Configurer la réflexion NAT sur l'ASA pour les périphériques VCS Expressway TelePresence

Contenu

Introduction

Ce document décrit comment mettre en oeuvre une configuration de réflexion NAT (Network Address Translation) sur les appliances de sécurité adaptatives Cisco pour des scénarios Cisco TelePresence spéciaux qui nécessitent ce type de configuration NAT sur le pare-feu.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration NAT de base de Cisco ASA (Adaptive Security Appliance).
- Configuration de base de Cisco TelePresence Video Communication Server (VCS) Control et VCS Expressway.

Note: Ce document est destiné à être utilisé uniquement lorsque la méthode de déploiement recommandée d'un VCS-Expressway ou d'Expressway-Edge avec les deux interfaces NIC dans des DMZ différentes ne peut pas être utilisée. Pour plus d'informations sur le déploiement recommandé à l'aide de cartes réseau doubles, consultez le lien suivant à la page 60 : Guide de déploiement de Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)

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 8.3 et ultérieures du logiciel.
- Cisco VCS version X8.x 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. If your network is live, make sure that you understand the potential impact of any command.

Remarque : Dans l'ensemble du document, les périphériques VCS sont appelés VCS Expressway et VCS Control. Cependant, la même configuration s'applique aux périphériques Expressway-E et Expressway-C.

Informations générales

Selon la documentation de Cisco TelePresence, il existe deux types de scénarios TelePresence dans lesquels la configuration de réflexion NAT est requise sur les pare-feu afin de permettre au contrôle VCS de communiquer avec le VCS Expressway via l'adresse IP publique VCS Expressway.

Le premier scénario implique un sous-réseau DMZ (zone démilitarisée) unique qui utilise une interface LAN VCS Expressway unique, et le second scénario implique une DMZ FW à 3 ports qui utilise une interface LAN VCS Expressway unique.

Astuce : Pour obtenir plus de détails sur la mise en oeuvre de TelePresence, reportez-vous au guide de déploiement Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway).

Topologies Cisco non recommandées pour la mise en oeuvre de VCS C et E

Il est important de noter que les topologies suivantes ne sont PAS recommandées par Cisco. La méthodologie de déploiement recommandée pour une périphérie VCS Expressway ou

Expressway consiste à utiliser deux DMZ différentes avec l'Expressway ayant une carte réseau dans chacune des DMZ. Ce guide est destiné aux environnements où la méthode de déploiement recommandée ne peut pas être utilisée.

DMZ à sous-réseau unique avec interface LAN VCS Expressway unique

Dans ce scénario, FW A peut acheminer le trafic vers FW B (et vice versa). Le VCS Expressway permet le trafic vidéo de passer par FW B sans réduire le flux de trafic sur FW B de l'extérieur vers les interfaces internes. L'Expressway VCS gère également la traversée de pare-feu sur son côté public.

Voici un exemple de ce scénario :

Ce déploiement utilise les composants suivants :

- Une DMZ de sous-réseau unique (10.0.10.0/24) qui contient :
  Interface interne de FW A (10.0.10.1)L'interface externe de FW B (10.0.10.2)Interface LAN1 du VCS Expressway (10.0.10.3)
- Sous-réseau LAN (10.0.30.0/24) contenant :
  Interface interne de FW B (10.0.30.1)Interface LAN1 du contrôle VCS (10.0.30.2)Interface réseau du serveur de gestion Cisco TelePresence (TMS) (10.0.30.3)

Une NAT statique un-à-un a été configurée sur le pare-feu A, qui exécute la NAT pour l'adresse publique 64.100.0.10 à l'adresse IP LAN1 du VCS Expressway. Le mode NAT statique a été activé pour l'interface LAN1 sur VCS Expressway, avec l'adresse IP NAT statique 64.100.0.10.

> **Note**: Vous devez entrer le nom de domaine complet (FQDN) de VCS Expressway sur la zone de client de traversée sécurisée VCS Control (adresse homologue) comme il est vu de l'extérieur du réseau. En mode NAT statique, VCS Expressway demande que la signalisation entrante et le trafic multimédia soient envoyés à son nom de domaine complet externe plutôt qu'à son nom privé. Cela signifie également que le FW externe doit autoriser le trafic du contrôle VCS vers le FQDN externe VCS Expressway. Cette fonction est appelée réflexion NAT et peut ne pas être prise en charge par tous les types de pare-feu.

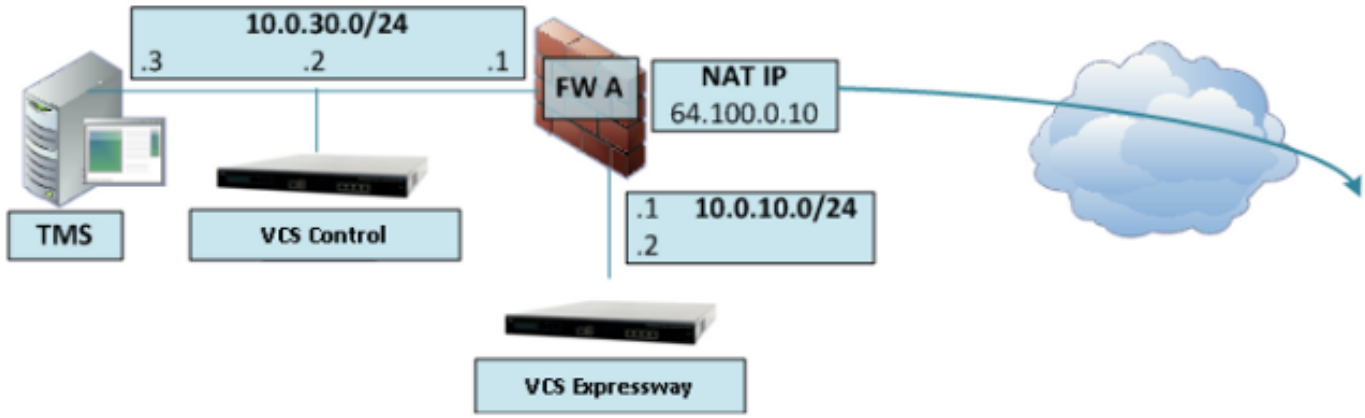
Dans cet exemple, le pare-feu B doit permettre la réflexion NAT du trafic provenant du contrôle VCS destiné à l'adresse IP externe (64.100.0.10) du VCS Expressway. La zone de traversée sur le contrôle VCS doit avoir 64.100.0.10 comme adresse homologue (après conversion FQDN en IP).

Le VCS Expressway doit être configuré avec une passerelle par défaut de **10.0.10.1**. Le fait que les routes statiques soient requises dans ce scénario dépend des fonctionnalités et des paramètres de FW A et de FW B. La communication entre le contrôle VCS et l'Expressway VCS s'effectue via l'adresse IP 64.100.0.10 de l'Expressway VCS ; et le trafic de retour de VCS Expressway au contrôle VCS peut devoir passer par la passerelle par défaut.

Le VCS Expressway peut être ajouté au Cisco TMS avec l'adresse IP 10.0.10.3 (ou avec l'adresse IP 64.100.0.10, si FW B le permet), puisque la communication de gestion du Cisco TMS n'est pas affectée par les paramètres de mode NAT statique sur le VCS Expressway.

DMZ FW 3 ports avec interface LAN VCS Expressway unique

Voici un exemple de ce scénario :



Dans ce déploiement, un pare-feu 3 ports est utilisé pour créer :

- Sous-réseau DMZ (10.0.10.0/24) contenant :
  L'interface DMZ de FW A (10.0.10.1)Interface LAN1 du VCS Expressway (10.0.10.2)
- Sous-réseau LAN (10.0.30.0/24) contenant :
  L'interface LAN de FW A (10.0.30.1)Interface LAN1 du contrôle VCS (10.0.30.2)Interface réseau de Cisco TMS (10.0.30.3)

Une NAT statique un à un a été configurée sur le pare-feu A, qui exécute la NAT de l'adresse IP publique 64.100.0.10 à l'adresse IP LAN1 du VCS Expressway. Le mode NAT statique a été activé pour l'interface LAN1 sur VCS Expressway, avec l'adresse IP NAT statique 64.100.0.10.

Le VCS Expressway doit être configuré avec une passerelle par défaut de 10.0.10.1. Puisque cette passerelle doit être utilisée pour tout le trafic qui quitte VCS Expressway, aucune route statique n'est requise dans ce type de déploiement.

La zone de client de traversée sur le contrôle VCS doit être configurée avec une adresse homologue qui correspond à l'adresse NAT statique de VCS Expressway (64.100.0.10 dans cet exemple) pour les mêmes raisons que celles décrites dans le scénario précédent.

> **Note**: Cela signifie que FW A doit autoriser le trafic en provenance du contrôle VCS avec l'adresse IP de destination 64.100.0.10. Cette fonction est également appelée réflexion NAT et il convient de noter que tous les types de pare-feu ne la prennent pas en charge.

Le VCS Expressway peut être ajouté au Cisco TMS avec l'adresse IP 10.0.10.2 (ou avec l'adresse IP 64.100.0.10, si FW A le permet), puisque la communication de gestion du Cisco TMS n'est pas affectée par les paramètres de mode NAT statique sur le VCS Expressway.

Configuration

Cette section décrit comment configurer la réflexion NAT dans l'ASA pour les deux scénarios d'implémentation VCS C et E différents.

DMZ à sous-réseau unique avec interface LAN VCS Expressway unique

Pour le premier scénario, vous devez appliquer cette configuration de réflexion NAT sur FW A afin de permettre la communication du contrôle VCS (10.0.30.2) qui est destiné à l'adresse IP externe (64.100.0.10) de VCS Expressway :

Dans cet exemple, l'adresse IP de contrôle VCS est **10.0.30.2/24** et l'adresse IP de VCS Expressway est **10.0.10.3/24**.

Si vous supposez que l'adresse IP de contrôle VCS 10.0.30.2 reste lorsqu'elle se déplace de l'intérieur vers l'interface externe de FW B lorsqu'elle recherche l'Expressway VCS avec l'adresse IP de destination 64.100.0.10, la configuration de réflexion NAT que vous devez implémenter sur FW B est présentée dans ces exemples.

Exemple pour ASA versions 8.3 et ultérieures :

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.3
host 10.0.10.3

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.3

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.
```

Exemple pour ASA versions 8.2 et antérieures :

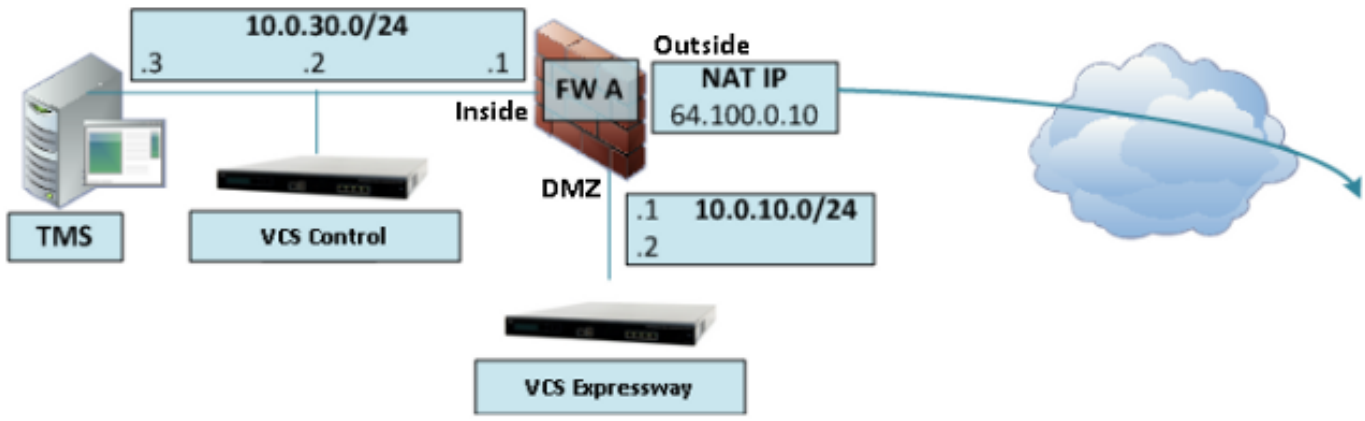
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

access-list OUT-IN-INTERFACE extended permit ip host 10.0.10.3 host 10.0.30.2
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

> **Note**: L'objectif principal de cette configuration de réflexion NAT est de permettre au contrôle VCS d'atteindre l'autoroute VCS, mais en utilisant l'adresse IP publique de l'autoroute VCS au lieu de son adresse IP privée. Si l'adresse IP source du contrôle VCS est modifiée lors de cette traduction NAT avec une configuration NAT double au lieu de la configuration NAT

suggérée qui vient d'être affichée, ce qui fait que VCS Expressway voit le trafic de sa propre adresse IP publique, alors les services téléphoniques des périphériques MRA ne s'afficheront pas. Il ne s'agit pas d'un déploiement pris en charge conformément à la section 3 de la section des recommandations ci-dessous.

DMZ FW 3 ports avec interface LAN VCS Expressway unique

Pour le deuxième scénario, vous devez appliquer cette configuration de réflexion NAT sur FW A afin de permettre la réflexion NAT du trafic entrant provenant du contrôle VCS 10.0.30.2 qui est destiné à l'adresse IP externe (64.100.0.10) de VCS Expressway :



Dans cet exemple, l'adresse IP de contrôle VCS est **10.0.30.2/24** et l'adresse IP de VCS Expressway est **10.0.10.2/24**.

Si vous supposez que l'adresse IP de contrôle VCS 10.0.30.2 reste lorsqu'elle passe de l'intérieur à l'interface DMZ de FW A lorsqu'elle recherche l'Expressway VCS avec l'adresse IP de destination 64.100.0.10, la configuration de réflexion NAT que vous devez implémenter sur FW A est illustrée dans ces exemples.

Exemple pour ASA versions 8.3 et ultérieures :

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.2
host 10.0.10.2

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.2

NOTE: After this NAT is applied you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the DMZ interface is being redirected.
WARNING: Users may not be able to access any service enabled on the DMZ interface.
```

Exemple pour ASA versions 8.2 et antérieures :

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,DMZ) 10.0.30.2 access-list IN-DMZ-INTERFACE
```

```
access-list DMZ-IN-INTERFACE extended permit ip host 10.0.10.2 host 10.0.30.2
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
```

> **Note**: L'objectif principal de cette configuration de réflexion NAT est de permettre au contrôle VCS d'atteindre la voie rapide VCS, mais avec l'adresse IP publique de la voie rapide VCS au lieu de son adresse IP privée. Si l'adresse IP source du contrôle VCS est modifiée lors de cette traduction NAT avec une configuration NAT double au lieu de la configuration NAT suggérée qui vient d'être affichée, ce qui fait que VCS Expressway voit le trafic de sa propre adresse IP publique, alors les services téléphoniques pour les périphériques MRA ne s'afficheront pas. Il ne s'agit pas d'un déploiement pris en charge conformément à la section 3 de la section des recommandations ci-dessous.

Vérification

Cette section fournit les sorties Packet Tracer que vous pouvez voir dans l'ASA afin de confirmer que la configuration de réflexion NAT fonctionne selon les besoins dans les deux scénarios d'implémentation VCS C et E.

DMZ à sous-réseau unique avec interface LAN VCS Expressway unique

Voici la sortie du traceur de paquets FW B pour ASA versions 8.3 et ultérieures :

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/80 to 10.0.10.3/80

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
```

```
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
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 2, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Voici la sortie du traceur de paquets FW B pour ASA versions 8.2 et antérieures :

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/0 to 10.0.10.3/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
```

```
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

DMZ FW 3 ports avec interface LAN VCS Expressway unique

Voici la sortie de FW A packet tracer pour ASA versions 8.3 et ultérieures :

FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/80 to 10.0.10.2/80

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
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 7, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: DMZ
output-status: up
output-line-status: up
Action: allow
```

Voici la sortie de FW A packet tracer pour ASA versions 8.2 et antérieures :

```
FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/0 to 10.0.10.2/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
```

```
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: DMZ
output-status: up
output-line-status: up
Action: allow
```

Dépannage

Vous pouvez configurer des captures de paquets sur les interfaces ASA afin de confirmer la traduction NAT lorsque les paquets entrent et quittent les interfaces FW concernées.

Capture de paquets appliquée au scénario « DMZ FW 3 ports avec interface LAN VCS Expressway unique »

```
FW-A# sh cap
capture capin type raw-data interface inside [Capturing - 5735 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capdmz type raw-data interface DMZ [Capturing - 5735 bytes]
  match ip host 10.0.10.2 host 10.0.30.2
FW-A# sh cap capin

71 packets captured
   1: 22:21:37.095270 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:21:37.100672 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101313 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:21:37.114373 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157371 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:21:37.174429 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234164 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:21:39.238528 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261110 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:21:39.270234 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170614 10.0.30.2.38953 > 64.100.0.10.23: S 1841210281:1841210281(0)
win 4128 <mss 536> 12: 22:21:47.198933 64.100.0.10.23 > 10.0.30.2.38953: S
3354834096:3354834096(0)
```

```
ack 1841210282 win 4128 <mss 536> 13: 22:21:47.235186 10.0.30.2.38953 > 64.100.0.10.23: . ack
3354834097
win 4128 14: 22:21:47.242815 64.100.0.10.23 > 10.0.30.2.38953: P 3354834097:3354834109(12)
ack 1841210282 win 4128 15: 22:21:47.243014 10.0.30.2.38953 > 64.100.0.10.23: P
1841210282:1841210294(12)
ack 3354834097 win 4128 16: 22:21:47.243258 10.0.30.2.38953 > 64.100.0.10.23: . ack 3354834097
win 4128 17: 22:21:47.261094 64.100.0.10.23 > 10.0.30.2.38953: P 3354834109:3354834151(42)
ack 1841210282 win 4128 18: 22:21:47.280411 64.100.0.10.23 > 10.0.30.2.38953: P
3354834151:3354834154(3)
ack 1841210294 win 4116 19: 22:21:47.280625 64.100.0.10.23 > 10.0.30.2.38953: P
3354834154:3354834157(3)
ack 1841210294 win 4116 20: 22:21:47.280838 64.100.0.10.23 > 10.0.30.2.38953: P
3354834157:3354834163(6)
ack 1841210294 win 4116 21: 22:21:47.281082 10.0.30.2.38953 > 64.100.0.10.23: P
1841210294:1841210297(3)
ack 3354834109 win 4116 22: 22:21:47.281296 10.0.30.2.38953 > 64.100.0.10.23: P
1841210297:1841210300(3)
ack 3354834109 win 4116
FW-A# sh cap capdmz

71 packets captured
   1: 22:21:37.095621 10.0.30.2 > 10.0.10.2: icmp: echo request
   2: 22:21:37.100626 10.0.10.2 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101343 10.0.30.2 > 10.0.10.2: icmp: echo request
   4: 22:21:37.114297 10.0.10.2 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157920 10.0.30.2 > 10.0.10.2: icmp: echo request
   6: 22:21:37.174353 10.0.10.2 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234713 10.0.30.2 > 10.0.10.2: icmp: echo request
   8: 22:21:39.238452 10.0.10.2 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261659 10.0.30.2 > 10.0.10.2: icmp: echo request
  10: 22:21:39.270158 10.0.10.2 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170950 10.0.30.2.38953 > 10.0.10.2.23: S 2196345248:2196345248(0)
win 4128 <mss 536> 12: 22:21:47.198903 10.0.10.2.23 > 10.0.30.2.38953: S
1814294604:1814294604(0)
ack 2196345249 win 4128 <mss 536> 13: 22:21:47.235263 10.0.30.2.38953 > 10.0.10.2.23: . ack
1814294605 win 4128 14: 22:21:47.242754 10.0.10.2.23 > 10.0.30.2.38953: P
1814294605:1814294617(12)
ack 2196345249 win 4128 15: 22:21:47.243105 10.0.30.2.38953 > 10.0.10.2.23: P
2196345249:2196345261(12)
ack 1814294605 win 4128 16: 22:21:47.243319 10.0.30.2.38953 > 10.0.10.2.23: . ack 1814294605 win
4128 17: 22:21:47.260988 10.0.10.2.23 > 10.0.30.2.38953: P 1814294617:1814294659(42)
ack 2196345249 win 4128 18: 22:21:47.280335 10.0.10.2.23 > 10.0.30.2.38953: P
1814294659:1814294662(3)
ack 2196345261 win 4116 19: 22:21:47.280564 10.0.10.2.23 > 10.0.30.2.38953: P
1814294662:1814294665(3)
ack 2196345261 win 4116 20: 22:21:47.280777 10.0.10.2.23 > 10.0.30.2.38953: P
1814294665:1814294671(6)
ack 2196345261 win 4116 21: 22:21:47.281143 10.0.30.2.38953 > 10.0.10.2.23: P
2196345261:2196345264(3)
ack 1814294617 win 4116 22: 22:21:47.281357 10.0.30.2.38953 > 10.0.10.2.23: P
2196345264:2196345267(3)
ack 1814294617 win 4116
```

Capture de paquets appliquée pour le scénario « Single Subnet DMZ with Single VCS Expressway LAN Interface »

```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2
```

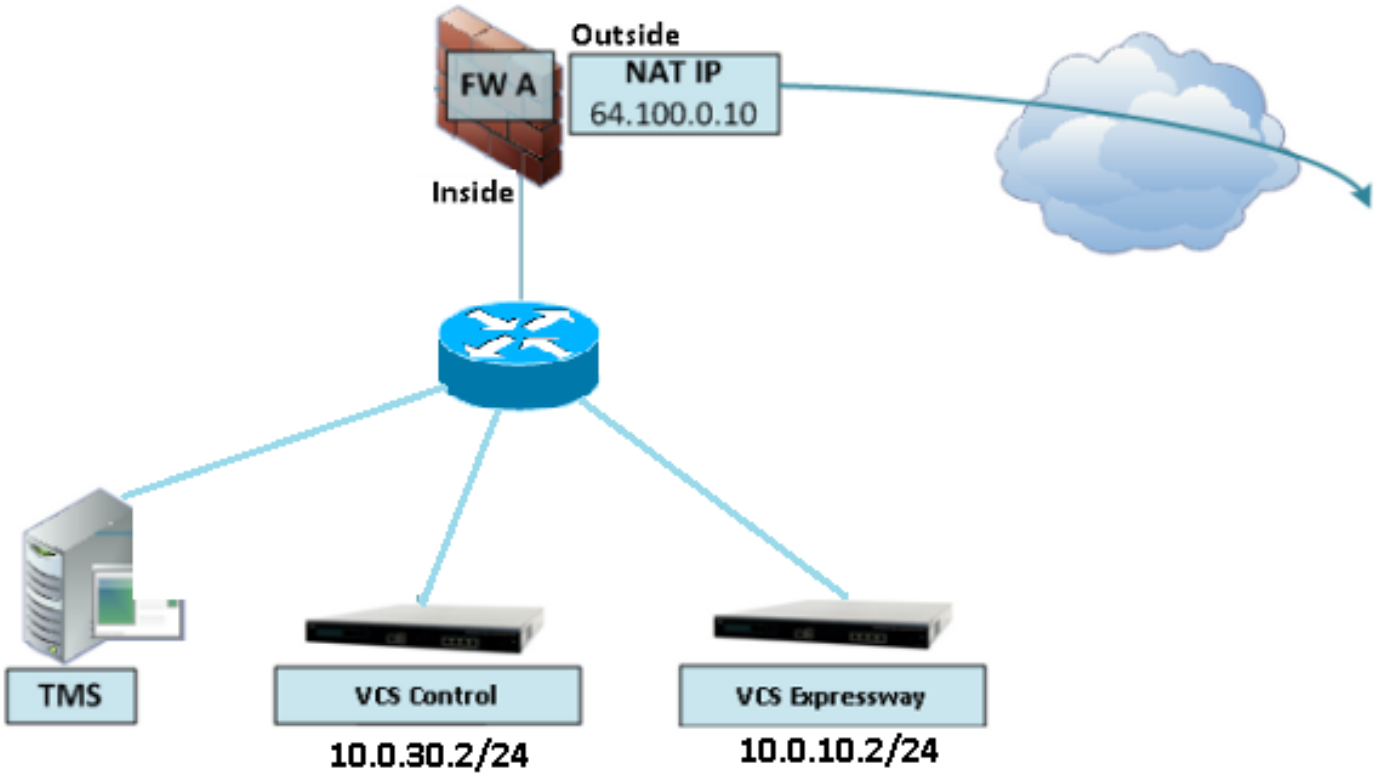
```
FW-B# sh cap capin

72 packets captured
   1: 22:30:06.783681 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:30:06.847856 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.877624 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156409 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:30:07.177496 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.802525 10.0.30.2.41596 > 64.100.0.10.23: S 1119515693:1119515693(0)
win 4128 <mss 536> 12: 22:30:13.861100 64.100.0.10.23 > 10.0.30.2.41596: S
2006020203:2006020203(0)
ack 1119515694 win 4128 <mss 536> 13: 22:30:13.935864 10.0.30.2.41596 > 64.100.0.10.23: . ack
2006020204 win 4128 14: 22:30:13.946804 10.0.30.2.41596 > 64.100.0.10.23: P
1119515694:1119515706(12)
ack 2006020204 win 4128 15: 22:30:13.952679 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204
win 4128 16: 22:30:14.013686 64.100.0.10.23 > 10.0.30.2.41596: P 2006020204:2006020216(12)
ack 1119515706 win 4116 17: 22:30:14.035352 64.100.0.10.23 > 10.0.30.2.41596: P
2006020216:2006020256(40)
ack 1119515706 win 4116 18: 22:30:14.045758 64.100.0.10.23 > 10.0.30.2.41596: P
2006020256:2006020259(3)
ack 1119515706 win 4116 19: 22:30:14.046781 64.100.0.10.23 > 10.0.30.2.41596: P
2006020259:2006020262(3)
ack 1119515706 win 4116 20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
1119515709:1119515712(3)
ack 2006020256 win 4076
ASA1# show cap capout

72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo request
   6: 22:30:06.999399 10.0.10.3 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.076808 10.0.30.2 > 10.0.10.3: icmp: echo request
   8: 22:30:07.134422 10.0.10.3 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156959 10.0.30.2 > 10.0.10.3: icmp: echo request
  10: 22:30:07.177420 10.0.10.3 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.803104 10.0.30.2.41596 > 10.0.10.3.23: S 2599614130:2599614130(0)
win 4128 <mss 536> 12: 22:30:13.860947 10.0.10.3.23 > 10.0.30.2.41596: S
4158597009:4158597009(0)
ack 2599614131 win 4128 <mss 536> 13: 22:30:13.936017 10.0.30.2.41596 > 10.0.10.3.23: . ack
4158597010 win 4128 14: 22:30:13.946941 10.0.30.2.41596 > 10.0.10.3.23: P
2599614131:2599614143(12)
ack 4158597010 win 4128 15: 22:30:13.952801 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win
4128 16: 22:30:14.013488 10.0.10.3.23 > 10.0.30.2.41596: P 4158597010:4158597022(12)
ack 2599614143 win 4116 17: 22:30:14.035108 10.0.10.3.23 > 10.0.30.2.41596: P
4158597022:4158597062(40)
ack 2599614143 win 4116 18: 22:30:14.045377 10.0.10.3.23 > 10.0.30.2.41596: P
4158597062:4158597065(3)
ack 2599614143 win 4116 19: 22:30:14.046384 10.0.10.3.23 > 10.0.30.2.41596: P
4158597065:4158597068(3)
ack 2599614143 win 4116 20: 22:30:14.047406 10.0.10.3.23 > 10.0.30.2.41596: P
4158597068:4158597074(6)
ack 2599614143 win 4116 21: 22:30:14.052395 10.0.30.2.41596 > 10.0.10.3.23: P
```

```
2599614143:2599614146(3)
ack 4158597062 win 4076 22: 22:30:14.089427 10.0.30.2.41596 > 10.0.10.3.23: P
2599614146:2599614149(3)
ack 4158597062 win 4076
```

Recommandations

1. Éviter la mise en oeuvre de toute topologie non prise en charge

Par exemple, si VCS Control et VCS Expressway sont tous deux connectés derrière l'interface ASA interne, comme illustré dans ce scénario :



Ce type d'implémentation nécessite que l'adresse IP de contrôle VCS soit traduite en adresse IP interne de l'ASA afin de forcer le trafic de retour à revenir à l'ASA pour éviter des problèmes de route asymétrique pour la réflexion NAT.

> **Remarque : si l'adresse IP source du contrôle VCS est modifiée lors de cette traduction NAT avec une configuration NAT double au lieu de la configuration de réflexion NAT suggérée, alors le VCS Expressway verra le trafic de sa propre adresse IP publique, alors les services téléphoniques des périphériques MRA ne seront pas activés. Il ne s'agit pas d'un déploiement pris en charge conformément à la section 3 de la section des recommandations ci-dessous.**

Ceci dit, il est fortement recommandé de mettre en oeuvre VCS Expressway en tant qu'implémentation d'interfaces réseau doubles Expressway-E plutôt qu'en tant que carte réseau unique avec réflexion NAT.

2. S'assurer 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
```

3. Assurez-vous que votre mise en oeuvre d'Expressway est conforme aux exigences suivantes suggérées par les développeurs Cisco TelePresence

- La configuration NAT entre l'Expressway-C et l'Expressway-E n'est pas prise en charge.
- Il n'est pas pris en charge lorsque les Expressway-C et Expressway-E obtiennent NATed à la même adresse IP publique, par exemple :
  Expressway-C est configuré avec l'adresse IP 10.1.1.1
  Expressway-E possède une seule carte réseau configurée avec l'adresse IP 10.2.2.1 et une NAT statique est configurée dans le pare-feu avec l'adresse IP publique 64.100.0.10
  Ensuite, l'Expressway-C ne peut pas être NATted à la même adresse publique 64.100.0.10

Mise en oeuvre recommandée de VCS Expressway

La mise en oeuvre recommandée pour le VCS Expressway au lieu du VCS Expressway avec la configuration NAT reflétant est la mise en oeuvre de la double interface réseau/double carte réseau VCS Expressway. Pour plus d'informations, consultez le lien suivant.

Configuration NAT ASA et recommandations pour la mise en oeuvre des interfaces réseau doubles Expressway-E.

Informations connexes

- Configuration NAT ASA et recommandations pour la mise en oeuvre des interfaces réseau doubles Expressway-E
- Guide de déploiement de Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)
- Utilisation des ports IP Cisco Expressway pour la traversée de pare-feu
- Placement d'un Cisco VCS Expressway dans une zone démilitarisée (DMZ) plutôt que sur l'Internet public