PORT SECURITY

4.7.1.1

Комплекс мероприятий для обеспечения защиты физических портов коммутатора от несанкционированного доступа известен как Port Security.

В отличие от упомянутых выше технологий, Port Security почти не регламентируют едиными промышленными стандартами. Серьезное исключение составляет стандарт 802.1X.

Рассмотрим Port Security применительно к сетевому оборудованию Cisco.

4.7.1.2

Port Security конфигурируют в отношении индивидуального L2-порта или группы L2-портов, что применимо только к портам доступа и транкам -- с учетом виланов (с L3-портами, DTP, EtherChannels и некоторыми другими возможностями совместимости нет).

4.7.1.3a

После включения Port Security, со ставшим таким образом защищенным портом (secure port) могут ассоциироваться статические и динамические доверительные MAC-адреса (secure MAC addresses), но их суммарное количество не должно превышать установленного максимума.

В рамках лимита, доверительными адресами автоматически становятся изученные первыми динамические адреса (в том числе изученные до включения Port Security) и явно указываемые статические адреса (в данном случае приоритета не имеют).

Все остальные динамические адреса считаются недоверительными, недоверительные статические адреса в отношении защищенного порта не поддерживаются.

Понятно, что отдельно взятый адрес может быть доверительным либо недоверительным.

4.7.1.3b

После включения опционального более «серьезного» изучения (sticky address learning) динамические доверительные адреса (в том числе изученные до включения этой возможности) считаются «липкими» (sticky) и, в результате, сохраняются не только в CAM-таблице, а и в рабочей конфигурации.

В добавок, можно явно указать какие адреса считать «липкими».

«Липкие» адреса не теряются при выключении-включении порта (физическая перекоммутация, административное выключение-включение и так далее).

Можно задать время валидности доверительных адресов (port security aging).

4.7.1.4

Как вы думаете, что можно рассматривать как попытку несанкционированного доступа при Port Security?

4.7.1.5

Если MAC-адрес источника из принятого портом кадра не содержится в окончательно сформированном списке доверительных адресов или содержится в списке доверительных адресов, привязанных к другому порту, то это рассматривается как попытка несанкционированного доступа (security violation).

Можно выбрать один из нескольких режимов реагирования на таковую ситуацию (violation mode).

	Protect	Restrict	Shutdown	Shutdown VLAN
Отброс несанкционированного пакета	+	+	+	+
SNMP-уведомление	-	+	-	-
Протоколирование	-	+	-	+
Сообщение об ошибке	-	-	-	-
Наращивание счетчика попыток несанкционированного доступа	-	+	+	+
Выключение порта	-	-	+	-

4.7.1.6

Срабатывание Port Security в режиме shutdown переключает порт в особое состояние -- `down (err-disabled)` (не `up`, не просто `down` и не `administratively down`).

Следует отметить, что в таковое состояние порт может перейти и по другим причинам (BPDU Guard, поздняя коллизия, цикл Ethernet keep-alive и так далее).

Для возврата порта в нормальное состояние необходимо административно выключить и затем снова включить порт (`shutdown` и `no shutdown`), либо предварительно настроить автоматическое восстановление командой `errdisable recovery`.

4.7.1.7a

Пример конфигурирования Port Security.

Включают отдельной командой -- `switchport port-security` (только один аргумент; опциональные параметры задают аргументами, следующими за этим, что Port Security не включает).

4.7.1.7b

```
Switch(config)# interface fa0/7
Switch(config-if)#switchport mode access !Либо trunk
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3 vlan access !Опциональный
                                                                 !учет виланов
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#switchport port-security mac-address 6045.cba7.f876
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security mac-address sticky 7054.d2bf.5b81
                  !Таким же образом вносится в рабочую конфигурацию
                  !автоматически (после предыдущей команды)
Switch(config-if)#switchport port-security aging time 1440 !Минуты
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#switchport port-security aging static
Switch(config-if)#exit
```

4.7.1.8

Основная команда для определения состояния Port Security -- это `show port-security` (без аргументов, с аргументом `address`, с аргументом `interface`).

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              2            2                  1         Shutdown
      Fa0/2              2            1                  2         Restrict
      Fa0/3              1            1                  0         Shutdown
      Fa0/4              1            1                  0         Protect
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
```

4.7.1.10a

Пример настройки автовосстановления.

4.7.1.10b

```
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#errdisable recovery interval 86400



Switch#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
link-flap                    Disabled
mac-limit                    Disabled
loopback                     Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Enabled
security-violation           Disabled
sfp-config-mismatch          Disabled
small-frame                  Disabled
storm-control                Disabled
udld                         Disabled
vmps                         Disabled

Timer interval: 86400 seconds

Interfaces that will be enabled at the next timeout:
```

4.7.1.11

Table ***Default Port Security Configuration***

Feature	Default Setting
Port security	Disabled on a port.
Sticky address learning	Disabled.
Maximum number of secure MAC addresses per port	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Port security aging	Disabled. Aging time is 0. Static aging is disabled. Type is absolute.

Конфигурация порта коммутатора Cisco по умолчанию применительно к Port Security [Cisco]

4.7.1.12

Table *Port Security Compatibility with Other Switch Features*

Type of Port or Feature on Port	Compatible with Port Security
DTP[1] port[2]	No
Trunk port	Yes
Dynamic-access port[3]	No
Routed port	No
SPAN source port	Yes
SPAN destination port	No
EtherChannel	No
Tunneling port	Yes
Protected port	Yes
IEEE 802.1x port	Yes
Voice VLAN port[4]	Yes
Private VLAN port	Yes
IP source guard	Yes
Dynamic Address Resolution Protocol (ARP) inspection	Yes
Flex Links	Yes

1. DTP = Dynamic Trunking Protocol
2. A port configured with the **switchport mode dynamic** interface configuration command.
3. A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.
4. You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.

Совместимость Port Security с другими возможностями [Cisco]

4.7.2.1

Кроме собственно Port Security, есть еще две технологии Cisco для защиты портов: Port Blocking (запрет передачи портом незнакомого юникаст- и мультикаст-трафика) и Protected Ports (трафик между protected-портами запрещен).

ACCESS CONTROL LISTS

4.8.1.1

ACLs (Access Control Lists) -- это универсальный механизм описания правил фильтрации пакетов, который может быть задействован различными подсистемами маршрутизаторов и коммутаторов.

ACLs не регламентируют едиными промышленными стандартами.

Рассмотрим ACLs применительно к сетевому оборудованию Cisco.

4.8.2.1

Один отдельно взятый ACL, то есть список, состоит из некоторого количества упорядоченных элементов -- ACEs (Access Control Entries).

Каждый элемент представляет собой отдельное правило фильтрации.

Правило может быть разрешающим (`permit`) либо запрещающим (`deny`).

ACL создается после ввода первого его правила. Затем, по мере ввода дополнительных правил, ACEs автоматически дописываются в конец списка.

При этом ACEs автоматически последовательно нумеруются начиная с 10 с шагом 10, что открывает возможность вставлять дополнительные ACEs в «нужные места», но редактировать список произвольным образом возможности нет.

Номера в рабочей конфигурации не сохраняются, поэтому таковая автоматическая перенумерация происходит и после перезагрузки.

Команда `ip access-list resequence` позволяет автоматически перенумеровать ACEs когда угодно.

4.8.3.1

Фундаментально ACLs делят на три типа:

1. Port ACLs -- применимы к L2-интерфейсам (физическим портам).

2. Router ACLs -- применимы к L3-интерфейсам (обычным сетевым интерфейсам, SVIs и L3-EtherChannels).

3. VLAN ACLs (VLAN maps) -- применимы к виланам.

4.8.3.2

С точки зрения направленности потока пакетов ACLs могут быть:

1. Входными (inbound) -- предназначены для фильтрации входящего трафика, проверка происходит еще до маршрутизации.

2. Выходными (outbound) -- предназначены для фильтрации исходящего трафика, проверка происходит после маршрутизации.

4.8.3.3

С одним интерфейсом одного уровня в одном направлении по одному протоколу может быть связан только один ACL.

При повторном связывании, предыдущий ACL вытесняется новым.

Аналогично, с одним виланом может быть связана только одна карта VLAN map. Применительно к VLAN map направление трафика не учитывается.

Port ACL проверяется перед router ACL и VLAN map.

4.8.4.1

Поступивший пакет последовательно, в направлении от начала к концу ACL, сопоставляется с ACEs -- вплоть до первого выполнения условия фильтрации.

При обнаружении «попадания» пакет дальше не подвергается анализу, то есть либо пропускается, либо отбрасывается.

Поэтому порядок ACEs критически важен.

ACL всегда заканчивается неявным запретом. Следовательно, при «непопадании» пакет отбрасывается (при отсутствии ACL, по умолчанию, пакет продвигается без ограничений).

4.8.4.2

Основное правило при выборе места для ACL заключается в том, что список нужно помещать туда, где он наиболее эффективен, то есть наилучшим образом сдерживает нежелательный трафик.

4.8.5.1

С точки зрения синтаксиса ACLs могут быть:

1. Нумерованными (numbered) -- идентифицируются уникальными номерами. «Рядовые». Особенны тем, что не подлежат редактированию.

2. Именованными (named) -- идентифицируются уникальными названиями. Совместимы не со всеми командами. В качестве названий можно присваивать и номера, но согласно правилам для нумерованных ACLs. Особенны тем, что их можно редактировать (в соответствующих режимах конфигурирования добавлять или удалять ACEs).

4.8.5.2

Table *Access List Numbers*

Access List Number	Type
1–99	IP standard access list
100–199	IP extended access list
200–299	Protocol type-code access list
300–399	DECnet access list
400–499	XNS standard access list
500–599	XNS extended access list
600–699	AppleTalk access list
700–799	48-bit MAC address access list
800–899	IPX standard access list
900–999	IPX extended access list
1000–1099	IPX SAP access list
1100–1199	Extended 48-bit MAC address access list
1200–1299	IPX summary address access list
1300–1999	IP standard access list (expanded range)
2000–2699	IP extended access list (expanded range)

Нумерация Cisco ACLs [Cisco]

4.8.5.3

Наибольший интерес представляют следующие виды ACLs:

1. Стандартные (standard) IP ACLs (зарезервированы номера 1 -- 99, 1300 -- 1999) -- позволяют выполнять фильтрацию только на основе IP-адресов источников. Применимы к L2- и к L3-интерфейсам.

2. Расширенные (extended) IP ACLs (зарезервированы номера 100 -- 199, 2000 -- 2699) -- позволяют выполнять фильтрацию на основе IP-адресов источников, IP-адресов назначения, L4-протоколов и номеров программных портов. Применимы к L2- и к L3-интерфейсам.

3. Расширенные MAC ACLs (зарезервированы номера 1100 -- 1199) -- позволяют выполнять фильтрацию на основе MAC-адресов источников, MAC-адресов назначения и L3-протоколов. Применимы к L2-интерфейсам.

4.8.6.1

Какая часть IP-адреса должна учитываться при фильтрации, задают с помощью так называемой *wildcard-маски*: нули соответствуют учитываемым битам, единицы -- неучитываемым.

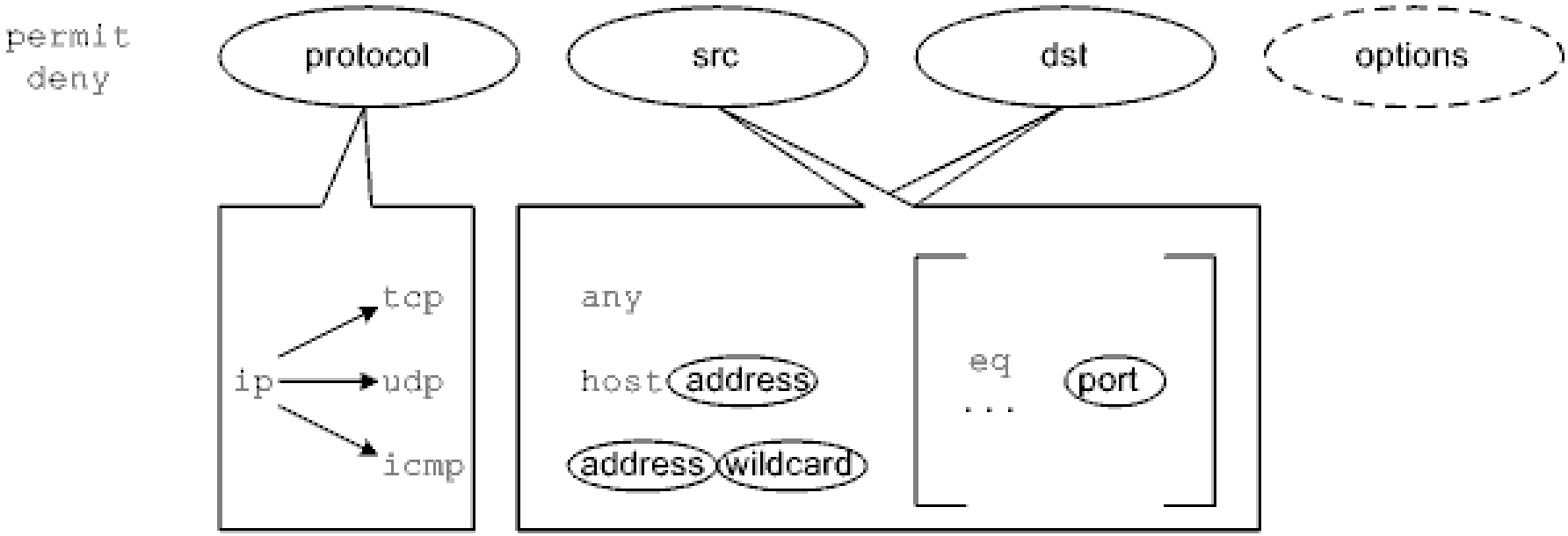
Ключевые слова `any` и `host` позволяют сослаться на любой и конкретный хост соответственно.

4.8.6.2

Условия в ACEs могут содержать следующие операторы: `eq` (equal), `gt` (greater than), `lt` (less than), `neq` (not equal) и `range` (inclusive range).

4.8.6.3

Наиболее полные варианты команд для ввода правил ACLs имеют достаточно сложный формат. Более того, набор допустимых аргументов вариативен, то есть наличие и значение некоторых аргументов зависит от наличия и значения других аргументов.



4.8.6.4

IOS упреждает конфликты между ACEs в ACL, не позволяя вводить соответствующие правила.

Если при вводе команды программный порт был указан цифрой, но предусмотрен символьный вариант (согласно именованию протокола), то при переносе в рабочую конфигурацию произойдет автоматическая замена на символьный вариант.

Предусмотрено также именование ICMP-сообщений.

4.8.6.5a

Table *Well-Known TCP Port Numbers and Key Words*

Keyword	Port Number	Description
aol	5190	America-Online
bgp	179	Border Gateway Protocol
chargen	19	Character Generator
citrix-ica	1494	Citrix Independent Computing Architecture Protocol
cmd	514	Same as exec, with automatic authentication
ctiqbe	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	13	Daytime
discard	9	Discard
domain	53	Domain Name System
echo	7	Echo
exec	512	Exec (RSH)
finger	79	Finger
ftp	21	File Transfer Protocol
ftp-data	20	FTP data connections
gopher	70	Gopher
h323	1720	H.323 call signaling
hostname	101	NIC hostname server
http	80	Hypertext Transfer Protocol
https	443	HTTP over TLS/SSL
ident	113	Ident Protocol
imap4	143	Internet Message Access Protocol, version 4
irc	194	Internet Relay Chat
kerberos	88	Kerberos
klogin	543	Kerberos Login
kshell	544	Kerberos Shell

Table *Well-Known TCP Port Numbers and Key Words (continued)*

Keyword	Port Number	Description
ldap	389	Lightweight Directory Access Protocol
ldaps	636	LDAP over TLS/SSL
login	513	Login (rlogin)
lotusnotes	1352	IBM Lotus Notes
lpd	515	Printer Service
matip-a	350	Mapping of Airline Traffic over Internet Protocol (MATIP) Type A
netbios-ssn	139	NetBIOS Session Service
nntp	119	Network News Transport Protocol
pcanywhere-data	5631	PC Anywhere data
pim-auto-rp	496	PIM Auto-RP
pop2	109	Post Office Protocol v2
pop3	110	Post Office Protocol v3
pptp	1723	Point-to-Point Tunneling Protocol, RFC 2637
rtsp	554	Real Time Streaming Protocol
sip	5060	Session Initiation Protocol
smtp	25	Simple Mail Transfer Protocol
sqlnet	1521	Structured Query Language Network
ssh	22	Secure Shell
sunrpc	111	Sun Remote Procedure Call
tacacs	49	Terminal Access Controller Access Control System
talk	517	Talk
telnet	23	Telnet
time	37	Time
uucp	540	Unix-to-Unix Copy Program
whois	43	Nicname
www	80	World Wide Web (HTTP)

Именование протоколов в Cisco ACLs [Cisco]

4.8.6.5b

Table *Well-Known UDP Port Numbers and Key Words*

Keyword	Port Number	Description
biff	512	Mail notification
bootpc	68	Bootstrap Protocol (BOOTP) client
bootps	67	Bootstrap Protocol (BOOTP) server
discard	9	Discard
dnsix	195	DNSIX Security protocol auditing (dn6-nlm-aud)
domain	53	Domain Name System
echo	7	Echo
isakmp	500	Internet Security Association Key Management Protocol
kerberos	88	Kerberos
mobile-ip	434	Mobile IP registration
nameserver	42	Host Name Server
netbios-dgm	138	NetBIOS datagram service
netbios-ns	137	NetBIOS name service
netbios-ssn	139	NetBIOS Session Service
ntp	123	Network Time Protocol
pcanywhere-status	5632	PC Anywhere status

Table *Well-Known UDP Port Numbers and Key Words (continued)*

Keyword	Port Number	Description
radius	1812	Remote Authentication Dial-in User Service
radius-acct	1813	RADIUS Accounting
rip	520	Routing Information Protocol
snmp	161	Simple Network Management Protocol
snmptrap	162	SNMP Traps
sunrpc	111	Sun Remote Procedure Call
syslog	514	System Logger
tacacs	49	Terminal Access Controller Access Control System
talk	517	Talk
tftp	69	Trivial File Transfer Protocol
time	37	Time
who	513	Who service (rwho)
wsp	9200	Connectionless Wireless Session Protocol
wsp-wtls	9202	Secure Connectionless WSP
wsp-wtp	9201	Connection-based WSP
wsp-wtp-wtls	9203	Secure Connection-based WSP
xdmcp	177	X Display Manager Control Protocol

Именование протоколов в Cisco ACLs [Cisco]

4.8.6.6

Table ICMP Types

ICMP Code Number	ICMP Type
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

Именование ICMP-сообщений в Cisco ACLs [Cisco]

4.8.6.7

ACE в ACL может быть с комментарием -- `remark` (до ста символов включительно).

Комментарий вносят до либо после правила к которому его относят (в какое место будет записан -- там и будет).

4.8.6.8a

Пример создания нумерованного стандартного IP ACL (запрет IP-трафика только от одной станции).

```
Router(config)#access-list 99 deny host 192.168.11.100
Router(config)#access-list 99 permit any
```

4.8.6.9a

Пример создания нумерованного расширенного IP ACL (запрет обращения станциям из подсети к серверу по протоколу HTTP).

```
Router(config)#access-list 199 deny tcp 192.168.11.128 0.0.0.31 host 192.168.11.11 eq www
Router(config)#access-list 199 permit tcp any any
```

4.8.6.10a

Пример создания именованного расширенного IP ACL (аналогичный запрет обращения станциям из подсети к серверу по протоколу HTTP).

Применительно к названиям ACLs, как и к другим названиям, Cisco рекомендует использовать прописные буквы. При этом прописные и строчные буквы различаются.

```
Router(config)#ip access-list extended WEB
Router(config-ext-nacl)#deny tcp 192.168.11.128 0.0.0.31 host 192.168.11.11 eq www
Router(config-ext-nacl)#permit tcp any any
Router(config-ext-nacl)#exit
```

4.8.6.11a

Пример создания именованного расширенного MAC ACL (разрешение трафика от одной станции).

```
Switch(config)#mac access-list extended ALLOWED-NODE
Switch(config-ext-macl)#permit host 000c.f044.4444 any
Switch(config-ext-macl)#exit
```

4.8.6.12a

Пример ICMP-фильтрации.

```
Router(config)#access-list 110 deny icmp host 192.168.0.5 host 10.0.0.5 echo-reply
Router(config)#access-list 110 permit icmp any any
```

4.8.6.13

ACL обязательно нужно привязать к чему-либо, иначе ACL не имеет смысла.

4.8.6.14a

Примеры привязки ACLs к интерфейсам.

```
Router(config)#interface gi0/0
Router(config-if)#ip access-group 99 in
Router(config-if)#exit

Router(config)#interface gi0/1
Router(config-if)#ip access-group WEB out
Router(config-if)#exit
```

4.8.6.15

Для просмотра состояния ACLs используют команду `show access-lists`.

При этом для каждого правила в скобках показывается число попаданий (на высокопроизводительных платформах с аппаратным ускорением могут отображаться некорректно).

Очистить счетчики попаданий можно командой `clear access-list counters`.

4.8.6.16

```
Router#show access-lists

Extended IP access list ACL-EVM-OUT
    10 permit tcp any eq 22 any (24047887 matches)
    20 permit tcp host 192.168.59.147 any (10492859 matches)
    30 permit ip any 192.168.251.0 0.0.0.255 (1269045049 matches)
    40 permit tcp any any eq 22 (158003244 matches)
    50 permit tcp any any eq ftp (1808 matches)
    60 permit tcp any any eq www (14101535 matches)
    70 permit tcp any any eq ftp-data (39 matches)
    80 permit tcp any any eq smtp (1087794 matches)
    90 permit udp any any eq ntp (2775399 matches)
    100 permit tcp any any eq pop3 (5027700 matches)
    110 permit tcp any any eq 143 (1093542 matches)
    112 permit tcp any any eq 443 (16603722 matches)
    114 permit tcp any any eq 873 (318056446 matches)
    116 permit tcp any any eq 993 (5123405 matches)
    117 permit tcp any any eq 995 (291224 matches)
    119 permit tcp any any eq 3690 (1383712 matches)
    120 permit icmp any any (640756 matches)
    130 permit ip host 192.168.11.15 any (4521298 matches)
    140 permit ip host 192.168.59.145 any (360655 matches)
    150 permit ip host 192.168.11.155 any
    160 permit ip host 192.168.11.156 any
    170 deny ip any any (38186043 matches)
```

4.8.6.17a

Пример редактирования именованного стандартного IP ACL.

```
Router(config)#ip access-list standard TEST
Router(config-std-nacl)#no 10
Router(config-std-nacl)#32 permit host 192.168.0.3
Router(config-std-nacl)#exit
```

4.8.7.1

Привязка ACL к линии возможна, но имеет особенности.

```
Router(config)#access-list 23 permit host 192.168.11.11
Router(config)#access-list 23 deny any

Router(config)#line vty 0 4
Router(config-if)#ip access-class 23 in
Router(config-if)#exit
```

4.8.8.1a

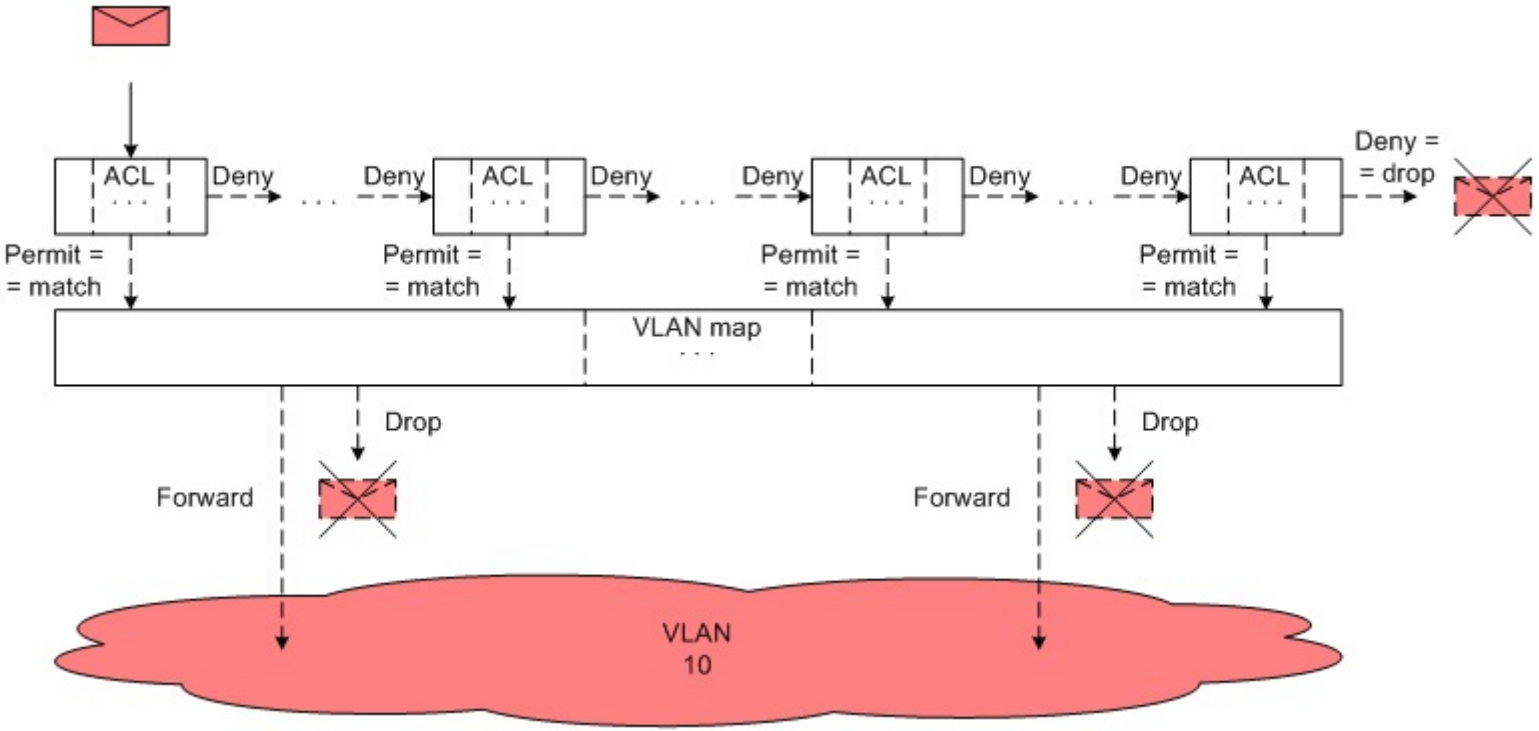
Карта VLAN map предназначена для отображения одного либо нескольких ACLs в один либо несколько виланов.

Карта указывает действие (`forward` -- по умолчанию, либо `drop`), которое нужно совершить с пакетом при попадании, то есть «срабатывании» одного из списков ACL (под «срабатыванием» ACL здесь понимают «срабатывание» именно одного из разрешающих правил; следовательно явные запрещающие правила практически не имеют смысла, разве что ускоряют обработку ACL при большом числе специфических разрешающих правил).

Если ни один из списков ACL «не сработал» то пакет неявно отбрасывается.

Карту идентифицируют названием и номером. Номер позволяет объединять отдельно взятые карты с одинаковыми названиями -- по аналогии с ACEs в ACL (если номер не указан, то присваивается автоматически с шагом 10). Название используют при привязке карты к виланам.

4.8.8.1b


ACL
Deny
Deny
ACL
Deny
Deny
ACL
Deny
Deny
ACL
Deny =
= drop
Permit =
= match
Permit =
= match
Permit =
= match
Permit =
= match
VLAN map
Drop
Drop
Forward
Forward
VLAN
10

4.8.8.2

Для просмотра карт используют команду `show vlan access-map` и `show vlan filter`.

4.8.8.3a

Пример создания и привязки VLAN map.

```
Switch(config)#vlan access-map MAP1 10
Switch(config-access-map)#match ip address ACL1
Switch(config-access-map)#action forward
Switch(config-access-map)#exit

Switch(config)#vlan access-map MAP1 20
Switch(config-access-map)#match ip address 190 191
Switch(config-access-map)#action drop
Switch(config-access-map)#exit

Switch(config)#vlan filter MAP1 vlan-list 2
```

4.8.9.1

IPv6 ACL в настоящее время находятся в состоянии разработки и имеют ограничения.

Отличия IPv6 ACL от IPv4 ACL:

1. Только именованные, причем только расширенные.
2. Привязывают к интерфейсу командой `ipv6 traffic-filter`.
3. Используют не wildcard-маски, а IPv6-префиксы.
4. Перед неявным запретом в самом конце, есть еще два неявных разрешающими правила: `permit icmp any any nd-na` и `permit icmp any any nd-ns`.

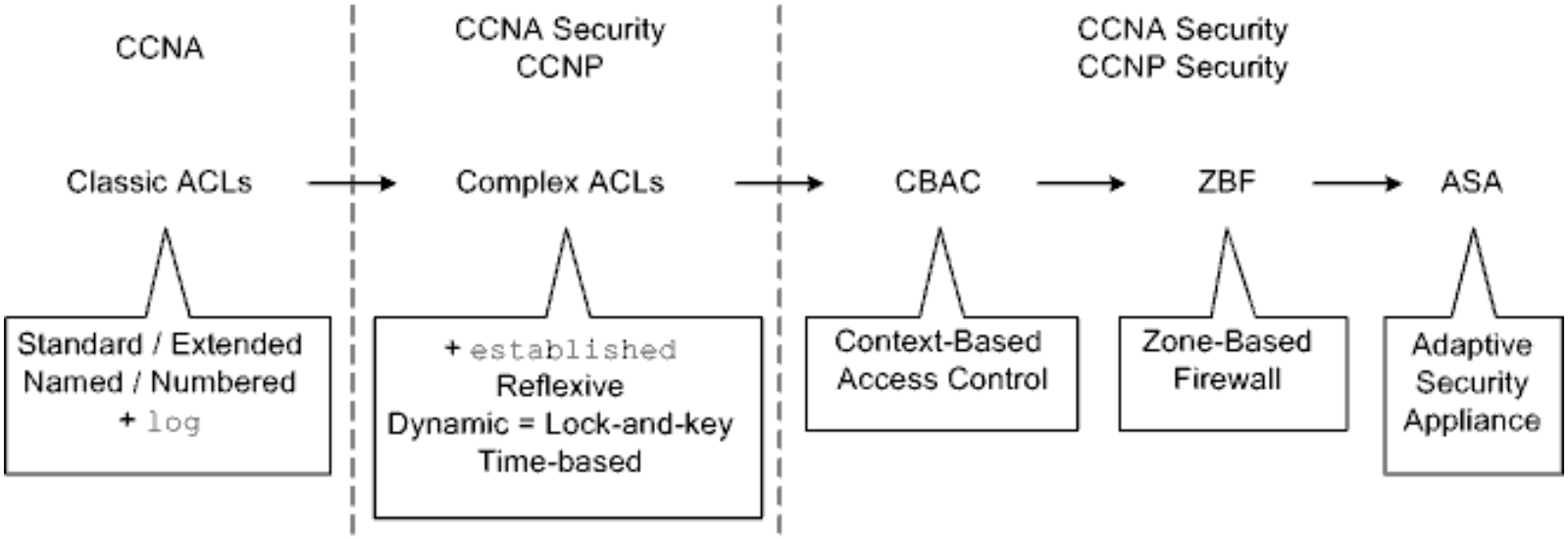
4.8.9.2a

Пример IPv6 ACL.

```
Switch(config)#ipv6 access-list ACL6
Switch(config-ipv6-acl)#deny tcp FE80:0:0:2::/64 any gt 1000 log
Switch(config-ipv6-acl)#permit ipv6 any any
Switch(config-ipv6-acl)#exit

Switch(config)#interface gi0/6
Switch(config-if)#no switchport
Switch(config-if)#ipv6 traffic-filter ACL6 in
Switch(config-if)#exit
```

4.8.10.1

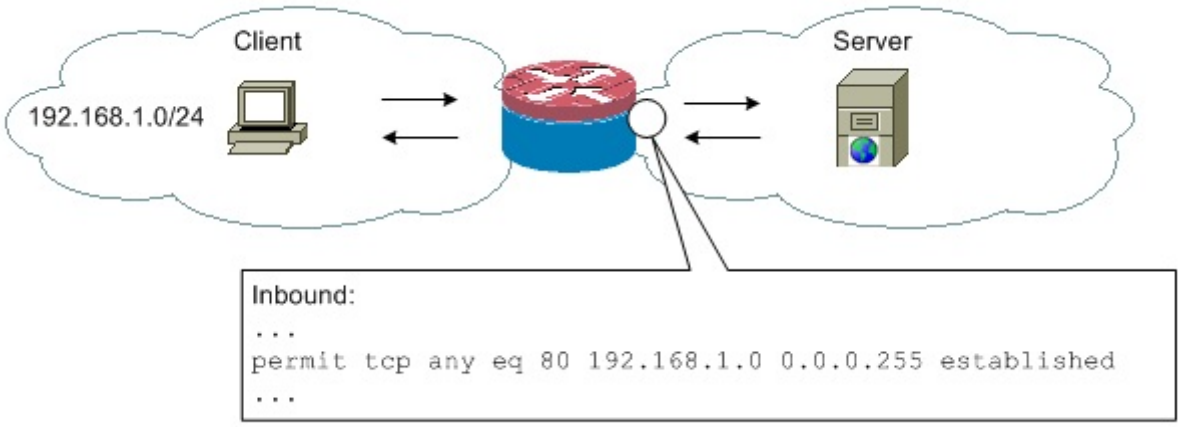


Эволюция Cisco ACLs

4.8.10.2

Правило для фильтрации TCP-трафика может содержать флаг `established` -- говорит о том, что правило будет применяться только к TCP-соединениям находящимся в таковом состоянии. Если флаг ACK в TCP-сегменте не установлен, то считается, что соединение устанавливается (например, извне) и сегмент отбрасывается.

4.8.10.3

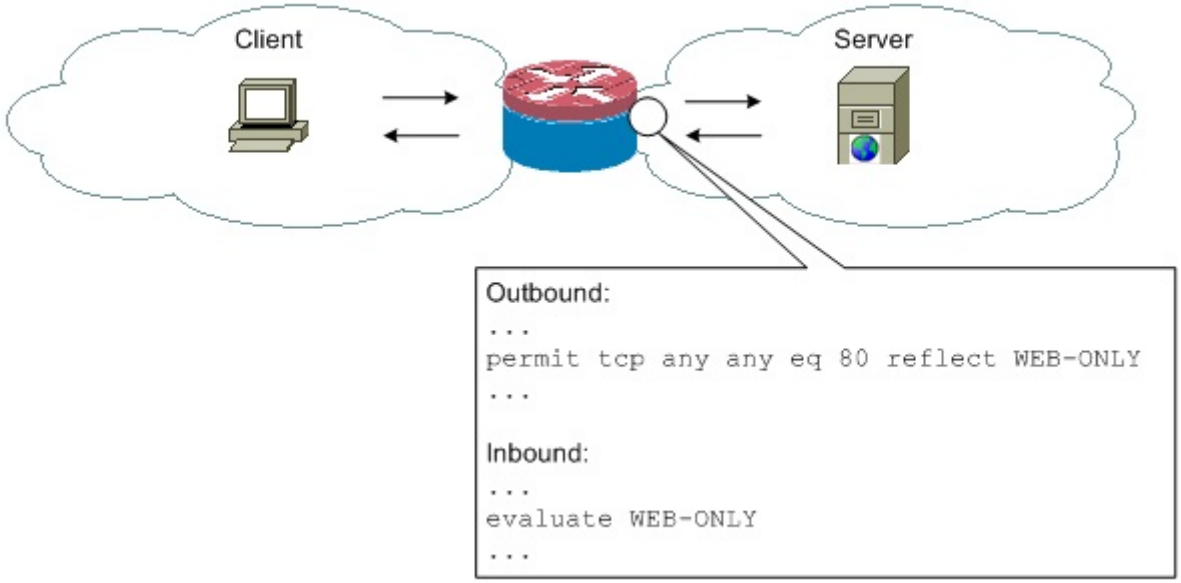


Пример ACL с флагом `established`

4.8.10.4

Идея рефлексивных ACLs заключается в том, чтобы для некоторого правила некоторого ACL автоматически активировать его особым образом описанное «обратное» правило другого ACL, «открывающее дверь» для ответного трафика.

4.8.10.5

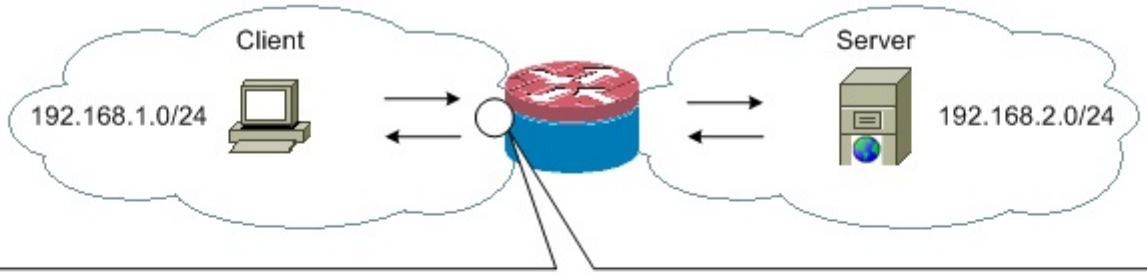


Пример рефлексивных ACLs

4.8.10.6

Идея динамических ACLs (по-другому, Lock-and-key) заключается в том, чтобы автоматически активировать на некоторое время подготовленное правило (placeholder) (только одно) некоторого ACL по условию. Условием является успешность аутентификации посредством Telnet либо SSH.

4.8.10.7



Inbound:

```
...
dynamic ACCESS-TO-SERVERS timeout 15 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 !
!Интервал времени доступа в минутах
...
```

Line:

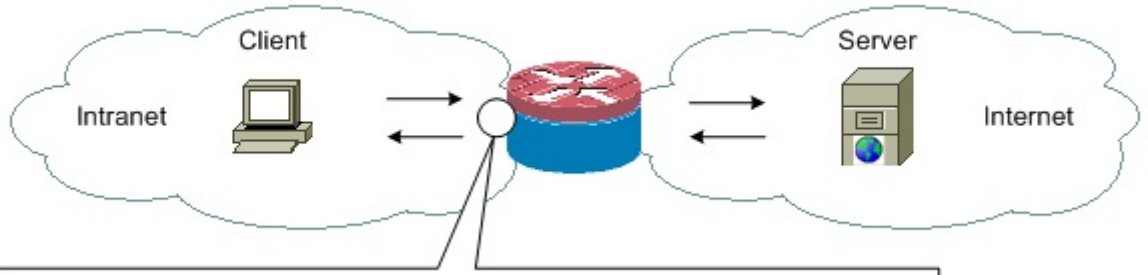
```
...
autocommand access-enable host timeout 5 !Интервал времени неактивности в минутах,
!по истечении которого доступ закрывается
...
```

Пример динамического ACL

4.8.10.8

Временны'е ACLs, в отличие от динамических, срабатывают по расписанию. В правило включается предварительно подготовленное макро `time-range`.

4.8.10.9



Macro:

```
Router(config)#time-range WORKTIME
Router(config-time-range)#periodic weekdays 8:30 to 17:30
Router(config-time-range)#exit
```

Inbound:

```
...
deny tcp any any time-range WORKTIME
...
```

Пример временно'го ACL

4.8.10.10

Более сложные технологии фильтрации являются дальнейшим развитием идеи автоматизации создания и активации правил.

Для облегчения работы с ACLs, если не обойтись без очень большого числа правил фильтрации, Cisco предлагает так называемые группы объектов (object groups).

Cisco FPM (Flexible Packet Matching) позволяет осуществлять фильтрацию пакетов по специальным шаблонам с точностью до бита.

4.8.11.1

В учебниках от Cisco безапелляционно сформулированы два базовых правила размещения ACLs:

1. Расширенные ACLs нужно располагать как можно ближе к источнику нежелательного трафика.

2. Стандартные ACLs нужно располагать как можно ближе к защищаемым станциям.