Настройка базовых правил фильтрации и инспектирования трафика на Cisco ASA

Наташа Самойленко

Сетевые Дни

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 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

access-list ACL_IN extended deny tcp port object-group DENIED
object-group WEB eq www
access-list ACL_IN extended permit ip any any
```

```
access-group ACL_IN in interface inside
```

Object

Object

Объекты могут использоваться в конфигурации вместо IP-адресов.

Два типа Object:

- network object
- service object

Объекты могут использоваться, например, в:

- Network Address Translation (NAT)
- ACL
- object groups

Network Object

В network object может быть указан IP-адрес/маска в таких вариантах:

- host
- subnet
- range

```
object network OBJECT1
 host 10.2.2.2

object network OBJECT2
 subnet 10.1.1.0 255.255.255.0

object network OBJECT3
 range 10.3.0.0 10.3.255.255
```

Service Object

В service object может быть указан:

- протокол
- порты отправителя/получателя

```
object network OBJECT4
 service tcp destination eq ssh
```

Object-group

Object-group

Группы объектов:

- используются для группировки однотипных обектов
- могут использоваться в ACL
- Типы object-group:
  - Protocol
  - Network
  - Service
  - ICMP type

Object Group

Protocol Object Group

```
 object-group protocol TCP_UDP_ICMP
  protocol-object tcp
  protocol-object udp
  protocol-object icmp
```

Network Object Group

```
object-group network ADMINS
 network-object host 10.2.2.4
 network-object host 10.2.2.78
 network-object host 10.2.2.34
```

Object-group

Service Object Group

```
object-group service SERVICE1 tcp-udp
 port-object eq domain

object-group service SERVICE2 udp
 port-object eq radius
 port-object eq radius-acct

object-group service SERVICE3 tcp
 port-object eq ldap
```

ICMP type Object Group

```
object-group icmp-type ping
 icmp-object echo
 icmp-object echo-reply
```

Nesting Object Groups

```
object-group network IT
 network-object host 10.1.1.1
 network-object host 10.1.1.4
 network-object host 10.1.1.8

object-group network HR
 network-object host 10.1.2.8
 network-object host 10.1.2.12

object-group network FINANCE
 network-object host 10.1.4.89
 network-object host 10.1.4.100

object-group network ADMIN
 group-object IT
 group-object HR
 group-object FINANCE
```

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 xdmcp
   inspect sip
   inspect netbios
   inspect tftp
   inspect ip-options
 service-policy global_policy global
```

Политика по умолчанию

```
class-map inspection_default
  match default-inspection-traffic

default-inspection-traffic  Match default inspection traffic:
                      ctiqbe----tcp--2748      dns-------udp--53
                      ftp-------tcp--21        gtp-------udp--2123,3386
                      h323-h225-tcp--1720      h323-ras--udp--1718-1719
                      http------tcp--80        icmp------icmp
                      ils-------tcp--389       mgcp------udp--2427,2727
                      netbios---udp--137-138   radius-acct---udp--1646
                      rpc-------udp--111       rsh-------tcp--514
                      rtsp------tcp--554       sip-------tcp--5060
                      sip-------udp--5060      skinny----tcp--2000
                      smtp------tcp--25        sqlnet----tcp--1521
                      tftp------udp--69        xdmcp-----udp--177
```

Настройка политик

Настройка политик

class-map

- описание трафика

policy-map

- назначение действий

service-policy

- применение к паре зон

class-map

```
ciscoasa(config-cmap)# match ?

mpf-class-map mode commands/options:
 access-list                     Match an Access List
 any                             Match any packet
 default-inspection-traffic      Match default inspection traffic
 dscp                            Match IP DSCP
 flow                            Flow based Policy
 port                            Match TCP/UDP port(s)
 precedence                      Match IP precedence
 rtp                             Match RTP port numbers
 tunnel-group                    Match a Tunnel Group
```

```
ciscoasa(config)# class-map CLASS1
ciscoasa(config-cmap)# match port tcp eq 43
ciscoasa(config-cmap)# match port tcp eq 45
ERROR: Multiple match commands are not supported except for the
'match tunnel-group or default-inspect-traffic' command.
```

policy-map

```
MPF policy-map class configuration commands:
  police                Rate limit traffic for this class
  priority              Strict scheduling priority for this class
  service-policy        Configure QoS Service Policy
  set                   Set connection values
  shape                 Traffic Shaping
  csc                   Content Security and Control service module
  flow-export           Configure filters for NetFlow events
  inspect               Protocol inspection services
  ips                   Intrusion prevention services
```

policy-map

```
ciscoasa(config-pmap-c)# set connection ?

mpf-policy-map-class mode commands/options:
  advanced-options            Configure advanced connection parameters
  conn-max                    Keyword to set the maximum number of all
                              simultaneous connections that are allowed.  Default
                              is 0 which means unlimited connections.
  decrement-ttl               Decrement Time to Live field
  embryonic-conn-max          Keyword to set the maximum number of TCP embryonic
                              connections that are allowed.  Default is 0 which
                              means unlimited connections.
  per-client-embryonic-max    Keyword to set the maximum number of TCP embryonic
                              connections that are allowed per client machine.
                              Default is 0 which means unlimited connections.
  per-client-max              Keyword to set the maximum number of all
                              simultaneous connections that are allowed per
                              client machine. Default is 0 which means unlimited
                              connections.
  random-sequence-number      Enable/disable TCP sequence number randomization.
                              Default is to enable TCP sequence number
                              randomization
  timeout                     Configure connection timeout parameters
```

service-policy

```
service-policy POLICY1 global
service-policy POLICY2 interface inside
```

Направление функций

Функционал	Политика на интерфейсе	Глобальная политика
Инспектирование приложений	Bidirectional	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS standart priority queue	Egress	Egress
QoS traffic shaping	Egress	Egress
Таймауты и ограничения сессий TCP и UDP рандомизация TCP sequence	Bidirectional	Ingress
TCP normalization	Bidirectional	Ingress
TCP state bypass	Bidirectional	Ingress

Порядок применения нескольких функций

1. QoS input policing
2. TCP normalization, TCP и UDP connection limits и timeouts, TCP sequence number randomization, и TCP state bypass
3. ASA CSC
4. Application inspections, которые могут быть скомбинированы с другими inspections:
    - IPv6
    - IP options
    - WAAS
5. Application inspections, которые не могут быть скомбинированы с другими inspections.
6. ASA IPS
7. ASA CX
8. QoS output policing
9. QoS standard priority queue
10. QoS traffic shaping, hierarchical priority queue

Ограничения

Class Map

Максимальное количество class-map 255:

- Layer 3/4 class maps (for through traffic and management traffic).
- Inspection class maps
- Regular expression class maps
- match commands used directly underneath an inspection policy map
- Включая default class maps

Policy Map

- К каждому интерфейсу может быть применена только одна policy map
- Одну и ту же политику можно применять к разным интерфейсам
- Всего в конфигурации можно создать 64 policy map

Инспектирование

Инспектирование

```
access-list LAN-OUT extended permit 10.1.0.0
255.255.0.0 any

class-map CLASS1
 match access-list LAN-OUT
 match default-inspection-traffic

class-map HTTP_8080
 match port tcp eq 8080

policy-map POLICY1
 class HTTP_8080
  inspect http
 class CLASS1
  inspect ftp
  inspect http
  inspect icmp

service-policy POLICY1 interface inside
```

Политика 7 уровня

Варианты настройки политик

```
class-map type inspect ftp NO_GET_CLASS
 match request-command get

policy-map type inspect ftp NO_GET
 class type inspect ftp NO_GET_CLASS
  reset

policy-map global_policy
 class inspection_default
  inspect ftp strict NO_GET
```

```
policy-map type inspect ftp NO_GET
 match request-command get
  reset

policy-map global_policy
 class inspection_default
  inspect ftp strict NO_GET
```

Политика инспектирования

```
regex FILE_TYPE_GIF ".+\.[Gg][Ii][Ff]"
regex FILE_TYPE_TXT ".+\.[Tt][Xx][Tt]"

class-map type regex match-any BAD_FILES
 match regex FILE_TYPE_TXT
 match regex FILE_TYPE_GIF

policy-map type inspect http BLOCK_FILES
 parameters
  match request uri regex class BAD_FILES
  drop-connection

class-map HTTP_TRAFFIC
 match port tcp eq http

policy-map INSIDE_POLICY
 class HTTP_TRAFFIC
  inspect http BLOCK_FILES

service-policy INSIDE_POLICY interface inside
```

Поиск неисправностей

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
```

Ping TCP

```
asa# ping tcp 10.0.1.100 23
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.1.100 port 23
from 10.0.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 122/153/184 ms
ciscoasa# ping tcp 10.0.1.100 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.1.100 port 80
from 10.0.1.1, timeout is 2 seconds:
RRRRR
Success rate is 0 percent (0/5)

asa# ping tcp
Interface: inside
Target IP address: 192.168.12.100
Destination port: [80]
Specify source? [n]: y
Source IP address: 10.0.1.100
Source port: [0] 5000
Repeat count: [5]
Timeout in seconds: [2]
Type escape sequence to abort.
Sending 5 TCP SYN requests to 192.168.12.100 port 80
from 10.0.1.100 starting port 5000, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/157/305 ms
```

Ping TCP

```
asa# ping tcp inside 192.168.12.100 80 source 10.0.1.100 5000
Type escape sequence to abort.
Sending 5 TCP SYN requests to 192.168.12.100 port 80
from 10.0.1.100 starting port 5000, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/107/289 ms
```

```
ciscoasa# sh xlate
8 in use, 8 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
TCP PAT from inside:10.0.1.100/5004 to outside:192.168.12.1/31725 flags ri idle 0:00:01 timeout 0:00:30
TCP PAT from inside:10.0.1.100/5003 to outside:192.168.12.1/52161 flags ri idle 0:00:01 timeout 0:00:30
TCP PAT from inside:10.0.1.100/5002 to outside:192.168.12.1/35413 flags ri idle 0:00:01 timeout 0:00:30
TCP PAT from inside:10.0.1.100/5001 to outside:192.168.12.1/34729 flags ri idle 0:00:01 timeout 0:00:30
TCP PAT from inside:10.0.1.100/5000 to outside:192.168.12.1/46013 flags ri idle 0:00:01 timeout 0:00:30
TCP PAT from inside:10.0.1.100/33370 to outside:192.168.12.1/46283 flags ri idle 0:08:31 timeout 0:00:30
TCP PAT from inside:10.0.1.100/45162 to outside:192.168.12.1/60192 flags ri idle 0:08:38 timeout 0:00:30
TCP PAT from inside:10.0.1.100/41539 to outside:192.168.12.1/45633 flags ri idle 0:08:44 timeout 0:00:30
```

show service-policy flow

```
asa# sh service-policy flow tcp host 10.0.1.100 host 192.168.12.100 eq 23

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      Match: any
      Action:
        Output flow:
Interface inside:
  Service-policy: INSIDE
    Class-map: TELNET
      Match: port tcp eq telnet
      Action:
        Input flow:  set connection conn-max 3
    Class-map: class-default
      Match: any
      Action:
        Output flow:
```

```
class-map TELNET
 match port tcp eq telnet

policy-map INSIDE
 class TELNET
  set connection conn-max 3

service-policy INSIDE interface inside
```

show asp drop

```
asa# show asp drop

Frame drop:
  No route to host (no-route)                                    5
  Flow is denied by configured rule (acl-drop)                  17
  Connection limit reached (conn-limit)                          4
  FP L2 rule drop (l2_acl)                                      78
  Interface is down (interface-down)                             2

Last clearing: Never

Flow drop:

Last clearing: Never
```

show local-host

```
asa# show local-host
Interface outside: 1 active, 1 maximum active, 0 denied
local host: <192.168.12.100>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
    TCP outside 192.168.12.100:23 inside 10.0.1.100:44423, idle 0:05:44,
bytes 123, flags UIO
    TCP outside 192.168.12.100:23 inside 10.0.1.100:39469, idle 0:03:02,
bytes 173, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.0.1.100>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Xlate:
    TCP PAT from inside:10.0.1.100/44423 to outside:192.168.12.1/10471 flags
ri idle 0:05:48 timeout 0:00:30
    TCP PAT from inside:10.0.1.100/39469 to outside:192.168.12.1/16460 flags
ri idle 0:05:57 timeout 0:00:30

  Conn:
    TCP outside 192.168.12.100:23 inside 10.0.1.100:44423, idle 0:05:44,
bytes 123, flags UIO
    TCP outside 192.168.12.100:23 inside 10.0.1.100:39469, idle 0:03:02,
bytes 173, flags UIO
```

show local-host brief

```
asa# show local-host brief
Interface outside: 1 active, 1 maximum active, 0 denied
local host: <192.168.12.100>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.0.1.100>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
```

Показать хосты у которых большое кол-во сессий

```
asa# show local-host detail  connection tcp 2
Interface outside: 1 active, 1 maximum active, 0 denied
local host: <192.168.12.100>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
    TCP outside:192.168.12.100/23 inside:10.0.1.100/44423,
        flags UIO, idle 3m52s, uptime 3m56s, timeout 1h0m, bytes 123
    TCP outside:192.168.12.100/23 inside:10.0.1.100/39469,
        flags UIO, idle 1m10s, uptime 4m5s, timeout 1h0m, bytes 173
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.0.1.100>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Xlate:
    TCP PAT from inside:10.0.1.100/44423 to outside:192.168.12.1/10471 flags
ri idle 0:03:56 timeout 0:00:30
    TCP PAT from inside:10.0.1.100/39469 to outside:192.168.12.1/16460 flags
ri idle 0:04:05 timeout 0:00:30

  Conn:
    TCP outside:192.168.12.100/23 inside:10.0.1.100/44423,
        flags UIO, idle 3m52s, uptime 3m56s, timeout 1h0m, bytes 123
    TCP outside:192.168.12.100/23 inside:10.0.1.100/39469,
        flags UIO, idle 1m10s, uptime 4m5s, timeout 1h0m, bytes 173
```

Порты выделенные под NAT

```
asa# sh nat pool
UDP PAT pool inside, address 10.0.1.1, range 1-511, allocated 0
UDP PAT pool inside, address 10.0.1.1, range 512-1023, allocated 0
UDP PAT pool inside, address 10.0.1.1, range 1024-65535, allocated 4
TCP PAT pool outside, address 192.168.12.1, range 1-511, allocated 0
TCP PAT pool outside, address 192.168.12.1, range 512-1023, allocated 0
TCP PAT pool outside, address 192.168.12.1, range 1024-65535, allocated 2
UDP PAT pool outside, address 192.168.12.1, range 1-511, allocated 0
UDP PAT pool outside, address 192.168.12.1, range 512-1023, allocated 0
UDP PAT pool outside, address 192.168.12.1, range 1024-65535, allocated 4
```

Сессии

```
asa# sh conn detail
3 in use, 3 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C -
CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f -
inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP
connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:192.168.12.100/80 inside:10.0.1.100/44954,
    flags U, idle 3s, uptime 3s, timeout 1h0m, bytes 0
TCP outside:192.168.12.100/23 inside:10.0.1.100/44423,
    flags UIO, idle 5s, uptime 9s, timeout 1h0m, bytes 123
TCP outside:192.168.12.100/23 inside:10.0.1.100/39469,
    flags UIO, idle 11s, uptime 18s, timeout 1h0m, bytes 122
```

Процессы

```
asa# sh processes cpu-usage sorted non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x0806a702   0xb5db4130     4.4%     0.9%     2.3%   ci/console
0x081d8531   0xb5dc0e58     0.9%     0.3%     0.1%   Dispatch Unit
0x081d6b94   0xb5dbf5f8     0.5%     0.2%     0.1%   dbgtrace
0x08af25bc   0xb5db3b18     0.1%     0.1%     0.1%   update_cpu_usage
```

Статистика по передаче данных

```
asa# show traffic
inside:
        received (in 919.920 secs):
                136 packets     14958 bytes
                0 pkts/sec      16 bytes/sec
        transmitted (in 919.920 secs):
                112 packets     10552 bytes
                0 pkts/sec      11 bytes/sec
      1 minute input rate 1 pkts/sec,  129 bytes/sec
      1 minute output rate 1 pkts/sec,  120 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  49 bytes/sec
      5 minute output rate 0 pkts/sec,  35 bytes/sec
      5 minute drop rate, 0 pkts/sec
outside:
        received (in 919.930 secs):
                130 packets     14546 bytes
                0 pkts/sec      15 bytes/sec
        transmitted (in 919.930 secs):
                119 packets     11828 bytes
                0 pkts/sec      12 bytes/sec
      1 minute input rate 1 pkts/sec,  131 bytes/sec
      1 minute output rate 1 pkts/sec,  123 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  48 bytes/sec
      5 minute output rate 0 pkts/sec,  39 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

Статистика по передаче данных (продолжение)

```
----------------------------------------
Aggregated Traffic on Physical Interface
----------------------------------------
GigabitEthernet0:
        received (in 922.010 secs):
                136 packets     16926 bytes
                0 pkts/sec      18 bytes/sec
        transmitted (in 922.010 secs):
                112 packets     12120 bytes
                0 pkts/sec      13 bytes/sec
      1 minute input rate 1 pkts/sec,  146 bytes/sec
      1 minute output rate 1 pkts/sec,  136 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  56 bytes/sec
      5 minute output rate 0 pkts/sec,  40 bytes/sec
      5 minute drop rate, 0 pkts/sec
GigabitEthernet1:
        received (in 922.020 secs):
                130 packets     16422 bytes
                0 pkts/sec      17 bytes/sec
        transmitted (in 922.020 secs):
                119 packets     13494 bytes
                0 pkts/sec      14 bytes/sec
      1 minute input rate 1 pkts/sec,  149 bytes/sec
      1 minute output rate 1 pkts/sec,  140 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  54 bytes/sec
      5 minute output rate 0 pkts/sec,  44 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

Ограничение сессий

```
access-list HOST_1 permit ip any 10.1.1.11 255.255.255.255

class-map LOCAL_SERVER
 match access-list HOST_1

class-map ALL-IP
 match any

policy-map LOCAL_POLICY
 class LOCAL_SERVER
  set connection conn-max 256
  random-sequence-number disable
 class ALL-IP
  set connection decrement-ttl

service-policy LOCAL_POLICY interface inside
```

Политика для менеджмент трафика

Политика для менеджмент-трафика

```
class-map type management MGMT_CMAP
 match port tcp eq telnet

policy-map MGMT_PMAP
 class MGMT_CMAP
  set connection conn-max 1

service-policy MGMT_PMAP interface inside
```

Политика для менеджмент-трафика

```
show service-policy
Interface inside:
  Service-policy: MGMT_PMAP
    Class-map: MGMT_CMAP
      Set connection policy: conn-max 1
        current conns 1, drop 3
```

```
show service-policy flow tcp host 10.0.1.2 host
10.0.1.1 eq 23
Interface inside:
  Service-policy: MGMT_PMAP
    Class-map: MGMT_CMAP
      Match: port tcp eq telnet
      Action:
        Input flow:  set connection conn-max 1
```

IPsec path thru

IPsec path thru

```
access-list IPSEC_ACL permit udp any any eq 500
access-list IPSEC_ACL permit udp any any eq 4500

class-map IPSEC_CLASS
 match access-list IPSEC_ACL

policy-map type inspect ipsec-pass-thru IPSEC
 parameters
  esp per-client-max 10

policy-map POLICY
 class IPSEC_CLASS
  inspect ipsec-pass-thru IPSEC

service-policy POLICY interface outside
```

TCP State Bypass

TCP State Bypass

```
access-list BYPASS permit tcp host 10.0.0.1 host 8.7.23.4 eq 25
access-list BYPASS permit tcp host 8.7.23.4 eq 25 host 10.0.0.1

class-map STATE-BYPASS
 match access-group STATE-BYPASS-ACL

policy-map global_policy
 class BYPASS
  set connection advanced-options tcp-state-bypass

service-policy global_policy global
```

Настройка базовых правил фильтрации и инспектирования трафика на Cisco ASA

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

Сетевые Дни