La configuration NAT et les recommandations ASA pour Expressway-e conjuguent implémentation d'interfaces réseau

Contenu

Introduction

Ce document décrit comment implémenter la configuration de Traduction d'adresses de réseau (NAT) exigée dans l'appliance de sécurité adaptable Cisco (ASA) pour la double implémentation d'interfaces réseau d'Expressway-e.

Conseil : Ce déploiement est l'option recommandée pour l'implémentation d'Expressway-e, plutôt que l'implémentation Simple-NIC avec la réflexion NAT.

Conditions préalables

Exigences

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 d'Expressway-C

Composants utilisés

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

- Cisco ASA 5500 et appliances de gamme 5500-X qui exécutent la version de logiciel 8.0 et plus tard.
- Version X8.0 de Cisco Expressway et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Note: Par le document entier, les périphériques d'autoroute désigné sous le nom d'Expressway-e et d'Expressway-C. Cependant, la même configuration s'applique pour le serveur de communication vidéo (VCS) Expressway et des périphériques de contrôle de VCS.

Informations générales

Par conception, Cisco Expressway-e peut être placé dans une zone démilitarisée (DMZ) ou avec une interface d'Internet-revêtement, alors qu'il peut communiquer avec Cisco Expressway-C dans un réseau privé. Quand Cisco Expressway-e est placé dans un DMZ, ce sont les allocations complémentaires :

- Dans le scénario le plus commun, Cisco Expressway-e est géré par le réseau privé. Quand Cisco Expressway-e est dans un DMZ, un Pare-feu (externe) de périmètre peut être utilisé pour bloquer l'accès non désiré à Expressway des réseaux externes par l'intermédiaire de l'hypertexte Transfer Protocol des demandes sécurisées (HTTPS) ou de Protocole Secure Shell (SSH).

- Si le DMZ ne permet pas les liaisons directes entre interne et les réseaux externes, des serveurs dédiés sont exigés pour traiter le trafic qui traverse le DMZ. Cisco Expressway peut agir en tant que serveur proxy pour le Protocole SIP (Session Initiation Protocol) et/ou H.323

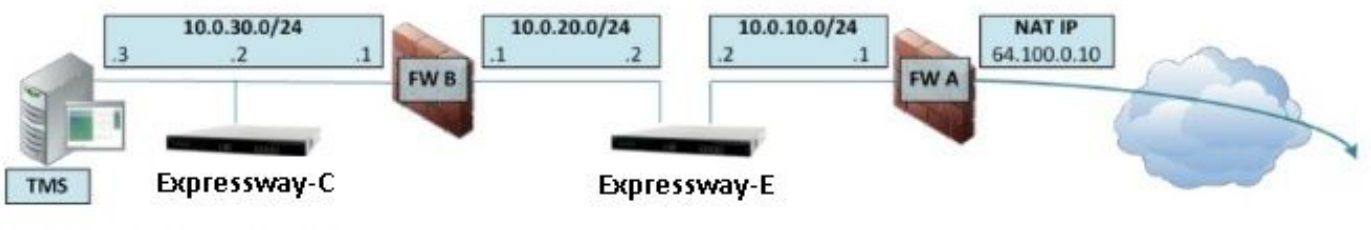
exprimer et le trafic visuel. Dans ce cas, vous pouvez utiliser la double option d'interfaces réseau qui permet à Cisco Expressway pour avoir deux adresses IP différentes, une pour le trafic à/de le pare-feu externe, et une pour le trafic à/de le Pare-feu interne.

- Cette installation empêche les liaisons directes du réseau externe au réseau interne. Ceci améliore la combinaison de Sécurité de réseau interne.

Conseil : Afin d'obtenir plus de détails au sujet de l'implémentation de TelePresence, référez-vous à Cisco Expressway-e et à Expressway-C - guide de déploiement de configuration de base et placement d'un VCS Expressway de Cisco dans un DMZ plutôt que dans l'Internet public.

C d'Expressway et E - Doubles interfaces réseau/double implémentation NIC

Cette image affiche un déploiement d'exemple pour Expressway-e avec de doubles interfaces réseau et NAT statique. Expressway-C agit en tant que client de traversée. Il y a deux Pare-feu (FW A et FWB). Typiquement, dans cette configuration DMZ, FW A ne peut pas conduire le trafic à FW B, et des périphériques tels qu'Expressway-e sont exigés pour valider et expédier le trafic du sous-réseau FW A au sous-réseau FW b (et vice versa).



Ce déploiement se compose de ces composants.

Sous-réseau DMZ 1 – 10.0.10.0/24

- Interface interne FW A – 10.0.10.1
- Interface d'Expressway-e LAN2 – 10.0.10.2

Sous-réseau DMZ 2 – 10.0.20.0/24

- Interface externe FW B – 10.0.20.1
- Interface d'Expressway-e LAN1 – 10.0.20.2

Sous-réseau LAN – 10.0.30.0/24

- Interface interne FW B – 10.0.30.1
- Interface d'Expressway-C LAN1 – 10.0.30.2
- Interface de réseau serveur de la suite logicielle de gestion Cisco TelePresence (TMS) – 10.0.30.3

Particularités de cette implémentation :

- FW A est le Pare-feu externe ou de périmètre ; il est configuré avec IP NAT (IP de public) de 64.100.0.10 qui est statiquement traduit à 10.0.10.2 (l'interface d'Expressway-e LAN2)
- FW B est le Pare-feu interne
- Expressway-e LAN1 a le mode NAT statique désactivé

- Expressway-e LAN2 a le mode NAT statique activé avec l'adresse NAT statique 64.100.0.10
- Expressway-C a une zone de client de traversée qui indique 10.0.20.2 (l'interface d'Expressway-e LAN1)
- Il n'y a aucun routage entre 10.0.20.0/24 et 10.0.10.0/24 sous-réseaux. Expressway-e jette un pont sur ces sous-réseaux et agit en tant que support de proxy pour la signalisation SIP/H.323 et le Protocole RTP (Real-Time Transport Protocol)/Control Protocol de RTP (RTCP).
- Cisco TMS a Expressway-e configuré avec l'adresse IP 10.0.20.2

Conditions requises/limites

Sous-réseaux non-recouverts

Si Expressway-e est configuré pour utiliser les deux interfaces de RÉSEAU LOCAL, la nécessité des interfaces LAN1 et LAN2 se trouvent dans des sous-réseaux non-superposés pour s'assurer que le trafic est envoyé à l'interface appropriée.

Groupement

En groupant des périphériques d'Expressway avec l'option avancée de réseau configurée, chaque pair de batterie doit être configuré avec sa propre adresse de l'interface LAN1. En outre, le groupement doit être configuré sur une interface qui n'a pas le mode NAT statique activé. Par conséquent, il est recommandé que vous utilisez le LAN2 comme interface externe, sur laquelle vous pouvez appliquer et configurer NAT statique le cas échéant.

Paramètres d'interface externes de RÉSEAU LOCAL

Les configurations externes de configuration d'interface de RÉSEAU LOCAL sur le contrôle de page de configuration IP que l'interface réseau utilise transversal utilisant des relais autour de NAT (TOUR). Dans une configuration d'Expressway-e de double interface réseau, ceci est normalement placé à l'interface externe de RÉSEAU LOCAL d'Expressway-e.

routes statique

Expressway-e doit être configuré avec une adresse de passerelle par défaut de 10.0.10.1 pour ce scénario. Ceci signifie que tout le trafic envoyé par l'intermédiaire du LAN2, par défaut, est envoyé à l'adresse IP 10.0.10.1.

Si FW B traduit le trafic envoyé du sous-réseau 10.0.30.0/24 à l'interface d'Expressway-e LAN1 (par exemple, le trafic de client de traversée d'Expressway-C ou le trafic d'administration de serveurs TMS), ce trafic apparaît pendant qu'il provient l'interface externe FWB (10.0.20.1) comme elle atteint Expressway-e LAN1. Expressway-e peut alors répondre à ce trafic par l'intermédiaire de son interface LAN1 puisque la source apparente de ce trafic se trouve sur le même sous-réseau.

Si NAT est activé sur FW B, le trafic envoyé d'Expressway-C à Expressway-e LAN1 affiche pendant qu'il provient 10.0.30.2. Si Expressway n'a pas une artère 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) du LAN2, car il ne se rend pas compte que le sous-réseau 10.0.30.0/24 se trouve derrière le Pare-feu interne (FW B). Par conséquent, une artère statique doit être ajoutée,

exécutent la commande de **RouteAdd** CLI de **xCommand** par une session de SSH à Expressway.

Dans cet exemple particulier, Expressway-e doit savoir qu'il peut atteindre le sous-réseau 10.0.30.0/24 derrière FW B, qui est accessible par l'intermédiaire de l'interface LAN1. Pour accomplir ceci, exécutez la commande :

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

> **Note**: La configuration de route statique peut être appliquée par le GUI d'Expressway-e aussi bien que sectionner le **système/réseau > les interfaces/artères de charge statique**.

Dans cet exemple, le paramètre d'interface peut également être placé à l'**automatique** car l'adresse de passerelle (10.0.20.1) est seulement accessible par l'intermédiaire du LAN1.

Si NAT n'est pas activé sur FW B et besoins d'Expressway-e de communiquer avec des périphériques dans les sous-réseaux (autre que 10.0.30.0/24) qui sont également situés derrière FW B, les artères statiques doit être ajouté pour ces périphériques/sous-réseaux.

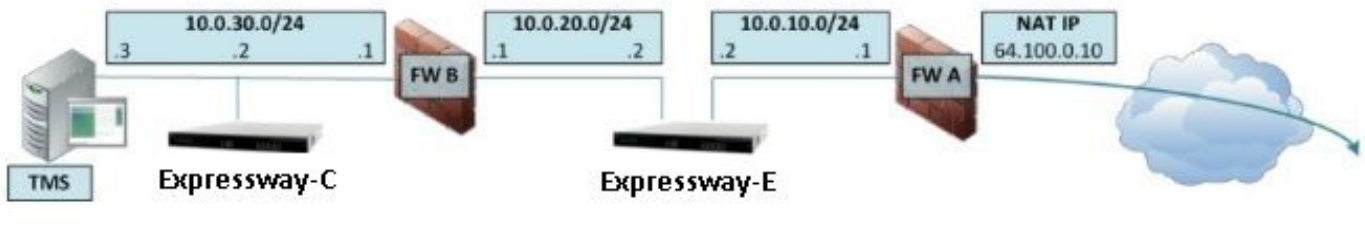
> **Note**: Ceci inclut des connexions de SSH et HTTPS des postes de travail de Gestion de réseau ou pour des services réseau comme le NTP, les DN, le LDAP/AD, ou le Syslog.

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

Configuration

Cette section décrit comment configurer le NAT statique exigé pour la double implémentation d'interface réseau d'Expressway-e sur l'ASA. Quelques recommandations modulaires supplémentaires de configuration du cadre de stratégie ASA (MPF) sont incluses pour traiter le trafic SIP/H323.

C d'Expressway et E - Doubles interfaces réseau/double implémentation NIC



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

Adresse IP d'Expressway-C : 10.0.30.2/24

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

Adresses IP d'Expressway-e :

Sur le LAN2 : 10.0.10.2/24

Sur le LAN1 : 10.0.20.2/24

Passerelle par défaut d'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 Expressway-e.

Comme expliqué dans la section Informations générales de ce document, le FW-A a une traduction NAT statique pour permettre à Expressway-e pour être accessible de l'Internet avec l'adresse IP publique 64.100.0.10. Est NATed à l'adresse IP 10.0.10.2/24 d'Expressway-e LAN2. Ce dite, ceci est la configuration NAT statique exigée FW-A.

Pour des versions 8.3 et ultérieures ASA :

```
! 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** : Quand vous vous appliquez le PAT statique vous commande reçoivent ce message d'erreur sur l'interface de ligne de commande ASA, « **ERREUR : Incapable NAT de réserver des ports »**. Après ceci, poursuivez pour effacer les entrées de xlate sur l'ASA, pour ceci, exécutent la commande **x.x.x.x clearxlatelocal, le fromwhere** x.x.x.x correspond à l'ASA en dehors de l'adresse IP. Cette commande efface toutes les traductions associées avec cette adresse IP, l'exécutent avec prudence dans les environnements de production.

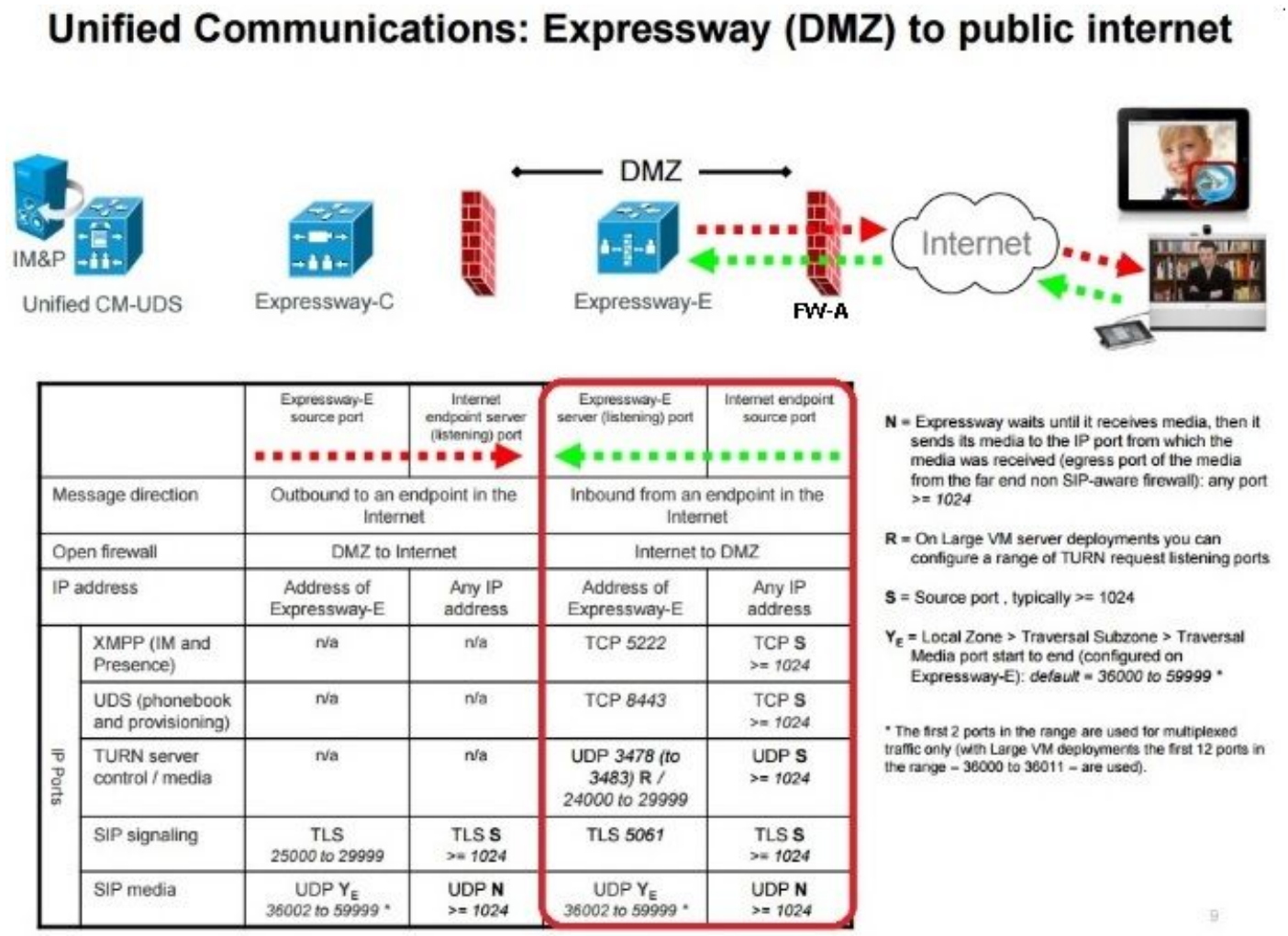
Pour des versions 8.2 et antérieures ASA :

```
! 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 liste de contrôle d'accès (ACL) permet les ports exigés de l'Internet à Expressway-e.

Selon la transmission unifiée : Expressway (DMZ) à la documentation d'Internet public, la liste de ports de TCP et UDP des lesquels Expressway-e exige de permettre dans FW-A, sont suivant les indications de l'image :



		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).

C'est la configuration d'ACL exigée comme d'arrivée dans le FW-A en dehors de l'interface.

Pour des versions 8.3 et ultérieures ASA :

```
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 des versions 8.2 et antérieures ASA :

```
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 exiger d'un NAT ou d'une configuration PAT dynamique de permettre le sous-réseau interne 10.0.30.0/24 à traduire à l'adresse IP 10.0.20.1 quand il va à l'interface extérieure du FW B.

Pour des versions 8.3 et ultérieures ASA :

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

Pour des versions 8.2 et antérieures ASA :

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

> **Conseil** : Soyez sûr que tous les ports exigés de TCP et UDP permettent à Expressway-C pour fonctionner correctement et sont ouverts dans le FW B, juste comme spécifié dans ce document Cisco : Utilisation de port IP de Cisco Expressway pour la traversée de Pare-feu

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Packet Tracer peut être utilisé sur l'ASA pour confirmer que les travaux de traduction NAT statique d'Expressway-e au besoin.

Packet Tracer pour tester 64.100.0.10 à 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 à 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 à 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
```

Dépanner

Étape 1. Comparez les captures de paquet.

Des captures de paquet peuvent être prises au d'entrée et aux interfaces 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 paquet pour 64.100.0.10 à 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 paquet pour 64.100.0.10 à 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. Examinez les captures accélérées de paquet de baisse de chemin de Sécurité (ASP).

Des pertes de paquets par une ASA sont capturées par la capture d'ASP ASA. **Toute l'**option, capture tous les possibles raison pourquoi l'ASA a relâché un paquet. Ceci peut être rétréci vers le bas s'il y a n'importe quelle raison suspectée. Pour une liste de raisons qu'une ASA l'utilise pour classifier ces baisses, exécutez la **baisse d'asp d'exposition de** commande**.**

```
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
```

> **Conseil** : La capture d'ASP ASA est utilisée dans ce scénario pour confirmer si les paquets de baisses ASA dus à un ACL manqué ou à une configuration NAT, qui exigeraient d'ouvrir un TCP ou un port UDP spécifique pour Expressway-e.

Conseil : La taille de mémoire tampon par défaut pour chaque capture ASA est 512 KO. Si trop de paquets sont lâchés par l'ASA, la mémoire tampon est remplie rapidement. La taille de mémoire tampon peut être augmentée avec l'option de **mémoire tampon**.

Recommandations

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

Il est fortement recommandé pour désactiver le SIP et H.323 l'inspection sur les Pare-feu qui traitent le trafic réseau à ou d'Expressway-e. Une fois activée, l'inspection SIP/H.323 s'avère fréquemment pour affecter négativement la fonctionnalité intégrée de traversée d'Expressway firewall/NAT.

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

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

Implémentation alternative d'Expressway de VCS

Une solution alternative pour implémenter Expressway-e avec de doubles interfaces réseau/double NIC est d'implémenter Expressway-e mais avec un NIC simple et une configuration NAT de réflexion sur les Pare-feu. Le prochain lien affiche que d'autres détails au sujet de cette implémentation configurent la réflexion NAT sur l'ASA pour des périphériques de TelePresence d'Expressway de VCS.

Conseil : L'implémentation recommandée pour le VCS Expressway est les doubles interfaces réseau/double implémentation d'Expressway de VCS NIC décrite dans ce document.

Informations connexes

- Configurez la réflexion NAT sur l'ASA pour des périphériques de TelePresence d'Expressway de VCS
- **Support et documentation techniques - Cisco Systems**
- Cisco Expressway-e et Expressway-C - Guide de déploiement de configuration de base
- Plaçant un VCS Expressway de Cisco dans un DMZ plutôt que dans l'Internet public
- Utilisation de port IP de Cisco Expressway pour la traversée de Pare-feu