

# FTDでのNATの設定と確認

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[タスク 1.FTDでのスタティックNATの設定](#)

[タスク 2.FTDでのポートアドレス変換\(PAT\)の設定](#)

[タスク 3.FTDでのNAT免除の設定](#)

[タスク 4.FTDでのオブジェクトNATの設定](#)

[タスク 5.FTDでのPATプールの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Firepower Threat Defense(FTD)の基本的なネットワークアドレス変換(NAT)を設定および確認する方法について説明します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTDコード6.1.0-226が稼働するASA5506X
- 6.1.0-226が稼働するFireSIGHT Management Center(FMC)
- 3台のWindows 7ホスト
- LAN-to-LAN(L2L)VPNを実行するCisco IOS® 3925ルータ

ラボ試験時間：1時間

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

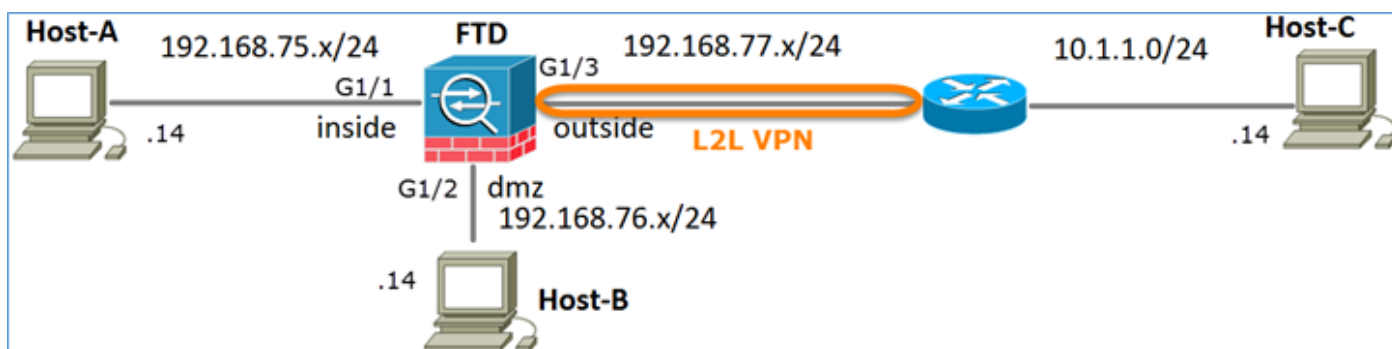
FTDは、従来の適応型セキュリティアプライアンス(ASA)と同じNAT設定オプションをサポートします。

- 以前のNATルール：これは、従来のASAのTwice NAT（セクション1）と同じです。
- 自動NATルール：従来のASAのセクション2
- 変更後のNATルール：これは、従来のASAのTwice NAT（セクション3）と同じです。

NAT設定の場合は、FTDの設定はFMCから行われるため、FMCのGUIとさまざまな設定オプションについて精通している必要があります。

## 設定

### ネットワーク図



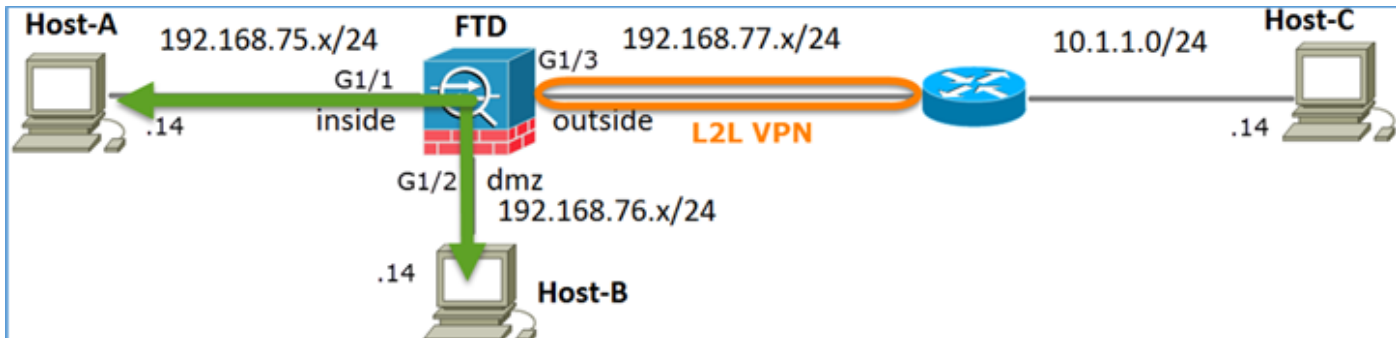
### タスク 1.FTDでのスタティックNATの設定

次の要件に従ってNATを設定します。

NATポリシー名	FTDデバイス名
NATルール	手動NATルール
NATタイプ	Static
挿入	セクション1
送信元インターフェイス	内部*

宛先インターフェイス	dmz*
オリジナルソース	192.168.75.14
変換済みソース	192.168.76.100

\*NATルールにセキュリティゾーンを使用する



スタティック NAT

ソリューション :

従来のASAでは、NATルールでnameifを使用する必要があります。FTDでは、セキュリティゾーンまたはインターフェイスグループを使用する必要があります。

ステップ 1: インターフェイスをセキュリティゾーン/インターフェイスグループに割り当てます。

この作業では、NATに使用されるFTDインターフェイスをセキュリティゾーンに割り当てることにします。または、図に示すように、インターフェイスグループに割り当てることができます。

## Edit Physical Interface

Mode:

Name:   Enabled  Management Only

Security Zone:

Description:

**General** IPv4 IPv6 Advanced Hardware Configuration

MTU:  (64 - 9198)

Interface ID:

ステップ 2 : 結果は図のようになります。

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)

ステップ 3 : 図に示すように、Objects > Object Managementページでインターフェイスグループとセキュリティゾーンを作成/編集できます。

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

Object Management Intrusion Rules

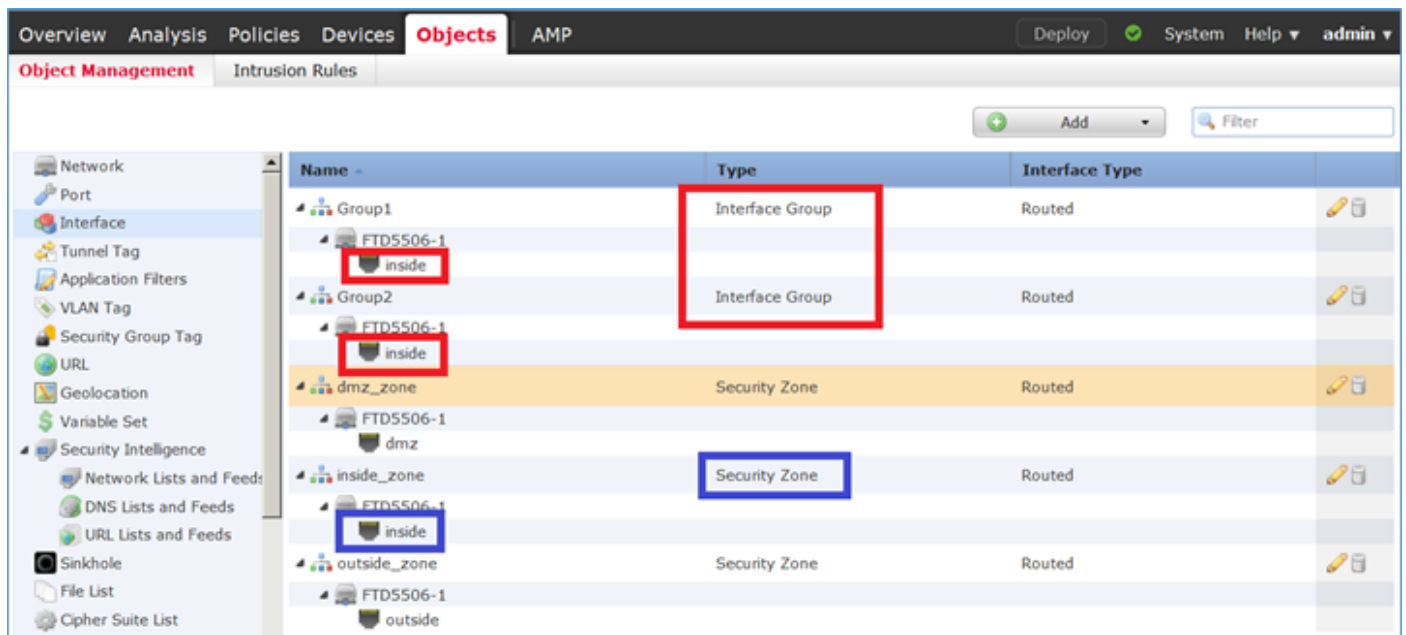
Name	Type	Interface Type
dmz_zone	Security	
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

### セキュリティゾーンとインターフェイスグループ

セキュリティゾーンとインターフェイスグループの主な違いは、インターフェイスは1つのセキュリティゾーンにのみ属することができるが、複数のインターフェイスグループに属することができるということです。実際には、インターフェイスグループの方が柔軟性が高くなります。

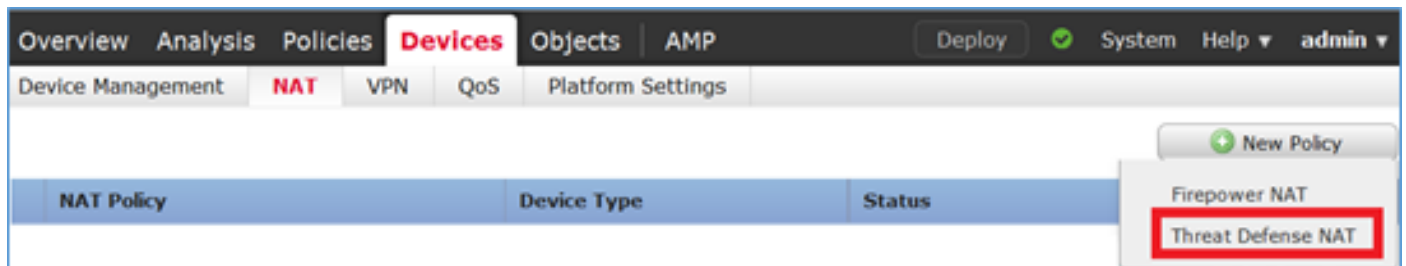
図に示すように、Insideのインターフェイスは2つの異なるインターフェイスグループに属してい

ますが、セキュリティゾーンは1つしかありません。

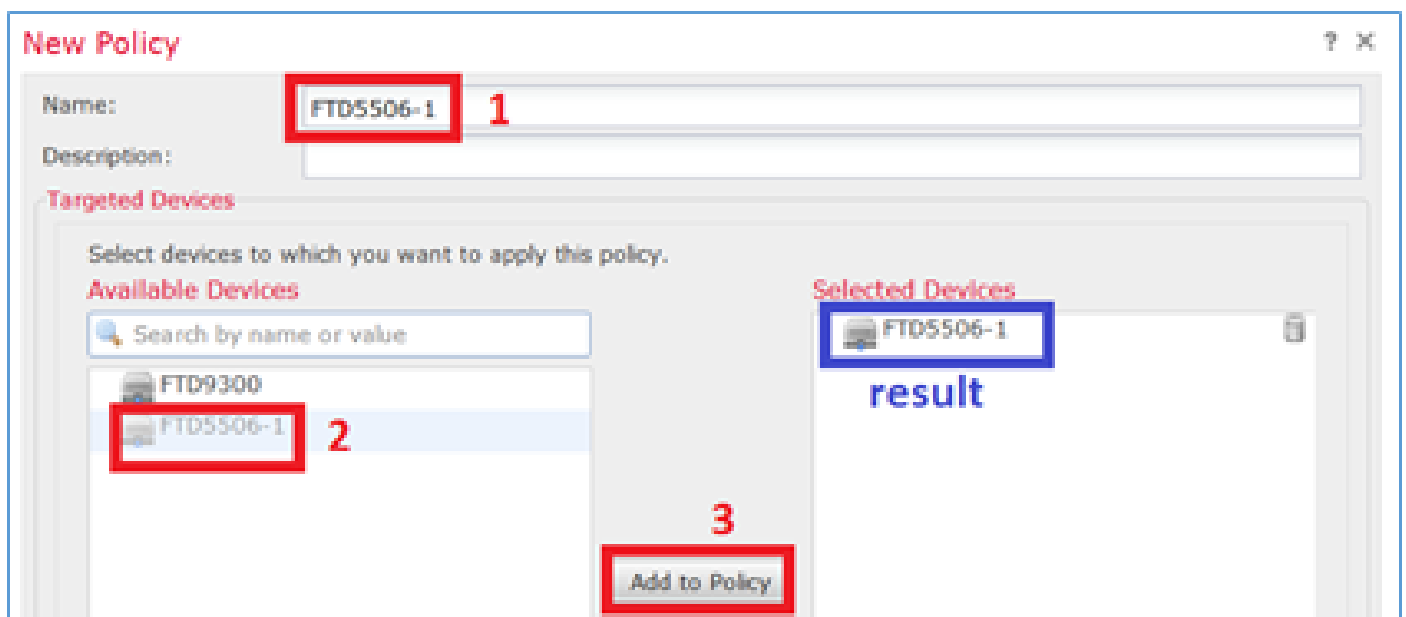


ステップ 4 : FTDでスタティックNATを設定します。

Devices > NATの順に移動し、NATポリシーを作成します。図に示すように、New Policy > Threat Defense NATの順に選択します。



ステップ 5 : 図に示すように、ポリシー名を指定してターゲットデバイスに割り当てます。



手順 6 : NATルールをポリシーに追加し、Add Ruleをクリックします。

図に示すように、タスク要件に従ってこれらを指定します。

**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 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:

ホストA = 192.168.75.14

ホストB = 192.168.76.100

<#root>

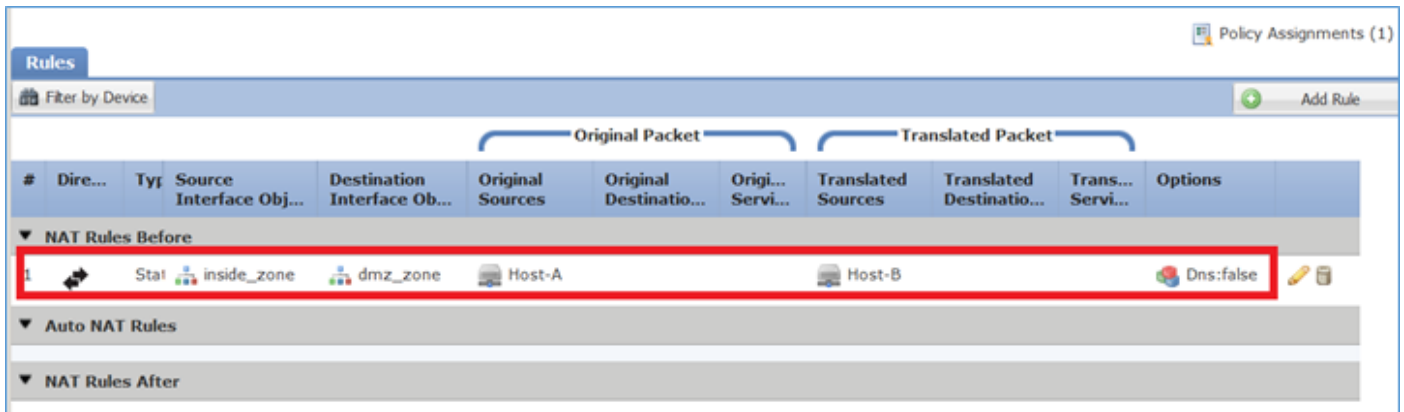
firepower#

show run object

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

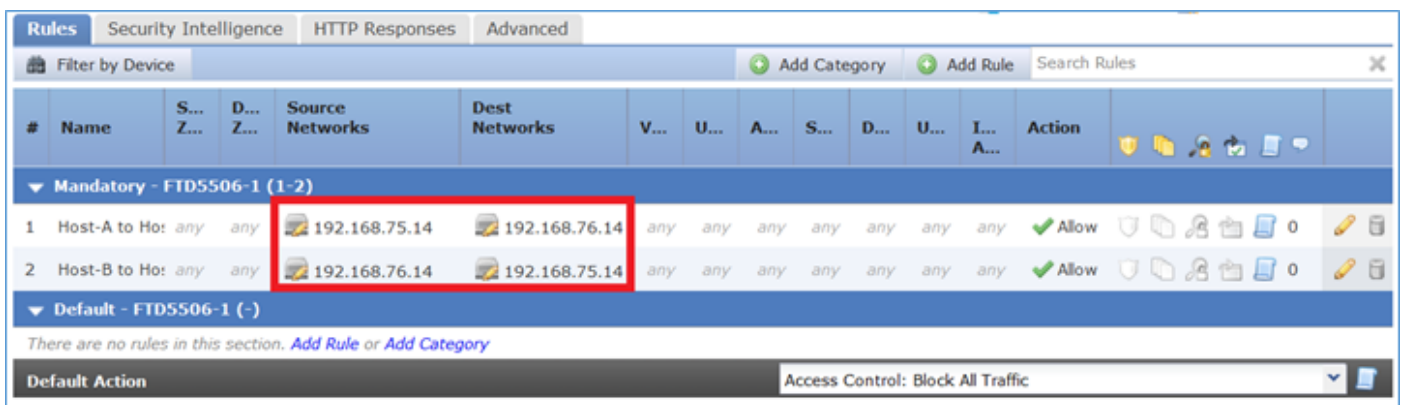
**警告**：スタティックNATを設定して、インターフェイスを変換済み送信元として指定した場合は、そのインターフェイスのIPアドレスを宛先とするすべてのトラフィックがリダイレクトされます。ユーザは、マッピングされたインターフェイスで有効になっているサービスにアクセスできません。このようなサービスの例としては、OSPFやEIGRPなどのルーティングプロトコルがあります。

手順 7：結果は図のようになります。



#	Dir...	Ty	Source Interface Obj...	Destination Interface Ob...	Original Sources	Original Destinati...	Original Servi...	Translated Sources	Translated Destinati...	Trans... Servi...	Options
1		Stat	inside_zone	dmz_zone	Host-A			Host-B			Dns:false

ステップ 8：Host-BからHost-Aへのアクセス、およびその逆のアクセスを許可するアクセスコントロールポリシー(ACL)があることを確認します。デフォルトではスタティックNATは双方向であることを注意してください。従来のASAと同様に、実際のIPの使用を参照してください。この実習では、図に示すようにLINAで9.6.1.xコードが実行されているため、これは正常な状態です。



#	Name	S... Z...	D... Z...	Source Networks	Dest Networks	V...	U...	A...	S...	D...	U...	L... 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

検証：

Lina CLIから：

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

NATルールは、期待どおりにセクション1に挿入されました。

```
<#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
```

---

 注：バックグラウンドで作成される2つのxlate。

---

```
<#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
```

ASP NATテーブル：

```
<#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

図に示すように、FTDのトレースの詳細を使用してキャプチャを有効にし、ホストBからホストAにpingします。

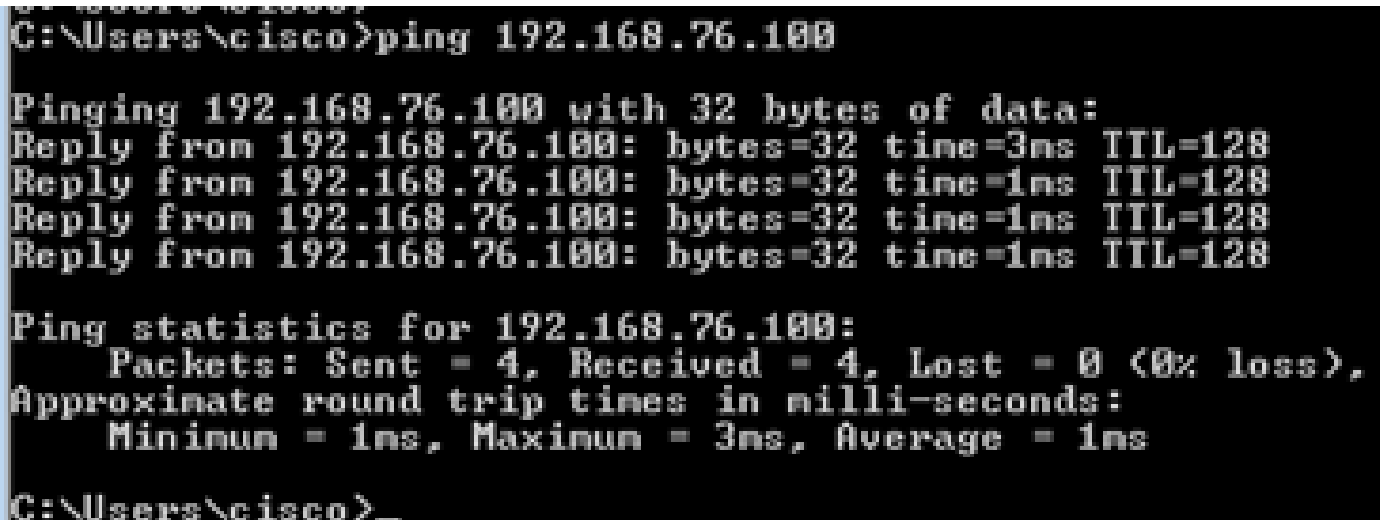
<#root>

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>
```

ヒットカウントはASPテーブルに示されています。

<#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
```

パケットキャプチャには次のように表示されます。

<#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

パケットのトレース ( 重要なポイントが強調表示されています ) 。

---

 注:NATルールのIDとASPテーブルとの関連付けです。

---

<#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

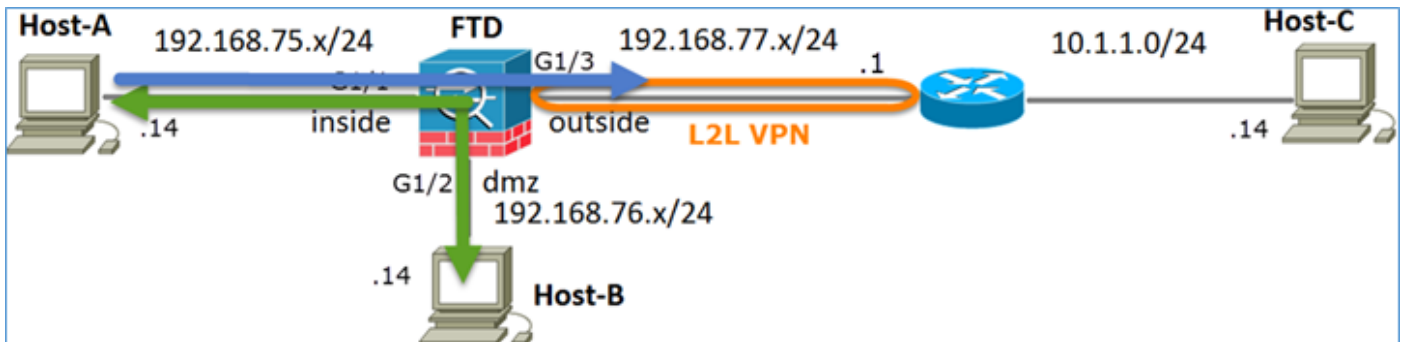


## タスク 2.FTDでのポートアドレス変換(PAT)の設定

次の要件に従ってNATを設定します。

NATルール	手動NATルール
NATタイプ	ダイナミック
挿入	セクション1
送信元インターフェイス	内部*
宛先インターフェイス	外部*
オリジナルソース	192.168.75.0/24
変換済みソース	外部インターフェイス(PAT)

\*NATルールにセキュリティゾーンを使用する



スタティック NAT

パット

ソリューション :

ステップ 1 : 2番目のNATルールを追加し、図に示すようにタスク要件に従って設定します。

### Add NAT Rule

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

Type: Dynamic  Enable

Description:

**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): outside\_zone

ステップ 2：次の図に示すように、PATの設定方法を示します。

### Add NAT Rule

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

Type: Dynamic  Enable

Description:

**Interface Objects** Translation PAT Pool Advanced

**Original Packet**

Original Source: \* Net\_192.168.75.0\_24bits

Original Destination: Address

Original Source Port:

Original Destination Port:

**Translated Packet**

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Destination:

Translated Source Port:

Translated Destination Port:

ステップ 3：結果は図のように表示されます。

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

ステップ 4：この実習の残りの部分では、すべてのトラフィックが通過できるようにアクセスコントロールポリシーを設定します。

検証：

NAT の設定

```
<#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
```

LINA CLIから、新しいエントリに注目します。

```
<#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
```

内部および外部インターフェイスでキャプチャを有効にします。内部キャプチャでトレースを有効にします。

```
<#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
```

図に示すように、ホストA(192.168.75.14)からIP 192.168.77.1にpingします。

```
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
```

LINAキャプチャで、PAT変換を確認できます。

```
<#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
```

重要なセクションが強調表示されたパケットのトレース：

<#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
```

dynamic xlateが作成されました ( riフラグに注意してください )。

```
<#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
```

LINAログには、次のように表示されます。

```
<#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
```

NATセクション :

```
<#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
```

## ASPテーブルの表示 :

```
<#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

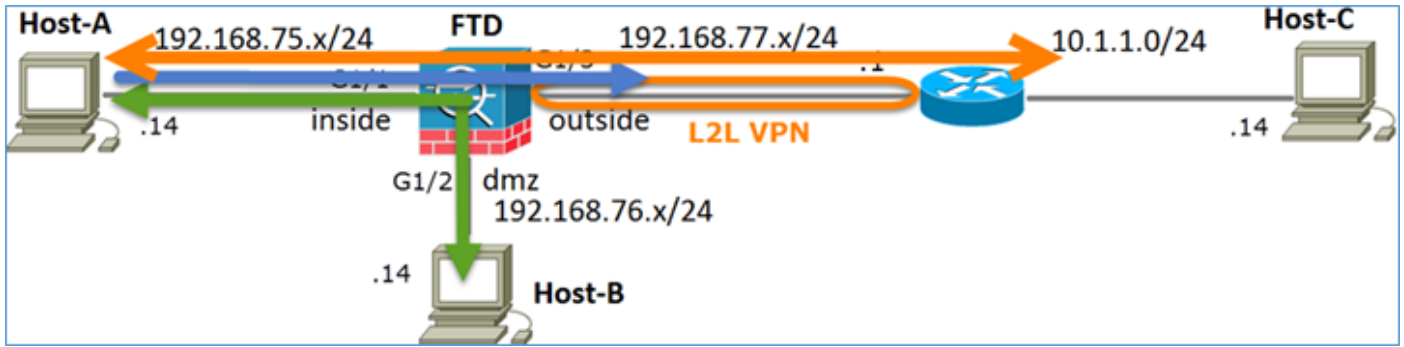
```

### タスク 3.FTDでのNAT免除の設定

次の要件に従ってNATを設定します。

NATルール	手動NATルール
NATタイプ	Static
挿入	セクション1のすべての既存のルール
送信元インターフェイス	内部*
宛先インターフェイス	外部*
オリジナルソース	192.168.75.0/24
変換済みソース	192.168.75.0/24
元の宛先	10.1.1.0/24
変換後の宛先	10.1.1.0/24

\*NATルールにセキュリティゾーンを使用する



スタティック NAT

パット


NATの除外

ソリューション :

ステップ 1 : 3番目のNATルールを追加し、図に示すようにタスクごとに要件を設定します。

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	↔		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	↔		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										

ステップ 2 : ルートルックアップを実行して出カインターフェイスを決定します。

 注 : 追加したルールと同様に、アイデンティティNATルールでは、出カインターフェイスの決定方法を変更し、図に示すように通常のルートルックアップを使用できます。

**Edit NAT Rule** ? X

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

Type: Static  Enable

Description:

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

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

**Perform Route Lookup for Destination Interface**

Unidirectional

検証：

<#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
```

内部ネットワークから発信された非VPNトラフィックに対してパケットトレーサを実行します。  
PATルールは想定どおりに使用されます。

<#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

VPNトンネルを通過する必要があるトラフィックに対してパケットトレーサを実行します (最初の試行でVPNトンネルを起動してから2回実行します)。

---

 注:NAT免除ルールを選択する必要があります。

---

最初のパケットトレーサの試行 :

<#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

2回目のパケットトレーサの試行 :

<#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
```

## NATヒットカウンターの検証：

```
<#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
```

## タスク 4.FTDでのオブジェクトNATの設定

次の要件に従ってNATを設定します。

NATルール	自動NATルール
NATタイプ	Static
挿入	セクション2
送信元インターフェイス	内部*
宛先インターフェイス	dmz*
オリジナルソース	192.168.75.99
変換済みソース	192.168.76.99
この規則に一致するDNS応答を変換する	Enabled

\*NATルールにセキュリティゾーンを使用する

ソリューション：

ステップ 1：図に示すように、タスク要件に従ってルールを設定します。

**Add NAT Rule**

NAT Rule: Auto NAT Rule

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:

Type:   Enable

Interface Objects **Translation** PAT Pool Advanced

**Original Packet**

Original Source:\*

Original Port:

**Translated Packet**

Translated Source:

Translated Port:

### Add NAT Rule

NAT Rule:

Type:   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

ステップ 2：結果は図のように表示されます。

Rules

Filter by Device

#	Direction	Type	Original Packet			Translated Packet				
			Source Interface	Destination Interface	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										

検証：

<#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 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 = 0, untranslate_hits = 0
```

パケットトレーサを使用した検証：

<#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

## タスク 5.FTDでのPATプールの設定

次の要件に従ってNATを設定します。

NATルール	手動NATルール
NATタイプ	ダイナミック
挿入	セクション3
送信元インターフェイス	内部*
宛先インターフェイス	dmz*
オリジナルソース	192.168.75.0/24
変換済みソース	192.168.76.20-22

範囲全体を使用する(1 ~ 65535)

Enabled

\*NATルールにセキュリティゾーンを使用する

ソリューション :

ステップ 1 : 図に示すように、タスクごとのルール要件を設定します。

**Add NAT Rule**

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

Type: Dynamic     Enable

Description:

**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 NAT Rule**    ? X

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

Type: Dynamic     Enable

Description:

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

**Original Packet**

Original Source:\* Net\_192.168.75.0\_24bits

Original Destination: Address

Original Source Port:

Original Destination Port:

**Translated Packet**

Translated Source: Address

Translated Destination:

Translated Source Port:

Translated Destination Port:

ステップ 2 : 図に示すように、Include Reserver Portsコマンドでフラットポート範囲を有効にして、範囲全体(1 ~ 65535)を使用できるようにします。



**Add NAT Rule** ? X

NAT Rule:  Insert:

Type:   Enable

Description:

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT:

Use Round Robin Allocation

Extended PAT Table

Flat Port Range

Include Reserve Ports

ステップ 3 : 結果は図のように表示されます。

Rules Filter by Device Add Rule

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

検証 :

<#root>

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
```

この規則は、セクション3にあります。

<#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 = 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
```

パケットトレーサによる検証：

```
<#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

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

検証については、個々のタスクセクションで説明しています。

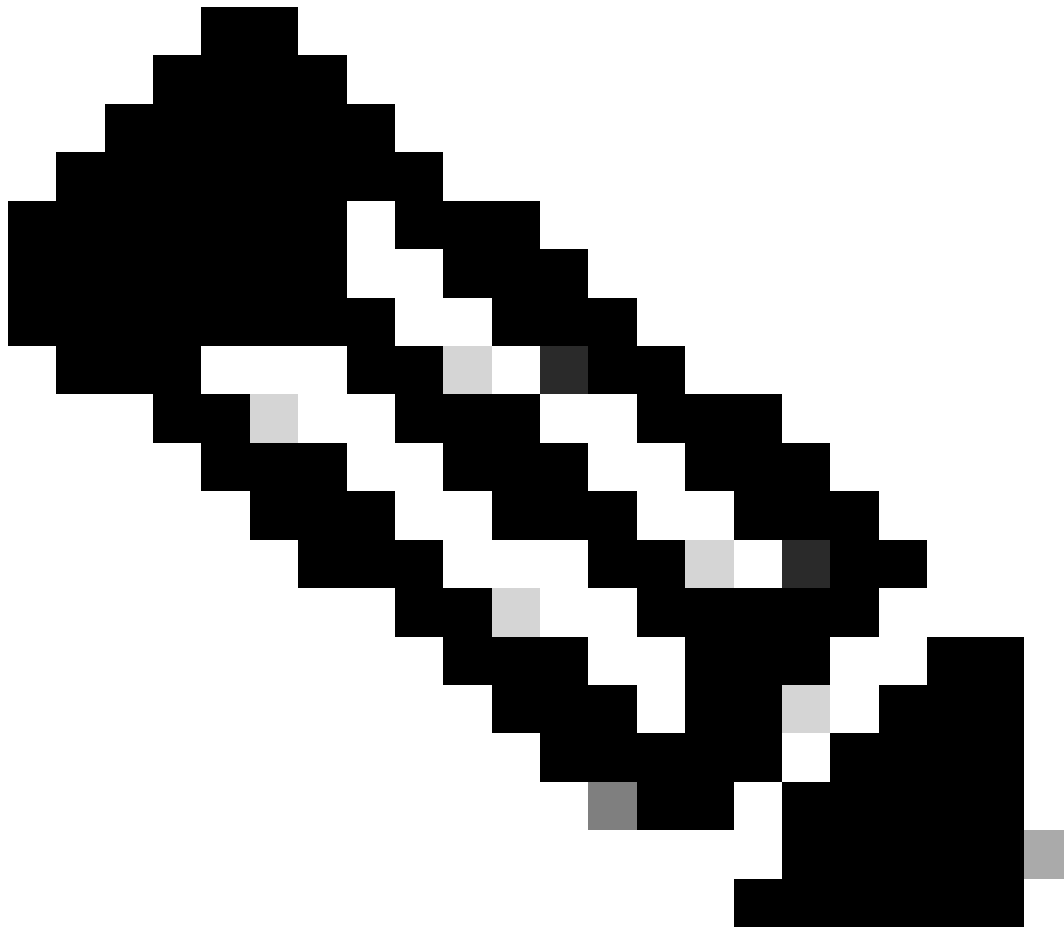
## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

FMCで高度なトラブルシューティングページを開き、パケットトレーサを実行してからshow nat

poolコマンドを実行します。

---



注：図に示すように、範囲全体を使用するエントリ。

---

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

## 関連情報

- Cisco Firepower Management Center(FMC)コンフィギュレーションガイドのすべてのバージョンは、次の場所にあります。

### [Cisco Secure Firewall Threat Defenseに関するドキュメントの参照](#)

- Cisco Global Technical Assistance Center(TAC)は、このビジュアルガイドを使用して、Cisco Firepower次世代セキュリティテクノロジーに関する詳細で実用的な知識を得ることを強く推奨します。このガイドには、次の記事に記載されているものを含まれます。

### [Cisco Press:Firepower Threat Defense \(火力の脅威に対する防御\)](#)

- Firepowerテクノロジーに関連するすべての設定とトラブルシューティングのテクニカルノートについては、次を参照してください。

### [Cisco Secureファイアウォール管理センター](#)

- [テクニカルサポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。