

Configurar e verificar o NAT no FTD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Tarefa 1. Configurar NAT estático no FTD](#)

[Tarefa 2. Configurar a Conversão de Endereço de Porta \(PAT - Port Address Translation\) no FTD](#)

[Tarefa 3. Configurar a isenção de NAT no FTD](#)

[Tarefa 4. Configurar NAT de objeto em FTD](#)

[Tarefa 5. Configurar o pool PAT no FTD](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e verificar a Network Address Translation (NAT) básica no Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA5506X que executa o código FTD 6.1.0-226
- FireSIGHT Management Center (FMC) com 6.1.0-226
- 3 hosts do Windows 7
- Roteador Cisco IOS® 3925 que executa VPN LAN a LAN (L2L)

Tempo de conclusão do laboratório: 1 hora

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

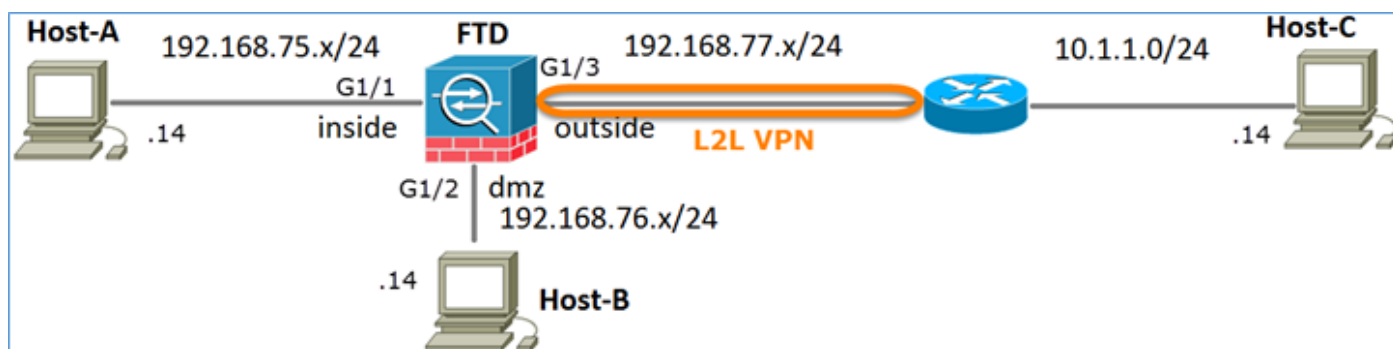
O FTD oferece suporte às mesmas opções de configuração de NAT que o ASA (Adaptive Security Appliance) clássico:

- Regras de NAT antes - Isso equivale ao NAT duas vezes (seção 1) no ASA clássico.
- Regras de NAT automático - Seção 2 sobre ASA clássico
- Regras de NAT depois - Isso equivale a duas vezes o NAT (seção 3) no ASA clássico.

Como a configuração do FTD é feita no FMC quando se trata da configuração do NAT, é necessário estar familiarizado com a GUI do FMC e as várias opções de configuração.

Configurar

Diagrama de Rede



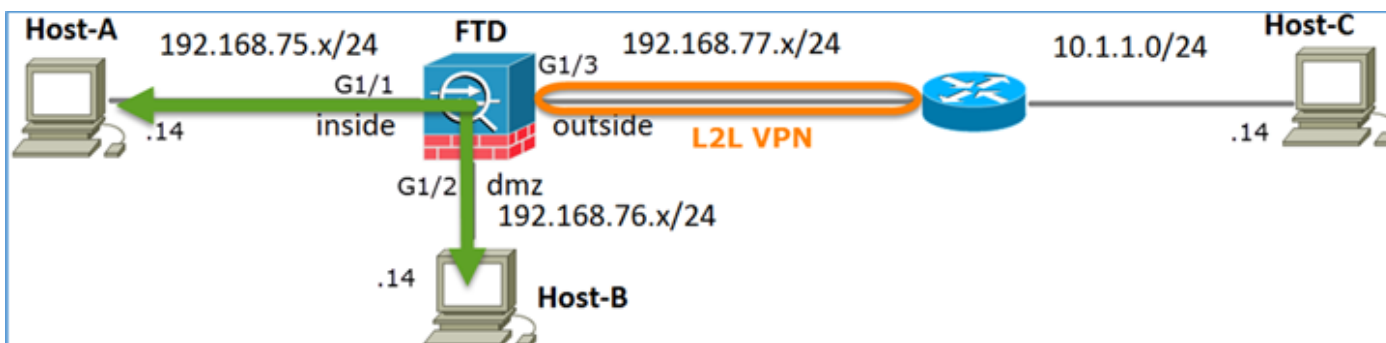
Tarefa 1. Configurar NAT estático no FTD

Configure o NAT de acordo com estes requisitos:

Nome da política de NAT	Nome do dispositivo de FTD
Regra NAT	Regra de NAT manual
Tipo de NAT	Estático
Inserir	Na Seção 1
Interface de origem	interno*

Interface de destino	dmz*
Origem Original	192.168.75.14
Fonte traduzida	192.168.76.100

*Usar Zonas de Segurança para a Regra NAT



NAT Estático

Solução:

No ASA clássico, você deve usar nameif nas regras de NAT. No FTD, você precisa usar Zonas de segurança ou Grupos de interface.

Etapa 1. Atribua interfaces a Zonas de segurança/Grupos de interface.

Nesta tarefa, decidiu-se atribuir as interfaces de FTD que são usadas para NAT a Zonas de segurança. Como alternativa, você pode atribuí-los a Grupos de interface como mostrado na imagem.

Edit Physical Interface

Mode:

Name: Enabled Management Only

Security Zone:

Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9198)

Interface ID:

Etapa 2. O resultado é o mostrado na imagem.

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)

Etapa 3. Você pode criar/editar Grupos de interface e Zonas de segurança na página Objetos > Gerenciamento de objetos como mostrado na imagem.

Overview | Analysis | Policies | Devices | **Objects** | AMP | Deploy | System | Help | admin

Object Management | Intrusion Rules

Network | Port | Interface | Tunnel Tag | Application Filters | VLAN Tag

Name	Type	Interface Type
dmz_zone	Security	
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

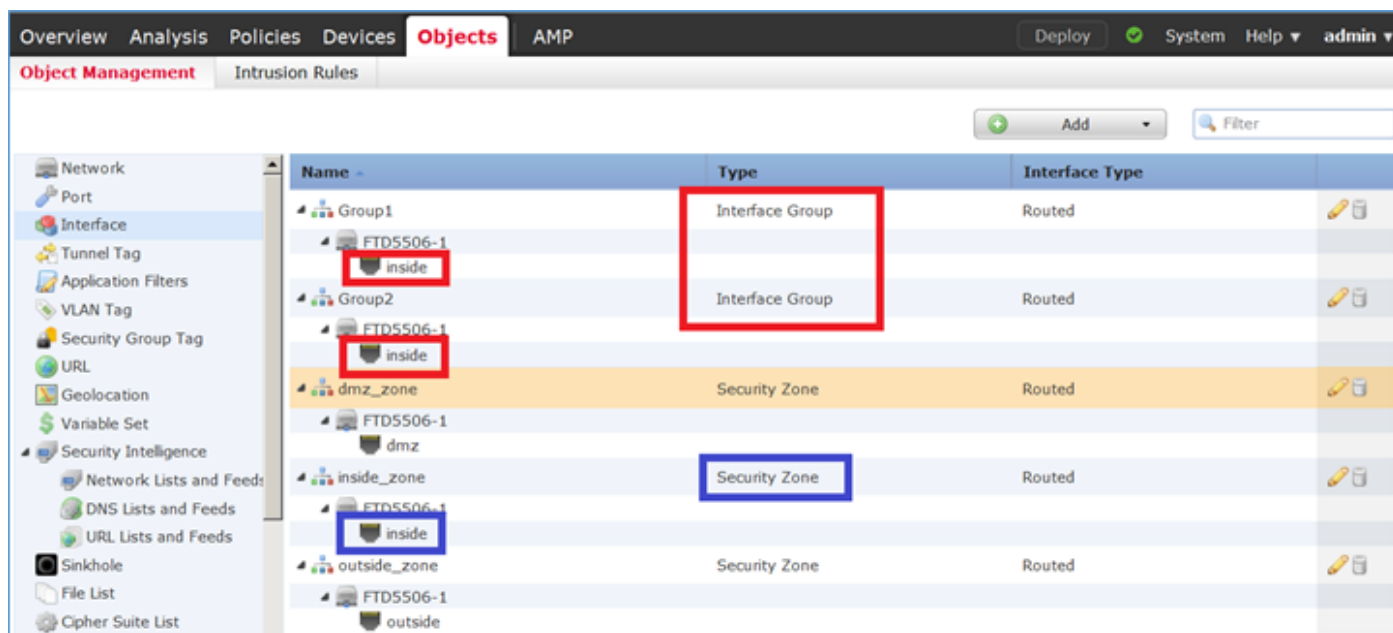
Filter

Zonas de segurança versus grupos de interface

A principal diferença entre Zonas de segurança e Grupos de interface é que uma interface pode pertencer a apenas uma Zona de segurança, mas pode pertencer a vários Grupos de interface. Praticamente, os grupos de interface fornecem mais flexibilidade.

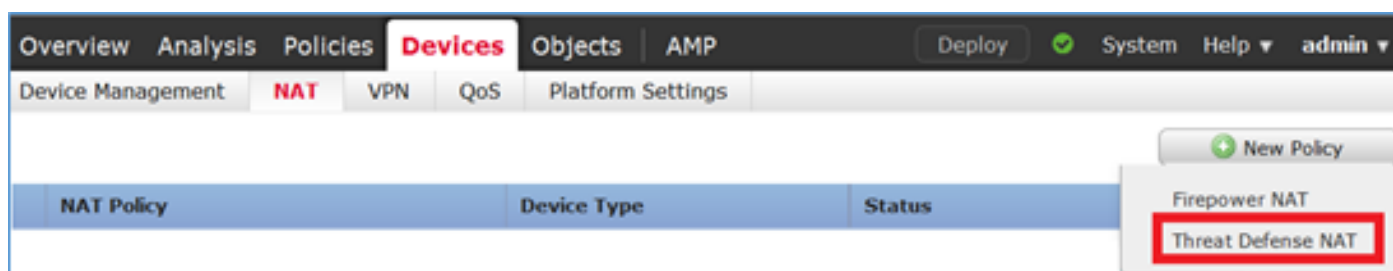
Você pode ver que a interface interna pertence a dois grupos de interface diferentes, mas apenas

uma zona de segurança, como mostrado na imagem.

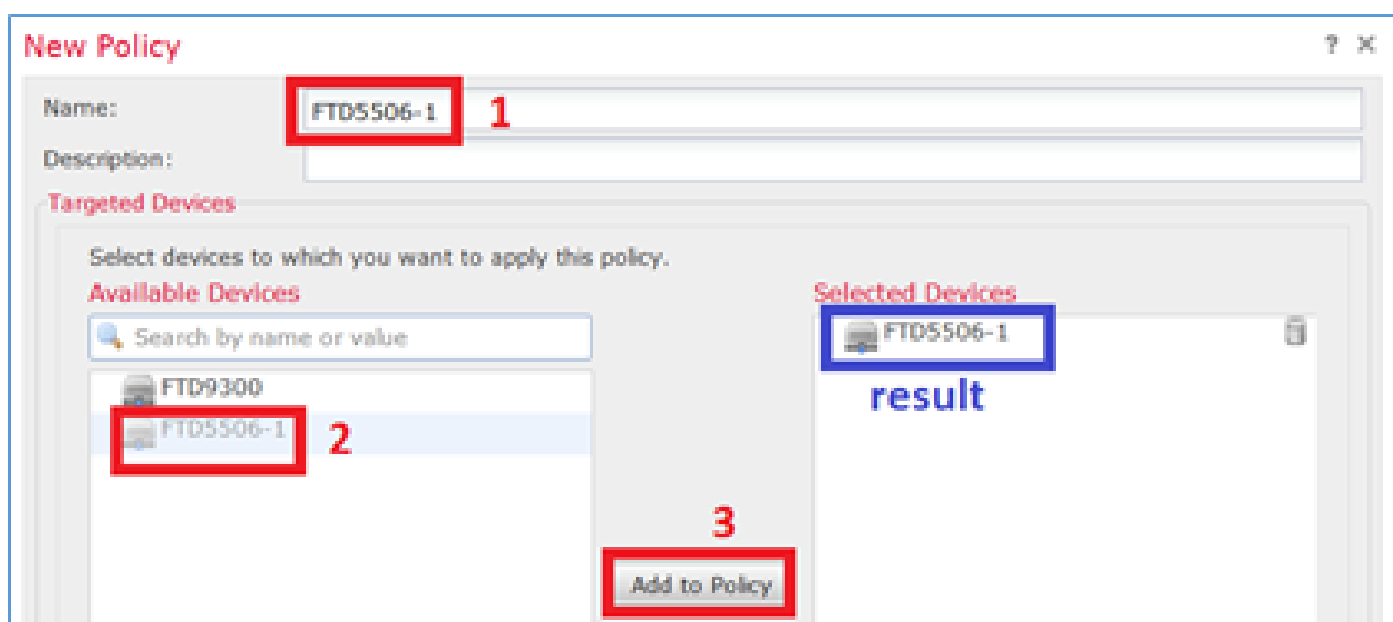


Etapa 4. Configure o NAT estático no FTD.

Navegue até Devices > NAT e crie uma política de NAT. Selecione New Policy > Threat Defense NAT como mostrado na imagem.



Etapa 5. Especifique o nome da política e atribua-o a um dispositivo de destino conforme mostrado na imagem.



Etapa 6. Adicione uma regra NAT à política e clique em Add Rule.

Especifique-os de acordo com os requisitos da tarefa, conforme mostrado nas imagens.

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

Search by name

- 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: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source: * Host-A

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

Translated Destination: Host-B

Translated Source Port:

Translated Destination Port:

Host-A = 192.168.75.14


Host-B = 192.168.76.100

<#root>

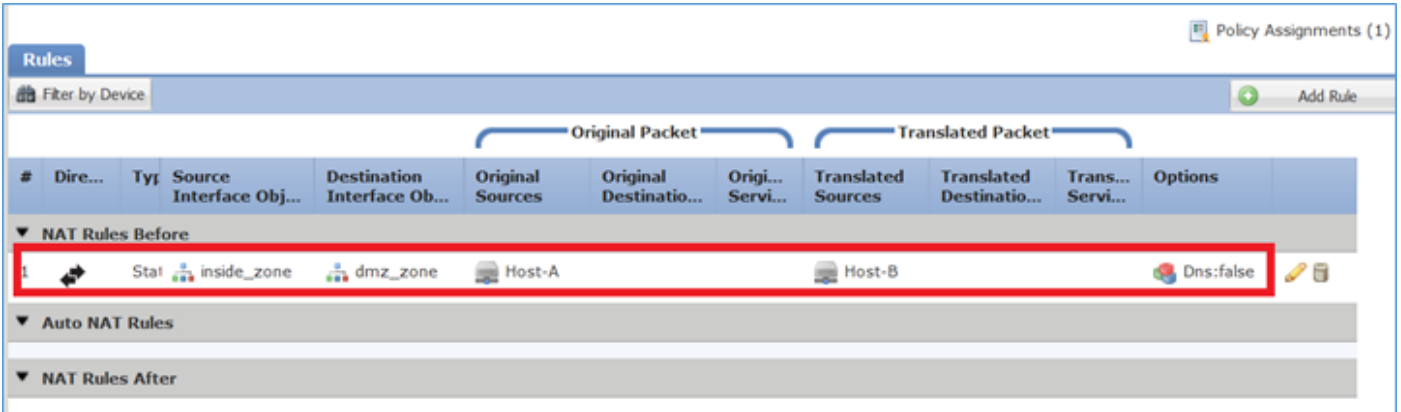
firepower#

show run object

```
object network Host-A
 host 192.168.75.14
object network Host-B
 host 192.168.76.100
```

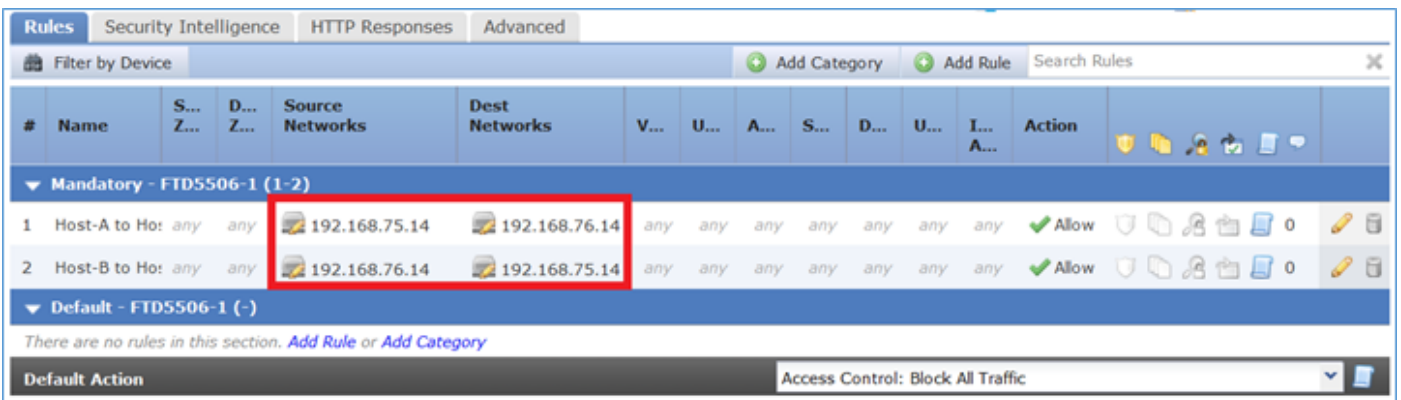
 Aviso: se você configurar o NAT estático e especificar uma interface como origem convertida, todo o tráfego destinado ao endereço IP da interface será redirecionado. Os usuários não podem acessar nenhum serviço habilitado na interface mapeada. Exemplos desses serviços incluem protocolos de roteamento como OSPF e EIGRP.

Passo 7. O resultado é o mostrado na imagem.



#	Dire...	Typ	Source Interface Obj...	Destination Interface Ob...	Original Sources	Original Destinatio...	Origi... Servi...	Translated Sources	Translated Destinatio...	Trans... Servi...	Options
1		Stat	inside_zone	dmz_zone	Host-A			Host-B			Dns:false

Etapa 8. Certifique-se de que haja uma Política de Controle de Acesso que permita ao Host-B acessar o Host-A e vice-versa. Lembre-se de que o NAT estático é bidirecional por padrão. Semelhante aos ASAs clássicos, veja o uso de IPs reais. Isso é esperado, pois neste laboratório, o LINA executa o código 9.6.1.x, como mostrado na imagem.



#	Name	S... Z...	D... Z...	Source Networks	Dest Networks	V...	U...	A...	S...	D...	U...	I... A...	Action
1	Host-A to Ho:	any	any	192.168.75.14	192.168.76.14	any	any	any	any	any	any	any	Allow
2	Host-B to Ho:	any	any	192.168.76.14	192.168.75.14	any	any	any	any	any	any	any	Allow

Verificação:

Do LINA CLI:

```
<#root>
```


```
firepower#
```

```
show run nat
```

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

A regra NAT foi inserida na Seção 1 como esperado:

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

 Observação: os 2 xlates criados em segundo plano.

```
<#root>
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
```

As tabelas NAT do ASP:

```
<#root>
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

<#root>

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

Ative a captura com detalhes de rastreamento no FTD e faça ping do Host-B para o Host-A e como mostrado na imagem.

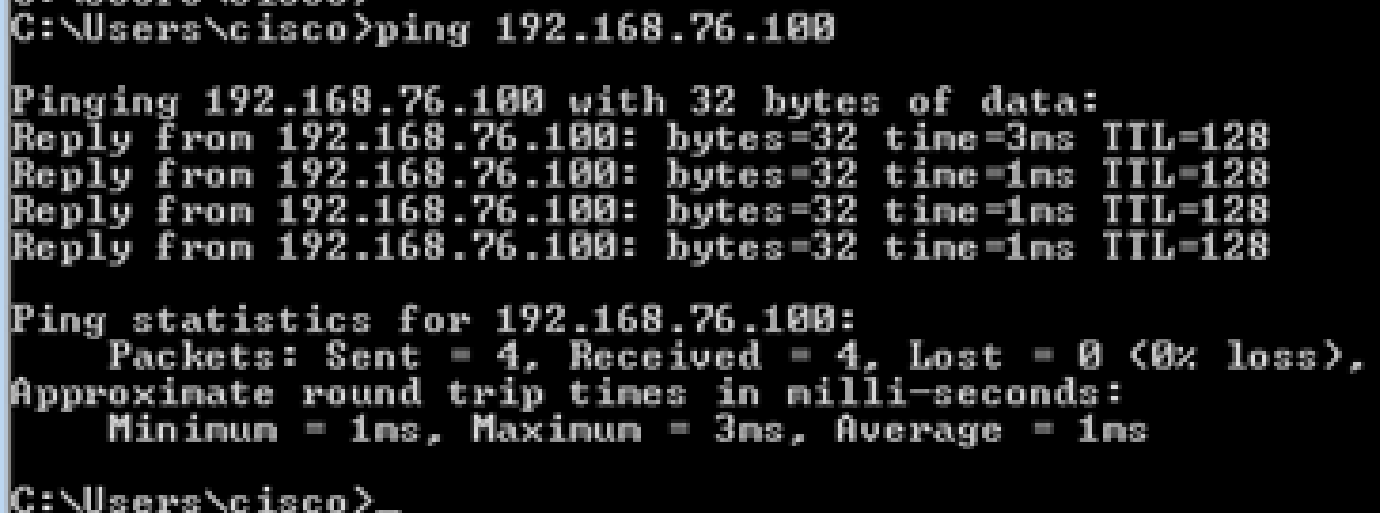
<#root>

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>
```

As contagens de ocorrências estão nas tabelas ASP:

<#root>

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
```

<#root>

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
```

A captura de pacotes mostra:

<#root>

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

Traços de um pacote (pontos importantes são destacados).

 Observação: o ID da regra NAT e sua correlação com a tabela ASP.

<#root>

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

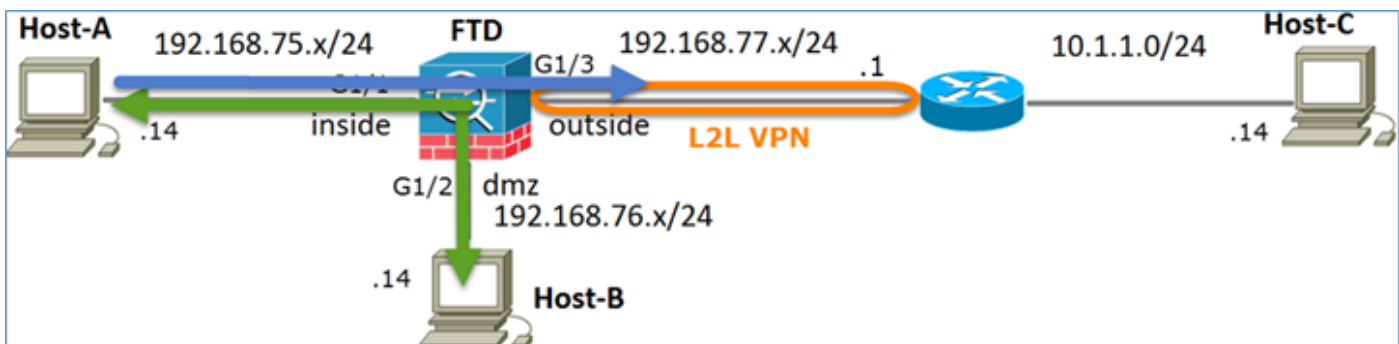
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
1 packet shown

Tarefa 2. Configurar a Conversão de Endereço de Porta (PAT - Port Address Translation) no FTD

Configure o NAT de acordo com estes requisitos:

Regra NAT	Regra de NAT manual
Tipo de NAT	Dinâmico
Inserir	Na Seção 1
Interface de origem	interno*
Interface de destino	externo*
Origem Original	192.168.75.0/24
Fonte traduzida	Interface externa (PAT)

*Usar Zonas de Segurança para a Regra NAT

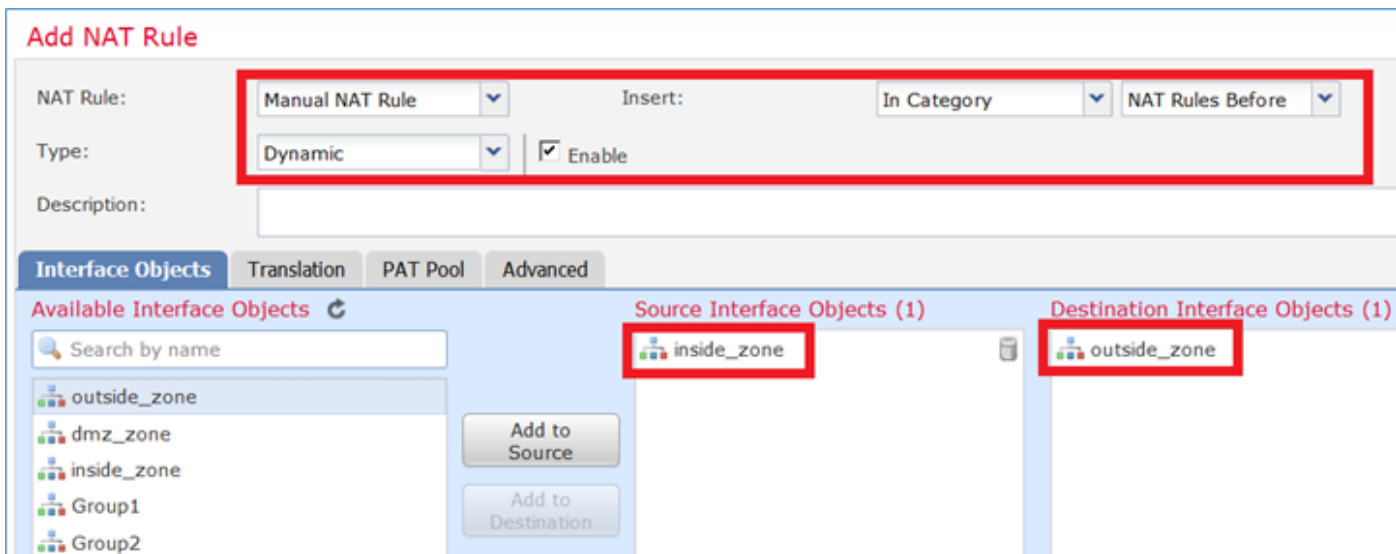


NAT Estático

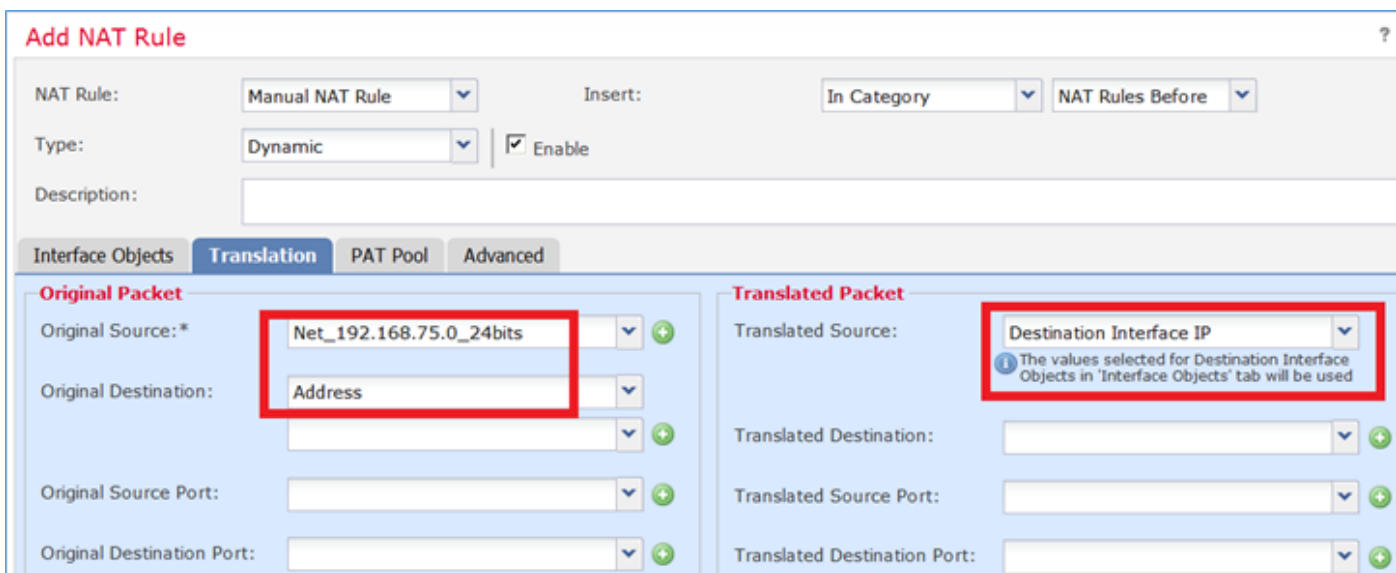
PAT

Solução:

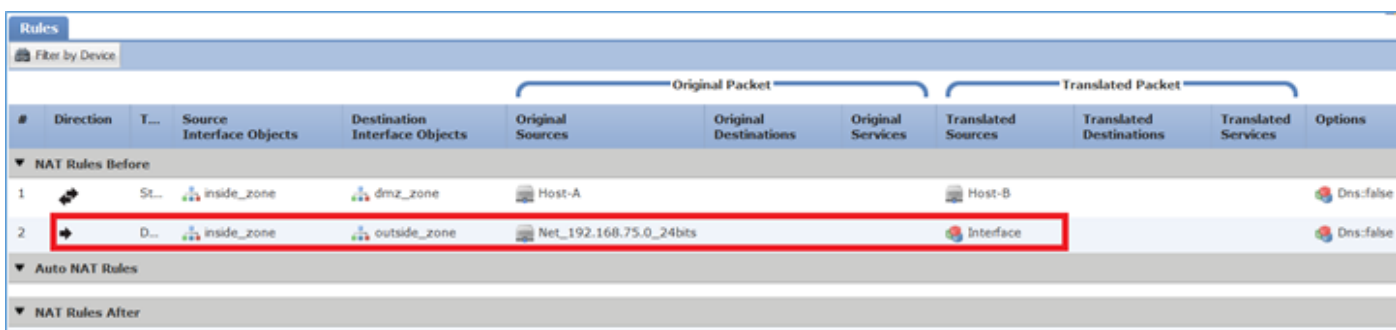
Etapa 1. Adicione uma segunda regra de NAT e configure de acordo com os requisitos da tarefa, conforme mostrado na imagem.



Etapa 2. Veja como o PAT é configurado conforme mostrado na imagem.



Etapa 3. O resultado é como mostrado na imagem.



Etapa 4. Para o restante deste laboratório, configure a Política de Controle de Acesso para permitir que todo o tráfego passe.

Verificação:

Configuração de NAT:

```
<#root>
```

```
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
```

No LINA CLI, observe a nova entrada:

```
<#root>
```

```
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
```

Ative a captura na interface interna e externa. Na captura interna, habilite o rastreamento:

```
<#root>
```

```
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
```

Faça um ping do Host-A (192.168.75.14) para o IP 192.168.77.1 como mostrado na imagem.

```
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
```

Nas capturas LINA, você pode ver a tradução PAT:

<#root>

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

<#root>

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

Rastreamentos de um pacote com seções importantes destacadas:

<#root>

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

O xlate dinâmico foi criado (observe os sinalizadores ri):

```
<#root>
```

```
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
```

Nos registros LINA você vê:

```
<#root>
```

```
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 192.168.77.6/1
```

```
May 31 2016 18:54:43: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.75.14/1 gaddr 192.168.77.6/1
```

```
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
```

Seções NAT:

```
<#root>
```

```
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
```

As tabelas ASP mostram:

```
<#root>
```

```
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
```

```
<#root>
```

```
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

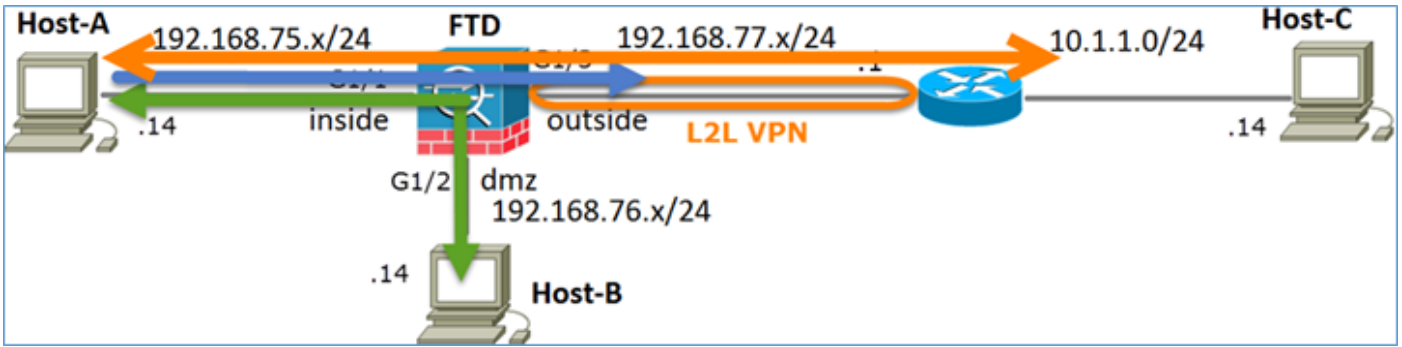
```

Tarefa 3. Configurar a isenção de NAT no FTD

Configure o NAT de acordo com estes requisitos:

Regra NAT	Regra de NAT manual
Tipo de NAT	Estático
Inserir	Na seção 1, todas as regras
Interface de origem	interno*
Interface de destino	externo*
Origem Original	192.168.75.0/24
Fonte traduzida	192.168.75.0/24
Destino original	10.1.1.0/24
Destino traduzido	10.1.1.0/24

*Usar Zonas de Segurança para a Regra NAT



NAT Estático

PAT

Isenção de NAT

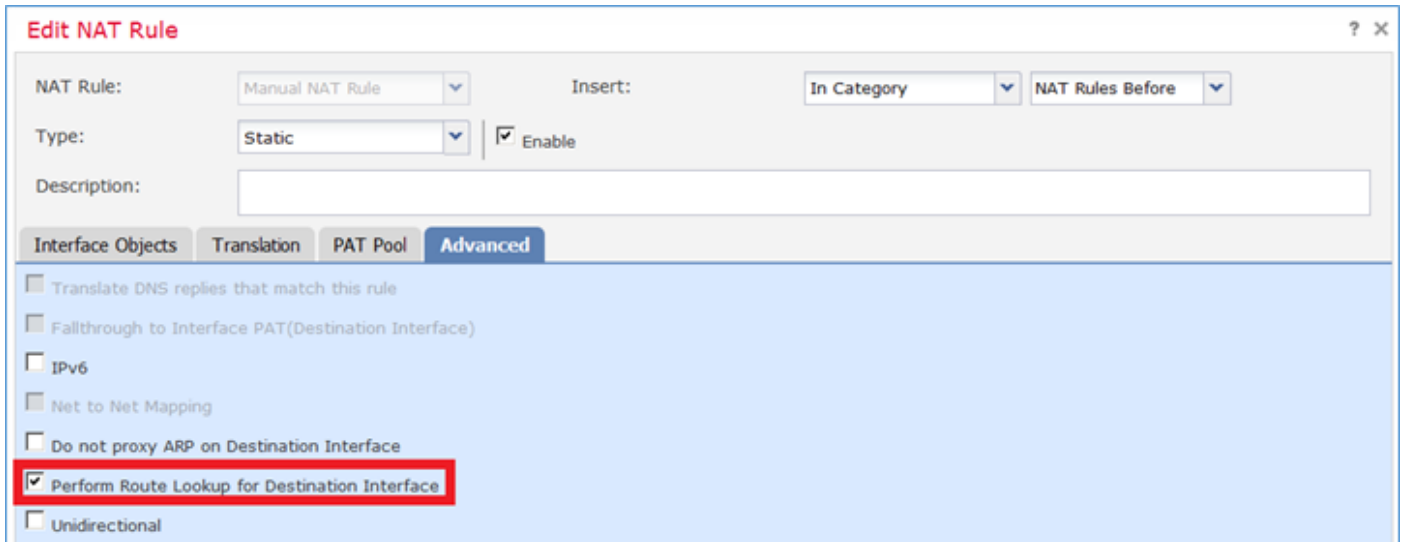
Solução:

Etapa 1. Adicione uma terceira regra de NAT e configure os requisitos por tarefa conforme mostrado na imagem.

#	Direction	Ty...	Original Packet			Translated Packet				
			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										

Etapa 2. Execute a pesquisa de rota para determinar a interface de saída.

✎ Observação: para regras de NAT de identidade, como a que você adicionou, você pode alterar como a interface de saída é determinada e usar a pesquisa de rota normal como mostrado na imagem.



Verificação:

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

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

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

```
<#root>
```

```
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 stati
  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
```

Execute o packet-tracer para o tráfego não VPN originado na rede interna. A regra PAT é usada como esperado:

```
<#root>
```

```
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

Execute o packet-tracer para o tráfego que deve passar pelo túnel VPN (execute-o duas vezes desde a primeira tentativa ativa o túnel VPN).

 Observação: você deve escolher a Regra de Isenção NAT.

Primeira tentativa do packet-tracer:

<#root>

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 ne

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 ne
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

Segunda tentativa do packet-tracer:

<#root>

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 ne
```

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 ne
```

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 n
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

Verificação de contagem de ocorrências de NAT:

<#root>

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
    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
```

Tarefa 4. Configurar NAT de objeto em FTD

Configure o NAT de acordo com estes requisitos:

Regra NAT	Regra de NAT automática
Tipo de NAT	Estático
Inserir	Na Seção 2
Interface de origem	interno*
Interface de destino	dmz*
Origem Original	192.168.75.99
Fonte traduzida	192.168.76.99
Traduzir respostas DNS que correspondam a esta regra	Habilitado

*Usar Zonas de Segurança para a Regra NAT

Solução:

Etapa 1. Configure a regra de acordo com os requisitos da tarefa conforme mostrado nas imagens.

Add NAT Rule

NAT Rule: **Auto NAT Rule** (dropdown)
Type: **Static** (dropdown) 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**

Buttons: Add to Source, Add to Destination

Add NAT Rule ? x

NAT Rule: **Auto NAT Rule** (dropdown)
Type: **Static** (dropdown) Enable

Interface Objects | **Translation** | PAT Pool | Advanced

Original Packet

Original Source:* **obj-192.168.75.99** (dropdown) +

Original Port: **TCP** (dropdown)

Translated Packet

Translated Source: **obj-192.168.76.99** (dropdown) +

Translated Port:

Add NAT Rule

NAT Rule:

Auto NAT Rule

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

Etapa 2. O resultado é como mostrado na imagem.

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										

Verificação:

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

```
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
```

<#root>

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
  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
```

Verificação com o packet-tracer:

<#root>

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

Tarefa 5. Configurar o pool PAT no FTD

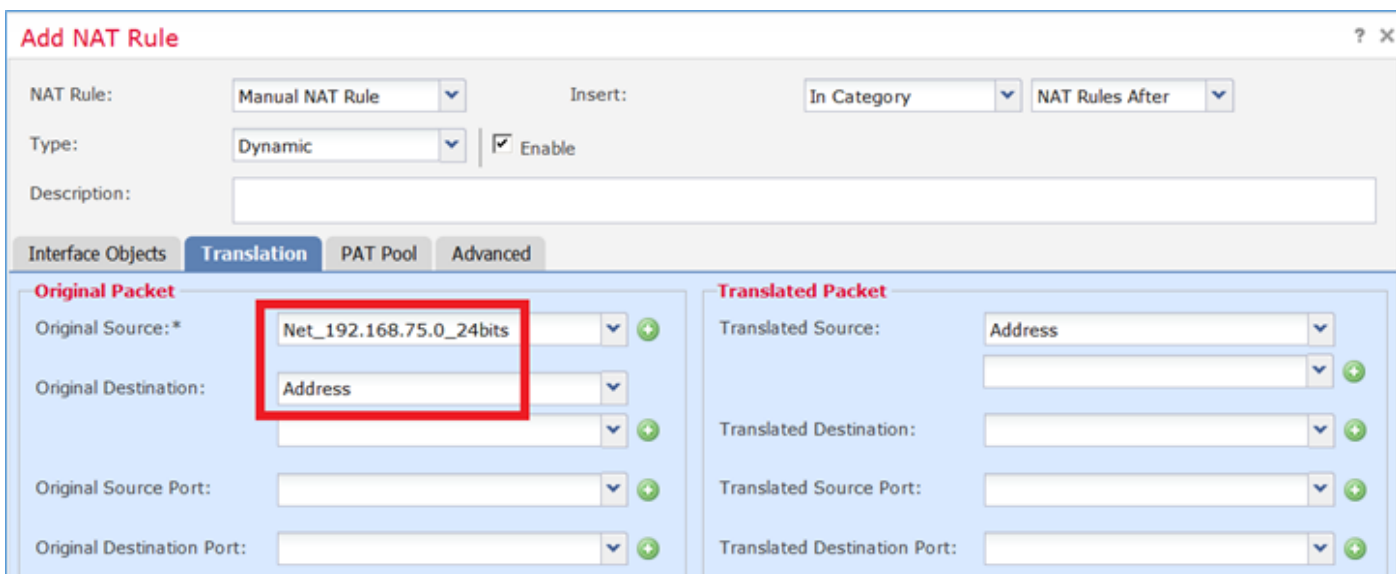
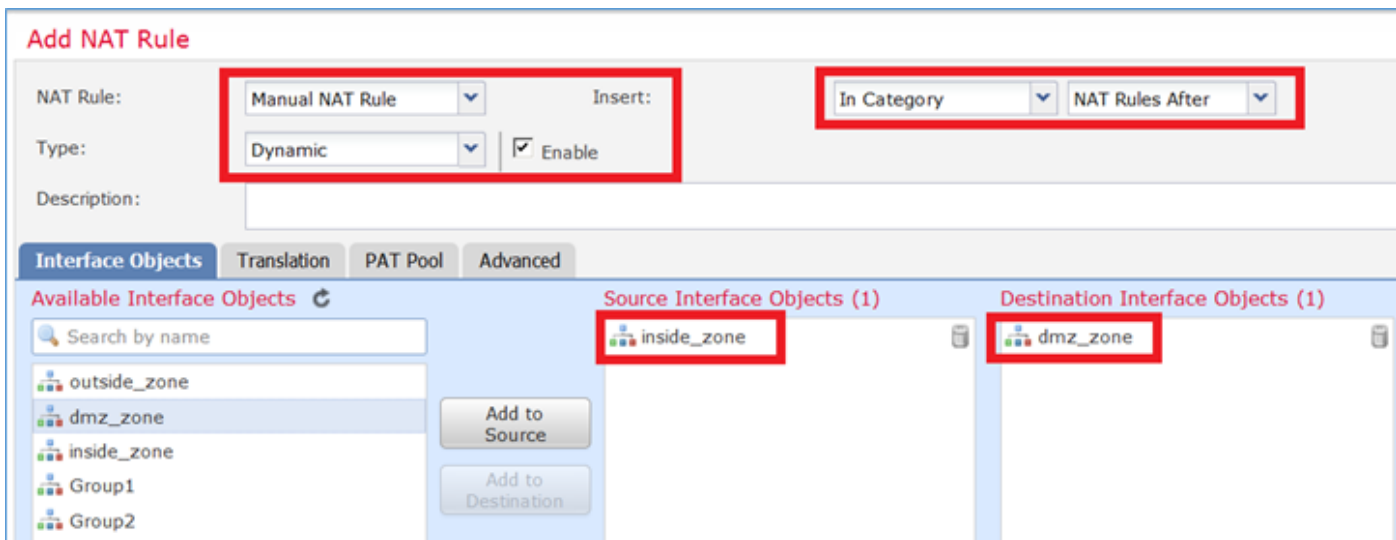
Configure o NAT de acordo com estes requisitos:

Regra NAT	Regra de NAT manual
Tipo de NAT	Dinâmico
Inserir	Na Seção 3
Interface de origem	interno*
Interface de destino	dmz*
Origem Original	192.168.75.0/24
Fonte traduzida	192.168.76.20-22
Usar todo o intervalo (1-65535)	Habilitado

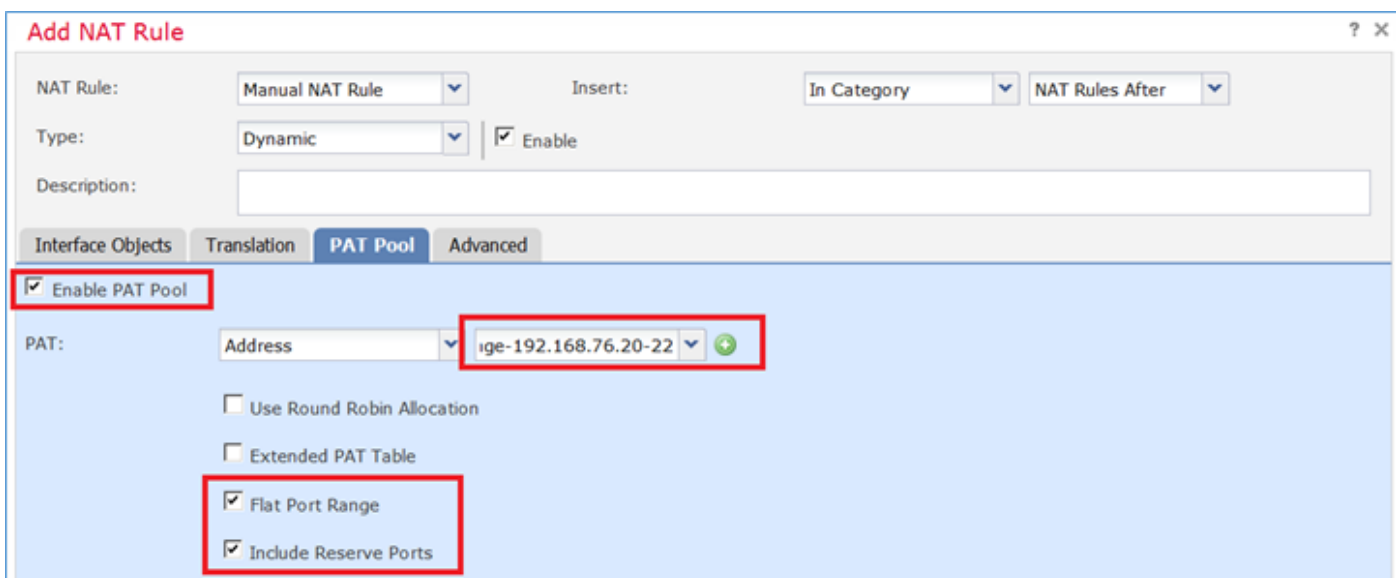
*Usar Zonas de Segurança para a Regra NAT

Solução:

Etapa 1. Configure os requisitos da regra por tarefa conforme mostrado nas imagens.



Etapa 2. Ative Flat Port Range com Incluir portas de reserva que permite o uso de todo o intervalo (1-65535) como mostrado na imagem.



Etapa 3. O resultado é como mostrado na imagem.

#	Direction	T...	Source Interface ...	Destination Interface Ob...	Original Packet		Translated Packet			Options
					Original Sources	Original Destinations	Translated Sources	Translated Destinations	Translated Services	
▼ 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

Verificação:

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

```
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
```

A regra está na Seção 3:

```
<#root>
```

```
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 stat
  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-
  translate_hits = 0, untranslate_hits = 0
```

Verificação do Packet Tracer:

<#root>

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
```

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
```

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A verificação foi explicada nas seções de tarefas individuais.

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Abra a página Advanced Troubleshooting no FMC, execute o packet-tracer e execute o comando show nat pool.



Observação: a entrada que usa todo o intervalo como mostrado na imagem.

Overview Analysis Policies Devices Objects AMP Deploy System

Configuration Users Domains Integration Updates Licenses Health Monitor

Advanced Troubleshooting

FTD5506-1

File Download ASA CLI

Command show Parameter nat pool 1

Output

```
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
```

2 Execute Back

Informações Relacionadas

- Todas as versões do guia de configuração do Cisco Firepower Management Center podem ser encontradas aqui:

[Navegação na documentação do Cisco Secure Firewall Threat Defense](#)

- O Cisco Global Technical Assistance Center (TAC) recomenda enfaticamente este guia visual para conhecimento prático aprofundado sobre as tecnologias de segurança de próxima geração Cisco Firepower, que inclui as mencionadas neste artigo:

[Cisco Press - Defesa contra ameaças do Firepower](#)

- Para todas as Notas técnicas de configuração e solução de problemas referentes às tecnologias do Firepower:

[Cisco Secure Firewall Management Center](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.