Configuration NAT ASA Et Recommandations Pour La Mise En Oeuvre Des Interfaces Réseau Double Expressway-E

Contenu

Introduction

Ce document décrit comment mettre en oeuvre la configuration NAT (Network Address Translation) requise dans l'appliance de sécurité adaptative (ASA) Cisco pour l'implémentation des interfaces réseau doubles Expressway-E.

Conseil : ce déploiement est l'option recommandée pour la mise en oeuvre d'Expressway-E, plutôt que pour la mise en oeuvre d'une carte réseau unique avec réflexion NAT.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de base de Cisco ASA et configuration NAT
- Configuration de base de Cisco Expressway-E et Expressway-C

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliances des gammes Cisco ASA 5500 et 5500-X qui exécutent les versions 8.0 et ultérieures du logiciel.
- Cisco Expressway version X8.0 et ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Remarque : Dans l'ensemble du document, les périphériques des autoroutes sont appelés Expressway-E et Expressway-C. Toutefois, la même configuration s'applique aux périphériques Expressway et VCS Control du serveur de communication vidéo (VCS).

Informations générales

Par conception, Cisco Expressway-E peut être placé dans une zone démilitarisée (DMZ) ou avec une interface orientée Internet, tout en étant en mesure de communiquer avec Cisco Expressway-C dans un réseau privé. Lorsque Cisco Expressway-E est placé dans une zone démilitarisée, voici les avantages supplémentaires suivants :

- Dans le scénario le plus courant, Cisco Expressway-E est géré par le réseau privé. Lorsque Cisco Expressway-E se trouve dans une zone DMZ, un pare-feu périmétrique (externe) peut être utilisé pour bloquer l'accès indésirable à Expressway à partir de réseaux externes via des requêtes HTTPS (Hypertext Transfer Protocol Secure) ou SSH (Secure Shell).

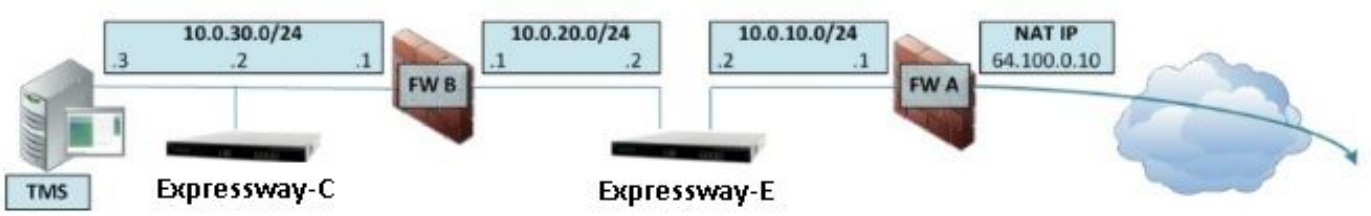
- Si la DMZ n'autorise pas les connexions directes entre les réseaux internes et externes, des serveurs dédiés sont nécessaires pour gérer le trafic qui traverse la DMZ. Cisco Expressway peut servir de serveur proxy pour le trafic voix et vidéo SIP (Session Initiation Protocol) et/ou H.323. Dans ce cas, vous pouvez utiliser l'option Dual Network Interfaces qui permet à Cisco Expressway d'avoir deux adresses IP différentes, l'une pour le trafic entrant/sortant du pare-feu externe et l'autre pour le trafic entrant/sortant du pare-feu interne.

- Cette configuration empêche les connexions directes du réseau externe au réseau interne. Cela améliore globalement la sécurité du réseau interne.

  Astuce : Pour obtenir plus de détails sur la mise en oeuvre de TelePresence, reportez-vous au Guide de déploiement de configuration de base de Cisco Expressway-E et Expressway-C et placez un Cisco VCS Expressway dans une zone démilitarisée plutôt que sur l'Internet public.

Expressway C et E - Mise en oeuvre de deux interfaces réseau/deux cartes réseau

Cette image montre un exemple de déploiement pour un Expressway-E avec deux interfaces réseau et NAT statique. Expressway-C agit en tant que client de traversée. Il existe deux pare-feu (FW A et FWB). Généralement, dans cette configuration DMZ, FW A ne peut pas acheminer le trafic vers FW B, et des périphériques tels que l'Expressway-E sont requis pour valider et transférer le trafic du sous-réseau de FW A vers le sous-réseau de FW B (et vice versa).



Ce déploiement se compose de ces composants.

Sous-réseau DMZ 1 - 10.0.10.0/24

- FW Interface interne - 10.0.10.1
- Interface LAN2 Expressway-E - 10.0.10.2

Sous-réseau DMZ 2 - 10.0.20.0/24

- Interface externe FW B - 10.0.20.1
- Interface LAN1 Expressway-E - 10.0.20.2

Sous-réseau LAN - 10.0.30.0/24

- Interface interne de FW B - 10.0.30.1
- Interface LAN1 Expressway-C - 10.0.30.2
- Interface réseau du serveur Cisco TelePresence Management Suite (TMS) - 10.0.30.3

Spécifications de cette mise en oeuvre :

- FW A est un pare-feu externe ou périmétrique ; il est configuré avec l'adresse IP NAT (public IP) de 64.100.0.10, qui est traduite de manière statique en 10.0.10.2 (interface LAN2 d'Expressway-E)
- FW B est le pare-feu interne
- Le mode NAT statique du LAN1 d'Expressway-E est désactivé
- Le mode NAT statique du LAN2 d'Expressway-E est activé avec l'adresse NAT statique 64.100.0.10
- Expressway-C possède une zone de client de traverse qui pointe vers 10.0.20.2 (interface

LAN1 Expressway-E)
- Il n'existe aucun routage entre les sous-réseaux 10.0.20.0/24 et 10.0.10.0/24. Expressway-E relie ces sous-réseaux et agit comme un proxy pour les supports SIP/H.323 de signalisation et RTP (Real-time Transport Protocol) / RTCP (RTP Control Protocol).
- Cisco TMS a Expressway-E configuré avec l'adresse IP 10.0.20.2

Exigences/limitations

Sous-réseaux sans chevauchement

Si Expressway-E est configuré pour utiliser les deux interfaces LAN, les interfaces LAN1 et LAN2 doivent être situées dans des sous-réseaux non superposés pour s'assurer que le trafic est envoyé à l'interface correcte.

Mise en grappe

Lorsque vous mettez en grappe des périphériques Expressway avec l'option Advanced Networking configurée, chaque homologue de cluster doit être configuré avec sa propre adresse d'interface LAN1. En outre, le clustering doit être configuré sur une interface dont le mode NAT statique n'est pas activé. Par conséquent, il est recommandé d'utiliser le LAN2 comme interface externe, sur laquelle vous pouvez appliquer et configurer la NAT statique le cas échéant.

Paramètres d'interface LAN externe

Les paramètres de configuration d'interface de réseau local externe de la page de configuration IP contrôlent quelle interface réseau utilise Transversal Using Relays around NAT (TURN). Dans une configuration Expressway-E à deux interfaces réseau, cette valeur est normalement définie sur l'interface LAN externe Expressway-E.

routes statique

Pour ce scénario, l'Expressway-E doit être configuré avec l'adresse de passerelle par défaut 10.0.10.1. Cela signifie que tout le trafic envoyé via LAN2 est, par défaut, envoyé à l'adresse IP 10.0.10.1.

Si FW B traduit le trafic envoyé à partir du sous-réseau 10.0.30.0/24 vers l'interface LAN1 d'Expressway-E (par exemple, le trafic client de traversée Expressway-C ou le trafic de gestion du serveur TMS), ce trafic apparaît comme provenant de l'interface externe FWB (10.0.20.1) lorsqu'il atteint le LAN1 d'Expressway-E. Expressway-E peut alors répondre à ce trafic via son interface LAN1, car la source apparente de ce trafic se trouve sur le même sous-réseau.

Si la NAT est activée sur le pare-feu B, le trafic envoyé de l'Expressway-C vers le réseau local LAN1 d'Expressway-E s'affiche lorsqu'il provient de 10.0.30.2. Si Expressway n'a pas de route statique ajoutée pour le sous-réseau 10.0.30.0/24, il envoie les réponses pour ce trafic à sa passerelle par défaut (10.0.10.1) depuis le LAN2, car il ne sait pas que le sous-réseau 10.0.30.0/24 est situé derrière le pare-feu interne (FW B). Par conséquent, une route statique doit être ajoutée, exécutez la commande CLI **xCommand RouteAdd** via une session SSH vers Expressway.

Dans cet exemple particulier, Expressway-E doit savoir qu'il peut atteindre le sous-réseau

10.0.30.0/24 derrière FW B, accessible via l'interface LAN1. Pour ce faire, exécutez la commande suivante :

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

> **Note** : SLa configuration de la route statique peut être appliquée via l'interface utilisateur graphique de l'Expressway-E ainsi que la section **System/Network > Interfaces/Static Routes**.

Dans cet exemple, le paramètre Interface peut également être défini sur **Auto** car l'adresse de passerelle (10.0.20.1) est accessible uniquement via le réseau local LAN1.

Si la NAT n'est pas activée sur le pare-feu B et Expressway-E doit communiquer avec les périphériques des sous-réseaux (autres que 10.0.30.0/24) qui sont également situés derrière le pare-feu B, des routes statiques doivent être ajoutées pour ces périphériques/sous-réseaux.

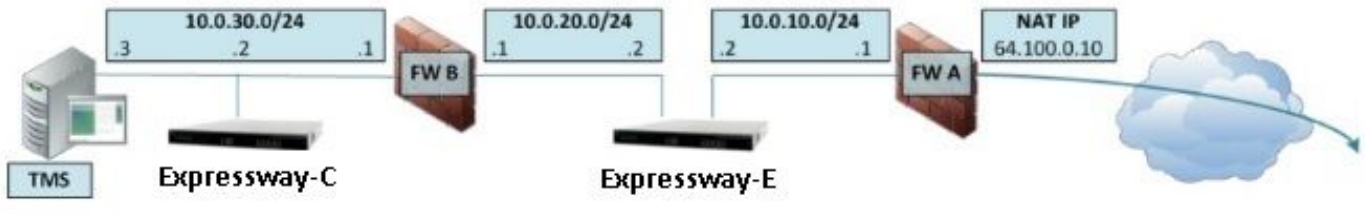
> **Note**: Ceci inclut Connexions SSH et HTTPS à partir de stations de travail de gestion de réseau ou pour des services réseau tels que NTP, DNS, LDAP/AD ou Syslog.

La commande et la syntaxe **xCommand RouteAdd** sont décrites en détail dans le Guide de l'administrateur VCS.

Configuration

Cette section décrit comment configurer la NAT statique requise pour la mise en oeuvre de l'interface réseau double Expressway-E sur l'ASA. Des recommandations supplémentaires de configuration du cadre de politique modulaire ASA (MPF) sont incluses pour la gestion du trafic SIP/H323.

Expressway C et E : double interface réseau/double carte réseau



Dans cet exemple, l'affectation d'adresse IP est la suivante.

Adresse IP d'Expressway-C : 10.0.30.2/24

Passerelle par défaut Expressway-C : 10.0.30.1 (FW-B)

Adresses IP Expressway-E :

Sur le réseau local LAN2 : 10.0.10.2/24

Sur LAN1 : 10.0.20.2/24

Passerelle par défaut Expressway-E : 10.0.10.1 (FW-A)

Adresse IP TMS : 10.0.30.3/24

Configuration FW-A

Étape 1. Configuration NAT statique pour l'Expressway-E.

Comme expliqué dans la section Informations générales de ce document, le FW-A dispose d'une traduction NAT statique pour permettre à Expressway-E d'être accessible à partir d'Internet avec l'adresse IP publique 64.100.0.10. Ce dernier est NATed à l'adresse IP 10.0.10.2/24 du réseau local LAN2 Expressway-E. Ceci dit, il s'agit de la configuration NAT statique FW-A requise.

Pour ASA versions 8.3 et ultérieures :

```
! 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
```

> **Attention** : Lorsque vous appliquez les commandes PAT statiques, vous recevez ce message d'erreur sur l'interface de ligne de commande ASA, "**ERREUR : NAT ne peut pas réserver de ports »**. Après cela, supprimez les entrées xlate sur l'ASA, pour cela, exécutez la commande **clear xlatelocal x.x.x.x,** où x.x.x.x correspond à l'adresse IP externe ASA. Cette commande efface toutes les traductions associées à cette adresse IP, exécutez-la avec prudence dans les environnements de production.

Pour ASA versions 8.2 et antérieures :

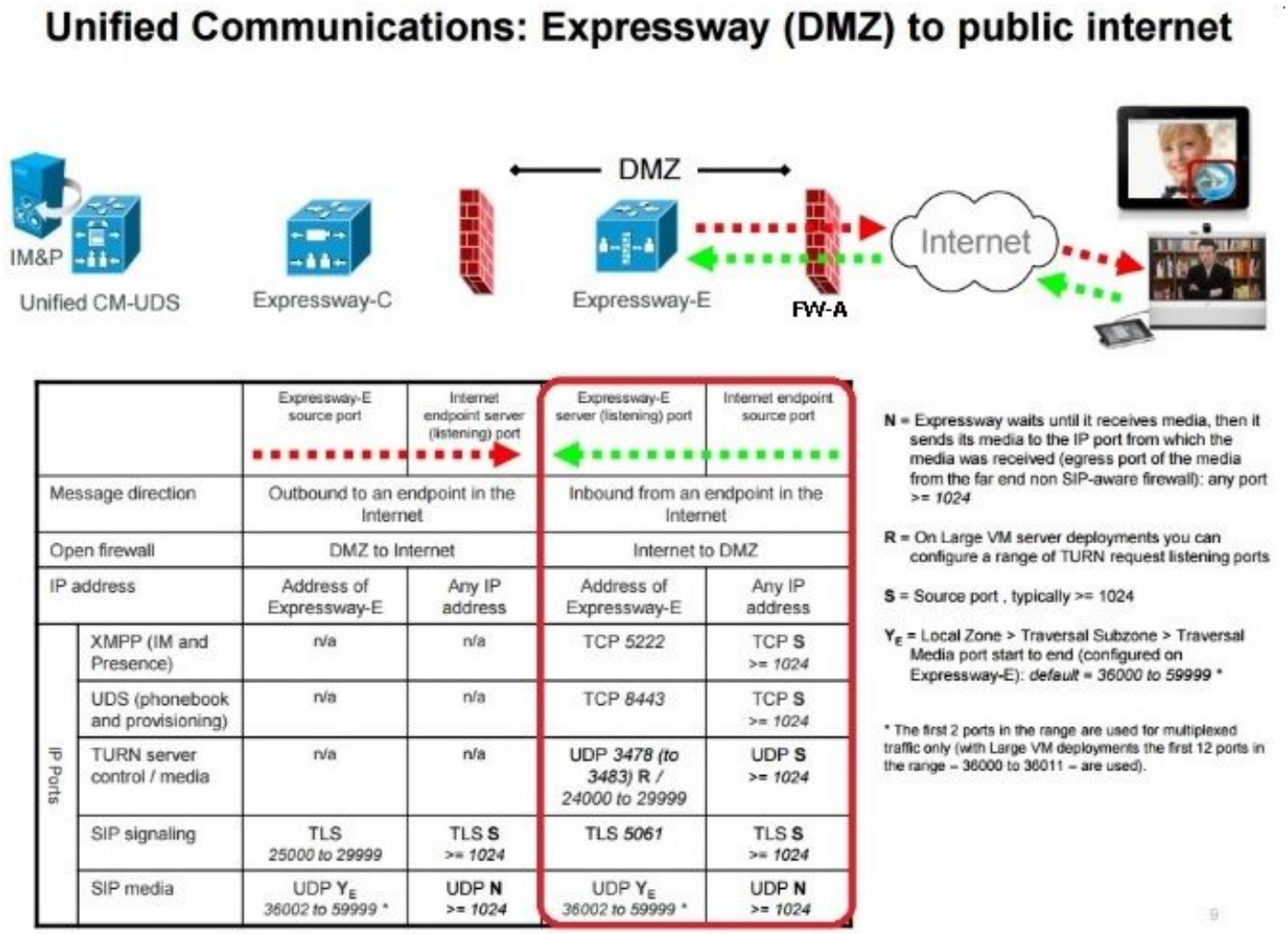
```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

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

Étape 2. La configuration de la liste de contrôle d'accès (ACL) autorise les ports requis d'Internet à l'Expressway-E.

Selon la communication unifiée : La liste des ports TCP et UDP que l'Expressway-E doit autoriser dans FW-A est présentée dans la documentation Internet publique d'Expressway (DMZ), comme

illustré dans l'image :



Il s'agit de la configuration de la liste de contrôle d'accès requise en entrée dans l'interface FW-A externe.

Pour ASA versions 8.3 et ultérieures :

```
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
```

Pour ASA versions 8.2 et antérieures :

```
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
```

Configuration FW-B

Comme expliqué dans la section Informations générales de ce document, FW B peut nécessiter une configuration NAT ou PAT dynamique pour permettre la traduction du sous-réseau interne 10.0.30.0/24 en adresse IP 10.0.20.1 lorsqu'il va à l'interface externe du FW B.

Pour ASA versions 8.3 et ultérieures :

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

Pour ASA versions 8.2 et antérieures :

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

> **Conseil** : assurez-vous que tous les ports TCP et UDP requis permettent à Expressway-C de fonctionner correctement et sont ouverts dans le pare-feu B, comme spécifié dans ce document Cisco : [Utilisation des ports IP de Cisco Expressway pour la traversée de pare-feu]

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Packet Tracer peut être utilisé sur l'ASA pour confirmer que la traduction NAT statique Expressway-E fonctionne selon les besoins.

Packet Tracer pour tester 64.100.0.10 sur TCP/5222

```
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
```

Packet Tracer pour tester 64.100.0.10 sur TCP/8443

```
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
```

Packet Tracer pour tester 64.100.0.10 sur TCP/5061

```
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
```

Packet Tracer pour tester 64.100.0.10 à UDP/24000

```
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
```

Packet Tracer pour tester 64.100.0.10 à UDP/36002

```
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
```

Dépannage

Étape 1. Comparer les captures de paquets.

Les captures de paquets peuvent être prises à la fois sur les interfaces d'entrée et de sortie ASA.

```
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
```

Captures de paquets pour 64.100.0.10 sur TCP/5222 :

```
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
```

Captures de paquets pour 64.100.0.10 sur TCP/5061 :

```
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
```

Étape 2. Inspecter les captures de paquets par le chemin de sécurité accéléré (ASP)

Les pertes de paquets par un ASA sont capturées par la capture ASP ASA. L'option **all**, capture toutes les raisons possibles pour lesquelles l'ASA a abandonné un paquet. Cela peut être réduit s'il y a une raison suspecte. Pour une liste des raisons utilisées par un ASA pour classer ces pertes, exécutez la commande **show asp drop.**

```
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
```

> **Astuce** : La capture ASA ASP est utilisée dans ce scénario pour confirmer si l'ASA abandonne des paquets en raison d'une liste de contrôle d'accès manquée ou d'une configuration NAT, ce qui nécessiterait d'ouvrir un port TCP ou UDP spécifique pour l'Expressway-E.

Astuce : La taille de tampon par défaut de chaque capture ASA est de 512 Ko. Si l'ASA abandonne trop de paquets, la mémoire tampon est rapidement remplie. La taille du tampon peut être augmentée avec l'option **tampon**.

Recommandations

Assurez-vous que l'inspection SIP/H.323 est complètement désactivée sur les pare-feu concernés.

Il est fortement recommandé de désactiver l'inspection SIP et H.323 sur les pare-feu qui gèrent le trafic réseau à destination ou en provenance d'un Expressway-E. Lorsqu'elle est activée, l'inspection SIP/H.323 affecte souvent négativement la fonctionnalité de traversée NAT/pare-feu intégrée d'Expressway.

Voici un exemple de la façon de désactiver les inspections SIP et H.323 sur l'ASA :

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

Mise en oeuvre alternative de VCS Expressway

Une autre solution pour mettre en oeuvre l'Expressway-E avec deux interfaces réseau/deux cartes réseau consiste à mettre en oeuvre l'Expressway-E, mais avec une seule carte réseau et une configuration NAT réfléchissante sur les pare-feu. Le lien suivant présente plus de détails sur cette mise en oeuvre Configurer la réflexion NAT sur l'ASA pour les périphériques TelePresence VCS Expressway.

Astuce : La mise en oeuvre recommandée pour VCS Expressway est la mise en oeuvre de VCS Expressway double interface réseau/double carte réseau décrite dans ce document.

Informations connexes

- Configuration de la réflexion NAT sur l'ASA pour les périphériques VCS Expressway TelePresence
- Support et documentation techniques - Cisco Systems
- Cisco Expressway-E et Expressway-C - Guide de déploiement de la configuration de base
- Placement d'un Cisco VCS Expressway dans une zone démilitarisée (DMZ) plutôt que sur l'Internet public
- Utilisation des ports IP Cisco Expressway pour la traversée de pare-feu