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

## Sommario



## Introduzione

In questo documento viene descritto come implementare la configurazione NAT (Network Address Translation) richiesta in Cisco Adaptive Security Appliance (ASA) per l'implementazione delle interfacce di rete doppie Expressway-E.

**Suggerimento**: questa distribuzione è l'opzione consigliata per l'implementazione di Expressway-E, anziché l'implementazione di una singola NIC con riflessione NAT.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di base Cisco ASA e configurazione NAT
- Configurazione di base di Cisco Expressway-E ed Expressway-C

## 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 8.0 e successive.
- Cisco Expressway versione X8.0 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 EXPRESSWAY sono denominati Expressway-E ed Expressway-C. Tuttavia, la stessa configurazione si applica ai dispositivi Expressway e VCS Control di Video Communication Server (VCS).

# Premesse

In base alla progettazione, Cisco Expressway-E può essere posizionato in una zona demilitarizzata (DMZ) o con un'interfaccia con connessione Internet, mentre è in grado di comunicare con Cisco Expressway-C in una rete privata. Se Cisco Expressway-E è inserito in una DMZ, i vantaggi aggiuntivi sono i seguenti:

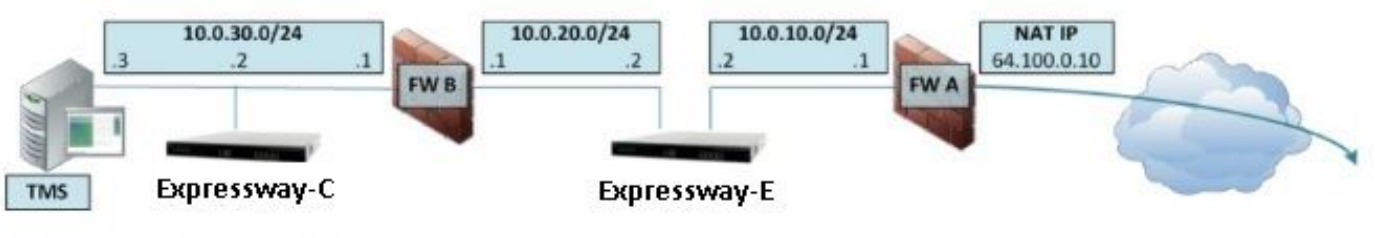
- Nello scenario più comune, Cisco Expressway-E viene gestito da una rete privata. Quando Cisco Expressway-E si trova in una DMZ, è possibile utilizzare un firewall perimetrale (esterno) per bloccare l'accesso indesiderato a Expressway da reti esterne tramite le richieste HTTP (Hypertext Transfer Protocol Secure) o SSH (Secure Shell).
- Se la DMZ non consente connessioni dirette tra reti interne ed esterne, per gestire il traffico che attraversa la DMZ sono necessari server dedicati. Cisco Expressway può fungere da server proxy per il traffico voce e video H.323 e/o il protocollo SIP (Session Initiation Protocol). In questo caso, è possibile utilizzare l'opzione Dual Network Interfaces per consentire a Cisco Expressway di avere due indirizzi IP diversi, uno per il traffico da/verso il firewall esterno e uno per il traffico da/verso il firewall interno.

- Questa configurazione impedisce le connessioni dirette dalla rete esterna alla rete interna. Ciò migliora la sicurezza complessiva della rete interna.

  **Suggerimento**: Per ulteriori informazioni sull'implementazione di TelePresence, fare riferimento alla Cisco Expressway-E e Expressway-C - Basic Configuration Deployment Guide e all'inserimento di Cisco VCS Expressway in una DMZ anziché nella rete Internet pubblica.

## Expressway C ed E - Implementazione di due interfacce di rete/due NIC

Nell'immagine viene mostrato un esempio di implementazione di un Expressway-E con interfacce di rete doppie e NAT statico. Expressway-C funge da client di attraversamento. Ci sono due firewall (FW A e FWB). In questa configurazione DMZ, l'FW A non può indirizzare il traffico verso l'FW B e dispositivi come l'Expressway-E sono richiesti per convalidare e inoltrare il traffico dalla subnet dell'FW A alla subnet dell'FW B (e viceversa).




Questa distribuzione è costituita da questi componenti.

Subnet DMZ 1 - 10.0.10.0/24

- Interfaccia interna FW A - 10.0.10.1
- Interfaccia LAN2 Expressway-E - 10.0.10.2

Subnet DMZ 2 - 10.0.20.0/24

- Interfaccia esterna FW B - 10.0.20.1
- Interfaccia LAN1 Expressway-E - 10.0.20.2

Subnet LAN - 10.0.30.0/24

- Interfaccia interna FW B - 10.0.30.1
- Interfaccia LAN1 Expressway-C - 10.0.30.2
- Interfaccia di rete server Cisco TelePresence Management Suite (TMS) - 10.0.30.3

Specifiche di questa implementazione:

- FW A è il firewall esterno o perimetrale; è configurato con NAT IP (public IP) 64.100.0.10, convertito staticamente in 10.0.10.2 (Expressway-E LAN2 interface)
- FW B è il firewall interno
- Modalità NAT statica disabilitata per Expressway-E LAN1
- Expressway-E LAN2 ha la modalità NAT statica abilitata con l'indirizzo NAT statico 64.100.0.10
- Expressway-C dispone di una zona client trasversale che punta a 10.0.20.2 (interfaccia Expressway-E LAN1)

- Non è presente alcun routing tra le subnet 10.0.20.0/24 e 10.0.10.0/24. Expressway-E collega queste subnet e funge da proxy per i supporti SIP/H.323 Signaling e Real-time Transport Protocol (RTP) / RTP Control Protocol (RTCP).
- Cisco TMS ha Expressway-E configurato con l'indirizzo IP 10.0.20.2

# Requisiti/Limitazioni

## Subnet non sovrapposte

Se Expressway-E è configurato per l'utilizzo di entrambe le interfacce LAN, le interfacce LAN1 e LAN2 devono trovarsi in subnet non sovrapposte per garantire che il traffico venga inviato all'interfaccia corretta.

## Clustering

Quando si raggruppano i dispositivi Expressway con l'opzione di rete avanzata configurata, ogni peer del cluster deve essere configurato con il proprio indirizzo di interfaccia LAN1. Inoltre, il clustering deve essere configurato su un'interfaccia per cui non è abilitata la modalità NAT statica. Pertanto, si consiglia di utilizzare LAN2 come interfaccia esterna, su cui è possibile applicare e configurare NAT statico, ove applicabile.

## Impostazioni interfaccia LAN esterna

Le impostazioni di configurazione dell'interfaccia LAN esterna nella pagina di configurazione IP determinano quale interfaccia di rete utilizza i relè trasversali attorno a NAT (TURN). In una configurazione Expressway-E con interfaccia di rete doppia, questa impostazione viene in genere impostata sull'interfaccia LAN esterna Expressway-E.

## Route statiche

Per questo scenario, Expressway-E deve essere configurato con un indirizzo gateway predefinito di 10.0.10.1. Pertanto, per impostazione predefinita, tutto il traffico inviato tramite LAN2 viene inviato all'indirizzo IP 10.0.10.1.

Se l'FW B converte il traffico inviato dalla subnet 10.0.30.0/24 all'interfaccia Expressway-E LAN1 (ad esempio, il traffico del client di attraversamento Expressway-C o il traffico di gestione del server TMS), questo traffico viene visualizzato come proveniente dall'interfaccia esterna FWB (10.0.20.1) quando raggiunge Expressway-E LAN1. Expressway-E è quindi in grado di rispondere a questo traffico tramite l'interfaccia LAN1 poiché l'origine apparente del traffico si trova sulla stessa subnet.

Se NAT è abilitato sull'FW B, il traffico inviato da Expressway-C a Expressway-E LAN1 viene visualizzato come proveniente da 10.0.30.2. Se Expressway non dispone di una route statica aggiunta per la subnet 10.0.30.0/24, invia le risposte per questo traffico al gateway predefinito (10.0.10.1) dalla LAN2, in quanto non è a conoscenza del fatto che la subnet 10.0.30.0/24 si trova dietro il firewall interno (FW B). Pertanto, è necessario aggiungere una route statica, eseguire il comando **xCommand RouteAdd** CLI tramite una sessione SSH in Expressway.

In questo esempio, Expressway-E deve poter raggiungere la subnet 10.0.30.0/24 dietro FW B, raggiungibile tramite l'interfaccia LAN1. A tale scopo, eseguire il comando:

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

> **Nota**: SLa configurazione statica del percorso può essere applicata tramite l'interfaccia grafica Expressway-E e la sezione **System/Network > Interfaces/Static Routes**.

Nell'esempio, il parametro Interface può essere impostato su **Auto** anche perché l'indirizzo del gateway (10.0.20.1) è raggiungibile solo tramite LAN1.

Se NAT non è abilitato sull'FW B e Expressway-E deve comunicare con i dispositivi nelle subnet (diverse da 10.0.30.0/24) che si trovano anche dietro l'FW B, è necessario aggiungere route statiche per questi dispositivi/subnet.

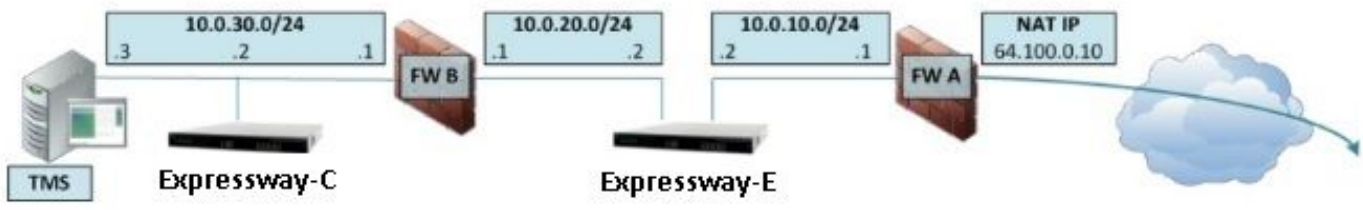
> **Nota:** Ciò include Connessioni SSH e HTTPS da workstation di gestione di rete o per servizi di rete quali NTP, DNS, LDAP/AD o Syslog.

Il comando **xCommand RouteAdd** e la relativa sintassi sono descritti in dettaglio nella Guida dell'amministratore di VCS.

# Configurazione

In questa sezione viene descritto come configurare il NAT statico richiesto per l'implementazione dell'interfaccia di rete doppia Expressway-E sull'appliance ASA. Per la gestione del traffico SIP/H323, sono incluse alcune raccomandazioni aggiuntive sulla configurazione di ASA Modular Policy Framework (MPF).

## Expressway C ed E - Implementazione di due interfacce di rete/due NIC




Nell'esempio, l'assegnazione dell'indirizzo IP è la successiva.

Indirizzo IP Expressway-C: 10.0.30.2/24

Expressway-C default-gateway: 10.0.30.1 (FW-B)

Indirizzi IP Expressway-E:

- Su LAN2: 10.0.10.2/24
- Su LAN1: 10.0.20.2/24

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

Indirizzo IP TMS: 10.0.30.3/24

## Configurazione FW-A

### Passaggio 1. Configurazione NAT statica per Expressway-E.

Come spiegato nella sezione Informazioni di base di questo documento, l'FW-A ha una traduzione NAT statica per consentire a Expressway-E di essere raggiungibile da Internet con indirizzo IP pubblico 64.100.0.10. Quest'ultimo è NAT per Expressway-E LAN2 indirizzo IP 10.0.10.2/24. Ciò detto, questa è la configurazione NAT statica FW-A richiesta.

Per ASA versioni 8.3 e successive:

```
! 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
```

> **Attenzione**: quando si applicano i comandi statici PAT, viene visualizzato questo messaggio di errore sull'interfaccia della riga di comando ASA, "**ERROR: NAT cannot to reserve ports" (NAT non è in grado di riservare porte)**. Quindi, cancellare le voci xlate sull'appliance ASA ed eseguire il comando **clear xlatelocal x.x.x.x,**da cui x.x.x.x corrisponde all'indirizzo IP esterno dell'appliance ASA. Questo comando cancella tutte le traduzioni associate all'indirizzo IP ed eseguilo con cautela negli ambienti di produzione.

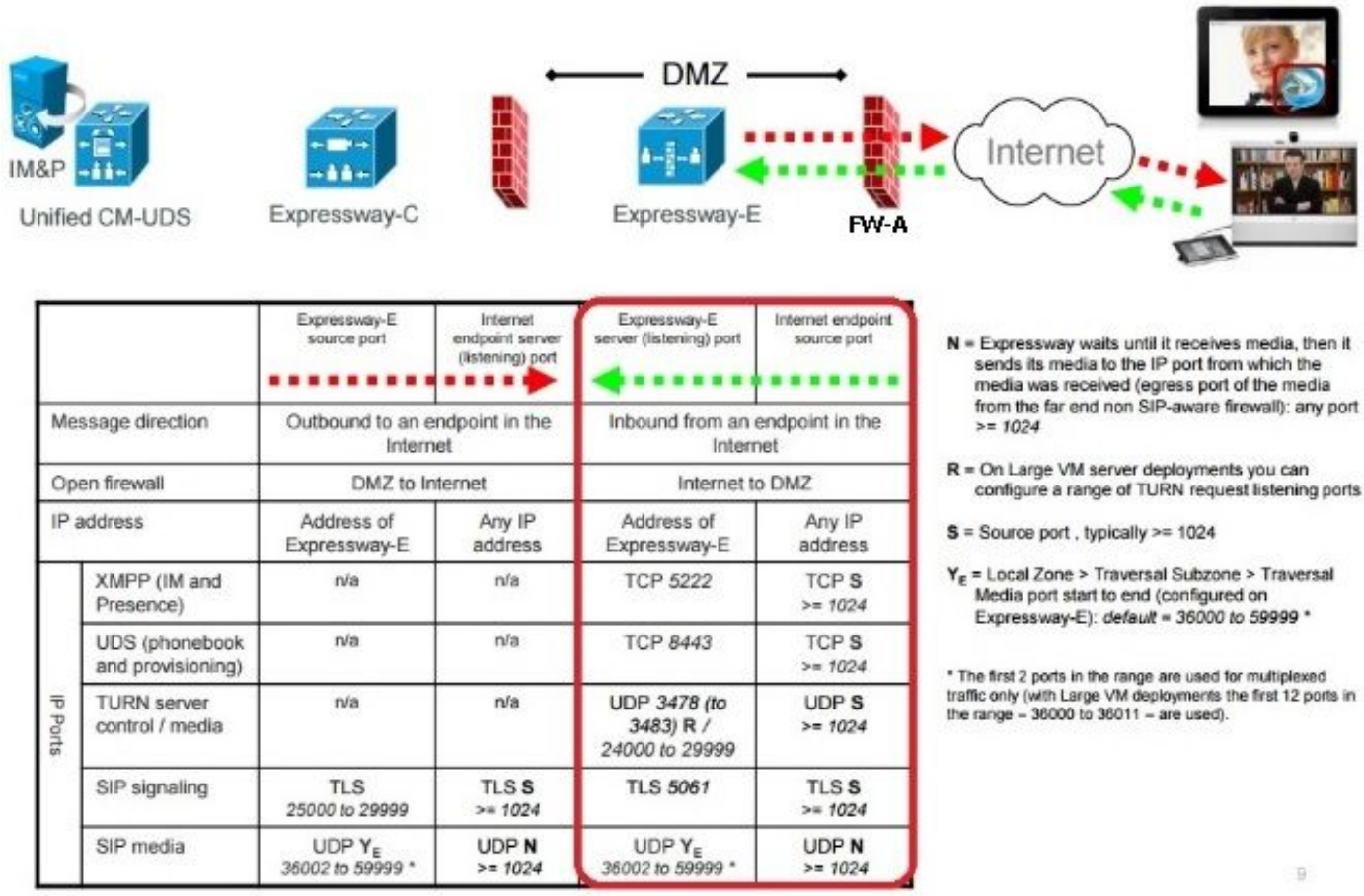
Per ASA versioni 8.2 e precedenti:

```
! 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
```

### Passaggio 2. La configurazione dell'elenco di controllo di accesso (ACL) consente di configurare le porte necessarie da Internet a Expressway-E.

Secondo la comunicazione unificata: Expressway (DMZ) nella documentazione pubblica di Internet, l'elenco delle porte TCP e UDP che Expressway-E richiede di consentire in FW-A, sono indicate nell'immagine:




Questa è la configurazione ACL richiesta per il traffico in entrata nell'interfaccia esterna FW-A.

Per ASA versioni 8.3 e successive:

```
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
```

Per ASA versioni 8.2 e precedenti:

```
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
```

### Configurazione FW-B

Come spiegato nella sezione Background Information di questo documento, il firmware B può richiedere una configurazione NAT o PAT dinamica per consentire la conversione della subnet interna 10.0.30.0/24 nell'indirizzo IP 10.0.20.1 quando raggiunge l'interfaccia esterna del firmware B.

Per ASA versioni 8.3 e successive:

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

Per ASA versioni 8.2 e precedenti:

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

> **Suggerimento**: verificare che tutte le porte TCP e UDP richieste consentano a Expressway-C di funzionare correttamente e che siano aperte nel firmware B, come specificato in questo documento di Cisco: Utilizzo della porta IP di Cisco Expressway per il passaggio del firewall

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Packet Tracer può essere usato sull'appliance ASA per verificare che la traduzione NAT statica Expressway-E funzioni correttamente.

### Packet Tracer per test 64.100.0.10 su 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 per test 64.100.0.10 su 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 per test 64.100.0.10 su 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 per il test 64.100.0.10 su 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 per il test 64.100.0.10 su 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
```

# Risoluzione dei problemi

## Passaggio 1. Confrontare le acquisizioni dei pacchetti.

Le acquisizioni dei pacchetti possono avvenire sia sulle interfacce ASA in entrata che su quelle in uscita.

```
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
```

Pacchetti acquisiti per 64.100.0.10 su 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
```

Pacchetti acquisiti per 64.100.0.10 su 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
```

## Passaggio 2. Ispezionare le acquisizioni di pacchetti con percorso di sicurezza accelerato (ASP).

Le perdite di pacchetti da parte di un'ASA vengono acquisite dall'acquisizione ASP dell'ASA. L'opzione **all** (tutti) mostra tutte le possibili ragioni per cui l'appliance ASA ha scartato un pacchetto. Questo può essere ridotto se ci sono ragioni sospette. Per un elenco dei motivi per cui un'appliance ASA classifica le perdite, eseguire il comando **show asp drop.**

```
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
```

> **Suggerimento**: In questo scenario, l'acquisizione ASP ASA viene usata per confermare se l'ASA scarta i pacchetti a causa di un ACL o di una configurazione NAT mancante, che richiederebbe l'apertura di una porta TCP o UDP specifica per Expressway-E.

> **Suggerimento**: La dimensione predefinita del buffer per ogni acquisizione ASA è 512 KB. Se l'ASA elimina troppi pacchetti, il buffer viene riempito rapidamente. La dimensione del buffer

può essere aumentata con l'opzione **buffer**.

## Raccomandazioni

Accertarsi 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
```

## Implementazione alternativa di VCS Expressway

Una soluzione alternativa per implementare Expressway-E con due interfacce di rete/doppia NIC consiste nell'implementare Expressway-E ma con una singola NIC e configurazione di riflessione NAT sui firewall. Il collegamento successivo mostra ulteriori dettagli su questa implementazione. Configurare la riflessione NAT sull'appliance ASA per i dispositivi VCS Expressway TelePresence.

> **Suggerimento**: L'implementazione consigliata per VCS Expressway è l'implementazione di due interfacce di rete/due schede NIC VCS Expressway descritta in questo documento.

## Informazioni correlate

- Configurazione della riflessione NAT sull'appliance ASA per i dispositivi VCS Expressway TelePresence
- Documentazione e supporto tecnico – Cisco Systems
- Cisco Expressway-E ed Expressway-C - Guida alla configurazione di base
- Posizionamento di Cisco VCS Expressway in una DMZ piuttosto che nella rete Internet pubblica
- Cisco Expressway Utilizzo porta IP per attraversamento firewall