ASA 8. 4 (x) подключения одиночная внутренняя сеть к интернет-примеру конфигурации

Содержание

Введение

Этот документ описывает, как установить устройство адаптивной защиты Cisco (ASA) с Версией 8.4 (1) для использования в одиночной внутренней сети.

См. [PIX/ASA: Соединение Одиночной внутренней сети с интернет-Примером конфигурации](#) для одинаковой конфигурации на ASA с Версиями 8.2 и ранее.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основываются на ASA с Версией 8.4 (1).

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

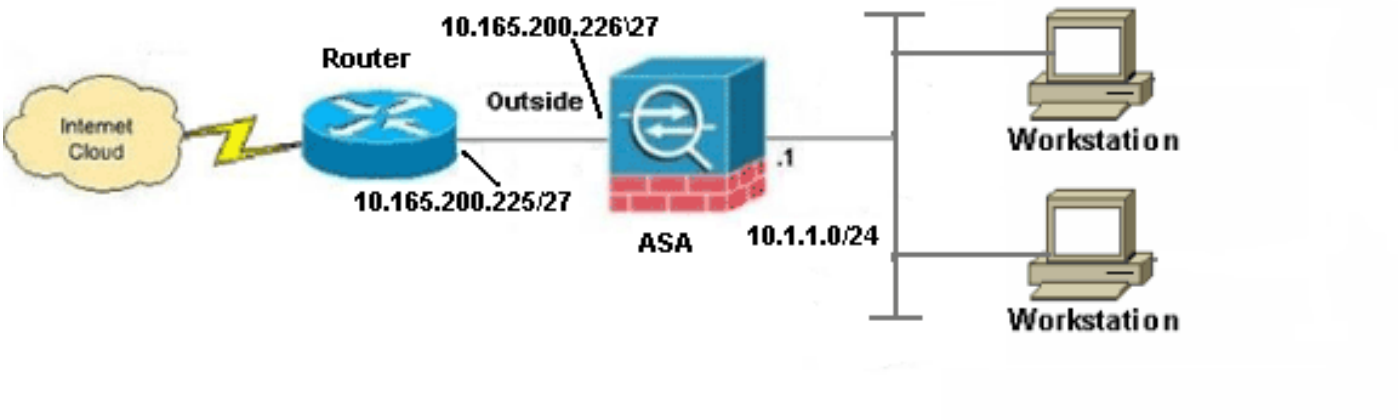
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

> **Примечание:** Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



> **Примечание:** Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Конфигурация

ASA 8. 4

Эти конфигурации используются в данном документе:

- Настройка маршрутизатора
- ASA 8. 4 и более поздняя конфигурация

Настройка маршрутизатора

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

ASA 8. 4 и более поздняя конфигурация

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
```

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (PAT) to the outside interface IP
!--- on the ASA (or 10.165.200.226) for Internet bound traffic.
!
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
!
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
```

```
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
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
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

> **Примечание:** Для получения дополнительной информации о конфигурации Технологии NAT и Преобразования адресов портов (PAT) на Версии ASA 8.4, обратитесь к информации О NAT.
>
> Для получения дополнительной информации о конфигурации списков доступа на Версии ASA 8.4, обратитесь к информации О Списках доступа.

Проверка

Попытайтесь обратиться к веб-сайту через HTTP с web-браузером. Данный пример использует сайт, который размещен в 198.51.100.100. Если соединение успешно, эти выходные данные могут быть замечены на CLI ASA:

Соединение

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA является самонастраивающимся межсетевым экраном, и ответный трафик от Web-сервера позволен назад через межсетевой экран, потому что это совпадает ***с соединением***

в таблице подключений межсетевого экрана. Трафик, который совпадает с соединением, которое существует ранее, позволен через межсетевой экран, не будучи заблокированным интерфейсным ACL.

В предыдущих выходных данных клиент на внутреннем интерфейсе установил соединение с этими 198.51.100.100 хостами прочь внешнего интерфейса. Это соединение сделано с протоколом TCP и было простаивающим в течение шести секунд. Флаги соединения указывают на текущее состояние этого соединения. Дополнительные сведения о флагах соединения могут быть найдены во Флагах TCP - подключения ASA.

Системный журнал

```
ASA(config)# show log | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.1.1.154/58799 (10.165.200.226/58799)
```

Межсетевой экран ASA генерирует системные журналы во время нормальной работы. Системные журналы располагаются в многословии на основе конфигурации журнала. Выходные данные показывают два системных журнала, которые замечены на уровне шесть или **'информационном'** уровне.

В данном примере существует два генерируемые системных журнала. Первым является сообщение журнала, которое указывает, что межсетевой экран создал **трансляцию**, в частности динамическую трансляцию TCP (PAT). Это указывает на IP - адрес источника и порт и преобразованный IP-адрес и порт, поскольку трафик пересекает от внутренней части до внешних интерфейсов.

Второй системный журнал указывает, что межсетевой экран создал **соединение** в своей таблице подключений для этого определенного трафика между клиентом и сервером. Если бы межсетевой экран был настроен для блокирования этой попытки подключения, или некоторый другой фактор запретил создание этого соединения (ограничения ресурса или вероятная неверная конфигурация), то межсетевой экран не генерировал бы журнал, который указывает, что было создано соединение. Вместо этого это регистрировало бы причину для соединения, которое будет запрещено или индикация о том, какой фактор запретил соединению то, чтобы быть созданным.

Преобразования NAT (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 timeout 0:00:30
```

Как часть этой конфигурации, PAT настроен для перевода IP-адресов внутреннего хоста в адреса, которые маршрутизируемы в Интернете. Чтобы подтвердить, что эти трансляции созданы, можно проверить xlate (трансляция) таблица. **Команда show xlate,** когда объединено с **ключевым словом local** и IP-адресом внутреннего хоста, показывает весь подарок записей в таблице преобразования для того хоста. Предыдущие выходные данные

показывают, что существует трансляция, в настоящее время создаваемая для этого хоста между внутренними и внешними интерфейсами. IP внутреннего хоста и порт преобразованы в эти 10.165.200.226 адреса на нашу конфигурацию. Перечисленные флаги, r i, указывают, что трансляция является **динамичной** и **portmap**. Дополнительные сведения о других конфигурациях NAT могут быть найдены здесь: информация О NAT.

Устранение неполадок

ASA предоставляет множественным программным средствам, с которыми можно устранить неполадки подключения. Если проблема сохраняется после того, как вы проверяете конфигурацию и проверяете выходные данные, перечисленные ранее, эти программные средства и способы могли бы помочь определять причину вашего сбоя подключения.

Средство трассировки пакетов

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 1234 198.51.100.100 80


--Omitted--

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

Пакетная функциональность **трассировщика** на ASA позволяет вам задавать *моделируемый* пакет и видеть все различные шаги, проверки и функции, которые проходит межсетевой экран, когда это обрабатывает трафик. С этим программным средством полезно определить пример трафика, которому вы верите *, должен* быть позволен пройти через межсетевой экран и использование, что 5-tupple для моделирования трафика. В предыдущем примере пакетный трассировщик используется для моделирования попытки подключения, которая соответствует этим критериям:

- Моделируемый пакет поступает во **внутреннюю часть**.
- Используемый протокол является **TCP**.
- Моделируемый IP-адрес клиента **10.1.1.154**.
- Клиент передает трафик, полученный от **порта 1234**.
- Трафик предназначен к серверу в IP-адресе **198.51.100.100**.
- Трафик предназначен к **порту 80**.

Заметьте, что не было никакого упоминания об интерфейсе **снаружи** в команде. Это пакетным дизайном трассировщика. Программное средство говорит вам, как межсетевой экран обрабатывает ту попытку типа соединения, которая включает, как это направило бы его, и из который интерфейс. Дополнительные сведения о пакетном трассировщике могут быть найдены в Отслеживании пакетов с Пакетным Трассировщиком.

Перехват

```
ASA# capture capin interface inside match tcp host 10.1.1.154 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#  show capture capin

3 packets captured

  1: 11:31:23.432655      10.1.1.154.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518      198.51.100.100.80 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884      10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869      10.165.200.226.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472      198.51.100.100.80 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914      10.165.200.226.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Межсетевой экран ASA может перехватить трафик, который вводит или оставляет его интерфейсы. Эта функциональность перехвата является фантастической, потому что может окончательно оказаться, поступает ли трафик в или уезжает от, межсетевой экран. Предыдущий пример показал конфигурацию двух перехватов, названных **capin** и **capout** на внутренних и внешних интерфейсах соответственно. Команды перехвата использовали ключевое слово **соответствия**, которое позволяет вам быть определенными, о каком трафике вы хотите перехватить.

Для **capin** перехвата вы указали, что хотели совпасть с трафиком, замеченным на внутреннем интерфейсе (вход или выход), который совпадает **с хостом 198.51.100.100 хоста 10.1.1.154 tcp**. Другими словами, вы хотите перехватить любой Трафик TCP, который передается от **хоста 10.1.1.154** до **хоста 198.51.100.100** или **наоборот**.
Использование ключевого слова **соответствия** позволяет межсетевому экрану перехватывать тот трафик двунаправленным образом. Команда перехвата, определенная для внешнего интерфейса, не ссылается на IP-адрес внутреннего клиента, потому что межсетевой экран проводит PAT на том IP-адресе клиента. В результате вы не можете **совпасть** с тем IP-адресом клиента. Вместо этого данный пример использует **любого**, чтобы указать, что все возможные IP-адреса совпали бы с тем условием.

После настройки перехватов вы тогда делали бы попытку устанавливания соединения снова и продолжили бы просматривать перехваты с командой ***<capture_name>*** **show capture**. В данном примере вы видите, что клиент смог соединиться с сервером как очевидный трехсторонним квитированием TCP, замеченным в перехватах.

Дополнительные сведения

- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES

- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация