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 (ASA) pour les scénarios spéciaux de TelePresence Cisco qui exigent ce genre de configuration NAT sur le Pare-feu (FW).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration NAT de base de Cisco ASA
- Contrôle du serveur de communication vidéo Cisco TelePresence (VCS) et configuration de base d'autoroute VCS

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 8.5 de Cisco VCS X

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

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 VCS pour communiquer avec l'autoroute VCS par l'intermédiaire de l'adresse IP publique d'autoroute VCS.

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

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

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

Voici un exemple :

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 de l'autoroute VCS (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 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 de l'autoroute VCS. Le mode NAT statique a été activé pour l'interface LAN1 sur l'autoroute VCS, avec une adresse IP NAT statique de 64.100.0.10.

> Remarque: Vous devez écrire le nom de domaine complet (FQDN) de l'autoroute VCS. On le voit de l'extérieur de du réseau comme l'adresse de pair sur la zone sécurisée de traversée de contrôle VCS. La raison pour ceci est celle dans le mode NAT statique, l'autoroute VCS 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 VCS au FQDN externe d'autoroute 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 A doit permettre la réflexion NAT du trafic qui provient le contrôle VCS qui est destiné à l'adresse IP externe (64.100.0.10) de l'autoroute VCS. La zone de traversée sur le contrôle VCS doit avoir 64.100.0.10 comme adresse de pair.

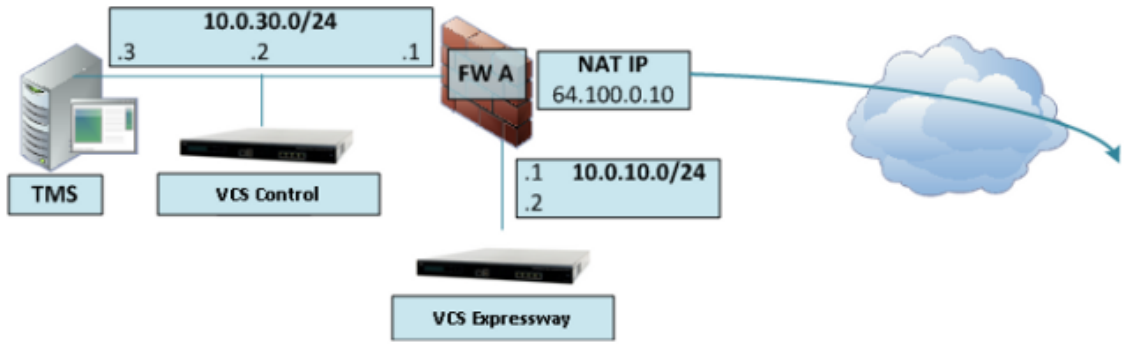
L'autoroute VCS devrait être configurée avec une passerelle par défaut de 10.0.10.1. Si les artères statiques sont exigées dans ce scénario dépend des capacités et des configurations de FW A et de FW B. La transmission du contrôle VCS à l'autoroute VCS se produisent par l'intermédiaire de l'adresse IP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

Si une artère statique est ajoutée à l'autoroute VCS de sorte que le trafic de réponse passe de l'autoroute VCS et directement par FW B au sous-réseau 10.0.30.0/24, il signifie que le routage asymétrique se produit. Ceci ne pourrait pas fonctionner, dépendant sur les capacités FW.

L'autoroute VCS peut être ajoutée à Cisco TMS avec l'adresse IP 10.0.10.3 (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 l'autoroute VCS.

3-Port FW DMZ avec l'interface simple de RÉSEAU LOCAL d'autoroute 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 de l'autoroute VCS (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 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 de l'autoroute VCS. Le mode NAT statique a été activé pour l'interface LAN1 sur l'autoroute VCS, avec une adresse IP NAT statique de 64.100.0.10.

L'autoroute VCS devrait être configurée avec une passerelle par défaut de 10.0.10.1. Puisque cette passerelle doit être utilisée pour tout les trafic qui laisse l'autoroute VCS, aucune artère de charge statique n'est exigée dans ce type de déploiement.

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

> Remarque: Ceci signifie que FW A doit permettre le trafic du contrôle 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.

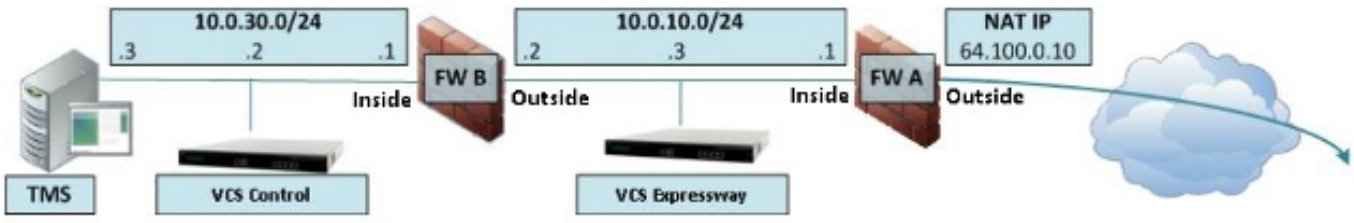
L'autoroute VCS peut être ajoutée à Cisco TMS avec l'adresse IP de 10.0.10.2 (ou avec adresse IP 64.100.0.10, si FW A permet ceci), puisque la communication de la direction de Cisco TMS n'est pas affectée par les configurations statiques de mode NAT sur l'autoroute VCS.

Configurez

Cette section décrit comment configurer la réflexion NAT pour les deux scénarios différents d'implémentation de TelePresence.

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

Pour le premier scénario, vous devez appliquer cette configuration NAT de réflexion sur FW A afin de



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

Si vous supposez que l'adresse IP de contrôle VCS de 10.0.30.2 est traduite à l'adresse IP 10.0.10.2 quand elle se déplace de l'intérieur à l'interface extérieure de FW B, alors la configuration NAT de réflexion que vous devriez implémenter sur FW B est affichée dans les exemples suivants.

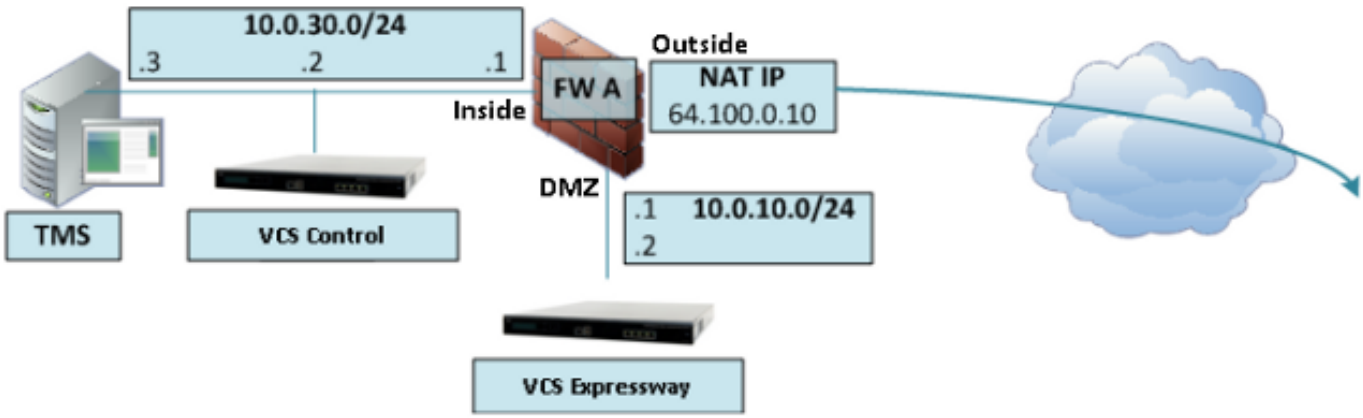
Pour des versions 8.3 et ultérieures ASA :

Pour des versions 8.2 et antérieures ASA :

> Remarque: Il est facultatif pour traduire l'adresse IP source des paquets pour cette circulation. L'objectif principal de cette traduction NAT de réflexion est de permettre au contrôle VCS pour atteindre l'autoroute VCS, mais utilise l'adresse IP publique d'autoroute VCS au lieu de son adresse IP privée.

3-Port FW DMZ avec l'interface simple de RÉSEAU LOCAL d'autoroute 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 VCS qui est destiné à l'adresse IP externe (64.100.0.10) de l'autoroute VCS :



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

Si vous supposez que l'adresse IP de contrôle VCS de 10.0.30.2 est traduite à l'adresse IP 10.0.10.1 quand elle se déplace de l'intérieur à l'interface DMZ de FW A, alors la configuration NAT de réflexion que vous devriez implémenter sur FW A est affichée dans les exemples suivants.

Pour des versions 8.3 et ultérieures ASA :

Pour des versions 8.2 et antérieures ASA :

> Remarque: Il est facultatif pour traduire l'adresse IP source des paquets pour cette circulation. L'objectif principal de cette traduction NAT de réflexion est de permettre au contrôle VCS pour atteindre l'autoroute VCS, mais utilise l'adresse IP publique d'autoroute

VCS au lieu de son adresse IP privée.

Vérifiez

Cette section fournit les sorties de traceur de paquet que vous pouvez employer afin de confirmer la configuration NAT correcte de réflexion dans chacun des deux scénarios de TelePresence.

Sous-réseau unique DMZ avec l'interface simple de RÉSEAU LOCAL d'autoroute 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: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.10.2 destination static
obj-64.100.0.10 obj-10.0.10.3
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/80 to 10.0.10.3/80

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.10.2 destination static
obj-64.100.0.10 obj-10.0.10.3
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.10.2/1234

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: FOVER
Subtype: standby-update
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.10.2 destination static
obj-64.100.0.10 obj-10.0.10.3
Additional Information:

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 421, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
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: ACCESS-LIST
Subtype:
```

```
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
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 10.0.10.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 1
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: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: SSM-DIVERT
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: SSM_SERVICE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,outside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.10.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.10.2/0 using netmask 255.255.255.255

Phase: 7
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,outside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.10.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 8
```

```
Type: SSM_SERVICE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
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 10.0.10.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 316, 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'autoroute 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: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.10.1 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: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.10.1 destination static
obj-64.100.0.10 obj-10.0.10.2
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.10.1/1234

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FOVER
Subtype: standby-update
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.10.1 destination static
obj-64.100.0.10 obj-10.0.10.2
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
```

```
Additional Information:
New flow created with id 424, 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: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.10.1
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 1
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: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: SSM-DIVERT
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: SSM_SERVICE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
```

```
static (inside,DMZ) interface access-list IN-DMZ-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.10.1
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.10.1/0 using netmask 255.255.255.255

Phase: 7
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,DMZ) interface access-list IN-DMZ-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.10.1
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 8
Type: SSM_SERVICE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.10.1
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 10
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.10.1
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 750, 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
```

Dépannez

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