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	Interfac	e		
Mode:	None		~	
Name:	inside		C Enabled	Management Only
Security Zone:	inside_zo	ne	~	
Description:				
General IPv	4 IPv6	Advanced	Hardware Con	figuration
MTU:		1500		(64 - 9198)
Interface ID:		GigabitEthe	rmet1/1	

Schritt 2. Das Ergebnis ist wie im Bild dargestellt.

Devices	Routing	Interfaces	Inline Sets	DHCP				
2							0	Add Interfaces •
Interface		Logie	al Name	Туре	Interface Objects	Mac Address(Active/Standby)	IP Address	
GigabitEt	hemet1/1	inside	1	Physical	inside_zone		192.168.75.6/24(Static)	J
GigabitEt	hemet1/2	dmz		Physical	dmz_zone		192.168.76.6/24(Static)	ø
GigabitEt	hemet1/3	outsi	de	Physical	outside_zone		192.168.77.6/24(Static)	ø

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

Objektverwaltung erstellen/bearbeiten, wie im Bild gezeigt.

Overview Analysis	Policies Devices Objects AM	1P Deploy 🤗 System Help 🔻 admin 🔻
Object Management	Intrusion Rules	
		Add • Filter
Retwork	▲ Name ▲	Type Security Zone ace Type
JP Port	▷ 👬 dmz_zone	Security
M Interface	b 😤 incide zono	Security Zana Deuted
🚰 Tunnel Tag	✓ Inside_zone	Security Zone Routed
Application Filters	b 📩 outside_zone	Security Zone Routed 🥔 🗍
📎 VLAN Tag		

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.

Overview Analysis Polici	ies Devices Objects AMP		Deploy 🥝 System Help 🔻	admin 🔻
Object Management Intrus	sion Rules			
		C	Add • Riter	
Network	Name -	Туре	Interface Type	
JP Port	🖌 📩 Group 1	Interface Group	Routed	J 🕯
Tunnel Tag	4 🚃 FTD5506-1			
Application Filters	inside			
📎 VLAN Tag	4 📩 Group2	Interface Group	Routed	6
Security Group Tag	FTD5506-1 inside			
ORL .	t and the second	Convitu Zono	Devited	28
Seolocation	- and amz_zone	Security Zone	Routed	60
S Variable Set	dmz			
 Security Intelligence Network Lists and Feeds 	d da inside zone	Security Zone	Routed	28
DNS Lists and Feeds	4 = ETD5506-1			
URL Lists and Feeds	👿 inside			
Sinkhole	a 📩 outside_zone	Security Zone	Routed	20
C File List	4 🚃 FTD5506-1			
Opher Suite List	📕 outside			

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.

Overview	Analysis	Policies	Devices	Objects AMP	Deploy 🥏	Syste	m Help 🔻	admin 🔻
Device Mana	gement	NAT	/PN QoS	Platform Settings				
							O New	Policy
NAT Poli	icy			Device Type	Status		Firepower N	AT
							Threat Defer	nse NAT

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

New Policy	?	×
Name: FTD5506-1 1 Description: Targeted Devices		
Select devices to which you want to apply this policy. Available Devices Selected Devices Selected Devices FTD5506-1 Tesuit	5	
3 Add to Policy		

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.

Add NAT Rule							
NAT Rule:	Manual NAT Ruk	Insert:	In Cate	gory	V NAT Rules B	efore	~
Type:	Static Y F Sa	L.L.				_	_
type.	Stabe	a Die					
Description:							
Interface Objects	Translation PAT Pool Advanced						
Available Interface	Objects C	Sourc	e Interface Objects (1)		Destination Interfa	ce Obj	ects (
🔍 Search by name		- mir	nside_zone	8	📩 dmz_zone		
a outside_zone						_	
🚠 dmz_zone	Add to						
📩 inside_zone	Source						
🚑 Group1	Add to Destination						
🚓 Group2							
Add NAT Rule							? X
NAT Rule:	Manual NAT Rule Y Ins	ert:	In Category	▼ NA	T Rules Before		
Type:	Static 💌 🔽 Enable						
Description:							
Interfere Oblights	Different Advanced						
Interface Objects	Instation PAT Pool Advanced		Translated Backet				
Original Source-*	Most A		Translated Source:	Address		~	
ongina source.	HOSEA	•••	Transactor Source.	Houress			
Original Destination:	Address	*		Host-B		*	•
		× 0	Translated Destination:			~	0
Original Source Port:		~ 0	Translated Source Port:			Y	0
Original Destination Por	t:	~ 0	Translated Destination Port:			¥	0

Host-A = 192.168.75.14

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.

											Policy /	Assignments (1)
R	iles Eter hu Da	uire .									0	Add Duly
.00	rice by be	VAC .				ioinal Packet		To	nelated Packet		v	Add Kule
		-			~	inginal Packet	٦	r	Islated Packet	ſ		
*	Dire	Typ	Source Interface Obj	Destination Interface Ob	Original Sources	Original Destinatio	Origi Servi	Translated Sources	Translated Destinatio	Trans Servi	Options	
٠	NAT Rule	s Bef	ore									
1	*	Stat	🚑 inside_zone	🚑 dmz_zone	👼 Host-A			👼 Host-B			🍓 Dns:false	/ 8
٠	▼ Auto NAT Rules											
٠	NAT Rule	s Aft	er									

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.

R	Rules Security Intelligence HTTP Responses Advanced															
68	B Filter by Device			Add Category		🔾 Add Rule		Search R	ules		×					
#	Name	S Z	D Z	Source Networks	Dest Networks	v	U	A	s	D	U	I A	Action	U 🖬 🤉	e 🕁 🔳 🖛	
-	Mandatory -	FTD55	06-1 (1-2)												
1	Host-A to Ho:	any	any	2 192.168.75.14	👳 192.168.76.14	any	any	any	any	any	any	any	🖋 Allow	UDA	e 💼 🗾 o	/ 🗊
2	Host-B to Ho:	any	any	2 192.168.76.14	2 192.168.75.14	any	any	any	any	any	any	any	🖋 Allow	001	e 💼 🗾 o	0
-	▼ Default - FTD5506-1 (-)															
Th	There are no rules in this section. Add Rule or Add Category															
De	fault Action							A	ccess (Control:	Block	All Traffi	c			× 🗾

Bestätigung:

Von LINA CLI:

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
```

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

```
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 IIL=128 Reply from 192.168.76.100: bytes=32 time=1ms IIL=128 Reply from 192.168.76.100: bytes=32 time=1ms IIL=128 Reply from 192.168.76.100: bytes=32 time=1ms IIL=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
   id=0x7ff603696860, priority=6, domain=nat, deny=false
in
       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=0x7ff602c72be0, priority=13, domain=capture, deny=false
       hits=55, user_data=0x7ff602b74a50, 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:
    id=0x7ff603612200, priority=1, domain=permit, deny=false
in
       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:
```

```
id=0x7ff602220020, priority=0, domain=nat-per-session, deny=true
 in
        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

1 packet shown

Action: allow

output-line-status: up

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

Konfigurieren Sie NAT wie folgt:

NAT-Regel NAT-Typ Einfügen Quellschnittstelle Zielschnittstelle Ursprüngliche Quelle Übersetzte Quelle

- Manuelle NAT-Regel Dynamisch In Abschnitt 1 Innen* Außen* 192.168.75.0/24 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 NA	T Rule	*	Insert:	In Category	▼ NAT	T Rules Before 💌
Туре:	Dynamic		Y Enal	ble			
Description:							
Interface Objects	Translation	PAT Pool	Advanced				
Available Interface (Objects 🖒			Source Interface Object	ts (1)	Destination	n Interface Objects (1
Search by name				inside_zone	ï	💼 outside	_zone
📩 outside_zone							
👬 dmz_zone			Add to				
inside_zone			Source				
📇 Group1			Add to				
📩 Group2			Desultation				



Add NAT Rule				?						
NAT Rule:	Manual NAT Rule 💙	Insert:	In Category	▼ NAT Rules Before ▼						
Type:	Dynamic 💌 🗹 Enabl	e								
Description:										
Interface Objects Tra	Interface Objects Translation PAT Pool Advanced									
Original Packet			Translated Packet							
Original Source:*	Net_192.168.75.0_24bits		Translated Source:	Destination Interface IP						
Original Destination:	Address	~		The values selected for Destination Interface Objects in 'Interface Objects' tab will be used						
		~ O	Translated Destination:	× 0						
Original Source Port:		× 0	Translated Source Port:	· · · ·						
Original Destination Por	t:	~ ()	Translated Destination Port:	▼ 3						

Schritt 3. Das Ergebnis ist wie im Bild dargestellt.

Ru	es										
881	iter by Device										
					Original Packet			Translated Packet			
•	Direction	Ť	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
۰,	▼ NAT Rules Before										
1	*	St	👍 inside_zone	👍 dmz_zone	📷 Host-A			🙀 Host-B			🝓 Dos:false
2	+	D	🚠 inside_zone	A outside_zone	Ret_192.168.75.0_24bits			🚳 Interface			🝓 Dos:false
• /	▼ Auto NAT Rules										
۰,	IAT Rules Aft	er									

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 TIL=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 p	ack	ets 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

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-6-302021: 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

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

R	iles										
đB	Filter by Device										
					Original Packet				Translated Packet		
*	Direction	Ту	Source Interface O	Destination Interface Obj	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1	*	Sta	🚠 inside_zone	🚠 outside_zone	Ret_192.168.75.0_24bits	💼 net_10.1.1.0_24bits		Ret_192.168.75.0_24	anet_10.1.1.0_24bit	5	
2	*	Sta	👬 inside_zone	🚠 dmz_zone	Host-A			📻 Host-B			
3	+	Dy	👬 inside_zone	🚑 outside_zone	Ret_192.168.75.0_24bits			🥞 Interface			
٠	Auto NAT Rules										
٠	NAT Rules After										

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 💙					
Туре:	Static	▼ Finable						
Description:								
Interface Objects	Translation PAT Poo	Advanced						
Translate DNS rep	plies that match this rule							
Fallthrough to Int	erface PAT(Destination I	nterface)						
IPv6								
Net to Net Mappi	ng							
Do not proxy ARP	Do not proxy ARP on Destination Interface							
Perform Route Lo	Perform Route Lookup for Destination Interface							
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
```

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:

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

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

output-line-status: up

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.

Add NAT Rule					
NAT Rule:	Auto NAT Rule				
Type:	Static	Y Enable			
Interface Objects	Translation PAT Poo	Advanced			
Available Interface	Objects 🖒		Source Interface Objects ((1) Destination	on Interface Objects (1)
🔍 Search by name			🚠 inside_zone	🗑 🚠 dmz_z	zone
utside_zone					
dmz_zone		Add to			
👬 inside_zone		Source			
🚠 Group1		Add to Destination			
Group2					
Add NAT Rule					? ×
		-			
NAT Rule:	Auto NAT Rule				
Type:	Static	Enable			
Interface Objects Tra	nslation PAT Pool	Advanced			
Original Packet			Translated Packet		
Original Source:*	obj-192.168.75.99	~ (Translated Source:	Address	×
				obj-192.168.76.99	· · · ·
Original Port:	тср 👻				
			Translated Port:		
Add NAT Rule					
NAT Rule:	Auto NAT Rule	• •			
Type:	Static	~	Enable		
Interface Objects	Translation PAT	Pool Advanc	ed		
Translate DNS r	eplies that match this	s rule			

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.

Falthrough to Interface PAT(Destination Interface)

IPv6

Rul	Rules										
db /	At Res by Device										
						Driginal Packet		Т	anslated Packet		
*	Direction	Ту	Source Interface O	Destination Interface Obj	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
¥ 8	NAT Rules Before										
1	**	Sta	📩 inside_zone	👬 outside_zone	Ret_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24b	a met_10.1.1.0_24bits		
2	*	Sta	📩 inside_zone	击 dmz_zone	📻 Host-A			📻 Host-B			
3	+	Dy	🚑 inside_zone	🚠 outside_zone	Ret_192.168.75.0_24bits			🝓 Interface			
• /	uto NAT Rules										
	4	Sta	🚠 inside_zone	👬 dmz_zone	🚃 obj-192.168.75.99			📄 obj-192.168.76.99			
¥ N	AT Rules After										

```
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 NAT-Typ Einfügen Quellschnittstelle Zielschnittstelle Ursprüngliche Quelle Übersetzte Quelle Gesamten Bereich verwenden (1-65535) Manuelle NAT-Regel Dynamisch In Abschnitt 3 Innen* DMZ* 192.168.75.0/24 192.168.76.20-22 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: Type:	Manual NAT	ſ Rule	▼ ▼ Fnab	Insert: le		In Catego	ry	▼ NAT Rules After ▼	
Description:									
Interface Objects	Translation	PAT Pool	Advanced						
Available Interface	Objects 🖒			Source	Interface C	bjects (1)		Destination Interface Objects (1)	
🔍 Search by name				👬 insi	de_zone		8	🚔 dmz_zone	8
📩 outside_zone									
🚠 dmz_zone			Add to						
👬 inside_zone		l	Source						
👬 Group1			Add to Destination						
👬 Group2									

Add NAT Rule		? >	×
NAT Rule:	Manual NAT Rule Insert:	In Category V NAT Rules After V	
Type:	Dynamic 💌 🗹 Enable		
Description:			
Interface Objects Tra	Islation PAT Pool Advanced		
Original Packet	Trans	lated Packet	1
Original Source:*	Net_192.168.75.0_24bits V 🔇 Transl	ated Source: Address 👻	
Original Destination:	Address	✓ Q	
	Transl	ated Destination:	
Original Source Port:	✓ ③ Transl	ated Source Port:	
Original Destination Por	: Transl	ated Destination Port:	

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

Add NAT Rule					? X
NAT Rule:	Manual NAT Rule	 Insert: 	In Category 👻	NAT Rules After	
Type:	Dynamic	F Enable			
Description:					
Interface Objects	Translation PAT Pool A	Advanced			
Enable PAT Pool]				
PAT:	Address 👻	ige-192.168.76.20-22 💙 🥥			
	Use Round Robin Allocati	ion			
	Extended PAT Table	_			
	Flat Port Range				
	Include Reserve Ports				

Schritt 3. Das Ergebnis ist wie im Bild dargestellt.

R	des										<u></u>		
68	Fiber by Device											0	Add Rule
					Original Packet			Translated Packet					
•	Direction	T	Source Interface	Destination Interface Ob	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options		
▼ NAT Rules Before													
1	**	St	📩 inside_zone	🔒 outside_zone	Ret_192.168.75.0_24bits	net_10.1.1.0_24bits		Ret_192.168.75.0_24bits	net_10.1.1.0_24bit		🝓 Dns:false		/8
2	*	St	👍 inside_zone	📩 dmz_zone	Host-A			📷 Host-B			🝓 Dns:false		/8
3	+	Dy	📩 inside_zone	🚠 outside_zone	Ret_192.168.75.0_24bits			🍓 Interface			🧠 Dns:false		/8
▼ Auto NAT Rules													
	4	St	🚠 inside_zone	🚠 dmz_zone	🚎 obj-192.168.75.99			🚎 obj-192.168.76.99			🭓 Dns:true		/8
▼ NAT Rules After													
4	•	Dy	📩 inside_zone	📩 dmz_zone	Ret_192.168.75.0_24bits			🚔 range-192.168.76.20-22			Ons:false fat fat fat fat	erve	/ 9

Bestätigung:

```
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

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

Phase: 1

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.



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/firepowerroadmap.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-serieshome.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.