Konfigurieren der NAT-Reflektion auf der ASA für die VCS Expressway TelePresence-Geräte

Inhalt

Einführung

Dieses Dokument beschreibt die Implementierung einer NAT-Reflektionskonfiguration (Network Address Translation) auf den Cisco Adaptive Security Appliances für spezielle Cisco TelePresence-Szenarien, die eine solche NAT-Konfiguration auf der Firewall erfordern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende NAT-Konfiguration der Cisco ASA (Adaptive Security Appliance)
- Grundkonfiguration des Cisco TelePresence Video Communication Server (VCS) Control und VCS Expressway.

> **Hinweis**: Dieses Dokument ist nur für den Fall vorgesehen, dass die empfohlene Bereitstellungsmethode eines VCS-Expressway oder Expressway-Edge mit beiden NIC-Schnittstellen in unterschiedlichen DMZs nicht verwendet werden kann. Weitere Informationen zur empfohlenen Bereitstellung mit dualen NICs finden Sie unter dem folgenden Link auf Seite 60: Implementierungsleitfaden für Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Appliances der Serien ASA 5500 und 5500-X, auf denen die Software Version 8.3 und höher ausgeführt wird.
- Cisco VCS Version X8.x und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

> **Hinweis**: Im gesamten Dokument werden VCS-Geräte als VCS Expressway und VCS Control bezeichnet. Die gleiche Konfiguration gilt jedoch auch für Expressway-E- und Expressway-C-Geräte.

Hintergrundinformationen

Gemäß der Dokumentation zu Cisco TelePresence gibt es zwei Arten von TelePresence-Szenarien, bei denen die NAT-Reflektionskonfiguration auf den FWs erforderlich ist, damit das VCS Control über die öffentliche IP-Adresse des VCS Expressway mit dem VCS Expressway kommunizieren kann.

Das erste Szenario umfasst eine einzige demilitarisierte Zone (DMZ), die eine VCS Expressway LAN-Schnittstelle verwendet, und das zweite Szenario eine FW-DMZ mit drei Ports, die eine VCS Expressway LAN-Schnittstelle verwendet.

> **Tipp**: Weitere Informationen zur TelePresence-Implementierung finden Sie im Bereitstellungsleitfaden für Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway).

Für die VCS C- und E-Implementierung nicht empfohlene Cisco Topologien

Die folgenden Topologien werden von Cisco NICHT empfohlen. Die empfohlene

Bereitstellungsmethode für einen VCS Expressway- oder Expressway-Edge besteht darin, zwei verschiedene DMZs zu verwenden, wobei der Expressway über eine NIC in jeder der DMZs verfügt. Dieser Leitfaden ist für Umgebungen vorgesehen, in denen die empfohlene Bereitstellungsmethode nicht verwendet werden kann.

Einzel-Subnetz-DMZ mit einer VCS Expressway-LAN-Schnittstelle

In diesem Szenario kann FW A Datenverkehr an FW B weiterleiten (und umgekehrt). Der VCS Expressway ermöglicht die Weiterleitung von Videodatenverkehr über FW B, ohne dass der Datenverkehrsfluss auf FW B von außen zu den internen Schnittstellen reduziert wird. Der VCS Expressway verarbeitet auch FW-Traversal auf seiner öffentlichen Seite.

Hier ein Beispiel für dieses Szenario:

Bei dieser Bereitstellung werden folgende Komponenten verwendet:

- Eine einzelne Subnetz-DMZ (10.0.10.0/24), die Folgendes enthält:
  Die interne Schnittstelle von FW A (10.0.10.1)Die externe Schnittstelle von FW B (10.0.10.2)Die LAN1-Schnittstelle des VCS Expressway (10.0.10.3)
- Ein LAN-Subnetz (10.0.30.0/24), das Folgendes enthält:
  Die interne Schnittstelle von FW B (10.0.30.1)Die LAN1-Schnittstelle des VCS Control (10.0.30.2)Die Netzwerkschnittstelle des Cisco TelePresence Management Server (TMS) (10.0.30.3)

Für FW A wurde eine statische Eins-zu-Eins-NAT konfiguriert, die die NAT für die öffentliche Adresse 64.100.0.10 an die LAN1-IP-Adresse des VCS Expressway ausführt. Der statische NAT-Modus wurde für die LAN1-Schnittstelle auf dem VCS Expressway mit der statischen NAT-IP-Adresse 64.100.0.10 aktiviert.

> **Hinweis**: Sie müssen den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des VCS Expressway in der VCS Control Secure Traversal Client Zone (Peer-Adresse) eingeben, wie er von außerhalb des Netzwerks gesehen wird. Der Grund hierfür ist, dass der VCS Expressway im statischen NAT-Modus die Übermittlung des eingehenden Signalisierungs- und Mediendatenverkehrs an seinen externen FQDN anfordert, anstatt an seinen privaten Namen. Dies bedeutet auch, dass die externe FW den Datenverkehr vom VCS Control zum externen VCS Expressway FQDN erlauben muss. Dies wird als NAT-Reflektion bezeichnet und wird möglicherweise nicht von allen FW-Typen unterstützt.

In diesem Beispiel muss FW B die NAT-Reflektion des Datenverkehrs des VCS Control ermöglichen, der für die externe IP-Adresse (64.100.0.10) des VCS Expressway bestimmt ist. Die Traversal-Zone im VCS Control muss als Peer-Adresse 64.100.0.10 aufweisen (nach FQDN-IP-Konvertierung).

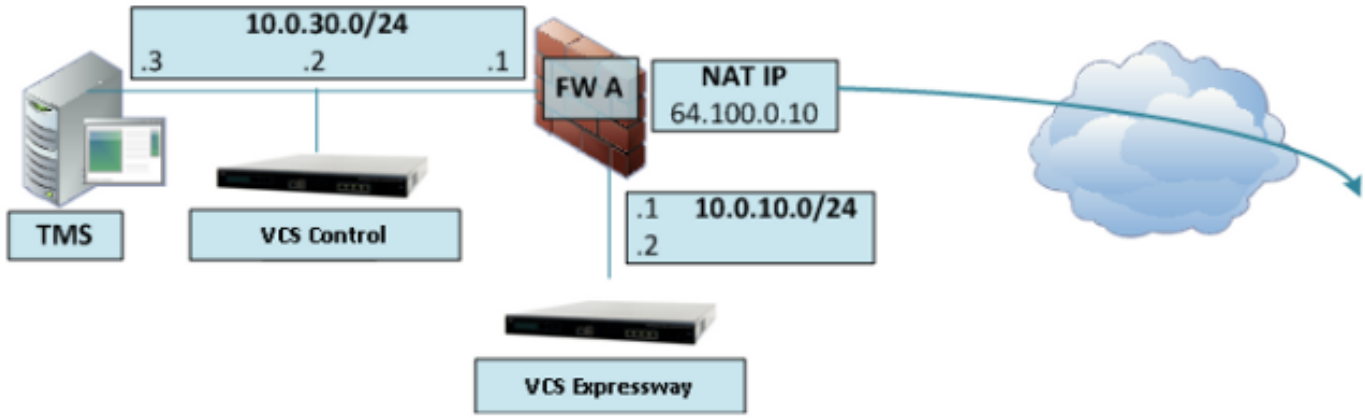
Der VCS Expressway sollte mit einem Standard-Gateway von **10.0.10.1** konfiguriert werden. Ob in

diesem Szenario statische Routen erforderlich sind, hängt von den Funktionen und Einstellungen von FW A und FW B ab. Die Kommunikation vom VCS Control zum VCS Expressway erfolgt über die IP-Adresse 64.100.0.10 des VCS Expressway; und der Rückverkehr vom VCS Expressway zum VCS Control muss möglicherweise über das Standard-Gateway weitergeleitet werden.

Der VCS Expressway kann dem Cisco TMS mit der IP-Adresse 10.0.10.3 (oder mit der IP-Adresse 64.100.0.10, falls FW B dies zulässt) hinzugefügt werden, da die Cisco TMS-Managementkommunikation nicht von den statischen Einstellungen des NAT-Modus auf dem VCS Expressway beeinflusst wird.

FW-DMZ mit 3 Ports und einer VCS Expressway-LAN-Schnittstelle

Hier ein Beispiel für dieses Szenario:



Bei dieser Bereitstellung wird eine FW mit 3 Ports verwendet, um Folgendes zu erstellen:

- Ein DMZ-Subnetz (10.0.10.0/24), das Folgendes enthält:
  Die DMZ-Schnittstelle von FW A (10.0.10.1)Die LAN1-Schnittstelle des VCS Expressway (10.0.10.2)
- Ein LAN-Subnetz (10.0.30.0/24), das Folgendes enthält:
  Die LAN-Schnittstelle von FW A (10.0.30.1)Die LAN1-Schnittstelle des VCS Control (10.0.30.2)Die Netzwerkschnittstelle der Cisco TMS (10.0.30.3)

Für FW A wurde eine statische Eins-zu-Eins-NAT konfiguriert, die die NAT der öffentlichen IP-Adresse 64.100.0.10 für die LAN1-IP-Adresse des VCS Expressway ausführt. Der statische NAT-Modus wurde für die LAN1-Schnittstelle auf dem VCS Expressway mit der statischen NAT-IP-Adresse 64.100.0.10 aktiviert.

Der VCS Expressway sollte mit einem Standard-Gateway von 10.0.10.1 konfiguriert werden. Da dieses Gateway für den gesamten Datenverkehr verwendet werden muss, der den VCS Expressway verlässt, sind für diese Art der Bereitstellung keine statischen Routen erforderlich.

Die Traversal-Clientzone im VCS Control muss mit einer Peer-Adresse konfiguriert werden, die der statischen NAT-Adresse des VCS Expressway entspricht (in diesem Beispiel 64.100.0.10), und zwar aus den gleichen Gründen wie im vorherigen Szenario.

> **Hinweis**: Das bedeutet, dass FW A Datenverkehr vom VCS Control mit der Ziel-IP-Adresse 64.100.0.10 zulassen muss. Dies wird auch als NAT-Reflektion bezeichnet, und dies wird nicht von allen FW-Typen unterstützt.

Der VCS Expressway kann dem Cisco TMS mit der IP-Adresse 10.0.10.2 (oder mit der IP-Adresse 64.100.0.10, falls FW A dies zulässt) hinzugefügt werden, da die Cisco TMS-Managementkommunikation nicht von den statischen Einstellungen des NAT-Modus auf dem VCS Expressway beeinflusst wird.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie die NAT-Reflektion in der ASA für die beiden verschiedenen VCS C- und E-Implementierungsszenarien konfiguriert wird.

Einzel-Subnetz-DMZ mit einer VCS Expressway-LAN-Schnittstelle

Im ersten Szenario müssen Sie diese NAT-Reflektionskonfiguration auf FW A anwenden, um die Kommunikation vom VCS Control (10.0.30.2) zu ermöglichen, das für die externe IP-Adresse (64.100.0.10) des VCS Expressway bestimmt ist:

In diesem Beispiel lautet die IP-Adresse des VCS Control **10.0.30.2/24**, und die IP-Adresse des VCS Expressway lautet **10.0.10.3/24**.

Wenn Sie annehmen, dass die IP-Adresse 10.0.30.2 der VCS Control, wenn sie von innen zur Außenschnittstelle von FW B verschoben wird, wenn Sie den VCS Expressway mit der Ziel-IP-Adresse 64.100.0.10 suchen, wird in diesen Beispielen die NAT-Reflektionskonfiguration gezeigt, die Sie auf FW B implementieren sollten.

Beispiel für ASA Version 8.3 und höher:

```
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.
```

Beispiel für ASA Version 8.2 und frühere Versionen:

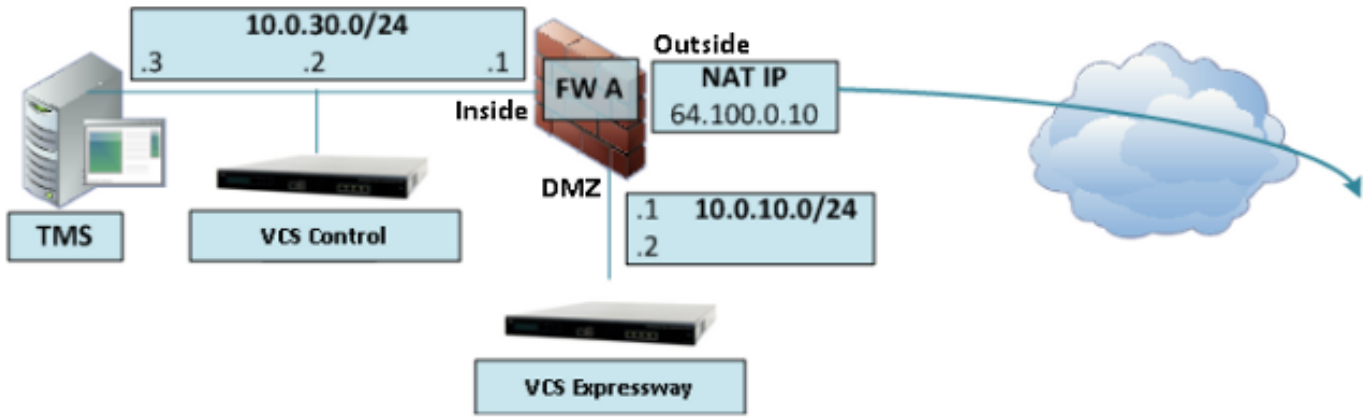
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
```

```
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
```

Hinweis: Das Hauptziel dieser NAT-Reflektionskonfiguration besteht darin, dem VCS Control die Erreichbarkeit der VCS-Schnellstraße zu ermöglichen. Dabei wird jedoch die öffentliche IP-Adresse des VCS-Schnellstraße anstelle der privaten IP-Adresse verwendet. Wenn die Quell-IP-Adresse des VCS Control während dieser NAT-Übersetzung mit einer doppelten NAT-Konfiguration anstelle der vorgeschlagenen NAT-Konfiguration geändert wird, sodass der Datenverkehr von der eigenen öffentlichen IP-Adresse des VCS Expressway empfangen wird, werden die Telefondienste für die MRA-Geräte nicht angezeigt. Diese Bereitstellung wird gemäß Abschnitt 3 im Abschnitt "Empfehlungen" unten nicht unterstützt.

FW-DMZ mit 3 Ports und einer VCS Expressway-LAN-Schnittstelle

Im zweiten Szenario müssen Sie diese NAT-Reflektionskonfiguration auf FW A anwenden, um die NAT-Reflektion des eingehenden Datenverkehrs vom VCS Control 10.0.30.2 zu ermöglichen, der für die externe IP-Adresse (64.100.0.10) des VCS Expressway bestimmt ist:



In diesem Beispiel lautet die IP-Adresse des VCS Control **10.0.30.2/24**, und die IP-Adresse des VCS Expressway lautet **10.0.10.2/24**.

Wenn Sie annehmen, dass die IP-Adresse 10.0.30.2 der VCS Control, wenn sie von innen zur DMZ-Schnittstelle von FW A verschoben wird, wenn Sie den VCS Expressway mit der Ziel-IP-Adresse 64.100.0.10 suchen, wird in diesen Beispielen die NAT-Reflektionskonfiguration gezeigt, die Sie auf FW A implementieren sollten.

Beispiel für ASA Version 8.3 und höher:

```
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.
```

Beispiel für ASA Version 8.2 und frühere Versionen:

```
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
```

> **Hinweis**: Das Hauptziel dieser NAT-Reflektionskonfiguration besteht darin, dem VCS Control die Möglichkeit zu geben, die VCS-Schnellstraße zu erreichen, jedoch mit der öffentlichen IP-Adresse der VCS-Schnellstraße anstelle der privaten IP-Adresse. Wenn die Quell-IP-Adresse des VCS Control während dieser NAT-Übersetzung mit einer doppelten NAT-Konfiguration anstelle der vorgeschlagenen NAT-Konfiguration geändert wird, sodass der VCS Expressway Datenverkehr von seiner eigenen öffentlichen IP-Adresse empfängt, werden die Telefondienste für die MRA-Geräte nicht angezeigt. Diese Bereitstellung wird gemäß Abschnitt 3 im Abschnitt "Empfehlungen" unten nicht unterstützt.

Überprüfen

Dieser Abschnitt enthält die Pakettracer-Ausgaben, die in der ASA angezeigt werden, um zu bestätigen, dass die NAT-Reflektionskonfiguration in beiden VCS C- und E-Implementierungsszenarien nach Bedarf funktioniert.

Einzel-Subnetz-DMZ mit einer VCS Expressway-LAN-Schnittstelle

Hier ist die FW B Packet Tracer-Ausgabe für ASA Version 8.3 und höher:

```
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
```

Hier ist die Ausgabe des FW B-Paket-Tracers für ASA Version 8.2 und frühere Versionen:

```
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
```

FW-DMZ mit 3 Ports und einer VCS Expressway-LAN-Schnittstelle

Hier ist die Ausgabe von FW A Packet Tracer für ASA Version 8.3 und höher:

```
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
```

Hier ist die Ausgabe des FW A-Paket-Tracers für ASA Version 8.2 und frühere Versionen:

```
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
```

Fehlerbehebung

Sie können Paketerfassungen auf den ASA-Schnittstellen konfigurieren, um die NAT-Übersetzung zu bestätigen, wenn die Pakete die betroffenen FW-Schnittstellen eingehen und verlassen.

Paketerfassung für das Szenario "3-Port-FW-DMZ mit Single VCS Expressway LAN Interface"

```
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
```

Paketerfassung für das Szenario "Einzel-Subnetz-DMZ mit Einzel-VCS-Expressway-LAN-Schnittstelle" angewendet

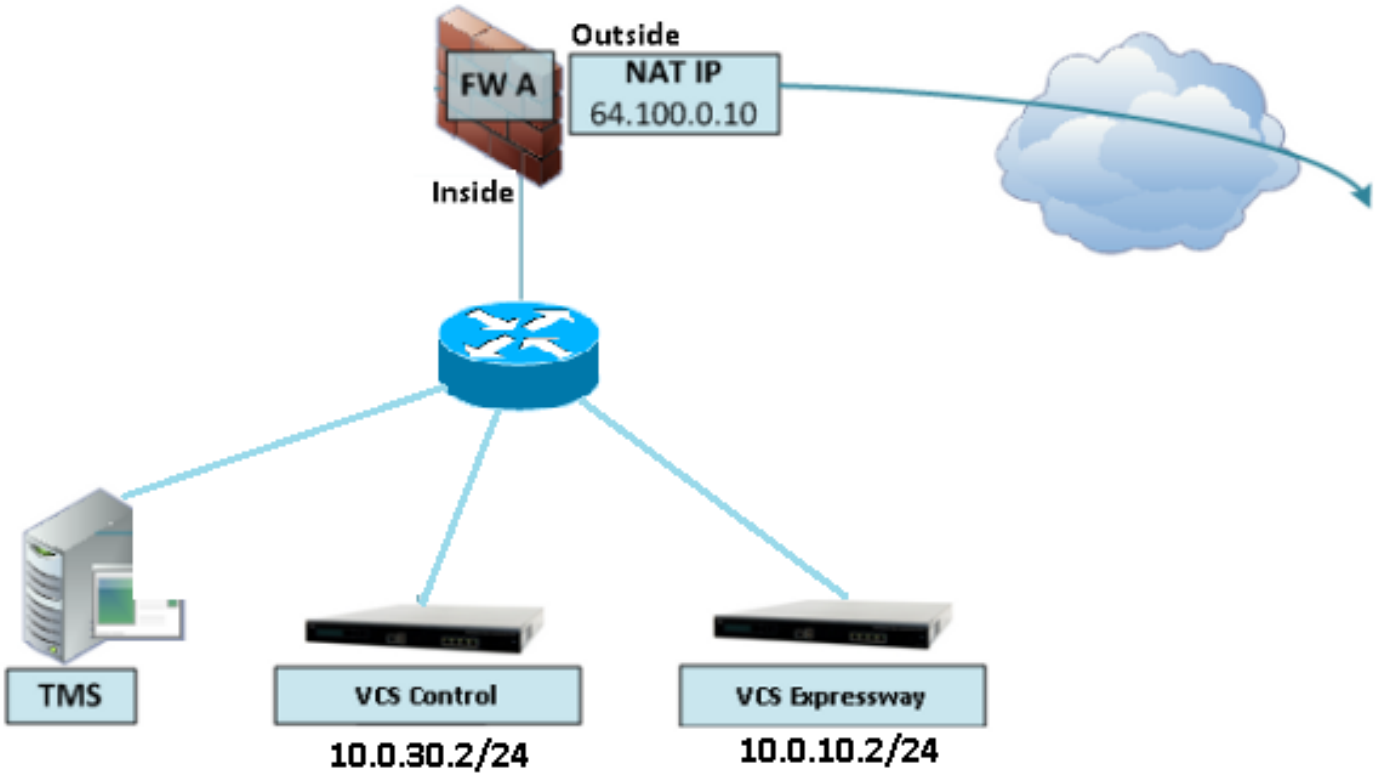
```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

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
```

Empfehlungen

1. Implementieren Sie keine nicht unterstützte Topologie.

Wenn beispielsweise hinter der internen ASA-Schnittstelle sowohl das VCS Control als auch der VCS Expressway verbunden sind, wie in diesem Szenario gezeigt:



Für eine solche Implementierung muss die VCS Control IP-Adresse in die interne IP-Adresse der ASA übersetzt werden, damit der zurückkehrende Datenverkehr zur ASA zurückgeleitet wird, um Probleme mit asymmetrischen Routen für die NAT-Reflektion zu vermeiden.

> **Hinweis: Wenn die Quell-IP-Adresse des VCS Control während dieser NAT-Übersetzung mit einer Konfiguration mit doppelter NAT anstelle der vorgeschlagenen NAT-Reflektionskonfiguration geändert wird, wird der VCS Expressway Datenverkehr von seiner eigenen öffentlichen IP-Adresse sehen, dann werden die Telefondienste für die MRA-Geräte nicht angezeigt. Diese Bereitstellung wird gemäß Abschnitt 3 im Abschnitt "Empfehlungen" unten nicht unterstützt.**

Dennoch wird dringend empfohlen, den VCS Expressway als Expressway-E Dual Network Interfaces Implementation anstelle der NIC mit NAT Reflection zu implementieren.

2. Stellen Sie sicher, dass die SIP/H.323-Inspektion für die beteiligten Firewalls vollständig deaktiviert ist.

Es wird dringend empfohlen, die SIP- und H.323-Inspektion auf Firewalls zu deaktivieren, die den Netzwerkverkehr zu oder von einem Expressway-E behandeln. Bei Aktivierung wird häufig festgestellt, dass sich die SIP/H.323-Inspektion negativ auf die integrierte Firewall-/NAT-Traversal-Funktionalität von Expressway auswirkt.

Dies ist ein Beispiel dafür, wie SIP- und H.323-Inspektionen auf der ASA deaktiviert werden.

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

3. Stellen Sie sicher, dass Ihre eigentliche Expressway-Implementierung die nächsten Anforderungen erfüllt, die von den Cisco TelePresence-Entwicklern vorgeschlagen wurden.

- Die NAT-Konfiguration zwischen Expressway-C und Expressway-E wird nicht unterstützt.
- Es wird nicht unterstützt, wenn Expressway-C und Expressway-E NAT an dieselbe öffentliche IP-Adresse senden, z. B.:
  Expressway-C wird mit der IP-Adresse 10.1.1.1 konfiguriert.
  Für Expressway-E ist eine einzelne NIC mit der IP-Adresse 10.2.2.1 konfiguriert, und in der Firewall wird eine statische NAT mit der öffentlichen IP-Adresse 64.100.0.10 konfiguriert.
  Anschließend kann der Expressway-C nicht an dieselbe öffentliche Adresse 64.100.0.10 geleitet werden.

Empfohlene VCS Expressway-Implementierung

Die empfohlene Implementierung für den VCS Expressway anstelle des VCS Expressway mit der NAT Reflection Konfiguration ist die Implementierung von zwei Netzwerkschnittstellen/Dual NIC VCS Expressway. Weitere Informationen hierzu finden Sie unter dem nächsten Link.

ASA NAT-Konfiguration und Empfehlungen für die Implementierung von Expressway-E Dual Network Interfaces

Zugehörige Informationen

- ASA NAT-Konfiguration und Empfehlungen für die Implementierung von Expressway-E Dual Network Interfaces
- Cisco TelePresence Video Communication Server - Grundkonfiguration (Steuerung mit Expressway) - Implementierungsleitfaden
- Verwendung der Cisco Expressway-IP-Ports für Firewall-Überbrückung

- Platzieren eines Cisco VCS Expressway in einer DMZ statt im öffentlichen Internet