Konfigurieren der ASA für zwei interne Netzwerke

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Cisco Adaptive Security Appliance (ASA) konfigurieren, die Software Version 9.x für die Verwendung von zwei internen Netzwerken ausführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA, die die Software Version 9.x ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Wenn Sie ein zweites internes Netzwerk hinter einer ASA-Firewall hinzufügen, sollten Sie folgende wichtige Informationen berücksichtigen:

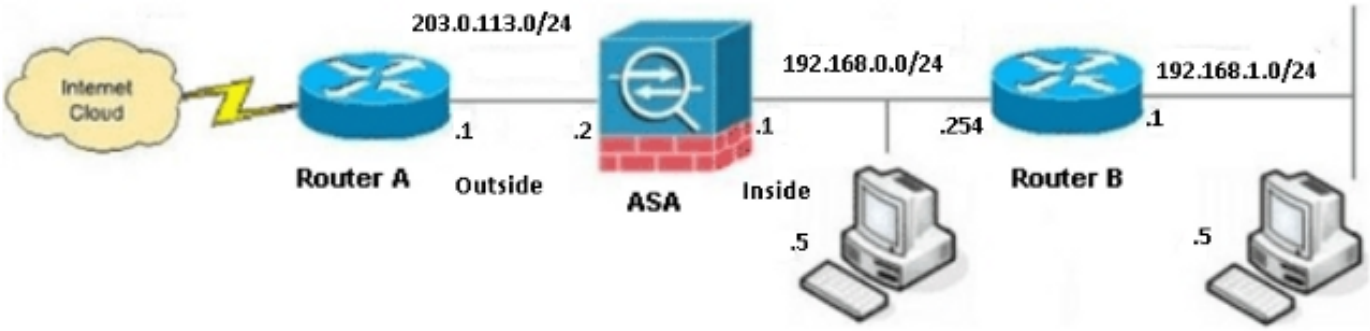
- Die ASA unterstützt keine sekundäre Adressierung.
- Hinter der ASA muss ein Router verwendet werden, um das Routing zwischen dem aktuellen Netzwerk und dem neu hinzugefügten Netzwerk zu ermöglichen.
- Das Standard-Gateway für alle Hosts muss auf den internen Router zeigen.
- Sie müssen dem internen Router eine Standardroute hinzufügen, die auf die ASA verweist.
- Sie müssen den ARP-Cache (Address Resolution Protocol) auf dem internen Router löschen.

Konfigurieren

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um die ASA zu konfigurieren.

Netzwerkdiagramm

Die folgende Topologie wird für die Beispiele in diesem Dokument verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet werden.

ASA 9.x-Konfiguration

Wenn der Befehl **write terminal** von Ihrem Cisco Gerät ausgegeben wird, können Sie das Output Interpreter-Tool (nur registrierte Kunden) verwenden, um potenzielle Probleme und Fixes anzuzeigen.

Die folgende Konfiguration für die ASA-Software Version 9.x wird ausgeführt:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.
```

```
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

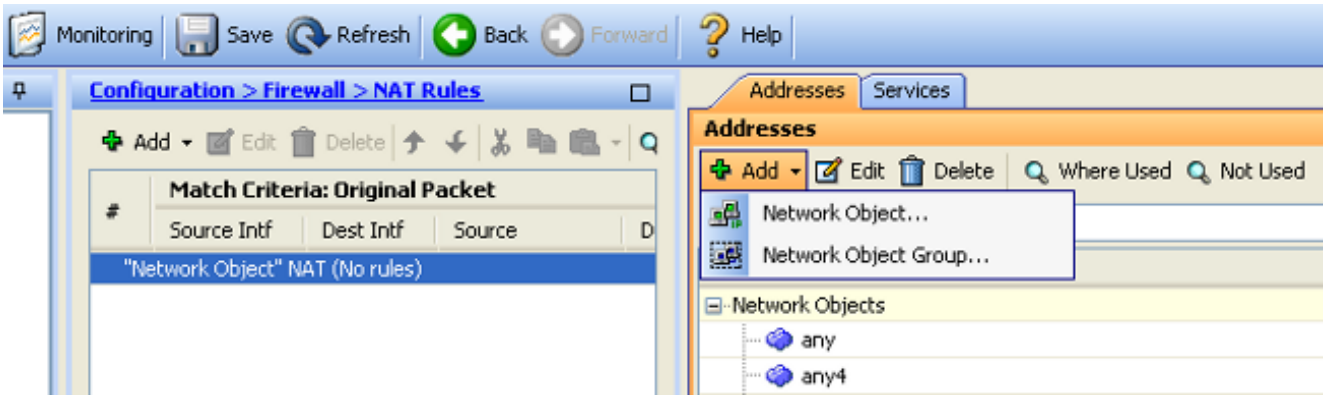
Zugriff für interne Hosts auf externe Netzwerke mit PAT zulassen

Wenn die internen Hosts eine einzige öffentliche Adresse für die Übersetzung freigeben sollen, verwenden Sie die Port Address Translation (PAT). Eine der einfachsten PAT-Konfigurationen

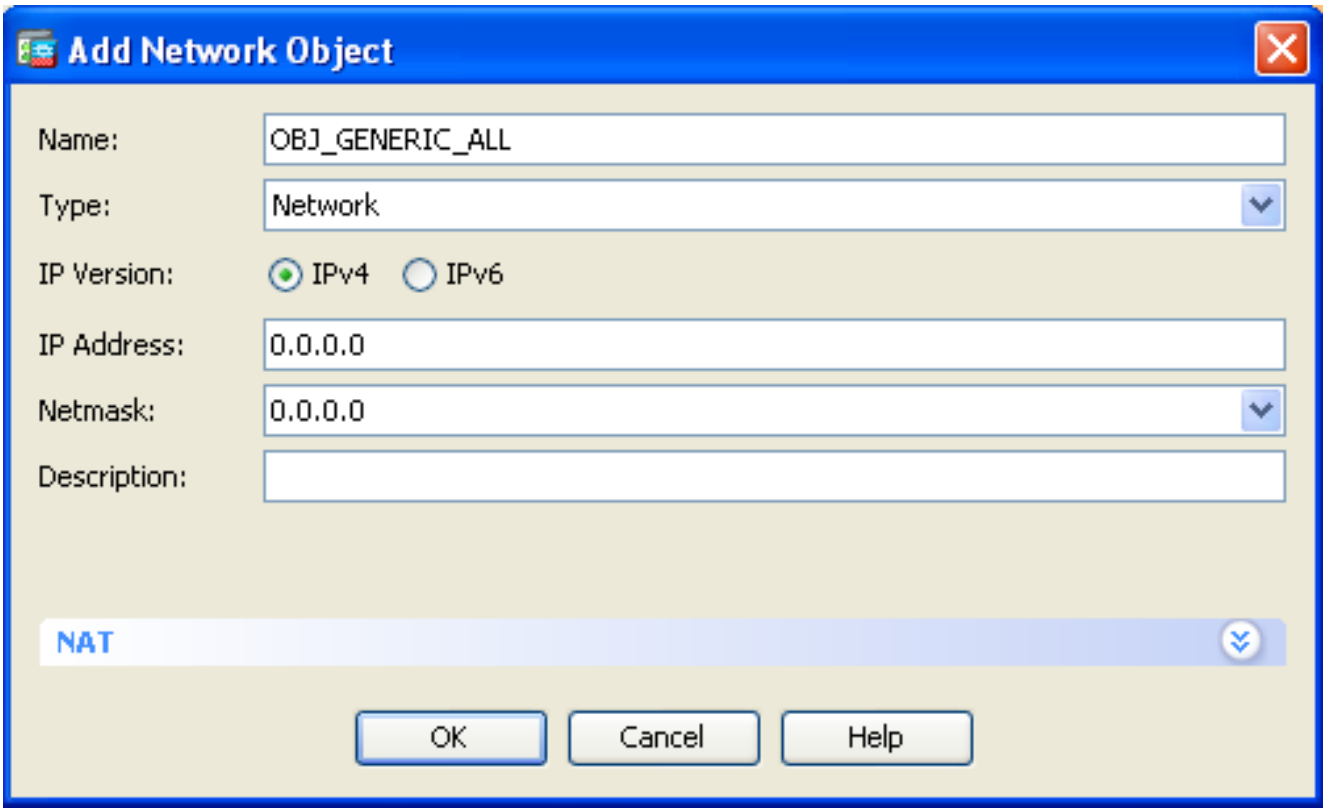
beinhaltet die Übersetzung aller internen Hosts, sodass diese als IP-Adresse der externen Schnittstelle erscheinen. Dies ist die typische PAT-Konfiguration, die verwendet wird, wenn die Anzahl der routbaren IP-Adressen, die vom ISP zur Verfügung stehen, auf wenige oder nur eine beschränkt ist.

Gehen Sie wie folgt vor, um den internen Hosts den Zugriff auf die externen Netzwerke mit PAT zu ermöglichen:

1. Navigieren Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie **Network Object (Netzwerkobjekt) aus, um eine dynamische NAT-Regel zu konfigurieren:**

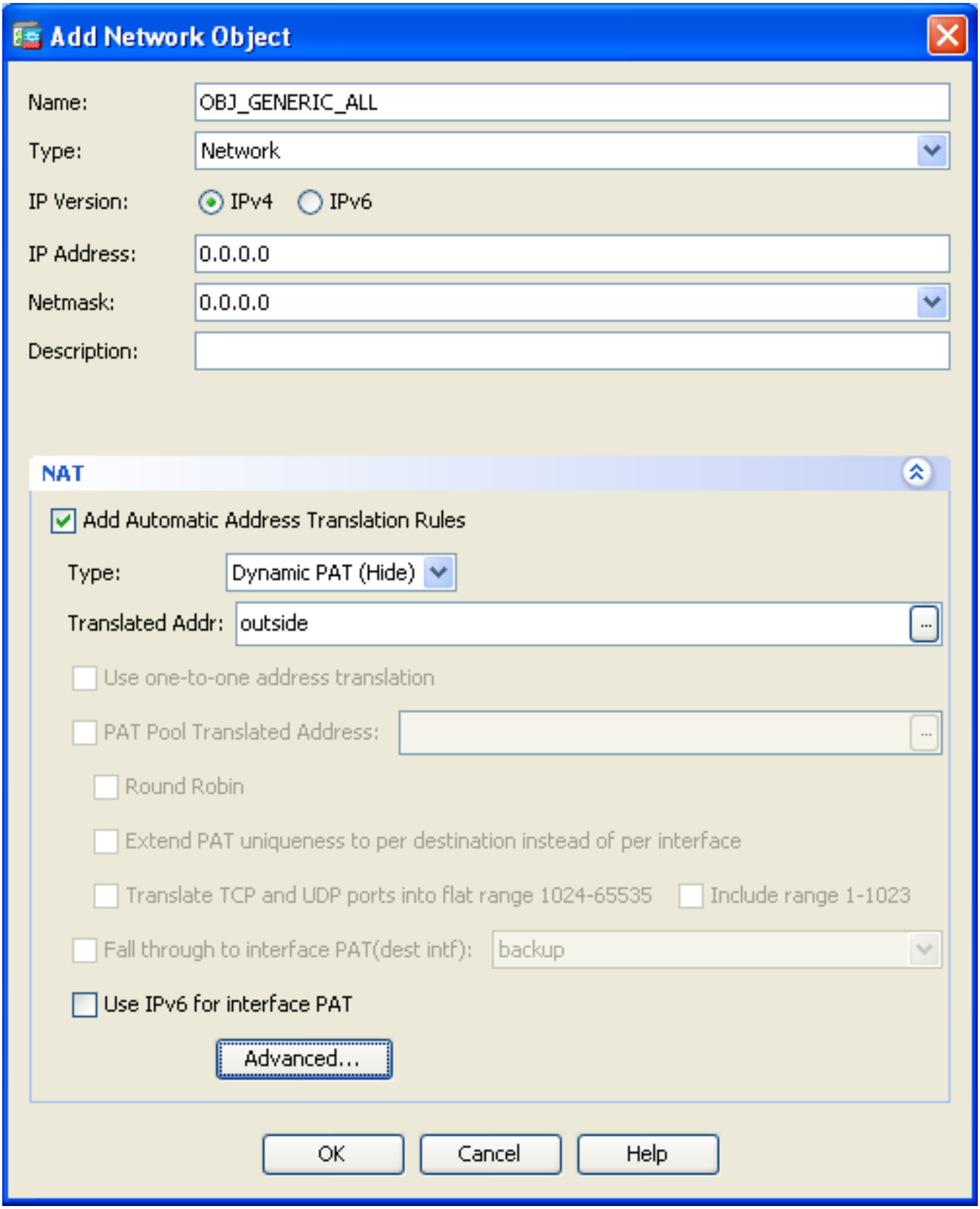


2. Konfigurieren Sie das Netzwerk/den Host/den Bereich, für den die dynamische PAT erforderlich ist. In diesem Beispiel wurden alle internen Subnetze ausgewählt. Dieser Vorgang muss für die spezifischen Subnetze wiederholt werden, die Sie in dieser Weise übersetzen möchten:

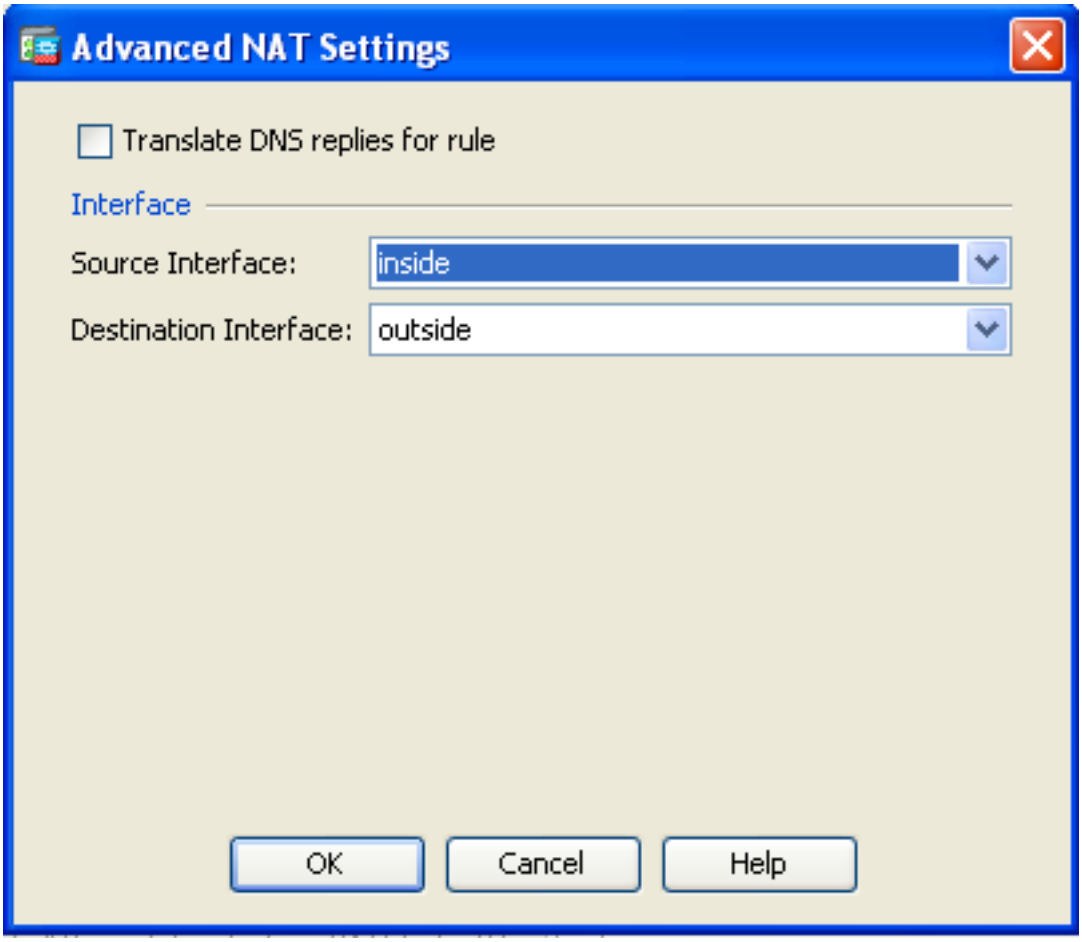


3. Klicken Sie auf **NAT**, aktivieren Sie das Kontrollkästchen **Automatische**

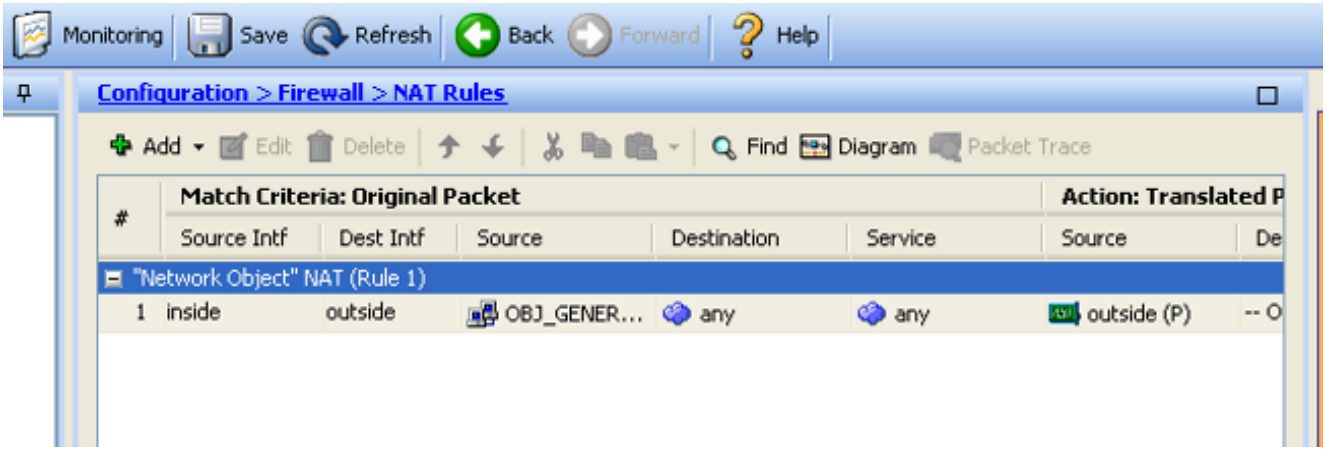
Adressenumwandlungsregel hinzufügen, geben Sie **Dynamic ein** und legen Sie die **Option Translated Addr so fest, dass sie die externe Schnittstelle wiedergibt.** Wenn Sie auf die Schaltfläche mit den Auslassungszeichen klicken, können Sie ein vorkonfiguriertes Objekt auswählen, z. B. die externe Schnittstelle:



4. Klicken Sie auf **Erweitert**, um eine Quell- und Zielschnittstelle auszuwählen:



5. Klicken Sie auf **OK** und dann auf **Übernehmen**, um die Änderungen anzuwenden. Nach Abschluss dieses Vorgangs zeigt der Adaptive Security Device Manager (ASDM) die NAT-Regel:



Router B-Konfiguration

Die Konfiguration für Router B sieht wie folgt aus:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Überprüfen

Zugreifen auf eine Website über HTTP über einen Webbrowser, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

In diesem Beispiel wird eine Site verwendet, die unter der IP-Adresse *198.51.100.100* gehostet wird. Wenn die Verbindung erfolgreich hergestellt wurde, sind die in den folgenden Abschnitten bereitgestellten Ausgaben in der ASA CLI zu sehen.

Verbindung

Geben Sie den Befehl **show connection address** ein, um die Verbindung zu überprüfen:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

Die ASA ist eine Stateful-Firewall, und der Rückverkehr vom Webserver wird durch die Firewall zugelassen, da er mit einer ***Verbindung*** in der Firewall-Verbindungstabelle übereinstimmt. Der Datenverkehr, der mit einer bereits vorhandenen Verbindung übereinstimmt, wird durch die Firewall zugelassen, ohne durch eine Zugriffskontrollliste (ACL) für die Schnittstelle 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 zeigen den aktuellen Status dieser Verbindung an.

> **Hinweis**: Weitere Informationen zu den Verbindungsflags finden Sie im Cisco Dokument ASA TCP Connection Flags (Verbindungsaufbau und -entfernen).

Fehlerbehebung

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um Konfigurationsprobleme zu beheben.

Syslogs

Geben Sie den Befehl **show log** ein, um die Syslogs anzuzeigen:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 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:192.168.1.5/58799 (203.0.113.2/58799)
```

Die ASA-Firewall erzeugt im Normalbetrieb Syslogs. Die Syslogs sind abhängig von der Protokollierungskonfiguration ausführlich dargestellt. Die Ausgabe zeigt zwei Syslogs, die auf Stufe 6 angezeigt werden, oder die *informative* Ebene.

In diesem Beispiel werden zwei Syslogs generiert. Die erste ist eine Protokollmeldung, die angibt, dass die Firewall eine Übersetzung erstellt hat. Dies ist insbesondere eine dynamische TCP-Übersetzung (PAT). Es gibt die Quell-IP-Adresse und den Port sowie die übersetzte IP-Adresse und den übersetzten Port an, wenn der Datenverkehr von innen zu den externen Schnittstellen verläuft.

Das zweite Syslog gibt an, dass die Firewall eine Verbindung in ihrer Verbindungstabelle für diesen spezifischen Datenverkehr zwischen Client und Server erstellt hat. Wenn die Firewall

konfiguriert wurde, um diesen Verbindungsversuch zu blockieren, oder ein anderer Faktor die Erstellung dieser Verbindung (Ressourceneinschränkungen oder eine mögliche Fehlkonfiguration) behinderte, generiert die Firewall kein Protokoll, das angibt, dass die Verbindung erstellt wurde. Stattdessen wird ein Grund für die Ablehnung der Verbindung oder ein Hinweis auf den Faktor protokolliert, der die Herstellung der Verbindung verhindert hat.

Packet Tracer

Geben Sie den folgenden Befehl ein, um die Funktion der Paketverfolgung zu aktivieren:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 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 Packet Tracer-Funktion auf der ASA können Sie ein *simuliertes* Paket angeben und alle Schritte, Überprüfungen und Funktionen anzeigen, die die Firewall bei der Verarbeitung des Datenverkehrs durchführt. Mit diesem Tool ist es hilfreich, ein Beispiel für den Datenverkehr zu identifizieren, der Ihrer Meinung nach die Firewall passieren darf, und diesen 5-Tupel zu verwenden, um den Datenverkehr zu simulieren. Im vorherigen Beispiel wird der Paket-Tracer verwendet, um einen Verbindungsversuch zu simulieren, der die folgenden Kriterien erfüllt:

- Das simulierte Paket erreicht die interne Schnittstelle.
- Das verwendete Protokoll ist TCP.
- Die simulierte Client-IP-Adresse lautet 192.168.1.5.
- Der Client sendet Datenverkehr, der von Port 1234 stammt.
- Der Datenverkehr ist für einen Server mit der IP-Adresse 198.51.100.100 bestimmt.
- Der Datenverkehr ist für Port 80 bestimmt.

Beachten Sie, dass im Befehl die externe Schnittstelle nicht erwähnt wurde. Dies liegt an der Packet Tracer-Entwicklung. Das Tool erklärt Ihnen, wie die Firewall diesen Verbindungsversuch verarbeitet, einschließlich der Art der Weiterleitung und der Schnittstelle.

> **Tipp**: Weitere Informationen über die Funktion der Paket-Tracer finden Sie im Abschnitt Tracing-Pakete mit Packet Tracer im *Konfigurationsleitfaden zur Cisco Serie ASA 5500 unter Verwendung der CLI, 8.4 und 8.6*.

Erfassung

Geben Sie folgende Befehle ein, um eine Erfassung anzuwenden:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 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 192.168.1.5.58799 > 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 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

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 der Schnittstellen erfassen. Diese Erfassungsfunktion ist fantastisch, da sie definitiv belegen kann, ob der Datenverkehr eine Firewall erreicht oder verlässt. Im vorherigen Beispiel wird die Konfiguration von zwei Aufnahmen mit dem Namen **capin** und **capout** auf der Innen- bzw. der Außenschnittstelle veranschaulicht. Die **Capture-**Befehle verwenden das **match**-Schlüsselwort, mit dem Sie den Datenverkehr angeben können, den Sie erfassen möchten.

Im Capin Capture-Beispiel wird angegeben, dass Sie den Datenverkehr der internen Schnittstelle (ein- oder ausgehend) abgleichen möchten, der mit dem *TCP-Host 192.168.1.5-Host 198.51.100.100 übereinstimmt*. Mit anderen Worten, Sie möchten jeden TCP-Datenverkehr erfassen, der von Host *192.168.1.5* zum Host *198.51.100.100* gesendet wird, oder umgekehrt. Durch die Verwendung des **match-**Schlüsselworts kann die Firewall diesen Datenverkehr bidirektional erfassen. Der für die externe Schnittstelle definierte **Erfassungsbefehl** verweist nicht auf die interne Client-IP-Adresse, da die Firewall PAT für diese Client-IP-Adresse durchführt. Aus diesem Grund können Sie nicht mit dieser Client-IP-Adresse übereinstimmen. Stattdessen wird in diesem Beispiel **jeder** verwendet, um anzugeben, dass alle möglichen IP-Adressen mit dieser Bedingung übereinstimmen.

Nachdem Sie die Captures konfiguriert haben, können Sie erneut versuchen, eine Verbindung herzustellen, und die Captures mit dem Befehl **show capture***<capture_name>* anzeigen. In diesem Beispiel sehen Sie, dass der Client eine Verbindung zum Server herstellen kann, wie der TCP-Drei-Schritte-Handshake zeigt, der in den Captures zu sehen ist.

Zugehörige Informationen

- Cisco Adaptive Security Device Manager
- Cisco Firewalls der nächsten Generation der Serie ASA 5500-X
- Anforderungen für Kommentare (RFC)
- Konfigurationsleitfaden für die CLI der Cisco ASA-Serie, 9,0 â Â Konfigurieren von statischen und Standard-Routen
- Technischer Support und Dokumentation â Â Cisco Systems