VCS Expressway TelePresenceデバイスのASAでのNATリフレクションの設定

内容

概要

このドキュメントでは、Cisco Adaptive Security Appliances（ASA；適応型セキュリティアプライアンス）にネットワークアドレス変換(NAT)リフレクション設定を実装し、ファイアウォールでこの種のNAT設定を必要とする特殊なCisco TelePresenceシナリオを作成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ASA（適応型セキュリティアプライアンス）の基本的なNAT設定。
- Cisco TelePresence Video Communication Server(VCS)ControlおよびVCS Expresswayの基本設定

注：このドキュメントは、異なるDMZの両方のNICインターフェイスを持つVCS-ExpresswayまたはExpressway-Edgeの推奨導入方法を使用できない場合にのみ使用することを目的としています。デュアルNICを使用した推奨される導入の詳細については、60ページの次のリンクを参照してください。Cisco TelePresence Video Communication Server Basic Configuration (Control with 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いています。

- ソフトウェアバージョン8.3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以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

注:ドキュメント全体を通じて、VCSデバイスはVCS ExpresswayおよびVCS Controlと呼ばれます。ただし、Expressway-EデバイスとExpressway-Cデバイスにも同じ設定が適用されます。

背景説明

Cisco TelePresenceのドキュメントに従って、VCS ControlがVCS Expresswayのパブリックアドレスを介してVCS Expresswayと通信できるようにするには、FWにNATリフレクション設定が必要となる2種類のTelePresenceシナリオがあります。

最初のシナリオでは、1つのVCS Expressway LANインターフェイスを使用する1つのサブネットの非武装地帯(DMZ)を使用し、2番目のシナリオでは、1つのVCS Expressway LANインターフェイスを使用する3ポートFW DMZを使用します。

ヒント：TelePresenceの実装の詳細については、『Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)導入ガイド』を参照してください。

VCS CおよびVCS Eの実装に推奨されないシスコトポロジ

次のトポロジはシスコでは推奨されないことに注意してください。VCS ExpresswayまたはExpressway工ッジに推奨される展開方法は、Expresswayで2つの異なるDMZを使用し、各DMZにNICを備えることです。このガイドは、推奨される導入方法を使用できない環境で使用す

ることを目的としています。

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

このシナリオでは、FW Aはトラフィックを FW Bに（またはその逆に）ルーティングできます。VCS Expresswayを使用すると、外部インターフェイスから内部インターフェイスへのFW Bのトラフィックフローを低下させることなく、ビデオトラフィックをFW Bを通過させることができます。VCS Expresswayは、パブリック側でFWトラバーサルも処理します。

このシナリオの例を次に示します。

この導入では、次のコンポーネントを使用します。

- 次を含む単一のサブネットDMZ(10.0.10.0/24)。
  FW A(10.0.10.1)の内部インターフェイスFW B(10.0.10.2)の外部インターフェイスVCS ExpresswayのLAN1インターフェイス(10.0.10.3)
- 次を含むLANサブネット(10.0.30.0/24)。
  FW B(10.0.30.1)の内部インターフェイスVCS Control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)

FW Aにスタティック1対1のNATが設定されており、VCS ExpresswayのLAN1 IPアドレスに対してパブリックアドレス64.100.0.10のNATが実行されます。スタティックNATモードは、VCS ExpresswayのLAN1インターフェイスに対して有効になっており、スタティックNAT IPアドレスは64.100.0.10です。

> **注：**VCS Expresswayの完全修飾ドメイン名(FQDN)を、VCS Controlセキュアトラバーサルクライアントゾーン（ピアアドレス）に入力する必要があります。これは、ネットワークの外部からどのように見えるかということです。この理由は、スタティックNATモードでは、VCS Expresswayが着信シグナリングとメディアトラフィックをプライベート名ではなく外部FQDNに送信するように要求するためです。これは、外部FWがVCS ControlからVCS Expressway外部FQDNへのトラフィックを許可する必要があることを意味します。これはNATリフレクションと呼ばれ、すべてのタイプのFWでサポートされているとは限りません。

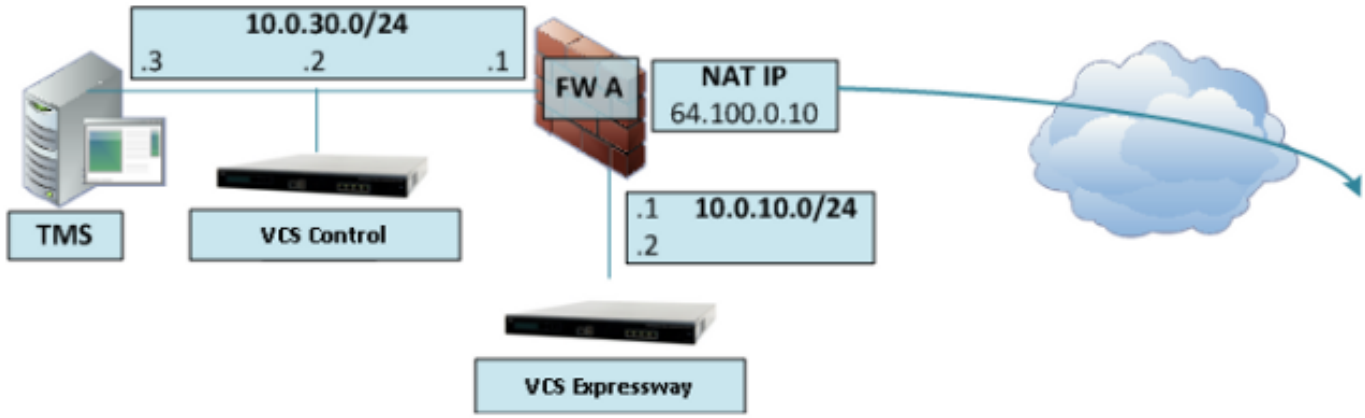
この例では、FW Bが、VCS Expresswayの外部IPアドレス(64.100.0.10)を宛先とするVCS ControlからのトラフィックのNATリフレクションを許可する必要があります。VCS Controlのトラバーサルゾーンには、ピアアドレスとして64.100.0.10が必要です（FQDNからIPへの変換後）。

VCS Expresswayは、デフォルトゲートウェイ**10.0.10.1で設定する必要があります**。このシナリオでスタティックルートが必要かどうかは、FW AとFW Bの機能と設定によって異なります。VCS ControlからVCS Expresswayへのへの通信は、VCS ExpresswayからVCS Controlへのリターントラフィックは、デフォルトゲートウェイを経由する必要がある場合があります。

VCS Expresswayは、IPアドレスが10.0.10.3のCisco TMSに追加できます(FW Bが許可する場合はIPアドレスが64.100.0.10の場合)。これは、Cisco TMS管理通信がVCS ExpresswayのスタティックNATモード設定設定にのの影響を受影響を受受受受けないためです。

単一のVCS Expressway LANインターフェイスを使用した3ポートFW DMZ

このシナリオの例を次に示します。



この展開では、3ポートFWを使用して次の項目を作成します。

- 次を含むDMZサブネット(10.0.10.0/24)
  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)
- 次を含むLANサブネット(10.0.30.0/24)。
  FW AのLANインターフェイス(10.0.30.1)VCS Control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)

スタティック1対1のNATがFW Aに設定されており、パブリックIPアドレス64.100.0.10からVCS ExpresswayのLAN1 IPアドレスへのNATが実行されます。スタティックNATモードは、VCS ExpresswayのLAN1インターフェイスに対して有効になっており、スタティックNAT IPアドレスは64.100.0.10です。

VCS Expresswayはデフォルトゲートウェイ10.0.10.1で設定する必要があります。このゲートウェイはVCS Expresswayから発信されるすべてのトラフィックに使用する必要があるため、このタイプの展開ではスタティックルートは必要ありません。

VCS Controlのトラバーサルクライアントゾーンは、前のシナリオで説明したのと同じ理由で、VCS ExpresswayのスタティックNATアドレス(この例では64.100.0.10)と一致するピアアドレスで設定する必要があります。

> **注**：これは、FW Aが宛先IPアドレス64.100.0.10を持つVCS Controlからのトラフィックを許可する必要があることを意味します。これはNATリフレクションとも呼ばれ、すべてのタイプのFWでサポートされているわけではないことに注意してください。

VCS Expresswayは、IPアドレスが10.0.10.2のCisco TMSに追加できます(FW Aが許可する場合はIPアドレスが64.100.0.10の場合)。これは、Cisco TMS管理通信がVCS ExpresswayのスタティックNATモード設定の設定のの影響を影響を受受受受受けないためです。

設定

このセクションでは、2つの異なるVCS CおよびE実装シナリオに対してASAでNATリフレクションを設定する方法について説明します。

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

最初のシナリオでは、VCS Expresswayの外部IPアドレス(64.100.0.10)宛てのVCS Control(10.0.30.2)からの通信を許可するために、FW AにこのNATリフレクション設定を適用する必要があります。

この例では、VCS ControlのIPアドレスは**10.0.30.2/24**で、VCS ExpresswayのIPアドレスは**10.0.10.3/24です。**

宛先IPアドレスが64.100.0.10のVCS Expresswayを検索する際に、VCS Control IPアドレス10.0.30.2がFW Bの内部インターフェイスから外部インターフェイスに移動しても残ると仮定すると、FW Bに実装するNATリフレクション設定がを次のの例にに示示します。

ASAバージョン8.3以降の例：

```
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以前の例：

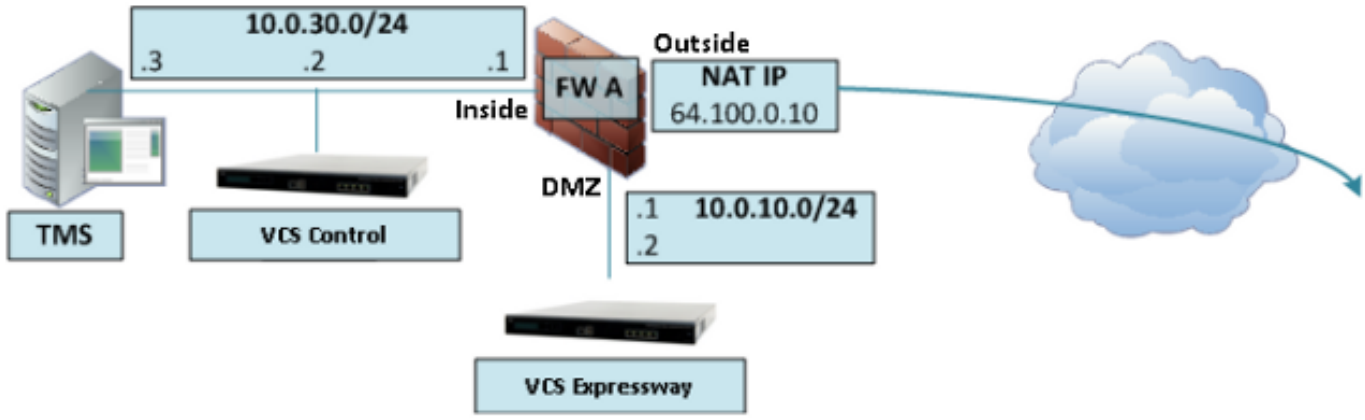
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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リフレクション設定の主な目的は、VCS ControlがVCS Expresswayに到達できるようにしながら、プライベートIPアドレスではなくVCS Expresswayパブリックアドレスを使用できるようにすることです。VCS Controlの送信元IPアドレスが、提示された推奨NAT設定ではなく2回のNAT設定を使用してこのNAT変換中に変更された場合、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認識します。この導入は

、セクション3に示す推奨セクションではサポートされていません。

単一のVCS Expressway LANインターフェイスを使用した3ポートFW DMZ

2番目のシナリオでは、VCS Expresswayの外部IPアドレス(64.100.0.10)を宛先とするVCS Control 10.0.30.2からの着信トラフィックのNATリフレクションを許可するために、次のNATリフレクション設定をFW Aに適用する必要があります。



この例では、VCS ControlのIPアドレスは**10.0.30.2/24**で、VCS ExpresswayのIPアドレスは**10.0.10.2/24です**。

宛先IPアドレスが64.100.0.10のVCS Expresswayを探す際に、VCS Control IPアドレス10.0.30.2がFW Aの内部インターフェイスからDMZインターフェイスに移動しても残ると仮定すると、FW Aに実装するNATリフレクション設定をを次に示します。

ASAバージョン8.3以降の例：

```
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以前の例：

```
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リフレクション設定の主な目的は、VCS ControlがVCS Expresswayに到達で

きるようにし、プライベートIPアドレスではなくVCS ExpresswayパブリックIPアドレスを使用できるようにすることです。このNAT変換中にVCS Controlの送信元IPアドレスが、提示された推奨NAT設定ではなく2回のNAT設定で変更された場合、VCS Expresswayが自身のパブリックIPアドレスからのトラフィックを確認すると、MRAデバイスのののの電話サービスがが行されません。これは、次の推奨セクションのセクション3に従ってサポートされている導入ではありません。

確認

このセクションでは、VCS CとEの両方の実装シナリオで必要に応じてNATリフレクション設定が機能していることを確認するために、ASAで確認できるパケットトレーサの出力を示します。

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

ASAバージョン8.3以降のFW Bパケットトレーサ出力を次に示します。

```
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以前のFW Bパケットトレーサ出力を次に示します。

```
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
```

単一のVCS Expressway LANインターフェイスを使用した3ポートFW DMZ

ASAバージョン8.3以降のFW Aパケットトレーサ出力を次に示します。

```
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以前のFW Aパケットトレーサ出力を次に示します。

```
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
```

トラブルシュート

ASAインターフェイスでパケットキャプチャを設定して、パケットが関与するFWインターフェイスに出入りするときにNAT変換を確認できます。

単一のVCS Expressway LANインターフェイスを使用する3ポートFW DMZに適用されるパケットキャプチャのシナリオ

```
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
```

「単一のVCS Expressway LANインターフェイスを使用する単一サブネットDMZ」シナリオに適用されるパケットキャプチャ

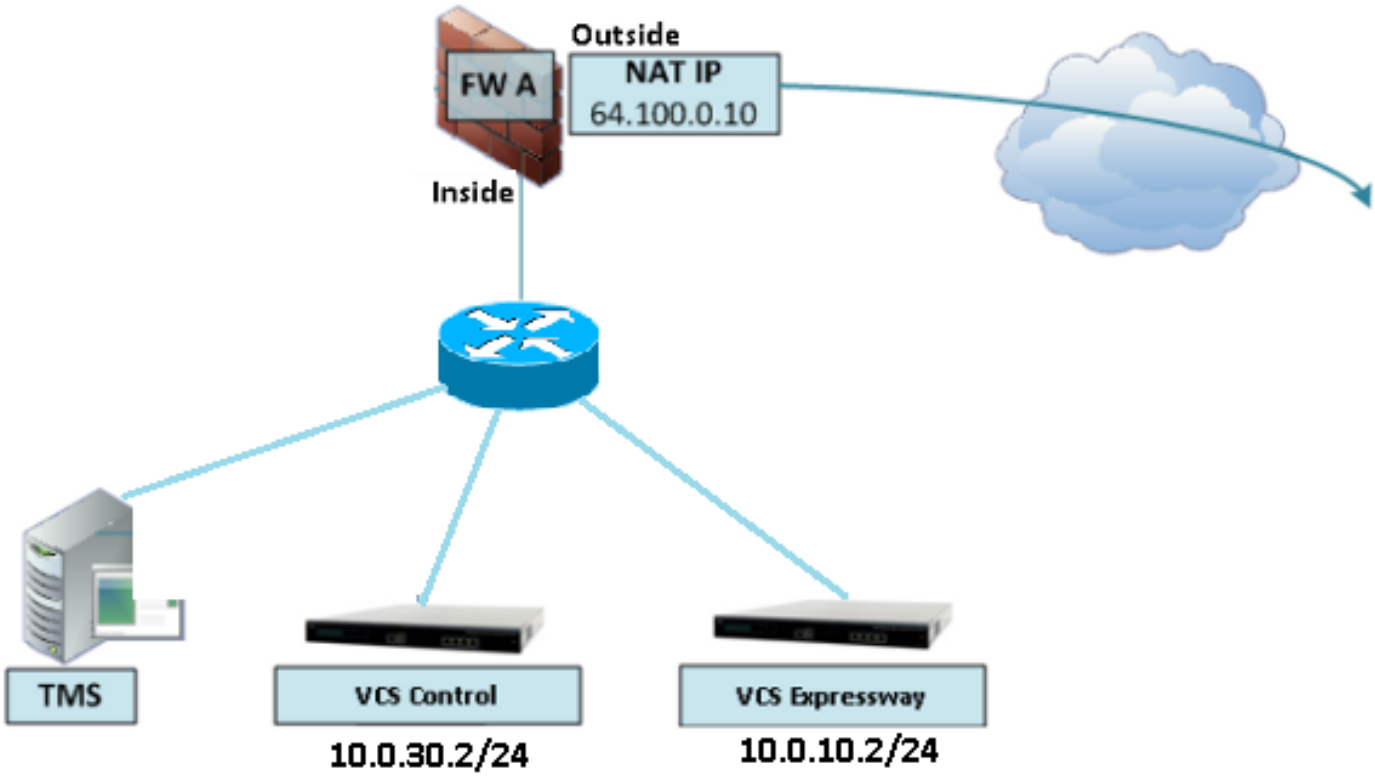
```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

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
2599614146:2599614149(3)
ack 4158597062 win 4076
```

推奨事項

1.サポートされていないトポロジの実装を避ける

たとえば、次のシナリオに示すように、VCS ControlとVCS Expresswayの両方を内部ASAインターフェイスの背後に接続している場合は、次のようになります。



このような実装では、NATリフレクションの非対称ルートの問題を回避するために、リターントラフィックを強制的にASAに戻すために、VCS Control IPアドレスをASAの内部IPアドレスに変換する必要があります。

> 注：このNAT変換中にVCS Controlの送信元IPアドレスが推奨されるNATリフレクション設定ではなく2回のNAT設定で変更された場合、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認識します。これは、次の推奨セクションのセクション3に従ってサポートされている導入ではありません。

ただし、VCS Expresswayを、NATリフレクションを備えた単一のNICの代わりに、Expressway-Eデュアルネットワークインターフェイス実装として実装することを強く推奨します。

2. SIP/H.323インスペクションが、関係するファイアウォールで完全に無効になっていることを確認します

Expressway-Eとの間で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で、SIPおよびH.323インスペクションを無効にすることを強く推奨します。SIP/H.323インスペクションが有効になっている場合、Expresswayの組み込みファイアウォール/NATトラバーサル機能に悪影響を及ぼすことが頻繁に見られます。

これは、ASAでSIPおよびH.323インスペクションを無効にする方法の例です。

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

3.実際のExpresswayの実装が、Cisco telepresence開発者が提案する次の要件に適合していることを確認します

- Expressway-CとExpressway-E間のNAT設定はサポートされていません。
- Expressway-CとExpressway-Eが同じパブリックIPアドレスにNATを取得する場合、次のようにサポートされません。
  Expressway-CにはIPアドレス10.1.1.1が設定されています
  Expressway-EにはIPアドレス10.2.2.1が設定された単一のNICがあり、パブリックIPアドレス64.100.0.10のスタティックNATがファイアウォールで設定されています
  その後、Expressway-Cを同じパブリックアドレス64.100.0.10にNAT変換することはできません

推奨されるVCS Expresswayの実装

NATリフレクション構成のVCS Expresswayの代わりにVCS Expresswayの推奨される実装は、デュアルネットワークインターフェイス/デュアルNIC VCS Expresswayの実装です。詳細については、次のリンクを確認してください。

Expressway-Eデュアルネットワークインターフェイス実装のASA NATの設定と推奨事項

関連情報

- Expressway-Eデュアルネットワークインターフェイス実装のASA NAT設定と推奨事項
- 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