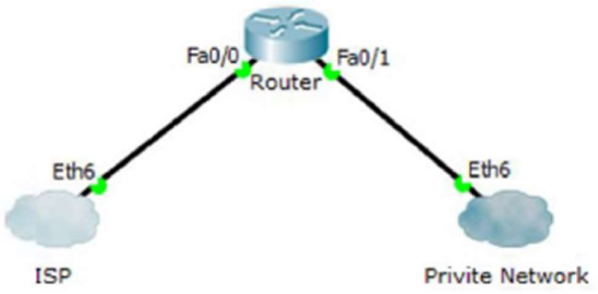
Защита№7

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ. DMZ

1. Назначение и принцип работы ACL.

Списки контроля доступа (Access Control List, ACL) – это набор правил, которые устанавливают критерии проверки определённых заголовков и советующие действия над пакетом при совпадении указанных критериев в правилах с содержимым его заголовков. При настройке ACL разрешаются или запрещаются IP-пакеты, при этом возможен анализ IP-пакета по типу пакета, TCP и UDP порты. Также ACL можно настроить для различных сетевых протоколов. В основном применение списков доступа рассматривают для реализации сетевой фильтрации. Списки доступа позволяют создавать правила управления трафиком, по которым будет происходить межсетевое взаимодействие, как в локальных, так и в глобальных сетях. Применительно к сетевой фильтрации на маршрутизаторах, разные ACL создаются независимо и применяются к определенным интерфейсам, после чего маршрутизатор анализирует трафик как входящий и исходящий только на указанном интерфейсе. Тот трафик, который приходит на интерфейс маршрутизатора называется входящим, тот который выходит - исходящий. Соответственно ACL могут размещаться на входящем или на исходящем направлении интерфейса.

Рассмотрим принцип работы ACL на примере сети, представленной на рисунке 7.1.

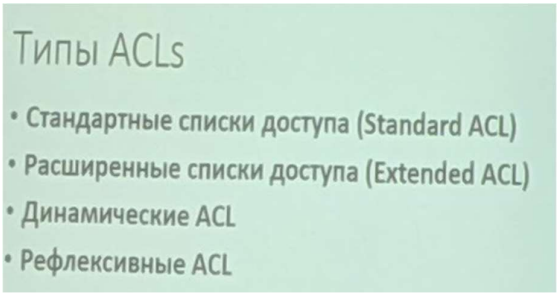


Например, из частной сети приходит пакет на интерфейс маршрутизатора FaO/1, маршрутизатор проверяет, есть ли ACL на входящем направлении интерфейса FaO/1 или нет. Если он есть, то дальше анализ пакета ведется по правилам списка контроля доступа строго в том порядке, в котором записаны правила. Если маршрутизатор обнаруживает совпадение указанных в правиле параметров (IP-адреса, номера портов) с содержимым заголовков анализируемого пакета, то проверяется соответствующее данному правилу действие (запретить или разрешить прохождение данного пакета). Если списка контроля доступа нет - пакет проходит без всяких ограничений на интерфейс FaO/O. Перед тем как отправить пакет маршрутизатор проверяет наличие ACL на исходящем направлении интерфейса FaO/O.

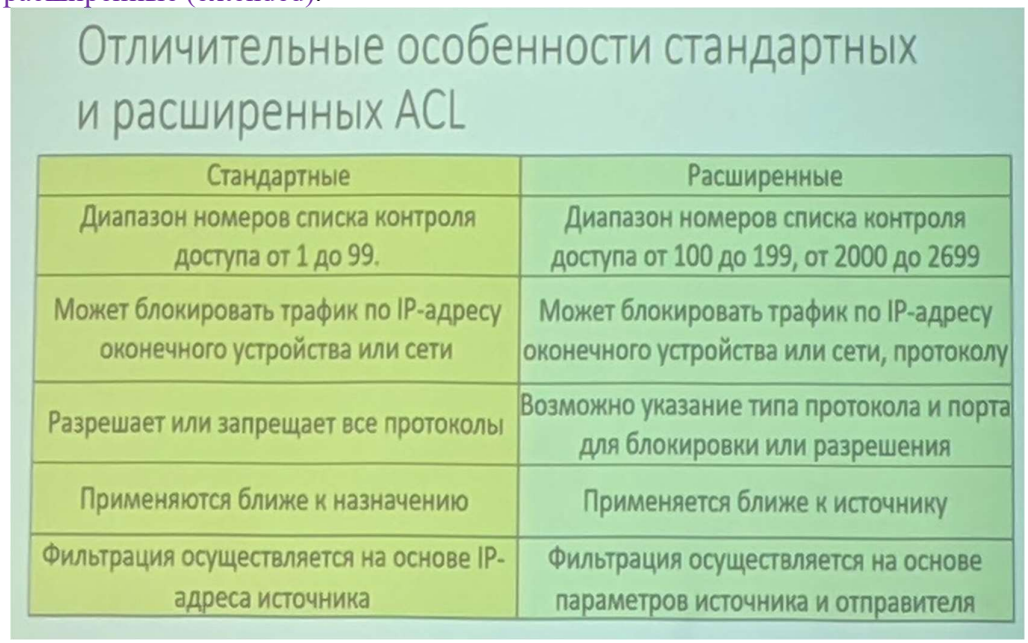
Если ACL с правилом блокировки доступа к глобальной сети внутренним устройствам настроен на входящем направлении интерфейса FaO/1, то пакет будет сразу заблокирован, не потребуется его дополнительная обработка (проверка таблицы маршрутизации, передача на интерфейс FaO/O и проверка ACL на данном интерфейсе).

Работа списка доступа напрямую зависит от порядка следования правил в этом списке, где в каждой строке записано правило обработки трафика. Просматриваются все правила списка с первого до последнего по порядку, но просмотр завершается, как только было найдено первое соответствие, т.е. если для пришедшего пакета было найдено правило, под которое он подпадает, остальные правила проверяться не будут. Если пакет не подпал ни под одно из правил, то включается правило указанное по умолчанию в самом конце ACL.

2. Типы ACL и их отличия.



Существует два основных типа списков доступа: стандартные (standart) и расширенные (extended).



Также выделяют динамические (Dynamic ACL) и рефлексивные (Reflexive ACL) списки доступа.

Динамический ACL позволяет ограничивать доступ к серверам из внешней сети. Например, на маршрутизаторе, который подключен к какому-то серверу, необходимо закрыть доступ из внешней сети, но в тоже время есть несколько пользователей, которым разрешен доступ к серверу. Для этого настраивается динамический список контроля доступа на входящем направлении, а дальше пользователям, которым разрешен доступ к серверу, необходимо подключиться через Telnet к данному устройству, в результате динамический ACL открывает доступ к серверу, и пользователь может осуществлять доступ по протоколу HTTP или HTTPS. По умолчанию через 10 минут это соединение закрывается, и пользователь вынужден ещё раз выполнить авторизацию по протоколу Telnet, чтобы подключиться к серверу.

Рефлексивные ACL работают следующим образом, блокируется полностью доступ (deny any), при этом формируется ещё один специальный ACL, который анализирует параметры пользовательских соединений, сгенерированных из локальной сети и для них игнорировать правило блокировки трафика. В результате пользователи из сети Интернет не смогут установить соединение, но запросы пользователей, соединения которых сгенерированы из локальной сети, будут приходить ответы. Рефлексивные списки доступа обеспечивают повышенную защиту доступа. Например, когда пользователь в локальной сети отправляет TCP запрос во внешнюю сеть, должно устанавливаться соединение, чтобы пришел TCP ответ от внешнего сервера. Если соединение установлено не будет - пакеты из внешней сети будут блокироваться. При этом такой открытой сессией и ее параметрами может воспользоваться злоумышленник для проникновения в частную сеть.

3. Отличительные особенности настройки стандартных и расширенных списков контроля доступа. Примеры конфигурации стандартных и расширенных ACL.

Для того, чтобы создать стандартный список доступа, необходимо выполнить следующие три этапа:

1. Создать список контроля доступа;
2. Составить правила обработки трафика;
3. Применить список доступа к интерфейсу устройства на вход или на выход.

```
Router1(config)#ip access-list standard 90
Router1(config-std-nacl)# deny 172.20.0.16 0.0.0.15
Router1(config-std-nacl)# permit any
Router1(config)#interface GigabitEthernet0/1.6
Router1(config-subif)#ip access-group 90 out
```

Создание расширенных списков контроля доступа отличается тем, что в правилах после указания действия (permit или deny) должен находиться параметр протокола (IP, TCP, UDP, ICMP и др.), который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с заголовками ICMP, TCP или UDP. Также можно задать проверку определенных номеров портов протоколов TCP или UDP.

Рассмотрим пример запрета доступа по протоколу HTTP к серверу Security.by с IP-адресом 172.20.0.206 (см. рисунок 7.3) всем устройствам кроме устройства администратора с IP-адресом 172.20.0.42:

```
Router6(config)#ip access-list extended Branch1
Router6(config-ext-nacl)#permit tcp host 172.20.0.42 host
172.20.0.206 eq 80
Router6(config-ext-nacl)#deny tcp any any
```

4. Номера портов для разных видов протоколов.

Соответствие номеров протоколов и портов

Номер порта	Протокол	Приложение	Ключевое слово в команде access_list
20	TCP	FTP	data ftp_data
21	TCP	Server Management FTP	ftp
22	TCP	SSH	ssh
23	TCP	Telnet	telnet
25	TCP	SMTP	Smtp
53	UDP, TCP	DNS	Domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	Tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	Snmp

5. Динамические и рефлексивные списки доступа.

(см. вопрос 2)

6. Межсетевое экранирование, функции Cisco ASA.

Межсетевое экранирование - это комплекс аппаратных, программных средств и их комбинации для управления потоком сетевого трафика, предотвращения угроз и несанкционированного доступа, анализа уязвимостей в соответствии с требованиями безопасности.

Межсетевые экраны - это оборудование, программное обеспечение или их комбинация для управления и инспекции и фильтрации потока сетевого трафика между внешними и внутренними локальными сетями (доверенными и ненадежными сетями) с помощью предварительно настроенных правил или фильтров на основе требований безопасности.

Межсетевое экранирование основано на инспектировании трафика в различных системах фильтрации, в которых настроены правила блокировки и пропуска пакетов.

Межсетевой экран Cisco ASA 5505 - многофункциональное программно-аппаратное устройство защиты ресурсов локальной сети от внешних атак.
Основные функции межсетевого экрана Cisco ASA 5505:
- статическая, динамическая маршрутизация;
- поддержка коммутации и маршрутизации более 4000 VLAN;
- ограниченное управление качеством обслуживания (QoS);
- статический, динамический NAT, PAT;
- глубокий анализ содержимого пакетов;
- обнаружения угроз (сканирования и DoS атак);
- инспектирование трафика;
- конфигурация демилитаризованной зоны (DMZ, Demilitarized Zone);
- поддержка различных видов VPN туннелей;
- управление и конфигурация посредством графического (GUI, Graphical User Interface) и командного (CLI, Command Line Interface) интерфейса.
- интегрированный графический менеджер Cisco Adaptive Security Device Manager (ASDM);
- поддержка Power over Ethernet (PoE) и др.

7. Типы систем фильтрации.

Системы фильтрации классифицируют в зависимости от способа анализа содержимого пакета при его прохождении через сетевое оборудования:

- канальная фильтрация, анализ заголовков канального уровня модели OSI, а именно полей заголовков содержащих информацию о MAC-адресах и идентификаторах VLAN, такие системы используются в коммутаторах L2;

- сетевая фильтрация – анализ заголовков сетевого и транспортного уровней модели OSI, а именно полей заголовков содержащих информацию об IP-адресах и портах в TCP и UDP заголовках, такие системы используются в стандартных или в расширенных списках контроля доступа, настраиваемых на межсетевых экранах и маршрутизаторах;

- сеансовая фильтрация – является развитием сетевой фильтрации с возможность создания виртуального соединения от внешнего IP-адреса для исключения прямого соединения из внутренней сети, сеансовая фильтрация реализуется за счет использования технологий NAT;

- фильтрация с контролем состояния – основана на подробном анализе заголовков транспортного уровня, отслеживания типов пакетов TCP, их порядковых номеров и других параметров, которые регистрируются в таблице исходящих TCP-соединений, соответствующих каждой сессии.

- прикладная фильтрация – анализирует содержимое всех заголовков всех уровней модели OSI и передаваемые данные, сочетает в себе функции всех вышеперечисленных

способов фильтрации и обеспечивает дополнительные возможности, такие как аутентификация и авторизация пользователей, разграничение доступа к ресурсам, антивирусная проверка передаваемых данных, фильтрация по URL (веб-фильтрация) и используемых приложений, отслеживание и предотвращение DDoS-атак и др.

8. Принципы базовой конфигурации межсетевого экрана Cisco ASA.

Несмотря на наличие графического интерфейса управления конфигурации межсетевого экрана Cisco ASA 5505, первоначальная настройка производится через интерфейс CLI. Базовые команды для Cisco ASA, практические не отличаются от команд для других сетевых устройств Cisco. В Cisco PT функции межсетевого экрана Cisco ASA существенно ограничены. Например, индивидуальное имя устройства и установка пароля для привилегированного режима настраивается следующими командами:

```
ciscoasa(config)#hostname ASA25106
ASA25106(config)#enable password пароль
```

Для очистки файла конфигурации используется следующая команда:

```
ciscoasa #write erase
ciscoasa #reload
```

При организации сетей с помощью межсетевого экрана Cisco ASA можно организовать внутренние сети, сети с демилитаризованной зоной и внешнюю сеть (рисунок 7.4), для каждой из которых создаются VLAN.

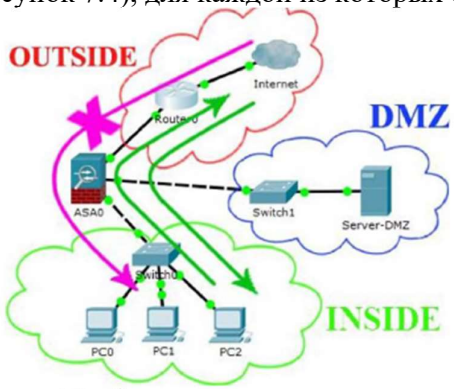


Рисунок 7.4 – Организация сети при использовании межсетевого экрана Cisco ASA

По умолчанию на межсетевом экране Cisco ASA активирована ограниченная лицензия, которая позволяет создать только три VLAN. Для активации расширенной лицензии Security Plus необходимо ввести ключ активации, который можно просмотреть с помощью команды *show activation-key.* После ввода значения ключа в команде activation-key и перезагрузки межсетевого экрана, будет доступно создание двадцати VLAN.

Параметр security level (уровень безопасности) - это число от 0 до 100, которое позволяет сравнить 2 интерфейса и определить, для какого из них уровень безопасности трафика выше. Обычно для внутренних сетей устанавливается уровень безопасности больше, чем для внешних, т.е. с интерфейса с большим уровнем безопасности на интерфейс с меньшим уровнем безопасности трафик пропускается, сессия запоминается и обратно пропускаются только ответы по этим сессиям, такой трафик называется инспектированным. Трафик, идущий в внутреннюю сеть, по умолчанию запрещен.

Параметр nameif (имя интерфейса) позволяет использовать в настройках не физическое наименование интерфейса, а его имя, которое определяет тип сети (inside, outside, dmz и т.д.).

```
ASA25106(config-if)#interface Vlan10
ASA25106(config-if)#nameif inside1
ASA25106(config-if)#security-level 100
ASA25106(config-if)#ip address 192.168.10.1 255.255.255.0
ASA25106(config-if)#no shutdown
ASA25106(config-if)#interface Vlan11

ASA25106(config-if)#nameif inside2
ASA25106(config-if)#security-level 100
ASA25106(config-if)#ip address 192.168.11.1 255.255.255.0
ASA25106(config-if)#no shutdown
ASA25106(config-if)#interface Vlan13
ASA25106(config-if)#nameif outside
ASA25106(config-if)#security-level 0
ASA25106(config-if)#ip address 194.62.64.110
255.255.255.252
ASA25106(config-if)#no shutdown
```

9. Особенности организации сети с межсетевым экраном и демилитаризованной зоной.

(см. вопрос 8)

10. Назначение и принцип конфигурации демилитаризованной зоны.

Демилитаризованная зона используется для размещения в ней общедоступных сервисов, к которым организовывается доступ как из внешней, так и из внутренней сети. При этом трафик из демилитаризованной зоны не должен по ступать во внутреннюю сеть, для исключения атак. Для выполнения этих условий необходимо создать расширенные ACL.

Для настройки демилитаризованной зоны сети используется отдельный VLAN и уровень защиты ниже, чем для внутренней сети. Пример создания демилитаризованной зоны для сети Branch2:

```
ASA25106(config-if)#interface Vlan12
ASA25106(config-if)#nameif DMZ
ASA25106(config-if)#security-level 50
ASA25106(config-if)#ip address 192.168.12.1 255.255.255.0
ASA25106(config-if)#no shutdown
```

К интерфейсу, к которому подключается демилитаризованная зона, прикрепляется созданный VLAN.

```
ASA25106(config)#interface Ethernet0/2
ASA25106(config-if)# switchport access vlan 12
```

вий необходимо создать расширенные ACL. Например, в сети Branch2 есть TLD сервер, к которому по протоколу DNS обращается сервер ROOT, а также на данном сервере активирована электронная почта, на основе этого составляются разрешающие правила ACL и ACL активируется на внешнем интерфейсе.

```
ASA25106(config)#access-list OUTSIDE-DMZ extended permit
tcp any host 194.62.64.118 eq 25
ASA25106(config)#access-list OUTSIDE-DMZ extended permit
tcp any host 194.62.64.118 eq 110
ASA25106(config)#access-list OUTSIDE-DMZ extended permit
udp host 194.62.64.125 host 194.62.64.118 eq 53
ASA25106(config)#access-group OUTSIDE-DMZ in interface
outside
```