

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[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](#)

[必要条件/制限](#)

[オーバーラップしていないサブネット](#)

[クラスタリング](#)

[外部 LAN インターフェイス設定](#)

[スタティック ルート](#)

[設定](#)

[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](#)

[FW-A 設定:](#)

[ステップ 1. Expressway-E のためのスタティック NAT 設定](#)

[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](#)

[FW-B 設定。](#)

[確認](#)

[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。](#)

[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。](#)

[推奨事項](#)

[SIP/H.323 インспек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](#)

[代替案](#)

[関連リンク](#)

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 ローベツツ 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 additional 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、perimteral (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

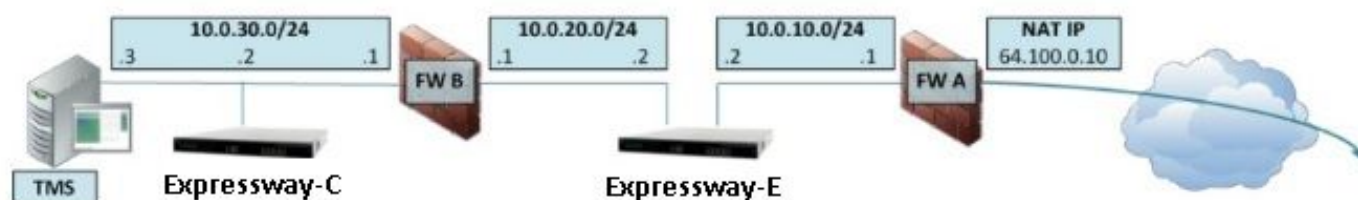
ます。

- 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 FW B) 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 インターフェース– 10.0.10.2

DMZ サブネット 2 – 10.0.20.0/24

- FW B 外部インターフェース– 10.0.20.1
- Expressway-E LAN1 インターフェース– 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 インターフェース– 10.0.30.2
- Cisco TelePresence Management Suite (TMS) サーバネットワーク インターフェース– 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 インターフェース) 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ることが、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が 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ソース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 設定によりモバイ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。

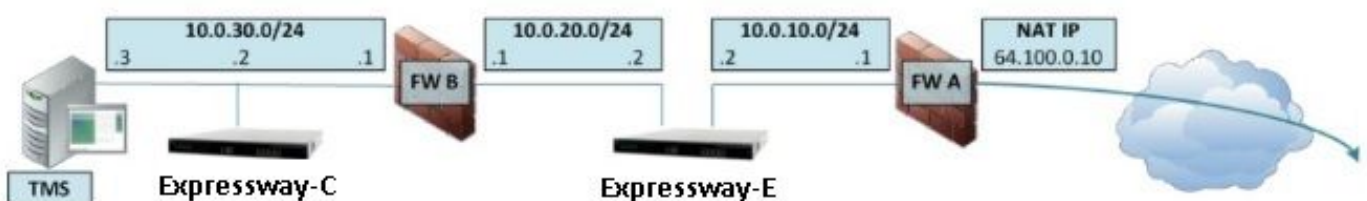
FW B が 10.0.30.0/24 以外またこのネットワークワークステーションからのまたは NTP、DNS、LDAP/AD や Syslog のようなネットワークサービスのための SSH および HTTPS 接続のような FW B の後ろにあるサブネットのデバイスと通信する NAT および Expressway-E 必要をしなければ、スタティック・ルートはこれらのデバイス/サブネットのために追加する必要があります。

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 モジュール 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 assignment 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せん。

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:

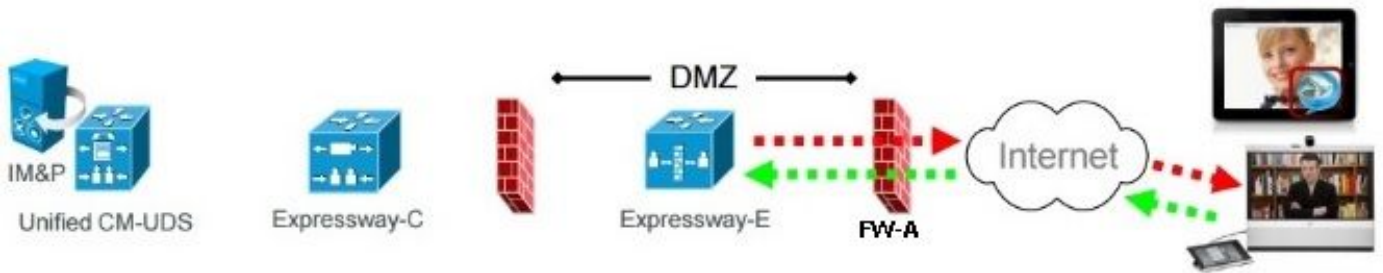
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.

This example 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:

Unified Communications: Expressway (DMZ) to public internet



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

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

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

S = Source port, typically >= 1024

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

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

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。

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

access-group outside-in in interface outside

ASA バージョン 8.2 および それ 以前に関しては。

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
```

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

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

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спек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。

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

ASA バージョン 8.2 および それ 以前に関しては。

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

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спек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。

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

```
Phase: 1
Type: UN-NAT
Subtype: static
```


Result: ALLOW
Config:
object network obj-10.0.10.2
nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

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

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

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

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

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

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

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

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

Phase: 1
Type: UN-NAT
Subtype: static

Result: ALLOW
Config:
object network obj-10.0.10.2
nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

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

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

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

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

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

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

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

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

Phase: 1
Type: UN-NAT
Subtype: static

Result: ALLOW
Config:
object network obj-10.0.10.2
nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

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

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

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

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

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

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

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

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

Phase: 1
Type: UN-NAT
Subtype: static

```
Result: ALLOW
Config:
object network obj-10.0.10.2
  nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000

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

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

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

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

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

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

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

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

```
Phase: 1
Type: UN-NAT
Subtype: static
```

```
Result: ALLOW
Config:
object network obj-10.0.10.2
  nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

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

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

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

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

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

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

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

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

TCP/5222 の 64.100.0.10 のためのパケットキャプチャ:

```
FW-A# sh cap capout
2 packets captured
  1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
  2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown
```

```
FW-A# sh cap capin
2 packets captured
  1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
  2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

TCP/5061 の 64.100.0.10 のためのパケットキャプチャ:

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

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 suspected 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滿します。 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 が Expressway-E のための UDP ポートをオープンにする抜けた ACL が NAT による ASA ドロップ パケット。

推奨事項

SIP/H.323 インспек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спек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спекションをディセーブルにするです。

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

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](#)