Устранение неполадок с подключениями через PIX и ASA

Содержание

Введение

В данном документе содержатся идеи и предложения по устранению неисправностей при использовании модуля адаптивной защиты (ASA) серии Cisco ASA 5500 и устройства защиты серии Cisco PIX 500. Когда приложения или сетевые источники не работают или недоступны, наиболее вероятной причиной сбоя являются брандмауэры (PIX или ASA). При помощи тестирования ASA или PIX администратор может определить, является ли ASA/PIX причиной проблемы.

См. раздел PIX/ASA: Установление подключения и устранение неполадок подключения через устройство защиты Cisco для получения дополнительной информации об интерфейсе для устранения неполадок устройств защиты Cisco.

Примечание: В данном документе рассматривается ASA и PIX. После устранения неполадок на ASA или PIX может потребоваться дополнительное устранение неполадок на других устройствах (маршрутизаторы, коммутаторы, серверы и т.д.). В данном документе рассматривается ASA и PIX.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Сведения, содержащиеся в данном документе, основаны на Cisco ASA 5510 с ОС

Данные для документа были получены в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с пустой (стандартной) конфигурацией. Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Сопутствующие продукты

Этот документ может также использоваться со следующими версиями оборудования и программного обеспечения:

- ОС PIX 6.3
- ОС ASA и PIX 7.0 и 7.1
- Firewall Services Module (FWSM) 2.2, 2.3 и 3.1

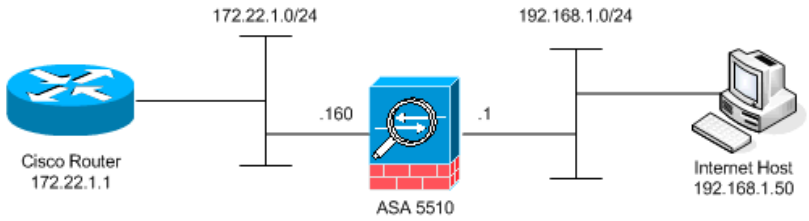
Примечание: Определенные команды и синтаксис могут изменяться в зависимости от версии программного обеспечения.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в документе Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Общие сведения

В примерах считается, что ASA или PIX установлены. Настройка ASA/PIX может быть относительно простой (только 50 строк конфигурации) или сложной (сотни или тысячи строк конфигурации). Пользователи (клиенты) или серверы могут быть в безопасной сети (внутри) или в небезопасной сети (DMZ или снаружи).



ASA запускается в данной конфигурации. Данная конфигурация играет роль эталонной.

Начальная конфигурация ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
shutdown
no nameif
```

```
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host 172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0 255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0
static (inside,outside) 192.168.1.100 172.22.1.254 netmask 255.255.255.255
access-group outside_acl in interface outside
access-group inside_acl in interface inside
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 uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
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 netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Проблема

Пользователь обращается в ИТ-отдел и сообщает, что приложение X больше не работает. Инцидент направляется администратору ASA/PIX. Администратор имеет недостаточно знаний о данном конкретном приложении. При помощи ASA/PIX администратор выясняет, какие порты и протоколы использует приложение X, а также, что может являться причиной проблемы.

Решение

Администратору ASA/PIX требуется получить от пользователя как можно больше сведений. Полезные сведения включают:

- Исходный IP-адрес—Обычно это рабочая станция или компьютер пользователя.

- IP-адрес назначения—IP-адрес сервера, к которому пытается подключиться пользователь или приложение.
- Порты и протоколы, используемые приложением

Часто удачей можно считать, если администратору удастся получить ответ на хотя бы один из этих вопросов. Например, администратору не удалось получить никаких сведений. Просмотр сообщений системного журнала ASA/PIX является отличным решением, но администратору трудно обнаружить проблему, если он не знает, что ему искать.

Шаг 1 — Определение IP-адреса пользователя

Существует множество способов определения IP-адреса пользователя. Данный документ относится к ASA и PIX, поэтому в данном примере используется ASA и PIX для определения IP-адреса.

Пользователь пытается связаться с ASA/PIX. Данная связь может осуществляться по протоколу ICMP, Telnet, SSH или HTTP. Выбранный протокол должен иметь ограниченную активность на ASA/PIX. В данном примере пользователь выполняет проверку связи с внутренним интерфейсом ASA.

Администратору требуется установить один или несколько из следующих параметров, а затем принять запрос пользователя на внутреннем интерфейсе ASA.

- **Системный журнал**

  Убедитесь, что ведение журнала включено. Должен быть установлен уровень ведения журнала **debug**. Журнал может отправляться в несколько мест. В данном примере используется буфер журнала ASA. В рабочей среде может потребоваться внешний сервер журнала.

```
ciscoasa(config)#logging enable
ciscoasa(config)#logging buffered debugging
```

  Пользователь проверяет связь с внутренним интерфейсом ASA (ping 192.168.1.1). Отображаются следующие выходные данные.

```
ciscoasa#show logging
     !--- Output is suppressed.

%ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
%ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
!--- The user IP address is 192.168.1.50.
```

- **Функция захвата ASA**

  Администратору необходимо создать список доступа, который определяет, какой трафик ASA требуется захватывать. После создания списка доступа команда **capture** использует список доступа и применяет его к интерфейсу.

```
ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#capture inside_interface access-list inside_test interface inside
```

  Пользователь проверяет связь с внутренним интерфейсом ASA (ping 192.168.1.1). Отображаются следующие выходные данные.

```
ciscoasa#show capture inside_interface
  1: 13:04:06.284897 192.168.1.50 > 192.168.1.1: icmp: echo request
!--- The user IP address is 192.168.1.50.
```

  Примечание: Для загрузки файла захвата в систему, такую как ethereal, можно использовать следующий способ.

```
!--- Open an Internet Explorer and browse with this https link format:

https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap
```

- **Отладка**

  Команда **debug icmp trace** используется для захвата ICMP-трафика пользователя.

```
ciscoasa#debug icmp trace
```

  Пользователь проверяет связь с внутренним интерфейсом ASA (ping 192.168.1.1). На консоли отображаются следующие выходные данные.

```
ciscoasa#
!--- Output is suppressed.

ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512 seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
!--- The user IP address is 192.168.1.50.
```

  Для отключения **debug icmp trace**используйте одну из этих команд:

  - **no debug icmp trace**
  - **undebug icmp trace**
  - **undebug all**, **Undebug all**или **un all**

Каждый из этих вариантов помогает администратору определить исходный IP-адрес. В данном примере исходный IP-адрес пользователя — 192.168.1.50. Администратор готов узнать больше о приложении X и определить причину проблемы.

Шаг 2 — Определение причины проблемы

Благодаря информации, полученной на Шаге 1 данного документа администратор знает источник сеанса приложения X. Администратор готов узнать больше о приложении X и начать поиск причины проблемы.

Администратору ASA/PIX необходимо подготовить ASA для проверки одного из перечисленных предположений. Когда администратор готов, пользователь запускает приложение X и ограничивает другую деятельность, поскольку дополнительные действия пользователя могут ввести в заблуждение администратора ASA/PIX.

- **Наблюдайте за сообщениями системного журнала.**

  Найдите исходный IP-адрес пользователя, определенный на Шаге 1. Пользователь запускает приложение X. Администратор ASA выполняет команду **show logging** и просматривает выходные данные.

```
ciscoasa#show logging
     !--- Output is suppressed.

%ASA-7-609001: Built local-host inside:192.168.1.50
%ASA-6-305011: Built dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025
%ASA-6-302013: Built outbound TCP connection 90 for outside:172.22.1.1/80
(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
```

  Журнал показывает, что IP-адресом назначения является 172.22.1.1, используется протокол TCP, порт назначения — HTTP/80, а трафик отправляется на внешний интерфейс.

- **Измените фильтры захвата.**

  Команда **access-list inside_test** использовалась ранее и используется здесь.

```
ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
     !--- This ACL line captures all traffic from 192.168.1.50
!--- that goes to or through the ASA.

ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
     !--- This ACL line captures all traffic that leaves
!--- the ASA and goes to 192.168.1.50.

ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#clear capture inside_interface
     !--- Clears the previously logged data.
!--- The no capture inside_interface removes/deletes the capture.
```

  Пользователь запускает приложение X. Затем администратор ASA выполняет команду **show capture inside_interface** и просматривает выходные данные.

```
ciscoasa(config)#show capture inside_interface
1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
```

  Захватываемый трафик предоставляет администратору немного полезной информации:

  - Адрес назначения—172.22.1.1
  - Номер порта—80/http
  - Протокол—TCP (обратите внимание на флаг "S" или syn)

  Кроме того, администратор также знает, что трафик данных приложения X не достигает ASA.

  Если выходные данные были выходными данными команды **show capture inside_interface** , трафик приложения либо не достигает ASA, либо фильтр захвата не был настроен для захвата трафика:

```
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

  В этом случае администратору следует проверить компьютер пользователя и все маршрутизаторы или другие сетевые устройства на пути между компьютером пользователя и ASA.

  Примечание: Когда трафик поступает на интерфейс, команда **capture** записывает данные, перед тем, как какая-либо политика безопасности ASA проанализирует трафик. Например, список доступа отклоняет весь входящий трафик на интерфейсе. Команда **capture** все равно будет записывать трафик. Политика безопасности ASA затем будет анализировать трафик.

- **Отладка**

  Администратор не знаком с приложением X, и поэтому не знает, какие службы отладки следует включить, чтобы исследовать приложение X. Отладка может оказаться неэффективным средством устранения неполадок на данном этапе.

При помощи полученной на Шаге 2 информации администратор ASA получил немного ценной информации. Администратор знает, что трафик поступает на внутренний интерфейс ASA, знает исходный IP-адрес, IP-адрес назначения и используемую приложением X службу (TCP/80). Из системного журнала администратор также знает, что связь была изначально разрешена.

Шаг 3 — Проверка и мониторинг трафика приложения

Администратор ASA хочет проверить, что трафик приложения X покидает ASA, а также понаблюдать за ответным трафиком от сервера приложения X.

- **Наблюдайте за сообщениями системного журнала.**

  Отфильтруйте сообщения системного журнала по исходному IP-адресу (192.168.1.50) или IP-адресу назначения (172.22.1.1). В командной строке команда фильтрации сообщений системного журнала выглядит как **show logging | include 192.168.1.50** или **show logging | include 172.22.1.1**. В данном примере команда **show logging** используется без фильтрации. Выходные данные подавляются, чтобы упростить чтение.

```
ciscoasa#show logging
     !--- Output is suppressed.

%ASA-7-609001: Built local-host inside:192.168.1.50
%ASA-7-609001: Built local-host outside:172.22.1.1
%ASA-6-305011: Built dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025
%ASA-6-302013: Built outbound TCP connection 90 for outside:172.22.1.1/80
(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
%ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

  Сообщения системного журнала указывают на то, что подключение было закрыто из-за тайм-аута синхронизации (SYN). Это говорит администратору о том, что ответы сервера приложения X не были получены ASA. Окончания сообщения системного журнала могут изменяться. См. раздел ASA Системные сообщения для получения дополнительных сведений о сообщениях системного журнала.

- **Создайте новый фильтр захвата.**

  Из ранее захваченного трафика и сообщений системного журнала администратор знает, что приложение X должно покидать ASA через внешний интерфейс.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
     !--- When you leave the source as 'any', it allows
!--- the administrator to monitor any network address translation (NAT).

ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any
     !--- When you reverse the source and destination information,
!--- it allows return traffic to be captured.

ciscoasa(config)#capture outside_interface access-list outside_test interface outside
```

  Пользователю необходимо запустить новый сеанс при помощи приложения X. После того, как пользователь начнет новый сеанс приложения X, администратору ASA необходимо выполнить команду **show capture outside_interface** на ASA.

```
ciscoasa(config)#show capture outside_interface
3 packets captured
  1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80:
S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK>
  2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
  3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
3 packets shown
```

  Данная команда покажет трафик, покидающий внешний интерфейс, но не покажет ответный трафик от сервера 172.22.1.1. Данный захват отображает данные, которые покидают ASA.

- **Используйте параметр packet-tracer.**

  Из предыдущих разделов администратор ASA узнал достаточно, чтобы воспользоваться в ASA параметром **packet-tracer.**

  Примечание: ASA поддерживает команду **packet-tracer** начиная с версии 7.2.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
     !--- This line indicates a source port of 1025. If the source
!--- port is not known, any number can be used.
!--- More common source ports typically range
!--- between 1025 and 65535.

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

Phase: 4
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   172.22.1.0      255.255.255.0   outside

Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

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

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
 match ip inside 192.168.1.0 255.255.255.0 outside any
   dynamic translation to pool 1 (172.22.1.254)
   translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
```

```
 match ip inside 192.168.1.0 255.255.255.0 outside any
   dynamic translation to pool 1 (172.22.1.254)
   translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 94, packet dispatched to next module

Phase: 15
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.1 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 11
!--- The MAC address is at Layer 2 of the OSI model.
!--- This tells the administrator the next host
!--- that should receive the data packet.


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

Наиболее важными выходными данными команды **packet-tracer** является последняя строка `Action: allow`.

Три параметра на Шаге 3 показывают администратору, что ASA не является причиной проблем с приложением X. Трафик приложения X покидает ASA и ASA не получает ответ от сервера приложения X.

Что дальше?

Существует множество компонентов, которые обеспечивают нормальную работу приложения X. Эти компоненты включают пользовательский компьютер, клиент приложения X, политики маршрутизации и доступа и сервер приложения X. В предыдущем примере мы доказали, что ASA принимает и пересылает трафик приложения X. Теперь проблему следует передать администраторам сервера и приложения X. Администраторы должны проверить, что службы приложения работают, просмотреть все журналы на сервере и проверить, что трафик пользователя, получается сервером и приложением X.

Дополнительные сведения

- **Справочник по командам Cisco ASA**
- **Справочник по командам Cisco PIX**
- **Сообщения об ошибках и системные сообщения Cisco ASA**
- **Сообщения об ошибках и системные сообщения Cisco PIX**
- **Поддержка Cisco ASA 5500 Series Adaptive Security Appliances**
- **Поддержка Cisco PIX 500 Series Security Appliances**
- **Техническая поддержка и документация Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/105409/asa-pix-troubleshooting.shtml

---