Конфигурация NAT ASA и рекомендации для реализации интерфейсов сдвоенной сети скоростной-автомагистрали-E и скоростной-автомагистрали-C.

Содержание

Введение

Этот документ описывает, как внедрить конфигурацию Технологии NAT, требуемую в устройстве адаптивной защиты Cisco (ASA) для Контроллера интерфейса Интерфейсов/Сдвоенной сети Сдвоенной сети Скоростной-автомагистрали-E и Скоростной-

автомагистрали-C (NIC) реализация.

Это развертывания являются рекомендуемой опцией для реализации Скоростной-автомагистрали-E и устройств Скоростной-автомагистрали-C вместо того, чтобы использовать отражение NAT.

Внесенный Кристианом Эрнандесом и Сесаром Лопесом Самаррипой, специалистами службы технической поддержки Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco ASA основной NAT и конфигурация
- Скоростная-автомагистраль-E Cisco и базовая конфигурация Скоростной-автомагистрали-C

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройства Cisco ASA 5500 и 5500-X Series, которые работают под управлением ПО версии 8.0 и позже.
- Версия 8.x Скоростной автомагистрали Cisco и позже.

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.

> **Примечание:** Через весь документ устройства Скоростной автомагистрали отнесены как Скоростная-автомагистраль-E и Скоростная-автомагистраль-C. Однако одинаковая конфигурация применяется к Скоростной автомагистрали сервера Video Communication Server (VCS) и Устройствам управления VCS.

Общие сведения

Дизайном Скоростная-автомагистраль-E Cisco может быть размещена или в Демилитаризованную зону (DMZ) или в Открытую сеть направления (Интернет), и это в состоянии со Скоростной-автомагистралью-C Cisco в Частной сети. Однако, когда Скоростная-автомагистраль-E Cisco помещена в DMZ, это дополнительные преимущества.

- В наиболее распространенном сценарии Скоростной-автомагистралью-E Cisco управляют от Частной сети. Путем размещения Скоростной-автомагистрали-E Cisco в DMZ permietral (внешний) межсетевой экран может использоваться для блокирования

нежелательного доступа к Скоростной автомагистрали такой как (Безопасный Протокол передачи гипертекстовых файлов) запросы Secure Shell (SSH) или HTTPS.

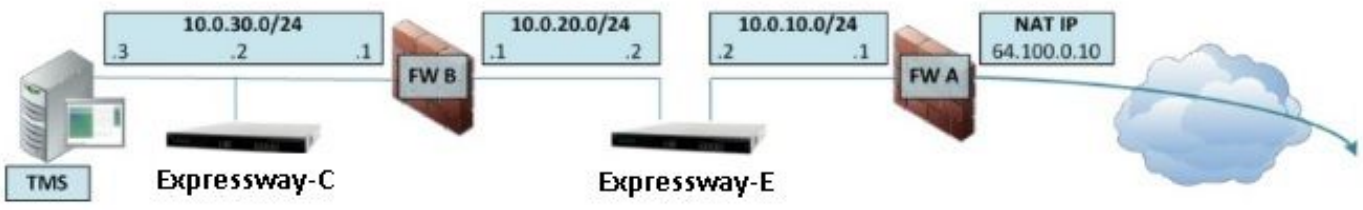
- Если DMZ не разрешает, чтобы прямые подключения между внутренним и внешними сетями, выделенные серверы потребовались, чтобы обрабатывать трафик, который пересекает DMZ. Скоростная автомагистраль Cisco может действовать как тот сервер для Протокола SIP и/или голоса H.323 и видеотрафика. В этом случае можно использовать опцию Dual Network Interfaces, которая позволяет Скоростной автомагистрали Cisco иметь два других IP-адреса, один для к/ота трафика внешний межсетевой экран, и один для к/ота трафика внутренний межсетевой экран.

- Эта настройка предотвращает внешнюю связь для соединения непосредственно с внутренней сетью. Это улучшает безопасность внутренней сети в целом.

Совет: Для получения большего количества подробных данных о реализации TelePresence обратитесь к Скоростной-автомагистрали-E Cisco и Скоростной-автомагистрали-C - Руководство по развертыванию Базовой конфигурации и Размещение Скоростной автомагистрали VCS Cisco в DMZ, а не в общем Интернете.

Скоростная автомагистраль C и E - Сдвоенная сеть реализация Интерфейсов/сдвоенного NIC

Эта схема показывает пример развертывания для Скоростной-автомагистрали-E с интерфейсами сдвоенной сети и статический NAT. Скоростная-автомагистраль-C, действующая как пересекающийся клиент и два межсетевых экрана (FW A и FWB). Как правило, в этой конфигурации DMZ, FW A не может направить трафик к FW B, и устройства, такие как Скоростная-автомагистраль-E сдвоенного интерфейса требуются, чтобы проверять и передавать трафик от подсети A FW до подсети B FW (и наоборот).



Эти развертывания состоят из этих компонентов.

Подсеть DMZ 1 – 10.0.10.0/24

- FW внутренний интерфейс – 10.0.10.1
- Интерфейс LAN2 скоростной-автомагистрали-E – 10.0.10.2

Подсеть DMZ 2 – 10.0.20.0/24

- FW B внешний интерфейс – 10.0.20.1
- Интерфейс LAN1 скоростной-автомагистрали-E – 10.0.20.2

Подсеть LAN – 10.0.30.0/24

- FW B внутренний интерфейс – 10.0.30.1

- Интерфейс LAN1 скоростной-автомагистрали-C – 10.0.30.2
- Система управления Cisco TelePresence (TMS) Серверный сетевая интерфейс – 10.0.30.3

- FW A является внешним или permitetral межсетевым экраном; это настроено с IP NAT (общий IP) 64.100.0.10, который статически преобразован в 10.0.10.2 (Интерфейс LAN2 Скоростной-автомагистрали-E)

- FW B является внутренним межсетевым экраном

- LAN1 скоростной-автомагистрали-E отключили статический NAT режим

- LAN2 скоростной-автомагистрали-E включили статический NAT режим со Статическим NAT адресом 64.100.0.10

- Скоростная-автомагистраль-C имеет пересекающуюся клиентскую зону, которая указывает к 10.0.20.2 (Интерфейс LAN1 Скоростной-автомагистрали-E)

- Нет никакой маршрутизации между 10.0.20.0/24 и 10.0.10.0/24 подсетями. Скоростная-автомагистраль-E соединяет эти подсети и действия как прокси для сигнализации SIP/H.323 и Протокола RTP / Протокол управления RTP (RTCP) среды.

- TMS Cisco настроили Скоростную-автомагистраль-E с IP-адресом 10.0.20.2

Требования/Ограничения

Неперекрывающиеся подсети

Если Скоростная-автомагистраль-E настроена для использования обоих интерфейсов LAN (локальной сети), LAN1 и интерфейсы LAN2 должны быть расположены в неперекрывающихся подсетях, чтобы гарантировать, что трафик отослан в корректный интерфейс.

Кластеризация

Когда кластеризующим устройствам Скоростной автомагистрали настроили **Усовершенствованный Сетевой параметр**, для каждого узла кластера нужен его собственный адрес интерфейса LAN1. Кроме того, объединение в кластеры должно быть настроено на интерфейсе, которому не включили Статический NAT режим. Поэтому рекомендуется использовать LAN2 в качестве внешнего интерфейса, и LAN2 используется в качестве статического NAT интерфейса когда это применимо.

Внешние параметры настройки интерфейса LAN (локальной сети)

Внешние параметры конфигурации интерфейса LAN (локальной сети) на контроле за страницей IP - конфигурации, какой сетевой интерфейс использует Трансверсальное Использование Реле вокруг NAT (TURN). В конфигурации Скоростной-автомагистрали-E интерфейса сдвоенной сети это может обычно устанавливаться в Скоростную-автомагистраль-E внешний интерфейс LAN (локальной сети).

Статические маршруты

Скоростная-автомагистраль-E должна быть настроена с адресом шлюза по умолчанию 10.0.10.1 для этого сценария. Это означает, что весь трафик, отосланный через LAN2, по умолчанию, передается IP-адресу 10.0.10.1.

Если FW B преобразовывает трафик, передаваемый с 10.0.30.0/24 подсети на интерфейс LAN1 Скоростной-автомагистрали-E (например, трафик клиента обхода Скоростной-автомагистрали-C или трафик управления сервером TMS), этот трафик появляется, как это прибывает из внешнего интерфейса FWB (10.0.20.1), поскольку это достигает LAN1 Скоростной-автомагистрали-E. Скоростная-автомагистраль-E тогда в состоянии ответить на этот трафик через его интерфейс LAN1, так как очевидный источник того трафика расположен в той же подсети.

Если FW B не делает NAT, трафик, передаваемый от Скоростной-автомагистрали-C до LAN1 Скоростной-автомагистрали-E, показывает , как это прибывает от 10.0.30.2. Если Скоростной автомагистрали не добавили статический маршрут для 10.0.30.0/24 подсети, она передает ответы за этим трафиком к его шлюзу по умолчанию (10.0.10.1) из LAN2, поскольку это не знает, что 10.0.30.0/24 подсеть расположена позади внутреннего межсетевого экрана (FW B). Поэтому статический маршрут должен быть добавлен, с помощью **команды CLI xCommand RouteAdd** через Сеанс SSH к Скоростной автомагистрали.

В этом конкретном примере Скоростная-автомагистраль-E должна знать, что это может достигнуть 10.0.30.0/24 подсети позади FW B, который достижим через интерфейс LAN1. Это выполнено с помощью этой команды.

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **Примечание:** Конфигурирование статических маршрутов может быть применено через Графический пользовательский интерфейс (GUI) Скоростной-автомагистрали-E в **Системе/Сети** раздела**> Интерфейсы/Статические маршруты.**

> **Примечание:** Рекомендуется избежать использования NAT в FW-B для Скоростной-автомагистрали-C. Это позволяет Скоростной-автомагистрали-E достигать Скоростной-автомагистрали-C со своим реальным IP - адресом 10.0.30.2. Это избегает определенных проблем телефонных служб. Было подтверждено, что конфигурация NAT для Скоростной-автомагистрали-C может заставить Мобильный и Удаленный доступ (MRA) устройства не подходить.

В данном примере Интерфейсный параметр может также быть установлен на **Автоматический**, поскольку адрес шлюза (10.0.20.1) только достижим через LAN1.

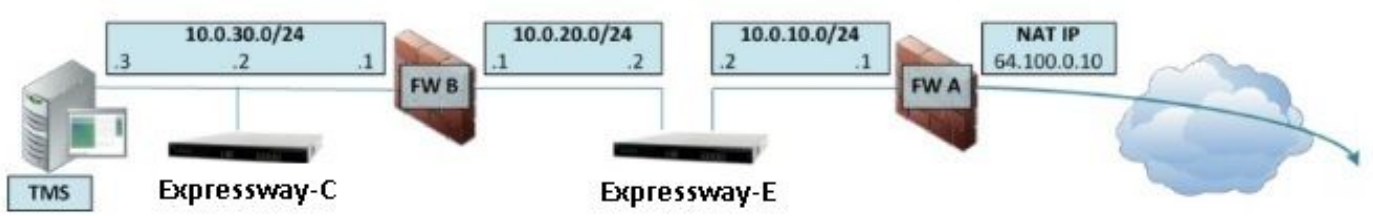
Если FW B не делает NAT, и Скоростная-автомагистраль-E должна связаться с устройствами в подсетях кроме 10.0.30.0/24, которые также расположены позади FW B, такого как SSH и Подключения HTTPS от этого сетевые рабочие станции или для сетевых сервисов как NTP, DNS, LDAP/AD и/или Sylog, статические маршруты должны быть добавлены для этих устройств/подсетей.

Команда xCommand RouteAdd и синтаксис описаны в во всей подробности в *Руководстве администратора VCS.*

!--- конфигурацию

В этом разделе описывается настроить статическое NAT, требуемое для реализации интерфейсов/сдвоенного NIC сдвоенной сети Скоростной-автомагистрали-C и Скоростной-автомагистрали-E на ASA. Кроме того, некоторые рекомендации по конфигурации Модульной системы политик (MPF) ASA для обработки трафика SIP/H323 через ASA.

Скоростная автомагистраль C и E - Сдвоенная сеть реализация Интерфейсов/сдвоенного NIC



В данном примере присвоение IP-адреса следующие.

IP скоростной-автомагистрали-C address:10.0.30.2/24

Default-gateway скоростной-автомагистрали-C: 10.0.30.1 (FW-B)

IP-адреса скоростной-автомагистрали-E

На LAN2: 10.0.10.2/24

На LAN1: 10.0.20.2/24

Default-gateway скоростной-автомагистрали-E: 10.0.10.1 (FW-A)

IP-адрес TMS: 10.0.30.3/24

Конфигурация FW-A:

Шаг 1. Статическая конфигурация NAT для Скоростной-автомагистрали-E

Как объяснено **в фоновом режиме Раздел сведений** этого документа, FW-A имеет статическое преобразование NAT, чтобы позволить Скоростной-автомагистрали-E быть достижимой из Интернета с помощью открытого IP - адреса 64.100.0.10. Этот последний преобразован посредством NAT к IP-адресу LAN2 Скоростной-автомагистрали-E 10.0.10.2/24, это сказанное, это - требуемая статическая конфигурация NAT FW-A.

Для Версий ASA 8.3 и позже:

```
! To use PAT with specific ports range: object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
```

```
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR ! To use with static one-to-one NAT: object network obj-10.0.10.2 nat
(inside,outside) static interface
```

> **Примечание:** Если при попытке применить статические PAT команды вы получаете сообщение об ошибках **'ОШИБКА: NAT, неспособный резервировать порты** на интерфейсе командной строки ASA, тогда, очищает записи xlate с **командой clear xlate локальный x. x. x. x** , где x. x. x. x соответствует внешнему IP - адресу ASA. Эта команда очищает все трансляции, привязанные к этому IP так в производственных средах, выполните его с осторожностью.

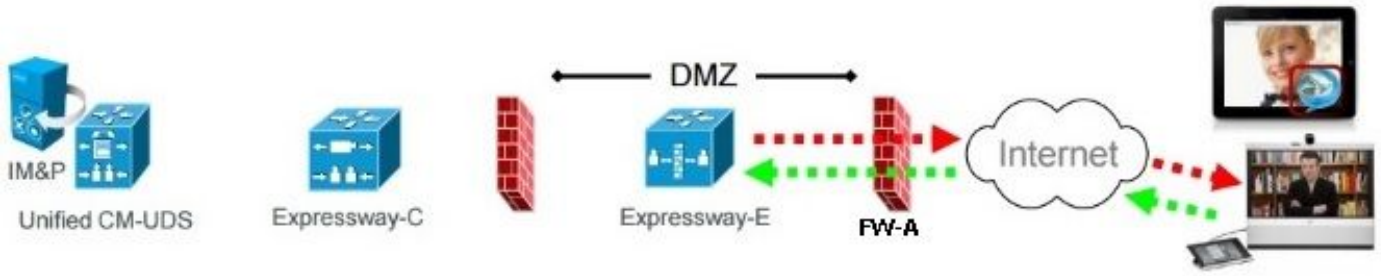
Для Версий ASA 8.2 и ранее:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used. static (inside,outside) interface
10.0.10.2 netmask 255.255.255.255
```

Шаг 2. Конфигурация Списка контроля доступа (ACL) для разрешения портов, требуемых от Интернета до Скоростной-автомагистрали-E

Согласно *Объединенным коммуникациям: Скоростная автомагистраль (DMZ) к общей интернет-* документации, это - список TCP и портов UDP, которых Скоростная-автомагистраль-E требует, чтобы быть позволенной в FW-A:

Unified Communications: Expressway (DMZ) to public internet



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999 **	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999 **	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

Это - конфигурация списков управления доступом (ACL), требуемая как входящая в FW внешний интерфейс.

Для Версий ASA 8.3 и позже.

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

Для Версий ASA 8.2 и ранее.

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061
```

```
access-group outside-in in interface outside
```

> **Примечание:** Это настоятельно рекомендовано для отключения SIP и Проверок H.323 на сетевом трафике переноса межсетевого экрана к или от Скоростной-автомагистрали-E, как тогда, когда включено, это, как часто находят, негативно влияет на функциональность обхода/NAT встроенного межсетевого экрана Скоростной-автомагистрали-E.

Конфигурация FW-B.

Как объяснено в фоновом режиме **Раздел сведений** этого документа, FW B просто требует, чтобы динамический NAT или конфигурация PAT позволили внутренней подсети 10.0.30.0/24 быть преобразованной в IP-адрес 10.0.20.1 когда выходящий во внешний интерфейс FW B.

Для Версий ASA 8.3 и позже.

```
object network obj-10.0.30.0
   subnet 10.0.30.0 255.255.255.0
   nat (inside,outside) dynamic interface
```

Для Версий ASA 8.2 и ранее.

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

> **Примечание:** Это настоятельно рекомендовано для отключения SIP и Проверок H.323 на сетевом трафике переноса межсетевого экрана к или от Скоростной-автомагистрали-E, как, когда включено это, как часто находят, негативно влияет на функциональность обхода/NAT встроенного межсетевого экрана Скоростной-автомагистрали-E.

> **Совет:** Убедитесь, что весь требуемый TCP и порты UDP для Скоростной-автомагистрали-C для работы должным образом открыт в FW B, столь же заданный в этом Документе Cisco: Использование портов IP Скоростной автомагистрали Cisco для прохождения Межсетевого экрана

Проверка

Пакетный Трассировщик может использоваться на ASA, чтобы подтвердить, что статическое преобразование NAT Скоростной-автомагистрали-E работает как требуется.

Пакетный Трассировщик для тестирования 64.100.0.10 в TCP/5222.

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
```

```
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 13, packet dispatched to next module

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

Пакетный Трассировщик для тестирования 64.100.0.10 в TCP/8443.

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
```

```
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 14, packet dispatched to next module

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

Пакетный Трассировщик для тестирования 64.100.0.10 в TCP/5061.

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
```

```
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 15, packet dispatched to next module

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

Пакетный Трассировщик для тестирования 64.100.0.10 в UDP/24000:

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
```

```
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 16, packet dispatched to next module

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

Пакетный Трассировщик для тестирования 64.100.0.10 в UDP/36002.

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
```

```
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 17, packet dispatched to next module

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

Устранение неполадок

Шаг 1. Захваты пакетов.

Захваты пакета могут быть взяты и во входе ASA и в исходящих интерфейсах

```
FW-A# sh cap
capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

Захваты пакета для 64.100.0.10 в TCP/5222:

```
FW-A# sh cap capout

2 packets captured
   1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
   2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown

FW-A# sh cap capin

2 packets captured
   1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
   2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

Захваты пакета для 64.100.0.10 в TCP/5061:

```
FW-A# sh cap capout
2 packets captured

   1: 21:42:14.920576 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
   2: 21:42:16.992380 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
2 packets shown
FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

Шаг 2. Захваты пакета отбрасывания Ускоренного пути безопасности (ASP).

Перехваты отбрасывания ASP ASA берут пакеты, которые ASA решил отбросить. Опция **все** перехваты все возможные причины, почему ASA отбросил пакет. Если существует какая-либо причина supected, это может быть сужено. Для списка причин использование ASA для классификации это понижается, **команда show asp drop** может использоваться.

Буфер по умолчанию для каждого перехвата ASA составляет 512 КБ. Если будет много пакетов, отбрасываемых этим ASA, то этот буфер будет заполнен очень быстро. Этот буфер может быть инкрементно увеличен с помощью **буфера** опции.

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

> **Совет:** Этот перехват ASP ASA очень полезен в этом сценарии, чтобы подтвердить, отбрасывает ли ASA пакеты из-за недостающего ACL или NAT для открытия определенного TCP или порта UDP для Скоростной-автомагистрали-E.

Рекомендации

Гарантируйте, что проверки SIP/H.323 полностью отключены во включенных межсетевых экранах

Это настоятельно рекомендовано для отключения SIP и проверок H.323 на межсетевых экранах, которые обрабатывают сетевой трафик к или от Скоростной-автомагистрали-E, как, когда включено это, как часто находят, негативно влияет на функциональность обхода/NAT встроенного межсетевого экрана Скоростной автомагистрали.

Это - пример того, как отключить SIP и проверки H.323 на ASA.

```
policy-map global_policy
 class inspection_default
  no inspect h323 h225
  no inspect h323 ras
  no inspect sip
```

Альтернативное решение

Альтернативное решение вместо того, чтобы внедрить Скоростную-автомагистраль-E с помощью интерфейсов/сдвоенного NIC сдвоенной сети, должно внедрить Скоростную-автомагистраль-E с помощью конфигурации отражения NAT в межсетевых экранах, эта ссылка показывает более подробную информацию об этом сценарии.

ASA: конфигурация отражения NAT для реализаций скоростной автомагистрали VCS.

Однако как это было упомянуто в начале этого документа, настройка Сдвоенной сети рекомендуется по отражению NAT.

Ссылки по теме

Скоростная-автомагистраль-E Cisco и скоростная-автомагистраль-C - Руководство по развертыванию базовой конфигурации

Размещение Скоростной автомагистрали VCS Cisco в DMZ, а не в общем Интернете

Использование портов IP скоростной автомагистрали Cisco для прохождения межсетевого экрана