Konfigurieren der Network Address Translation und der ACLs auf einer ASA-Firewall

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Network Address Translation (NAT) und Access Control Lists (ACLs) auf einer ASA-Firewall konfiguriert werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer ASA-Firewall der Serie 5510, die mit dem ASA-Code der Version 9.1(1) ausgeführt wird.

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

In diesem Dokument wird ein einfaches Beispiel für die Konfiguration von NAT und ACLs auf einer ASA-Firewall beschrieben, um sowohl ausgehende als auch eingehende Verbindungen zu ermöglichen. Sie wurde mit einer ASA 5510-Firewall (Adaptive Security Appliance) entwickelt, die den ASA-Code Version 9.1(1) nicht unterstützt. Dies kann jedoch problemlos auf jede andere ASA-Firewall-Plattform angewendet werden. Wenn Sie eine Plattform wie ASA 5505 verwenden, die VLANs anstelle einer physischen Schnittstelle verwendet, müssen Sie die Schnittstellentypen entsprechend ändern.

Überblick

Ziele

In dieser Beispielkonfiguration können Sie untersuchen, welche NAT- und ACL-Konfigurationen erforderlich sind, um eingehenden Zugriff auf einen Webserver in der DMZ einer ASA-Firewall und ausgehende Verbindungen von internen und DMZ-Hosts zu ermöglichen. Zusammenfassend erreichen Sie mit dieser Konfiguration zwei Ziele:

1. Sie erlauben internen Hosts und DMZ die ausgehende Konnektivität mit dem Internet.
2. Sie ermöglichen Hosts im Internet den Zugriff auf einen Webserver in der DMZ mit der IP-Adresse 192.168.1.100.

Bevor Sie die erforderlichen Schritte durchführen, um diese beiden Ziele zu erreichen, wird in diesem Dokument kurz die Funktionsweise von ACLs und NAT für die neueren Versionen von ASA-Code (Version 8.3 und höher) erläutert.

Übersicht über Zugriffskontrolllisten (Access Control Lists, ACLs)

Zugriffskontrolllisten (kurz „Zugriffslisten“ oder „ACLs“) sind die Methode, mit der die ASA-Firewall bestimmt, ob Datenverkehr zugelassen oder verweigert wird. Standardmäßig wird Datenverkehr von einer niedrigeren zu einer höheren Sicherheitsstufe abgelehnt. Dies kann durch eine ACL überschrieben werden, die auf diese niedrigere Sicherheitsschnittstelle angewendet wird. Außerdem lässt die ASA standardmäßig Datenverkehr von höheren zu niedrigeren Sicherheitsschnittstellen zu. Dieses Verhalten kann ebenfalls mit einer ACL außer Kraft gesetzt werden.

In früheren Versionen des ASA-Codes (8.2 und früher) verglich die ASA eine eingehende Verbindung oder ein eingehendes Paket mit der ACL auf einer Schnittstelle, ohne zuerst die Übersetzung des Pakets aufzuheben. Mit anderen Worten, die ACL musste das Paket zulassen, als ob Sie dieses Paket auf der Schnittstelle erfassen würden. Bei dem Code der Version 8.3 und höher hebt die ASA die Übersetzung dieses Pakets auf, bevor sie die Schnittstellen-ACLs überprüft. Dies bedeutet, dass bei dem Code ab Version 8.3 und in diesem Dokument der Datenverkehr zur tatsächlichen IP des Hosts zulässig ist und nicht zur übersetzten IP des Hosts.

Weitere Informationen zu Zugriffskontrolllisten finden Sie im Abschnitt Configuring Access Rules in Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1.

NAT-Übersicht

Die Netzwerkadressübersetzung (Network Address Translation, kurz „NAT“) ist auf der ASA in Version 8.3 und höher in zwei Typen unterteilt: Automatische NAT (Objekt-NAT) und Manuelle NAT (Doppelte NAT). Der erste der beiden Typen (Objekt-NAT) wird innerhalb der Definition eines Netzwerkobjekts konfiguriert. Ein Beispiel hierfür finden Sie weiter unten in diesem Dokument. Ein wichtiger Vorteil dieser NAT-Methode ist, dass die ASA automatisch die Regeln für die Verarbeitung sortiert, um Konflikte zu vermeiden. Dies ist die einfachste Form von NAT, aber diese Einfachheit bringt auch Einbußen bei der Feinabstimmung der Konfiguration mit sich. Beispiel: Sie können keine Übersetzungsentscheidung basierend auf dem Ziel im Paket treffen, wie dies beim zweiten NAT-Typ der manuellen NAT der Fall ist. Die manuelle NAT bietet eine höhere Genauigkeit, erfordert jedoch, dass die Zeilen in der richtigen Reihenfolge konfiguriert werden, damit das richtige Verhalten erreicht wird. Dieser NAT-Typ wird dadurch kompliziert und kann daher in diesem Konfigurationsbeispiel nicht verwendet werden.

Weitere Informationen zu NAT finden Sie im Abschnitt Informationen zu NAT in Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1.

Konfigurieren

Jetzt durchstarten

Die grundlegende Konfiguration der ASA besteht aus drei Schnittstellen, die mit drei Netzwerksegmenten verbunden sind. Das ISP-Netzwerksegment ist mit der Ethernet0/0-Schnittstelle verbunden und als außen mit der Sicherheitsstufe 0 gekennzeichnet. Das interne Netzwerk wurde mit Ethernet0/1 verbunden und als innen mit einer Sicherheitsstufe von 100 gekennzeichnet. Das DMZ-Segment, in dem sich der Webserver befindet, ist mit Ethernet0/2 verbunden und als DMZ mit der Sicherheitsstufe 50 gekennzeichnet.

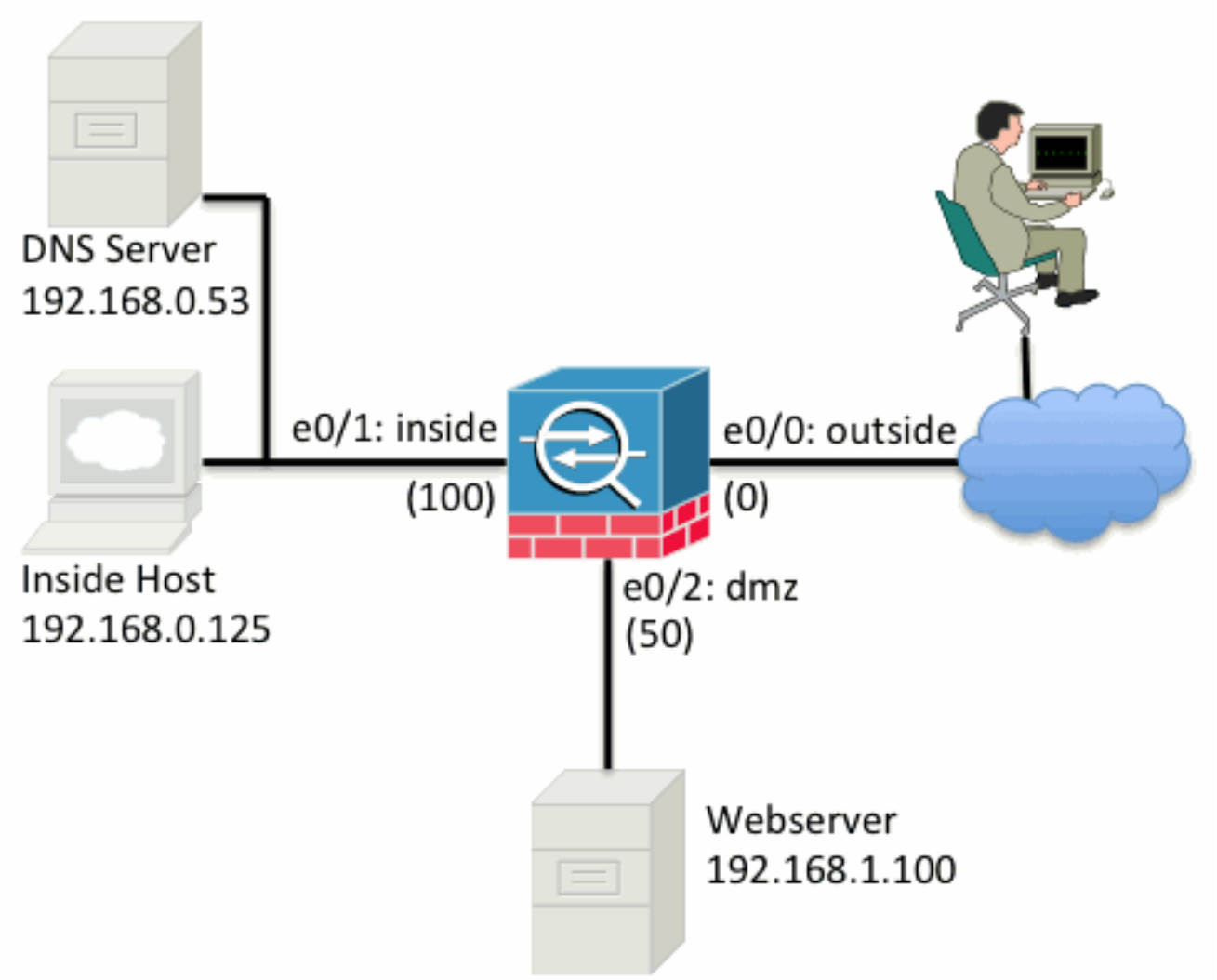
Die Schnittstellenkonfiguration und die IP-Adressen für das Beispiel finden Sie hier:

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

Hier sehen Sie, dass die innere Schnittstelle der ASA auf die IP-Adresse 192.168.0.1 eingestellt ist und als Standardgateway für die internen Hosts fungiert. Die äußere Schnittstelle der ASA wird mit einer vom ISP bezogenen IP-Adresse konfiguriert. Es gibt eine Standardroute, die das ISP-Gateway als nächsten Hop festlegt. Wenn Sie DHCP verwenden, wird dies automatisch bereitgestellt. Die DMZ-Schnittstelle ist mit der IP-Adresse 192.168.1.1 konfiguriert und fungiert als Standardgateway für Hosts im DMZ-Netzwerksegment.

Topologie

Hier finden Sie einen grafischen Überblick über die Verkabelung und Konfiguration:



Schritt 1: NAT so konfigurieren, dass Hosts Zugang zum Internet erhalten

In diesem Beispiel wird Object NAT, auch als AutoNAT bezeichnet, verwendet. Zuerst müssen die NAT-Regeln konfiguriert werden, die es den Hosts im Inneren und den DMZ-Segmenten ermöglichen, eine Verbindung zum Internet herzustellen. Da diese Hosts private IP-Adressen verwenden, müssen Sie sie in etwas übersetzen, das im Internet routingfähig ist. Übersetzen Sie in diesem Fall die Adressen so, dass sie wie die äußere Schnittstellen-IP-Adresse der ASA aussehen. Wenn sich Ihre externe IP häufig ändert (möglicherweise aufgrund von DHCP), ist dies die einfachste Möglichkeit, dies einzurichten.

Um diese NAT zu konfigurieren, müssen Sie ein Netzwerkobjekt erstellen, das sowohl das innere Subnetz als auch das DMZ-Subnetz darstellt. Konfigurieren Sie in jedem dieser Objekte eine dynamische NAT-Regel, die die Port-Adressumwandlung (PAT) dieser Clients beim Übergang von ihren jeweiligen Schnittstellen zur externen Schnittstelle unterstützt.

Diese Konfiguration ähnelt der folgenden:

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
```

```
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

Wenn Sie sich die aktuelle Konfiguration an dieser Stelle (mit der Ausgabe des Befehls show run) ansehen, sehen Sie, dass die Objektdefinition in zwei Teile der Ausgabe aufgeteilt ist. Der erste Teil gibt nur an, was sich im Objekt befindet (Host/Subnetz, IP-Adresse usw.), während der zweite Abschnitt zeigt, dass die NAT-Regel an dieses Objekt gebunden ist. Wenn Sie den ersten Eintrag in der vorherigen Ausgabe verwenden:

Wenn Hosts, die mit dem Subnetz 192.168.0.0/24 übereinstimmen, von der inneren Schnittstelle zur äußeren Schnittstelle wechseln, sollen sie dynamisch in die äußere Schnittstelle übersetzt werden.

Schritt 2: NAT für den Zugriff auf den Webserver über das Internet konfigurieren

Jetzt, da die Hosts im Inneren und die DMZ-Schnittstellen auf das Internet zugreifen können, müssen Sie die Konfiguration so ändern, dass Benutzer im Internet auf unseren Webserver am TCP-Port 80 zugreifen können. In diesem Beispiel ist das System so eingerichtet, dass sich Personen im Internet mit einer anderen vom ISP bereitgestellten IP-Adresse verbinden können, einer zusätzlichen IP-Adresse, die wir *besitzen*. Verwenden Sie für dieses Beispiel 198.51.100.101. Mit dieser Konfiguration können Benutzer im Internet den DMZ-Webserver über den TCP-Port 80 auf 198.51.100.101 zugreifen. Verwenden Sie für diese Aufgabe Object NAT, und die ASA kann TCP-Port 80 auf dem Webserver (192.168.1.100) so übersetzen, dass er auf TCP-Port 80 außen wie 198.51.100.101 aussieht. Ähnlich wie zuvor können Sie ein Objekt und Übersetzungsregeln für dieses Objekt definieren. Definieren Sie auch ein zweites Objekt, um die IP darzustellen, in die Sie diesen Host übersetzen können.

Diese Konfiguration ähnelt der folgenden:

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

Die Bedeutung dieser NAT-Regel in diesem Beispiel lässt sich kurz zusammenfassen:

Wenn ein Host, der mit der IP-Adresse 192.168.1.100 in den DMZ-Segmenten übereinstimmt, eine Verbindung herstellt, die vom TCP-Port 80 (www) ausgeht, und diese Verbindung die äußere Schnittstelle verlässt, soll dies in TCP-Port 80 (www) auf der äußeren Schnittstelle und die IP-Adresse in 198.51.100.101 übersetzt werden.

Das scheint etwas seltsam... "von TCP-Port 80 (www) bezogen", aber Web-Datenverkehr ist für Port 80 bestimmt. Es ist wichtig zu verstehen, dass diese NAT-Regeln bidirektional sind. Infolgedessen können Sie die Formulierung umdrehen, um diesen Satz neu zu formulieren. Das Ergebnis ergibt viel mehr Sinn:

Wenn Hosts an der Außenseite eine Verbindung mit 198.51.100.101 an dem Ziel-TCP-Port 80 (www) herstellen, können Sie die Ziel-IP-Adresse in 192.168.1.100 und den Ziel-Port in TCP-Port 80 (www) umwandeln und an die DMZ senden.

Es ergibt mehr Sinn, wenn es so formuliert wird. Als Nächstes müssen Sie die ACLs einrichten.

Schritt 3: Konfigurieren von ACLs

NAT ist konfiguriert und diese Konfiguration ist nahezu abgeschlossen. Denken Sie daran, dass Sie mit ACLs auf der ASA das Standardsicherheitsverhalten wie folgt überschreiben können:

- Datenverkehr von einer Schnittstelle mit niedrigerer Sicherheit wird verweigert, wenn er an eine Schnittstelle mit höherer Sicherheit weitergeleitet wird.
- Datenverkehr, der von einer Schnittstelle mit höherer Sicherheit stammt, ist zulässig, wenn er zu einer Schnittstelle mit niedrigerer Sicherheit geleitet wird.

Ohne das Hinzufügen von ACLs zur Konfiguration funktioniert dieser Datenverkehr im Beispiel also wie folgt:

- Hosts im Inneren (Sicherheitsstufe 100) können sich mit Hosts in der DMZ (Sicherheitsstufe 50) verbinden.
- Hosts im Inneren (Sicherheitsstufe 100) können sich mit äußeren Hosts (Sicherheitsstufe 0) verbinden.
- Hosts in der DMZ (Sicherheitsstufe 50) können sich mit äußeren Hosts (Sicherheitsstufe 0) verbinden.

Dieser Datenverkehr wird jedoch abgelehnt:

- Äußere Hosts (Sicherheitsstufe 0) können keine Verbindung zu Hosts im Inneren (Sicherheitsstufe 100) herstellen.
- Äußere Hosts (Sicherheitsstufe 0) können keine Verbindung zu Hosts in der DMZ (Sicherheitsstufe 50) herstellen.
- Hosts in der DMZ (Sicherheitsstufe 50) können keine Verbindung zu Hosts im Inneren (Sicherheitsstufe 100) herstellen.

Da der Datenverkehr von außen zum DMZ-Netzwerk von der ASA mit der aktuellen Konfiguration abgelehnt wird, können Benutzer im Internet den Webserver trotz der NAT-Konfiguration in Schritt 2 nicht erreichen. Sie müssen diesen Datenverkehr explizit zulassen. Im Code der Version 8.3 und höher müssen Sie die tatsächliche IP des Hosts in der ACL und nicht die übersetzte IP verwenden. Das bedeutet, dass die Konfiguration den für 192.168.1.100 bestimmten Verkehr zulassen muss und NICHT den für 198.51.100.101 bestimmten Verkehr an Port 80. Der Einfachheit halber können die in Schritt 2 definierten Objekte auch für diese ACL verwendet werden. Sobald die ACL erstellt wurde, müssen Sie sie in eingehender Richtung auf die äußere Schnittstelle anwenden.

Die Konfigurationsbefehle sehen wie folgt aus:

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

Die Zeile der Zugriffsliste lautet wie folgt:

Erlauben Sie Datenverkehr von jedem (any (where)) zu dem Host, der durch den Objekt-Webserver (192.168.1.100) an Port 80 dargestellt wird.

Es ist wichtig, dass die Konfiguration hier das Schlüsselwort any verwendet. Da die Quell-IP-Adresse von Clients nicht bekannt ist, wenn sie Ihre Website erreicht, geben Sie „any“ an, was

„eine beliebige IP-Adresse“ bedeutet.

Was ist mit dem Datenverkehr aus dem DMZ-Segment, der für Hosts im inneren Netzwerksegment bestimmt ist? Beispiel: Ein Server im inneren Netzwerk, mit dem sich die Hosts in der DMZ verbinden müssen. Wie kann die ASA nur diesen spezifischen Datenverkehr zulassen, der für den inneren Server bestimmt ist, und alles andere blockieren, das für das innere Segment aus der DMZ bestimmt ist?

In diesem Beispiel wird angenommen, dass sich im inneren Netzwerk unter der IP-Adresse 192.168.0.53 ein DNS-Server befindet, auf den die Hosts in der DMZ für die DNS-Auflösung zugreifen müssen. Sie erstellen die erforderliche ACL und wenden sie auf die DMZ-Schnittstelle an, damit die ASA dieses eingangs erwähnte Standardsicherheitsverhalten für Datenverkehr überschreiben kann, der über diese Schnittstelle eingeht.

Die Konfigurationsbefehle sehen wie folgt aus:

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

Die ACL ist komplexer als nur den Datenverkehr zum DNS-Server an UDP-Port 53 zuzulassen. Wenn wir nur diese erste Zulässigkeitsleitung verwenden würden, würde der gesamte Datenverkehr von der DMZ zu Hosts im Internet blockiert. ACLs enthalten ganz unten die implizite Anweisung „deny ip any any“. Infolgedessen wären Ihre DMZ-Hosts nicht in der Lage, sich mit dem Internet zu verbinden. Obwohl Datenverkehr von der DMZ nach außen standardmäßig zulässig ist, sind bei Anwendung einer ACL auf die DMZ-Schnittstelle diese sicherheitsbezogenen Standardverhaltensweisen für die DMZ-Schnittstelle nicht mehr wirksam, und Sie müssen den Datenverkehr in der Schnittstellen-ACL explizit zulassen.

Schritt 4: Testkonfiguration mit der Packet Tracer-Funktion

Nachdem die Konfiguration abgeschlossen ist, müssen Sie sie testen, um sicherzustellen, dass sie funktioniert. Die einfachste Methode ist die Verwendung von tatsächlichen Hosts (falls es sich um Ihr Netzwerk handelt). Um dies jedoch über die CLI zu testen und einige der ASA-Tools genauer zu erkunden, verwenden Sie den Packet Tracer, um festgestellte Probleme zu testen und möglicherweise zu debuggen.

Der Packet Tracer simuliert ein Paket basierend auf einer Reihe von Parametern und fügt dieses Paket in den Schnittstellendatenpfad ein, ähnlich wie ein echtes Paket, wenn es aus der Übertragung abgerufen würde. Dieses Paket wird durch die unzähligen Prüfungen und Prozesse verfolgt, die durchgeführt werden, während es die Firewall passiert, und der Packet Tracer notiert das Ergebnis. Simulieren Sie den internen Host, der sich mit einem Host im Internet verbindet. Dieser Befehl weist die Firewall an,

Simulieren eines TCP-Pakets, das über die innere Schnittstelle von der IP-Adresse 192.168.0.125 an Quellport 12345 eingeht und für die IP-Adresse 203.0.113.1 an Port 80 bestimmt ist.

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80
```

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, 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
```

Das Endergebnis ist, dass der Datenverkehr zugelassen wird, was bedeutet, dass er alle NAT- und ACL-Prüfungen in der Konfiguration bestanden hat und über die Egress-Schnittstelle nach außen gesendet wurde. Beachten Sie, dass das Paket in Phase 3 übersetzt wurde und die Details dieser Phase zeigen, welche Regel betroffen ist. Der Host 192.168.0.125 wird je nach Konfiguration dynamisch in 198.51.100.100 übersetzt.

Führen Sie das Ganze jetzt für eine Verbindung vom Internet zum Webserver aus. Denken Sie daran, dass Hosts im Internet auf den Webserver zugreifen können, indem sie sich mit 198.51.100.101 an der externen Schnittstelle verbinden. Ähnlich wie zuvor bewirkt dieser nächste Befehl folgenden Vorgang:

Simulieren eines TCP-Pakets, das über die äußere Schnittstelle von der IP-Adresse 192.0.2.123 an Quellport 12345 eingeht und für die IP-Adresse 198.51.100.101 an Port 80 bestimmt ist.

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
```

```
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

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

Auch dies hat zur Folge, dass das Paket zugelassen wird. Die Zugriffskontrolllisten werden ausgecheckt, die Konfiguration wird einwandfrei angezeigt, und Benutzer im Internet (außerhalb) können über die externe IP-Adresse auf diesen Webserver zugreifen.

Überprüfung

In „Schritt 4 – Testen der Konfiguration mit der Packet Tracer-Funktion“ sind Verifizierungsverfahren enthalten.

Fehlerbehebung

Derzeit sind keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Schlussfolgerung

Die Konfiguration einer ASA für grundlegende NAT ist keine allzu schwierige Aufgabe. Das Beispiel in diesem Dokument kann an Ihr spezifisches Szenario angepasst werden, wenn Sie die in den Beispielkonfigurationen verwendeten IP-Adressen und Ports ändern. Die endgültige ASA-Konfiguration für diese Kombination sieht ähnlich aus wie die folgende für eine ASA 5510:

```
ASA Version 9.1(1)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Auf einer ASA 5505 beispielsweise, bei der die Schnittstellen wie zuvor gezeigt verbunden sind (außen verbunden mit Ethernet0/0, innen verbunden mit Ethernet0/1 und die DMZ verbunden mit Ethernet0/2):

```
ASA Version 9.1(1)
!
interface Ethernet0/0
description Connected to Outside Segment
switchport access vlan 2
!
interface Ethernet0/1
description Connected to Inside Segment
switchport access vlan 1
!
interface Ethernet0/2
description Connected to DMZ Segment
switchport access vlan 3
!
```

```
interface Vlan2
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

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.