ASA NAT-configuratie en -aanbevelingen voor de implementatie van snelwegen-E met twee netwerken

Inhoud

Inleiding

Dit document beschrijft hoe de configuratie van het Netwerkadresomzetting (NAT) moet worden geïmplementeerd die in de adaptieve security applicatie (ASA) van Cisco vereist is voor de implementatie van snelheden tussen de snelheden en de twee netwerken.

Tip: deze implementatie is de aanbevolen optie voor de E-implementatie bij expressies in plaats van de één-NIC-implementatie met NAT-reflectie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ASA basisconfiguratie en NAT-configuratie
- Cisco PowerSwitch-E en Express-C basisconfiguratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 en 5500-X Series apparaten die software versie 8.0 en hoger uitvoeren.
- Cisco Express versie X8.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Opmerking: Via het gehele document worden de snelwegapparaten aangeduid als snelwegen-E en snelwegen-C. Dezelfde configuratie is echter van toepassing op de VCS-snelwegen (Video Communication Server) en VCS-regelaars.

Achtergrondinformatie

Door ontwerp, kan Cisco Expressway-E in een gedemilitariseerde Zone (DMZ) of met een interface met het internet worden geplaatst, terwijl het in staat is met Cisco Expressway-C in een privaat netwerk te communiceren. Wanneer Cisco Expressway-E in een DMZ wordt geplaatst, zijn dit de extra voordelen:

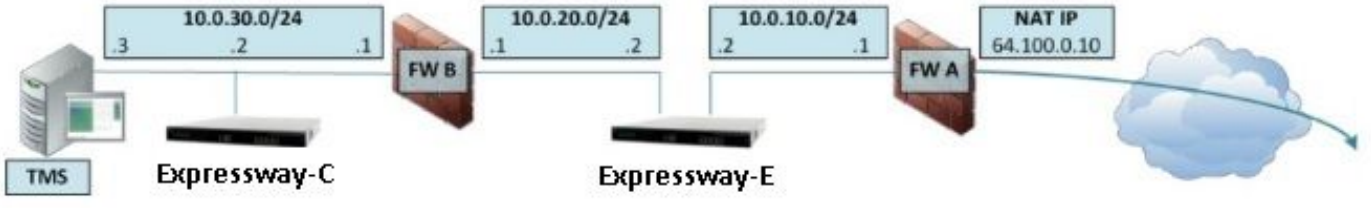
- In het meest gebruikelijke scenario wordt Cisco Expressway-E beheerd door het Private Network. Wanneer Cisco Expressway-E in een DMZ is, kan een experimentele (externe) firewall worden gebruikt om ongevraagde toegang tot Expressway uit externe netwerken te blokkeren via Hypertext Transfer Protocol Secure (HTTPS) of Secure Shell (SSH)-verzoeken.
- Als de DMZ geen rechtstreekse verbindingen tussen interne en externe netwerken toestaat, zijn er speciale servers nodig om verkeer te verwerken dat de DMZ overbrengt. Cisco Express kan fungeren als een proxy server voor Session Initiation Protocol (SIP) en/of H.323 voor spraak- en videoverkeer. In dit geval kunt u de optie Dubbele netwerkinterfaces gebruiken die Cisco Expressway toestaan om twee verschillende IP-adressen te hebben, één voor verkeer naar/van de externe firewall en één voor verkeer naar/van de interne firewall.

- Deze instelling voorkomt directe verbindingen van het externe netwerk naar het interne netwerk. Dit verbetert de algemene netwerkbeveiliging.

Tip: Om meer informatie over de TelePresence-implementatie te verkrijgen, raadpleegt u Cisco Expressway-E en Expressway-C - Basic Configuration Deployment Guide en plaatst u een Cisco VCS-snelweg in een DMZ in plaats van in het openbare internet.

Sneltoets C en E - dubbele netwerkinterfaces/dubbele NIC-implementatie

Dit beeld toont een voorbeeldplaatsing voor een Expressway-E met dubbele netwerkinterfaces en statische NAT. Expressway-C treedt op als de verplaatsen-client. Er zijn twee firewalls (FW A en FWB). Meestal kan FW A in deze DMZ-configuratie geen verkeer naar FW B routeren, en apparaten zoals de Expressway-E moeten verkeer vanaf het subnet van FW A naar het subnet van FW B valideren en doorsturen (en omgekeerd).



Deze inzet bestaat uit deze componenten.

DMZ-subversie 1 - 10.0.10.0/24

- FW A interne interface - 10.0.10.1
- E2-interface voor snelweg - 10.0.10.2

DMZ subtype 2 - 10.0.20.0/24

- FW B externe interface - 10.0.20.1
- Snelle LAN1-interface - 10.0.20.2

LAN-ondersteuning - 10.0.30.0/24

- FW B interne interface - 10.0.30.1
- Direct-C LAN1-interface - 10.0.30.2
- Cisco TelePresence Management Suite (TMS) servernetwerkinterface - 10.0.30.3

Specificaties van deze implementatie:

- FW A is de externe of omtrek-firewall; Het wordt geconfigureerd met NAT IP (openbare IP) van 64.100.0.10, die statistisch wordt vertaald naar 10.0.10.2 (Expressway-E LAN2-interface)
- FW B is de interne firewall
- Snelweg-E LAN1 heeft een statische NAT-modus uitgeschakeld
- Expressway-E LAN2 heeft statische NAT-modus ingeschakeld met Statisch NAT-adres 64.100.0.10
- Expressway-C heeft een verplaatsen-clientzone die wijst op 10.0.20.2 (E1 interface met snelweg)
- Er is geen routing tussen 10.0.20.0/24 en 10.0.10.0/24 subnetwerken. Expressway-E brugt deze subnetten en fungeert als een proxy voor SIP/H.323 signalering en Real-time Transport

Protocol (RTP)/RTP Control Protocol (RTCP)-media.
- Cisco TMS heeft Express-E ingesteld met IP-adres 10.0.20.2

Vereisten/beperkingen

Niet-overlappende subnetten

Als Expressway-E is geconfigureerd voor het gebruik van beide LAN interfaces, moeten LAN1 en LAN2 interfaces in niet-overlappende subnetten gelegen zijn om er zeker van te zijn dat het verkeer naar de juiste interface wordt verzonden.

clusteren

Wanneer clustering van expressway-apparaten met de optie Advanced Network wordt geconfigureerd, moet elke clusterpeer worden geconfigureerd met zijn eigen LAN1-interfaceadres. Daarnaast moet clustering worden geconfigureerd op een interface die geen statische NAT-modus heeft ingeschakeld. Daarom wordt aanbevolen om LAN2 als de externe interface te gebruiken, waarop u statische NAT kunt toepassen en configureren waar van toepassing.

Externe LAN-interfaceinstellingen

De instellingen voor de configuratie van de externe LAN-interface in de IP-configuratiepagina zijn in de netwerkinterface gebruikgemaakt van Transversal met behulp van Relays rond NAT (TURN). In een dubbele netwerkinterface Express-E configuratie wordt dit normaal gesproken ingesteld op de Expressway-E externe LAN-interface.

Statische routers

Expressway-E moet voor dit scenario worden geconfigureerd met een standaard gateway-adres van 10.0.10.1. Dit betekent dat al het verkeer dat via LAN2 wordt verzonden standaard naar het IP-adres 10.0.10.1 wordt verzonden.

Als FW B verkeer vertaalt van 10.0.30.0/24 subtype naar de interface Expressway-E LAN1 (bijvoorbeeld autoverkeer met OCR-client of TMS Server Management-verkeer), verschijnt dit verkeer vanaf de FWB externe interface (10.0.20.1) omdat het Expressway-E LAN1 bereikt. Expressway-E kan dan via zijn netwerk op dit verkeer reageren1 interface sinds de klaarblijkelijke bron van dat verkeer ligt op zelfde voorwerp.

Als NAT op FW B is geactiveerd, toont het verkeer dat van snelweg-C naar snelweg-E LAN1 wordt verzonden als het van 10.0.30.2 komt. Als Expressway geen statische route voor 10.0.30.0/24 subnet heeft, stuurt het de antwoorden voor dit verkeer naar zijn standaardgateway (10.0.10.1) vanuit LAN2, omdat het zich niet bewust is van dat 1 0.0.30.0/24 Subnet bevindt zich achter de interne firewall (FW B). Daarom moet een statische route worden toegevoegd, voer de opdracht **xOpdracht RouteAdd** CLI door een SSH-sessie naar Expressway uit.

In dit specifieke voorbeeld moet Expressway-E weten dat het de 10.0.30.0/24 subster achter FW B kan bereiken, wat bereikbaar is via de LAN1 interface. U voert deze opdracht als volgt uit:

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

Opmerking: SDe statische routeconfiguratie kan worden toegepast via de expressway-E GUI evenals sectie **System/Network > Interfaces/Static Routes**.

In dit voorbeeld kan de interfaceparameter ook op **Auto** worden ingesteld omdat het gatewayadres (10.0.20.1) alleen via LAN1 bereikbaar is.

Indien NAT niet is ingeschakeld op FW B en Expressway-E moet communiceren met apparatuur in subnetten (anders dan 10.0.30.0/24) die zich ook achter FW B bevinden, moeten statische routes voor deze toestellen/subnetten worden toegevoegd.

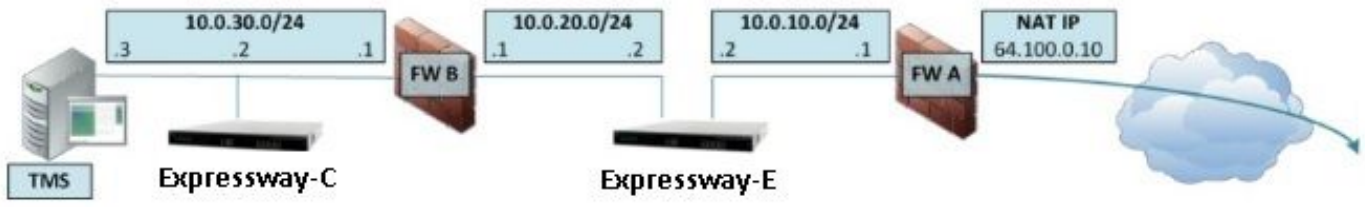
Opmerking: Hieronder vallen: SSH- en HTTPS-verbindingen van netwerkbeheerwerkstations of voor netwerkservices zoals NTP-, DNS-, LDAP-/AD- of SYSLOG.

De opdracht **xOpdracht RouteAdd** en de syntaxis worden in detail beschreven in de VCS Administrator Guide.

Configuratie

In dit gedeelte wordt beschreven hoe u de statische NAT dient te configureren die vereist is voor de implementatie van de I.F.-interface van het snelnetwerk op de ASA. Er zijn een aantal aanvullende ASA Modular Policy Framework (MPF) configuratie aanbevelingen opgenomen voor de verwerking van SIP/H323-verkeer.

Snelweg C en E - dubbele netwerkinterfaces/dubbele NIC-implementatie



In dit voorbeeld, is de IP adrestoewijzing de volgende.

IP-adres snelweg: 10.0.30.2/24

Standaard expressweg-C-gateway: 10.0.30.1 (FW-B)

IP-adressen van snelweg:

Op LAN2: 10.0.10.2/24

Op LAN1: 10.0.20.2/24

Standaard snelgateway: 10.0.10.1 (FW-A)

TMS IP-adres: 10.0.30.3/24

Configuratie FW-A

Stap 1. Statische NAT-configuratie voor de snelweg-E.

Zoals uitgelegd in het gedeelte Background Information van dit document heeft de FW-A een statische NAT-vertaling zodat Expressway-E vanaf het internet bereikbaar is met een openbaar IP-adres 64.100.0.10. Deze laatste is NATed tot Expressway-E LAN2 IP-adres 10.0.10.2/24. Dat gezegd hebbende, is dit de vereiste FW-A statische NAT-configuratie.

Voor ASA versies 8.3 en later:

```
! 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
```

> **Waarschuwing**: wanneer u de statische PAT-opdrachten toepast, ontvangt u deze foutmelding in de ASA opdrachtregel-interface "**FOUT: NAT kan havens niet reserveren"**. Daarna moet u de wachtrijen op de ASA opheffen, voor dit programma moet u de opdracht **klaring x.x.x.x,**van waaruit x.x.x.x overeenkomt met het ASA externe IP-adres. Deze opdracht maakt alle vertalingen die bij dit IP-adres zijn gekoppeld, voorzichtig uit in productieomgevingen.

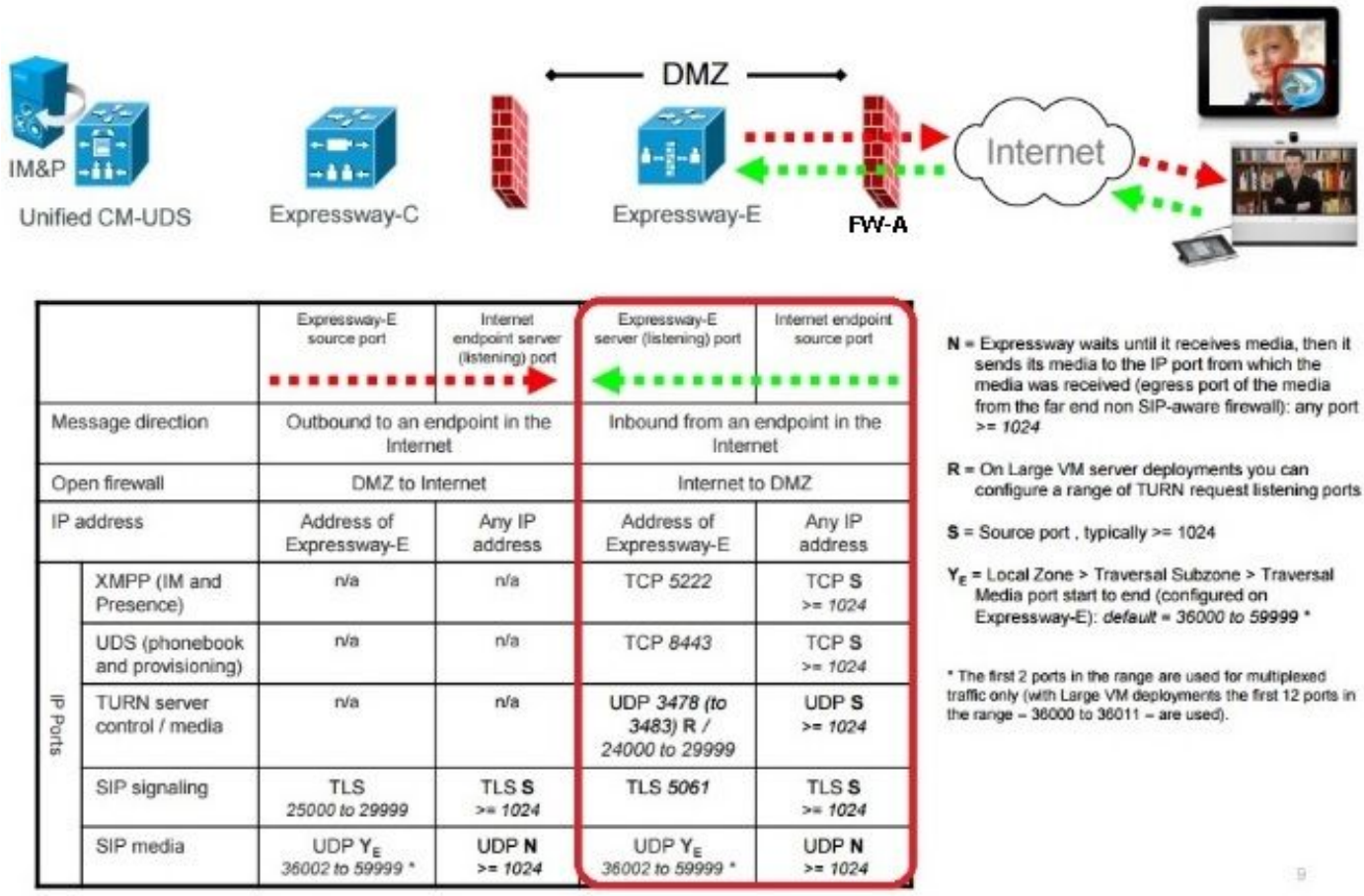
Voor ASA versies 8.2 en eerder:

```
! 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
```

Stap 2. Met de configuratie van toegangscontrolelijst (ACL) kunnen de gewenste poorten van het internet naar de sneltoets-E worden geopend.

Volgens de Unified Communications: Expressway (DMZ) met openbare internetdocumentatie. De lijst van TCP- en UDP-poorten die de expressway-E nodig heeft om in FW-A toe te staan, is zoals in de afbeelding getoond:



Dit is de ACL-configuratie die als inkomende in de FW-A externe interface vereist is.

Voor ASA versies 8.3 en later:

```
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
```

Voor ASA versies 8.2 en eerder:

```
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-configuratie

Zoals uitgelegd in het gedeelte Informatie op de achtergrond van dit document, kan FW B een dynamische NAT of PAT configuratie nodig hebben om het interne net 10.0.30.0/24 te kunnen vertalen naar het IP-adres 10.0.20.1 wanneer het naar de externe interface van FW B gaat.

Voor ASA versies 8.3 en later:

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

Voor ASA versies 8.2 en eerder:

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

> **Tip**: Zorg ervoor dat alle vereiste TCP- en UDP-poorten de sneltoets-C naar behoren laten werken en in FW B zijn geopend, net zoals in dit Cisco-document gespecificeerd: Cisco-poort in gebruik voor firewall-verplaatsingen

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Packet Tracer kan op de ASA worden gebruikt om te bevestigen dat de expressway-E statische NAT-vertaling naar wens werkt.

Packet Tracer naar Test 64.100.0.10 bij TCP/522

```
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 naar Test 64.100.0.10 bij 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 naar Test 64.100.0.10 bij 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 naar Test 64.100.0.10 bij UDP/2400

```
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 naar Test 64.100.0.10 bij 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
```

Problemen oplossen

Stap 1. Vergelijk pakketvastlegging.

Packet Capture kan zowel op ASA inloop- als spanningsinterfaces worden gemaakt.

```
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
```

Packet Captures voor 64.100.0.10 bij 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
```

Packet Captures voor 64.100.0.10 bij 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
```

Stap 2. Controleer de afdrukking van het Accelerated Security Path (ASP).

Pakketdruppels van een ASA worden opgenomen door de ASA ASP-opname. De optie geeft alle mogelijke redenen op waarom de ASA een pakje heeft laten vallen. Dit kan worden beperkt als er een vermoedelijke reden is. Om een lijst van redenen gebruikt een ASA deze druppels om te classificeren, voer de opdracht **show asp druppel uit.**

```
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
```

> **Tip**: De ASA ASP-opname wordt in dit scenario gebruikt om te bevestigen of de ASA-pakketten worden neergelegd door een gemiste ACL of NAT-configuratie, die een specifieke TCP- of UDP-poort voor de expressway-E zou moeten openen.

> **Tip**: De standaardbuffergrootte voor elke ASA opname is 512 KB. Als de ASA te veel pakketten laat vallen is de buffer snel gevuld. De buffergrootte kan met de **bufferoptie** worden verhoogd.

Aanbevelingen

Zorg ervoor dat de SIP/H.323-inspectie volledig is uitgeschakeld aan de betrokken firewalls.

Het wordt sterk aanbevolen om SIP en H.323 inspectie op firewalls uit te schakelen die netwerkverkeer naar of van een snelweg-E afhandelen. Als deze optie wordt ingeschakeld, wordt vaak vastgesteld dat SIP/H.323-inspectie een negatieve invloed heeft op de ingebouwde firewall/NAT-traversale functionaliteit.

Dit is een voorbeeld van hoe te om SIP en H.323 inspecties van de ASA uit te schakelen:

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

Alternatieve VCS-doorvoerimplementatie

Een alternatieve oplossing voor de implementatie van de snelweg-E met dubbele netwerkinterfaces/dubbele NIC is de implementatie van de Expressway-E maar met één enkele NIC en NAT reflectie configuratie op de firewalls. De volgende link toont verdere details over deze implementatie Configureer NAT-reflectie op de ASA for VCS Express TelePresence Devices.

> **Tip**: De aanbevolen implementatie voor de VCS-snelweg is de dubbele netwerkinterfaces/dubbele NIC VCS-snelweg die in dit document wordt beschreven.

Gerelateerde informatie

- NAT-reflectie op de ASA for VCS Express TelePresence-apparaten configureren
- Technische ondersteuning en documentatie – Cisco Systems
- Cisco oE-handleiding voor snelwegen en snelwegen-C-handleiding voor configuratie
- Een Cisco VCS-snelweg plaatsen in een DMZ in plaats van op het openbare internet
- Cisco IP-poortgebruik voor firewall-trajecten