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 インターフェースニ倍になります。

目次

概要

この資料が Expressway-E 二重ネットワーク インターフェース実装にで Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア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（ASA）記述されています。

> **ヒント**： この配備は NAT リフレクションとの単一 NIC 実装よりもむしろ Expressway-E 実装のための推奨されるオプション、です。

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 基本設定および NAT 設定
- Cisco Expressway-E および Expressway C 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 X8.0 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。 対象のネットワークが実稼働中である場合には、どのような作業についても、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:** 全体の資料によって、高速道路デバイスは Expressway-E および Expressway C と言われます。 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） Expressway および VCS 制御装置に適用されます。

背景説明

それはプライベート ネットワークの Cisco Expressway C と通信ことはできるが意図的に、Cisco Expressway-E は非武装地帯（DMZ）にまたはインターネット向きインターフェイスと置くことができます。 Cisco Expressway-E が DMZ に置かれるとき、これらは追加の利点です:

- ほとんどの一般的なシナリオでは、Cisco Expressway-E はプライベート ネットワークによって管理されます。 Cisco Expressway-E が DMZ にあるとき、境界（外部）ファイアウォールが（HTTPS）またはセキュア シェル（SSH） 要求によって外部ネットワークからの Expressway への不必要なアクセスをセキュアの Hypertext Transfer Protocol（HTTP）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 が内部および外部ネットワーク間の割り当て直接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 はセッション開始プロトコル（SIP）のためのプロキシ・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

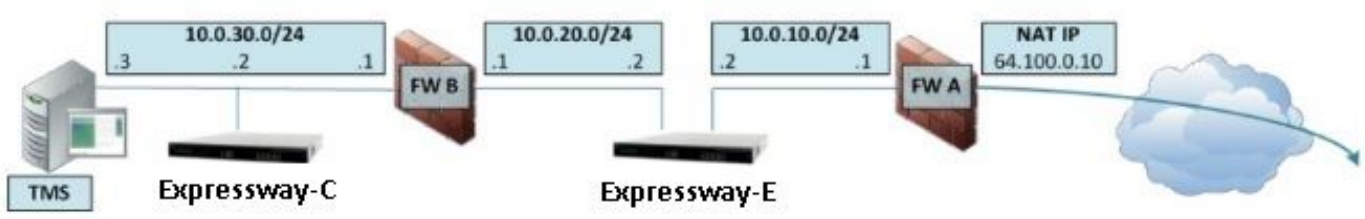
Expressway が 2 異なる IP アドレスがあるようにする二重ネットワーク インターフェース オプション 1、および内部 ファイアウォールに出入するトラフィックのための 1 を使用できます。

- この設定は外部ネットワークから内部ネットワークへの直接接続を防ぎます。 これは内部ネットワーク 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 Expressway C 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 インターフェース/二重 NIC 実装

このイメージは二重ネットワーク インターフェー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。 Expressway C は走査クライアントとして機能します。 2 ファイアウォール（FW A および FWB）があります。 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 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 外部インタフェース– 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
- Expressway C 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

この実装の仕様:

- FW A は外部または境界 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 に無効に なる 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
- Expressway C 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転送プロトコル（ 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非オーバーラップされたサブネットで見つける必要があります。

クラスタ化すること

高度ネットワーキング オプションが設定されている Expressway デバイスをクラスタ化するとき各クラスタ ピアは自身の LAN1 インターフェイス アドレスで設定される必要があります。 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。 従ってところで適当スタティック NAT を適用し、設定できる外部インタフェースとして LAN2 を使用することが、推奨されます。

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 （ TURN ）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 Configuration 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 インターフェース 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 されます。

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、Expressway C 走査クライアント トラフィックか TMS サーバ 管理 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 外部インタフェー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。

NAT が FW B で有効に なる場合、Expressway C 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実行します **xCommand RouteAdd** CLI コマンドを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。 これを達成するために、コマンドを実行して下さい:

```
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 Expressway-E GUI によって適用し、また**システム/ネットワーク > インターフェイス/スタティック・ ルートを**区分できます。

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。

NAT が FW B および Expressway-E 必要でまた FW B の後ろにあるサブネットのデバイスと通信する有効に ならなければ（10.0.30.0/24 以外）、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。

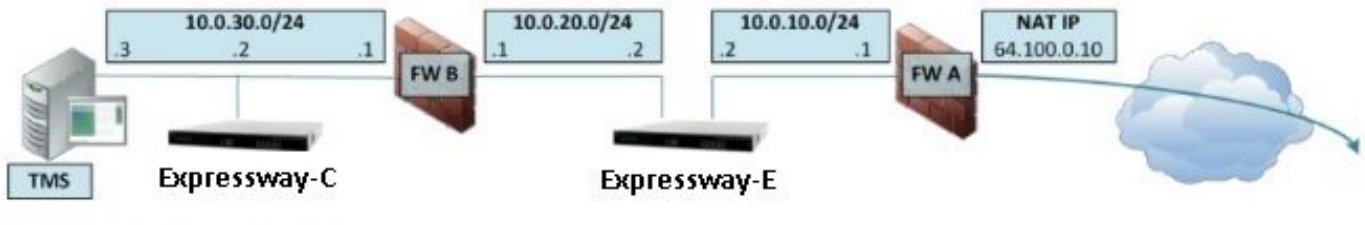
> **注:** これにはネットワーク管理 ワークステーションからのまたは NTP、DNS、LDAP/AD、または Syslog のようなネットワーク サービスのための SSH および HTTPS 接続が含まれています。

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 ASA の Expressway-E 二重ネットワーク インターフェース実装に必要なスタティック NAT を設定する方法を記述します。 いくつかの追加 ASA モジュラ政策の枠組（MPF）設定に関する 推奨事項は SIP/H323 トラフィックを処理するために含まれています。

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



この例では、IP アドレス 割り当ては次のものです。

Expressway C IP アドレス: 10.0.30.2/24

Expressway C 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 の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 にネットワークアドレス交換されます。 これ必須 FW-A スタティック NAT 設定です。

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
```

> **注意**： 適用するときスタティックPAT は「**エラー** ASA コマンドラインインターフェイスのこのエラー メッセージを受け取るように命じます: **ポートを」予約することが不可能な NAT。** これの後で、実行しますコマンド **clearxlatelocal x.x.x.x を、fromwhere** x.x.x.x は IP アドレスの外部の ASA に対応します ASA の xlate エントリを、これのために削除することを続行します。 このコマンドは運用環境でこの IP アドレスと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:

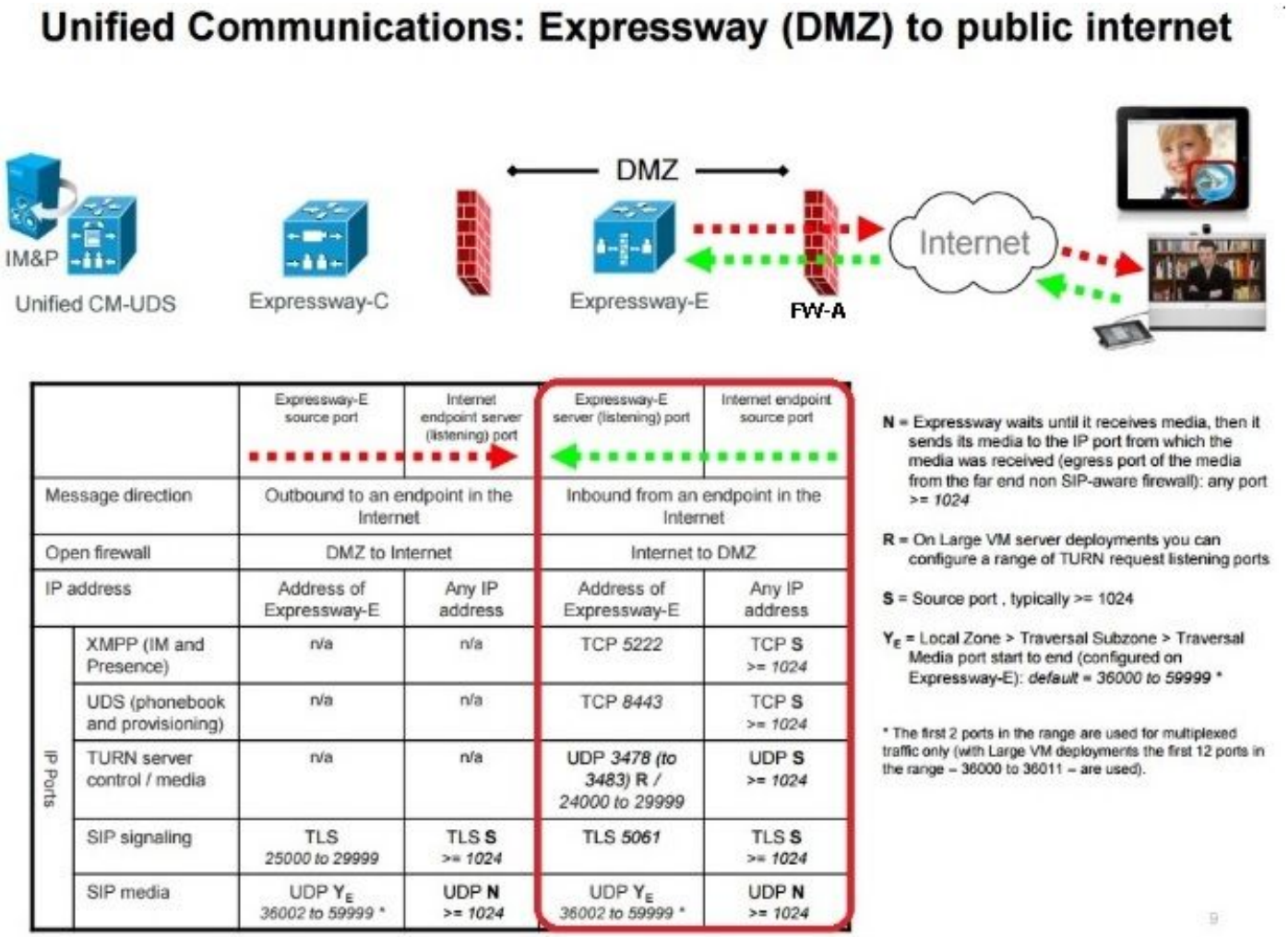
```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

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

ステップ 2. Access Control List（ACL）設定はインターネットから Expressway-E に必須ポート

を可能にします。

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) はイメージに示すように、Expressway-E は FW-A で可能にするように要求する TCP および UDP ポートのリストあります:



		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:

```
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
```

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、FW B.の outside インターフェイスに行くとき FW B はダイナミック NAT または PAT 設定が内部 サブネット 10.0.30.0/24 が IP アドレス 10.0.20.1 に変換されるように要求するかもしれません。

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
```

> **ヒント**： 必須 TCP および UDP ポートすべてが Expressway C がきちんとはたらくようにし、FW B で開いていることをこの 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]

確認

このセクションでは、設定が正常に機能していることを確認します。

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 キャプチャを比較して下さい。

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. Inspect によって加速されるセキュリティ パス (ASP) ドロップするパケット キャプチャ。

ASA によって廃棄されるパケットは ASA ASP キャプチャによってキャプチャされます。 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。 これは疑われた原因がある場合狭くすることができます。 原因のリストに関しては、ASA は実行しますコマンドを**示します非対称多重処理システム ドロップするを**これらのドロップを分類するのに使用します。

各 ASA キャプチャのための既定のバッファーは 512 KB です。 過剰なパケットが ASA によって廃棄される場合、バッファはすぐに充満します。 バッファサイズは**バッファ** オプションを使用する場合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**： このシナリオで ASA ASP キャプチャが ASA が（仕様 TCP か Expressway-E のための UDP ポートをオープンにするためにパケットをよる必要となる）に抜けていた ACL か NAT 廃棄するかどうか確認するのに使用されています。

推奨事項

SIP/H.323 インスペク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 インスペクションを無効に 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 インスペクションは頻繁にあります。

これは方法の例 ASA の SIP および H.323 インスペクションを無効に 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 インターフェース/二重 NIC の Expressway-E を設定する代替案はファイアウォールの NAT リフレクション設定の単一 NIC およびスタティック NAT の Expressway-E を、設定することです。 このリンクはこのシナリオについての更に詳しい情報を示します:

> **注:** それがこの資料の始めに述べられたと同時に、Expressway-E のための二重 NIC 実装は NAT リフレクションに推奨されます。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems
- Cisco Expressway-E および Expressway C -基本設定配備ガイド
- 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