Configurazione della riflessione NAT sull'appliance ASA per i dispositivi VCS Expressway TelePresence

Sommario

Introduzione

Questo documento descrive come implementare una configurazione di riflessione Network Address Translation (NAT) su Cisco Adaptive Security Appliance per scenari Cisco TelePresence speciali che richiedono questo tipo di configurazione NAT sul firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione NAT di base Cisco ASA (Adaptive Security Appliance).
- Cisco TelePresence Video Communication Server (VCS) Control e configurazione base VCS Expressway.

> **Nota:** Questo documento deve essere utilizzato solo quando non è possibile usare il metodo di distribuzione consigliato di VCS-Expressway o Expressway-Edge con entrambe le interfacce NIC in DMZ diverse. Per ulteriori informazioni sull'installazione consigliata con due schede NIC, consultare il seguente collegamento a pagina 60: Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance Cisco ASA serie 5500 e 5500-X con software versione 8.3 e successive.
- Cisco VCS versione X8.x e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota**: in tutto il documento, i dispositivi VCS sono denominati VCS Expressway e VCS Control. Tuttavia, la stessa configurazione si applica alle periferiche Expressway-E ed Expressway-C.

Premesse

Come indicato nella documentazione di Cisco TelePresence, esistono due tipi di scenari TelePresence in cui è richiesta la configurazione della riflessione NAT sui firmware per consentire al controllo VCS di comunicare con VCS Expressway tramite l'indirizzo IP pubblico di VCS Expressway.

Il primo scenario riguarda una singola subnet demilitarizzata zone (DMZ) che utilizza una singola interfaccia LAN VCS Expressway, mentre il secondo scenario riguarda una DMZ FW a 3 porte che utilizza una singola interfaccia LAN VCS Expressway.

> **Suggerimento**: Per ulteriori informazioni sull'implementazione di TelePresence, consultare la guida alla distribuzione di Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway).

Topologie Cisco non consigliate per l'implementazione di VCS C ed E

Èimportante notare che le seguenti topologie NON sono consigliate da Cisco. La metodologia

consigliata per l'implementazione di VCS Expressway o Expressway Edge consiste nell'utilizzare due DMZ diverse, ognuna delle quali dotata di una scheda NIC. Questa guida è destinata all'utilizzo in ambienti in cui non è possibile utilizzare il metodo di distribuzione consigliato.

DMZ a subnet singola con interfaccia LAN Expressway VCS singola

In questo scenario, FW A può instradare il traffico verso FW B (e viceversa). VCS Expressway consente di far passare il traffico video attraverso FW B senza ridurre il flusso di traffico su FW B dall'esterno alle interfacce interne. VCS Expressway gestisce inoltre l'attraversamento FW sul lato pubblico.

Di seguito è riportato un esempio di questo scenario:

Questa distribuzione utilizza i seguenti componenti:

- Una subnet DMZ singola (10.0.10.0/24) contenente:
  L'interfaccia interna di FW A (10.0.10.1)L'interfaccia esterna di FW B (10.0.10.2)L'interfaccia LAN1 di VCS Expressway (10.0.10.3)
- Una subnet LAN (10.0.30.0/24) contenente:
  L'interfaccia interna di FW B (10.0.30.1)L'interfaccia LAN1 del controllo VCS (10.0.30.2)L'interfaccia di rete di Cisco TelePresence Management Server (TMS) (10.0.30.3)

Sul firmware A è stato configurato un NAT statico uno a uno, che esegue il NAT per l'indirizzo pubblico 64.100.0.10 sull'indirizzo IP LAN1 del VCS Expressway. La modalità NAT statica è stata abilitata per l'interfaccia LAN1 su VCS Expressway con un indirizzo IP NAT statico di 64.100.0.10.

> **Nota:** È necessario immettere il nome di dominio completo (FQDN) di VCS Expressway nella zona client di attraversamento sicuro di VCS Control (indirizzo peer) come visualizzato dall'esterno della rete. In modalità NAT statica, VCS Expressway richiede l'invio della segnalazione in ingresso e del traffico multimediale al nome di dominio completo (FQDN) esterno anziché al nome privato. Ciò significa anche che l'FW esterno deve consentire il traffico dal controllo VCS all'FQDN esterno di VCS Expressway. Questo processo è noto come riflessione NAT e potrebbe non essere supportato da tutti i tipi di firmware.

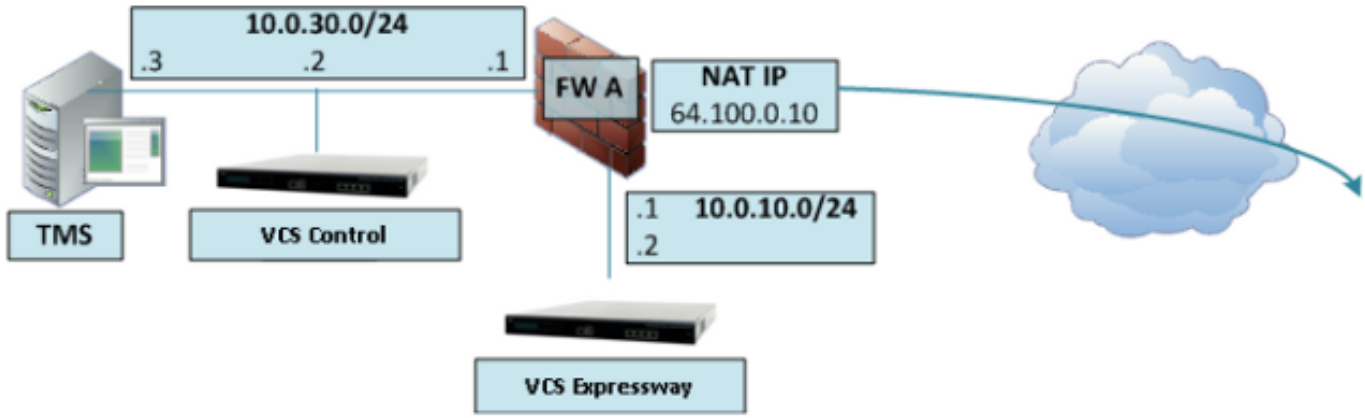
Nell'esempio, il firmware B deve consentire la riflessione NAT del traffico proveniente dal controllo VCS destinato all'indirizzo IP esterno (64.100.0.10) del VCS Expressway. La zona trasversale sul controllo VCS deve avere 64.100.0.10 come indirizzo peer (dopo la conversione da FQDN a IP).

VCS Expressway deve essere configurato con un gateway predefinito di **10.0.10.1**. La necessità di utilizzare route statiche in questo scenario dipende dalle funzionalità e dalle impostazioni di FW A e FW B. La comunicazione tra VCS Control e VCS Expressway avviene tramite l'indirizzo IP 64.100.0.10 di VCS Expressway; e il traffico di ritorno da VCS Expressway a VCS Control potrebbe dover passare attraverso il gateway predefinito.

VCS Expressway può essere aggiunto al Cisco TMS con l'indirizzo IP 10.0.10.3 (o con l'indirizzo IP 64.100.0.10, se il firmware B lo consente), in quanto la comunicazione della gestione TMS di Cisco non è influenzata dalle impostazioni statiche della modalità NAT su VCS Expressway.

DMZ FW a 3 porte con interfaccia LAN Single VCS Expressway

Di seguito è riportato un esempio di questo scenario:



In questa implementazione, viene utilizzato un firmware a 3 porte per creare:

- Subnet DMZ (10.0.10.0/24) contenente:
  L'interfaccia DMZ dell'FW A (10.0.10.1)L'interfaccia LAN1 di VCS Expressway (10.0.10.2)
- Una subnet LAN (10.0.30.0/24) contenente:
  L'interfaccia LAN dell'FW A (10.0.30.1)L'interfaccia LAN1 del controllo VCS (10.0.30.2)L'interfaccia di rete del Cisco TMS (10.0.30.3)

Sul firmware A è stato configurato un NAT statico uno a uno, che esegue il NAT dell'indirizzo IP pubblico 64.100.0.10 sull'indirizzo IP LAN1 del VCS Expressway. La modalità NAT statica è stata abilitata per l'interfaccia LAN1 su VCS Expressway con un indirizzo IP NAT statico di 64.100.0.10.

VCS Expressway deve essere configurato con un gateway predefinito di 10.0.10.1. Poiché questo gateway deve essere utilizzato per tutto il traffico che esce da VCS Expressway, in questo tipo di distribuzione non sono necessarie route statiche.

La zona client trasversale sul controllo VCS deve essere configurata con un indirizzo peer corrispondente all'indirizzo NAT statico di VCS Expressway (64.100.0.10 nell'esempio) per gli stessi motivi descritti nello scenario precedente.

> **Nota:** Ciò significa che il firmware A deve consentire il traffico proveniente dal controllo VCS con un indirizzo IP di destinazione di 64.100.0.10. Questa condizione è nota anche come reflection NAT e non è supportata da tutti i tipi di firmware.

VCS Expressway può essere aggiunto al Cisco TMS con l'indirizzo IP 10.0.10.2 (o con l'indirizzo IP 64.100.0.10, se il firmware A lo consente), poiché la comunicazione della gestione del Cisco TMS non è influenzata dalle impostazioni statiche della modalità NAT su VCS Expressway.

Configurazione

In questa sezione viene descritto come configurare la reflection NAT nell'appliance ASA per i due diversi scenari di implementazione di VCS C ed E.

DMZ a subnet singola con interfaccia LAN Expressway VCS singola

Per il primo scenario, è necessario applicare questa configurazione di riflessione NAT sul firmware A per consentire la comunicazione dal controllo VCS (10.0.30.2) destinato all'indirizzo IP esterno (64.100.0.10) del VCS Expressway:

Nell'esempio, l'indirizzo IP di VCS Control è **10.0.30.2/24**, mentre l'indirizzo IP di VCS Expressway è **10.0.10.3/24**.

Se si suppone che l'indirizzo IP 10.0.30.2 di VCS Control rimanga quando si sposta dall'interfaccia interna verso l'interfaccia esterna del firmware B durante la ricerca di VCS Expressway con l'indirizzo IP 64.100.0.10 di destinazione, in questi esempi viene mostrata la configurazione di riflessione NAT da implementare sul firmware B.

Esempio di appliance ASA versione 8.3 e successive:

```
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.
```

Esempio di appliance ASA versione 8.2 e precedenti:

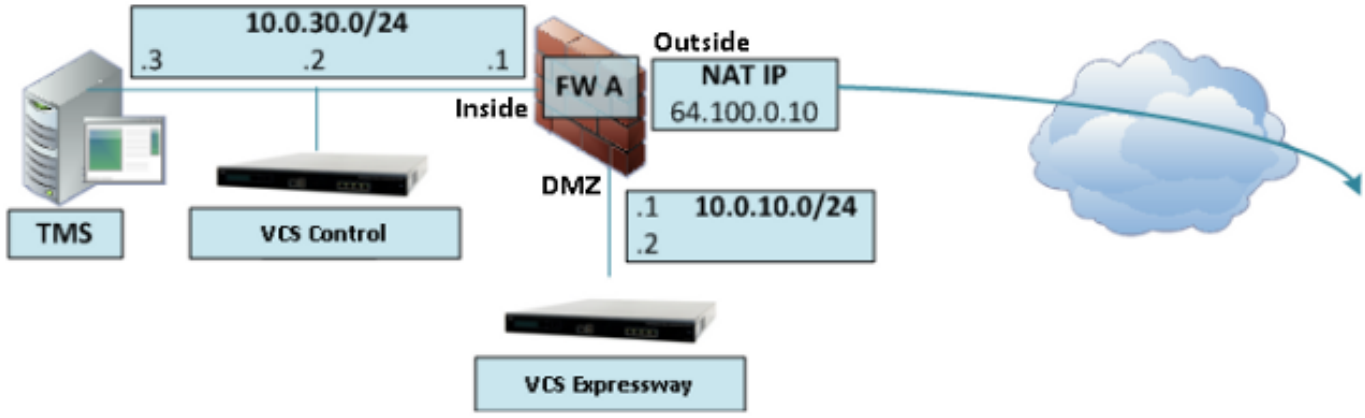
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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
```

> **Nota:** L'obiettivo principale di questa configurazione di riflessione NAT è consentire al controllo VCS di raggiungere l'autostrada VCS, ma utilizzando l'indirizzo IP pubblico dell'autostrada VCS invece dell'indirizzo IP privato. Se l'indirizzo IP di origine del controllo VCS viene modificato durante la traduzione NAT con una configurazione NAT doppia

anziché la configurazione NAT suggerita appena mostrata, in modo che VCS Expressway visualizzi il traffico proveniente dal proprio indirizzo IP pubblico, i servizi telefonici per i dispositivi MRA non verranno visualizzati. Questa distribuzione non è supportata in base alla sezione 3 della sezione relativa ai suggerimenti riportata di seguito.

DMZ FW a 3 porte con interfaccia LAN Single VCS Expressway

Per il secondo scenario, è necessario applicare questa configurazione di riflessione NAT sul firmware A per consentire la riflessione NAT del traffico in entrata dal VCS Control 10.0.30.2 destinato all'indirizzo IP esterno (64.100.0.10) del VCS Expressway:



Nell'esempio, l'indirizzo IP di VCS Control è **10.0.30.2/24**, mentre l'indirizzo IP di VCS Expressway è **10.0.10.2/24**.

Se si suppone che l'indirizzo IP 10.0.30.2 di VCS Control rimanga quando si sposta dall'interno all'interfaccia DMZ del firmware A durante la ricerca di VCS Expressway con l'indirizzo IP 64.100.0.10 di destinazione, in questi esempi viene mostrata la configurazione di riflessione NAT da implementare sul firmware A.

Esempio di appliance ASA versione 8.3 e successive:

```
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.
```

Esempio di appliance ASA versione 8.2 e precedenti:

```
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
```

> **Nota:** L'obiettivo principale di questa configurazione di riflessione NAT è consentire al controllo VCS di raggiungere l'autostrada VCS, ma con l'indirizzo IP pubblico dell'autostrada VCS invece del suo indirizzo IP privato. Se durante la conversione NAT l'indirizzo IP di origine del controllo VCS viene modificato con una configurazione NAT doppia rispetto alla configurazione NAT suggerita appena mostrata, in modo che VCS Expressway visualizzi il traffico proveniente dal proprio indirizzo IP pubblico, i servizi telefonici per i dispositivi MRA non verranno visualizzati. Questa distribuzione non è supportata in base alla sezione 3 della sezione relativa ai suggerimenti riportata di seguito.

Verifica

In questa sezione vengono forniti gli output del tracer dei pacchetti che è possibile visualizzare nell'ASA per confermare che la configurazione della riflessione NAT funziona come necessario in entrambi gli scenari di implementazione del software VCS C ed E.

DMZ a subnet singola con interfaccia LAN Expressway VCS singola

Di seguito è riportato l'output del tracer dei pacchetti FW B per ASA versioni 8.3 e successive:

```
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
```

Di seguito è riportato l'output del tracer dei pacchetti FW B per ASA versioni 8.2 e precedenti:

```
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 a 3 porte con interfaccia LAN Single VCS Expressway

Di seguito è riportato l'output del tracer dei pacchetti FW-A per ASA versioni 8.3 e successive:

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
```

Di seguito è riportato l'output del tracer dei pacchetti FW-A per ASA versioni 8.2 e precedenti:

```
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
```

Risoluzione dei problemi

Èpossibile configurare le acquisizioni dei pacchetti sulle interfacce ASA in modo da confermare la conversione NAT quando i pacchetti entrano e escono dalle interfacce FW coinvolte.

Acquisizione pacchetti applicata per lo scenario "DMZ FW a 3 porte con interfaccia LAN Expressway VCS singola"

```
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
```

Acquisizione pacchetti applicata per lo scenario "DMZ subnet singola con interfaccia LAN Expressway VCS singola"

```
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
```

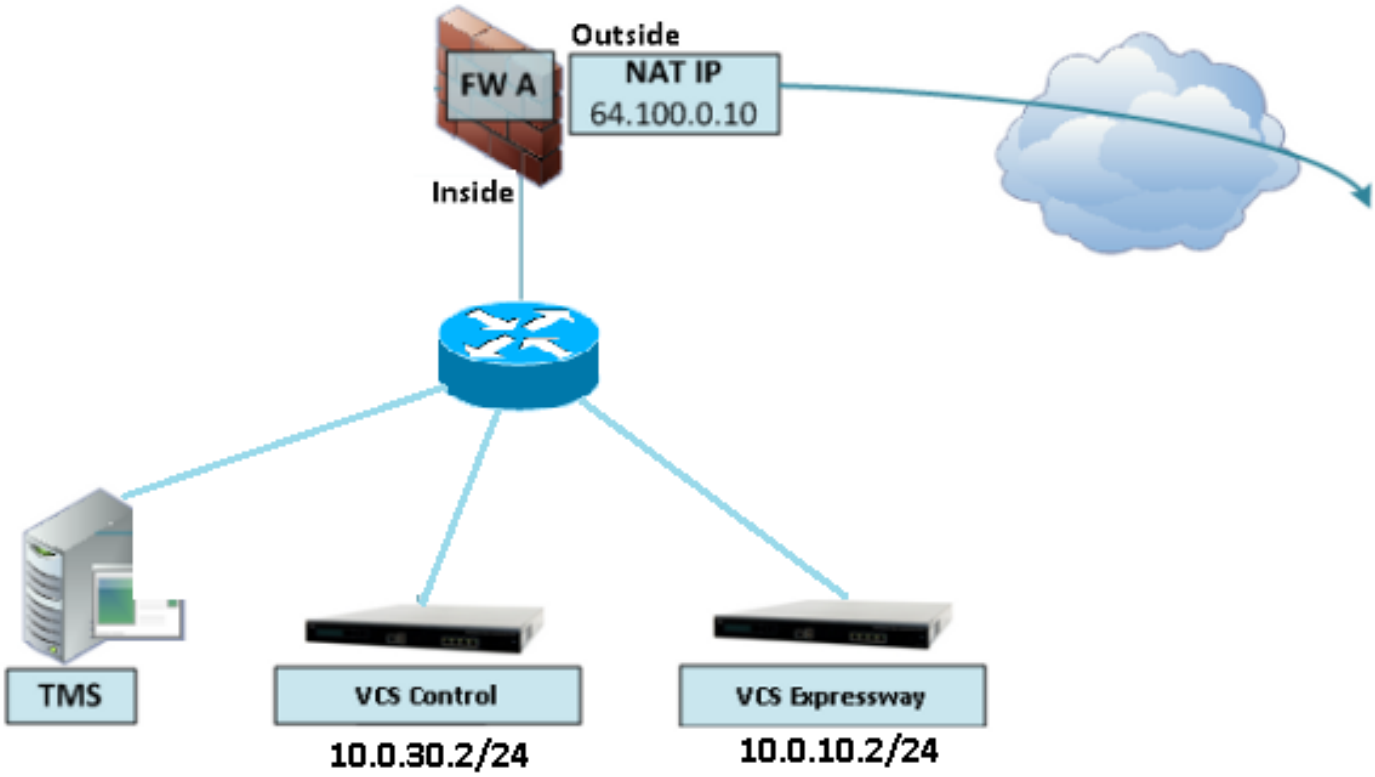
```
FW-B# sh cap capin

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
```

Raccomandazioni

1. Evitare l'implementazione di una topologia non supportata

Ad esempio, se il controllo VCS e VCS Expressway sono collegati dietro l'interfaccia ASA interna, come mostrato di seguito:



Questo tipo di implementazione richiede la conversione dell'indirizzo IP di controllo VCS nell'indirizzo IP interno dell'appliance ASA per forzare il traffico di ritorno sull'appliance ASA e evitare problemi di route asimmetrici per la reflection NAT.

> **Nota: se durante la conversione NAT l'indirizzo IP di origine del controllo VCS viene modificato con una configurazione NAT doppia anziché con la configurazione di riflessione NAT consigliata, VCS Expressway visualizzerà il traffico proveniente dal proprio indirizzo IP pubblico, quindi i servizi telefonici per i dispositivi MRA non verranno visualizzati. Questa distribuzione non è supportata in base alla sezione 3 della sezione relativa ai suggerimenti riportata di seguito.**

Detto questo, si consiglia di implementare VCS Expressway come implementazione di interfacce di rete doppie Expressway-E anziché come NIC singola con riflessione NAT.

2. Assicurarsi che l'ispezione SIP/H.323 sia completamente disabilitata sui firewall interessati

Si consiglia vivamente di disabilitare l'ispezione SIP e H.323 sui firewall che gestiscono il traffico di

rete da e verso Expressway-E. Se abilitato, l'ispezione SIP/H.323 ha spesso effetti negativi sulla funzionalità di attraversamento firewall/NAT integrata in Expressway.

Questo è un esempio di come disabilitare le ispezioni SIP e H.323 sull'appliance ASA.

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

3. Assicurati che la tua effettiva implementazione di Expressway sia conforme ai prossimi requisiti suggeriti dagli sviluppatori di soluzioni di telepresenza Cisco

- La configurazione NAT tra Expressway-C ed Expressway-E non è supportata.
- Non è supportato quando Expressway-C ed Expressway-E, ottengono NATed allo stesso indirizzo IP pubblico, ad esempio:
  Expressway-C è configurato con l'indirizzo IP 10.1.1.1
  Expressway-E ha una singola scheda NIC configurata con l'indirizzo IP 10.2.2.1 e una NAT statica è configurata nel firewall con l'indirizzo IP pubblico 64.100.0.10
  Quindi Expressway-C non può essere NATted allo stesso indirizzo pubblico 64.100.0.10

Implementazione VCS Expressway consigliata

L'implementazione consigliata per VCS Expressway anziché per VCS Expressway con configurazione di riflessione NAT è l'implementazione di due interfacce di rete/due schede di interfaccia di rete VCS Expressway. Per ulteriori informazioni, visitare il collegamento successivo.

Configurazione ASA NAT e raccomandazioni per l'implementazione delle interfacce di rete doppie Expressway-E.

Informazioni correlate

- Configurazione ASA NAT e raccomandazioni per l'implementazione delle interfacce di rete doppie Expressway-E
- Guida all'installazione di Cisco TelePresence Video Communication Server di configurazione base (controllo con Expressway)
- Cisco Expressway Utilizzo porta IP per attraversamento firewall
- Posizionamento di Cisco VCS Expressway in una DMZ piuttosto che nella rete Internet pubblica