Тема 2. Обеспечение информационной безопасности на сетевом уровне

Лекция 7. Методы и средства обеспечения ИБ сетевого оборудования и протоколов маршрутизации

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Внедрение технологий межсетевого экрана

Учебные вопросы:

1. Списки контроля доступа.
2. Технологии межсетевого экрана.
3. Экранирование основанное на зонах (ZBF).

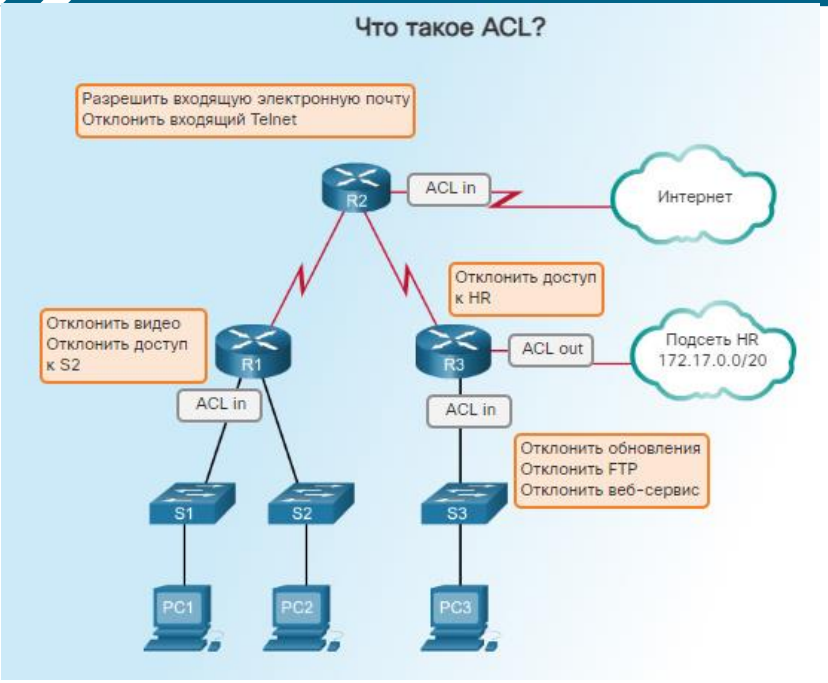
Вступительная часть

С течением времени сети продолжали разрастаться, с их помощью передавалось и хранилось все большее количество важных данных. Соответственно, увеличилась и потребность в более надежных технологиях безопасности, что привело к созданию межсетевого экрана. Название межсетевого экрана, на английском языке firewall, буквально переводится как «огнезадерживающая стена» (или перегородка): она сделана из камня или металла и предотвращает распространение пламени между соседними сооружениями. В сфере сетевых технологий межсетевой экран отделяет защищенные области от незащищенных. Это не позволяет пользователям без соответствующих полномочий получать доступ к защищенным сетевым ресурсам.

Первоначально единственным средством для обеспечения защитных функций межсетевого экрана были простые списки контроля доступа (access control list, ACL), которые включали стандартные, расширенные, нумерованные и именованные списки. Другие технологии для межсетевого экрана стали появляться в конце 90-х годов XX века. В межсетевых экранах с сохранением состояния используются таблицы для комплексного отслеживания в реальном времени состояний рабочих сеансов. Межсетевые экраны с сохранением состояния основаны на сеансовом характере сетевого трафика. В первых версиях межсетевых экранов с сохранением состояния для списков контроля доступа (ACL) использовалась опция TCP established.

В настоящее время существует множество разновидностей межсетевых экранов, среди которых: межсетевые экраны с фильтрацией пакетов, с сохранением состояния, шлюз прикладного уровня, прокси, с преобразованием адресов, на основе хостов, прозрачные и гибридные межсетевые экраны. При разработке современных сетей необходимо тщательно продумать включение одного или нескольких межсетевых экранов, чтобы обеспечить защиту для требующих этого ресурсов, разрешив при этом защищенный доступ к ресурсам, которые должны оставаться открытыми.

Первый учебный вопрос.
Списки контроля доступа.



Списки контроля доступа ACL широко используются для обеспечения работы компьютерных сетей и сетевой безопасности с целью предотвращения атак и управления трафиком. Администраторы могут использовать списки ACL для определения классов трафика и управления ими на сетевых устройствах в соответствии с комплексными требованиями по безопасности, как это показано на рисунке. Списки ACL можно определять для уровней 2, 3, 4 и 7, относящихся к модели взаимодействия открытых систем (Open Systems Interconnection, OSI).

Исторически сложилось, что тип списка ACL определяется числовым значением, как это показано на рисунке. Например, списки ACL с номерами в диапазоне 200–299 использовались для управления трафиком в соответствии с типом Ethernet-интерфейса. Номера списков ACL в диапазоне 700–799 указывают на то, что трафик классифицируется и управляется в соответствии с MAC-адресами.

Сегодня для классификации трафика в наиболее распространенных типах списков ACL используются адреса, формируемые по протоколам IPv4 и IPv6, а также номера портов, соответствующие протоколу управления передачей (TCP) и протоколу пользовательских датаграмм (UDP). Стандартные и расширенные списки ACL для протокола IPv4 могут быть именованными или нумерованными.

Типы ACL-списков

Протокол	Диапазон адресов
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Код типа Ethernet	200-299
DECnet и Extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Ethernet-адрес	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Расширенное прозрачное мостовое соединение	1100-1199

Первый учебный вопрос.
Списки контроля доступа.

Синтаксис стандартного нумерованного списка ACL

```
access-list {acl-#} {permit | deny | remark} source-addr [source-wildcard][log]
```

Стандартные списки ACL фильтруют IP-пакеты только по адресу источника.

Параметр	Описание
acl-#	Это десятичное число в диапазоне от 1 до 99 или от 1300 до 1999.
deny	Отклоняет доступ в случае совпадения условий.
permit	Разрешает доступ в случае совпадения условий.
remark	Добавление замечания о записях в списке IP-доступа для упрощения работы со списком.
source-addr	Номер сети или хоста, с которого отправляется пакет. Существует два способа указания адреса *source-addr*: • Используйте 32-разрядный точечно-десятичный формат, содержащий четыре части. • Используйте ключевое слово any как сокращение для *source* и *source-wildcard* 0.0.0.0 255.255.255.255.
source-wildcard	(Необязательно) 32-разрядная шаблонная маска, применяемая к источнику. Помещает единицы в позиции битов, которые нужно игнорировать.
log	(Необязательно) Вызывает информационное сообщение журнала о пакете, соответствующем записи, которая должна быть отправлена на консоль. (Для управления уровнем сообщений, регистрируемых на консоли, применяется команда logging

Настройка нумерованных и именованных списков ACL

Список ACL представляет собой последовательный перечень разрешающих или запрещающих правил, известных как записи контроля доступа (access control entries, ACE). Записи ACE также называются операторами списков управления доступа ACL. Записи ACE можно создавать для выполнения фильтрации трафика на основе определенного критерия, например адреса источника или адреса назначения, протокола и номера порта.

Стандартные списки ACL обрабатывают пакеты, проверяя поле IP-адреса источника и IP-заголовок. Такие списки ACL используются для фильтрации пакетов только на основании информации об источнике, соответствующей уровню 3. При настройке стандартных нумерованных списков ACL следует использовать синтаксис, указанный на рисунке.

Синтаксис расширенного нумерованного списка ACL

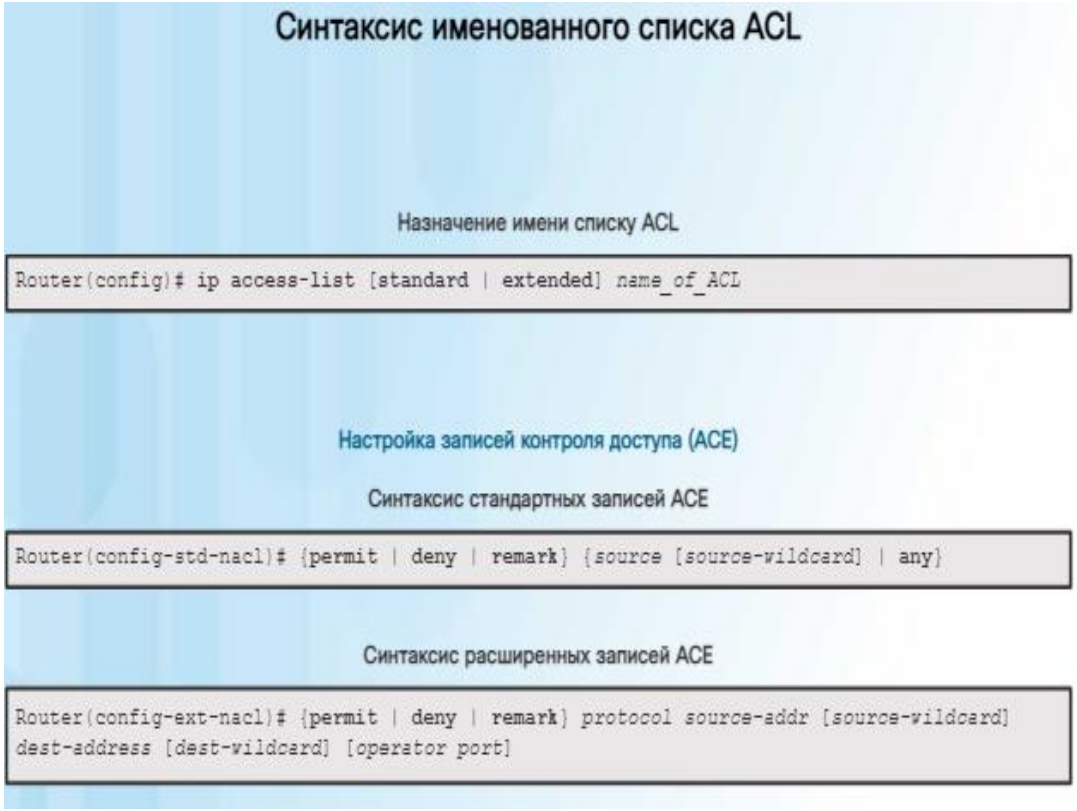
```
access-list acl-# {permit | deny | remark} protocol source-addr [source-wildcard]
dest-addr [dest-wildcard][operator port][established]
```

Параметр	Описание
acl-#	Определяет список доступа с помощью номера в диапазоне 100-199 (для расширенного списка IP ACL) и 2000-2699 (расширенные списки IP ACL).
deny	Отклоняет доступ в случае совпадения условий.
permit	Разрешает доступ в случае совпадения условий.
remark	Используется для ввода замечания или комментария.
protocol	Имя или номер интернет-протокола. Общие ключевые слова - icmp, ip, tcp или udp. Чтобы обеспечить соответствие с любым интернет-протоколом (включая ICMP, TCP и UDP), используйте ключевое слово ip .
source-addr	Номер сети или хоста, из которого отправляется пакет.
source-wildcard	Шаблонные биты, которые должны быть применены к источнику.
destination-addr	Номер сети или хоста, в который отправляется пакет.
destination-wildcard	Шаблонные биты, которые должны быть применены к адресу назначению.
operator	(Необязательно) Сравнивает порты источника или порты назначения. Возможны следующие операнды: lt (меньше чем), gt (больше чем), eq (равно), neq (не равно) и range

В расширенных списках ACL пакеты проверяются на основе информации уровней 3 и 4 об источнике и адресе назначения.

Уровень 4 может включать информацию о портах TCP и UDP. По сравнению со стандартными расширенные списки ACL предоставляют более гибкие возможности по управлению доступом к сети.

Для настройки нумерованных расширенных списков ACL следует использовать синтаксис команд, указанный на рисунке.



Вместо номеров при настройке ACL можно использовать имена.

В отношении именованных списков ACL необходимо указывать, являются ли они стандартными или расширенными.

Для настройки именованных стандартных или расширенных списков ACL следует использовать синтаксис команд, указанный на рисунке.

Синтаксис для применения ACL-списка

Применение ACL-списка к интерфейсу

```
Router(config-if)# ip access-group {acl-#|name} {in|out}
```

Применение ACL-списка к линиям VTY

```
Router(config-line)# access-class {acl-#|name} {in|out}
```

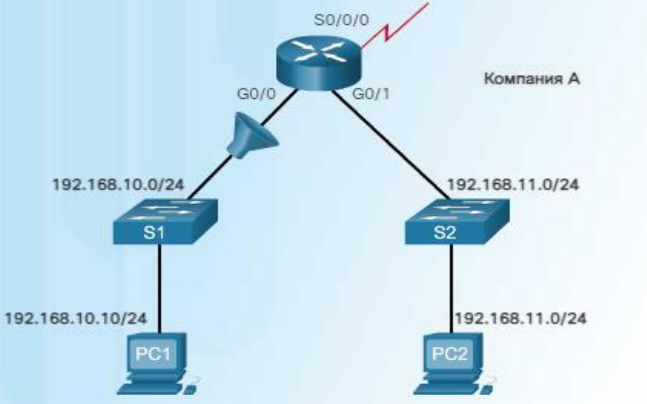
Применение списка ACL

После создания списка ACL администратор может применить его несколькими способами.

На рисунке показан синтаксис команды для применения списка ACL к интерфейсу или к линиям VTY.

На рисунке демонстрируется применение именованного стандартного списка ACL к исходящему трафику.

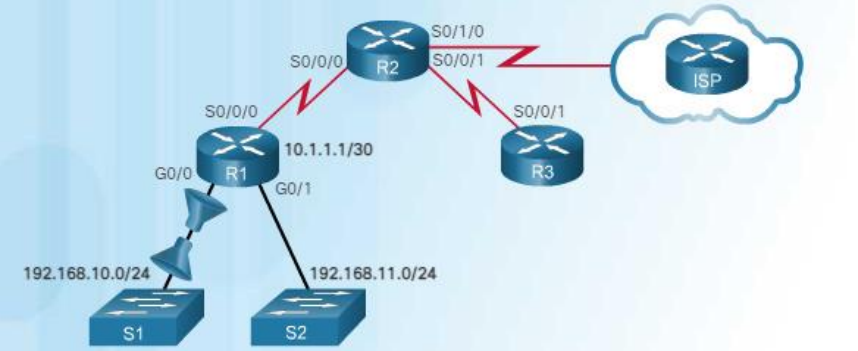
Пример именованного стандартного ACL-списка




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Первый учебный вопрос.
Списки контроля доступа.

Пример именованного расширенного ACL-списка




```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

Список ACL с именем SURFING применяется к входящему трафику, а список ACL с именем BROWSING к исходящему. На рисунке показано применение именованного стандартного списка ACL к входящему трафику на линиях VTY.

На рисунке приводятся два именованных расширенных списка ACL.

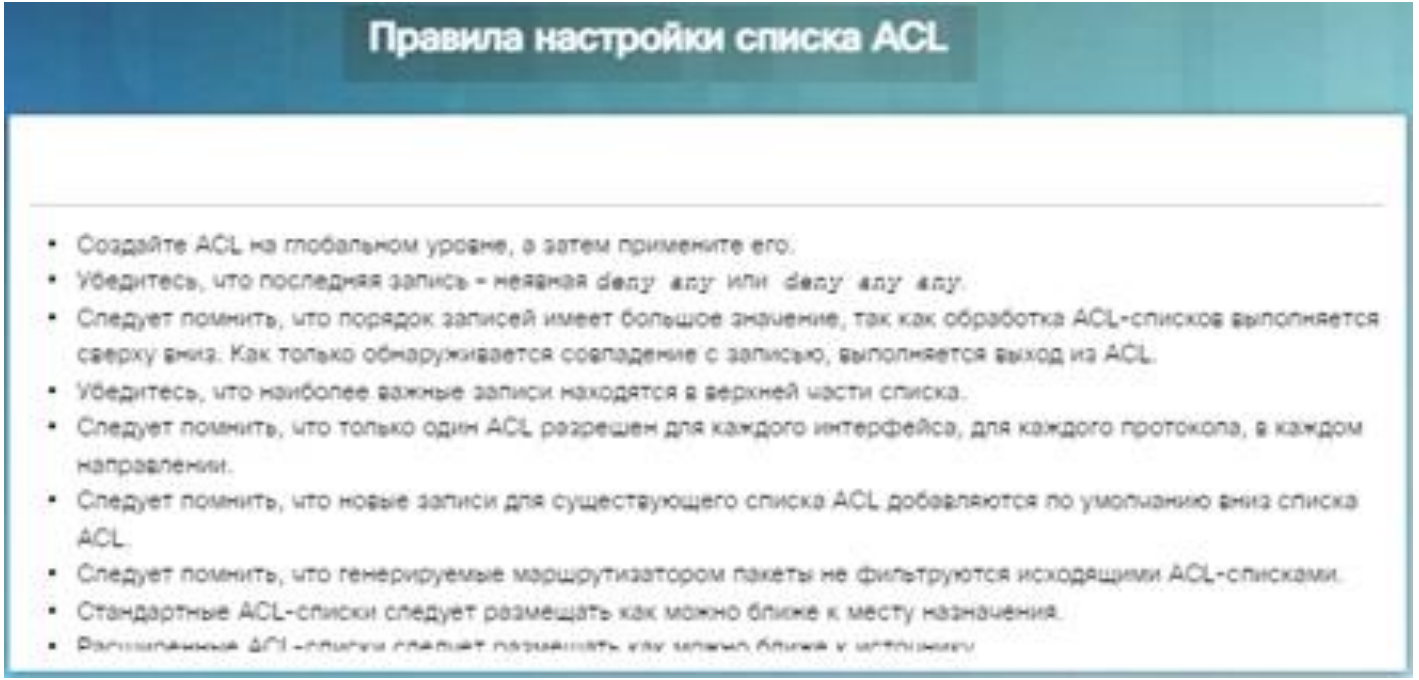
Именованный ACL-список на линиях VTY с записью в журнал

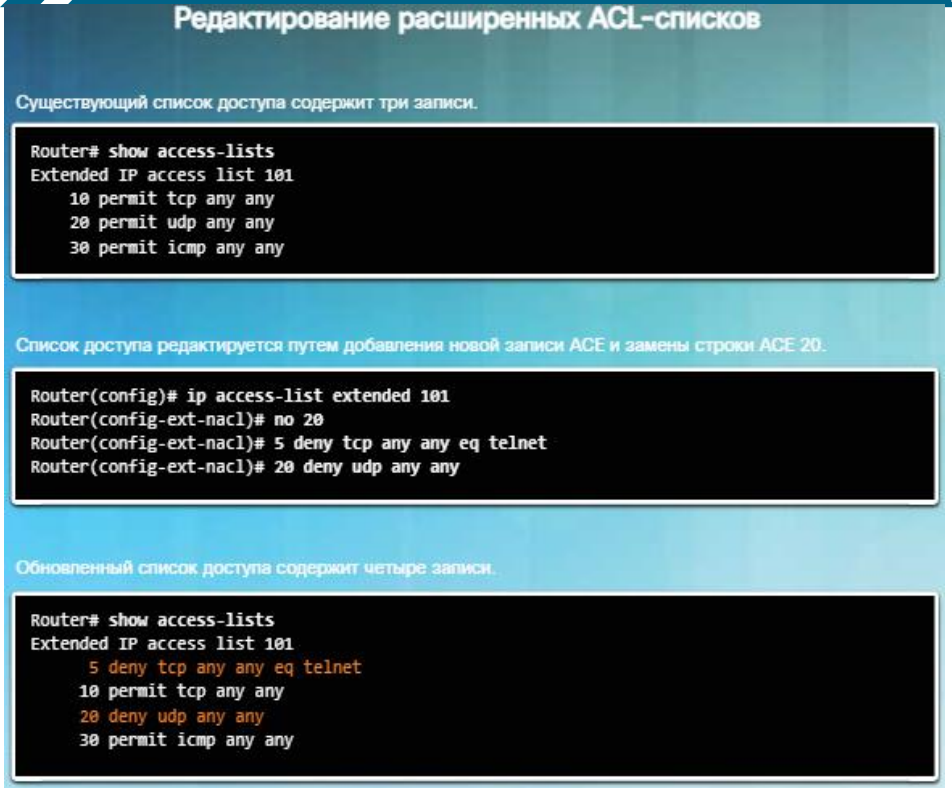

```
R1(config)# ip access-list standard VTY_ACCESS
R1(config-std-nacl)# permit 192.168.10.10 log
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# access-class VTY_ACCESS in
R1(config-line)# end
R1#
R1#!The administrator accesses the vty lines from 192.168.10.10
R1#
*Feb 26 18:58:30.579: %SEC-6-IPACCESSLOGNP: list VTY_ACCESS permitted 0
192.168.10.10 -> 0.0.0.0, 5 packets
R1# show access-lists
Standard IP access list VTY_ACCESS
    10 permit 192.168.10.10 log (6 matches)
    20 deny any
```

Первый учебный вопрос.
Списки контроля доступа.

Составными элементами списка ACL являются записи контроля доступа (ACE) или операторы, которых должно быть не менее одного.

При настройке и применении списков ACL необходимо строго соблюдать указания, приведенные на рисунке.



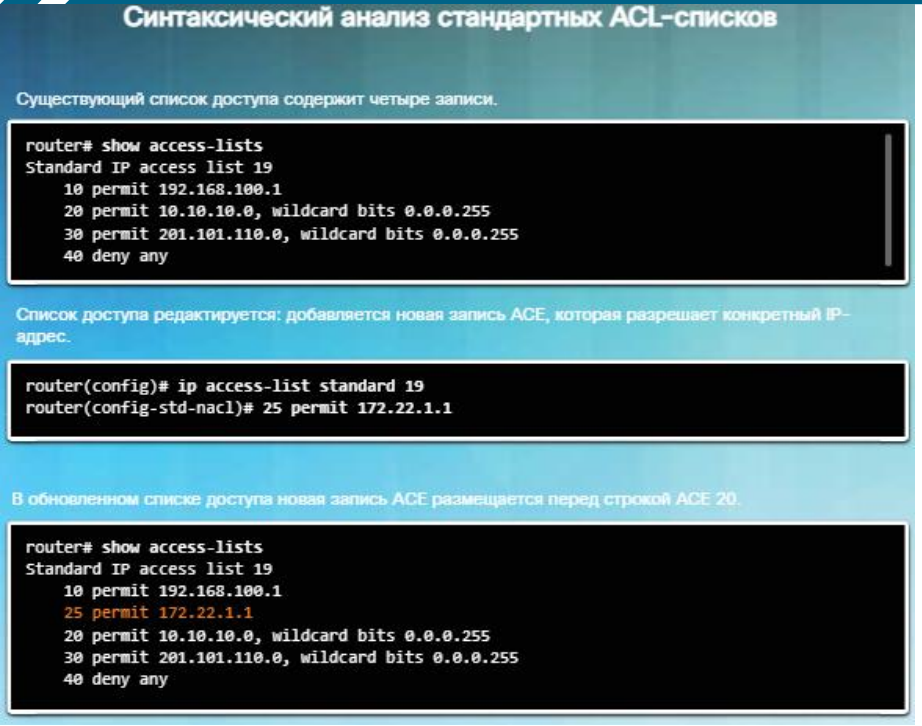


Редактирование существующих списков ACL

По умолчанию нумерация выполняется с шагом 10, и номера присваиваются каждой записи контроля доступа (ACE), имеющейся в списке ACL. После создания и применения списка ACL, его можно редактировать, используя эти порядковые номера.

С помощью этих номеров можно удалять или добавлять какие-либо записи ACE в различные позиции последовательности, как это показано на рисунке.

Если для новой записи порядковый номер не указывается, то маршрутизатор автоматически добавит эту запись в конец списка и присвоит ей соответствующий порядковый номер.



Порядковые номера и стандартные списки ACL

К стандартным спискам управления доступом в Cisco IOS применяется внутренний алгоритм для выполнения настройки записей ACE и проверки самих списков ACL. Записи хостов (с конкретными адресами стандарта IPv4) перечисляются в первую очередь, но не обязательно в той последовательности, которая соответствует порядку их внесения в список. Сначала IOS располагает записи хостов в строгой последовательности, определяемой специальной функцией хеширования. Получаемая в итоге последовательность позволяет оптимизировать поиск записи из списка ACL для какого-либо хоста. Это необязательно, что расположение записей будет в том же порядке, что расположение IPv4-адресов.

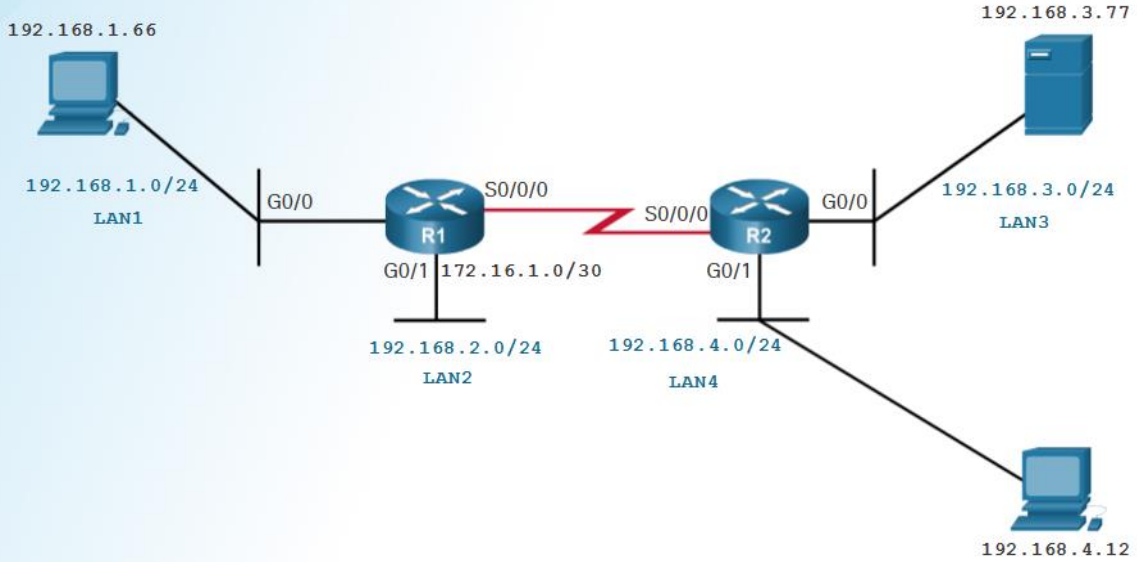
В примере на рисунке представлены различные записи существующего стандартного списка ACL 19. Администратор пытается добавить в список доступа 19 запись с порядковым номером 25, которая должна разрешить доступ для IP-адреса 172.22.1.1. Несмотря на то что указанный порядковый номер больше порядкового номера, соответствующего сети 10.10.10.0, новая запись добавляется перед записью ACE для адреса 10.10.10.0. Это обеспечивает более высокий приоритет записи конкретного хоста относительно записей сети или диапазона адресов.

Порядковый номер не влияет на очередность обработки в стандартном списке ACL. Однако он может использоваться в качестве идентификатора для удаления определенной записи.

Выводы по вопросу
Списки контроля доступа.

Топология – настройка стандартных ACL-списков

Используйте эту диаграмму топологии сети при ответе на три сценария. При необходимости вы можете снова вернуться к этой топологии. Нажмите кнопку 2, чтобы продолжить это действие.

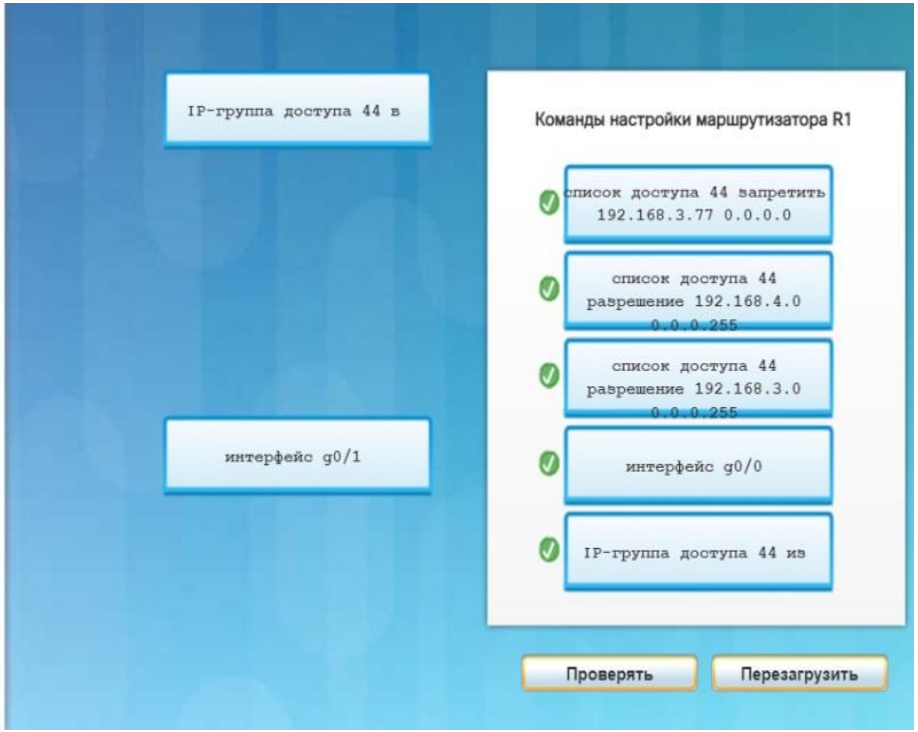


Выводы по вопросу
Списки контроля доступа.

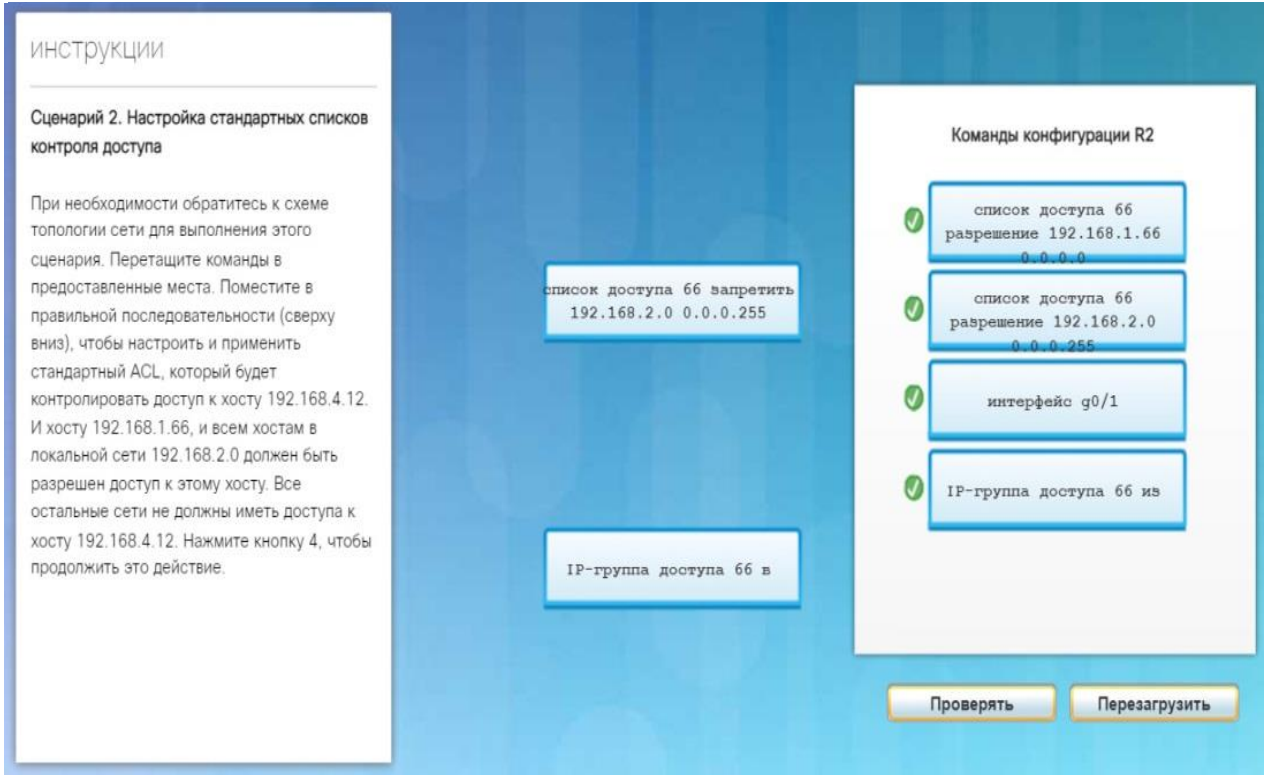
инструкции

Сценарий 1. Настройка стандартных списков контроля доступа

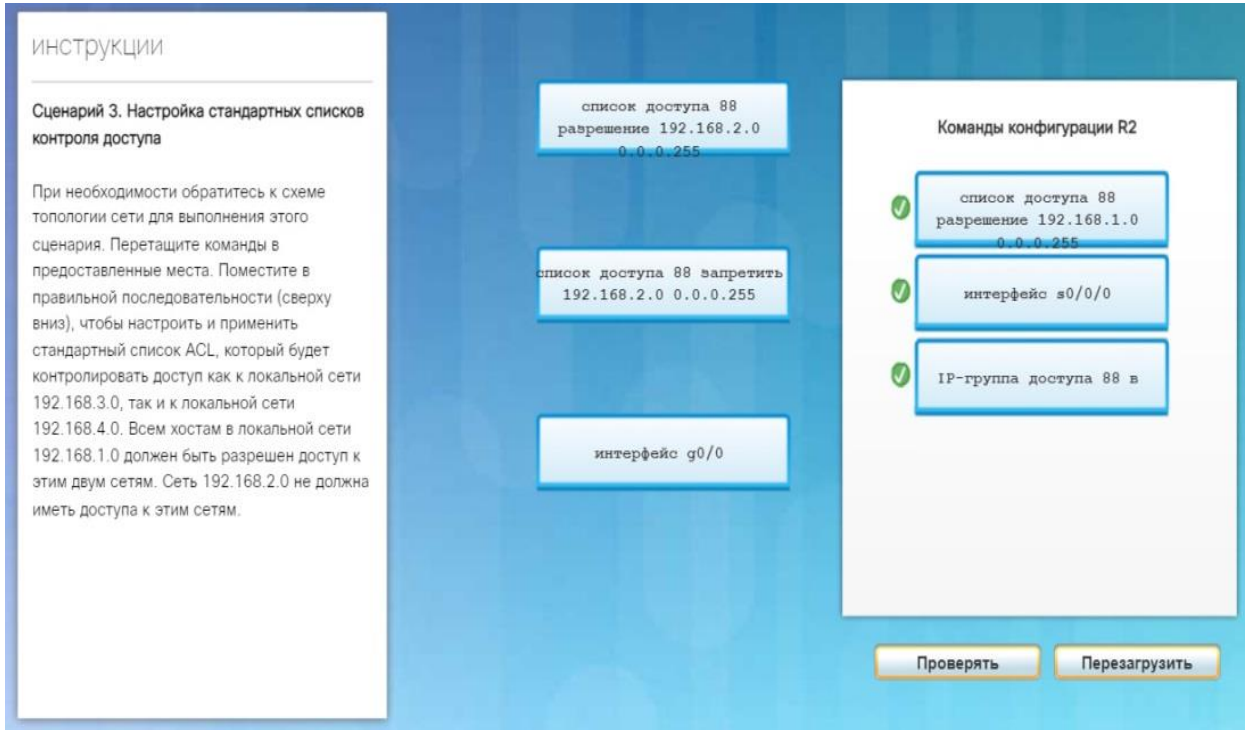
При необходимости обратитесь к схеме топологии сети для выполнения этого сценария. Перетащите команды в предоставленные места. Поместите в правильной последовательности (сверху вниз), чтобы настроить и применить стандартный ACL, который будет контролировать вход в локальную сеть 192.168.1.0. Хост 192.168.3.77 не должен иметь доступа к этой локальной сети, но всем остальным хостам в сетях 192.168.3.0 и 192.168.4.0 должен быть разрешен доступ. Нажмите кнопку 3, чтобы продолжить это действие.



Выводы по вопросу
Списки контроля доступа.



Выводы по вопросу
Списки контроля доступа.



Первый учебный вопрос.
Нейтрализация атак с помощью списков контроля доступа ACL

Нейтрализация атак спуфинга адреса

На входе в S0/0/0

```
R1(config)# access-list 150 deny ip host 0.0.0.0 any
R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any
R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any
R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any
R1(config)# access-list 150 deny ip host 255.255.255.255 any
```

На входе в G0/0

```
R1(config)# access-list 105 permit ip 192.168.1.0 0.0.0.255 any
```

Списки ACL могут использоваться для предотвращения многих сетевых угроз, включая атаки спуфинга IP-адресов и атаки «отказ в обслуживании» (DoS). В большинстве DoS-атак используется какая-либо разновидность спуфинга. При спуфинге IP-адресов процесс стандартного создания пакета нарушается и происходит добавление произвольного IP-заголовка с другим IP-адресом источника. Спуфинг IP-адреса источника позволяет атакующим злоумышленникам скрыть свои идентификационные данные.

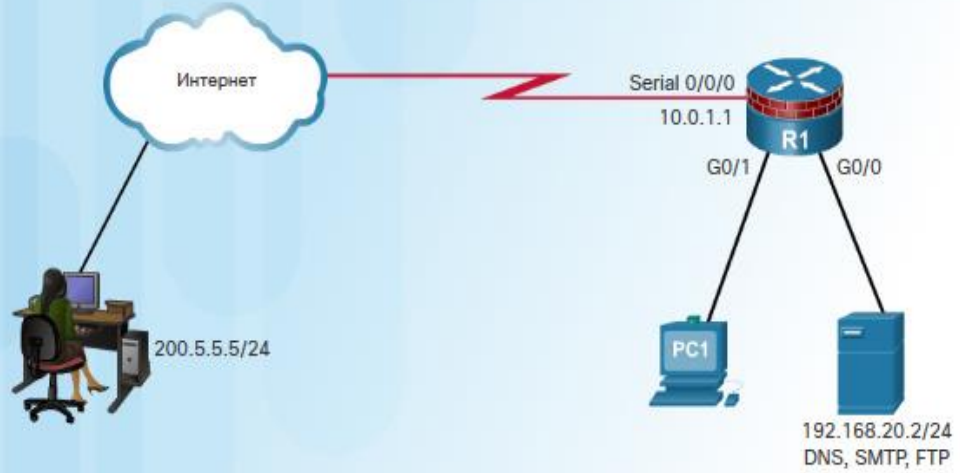
Существует большое количество уже известных классов IP-адресов, которые не могут выступать в роли IP-адресов источника для трафика, попадающего в корпоративную сеть. Например, на приведенном рисунке интерфейс S0/0/0 подключен к сети Интернет и не должен принимать входящие пакеты со следующих адресов:

Все адреса с нулевыми значениями
Широковещательные адреса
Адреса локальных хостов (127.0.0.0/8)
Зарезервированные частные адреса (согласно RFC 1918)
Групповые (multicast) IP-адреса (224.0.0.0/4)

Сеть 192.168.1.0/24 подключена к интерфейсу G0/0 маршрутизатора R1. Этот интерфейс должен пропускать только входящие пакеты с адресом источника из данной сети. Список ACL для G0/0, показанный на рисунке, пропускает только входящие пакеты из сети 192.168.1.0/24. Все остальные пакеты будут игнорироваться.

Первый учебный вопрос.
Нейтрализация атак с помощью списков контроля доступа ACL

Разрешение необходимого трафика через межсетевой экран



На входе в Serial 0/0/0

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap
```

Эффективной стратегией для предотвращения атак является явное разрешение прохождения через межсетевой экран только определенных типов трафика. Например, система доменных имен (Domain Name System, DNS), протокол простой передачи почты (Simple Mail Transfer Protocol, SMTP) и протокол передачи файлов (FTP) являются теми службами, работа которых должна быть разрешена через межсетевой экран. Распространенной практикой также является такая настройка межсетевого экрана, которая предоставляет администраторам удаленный доступ через межсетевой экран. Протокол Secure Shell (SSH), служба Syslog и простой протокол управления сетью (Simple Network Management Protocol, SNMP) являются примерами служб, работа которых должна быть предусмотрена на маршрутизаторе. Хотя многие из упомянутых служб являются полезными с практической точки зрения, их все же необходимо контролировать и отслеживать. Злонамеренное использование этих служб может привести к появлению уязвимостей в системе безопасности.

На рисунке показан пример топологии с возможными настройками списка ACL для разрешения работы определенных служб через последовательный интерфейс 0/0/0.

Первый учебный вопрос.
Нейтрализация атак с помощью списков контроля доступа ACL

Противодействие злоумышленному использованию протокола ICMP

На входе в S0/0/0

```
R1(config)# access-list 112 permit icmp any any echo-reply
R1(config)# access-list 112 permit icmp any any source-quench
R1(config)# access-list 112 permit icmp any any unreachable
R1(config)# access-list 112 deny icmp any any
R1(config)# access-list 112 permit ip any any
```

На входе в G0/0

```
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
R1(config)# access-list 114 deny icmp any any
R1(config)# access-list 114 permit ip any any
```

Хакеры могут использовать эхо-запросы, отправляемые по протоколу управляющих сообщений в Интернете (ICMP), чтобы обнаруживать подсети или хосты в защищенных сетях для проведения DoS-атак с насыщением трафиком (flood-атаки). Хакеры могут использовать перенаправления сообщений по протоколу ICMP, чтобы изменить таблицу маршрутизации для хостов. И эхо-запросы, и перенаправление сообщений по протоколу ICMP должны блокироваться маршрутизатором для входящего трафика.

Рекомендуется разрешить использование во внутренней сети ICMP-сообщений нескольких типов для обеспечения надлежащего функционирования сети:

Эхо-отклик – Позволяет пользователям отправлять эхо-запросы на внешние хосты.

Подавление источника – Направление отправителю запросов об уменьшении скорости трафика сообщений.

Недоступный – Формируется для пакетов, административно запрещенных списком ACL.

Некоторые типы ICMP-сообщений необходимы для корректной работы сети и должны быть разрешены для выполнения выхода:

Эхо-запрос – Позволяет пользователям отправлять эхо-запросы на внешние хосты.

Проблема с параметром – Уведомляет хост о проблемах с заголовком пакета.

Слишком большой пакет – Обеспечивает проверку максимального размера блока передачи данных (maximum transmission unit, MTU).

Подавление источника – Ограничивает при необходимости трафик.

Как правило, следует блокировать все другие типы ICMP-сообщений в исходящем трафике.

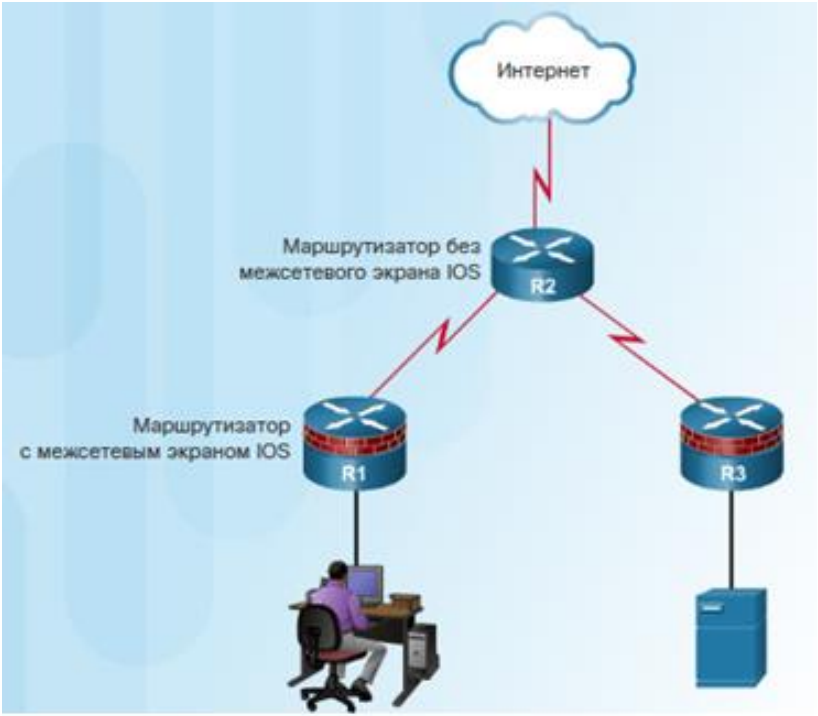
Списки ACL используются для блокирования спуфинга IP-адресов, обеспечения работы через межсетевой экран отдельных служб и для разрешения только необходимых ICMP-сообщений. На рисунке приводится пример топологии и возможных настроек списка ACL для разрешения работы определенных служб ICMP на интерфейсах G0/0 и S0/0/0.

Протоколы управления, такие как SNMP, подходят для осуществления удаленного мониторинга и управления подключенными к сети устройствами. Однако они могут быть использованы опасным образом. Если протокол SNMP необходим, то вредоносное использование его уязвимостей можно предотвратить, применяя списки ACL к интерфейсу для фильтрации SNMP-пакетов, поступающих от неавторизованных систем. Использование эксплойта остается возможным, если источником SNMP-пакета является фальсифицированный адрес, который относится к разрешенным в списке ACL.

Указанные выше меры безопасности являются полезными, но для предотвращения вредоносного использования наиболее эффективно отключение SNMP-сервера на устройствах с IOS, где он не требуется. Как показано на рисунке, использование команды **no snmp-server** позволяет отключить обработку протокола SNMP на устройствах с Cisco IOS.

В рамках первого вопроса мы с вами рассмотрели защиту от спуфинга с помощью списков контроля доступа, противодействие злоумышленному использованию протокола ICMP, нейтрализация эксплойтов протокола SNMP

Второй учебный вопрос.
Технологии межсетевого экрана



Определение межсетевых экранов

Название межсетевого экрана, на английском языке firewall, буквально переводится как «огнезадерживающая стена» (или перегородка): она сделана из камня или металла и предотвращает распространение пламени между соседними сооружениями. Позднее словом firewall обозначалась металлическая пластина, отделявшая моторный отсек транспортного средства или самолета от пассажирского салона. Со временем данный термин был принят к использованию в компьютерных сетях: межсетевой экран (firewall) не допускает проникновение нежелательного трафика в заданные сегменты сети.

Межсетевые экраны различаются в зависимости от категорий пользователей и организаций, но все они имеют некоторые общие свойства:

- Межсетевые экраны противодействуют атакам злоумышленников.
- Межсетевые экраны являются единственными транзитными точками между сетями, так как через них проходит весь трафик.
- Межсетевые экраны обеспечивают реализацию политики управления доступом.

Межсетевой экран представляет собой систему или совокупность систем, которая обеспечивает реализацию политики по управлению доступом между сетями, как показано на этом рисунке. Сюда могут входить различные компоненты, такие как маршрутизатор с пакетной фильтрацией, коммутатор с двумя сетями VLAN и множество хостов с программными межсетевыми экранами.

Преим

Сущес к экранов в сетях:

- Пред жащих прав.

- Очи ользование уязвимостей этого протокола.

- Блок

- Упро евым доступом на несколько межсетевых

Межс

- Нев и, например к превращению в единую точ

- Данн ищенном режиме.

- Поли заблокированных материалов, что создает д

- Мож

- Запр ия через межсетевой экран.

Нажм

Важно енности, чтобы использовать в каждом слу

Описание типов межсетевых экранов

Система межсетевого экрана может состоять из большого количества различных устройств и компонентов. Одним из компонентов является фильтрация трафика, именно эта функция и рассматривается обычно в качестве межсетевого экрана.

На данном занятии рассматриваются межсетевые экраны трех следующих типов:

- Межсетевой экран с фильтрацией пакетов – Как правило, это маршрутизатор с возможностью фильтрации каких-либо пакетных данных, например, это может быть информация, относящаяся к уровню 3 и иногда к уровню 4 (рис. 1).

- Межсетевой экран с сохранением состояния – Выполняет отслеживание таких параметров, как состояния соединений, были ли они инициализированы, передача данных или состояние после завершения использования (рис. 2).

- Шлюз прикладного уровня (прокси-сервер) – Фильтрует информацию на уровнях 3, 4, 5 и 7 базовой модели OSI. Большинство операций по управлению и фильтрации выполняется межсетевым экраном программным образом (рис. 3). Когда клиенту необходимо получить доступ к удаленному серверу, он подключается к прокси-серверу. Прокси-сервер соединяется с удаленным сервером по поручению этого клиента. Поэтому сервер видит только соединение от прокси-сервера.

К другим методам реализации функций межсетевого экрана относятся:

- Межсетевой экран на основе хоста (серверный и персональный) – Представляет собой ПК с работающим на нем программным межсетевым экраном.

- Прозрачный межсетевой экран - Фильтрует IP-трафик между парой интерфейсов, соединенных друг с другом через мост.

- Гибридный межсетевой экран - Является комбинацией межсетевых экранов различного типа. Например, межсетевой экран для контроля за приложениями представляет собой комбинацию межсетевого экрана с сохранением состояния и шлюза прикладного уровня.

Второй учебный вопрос.
Технологии межсетевого экрана

Межсетевые экраны с фильтрацией пакетов обычно являются частью межсетевого экрана маршрутизатора и разрешают или отклоняют трафик на основе информации уровней 3 и 4. Это межсетевые экраны без сохранения состояния, они используют метод простого поиска в таблице политик, когда трафик фильтруется на основе определенных критериев, как это продемонстрировано на рисунке. Например, SMTP-сервер по умолчанию прослушивает порт 25. Администратор может настроить межсетевой экран с пакетной фильтрацией так, чтобы блокировать порт 25 для конкретной рабочей станции, предотвращая таким образом рассылку вирусной электронной почты с этой станции.

Использование межсетевых экранов с фильтрацией пакетов имеет ряд преимуществ:

- При пакетной фильтрации применяется простой набор разрешающих или запрещающих правил.
- Пакетные фильтры слабо влияют на производительность сети.
- Пакетные фильтры легко реализовать, и они поддерживаются большинством маршрутизаторов.
- Пакетные фильтры обеспечивают начальную степень безопасности на сетевом уровне.
- Пакетные фильтры позволяют решать почти что все задачи, как и многофункциональные межсетевые экраны, но при значительно меньших затратах.

Второй учебный вопрос.
Технологии межсетевого экрана

Пакетные фильтры не обеспечивают получение всеобъемлющего решения для межсетевых экранов, но являются для последних важным элементом политики безопасности. Использование межсетевых экранов с пакетной фильтрацией сопряжено и с несколькими недостатками:

- Пакетные фильтры уязвимы для спуфинга IP-адресов. Хакеры могут отправлять пакеты, соответствующие критериям из списка ACL, которые будут проходить через фильтр.

- Пакетные фильтры плохо справляются с фрагментированными пакетами. Так как у фрагментированных IP-пакетов заголовок TCP передается в первом фрагменте, а пакетные фильтры обрабатывают только информацию из заголовка TCP, все фрагменты, следующие за первым, проходят без ограничений. При принятии решений об использовании пакетных фильтров необходимо быть уверенным в том, что фильтрация первого фрагмента гарантирует строгое соблюдение политики безопасности.

- При пакетной фильтрации используются сложные списки ACL, которые не просто реализовывать и обслуживать.

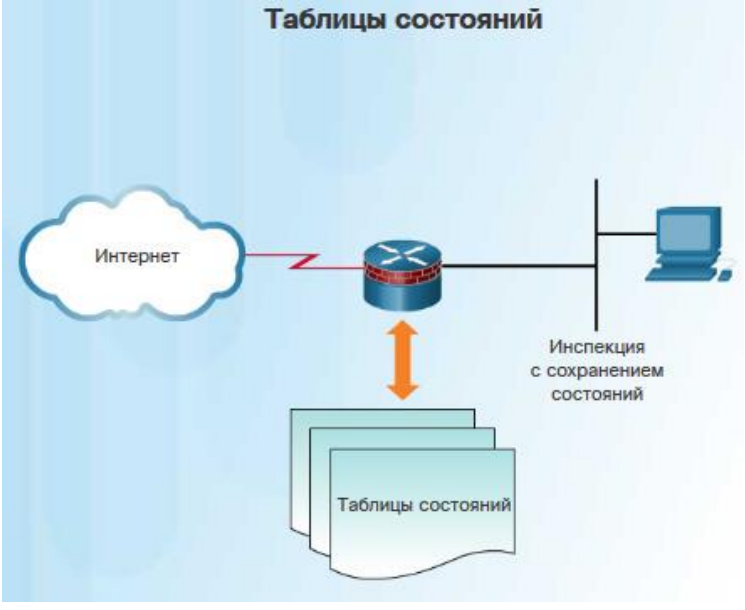
- Пакетная фильтрация не может обеспечить динамическую фильтрацию некоторых устройств. Например, в сессиях, где используется динамическое согласование портов, сложно выполнить фильтрацию без открытия доступа ко всему диапазону портов.

- Пакетные фильтры не сохраняют состояния. Они проверяют каждый пакет по отдельности, не учитывая состояние соединения.

Второй учебный вопрос.
Технологии межсетевого экрана

Технологии межсетевых экранов с сохранением состояний являются наиболее универсальными и широко применяемыми. Межсетевые экраны с сохранением состояний выполняют соответствующую фильтрацию пакетов благодаря использованию информации о соединениях, содержащейся в таблице состояний. Фильтрация с сохранением состояний является одной из архитектур межсетевого экрана, которая классифицируется на сетевом уровне. В данном случае также выполняется анализ трафика на уровнях 4 и 5 модели OSI, как это показано на рисунке.

В отличие от межсетевого экрана без сохранения состояний, в котором происходит статическая фильтрация пакетов, при фильтрации с сохранением состояний учитываются все соединения, проходящие через все интерфейсы межсетевого экрана, и подтверждается, что они являются действительными. Для контроля за фактическим процессом обмена данными в межсетевых экранах с сохранением состояний используется таблица состояний, как показано на рисунке. Межсетевой экран проверяет информацию в заголовках пакетов уровня 3 и сегментов уровня 4. Например, чтобы определить состояние соединения, межсетевой экран может проверять заголовок TCP на наличие таких управляющих кодов, как синхронизация (SYN), сброс (RST), подтверждение (ACK), завершение (FIN) и других.



Каждый раз, когда устанавливается входящее или исходящее соединение по протоколам TCP или UDP, межсетевой экран с сохранением состояний записывает необходимую информацию в таблицу состояний конкретного потока данных. В примере на рисунке хост 10.1.1.1 запрашивает веб-страницу с сервера, расположенного по адресу 209.165.201.3. Межсетевой экран, фильтрующий пакеты с сохранением состояний, сохраняет определенные данные о состоянии запроса в таблице состояний. В приведенном примере маршрутизатор динамически добавил запись об управлении доступом для возвратного трафика, который поступает с порта 80 сервера 209.165.201.3 и направляется на порт 1500 хоста 10.1.1.1.

Описанная здесь реализация функций межсетевого экрана с сохранением состояний применялась в предыдущих версиях IOS. В более современной версии межсетевого экрана из состава Cisco IOS, применяется подход на основе зональных политик, который описывается далее в рамках данного занятия.

Преимущества	Ограничения
Основные средства защиты	Контроль на прикладном уровне не выполняется
Строгая фильтрация пакетов	Ограниченный контроль протоколов без сохранения состояния
Более высокая производительность по сравнению с фильтрами пакетов	Трудно защищать от динамического согласования порта
Защищает от спуфинга и DoS-атак	Аутентификация не поддерживается
Более подробный журнал данных	

У межсетевых экранов с сохранением состояний имеются также **и некоторые ограничения**:

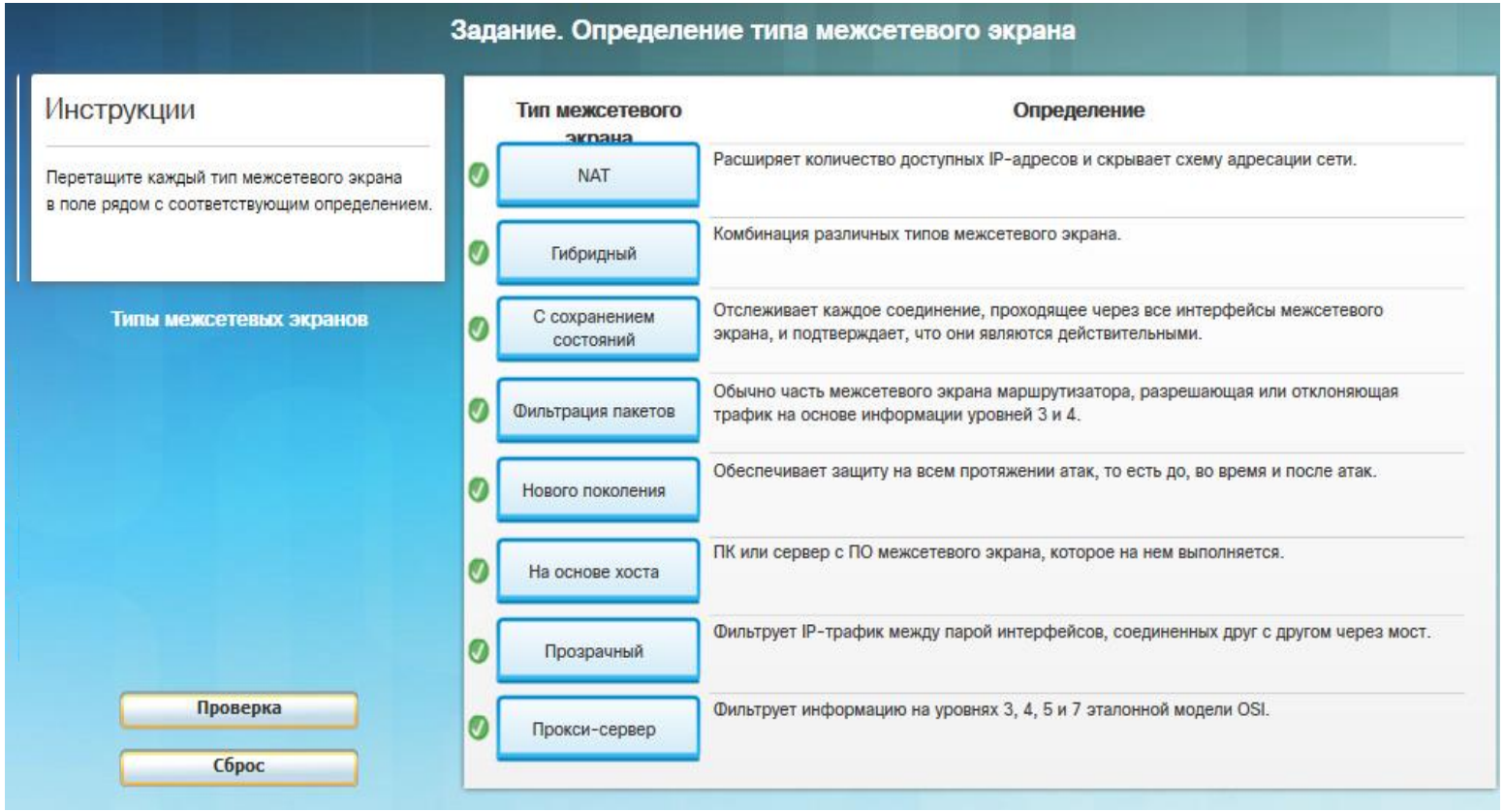
- Межсетевые экраны с сохранением состояний не могут предотвратить атаки на прикладном уровне, так как не контролируют фактические данные, передаваемые через HTTP-соединение.
- Не все протоколы поддерживают сохранение состояний. Например, протоколы UDP и ICMP не формируют информацию о соединениях, необходимую для таблицы состояний, и поэтому их вклад в процесс фильтрации незначителен.
- Сложность представляет также отслеживание соединений, в которых используется динамическое согласование портов. Некоторые приложения открывают несколько соединений. И чтобы установить дополнительные соединения, необходимо открывать новый диапазон портов.
- Межсетевые экраны с сохранением состояний не поддерживают аутентификацию пользователей.

Преимущества и ограничения межсетевых экранов с сохранением состояния

Существует несколько **преимуществ,** обеспечиваемых использованием межсетевых экранов с сохранением состояний в сетях:

- Межсетевые экраны с сохранением состояний часто используются в качестве основного средства защиты путем фильтрации нежелательного, ненужного или подозрительного трафика.
- Межсетевые экраны с сохранением состояний усиливают пакетную фильтрацию, обеспечивая более строгий контроль за безопасностью.
- Межсетевые экраны с сохранением состояний обладают более высокой производительностью по сравнению с пакетными фильтрами или прокси-серверами.
- Межсетевые экраны с сохранением состояний способны противостоять спуфингу и DoS-атакам благодаря возможности определять, принадлежат ли пакеты существующему соединению или поступают от неавторизованного источника.
- Межсетевые экраны с сохранением состояний записывают более подробную информацию в журнал событий, нежели межсетевые экраны с пакетной фильтрацией.

Второй учебный вопрос.
Технологии межсетевого экрана



Знакомство с классическим межсетевым экраном

Классический межсетевой экран Cisco IOS, который ранее назывался средством контроля доступа на основе контекста (context-based access control, CBAC), относится к категории межсетевых экранов с сохранением состояний и входил в состав Cisco IOS до версии 12.0.

Классический межсетевой экран выполняет четыре основных функции:

- фильтрация трафика (показано на рисунке),
- проверка трафика,
- обнаружение вторжений,
- также регистрация учетных данных и отправка оповещений.

Классический межсетевой экран может анализировать поддерживаемые соединения на наличие информации о встроенных NAT и о преобразовании адреса и номера порта (Port Address Translation, PAT), а также выполнять необходимую трансляцию адресов. Классический межсетевой экран может блокировать соединения между удаленными узлами (peer-to-peer, P2P), используемые, например, в приложениях Gnutella и KaZaA. Может блокироваться трафик по обмену мгновенными сообщениями таких приложений, как Yahoo!, AOL и MSN.

Однако классический межсетевой экран обеспечивает фильтрацию только для тех протоколов, которые указаны администратором. Если протокол не указан, то применение к нему фильтрации будет определяться существующими расширенными списками контроля доступа ACL, и временное открытое окно при этом создаваться не будет. Помимо этого, классический межсетевой экран обнаруживает атаки и защищает только от тех атак, которые проникают через межсетевой экран. Как правило, он не обеспечивает защиты против атак, осуществляемых из защищенных сетей, если только этот трафик не передается через внутренний маршрутизатор с Cisco IOS, где задействована функция межсетевого экрана.

Классический программный межсетевой экран Cisco IOS будет поддерживаться в ближайшем обозримом будущем, но его существенное усовершенствование за счет добавления новых возможностей не планируется. Вместо этого в качестве стратегического направления для программного межсетевого экрана с проверкой состояний, входящего в состав Cisco IOS, выбрана реализация зонального межсетевого экрана (Zone-Based Policy Firewall, ZBF).

Второй учебный вопрос.
Технологии межсетевого экрана

Классический межсетевой экран создает временные открытые окна в списках ACL, чтобы разрешить возврат трафика. Эти записи создаются по мере того, как отслеживаемый трафик покидает сеть, и удаляются после закрытия соединения или когда истекает период бездействия при установлении соединения.

Предположим, например, что некий пользователь инициирует SSH-подключение из защищенной сети к внешней сети и что классический межсетевой экран настроен для отслеживания SSH-трафика. Предположим также, что ACL-список применяется на внешнем интерфейсе, блокируя для SSH-трафика доступ в защищенную сеть. Указанное соединение будет обработано в несколько этапов, в результате чего в межсетевом экране будет создано временно открытое окно, как показано на рисунке.

1. Когда трафик генерируется впервые и проходит через маршрутизатор, обрабатывается входящий ACL-список. Если этот ACL-список блокирует соединение данного типа, то пакет отклоняется. Если же ACL-список разрешает это соединение, тогда анализируются правила инспектирования классического межсетевого экрана.

2. Программное обеспечение Cisco IOS должно осуществить проверку этого соединения в соответствии с правилами инспектирования классического межсетевого экрана. Если SSH-трафик относится к категории неконтролируемого, прохождение пакета разрешается, и никакая другая информация не фиксируется. В противном случае для подключения выполняется следующий шаг.

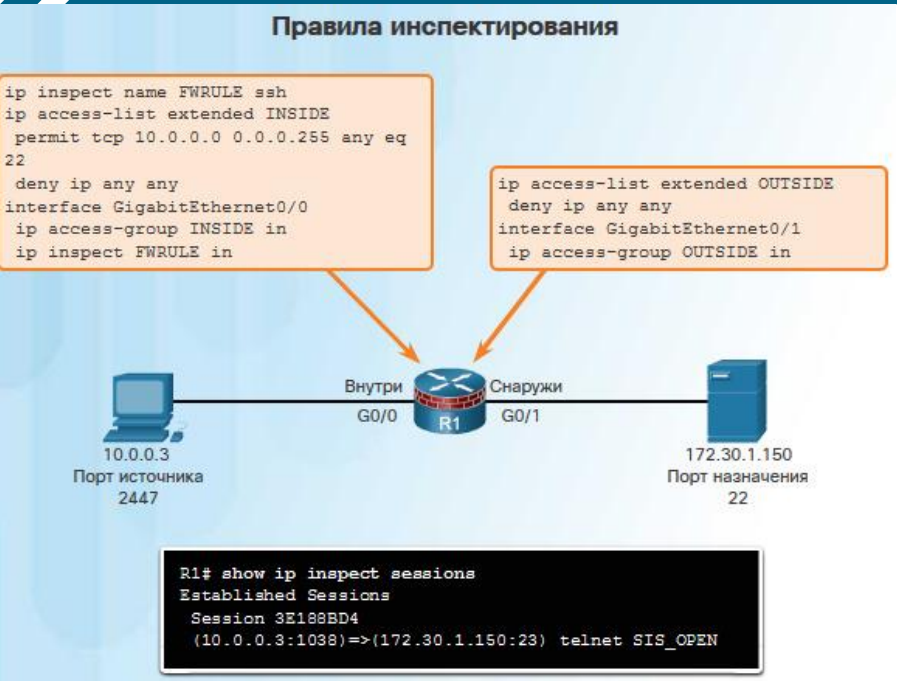
3. Информация о соединении сравнивается с записями в таблице состояний. Если это соединение не существует в настоящее время, добавляется соответствующая запись. Если же оно существует, происходит сброс таймера простоя для данного соединения.

4. При необходимости добавления новой записи, в список ACL добавляется динамическая запись, разрешающая возврат SSH-трафика, который является частью того же самого соединения. Это временно открытое окно функционирует до тех пор, пока остается открытой соответствующая сессия. Такие динамические записи из списков ACL не сохраняются в энергонезависимом ОЗУ (NVRAM).

5. После завершения сессии динамическая информация из таблицы состояний и динамическая запись из списка ACL удаляются.

Классический межсетевой экран также может быть настроен для проверки трафика в двух направлениях: входящем и исходящем. Такой подход удобен при защите двух сегментов сети, в которых обе стороны инициируют определенные соединения и разрешается, чтобы возвратный трафик попадал к источнику.

Второй учебный вопрос.
Технологии межсетевого экрана



Настройка классического межсетевого экрана

Ознакомьтесь с топологией, показанной на рисунке. Администратор хочет разрешить SSH-сеансы между сетями 10.0.0.0 и 172.30.0.0. Однако инициировать SSH-сеансы разрешается только хостам из сети 10.0.0.0. Все остальные типы доступа запрещены. Чтобы настроить подобную политику с помощью классического межсетевого экрана, необходимо выполнить четыре шага.

Шаг 1. Выберите внутренний и внешний интерфейсы.

В данном примере G0/0 является внутренним интерфейсом, а G0/1 внешним.

Шаг 2. Сконфигурируйте ACL-списки для каждого интерфейса.

Список INSIDE ACL разрешает трафик только из сети 10.0.0.0. Этот список применяется к интерфейсу G0/0. Пока не настроено правило инспектирования, список OUTSIDE ACL будет отклонять входящий трафик из сети 172.30.0.0. Такой подход реализуется для интерфейса G0/1.

Шаг 3. Определите правила инспектирования.

Правило инспектирования FWRULE определяет, что трафик будет проверяться для SSH-соединений. Это правило инспектирования является недействительным, пока не будет применено к какому-либо интерфейсу. Хотя SSH-соединения будут разрешены на интерфейсе G0/0 и смогут достигнуть хоста в сети 172.30.0.0, возвратный SSH-трафик, являющийся входящим для G0/1, по-прежнему будет отклоняться.

Шаг 4. Примените правило инспектирования к интерфейсу.

При применении правила FWRULE к входящему трафику на интерфейсе G0/0 в настройки классического межсетевого экрана будет добавлена запись, разрешающая входящий SSH-трафик между двумя данными хостами. Команда **show ip inspect sessions** позволяет проверить это.

Внутренние и внешние сети

Проектирование межсетевых экранов затрагивает в первую очередь интерфейсы устройств, где трафик разрешается или блокируется по критериям источника, назначения и типа трафика. Некоторые варианты проектных решений представляют собой простое назначение внешних и внутренних сетей, которые определены на двух интерфейсах межсетевого экрана. Как показано на рисунке, публичная (или внешняя) сеть является недоверенной, а частная (внутренняя) сеть является доверенной. Как правило, настройка межсетевого экрана с двумя интерфейсами осуществляется следующим образом:

Трафик из частной сети является разрешенным и контролируется на пути распространения к публичной сети. Контролируемый трафик, возвращающийся из публичной сети и связанный с трафиком, созданным в частной сети, также является разрешенным.

Трафик из публичной сети, поступающий в частную сеть, обычно блокируется.

Второй учебный вопрос.
Технологии межсетевого экрана

Демилитаризованные зоны

Демилитаризованная зона (DMZ) – это такой дизайн межсетевого экрана, в котором один внутренний интерфейс подключен к частной сети, один внешний интерфейс подключен к публичной сети, а имеющийся еще один интерфейс DMZ подключен, как указано на рисунке.

Трафик, исходящий из частной сети, контролируется на пути распространения к публичной сети или сети DMZ. Этот трафик является разрешенным с минимальными ограничениями или без ограничений. Инспектируемый трафик, возвращающийся из сети DMZ или публичной сети в частную сеть, тоже является разрешенным.

Трафик, исходящий из сети DMZ и поступающий в частную сеть, обычно блокируется.

Трафик, исходящий из сети DMZ и поступающий в публичную сеть, разрешается выборочно, в соответствии с требованиями сетевых служб.

Трафик, исходящий из публичной сети и поступающий в сеть DMZ, разрешается выборочно и инспектируется. Такой трафик обычно относится к электронной почте, службе DNS или к соединениям по протоколам HTTP и HTTPS. Возвратный трафик из сети DMZ, поступающий в публичную сеть, разрешается динамически.

Трафик, исходящий из публичной сети и поступающий в частную сеть, блокируется.

Зональные межсетевые экраны (ZBF)

В зональных межсетевых экранах (ZBF) используется концепция зон, которая предоставляет дополнительные возможности для более гибкой настройки. Под зоной подразумевается группа из одного или нескольких интерфейсов с одинаковыми функциями или характеристиками. Концепция зоны помогает определить, в каком месте должен применяться межсетевой экран Cisco IOS.

На рисунке политики безопасности для сетей LAN 1 и LAN 2 идентичны и могут быть сгруппированы в «зону» с целью выполнения настройки межсетевого экрана. По умолчанию трафик между интерфейсами в пределах одной и той же зоны не подпадает под действие какой-либо политики и распространяется беспрепятственно. Однако весь межзональный трафик блокируется. Чтобы разрешить передачу трафика между зонами, необходимо сконфигурировать соответствующую политику, разрешающую трафик или обеспечивающую контроль над ним.

Единственным исключением из этой политики по умолчанию является зона Self маршрутизатора. В зону Self маршрутизатора входит сам маршрутизатор и все IP-адреса его интерфейсов. Настройка политики, включающей зону Self, должна распространяться на входящий и исходящий трафик маршрутизатора. По умолчанию не существует политики для трафика такого типа. При разработке политики для зоны Self необходимо принять во внимание трафик, относящийся к плоскости управления, плоскости менеджмента, а также к протоколам SSH, SNMP и маршрутизации.

Второй учебный вопрос.
Технологии межсетевого экрана

Мн

При многоуровневой защите различные типы меж
безопасности организации дополнительные возможности.

Политики могут применяться как на участках м
определяют, пересылается трафик или отклоняется. Тр
пакетов на граничном маршрутизаторе. Если трафик ра
на систему бастионных хостов, где к нему применяетс
представляет из себя хорошо защищенный компьютер,
трафик поступает на внутренний экранированный маршр
успешного прохождения всех точек применения политик
тип настройки DMZ называется конфигурацией с экранир

Многоуровневая защита не может сама по себе
комплексной эшелонированной системы защиты сетевому

- Межсетевые экраны, как правило, не предотвращ
- Межсетевые экраны не обеспечивают защиты про
- Межсетевые экраны не являются заменой техн

проведения атак или при сбоях оборудования.

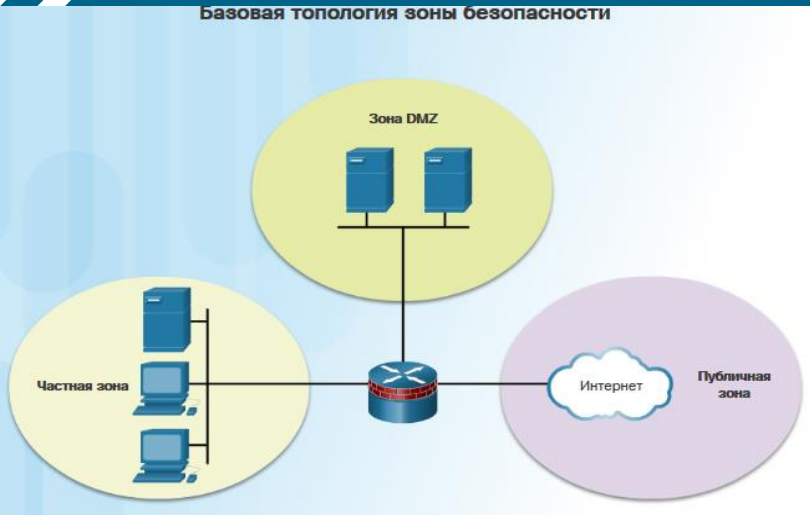
- Межсетевые экраны не могут заменить квалифиц

политики безопасности для межсетевого экрана.

Практические рекомендации для межсетевого экрана

- Устанавливайте межсетевые экраны на границах системы безопасности.
- Межсетевые экраны – это критически важная часть системы безопасности сети. Но для обеспечения безопасности недостаточно полагаться исключительно на межсетевой экран.
- По умолчанию запрещайте любой трафик. Разрешайте только необходимые сервисы.
- Обеспечьте контролируемый физический доступ к межсетевому экрану.
- Следите за системными логами межсетевого экрана.
- Применяйте процедуру управления изменениями в случае изменений конфигурации межсетевого экрана.
- Помните, что межсетевые экраны главным образом защищают от технических атак, происходящих извне.

Третий учебный вопрос.
Зональные межсетевые экраны



Преимущества зональных межсетевых экранов (ZBF)

Существует две модели конфигурации для межсетевого экрана Cisco IOS:

Классический межсетевой экран – Традиционная модель конфигурации, в которой политика межсетевого экрана применяется на интерфейсах.

Зональный межсетевой экран (ZBF) – Новая модель конфигурации, в которой интерфейсы назначаются для зон безопасности, а политика межсетевого экрана применяется к трафику, распространяющемуся между этими зонами.

Как показано на рисунке, при добавлении какого-либо интерфейса к частной зоне подключенные к нему хосты из этой частной зоны могут транслировать трафик всем другим хостам на уже существующих интерфейсах в этой же зоне.

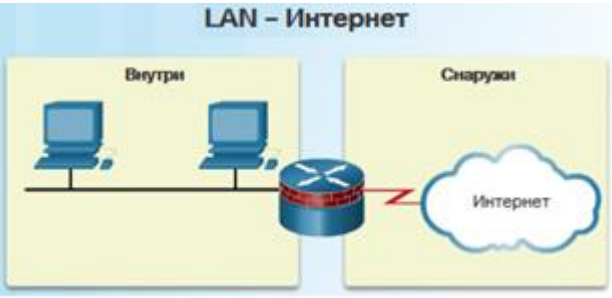
Основными причинами для специалистов по сетевой безопасности к переходу на модель ZBF являются структурированность и удобство использования. Структурный подход удобен для ведения документации и обмена информацией. Удобство использования позволяет реализовывать надежную сетевую безопасность гораздо большему количеству специалистов в этой области.

У зональных межсетевых экранов (ZBF) имеется несколько преимуществ:

- Они не зависят от ACL-списков.
- Маршрутизатор для обеспечения безопасности блокирует трафик, если нет явного разрешения.
- Содержание политик легко читать и исправлять с помощью **Cisco Common Classification Policy Language** (C3PL). C3PL представляет собой метод создания политик для трафика на основе событий, условий и действий. Обеспечивается масштабируемость: одна политика влияет на любой заданный трафик, при этом становятся ненужными списки ACL и действия по инспектированию.
- При выборе между реализацией классического межсетевого экрана или зонального межсетевого экрана (ZBF) необходимо иметь в виду, что обе модели конфигураций могут быть задействованы на маршрутизаторе одновременно. Однако данные модели не могут использоваться на одном и том же интерфейсе. Например, нельзя сконфигурировать интерфейс как элемент зональной безопасности и одновременно использовать его для инспекции IP-адресов.

Дизайн ZBF

Наиболее распространенным является дизайн ZBF при подключении типа LAN – Интернет, который изображен на рис. 1. Межсетевой экран с публичными серверами показан на рисунках 2 и 3. На рис. 4 показаны резервируемые межсетевые экраны. Комплексные межсетевые экраны показаны на рис. 5.



Создание дизайна межсетевых экранов ZBF состоит из нескольких шагов:

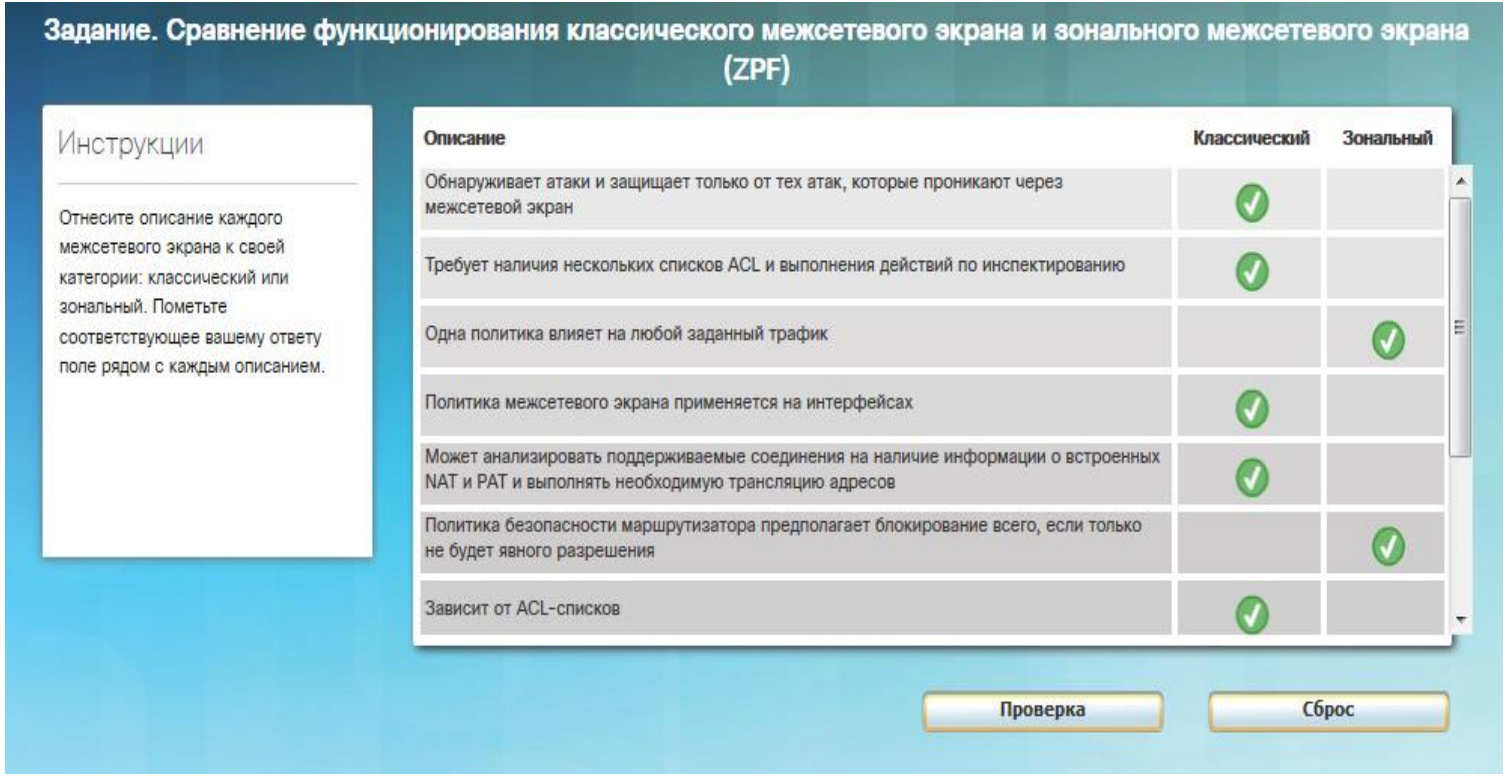
Шаг 1. Определите зоны. – Здесь основной задачей администратора является разделение сетей на зоны. Например, публичная сеть может быть одной из зон, а внутренняя сеть другой.

Шаг 2. Установите политики для зон. – Для каждой пары зон типа «источник-место назначения» (например, из внутренней сети к Интернету) необходимо определить сессии, в рамках которых у клиентов из зоны источника будет возможность отправлять запросы на серверы из зоны места назначения. В таких сессиях наиболее часто используются протоколы TCP и UDP, но может применяться и протокол ICMP, например для отправки эхо-запросов. Для трафика, к которому неприменимо понятие сессии, администратору необходимо определить ненаправленные потоки от источника к месту назначения и наоборот.

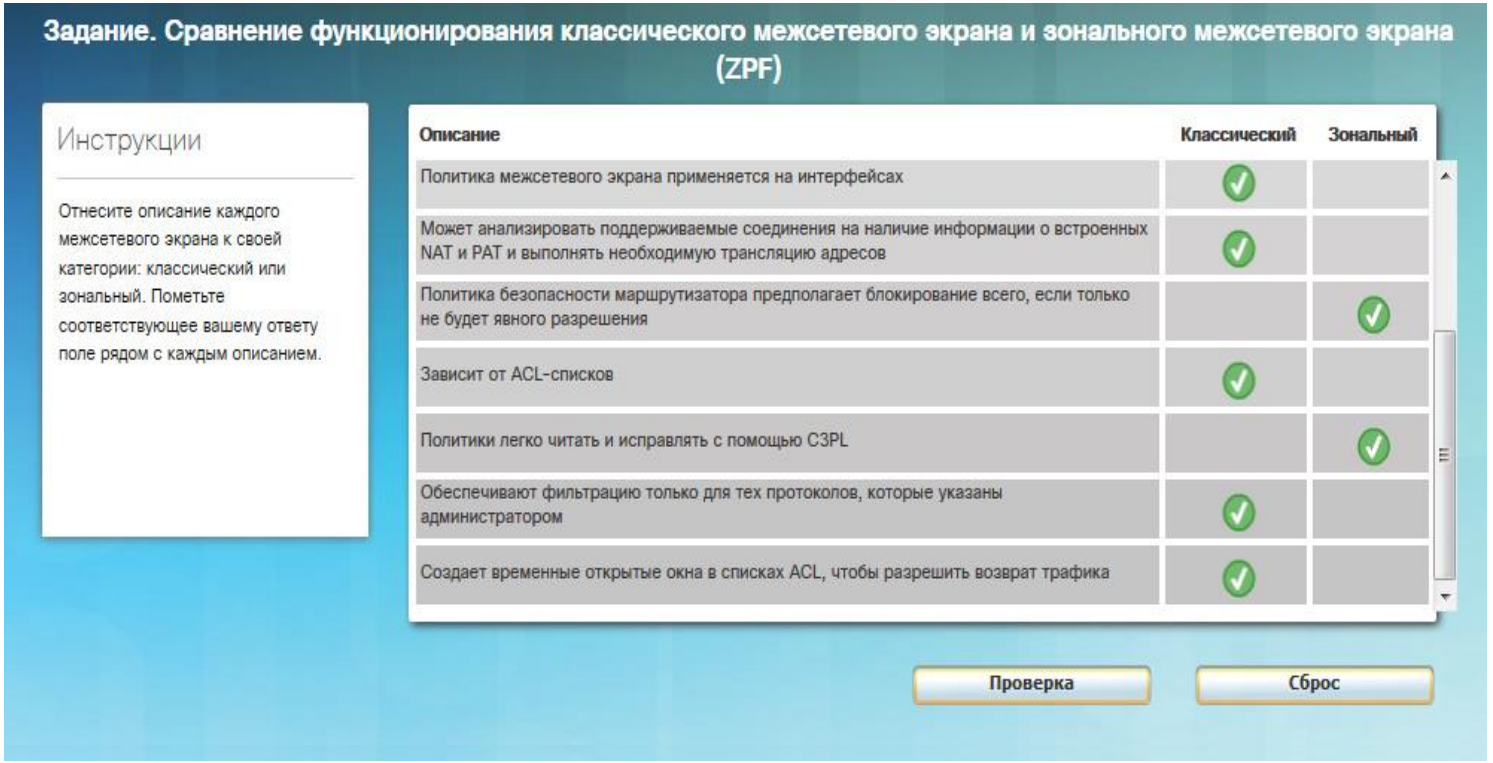
Шаг 3. Составьте схему физической инфраструктуры. – После определения зон и документального оформления требований в отношении трафика между ними администратору необходимо спроектировать физическую инфраструктуру. При этом администратор должен принять во внимание требования, касающиеся безопасности и доступности. Сюда входит, с одной стороны, задание количества устройств для участков между наиболее и наименее защищенными зонами, а с другой – определение резервируемых устройств.

Шаг 4. Определите множества устройств в рамках зон и объедините требования к их трафику. – Для каждого устройства, входящего в состав межсетевого экрана, администратор должен определить зональные множества устройств, подключенные к интерфейсам этого устройства, и объединить для этих зон требования к их трафику. Например, может оказаться, что несколько зон будут опосредованно подключены к одному и тому же интерфейсу межсетевого экрана. Это должно быть отражено в межзональной политике для конкретного устройства.

Третий учебный вопрос.
Зональные межсетевые экраны



Третий учебный вопрос.
Зональные межсетевые экраны



Операции, выполняемые ZBF

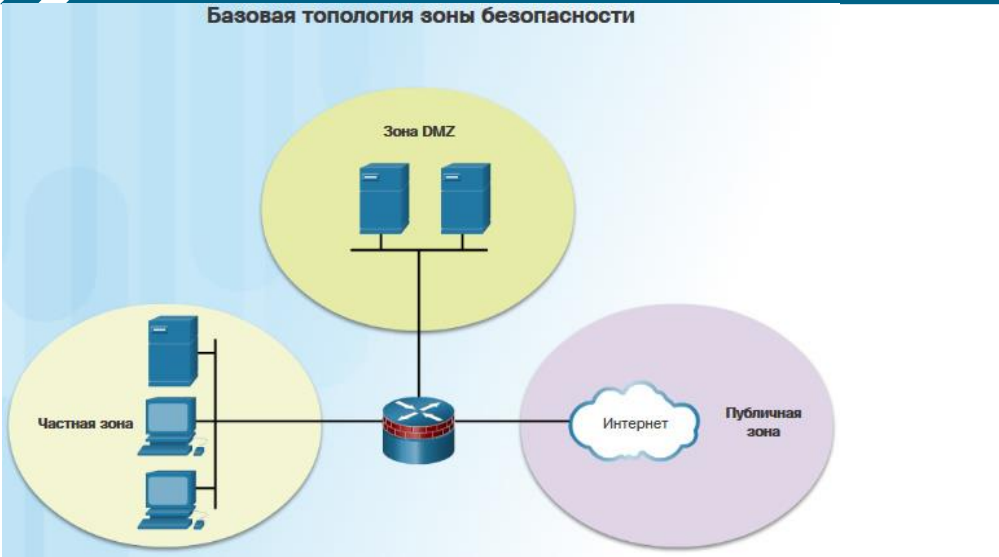
Межсетевой экран ZBF, входящий в Cisco IOS, может выполнять три операции:

Инспектирование – Реализует механизм Cisco IOS инспектирования пакетов с сохранением состояний.

Отбрасывание – Является аналогом оператора запрета из списка ACL. А **log** позволяет фиксировать в журнале информацию об отклоненных пакетах.

Пропуск – Является аналогом оператора разрешения из списка ACL. Действие по пропуску трафика не отслеживает состояние подключения или сеансов в трафике.

Третий учебный вопрос.
Зональные межсетевые экраны



Транзитный трафик: пропуск, отбрасывание или инспектирование?

Интерфейс источника – член зоны?	Интерфейс назначения – член зоны?	Пара зон существует?	Политика существует?	Результат
НЕТ	НЕТ	Н/П	Н/П	ПРОПУСК
ДА	НЕТ	Н/П	Н/П	ОТБРАСЫВАНИЕ
НЕТ	ДА	Н/П	Н/П	ОТБРАСЫВАНИЕ
ДА (частная)	ДА (частная)	Н/П	Н/П	ПРОПУСК
ДА (частная)	ДА (общедоступная)	НЕТ	Н/П	ОТБРАСЫВАНИЕ
ДА (частная)	ДА (общедоступная)	ДА	НЕТ	ПРОПУСК
ДА (частная)	ДА (общедоступная)	ДА	ДА	ИНСПЕКТИРОВАНИЕ

Правила для транзитного трафика

Трафик, проходящий через интерфейс маршрутизатора, подвергается проверке на соответствие нескольким правилам, определяющим работу интерфейса. С примером транзитного трафика можно ознакомиться на рис. 1, где приведена соответствующая топология.

Правила зависят от того, являются ли входные и выходные интерфейсы членами одной и той же зоны, как показано на рис. 2:

Если ни один из интерфейсов не является членом зоны, то прохождение трафика разрешается.

Если оба интерфейса является членами одной и той же зоны, то прохождение трафика разрешается.

Если один из интерфейсов является членом зоны, а второй им не является, то результатом будет отбрасывание трафика, вне зависимости от того, существует ли соответствующая пара зон.

Если оба интерфейса принадлежат одной и той же паре зон и для нее существует политика, выполнение операций инспектирования, разрешения или отбрасывания определяется в соответствии с этой политикой.

Третий учебный вопрос.
Зональные межсетевые экраны

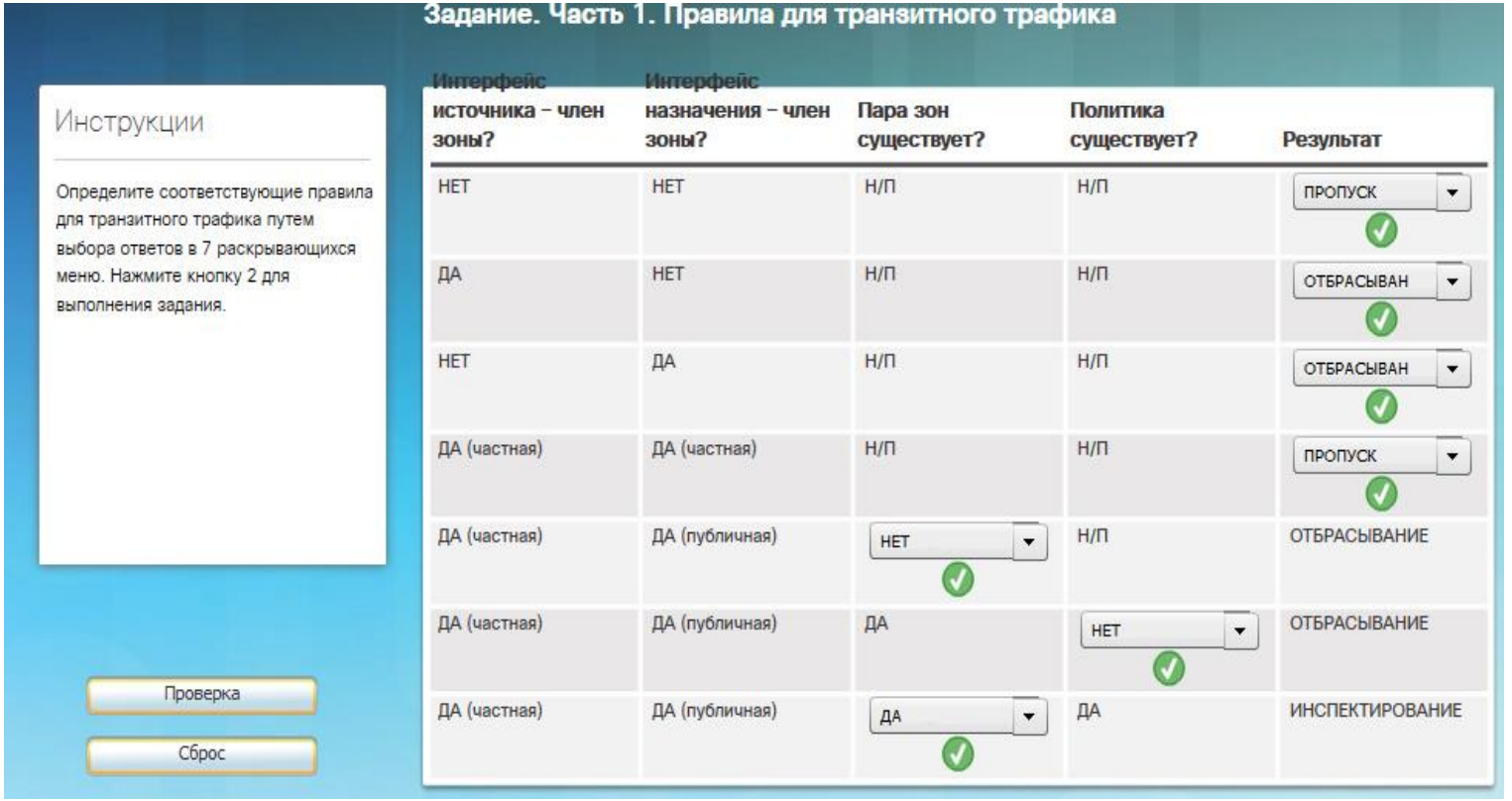
Трафик собственной (Self) зоны: пропуск, отбрасывание или инспектирование?

Интерфейс источника – член зоны?	Интерфейс назначения – член зоны?	Пара зон существует?	Политика существует?	Результат
YES (собственная зона)	ДА	НЕТ	Н/П	ПРОПУСК
YES (собственная зона)	ДА	ДА	НЕТ	ПРОПУСК
YES (собственная зона)	ДА	ДА	ДА	ИНСПЕКТИРОВАНИЕ
ДА	YES (собственная зона)	НЕТ	Н/П	ПРОПУСК
ДА	YES (собственная зона)	ДА	НЕТ	ПРОПУСК
ДА	YES (собственная зона)	ДА	ДА	ИНСПЕКТИРОВАНИЕ

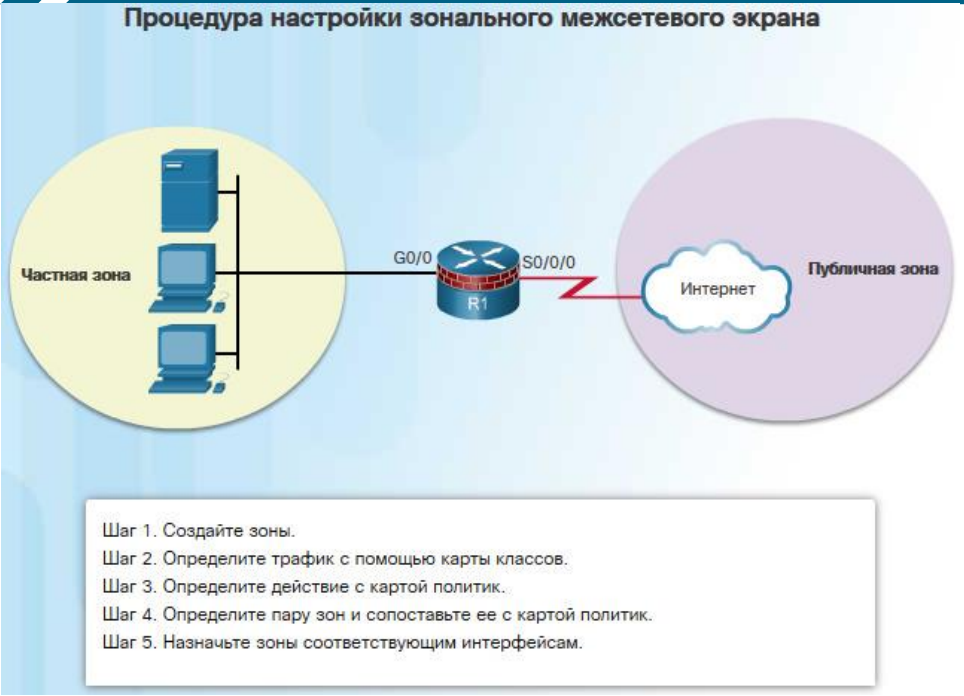
Правила для трафика, идущего в собственную (self) зону

В собственную зону (Self) маршрутизатора входит сам маршрутизатор и все IP-адреса его интерфейсов. Правила для межсетевого экрана ZBF в зоне **Self** определяются иначе. С примером трафика в зоне Self можно ознакомиться на рис. 1, где приведена соответствующая топология.

Правила зависят от того, является ли маршрутизатор источником или местом назначения трафика, как показано на рис. 2: Если маршрутизатор является источником или местом назначения, тогда весь трафик пропускается. Единственное исключение представляет ситуация, когда источник и место назначения являются парой зон со специальной политикой обслуживания. В таком случае эта политика применяется ко всему трафику.


Задание. Часть 1. Правила для транзитного трафика
Инструкции
Определите соответствующие правила для транзитного трафика путем выбора ответов в 7 раскрывающихся меню. Нажмите кнопку 2 для выполнения задания.
Проверка
Сброс
Интерфейс источника – член зоны?
Интерфейс назначения – член зоны?
Пара зон существует?
Политика существует?
Результат
НЕТ
НЕТ
Н/П
Н/П
ПРОПУСК
ДА
НЕТ
Н/П
Н/П
ОТБРАСЫВАН
НЕТ
ДА
Н/П
Н/П
ОТБРАСЫВАН
ДА (частная)
ДА (частная)
Н/П
Н/П
ПРОПУСК
ДА (частная)
ДА (публичная)
НЕТ
Н/П
ОТБРАСЫВАНИЕ
ДА (частная)
ДА (публичная)
ДА
НЕТ
ОТБРАСЫВАНИЕ
ДА (частная)
ДА (публичная)
ДА
ДА
ИНСПЕКТИРОВАНИЕ

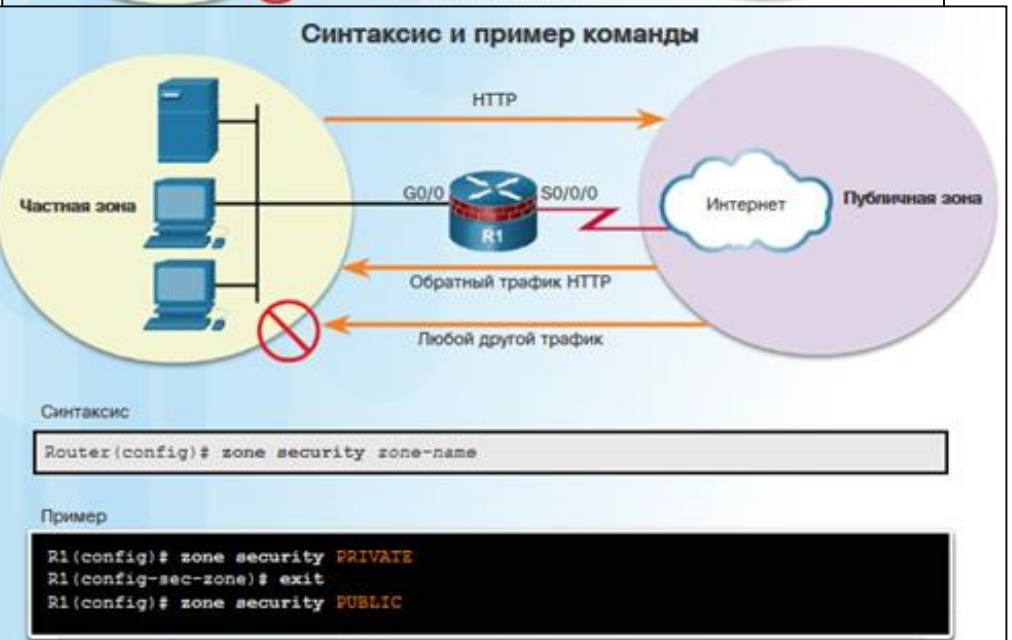
Третий учебный вопрос.
Зональные межсетевые экраны



Настройка межсетевого экрана ZBF

Топология и шаги, приведенные на рисунке, будут использоваться в этом разделе для демонстрации процесса настройки зонального межсетевого экрана ZBF. Выполнение всей последовательности шагов необязательно. Однако некоторые действия по настройке необходимо выполнять в указанном порядке. Например, карту классов необходимо сконфигурировать перед тем, как назначать ее карте политик. Также нельзя назначать карту политик паре зон, не выполнив прежде конфигурацию политики. При попытке настройки раздела, который зависит от другой, но еще не настроенной части конфигурации, ответом маршрутизатора будет сообщение об ошибке.

Третий учебный вопрос.
Зональные межсетевые экраны



Создайте зоны

Первый шаг, как показано на рис. 1, состоит в создании зон. Однако до создания зон необходимо ответить на несколько вопросов:

Какие интерфейсы должны быть включены в эту зону?

Какие названия будут у зон?

Какой трафик между зонами является необходимым и в каком направлении?

В топологии из приведенного примера имеется два интерфейса и две зоны, а трафик распространяется только в одном направлении. Трафик, поступающий из публичной зоны, не будет допущен. Создайте зоны для межсетевого экрана с помощью команды **zone security**, как показано на рис. 2.

Шаг 2. Определите трафик

Второй шаг, как показано на рис. 1, состоит в использовании карты классов для определения трафика. Класс используется для идентификации набора пакетов на основе их содержимого с использованием условий соответствия. Как правило, класс определяется таким образом, чтобы можно было применять к идентифицированному трафику какое-либо действие, отражающее определенную политику. Класс определяется с помощью карт классов.

Синтаксис команды class-map

```
Router(config)# class-map type inspect [match-any | match-all] class-map-name
```

Параметр	Описание
match-any	Если пакеты удовлетворяют одному из критериев совпадения, они считаются членом класса.
match-all	Если пакеты удовлетворяют всем критериям совпадения, они считаются членом класса.
class-map-name	Имя карты классов, используемой для настройки политики для класса в карте политик.

На рис. 2 представлен синтаксис команды **class-map**. Карты классов бывают нескольких типов. Ключевое слово **inspect** используется для определения карты классов при конфигурации межсетевого экрана ZBF. Определите способ оценки пакетов для ситуации с несколькими критериями совпадения. Пакеты должны удовлетворять одному из критериев совпадения (**match-any**) или всем критериям совпадения (**match-all**), чтобы считаться членом класса.

Синтаксис субрежима команды class-map

```
Router(config-cmap)# match access-group {acl-# | acl-name }
Router(config-cmap)# match protocol protocol-name
Router(config-cmap)# match class-map class-map-name
```

Параметр	Описание
match access-group	Настраивает критерии совпадения для карты классов на основе заданного номера или имени списка ACL.
match protocol	Настраивает критерии совпадения для карты классов на основе заданного протокола.
match class-map	Использует другую карту классов для определения трафика.

На рис. 3 представлен синтаксис для правил совпадения в субрежиме команды class-map. Выполните проверку трафика на соответствие по списку ACL, по определенному протоколу или даже по другой карте классов.

В топологии на рис. 4 HTTP-трафик разрешен для прохождения от маршрутизатора R1 к зоне PUBLIC. В случае разрешения HTTP-трафика рекомендуется явным образом включать в категорию разрешенных также протоколы HTTPS и DNS. Чтобы получить статус члена класса HTTP-TRAFFIC, трафик может удовлетворять любому из указанных правил.

Пример настройки карты class-map


```
R1(config)# class-map type inspect match-any HTTP-TRAFFIC
R1(config-cmap)# match protocol http
R1(config-cmap)# match protocol https
R1(config-cmap)# match protocol dns
```

Третий учебный вопрос.
Зональные межсетевые экраны

Шаг 3.Определите действие

Третий шаг, как показано на рис. 1, состоит в использовании карты политик с целью определения применяемых действий для трафика, принадлежащего некоторому классу. На рис. 2 показан синтаксис команды для конфигурирования карты политик. Под действиями подразумеваются выполняемые функции. Они обычно относятся к классу трафика. Например, **inspect**, **drop** и **pass** являются действиями.

Синтаксис команды policy-map

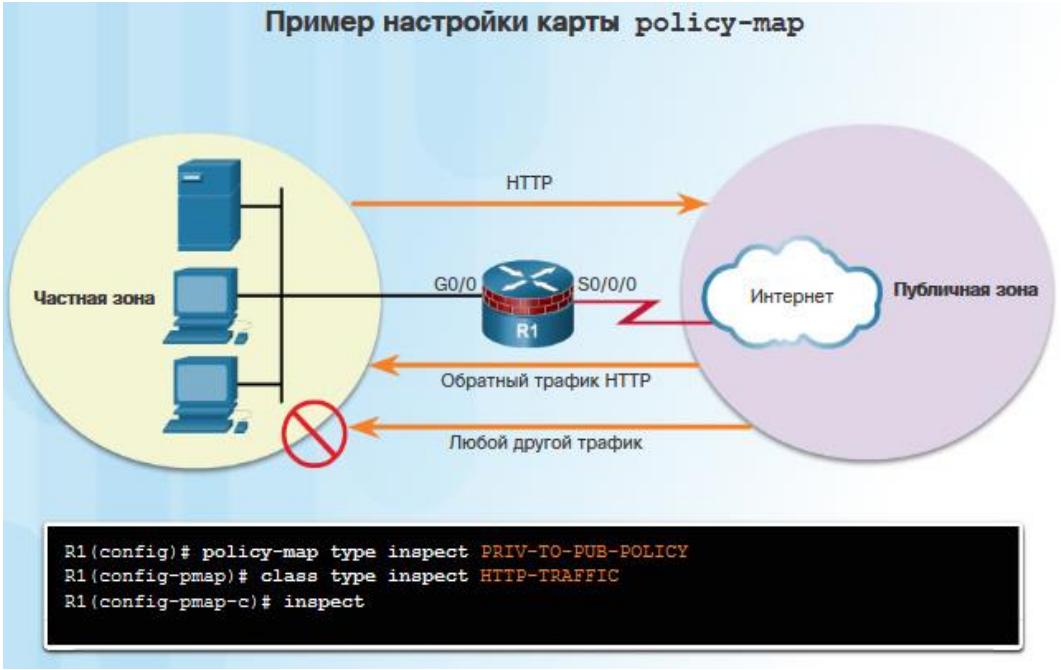
```
Router(config)# policy-map type inspect policy-map-name
Router(config-pmap)# class type inspect class-map-name
Router(config-pmap-c)# { inspect | drop | pass }
```

Параметр	Описание
inspect	Действие, которое обеспечивает контроль трафика на основе состояния. Маршрутизатор отслеживает информацию о сеансе для протоколов TCP и UDP и разрешает обратный трафик.
drop	Отбрасывает нежелательный трафик
pass	Действие без отслеживания состояния, которое позволяет маршрутизатору отправлять трафик из одной зоны в другую

inspect – Это действие обеспечивает контроль трафика на основе состояния. Например, если трафик, распространяющийся из зоны **PRIVATE** к зоне **PUBLIC**, является контролируемым, то маршрутизатор сохраняет информацию о подключениях и сессиях для трафика по протоколам TCP и UDP. Маршрутизатор в таком случае разрешает возвратный трафик, поступающий от хостов зоны **PUBLIC** в ответ на запросы, направляемые через подключения из зоны **PRIVATE.**

drop – Данное действие применяется по умолчанию ко всему трафику. Аналогично оператору **deny any**, применяемому по умолчанию в конце каждого списка ACL, существует явное действие **drop**, применяемое IOS в конце каждой карты политик. Это обозначено как **class class-default** в последнем разделе каждой конфигурации карты политик. Другие карты классов в карте политик также могут быть сконфигурированы для отбрасывания нежелательного трафика. В противоположность спискам ACL, отбрасывание трафика никак не обозначается, и сообщения по протоколу ICMP о недоступности не отправляются источнику трафика.

pass – Это действие позволяет маршрутизатору отправлять трафик из одной зоны в другую. При выполнении действия pass не ведется отслеживание состояния подключений. Это действие разрешает прохождение трафика только в одном направлении. Чтобы разрешить возвратный трафик в обратном направлении, необходимо применить соответствующую политику. Действие pass идеально подходит для защищенных протоколов с предсказуемым поведением, таких как IPsec.



На рис. 3 приводится пример конфигурации карты политик. Класс **HTTP-TRAFFIC**, который сконфигурирован на предыдущем шаге, связан с новой картой политик, обозначенной как **PRIV-TO-PUB-POLICY**.

Третья по счету команда **inspect** выполняет конфигурирование маршрутизатора R1 для сохранения информации о состоянии всего трафика, который является членом класса **HTTP-TRAFFI**C.

Синтаксис команд zone-pair и service-policy

```
Router(config)# zone-pair security zone-pair-name source {source-zone-name | self
} destination {destination-zone-name | self }
Router(config-sec-zone-pair)# service-policy type inspect policy-map-name
```

Параметр	Описание
`source source-zone-name`	Указывает имя зоны, из которой поступает трафик.
`destination destination-zone-name`	Указывает имя зоны, в которую должен быть отправлен трафик.
`self`	Указывает зону, определенную системой. Указывает, будет ли трафик передаваться в маршрутизатор или из него.

Шаг 4. Определите пару зон и политику для совпадений

Содержание четвертого шага, как показано на рис. 1, составляет определение пары зон и привязка этой пары зон к карте политик.

На рис. 2 показан синтаксис соответствующей команды. Создайте пару зон с помощью команды **zone-pair security** . Затем используйте команду **service-policy type inspect** , чтобы привязать карту политик и связанные с ней действия к паре зон.

На рис. 3 приводится пример конфигурации пары зон. При создании пары зон **PRIV-PUB**, для нее назначена в качестве источника зона **PRIVATE**, а в качестве места назначения зона **PUBLIC**. Затем к этой паре зон прикреплена карта политик, созданная на предыдущем шаге.

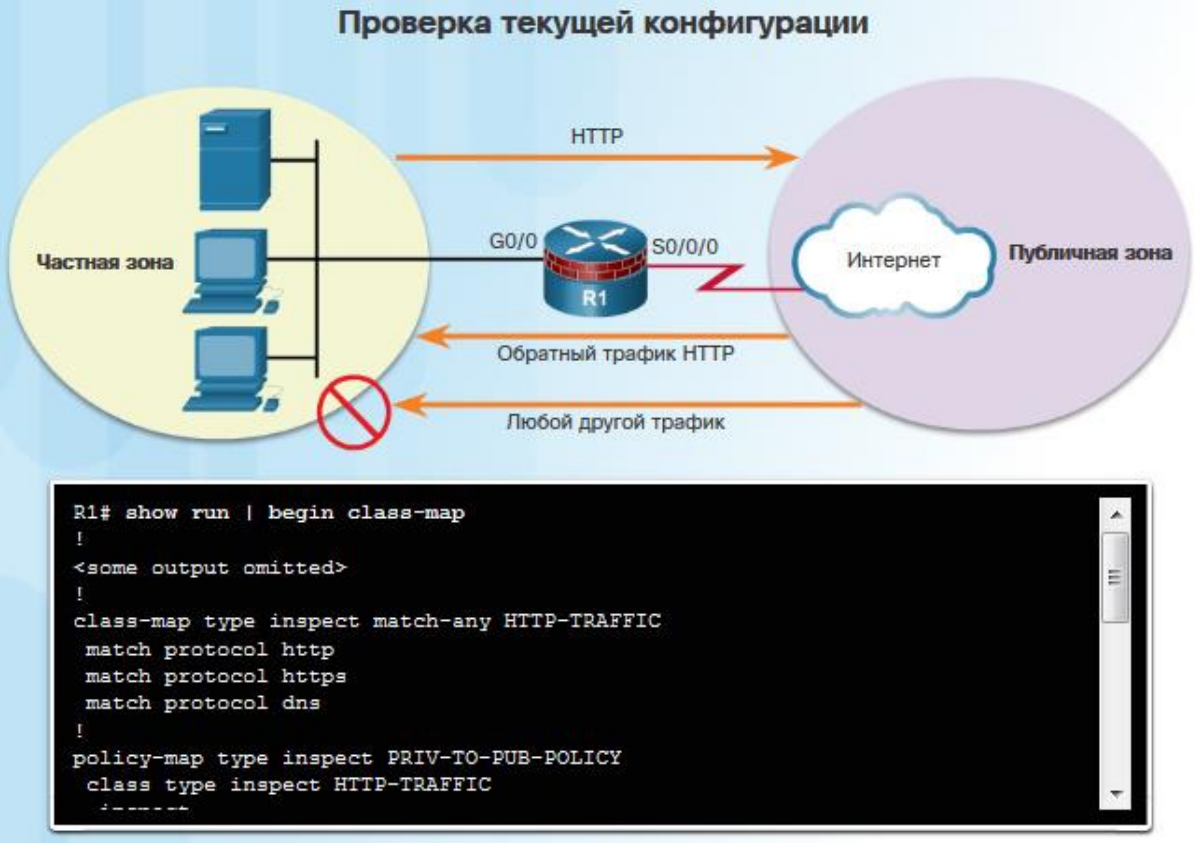
После выполнения конфигурации межсетевого экрана администратор применяет его к трафику между парой зон с помощью команды **zone-pair security**. Для применения политики ее необходимо назначить для пары зон. Для формирования пары зон необходимо указать зону источника, зону назначения и политику для обработки трафика между этими зонами.

Для назначения зоны интерфейсу необходимо использовать команду **zone-member** security, как показано на рис. 2. В данном примере интерфейс GigabitEthernet 0/0 назначен зоне **PRIVATE**, а интерфейс Serial 0/0/0 назначен зоне **PUBLIC**.

Теперь политика обслуживания будет функционировать. Трафик по протоколам HTTP, HTTPS и DNS, исходящий из зоны **PRIVATE** и предназначенный для зоны **PUBLIC**, будет контролироваться. Трафик, исходящий из зоны **PUBLIC** и предназначенный для зоны **PRIVATE**, будет пропускаться только в случае, если он является частью сессий, изначально инициированных хостами из зоны **PRIVATE**.

Шаг 5. Назначьте зоны интерфейсам

Пятый шаг, как показано на рис. 1, состоит в назначении зон соответствующим интерфейсам. Привязка зоны к интерфейсу незамедлительно влечет за собой применение политики обслуживания, которая была назначена этой зоне. Если политика обслуживания еще не сконфигурирована для зоны, весь транзитный трафик будет отбрасываться.



Проверка конфигурации ZBF

Выполните проверку текущей конфигурации межсетевого экрана ZBF, оценивая ее, как это показано на рис. 1. Обратите внимание, что сначала приводится карта классов. Затем карта политик использует эту карту классов. Также следует отметить специально выделенное действие **class class-default**, которое отбрасывает весь трафик, не являющийся членом класса HTTP-TRAFFIC.

Конфигурации зон располагаются после конфигураций карт политик, где указываются названия зон, пары зон и выполняется назначение политик обслуживания парам зон. И в конце зоны назначаются интерфейсам.


```
R1# show policy-map type inspect zone-pair sessions

policy exists on zp PRIV-PUB
  Zone-pair: PRIV-PUB

  Service-policy inspect : PRIV-TO-PUB-POLICY

    Class-map: HTTP-TRAFFIC (match-any)
      Match: protocol http
        12 packets, 384 bytes
        30 second rate 0 bps
      Match: protocol https
        5 packets, 160 bytes
```

На рис. 2 показана проверочная информация после тестирования конфигурации межсетевого экрана ZBF. Хост 192.168.1.3 из зоны PRIVATE установил HTTPS-сессию с веб-сервером по адресу 10.1.1.2.

Обратите внимание далее в результате команды на то, что четыре пакета оказались соответствующими классу **class class-default**.

Эта проверочная информация была создана при отправке хостом 192.168.1.3 эхо-запроса на веб-сервер с адресом 10.1.1.2.


```
Router# show class-map type inspect
Router# show zone security
Router# show zone-pair security
Router# show policy-map type inspect
```

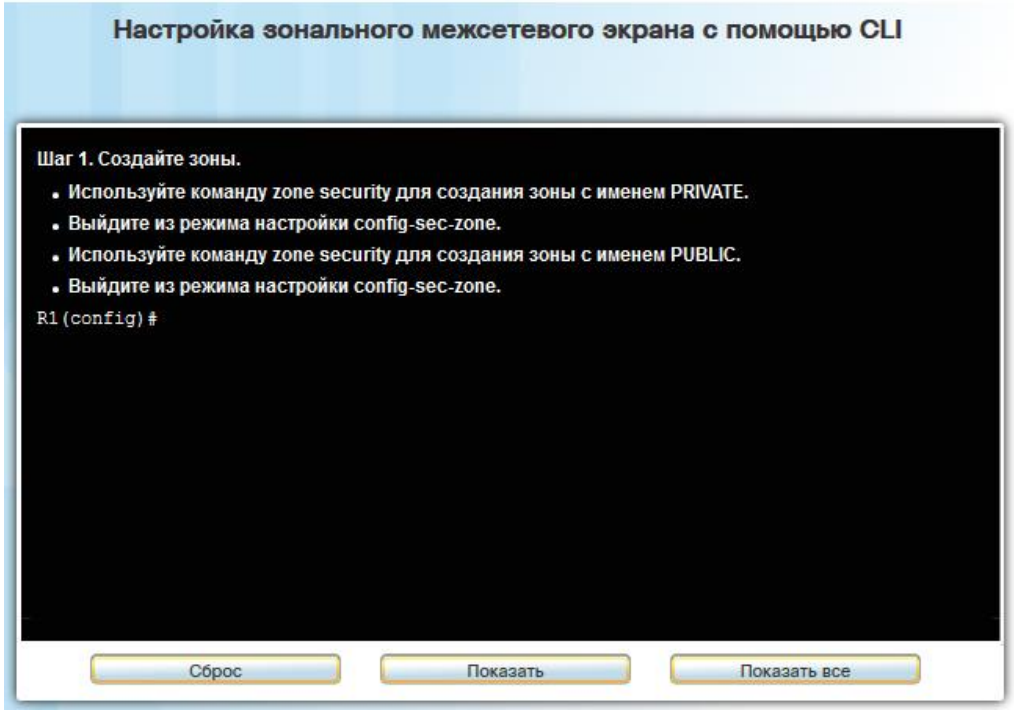
```
R1# show class-map type inspect
 Class Map type inspect match-any HTTP-TRAFFIC (id 1)
   Match protocol http
   Match protocol https
   Match protocol dns

R1# show zone security
zone self
Description: System Defined Zone
```

На рис. 3 приводятся дополнительные проверочные команды, которые позволяют просматривать отдельные части конфигурации межсетевого экрана ZBF.

Выводы по третьему вопросу. Зональные межсетевые экраны

С помощью средства проверки синтаксиса, приведенного на рисунке, сконфигурируйте маршрутизатор R1 с межсетевым экраном ZBF.



Внедрение технологий межсетевого экрана

Учебные вопросы:

1. Списки контроля доступа.
2. Технологии межсетевого экрана.
3. Зональные межсетевые экраны.

Заключение

Межсетевые экраны отделяют защищенные области сети от незащищенных. Это не позволяет пользователям без соответствующих полномочий получать доступ к защищенным сетевым ресурсам.

Существует два наиболее распространенных метода для реализации межсетевых экранов:

Межсетевой экран с фильтрацией пакетов - Как правило, это маршрутизатор с возможностью фильтрации каких-либо пакетных данных, например это может быть информация, относящаяся к уровню 3 и иногда к уровню 4 с помощью списков ACL.

Межсетевой экран с сохранением состояния - Выполняет отслеживание таких параметров, как инициирование, передача данных или состояние после завершения использования.

Возможность пакетной фильтрации в межсетевых экранах обеспечивается стандартными или расширенными списками ACL для IP-адресов. Такие межсетевые экраны являются базовыми инструментами как для фильтрации трафика, так и для предотвращения самых разных сетевых атак. Выбор конкретного варианта межсетевого экрана определяется типом трафика, а также характеристиками источника и места назначения этого трафика. Списки ACL привязаны к потоку сетевого трафика. Содержание и применение списков ACL определяется сетевой топологией.

Межсетевые экраны с отслеживанием состояний могут быть реализованы тремя способами:

Решения для фильтрации трафика - Сюда входят списки ACL, в которых используется параметр протокола TCP **established**, и рефлексивные списки ACL с расширенными функциональными возможностями, учитывающими двунаправленный характер сетевого трафика.

Классический межсетевой экран Cisco IOS - Ранее обозначавшийся как CBAC классический межсетевой экран предоставляет возможности для эффективной и учитывающей состояния фильтрации трафика от большинства современных приложений. Настройка классического межсетевого экрана – процесс достаточно сложный и зависит от надлежащего применения списков ACL и правил инспектирования к соответствующим интерфейсам.

Зональный межсетевой экран (ZBF) - Появившись в 2006 году, эта технология является на данный момент самой передовой для межсетевых экранов. Основной задачей при настройке конфигурации межсетевого экрана ZBF является создание зон, которые соотнесены с различными сегментами сети и предназначены для обеспечения разных уровней защиты. Реализация межсетевого экрана ZBF является более структурированной и удобной для понимания по сравнению с CBAC.

Для классификации и фильтрации трафика в ZBF используются такие средства, как карты классов и карты политик.