Настройте отражение NAT o ASA для устройств TelePresence скоростной автомагистрали VCS

Содержание

Введение

Этот документ описывает, как внедрить конфигурацию отражения Технологии NAT на устройствах адаптивной защиты Cisco для специальных сценариев Cisco TelePresence ,

которые требуют этого вида конфигурации NAT на Межсетевом экране.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco ASA (Устройство адаптивной безопасности) основная конфигурация NAT
- Контроль за сервером Video Communication Server (VCS) Cisco TelePresence и базовая конфигурация Скоростной автомагистрали VCS

Примечание: Этот документ предназначен, чтобы использоваться только, когда не может использоваться метод рекомендуемого развертывания Скоростной автомагистрали VCS или Края скоростной автомагистрали с обоими интерфейсами NIC в другом DMZ. Для получения дополнительной информации на рекомендуемом развертывании с помощью двойных NIC проверьте следующую ссылку в странице 60: Базовая конфигурация Сервера Передачи видеоданных Cisco TelePresence (Контроль со Скоростной автомагистралью) Руководство по развертыванию

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 8.3 и позже.
- Версия X8.x VCS 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 VCS отнесены как Скоростная автомагистраль VCS и Контроль за VCS. Однако одинаковая конфигурация применяется к устройствам Скоростной-автомагистрали-E и Скоростной-автомагистрали-C.

Общие сведения

Согласно документации Cisco TelePresence, существует два вида сценариев TelePresence, где конфигурация отражения NAT требуется на FW, чтобы позволить Контролю за VCS связываться со Скоростной автомагистралью VCS через открытый IP - адрес Скоростной автомагистрали VCS.

Первый сценарий включает De-Militarized Zone (DMZ) одиночной подсети, который использует одиночный интерфейс LAN (локальной сети) Скоростной автомагистрали VCS, и второй сценарий включает DMZ FW с 3 портами, который использует одиночный интерфейс

LAN (локальной сети) Скоростной автомагистрали VCS.

> **Совет:** Для получения большего количества подробных данных о реализации TelePresence обратитесь к Базовой конфигурации Сервера Передачи видеоданных Cisco TelePresence (Контроль со Скоростной автомагистралью) руководство по развертыванию.

Топология Cisco, нерекомендуемая для VCS C и реализации E

Следует отметить, что следующая топология НЕ рекомендуется Cisco. Методология рекомендуемого развертывания для края Скоростной автомагистрали или Скоростной автомагистрали VCS должна использовать два других DMZ со Скоростной автомагистралью, имеющей NIC в каждом DMZ. Это руководство предназначается, чтобы использоваться в средах, где не может использоваться метод рекомендуемого развертывания.

DMZ одиночной подсети с одиночным интерфейсом LAN (локальной сети) скоростной автомагистрали VCS

В этом сценарии FW *A* может направить трафик к FW *B* (и наоборот). Скоростная автомагистраль VCS позволяет видеотрафику быть переданным через FW B без сокращения трафика на FW B от внешней стороны до внутренних интерфейсов. Скоростная автомагистраль VCS также обрабатывает обход FW на своей общедоступной стороне.

Вот пример этого сценария:

Эти развертывания используют эти компоненты:

- DMZ одиночной подсети (10.0.10.0/24), который содержит:
  Внутренний интерфейс FW (10.0.10.1)Внешний интерфейс FW B (10.0.10.2)Интерфейс LAN1 Скоростной автомагистрали VCS (10.0.10.3)
- Подсеть LAN (10.0.30.0/24), который содержит:
  Внутренний интерфейс FW B (10.0.30.1)Интерфейс LAN1 Контроля за VCS (10.0.30.2)Сетевой интерфейс Сервера управления Cisco TelePresence (TMS) (10.0.30.3)

Статический непосредственный NAT был настроен на FW A, который выполняет NAT для общего адреса 64.100.0.10 к IP-адресу LAN1 Скоростной автомагистрали VCS. Статический NAT режим был включен для интерфейса LAN1 на Скоростной автомагистрали VCS со статическим NAT IP-адресом 64.100.0.10.

> **Примечание:** Необходимо ввести Полное доменное имя (FQDN) Скоростной

автомагистрали VCS на Контроле за VCS безопасная пересекающаяся клиентская зона (адрес партнера (peer)) как, как это замечено снаружи сети. Причина для этого, то, что в статическом NAT режиме, Скоростная автомагистраль VCS запрашивает, чтобы входящая сигнализация и трафик данных были переданы его внешнему FQDN, а не его частному названию. Это также означает, что внешний FW должен позволить трафик от Контроля за VCS до Скоростной автомагистрали VCS внешний FQDN. Это известно как отражение NAT и не могло бы поддерживаться всеми типами FW.

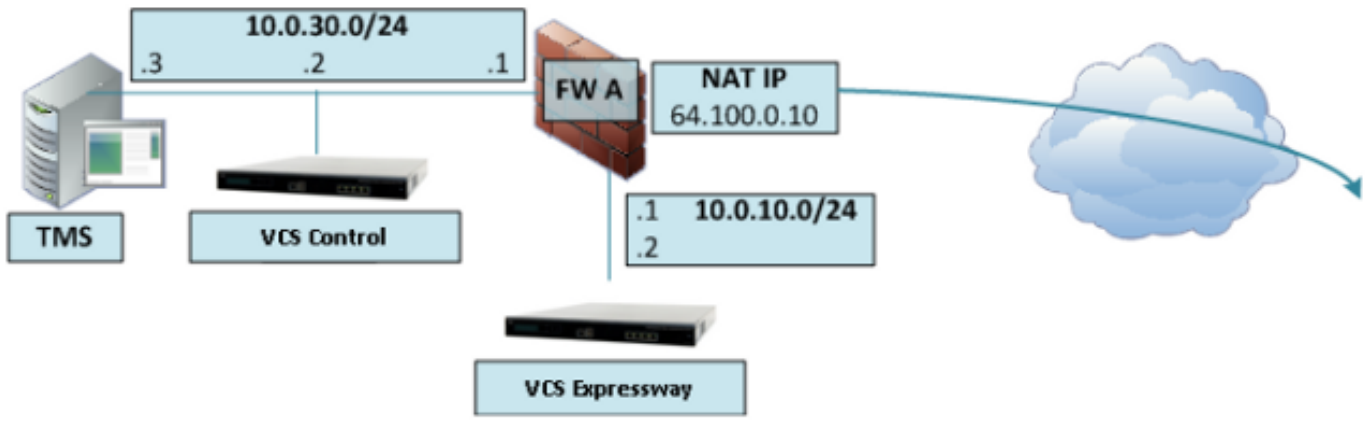
В данном примере FW B должен позволить отражение NAT трафика, который прибывает из Контроля за VCS, который предназначен для внешнего IP - адреса (64.100.0.10) из Скоростной автомагистрали VCS. Пересекающаяся зона на Контроле за VCS должна иметь 64.100.0.10 как адрес партнера (peer) (после FQDN к конверсии IP).

Скоростная автомагистраль VCS должна быть настроена со шлюзом по умолчанию **10.0.10.1**. Требуются ли статические маршруты в этом сценарии, зависит от возможностей и параметров настройки FW A и FW B. Связь от Контроля за VCS до Скоростной автомагистрали VCS происходит через 64.100.0.10 IP-адреса Скоростной автомагистрали VCS; и ответному трафику от Скоростной автомагистрали VCS до Контроля за VCS, возможно, придется пройти через шлюз по умолчанию.

Скоростная автомагистраль VCS может быть добавлена к TMS Cisco с IP-адресом 10.0.10.3 (или с IP-адресом 64.100.0.10, если FW B позволяет это), так как на связь управления TMS Cisco не влияют статические NAT параметры настройки режима на Скоростной автомагистрали VCS.

DMZ FW с 3 портами с одиночным интерфейсом LAN (локальной сети) скоростной автомагистрали VCS

Вот пример этого сценария:



В этих развертываниях FW с 3 портами используется для создания:

- Подсеть DMZ (10.0.10.0/24), который содержит:
  Интерфейс DMZ FW (10.0.10.1)Интерфейс LAN1 Скоростной автомагистрали VCS (10.0.10.2)
- Подсеть LAN (10.0.30.0/24), который содержит:
  Интерфейс LAN (локальной сети) FW (10.0.30.1)Интерфейс LAN1 Контроля за VCS (10.0.30.2)Сетевой интерфейс TMS Cisco (10.0.30.3)

Статический непосредственный NAT был настроен на FW A, который выполняет NAT

открытого IP - адреса 64.100.0.10 к IP-адресу LAN1 Скоростной автомагистрали VCS. Статический NAT режим был включен для интерфейса LAN1 на Скоростной автомагистрали VCS со статическим NAT IP-адресом 64.100.0.10.

Скоростная автомагистраль VCS должна быть настроена со шлюзом по умолчанию 10.0.10.1. Так как этот шлюз должен использоваться для всего трафика, который покидает Скоростную автомагистраль VCS, никакие статические маршруты не требуются в этом типе развертываний.

Пересекающаяся клиентская зона на Контроле за VCS должна быть настроена с адресом партнера (peer), который совпадает со статическим NAT адресом Скоростной автомагистрали VCS (64.100.0.10 в данном примере) по тем же причинам как описанные в предыдущем сценарии.

> **Примечание:** Это означает, что FW Необходимость позволяет трафик от Контроля за VCS с IP - адресом назначения 64.100.0.10. Это также известно как отражение NAT, и нужно обратить внимание, что это не поддерживается всеми типами FW.

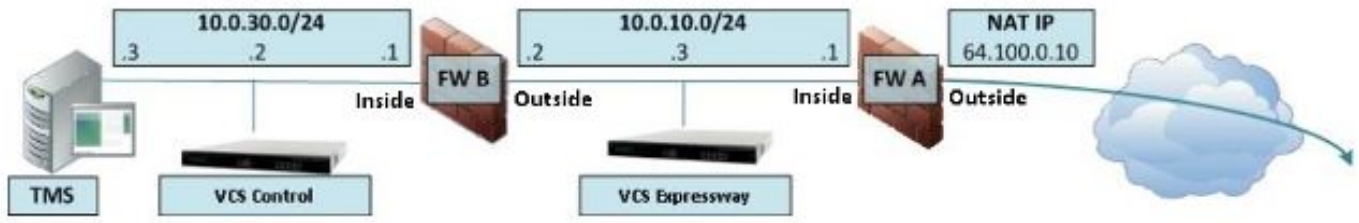
Скоростная автомагистраль VCS может быть добавлена к TMS Cisco с IP-адресом 10.0.10.2 (или с IP-адресом 64.100.0.10, если FW A позволяет это), так как на связь управления TMS Cisco не влияют статические NAT параметры настройки режима на Скоростной автомагистрали VCS.

Настройка

В этом разделе описывается настроить отражение NAT в ASA для двух других VCS C и сценариев реализации E.

DMZ одиночной подсети с одиночным интерфейсом LAN (локальной сети) скоростной автомагистрали VCS

Для первого сценария необходимо применить эту конфигурацию отражения NAT на FW для разрешения связи от Контроля за VCS (10.0.30.2), который предназначен к внешнему IP - адресу (64.100.0.10) из Скоростной автомагистрали VCS:



В данном примере IP-адрес Контроля за VCS является **10.0.30.2/24**, и IP-адрес Скоростной автомагистрали VCS является **10.0.10.3/24**.

Если вы предполагаете, что IP-адрес Контроля за VCS 10.0.30.2 остается, когда он перемещается от внутренней части до внешнего интерфейса FW B при поиске Скоростной автомагистрали VCS с IP - адресом назначения 64.100.0.10, то конфигурацию отражения NAT, которую необходимо внедрить на FW B, показывают в этих примерах.

Exmpla для Версий ASA 8.3 и позже:

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.3
host 10.0.10.3

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.3

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.
```

Пример для Версий ASA 8.2 и ранее:

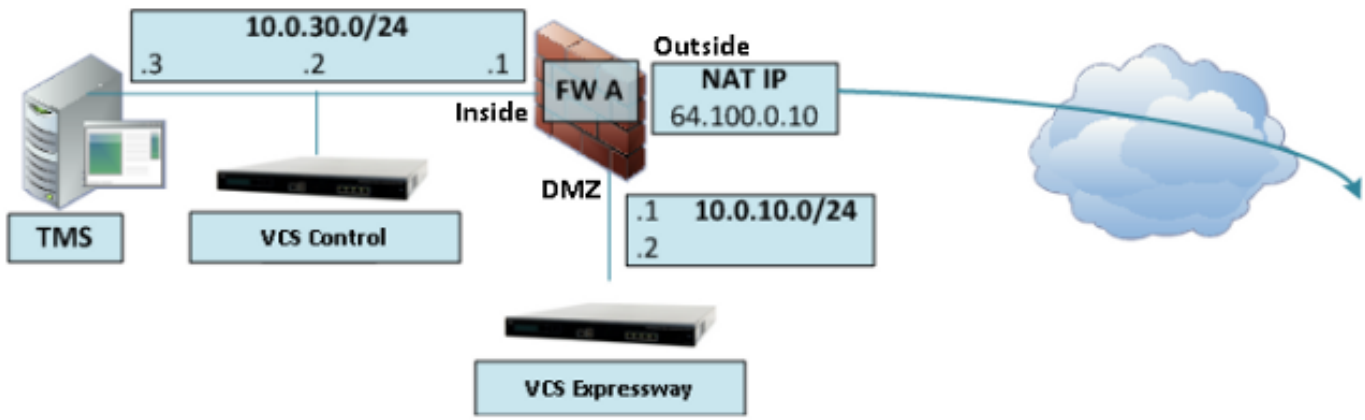
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

access-list OUT-IN-INTERFACE extended permit ip host 10.0.10.3 host 10.0.30.2
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

> **Примечание:** Главная цель этой конфигурации отражения NAT должна позволить Контролю за VCS быть в состоянии достигнуть скоростной автомагистрали VCS, но использования открытого IP - адреса скоростной автомагистрали VCS вместо его закрытого IP - адреса. Если IP - адрес источника Контроля за VCS будет изменен во время этого преобразования NAT с дважды конфигурация NAT вместо предложенной конфигурации NAT, просто показанной, приводя к трафику наблюдения Скоростной автомагистрали VCS от его собственного открытого IP - адреса, то телефонные службы для устройств MRA не подойдут. Это не поддерживаемые развертывания согласно разделу 3 на разделе рекомендаций ниже.

DMZ FW с 3 портами с одиночным интерфейсом LAN (локальной сети) скоростной автомагистрали VCS

Для второго сценария необходимо применить эту конфигурацию отражения NAT на FW для разрешения отражения NAT входящего трафика от Контроля за VCS 10.0.30.2, который предназначен к внешнему IP - адресу (64.100.0.10) из Скоростной автомагистрали VCS:



В данном примере IP-адрес Контроля за VCS является **10.0.30.2/24**, и IP-адрес Скоростной автомагистрали VCS является **10.0.10.2/24**.

Если вы предполагаете, что IP-адрес Контроля за VCS 10.0.30.2 остается, когда он перемещается с внутренней части на интерфейс DMZ FW при поиске Скоростной автомагистрали VCS с IP - адресом назначения 64.100.0.10, то конфигурацию отражения NAT, которую необходимо внедрить на FW A, показывают в этих примерах.

Пример для Версий ASA 8.3 и позже:

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.2
host 10.0.10.2

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.2

NOTE: After this NAT is applied you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the DMZ interface is being redirected.
WARNING: Users may not be able to access any service enabled on the DMZ interface.
```

Пример для Версий ASA 8.2 и ранее:

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,DMZ) 10.0.30.2 access-list IN-DMZ-INTERFACE

access-list DMZ-IN-INTERFACE extended permit ip host 10.0.10.2 host 10.0.30.2
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
```

> **Примечание:** Главная цель этой конфигурации отражения NAT должна позволить Контролю за VCS быть в состоянии достигнуть скоростной автомагистрали VCS, но с открытым IP - адресом скоростной автомагистрали VCS вместо его закрытого IP - адреса. Если IP - адрес источника Контроля за VCS будет изменен во время этого преобразования NAT с дважды конфигурация NAT вместо предложенной конфигурации NAT, просто показанной, приводя к трафику наблюдения Скоростной автомагистрали VCS от его собственного открытого IP - адреса, то телефонные службы для устройств MRA не подойдут. Это не поддерживаемые развертывания согласно разделу 3 на разделе рекомендаций ниже.

Проверка

Этот раздел предоставляет пакетные выходные данные трассировщика, которые вы видите в ASA, чтобы подтвердить, что конфигурация отражения NAT работает по мере необходимости в обоих из VCS C и сценариев реализации E.

DMZ одиночной подсети с одиночным интерфейсом LAN (локальной сети) скоростной автомагистрали VCS

Вот является FW B пакетными выходными данными трассировщика для Версий ASA 8.3 и позже:

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/80 to 10.0.10.3/80

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
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 2, packet dispatched to next module

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

Вот является FW B пакетными выходными данными трассировщика для Версий ASA 8.2 и

ранее:

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/0 to 10.0.10.3/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
```

```
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

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

DMZ FW с 3 портами с одиночным интерфейсом LAN (локальной сети) скоростной автомагистрали VCS

Вот является FW пакетными выходными данными трассировщика для Версий ASA 8.3 и позже:

```
FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/80 to 10.0.10.2/80

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
```

```
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
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 7, packet dispatched to next module

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

Вот является FW пакетными выходными данными трассировщика для Версий ASA 8.2 и ранее:

```
FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/0 to 10.0.10.2/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
```

```
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: DMZ
output-status: up
output-line-status: up
```

```
Action: allow
```

Устранение неполадок

Можно настроить захваты пакета на интерфейсах ASA для подтверждения преобразования NAT, когда пакеты вводят и оставляют интерфейсы FW, которые включены.

Захват пакета просил "DMZ FW с 3 портами с одиночным сценарием" интерфейса LAN (локальной сети) скоростной автомагистрали VCS

```
FW-A# sh cap
capture capin type raw-data interface inside [Capturing - 5735 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capdmz type raw-data interface DMZ [Capturing - 5735 bytes]
  match ip host 10.0.10.2 host 10.0.30.2
FW-A# sh cap capin

71 packets captured
   1: 22:21:37.095270 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:21:37.100672 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101313 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:21:37.114373 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157371 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:21:37.174429 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234164 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:21:39.238528 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261110 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:21:39.270234 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170614 10.0.30.2.38953 > 64.100.0.10.23: S 1841210281:1841210281(0)
win 4128 <mss 536> 12: 22:21:47.198933 64.100.0.10.23 > 10.0.30.2.38953: S
3354834096:3354834096(0)
ack 1841210282 win 4128 <mss 536> 13: 22:21:47.235186 10.0.30.2.38953 > 64.100.0.10.23: . ack
3354834097
win 4128 14: 22:21:47.242815 64.100.0.10.23 > 10.0.30.2.38953: P 3354834097:3354834109(12)
ack 1841210282 win 4128 15: 22:21:47.243014 10.0.30.2.38953 > 64.100.0.10.23: P
1841210282:1841210294(12)
ack 3354834097 win 4128 16: 22:21:47.243258 10.0.30.2.38953 > 64.100.0.10.23: . ack 3354834097
win 4128 17: 22:21:47.261094 64.100.0.10.23 > 10.0.30.2.38953: P 3354834109:3354834151(42)
ack 1841210282 win 4128 18: 22:21:47.280411 64.100.0.10.23 > 10.0.30.2.38953: P
3354834151:3354834154(3)
ack 1841210294 win 4116 19: 22:21:47.280625 64.100.0.10.23 > 10.0.30.2.38953: P
3354834154:3354834157(3)
ack 1841210294 win 4116 20: 22:21:47.280838 64.100.0.10.23 > 10.0.30.2.38953: P
3354834157:3354834163(6)
ack 1841210294 win 4116 21: 22:21:47.281082 10.0.30.2.38953 > 64.100.0.10.23: P
1841210294:1841210297(3)
ack 3354834109 win 4116 22: 22:21:47.281296 10.0.30.2.38953 > 64.100.0.10.23: P
1841210297:1841210300(3)
ack 3354834109 win 4116
FW-A# sh cap capdmz

71 packets captured
   1: 22:21:37.095621 10.0.30.2 > 10.0.10.2: icmp: echo request
   2: 22:21:37.100626 10.0.10.2 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101343 10.0.30.2 > 10.0.10.2: icmp: echo request
   4: 22:21:37.114297 10.0.10.2 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157920 10.0.30.2 > 10.0.10.2: icmp: echo request
   6: 22:21:37.174353 10.0.10.2 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234713 10.0.30.2 > 10.0.10.2: icmp: echo request
   8: 22:21:39.238452 10.0.10.2 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261659 10.0.30.2 > 10.0.10.2: icmp: echo request
```

```
  10: 22:21:39.270158 10.0.10.2 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170950 10.0.30.2.38953 > 10.0.10.2.23: S 2196345248:2196345248(0)
win 4128 <mss 536> 12: 22:21:47.198903 10.0.10.2.23 > 10.0.30.2.38953: S
1814294604:1814294604(0)
ack 2196345249 win 4128 <mss 536> 13: 22:21:47.235263 10.0.30.2.38953 > 10.0.10.2.23: . ack
1814294605 win 4128 14: 22:21:47.242754 10.0.10.2.23 > 10.0.30.2.38953: P
1814294605:1814294617(12)
ack 2196345249 win 4128 15: 22:21:47.243105 10.0.30.2.38953 > 10.0.10.2.23: P
2196345249:2196345261(12)
ack 1814294605 win 4128 16: 22:21:47.243319 10.0.30.2.38953 > 10.0.10.2.23: . ack 1814294605 win
4128 17: 22:21:47.260988 10.0.10.2.23 > 10.0.30.2.38953: P 1814294617:1814294659(42)
ack 2196345249 win 4128 18: 22:21:47.280335 10.0.10.2.23 > 10.0.30.2.38953: P
1814294659:1814294662(3)
ack 2196345261 win 4116 19: 22:21:47.280564 10.0.10.2.23 > 10.0.30.2.38953: P
1814294662:1814294665(3)
ack 2196345261 win 4116 20: 22:21:47.280777 10.0.10.2.23 > 10.0.30.2.38953: P
1814294665:1814294671(6)
ack 2196345261 win 4116 21: 22:21:47.281143 10.0.30.2.38953 > 10.0.10.2.23: P
2196345261:2196345264(3)
ack 1814294617 win 4116 22: 22:21:47.281357 10.0.30.2.38953 > 10.0.10.2.23: P
2196345264:2196345267(3)
ack 1814294617 win 4116
```

Захват пакета просил "DMZ одиночной подсети с одиночным сценарием" интерфейса LAN (локальной сети) скоростной автомагистрали VCS

```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

FW-B# sh cap capin

72 packets captured
   1: 22:30:06.783681 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:30:06.847856 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.877624 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156409 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:30:07.177496 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.802525 10.0.30.2.41596 > 64.100.0.10.23: S 1119515693:1119515693(0)
win 4128 <mss 536> 12: 22:30:13.861100 64.100.0.10.23 > 10.0.30.2.41596: S
2006020203:2006020203(0)
ack 1119515694 win 4128 <mss 536> 13: 22:30:13.935864 10.0.30.2.41596 > 64.100.0.10.23: . ack
2006020204 win 4128 14: 22:30:13.946804 10.0.30.2.41596 > 64.100.0.10.23: P
1119515694:1119515706(12)
ack 2006020204 win 4128 15: 22:30:13.952679 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204
win 4128 16: 22:30:14.013686 64.100.0.10.23 > 10.0.30.2.41596: P 2006020204:2006020216(12)
ack 1119515706 win 4116 17: 22:30:14.035352 64.100.0.10.23 > 10.0.30.2.41596: P
2006020216:2006020256(40)
ack 1119515706 win 4116 18: 22:30:14.045758 64.100.0.10.23 > 10.0.30.2.41596: P
2006020256:2006020259(3)
ack 1119515706 win 4116 19: 22:30:14.046781 64.100.0.10.23 > 10.0.30.2.41596: P
2006020259:2006020262(3)
ack 1119515706 win 4116 20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
```

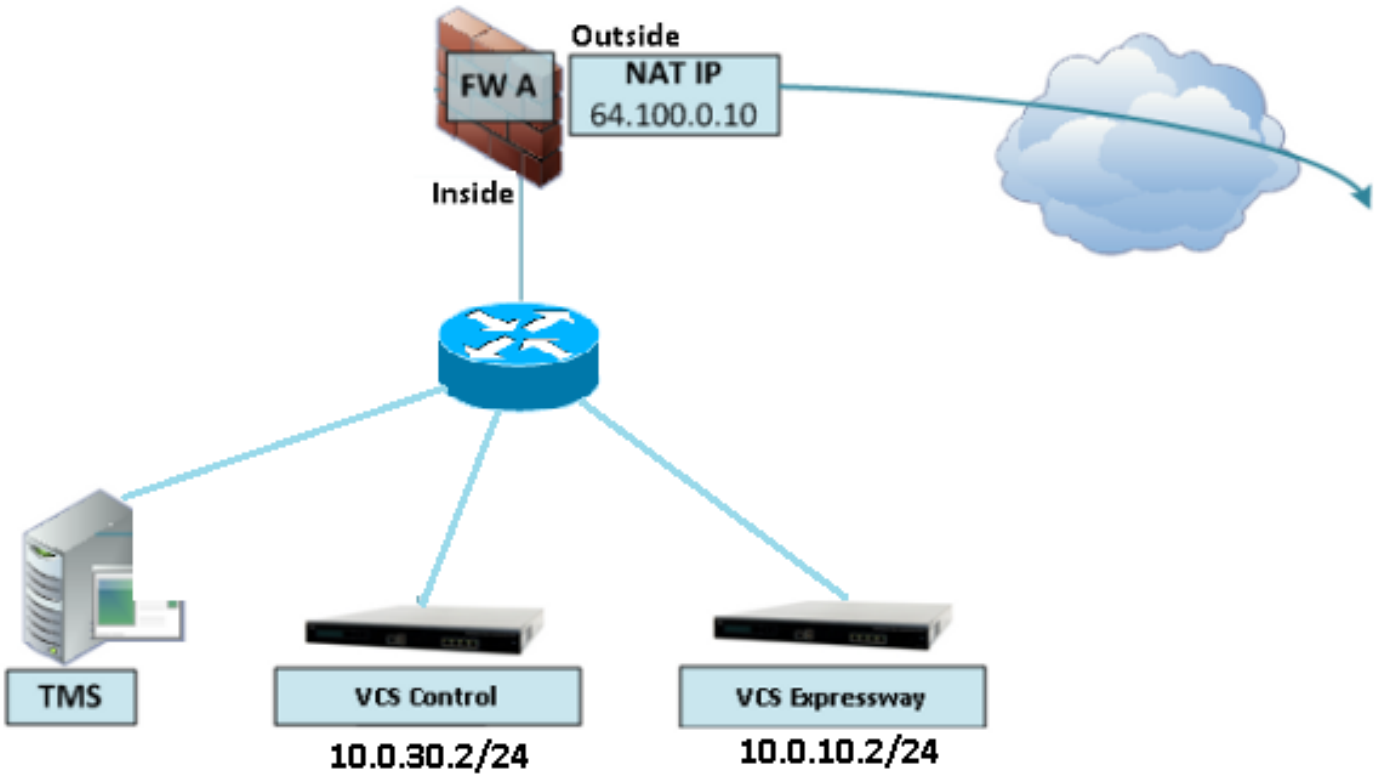
```
1119515709:1119515712(3)
ack 2006020256 win 4076
ASA1# show cap capout

72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo request
   6: 22:30:06.999399 10.0.10.3 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.076808 10.0.30.2 > 10.0.10.3: icmp: echo request
   8: 22:30:07.134422 10.0.10.3 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156959 10.0.30.2 > 10.0.10.3: icmp: echo request
  10: 22:30:07.177420 10.0.10.3 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.803104 10.0.30.2.41596 > 10.0.10.3.23: S 2599614130:2599614130(0)
win 4128 <mss 536> 12: 22:30:13.860947 10.0.10.3.23 > 10.0.30.2.41596: S
4158597009:4158597009(0)
ack 2599614131 win 4128 <mss 536> 13: 22:30:13.936017 10.0.30.2.41596 > 10.0.10.3.23: . ack
4158597010 win 4128 14: 22:30:13.946941 10.0.30.2.41596 > 10.0.10.3.23: P
2599614131:2599614143(12)
ack 4158597010 win 4128 15: 22:30:13.952801 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win
4128 16: 22:30:14.013488 10.0.10.3.23 > 10.0.30.2.41596: P 4158597010:4158597022(12)
ack 2599614143 win 4116 17: 22:30:14.035108 10.0.10.3.23 > 10.0.30.2.41596: P
4158597022:4158597062(40)
ack 2599614143 win 4116 18: 22:30:14.045377 10.0.10.3.23 > 10.0.30.2.41596: P
4158597062:4158597065(3)
ack 2599614143 win 4116 19: 22:30:14.046384 10.0.10.3.23 > 10.0.30.2.41596: P
4158597065:4158597068(3)
ack 2599614143 win 4116 20: 22:30:14.047406 10.0.10.3.23 > 10.0.30.2.41596: P
4158597068:4158597074(6)
ack 2599614143 win 4116 21: 22:30:14.052395 10.0.30.2.41596 > 10.0.10.3.23: P
2599614143:2599614146(3)
ack 4158597062 win 4076 22: 22:30:14.089427 10.0.30.2.41596 > 10.0.10.3.23: P
2599614146:2599614149(3)
ack 4158597062 win 4076
```

Рекомендации

Избегите реализации любой неподдерживаемой топологии

Например, имея и Контроль за VCS и Скоростную автомагистраль VCS позади Внутреннего интерфейса ASA, столь же показанного в этом сценарии:



Этот вид реализации требует, чтобы IP-адрес Контроля за VCS был преобразован во внутренний IP-адрес ASA, чтобы вынудить ответный трафик возвратиться к ASA для предотвращения проблем асимметричной маршрутизации во время отражения NAT.

> ВАЖНОЕ ПРИМЕЧАНИЕ: Если IP - адрес источника Контроля за VCS будет изменен во время этого преобразования NAT с дважды конфигурация NAT вместо предложенной конфигурации NAT, просто показанной, приводя к трафику наблюдения Скоростной автомагистрали VCS от его собственного открытого IP - адреса, то телефонные службы для устройств MRA не подойдут. Это не поддерживаемые развертывания согласно разделу 3 на разделе рекомендаций ниже.

Однако это настоятельно рекомендовано для реализации VCS край Expresswy/Expressway с помощью двух интерфейсов - оба из которых находятся в отдельном DMZ.

Убедитесь, что контроль SIP/H323 полностью отключен в межсетевом экране

Это требуется, чтобы отключать SIP и H.323 ALGs на маршрутизаторах/межсетевых экранах, несущих сетевой трафик к или от Скоростной автомагистрали VCS, как, когда включено это, как часто находят, негативно влияет на функциональность обхода/NAT встроенного межсетевого экрана самой Скоростной автомагистрали VCS.

Для отключения контроля SIP/H323 по умолчанию в ASA Cisco примените следующую конфигурацию:

```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2
```

```
FW-B# sh cap capin

72 packets captured
   1: 22:30:06.783681 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:30:06.847856 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.877624 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156409 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:30:07.177496 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.802525 10.0.30.2.41596 > 64.100.0.10.23: S 1119515693:1119515693(0)
win 4128 <mss 536> 12: 22:30:13.861100 64.100.0.10.23 > 10.0.30.2.41596: S
2006020203:2006020203(0)
ack 1119515694 win 4128 <mss 536> 13: 22:30:13.935864 10.0.30.2.41596 > 64.100.0.10.23: . ack
2006020204 win 4128 14: 22:30:13.946804 10.0.30.2.41596 > 64.100.0.10.23: P
1119515694:1119515706(12)
ack 2006020204 win 4128 15: 22:30:13.952679 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204
win 4128 16: 22:30:14.013686 64.100.0.10.23 > 10.0.30.2.41596: P 2006020204:2006020216(12)
ack 1119515706 win 4116 17: 22:30:14.035352 64.100.0.10.23 > 10.0.30.2.41596: P
2006020216:2006020256(40)
ack 1119515706 win 4116 18: 22:30:14.045758 64.100.0.10.23 > 10.0.30.2.41596: P
2006020256:2006020259(3)
ack 1119515706 win 4116 19: 22:30:14.046781 64.100.0.10.23 > 10.0.30.2.41596: P
2006020259:2006020262(3)
ack 1119515706 win 4116 20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
1119515709:1119515712(3)
ack 2006020256 win 4076
ASA1# show cap capout

72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo request
   6: 22:30:06.999399 10.0.10.3 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.076808 10.0.30.2 > 10.0.10.3: icmp: echo request
   8: 22:30:07.134422 10.0.10.3 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156959 10.0.30.2 > 10.0.10.3: icmp: echo request
  10: 22:30:07.177420 10.0.10.3 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.803104 10.0.30.2.41596 > 10.0.10.3.23: S 2599614130:2599614130(0)
win 4128 <mss 536> 12: 22:30:13.860947 10.0.10.3.23 > 10.0.30.2.41596: S
4158597009:4158597009(0)
ack 2599614131 win 4128 <mss 536> 13: 22:30:13.936017 10.0.30.2.41596 > 10.0.10.3.23: . ack
4158597010 win 4128 14: 22:30:13.946941 10.0.30.2.41596 > 10.0.10.3.23: P
2599614131:2599614143(12)
ack 4158597010 win 4128 15: 22:30:13.952801 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win
4128 16: 22:30:14.013488 10.0.10.3.23 > 10.0.30.2.41596: P 4158597010:4158597022(12)
ack 2599614143 win 4116 17: 22:30:14.035108 10.0.10.3.23 > 10.0.30.2.41596: P
4158597022:4158597062(40)
ack 2599614143 win 4116 18: 22:30:14.045377 10.0.10.3.23 > 10.0.30.2.41596: P
4158597062:4158597065(3)
ack 2599614143 win 4116 19: 22:30:14.046384 10.0.10.3.23 > 10.0.30.2.41596: P
4158597065:4158597068(3)
ack 2599614143 win 4116 20: 22:30:14.047406 10.0.10.3.23 > 10.0.30.2.41596: P
4158597068:4158597074(6)
```

```
ack 2599614143 win 4116 21: 22:30:14.052395 10.0.30.2.41596 > 10.0.10.3.23: P
2599614143:2599614146(3)
ack 4158597062 win 4076 22: 22:30:14.089427 10.0.30.2.41596 > 10.0.10.3.23: P
2599614146:2599614149(3)
ack 4158597062 win 4076
```

Гарантируйте, что ваша фактическая реализация Скоростной автомагистрали соответствует следующим требованиям, подтвержденным разработчиками дистанционного присутствия

- Мы действительно поддерживаем NAT между Скоростной-автомагистралью-C и Скоростной-автомагистралью-E
- Но мы не поддерживаем определенную ситуацию от того, где Скоростная-автомагистраль-C преобразована посредством NAT к IP-адресу, который настроен как статический NAT на Скоростной-автомагистрали-E, примере:
  Скоростная-автомагистраль-C настроена с IP1
  Скоростная-автомагистраль-E имеет одиночный NIC с IP2 настроенный и статический NAT IP3
  Затем Скоростная-автомагистраль-C не может быть преобразована посредством NAT к IP3

Рекомендуемое решение

Рекомендуемое решение вместо того, чтобы внедрить Скоростную автомагистраль VCS с помощью конфигурации отражения NAT должно внедрить его с помощью реализации Скоростной автомагистрали VCS интерфейсов/сдвоенного NIC сдвоенной сети для получения дополнительной информации, проверьте следующую ссылку:

Дополнительные сведения

Базовая конфигурация сервера передачи видеоданных Cisco TelePresence (Контроль со скоростной автомагистралью) руководство по развертыванию

Использование портов IP скоростной автомагистрали Cisco для прохождения межсетевого экрана

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