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

Inhalt

Einführung

Dieses Dokument beschreibt die Implementierung der Network Address Translation (NAT)-Konfiguration, die in der Cisco Adaptive Security Appliance (ASA) für die Implementierung von Expressway-E Dual Network Interfaces erforderlich ist.

Tipp: Diese Bereitstellung ist die empfohlene Option für die Expressway-E-Implementierung und nicht die Single-NIC-Implementierung mit NAT-Reflektion.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Konfiguration und NAT-Konfiguration von Cisco ASA
- Basiskonfiguration für Cisco Expressway-E und Expressway-C

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 8.0 und höher ausgeführt wird.
- Cisco Expressway Version X8.0 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 die Schnellstraßengeräte als Expressway-E und Expressway-C bezeichnet. Die gleiche Konfiguration gilt jedoch auch für die Video Communication Server (VCS) Expressway- und VCS Control-Geräte.

Hintergrundinformationen

Cisco Expressway-E kann standardmäßig entweder in einer demilitarisierten Zone (DMZ) oder über eine Internet-Schnittstelle bereitgestellt werden, während es in einem privaten Netzwerk mit Cisco Expressway-C kommunizieren kann. Wenn Cisco Expressway-E in einer DMZ platziert wird, ergeben sich folgende zusätzliche Vorteile:

- Im gängigsten Szenario wird Cisco Expressway-E vom privaten Netzwerk verwaltet. Wenn sich Cisco Expressway-E in einer DMZ befindet, kann eine Perimeter-Firewall (extern) verwendet werden, um unerwünschten Zugriff auf Expressway aus externen Netzwerken über Hypertext Transfer Protocol Secure (HTTPS)- oder Secure Shell (SSH)-Anfragen zu blockieren.

- Wenn die DMZ keine direkten Verbindungen zwischen internen und externen Netzwerken zulässt, sind dedizierte Server erforderlich, um Datenverkehr zu verarbeiten, der die DMZ passiert. Cisco Expressway kann als Proxyserver für SIP (Session Initiation Protocol) und/oder H.323-Sprach- und Videodatenverkehr fungieren. In diesem Fall können Sie die

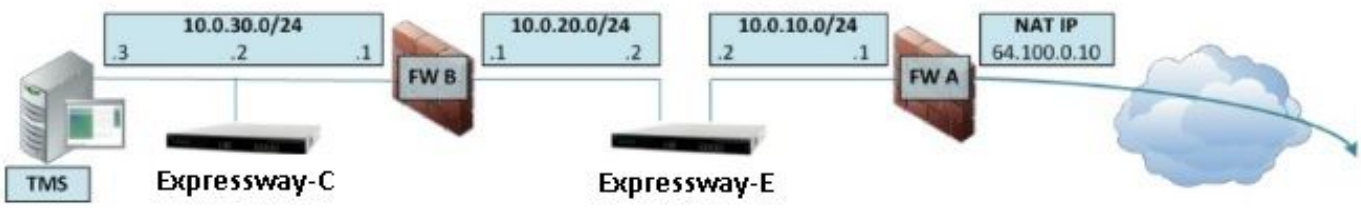
Dual-Network-Schnittstellen-Option verwenden, mit der Cisco Expressway über zwei verschiedene IP-Adressen verfügen kann: eine für den Datenverkehr zur/von der externen Firewall und eine für den Datenverkehr zur/von der internen Firewall.

- Diese Konfiguration verhindert direkte Verbindungen vom externen Netzwerk zum internen Netzwerk. Dadurch wird die interne Netzwerksicherheit insgesamt verbessert.

Tipp: Weitere Informationen zur TelePresence-Implementierung finden Sie unter Cisco Expressway-E und Expressway-C - Basic Configuration Deployment Guide und Placing a Cisco VCS Expressway in a DMZ and in a public internet.

Expressway C und E - Dual Network Interfaces/Dual NIC Implementation

Dieses Bild zeigt eine Beispielbereitstellung für ein Expressway-E mit dualen Netzwerkschnittstellen und statischer NAT. Expressway-C agiert als Traversal-Client. Es gibt zwei Firewalls (FW A und FWB). In der Regel kann FW A in dieser DMZ-Konfiguration den Datenverkehr nicht an FW B weiterleiten. Geräte wie der Expressway-E müssen Datenverkehr vom Subnetz von FW A zum Subnetz von FW B validieren und weiterleiten (und umgekehrt).



Diese Bereitstellung besteht aus diesen Komponenten.

DMZ-Subnetz 1 - 10.0.10.0/24

- FW Eine interne Schnittstelle - 10.0.10.1
- Expressway-E LAN2-Schnittstelle - 10.0.10.2

DMZ-Subnetz 2 - 10.0.20.0/24

- Externe FW B-Schnittstelle - 10.0.20.1
- Expressway-E LAN1-Schnittstelle - 10.0.20.2

LAN-Subnetz - 10.0.30.0/24

- Interne FW B-Schnittstelle - 10.0.30.1
- Expressway-C LAN1-Schnittstelle - 10.0.30.2
- Cisco TelePresence Management Suite (TMS) Server-Netzwerkschnittstelle - 10.0.30.3

Einzelheiten dieser Implementierung:

- FW A ist die externe oder Perimeterfirewall. Es wird mit NAT IP (Public IP, öffentliche IP) von 64.100.0.10 konfiguriert, das statisch in 10.0.10.2 übersetzt wird (Expressway-E LAN2-Schnittstelle).
- FW B ist die interne Firewall
- Expressway-E LAN1 ist im statischen NAT-Modus deaktiviert.
- Für Expressway-E LAN2 ist der statische NAT-Modus mit der statischen NAT-Adresse

64.100.0.10 aktiviert.
- Expressway-C verfügt über eine Traversal-Clientzone, die auf 10.0.20.2 zeigt (Expressway-E LAN1-Schnittstelle).
- Zwischen den Subnetzen 10.0.20.0/24 und 10.0.10.0/24 gibt es kein Routing. Expressway-E überbrückt diese Subnetze und fungiert als Proxy für SIP/H.323-Signalisierungs- und Real-Time Transport Protocol (RTP)/RTP Control Protocol (RTCP)-Medien.
- Für Cisco TMS wurde Expressway-E mit der IP-Adresse 10.0.20.2 konfiguriert.

Anforderungen/Einschränkungen

Nicht überlappende Subnetze

Wenn Expressway-E für die Verwendung beider LAN-Schnittstellen konfiguriert ist, müssen sich die LAN1- und LAN2-Schnittstellen in nicht überlappenden Subnetzen befinden, um sicherzustellen, dass der Datenverkehr an die richtige Schnittstelle gesendet wird.

Clustering

Beim Clustering von Expressway-Geräten mit konfigurierter Advanced Networking-Option muss jeder Cluster-Peer mit einer eigenen LAN1-Schnittstellenadresse konfiguriert werden. Darüber hinaus muss das Clustering auf einer Schnittstelle konfiguriert werden, für die der statische NAT-Modus nicht aktiviert ist. Daher wird empfohlen, LAN2 als externe Schnittstelle zu verwenden, auf die Sie ggf. statische NAT anwenden und konfigurieren können.

Einstellungen für externe LAN-Schnittstellen

Die Konfigurationseinstellungen für die externe LAN-Schnittstelle auf der IP-Konfigurationsseite, die von der Netzwerkschnittstelle mithilfe von Transversal Using Relays around NAT (TURN) verwendet wird. In einer Expressway-E Konfiguration mit dualer Netzwerkschnittstelle wird diese normalerweise auf die externe Expressway-E LAN-Schnittstelle eingestellt.

Statische Routen

Für dieses Szenario muss Expressway-E mit der Standard-Gateway-Adresse 10.0.10.1 konfiguriert werden. Das bedeutet, dass der gesamte über LAN2 gesendete Datenverkehr standardmäßig an die IP-Adresse 10.0.10.1 gesendet wird.

Wenn FW B Datenverkehr übersetzt, der vom Subnetz 10.0.30.0/24 an die LAN1-Schnittstelle Expressway-E gesendet wird (z. B. Expressway-C-Traversal Client-Datenverkehr oder TMS Server Management-Datenverkehr), wird dieser Datenverkehr so angezeigt, als er von der externen FWB-Schnittstelle (10.0.20.1) kommt, wenn er Expressway-E LAN1 erreicht. Expressway-E kann dann über seine LAN1-Schnittstelle auf diesen Datenverkehr antworten, da sich die scheinbare Quelle dieses Datenverkehrs im gleichen Subnetz befindet.

Wenn NAT auf FW B aktiviert ist, wird der vom Expressway-C an Expressway-E LAN1 gesendete Datenverkehr als Ausgangswert von 10.0.30.2 angezeigt. Wenn Expressway keine statische Route für das Subnetz 10.0.30.0/24 hinzugefügt hat, sendet es die Antworten für diesen Datenverkehr an das Standard-Gateway (10.0.10.1) aus LAN2, da es nicht weiß, dass sich das Subnetz 10.0.30.0/24 hinter der internen Firewall (FW B) befindet. Daher muss eine statische

Route hinzugefügt werden. Führen Sie den Befehl **xCommand RouteAdd** CLI über eine SSH-Sitzung mit Expressway aus.

In diesem Beispiel muss Expressway-E wissen, dass es das Subnetz 10.0.30.0/24 hinter FW B erreichen kann, das über die LAN1-Schnittstelle erreichbar ist. Führen Sie dazu den folgenden Befehl aus:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **Hinweis**: SDie statische Routenkonfiguration kann über die Expressway-E GUI sowie über **System/Netzwerk > Schnittstellen/Static Routes** angewendet werden.

In diesem Beispiel kann der Parameter Interface (Schnittstelle) auch auf **Auto (Automatisch)** festgelegt werden, da die Gateway-Adresse (10.0.20.1) nur über LAN1 erreichbar ist.

Wenn NAT auf FW B nicht aktiviert ist und Expressway-E mit Geräten in Subnetzen (außer 10.0.30.0/24) kommunizieren muss, die sich ebenfalls hinter FW B befinden, müssen für diese Geräte/Subnetze statische Routen hinzugefügt werden.

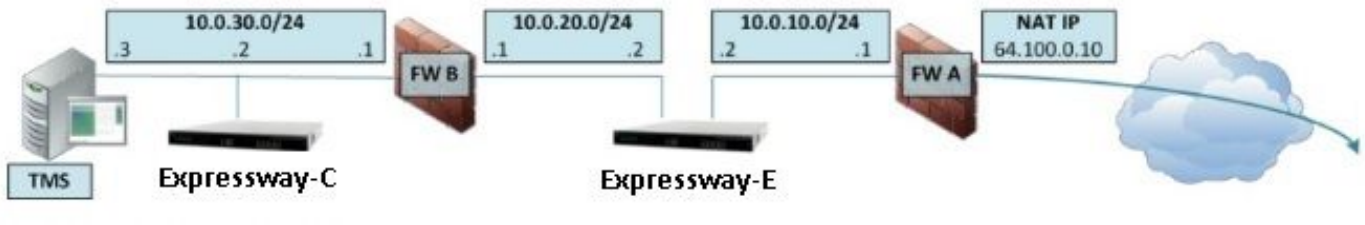
> **Hinweis**: Dazu gehören SSH- und HTTPS-Verbindungen von Netzwerkmanagement-Workstations oder für Netzwerkdienste wie NTP, DNS, LDAP/AD oder Syslog.

Der Befehl **xCommand RouteAdd** und die Syntax werden ausführlich im VCS-Administratorhandbuch beschrieben.

Konfiguration

In diesem Abschnitt wird beschrieben, wie die für die Expressway-E Dual-Network Interface-Implementierung auf der ASA erforderliche statische NAT konfiguriert wird. Für die Verarbeitung von SIP-/H323-Datenverkehr sind einige zusätzliche Konfigurationsempfehlungen für das ASA Modular Policy Framework (MPF) enthalten.

Expressway C und E - Dual Network Interfaces/Dual NIC Implementation



In diesem Beispiel ist die IP-Adressenzuweisung die nächste.

Expressway-C IP-Adresse: 10.0.30.2/24

Expressway-C Standard-Gateway: 10.0.30.1 (FW-B)

Expressway-E-IP-Adressen:

Im LAN2: 10.0.10.2/24

In LAN1: 10.0.20.2/24

Expressway-E Standard-Gateway: 10.0.10.1 (FW-A)

TMS-IP-Adresse: 10.0.30.3/24

FW-A-Konfiguration

Schritt 1: Statische NAT-Konfiguration für Expressway-E.

Wie im Abschnitt "Hintergrundinformationen" dieses Dokuments erläutert, verfügt FW-A über eine statische NAT-Übersetzung, um Expressway-E über das Internet mit der öffentlichen IP-Adresse 64.100.0.10 erreichbar zu machen. Diese letzte Adresse ist NATed to Expressway-E LAN2 IP address 10.0.10.2/24. Dies ist jedoch die erforderliche statische FW-A-NAT-Konfiguration.

Für ASA Version 8.3 und höher:

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR ! To use with static one-to-one NAT: object network obj-10.0.10.2 nat
(inside,outside) static interface
```

> **Vorsicht**: Wenn Sie die statischen PAT-Befehle anwenden, erhalten Sie diese Fehlermeldung in der ASA-Befehlszeilenschnittstelle **"FEHLER: NAT kann keine Ports reservieren"**. Danach löschen Sie die Xlate-Einträge auf der ASA. Führen Sie hierfür den Befehl **clearxlatelocal x.x.x.x aus,** wobei x.x.x.x der externen ASA-IP-Adresse entspricht. Dieser Befehl löscht alle Übersetzungen, die dieser IP-Adresse zugeordnet sind, und führt sie in Produktionsumgebungen mit Vorsicht aus.

Für ASA Version 8.2 und frühere Versionen:

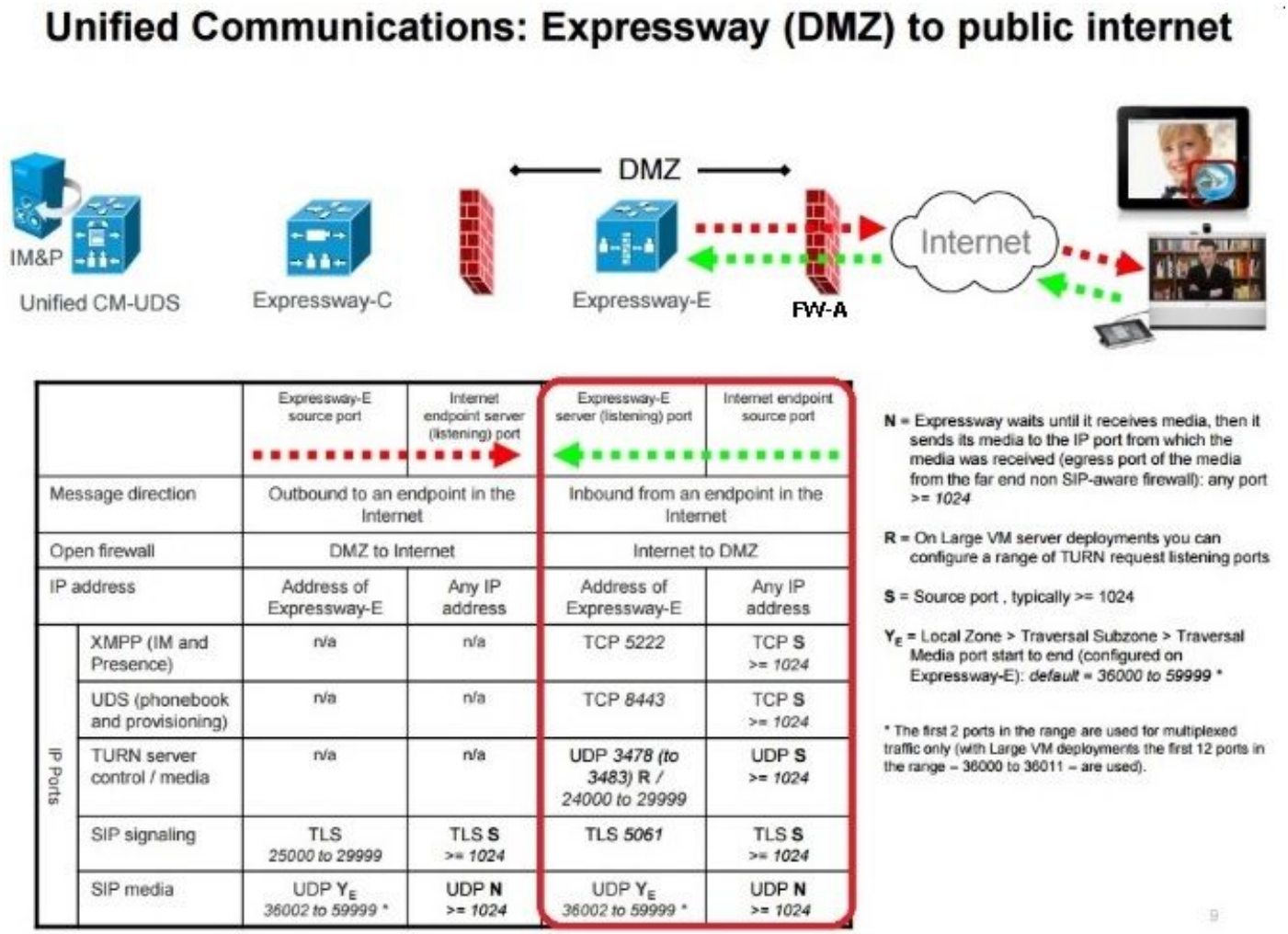
```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Schritt 2: Die ACL-Konfiguration (Access Control List) ermöglicht die erforderlichen Ports vom

Internet zum Expressway-E.

Laut Unified Communication: Expressway (DMZ) zur Dokumentation des öffentlichen Internets. Die Liste der TCP- und UDP-Ports, die Expressway-E in FW-A zulassen muss, ist im Bild dargestellt:



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

Dies ist die erforderliche ACL-Konfiguration für eingehenden Datenverkehr an der externen FW-A-Schnittstelle.

Für ASA Version 8.3 und höher:

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

Für ASA Version 8.2 und frühere Versionen:

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061

access-group outside-in in interface outside
```

FW-B-Konfiguration

Wie im Abschnitt Hintergrundinformationen dieses Dokuments erläutert, erfordert FW B möglicherweise eine dynamische NAT- oder PAT-Konfiguration, damit das interne Subnetz 10.0.30.0/24 in die IP-Adresse 10.0.20.1 übersetzt werden kann, wenn es zur externen Schnittstelle von FW B wechselt.

Für ASA Version 8.3 und höher:

```
object network obj-10.0.30.0
   subnet 10.0.30.0 255.255.255.0
   nat (inside,outside) dynamic interface
```

Für ASA Version 8.2 und frühere Versionen:

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

> **Tipp**: Stellen Sie sicher, dass alle erforderlichen TCP- und UDP-Ports den Expressway-C ordnungsgemäß funktionieren und im FW B offen sind, wie in diesem Cisco Dokument beschrieben: Cisco Expressway IP Port Usage for Firewall Traversal

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Packet Tracer kann auf der ASA verwendet werden, um zu bestätigen, dass die statische Expressway-E NAT-Übersetzung nach Bedarf funktioniert.

Packet Tracer auf Test 64.100.0.10 bei TCP/5222

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
```

```
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 13, packet dispatched to next module

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

Packet Tracer auf Test 64.100.0.10 bei TCP/8443

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
```

```
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 14, packet dispatched to next module

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

Packet Tracer auf Test 64.100.0.10 unter TCP/5061

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
```

```
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 15, packet dispatched to next module

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

Packet Tracer auf Test 64.100.0.10 mit UDP/24000

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
```

```
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 16, packet dispatched to next module

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

Packet Tracer auf Test 64.100.0.10 mit UDP/36002

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
```

```
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 17, packet dispatched to next module

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

Fehlerbehebung

Schritt 1: Vergleichen von Paketerfassungen.

Paketerfassungen können sowohl an der ASA-Eingangs- als auch an der Ausgangs-Schnittstelle durchgeführt werden.

```
FW-A# sh cap
capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

Paketerfassungen für 64.100.0.10 bei TCP/5222:

```
FW-A# sh cap capout

2 packets captured
   1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
   2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown

FW-A# sh cap capin

2 packets captured
   1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
   2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

Paketerfassungen für 64.100.0.10 bei TCP/5061:

```
FW-A# sh cap capout
2 packets captured

   1: 21:42:14.920576 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
   2: 21:42:16.992380 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
2 packets shown
FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

Schritt 2: Überprüfen Sie die ASP-Paketerfassung (Accelerated Security Path).

Paketverluste durch eine ASA werden durch die ASA ASP-Erfassung erfasst. Die Option **all** erfasst alle möglichen Gründe, warum die ASA ein Paket verworfen hat. Dies kann bei Verdacht auf einen Grund eingeschränkt werden. Führen Sie aus einer Liste von Gründen, aus denen eine ASA diese Verwerfen klassifiziert, den Befehl **show asp drop aus.**

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

Tipp: Die ASA ASP-Erfassung wird in diesem Szenario verwendet, um zu überprüfen, ob die

ASA Pakete aufgrund einer verpassten ACL- oder NAT-Konfiguration verwirft, die das Öffnen eines bestimmten TCP- oder UDP-Ports für Expressway-E erfordern würde.

Tipp: Die Standardpuffergröße für jede ASA-Erfassung beträgt 512 KB. Wenn die ASA zu viele Pakete verwirft, wird der Puffer schnell gefüllt. Die Puffergröße kann mit der **Pufferoption** erhöht werden.

Empfehlungen

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
```

Alternative VCS Expressway-Implementierung

Eine Alternative zur Implementierung des Expressway-E mit dualen Netzwerkschnittstellen/dualen NIC ist die Implementierung des Expressway-E, jedoch mit einer einzigen NIC- und NAT-Reflektionskonfiguration auf den Firewalls. Der nächste Link enthält weitere Details zur Implementierung Konfigurieren der NAT-Reflektion auf der ASA für VCS Expressway TelePresence-Geräte.

Tipp: Die empfohlene Implementierung für den VCS Expressway ist die Implementierung von zwei Netzwerkschnittstellen/zwei NIC VCS Expressway, die in diesem Dokument beschrieben wird.

Zugehörige Informationen

- Konfigurieren der NAT-Reflektion auf der ASA für VCS Expressway TelePresence-Geräte
- Technischer Support und Dokumentation - Cisco Systems
- Cisco Expressway-E und Expressway-C - Implementierungsleitfaden für die grundlegende Konfiguration
- Platzieren eines Cisco VCS Expressway in einer DMZ statt im öffentlichen Internet

- Verwendung der Cisco Expressway-IP-Ports für Firewall-Überbrückung