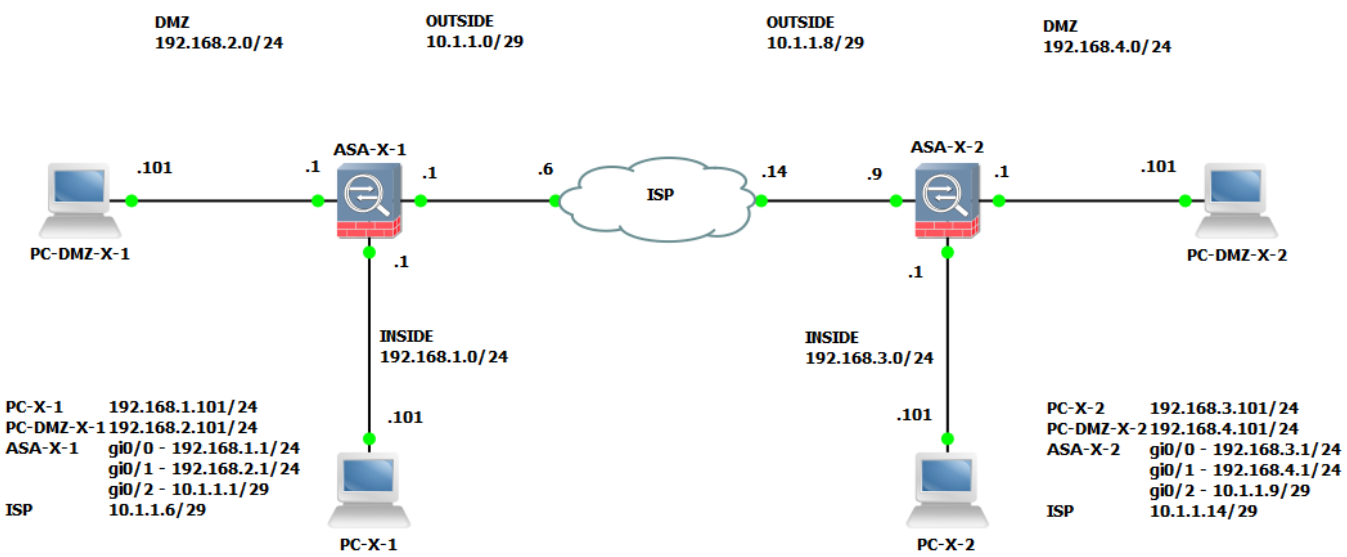
CCNA Security

Лабораторная работа 20

Настройка основных параметров безопасности на Cisco ASA

Топология



Описание

В этой лабораторной работе вы познакомитесь с объектами, группами объектов, объектным NAT, функционалом «packet-tracer» и списками контроля доступа.

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Имя (для команды nameif)	Security Level
ASA-X-1	G0/0	192.168.1.1/24	inside	100
	G0/1	192.168.2.1/24	dmz	50
	G0/2	10.1.1.1/29	outside	0
ASA-X-2	G0/0	192.168.3.1/24	inside	100
	G0/1	192.168.4.1/24	dmz	50
	G0/2	10.1.1.9/29	outside	0

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	DNS-сервер
PC-X-1	NIC	192.168.1.101/24 или DHCP	192.168.1.1	10.1.1.6
PC-DMZ-X-1	NIC	192.168.2.101/24	192.168.2.1	10.1.1.6
PC-X-2	NIC	192.168.3.101/24 или DHCP	192.168.3.1	10.1.1.14
PC-DMZ-X-2	NIC	192.168.4.101/24	192.168.4.1	10.1.1.14

Имена пользователей и пароли

	Console		SSH		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
ASA-X-1	-	-	admin	cisco12345	cisco12345
ASA-X-2	-	-	admin	cisco12345	cisco12345

Устройство	Имя пользователя	Пароль
PC-X-1	Student1	1
PC-DMZ-X-1	Student1	1
PC-X-2	Student1	1
PC-DMZ-X-2	Student1	1

Часть 1: Объекты и объектный NAT

1. Перейдите в виртуальную машину PC (PC-X-1 или PC-X-2).

2. Откройте командную строку, проверьте связь с маршрутизатором провайдера с помощью команды **ping**. Проверка связи будет неуспешна, потому что провайдер ничего не знает о ваших внутренних сетях, необходимо настроить NAT.

C:\Users\Student1> **ping 10.1.1.6**	C:\Users\Student1> **ping 10.1.1.14**

3. Cisco ASA поддерживает большое количество типов NAT, одним из самых простых вариантов является объектный NAT (Object NAT). Для настройки объектного NAT потребуется создать объекты. Объекты также пригодятся при написании списков контроля доступа. Объекты делятся на две категории: сетевые (network) и сервисные (service). Сетевые объекты – это узел, подсеть, диапазон адресов или FQDN. Сервисные объекты – это протоколы и порты (если протокол их поддерживает). Вернитесь в консоль ASA. Войдите в режим конфигурирования. Посмотрите подсказку для команды object.

```
ASA-X-1# conf t
ASA-X-1(config)# object ?

configure mode commands/options:
  network  Specifies a host, subnet or range IP addresses
  service  Specifies a protocol/port
```

4. Создайте сетевой объект OBJN_LAN.

```
ASA-X-1(config)# object network OBJN_LAN
ASA-X-1(config-network-object)#
```

5. В подрежиме конфигурирования сетевого объекта можно задать сам объект (команды host, subnet, range или fqdn), дать ему описание (команда description), настроить объектный NAT (команда nat). Помните, что один объект может содержать только одну сущность и одно правило NAT. Например, если вам нужно выбрать две подсети, то нужно создать два объекта, а затем объекты можно объединить в объектную группу для удобства управления.

```
ASA-X-1(config-network-object)# ?

  description  Specify description text
  fqdn         Enter this keyword to specify an FQDN
  help         Help for network object configuration commands
  host         Enter this keyword to specify a single host object
  nat          Enable NAT on a singleton object
  no           Remove an object or description from object
  range        Enter this keyword to specify a range
  subnet       Enter this keyword to specify a subnet
```

6. Укажите подсеть с PC.

ASA-X-1(config-network-object)# **subnet 192.168.1.0 255.255.255.0**	ASA-X-2(config-network-object)# **subnet 192.168.3.0 255.255.255.0**

7. Настройте объектный NAT. Читайте команду следующим образом: если пакет с адресом отправителя из указанной сети поступит на интерфейс с именем inside и должен будет выйти с интерфейса с именем outside, то будет выполняться PAT. В качестве нового адреса отправителя в пакете будет указан адрес с интерфейса outside самой ASA.

```
ASA-X-1(config-network-object)# nat (inside,outside) dynamic interface
ASA-X-1(config-network-object)# exit
```

8. Проверьте созданный объект и объектный NAT. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show run object
object network OBJN_LAN
 subnet 192.168.1.0 255.255.255.0

ASA-X-1(config)# show run nat
!
object network OBJN_LAN
 nat (inside,outside) dynamic interface
```

9. Вернитесь в виртуальную машину PC (PC-X-1 или PC-X-2).

10. Откройте командную строку, ещё раз проверьте связь с маршрутизатором провайдера с помощью команды **ping**. Проверка связи будет успешна. Быстро перейдите к следующему шагу.

C:\Users\Student1> **ping 10.1.1.6**	C:\Users\Student1> **ping 10.1.1.14**

11. Вернитесь в консоль ASA.

12. Посмотрите список трансляций. Команда поменялась, теперь она звучит как **show xlate**. Вы увидите, что выполняется PAT для протокола ICMP, пакет пришёл на интерфейс с именем inside, ушёл с интерфейса с именем outside, IPv4-адрес 192.168.1.51 заменили на 10.1.1.1. Флаг r – замена портов (для ICMP это замена QueryID), i – динамический NAT. Время жизни у записи – 30 секунд. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show xlate
0 in use, 3 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.51/1 to outside:10.1.1.1/1 flags ri idle 0:00:05
timeout 0:00:30

< Подождите примерно 30 секунд >
ASA-X-1(config)# show xlate
0 in use, 3 most used
< Тут пусто, трансляция ушла по таймауту >
```

13. Вернитесь в виртуальную машину PC (PC-X-1 или PC-X-2).

14. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **адрес 8.8.8.8**. Проверка связи будет успешна. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.

15. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **доменное имя ya.ru**. Проверка связи будет успешной. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.

16. Откройте браузер, попробуйте зайти на сайт **по доменному имени ya.ru**. Страница откроется. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.

Часть 2: Статический объектный NAT

1. Вернитесь в консоль ASA.

2. Создайте сетевой объект OBJN_WWW1_MAPPED. За этим объектом будет скрываться mapped адрес вашего сервера в DMZ. В терминологии ASA в NAT есть два типа адреса: real и mapped. Real – адрес, который действительно назначен на узле в настройках (статически или по протоколу DHCP), аналог inside local адреса на маршрутизаторе. Mapped – адрес, который будет в пакете после процесса NAT, аналог inside global адреса на маршрутизаторе.

ASA-X-1(config)# **object network OBJN_WWW1_MAPPED** ASA-X-1(config-network-object)# **host 10.1.1.2** ASA-X-1(config-network-object)# **exit**	ASA-X-2(config)# **object network OBJN_WWW1_MAPPED** ASA-X-2(config-network-object)# **host 10.1.1.10** ASA-X-2(config-network-object)# **exit**

3. Создайте сетевой объект OBJN_WWW1. За этим объектом будет скрываться real адрес вашего сервера в DMZ. Внутри объекта задайте правило объектного NAT.

ASA-X-1(config)# **object network OBJN_WWW1** ASA-X-1(config-network-object)# **host 192.168.2.101** ASA-X-1(config-network-object)# **nat (dmz,outside) static OBJN_WWW1_MAPPED** ASA-X-1(config-network-object)# **exit**	ASA-X-2(config)# **object network OBJN_WWW1** ASA-X-2(config-network-object)# **host 192.168.4.101** ASA-X-2(config-network-object)# **nat (dmz,outside) static OBJN_WWW1_MAPPED** ASA-X-2(config-network-object)# **exit**

4. Имея объекты, гораздо легче вносить изменения. Если поменяется адрес сервера (внутренний или внешний), то достаточно будет зайти в нужный объект и заменить адрес, все остальные правила менять не придётся. Разве это не прекрасно? Проверьте созданные объекты и объектный NAT. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show run object
object network OBJN_LAN
 subnet 192.168.1.0 255.255.255.0
object network OBJN_WWW1_MAPPED
 host 10.1.1.2
object network OBJN_WWW1
 host 192.168.2.101

ASA-X-1(config)# show run nat
!
object network OBJN_LAN
 nat (inside,outside) dynamic interface
object network OBJN_WWW1
 nat (dmz,outside) static OBJN_WWW1_MAPPED
```

5. Посмотрите список трансляций. Статические трансляции будут присутствовать в таблице всегда, даже если нет реального траффика. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show xlate
0 in use, 3 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.2.101 to outside:10.1.1.2
    Flags s idle 0:06:59 timeout 0:00:00
```

6. Вернитесь в виртуальную машину PC-DMZ (PC-DMZ-X-1 или PC-DMZ-X-2).

7. Откройте командную строку и проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **адрес 8.8.8.8**. Проверка связи будет успешна. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.

8. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **доменное имя ya.ru**. Проверка связи будет успешной. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.

9. Откройте браузер, попробуйте зайти на сайт **по доменному имени ya.ru**. Страница откроется. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.

Часть 3: Сервисные объекты и группы объектов

1. Чтобы на ваш сервер смогли попасть из внешних сетей недостаточно настроить NAT, также потребуется явно разрешить траффик в списках контроля доступа. Почему? Потому что траффик пойдёт с интерфейса outside на интерфейс dmz, с уровня безопасности 0 в уровень безопасности 50, из меньшего уровня безопасности в больший. Следовательно, траффик входящий, а входящий траффик по умолчанию запрещён.
   Представим, что вскоре однотипных серверов будет пять. Тогда проще сразу создать группу объектов и указывать в списках контроля доступа именно её.
   Создайте группу сетевых объектов и добавьте в неё объект, представляющий сервер.
   ```
   ASA-X-1(config)# object-group network OBJGN_WWW_SERVERS
   ASA-X-1(config-network-object-group)# network-object object OBJN_WWW1
   ASA-X-1(config-network-object-group)# exit
   ```

2. Проверьте созданные группы объектов.
   ```
   ASA-X-1(config)# show run object-group
   object-group network OBJGN_WWW_SERVERS
    network-object object OBJN_WWW1
   ```

3. Доступ к серверам нужно будет разрешить по протоколам HTTP и HTTPS на стандартные порты получателя. Создайте два сервисных объекта.
   ```
   ASA-X-1(config)# object service OBJS_TCP80
   ASA-X-1(config-service-object)# service tcp destination eq 80
   ASA-X-1(config-service-object)# exit

   ASA-X-1(config)# object service OBJS_TCP443
   ASA-X-1(config-service-object)# service tcp destination eq 443
   ASA-X-1(config-service-object)# exit
   ```

4. Проверьте созданные сервисные объекты. Для вывода только сервисных объектов добавьте дополнительный параметр service.
   ```
   ASA-X-1(config)# show run object service
   object  service OBJS_TCP80
    service tcp destination eq www
   object service OBJS_TCP443
    service tcp destination eq https
   ```

5. Создайте группу сервисных объектов и добавьте в неё два сервисных объекта, созданных ранее.
   ```
   ASA-X-1(config)# object-group service OBJGS_WWW_SERVERS_PORTS
   ASA-X-1(config-service-object-group)# service-object object OBJS_TCP80
   ASA-X-1(config-service-object-group)# service-object object OBJS_TCP443
   ASA-X-1(config-service-object-group)# exit
   ```

6. Проверьте созданные группы объектов. Для вывода только групп сервисных объектов добавьте дополнительный параметр service.
   ```
   ASA-X-1(config)# show run object-group service
   object-group service OBJGS_WWW_SERVERS_PORTS
    service-object object OBJS_TCP80
    service-object object OBJS_TCP443
   ```

Часть 4: Функционал “packet-tracer”

1. Не всегда есть возможность практической проверки. В таких случаях для базовой проверки движения пакета можно воспользоваться встроенным функционалом packet-tracer. Помните, что packet-tracer не является полноценной заменой практической проверки, не все случаи будут отображены корректно.
   Смоделируйте движение сегмента TCP с адреса отправителя 8.8.8.8 с порта 40001 на внешний адрес вашего сервера на порт 80. Само собой, сегмент поступил на внешний интерфейс с именем outside.

`ASA-X-1(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.2 80`	`ASA-X-2(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.10 80`

2. Изучите вывод. Вывод поделён на несколько фаз. В зависимости от настроенного функционала количество фаз может варьироваться. Пакет был заблокирован на фазе 4 (проверка списком контроля доступа, пакет попал под неявный запрет). В самом низу представлен итог (Action: drop). Ниже представлен вывод для левой части топологии.

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network OBJN_WWW1
 nat (dmz,outside) static OBJN_WWW1_MAPPED
Additional Information:
NAT divert to egress interface dmz
Untranslate 10.1.1.2/80 to 192.168.2.101/80

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
```

```
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Часть 5: Списки контроля доступа

1. Списки контроля доступа на Cisco ASA похожи на списки контроля доступа на маршрутизаторе. Основные отличия:
   - списки всегда именованные;
   - списки всегда расширенные;
   - в одном списке содержатся одновременно правила и IPv4, и IPv6;
   - маски всегда обычные.

   Кроме расширенных списков есть и стандартные, но

   - обычно их не применяют для фильтрации траффика, а только для работы с протоколами динамической маршрутизации;
   - в них можно указывать только адрес получателя.

   Создайте расширенный список контроля доступа с именем OUTSIDE_IN, добавьте в него одно правило «Разрешить доступ с любого адреса IPv4 к группе сетевых объектов OBJGN_WWW_SERVERS на порты, определённые в группе сервисных объектов OBJGS_WWW_SERVERS_PORTS». Ключевое слово any обозначает любой адрес отправителя (как IPv4, так и IPv6), any4 – любой IPv4-адрес отправителя, any6 – любой IPv6 адрес отправителя. Если не указан номер правила, то правило добавляется в конец.

   ```
   ASA-X-1(config)# access-list OUTSIDE_IN extended permit object-group OBJGS_WWW_SERVERS_PORTS any4 object-group OBJGN_WWW_SERVERS
   ```

2. Проверьте созданный список контроля доступа. Обратите внимание, что ASA автоматически развернула одну написанную строку в две строки. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show access-list
< Вывод опущен >
access-list OUTSIDE_IN line 1 extended permit object-group OBJGS_WWW-SERVERS_PORTS any4
object-group OBJGN_WWW_SERVERS (hitcnt=0) 0x5abe3f8c

  access-list OUTSIDE_IN line extended permit tcp any4 host 192.168.2.101 eq www
(hitcnt=0) 0x06efd281
  access-list OUTSIDE_IN line 1 extended permit tcp any4 host 192.168.2.101 eq https
(hitcnt=0) 0x4012d9ac
```

3. Прикрепите созданный список контроля доступа на вход интерфейса с именем outside.
   ```
   ASA-X-1(config)# access-group OUTSIDE_IN in interface outside
   ```

4. Выполните проверку с помощью функционала packet-tracer ещё раз. Обратите внимание на фазу 2. В этот раз пакет попал под разрешающую строку. Ниже представлен вывод для левой части топологии.

`ASA-X-1(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.2 80`	`ASA-X-2(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.10 80`

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
```

```
Config:
object network OBJN_WWW1
 nat (dmz,outside) static OBJN_WWW1_MAPPED
Additional Information:
NAT divert to egress interface dmz
Untranslate 10.1.1.2/80 to 192.168.2.101/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group OUTSIDE_IN in interface outside
access-list OUTSIDE_IN extended permit object-group
OBJGS_WWW_SERVERS_PORTS any4 object-group OBJGN_WWW_SERVERS
object-group service OBJGS_WWW_SERVERS_PORTS
 service-object object OBJS_TCP80
 service-object object OBJS_TCP443
object-group network OBJGN_WWW_SERVERS
 network-object object OBJN_WWW1
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network OBJN_WWW1
 nat (dmz,outside) static OBJN_WWW1_MAPPED
```

```
Additional Information:

Phase: 7
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 187, packet dispatched to next module

Result:
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

5. Выполните проверку с помощью функционала packet-tracer ещё раз, но укажите порт получателя 443. Будет ли пакет разрешён?

`ASA-X-1(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.2 443`	`ASA-X-2(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.10 443`

6. Выполните проверку с помощью функционала packet-tracer ещё раз, но укажите порт получателя 8080. Будет ли пакет разрешён?

`ASA-X-1(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.2 8080`	`ASA-X-2(config)# packet-tracer input outside tcp 8.8.8.8 40001 10.1.1.10 8080`

7. Чем больше у вас однотипных узлов и правил, тем большее преимущество вы получаете от использования объектов и групп объектов.
   У вас появились ещё четыре WWW-сервера. На эти сервера распространяется та же политика безопасности, что и на первый сервер. Что необходимо сделать? Создать четыре сетевых объекта и занести их в существующую группу сетевых объектов OBJGN_WWW_SERVERS.
   У вас появилась нужда предоставить доступ к этим серверам ещё по двум портам. Что необходимо сделать? Создать два сервисных объекта и занести и в существующую группу сетевых объектов OBJGS_WWW_SERVERS_PORTS.
   В обоих случаях исправлять список контроля доступа не потребуется, а ASA сама развернёт все нужные объекты и группы. Пять серверов, по четыре порта к каждому серверу – итого одна строка развернётся в 20 строк правил. Десять серверов, по пять портов к каждому серверу – уже 50 строк.
   Сохраните конфигурацию.

```
ASA-X-1# copy run start

Source filename [running-config]? < Нажмите Enter >
Cryptochecksum: 12e9b0be c4f97f5c e9f5da33 7c509a95

7888 bytes copied in 0.220 secs
ASA-X-1#
```