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

内容

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 - デュアル ネットワーク インターフェイス/デュアル NIC 実装
要件/制限事項
重なり合わないサブネット
クラスタリング
外部 LAN インターフェイスの設定
スタティック ルート
コンフィギュレーション
Expressway C および E - デュアル ネットワーク インターフェイス/デュアル NIC 実装
FW-Aの設定
ステップ 1：Expressway-E 用のスタティック NAT 設定.
ステップ2：アクセスコントロールリスト(ACL)の設定により、インターネットからExpressway-Eへの必要なポートを許可します。
FW-Bの設定
確認
TCP/5222で64.100.0.10をテストするためのパケットトレーサ
TCP/8443で64.100.0.10をテストするためのPacket Tracer
TCP/5061で64.100.0.10をテストするためのPacket Tracer
UDP/24000でテスト64.100.0.10へのパケットトレーサ
UDP/36002でテスト64.100.0.10へのPacket Tracer
トラブルシュート
ステップ1：パケットキャプチャの比較

ステップ2：高速セキュリティパス(ASP)ドロップパケットキャプチャを検査します。
推奨事項
代替VCS Expresswayの実装
関連情報

概要

このドキュメントでは、Expressway-Eデュアルネットワークインターフェイスの実装にCisco適応型セキュリティアプライアンス(ASA)で必要なネットワークアドレス変換(NAT)設定を実装する方法について説明します。

ヒント：この導入は、NATリフレクションを使用したシングルNIC実装ではなく、Expressway-E実装に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あることが推奨されます。

- Cisco ASAの基本設定とNATの設定
- 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いています。

- ソフトウェア バージョン 8.0 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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

注：ドキュメント全体では、ExpresswayデバイスをExpressway-EおよびExpressway-Cと呼びます。ただし、Video Communication Server(VCS)ExpresswayおよびVCS Controlデバイスにも同じ設定が適用されます。

背景説明

設計により、Cisco Expressway-Eは非武装地帯(DMZ)またはインターネットに面したインターフェイスに配置でき、プライベートネットワーク内のCisco Expressway-Cと通信できます。Cisco Expressway-EをDMZに配置すると、次のような利点が得られます。

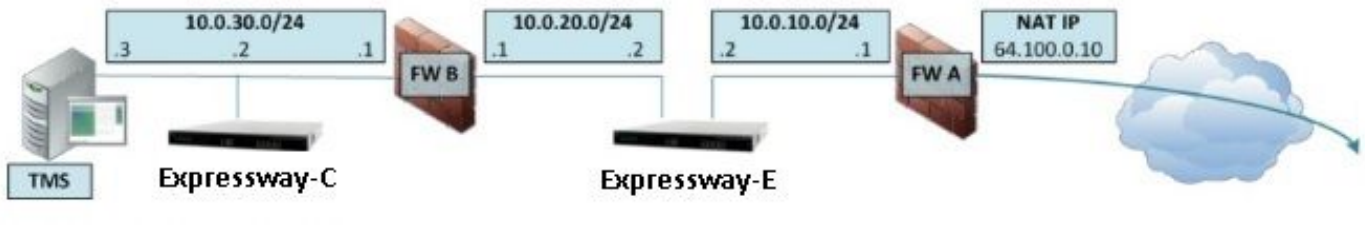
- 最も一般的なシナリオでは、Cisco Expressway-Eはプライベートネットワークによって管理されます。Cisco Expressway-EがDMZにある場合、境界（外部）ファイアウォールを使用して、Hypertext Transfer Protocol(HTTPS)またはセキュアシェル(SSH)要求を介して、外部ネットワークからExpresswayへの不要なアクセスをブロックできます。
- DMZ が内部ネットワークと外部ネットワークの間の直接接続を許可しない場合は、DMZ を通過するトラフィックを処理するための専用サーバが必要です。Cisco Expresswayは、Session Initiation Protocol(SIP)やH.323音声およびビデオトラフィックのプロキシサーバとして機能できます。この場合、デュアル ネットワーク インターフェイス オプションを使用でき、これによって Cisco Expressway で 2 種類の IP アドレス（外部ファイアウォールとやり取りするトラフィック用と内部ファイアウォールとやり取りするトラフィック用）が使用可能になります。

- これにより、外部ネットワークから内部ネットワークへの直接接続が防止されます。こうして内部ネットワークの全体的なセキュリティが強化されます。

  ヒント：TelePresence 実装の詳細については、『Cisco Expressway-E と Expressway-C - 基本設定導入ガイド』と『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』を参照してください。

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

この図は、デュアルネットワークインターフェイスとスタティックNATを使用したExpressway-Eの展開例を示しています。Expressway-Cはトラバーサルクライアントとして機能します。ファイアウォールは2つあります（FW AとFWB）。 通常、このDMZ設定では、FW Aはトラフィックをfw Bにルーティングできず、FW Aのサブネットからfw Bのサブネットへのトラフィックの検証と転送には、Expressway-Eなどのデバイスが必要です（逆も同様）。



この導入は、次のコンポーネントから成ります。

DMZ サブネット 1 – 10.0.10.0/24

- FW A 内部インターフェイス – 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 内部インターフェイス – 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

この実装の詳細：

- FW Aは外部または境界ファイアウォールです。NAT IP（パブリック IP）64.100.0.10 で設定され、これが 10.0.10.2（Expressway-E LAN2 インターフェイス）に静的に変換されます。
- FW B は内部ファイアウォールです。
- Expressway-E LAN1 ではスタティック NAT モードが無効になっています
- Expressway-E LAN2 ではスタティック NAT モードが有効になっており、スタティック NAT アドレス 64.100.0.10 が設定されています
- Expressway-C には 10.0.20.2（Expressway-E LAN1 インターフェイス）を指すトラバーサル クライアント ゾーンがあります。

- 10.0.20.0/24 サブネットと 10.0.10.0/24 サブネットの間でルーティングは発生しません。Expressway-E はこれらのサブネットをブリッジし、SIP/H.323 シグナリングおよび Real-Time Transport Protocol（RTP）/RTP Control Protocol（RTCP）メディア用のプロキシとして機能します。
- Cisco TMS には IP アドレス 10.0.20.2 の Expressway-E が設定されています。

要件/制限事項

重なり合わないサブネット

Expressway-Eが両方のLANインターフェイスを使用するように設定されている場合、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、LAN1インターフェイスとLAN2インターフェイスを重複しないサブネットに配置する必要があります。

クラスタリング

Advanced Networkingオプションを設定してExpresswayデバイスをクラスタリングする場合、各クラスタピアには独自のLAN1インターフェイスアドレスを設定する必要があります。さらに、[Static NAT mode] が有効になっていないインターフェイス上でクラスタリングが設定される必要があります。したがって、LAN2を外部インターフェイスとして使用することを推奨します。外部インターフェイスでは、必要に応じてスタティックNATを適用および設定できます。

外部 LAN インターフェイスの設定

IP 設定ページ上の外部 LAN インターフェイス設定は、どのネットワーク インターフェイスが Transversal Using Relays around NAT（TURN）を使用するかを制御します。 デュアルネットワークインターフェイスExpressway-E設定では、通常、これはExpressway-E外部LANインターフェイスに設定されます。

スタティック ルート

このシナリオでは、Expressway-E をデフォルト ゲートウェイ アドレス 10.0.10.1 に設定する必要があります。これは、LAN2 から送出されるすべてのトラフィックがデフォルトで IP アドレス 10.0.10.1 に送信されることを意味します。

FW Bが10.0.30.0/24サブネットから送信されたトラフィックをExpressway-E LAN1インターフェイス（Expressway-Cトラバーサルクライアントトラフィックや TMSサーバ管理トラフィックなど）に変換すると、FWB外部インターフェイス(10.0.20.1)から送信されたトラフィックになります トラフィックの明白な送信元が同じサブネットにあるため、1インターフェイス。

NATがFW Bで有効な場合、Expressway-CからExpressway-E LAN1に送信されたトラフィックは10.0.30.2から送信されます。Expresswayに10.0.30.0/24サブネットのスタティックルートが追加されていない場合、10.0.30.0/24が内部ファイアウォールののの背後にに存在FW B)。 そのため、スタティックルートを追加する必要があります。ExpresswayへのSSHセッションを介して、**xCommand RouteAdd** CLIコマンドを実行します。

この特定の例では、LAN1 インターフェイスを介して到達可能な FW B の背後にある 10.0.30.0/24 サブネットに到達できることを Expressway-E が認識する必要があります。これを行うには、次のコマンドを実行します。

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

> **注**: Sスタティックルートの設定は、Expressway-E GUIおよび[**System/Network**] > [**Interfaces/Static Routes**]のセクションを介して適用できます。

この例では、ゲートウェイ アドレス (10.0.20.1) が LAN1 経由でのみ到達可能であるため、Interface パラメータを Auto **に設定することもできます。**

NATがFW Bで有効にされておらず、Expressway-EがFW Bの背後にあるサブネット(10.0.30.0/24以外)内のデバイスと通信する必要がある場合は、これらのデバイス/サブネットにスタティックルートを追加する必要があります。

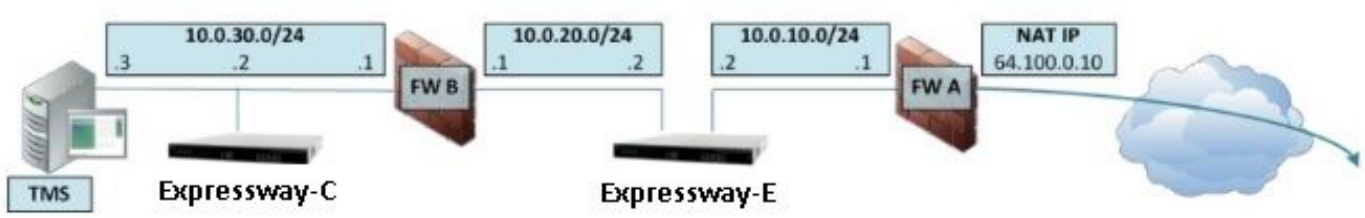
> **注：**これには次のものが含まれます ネットワーク管理ワークステーションまたはNTP、DNS、LDAP/AD、Syslogなどのネットワークサービスからの**SSH**および**HTTPS**接続。

xCommand RouteAddコマンドと構文の詳細については、『VCS Administrator Guide』を参照してください。

コンフィギュレーション

このセクションでは、ASAでのExpressway-Eデュアルネットワークインターフェイス実装に必要なスタティックNATの設定方法について説明します。SIP/H323トラフィックを処理するための追加のASAモジュラポリシーフレームワーク(MPF)設定の推奨事項が含まれています。

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



この例では、IPアドレスの割り当てが次のアドレスです。

Expressway-C IP アドレス：10.0.30.2/24

Expressway-C デフォルト ゲートウェイ：10.0.30.1 (FW-B)

Expressway-EのIPアドレス：

LAN2上：10.0.10.2/24

LAN1 上：10.0.20.2/24

Expressway-Eデフォルトゲートウェイ：10.0.10.1(FW-A)

TMS IP アドレス：10.0.30.3/24

FW-Aの設定

ステップ 1：Expressway-E 用のスタティック NAT 設定.

このドキュメントの「背景説明」セクションで説明したように、FW-Aには、パブリックIPアドレス64.100.0.10のインターネットからExpressway-Eに到達できるスタティックNAT変換があります。最後の1つは、Expressway-E LAN2 IPアドレス10.0.10.2/24に変換されます。

ASA バージョン 8.3 以降の場合：

```
! 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**:スタティックPATコマンドを適用すると、ASAコマンドラインインターフェイス(CLI)で「**ERROR:NAT unable to reserve ports**」というメッセージが表示されます。 この後、ASAのxlateエントリをクリアします。そのためには、**clearxlatelocal x.x.x.x**コマンドを実行します。x.x.x.xはASAの外部IPアドレスに対応します。このコマンドは、このIPアドレスに関連付けられたすべての変換をクリアし、実稼働環境で慎重に実行します。

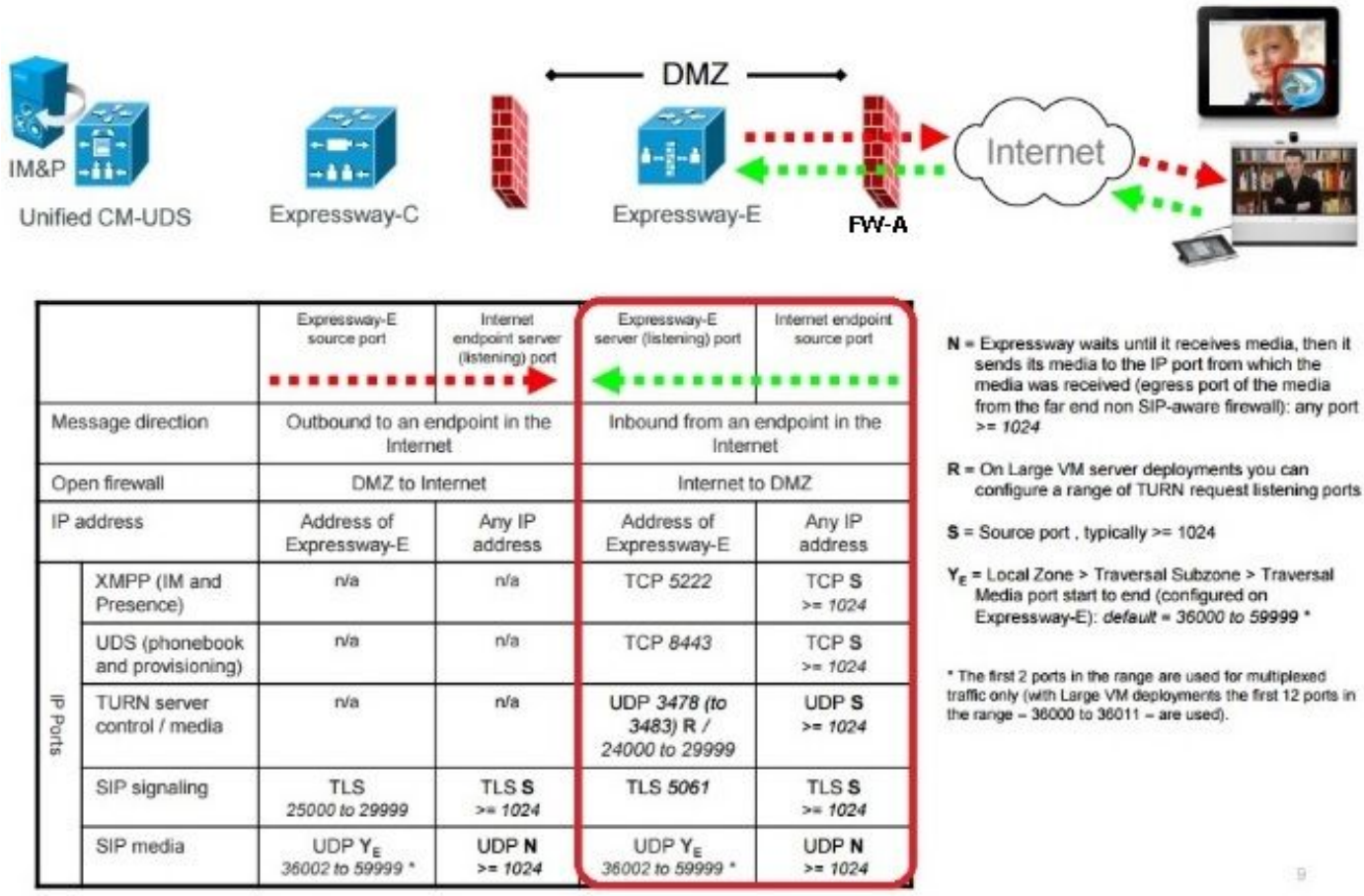
ASA バージョン 8.2 以前の場合：

```
! 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：アクセスコントロールリスト(ACL)の設定により、インターネットからExpressway-Eへの必要なポートを許可します。

『Unified Communication:Expressway(DMZ)からパブリックインターネットへのドキュメント、Expressway-EがFW-Aで許可するために必要なTCPポートとUDPポートのリストを次の図に示します。



これは、FW-A外部インターフェイスのインバウンドとして必要なACL設定です。

ASA バージョン 8.3 以降の場合：

```
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 以前の場合：

```
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の設定

このドキュメントの「背景説明」セクションで説明されているように、FW Bは、内部サブネット10.0.30.0/24をFW Bの外部インターフェイスに移動する際にIPアドレス10.0.20.1に変換するために、ダイナミックNATまたはPAT設定を必要とします。

ASA バージョン 8.3 以降の場合：

```
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 以前の場合：

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

> **ヒント**：必要なすべてのTCPポートとUDPポートでExpressway-Cが正常に動作し、FW Bで開いていることを確認します。このドキュメントの「Cisco Expressway IP Port Usage for Firewall Traversal(ファイアウォールトラバーサルのCisco Expressway IPIPIPIPIPIPIPIPIPIPIPIP))))」でIPPort)」

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ASA 上でパケット トレーサを使用して、Expressway-E スタティック NAT 変換が適切に機能することを確認できます。

TCP/5222で64.100.0.10をテストするためのパケットトレーサ

```
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をテストするためのPacket Tracer

```
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をテストするためのPacket Tracer

```
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でテスト64.100.0.10へのパケットトレーサ

```
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でテスト64.100.0.10へのPacket Tracer

```
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
```

トラブルシュート

ステップ1：パケットキャプチャの比較

パケット キャプチャは、ASA 入力インターフェイスと ASA 出力インターフェイスの両方で取得可能です.

```
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 における 64.100.0.10 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 における 64.100.0.10 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：高速セキュリティパス(ASP)ドロップパケットキャプチャを検査します。

ASAによるパケットドロップは、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**all**は、ASAがパケットをドロップした理由として考えられるすべての理由をキャプチャします。原因の疑いがある場合は、これを絞り込むことができます。ASAがこれらのドロップを分類するために使用する理由のリストについては、コマンド**show asp drop**を実行します。

```
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**：このシナリオでは、ASA ASPキャプチャを使用して、Expressway-Eの特定のTCPまたはUDPポートを開く必要があるACLまたはNAT設定のミスが原因でASAがパケットをドロップするかどうかを確認します。

> **ヒント**：各ASAキャプチャのデフォルトバッファサイズは512 KBです。ASAによってドロップされるパケットが多すぎる場合、バッファは迅速に満たされます。バッファサイズは、

バッファオプションを使用して増**大することが**できます。

推奨事項

SIP/H.323インスペクションが、関連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。

次に、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を示します。

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

代替VCS Expresswayの実装

デュアルネットワークインターフェイス/デュアルNICを備えたExpressway-Eを実装する別のソリューションは、Expressway-Eを実装し、ファイアウォールに単一のNICとNATリフレクション設定を実装することです。次のリンクでは、この実装に関する詳細を示しま[す。VCS Expressway TelePresenceデバイス用のASAでのNATリフレクションの設定](#)。

> **ヒント**：VCS Expresswayの推奨される実装は、このドキュメントで説明されている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。

関連情報

- [VCS Expressway TelePresenceデバイス用ASAでのNATリフレクションの設定](#)
- [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 - 基本設定導入ガイド](#)
- [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](#)
- [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](#)