Netwerkadresomzetting en ACL's op een ASA-firewall configureren

Inhoud

Inleiding

Dit document beschrijft hoe u de netwerkadresomzetting (NAT) en toegangscontrolelijsten (ACL's) op een ASA-firewall kunt configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Deze informatie is gebaseerd op een ASA 5510 firewall met ASA-code versie 9.1(1).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft een eenvoudig en eenvoudig voorbeeld van hoe u NAT en ACL's kunt configureren op een ASA-firewall om zowel uitgaande als inkomende connectiviteit mogelijk te maken. Het is geschreven met een adaptieve security applicatie (ASA) 5510 firewall dan ASA code versie 9.1(1), maar dit kan gemakkelijk van toepassing zijn op elk ander ASA firewall-platform. Als u een platform zoals een ASA 5505 gebruikt, met VLAN's in plaats van een fysieke interface, moet u de interfacetypen zo nodig wijzigen.

Overzicht

Doelen

In deze voorbeeldconfiguratie kunt u bekijken welke NAT- en ACL-configuraties nodig zijn om inkomende toegang tot een webserver in de DMZ van een ASA-firewall mogelijk te maken en uitgaande connectiviteit van interne en DMZ-hosts toe te staan. Dit kan worden omschreven in twee doelen:

1. Sta hosts intern en in de DMZ uitgaande verbinding met het internet toe.
2. Sta hosts op het internet toegang tot een webserver in de DMZ met IP-adres 192.168.1.100 toe.

Alvorens u de stappen uitvoert die moeten worden voltooid om deze twee doelstellingen te verwezenlijken, gaat dit document kort over de manier ACLs en het werk NAT aan de nieuwere versies van ASA code (versie 8.3 en later).

Overzicht van toegangscontrolelijsten

Toegangscontrolelijsten (ook wel toegangslijsten of ACL's) zijn de methode waarmee de ASA-firewall bepaalt of verkeer wordt geaccepteerd of geweigerd. Verkeer dat van een lager naar een hoger security niveau gaat wordt standaard geweigerd. Dit kan worden gewijzigd met een ACL die op die lagere security interface wordt toegepast. Bovendien staat de ASA verkeer van hogere naar lagere security interfaces standaard toe. Ook dit gedrag kan met een ACL worden gewijzigd.

In eerdere versies van ASA-code (8.2 en lager) vergeleek de ASA een inkomende verbinding of inkomend pakket met de ACL op een interface zonder het pakket eerst terug te zetten. Met andere woorden: de ACL moest het pakket toelaten alsof u het pakket als zodanig op de interface moet vastleggen. In versie 8.3 en hoger zet de ASA dit pakket terug voordat deze de interface-ACL's controleert. Dit betekent dat in versie 8.3 en hoger, en dit document, verkeer naar het daadwerkelijke IP-adres van de host wordt toegestaan en niet naar het omgezette IP-adres van de host.

Zie de sectie Toegangsregels configureren van Boek 2: Cisco ASA Series firewall CLI-configuratiehandleiding, 9.1 voor meer informatie over ACL's.

Overzicht van NAT

NAT op de ASA in versie 8.3 en hoger wordt onderverdeeld in twee typen die bekend staan als

Automatische NAT (Object-NAT) en Handmatige NAT (Dubbele NAT). De eerste is Object-NAT en wordt geconfigureerd binnen de definitie van een netwerkobject. U vindt verderop in dit document een voorbeeld hiervan. Een belangrijk voordeel van deze NAT-methode is dat de ASA de regels voor verwerking automatisch rangschikt om conflicten te voorkomen. Dit is de makkelijkste vorm van NAT, maar dit gemak brengt een beperkte gedetailleerdheid in de configuratie met zich mee. U kunt bijvoorbeeld geen omzettingsbeslissing nemen op basis van de bestemming van het pakket zoals u kunt met het andere type NAT: Handmatige NAT. Handmatige NAT is gedetailleerder, maar vereist dat de regels in de juiste volgorde worden geconfigureerd om correct te kunnen functioneren. Dit compliceert dit NAT-type en kan daarom niet worden gebruikt in dit configuratievoorbeeld.

Raadpleeg de sectie Informatie over NAT in Boek 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1 voor meer informatie over NAT.

Configureren

Aan de slag

De basisconfiguratie van ASA is drie interfaces verbonden met drie netwerksegmenten. Het ISP netwerksegment is verbonden met de Ethernet0/0-interface en wordt aan de buitenkant gelabeld met een beveiligingsniveau van 0. Het interne netwerk is verbonden met Ethernet0/1 en aangeduid als binnenkant met een beveiligingsniveau van 100. Het DMZ-segment, waar de webserver zich bevindt, is verbonden met Ethernet0/2 en aangeduid als DMZ met een beveiligingsniveau van 50.

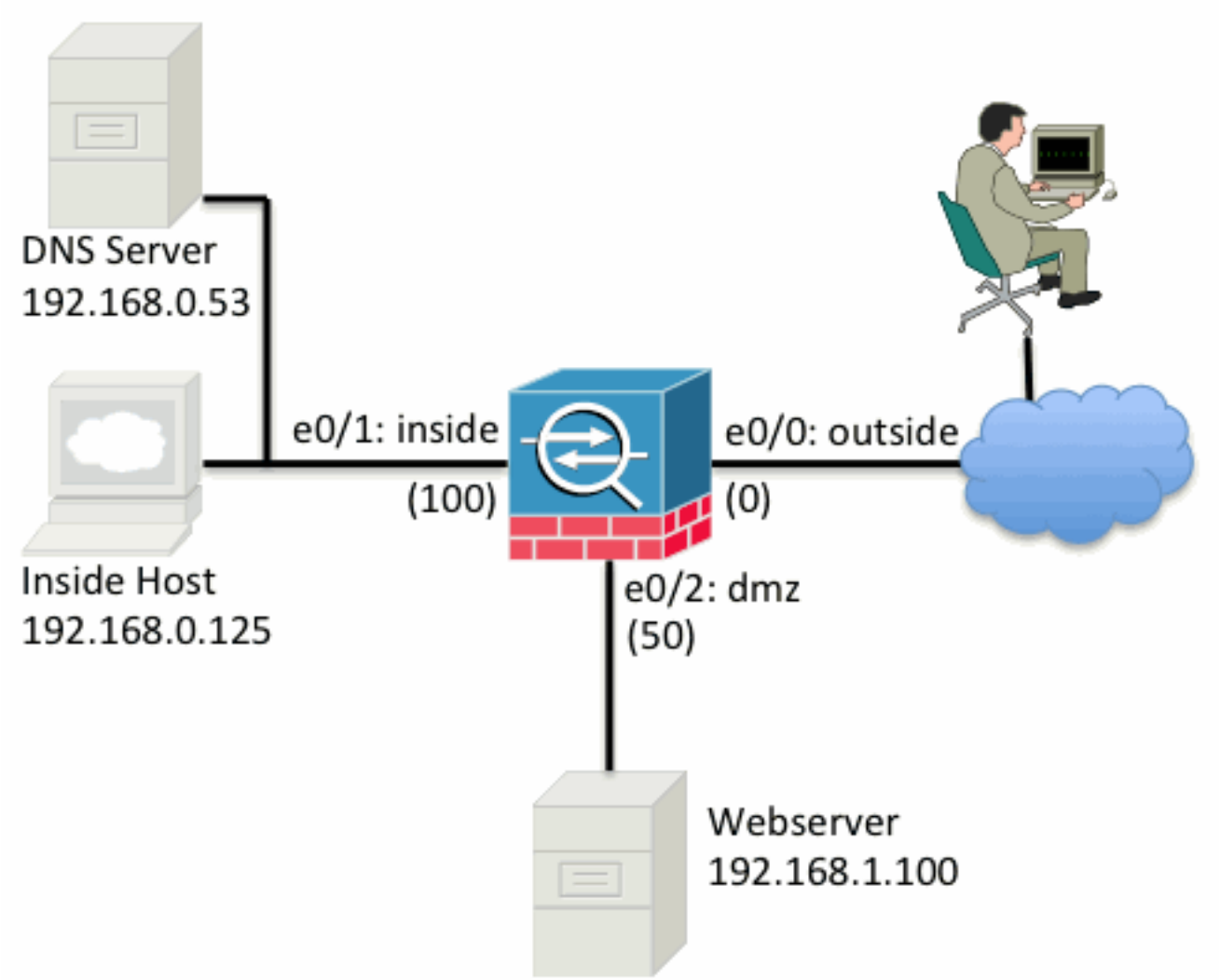
De interface-configuratie en IP-adressen die in het voorbeeld worden gebruikt zijn:

```
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 kunt u zien dat de inside-interface van de ASA is ingesteld op het IP-adres 192.168.0.1. Dit is de standaardgateway voor de interne hosts. De outside-interface van de ASA wordt geconfigureerd met een IP-adres dat de ISP heeft verstrekt. Er is een standaardroute ingesteld die de next-hop instelt op de ISP-gateway. Dit gebeurt automatisch als u DHCP gebruikt. De DMZ-interface wordt geconfigureerd met IP-adres 192.168.1.1 en is de standaardgateway voor hosts in het DMZ-netwerksegment.

Topologie

Hier kan u zien hoe dit wordt bekabeld en geconfigureerd:



Stap 1. Configureer NAT om hosts naar het internet te laten gaan

In dit voorbeeld wordt Object NAT, ook bekend als AutoNAT, gebruikt. Allereerste moeten de NAT-regels worden geconfigureerd waarmee de hosts in de segmenten inside en DMZ verbinding kunnen maken met het internet. Omdat deze hosts privé IP-adressen gebruiken, moet u deze omzetten in iets dat op het internet routeerbaar is. Zet de adressen in dit geval zo om, dat ze lijken op het IP-adres van de outside-interface van de ASA. Dit is de eenvoudigste manier om dit in te stellen als uw externe IP-adres regelmatig verandert (bijvoorbeeld door DHCP).

Om deze NAT te configureren moet u een netwerkobject maken dat de inside-subnet vertegenwoordigt, en een die de subnet van de DMZ vertegenwoordigt. In elk van deze objecten moet u een dynamische NAT-regel configureren die poortadresomzetting (PAT) mogelijk maakt voor deze clients aangezien deze van hun respectieve interfaces naar de buiteninterface overgaan.

De configuratie ziet er ongeveer zo uit:

```
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
```

Als u de lopende configuratie op dit punt (met de output van het bevel van de show looppas) bekijkt, kunt u zien dat de objectdefinitie in twee delen van de output wordt verdeeld. Het eerste deel geeft alleen aan wat er in het object staat (host/subnet, IP-adres, enz.) terwijl het andere deel de NAT-regel laat zien die aan dat object is gekoppeld. Als u naar de eerste vermelding in de output neemt:

Wanneer hosts die overeenkomen met subnet 192.168.0.0/24 vanaf de inside-interface naar de outside-interface gaan, moet u deze dynamisch omzetten in de outside-interface.

Stap 2. NAT configureren voor toegang tot de webserver via internet

Nu de hosts aan de binnenkant en DMZ interfaces naar het internet kunnen komen, moet u de configuratie wijzigen zodat gebruikers op het internet toegang hebben tot onze webserver op TCP poort 80. In dit voorbeeld is de installatie zo dat mensen op het internet verbinding kunnen maken met een ander IP-adres dat door de ISP wordt opgegeven, een extra IP-adres dat wij *bezitten*. Gebruik bij dit voorbeeld 198.51.100.101. Met deze configuratie kunnen gebruikers op het internet de DMZ webserver bereiken door 198.51.100.101 te gebruiken op TCP poort 80. Gebruik Object NAT voor deze taak en de ASA kan TCP poort 80 op de webserver (192.168.1.100) vertalen om er als 198.51.100.101 op TCP poort 80 aan de buitenkant uit te zien. Net zoals eerder definieert u een object en omzettingsregels voor dit object. Definieer ook een tweede object dat de IP vertegenwoordigt waarop u deze host kunt vertalen.

De configuratie ziet er ongeveer zo uit:

```
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
```

Om samen te vatten wat de NAT-regel in dit voorbeeld inhoudt:

Wanneer een host die overeenkomt met IP-adres 192.168.1.100 in de DMZ-segmenten een verbinding opbouwt via TCP-poort 80 (www) en die verbinding naar de outside-interface gaat, moet u deze omzetten in TCP-poort 80 (www)op de outside-interface. Het IP-adres moet worden omgezet in 198.51.100.101.

Dat lijkt een beetje vreemd... "afkomstig van TCP poort 80 (www)", maar webverkeer is bestemd voor poort 80. Het is belangrijk om te begrijpen dat deze NAT-regels bidirectioneel van aard zijn. Daarom kunt u de verwoording omdraaien om deze zin opnieuw te formuleren. Het resultaat hiervan is logischer:

Wanneer hosts aan de buitenkant een verbinding tot stand brengen met 198.51.100.101 op de bestemming TCP-poort 80 (www), kunt u het doelIP-adres vertalen naar 192.168.1.100 en de bestemmingshaven kan TCP-poort 80 (www) zijn en de poort naar de DMZ sturen.

Zo is het logischer geformuleerd. Nu moeten de ACL’s worden ingesteld.

Stap 3. ACL’s configureren

NAT is geconfigureerd en deze configuratie is bijna voltooid. Vergeet niet dat u met ACL’s op de ASA het volgende standaard security gedrag kunt overschrijven:

- Verkeer dat van een lagere security interface gaat wordt geweigerd wanneer het richting een hogere security interface gaat.
- Verkeer dat van een hogere security interface gaat wordt geaccepteerd wanneer het richting een lagere security interface gaat.

Wanneer er geen ACL's aan de configuratie worden toegevoegd, verloopt het verkeer in het voorbeeld als volgt:

- De hosts aan de inside (security niveau 100) kunnen worden verbonden met de hosts in de DMZ (security niveau 50).
- De hosts aan de inside (security niveau 100) kunnen worden verbonden met de hosts aan de outside (security niveau 0).
- De hosts op de DMZ (security niveau 50) kunnen worden verbonden met de hosts aan de outside (security niveau 0).

Het volgende verkeer wordt echter geweigerd:

- De hosts aan de outside (security niveau 0) kunnen niet worden verbonden met de hosts aan de inside (security niveau 100).
- De hosts aan de outside (security niveau 0) kunnen niet worden verbonden met de hosts in de DMZ (security niveau 50).
- De hosts in de DMZ (security niveau 50) kunnen niet worden verbonden met de hosts aan de inside (security niveau 100).

Omdat het verkeer van buiten naar het DMZ-netwerk door de ASA met zijn huidige configuratie wordt ontkend, kunnen gebruikers op het internet de webserver niet bereiken ondanks de NAT-configuratie in stap 2. U moet dit verkeer expliciet toestaan. In versie 8.3 en hoger moet u de Real IP van de host in de ACL gebruiken en niet de omgezette IP. Dit betekent dat de configuratie verkeer moet toestaan dat bestemd is voor 192.168.1.100 en NIET voor 198.51.100.101 op poort 80. Omwille van de eenvoud kunnen de in stap 2 gedefinieerde objecten ook voor deze ACL worden gebruikt. Zodra de ACL wordt gecreëerd moet u deze inkomend op de outside-interface toepassen.

De configuratieopdrachten zien er als volgt uit:

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

Op de regel voor de toegangslijst staat:

Al het verkeer toestaan naar de host die wordt vertegenwoordigd door het object webserver (192.168.1.100) op poort 80.

Het is belangrijk dat de configuratie hier het trefwoord any bevat. Omdat het bron-IP-adres van clients niet bekend is wanneer het uw website bereikt, geeft u hier 'any' op om voor elk IP-adres te gelden.

Maar hoe zit het met het verkeer van het DMZ-segment dat bestemd is voor hosts op het inside-netwerksegment? Bijvoorbeeld een server op het inside-netwerk waarmee de hosts in de DMZ verbinding moeten maken. Hoe kan de ASA alleen dat specifieke verkeer toestaan dat bestemd is voor de inside-server en alles wat bestemd is voor het inside-segment van de DMZ blokkeren?

In dit voorbeeld wordt aangenomen dat er een DNS-server is op het inside-netwerk met IP-adres 192.168.0.53, waar de hosts in de DMZ toegang toe moeten hebben voor DNS-omzetting. U creëert de vereiste ACL en past deze toe op de DMZ-interface, zodat de ASA het standaard security gedrag, zoals eerder omschreven, kan overschrijven voor het verkeer dat de interface binnengaat.

De configuratieopdrachten zien er als volgt uit:

```
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
```

ACL is complexer dan eenvoudig het toelaten van dat verkeer aan de DNS server op UDP haven 53. Als alles wat we deden is die eerste vergunningslijn, dan zou al verkeer worden geblokkeerd van de DMZ naar hosts op het internet. ACL's hebben een impliciete regel 'deny ip any any' aan het einde van de ACL. Hierdoor zouden uw DMZ-hosts het internet niet kunnen bereiken. Zelfs al is verkeer van de DMZ naar de outside standaard toegestaan door de toepassing van een ACL op de DMZ-interface, is het standaard security gedrag voor de DMZ-interface niet langer van kracht en moet u het verkeer expliciet toestaan in de interface-ACL.

Stap 4. Testconfiguratie met de pakkettraceerfunctie

Nu de configuratie is voltooid, moet u deze testen om er zeker van te zijn dat deze werkt. De makkelijkste methode is om de daadwerkelijke hosts te gebruiken (als dit uw netwerk is). Echter, in het belang om dit te testen van de CLI en verder te verkennen enkele van de ASA tools, gebruik de pakkettracer om eventuele problemen die zijn aangetroffen te testen en te zuiveren.

Packet Tracer werkt door een pakket te simuleren dat is gebaseerd op een reeks parameters en dat pakket te injecteren in het datapad van de interface. Dit is vergelijkbaar met wat er met een echt pakket zou gebeuren. Dit pakket wordt gevolgd door een groot aantal controles en processen die worden uitgevoerd wanneer het door de firewall gaat. Packet Tracer noteert het resultaat. Simuleer de interne host die een host op het internet probeert te bereiken. Met deze opdracht wordt de firewall geïnstrueerd:

Simuleer een TCP-pakket dat binnenkomt via de inside-interface vanaf IP-adres 192.168.0.125 op bronpoort 12345, bestemd voor IP-adres 203.0.113.1 op poort 80.

```
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
```

Het resultaat is dat het verkeer toegestaan is. Dit betekent dat het alle NAT- en ACL-controles in de configuratie is gepasseerd en is doorgestuurd naar de uitgaande interface outside. Vergeet niet dat het pakket in fase 3 is omgezet en dat de gegevens van die fase laten zien welke regel is toegepast. Het host-IP-adres 192.168.0.125 wordt in overeenstemming met de configuratie dynamisch omgezet in 198.51.100.100.

Doe dit nu voor een verbinding van het internet naar de webserver. Vergeet niet dat hosts op het internet toegang hebben tot de webserver door verbinding te maken met 198.51.100.101 op de buiteninterface. De volgende opdracht laat zich wederom vertalen tot:

Simuleer een TCP-pakket dat binnenkomt via de outside-interface vanaf IP-adres 192.0.2.123 op bronpoort 12345, bestemd voor IP-adres 198.51.100.101 op poort 80.

```
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
```

Het resultaat is wederom dat het pakket wordt toegestaan. De ACL's controleren, de configuratie ziet er goed uit en gebruikers op het internet (buiten) kunnen toegang krijgen tot die webserver met het externe IP.

Verifiëren

Verificatieprocedures zijn opgenomen in Stap 4: Configuratie testen met Packet Tracer.

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar over hoe u deze configuratie kunt oplossen.

Conclusie

De configuratie van een ASA om basis-NAT te doen is niet zo moeilijk. Het voorbeeld in dit document kan aan uw specifieke scenario worden aangepast als u de IP-adressen en poorten aanpast die in de voorbeeldconfiguraties worden gebruikt. De definitieve ASA-configuratie hiervoor zal, wanneer samengevoegd, erg lijken op die voor een 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
```

Neem bijvoorbeeld een ASA 5505, met de interfaces verbonden zoals eerder weergegeven (outside verbonden met Ethernet0/0, inside verbonden met Ethernet0/1 en DMZ verbonden met 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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.