Konfigurieren von ASA-Port Forwarding Version 9 mit NAT

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Zulassen des Zugriffs auf externe Netzwerke für interne Hosts mit PAT NAT ermöglicht internen Hosts den Zugriff auf externe Netzwerke Zulassen des Zugriffs nicht vertrauenswürdiger Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk Statische Identität NAT Port-Umleitung (Weiterleitung) mit statischer Überprüfung Verbindung Syslog **Packet Tracer** Erfassung Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie die Port Redirection (Forwarding) und die externen Network Address Translation (NAT)-Funktionen in der Adaptive Security Appliance (ASA) Software Version 9.x unter Verwendung der CLI oder des Adaptive Security Device Manager (ASDM) konfiguriert werden.

Weitere Informationen finden Sie im Cisco ASA Series Firewall ASDM Configuration Guide.

Voraussetzungen

Anforderungen

Weitere Informationen zur Konfiguration des Geräts durch den ASDM finden Sie unter Configuring Management Access.

Verwendete Komponenten

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

Versionen:

- Cisco Security Appliance der Serie ASA 5525 Software Version 9.x und höher
- ASDM Version 7.x und höher

"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 potenziellen Auswirkungen aller Befehle verstehen."

Konfigurieren

Netzwerkdiagramm



Die in dieser Konfiguration verwendeten IP-Adressschemata können nicht legal im Internet geroutet werden. Es handelt sich um RFC 1918-Adressen, die in einer Lab-Umgebung verwendet wurden.

Zulassen des Zugriffs auf externe Netzwerke für interne Hosts mit PAT

Wenn interne Hosts eine einzelne öffentliche Adresse für die Übersetzung gemeinsam nutzen sollen, verwenden Sie Port Address Translation (PAT). Eine der einfachsten PAT-Konfigurationen besteht darin, dass alle internen Hosts so umgewandelt werden, dass sie wie die IP-Adresse der externen Schnittstelle aussehen. Dies ist die typische PAT-Konfiguration, die verwendet wird, wenn die Anzahl der vom ISP verfügbaren routbaren IP-Adressen auf wenige oder möglicherweise nur eine beschränkt ist.

Führen Sie diese Schritte aus, um internen Hosts den Zugriff auf externe Netzwerke mit PAT zu ermöglichen:

1. Wählen Sie **Configuration > Firewall > NAT Rules aus**. Klicken Sie auf **Add** (**Hinzufügen**), und wählen Sie dann **Network Object** (**Netzwerkobjekt**) aus, um eine dynamische NAT-Regel zu konfigurieren.

Monitoring 🔚 Save 💽 Refresh 💽 Back 🜔	Forward ? Help CISCO
Configuration > Firewall > NAT Rules	Addresses Services
💠 Add 🗸 🌈 Edit 🗊 Delete 🛧 🗲 👗 🐚	Addresses 라우×
# Match Criteria: Original Packet * Source Intf Dest Intf Source	Add Add Carl Edit Carl Delete Carl Where Used Carl Network Object Filter Clear
"Network Object" NAT (Rule 1)	
1 Any outside 🚅 Inside_h	⊡-Network Objects

2. Konfigurieren Sie das Netzwerk/den Host/den Bereich, für das/den **Dynamic PAT** erforderlich ist. In diesem Beispiel wurde eines der internen Subnetze ausgewählt. Dieser Prozess kann für andere Subnetze wiederholt werden, die Sie auf diese Weise übersetzen möchten.

📧 Add Networ	k Object	×
Name:	obj_172.16.11.0	
Туре:	Network	*
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	~
Description:		
NAT		*
	OK Cancel Help	

 Erweitern Sie NAT. Aktivieren Sie das Kontrollkästchen Automatische Adressumwandlungsregeln hinzufügen. Wählen Sie in der Dropdown-Liste Typ die Option Dynamische PAT (Ausblenden) aus. Wählen Sie im Feld Translated Addr (Umgewandelte Adresse) die Option aus, die die externe Schnittstelle widerspiegelt. Klicken Sie auf Erweitert.

				^ L:	
	Ann	NPI	wnrk		err
- 100 C		1.00		00	

Add Network	k object 🔼
Name:	obi 172.16.11.0
Type:	Network
JP Version:	
ID Address	172 16 11 0
IP Address:	
Netmask:	255.255.255.0
Description:	
NAT	۲
🔽 Add Automa	atic Address Translation Rules
Type:	Dynamic PAT (Hide) 🗸
Translated Ad	Idr: outside
Use one-c	co-one address translation
PAT Pool	Translated Address:
Round I	Robin
Extend	PAT uniqueness to per destination instead of per interface
🔄 Transla	te TCP and UDP ports into flat range 1024-65535 🔄 Include range 1-1023
E Fall throu	gh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

4. Wählen Sie in den Dropdown-Listen Source Interface (Quellschnittstelle) und Destination Interface (Zielschnittstelle) die entsprechenden Schnittstellen aus. Klicken Sie auf OK und dann auf Übernehmen, damit die Änderungen wirksam werden.

🖀 Advanced NAT Set	ttings	×
Ranslate DNS repli	es for rule	
Interface		
Source Interface:	inside 💌 👻	
Destination Interface:	outside 💌	
ОК	Cancel Help	

Dies ist die entsprechende CLI-Ausgabe für diese PAT-Konfiguration:

object network obj_172.16.11.0 subnet 172.16.11.0 255.255.255.0 nat (inside,outside) dynamic interface

NAT ermöglicht internen Hosts den Zugriff auf externe Netzwerke

Sie können einer Gruppe von internen Hosts/Netzwerken mithilfe der Konfiguration der dynamischen NAT-Regeln den Zugriff auf die Außenwelt gestatten. Im Gegensatz zu PAT weist Dynamic NAT übersetzte Adressen aus einem Adresspool zu. Dadurch wird ein Host seiner eigenen umgewandelten IP-Adresse zugeordnet, und zwei Hosts können nicht dieselbe umgewandelte IP-Adresse gemeinsam nutzen.

Um dies zu erreichen, müssen Sie die reale Adresse der Hosts/Netzwerke auswählen, die Zugriff erhalten sollen, und diese dann einem Pool übersetzter IP-Adressen zuordnen.

Führen Sie die folgenden Schritte aus, um internen Hosts den Zugriff auf externe Netzwerke mit NAT zu ermöglichen:

 Wählen Sie Configuration > Firewall > NAT Rules aus. Klicken Sie auf Add (Hinzufügen), und wählen Sie dann Network Object (Netzwerkobjekt) aus, um eine dynamische NAT-Regel zu konfigurieren.

Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫	Forward 🤗 Help	CISCO
Configuration > Firewall > NAT Rules	Addresses Services	
🗣 Add 🗸 📝 Edit 🗊 Delete 🛧 🗲 🐰 🖿	Addresses	5
# Match Criteria: Original Packet	Add - C Edit Delete Q Whe	ere Used 🔍 Not Used
Source Intf Dest Intf Source	Network Object Group	
1 Any outside 🛃 Inside_h	□-Network Objects	
	🍫 any 🏈 any4 🏈 any6	

2. Konfigurieren Sie das Netzwerk/den Host/den Bereich, für das/den dynamische PAT erforderlich ist. In diesem Beispiel wurde das gesamte *interne Netzwerk* ausgewählt.

📴 Add Network	k Object	×
Name:	obj_172.16.11.0	
Туре:	Network	~
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	~
Description:		
NAT	8	Σ
	OK Cancel Help	

 Erweitern Sie NAT. Aktivieren Sie das Kontrollkästchen Automatische Adressumwandlungsregeln hinzufügen. Wählen Sie in der Dropdown-Liste Typ die Option Dynamisch aus. Wählen Sie im Feld "Translated Addr" die entsprechende Auswahl aus. Klicken Sie auf Erweitert.

📴 Edit Networ	k Object 🛛 🔀
ľ.,	
Name:	obj_172.16.11.0
Туре:	Network
IP Version:	⊙ IPv4 O IPv6
IP Address:	172.16.11.0
Netmask:	255.255.255.0
Description:	
NAT	۲
Add Autom	atic Address Translation Rules
Туре:	Dynamic 💌
Translated A	ddr:
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
🔄 Transla	ate TCP and UDP ports into flat range 1024-65535 📄 Include range 1-1023
🔄 Fall throu	ugh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

 Klicken Sie auf Hinzufügen, um das Netzwerkobjekt hinzuzufügen. Wählen Sie in der Dropdown-Liste Typ die Option Bereich aus. Geben Sie in die Felder "Start Address" (Startadresse) und "End Address" (Endadresse) die Start- und End-PAT-IP-Adresse ein. Klicken Sie auf OK.

📧 Add Networ	k Object 🛛 🔀
Name:	obj-my-range
Туре:	Range
IP Version:	⊙ IPv4 O IPv6
Start Address:	203.0.113.10
End Address:	203.0.113.20
Description:	
NAT	× 1
	OK Cancel Help

5. Wählen Sie im Feld Translated Addr (Umgewandelte Adresse) das Adressobjekt aus. Klicken Sie auf **Erweitert**, um die Quell- und Zielschnittstelle auszuwählen.

🧱 Edit Networ	k Object 🛛 🔊	<
Name:	obi 172 16 11 0	
Tupe:	Network	
туре:		
IP Version:	● IPv4 ● IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	
Description:		
NAT	۵	
🗹 Add Autom	atic Address Translation Rules	
Type:	Dynamic 🖌	
Translated A	ddr: obj-my-range 🛄	
Use one-	to-one address translation	
PAT Pool	Translated Address:	
Round	Robin	
Extend	PAT uniqueness to per destination instead of per interface	
Transla	ate TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023	
🔄 Fall throu	igh to interface PAT(dest intf): backup	
Use IPv6	for interface PAT	
	Advanced	
	OK Cancel Help	

6. Wählen Sie in den Dropdown-Listen Source Interface (Quellschnittstelle) und Destination Interface (Zielschnittstelle) die entsprechenden Schnittstellen aus. Klicken Sie auf **OK** und dann auf **Übernehmen**, damit die Änderungen wirksam werden.

🖀 Advanced NAT Set	ttings	×
Translate DNS repli	es for rule	
Interface		
Source Interface:	inside	*
Destination Interface:	outside	*
ОК	Cancel Help	

Dies ist die entsprechende CLI-Ausgabe für diese ASDM-Konfiguration:

```
object network obj-my-range
range 203.0.113.10 203.0.113.20
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat(inside,outside) dynamic obj-my-range
```

Gemäß dieser Konfiguration werden die Hosts im Netzwerk 172.16.11.0 aus dem NAT-Pool in eine beliebige IP-Adresse übersetzt, 203.0.113.10 - 203.0.113.20. Wenn der zugeordnete Pool weniger Adressen als die reale Gruppe hat, können Ihnen die Adressen ausgehen. Als Ergebnis können Sie versuchen, dynamische NAT mit einem dynamischen PAT-Backup zu implementieren, oder Sie können versuchen, den aktuellen Pool zu erweitern.

 Wiederholen Sie die Schritte 1 bis 3 der vorherigen Konfiguration, und klicken Sie erneut auf Hinzufügen, um ein Netzwerkobjekt hinzuzufügen. Wählen Sie in der Dropdown-Liste Type (Typ) die Option Host aus. Geben Sie im Feld IP Address (IP-Adresse) die IP-Adresse für die PAT-Sicherung ein. Klicken Sie auf OK.

🔄 Add Networ	k Object 🛛 🛛 🔀	
Name: (optional)	obj-pat-ip	
Туре:	Host	
IP Version:	● IPv4 ○ IPv6	
IP Address:	203.0.113.21	
Netmask:	255.255.255.0	
FQDN:		
Description:		
NAT	<u>()</u>	
	OK Cancel Help	

2. Klicken Sie auf **Hinzufügen**, um eine Netzwerkobjektgruppe hinzuzufügen. Geben Sie im Feld Gruppenname einen Gruppennamen ein, und **fügen Sie** beide Adressobjekte (NAT-Bereich und PAT-IP-Adresse) der Gruppe hinzu.

oup Name: nat-pat-group escription:							
Existing Network Objects	/Groups:				Members in Group:		
Name 🔺 1	IP Address	Netmask	Description		Name	IP Address	NetmaskPrefi
■ Network Objects					💬 🖳 obj-pat-ip	203.0.113.21	
- 🏈 any					👇 률 ob)-my-range	203.0.113.10-203.0	
- 🏈 any4							
- 🏈 any6							
- milde-net	19.19.19.0	255.255.255.0					
- 🛃 obj_172.1	172.16.11.0	255.255.255.0					
			ſ	<pre>c< hb</pre>			
			(Add >>			
			(Add >>			
			(Add >>			

3. Wählen Sie die konfigurierte NAT-Regel aus, und ändern Sie die umgewandelte Adresse in die neu konfigurierte Gruppe "nat-pat-group" (zuvor "obj-my-range"). Klicken Sie auf **OK**.

🔄 Browse Translated	Addr			×
Filter:	Delete Q Where	Used 🔍 Not Us	ed	Filter Clear
Name 🔺 1	IP Address	Netmask	Description	Object NAT Address
-Network Objects				
- 🥵 obj-my-ra	203.0.113.10-203			
🖳 🖳 obj-pat-ip	203.0.113.21			
-Network Object Gro	ups			
🚊 🚮 nat-pat-g				
Interfaces				
- 🔤 backup				
🎫 inside				
🔤 outside				
Colorised Translater d Add				
Selected Translated Add				
Translated Addr ->	nat-pat-group			
				OK Cancel

4. Klicken Sie auf **OK**, um die NAT-Regel hinzuzufügen. Klicken Sie auf **Erweitert**, um die Quellund Zielschnittstelle auszuwählen.

📧 Edit Networ	k Object 🛛 🔀
Name:	obi 172 16 11 0
Tuper N	Network
Type, K	
IP Version:	
IP Address:	172.16.11.0
Netmask:	255.255.255.0
Description:	
NAT	
	Nie Address Translation Dulas
Maa Autom	acic Address Translation Rules
Type:	Dynamic 💌
Translated A	ddr: nat-pat-group
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
Transla	te TCP and UDP ports into flat range 1024-65535 📄 Include range 1-1023
🔄 Fall throu	gh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

5. Wählen Sie in den Dropdown-Listen Source Interface (Quellschnittstelle) und Destination Interface (Zielschnittstelle) die entsprechenden Schnittstellen aus. Klicken Sie auf **OK**.

🖼 Advanced NAT Settings 🛛 🛛 🔀						
Translate DNS replies for rule						
Interface						
Source Interface:	inside 💌					
Destination Interface:	outside 💌					
ОК	Cancel Help					

6. Klicken Sie auf Apply (Übernehmen), damit die Änderungen wirksam werden.

• I XI	Ricken Sie auf Appig (Obernenmen), dannt die Anderdingen wirksam werden.							
S	Home 🦓 Configuration 🔯 Monitor	no 📔	Ныр	CISCO				
	Firewall 🗗 🖗	Con	figuration > Fi	rewall > NAT	Rules 🗆	Addresses Services		
e Da	Access Rules	4	Add 👻 📝 Edit	👔 Delete 🚽	「子品物園。」	Addresses	9 th X	
Devi			Match Crit	eria: Original	Packet	💠 Add - 📝 Edit 🎬 Delete 🔍 Wi	tere Used 🔍 Not Used	
	Device Setup	*	Source Intf	Dest Intf	Source	Fiker:	Filter Clear	
	🚮 Frewal		Network Object*	NAT (Rule 1)		Name		
	CA Benche Access IIPN		1 inside	outside	abi_172.16	Network Objects	^	
						any any		
	Ste-to-Site VPN					- @ any6	=	
	Device Management	<			>	- 📸 inside-network/24		
	×		Ar		Reset	- 📸 obj-my-range		
	-					└- 🚮 obj_172.16.11.0	~	

Dies ist die entsprechende CLI-Ausgabe für diese ASDM-Konfiguration:

object network obj-my-range range 203.0.113.10 203.0.113.20 object network obj-pat-ip host 203.0.113.21 object-group network nat-pat-group network-object object obj-my-range network-object object obj-pat-ip object network obj_172.16.11.0 subnet 172.16.11.0 255.255.255.0

Zulassen des Zugriffs nicht vertrauenswürdiger Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk

Dies kann durch die Anwendung einer statischen NAT-Übersetzung und einer Zugriffsregel erreicht werden, die diese Hosts zulässt. Sie müssen diese Konfiguration immer dann vornehmen, wenn ein externer Benutzer auf einen beliebigen Server in Ihrem internen Netzwerk zugreifen möchte. Der Server im internen Netzwerk kann über eine private IP-Adresse verfügen, die im Internet nicht routbar ist. Daher müssen Sie diese private IP-Adresse mithilfe einer statischen NAT-Regel in eine öffentliche IP-Adresse übersetzen. Angenommen, Sie haben einen internen Server (172.16.11.5). Damit dies funktioniert, müssen Sie diese private Server-IP-Adresse in eine öffentliche IP-Adresse übersetzen. In diesem Beispiel wird die Implementierung der bidirektionalen statischen NAT für die Übersetzung von 172.16.11.5 in 203.0.113.5 beschrieben.

 Wählen Sie Configuration > Firewall > NAT Rules aus. Klicken Sie auf Hinzufügen, und wählen Sie dann Netzwerkobjekt aus, um eine statische NAT-Regel zu konfigurieren. Erweitern Sie NAT.

bject 🛛 🔀
j_172.16.11.5
ist 🛛 👻
IPv4 🔘 IPv6
2.16.11.5
OK Cancel Help
j

 Aktivieren Sie das Kontrollkästchen Automatische Adressumwandlungsregeln hinzufügen. Wählen Sie in der Dropdown-Liste Typ die Option Statisch aus. Geben Sie im Feld "Translated Addr" (Umgewandelte Adresse) die IP-Adresse ein. Klicken Sie auf Erweitert, um die Quell- und Zielschnittstelle auszuwählen.

🔚 Add Networ	k Object 🛛 🛛 🔀								
Name:	obj_172.16.11.5								
Туре:	Host								
IP Version:	⊙ IPv4 ○ IPv6								
IP Address:	172.16.11.5								
Description:									
NAT	*								
🛃 Add Automa	atic Address Translation Rules								
Type:	Static 🖌								
Translated Ac	ddr: 203.0.113.5								
🔽 Use one-t	co-one address translation								
PAT Pool	Translated Address:								
Round	Robin								
Extend	PAT uniqueness to per destination instead of per interface								
🔄 Transla	te TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023								
Fall throu	Fall through to interface PAT(dest intf): backup								
Use IPv6	Use IPv6 for interface PAT								
	Advanced								
	OK Cancel Help								

3. Wählen Sie in den Dropdown-Listen Source Interface (Quellschnittstelle) und Destination Interface (Zielschnittstelle) die entsprechenden Schnittstellen aus. Klicken Sie auf OK.

🖼 Advanced NAT Settings 🛛 🛛 🔀						
Translate DNS replies for rule						
Interface						
Source Interface:	inside 🔽 👻					
Destination Interface:	outside 💌					
ОК	Cancel Help					

4. Hier sehen Sie den konfigurierten statischen NAT-Eintrag. Klicken Sie auf **Apply**, um dies an die ASA zu senden.

onfic	uration > Fir	ewall > NAT I	Rules		L3				
💠 Add 👻 📷 Edit 👕 Delete 🛛 🛧 🌾 🐇 🐚 🏨 🗸 🔍 Find 🖼 Diagram 🐙 Packet Trace									
	Match Crite	eria: Original I	Packet			Action: Translat	ted Packet		
Ŧ	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	
"Ne	etwork Object"	NAT (Rule 1)							
1	inside	outside	遇 obj_172.16	🌍 any	🥥 any	🖳 203.0.113.5 (S) Original	Original	
	outside	inside	🏟 any	3 203.0.113.5	🧼 any	Original (S)	🖪 obj_172.16	Original	
				Apply	Reset				

Dies ist die entsprechende CLI-Ausgabe für diese NAT-Konfiguration:

object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5

Statische Identität NAT

NAT Exempt ist eine nützliche Funktion, bei der interne Benutzer versuchen, auf einen entfernten VPN-Host/Server oder einen Host/Server zuzugreifen, der hinter einer anderen Schnittstelle der

ASA gehostet wird, ohne eine NAT abzuschließen. Um dies zu erreichen, kann der interne Server, der über eine private IP-Adresse verfügt, auf sich selbst identitätsübersetzt werden und der seinerseits auf das Ziel zugreifen darf, das eine NAT durchführt.

In diesem Beispiel muss der interne Host 172.16.11.15 auf den Remote-VPN-Server 172.20.21.15 zugreifen.

Gehen Sie wie folgt vor, um internen Hosts den Zugriff auf das Remote-VPN-Netzwerk mit Abschluss einer NAT zu ermöglichen:

1. Wählen Sie **Configuration > Firewall > NAT Rules aus**. Klicken Sie auf **Hinzufügen**, um eine Regel für NAT-Freistellung zu konfigurieren.



2. Wählen Sie in den Dropdown-Listen Source Interface (Quellschnittstelle) und Destination Interface (Zielschnittstelle) die entsprechenden Schnittstellen aus. Wählen Sie im Feld "Source Address" (Quelladresse) den entsprechenden Eintrag aus.

📑 Add NAT Rule					×
Match Criteria: Original Packet					
Source Interface:	inside	~	Destination Interface:	outside	~
Source Address:	any		Destination Address:	any	
			Service:	any	
Action: Translated Packet					
Source NAT Type:	Static 👔	🗧 Browse Ori	ginal Source Addres	S	
Source Address:	Origina				
Use one-to-one address transla	ation	🔂 Add 🛨 🛛	💣 Edit 📋 Delete 🔍	Where Used 🔍 No	ot Used
PAT Pool Translated Address:		Filter:			
Round Robin		Name	▲ 1 IP Address		Netmask
Extend PAT uniqueness to pe	er destinal	in 🍪 an	y V		
Translate TCP and UDP ports	; into flat r				
Fall through to interface PAT					
Use IPv6 for source interface P	AT				
Options					
🗹 Enable rule					
Translate DNS replies that mate	th this rule				

3. Klicken Sie auf **Hinzufügen**, um ein Netzwerkobjekt hinzuzufügen. Konfigurieren der Host-IP-Adresse

🐻 Add Networ	k Object 🛛 🔀
Name:	obj 172.16.11.15
Туре:	Host
IP Version:	
IP Address:	172 16 11 15
Description:	
NAT	8
	OK Cancel Help

4. Navigieren Sie ebenfalls zur **Zieladresse**. Klicken Sie auf **Hinzufügen**, um ein Netzwerkobjekt hinzuzufügen. Konfigurieren der Host-IP-Adresse

📴 Add Networ	k Object 🛛 🛛 🔀]
Name: Type: IP Version: IP Address: Description:	pbj_172.20.21.15 Host IPv4 IPv6 172.20.21.15	
NAT		
	OK Cancel Help	

5. Wählen Sie die konfigurierten Quell- und Zieladressobjekte aus. Aktivieren Sie die Kontrollkästchen Proxy-ARP an der Ausgangsschnittstelle deaktivieren und Routentabelle suchen, um die Ausgangsschnittstelle zu suchen. Klicken Sie auf OK.

📧 Add NAT Rule			×		
Match Criteria: Original Packet					
Source Interface:	inside 💌	Destination Interface:	outside 💌		
Source Address:	obj_172.16.11.15 🔄	Destination Address:	obj_172.20.21.15		
		Service:	any 💮		
Action: Translated Packet					
Source NAT Type:	Static 💌				
Source Address:	Original 📰	Destination Address:	Original 🛛 😨		
Use one-to-one address transla	ition				
PAT Pool Translated Address:		Service:	Original 🛛 🛄		
Round Robin					
Extend PAT uniqueness to pe	r destination instead of per int	erface			
Translate TCP and UDP ports	Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023				
Fall through to interface PAT	Fall through to interface PAT				
Use IPv6 for source interface P	AT	Use IPv6 for destin	ation interface PAT		
Options					
🔽 Enable rule					
Translate DNS replies that mate	h this rule				
✓ Disable Proxy ARP on egress interface					
Cookup route table to locate egress interface					
Direction: Both 💉					
Description:					
OK Cancel Help					

6. Klicken Sie auf **Apply** (Übernehmen), damit die Änderungen wirksam werden.

🗞 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🧳 Help						
a e 🚺	Confi	guration > Fire	ewall > NAT P	tules		Addresses D
ass Rules	4	dd 🔻 📝 Edit 🕯	🗊 Delete 🗲	4 X ha ma -	Q, Find	♣ Add
rice Policy Rules		Match Criteria: Original Packet				Fiter: E
(Rules	*	Source Intf	Dest Intf	Source	Destina	Name
r Rules	1	inside	outside	🖪 obj_172.16	🖪 obj_	 Network Objects
e Setup	''N	"Network Object" NAT (No rules)				🧼 any
al						🧼 any6
te Access VPN						- 🙀 inside-network/24
						- 📇 obj_172.16.11.15
o-Site VPN						🖳 obj_172.20.21.15
e Management	<	Ш			>	
×			Apply	Reset		

Dies ist die entsprechende CLI-Ausgabe für die NAT Exempt- oder Identity NAT-Konfiguration:

object network obj_172.16.11.15 host 172.16.11.15 object network obj_172.20.21.15 host 172.20.21.15

nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup

Port-Umleitung (Weiterleitung) mit statischer

Port Forwarding oder Port Redirection ist eine nützliche Funktion, wenn externe Benutzer versuchen, auf einen internen Server an einem bestimmten Port zuzugreifen. Um dies zu erreichen, kann der interne Server, der über eine private IP-Adresse verfügt, in eine öffentliche IP-Adresse übersetzt werden, die wiederum Zugriff für den jeweiligen Port erhält.

In diesem Beispiel möchte der externe Benutzer auf den SMTP-Server 203.0.113.15 an Port 25 zugreifen. Dies geschieht in zwei Schritten:

- 1. Übertragen Sie den internen Mailserver, 172.16.11.15 auf Port 25, an die öffentliche IP-Adresse 203.0.113.15 auf Port 25.
- 2. Zulassen des Zugriffs auf den öffentlichen Mailserver 203.0.113.15 an Port 25

Wenn der externe Benutzer versucht, auf den Server 203.0.113.15 an Port 25 zuzugreifen, wird dieser Datenverkehr an den internen Mailserver 172.16.11.15 an Port 25 umgeleitet.

1. Wählen Sie **Configuration > Firewall > NAT Rules aus**. Klicken Sie auf **Hinzufügen**, und wählen Sie dann **Netzwerkobjekt** aus, um eine statische NAT-Regel zu konfigurieren.

Monitoring 🔚 Save 🔇 Refresh 🔇 Back 📀	Forward 🦻 Help	CISCO
Configuration > Firewall > NAT Rules	Addresses Services	
🗣 Add 🗸 📝 Edit 🛱 Delete 🛧 🐇 🖿	Addresses	급 中 ×
# Match Criteria: Original Packet Source Intf Dest Intf Source	♣ Add ▼ ☑ Edit Î Delete Q W Image: Network Object	here Used 🔍 Not Used
"Network Object" NAT (Rule 1)	Network Object Group	▲ 1
1 Any outside 🛃 Inside_h	■ Network Objects	
	- 🌍 any	
	- 🌍 any4	
	📗 🧼 🌍 any6	

2. Konfigurieren Sie den Host, für den eine Port-Weiterleitung erforderlich ist.

📧 Edit Network Object 🛛 🛛 🔀		
Name:	obj_172.16.11.15]
Туре:	Host	
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.15]
Description:]
NAT	 S 	
	OK Cancel Help	

 Erweitern Sie NAT. Aktivieren Sie das Kontrollkästchen Automatische Adressumwandlungsregeln hinzufügen. Wählen Sie in der Dropdown-Liste Typ die Option Statisch aus. Geben Sie im Feld "Translated Addr" (Umgewandelte Adresse) die IP-Adresse ein. Klicken Sie auf Erweitert, um den Service sowie die Quell- und Zielschnittstellen auszuwählen.

📧 Edit Network	k Object	×	
Name	obi 172 16 11 15		
Turner	Uppt		
Type:		*	
IP Vysion:	● IPv4 ○ IPv6		
IP Address:	172.16.11.15		
Description:			
		····	
Add Automa	itic Address Translation Rules		
Туре:	Static		
Translated Ad	idr: 203.0.115.15		
Use one-to	o-one address translation		
PAT Pool T	PAT Pool Translated Address:		
Round Robin			
Extend PAT uniqueness to per destination instead of per interface			
Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023			
Fall through to interface PAT(dest intf): backup			
Use IPv6 for interface PAT			
	Advanced		
	OK Cancel Help		

4. Wählen Sie in den Dropdown-Listen Source Interface (Quellschnittstelle) und Destination Interface (Zielschnittstelle) die entsprechenden Schnittstellen aus. Konfigurieren Sie den Dienst. Klicken Sie auf **OK**.

🖬 Advanced NAT Settings 🛛 🛛 🔀			
Translate DNS replies for rule			
Disable Proxy ARP on egress interface			
Lookup route table to locate egress interface			
Interface			
Source Interface:	inside 💌		
Destination Interface:	outside 💌		
Service			
Protocol:	😰 tcp 🔽		
Real Port:	smtp		
Mapped Port:	smtp		
OK Cancel Help			

5. Klicken Sie auf Apply (Übernehmen), damit die Änderungen wirksam werden.



Dies ist die entsprechende CLI-Ausgabe für diese NAT-Konfiguration:

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp
```

Überprüfung

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

Der <u>Cisco CLI Analyzer</u> (nur <u>registrierte</u> Kunden) unterstützt bestimmte **show-**Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe** des Befehls **show** anzuzeigen.

Zugriff auf eine Website über HTTP mit einem Webbrowser In diesem Beispiel wird eine Site verwendet, die unter 198.51.100.100 gehostet wird. Wenn die Verbindung erfolgreich hergestellt werden kann, wird diese Ausgabe in der ASA CLI angezeigt.

Verbindung

ASA(config)# show connection address 172.16.11.5 6 in use, 98 most used TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937, flags UIO Die ASA ist eine Stateful-Firewall, und der zurückkehrende Datenverkehr vom Webserver wird zurück durch die Firewall zugelassen, da er mit einer *Verbindung* in der Firewall-Verbindungstabelle übereinstimmt. Datenverkehr, der mit einer bereits vorhandenen Verbindung

übereinstimmt, wird über die Firewall zugelassen, ohne von einer Schnittstelle-ACL blockiert zu werden.

In der vorherigen Ausgabe hat der Client auf der internen Schnittstelle eine Verbindung zum Host 198.51.100.100 der externen Schnittstelle hergestellt. Diese Verbindung wird mit dem TCP-Protokoll hergestellt und ist seit sechs Sekunden inaktiv. Die Verbindungsflags geben den aktuellen Status dieser Verbindung an. Weitere Informationen zu Verbindungsflags finden Sie unter <u>ASA TCP-Verbindungsflags</u>.

Syslog

ASA(config)# show log | in 172.16.11.5

6 gesehen werden, oder die 'informative' Ebene.

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside: 172.16.11.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside: 198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799) Die ASA Firewall generiert Syslogs im normalen Betrieb. Die Syslogs sind abhängig von der Konfiguration der Protokollierung sehr ausführlich. Die Ausgabe zeigt zwei Syslogs, die auf Ebene

In diesem Beispiel werden zwei Syslogs generiert. Die erste ist eine Protokollmeldung, die anzeigt, dass die Firewall eine Übersetzung erstellt hat, insbesondere eine dynamische TCP-Übersetzung (PAT). Er gibt die IP-Quelladresse und den Port sowie die umgewandelten IP-Adressen und den Port an, während der Datenverkehr von den internen zu den externen Schnittstellen übertragen wird.

Das zweite Syslog gibt an, dass die Firewall in ihrer Verbindungstabelle eine Verbindung für diesen spezifischen Datenverkehr zwischen Client und Server hergestellt hat. Wenn die Firewall konfiguriert wurde, um diesen Verbindungsversuch zu blockieren, oder ein anderer Faktor die Herstellung dieser Verbindung verhindert hat (Ressourcenbeschränkungen oder eine mögliche Fehlkonfiguration), würde die Firewall kein Protokoll generieren, das anzeigt, dass die Verbindung hergestellt wurde. Stattdessen würde sie einen Grund für die Ablehnung der Verbindung oder einen Hinweis darauf protokollieren, welcher Faktor die Herstellung der Verbindung verhindert hat.

Packet Tracer

ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80

--Omitted--

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

Mit der Paketverfolgungsfunktion auf der ASA können Sie ein *simuliertes* Paket angeben und alle verschiedenen Schritte, Prüfungen und Funktionen anzeigen, die die Firewall durchläuft, wenn sie Datenverkehr verarbeitet. Mit diesem Tool ist es hilfreich, ein Beispiel für Datenverkehr zu identifizieren, von dem Sie glauben, dass er durch die Firewall geleitet werden *kann*, und dieses 5-Tupel zu verwenden, um Datenverkehr zu simulieren. Im vorherigen Beispiel wird der Paket-Tracer verwendet, um einen Verbindungsversuch zu simulieren, der folgende Kriterien erfüllt:

- Das simulierte Paket kommt im Inneren an.
- Das verwendete Protokoll ist TCP.
- Die simulierte Client-IP-Adresse lautet 172.16.11.5.
- Der Client sendet Datenverkehr von Port 1234.
- Der Datenverkehr ist an einen Server mit der IP-Adresse 198.51.100.100 gerichtet.
- Der Datenverkehr ist für Port 80 bestimmt.

Beachten Sie, dass die Schnittstelle außerhalb des Befehls nicht erwähnt wurde. Dies erfolgt über das Packet-Tracer-Design. Das Tool teilt Ihnen mit, wie die Firewall diese Art von Verbindungsversuch verarbeitet, einschließlich, wie sie diese routen würde, und von welcher Schnittstelle aus. Weitere Informationen über Packet Tracer finden Sie unter Tracing Packets with Packet Tracer.

Erfassung

Erfassung anwenden

ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100 ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448: 780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK> 2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067: 2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8> 3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068 win 32768 1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465: 1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK> 2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629: 95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8> 3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630 win 32768/pre>

Die ASA-Firewall kann den ein- oder ausgehenden Datenverkehr erfassen. Diese Erfassungsfunktion ist fantastisch, da sie eindeutig belegen kann, ob Datenverkehr bei einer Firewall eingeht oder diese verlässt. Das vorherige Beispiel zeigte die Konfiguration von zwei Captures namens capin und capout auf der internen bzw. externen Schnittstelle. Die Capture-Befehle verwendeten das Match-Schlüsselwort, mit dem Sie den zu erfassenden Datenverkehr genau bestimmen können.

Für die Capture-**Schnittstelle** haben Sie angegeben, dass Sie den Datenverkehr auf der internen Schnittstelle (Eingang oder Ausgang), der mit dem TCP-Host 172.16.11.5 Host 198.51.100.100 übereinstimmt, abgleichen möchten. Mit anderen Worten, Sie möchten den TCP-Datenverkehr erfassen, der von Host 172.16.10 gesendet wird. 11.5 auf Host 198.51.100.100 oder umgekehrt. Durch die Verwendung des Match-Schlüsselworts kann die Firewall diesen Datenverkehr bidirektional erfassen. Der für die externe Schnittstelle definierte Erfassungsbefehl referenziert nicht die interne Client-IP-Adresse, da die Firewall PAT für diese Client-IP-Adresse durchführt. Daher können Sie keine Übereinstimmung mit dieser Client-IP-Adresse herstellen. Stattdessen wird in diesem Beispiel any verwendet, um anzugeben, dass alle möglichen IP-Adressen mit dieser Bedingung übereinstimmen.

Nachdem Sie die Aufzeichnungen konfiguriert haben, versuchen Sie erneut, eine Verbindung herzustellen, und fahren Sie mit dem Befehl **show capture** *<capture_name> fort, die Aufzeichnungen anzuzeigen*. In diesem Beispiel können Sie sehen, dass der Client eine Verbindung zum Server herstellen konnte, wie der TCP 3-Wege-Handshake in den Aufnahmen zeigt.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <u>ASA Syslog-Konfigurationsbeispiel</u>
- ASA-Paketerfassung mit CLI und ASDM Konfigurationsbeispiel
- 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.