МСС-MSN
Тема 12. Лекция 1

ИБ в МСС
Списки управления (контроля) доступом L2 / L3 / L4 — ACL (Access Control List).

Костюкович А.Е.
Каф.АЭС, СибГУТИ
www.aek-54.ru

Классификация угроз информационной безопасности (ИБ)

Угрозы безопасности сетям связи общего пользования. Определения и классификация.

Под угрозами информационной безопасности (ИБ) систем (сетей) связи принято понимать «**воздействия нарушителя ИБ на информационную сферу, которые, будучи не предотвращенными, не обнаруженными и не ликвидированными могут привести к снижению качества услуг и нарушению функционирования сети связи и, как следствие, нанесению ущерба государству, пользователям и (или) поставщикам услуг**».

Различают **три вида источников угроз ИБ**, обусловленные:

1.действием злоумышленников;

2.техническими средствами;

3.стихийными явлениями.

Угрозы **первой группы** включают:

- кражу и разрушение технических средств;
- нарушение нормального функционирования сетей связи;
- подмену операционных систем и другого программного обеспечения;
- отказ от фактов отправки и получения сообщений;
- снижение качества услуг;
- извлечение информации из наводок на электрические и акустические системы.

В число угроз **второй группы** входят:

- нарушение функционирования систем обработки информации и систем (сетей) связи;
- уничтожение средств хранения информации;
- разрушение зданий и помещений;
- нанесение увечий и угрозы жизни персонала;
- изменение программного обеспечения.

Угрозы **третьей группы** вызываются стихийными явлениями:

- землетрясения, наводнения, гроза, цунами и т. п., пожарами, электромагнитными воздействиями при авариях линий передачи.

Они могут приводить к:

- уничтожению технических средств и программного обеспечения;
- поражению или гибели персонала.

Классификация угроз распространяется на три уровня:

1.инфраструктуру сети (охватывает **информацию пользователей**),

2.услуги связи (охватывает **транспортные услуги** сети),

3.приложения (охватывает **приложения, в том числе телематические службы,** организуемые на базе сетей).

Угрозы **системе передачи информации** включают:

•разрушение информации и/или других ресурсов;

•искажение или модификацию информации;

•кражу, исключение или потерю информации и/или других ресурсов;

•раскрытие содержания информации;

•прерывание связи.

К угрозам информационной безопасности относятся:

1. маскировка под логический объект (маскарад, спуфинг);
2. нарушение целостности информации;
3. модификация сообщения;
4. отказ в обслуживании;
5. вирусы, черви, троянские кони, гибриды;
6. спам;
7. слежка;
8. закладки в оборудование и программное обеспечение;
9. использование сниферов пакетов;
10. злоупотребление доверием;
11. переадресация портов;
12. вставка фальшивого трафика;

Цели (объекты) угроз

Поскольку современные системы связи представляют собой автоматизированные системы, построенные на базе аппаратных и программируемых устройств, то угрозы обращены как на аппаратуру, так и на программные продукты.

Целями атак злоумышленников становятся в первую очередь подсистемы и устройства, общие для большого объема передаваемой информации, а именно:

- маршрутизаторы;
- коммутаторы;
- сеть в целом
- регенераторы;
- мультиплексоры;
- хосты;
- подсистемы управления, сигнализации, мониторинга, синхронизации, биллинга, энергоснабжения.

Методы борьбы с угрозами ИБ на уровне МСС

В транспортной сети МСС реализуются функции трех нижних уровней модели OSI, следовательно, возможности борьбы с угрозами ИБ достаточно ограничены, имея ввиду, что основной задачей МСС является доставка любого вида трафика с минимальными задержками.

По этой причине, основные методы борьбы с угрозами ИБ в МСС сводятся к реализации так называемых списков управления доступом – Access Control List , реализуемым на уровнях L2, L3 и частично L4.

ACL (**Access Control List**) – список контроля доступа – определяет, кто может получать доступ к объекту, и какие операции разрешено или запрещено проводить над объектом.

ACL изначально служили основой систем фильтрации (ограничений прав доступа к файлам, папкам и др. ресурсам) при администрировании сетевых устройств в ОС Unix/Linux, Windows, ...

ACL представляет собой структуру данных (таблицу), содержащую записи (ACE), определяющие права пользователя на системные объекты (программы, процессы или файлы).

Типичные права – **R, RW, RWM, RWD**, …

В целом – ACL позволяет классифицировать трафик, а потом что-то с ним сделать в зависимости от того, к какому списку отнесен данный трафик.

По этой причине сегодня ACL широко применяется в сетевых устройствах для разных целей, например:

- **На интерфейсе** - *Для фильтрация пакетов*
- **На линии Telnet**: *ограничения доступа к маршрутизатору*
- **В рамках VPN**: *какой трафик нужно шифровать*
- **В рамках QoS**: *какой трафик обрабатывать приоритетнее*
- **В рамках NAT**: *какие адреса транслировать («пробрасывать» через NAT-шлюз)*

ACL представляет собой последовательность условий проверки параметров пакетов данных на разных уровнях модели OSI. В частности, коммутатор или маршрутизатор проверяет информацию в кадрах на совпадение с критериями фильтрации, определенными в ACL, и выполняет над пакетами одно из действий:

- **Permit ("Разрешить")**
- **Deny ("Запретить").**

Критерии фильтрации могут быть определены на основе следующей информации уровня L2/L3/L4, содержащейся в пакете:

- порт коммутатора;
- MAC / IP-адрес;
- тип Ethernet / тип протокола в заголовке IP;
- VID / VLAN;
- 802.1p – CoS / DSCP;
- порт TCP / UDP (тип приложения);
- первые 80 байт пакета, включая поле данных и т.д.

Списки доступа на уровне **L3/L4**, обрабатываемые маршрутизаторами, значительно повышают гибкость сети.

Например, списки, ограничивающие видеотрафик, могут уменьшить нагрузку сети и повысить ее пропускную способность для передачи других типов данных, например, аудиосигналов.

Список доступа ACL составляется из **утверждений (условий)**, которые определяют, следует ли пакеты принимать или отклонять во входных и выходных интерфейсах маршрутизатора.

Если ACL отсутствует на маршрутизаторе, то все проходящие через маршрутизатор пакеты будут иметь доступ к сети.

Каждый список ACL имеет **уникальный номер/имя**, который идентифицирует тип созданного списка доступа.

В Cisco IOS есть следующие **типы ACL**:

- **Стандартные** (только IP-адрес источника)
- **Расширенные** (IP-адреса, № протокола, порт TCP/UDP)
- **Именованные** (любое символическое имя).

Использование нумерованных, либо именованных списков доступа определяется их применением.

Некоторые протоколы требуют использования только нумерованных списков, некоторые - допускают как именованные, так и нумерованные списки.

Примеры номеров списков доступа	
Название списка доступа	**Диапазон номеров**
IP standard ACL	**1-99**
IP extended ACL	**100-199**
Ethernet address ACL	**700…799**

Особенности применения ACL:

- ACL могут использоваться, чтобы разрешать (permit) или запрещать (deny) продвижение пакетов.
- Запрет или разрешение сетевого трафика через интерфейс реализуется на основании анализа совпадения определенных в ACL условий.
- В списке доступа ACL могут анализироваться адреса источника, адреса назначения, протокол и номера порта верхнего уровня.
- Каждый список должен иметь уникальный номер.
- Стандартные списки доступа анализируют в IP-пакете только IP-адрес источника.
- Расширенные списки доступа проверяют IP-адрес источника, IP-адрес назначения, поле протокола и номер порта в заголовке TCP/UDP.
- При анализе ACL используется принцип – «**Запрещено все, что не разрешено**»

Стандартные списки доступа в Cisco.

1. Общий вид правила:

access-list номер действие источник

- номер - число идентифицирующее список
- действие - **permit** или **deny** (**разрешить**, **запретить**)
- источник - IP-адрес источника пакетов

Пример:

```
access-list 5 deny 10.10.10.0 0.0.0.255
access-list 5 deny 10.10.20.0 0.0.0.255
access-list permit any
```

Пример запрещает доступ для сетей 10.10.10.0 и 10.10.20.0 и разрешает для всех остальных.

- маршрутизатор обрабатывает правила **последовательно** и если поставить строку **access-list permit any** первой, то остальные два отрабатывать не будут.

2. Применение списка доступа к интерфейсу

```
interface FastEthernet0/1 ip access-group out
```

запрещается **исходящий трафик (out)** на интерфейсе FastEthernet0/1 для вышеперечисленных сетей.

- Стандартные списки доступа должны располагаться **поближе к защищаемой сети (граничные маршрутизаторы)**.
- Расширенные списки доступа должны быть установлены **близко к источнику сообщений (серверу, терминалу)**.
- Условие **deny any** (**запретить все остальное**) **неявно присутствует** в конце любого списка доступа.
- Создание списка доступа производится в режиме **глобального конфигурирования**. Формат команды создания стандартного списка доступа следующий:

Router(config)#access-list {№} {permit или deny} {адрес источника}.

- Привязка списка доступа к интерфейсу производится в режиме **детального конфигурирования интерфейса**.

Формат команды привязки списка к интерфейсу следующий:

Router(config-if)#{протокол} access-group {номер} {in или out}

- Формат команды создания расширенного списка доступа следующий:

Router(config)#access-list {номер} {permit или deny} {протокол} {адрес источника} {адрес назначения} {порт}

- Именованные списки доступа позволяют за счет введения имени списка сократить объем записи при конфигурировании.