Основы настройки Cisco ASA

Наташа Самойленко

Сетевые Дни

Работа с конфигурацией

Работа с конфигурационными файлами и ОС

Посмотреть текущую конфигурацию:

```
asa1# show running-config
```

Посмотреть текущую конфигурацию и скрытые команды:

```
asa1# show running-config [all] [command]
```

Посмотреть стартовую конфигурацию:

```
asa1# show startup-config
```

Удалить стартовую конфигурацию:

```
asa1# write erase
```

Удалить текущую конфигурацию:

```
asa1# clear configure all
```

Скопировать текущую конфигурацию в стартовую:

```
asa1# copy run start
asa1# wr
```

Управление процессом загрузки ОС и конфигурационных файлов

Показать содержимое директорий:

```
asa1# show dir
```

Показать содержимое файла:

```
asa1# more <файл>
```

Указать файл ОС, который будет использовать ASA:

```
asa1(config)# boot system flash:/image.bin
```

Просмотр текущих настроек загрузки ОС и конфигурационного файла:

```
asa1# show bootvar

BOOT variable =
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

Настройка интерфейсов

Уровни безопасности интерфейсов

На ASA каждому интерфейсу присваивается уровень безопасности:

- Значение уровня безопасности может быть от 0 до 100
- 100 — максимальный уровень безопасности. Как правило, присваивается интерфейсу, который находится в локальной сети
- 0 — минимальный уровень безопасности. Присваивается внешнему интерфейсу
- По умолчанию на всех интерфейсах уровень безопасности 0

Правила взаимодействия интерфейсов

- По умолчанию трафик, который идет с интерфейса с более высоким уровнем безопасности на интерфейс с меньшим уровнем безопасности, разрешен.
- Хосты, которые находятся на более безопасном интерфейсе могут получить доступ к любому хосту, находящемуся на менее безопасном интерфейсе.
- Это правило можно ограничить, применив access-list.

Интерфейсы с одинаковыми уровнями безопасности

По умолчанию передача трафика между интерфейсами с одинаковыми уровнями безопасности **не разрешена**.

Разрешить передачу трафика между интерфейсами с одинаковыми уровнями безопасности:

```
same-security-traffic permit inter-interface
```

Настройка интерфейсов

Для того чтобы разрешить прохождение трафика через интерфейсы ASA, необходимо задать имя интерфейса и IP-адрес (для режима routed).

```
interface gi1
   nameif inside
   security-level 100
   ip address 10.1.1.1 255.255.255.0
   no shut
```

Проверка интерфейсов

```
asa1# sh nameif
Interface                  Name                  Security
GigabitEthernet0/0         outside               0
GigabitEthernet0/1         inside                100
```

Информация о статусе интерфейсов и IP-адресах:

```
asa1# sh int ip br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.0.1.1        YES unset  administratively down down
GigabitEthernet0/1     192.168.1.1     YES unset  administratively down down
GigabitEthernet0/      unassigned      YES unset  administratively down down
GigabitEthernet0/      unassigned      YES unset  administratively down down
Internal-Control0/0    127.0.1.1       YES unset  up                    up
Internal-Data0/0       unassigned      YES unset  up                    up
Management0/0          unassigned      YES unset  administratively down down
```

Статическая маршрутизация

Статическая маршрутизация

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route outside 10.10.10.0 255.255.255.0 10.0.1.1
```

Маршрут по умолчанию:

```
route outside 0 0 16.0.0.1
```

Доступ к ASA

Доступ к ASA

Настройка SSH:

```
crypto key generate rsa modulus 1024
username user1 password 12345678
aaa authentication ssh console LOCAL

ssh 10.1.3.3 255.255.255.255 inside
ssh 10.1.1.0 255.255.255.0 inside
```

Настройка HTTPS (для ASDM):

```
http server enable
http 10.1.3.3 255.255.255.255 inside
http 10.1.1.0 255.255.255.0 inside
```

Базовая настройка ACL

ACL в ASA

В Cisco ASA ACL могут применяться:

- К интерфейсу
  - для входящего и для исходящего трафика (относительно интерфейса)
- Глобально
  - Глобальные ACL всегда применяются только ко входящему трафику
- ACL, которые применены к интерфейсу, обрабатываются до глобальных ACL

```
access-list IN-OUT extended permit tcp host 10.1.1.1 host 29.15.2.225 eq www
access-list IN-OUT extended permit tcp host 10.1.2.67 any
access-list IN-OUT extended permit ip host 10.1.3.34 50.1.1.0 255.255.255.0

access-group IN-OUT out interface outside
```

Правила для ответного трафика

Для TCP и UDP соединений не нужно разрешать пакеты в ACL, так как ASA пропускает весь ответный трафик, для установленных, двухсторонних соединений.

Для протоколов у которых не используются сессии, таких как ICMP, ASA устанавливает только однонаправленые соединения.

В таком случае, надо или включить инспектирование протокола, или добавить соответствующие записи в ACL

Object-groups

```
access-list ACL_IN extended deny tcp host 10.1.1.4 host 29.15.201.29 eq www
access-list ACL_IN extended deny tcp host 10.1.1.78 host 29.15.201.29 eq www
access-list ACL_IN extended deny tcp host 10.1.1.89 host 29.15.201.29 eq www
access-list ACL_IN extended deny tcp host 10.1.1.4 host 29.15.201.16 eq www
access-list ACL_IN extended deny tcp host 10.1.1.78 host 29.15.201.16 eq www
access-list ACL_IN extended deny tcp host 10.1.1.89 host 29.15.201.16 eq www
access-list ACL_IN extended deny tcp host 10.1.1.4 host 29.15.201.78 eq www
access-list ACL_IN extended deny tcp host 10.1.1.78 host 29.15.201.78 eq www
access-list ACL_IN extended deny tcp host 10.1.1.89 host 29.15.201.78 eq www
access-list ACL_IN extended permit ip any any
access-group ACL_IN in interface inside

object-group network DENIED
 network-object host 10.1.1.4
 network-object host 10.1.1.78
 network-object host 10.1.1.89
 object-group network WEB
 network-object host 29.15.201.29
 network-object host 29.15.201.16
 network-object host 29.15.201.78
 access-list ACL_IN extended deny tcp port object-group DENIED
object-group WEB eq www
 hostname(config)# access-list ACL_IN extended permit ip any any
 hostname(config)# access-group ACL_IN in interface inside
```

Политика по умолчанию

Политика по умолчанию

```
class-map inspection_default
  match default-inspection-traffic
 policy-map type inspect dns preset_dns_map
  parameters
     message-length maximum 512
 policy-map global_policy
  class inspection_default
   inspect dns preset_dns_map
   inspect ftp
   inspect h323 h225
   inspect h323 ras
   inspect rsh
   inspect rtsp
   inspect esmtp
   inspect sqlnet
   inspect skinny
   inspect sunrpc
   inspect xdmcp
   inspect sip
   inspect netbios
   inspect tftp
   inspect ip-options
 service-policy global_policy global
```

ICMP и ASA

Сквозной ICMP трафик

Сквозной ICMP-трафик с более безопасного интерфейса на менее безопасный

- По умолчанию ASA пропускает через себя трафик только с более безопасного интерфейса на менее безопасный
- Поэтому если, например, с хоста за интерфейсом inside отправить ICMP-запрос на хост за интерфейсом outside, то ASA отбросит ответ на outside интерфейсе
- Для того чтобы ASA пропускала ICMP-ответы от хостов, которые находятся на менее безопасном интерфейсе, достаточно включить инспектирование ICMP.
- После включения инспектирования ASA пропускает ICMP-пакеты, входящие в менее безопасный интерфейс (outside), только в том случае, если они являются ответом на сессию инициированную с более безопасного интерфейса.

```
policy-map global_policy
 class inspection_default
  inspect icmp
```

Сквозной ICMP трафик

С менее безопасного интерфейса на более безопасный

- Если необходимо разрешить пинговать хосты на более безопасных интерфейсах, из сетей за менее безопасными интерфейсами, то необходимо применять к менее безопасным интерфейсам ACL.

```
access-list ICMP extended permit icmp any any
access-group ICMP in interface outside
```

ICMP и интерфейсы ASA

По умолчанию разрешены все ICMP-пакеты на интерфейсы ASA.

Интерфейсы ASA отвечают на ICMP-запросы только если они пришли из сетей находящихся на том же интерфейсе.

Команда icmp позволяет указать правила для ICMP-пакетов, которые идут на интерфейсы ASA:

```
icmp permit any echo-reply inside
```

Сессии

Сесии

show conn

```
1 in use, 9 most used
TCP outside 192.168.100.10:80 inside inhost:40000, idle 0:00:06, bytes 0, flags E
TCP outside 10.99.55.44(18.17.16.15):11515 inside 10.88.77.66:30854, idle 0:02:48,
bytes 178, flags UIO
TCP outside 77.66.55.44:49368 VPN 15.15.15.15:443, idle 0:00:21, bytes 100531, flags
UfrIOB
UDP outside 10.17.17.17:8500 inside 10.20.20.20:4167, idle 0:01:38, bytes 616, flags -
TCP outside 77.66.55.44:30031 inside 10.20.20.20:51716, idle 0:00:11, bytes 0, flags U
TCP outside 10.20.20.20:10101 outside 10.30.30.30:4450, idle 0:00:14, bytes 0, flags
SaAB
TCP outside 20.30.40.50:45174 inside 10.30.30.30:443, idle 0:00:05, bytes 0, flags aB
```

show local-host 10.1.1.91 detail

```
 Interface third: 0 active, 0 maximum active, 0 denied
 Interface inside: 1 active, 1 maximum active, 0 denied
 local host: <10.1.1.91>,
 TCP flow count/limit = 1/unlimited
 TCP embryonic count to (from) host = 0 (0)
 TCP intercept watermark = unlimited
 UDP flow count/limit = 0/unlimited
 Xlate:
 TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri
 Conn:
 TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1
active, 1
maximum active, 0 denied
 The following example shows all hosts who have at least four udp connections and have
between one
to 10 tcp connections at the same time:
```

Трансляция адресов

Типы NAT

Cisco ASA использует два типа NAT:

- **Network Object NAT (Auto NAT)**
  - Настраивается внутри network object
- **Twice NAT (Manual NAT)**
  - Настраивается в конфигурационном режиме

Network Object NAT

Как задаются real адреса:

- Правило NAT указывается как параметр в network object
- Network object может указывать хост, диапазон адресов или подсеть
- IP-адрес в network object используется как real адрес

Как настраивается source и destination NAT

- Каждое правило может относиться или к адресу отправителя или к адресу получателя в пакете
- Если нужно менять оба, то в таком виде NAT надо настроить два правила

Network Object NAT

Статический NAT

```
object network WEB_server1
 host 10.255.1.100
 nat (dmz,outside) static 16.0.0.7
```

Статический PAT (проброс портов)

```
object network WEB_server2
 host 10.255.1.101
 nat (dmz,outside) static 16.0.0.8 service tcp 80 8080
```

Динамический PAT

```
object network Local_LAN
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

Динамический PAT с интерфейсом any

```
object network Local_LAN
 subnet 10.1.0.0 255.255.0.0
 nat (any,outside) dynamic interface
```

Twice NAT

Как задаются real адреса:

- Для real и mapped адресов создаются object group
- Но правило NAT НЕ указывается как параметр в network object
- Наоборот, объекты являются параметрами конфигурации NAT

Как настраивается source и destination NAT

- Одно правило используется для трансляции и отправителя и получателя
- Позволяет указывать как транслировать адреса, в зависимости от получателя (policy NAT). Используется, например, для VPN

Twice NAT

Исключение для Site-to-Site VPN

```
object network LAN
  subnet 10.1.0.0 255.255.0.0
object network VPN
  range 10.3.0.0 10.3.255.255
nat (inside,outside) source static LAN LAN dest static VPN VPN
```

Динамический PAT с Twice NAT:

```
object network Local_LAN
 subnet 10.1.1.0 255.255.255.0
nat (inside,outside) source dynamic Local_LAN interface
```

Порядок правил NAT

В таблице трансляции три секции:

1. **Twice NAT (Manual NAT)**
   - Сюда по умолчанию попадают правила Twice NAT
   - Между собой просматриваются в порядке настройки в конфигурации
2. **Network object NAT (Auto NAT)**
   - Все правила Object NAT
   - Между собой правила упорядочиваются так:
     - Первыми идут правила с наиболее специфическими адресами в объектах
     - Если правила используют сети одинакового размера, то по адресам
     - Если адреса одинаковые, то по именам объектов
3. **Twice NAT**
   - Правила с указанным параметром **after-auto**
   - Между собой просматриваются в порядке настройки в конфигурации

Troubleshooting Cisco ASA

Capture

Команда capture позволяет перехватывать трафик, который проходит через ASA для дальнейшего анализа.
Параметры команды capture:

- access-list — перехватывать пакеты, которые совпадают с указанным ACL;
- buffer — настроить размер буфера (в байтах) в который помещаются перехваченные пакеты. По умолчанию размер буфера 512 Kb;
- circular-buffer — после заполнения буфера заполнять его сначала заново. По умолчанию буфер не перезаписывается;
- ethernet-type — перехватывать Ethernet-пакеты определенного типа. По умолчанию IP;
- interface <intf-name> — перехватывать пакеты на указанном интерфейсе. Могут быть указаны такие интерфейсы:
- match — перехватывать пакеты совпадающие с указанными далее критериями (критерии аналогичны синтаксису ACL);
- trace [trace-count <count>] — позволяет отслеживать каким образом ASA обрабатывает пакеты внутри себя (если этот параметр не указан при задании правила, то при просмотре информации опция trace не будет отображать как ASA обрабатывала пакет). Параметр trace-count позволяет задать максимальное количество пакетов, которые будут отслеживаться. По умолчанию 50, диапазон значений от 1 до 1000;
- type — перехватывать пакеты указанного типа:
- asp-drop — перехватывать пакеты отброшенные по определенной причине,

Capture

```
ASA1(config)# capture cap_inside interface inside
ASA1(config)# sh capture cap_inside

14 packets captured

   1: 14:46:11.080623 192.168.1.10 > 192.168.3.10: icmp: echo request
   2: 14:46:11.083247 192.168.3.10 > 192.168.1.10: icmp: echo reply
   3: 14:46:12.080638 192.168.1.10 > 192.168.3.10: icmp: echo request
   4: 14:46:12.081309 192.168.3.10 > 192.168.1.10: icmp: echo reply
   5: 14:46:31.081569 192.168.1.10.58226 > 192.168.3.10.80: S
4052042955:4052042955(0) win 65535 <mss 1460,nop,wscale 0,
   6: 14:46:31.081676 192.168.3.10.80 > 192.168.1.10.58226: R 0:0(0) ack
4052042956 win 65535
   7: 14:46:38.426171 0.0.0.0.68 > 255.255.255.255.67:  udp 300
   8: 14:46:39.543947 0.0.0.0.68 > 255.255.255.255.67:  udp 300
   9: 14:46:41.782857 0.0.0.0.68 > 255.255.255.255.67:  udp 300
  10: 14:46:44.746955 192.168.1.10.58227 > 192.168.3.10.80: S
416086651:416086651(0) win 65535 <mss 1460,nop,wscale 0,no
  11: 14:46:44.747062 192.168.3.10.80 > 192.168.1.10.58227: R 0:0(0) ack
416086652 win 65535
  12: 14:46:45.322950 192.168.1.10.58228 > 192.168.3.10.80: S
787702359:787702359(0) win 65535 <mss 1460,nop,wscale 0,no
  13: 14:46:45.323042 192.168.3.10.80 > 192.168.1.10.58228: R 0:0(0) ack
787702360 win 65535
  14: 14:46:46.440452 0.0.0.0.68 > 255.255.255.255.67:  udp 300
14 packets shown
```

Packet tracer

Команда packet-tracer:

- позволяет проверить как ASA обработает пакет не генерируя при этом реальный трафик с соответствующих хостов
- ASA сама создает пакет и пропускает его через себя
- В результате выполнения команды будет отображен порядок обработки указанного пакета внутри ASA и результат обработки.
- При поиске неисправностей packet tracer один из самых удобных инструментов
- Так как packet-tracer генерирует указанный пакет, то информацию о нём можно посмотреть в различной статистике, счётчиках, таблицах трансляции.
- Команда packet-tracer может использоваться в связке с capture. Даже если при перехвате трафика не использовался параметр trace, с помощью packet-tracer можно получить аналогичный вывод для реального пакета.
- Утилита packet tracer доступна и в веб-интерфейсе ASDM.

Packet tracer

Синтаксис команды немного меняется в зависимости от того пакет какого протокола надо сгенерировать.

```
ASA1# packet-tracer input <intf-name> <protocol>
<sIP> <protocol-param> <dIP> [detailed|xml]
```

Общие параметры команды packet-tracer:

- intf-name — имя интерфейса ASA через который входит пакет,
- protocol — протокол, который будет использоваться:
- TCP,
- UDP,
- RAW IP,
- ICMP,
- protocol-param — параметры, которые зависят от того какой протокол был выбран. Описаны далее в соответствующих разделах,
- sIP — IP-адрес отправителя,
- dIP — IP-адрес получателя,
- detailed — более подробный вывод команды,
- xml — вывод результата в формате xml.

Packet tracer

```
packet-tracer input inside tcp 192.168.1.10 40000 192.168.100.10 80

Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   192.168.100.0   255.255.255.0   outside

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group permit_web in interface inside
access-list permit_web extended permit tcp 192.168.1.0 255.255.255.0 any
eq www
Additional Information:
```

Packet tracer

```
Phase: 4
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map any
 match any
policy-map global_policy
 class any
  set connection decrement-ttl
service-policy global_policy global

Phase: 5
Type: IP-OPTIONS
Result: ALLOW

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 0.0.0.0 0.0.0.0
  match ip inside any outside any
    dynamic translation to pool 1 (192.168.3.1 [Interface PAT])
    translate_hits = 2, untranslate_hits = 0
Additional Information:
Dynamic translate inhost/40000 to 192.168.3.1/51495 using netmask
255.255.255.255
```

Packet tracer

```
Phase: 7
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 0.0.0.0 0.0.0.0
  match ip inside any inside any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0

Phase: 8
Type: IP-OPTIONS
Result: ALLOW

Phase: 9
Type: FLOW-CREATION
Result: ALLOW
Additional Information:
New flow created with id 143, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Основы настройки Cisco ASA

Автор курса: Наташа Самойленко
nataliya.samoylenko@gmail.com

Сетевые Дни