Verwendung der NAT- und PAT-Anweisung im Konfigurationsbeispiel für die Cisco Secure ASA Firewall

Inhalt

Einführung

Dieses Dokument enthält Beispiele für grundlegende Network Address Translation (NAT)- und Port Address Translation (PAT)-Konfigurationen auf der Cisco Secure Adaptive Security Appliance (ASA)-Firewall. Dieses Dokument enthält auch vereinfachte Netzwerkdiagramme. Weitere Informationen finden Sie in der ASA-Dokumentation für Ihre ASA-Softwareversion.

Dieses Dokument bietet eine individuelle Analyse Ihres Cisco Geräts.

Weitere Informationen finden Sie in der NAT-Konfiguration auf den Security Appliances der Serien

ASA 5500/5500-X.

Voraussetzungen

Anforderungen

Cisco empfiehlt, die Cisco Secure ASA Firewall kennen zu lernen.

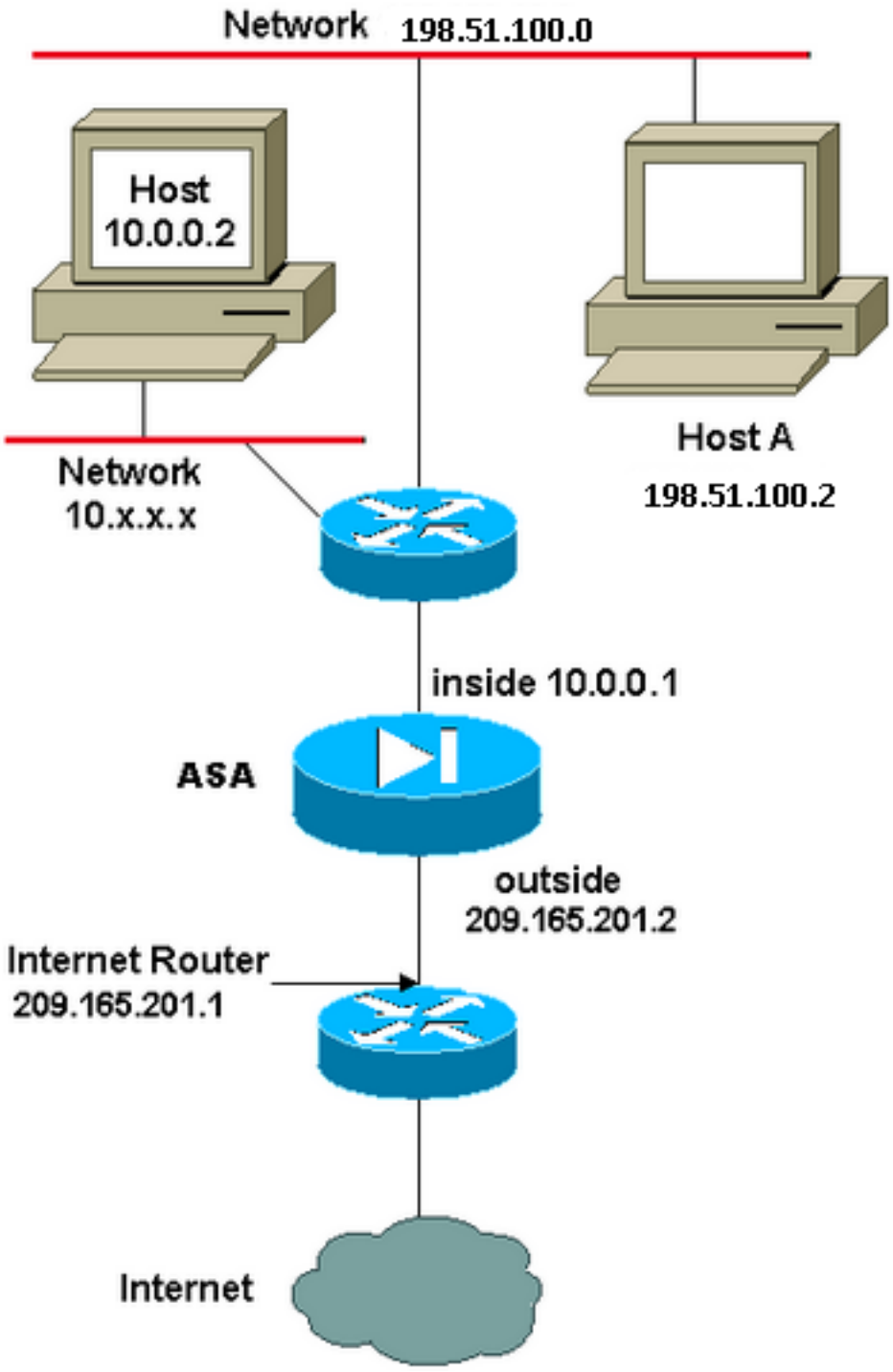
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Secure ASA Firewall Software Version 8.4.2 und höher.

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.

Konfiguration - Mehrere NAT-Anweisungen mit manueller und automatischer NAT

Netzwerkdiagramm



In diesem Beispiel stellt der ISP dem Netzwerkmanager den IP-Adressblock 209.165.201.0/27 zur Verfügung, der zwischen 209.165.201.1 und 209.165.201.30 liegt. Der Netzwerkmanager beschließt, die interne Schnittstelle des Internet-Routers mit dem Wert 209.165.201.1 und die externe Schnittstelle mit dem Wert 209.165.201.2 zu verknüpfen.

Der Netzwerkadministrator verfügt bereits über eine dem Netzwerk zugewiesene Class C-Adresse, 198.51.100.0/24, und einige Workstations verwenden diese Adressen, um auf das Internet zuzugreifen. Diese Workstations erfordern keine Adressübersetzung, da sie bereits gültige Adressen haben. Neue Workstations werden jedoch Adressen im Netzwerk 10.0.0.0/8 zugewiesen und müssen übersetzt werden (da 10.x.x.x einer der nicht routbaren Adressbereiche gemäß RFC 1918 ist.

Um dieses Netzwerkdesign umzusetzen, muss der Netzwerkadministrator zwei NAT-Anweisungen und einen globalen Pool in der ASA-Konfiguration verwenden:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Diese Konfiguration übersetzt keine Quelladresse für ausgehenden Datenverkehr aus dem Netzwerk 198.51.100.0/24. Sie übersetzt eine Quelladresse im Netzwerk 10.0.0.0/8 in eine Adresse zwischen 209.165.201.3 und 209.165.201.30.

> **Hinweis**: Wenn Sie über eine Schnittstelle mit einer NAT-Richtlinie verfügen und kein globaler Pool zu einer anderen Schnittstelle vorhanden ist, müssen Sie nat 0 verwenden, um eine NAT-Ausnahme einzurichten.

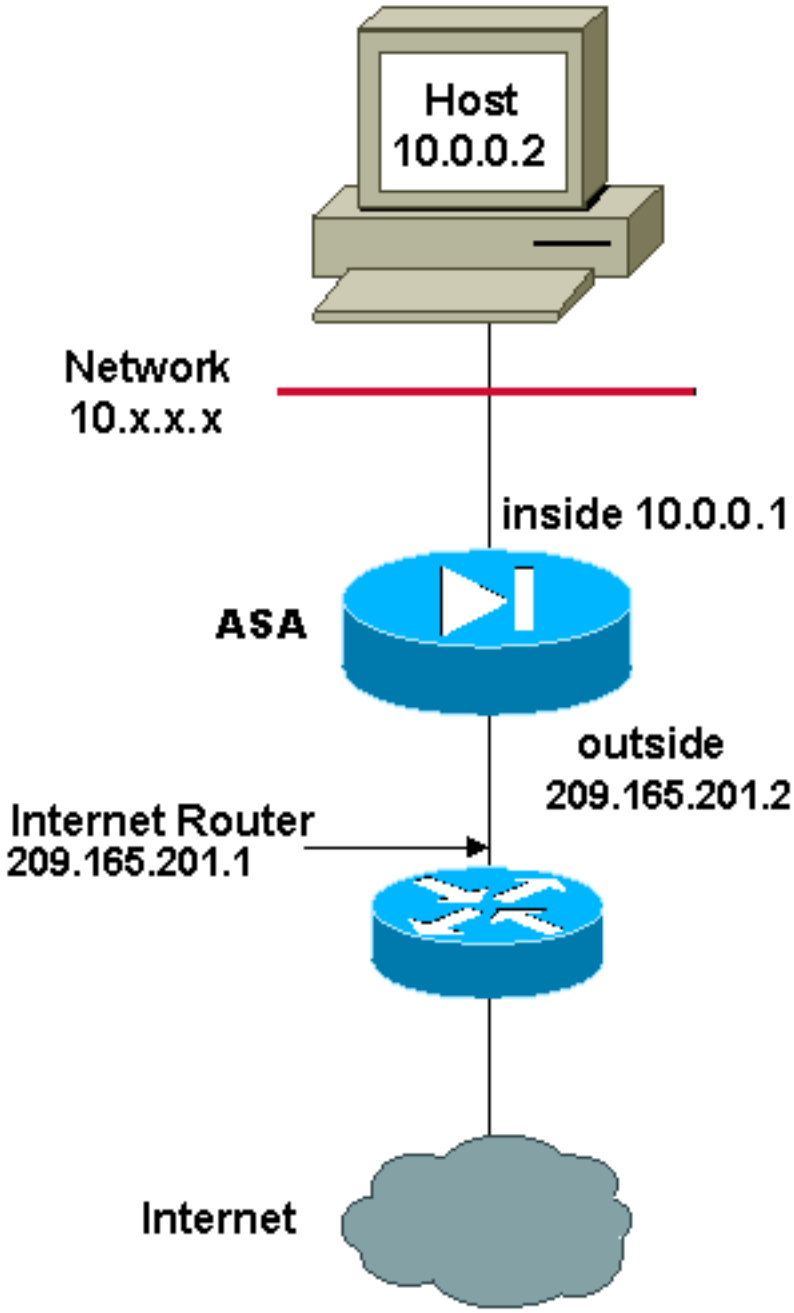
ASA Version 8.3 und höher

Hier ist die Konfiguration.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Konfiguration - Mehrere globale Pools

Netzwerkdiagramm



In diesem Beispiel verfügt der Netzwerkmanager über zwei Bereiche von IP-Adressen, die im Internet registriert sind. Der Netzwerkmanager muss alle internen Adressen im Bereich 10.0.0.0/8 in registrierte Adressen umwandeln. Die IP-Adressen, die der Netzwerkmanager verwenden muss, sind 209.165.201.1 bis 209.165.201.30 und 209.165.200.225 bis 209.165.200.25. 4. Dazu kann der Netzwerkmanager folgende Aufgaben ausführen:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> **Hinweis**: In der NAT-Anweisung wird ein Platzhalter-Adressierungsschema verwendet. Diese Anweisung weist die ASA an, jede interne Quelladresse zu übersetzen, wenn sie ins Internet geht. Die Adresse in diesem Befehl kann bei Bedarf genauer angegeben werden.

ASA Version 8.3 und höher

Hier ist die Konfiguration.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

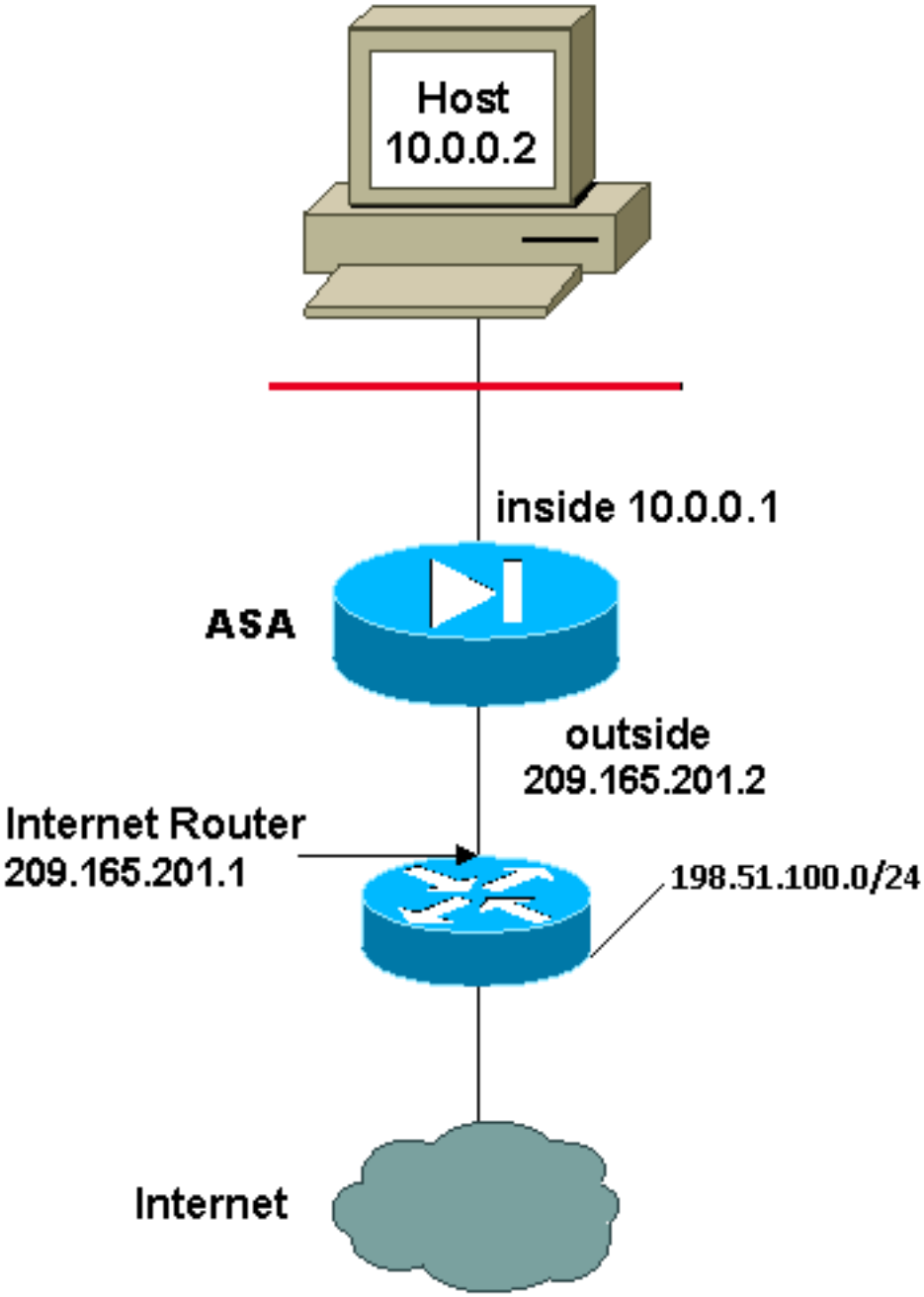
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Konfiguration - Kombination von NAT- und PAT-Anweisungen

Netzwerkdiagramm



In diesem Beispiel stellt der ISP dem Netzwerkmanager einen Adressbereich von 209.165.201.1 bis 209.165.201.30 für das Unternehmen zur Verfügung. Der Netzwerkmanager hat beschlossen, 209.165.201.1 für die interne Schnittstelle auf dem Internet-Router und 209.165.201.2 für die externe Schnittstelle auf der ASA zu verwenden. Sie haben dann die Nummern 209.165.201.3 bis 209.165.201.30, die Sie für den NAT-Pool verwenden können. Dem Netzwerkmanager ist jedoch bekannt, dass es jederzeit mehr als 28 Personen geben kann, die versuchen, die ASA zu verlassen. Der Netzwerkmanager hat beschlossen, 209.165.201.30 als PAT-Adresse zu verwenden, damit mehrere Benutzer gleichzeitig eine Adresse verwenden können.

Diese Befehle weisen die ASA an, die Quelladresse in 209.165.201.3 bis 209.165.201.29 zu übersetzen, damit die ersten 27 internen Benutzer die ASA passieren können. Nachdem diese Adressen ausgeschöpft sind, übersetzt die ASA alle nachfolgenden Quelladressen in 209.165.201.30, bis eine der Adressen im NAT-Pool frei ist.

Hinweis: In der NAT-Anweisung wird ein Platzhalter-Adressierungsschema verwendet. Diese Anweisung weist die ASA an, jede interne Quelladresse zu übersetzen, wenn sie ins Internet

geht. Die Adresse in diesem Befehl kann bei Bedarf genauer angegeben werden.

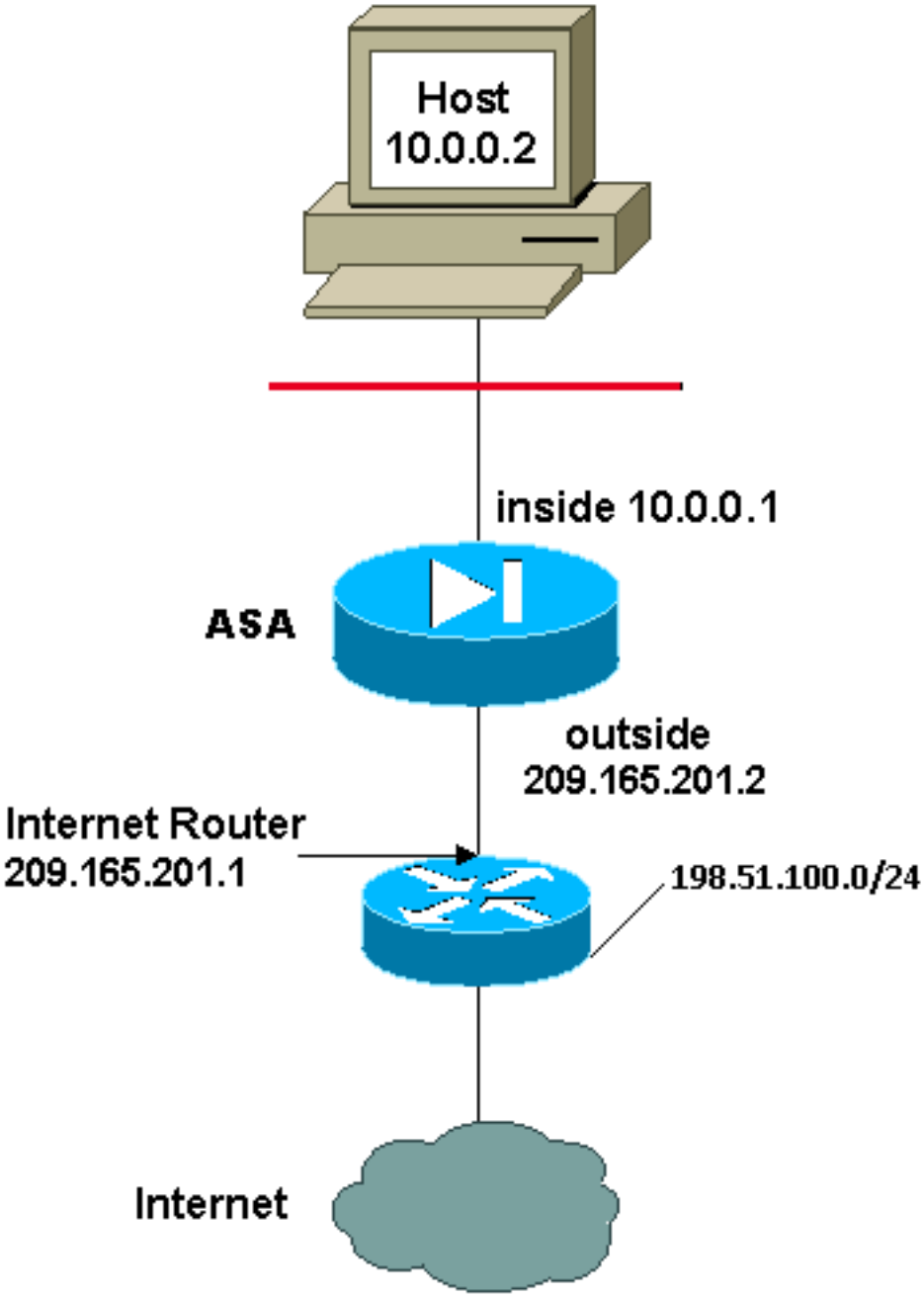
ASA Version 8.3 und höher

Hier ist die Konfiguration.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Konfigurieren - Mehrere NAT-Anweisungen mit manuellen Anweisungen

Netzwerkdiagramm



In diesem Beispiel stellt der ISP dem Netzwerkmanager erneut einen Adressbereich von 209.165.201.1 bis 209.165.201.30 zur Verfügung. Der Netzwerkmanager beschließt, die interne Schnittstelle des Internet-Routers mit dem Wert 209.165.201.1 und die externe Schnittstelle mit dem Wert 209.165.201.2 zuzuweisen.

In diesem Szenario wird jedoch ein anderes privates LAN-Segment vom Internet-Router getrennt. Der Netzwerkmanager verschwendet keine Adressen aus dem globalen Pool, wenn die Hosts in diesen beiden Netzwerken miteinander kommunizieren. Der Netzwerkmanager muss die Quelladresse für alle internen Benutzer (10.0.0.0/8) übersetzen, wenn er ins Internet geht.

Diese Konfiguration übersetzt diese Adressen nicht mit der Quelladresse 10.0.0.0/8 und der Zieladresse 198.51.100.0/24. Sie übersetzt die Quelladresse aus jedem Datenverkehr, der vom Netzwerk 10.0.0.0/8 aus initiiert und für einen anderen Ort als 198.51.100.0/24 bestimmt ist, in eine Adresse zwischen 209.165.201.3 und 209.165.201.30.

Wenn Sie die Ausgabe eines Befehls **zum Schreiben von Terminals** von Ihrem Cisco Gerät haben, können Sie das Output Interpreter Tool (nur registrierte Kunden) verwenden.

ASA Version 8.3 und höher

Hier ist die Konfiguration.

Using the Manual Nat statements:

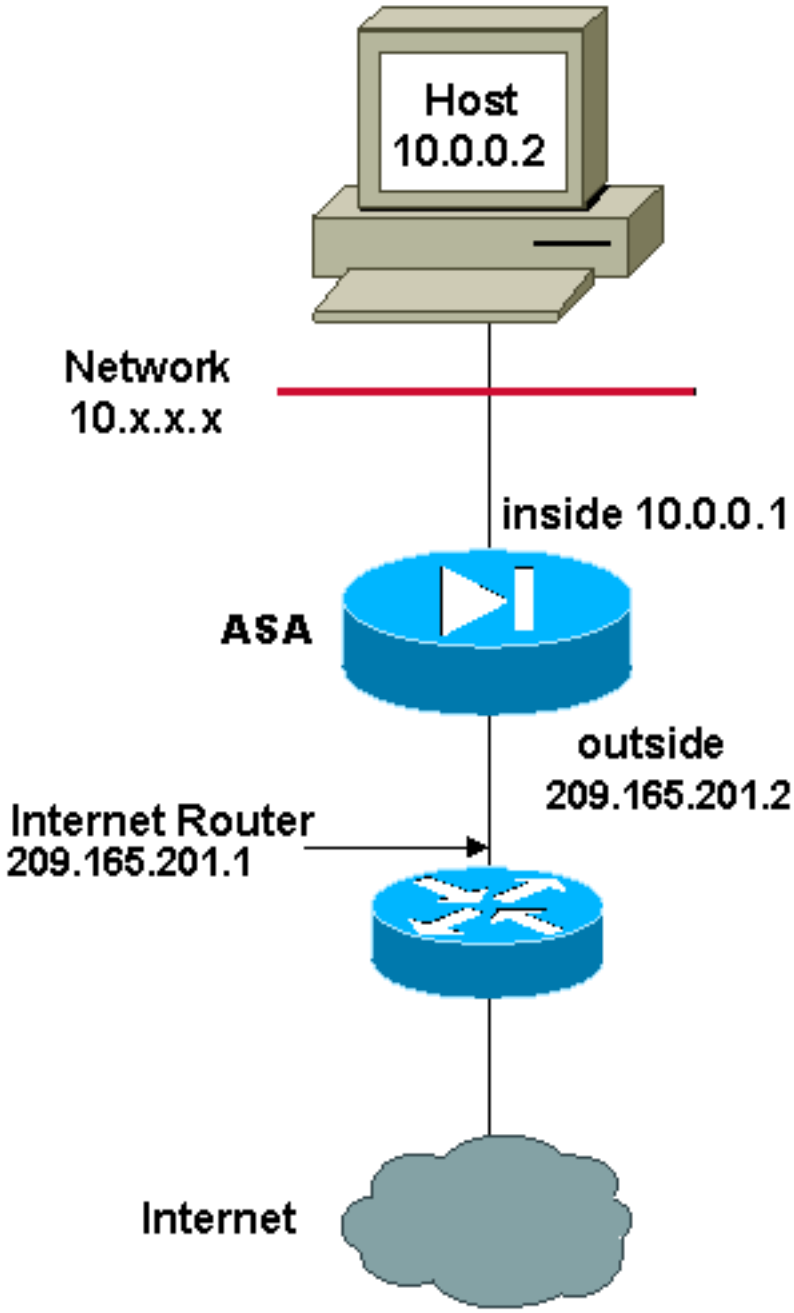
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Konfigurieren - Verwenden von Richtlinie NAT

Netzwerkdiagramm



Wenn Sie eine Zugriffsliste mit dem Befehl **nat** für eine andere NAT-ID als 0 verwenden, aktivieren Sie die Richtlinie NAT.

Policy NAT ermöglicht Ihnen die Identifizierung des lokalen Datenverkehrs zur Adressenübersetzung anhand der Angabe der Quell- und Zieladressen (oder Ports) in einer Zugriffsliste. Die reguläre NAT verwendet nur Quelladressen/Ports. Die Richtlinien-NAT verwendet sowohl Quell- als auch Zieladressen/-ports.

> **Hinweis**: Alle Typen von NAT-Support-Richtlinien mit Ausnahme der NAT-Ausnahme (Access-List der Nat 0). Bei der NAT-Ausnahme wird eine Zugriffskontrollliste (ACL) verwendet, um lokale Adressen zu identifizieren. Sie unterscheidet sich jedoch von der Richtlinie-NAT, da die Ports nicht berücksichtigt werden.

Mit Policy NAT können Sie mehrere NAT- oder statische Anweisungen erstellen, die dieselbe lokale Adresse identifizieren, solange die Kombination aus Quelle, Port und Ziel/Port für jede Anweisung eindeutig ist. Anschließend können Sie verschiedenen globalen Adressen für jedes Quell-/Port- und Ziel-/Port-Paar zuordnen.

In diesem Beispiel muss der Netzwerkmanager den Zugriff für die Ziel-IP-Adresse 172.30.1.11 für Port 80 (Web) und Port 23 (Telnet) bereitstellen, jedoch zwei verschiedene IP-Adressen als Quelladresse verwenden. 209.165.201.3 wird als Quelladresse für das Internet verwendet, und 209.165.201.4 wird für Telnet verwendet und muss alle internen Adressen im Bereich 10.0.0.0/8 konvertieren. Dazu kann der Netzwerkmanager folgende Aufgaben ausführen:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA Version 8.3 und höher

Hier ist die Konfiguration.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> **Hinweis**: Weitere Informationen zur Konfiguration von NAT und PAT auf ASA Version 8.4 finden Sie unter Informationen zu NAT.
>
> Weitere Informationen zur Konfiguration von Zugriffslisten auf ASA Version 8.4 finden Sie unter Informationen zu Zugriffslisten.

Überprüfen

Versuchen Sie, über HTTP mit einem Webbrowser auf eine Website zuzugreifen. In diesem

Beispiel wird eine Site verwendet, die unter 198.51.100.100 gehostet wird. Wenn die Verbindung erfolgreich hergestellt wurde, wird die Ausgabe im nächsten Abschnitt in der ASA CLI angezeigt.

Verbindung

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
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. Datenverkehr, der mit einer bereits vorhandenen Verbindung übereinstimmt, wird durch die Firewall zugelassen, ohne durch eine 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 zeigen den aktuellen Status dieser Verbindung an. Weitere Informationen zu Verbindungsflags finden Sie in den ASA TCP-Verbindungsflags.

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 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:10.0.0.2/57431 (209.165.201.3/57431)
```

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

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). 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 für diesen spezifischen Datenverkehr zwischen Client und Server eine **Verbindung** in der Verbindungstabelle erstellt hat. Wenn die Firewall konfiguriert wurde, um diesen Verbindungsversuch zu blockieren, oder ein anderer Faktor die Erstellung dieser Verbindung behinderte (Ressourcenbeschränkungen oder eine mögliche Fehlkonfiguration), würde die Firewall kein Protokoll generieren, das angibt, dass die Verbindung hergestellt wurde. Stattdessen wird ein Grund für die Ablehnung der Verbindung oder ein Hinweis darauf angegeben, welcher Faktor die Verbindung verhindert.

NAT-Übersetzungen (Xlate)

```
ASA(config)# show xlate local 10.0.0.2
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

Im Rahmen dieser Konfiguration wird PAT so konfiguriert, dass die internen Host-IP-Adressen in Adressen übersetzt werden, die im Internet routbar sind. Um zu bestätigen, dass diese Übersetzungen erstellt wurden, können Sie die Tabelle "Übersetzung" überprüfen. Der Befehl **show xlate** zeigt in Kombination mit dem **lokalen** Schlüsselwort und der IP-Adresse des internen Hosts alle Einträge, die in der Übersetzungstabelle für diesen Host enthalten sind. Die vorherige Ausgabe zeigt, dass für diesen Host derzeit eine Übersetzung zwischen der internen und der externen Schnittstelle erstellt wird. Die interne Host-IP-Adresse und der interne Port werden pro Konfiguration in die Adresse 10.165.200.226 übersetzt.

Die aufgeführten Flags **r i** ,geben an, dass die Übersetzung **dynamisch** und **portmap** ist. Weitere Informationen zu verschiedenen NAT-Konfigurationen finden Sie in Information About NAT.

Fehlerbehebung

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