроль сетевой активности компьютера, на котором он установлен, а также фильтрацию трафика в соответствии с заданными правилами.

В отличие от межсетевого экрана, персональный сетевой экран устанавливается непосредственно на защищаемом компьютере.

Пример — персональный межсетевой экран **Windows Firewall.**


Брандмауэр Windows в режиме повышенной безопасности
Файл Действие Вид Справка
Брандмауэр Windows в режиме повышенной
Правила для входящих подключений
Правила для исходящего подключения
Правила безопасности подключения
Наблюдение
Правила для входящих подключений
Имя
Группа
Firefox (C:\Program Files\Mozilla Firefox)
Firefox (C:\Program Files\Mozilla Firefox)
qBittorrent - A Bittorrent Client
qBittorrent - A Bittorrent Client
VMware Authd Service
VMware Authd Service (private)
VMware Workstation Server
VMware Workstation Server (private)
Обнаружение кэширующих узлов Bran... BranchCache - обнаружен...
Получение содержимого BranchCache ... BranchCache - получение ...
Сервер размещенного кэша BranchCa... BranchCache - сервер разм...
Secure Socket Tunneling Protocol (SSTP-... Secure Socket Tunneling Pr...
Беспроводные переносные устройства... Беспроводные переносны...
Беспроводные переносные устройства... Беспроводные переносны...
Дистанционное управление рабочим с... Дистанционное управлени...
Домашняя группа: входящий трафик Домашняя группа
Домашняя группа: входящий трафик (... Домашняя группа
Журналы и оповещения производител... Журналы и оповещения п...
Журналы и оповещения производител... Журналы и оповещения п...
Журналы и оповещения производител... Журналы и оповещения п...
Журналы и оповещения производител... Журналы и оповещения п...
Инструментарий управления Windows ... Инструментарий управлен...
Инструментарий управления Windows ... Инструментарий управлен...
Инструментарий управления Windows ... Инструментарий управлен...
Инструментарий управления Windows ... Инструментарий управлен...
Инструментарий управления Windows ... Инструментарий управлен...
Инструментарий управления Windows ... Инструментарий управлен...
Инфраструктура одноранговых подкл... Инфраструктура одноранг...
Инфраструктура одноранговых подкл... Инфраструктура одноранг...
Инфраструктура одноранговых подкл... Инфраструктура одноранг...
Инфраструктура одноранговых подкл... Инфраструктура одноранг...
Координатор распределенных транзак... Координатор распределен...
Действия
Правила для входящих подключений
Создать правило...
Фильтровать по профилю
Фильтровать по состоянию
Фильтровать по группе
Вид
Обновить
Экспортировать список...
Справка

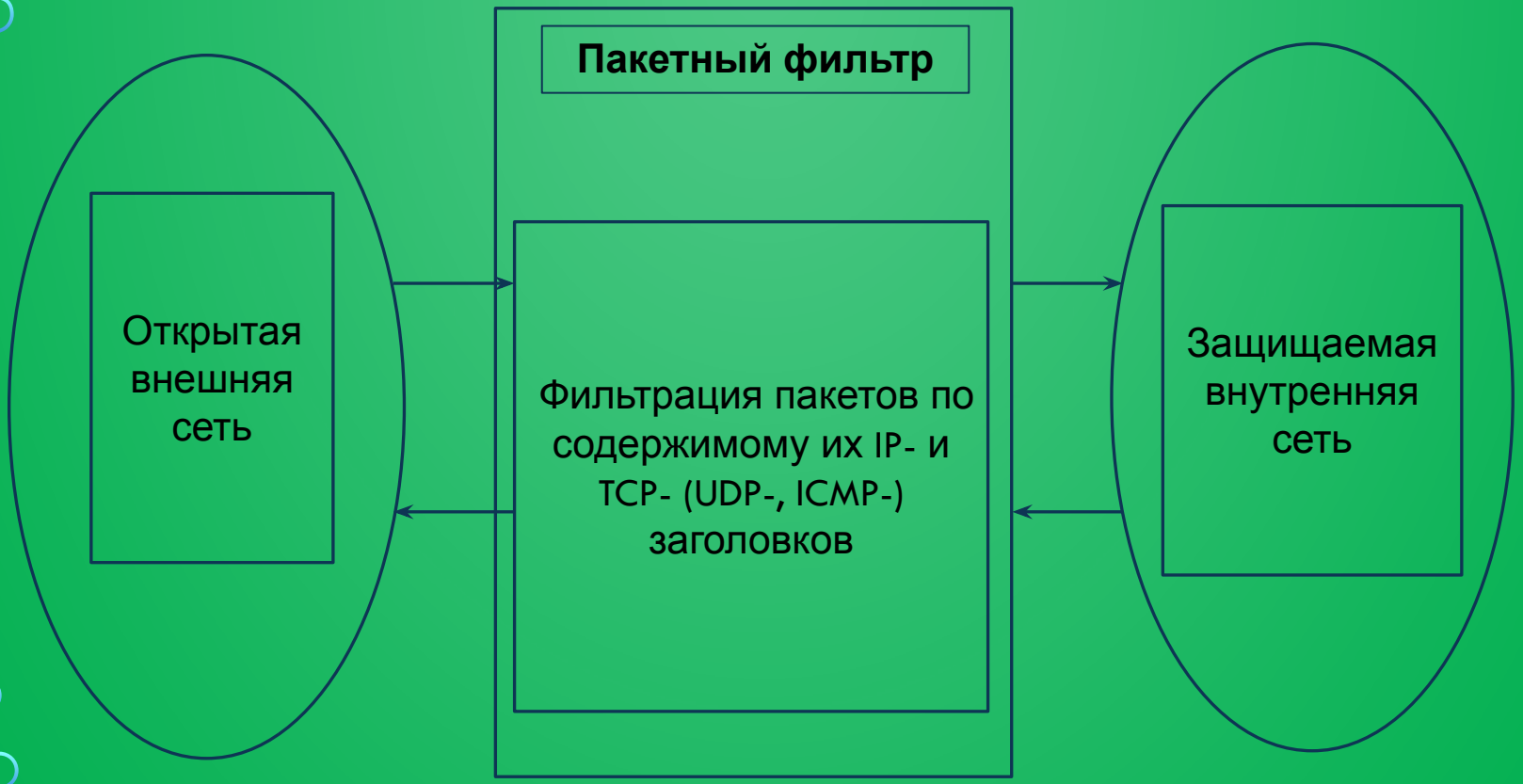
Пакетные фильтры

Первый тип межсетевого экрана называется **пакетным фильтром.**

Вначале пакетные фильтры функционировали на **сетевом (3) уровне** модели OSI, в настоящее время все пакетные фильтры также анализируют и **транспортный (4) уровень.**

Управление доступом обеспечивается независимо для каждого пакета на основе заданных правил фильтрации.

Для принятия решения анализируются заголовки пакетов сетевого и транспортного


Пакетный фильтр
Открытая внешняя сеть
Фильтрация пакетов по содержимому их IP- и TCP- (UDP-, ICMP-) заголовков
Защищаемая внутренняя сеть

В качестве анализируемых полей заголовков IP и TCP (UDP) каждого пакета могут использоваться:

1) **адрес отправителя** (IP-заголовок) — IP-адрес;
2) **адрес получателя** (IP-заголовок) — IP-адрес;
3) **тип пакета** (поле **Protocol** в IP-заголовке) — код протокола ICMP, соответствующего сетевому уровню, либо код протокола транспортного уровня (TCP или UDP), к которому относится анализируемый IP-пакет;

4) **флаг фрагментации пакета** (IP-заголовок) — наличие или отсутствие фрагментации IP –пакетов;
5) **номер порта источника** (TCP- или UDP-заголовок);
6) **номер порта получателя** (TCP- или UDP-заголовок).

При обработке каждого пакета пакетный фильтр последовательно просматривает заданную таблицу правил, пока не найдет правила, с которым согласуется совокуп ность параметров, указанных в заголовках данного пакета.

Если пакетный фильтр получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию.

Из соображений безопасности правило по умолчанию обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

Пакетные фильтры могут быть реализованы как аппаратно, так и программно.

В качестве пакетного фильтра могут быть использованы как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты.

Пакетные фильтры имеют возможность блокировать DoS-атаки и связанные с ними атаки т.е. ***пакетные фильтры, встроенные в пограничные роутеры,*** идеально подходят для размещения на границе с сетью с меньшей степенью доверия.

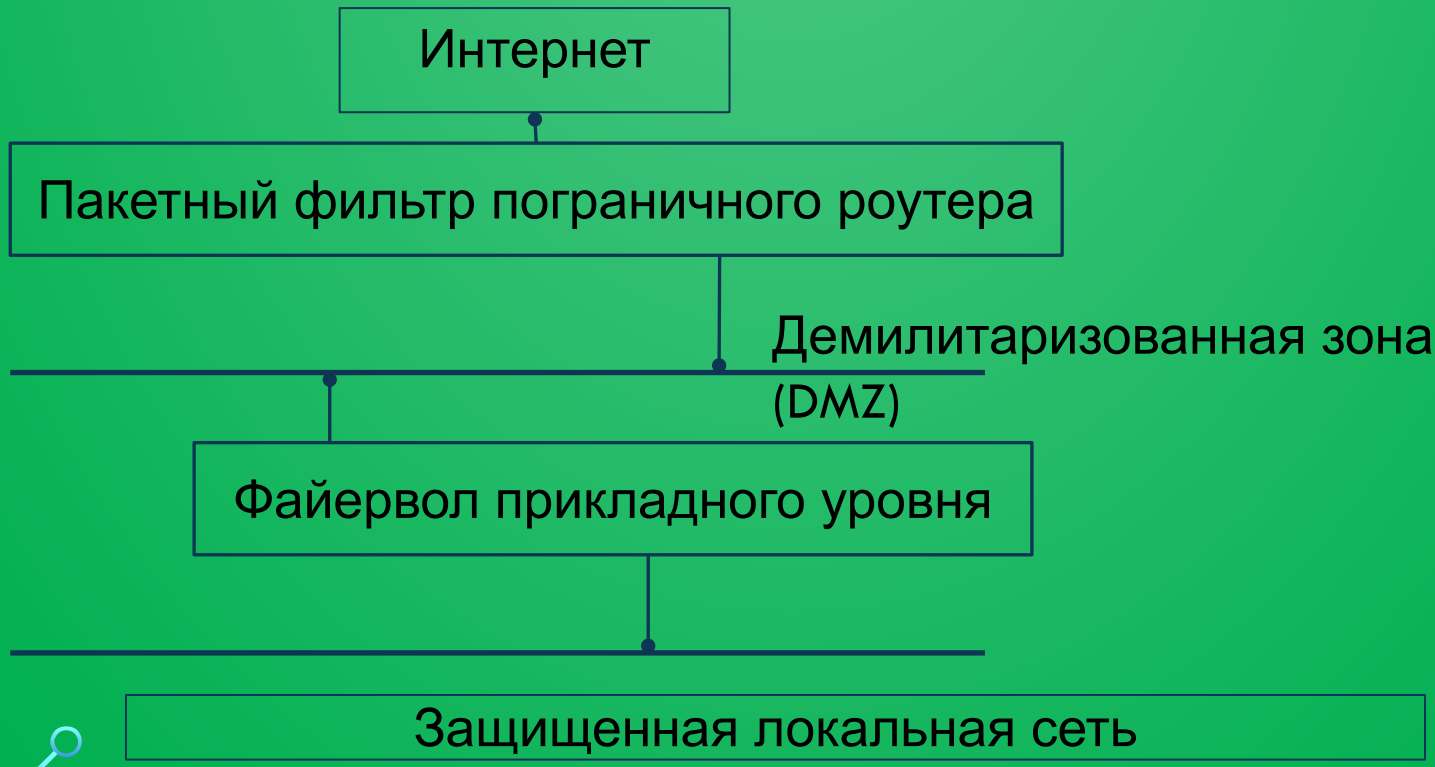
Пакетные фильтры, встроенные в пограничные роутеры, могут блокировать основные атаки, фильтруя нежелательные протоколы и затем передавая трафик другим файерволам для проверки более высоких уровней стека OSI.

Пример топологии сети, использующей пакетный фильтр, встроенный в пограничный роутер

Роутер:

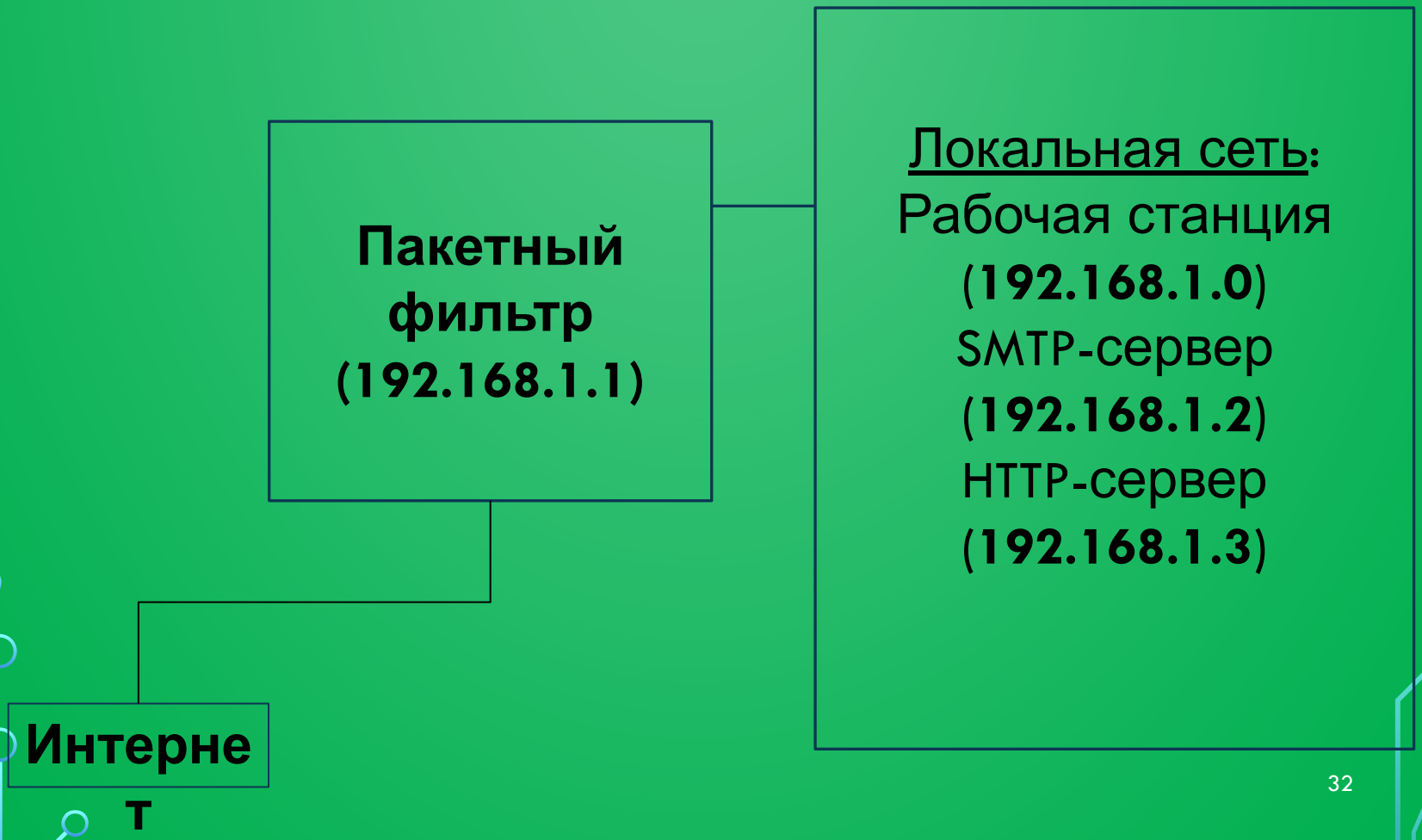
1) принимает пакеты от недоверяемой сети.
2) выполняет контроль доступа в соответствии со своей политикой, например, блокирует SNMP, разрешает HTTP и т.п.
3) передает пакеты более мощному файерволу для дальнейшего управления доступом и фильтрования

Демилитаризованная зона (DMZ) — промежуточная сеть между пограничным роутером и внутренним файерволом, содержит общедоступные сервисы и отделяет их от частных.



ПРИМЕР НАБОРА ПРАВИЛ ПАКЕТНОГО ФИЛЬТРА

Топология сети:



№	Адрес источника	Порт источ.	Адрес назначения	Порт назн.	Дейст.
1	Any	Any	192.168.1.0 (рабочая станция)	>1023	Allow
2	192.168.1.1 (пакет. фильтр)	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2 (SMTP-сервер)	SMTP	Allow
6	Any	Any	192.168.1.3 (HTTP-сервер)	HTTP	Allow
7	Any	Any	Any	Any	Deny

Если найдено правило, которое соответствует анализируемой в пакете информации, то выполняется указанное в правиле действие:

- **Accept** (**Allow** или **Pass**) — пакетный фильтр пропускает пакет.
- **Deny** — пакетный фильтр отбрасывает пакет без его передачи; источнику пакета возвращается сообщение об ошибке ("**host unreachable**").

Discard (**Unreach**, **Block** или **Reject**) — пакетный фильтр отбрасывает пакет и **не** возвращает сообщение об ошибке источнику пакета.

Данное действие используется для реализации «черной дыры», когда МЭ не обнаруживает свое присутствие для внешней стороны.

Два способа настройки межсетевых экранов:

1) запрещено все, что явно не разрешено — большая безопасность.
2) разрешено все, что явно не запрещено —

- В приведённой таблице реализовано правило: разрешает, чтобы пакеты от внешних систем возвращались во внутренние системы, тем самым разрешая завершать создание TCP-соединения.

Когда TCP создаёт сеанс с удалённой системой, открывается порт в исходной системе для получения сетевого трафика от системы назначения.

В соответствии со спецификацией TCP, данный порт источника будет некоторым числом, большим, чем 1023 и меньшим, чем 16384 .

№	Адрес источника	Порт источника	Адрес назначения	Порт назначения	Действие
1	Any	Any	192.168.1.0 (рабочая станция)	>1023	Allow

Второе правило запрещает файерволу пересылать любые пакеты, в которых адрес источника совпадает с адресом файервола.

Данное условие предотвращает возможность атакующего подделать адрес файервола, заменив свой адрес на адрес файервола, чтобы файервол передал пакет внутреннему получателю.

№	Адрес источника	Порт источника	Адрес назначения	Порт назначения	Действие
2	192.168.1.1 (пакетный фильтр)	Any	Any	Any	Deny

Если предполагается, что на данном хосте не установлено никаких других приложений, к которым необходим доступ.

Тогда редактирование правил файервола возможно только с консоли хоста, что не всегда бывает возможно.

Например, может понадобиться доступ к хосту по протоколу SSH для редактирования правил самого файервола.

Третье правило

№	Адрес источника	Порт источника	Адрес назначения	Порт назначен.	Действие
3	Any	Any	192.168.1.1	Any	Deny

Блокирует все пакеты от непосредственного доступа к файерволу.

Четвёртое правило

№	Адрес источника	Порт источника	Адрес назначения	Порт назначен.	Действие
4	192.168.1.0	Any	Any	Any	Allow

Разрешает внутренним системам соединяться с внешними системами, используя любые внешние адреса и любой

Правила 5 и 6

№	Адрес источника	Порт источника	Адрес назначения	Порт назначен.	Действие
5	Any	Any	192.168.1.2 (SMTP-сервер)	SMTP	Allow
6	Any	Any	192.168.1.3 (HTTP-сервер)	HTTP	Allow

Разрешают внешним пакетам проходить через файервол к серверам SMTP и HTTP, если они содержат SMTP- или HTTP-данные соответственно.

Правило 7 запрещает все, что не разрешено.

№	Адрес источника	Порт источника	Адрес назначения	Порт назначен.	Действие
7	Any	Any	Any	Any	Deny

В целом политика информационной безопасности для сети следующая:

1) любой тип доступа изнутри наружу разрешён;
2) никакой доступ снаружи внутрь не разрешен, за исключением SMTP и HTTP;
3) SMTP- и HTTP-серверы расположены позади файервола;
4) на сам файервол доступ не разрешён.

Пакетные фильтры с простой (stateless) фильтрацией: преимущества и недостатки

Основным преимуществом пакетных фильтров с простой фильтрацией (**stateless firewalls**) является их **скорость**.

Недостатки пакетных фильтров stateless

- не анализируют данные более высоких уровней т.е. не могут предотвратить атаки, которые используют уязвимости или функции, специфичные для приложения, например, не могут

- не поддерживают возможность аутентификации пользователя;
- уязвимы для атак, которые используют такие проблемы TCP/IP, как подделка сетевого адреса: многие пакетные фильтры не могут определить, что в сетевом пакете изменена адресная информация уровня 3 OSI;
- трудно конфигурировать; можно случайно переконфигурировать пакетный фильтр для разрешения типов трафика, источников и назначений, которые должны быть запрещены на основе политики безопасности организации.

Пакетные фильтры с контролем состояния

Когда TCP создает сеанс с удаленной системой, в исходной системе открывается порт с номером, большим 1023 для получения сетевого трафика от системы назначения.

Пакетные фильтры должны разрешать входящий сетевой трафик для всех таких портов, т.к. это будут возвращаемые пакеты от системы назначения.

Но! Открытие портов создает риск

Пакетные фильтры с контролем состояния (Stateful Inspection Firewall) решают эту проблему созданием таблицы для исходящих TCP-соединений, соответствующих каждому сеансу.

Эта таблица состояний затем используется для проверки допустимости любого входящего трафика.

Отслеживать используемые порты каждого клиента лучше, чем открывать для внешнего доступа все порты с номерами > 1023 т.е. пакетные фильтры с контролем состояния являются более безопасными.

Пакетный фильтр с контролем состояния отслеживает **состояние сетевых соединений.**

Состояние сетевого соединения — совокупность **атрибутов** соединения.

Атрибуты соединения могут включать в себя IP-адреса, номера портов, участвующих в соединениях, порядковые номера пакетов, проходящих через соединение.

Пакетный фильтр с контролем состояния запоминает информацию о текущем состоянии сеанса в динамически формируемой таблице и производит анализ всех входящих пакетов для проверки их корректности.

Если входящий пакет не является корректным (например, адрес отправителя не равен адресу, к которому посылался запрос или номер пакета не соответствует ожидаемому), он блокируется, в журнале появляется запись о таком событии.

ПРИМЕР ТАБЛИЦЫ СОСТОЯНИЙ СОЕДИНЕНИЙ

Адрес источника	Порт источника	Адрес назначения	Порт назначения	Состояние соединения
192.168.1.100	1030	210.9.88.29	80	Establish
192.168.1.102	1031	216.32.42.123	80	Establish
192.168.1.101	1033	173.66.32.122	25	Establish
192.168.1.106	1035	177.66.32.122	79	Establish
223.43.21.231	1990	192.168.1.6	80	Establish
219.22.123.32	2112	192.168.1.6	80	Establish
210.99.212.18	3321	192.168.1.6	80	Establish
24.102.32.23	1025	192.168.1.6	80	Establish
223.212.212	1046	192.168.1.6	80	Establish

Пример. Организация межсетевого экрана в Linux

Сетевой экран — это способ защитить ПК от нежелательного внешнего трафика.

Сетевой экран позволяет пользователям контролировать входящий сетевой трафик, определяя набор правил.

Сетевой экран реализован в ***ядре*** Linux с помощью подсистемы **Netfilter**, что позволяет проверять каждый входящий пакет в соответствие с заданными правилами и воздействовать на такой пакет, разрешая или блокируя его.

Для управления сетевыми экранами Linux в разное время были разработаны различные

Демон firewalld

Многие современные дистрибутивы Linux масштаба предприятия используют для управления сетевыми экранами службу **firewalld.**

Название службы **firewalld**, как принято в Unix, заканчивается на букву **d**, чтобы показать, что этот процесс является **демоном.**

Демон в Unix — программа, запускаемая операционной системой и работающая в фоновом режиме без прямого взаимодействия с пользователем.

Демон firewalld. Зоны

Демон **firewalld** использует понятия **зон** и **сервисов** для управления трафиком.

Зона — это набор правил, которые применяются к входящим пакетам, соответствующим конкретному ***адресу источника*** или ***сетевому интерфейсу.***

Использование зон особенно важно на серверах с несколькими сетевыми интерфейсами.

На таких серверах зоны позволяют администраторам легко назначать определенный набор правил.

Например, интерфейсы Wi-Fi и LAN могут иметь разные правила фильтрации пакетов.

Firewalld работает с некоторыми зонами по умолчанию.

ДЕМОН FIREWALLD. ЗОНЫ ПО УМОЛЧАНИЮ

Зона	Описание
drop	Любые входящие сетевые пакеты отбрасываются без каких-либо уведомлений. Возможны только исходящие сетевые подключения.
block	Любые входящие сетевые подключения отклоняются с отправлением сообщения **icmp-host-prohibited** для IPv4 и **icmp6-adm-prohibited** для IPv6. Возможны только сетевые подключения, инициированные внутри этой системы.
public	Для использования в общественных местах. Вы не доверяете другим компьютерам в сети, чтобы не нанести вред вашему компьютеру. Принимаются только выбранные входящие соединения.
external	Для использования во внешних сетях с включенным механизмом **преобразования сетевых адресов (NAT)**, особенно для маршрутизаторов. Вы не доверяете другим компьютерам в сети, чтобы не нанести вред вашему компьютеру. Принимаются только выбранные входящие

Зона	Описание
dmz	Для компьютеров в вашей демилитаризованной зоне, которые являются доступными публично для внешней сети и имеют ограниченный доступ к вашей внутренней сети. Принимаются только выбранные входящие соединения.
work	Для использования в рабочих зонах. Вы в основном доверяете другим компьютерам в сети, чтобы не навредить вашему компьютеру. Принимаются только выбранные входящие соединения.
home	Для использования в домашних условиях. Вы в основном доверяете другим компьютерам в сети, чтобы не навредить вашему компьютеру. Принимаются только выбранные входящие соединения.
internal	Для использования во внутренних сетях. Вы в основном доверяете другим компьютерам в сети, чтобы не навредить вашему компьютеру. Принимаются только выбранные входящие соединения.
trusted	Все сетевые подключения принимаются.

Демон firewalld. Сервисы

Вторым ключевым элементом при работе с демоном **firewalld** является **сервис** (**service**).

Понятие сервиса (службы) в **firewalld** отличается от понятия системной службы (демона) в **systemd.**

Сервис в **firewalld** представляет собой комбинацию записей, состоящих из порта и/или протокола.

В **firewalld** определены сервисы по умолчанию, которые позволяют администраторам легко разрешать или запрещать доступ к определенным портам на сервере.

Каждому сервису **firewalld** соответствует файл конфигурации, который объясняет, какие порты UDP или TCP задействованы.

Средства настройки сетевого экрана

Для взаимодействия с демоном **firewalld** в пространстве пользователя доступны два инструмента:

- приложение с графическим интерфейсом **firewall-config**;
- утилита командной строки **firewall-cmd** — сценарий на языке Python.

Все настройки сетевого экрана можно выполнить с помощью одного из этих средств

При работе с любым из этих инструментов следует знать, **где именно вносятся изменения**.

Оба инструмента работают с состоянием конфигурации, хранящимся в памяти, в дополнение к состоянию конфигурации, хранящемуся на диске (постоянному состоянию).

При изменении параметров конфигурации сетевого экрана на постоянной основе следует сделанные изменения передать на диск.

Далее рассмотрим применение утилиты **firewall-cmd**

Управление сетевым экраном с помощью firewall-cmd

Получить статус **firewalld**:

```
firewall-cmd --state
```

Перезагрузить брандмауэр, не теряя информацию о состоянии:

```
firewall-cmd --reload
```

Получить список всех поддерживаемых зон:

```
firewall-cmd --get-zones
```

Получить список всех поддерживаемых сервисов:

УПРАВЛЕНИЕ СЕТЕВЫМ ЭКРАНОМ С ПОМОЩЬЮ FIREWALL-CMD

```
[root@xfce ~]# firewall-cmd --state
running
[root@xfce ~]# firewall-cmd --get-zones
block dmz drop external home internal public trusted work
[root@xfce ~]# firewall-cmd --get-service
RH-Satellite-6 amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bgp bitcoin bitcoi
n-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-clie
nt distcc dns docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger freeip
a-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master git gre high-availabi
lity http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kerberos kibana klog
in kpasswd kprop kshell ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns minidln
a mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-im
ageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy
proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh rsyncd rtsp salt-master samba samba-c
lient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh steam-st
reaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks tra
nsmission-client upnp-client vdsm vnc-server wbem-http wbem-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmp
p-local xmpp-server zabbix-agent zabbix-server
[root@xfce ~]#
```

Получить список всех зон с включенными функциями:

```
firewall-cmd --list-all-zones
```

Распечатать зону *<zone>* с включенными функциями. Если зона *<zone>* опущена, будет использоваться зона по умолчанию

```
firewall-cmd [--zone=<zone>] --list-all
```

Получить зону по умолчанию, установленную для сетевых подключений:

```
firewall-cmd --get-default-zone
```

Установить зону по умолчанию:

`firewall-cmd --set-default-zone=<zone>`

Все интерфейсы, расположенные в зоне по умолчанию, будут помещены в новую зону по умолчанию, что определяет ограничения для новых попыток подключения, инициированного извне.

Активные соединения не затрагиваются.

Получить активные зоны:

```
firewall-cmd
--get-active-zones
```

Получить зону, связанную с интерфейсом:

```
firewall-cmd
--get-zone-of-interface=<interfa
ce>
```

Добавить интерфейс в зону:

```
firewall-cmd [--zone=<zone>]
--add-interface=<interface>
```

Изменить зону, к которой принадлежит интерфейс:

```
firewall-cmd [--zone=<zone>] --change-interface=<interface>
```

Удалить интерфейс из зоны:

```
firewall-cmd [--zone=<zone>] --remove-interface=<interface>
```

Запросить, находится ли интерфейс в зоне:

```
firewall-cmd [--zone=<zone>] --query-interface=<interface>
```

Список сервисов, включенных в зоне <*zone*>:

```
firewall-cmd [ --zone=<zone> ] --list-services
```

Включить сервис в зоне:

```
firewall-cmd [--zone=<zone>] --add-service=<service> [--timeout=<seconds>]
```

Отключить сервис в зоне:

```
firewall-cmd [--zone=<zone>] --remove-service=<service>
```

Запросить, включен ли сервис в зоне:

`firewall-cmd [--zone=<zone>] --query-service=<service>`

```
[root@xfce ~]# firewall-cmd --query-service=http
no
[root@xfce ~]# firewall-cmd --query-service=ssh
yes
[root@xfce ~]#
```

Включить комбинацию порта и протокола в зоне:

```
firewall-cmd [--zone=<zone>]
--add-port=<port>[-<port>]/<pro
tocol> [--timeout=<seconds>]
```

Позволяет использовать комбинацию порта и протокола. Порт может быть одним портом *<port>* или диапазоном портов *<port>* - *<port>*. Протокол может быть либо **tcp**, либо **udp**.

Отключить комбинацию порта и протокола в зоне:

`firewall-cmd [--zone=<zone>] --remove-port=<port>[-<port>]/<protocol>`

Запросить, включена ли комбинация порта и протокола в зоне:

`firewall-cmd [--zone=<zone>] --query-port=<port>[-<port>]/<protocol>`

```
[root@xfce ~]# firewall-cmd --query-port=22/tcp
no
[root@xfce ~]# firewall-cmd --query-port=22/udp
no
[root@xfce ~]# firewall-cmd --query-port=80/tcp
no
[root@xfce ~]#
```

Включить блокировку ICMP в зоне:

```
firewall-cmd [--zone=<zone>]
  --add-icmp-block=<icmptype>
```

Позволяет заблокировать выбранное сообщение ICMP.

Сообщения ICMP являются либо информационными запросами, либо создаются как ответ на информационные запросы или в условиях ошибки.

Отключить блокировку ICMP в зоне:

```
firewall-cmd [--zone=<zone>]
--remove-icmp-block=<icmptype>
```

Запрос о состоянии ICMP-блокировки в зоне

```
firewall-cmd [--zone=<zone>]
--query-icmp-block=<icmptype>
```

```
[root@xfce ~]# firewall-cmd --query-icmp-block=echo-request
no
[root@xfce ~]# firewall-cmd --query-icmp-block=echo-reply
no
[root@xfce ~]#
```