Configurez la réflexion NAT sur l'ASA pour les périphériques de TelePresence d'Expressway de VCS

Contenu

Introduction

Ce document décrit comment implémenter une configuration de réflexion de Traduction d'adresses de réseau (NAT) sur les appliances de sécurité adaptable Cisco pour les scénarios spéciaux de TelePresence Cisco qui exigent ce genre de configuration NAT sur le Pare-feu.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration NAT de base de Cisco ASA (appliance de sécurité adaptable).
- Contrôle de serveur de communication vidéo Cisco TelePresence (VCS) et configuration de base d'Expressway de VCS.

> **Note**: Ce document est destiné pour être utilisé seulement quand la méthode recommandée de déploiement de VCS-Expressway ou d'Expressway-périphérie avec les deux interfaces NIC dans différents DMZ ne peut pas être utilisée. Pour plus d'informations sur le déploiement recommandé utilisant de doubles NIC veuillez vérifient le lien suivant à la page 60 : Guide de déploiement de la configuration de base de serveur de communication vidéo Cisco TelePresence (contrôle avec Expressway)

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 8.3 et plus tard.
- Version X8.x de VCS de Cisco 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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> **Note**: Par le document entier, des périphériques de VCS désigné sous le nom du contrôle de VCS Expressway et de VCS. Cependant, la même configuration applique aux périphériques d'Expressway-e et d'Expressway-C.

Informations générales

Selon la documentation de TelePresence Cisco, il y a deux genres de scénarios de TelePresence où la configuration NAT de réflexion est exigée sur le FWs afin de permettre au contrôle de VCS pour communiquer avec le VCS Expressway par l'intermédiaire de l'adresse IP publique d'Expressway de VCS.

Le premier scénario implique une zone démilitarisée de sous-réseau unique (DMZ) cette des utilisations une interface simple de RÉSEAU LOCAL d'Expressway de VCS, et le deuxième scénario implique un 3-port FW DMZ qui utilise une interface simple de RÉSEAU LOCAL d'Expressway de VCS.

> **Conseil** : Afin d'obtenir plus de détails au sujet de l'implémentation de TelePresence, référez-vous au guide de déploiement de la configuration de base de serveur de communication vidéo Cisco TelePresence (contrôle avec Expressway).

Topologies de Cisco Non-recommandées pour le C de VCS et

l'implémentation E

Il est important de noter que les topologies suivantes ne sont pas recommandées de Cisco. La méthodologie recommandée de déploiement pour un VCS Expressway ou la périphérie d'Expressway est d'utiliser deux DMZ différents avec Expressway ayant un NIC dans chacun des DMZ. Ce guide est censé pour être utilisé dans les environnements où la méthode recommandée de déploiement ne peut pas être utilisée.

Sous-réseau unique DMZ avec l'interface simple de RÉSEAU LOCAL d'Expressway de VCS

Dans ce scénario, FW A peut conduire le trafic à FW B (et vice versa). Le VCS Expressway permet au trafic visuel pour être FW traversé B sans réduction de la circulation sur FW B de l'extérieur aux interfaces internes. Le VCS Expressway manipule également la traversée FW de son côté public.

Voici un exemple de ce scénario :

Ce déploiement utilise ces composants :

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

Un NAT linéaire statique a été configuré sur FW A, qui exécute le NAT pour l'annonce 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 le VCS Expressway, avec une adresse IP NAT statique de 64.100.0.10.

> **Note**: Vous devez écrire le nom de domaine complet (FQDN) du VCS Expressway sur la zone sécurisée de client de traversée de contrôle de VCS (adresse de pair) comme comment on le voit de l'extérieur du réseau. La raison pour ceci est celle dans le mode NAT statique, le VCS Expressway demande que la signalisation et les medias d'arrivée trafiquent soient envoyés à son FQDN externe plutôt que son nom privé. Ceci signifie également que le FW externe doit permettre le trafic du contrôle de VCS au FQDN externe d'Expressway de VCS. Ceci est connu en tant que réflexion NAT, et ne pourrait pas être pris en charge par tous les types de FWs.

Dans cet exemple, FW B doit permettre la réflexion NAT du trafic qui provient le contrôle de VCS qui est destiné à l'adresse IP externe (64.100.0.10) du VCS Expressway. La zone de traversée sur le contrôle de VCS doit avoir 64.100.0.10 comme adresse de pair (après FQDN à la conversion

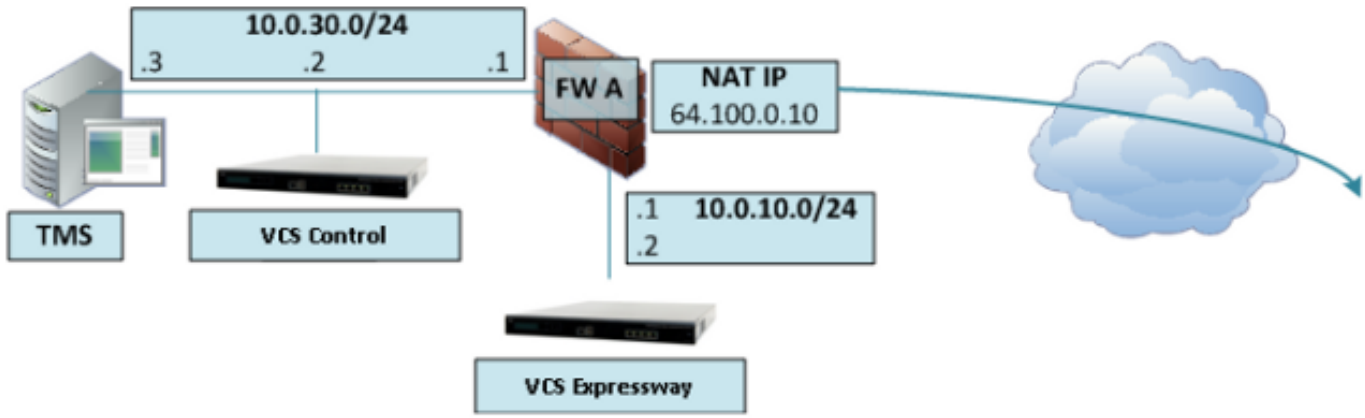
IP).

Le VCS Expressway devrait être configuré avec une passerelle par défaut de **10.0.10.1**. Si les artères statiques sont exigées dans ce scénario dépend des capacités et des configurations de FW A et de FW B. La transmission du contrôle de VCS au VCS Expressway se produit par l'intermédiaire de l'adresse IP de 64.100.0.10 du VCS Expressway ; et le trafic de retour du VCS Expressway au contrôle de VCS pourrait devoir passer par l'intermédiaire de la passerelle par défaut.

Le VCS Expressway peut être ajouté à Cisco TMS avec l'adresse IP 10.0.10.3 (ou avec adresse IP 64.100.0.10, si FW B permet ceci), puisque la communication de la direction de Cisco TMS n'est pas affectée par les configurations statiques de mode NAT sur le VCS Expressway.

3-Port FW DMZ avec l'interface simple de RÉSEAU LOCAL d'Expressway de VCS

Voici un exemple de ce scénario :



Dans ce déploiement, un 3-port FW est utilisé afin de créer :

- Un sous-réseau DMZ (10.0.10.0/24) qui contiennent :
  L'interface DMZ de FW A (10.0.10.1)L'interface LAN1 du VCS Expressway (10.0.10.2)
- Un sous-réseau LAN (10.0.30.0/24) qui contiennent :
  L'interface de RÉSEAU LOCAL de FW A (10.0.30.1)L'interface LAN1 du contrôle de VCS (10.0.30.2)L'interface réseau de Cisco TMS (10.0.30.3)

Un NAT linéaire statique a été configuré sur FW A, qui exécute le 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 le VCS Expressway, avec une adresse IP NAT statique de 64.100.0.10.

Le VCS Expressway devrait être configuré avec une passerelle par défaut de 10.0.10.1. Puisque cette passerelle doit être utilisée pour tout les trafic qui part du VCS Expressway, aucune artère de charge statique n'est exigée dans ce type de déploiement.

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

> **Note**: Ceci signifie que FW A doit permettre le trafic du contrôle de VCS avec une adresse IP de destination de 64.100.0.10. Ceci est également connu en tant que réflexion NAT, et il convient noter que ceci n'est pas pris en charge par tous les types de FWs.

Le VCS Expressway peut être ajouté à Cisco TMS avec l'adresse IP de 10.0.10.2 (ou avec adresse IP 64.100.0.10, si FW A permet ceci), puisque la communication de la direction de Cisco TMS n'est pas affectée par les configurations statiques de mode NAT sur le VCS Expressway.

Configurer

Cette section décrit comment configurer la réflexion NAT dans l'ASA des scénarios pour deux de VCS de C et E implémentations différentes.

Sous-réseau unique DMZ avec l'interface simple de RÉSEAU LOCAL d'Expressway de VCS

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

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

Si vous supposez que l'adresse IP 10.0.30.2 de contrôle de VCS demeure quand elle se déplace de l'intérieur à l'interface extérieure de FW B quand recherchant le VCS Expressway avec l'adresse IP 64.100.0.10 de destination, alors la configuration NAT de réflexion que vous devriez implémenter sur FW B est affiché dans ces exemples.

Exemple pour des versions 8.3 et ultérieures ASA :

```
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 des versions 8.2 et antérieures ASA :

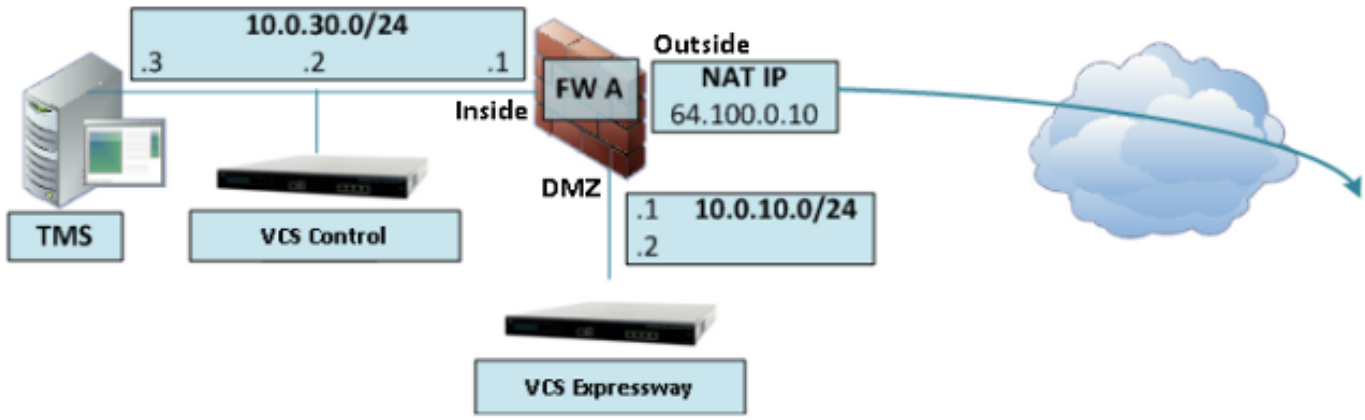
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
```

```
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 NAT de réflexion est de permettre au contrôle de VCS pour pouvoir atteindre l'autoroute de VCS, mais utiliser l'adresse IP publique d'autoroute de VCS au lieu de son adresse IP privée. Si l'adresse IP source du contrôle de VCS est changée pendant cette traduction NAT avec une configuration deux fois NAT au lieu de la configuration NAT suggérée juste affichée, ayant pour résultat le VCS Expressway voir le trafic de sa propre adresse IP publique, alors les services de téléphonie pour les périphériques MRA ne montera pas. Ce n'est pas un déploiement pris en charge selon la section 3 sur la section de recommandations ci-dessous.

3-Port FW DMZ avec l'interface simple de RÉSEAU LOCAL d'Expressway de VCS

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



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

Si vous supposez que l'adresse IP 10.0.30.2 de contrôle de VCS demeure quand elle se déplace de l'intérieur à l'interface DMZ de FW A quand recherchant le VCS Expressway avec l'adresse IP 64.100.0.10 de destination, alors la configuration NAT de réflexion que vous devriez implémenter sur FW A est affiché dans ces exemples.

Exemple pour des versions 8.3 et ultérieures ASA :

```
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 des versions 8.2 et antérieures ASA :

```
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 NAT de réflexion est de permettre au contrôle de VCS pour pouvoir atteindre l'autoroute de VCS, mais avec l'adresse IP publique d'autoroute de VCS au lieu de son adresse IP privée. Si l'adresse IP source du contrôle de VCS est changée pendant cette traduction NAT avec une configuration deux fois NAT au lieu de la configuration NAT suggérée juste affichée, ayant pour résultat le VCS Expressway voir le trafic de sa propre adresse IP publique, alors les services de téléphonie pour les périphériques MRA ne montera pas. Ce n'est pas un déploiement pris en charge selon la section 3 dans la section de recommandations ci-dessous.

Vérifiez

Cette section fournit les sorties de traceur de paquet que vous pouvez voir dans l'ASA afin de confirmer la configuration NAT de réflexion fonctionne comme nécessaire dans chacun des deux des scénarios de VCS de C et E implémentation.

Sous-réseau unique DMZ avec l'interface simple de RÉSEAU LOCAL d'Expressway de VCS

Voici le traceur de paquet FW B sorti pour des versions 8.3 et ultérieures ASA :

```
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 le traceur de paquet FW B sorti pour des versions 8.2 et antérieures ASA :

```
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
```

3-Port FW DMZ avec l'interface simple de RÉSEAU LOCAL d'Expressway de VCS

Voici le traceur de paquet FW A sorti pour des versions 8.3 et ultérieures ASA :

```
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 le traceur de paquet FW A sorti pour des versions 8.2 et antérieures ASA :

```
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
```

Dépanner

Vous pouvez configurer des captures de paquet sur les interfaces ASA afin de confirmer la traduction NAT quand les paquets écrivent et laissent les interfaces FW qui sont impliquées.

La capture de paquet a sollicité le "3-Port FW DMZ avec scénario de VCS d'Expressway d'interface simple de RÉSEAU LOCAL le »

```
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 paquet appliquée pour « sous-réseau unique DMZ avec le scénario de VCS d'Expressway d'interface simple de RÉSEAU LOCAL »

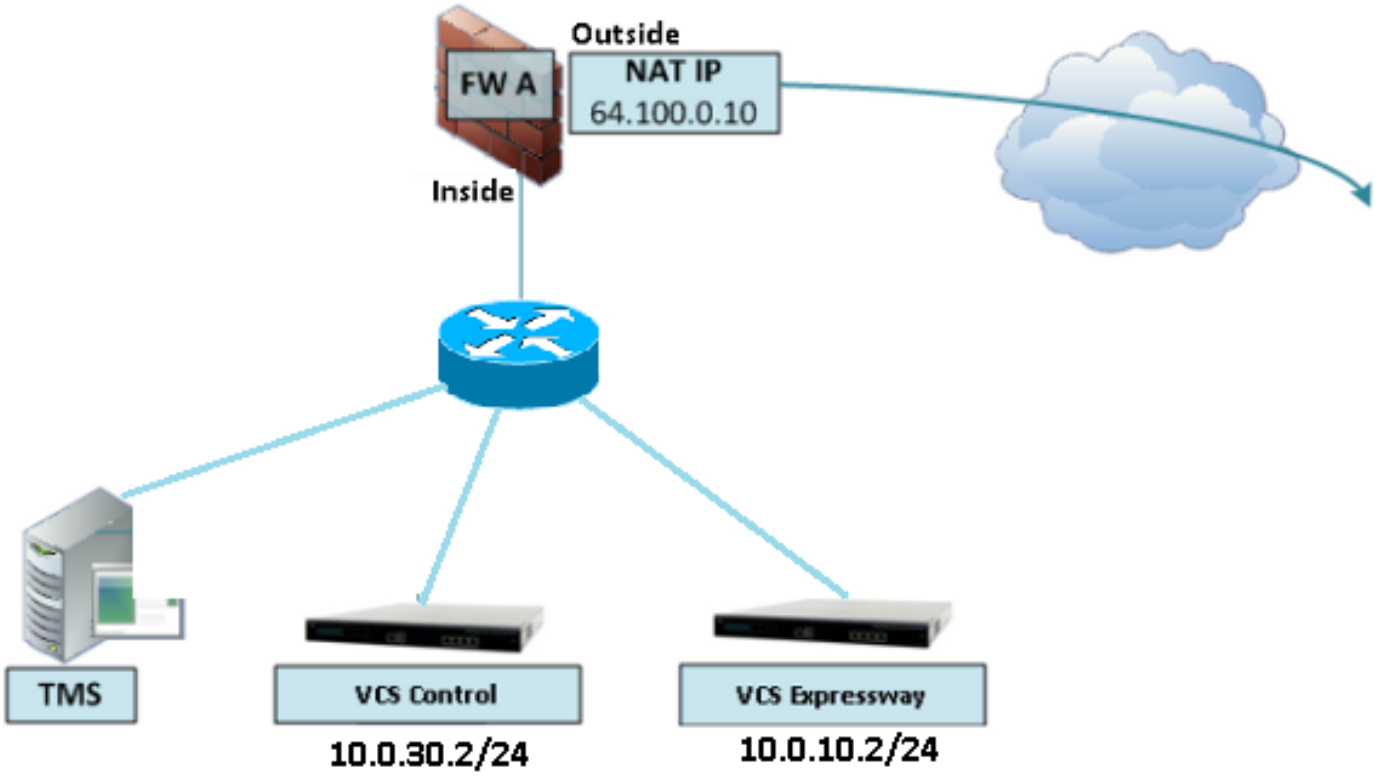
```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

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. Évitez l'implémentation de n'importe quelle topologie non vérifiée

Par exemple, si vous avez le contrôle et le VCS Expressway de VCS connecté derrière l'interface intérieure ASA, juste suivant les indications de ce scénario :



Ce genre d'implémentation exige de l'adresse IP de contrôle de VCS d'être traduite à l'adresse IP intérieure de l'ASA afin de forcer le trafic de retour pour revenir à l'ASA pour éviter des problèmes asymétriques d'artère pour la réflexion NAT.

> **Remarque: Si l'adresse IP source du contrôle de VCS est changée pendant cette traduction NAT avec une configuration deux fois NAT au lieu de la configuration NAT suggérée de réflexion, alors le VCS Expressway verra le trafic de sa propre adresse IP publique, alors les services de téléphonie pour les périphériques MRA ne seront pas soulevés. Ce n'est pas un déploiement pris en charge selon la section 3 dans la section de recommandations ci-**

dessous.

Cela dit, il est fortement recommandé pour implémenter le VCS Expressway comme double implémentation d'interfaces réseau d'Expressway-e au lieu du NIC simple avec la réflexion NAT.

2. 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.

```
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
```

3. Assurez que votre implémentation d'Expressway d'effectif est conforme aux prochaines conditions requises proposées par les développeurs de TelePresence Cisco

- La configuration NAT entre Expressway-C et Expressway-e n'est pas prise en charge.
- Il n'est pas pris en charge quand 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 a le NIC simple configuré avec l'adresse IP 10.2.2.1 et un NAT statique est configuré dans le Pare-feu avec l'adresse IP publique 64.100.0.10
  Alors Expressway-C ne peut pas être NATted à la même annonce publique 64.100.0.10

Implémentation recommandée d'Expressway de VCS

L'implémentation recommandée pour le VCS Expressway au lieu du VCS Expressway avec la configuration NAT de réflexion est les doubles interfaces réseau/double implémentation d'Expressway de VCS NIC, satisfont pour de plus amples informations vérifient le prochain lien.

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

Informations connexes

- La configuration NAT et les recommandations ASA pour Expressway-e conjuguent

implémentation d'interfaces réseau

- Guide de déploiement de la configuration de base de serveur de communication vidéo Cisco TelePresence (contrôle avec Expressway)
- Utilisation de port IP de Cisco Expressway pour la traversée de Pare-feu
- Plaçant un VCS Expressway de Cisco dans un DMZ plutôt que dans l'Internet public