

Configurazione e verifica di NAT su FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Task 1. Configurare NAT statico su FTD](#)

[Task 2. Configurare Port Address Translation \(PAT\) su FTD](#)

[Task 3. Configurare l'esenzione NAT su FTD](#)

[Task 4. Configurare l'oggetto NAT su FTD](#)

[Task 5. Configurare il pool PAT su FTD](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e verificare il protocollo NAT (Network Address Translation) di base su Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- ASA5506X con codice FTD 6.1.0-226
- Centro di gestione FireSIGHT (FMC) con versione 6.1.0-226
- 3 host Windows 7
- Router Cisco IOS® 3925 con VPN da LAN a LAN (L2L)

Ora di completamento del laboratorio: 1 ora.

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.

Premesse

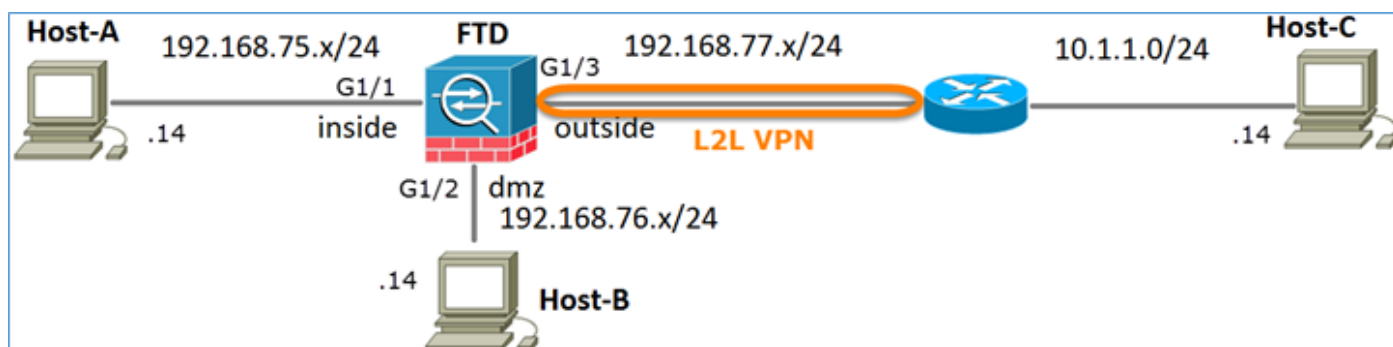
FTD supporta le stesse opzioni di configurazione NAT del classico Adaptive Security Appliance (ASA):

- NAT Rules Before - Equivale a Two NAT (sezione 1) su ASA classico
- Regole NAT automatiche - Sezione 2 sull'appliance ASA classica
- NAT Rules After - Equivale a Two NAT (sezione 3) su ASA classico

Poiché la configurazione FTD viene eseguita dal FMC per la configurazione NAT, è necessario conoscere l'interfaccia utente grafica del FMC e le varie opzioni di configurazione.

Configurazione

Esempio di rete

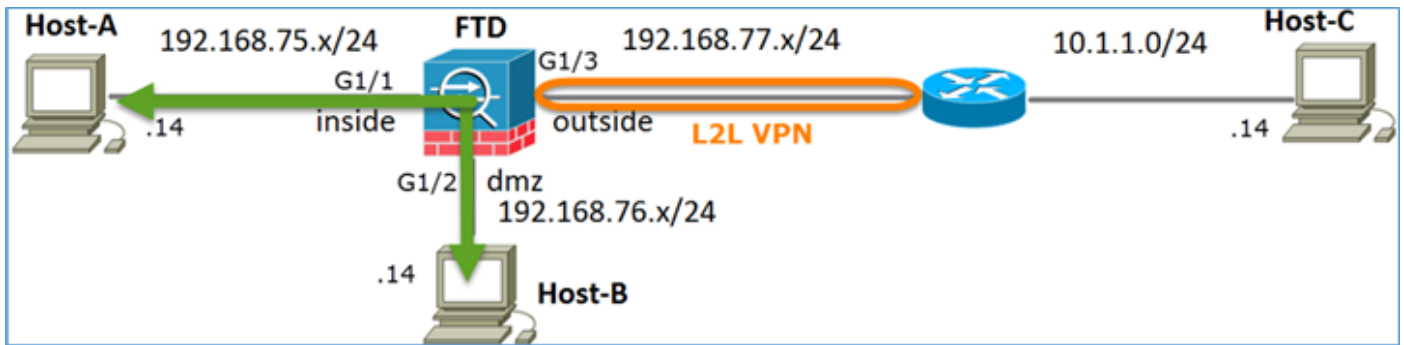


Task 1. Configurare NAT statico su FTD

Configurare NAT in base ai seguenti requisiti:

Nome criterio NAT	Nome del dispositivo FTD
Regola NAT	Regola NAT manuale
Tipo NAT	Statico
Inserisci	Nella sezione 1
Source interface	interno*
Interfaccia di destinazione	dmz*
Origine	192.168.75.14
Origine tradotta	192.168.76.100

*Usare le zone di sicurezza per la regola NAT



NAT statico

Soluzione:

Sulle appliance ASA classiche, è necessario usare il comando `name if` nelle regole NAT. Con FTD è necessario utilizzare le aree di sicurezza o i gruppi di interfacce.

Passaggio 1. Assegnare le interfacce alle aree di sicurezza/ai gruppi di interfacce.

In questa attività, si decide di assegnare le interfacce FTD utilizzate per NAT alle aree di sicurezza. In alternativa, è possibile assegnarli ai gruppi di interfacce come mostrato nell'immagine.

Edit Physical Interface

Mode:

Name: Enabled Management Only

Security Zone:

Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9198)

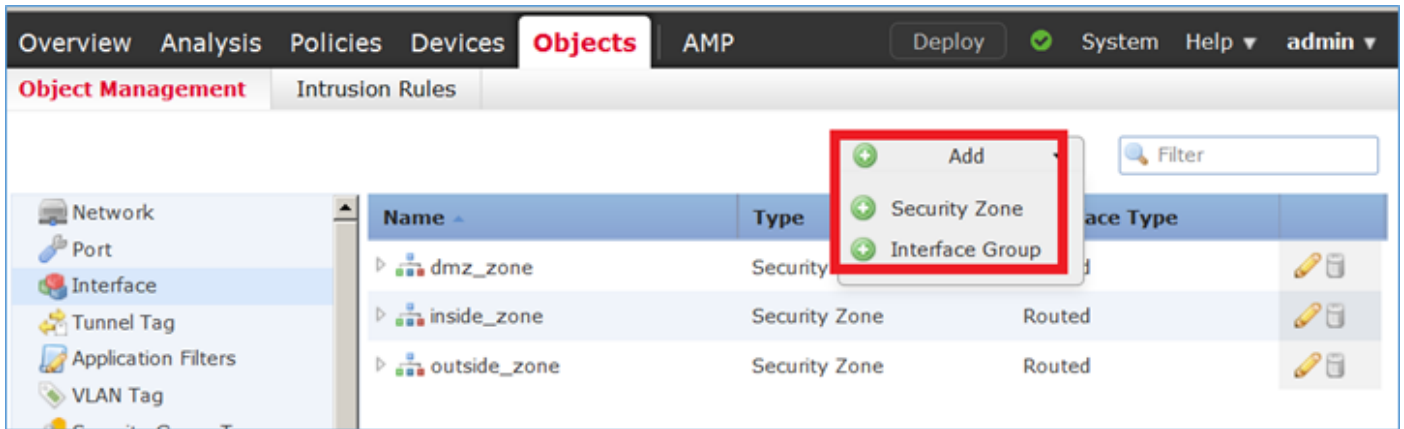
Interface ID:

Passaggio 2. Il risultato è quello mostrato nell'immagine.

Interface	Logical Name	Type	Interface Objects	Mac Address(Active/Standby)	IP Address
GigabitEthernet1/1	inside	Physical	inside_zone		192.168.75.6/24(Static)
GigabitEthernet1/2	dmz	Physical	dmz_zone		192.168.76.6/24(Static)
GigabitEthernet1/3	outside	Physical	outside_zone		192.168.77.6/24(Static)

Passaggio 3. È possibile creare/modificare gruppi di interfacce e aree di sicurezza dalla pagina

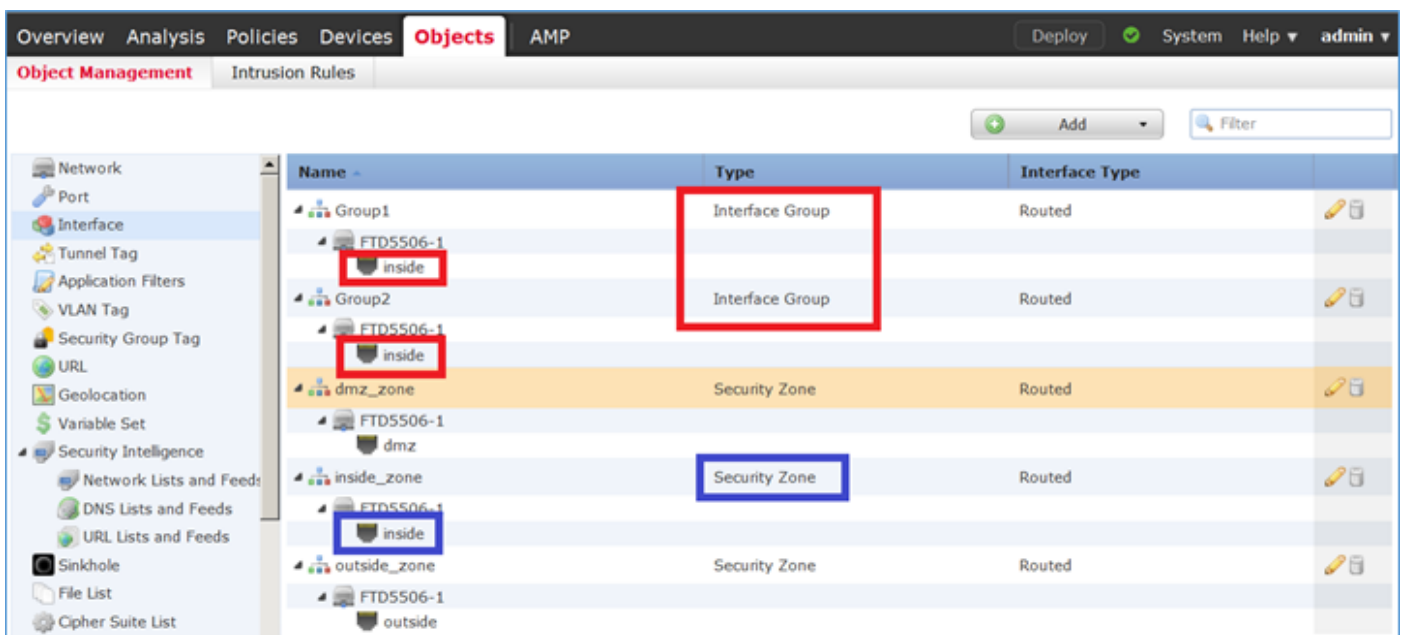
Oggetti > Gestione oggetti, come mostrato nell'immagine.



Are di sicurezza e gruppi di interfacce

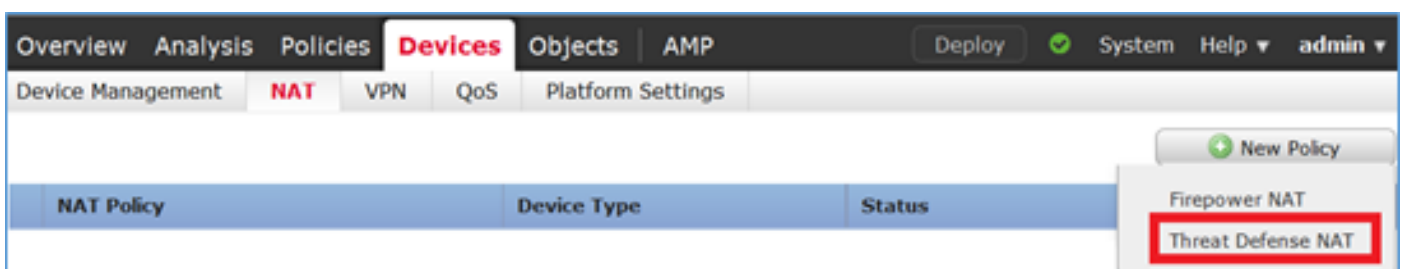
La differenza principale tra le aree di sicurezza e i gruppi di interfacce è che un'interfaccia può appartenere a una sola area di sicurezza, ma può appartenere a più gruppi di interfacce. In pratica, i gruppi di interfacce offrono maggiore flessibilità.

È possibile vedere che l'interfaccia **interna** appartiene a due diversi gruppi di interfacce, ma solo un'area di sicurezza, come mostrato nell'immagine.

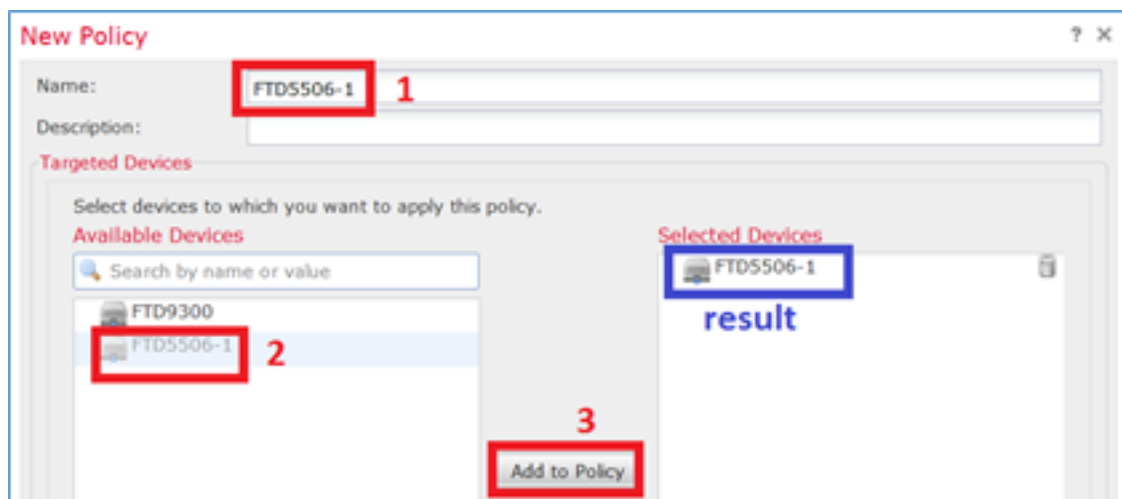


Passaggio 4. Configurare NAT statico su FTD.

Passare a **Dispositivi > NAT** e creare un criterio NAT. Selezionare **Nuovo criterio > NAT difesa dalle minacce** come mostrato nell'immagine.

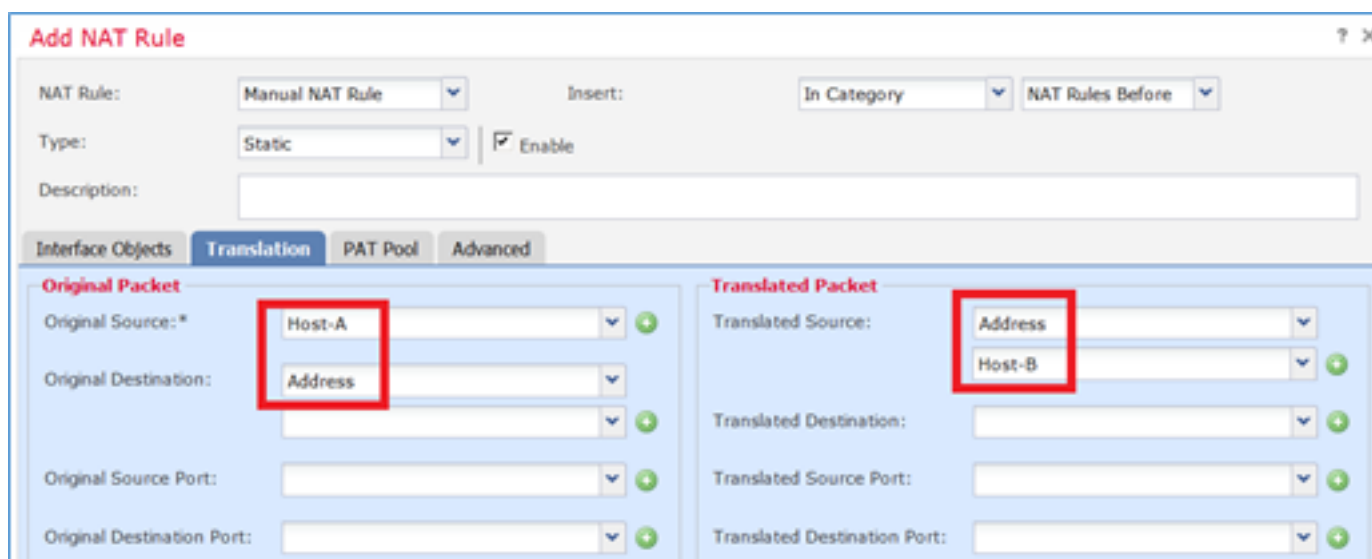
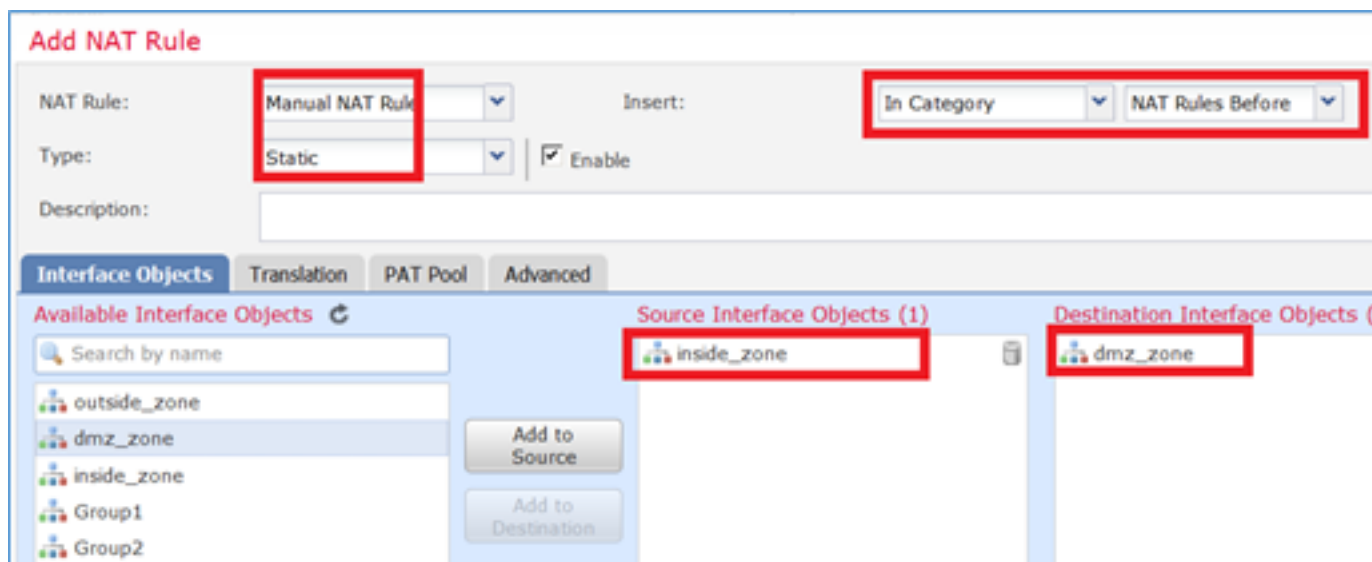


Passaggio 5. Specificare il nome del criterio e assegnarlo a un dispositivo di destinazione, come mostrato nell'immagine.



Passaggio 6. Aggiungere una regola NAT al criterio, fare clic su **Aggiungi regola**.

Specificatele in base ai requisiti dell'operazione, come mostrato nelle immagini.



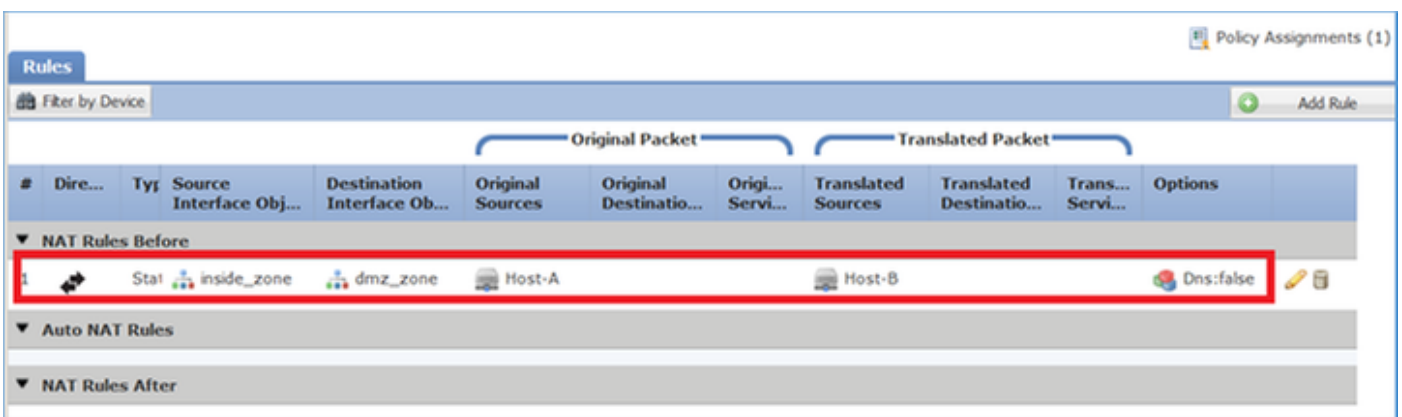
Host-A = 192.168.75.14

Host-B = 192.168.76.100

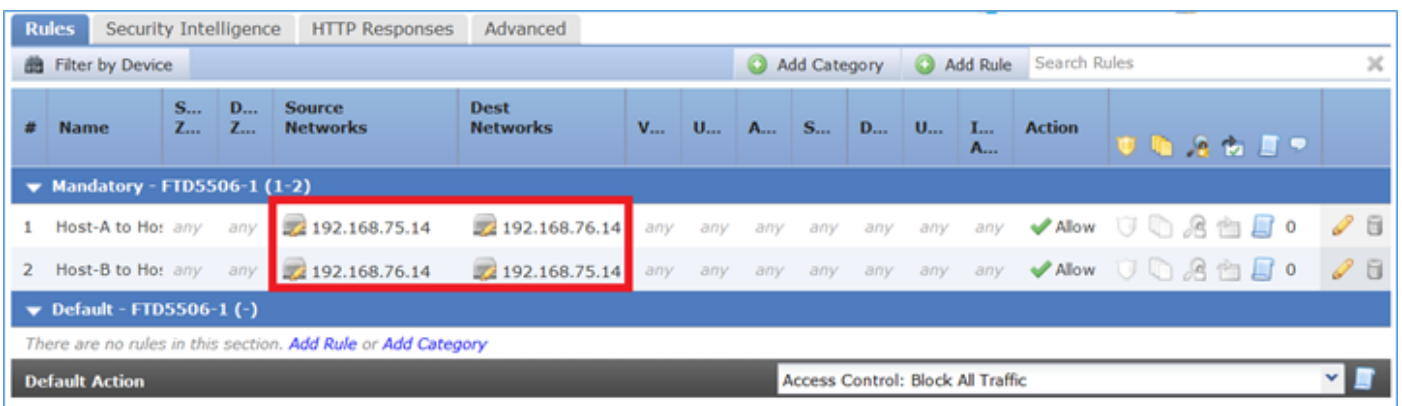
```
firepower# show run object
object network Host-A
  host 192.168.75.14
object network Host-B
  host 192.168.76.100
```

Avviso: Se si configura un NAT statico e si specifica un'interfaccia come origine tradotta, tutto il traffico destinato all'indirizzo IP dell'interfaccia viene reindirizzato. Gli utenti potrebbero non essere in grado di accedere ad alcun servizio abilitato sull'interfaccia mappata. Esempi di tali servizi includono protocolli di routing come OSPF e EIGRP.

Passaggio 7. Il risultato è quello mostrato nell'immagine.



Passaggio 8. Verificare che esista una policy di controllo dell'accesso che consenta all'host B di accedere all'host A e viceversa. Tenere presente che il protocollo NAT statico è bidirezionale per impostazione predefinita. Analogamente alle appliance ASA classiche, è importante notare l'uso di IP reali. Ciò è previsto perché in questa esercitazione, LINA esegue il codice 9.6.1.x, come mostrato nell'immagine.



Verifica:

Dalla CLI di LINA:

```
firepower# show run nat
nat (inside,dmz) source static Host-A Host-B
```

La regola NAT è stata inserita nella sezione 1 come previsto:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (dmz) source static Host-A Host-B
  translate_hits = 0, untranslate_hits = 0
```

Nota: I 2 xlate creati in background.

```
firepower# show xlate
2 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from inside:192.168.75.14 to dmz:192.168.76.100
  flags sT idle 0:41:49 timeout 0:00:00
NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0
  flags sIT idle 0:41:49 timeout 0:00:00
```

Tabelle ASP NAT:

```
firepower# show asp table classify domain nat
```

Input Table

```
in id=0x7ff6036a9f50, priority=6, domain=nat, deny=false
  hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=inside, output_ifc=dmz
in id=0x7ff603696860, priority=6, domain=nat, deny=false
  hits=0, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=inside
```

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never

```
firepower# show asp table classify domain nat-reverse
```

Input Table

Output Table:

```
out id=0x7ff603685350, priority=6, domain=nat-reverse, deny=false
  hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=inside
out id=0x7ff603638470, priority=6, domain=nat-reverse, deny=false
  hits=0, user_data=0x7ff602be3f80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=inside, output_ifc=dmz
```

```
L2 - Output Table:
```

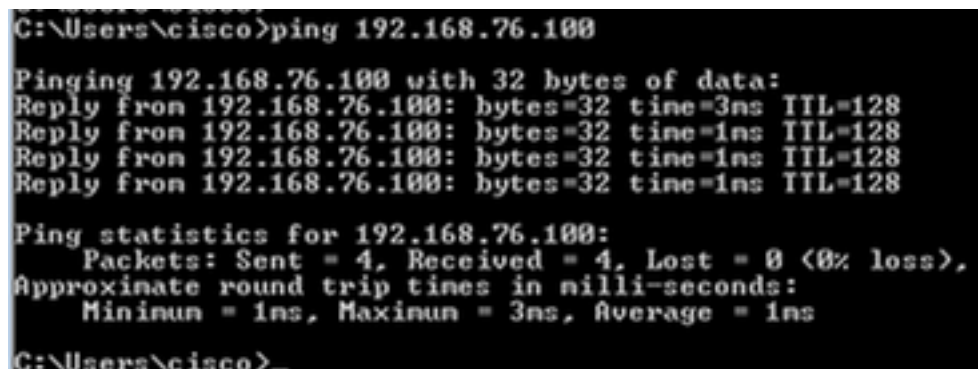
```
L2 - Input Table:
```

```
Last clearing of hits counters: Never
```

Abilitare l'acquisizione con i dettagli di traccia su FTD ed eseguire il ping tra host A e host B, come mostrato nell'immagine.

```
firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100
```

```
firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14
```



```
C:\Users\cisco>ping 192.168.76.100

Pinging 192.168.76.100 with 32 bytes of data:
Reply from 192.168.76.100: bytes=32 time=3ms TTL=128
Reply from 192.168.76.100: bytes=32 time=1ms TTL=128
Reply from 192.168.76.100: bytes=32 time=1ms TTL=128
Reply from 192.168.76.100: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.76.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\cisco>
```

Il numero di accessi è nelle tabelle ASP:

```
firepower# show asp table classify domain nat
```

```
Input Table
```

```
in id=0x7ff6036a9f50, priority=6, domain=nat, deny=false
    hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, flags=0x0, protocol=0
    src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=dmz
in id=0x7ff603696860, priority=6, domain=nat, deny=false
    hits=4, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
    input_ifc=dmz, output_ifc=inside
```

```
firepower# show asp table classify domain nat-reverse
```

```
Input Table
```

```
Output Table:
```

```
out id=0x7ff603685350, priority=6, domain=nat-reverse, deny=false
    hits=4, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
    input_ifc=dmz, output_ifc=inside
out id=0x7ff603638470, priority=6, domain=nat-reverse, deny=false
    hits=0, user_data=0x7ff602be3f80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
    src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=dmz
```


L'acquisizione dei pacchetti visualizza:

```
firepower# show capture DMZ
8 packets captured
 1: 17:38:26.324812      192.168.76.14 > 192.168.76.100: icmp: echo request
 2: 17:38:26.326505      192.168.76.100 > 192.168.76.14: icmp: echo reply
 3: 17:38:27.317991      192.168.76.14 > 192.168.76.100: icmp: echo request
 4: 17:38:27.319456      192.168.76.100 > 192.168.76.14: icmp: echo reply
 5: 17:38:28.316344      192.168.76.14 > 192.168.76.100: icmp: echo request
 6: 17:38:28.317824      192.168.76.100 > 192.168.76.14: icmp: echo reply
 7: 17:38:29.330518      192.168.76.14 > 192.168.76.100: icmp: echo request
 8: 17:38:29.331983      192.168.76.100 > 192.168.76.14: icmp: echo reply
8 packets shown
```

Tracce di un pacchetto (vengono evidenziati i punti importanti).

Nota: ID della regola NAT e relativa correlazione con la tabella ASP:

```
firepower# show capture DMZ packet-number 3 trace detail
8 packets captured
 3: 17:38:27.317991 000c.2998.3fec d8b1.90b7.32e0 0x0800 Length: 74
    192.168.76.14 > 192.168.76.100: icmp: echo request (ttl 128, id 9975)
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
  Forward Flow based lookup yields rule:
  in id=0x7ff602c72be0, priority=13, domain=capture, deny=false
      hits=55, user_data=0x7ff602b74a50, cs_id=0x0, l3_type=0x0
      src mac=0000.0000.0000, mask=0000.0000.0000
      dst mac=0000.0000.0000, mask=0000.0000.0000
      input_ifc=dmz, output_ifc=any
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
  Forward Flow based lookup yields rule:
  in id=0x7ff603612200, priority=1, domain=permit, deny=false
      hits=1, user_data=0x0, cs_id=0x0, l3_type=0x8
      src mac=0000.0000.0000, mask=0000.0000.0000
      dst mac=0000.0000.0000, mask=0100.0000.0000
      input_ifc=dmz, output_ifc=any
```

```
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,dmz) source static Host-A Host-B
Additional Information:
```

NAT divert to egress interface inside
Untranslate 192.168.76.100/0 to 192.168.75.14/0

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip host 192.168.76.14 host 192.168.75.14 rule-id 268434440

access-list CSM_FW_ACL_ remark rule-id 268434440: ACCESS POLICY: FTD5506-1 - Mandatory/2

access-list CSM_FW_ACL_ remark rule-id 268434440: L4 RULE: Host-B to Host-A

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached
Forward Flow based lookup yields rule:

in id=0x7ff602b72610, priority=12, domain=permit, deny=false

hits=1, user_data=0x7ff5fa9d0180, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.76.14, mask=255.255.255.255, port=0, tag=any, ifc=any

dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, ifc=any, vlan=0,

dscp=0x0

input_ifc=any, output_ifc=any

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7ff60367cf80, priority=7, domain=conn-set, deny=false

hits=1, user_data=0x7ff603677080, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0

input_ifc=dmz, output_ifc=any

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,dmz) source static Host-A Host-B

Additional Information:

Static translate 192.168.76.14/1 to 192.168.76.14/1

Forward Flow based lookup yields rule:

in **id=0x7ff603696860**, priority=6, domain=nat, deny=false

hits=1, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0

input_ifc=dmz, output_ifc=inside

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff602220020, priority=0, domain=nat-per-session, deny=true
  hits=2, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=any, output_ifc=any
```

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff6035c0af0, priority=0, domain=inspect-ip-options, deny=true
  hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=any
```

Phase: 9

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

```
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect icmp
service-policy global_policy global
```

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff602b5f020, priority=70, domain=inspect-icmp, deny=false
  hits=2, user_data=0x7ff602be7460, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
  src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=any
```

Phase: 10

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff602b3a6d0, priority=70, domain=inspect-icmp-error, deny=false
  hits=2, user_data=0x7ff603672ec0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
  src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=any
```

Phase: 11

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (inside,dmz) source static Host-A Host-B
```

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x7ff603685350, priority=6, domain=nat-reverse, deny=false
  hits=2, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=inside
```

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x7ff602220020, priority=0, domain=nat-per-session, deny=true
    hits=4, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=any
```

Phase: 13

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x7ff602c56d10, priority=0, domain=inspect-ip-options, deny=true
    hits=2, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=any
```

Phase: 14

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 5084, packet dispatched to next module

Module information for forward flow ...

snp_fp_inspect_ip_options

snp_fp_snort

snp_fp_inspect_icmp

snp_fp_translate

snp_fp_adjacency

snp_fp_fragment

snp_ifc_stat

Module information for reverse flow ...

snp_fp_inspect_ip_options

snp_fp_translate

snp_fp_inspect_icmp

snp_fp_snort

snp_fp_adjacency

snp_fp_fragment

snp_ifc_stat

Phase: 15

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 16

Type: SNORT

Subtype:

Result: ALLOW

Config:

```
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.75.14 using egress ifc inside

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 000c.2930.2b78 hits 140694538708414

Phase: 19
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
  out id=0x7ff6036a94e0, priority=13, domain=capture, deny=false
      hits=14, user_data=0x7ff6024aff90, cs_id=0x0, l3_type=0x0
      src mac=0000.0000.0000, mask=0000.0000.0000
      dst mac=0000.0000.0000, mask=0000.0000.0000
      input_ifc=inside, output_ifc=any

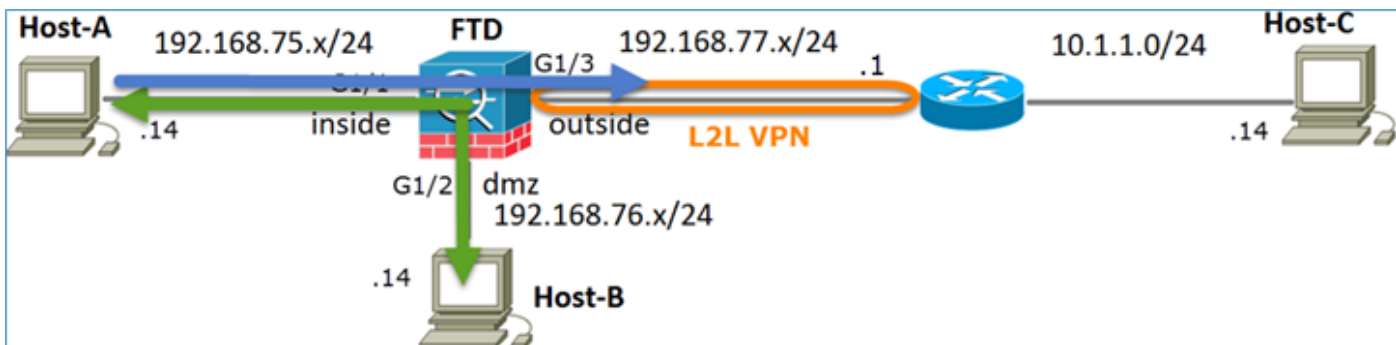
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
1 packet shown
```

Task 2. Configurare Port Address Translation (PAT) su FTD

Configurare NAT in base ai seguenti requisiti:

Regola NAT	Regola NAT manuale
Tipo NAT	Dinamica
Inserisci	Nella sezione 1
Source interface	interno*
Interfaccia di destinazione	esterno*
Origine	192.168.75.0/24
Origine tradotta	Interfaccia esterna (PAT)

*Usare le zone di sicurezza per la regola NAT



NAT statico

PAT

Soluzione:

Passaggio 1. Aggiungere una seconda regola NAT e configurare in base ai requisiti dell'attività, come mostrato nell'immagine.

Passaggio 2. Di seguito viene riportata la configurazione di PAT come mostrato nell'immagine.

Passaggio 3. Il risultato è quello mostrato nell'immagine.

#	Direction	T...	Original Packet			Translated Packet				Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	
▼ NAT Rules Before										
1		St...	inside_zone	dmz_zone	Host-A		Host-B			Dns:false
2		D...	inside_zone	outside_zone	Net_192.168.75.0_24bits		Interface			Dns:false
▼ Auto NAT Rules										
▼ NAT Rules After										

Passaggio 4. Nel prosieguo di questa esercitazione, configurare i criteri di controllo di accesso per consentire il passaggio di tutto il traffico.

Verifica:

Configurazione NAT:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (dmz) source static Host-A Host-B
  translate_hits = 26, untranslate_hits = 26
2 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
  translate_hits = 0, untranslate_hits = 0
```

Dalla CLI di LINA, notare la nuova voce:

```
firepower# show xlate
3 in use, 19 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from inside:192.168.75.14 to dmz:192.168.76.100
  flags sT idle 1:15:14 timeout 0:00:00
NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0
  flags sIT idle 1:15:14 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
  flags sIT idle 0:04:02 timeout 0:00:00
```

Abilita l'acquisizione sull'interfaccia interna ed esterna. Attiva traccia durante l'acquisizione interna:

```
firepower# capture CAPI trace interface inside match ip host 192.168.75.14 host 192.168.77.1
firepower# capture CAPO interface outside match ip any host 192.168.77.1
```

Eeguire il ping tra l'host A (192.168.75.14) e l'host IP 192.168.77.1, come mostrato nell'immagine.

```
C:\Windows\system32>ping 192.168.77.1
Pinging 192.168.77.1 with 32 bytes of data:
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.77.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Nelle clip di LINA, è possibile vedere la traduzione di PAT:

```
firepower# show cap CAPI
8 packets captured
 1: 18:54:43.658001      192.168.75.14 > 192.168.77.1: icmp: echo request
 2: 18:54:43.659099      192.168.77.1 > 192.168.75.14: icmp: echo reply
 3: 18:54:44.668544      192.168.75.14 > 192.168.77.1: icmp: echo request
 4: 18:54:44.669505      192.168.77.1 > 192.168.75.14: icmp: echo reply
 5: 18:54:45.682368      192.168.75.14 > 192.168.77.1: icmp: echo request
 6: 18:54:45.683421      192.168.77.1 > 192.168.75.14: icmp: echo reply
 7: 18:54:46.696436      192.168.75.14 > 192.168.77.1: icmp: echo request
 8: 18:54:46.697412      192.168.77.1 > 192.168.75.14: icmp: echo reply
```

```
firepower# show cap CAPO
8 packets captured
 1: 18:54:43.658672      192.168.77.6 > 192.168.77.1: icmp: echo request
 2: 18:54:43.658962      192.168.77.1 > 192.168.77.6: icmp: echo reply
 3: 18:54:44.669109      192.168.77.6 > 192.168.77.1: icmp: echo request
 4: 18:54:44.669337      192.168.77.1 > 192.168.77.6: icmp: echo reply
 5: 18:54:45.682932      192.168.77.6 > 192.168.77.1: icmp: echo request
 6: 18:54:45.683207      192.168.77.1 > 192.168.77.6: icmp: echo reply
 7: 18:54:46.697031      192.168.77.6 > 192.168.77.1: icmp: echo request
 8: 18:54:46.697275      192.168.77.1 > 192.168.77.6: icmp: echo reply
```

Tracce di un pacchetto con sezioni importanti evidenziate:

```
firepower# show cap CAPI packet-number 1 trace
8 packets captured
 1: 18:54:43.658001      192.168.75.14 > 192.168.77.1: icmp: echo request

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```


Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.77.1 using egress ifc outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:
Dynamic translate 192.168.75.14/1 to 192.168.77.6/1

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default

```
inspect icmp
service-policy global_policy global
```

Additional Information:

Phase: 10

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 11

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
```

Additional Information:

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 13

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 14

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 6981, packet dispatched to next module

Phase: 15

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 16

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Verdict: (pass-packet) allow this packet

Phase: 17

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.77.1 using egress ifc outside

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address c84c.758d.4980 hits 140694538709114

Phase: 19
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
1 packet shown

L'espressione dinamica è stata creata (notare i flag "ri"):

```
firepower# show xlate
4 in use, 19 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from inside:192.168.75.14 to dmz:192.168.76.100
      flags sT idle 1:16:47 timeout 0:00:00
NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0
      flags sIT idle 1:16:47 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
      flags sIT idle 0:05:35 timeout 0:00:00
```

```
ICMP PAT from inside:192.168.75.14/1 to outside:192.168.77.6/1 flags ri idle 0:00:30 timeout
0:00:30
```

Nei log LINA è possibile vedere:

```
firepower# show log
May 31 2016 18:54:43: %ASA-7-609001: Built local-host inside:192.168.75.14
May 31 2016 18:54:43: %ASA-6-305011: Built dynamic ICMP translation from inside:192.168.75.14/1
to outside:192.168.77.6/1
May 31 2016 18:54:43: %ASA-7-609001: Built local-host outside:192.168.77.1
May 31 2016 18:54:43: %ASA-6-302020: Built inbound ICMP connection for faddr 192.168.75.14/1
gaddr 192.168.77.1/0 laddr 192.168.77.1/0
May 31 2016 18:54:43: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.75.14/1 gaddr
192.168.77.1/0 laddr 192.168.77.1/0
May 31 2016 18:54:43: %ASA-7-609002: Teardown local-host outside:192.168.77.1 duration 0:00:00
May 31 2016 18:55:17: %ASA-6-305012: Teardown dynamic ICMP translation from
inside:192.168.75.14/1 to outside:192.168.77.6/1 duration 0:00:34
```

Sezioni NAT:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (dmz) source static Host-A Host-B
   translate_hits = 26, untranslate_hits = 26
2 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
   translate_hits = 94, untranslate_hits = 138
```

Le tabella ASP mostrano:

```
firepower# show asp table classify domain nat
```

Input Table

```
in id=0x7ff6036a9f50, priority=6, domain=nat, deny=false
   hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, flags=0x0, protocol=0
   src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
   dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=dmz
in id=0x7ff603696860, priority=6, domain=nat, deny=false
   hits=4, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
   input_ifc=dmz, output_ifc=inside
in id=0x7ff602c75f00, priority=6, domain=nat, deny=false
   hits=94, user_data=0x7ff6036609a0, cs_id=0x0, flags=0x0, protocol=0
   src ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any
   dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=outside
in id=0x7ff603681fb0, priority=6, domain=nat, deny=false
   hits=276, user_data=0x7ff60249f370, cs_id=0x0, flags=0x0, protocol=0
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=192.168.77.6, mask=255.255.255.255, port=0, tag=any, dscp=0x0
   input_ifc=outside, output_ifc=inside
```

```
firepower# show asp table classify domain nat-reverse
```

Input Table

Output Table:

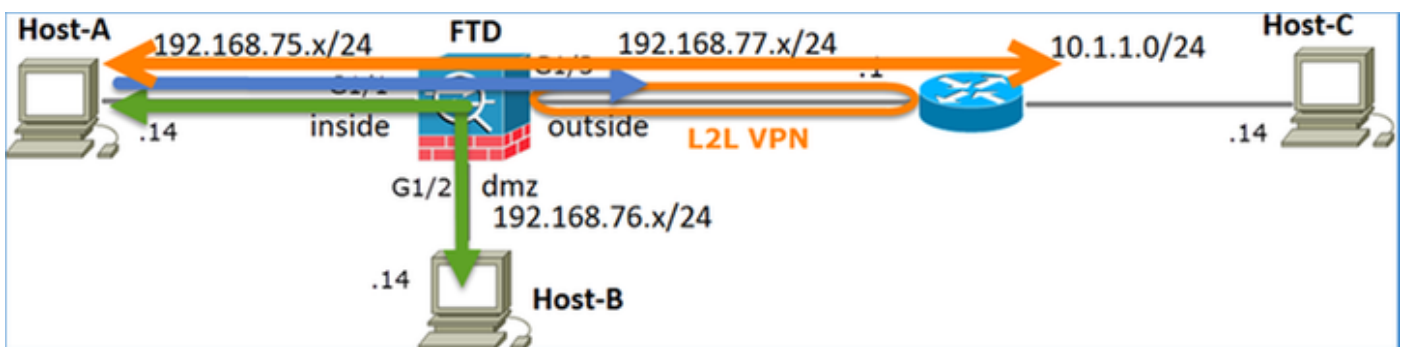
```
out id=0x7ff603685350, priority=6, domain=nat-reverse, deny=false
   hits=4, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
   input_ifc=dmz, output_ifc=inside
out id=0x7ff603638470, priority=6, domain=nat-reverse, deny=false
   hits=0, user_data=0x7ff602be3f80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
   src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
   dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=dmz
out id=0x7ff60361bda0, priority=6, domain=nat-reverse, deny=false
   hits=138, user_data=0x7ff6036609a0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
   input_ifc=outside, output_ifc=inside
out id=0x7ff60361c180, priority=6, domain=nat-reverse, deny=false
   hits=94, user_data=0x7ff60249f370, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
   src ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any
   dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=outside
```

Task 3. Configurare l'esenzione NAT su FTD

Configurare NAT in base ai seguenti requisiti:

Regola NAT	Regola NAT manuale
Tipo NAT	Statico
Inserisci	Nella sezione 1 tutte le norme esistenti
Source interface	interno*
Interfaccia di destinazione	esterno*
Origine	192.168.75.0/24
Origine tradotta	192.168.75.0/24
Destinazione originale	10.1.1.0/24
Destinazione tradotta	10.1.1.0/24

*Usare le zone di sicurezza per la regola NAT



NAT statico

PAT

Esenzione NAT

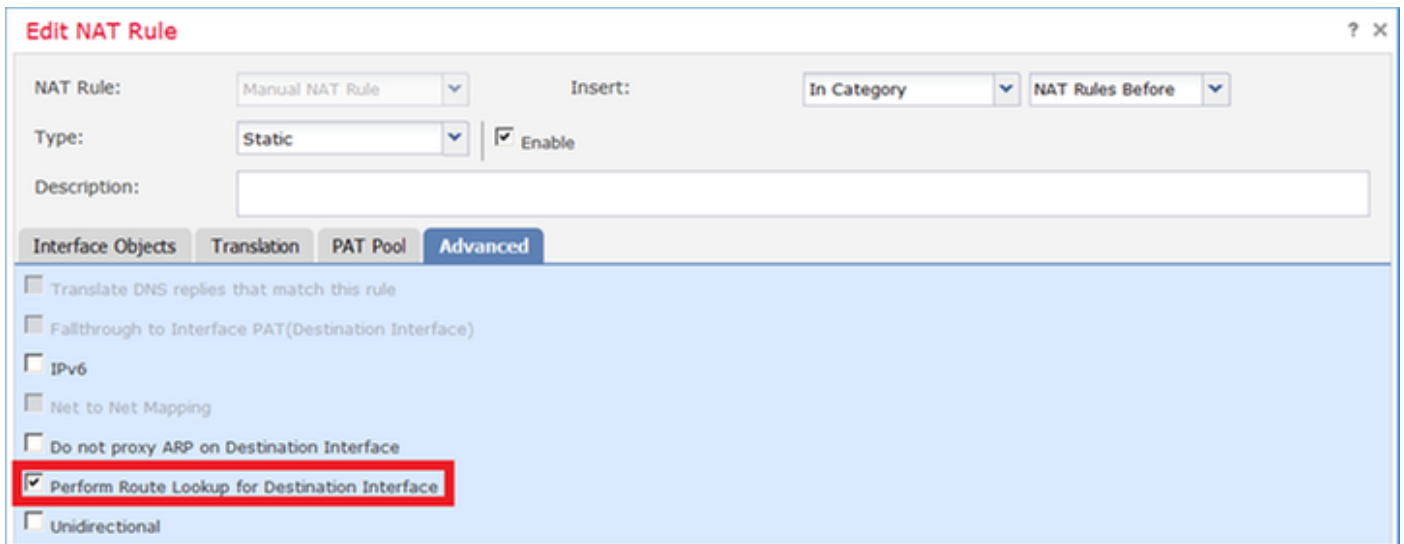
Soluzione:

Passaggio 1. Aggiungere una terza regola NAT e configurare i requisiti per attività come mostrato nell'immagine.

Rules										
Filter by Device										
	Original Packet					Translated Packet				
#	Direction	Ty...	Source Interface O...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before										
1	→	Sta...	inside_zone	outside_zone	Net_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24b	net_10.1.1.0_24bits	
2	→	Sta...	inside_zone	dmz_zone	Host-A			Host-B		
3	→	Dy...	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		
▼ Auto NAT Rules										
▼ NAT Rules After										

Passaggio 2. Eseguire la ricerca route per determinare l'interfaccia di uscita.

Nota: Per le regole NAT di identità, come quelle aggiunte, è possibile modificare la modalità di determinazione dell'interfaccia in uscita e utilizzare la ricerca route normale, come mostrato nell'immagine.



Verifica:

```
firepower# show run nat
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
static net_10.1.1.0_24bits net_10.1.1.0_24bits
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
```

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
   translate_hits = 0, untranslate_hits = 0
2 (inside) to (dmz) source static Host-A Host-B
   translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
   translate_hits = 96, untranslate_hits = 138
```

Esegui packet-tracer per il traffico non VPN proveniente dalla rete interna. La regola PAT viene utilizzata come previsto:

```
firepower# packet-tracer input inside tcp 192.168.75.14 1111 192.168.77.1 80
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
```

Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.77.1 using egress ifc outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:

Dynamic translate 192.168.75.14/1111 to 192.168.77.6/1111

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:

Phase: 10

Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7227, 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

Eeguire packet-tracer per il traffico che deve passare attraverso il tunnel VPN (eseguirlo due volte dal primo tentativo di attivazione del tunnel VPN).

Nota: È necessario rispettare la regola di esenzione NAT.

Primo tentativo di traccia dei pacchetti:

```
firepower# packet-tracer input inside tcp 192.168.75.14 1111 10.1.1.1 80
```

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits

Additional Information:

NAT divert to egress interface outside

Untranslate 10.1.1.1/80 to 10.1.1.1/80

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434

access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1

access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits

Additional Information:

Static translate 192.168.75.14/1111 to 192.168.75.14/1111

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: encrypt

Result: DROP

Config:

Additional Information:

Result:

input-interface: inside

```
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Secondo tentativo di traccia dei pacchetti:

```
firepower# packet-tracer input inside tcp 192.168.75.14 1111 10.1.1.1 80
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

Phase: 3

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
static net_10.1.1.0_24bits net_10.1.1.0_24bits
```

Additional Information:

NAT divert to egress interface outside

Untranslate 10.1.1.1/80 to 10.1.1.1/80

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
Additional Information:
```

This packet will be sent to snort for additional processing where a verdict will be reached

```
Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
  match any
policy-map global_policy
  class class-default
    set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits

Additional Information:

Static translate 192.168.75.14/1111 to 192.168.75.14/1111

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits

Additional Information:

Phase: 11

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 13

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 14

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7226, 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

Verifica conteggio visite NAT:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
   translate_hits = 9, untranslate_hits = 9
2 (inside) to (dmz) source static Host-A Host-B
   translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
   translate_hits = 98, untranslate_hits = 138
```

Task 4. Configurare l'oggetto NAT su FTD

Configurare NAT in base ai seguenti requisiti:

Regola NAT	Regola NAT automatica
Tipo NAT	Statico
Inserisci	Nella sezione 2
Source interface	interno*
Interfaccia di destinazione	dmz*
Origine	192.168.75.99
Origine tradotta	192.168.76.99
Traduci le risposte DNS corrispondenti a questa regola	Attivato

*Usare le zone di sicurezza per la regola NAT

Soluzione:

Passaggio 1. Configurare la regola in base ai requisiti del task come mostrato nelle immagini.

Add NAT Rule

NAT Rule: **Auto NAT Rule** Enable

Type: **Static** Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1): **inside_zone**

Destination Interface Objects (1): **dmz_zone**

Add to Source

Add to Destination

Add NAT Rule

NAT Rule: Auto NAT Rule Enable

Type: Static Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source: * **obj-192.168.75.99**

Original Port: TCP

Translated Packet

Translated Source: Address **obj-192.168.76.99**

Translated Port:

Add NAT Rule

NAT Rule: Auto NAT Rule Enable

Type: Static Enable

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Passaggio 2. Il risultato è quello mostrato nell'immagine.

Rules

Filter by Device

#	Direction	Ty...	Source Interface O...	Destination Interface Obj...	Original Packet			Translated Packet		
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
NAT Rules Before										
1	↔	Sta...	inside_zone	outside_zone	Net_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24b	net_10.1.1.0_24bits	
2	↔	Sta...	inside_zone	dmz_zone	Host-A			Host-B		
3	→	Dy...	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		
Auto NAT Rules										
#	↔	Sta...	inside_zone	dmz_zone	obj-192.168.75.99			obj-192.168.76.99		
NAT Rules After										

Verifica:

```
firepower# show run nat
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
static net_10.1.1.0_24bits net_10.1.1.0_24bits
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
!
object network obj-192.168.75.99
  nat (inside,dmz) static obj-192.168.76.99 dns
```

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
  translate_hits = 9, untranslate_hits = 9
2 (inside) to (dmz) source static Host-A Host-B
  translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
  translate_hits = 98, untranslate_hits = 138

Auto NAT Policies (Section 2)
1 (inside) to (dmz) source static obj-192.168.75.99 obj-192.168.76.99 dns
  translate_hits = 0, untranslate_hits = 0
```

Verifica con packet-tracer:

```
firepower# packet-tracer input inside tcp 192.168.75.99 1111 192.168.76.100 80

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.76.100 using egress ifc dmz

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

**object network obj-192.168.75.99
nat (inside,dmz) static obj-192.168.76.99 dns**

Additional Information:

Static translate 192.168.75.99/1111 to 192.168.76.99/1111

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 11

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 7245, 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

Task 5. Configurare il pool PAT su FTD

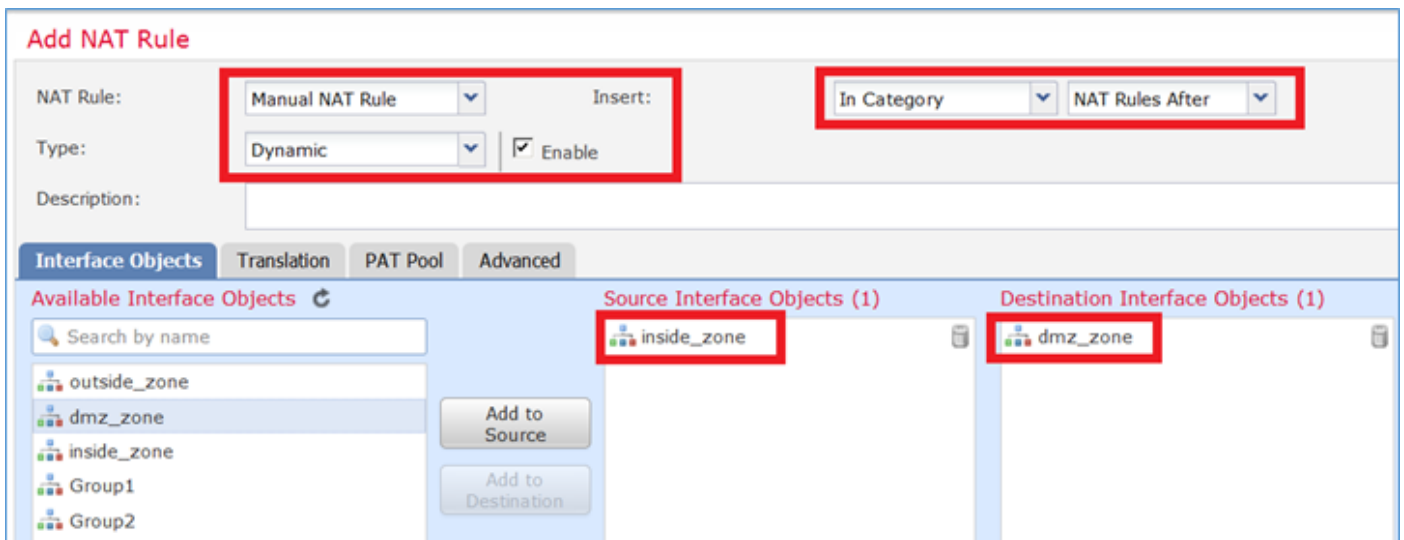
Configurare NAT in base ai seguenti requisiti:

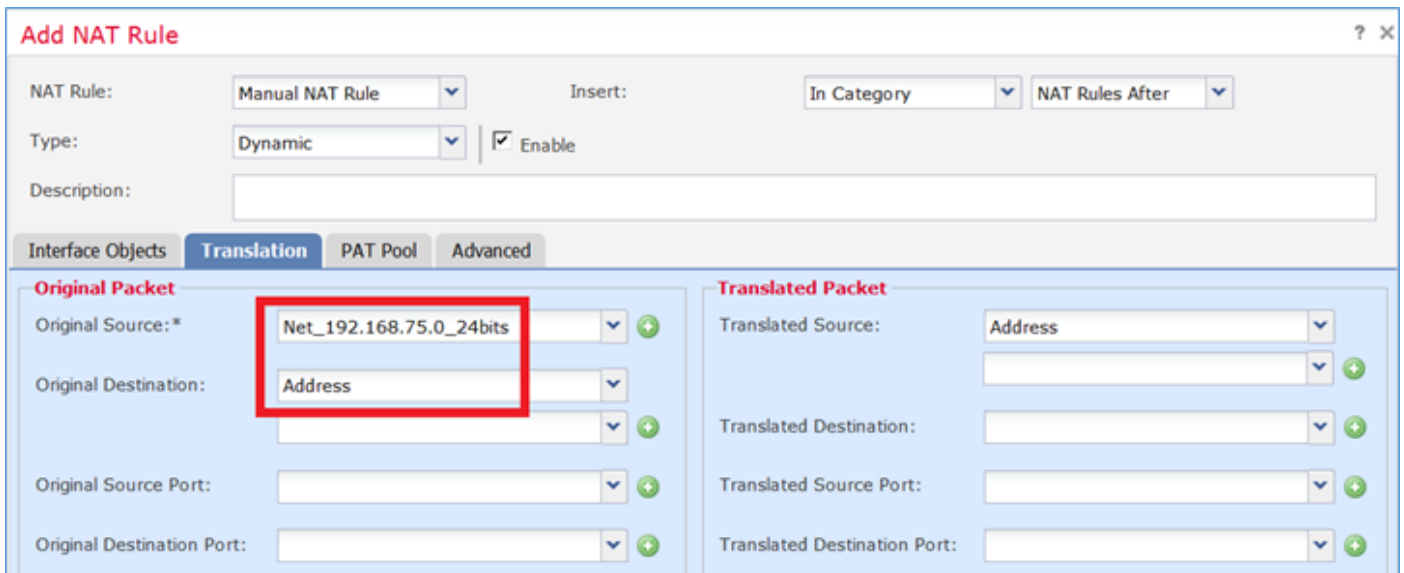
Regola NAT	Regola NAT manuale
Tipo NAT	Dinamica
Inserisci	Nella sezione 3
Source interface	interno*
Interfaccia di destinazione	dmz*
Origine	192.168.75.0/24
Origine tradotta	192.168.76.20-22
Utilizza l'intero intervallo (1-65535)	Attivato

*Usare le zone di sicurezza per la regola NAT

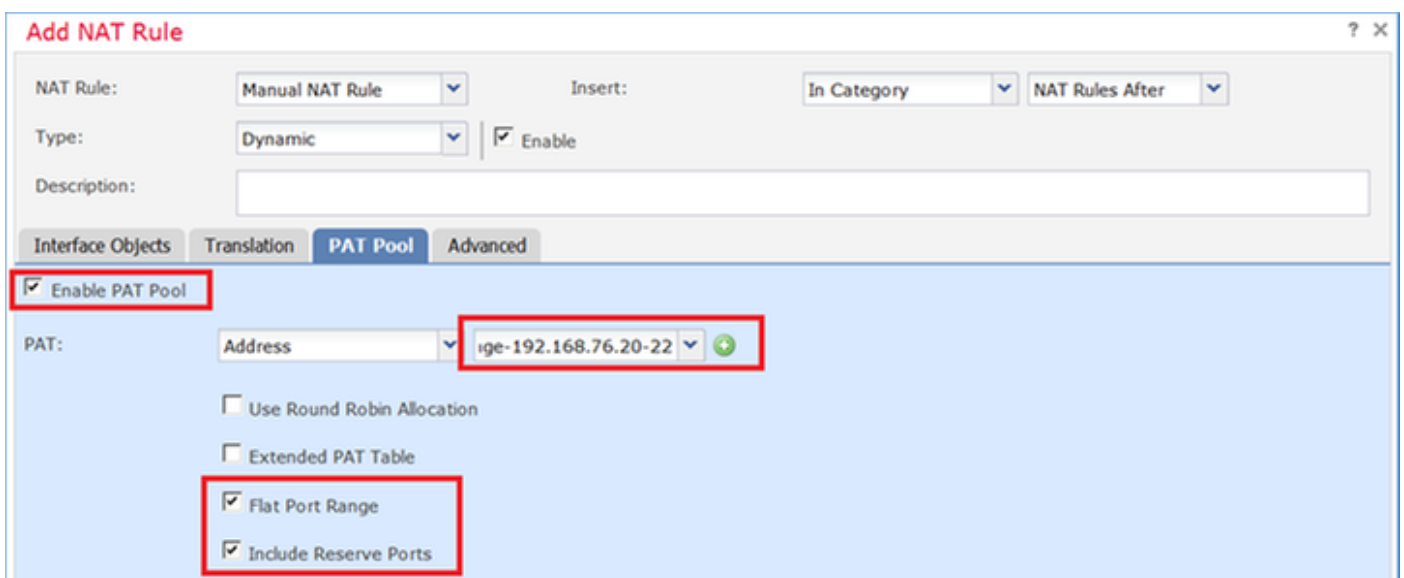
Soluzione:

Passaggio 1. Configurare i requisiti della regola per task come mostrato nelle immagini.





Passaggio 2. Abilitare l'intervallo di porte piatte con **Includi porte riservate** che consente l'utilizzo dell'intero intervallo (1-65535) come mostrato nell'immagine.



Passaggio 3. Il risultato è quello mostrato nell'immagine.

#	Direction	T...	Source Interface ...	Destination Interface Ob...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1	→	St...	inside_zone	outside_zone	Net_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24bits	net_10.1.1.0_24bi		Dns:false
2	→	St...	inside_zone	dmz_zone	Host-A			Host-B			Dns:false
3	→	Dy...	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface			Dns:false
▼ Auto NAT Rules											
#	→	St...	inside_zone	dmz_zone	obj-192.168.75.99			obj-192.168.76.99			Dns:true
▼ NAT Rules After											
4	→	Dy...	inside_zone	dmz_zone	Net_192.168.75.0_24bits			range-192.168.76.20-22			Dns:false flat include-reserve

Verifica:

```
firepower# show run nat
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
```

```
static net_10.1.1.0_24bits net_10.1.1.0_24bits
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
!
object network obj-192.168.75.99
  nat (inside,dmz) static obj-192.168.76.99 dns
!
nat (inside,dmz) after-auto source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat include-reserve
```

La regola è nella Sezione 3:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
  translate_hits = 9, untranslate_hits = 9
2 (inside) to (dmz) source static Host-A Host-B
  translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
  translate_hits = 98, untranslate_hits = 138

Auto NAT Policies (Section 2)
1 (inside) to (dmz) source static obj-192.168.75.99 obj-192.168.76.99 dns
  translate_hits = 1, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (inside) to (dmz) source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat include-reserve
  translate_hits = 0, untranslate_hits = 0
```

Verifica del tracer del pacchetto:

```
firepower# packet-tracer input inside icmp 192.168.75.15 8 0 192.168.76.5

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
```

found next-hop 192.168.76.5 using egress ifc dmz

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434

access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1

access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,dmz) after-auto source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat include-reserve

Additional Information:

Dynamic translate 192.168.75.15/0 to 192.168.76.20/11654

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

inspect icmp

service-policy global_policy global

Additional Information:

Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,dmz) after-auto source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat include-reserve
Additional Information:

Phase: 12
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7289, 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

Verifica

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

La verifica è stata spiegata nelle singole sezioni delle attività.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Aprire la pagina **Advanced Troubleshooting** (Risoluzione avanzata problemi) nel FMC, eseguire packet-tracer ed eseguire il comando **show nat pool**.

Notate la voce che usa l'intero intervallo come mostrato nell'immagine.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, and AMP. Below these are sub-tabs: Configuration, Users, Domains, Integration, Updates, Licenses, and Health & Monitor. The main heading is "Advanced Troubleshooting" for device FTD5506-1. There are two tabs: "File Download" and "ASA CLI". In the "ASA CLI" tab, there is a "Command" field with a dropdown menu set to "show" and a "Parameter" field with "nat pool". A red box highlights the "show" dropdown and the "Parameter" field, with a red "1" next to it. Below the command fields is the "Output" area, which contains the following text:
UDP PAT pool inside, address 192.168.75.6, range 1-511, allocated 2
UDP PAT pool inside, address 192.168.75.6, range 512-1023, allocated 1
UDP PAT pool inside, address 192.168.75.6, range 1024-65535, allocated 2
ICMP PAT pool dmz:range-192.168.76.20-22, address 192.168.76.20, range 1-65535, allocated 1
UDP PAT pool outside, address 192.168.77.6, range 1-511, allocated 3
UDP PAT pool outside, address 192.168.77.6, range 512-1023, allocated 0
UDP PAT pool outside, address 192.168.77.6, range 1024-65535, allocated 3
At the bottom of the interface, there is an "Execute" button and a "Back" button. A red box highlights the "Execute" button, with a red "2" next to it.

Informazioni correlate

- Tutte le versioni della guida alla configurazione di Cisco Firepower Management Center sono disponibili qui:

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- Cisco Global Technical Assistance Center (TAC) consiglia vivamente questa guida visiva per una conoscenza pratica e approfondita delle tecnologie di sicurezza di nuova generazione di Cisco Firepower, incluse quelle menzionate in questo articolo:

<http://www.ciscopress.com/title/9781587144806>

- Per tutte le note tecniche sulla configurazione e la risoluzione dei problemi relative alle tecnologie Firepower:

<https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series->

[home.html](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).