

Konfigurieren und Überprüfen von NAT auf FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Aufgabe 1: Konfigurieren von statischer NAT auf FTD](#)

[Schritt 2: Port-Adressumwandlung \(PAT\) auf FTD konfigurieren](#)

[Schritt 3: NAT-Freistellung für FTD konfigurieren](#)

[Aufgabe 4: Konfigurieren von Objekt-NAT auf FTD](#)

[Schritt 5: PAT-Pool auf FTD konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die grundlegende Network Address Translation (NAT) für Firepower Threat Defense (FTD) konfigurieren und überprüfen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA5506X mit FTD-Code 6.1.0-226
- FireSIGHT Management Center (FMC) mit 6.1.0-226
- 3 Windows 7-Hosts
- Cisco IOS® 3925-Router mit LAN-to-LAN (L2L)-VPN

Zeit bis zum Abschluss des Labors: 1 Stunde

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

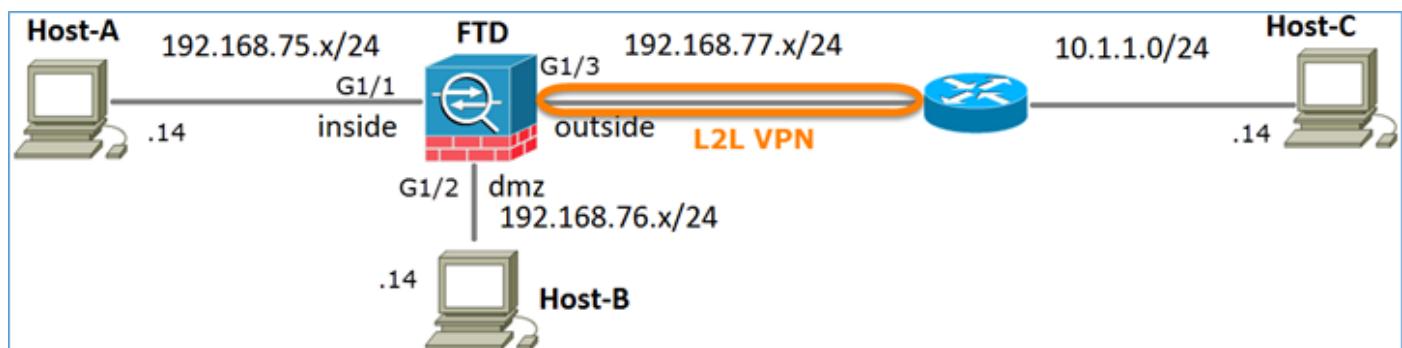
FTD unterstützt dieselben NAT-Konfigurationsoptionen wie die klassische Adaptive Security Appliance (ASA):

- NAT Rules Before - Dies entspricht Twice NAT (Abschnitt 1) auf klassischer ASA
- Auto NAT-Regeln - Abschnitt 2 zur klassischen ASA
- NAT Rules After (NAT-Regeln nachher) - Dies entspricht Twice NAT (Abschnitt 3) auf klassischer ASA.

Da die FTD-Konfiguration bei der NAT-Konfiguration vom FMC aus erfolgt, müssen Sie mit der FMC-GUI und den verschiedenen Konfigurationsoptionen vertraut sein.

Konfigurieren

Netzwerkdiagramm

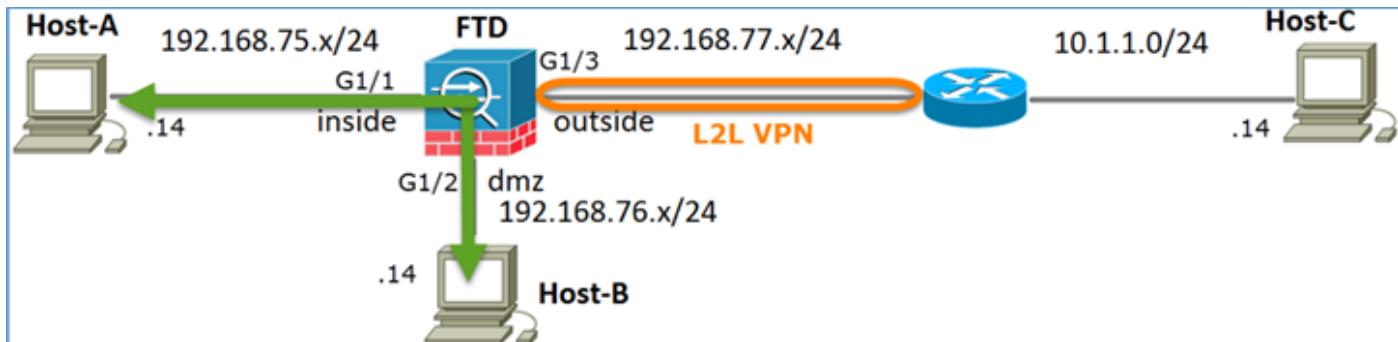


Aufgabe 1: Konfigurieren von statischer NAT auf FTD

Konfigurieren Sie NAT wie folgt:

NAT-Richtlinienname	Name des FTD-Geräts
NAT-Regel	Manuelle NAT-Regel
NAT-Typ	Statisch
Einfügen	In Abschnitt 1
Quellschnittstelle	Innen*
Zielschnittstelle	DMZ*
Ursprüngliche Quelle	192.168.75.14
Übersetzte Quelle	192.168.76.100

* Sicherheitszonen für NAT-Regel verwenden



Statisches NAT

Lösung:

Bei der klassischen ASA müssen Sie nameif in den NAT-Regeln verwenden. Auf FTD müssen Sie entweder Sicherheitszonen oder Schnittstellengruppen verwenden.

Schritt 1: Zuweisen von Schnittstellen zu Sicherheitszonen/Schnittstellengruppen

Bei dieser Aufgabe wird entschieden, die für NAT verwendeten FTD-Schnittstellen Sicherheitszonen zuzuweisen. Alternativ können Sie sie Schnittstellengruppen zuweisen, wie im Bild dargestellt.

Edit Physical Interface

Mode:	None
Name:	inside <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Management Only
Security Zone:	inside_zone <input type="text"/>
Description:	<input type="text"/>
<input type="button" value="General"/> <input type="button" value="IPv4"/> <input type="button" value="IPv6"/> <input type="button" value="Advanced"/> <input type="button" value="Hardware Configuration"/>	
MTU:	1500 (64 - 9198)
Interface ID:	GigabitEthernet1/1

Schritt 2. Das Ergebnis ist wie im Bild dargestellt.

Devices	Routing	Interfaces	Inline Sets	DHCP	Add Interfaces
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)

Schritt 3: Sie können Schnittstellengruppen und Sicherheitszonen auf der Seite Objekte >

Objektverwaltung erstellen/bearbeiten, wie im Bild gezeigt.

The screenshot shows the 'Objects' tab selected in the top navigation bar. On the left, a sidebar lists categories: Network, Port, Interface (which is selected), Tunnel Tag, Application Filters, and VLAN Tag. The main area displays a table with columns 'Name', 'Type', and 'Interface Type'. Three rows are listed: 'dmz_zone' (Security Zone, Routed), 'inside_zone' (Security Zone, Routed), and 'outside_zone' (Security Zone, Routed). A red box highlights the 'Add' button in the top right corner of the table header, along with options for 'Security Zone' and 'Interface Group'.

Sicherheitszonen und Schnittstellengruppen

Der Hauptunterschied zwischen Sicherheitszonen und Schnittstellengruppen besteht darin, dass eine Schnittstelle nur einer Sicherheitszone angehören kann, jedoch mehreren Schnittstellengruppen angehören kann. Praktisch gesehen bieten die Schnittstellengruppen also mehr Flexibilität.

Sie können sehen, dass die **interne** Schnittstelle zu zwei verschiedenen Schnittstellengruppen gehört, aber nur zu einer Sicherheitszone, wie im Bild gezeigt.

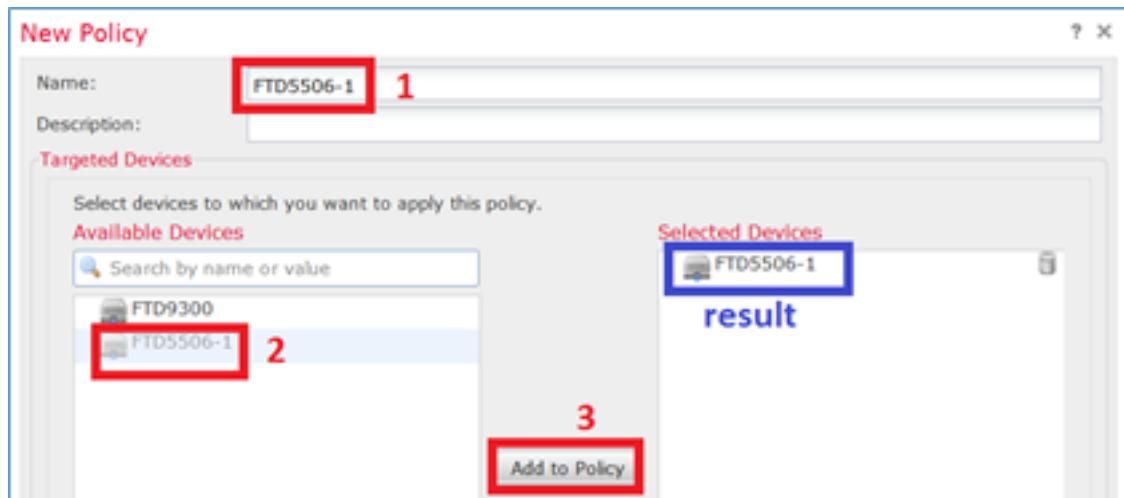
The screenshot shows the 'Objects' tab selected. The sidebar includes Network, Port, Interface (selected), Tunnel Tag, Application Filters, VLAN Tag, Security Group Tag, URL, Geolocation, Variable Set, Security Intelligence, Sinkhole, File List, and Cipher Suite List. The main area shows a tree view of interface groups and zones. Under 'Group1', there are two 'inside' interfaces. Under 'Group2', there are two 'inside' interfaces. Under 'dmz_zone', there is one 'dmz' interface. Under 'inside_zone', there is one 'inside' interface. Under 'outside_zone', there is one 'outside' interface. A red box highlights the 'inside' interface under 'Group1', another red box highlights the 'inside' interface under 'Group2', and a blue box highlights the 'inside' interface under 'inside_zone'.

Schritt 4: Konfigurieren der statischen NAT für FTD

Navigieren Sie zu **Devices > NAT**, und erstellen Sie eine NAT-Richtlinie. Wählen Sie **New Policy > Threat Defense NAT**, wie im Bild dargestellt.

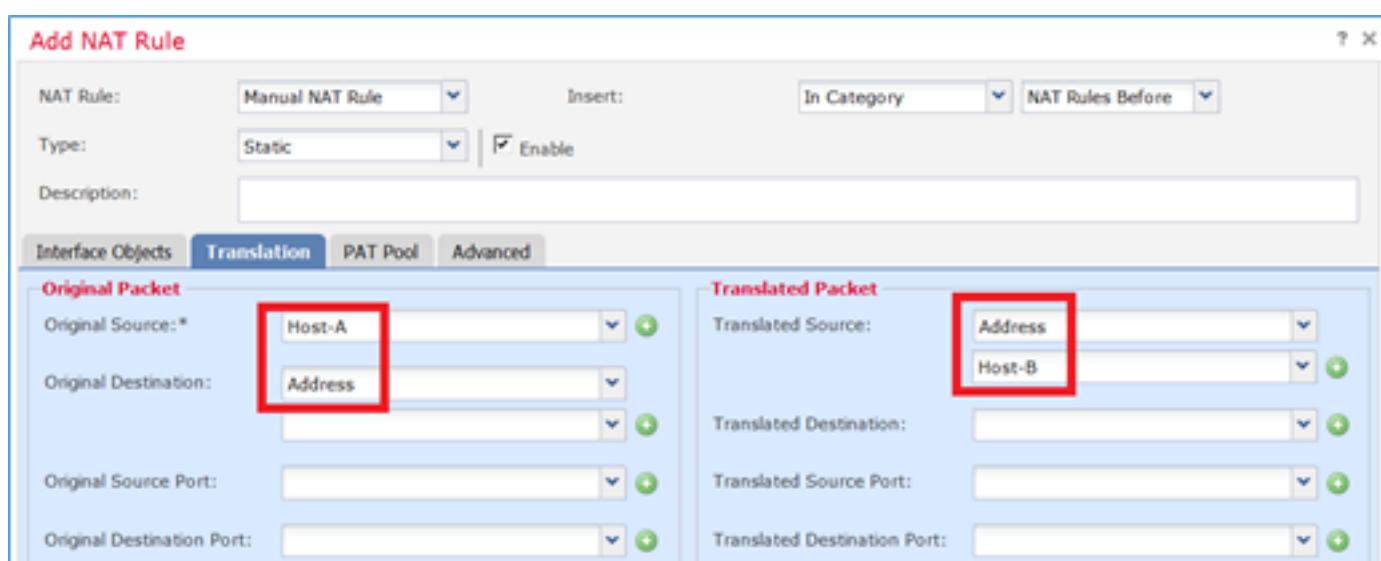
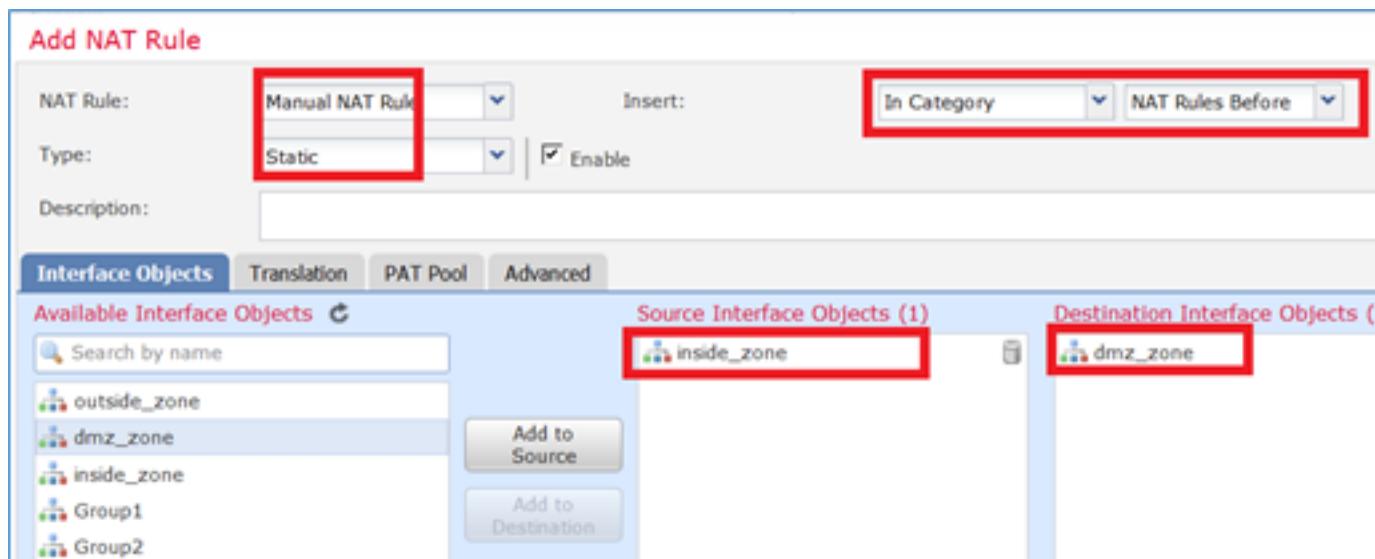
The screenshot shows the 'Devices' tab selected. The sidebar has tabs for Overview, Analysis, Policies, Devices (selected), Objects, and AMP. Below the sidebar are buttons for Device Management, NAT (which is selected), VPN, QoS, and Platform Settings. A large 'New Policy' button is visible in the top right. In the main area, a table has columns 'NAT Policy', 'Device Type', and 'Status'. A red box highlights the 'Threat Defense NAT' option in the status column of the first row.

Schritt 5: Geben Sie den Richtliniennamen an, und weisen Sie ihn, wie im Bild dargestellt, einem Zielgerät zu.



Schritt 6: Fügen Sie der Richtlinie eine NAT-Regel hinzu, und klicken Sie auf **Regel hinzufügen**.

Geben Sie diese nach Aufgabenanforderungen an, wie in den Bildern dargestellt.



Host-A = 192.168.75.14

Host-B = 192.168.76.100

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

Warnung: Wenn Sie Static NAT konfigurieren und eine Schnittstelle als übersetzte Quelle angeben, wird der gesamte an die IP-Adresse der Schnittstelle gerichtete Datenverkehr umgeleitet. Benutzer können möglicherweise nicht auf einen Dienst zugreifen, der auf der zugeordneten Schnittstelle aktiviert ist. Beispiele für solche Dienste sind Routing-Protokolle wie OSPF und EIGRP.

Schritt 7. Das Ergebnis ist wie im Bild dargestellt.

The screenshot shows the 'Rules' tab in the Firepower Management Center. A static NAT rule is listed under 'NAT Rules Before'. The rule details are as follows:

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

Schritt 8: Stellen Sie sicher, dass eine Zugriffskontrollrichtlinie vorhanden ist, die Host-B den Zugriff auf Host-A und umgekehrt ermöglicht. Beachten Sie, dass statische NAT standardmäßig bidirektional ist. Beachten Sie wie bei klassischen ASAs die Verwendung echter IPs. Dies wird erwartet, da LINA in dieser Übung den Code 9.6.1.x ausführt, wie im Bild gezeigt.

The screenshot shows the 'Rules' tab in the Firepower Management Center. Two access control rules are listed under 'Mandatory - FTD5506-1 (1-2)'. The rules details are as follows:

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

Bestätigung:

Von LINA CLI:

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

Die NAT-Regel wurde erwartungsgemäß in Abschnitt 1 eingefügt:

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

Anmerkung: Die 2 Xlate, die im Hintergrund erstellt werden.

```
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
```

Die ASP NAT-Tabellen:

```
firepower# show asp table classify domain nat

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

Output Table:
L2 - Output Table:
L2 - Input Table:
Last clearing of hits counters: Never
```

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

Input Table

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

```

input_ifc=inside, output_ifc=dmz

L2 - Output Table:
L2 - Input Table:
Last clearing of hits counters: Never

```

Aktivieren Sie die Erfassung mit Trace-Details für FTD, und pingen Sie von Host-A an Host-B, wie im Bild gezeigt.

```

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>_

```

Die Anzahl der Treffer ist in den ASP-Tabellen:

```

firepower# show asp table classify domain nat

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

firepower# show asp table classify domain nat-reverse

Input Table

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

```

Die Paketerfassung zeigt Folgendes:

```
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
```

Die Spuren eines Pakets (wichtige Punkte werden hervorgehoben).

Anmerkung: Die ID der NAT-Regel und ihre Korrelation mit der ASP-Tabelle:

```
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=0xff602c72be0, priority=13, domain=capture, deny=false
 hits=55, user_data=0xff602b74a50, cs_id=0x0, 13_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=0xff603612200, priority=1, domain=permit, deny=false
 hits=1, user_data=0x0, cs_id=0x0, 13_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_fragments
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_fragments
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

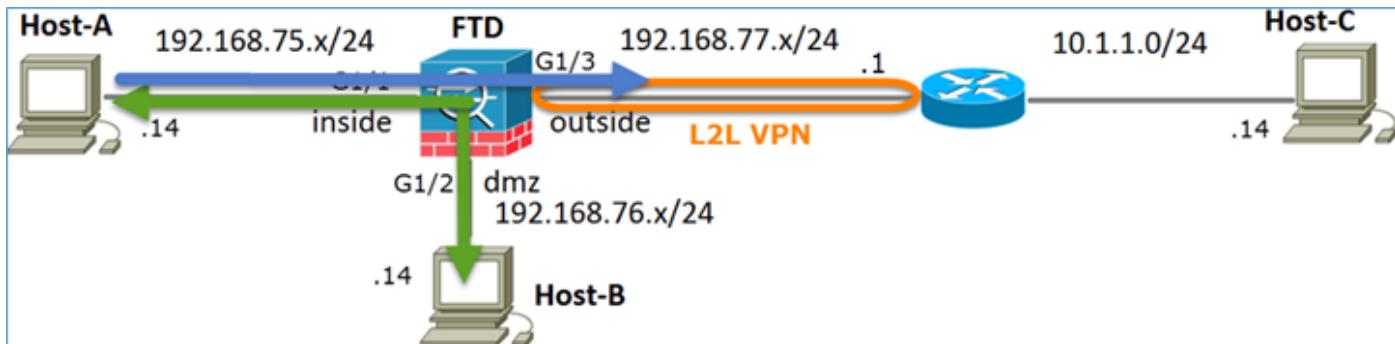
```

Schritt 2: Port-Adressumwandlung (PAT) auf FTD konfigurieren

Konfigurieren Sie NAT wie folgt:

NAT-Regel	Manuelle NAT-Regel
NAT-Typ	Dynamisch
Einfügen	In Abschnitt 1
Quellschnittstelle	Innen*
Zielschnittstelle	Außen*
Ursprüngliche Quelle	192.168.75.0/24
Übersetzte Quelle	Externe Schnittstelle (PAT)

* Sicherheitszonen für NAT-Regel verwenden



Statisches NAT

PAT

Lösung:

Schritt 1: Fügen Sie eine zweite NAT-Regel hinzu, und konfigurieren Sie sie wie im Bild gezeigt entsprechend den Aufgabenanforderungen.

Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules Before
Type:	Dynamic	<input checked="" type="checkbox"/> Enable		
Description:				

Interface Objects Translation PAT Pool Advanced

Available Interface Objects	Source Interface Objects (1)	Destination Interface Objects (1)
Search by name outside_zone dmz_zone inside_zone Group1 Group2	inside_zone	outside_zone
Add to Source Add to Destination		

Schritt 2: Die PAT wird wie im Bild dargestellt konfiguriert.

Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules Before
Type:	Dynamic	<input checked="" type="checkbox"/> 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:	

Schritt 3. Das Ergebnis ist wie im Bild dargestellt.

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

Schritt 4: Konfigurieren Sie für den Rest dieser Übung die Zugriffskontrollrichtlinie so, dass der gesamte Datenverkehr durchgelassen wird.

Bestätigung:

NAT-Konfiguration:

```
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
```

Beachten Sie in der LINA CLI den neuen Eintrag:

```
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
```

Aktivieren Sie die Erfassung an der inneren und äußeren Schnittstelle. Innerhalb der Erfassung aktivieren Sie die Ablaufverfolgung:

```
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
```

Pingen Sie von Host-A (192.168.75.14) an IP 192.168.77.1, wie im Bild gezeigt.

```
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

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
```

In LINA-Aufnahmen können Sie die PAT-Übersetzung sehen:

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

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

Die Spuren eines Pakets mit den folgenden wichtigen Abschnitten:

```
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
```

Der dynamische Ausdruck wurde erstellt (beachten Sie die "ri"-Flags):

```
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
```

In den LINA-Protokollen wird Folgendes angezeigt:

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

NAT-Abschnitte:

```

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-Tabellen zeigen:

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

```

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

```

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

```

Input Table

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

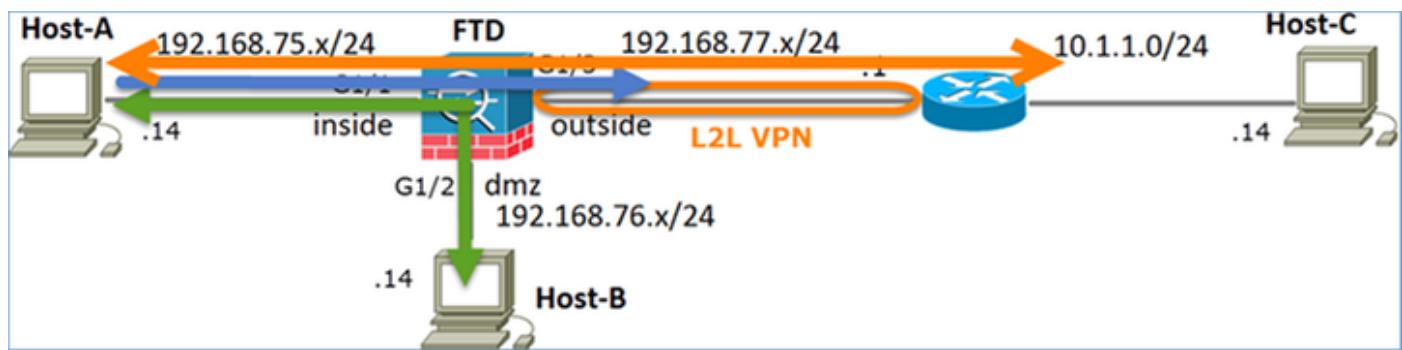
```

Schritt 3: NAT-Freistellung für FTD konfigurieren

Konfigurieren Sie NAT wie folgt:

NAT-Regel	Manuelle NAT-Regel
NAT-Typ	Statisch
Einfügen	In Abschnitt 1 werden vor allem bestehende Regeln
Quellschnittstelle	Innen*
Zielschnittstelle	Außen*
Ursprüngliche Quelle	192.168.75.0/24
Übersetzte Quelle	192.168.75.0/24
Ursprüngliches Ziel	10.1.1.0/24
Übersetztes Ziel	10.1.1.0/24

* Sicherheitszonen für NAT-Regel verwenden



Statisches NAT

PAT

NAT-Ausnahme

Lösung:

Schritt 1: Fügen Sie eine dritte NAT-Regel hinzu, und konfigurieren Sie die Anforderungen pro Task, wie im Bild dargestellt.

The screenshot shows the 'Rules' configuration table with the following data:

#	Direction	Type	Source Interface Obj...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
1	→	Static	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	→	Static	inside_zone	dmz_zone	Host-A			Host-B		
3	↔	Dynamic	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		

The first rule (rule 1) is highlighted with a red box. It maps traffic from the inside zone (source) to the outside zone (destination) using static NAT, translating the source port to 192.168.75.0_24bits and the destination port to 10.1.1.0_24bits. The second rule (rule 2) maps traffic from the inside zone to the dmz zone using static NAT, translating the source port to Host-A and the destination port to Host-B. The third rule (rule 3) is a dynamic NAT rule that maps traffic between the inside and outside zones, translating the source port to the interface and the destination port to the interface.

Schritt 2: Führen Sie eine Routensuche durch, um die Ausgangsschnittstelle zu bestimmen.

Anmerkung: Bei Identitäts-NAT-Regeln können Sie, wie bei den hinzugefügten, ändern, wie die Ausgangsschnittstelle bestimmt wird, und eine normale Routensuche verwenden, wie im Bild gezeigt.

Edit NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules Before
Type:	Static	<input checked="" type="checkbox"/> Enable		
Description:				
<input type="button" value="Interface Objects"/> <input type="button" value="Translation"/> <input type="button" value="PAT Pool"/> <input type="button" value="Advanced"/>				
<input type="checkbox"/> Translate DNS replies that match this rule <input type="checkbox"/> Fallthrough to Interface PAT(Destination Interface) <input type="checkbox"/> IPv6 <input type="checkbox"/> Net to Net Mapping <input type="checkbox"/> Do not proxy ARP on Destination Interface <input checked="" type="checkbox"/> Perform Route Lookup for Destination Interface <input type="checkbox"/> Unidirectional				

Bestätigung:

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

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

Ausführung der Paketverfolgung für Nicht-VPN-Datenverkehr aus dem internen Netzwerk Die PAT-Regel wird wie erwartet verwendet:

```
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

```

Packet-Tracer für Datenverkehr ausführen, der den VPN-Tunnel durchlaufen muss (zweimal ausführen, seit der erste Versuch den VPN-Tunnel aktiviert hat).

Anmerkung: Sie müssen die NAT-Freistellungsregel auswählen.

Erster Versuch der Paketverfolgung:

```

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

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

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

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

```

```
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
Additional Information:
NAT divert to egress interface outside
Untranslate 10.1.1.1/80 to 10.1.1.1/80
```

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

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

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
Additional Information:
static translate 192.168.75.14/1111 to 192.168.75.14/1111

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

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

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:

Result:
input-interface: inside

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

Zweiter Versuch der Paketverfolgung:

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

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

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

```
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
static net_10.1.1.0_24bits net_10.1.1.0_24bits
Additional Information:
NAT divert to egress interface outside
Untranslate 10.1.1.1/80 to 10.1.1.1/80
```

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

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

Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
Additional Information:
Static translate 192.168.75.14/1111 to 192.168.75.14/1111

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

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

Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
Additional Information:

Phase: 11
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

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

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

Phase: 14
Type: FLOW-CREATION

```

Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7226, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

```

Überprüfung der NAT-Trefferanzahl:

```

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

```

Aufgabe 4: Konfigurieren von Objekt-NAT auf FTD

Konfigurieren Sie NAT wie folgt:

NAT-Regel	Automatische NAT-Regel
NAT-Typ	Statisch
Einfügen	In Abschnitt 2
Quellschnittstelle	Innen*
Zielschnittstelle	DMZ*
Ursprüngliche Quelle	192.168.75.99
Übersetzte Quelle	192.168.76.99
Übersetzen von DNS-Antworten, die dieser Regel entsprechen	Aktiviert

* Sicherheitszonen für NAT-Regel verwenden

Lösung:

Schritt 1: Konfigurieren Sie die Regel gemäß den in den Bildern gezeigten Aufgabenanforderungen.

The screenshot shows the 'Add NAT Rule' configuration page. The 'NAT Rule' dropdown is set to 'Auto NAT Rule' and is highlighted with a red box. The 'Type' dropdown is set to 'Static' and is also highlighted with a red box. A checkbox labeled 'Enable' is checked. Below the configuration area are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Interface Objects' tab is selected and highlighted with a blue box. Under 'Available Interface Objects', there is a search bar and a list of objects: 'outside_zone', 'dmz_zone', 'inside_zone', 'Group1', and 'Group2'. The 'dmz_zone' object is currently selected and highlighted with a blue box. On the right side, under 'Source Interface Objects (1)', the 'inside_zone' object is listed and highlighted with a red box. Under 'Destination Interface Objects (1)', the 'dmz_zone' object is listed and highlighted with a red box. There are 'Add to Source' and 'Add to Destination' buttons.

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static | Enable

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

Original Packet	Translated Packet
Original Source: * <input type="text" value="obj-192.168.75.99"/>	Translated Source: <input type="text" value="obj-192.168.76.99"/>
Original Port: <input type="text" value="TCP"/>	Translated Port: <input type="text"/>

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static | Enable

Interface Objects Translation PAT Pool Advanced

Translate DNS replies that match this rule

Fallback to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Schritt 2. Das Ergebnis ist wie im Bild dargestellt.

Bestätigung:

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

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

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

Verifizierung mit Packet-Tracer:

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

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

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

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

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

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

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

```
Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-192.168.75.99
nat (inside,dmz) static obj-192.168.76.99 dns
Additional Information:
static translate 192.168.75.99/1111 to 192.168.76.99/1111
```

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

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

```
Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
```

New flow created with id 7245, packet dispatched to next module

Result:

```
input-interface: inside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Schritt 5: PAT-Pool auf FTD konfigurieren

Konfigurieren Sie NAT wie folgt:

NAT-Regel	Manuelle NAT-Regel
NAT-Typ	Dynamisch
Einfügen	In Abschnitt 3
Quellschnittstelle	Innen*
Zielschnittstelle	DMZ*
Ursprüngliche Quelle	192.168.75.0/24
Übersetzte Quelle	192.168.76.20-22
Gesamten Bereich verwenden (1-65535)	Aktiviert

* Sicherheitszonen für NAT-Regel verwenden

Lösung:

Schritt 1: Konfigurieren Sie die Regel für die einzelnen Aufgabenanforderungen, wie in den Bildern dargestellt.

Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules After
Type:	Dynamic	<input checked="" type="checkbox"/> Enable		
Description:				

Interface Objects Translation PAT Pool Advanced

Available Interface Objects	Source Interface Objects (1)	Destination Interface Objects (1)
<ul style="list-style-type: none">outside_zonedmz_zoneinside_zoneGroup1Group2	<ul style="list-style-type: none">inside_zone	<ul style="list-style-type: none">dmz_zone
<input type="button" value="Search by name"/>	<input type="button" value="Add to Source"/>	<input type="button" value="Add to Destination"/>

Add NAT Rule

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

Type: Dynamic | Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet		Translated Packet	
Original Source:*	Net_192.168.75.0_24bits	Translated Source:	Address
Original Destination:	Address	Translated Destination:	
Original Source Port:		Translated Source Port:	
Original Destination Port:		Translated Destination Port:	

Schritt 2: Aktivieren Sie Flat Port Range mit Include Reserve Ports, wodurch der gesamte Bereich (1-65535), wie im Bild dargestellt, verwendet werden kann.

Add NAT Rule

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

Type: Dynamic | Enable

Description:

Interface Objects Translation PAT Pool Advanced

Enable PAT Pool

PAT: Address range-192.168.76.20-22

Use Round Robin Allocation
 Extended PAT Table
 Flat Port Range
 Include Reserve Ports

Schritt 3. Das Ergebnis ist wie im Bild dargestellt.

#	Direction	T...	Source Interface ...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
Rules											
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_24bits		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											
4	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

Bestätigung:

```
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

```

Die Regel ist in Abschnitt 3:

```

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

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

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

```

Überprüfung des Paketverfolgungssystems:

```

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

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

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

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

```

```
found next-hop 192.168.76.5 using egress ifc dmz
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

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

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

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

Additional Information:

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

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
```

```
policy-map global_policy
```

```
class class-default
```

```
set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

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

Additional Information:

```
Dynamic translate 192.168.75.15/0 to 192.168.76.20/11654
```

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

```
class-map inspection_default
```

```
match default-inspection-traffic
```

```
policy-map global_policy
```

```
class inspection_default
```

```
inspect icmp
```

```
service-policy global_policy global
```

Additional Information:

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

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

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

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

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

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die Überprüfung wurde in den einzelnen Aufgabenabschnitten erläutert.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration

verwenden können.

Öffnen Sie die Seite **Erweiterte Fehlerbehebung** auf dem FMC, führen Sie die Paketverfolgung aus, und führen Sie dann den Befehl **show nat pool** aus.

Beachten Sie den Eintrag, der den gesamten Bereich verwendet, wie im Bild dargestellt.

The screenshot shows the FMC interface with the 'ASA CLI' tab selected. In the command input field, 'show' is selected from a dropdown, and 'Parameter' is set to 'nat pool'. The output pane displays several network configuration entries, with one specific entry highlighted by a red box and labeled '2': 'ICMP PAT pool dmz:range-192.168.76.20-22, address 192.168.76.20, range 1-65535, allocated 1'. Below this, other UDP PAT pool entries are listed.

Zugehörige Informationen

- Alle Versionen des Konfigurationsleitfadens für das Cisco FirePOWER Management Center finden Sie hier:

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

- Das Cisco Global Technical Assistance Center (TAC) empfiehlt dringend diese visuelle Anleitung, um detailliertes praktisches Wissen über die Cisco FirePOWER Sicherheitstechnologien der nächsten Generation zu erlangen, einschließlich der in diesem Artikel erwähnten Technologien:

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

- Für alle technischen Hinweise zur Konfiguration und Fehlerbehebung im Zusammenhang mit FirePOWER-Technologien:

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

- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.