Устранение неполадок в подключениях через PIX и ASA

Содержание

Введение

В этом документе описаны возможные способы и приведены советы по устранению неисправностей при использовании устройства адаптивной защиты Cisco ASA серии 5500 (ASA) и устройства защиты Cisco PIX серии 500. Как правило, когда приложения или

источники сети ломаются или не доступны, межсетевые экраны (PIX или ASA) имеют тенденцию быть основной целью и обвиненный как причина простоев. С некоторым тестированием на ASA или PIX, администратор может определить, причиняет ли ASA/PIX проблему.

См. PIX/ASA: Установите и Подключение Устранения неполадок через Cisco Security Appliance для узнавания больше об отнесенном устранении проблем интерфейса на устройствах Безопасности Cisco.

Примечание: Этот документ фокусируется на ASA и PIX. Как только устранение проблем завершено на ASA или PIX, вероятно, что дополнительное устранение проблем могло бы быть необходимым с другими устройствами (маршрутизаторы, коммутаторы, серверы, и т.д).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco ASA 5510 с ОС 7.2.1 и 8.3.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Данный документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- ASA и PIX OS 7.0, 7.1, 8.3, и позже
- Модуль сервисов межсетевого экрана (FWSM) 2.2, 2.3, и 3.1

Примечание: Определенные команды и синтаксис могут варьироваться между версиями программного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Пример принимает ASA, или PIX работает. Конфигурация ASA/PIX может быть относительно простой (только 50 линий конфигурации) или комплекс (сотни к тысячам строк настройки). Пользователи (клиенты) или серверы могут или быть в защищенной сети

(внутри) или небезопасной сети (DMZ или снаружи).

ASA запускается с этой конфигурации. Конфигурация предназначена, чтобы дать лабораторной работе контрольную точку.

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 !-
-- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
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 связывается с отделом ИТ и сообщает, что больше не работает приложение X. Инцидент возрастает администратору ASA/PIX. У администратора есть мало знания этого конкретного приложения. С использованием ASA/PIX администратор обнаруживает то,

что использует приложение X портов и протоколов, а также что могло бы быть причиной проблемы.

Решение

Администратор ASA/PIX должен собрать как можно больше информации от пользователя. Полезные сведения включают:

- IP - адрес источника — Это, как правило, - рабочая станция или компьютер пользователя.
- IP - адрес назначения — IP-адрес сервера, который пользователь или приложение пытаются подключить.
- Порты и протоколы использование приложения

Часто администратору повезло, если способный получить ответ на один из этих вопросов. Для данного примера администратор не в состоянии собрать любую информацию. Анализ сообщений системного журнала ASA/PIX идеален, но трудно определить местоположение проблемы, если администратор не знает, что искать.

Шаг 1 - обнаруживает IP-адрес пользователя

Существует много способов обнаружить IP-адрес пользователя. Этот документ о ASA и PIX, таким образом, данный пример использует ASA и PIX для обнаружения IP-адреса.

Пользователь пытается связаться с ASA/PIX. Эта связь может быть ICMP, Telnet, SSH или HTTP. Выбранный протокол должен был ограничить действие на ASA/PIX. В этом определенном примере пользователь пропинговывает внутренний интерфейс ASA.

Администратор должен установить один или больше этих опций и затем сделать, чтобы пользователь пропинговал внутренний интерфейс ASA.

- **Системный журнал**Удостоверьтесь регистрировав, включен. Уровень регистрации должен собираться **отладить**. Регистрация может быть передана различным местоположениям. Данный пример использует буфер журнала ASA. Вам, возможно, понадобился бы внешний сервер регистрации в производственных средах.`ciscoasa(config)#`**`logging enable`** `ciscoasa(config)#`**`logging buffered debugging`** Пользователь пропинговывает внутренний интерфейс ASA (пропингуйте 192.168.1.1). Эти выходные данные отображены.`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 перехвата ASA**Администратор должен создать access-list, который определяет, какой трафик ASA должен перехватить. После того, как access-list определен, команда **перехвата** включает access-list 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 пропинговывает внутренний интерфейс ASA (пропингуйте 192.168.1.1). Эти выходные данные отображены.`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 перехвата файла к системе такой как эфирного, можно сделать это как показано в выходных данных ниже.

```
!--- Open an Internet Explorer and browse with this https link format:
https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap
```
В документе ASA/PIX: Пакетное Получение с помощью CLI и Примера конфигурации ASDM для знания больше о Пакетном Получении в ASA.

- **.debug**Команда **debug icmp trace** используется для получения трафика ICMP пользователя.`ciscoasa#debug icmp trace` Пользователь пропинговывает внутренний интерфейс ASA (пропингуйте 192.168.1.1). Эти выходные данные отображены на консоли.`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**отрассировка icmp неотладкиundebug all, **Undebug all** или **ООН все**

Каждая из этих трех опций помогает администратору определять IP - адрес источника. В данном примере IP - адрес источника пользователя 192.168.1.50. Администратор готов узнать больше о приложении X и определить причину проблемы.

Шаг 2 - определяет местоположение причины проблемы

В отношении информации, перечисленной в разделе Шага 1 этого документа, администратор теперь знает источник сеанса приложения X. Администратор готов узнать больше о приложении X и начать располагаться, где проблемы могли бы быть.

Администратор ASA/PIX должен подготовить ASA к по крайней мере одному из этих перечисленных предложений. Как только администратор готов, пользователь инициирует приложение X и ограничивает все другое действие, так как дополнительное пользовательское действие могло бы вызвать беспорядок или ввести в заблуждение администратора ASA/PIX.

- **Сообщения системного журнала монитора.**Ищите IP - адрес источника пользователя, которого вы определили местоположение в Шаге 1. Пользователь инициирует 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)` Журналы показывают, что IP - адрес назначения 172.22.1.1, протокол является TCP, порт назначения является HTTP/80, и что трафик передается внешнему интерфейсу.
- **Модифицируйте фильтры перехвата.Команда access-list inside_test** ранее использовалась 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 инициирует приложение X. Администратор ASA тогда 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>` Перехваченный трафик предоставляет администратору несколько частей полезной информации:Адрес назначения (DA) — 172.22.1.1Номер порта — 80/httpПротокол — TCP (замечают "S" или флаг syn),Кроме того, администратор также знает, что трафик данных для приложения X действительно поступает в ASA.Если выходные данные были этими выходными данными **команды show capture inside_interface**, то трафик приложения или никогда не достигал, ASA или фильтр перехвата были "not set" для получения трафика:`ciscoasa#`**`show capture inside_interface`** `0 packet captured 0 packet shown` В этом случае администратор должен рассмотреть исследование компьютера пользователя и любого маршрутизатора или других сетевых устройств в пути между компьютером пользователей и ASA.**Примечание:** Когда трафик поступает в интерфейс, команда **перехвата** делает запись данных, прежде чем любая политика безопасности ASA проанализирует трафик. Например, access-list запрещает весь входящий трафик на интерфейсе. Команда **перехвата** все еще делает запись трафика. Политика безопасности ASA тогда анализирует трафик.

- **.debug**Администратор не знаком с приложением X и поэтому не знает который из сервисов отладки включать для расследования приложения X. Отладка не могла бы быть лучшей опцией устранения проблем на этом этапе.

С собранными сведениями в Шаге 2 администратор ASA получает несколько битов полезной информации. Администратор знает, что трафик поступает во внутренний интерфейс ASA, IP - адрес источника, IP - адрес назначения и сервисное приложение X используют (TCP/80). От системных журналов администратор также знает, что была первоначально разрешена связь.

Шаг 3 - подтверждает и контролирует трафик приложения

Администратор ASA хочет подтвердить, что трафик приложения X оставил ASA, а также контролирует любой ответный трафик из приложения X-сервер.

- **Сообщения системного журнала монитора.**Сообщения системного журнала фильтра для IP - адреса источника (192.168.1.50) или IP - адреса назначения (172.22.1.1). Из командной строки фильтрующие сообщения системного журнала похожи**, что show logging | включает 192.168.1.50**, или **show logging | включают 172.22.1.1**. В данном примере **команда show logging** используется без фильтров. Выходные данные подавлены для создания чтения легким.`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` Сообщение системного журнала указывает на соединение, закрытое потому что времени ожидания SYN. Это говорит администратору, что никакое заявление ответы X-сервера не было получено ASA. Причины завершения сообщения системного журнала могут варьироваться.Время ожидания SYN зарегистрировано из-за принудительного завершения подключения после 30 секунд, которое происходит после завершения трехэтапного установления связи. Если сервер не в состоянии отвечать на запрос подключения, и, в большинстве

случаев, не отнесен к конфигурации на PIX/ASA, эта проблема обычно происходит.Для решения этого вопроса обратитесь к этому чек-листу:Удостоверьтесь, что статическая команда введена правильно и что она не накладывается на другие статические команды, например,`static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255` Статическое NAT в ASA 8.3 и позже может быть настроено как показано здесь:`object network obj-y.y.y.y`
` host y.y.y.y`
` nat (inside,outside) static x.x.x.x`Удостоверьтесь, что список доступа существует для разрешения доступа к глобальному IP-адресу с внешней стороны и что это связано с интерфейсом:

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

Для успешного подключения с сервером шлюз по умолчанию на сервере должен указать к интерфейсу DMZ PIX/ASA.См. Системные сообщения ASA для получения дополнительной информации о сообщениях системного журнала.

- **Создайте новый фильтр перехвата.**От более раннего перехваченного трафика и сообщений системного журнала, администратор знает, что приложение X должно оставить 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`**
Пользователь должен инициировать новый сеанс с приложением X. После того, как пользователь инициировал новое приложение X сеансов, администратор ASA должен 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` Перехват показывает трафик, оставляя внешний интерфейс, но не показывает трафика ответа от 172.22.1.1 серверов. Этот перехват показывает данные, поскольку это оставляет ASA.
- **Используйте опцию packet-tracer.**От предыдущих разделов администратор ASA изучил достаточно информации для использования **опции packet-tracer** в ASA.**Примечание:** ASA поддерживает **команду packet-tracer**, запускающуюся в 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
```

Самые важные выходные данные **команды packet-tracer** являются последней линией, которая является `Action: allow`.

Эти три опции в Шаге 3, каждый показывает администратору, что ASA не ответственен за проблемы приложения X. Трафик приложения X оставляет ASA, и ASA не получает ответ от приложения X-сервер.

Что является Следующим?

Существует много компонентов, которые позволяют приложению X работать правильно для пользователей. Компоненты включают компьютер пользователя, приложение X-клиент, маршрутизация, политика доступа и приложение X-сервер. В предыдущем примере мы доказали, что ASA получает и передает трафик приложения X. Сервер и администраторы приложения X должны теперь принять участие. Администраторы должны проверить, что сервисы приложения выполняют, рассматривают любой вход в систему сервера и проверяют, что трафик пользователя получен сервером и приложением X.

Проблема: Завершение сообщения об ошибках прокси - подключения TCP

Отображается следующее сообщение об ошибке:

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

Решение

Пояснение: Это индикаторы сообщения, когда предел буфера сборки превышен во время сборки сегментов TCP.

- *source_address/source_port* - IP - адрес источника и исходный порт пакета, инициирующего соединение.
- *dest_address/dest_port* - IP - адрес назначения и порт назначения пакета, инициирующего соединение.
- *interface_inside* - Название интерфейса, в который поступает пакет, который инициировал соединение.
- *interface_outside* - Название то, интерфейса, на который пакет, который инициировал выходы соединения.
- *предел* - настроенный предел неустановившегося соединения для класса трафика.

Разрешение для этой проблемы должно отключить контроль RTSP в устройстве безопасности как показано.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

См. идентификатор ошибки Cisco CSCsl15229 (только зарегистрированные клиенты) для получения дополнительной информации.

Проблема: "%ASA-6-110003: Маршрутизация была не в состоянии определять местоположение следующего перехода для протокола из Сообщения об ошибках" интерфейса src

ASA отбрасывает трафик с сообщением об ошибках `error:%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port.`

Решение

Когда ASA пытается найти следующий переход на интерфейсной таблице маршрутизации, эта ошибка происходит. Когда ASA создали трансляцию (xlate) к одному интерфейсу и маршруту, указывающему на другой интерфейс, Как правило, это сообщение получено. Проверьте для неверной конфигурации на Выражениях NAT. Разрешение неверной конфигурации может решить ошибку.

Проблема: Соединение, Заблокированное ASA с "%ASA-5-305013: Асимметричные правила NAT совпали для форварда и обратных потоков" с Сообщением об ошибках

Соединение заблокировано ASA, и это сообщение об ошибках получено:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

Решение

Когда NAT выполнен, ASA также пытается инвертировать пакет и проверки, если это поражает какую-либо трансляцию. Если это не поражает никого или другое преобразование NAT, то существует несоответствие. Когда существуют другие правила NAT, настроенные для исходящего и входящего трафика с тем же источником и назначением, вы обычно видите это сообщение об ошибках. Проверьте Выражение NAT для заинтересованного трафика.

Проблема: Получите ошибку - %ASA-5-321001: Ресурс 'ведет'

предел 10000 достигнутых для системы

Решение

Эта ошибка показывает, что соединения для сервера, расположенного через ASA, достигли своего ограничения максимального значения. Это могло быть индикацией относительно атаки DoS к серверу в вашей сети. Используйте MPF на ASA и уменьшите предел неустановившихся соединений. Кроме того, включите Мертвое обнаружение соединения (DCD). См. этот фрагмент конфигурации:

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

Проблема: Получите ошибку %PIX-1-106021: Запретите проверку обратного пути TCP/UDP от src_addr до dest_addr на интерфейсе int_name

Решение

Когда проверка обратного пути включена, это сообщение журнала получено. Выполните эту команду, чтобы решить проблему и отключить проверку обратного пути:

no ip verify reverse-path interface *<interface name>*

Проблема: Прерывание интернет-соединения из-за Обнаружения Угрозы

Это сообщение об ошибках получено на ASA:

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

Решение

Когда аномальное Поведение трафика обнаружено, это сообщение генерируется обнаружением угрозы из-за конфигурации по умолчанию. Сообщение фокусируется на Miralix Licen 3000, который является портом TCP/UDP. Найдите устройство, которое использует порт 3000. Проверьте ASDM графическая статистика для обнаружения угрозы и проверьте главные атаки, чтобы видеть, показывает ли это порт 3000 и IP - адрес источника. Если это - легитимное устройство, можно инкрементно увеличить скорость базового обнаружения угроз на ASA для решения этого сообщения об ошибках.

Дополнительные сведения

- Справочник по командам Cisco ASA
- Справочник по командам Cisco PIX
- Ошибки и системные сообщения Cisco ASA
- Ошибки и системные сообщения PIX Cisco
- Поддержка устройств адаптивной защиты Cisco ASA серии 5500
- Поддержка Cisco PIX 500 Series Security Appliances
- Cisco Systems – техническая поддержка и документация