

VCS Expressway TelePresence デバイスのための ASA の設定 NAT 反射

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[VCS C および E 実装のための Cisco トポロジー非お勧めの](#)

[単一 VCS Expressway LAN インターフェイスとの単一のサブネット DMZ](#)

[単一 VCS Expressway LAN インターフェイスとの 3 ポート FW DMZ](#)

[設定](#)

[単一 VCS Expressway LAN インターフェイスとの単一のサブネット DMZ](#)

[単一 VCS Expressway LAN インターフェイスとの 3 ポート FW DMZ](#)

[確認](#)

[単一 VCS Expressway LAN インターフェイスとの単一のサブネット DMZ](#)

[単一 VCS Expressway LAN インターフェイスとの 3 ポート FW DMZ](#)

[トラブルシューティング](#)

[単一 VCS Expressway LAN インターフェイス」シナリオの "3 ポート FW DMZ を適用されるパケット キャプチャ](#)

[「単一 VCS Expressway LAN インターフェイス」シナリオをの単一のサブネット DMZ 適用されるパケット キャプチャ](#)

[推奨事項](#)

1. [あらゆるサポートされていないトポロジーの実装を避けて下さい](#)

2. [SIP/H.323 インспекションが含まれるファイアウォールで完全に無効になるようにして下さい](#)

3. [実際の Expressway 実装を従います Cisco TelePresence 開発者が提案する次の必要条件に確認して下さい](#)

[推奨される VCS Expressway 実装](#)

[関連情報](#)

概要

この資料にこの種類のファイアウォールの NAT 設定を必要とする特別な Cisco TelePresence シナリオのための Cisco のネットワーク アドレス変換 (NAT) リフレクション設定を適応型セキュリティ アプライアンス (ASA) 設定する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco ASA (適応型セキュリティ アプライアンス (ASA) ソフトウェア) 基本的な NAT 設定。
- Cisco TelePresence Video Communication Server (VCS) コントロールおよび VCS Expressway 基本設定。

注: この資料は異なる DMZ の両方の NIC インターフェイスが付いている VCS Expressway または Expressway エッジの推奨される展開方法が使用することができないときだけ使用されるように意図されています。二重 NIC を使用して推奨される配備のさらに詳しい詳細についてはページで 60 次のリンクをチェックして下さい: [Cisco TelePresence Video Communication Server 基本設定 \(Control および Expressway \) 導入ガイド](#)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.3 および以降を実行する Cisco ASA 5500 および 5500-X シリーズ アプライアンス。
- Cisco VCS バージョン X8.x および以降。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

注: 全体の資料によって、VCS デバイスは VCS Expressway および VCS コントロールと言われます。ただし、同じ設定は Expressway-E および Expressway C デバイ스에適用されます。

背景説明

Cisco TelePresence ドキュメンテーションによって、VCS コントロールが VCS Expressway パブリックIPアドレスによって VCS Expressway と通信するように NAT 反射設定が FW で必要となる 2 種類の TelePresence シナリオがあります。

最初のシナリオは単一のサブネット De-Militarized Zone (DMZ) を含み単一 VCS Expressway LAN インターフェイスを使用する、第 2 シナリオは単一 VCS Expressway LAN インターフェイスを使用する 3 ポート FW DMZ を含みます。

ヒント : TelePresence 実装についてのより多くの詳細を取得するために、[基本設定 \(Expressway とのコントロール \) 配備ガイド](#)を [Cisco TelePresence Video Communication Server \(VCS \)](#) 参照して下さい。

VCS C および E 実装のための Cisco トポロジー非お勧めの

次のトポロジーが Cisco によって推奨されないことに注意することは重要です。VCS Expressway または Expressway エッジのための推奨される配置方法論は DMZ のそれぞれで NIC を持っている Expressway によって 2 つの異なる DMZ を使用することです。このガイドは推奨される展開方法が使用することができない環境で使用されるために意味されます。

単一 VCS Expressway LAN インターフェイスとの単一のサブネット DMZ

このシナリオでは、FW A は FW B にトラフィックをルーティングできます（またその逆にも）。VCS Expressway はビデオトラフィックが外部からの内部インターフェイスへの FW B のトラフィックフローの減少なしで FW B によって通過するようにします。VCS Expressway はまた公衆側の FW 横断を処理します。

このシナリオの例はここにあります：



この配備はこれらのコンポーネントを使用します：

- 含んでいる単一のサブネット DMZ (10.0.10.0/24) :
FW A の内部インターフェイス (10.0.10.1) FW B の外部インターフェイス (10.0.10.2) VCS Expressway の LAN1 インターフェイス (10.0.10.3)
- LAN サブネット (10.0.30.0/24) 含んでいる:
FW B の内部インターフェイス (10.0.30.1) VCS コントロールの LAN1 インターフェイス (10.0.30.2) Cisco TelePresence Management Server (TMS) のネットワーク インターフェイス (10.0.30.3)

静的な 1 対 1 NAT は VCS Expressway の LAN1 IP アドレスへのパブリックアドレス 64.100.0.10 のための NAT を行う FW A で設定されました。スタティック NAT モードは 64.100.0.10 のスタティック NAT IP アドレスの VCS Expressway の LAN1 インターフェイスのために、有効になりました。

注: それがネットワーク以外からどのように見られるかのように VCS コントロール セキュア横断クライアント ゾーン (ピア アドレス) の VCS Expressway の完全修飾ドメイン名 (FQDN) を入力して下さい。この理由はスタティック NAT モードにそれです、受信 シグナリングおよびメディアトラフィックが私用名前よりもむしろ外部 FQDN に送信されるように VCS Expressway は要求します。これはまた外部 FW が VCS コントロールから VCS Expressway 外部 FQDN にトラフィックを可能にする必要があることを意味します。これは NAT リフレクションとして知られ、FW のすべての型によってサポートされないかもしれません。

この例では、FW B は VCS コントロールから来るトラフィックの NAT 反射を可能にする必要があります VCS Expressway の外部 IP アドレスに向かう (64.100.0.10)。VCS コントロールの traversal zone はようにピア アドレス 64.100.0.10 がなければなりません (IP 変換への FQDN の後)。

VCS Expressway は 10.0.10.1 のデフォルト ゲートウェイで設定する必要があります。スタティック・ルートがこのシナリオに必要となるかどうか決まります FW A および FW B.の機能および設定によって。VCS コントロールからの VCS Expressway へのコミュニケーションは VCS Expressway の IP アドレス 64.100.0.10 によって行われます; そして VCS Expressway からの VCS コントロールへのリターントラフィックはデフォルト ゲートウェイで渡らなければならないかもしれません。

VCS Expressway は IP アドレス 10.0.10.3 が付いている Cisco TMS に Cisco TMS 管理コミュニケーションが VCS Expressway のスタティック NAT モード設定から影響を受けないので、FW B がこれを可能にする場合 (または IP アドレス 64.100.0.10 と、) 追加することができます。

単一 VCS Expressway LAN インターフェイスとの 3 ポート FW DMZ

このシナリオの例はここにあります:



この配備では、3 ポート FW は作成するために使用されます:

- DMZ サブネット (10.0.10.0/24) 含んでいる:
FW A の DMZ インターフェイス (10.0.10.1) VCS Expressway の LAN1 インターフェイス (10.0.10.2)
- LAN サブネット (10.0.30.0/24) 含んでいる:
FW A の LAN インターフェイス (10.0.30.1) VCS コントロールの LAN1 インターフェイス (10.0.30.2) Cisco TMS のネットワーク インターフェイス (10.0.30.3)

静的な 1 対 1 NAT は VCS Expressway の LAN1 IP アドレスにパブリック IP アドレス 64.100.0.10 の NAT を行う FW A で設定されました。スタティック NAT モードは 64.100.0.10 のスタティック NAT IP アドレスの VCS Expressway の LAN1 インターフェイスのために、有効になりました。

VCS Expressway は 10.0.10.1 のデフォルト ゲートウェイで設定する必要があります。このゲートウェイが VCS Expressway を去るトラフィックすべてに使用するため、このタイプの配置にスタティック・ルートが必要となりません。

前のシナリオに説明があるそれらと同じ理由で VCS Expressway (この例の 64.100.0.10) のスタティック NAT アドレスと一致する VCS コントロールの横断クライアント ゾーンはピア アドレスで設定する必要があります。

注: これは FW A 絶対必要が 64.100.0.10 の宛先 IP アドレスの VCS コントロールからのトラフィックを可能にすることを意味します。これは別名 NAT リフレクションであり、これが FW のすべての型によってサポートされないことに注意する必要があります。

VCS Expressway は 10.0.10.2 の IP アドレスの Cisco TMS に Cisco TMS 管理コミュニケーションが VCS Expressway のスタティック NAT モード設定から影響を受けないので、FW A がこれを可能にする場合 (または IP アドレス 64.100.0.10 と、) 追加することができます。

設定

このセクションは 2 つの VCS C および E 実装のための ASA の NAT 反射を設定する方法をシナリオ記述します。

単一 VCS Expressway LAN インターフェイスとの単一のサブネット DMZ

最初のシナリオに関しては、VCS Expressway の外部 IP アドレスに向かう VCS コントロールからのコミュニケーションを許可するために FW A のこの NAT 反射設定を適用して下さい (10.0.30.2) (64.100.0.10) :



この例では、VCS コントロール IP アドレスは 10.0.30.2/24 であり、VCS Expressway IP アドレスは 10.0.10.3/24 です。

内部から FW B で設定する必要がある移ると VCS コントロール IP アドレス 10.0.30.2 は残ることを仮定すれば NAT 反射設定宛先 IP アドレス 64.100.0.10 と FW B の outside インターフェイスにとき VCS Expressway を探す、これらの例で示されています。

ASA バージョン 8.3 および それ 以降のための例:

```
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.

ASA バージョン 8.2 および それ 以前のための例:

```
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
```

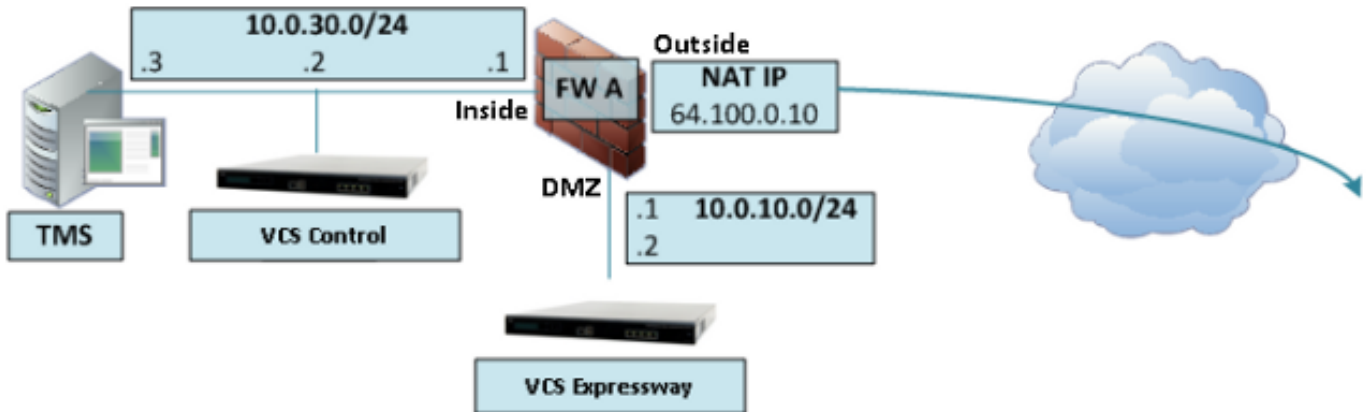
```
access-list OUT-IN-INTERFACE extended permit ip host 10.0.10.3 host 10.0.30.2
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

注: この NAT 反射設定の主要な目標は私用 IP アドレスの代わりに VCS 高速道路、しかし VCS 高速道路パブリックIPアドレスを使用することに達できません VCS コントロールがすることです。 VCS コントロールのソース IP アドレスがちょうど示されている推奨される NAT 設定の代わりに NAT 設定のこの NAT 変換の間に二度変更される場合 VCS Expressway に終って MRA デバイスについては自身のパブリックIPアドレスからのトラフィック、電話

サービスに会うことはアップしません。これは下記の推奨事項セクションのセクション 3 によってサポートされた配備ではないです。

単一 VCS Expressway LAN インターフェイスとの 3 ポート FW DMZ

第 2 シナリオに関しては、VCS Expressway の外部 IP アドレスに向かう VCS コントロール 10.0.30.2 からの受信トラフィックの NAT 反射を許可するために FW A のこの NAT 反射設定を適用して下さい (64.100.0.10) :



この例では、VCS コントロール IP アドレスは 10.0.30.2/24 であり、VCS Expressway IP アドレスは 10.0.10.2/24 です。

内部から FW A の DMZ インターフェイスにとき FW A で設定する必要がある移ると VCS コントロール IP アドレス 10.0.30.2 は残ることを仮定すれば NAT 反射設定 宛先 IP アドレス 64.100.0.10 の VCS Expressway を、探すこれらの例で示されています。

ASA バージョン 8.3 および それ 以降のための例:

```
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.
```

ASA バージョン 8.2 および それ 以前ののための例:

```
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
```

注: この NAT 反射設定の主要な目標は私用 IP アドレスの代わりに VCS 高速道路パブリック IP アドレスの VCS 高速道路に、しかし達できません VCS コントロールがすることです。VCS コントロールのソース IP アドレスがちょうど示されている推奨される NAT 設定の代わりに NAT 設定のこの NAT 変換の間に二度変更される場合 VCS Expressway に終って MRA デバイスについては自身のパブリック IP アドレスからのトラフィック、電話サービスに会うことはアップしません。これは下記の推奨事項セクションのセクション 3 によってサポートされた配備ではないです。

確認

このセクションは VCS C および E 実装の両方で必要に応じて NAT 反射設定作業を確認するために ASA でシナリオわかるパケット トレーサー出力を提供します。

単一 VCS Expressway LAN インターフェイスとの単一のサブネット DMZ

ASA バージョン 8.3 および それ 以降のために出力される FW B パケット トレーサーはここにあります:

```
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

ASA バージョン 8.2 および それ 以前のために出力される FW B パケット トレーサーはここにあります:

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
```

単一 VCS Expressway LAN インターフェイスとの 3 ポート FW DMZ

ASA バージョン 8.3 および それ 以降のために出力される FW A パケット トレーサーはここに
あります:

```
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

ASA バージョン 8.2 および それ 以前のために出力される FW A パケット トレーサーはここに
あります:

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
```

トラブルシューティング

パケットが複雑である FW インターフェイスに入り、去るとき NAT 変換を確認するために ASA インターフェイスのパケット キャプチャを設定できます。

単一 VCS Expressway LAN インターフェイス」シナリオの "3 ポート FW DMZ を適用されるパケット キャプチャ

```
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
```

「単一 VCS Expressway LAN インターフェイス」シナリオをの単一のサブネット DMZ 適用されるパケット キャプチャ

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
```

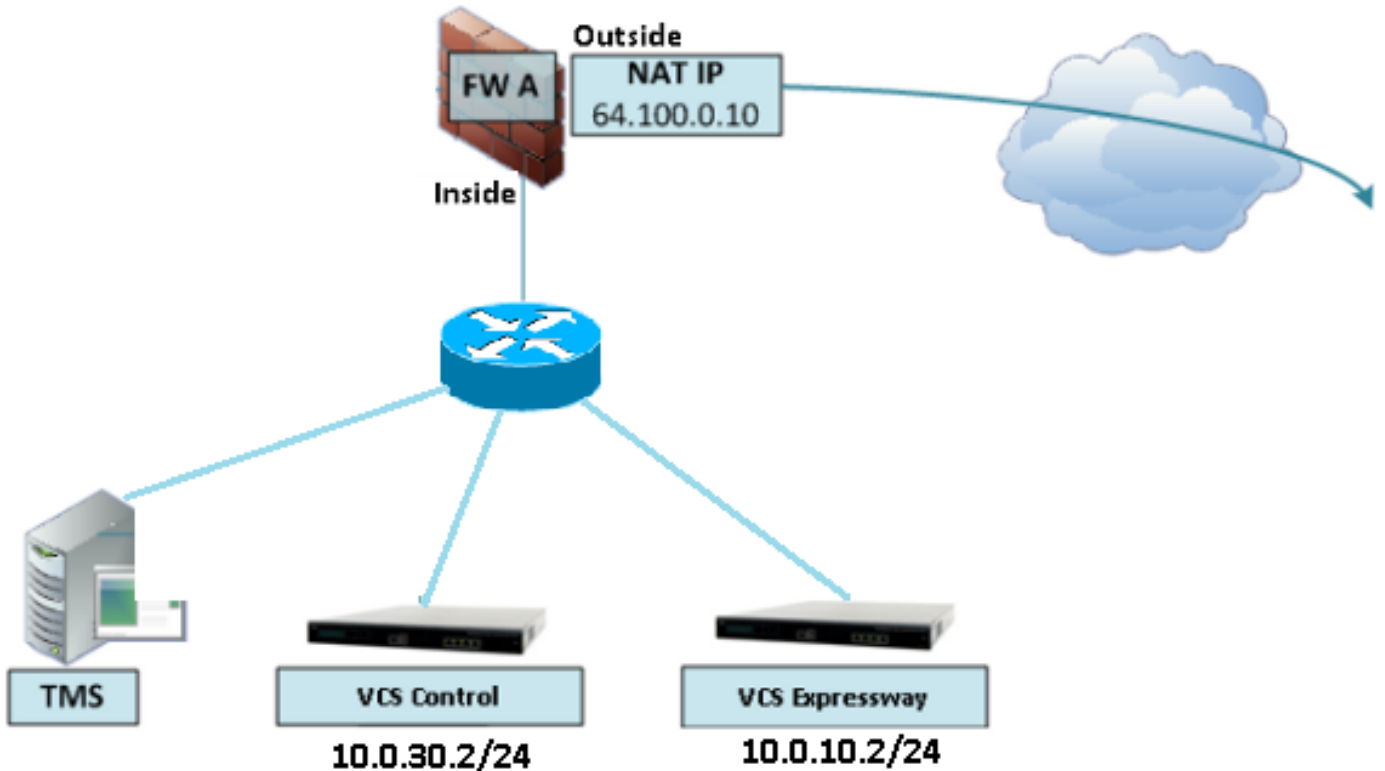
72 packets captured

```
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
```

推奨事項

1. あらゆるサポートされていないトポロジーの実装を避けて下さい

たとえば両方とも VCS コントロールおよび内部 ASA インターフェイスの後ろで接続される VCS Expressway あればちょうどこのシナリオに示すように:



この種類の実装は ASA に戻るように VCS コントロール IP アドレスをリターントラフィックを強制するために NAT 反射のための非対称的なルート問題を回避することを ASA の内部 IP アドレスに変換されるために要求します。

注: VCS コントロールのソース IP アドレスが推奨される NAT 反射設定の代わりに NAT 設定のこの NAT 変換の間に二度変更される場合、VCS Expressway は自身のパブリックIPアドレスからのトラフィックを見ます、MRA デバイスのための電話サービスはアップしません。これは下記の推奨事項セクションのセクション 3 によってサポートされた配備ではありません。

、NAT 反射の単一 NIC の代わりに [Expressway-E 二重ネットワーク・インターフェイス実装](#)として VCS Expressway を設定するためにそれは強く推奨されている。

2. SIP/H.323 インспекションが含まれるファイアウォールで完全に無効になるようにして下さい

それは強く推奨されています Expressway-E に/からネットワークトラフィックを処理するファイアウォールの SIP および H.323 インспекションを無効にするために。有効にされたとき、否定的に Expressway 組み込み firewall/NAT 走査機能性に影響を与えるために SIP/H.323 インスペ

クシヨンは頻繁にあります。

これは方法の例 ASA の SIP および H.323 インспекションを無効にするです。

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
```

3. 実際の Expressway 実装を従います Cisco TelePresence 開発者が提案する次の必要条件に確認して下さい

- Expressway C と Expressway-E 間の NAT 設定はサポートされません。
- それはたとえば Expressway C および Expressway-E が、同じパブリックIPアドレスにネットワークアドレス交換されて得るとき、サポートされません:
 - Expressway C は IP アドレス 10.1.1.1 で設定されます
 - Expressway-E に IP アドレス 10.2.2.1 で設定される単一 NIC があり、スタティック NAT はパブリックIPアドレス 64.100.0.10 でファイアウォールで設定されます
 - それから Expressway C は同じパブリックアドレス 64.100.0.10 へ NATted である場合もありません

推奨される VCS Expressway 実装

詳細については NAT 反射設定の VCS Expressway の代りの VCS Expressway のための推奨される実装は二重ネットワーク・ インターフェイス/二重 NIC VCS Expressway 実装、チェックします次のリンクをです。

[Expressway-E 実装に関する ASA NAT 設定および推奨事項はネットワーク インターフェース二倍になります。](#)

関連情報

- [Expressway-E 実装に関する ASA NAT 設定および推奨事項はネットワーク インターフェース二倍になります](#)
- [Cisco TelePresence Video Communication Server 基本設定 \(Control および Expressway \) 導入ガイド](#)
- [ファイアウォール トラバーサル用の Cisco Expressway IP ポートの使用](#)
- [パブリック インターネットではなく DMZ への Cisco VCS Expressway の配置](#)