La configuration NAT et les recommandations ASA pour l'autoroute-e et l'autoroute-C 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 de doubles interfaces réseau d'autoroute-e et d'autoroute-C/double implémentation du contrôleur d'interface réseau (NIC).

Ce déploiement est une option recommandée pour mettre en application des périphériques d'autoroute-e et d'autoroute-C plutôt qu'utilisant la réflexion NAT.

Contribué par le chrétien Hernandez et Cesar Lopez Zamarripa, ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- NAT de base et configuration de Cisco ASA
- Configuration de base d'autoroute-e et d'autoroute-C de Cisco

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 8.x et ultérieures d'autoroute urbaine de Cisco.

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> Remarque: Par le document entier, des périphériques d'autoroute sont référés comme autoroute-e et autoroute-C. Cependant, la même configuration applique aux périphériques d'autoroute du serveur de communication vidéo (VCS) et de contrôle VCS.

Informations générales

Par conception, l'autoroute-e de Cisco peut être placée ou dans une zone démilitarisée (DMZ) ou faisant face au réseau public (Internet) et il peut avec une autoroute-C de Cisco dans un réseau privé. Cependant, quand l'autoroute-e de Cisco est mise dans un DMZ, ce sont les allocations complémentaires.

- Dans le scénario le plus commun, l'autoroute-e de Cisco est gérée du réseau privé. En plaçant l'autoroute-e de Cisco dans un DMZ, un Pare-feu (externe) permietral peut être utilisé pour bloquer l'accès non désiré à l'autoroute telle que (hypertexte Transfer Protocol sécurisé) des demandes HTTPS ou de Protocole Secure Shell (SSH).

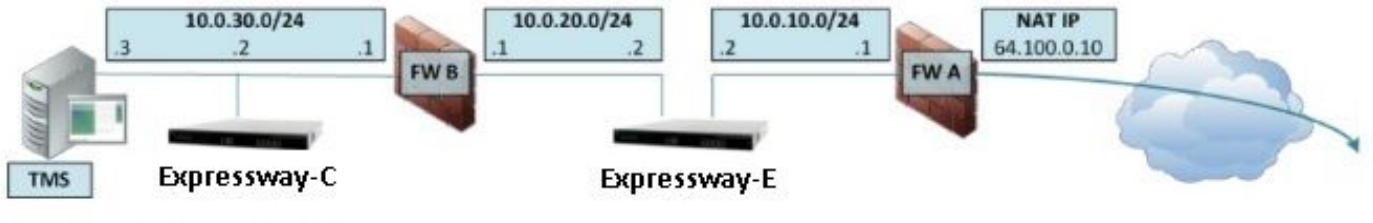
- Si le DMZ ne permet pas les liaisons directes entre interne et les réseaux externes, des serveurs dédiés sont exigés pour traiter le trafic qui traverse le DMZ. L'autoroute de Cisco peut agir en tant que ce serveur pour le Protocole SIP (Session Initiation Protocol) et/ou H.323 exprimer et le trafic visuel. Dans ce cas, vous pouvez utiliser la double option d'interfaces réseau qui permet à l'autoroute de Cisco 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 la transmission externe pour se connecter directement 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 l'autoroute-e de Cisco et à l'autoroute-C - guide de déploiement de configuration de base et placement d'une autoroute de Cisco VCS dans un DMZ plutôt que dans l'Internet public.

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

Ce diagramme affiche un déploiement d'exemple pour une autoroute-e avec de doubles interfaces réseau et NAT statique. Une autoroute-C agissant en tant que client de traversée et 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 que l'autoroute-e de double interface 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 de l'autoroute-e LAN2 – 10.0.10.2

Sous-réseau DMZ 2 – 10.0.20.0/24

- Interface externe FW B – 10.0.20.1
- Interface de l'autoroute-e LAN1 – 10.0.20.2

Sous-réseau LAN – 10.0.30.0/24

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

- FW A est le Pare-feu externe ou permitetral ; 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'autoroute-e LAN2)

- FW B est le Pare-feu interne

- L'autoroute-e LAN1 a le mode NAT statique désactivé

- L'autoroute-e LAN2 a le mode NAT statique activé avec l'adresse NAT statique 64.100.0.10

- L'autoroute-C a une zone de client de traversée qui indique 10.0.20.2 (l'interface d'autoroute-e LAN1)

- Il n'y a aucun routage entre 10.0.20.0/24 et 10.0.10.0/24 sous-réseaux. L'autoroute-e pont 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 l'autoroute-e configurée avec l'adresse IP 10.0.20.2

Conditions requises/limites

Sous-réseaux non-recouverts

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

Groupement

Quand les périphériques de groupement d'autoroute ont l'option **avancée de réseau** configurée, chaque pair de batterie a besoin de 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, et le LAN2 est utilisé comme interface 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'autoroute-e de double interface réseau, ceci peut normalement être placé à l'interface externe de RÉSEAU LOCAL d'autoroute-e.

Routes statique

L'autoroute-e doit être configurée 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 de l'autoroute-e LAN1 (par exemple, le trafic de client de traversée d'autoroute-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 l'autoroute-e LAN1. L'autoroute-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 FW B n'est pas faire NAT, le trafic envoyé de l'autoroute-C à l'autoroute-e LAN1 affiche pendant qu'il provient 10.0.30.2. Si l'autoroute n'a pas une artère statique ajoutée pour le sous-réseau 10.0.30.0/24, elle 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, utilisant la commande de **RouteAdd** CLI de **xCommand** par une session de SSH à l'autoroute.

Dans cet exemple particulier, l'autoroute-e doit savoir qu'elle peut atteindre le sous-réseau 10.0.30.0/24 derrière FW B, qui est accessible par l'intermédiaire de l'interface LAN1. Ce fait utilisant cette commande.

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

> Remarque: La configuration de route statique peut être appliquée par l'interface utilisateur graphique d'autoroute-e (GUI) dans le **système de** section**/réseau > les interfaces/artères statiques**.

> Remarque: Il est recommandé pour éviter l'utilisation de NAT dans FW-B pour l'autoroute-C. Ceci permet à l'autoroute-e pour atteindre l'autoroute-C avec sa vraie adresse IP 10.0.30.2. Ceci évite certaines questions de services de téléphonie. On l'a confirmé que la configuration NAT pour l'autoroute-C peut causer des périphériques de mobile et d'Accès à distance (MRA) de ne pas être soulevée.

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.

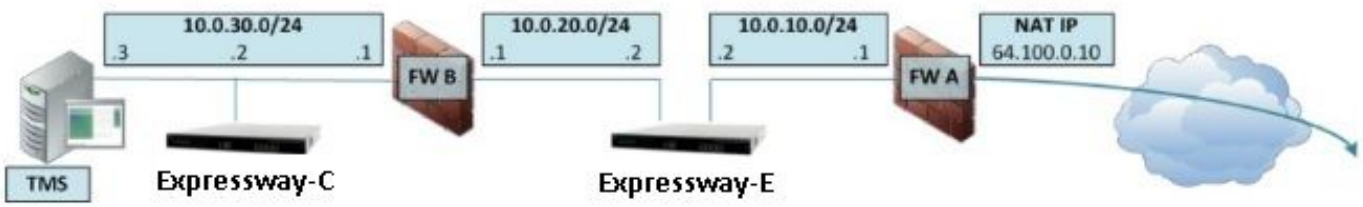
Si FW B n'est pas faire NAT et l'autoroute-e doit communiquer avec des périphériques dans les sous-réseaux autres que 10.0.30.0/24 qui sont également situés derrière FW B tel que des connexions de SSH et HTTPS des postes de travail de ce réseau ou pour des services réseau comme le NTP, les DN, le LDAP/AD et/ou le Sylog, des artères statiques doivent être ajoutées pour ces périphériques/sous-réseaux.

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

Configuration

Cette section décrit comment configurer le NAT statique exigé pour de doubles interfaces réseau d'autoroute-C et d'autoroute-e/double implémentation NIC sur l'ASA. En outre, quelques recommandations modulaires de configuration du cadre de stratégie ASA (MPF) pour traiter le trafic SIP/H323 par l'ASA.

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



Dans cet exemple l'assigment d'adresse IP sont le prochain.

IP address:10.0.30.2/24 d'autoroute-C

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

Adresses IP d'autoroute-e

Sur le LAN2 : 10.0.10.2/24

Sur le LAN1 : 10.0.20.2/24

Passerelle par défaut d'autoroute-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'autoroute-e

Comme expliqué dans la **section Informations générales de** ce document, le FW-A a une traduction NAT statique pour permettre à l'autoroute-e pour être accessible de l'Internet utilisant l'adresse IP publique 64.100.0.10. Est NATed à l'adresse IP 10.0.10.2/24 de l'autoroute-e LAN2, ce étant indiqué, 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
```

> Remarque: Si en essayant d'appliquer le PAT statique vous commande **ERREUR** reçoivent message d'erreur **« : Incapables NAT de réserver les ports** sur l'interface de ligne de commande ASA, alors, effacent les entrées de xlate avec les **gens du pays x.x.x.x de clear xlate de** commande **où** x.x.x.x correspond à l'ASA en dehors de l'adresse IP. **Cette commande efface toutes les traductions associées à cet IP ainsi dans les environnements de production, l'exécutent avec prudence.**

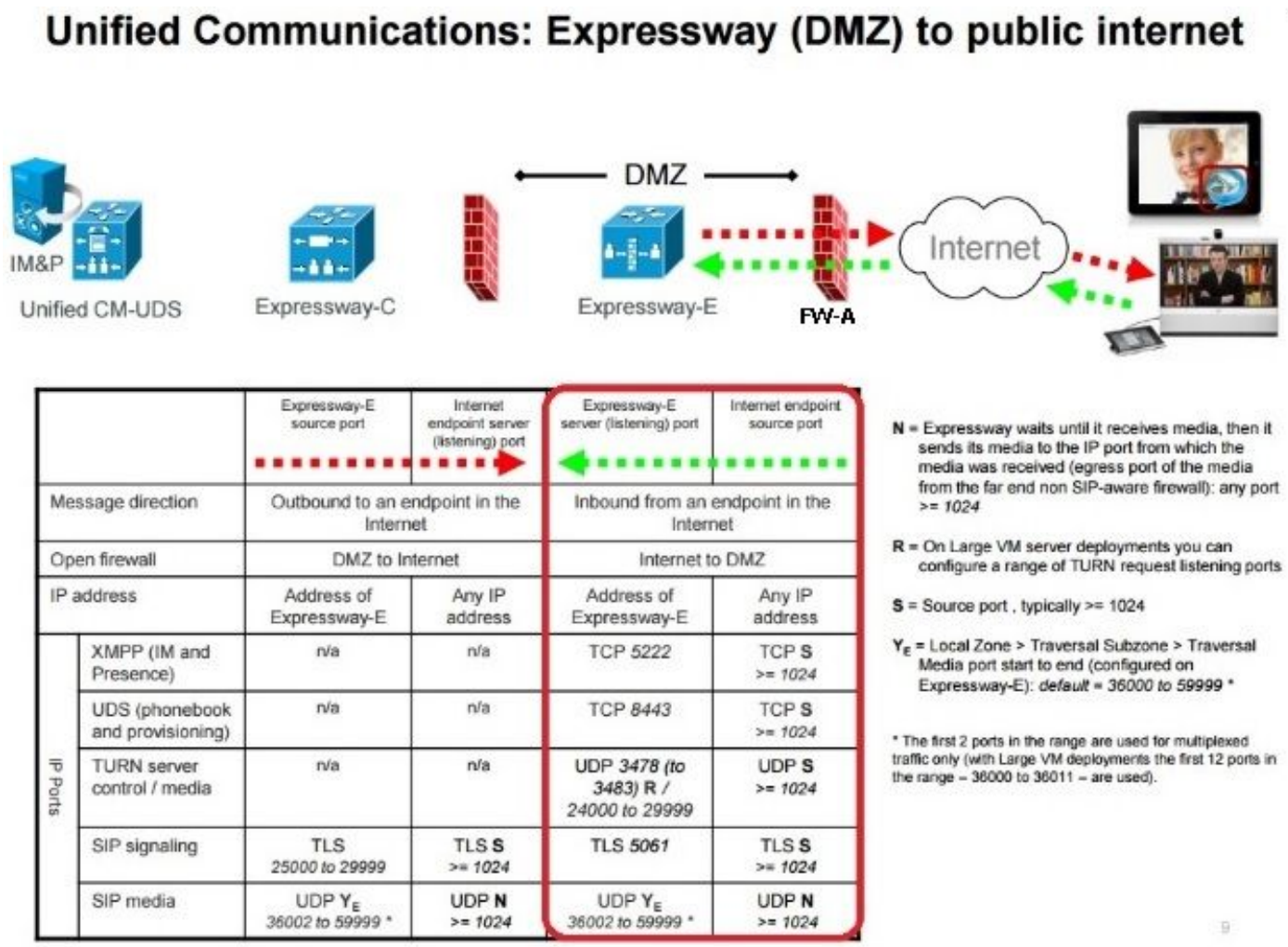
Pour des versions 8.2 et antérieures ASA :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample 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. Configuration de liste de contrôle d'accès (ACL) pour permettre les ports requis de l'Internet à l'autoroute-e

Selon la *transmission unifiée : L'autoroute (DMZ) à la* documentation d'*Internet public*, ceci

est liste de TCP et de ports UDP des lesquels l'autoroute-e exige pour être permis dans FW-A :



		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
```

> Remarque: Il est fortement recommandé pour désactiver le SIP et H.323 des inspections sur le trafic réseau de transport de Pare-feu à ou d'une autoroute-e, comme une fois activées, ceci s'avère fréquemment pour affecter négativement la fonctionnalité intégrée de traversée de l'autoroute-e firewall/NAT.

Configuration FW-B.

Comme expliqué dans la **section Informations générales de** ce document, FW B exige juste 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 en sortant 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
```

> Remarque: Il est fortement recommandé pour désactiver le SIP et H.323 les inspections sur le trafic réseau de transport de Pare-feu à ou d'une autoroute-e, as, une fois activé ceci s'avère fréquemment affecter négativement la fonctionnalité intégrée de traversée de l'autoroute-e firewall/NAT.

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

Vérifiez

Packet Tracer peut être utilisé sur l'ASA pour confirmer que les travaux de traduction NAT statique d'autoroute-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
```

Dépannez

Étape 1. 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. Captures accélérées de paquet de baisse de chemin de Sécurité (ASP).

Les captures de baisse d'ASP ASA prennent les paquets que l'ASA a décidé de relâcher. L'option **toute** 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 supected. Pour une liste des raisons une utilisation ASA de classifier ceci chute, la **baisse d'asp d'exposition de** commande peut être utilisée.

La mémoire tampon par défaut pour chaque capture ASA est 512 KO. S'il y a beaucoup de paquets relâché par cette ASA, cette mémoire tampon sera très rapide rempli. Cette mémoire tampon peut être incrémentée utilisant la **mémoire tampon d'**option.

```
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** : Il est très utile dans ce scénario confirmer cette capture d'ASP ASA si les paquets de baisses ASA dus à un ACL manquant ou NAT pour ouvrir un TCP ou un port UDP spécifique pour l'autoroute-e.

Recommandations

Assurez que les inspections SIP/H.323 sont complètement désactivées dans les

Pare-feu impliqués

Il est fortement recommandé pour désactiver le SIP et H.323 les inspections sur les Pare-feu qui traitent le trafic réseau à ou d'une autoroute-e, as, une fois activés ceci s'avèrent fréquemment affecter négativement la fonctionnalité intégrée de traversée de l'autoroute 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
```

Solution alternative

Une solution alternative au lieu de mettre en application l'autoroute-e utilisant de doubles interfaces réseau/double NIC, est d'implémenter l'autoroute-e utilisant une configuration NAT de réflexion dans les Pare-feu, des détails d'expositions de ce lien plus loin au sujet de ce scénario.

ASA : Configuration NAT de réflexion pour les réalisations d'autoroute VCS.

Cependant, car on lui a mentionné au début de ce document, la double configuration réseau est recommandée au-dessus de la réflexion NAT.

Liens connexes

Autoroute-e et autoroute-C de Cisco - Guide de déploiement de configuration de base

Plaçant une autoroute de Cisco VCS dans un DMZ plutôt que dans l'Internet public

Utilisation de port IP d'autoroute de Cisco pour la traversée de Pare-feu