Expressway-E に関する ASA NAT 設定および推奨事項および ExpresswayC は実装 ネットワーク インターフェイス二倍になります。

目次

概要

この資料が Expressway-E および ExpresswayC 二重ネットワーク インターフェイス/Network Interface Controller 二重 (NIC) 実装に Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェアで (ASA) 必要なネットワーク アドレス変換 (NAT) 設定を設定する方法を記述されています。

この配備は NAT リフレクションを使用してよりもむしろ Expressway-E および ExpresswayC デバイスを設定するための推奨されるオプションです。

クリスチャン ヘルナンデスおよび Cesar 口ーペッツ Zamarripa によって貢献される、Cisco TAC エンジニア。

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 基本 NAT および設定
- Cisco Expressway-E および ExpresswayC 基本設定

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 8.0 およびそれ以降を実行する Cisco ASA 5500 および 5500-X シリーズ アプライアンス。
- Cisco Expressway バージョン 8.x および それ 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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

> **注:** 全体の資料によって、Expressway デバイスは Expressway-E および ExpresswayC として呼ばれます。 ただし、同じ 設定はビデオ コミュニケーション コミュニケーション・サーバ（VCS）に Expressway および VCS 制御装置を加えます。

背景説明

意図的に、Cisco Expressway-E は非武装地帯（DMZ）に置くことができままたはパブリックネットワーク（インターネット）に面しますおよびプライベート ネットワークの Cisco ExpresswayC とできます。 ただし、Cisco Expressway-E が DMZ に置かれるとき、これらは additonal 利点です。

- もっとも一般的な シナリオでは、Cisco Expressway-E はプライベート ネットワークから管理されます。 DMZ に Cisco Expressway-E を置くことによって、permietral （外部）ファイアウォールが（Hypertext Transfer Protocol（HTTP）セキュア） HTTPS またはセキュア シェル（SSH） 要求のような Expressway に不必要なアクセスをブロックするのに使用することができます。

- DMZ を横断する DMZ が内部と外部ネットワーク間の割り当てダイレクト接続場合トラフィックを処理するために、専用 サーバが必要となります。 Cisco Expressway は Session Initiation Protocol （SIP）のためのそのサーバとしてや H.323 音声およびビデオトラフィック機能できます。 この場合、外部ファイアウォールに出入するトラフィックのために Cisco Expressway が 2 異なる IP アドレスがあるようにする二重ネットワーク インターフェイス オプション 1、および内部 ファイアウォールに出入するトラフィックのための 1 を使用でき

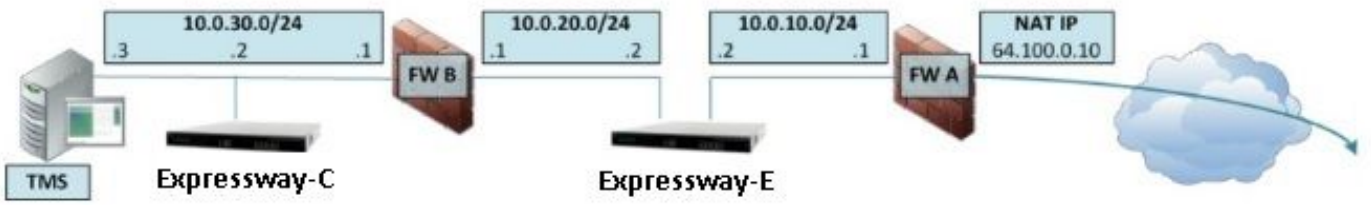
ます。

- このセットアップは内部ネットワークに直接接続するために外部コミュニケーションを防ぎます。 これは内部ネットワークのセキュリティ オーバーオールを改良します。

  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、Cisco Expressway-E および ExpresswayC を-公衆インターネットのよりもむしろ DMZ に基本設定 配置ガイドおよび Cisco VCS Expressway を置くこと参照して下さい。

Expressway C および E -二重ネットワーク インターフェイス/二重 NIC 実装

このダイアグラムは二重ネットワーク インターフェイスおよびスタティック NAT の Expressway-E のための配備例を示します。 走査クライアントおよび 2 ファイアウォール（FW A および FWB）として機能する ExpresswayC。 通常、この DMZ 設定で、FW A は FW B にトラフィックをルーティングできないし FW A サブネットから FW B サブネットにトラフィックを検証し、転送するためにデュアル インターフェイス Expressway-E のようなデバイスが必要となります（またその逆にも）。



この配備はこれらのコンポーネントで構成されています。

DMZ サブネット 1 – 10.0.10.0/24

- FW A 内部 インターフェース– 10.0.10.1
- Expressway-E LAN2 インターフェイス– 10.0.10.2

DMZ サブネット 2 – 10.0.20.0/24

- FW B 外部インターフェイス– 10.0.20.1
- Expressway-E LAN1 インターフェイス– 10.0.20.2

LAN サブネット– 10.0.30.0/24

- FW B 内部 インターフェース– 10.0.30.1
- ExpresswayC LAN1 インターフェイス– 10.0.30.2
- Cisco TelePresence Management Suite（TMS） サーバネットワーク インターフェイス– 10.0.30.3

- FW A は外部か permitetral ファイアウォールです; それは 10.0.10.2 （Expressway-E LAN2 インターフェイス）に静的に変換される 64.100.0.10 の NAT IP （パブリック IP）で設定されます

- FW B は内部 ファイアウォールです

- Expressway-E LAN1 にディセーブルにされるスタティック NAT モードがあります

- Expressway-E LAN2 にスタティック NAT アドレス 64.100.0.10 と有効に なる スタティック NAT モードがあります
- ExpresswayC は 10.0.20.2（Expressway-E LAN1 インターフェイス）を指す走査クライアント ゾーンを備えています
- 10.0.20.0/24 および 10.0.10.0/24 サブネット間にルーティングがありません。 Expressway-E はこれらのサブネットを繋ぎ、SIP/H.323 シグナリングおよびリアルタイムトランスポートプロトコル（RTP）/RTP制御プロトコル（RTCP）メディアのためのプロキシとして機能します。
- Cisco TMS に IP アドレス 10.0.20.2 で設定される Expressway-E があります

必要条件/制限

オーバーラップしていないサブネット

両方の LAN インターフェイスを使用するために Expressway-E が設定される場合トラフィックが正しいインターフェイスに送信されるようにするために LAN1 および LAN2 インターフェイスはオーバーラップしていないサブネットで見つける必要があります。

クラスタリング

クラスタ化する Expressway デバイスに設定される**高度ネットワーキング** オプションがあるとき各クラスタ ピアは自身の LAN1 インターフェイス アドレスを必要とします。 さらに、クラスタ化することは有効に なる スタティック NAT モードがないインターフェイスで設定する必要があります。 従って適当ところで外部インターフェイスとして LAN2 を使用する、LAN2 はスタティック NAT インターフェイスとして使用されますことが、推奨され。

外部 LAN インターフェイス設定

ネットワーク インターフェイスが NAT（回転）のまわりでリレーを使用してトランスバーサルを使用する IPコンフィギュレーション ページ制御の外部 LAN インターフェイス コンフィギュレーションの設定。 ネットワーク インターフェイス Expressway-E 二重設定では、これは Expressway-E 外部 LAN インターフェイスに普通設定 することができます。

スタティック ルート

Expressway-E はこのシナリオのための 10.0.10.1 のデフォルトゲートウェイアドレスで設定する必要があります。 これは LAN2 によって送信されるすべてのトラフィックが IP アドレス 10.0.10.1 に、デフォルトで、送信 されることを意味します。

FW B が 10.0.30.0/24 サブネットから Expressway-E LAN1 インターフェイスに送信 される トラフィックを（たとえば、ExpresswayC 走査クライアント トラフィックか TMS サーバ マネジメントトラフィック）変換すれば、このトラフィックは Expressway-E LAN1 に達するように FWB 外部インターフェイスから来ると同時に現われます（10.0.20.1）。 Expressway-E はそのトラフィックの明白な出典が同じ サブネットにあるので LAN1 インターフェイスによってこのトラフィックに答えられますそれから。

FW B が NAT をしない場合、ExpresswayC から Expressway-E LAN1 に送信 される トラフィックは 10.0.30.2 から来ると同時に示します。 Expressway に 10.0.30.0/24 サブネットのために追加されるスタティック ルートがない場合 10.0.30.0/24 サブネットは内部 ファイアウォール（B）FW の後ろにあることそれがわかっていないのでデフォルト ゲートウェイにこのトラフィックのための応答を送ります（10.0.10.1） LAN2 から。 従って、スタティック ルートは Expressway に SSH セッションによって **xCommand RouteAdd** CLI コマンドを使用して、追加される必要があります。

この特定の 例では、Expressway-E は LAN1 インターフェイスによって到達可能である FW B の後ろで 10.0.30.0/24 サブネットに到達できることを確認する必要があります。 これはこのコマンドを使用して堪能です。

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

> **注:** スタティック ルート 設定はセクション **システム/ネットワーク > インターフェイス/スタティック・ ルート**の Expressway-E グラフィカル ユーザ インターフェイス （GUI）によって適用します。

> **注:** ExpresswayC のための FW-B の NAT の使用を避けることを推奨します。 これは Expressway-E が実際のIPアドレス 10.0.30.2 の ExpresswayC に達するようにします。 これはある特定の電話サービス問題を避けます。 ExpresswayC のための NAT 設定によりモービルおよびリモートアクセス（MRA）デバイスはアップします場合があることが確認されました。

この例では、インターフェイス パラメータはまたゲートウェイアドレスとして**自動**に設定 することができます（10.0.20.1） LAN1 によってだけ到達可能です。

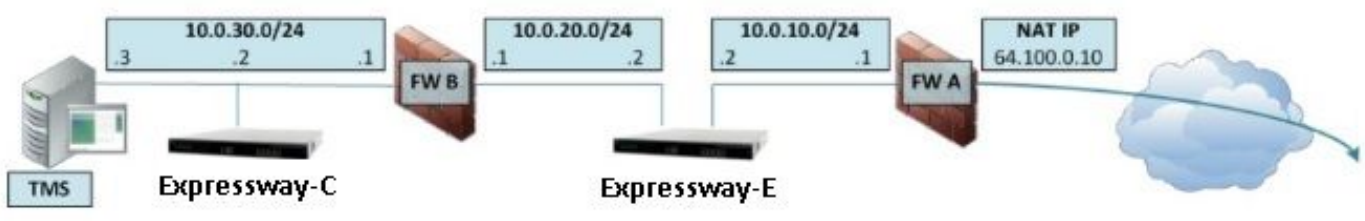
FW B が 10.0.30.0/24 以外またこのネットワーク ワークステーションからのまたは NTP、DNS、LDAP/AD や Sylog のようなネットワークサービスのための SSH および HTTPS 接続のような FW B の後ろにあるサブネットのデバイスと通信する NAT および Expressway-E 必要をしなければ、スタティック・ ルートはこれらのデバイス/サブネットのために追加する必要があります。

xCommand RouteAdd コマンドおよび構文は *VCS 管理者ガイド*の詳細に説明があります。

設定

このセクションが ExpresswayC および Expressway-E 二重ネットワーク インターフェイスに必要なスタティック NAT/ASA の二重 NIC 実装を設定する方法を記述します。 その上、ASA を通した SIP/H323 トラフィックの処理に関するいくつかの ASA モジュラ 政策の枠組（MPF）設定に 関する 推奨事項。

Expressway C および E -二重ネットワーク インターフェイス/二重 NIC 実装



この例で IP アドレス assigment は次の物です。

ExpresswayC IP address:10.0.30.2/24

ExpresswayC default-gateway: 10.0.30.1（FW-B）

Expressway-E IP アドレス

LAN2: 10.0.10.2/24

LAN1: 10.0.20.2/24

Expressway-E default-gateway: 10.0.10.1（FW-A）

TMS IP アドレス: 10.0.30.3/24

FW-A 設定:

ステップ 1. Expressway-E のためのスタティック NAT 設定

この資料の **Background Information セクション**で説明されているように、FW-A にパブリック IPアドレス 64.100.0.10 を使用してインターネットから到達可能であるように Expressway-E がする静的NAT交換があります。 この最後の 1 つは Expressway-E LAN2 IP アドレス 10.0.10.2/24 に、言われるそのこれです必須 FW-A スタティック NAT 設定ネットワークアドレス交換されます。

ASA バージョン 8.3 および それ 以降に関しては:

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR

! To use with static one-to-one NAT:

object network obj-10.0.10.2
nat (inside,outside) static interface
```

> **注:** スタティックPAT を加えることを試みた場合**エラー** エラーメッセージ「受け取るように命じれば: ASA コマンド ライン インターフェースの**ポートを**、従って**予約することが**、**不可能な NAT は** x.x.x.x が ASA 外部 IP アドレスに対応するコマンド **clear xlate ローカル** x.x.x.x の xlate エントリを削除します。 **このコマンドはこの IP に従って実稼働環境で関連**

付けられるすべての変換を慎重に実行しますそれをクリアします。

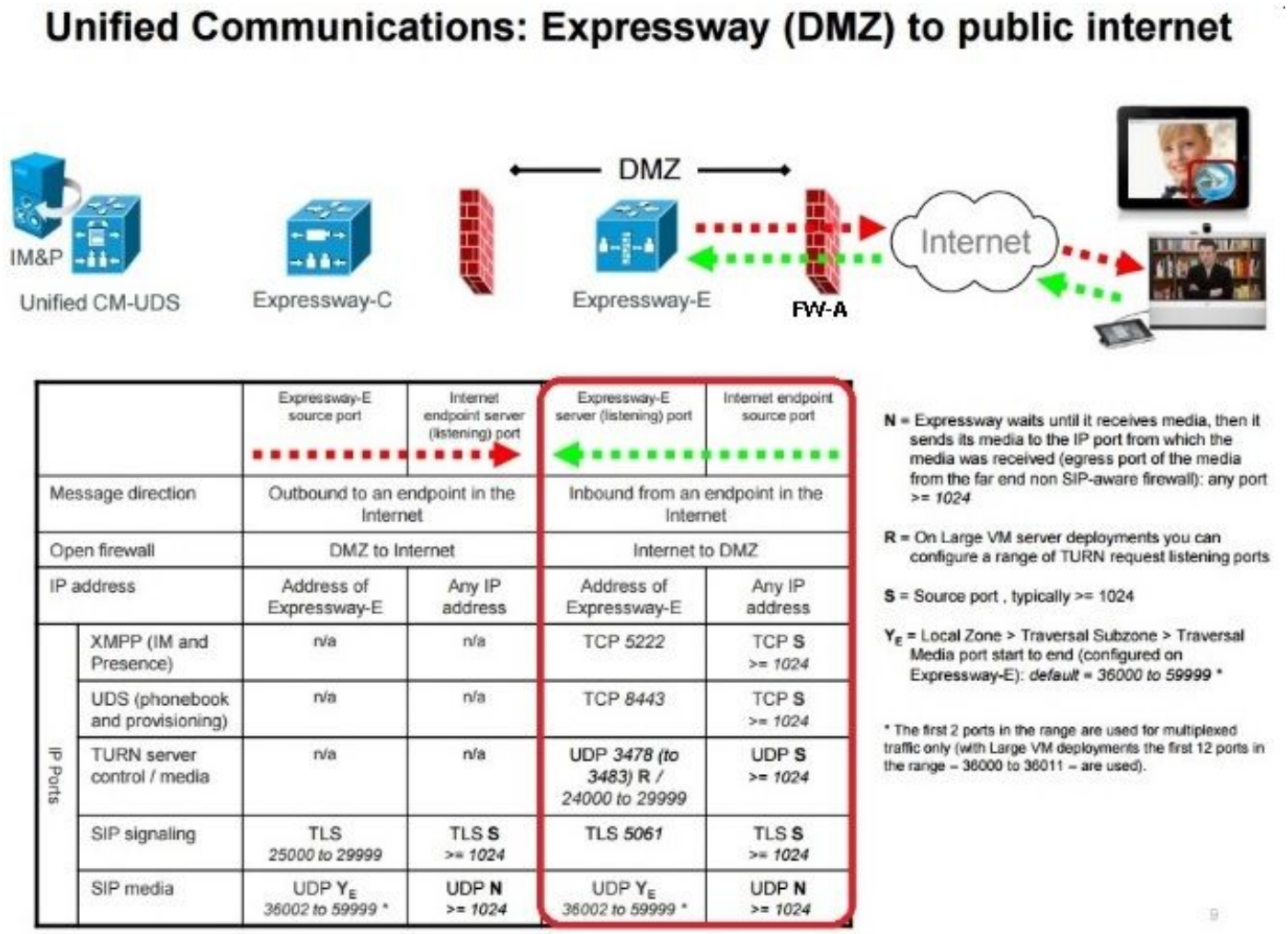
ASA バージョン 8.2 および それ 以前に関しては:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

ステップ 2.インターネットから Expressway-E に必要なポートを許可する Access Control List（ACL）設定

*統合された通信*に従って*: 公衆インターネット* ドキュメントへの *Expressway（DMZ）*は、これ Expressway-E は FW-A で許可されるように要求する TCP 及び UDP ポートのリストです:



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

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

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

S = Source port , typically >= 1024

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

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

これが FW A outside インターフェイスで受信ように必要な ACL構成です。

ASA バージョン 8.3 および それ 以降に関しては。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

ASA バージョン 8.2 および それ 以前に関しては。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.
```

```
static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

> **注:** それは有効に されたとき、否定的に Expressway-E 組み込み firewall/NAT 走査機能性に影響を与えるためにこれが頻繁にあるように強く推奨されています Expressway-E に/からファイアウォール運送ネットワークトラフィックの SIP および H.323 インスペクションをディセーブルにするために。

FW-B 設定。

この資料の **Background Information セクション**で説明されているように、出かけるとき FW B はちょうどダイナミック NAT または PAT 設定が内部 サブネット 10.0.30.0/24 が FW B.の outside インターフェイスへの IP アドレス 10.0.20.1 に変換されるように要求します。

ASA バージョン 8.3 および それ 以降に関しては。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

ASA バージョン 8.2 および それ 以前に関しては。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

> **注:** 強く推奨されています Expressway-E に/からファイアウォール運送ネットワークトラフィックの SIP および H.323 インスペクションを、as ディセーブルにするために、否定的に Expressway-E 組み込み firewall/NAT 走査機能性に影響を与えることをこれ有効に されたとき頻繁にあります。

> **ヒント**： FW B できちんとはたらく ExpresswayC のための必須 TCP 及び UDP ポートすべてがオープンになることをこの Ciscoドキュメントで指定どおりに、ちょうど確かめて下さい: [ファイアウォール走査のための Cisco Expressway IP ポート 使用方法]

確認

ASA でパケット トレーサーが確認するのにことを Expressway-E 静的NAT交換作業要求に応じて使用することができます。

TCP/5222 で 64.100.0.10 をテストするパケット トレーサー。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

TCP/8443 で 64.100.0.10 をテストするパケット トレーサー。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

TCP/5061 で 64.100.0.10 をテストするパケット トレーサー。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

UDP/24000 で 64.100.0.10 をテストするパケット トレーサー:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

UDP/36002 で 64.100.0.10 をテストするパケット トレーサー。

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

トラブルシューティング

ステップ 1.パケットキャプチャ。

パケットキャプチャは ASA 両方入力および出力 インターフェイスで奪取 することができます

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

TCP/5222 の 64.100.0.10 のためのパケットキャプチャ:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

TCP/5061 の 64.100.0.10 のためのパケットキャプチャ:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

ステップ 2.加速されたセキュリティ パス (ASP) ドロップする パケットキャプチャ。

ASA ASP ドロップするキャプチャは廃棄する ASA がことにしたパケットを必要とします。 オプションは**すべて** ASA がパケットをなぜ廃棄したかすべての考えられる原因をキャプチャ します。 これは supected 原因がある場合狭くすることができます。 ASA がこれを分類するのに使用する原因のリストに関しては**非対称多重処理システムがドロップする**使用することができることを、コマンド**示します**廃棄します。

各 ASA キャプチャのための既定のバッファーは 512 KB です。 この ASA によって廃棄される多くのパケットがある場合このバッファは非常に速く充満します。 このバッファはオプション **バッファ**を使用して増分することができます。

```
capture asp type asp-drop all

show cap asp

OR

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

> **ヒント**： この ASA ASP キャプチャは確認してこのシナリオで非常に役立ちますかどうか仕様 TCP か Expressway-E のための UDP ポートをオープンにする抜けた ACL か NAT による ASA ドロップ パケット。

推奨事項

SIP/H.323 インスペクションを完全にディセーブルにされます含まれるファイアウォールで確認して下さい

それは強く推奨されています否定的に Expressway 組み込み firewall/NAT 走査機能性に影響を与えるために Expressway-E に/からネットワークトラフィックを、これ有効に されたとき as 頻繁にある処理するファイアウォールの SIP および H.323 インスペクションをディセーブルにするために。

これは方法の例 ASA の SIP および H.323 インスペクションをディセーブルにするです。

```
capture asp type asp-drop all

show cap asp

OR

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

代替案

二重ネットワーク インターフェイス/二重 NIC を使用して Expressway-E を設定するかわりに代替案は、このリンク示しますこのシナリオについての更に詳しい情報をファイアウォールの NAT リフレクション設定を使用して Expressway-E を設定することです。

ASA: VCS Expressway 実装のための NAT 反射設定。

ただし、それがこの資料の始めに述べられたので、二重ネットワーク セットアップは NAT リフレクションに推奨されます。

関連リンク

Cisco Expressway-E および ExpresswayC -基本設定 配置ガイド

Cisco VCS Expressway を公衆インターネットのよりもむしろ DMZ に置きます

ファイアウォール走査のための Cisco Expressway IP ポート 使用方法