PIX/ASA 7.x: Communicatie tussen interfaces inschakelen/uitschakelen

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor verschillende vormen van communicatie tussen interfaces op het ASA/PIX-beveiligingsapparaat.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- IP-adressen en standaardgateway
- Fysieke netwerkconnectiviteit tussen apparaten
- Communicatiepoort # geïdentificeerd voor de uitgevoerde service

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Adaptieve security applicatie die software versie 7.x en hoger uitvoert
- Windows 2003-servers
- Windows XP-werkstations

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 de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt in combinatie met deze hardware- en softwareversies:

- PIX 500 Series firewalls die 7.x en hoger uitvoeren

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Dit document beschrijft de gewenste stappen om communicatie tussen verschillende interfaces mogelijk te maken. De communicatievormen zoals deze worden besproken:

1. Communicatie van hosts die zich aan de buitenkant bevinden die toegang tot middelen vereist die zich in de DMZ bevinden
2. Communicatie van hosts op het binnennetwerk die toegang tot middelen vereist die zich in de DMZ bevinden
3. Communicatie van hosts binnen en het DMZ-netwerk die toegang tot bronnen aan de buitenkant vereisen

NAT

In ons voorbeeld gebruiken we in onze configuratie netwerkadresomzetting (NAT) en poortadresomzetting (PAT). Adres vertaling vervangt het echte adres (lokaal) in een pakket met een in kaart gebracht adres (mondiaal) dat op het doelnetwerk routeerbaar is. NAT bestaat uit twee stappen: het proces waarin een echt adres wordt vertaald naar een in kaart gebracht adres en vervolgens het proces om de vertaling ongedaan te maken voor het teruggegeven verkeer. Er zijn twee vormen van adresomzetting die we gebruiken in deze configuratie gids: Statisch en dynamisch.

Dynamische vertalingen maken het mogelijk dat elke host een ander adres of poort gebruikt voor elke volgende vertaling. Dynamische vertalingen kunnen worden gebruikt wanneer lokale hosts delen of "zich achter" een of meer algemene adressen verbergen. In deze modus kan één lokaal adres geen algemeen adres voor vertaling reserveren. In plaats daarvan vindt adresomzetting plaats op een veel-naar-één-of veel-naar-veel basis, en vertalingen worden alleen aangemaakt als ze nodig zijn. Zodra een vertaling gratis is, wordt deze verwijderd en beschikbaar gesteld aan andere lokale hosts. Dit type vertaling is het meest handig voor uitgaande verbindingen, waarin

binnen hosts een dynamisch adres of poortnummer wordt toegewezen uitsluitend als er verbindingen worden gemaakt. Er zijn twee vormen van dynamische adresomzetting:

- Dynamische NAT - Lokale adressen worden vertaald in het volgende beschikbare mondiale adres in een pool. Vertaling vindt plaats op een één-op-één basis, zodat het mogelijk is om de pool van mondiale adressen te vullen als een groter aantal lokale hosts op een bepaald moment een vertaling nodig heeft.
- NAT Overload (PAT) - Lokale adressen worden vertaald in één mondiaal adres. elke verbinding wordt uniek gemaakt wanneer het volgende beschikbare hoge-orderpoortnummer van het mondiale adres wordt toegewezen als de bron van de verbinding. Vertaling vindt plaats op een veelvoudig-aan-eenbasis omdat veel lokale gastheren één gemeenschappelijk mondiaal adres delen.

Statische vertaling creëert een vaste vertaling van het (de) werkelijke adres(en) naar het (de) in kaart gebrachte adres(sen). Een statische NAT-configuratie stelt hetzelfde adres in voor elke verbinding door een host en is een persistente vertaalregel. Statische adresvertalingen worden gebruikt wanneer een interne of lokale host voor elke verbinding hetzelfde globale adres nodig heeft. adresomzetting vindt plaats op één-op-één-basis. Statische vertalingen kunnen worden gedefinieerd voor één host of voor alle adressen die deel uitmaken van een IP-telefoon.

Het belangrijkste verschil tussen dynamische NAT en een reeks adressen voor statische NAT is dat statische NAT een externe host toelaat om een verbinding naar een vertaalde host te openen (als er een toegangslijst is die deze mogelijkheid biedt), terwijl dynamisch NAT dit niet doet. U hebt ook een gelijk aantal in kaart gebrachte adressen met statische NAT nodig.

Het security apparaat vertaalt een adres wanneer een NAT-regel overeenkomt met het verkeer. Als er geen NAT-regelovereenkomsten zijn, wordt de verwerking van het pakket voortgezet. De uitzondering is wanneer u NAT-controle instelt. NAT-controle vereist dat pakketten die van een hogere veiligheidsinterface (binnenin) naar een lager veiligheidsniveau (buiten) worden verzonden overeenkomen met een NAT-regel, of andere verwerking voor de pakketeinden. Raadpleeg het PIX/ASA 7.x NAT- en PAT-document om informatie over de configuratie te bekijken. Voor een dieper begrip van hoe NAT werkt, verwijs naar de handleiding Hoe NAT werkt.

Tip: Als u de NAT-configuratie wijzigt, wordt u aangeraden de huidige NAT-vertalingen te verwijderen. U kunt de vertaaltabel wissen met de **duidelijke** opdracht. **Wees echter voorzichtig als u dit doet** omdat het verwijderen van de vertaaltabel alle huidige verbindingen ontkoppelt die vertalingen gebruiken. Het alternatief voor het wegwerken van de vertaaltabel is om op de huidige vertalingen te wachten tot de tijd is verstreken, maar dit wordt niet aanbevolen, omdat onverwacht gedrag kan resulteren in het aanleggen van nieuwe verbindingen met de nieuwe regels.

Beveiligingsniveaus

De waarde op veiligheidsniveau bepaalt hoe hosts/apparaten op de verschillende interfaces met elkaar in interactie treden. Standaard kunnen hosts/apparaten die zijn aangesloten op interfaces met hogere beveiligingsniveaus toegang hebben tot hosts/apparaten die zijn aangesloten op een interface met lagere beveiligingsniveaus. Hosten/apparaten die op interfaces met lager-veiligheidsinterfaces worden aangesloten kunnen tot hosts/apparaten geen verbinding maken met interfaces met hogere beveiligingsinterfaces zonder toestemming van toegangslijsten.

De opdracht **veiligheidsniveau** is nieuw in versie 7.0 en vervangt het gedeelte van de **naam indien** opdracht die het veiligheidsniveau voor een interface heeft toegewezen. Twee interfaces, "binnen" en "buiten" interfaces, hebben standaard beveiligingsniveaus, maar deze kunnen worden

overbrugd met de opdracht **veiligheidsniveau**. Als u een interface "binnenin" noemt, krijgt het een standaard veiligheidsniveau van 100; Een interface met de naam "buiten" krijgt een standaard beveiligingsniveau van 0. Alle andere nieuwe interfaces krijgen een standaard beveiligingsniveau van 0. Om een nieuw beveiligingsniveau aan een interface toe te wijzen, gebruikt u de opdracht **veiligheidsniveau** in de interface-opdrachtmodus. Beveiligingsniveaus variëren van 1 tot 100.

Opmerking: Beveiligingsniveaus worden uitsluitend gebruikt om te bepalen hoe de firewall het verkeer inspecteert en afhandelt. Bijvoorbeeld, verkeer dat van een hoger veiligheidsinterface in een lager wordt doorgestuurd door met minder streng standaardbeleid dan verkeer dat van een lagere veiligheidsinterface naar een hoger veiligheidsgebied komt. Raadpleeg de ASA/PIX 7.x-opdracht handleiding voor meer informatie over beveiligingsniveaus.

ASA/PIX 7.x introduceerde ook de mogelijkheid om meerdere interfaces met hetzelfde beveiligingsniveau te configureren. Bijvoorbeeld, meerdere interfaces verbonden met partners of andere DMZ's kunnen allen een veiligheidsniveau van 50 krijgen. Standaard kunnen deze zelfde veiligheidsinterfaces niet met elkaar communiceren. Om hieraan te werken werd de opdracht van de **beveiligingslicentie-interface** geïntroduceerd. Deze opdracht maakt communicatie tussen interfaces van hetzelfde beveiligingsniveau mogelijk. Voor meer informatie over zelfde veiligheid tussen interfaces, verwijs naar de gids van de Referentievan het Bevel, die de parameters van de Interface vormt, en zie dit voorbeeld.

ACL

Toegangscontrolelijsten bestaan doorgaans uit meerdere toegangscontrolelijsten (ACE) die intern door de security applicatie worden georganiseerd in een gekoppelde lijst. ACE's beschrijven een reeks verkeer zoals dat van een gastheer of netwerk en noemen een actie om op dat verkeer van toepassing te zijn, over het algemeen toestaan of ontkennen. Wanneer een pakket wordt onderworpen aan de controle van de toegangslijst, doorzoekt de Cisco security applicatie deze gekoppelde lijst met ACE's om er een te vinden die overeenkomt met het pakket. **Het eerste ACE dat overeenkomt met het security apparaat is het apparaat dat op het pakket wordt toegepast.** Zodra de match wordt gevonden, wordt de handeling in dat ACE (licentie of ontkennen) toegepast op het pakje.

Per interface, per richting is slechts één toegangslijst toegestaan. Dit betekent dat u slechts één toegangslijst kunt hebben die van toepassing is op verkeer inkomende op een interface en één toegangslijst die van toepassing is op verkeer uitgaande op een interface. Toegangslijsten die niet worden toegepast op interfaces, zoals NAT ACL's, zijn onbeperkt.

Opmerking: Standaard hebben alle toegangslijsten een impliciete ACE aan het eind die al verkeer ontkent, zodat al verkeer dat niet overeenkomt met een ACE dat u in de toegangslijst invoert, overeenkomt met de impliciete ontkennen aan het eind en wordt ingetrokken. U moet ten minste één vergunningsverklaring in een lijst van de interfacetoegang hebben om verkeer te stromen. Zonder vergunning wordt al het verkeer geweigerd.

Opmerking: De toegangslijst wordt uitgevoerd met de opdrachten **toegangslijst** en **toegangsgroep**. Deze opdrachten worden gebruikt in plaats van de opdrachten **voor** geleiding en **uitgang**, die in eerdere versies van de software van de PIX-firewall zijn gebruikt. Raadpleeg voor meer informatie over ACL's de IP-toegangslijst configureren.

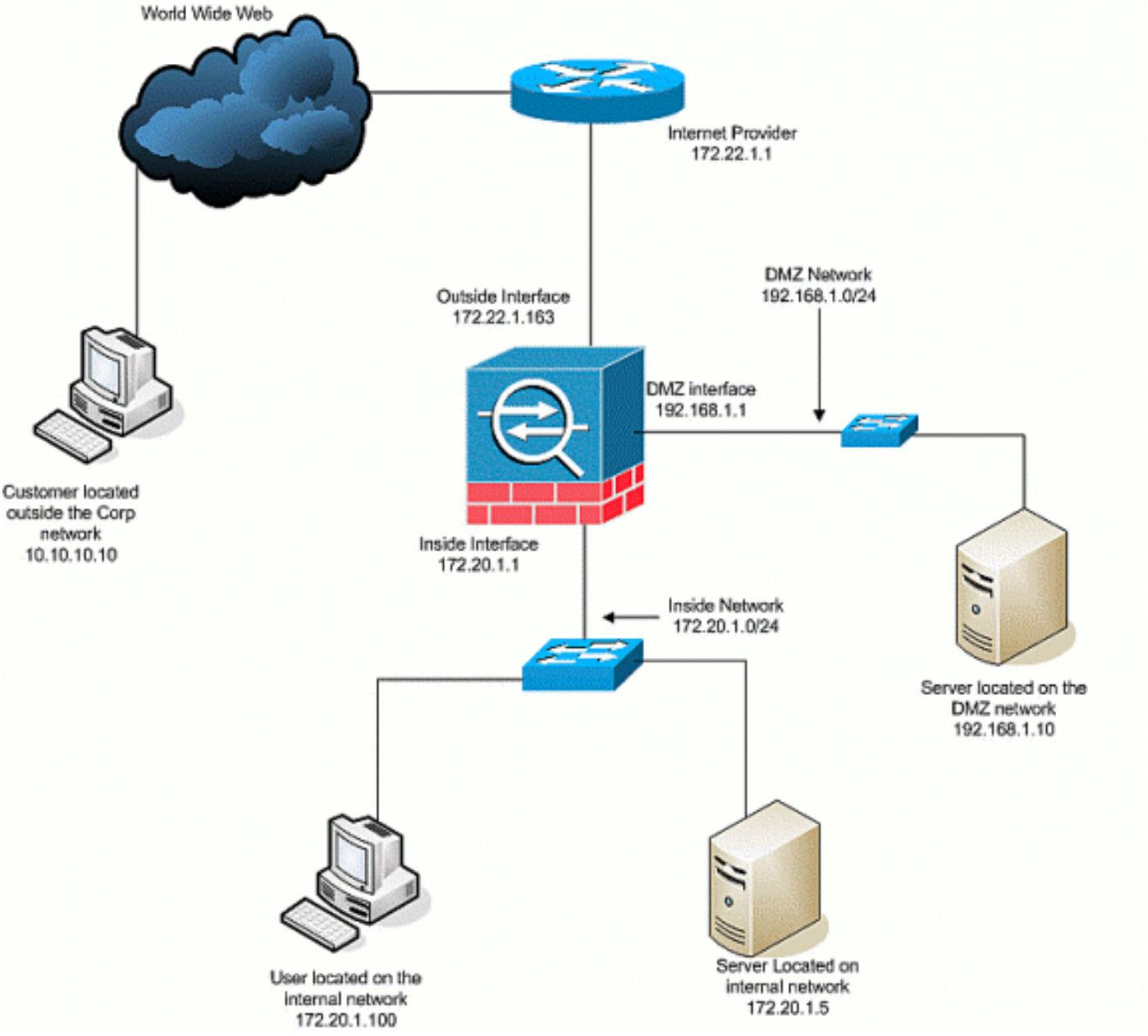
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Dit document gebruikt de volgende netwerkinstellingen:



Eerste configuratie

Dit document gebruikt deze configuraties:

- Bij deze fundamentele firewallconfiguratie zijn er momenteel geen NAT/STATIC verklaringen.
- Er zijn geen ACL's toegepast, dus de impliciete ACE van `ontkennen` wordt momenteel gebruikt.

Apparaatnaam 1

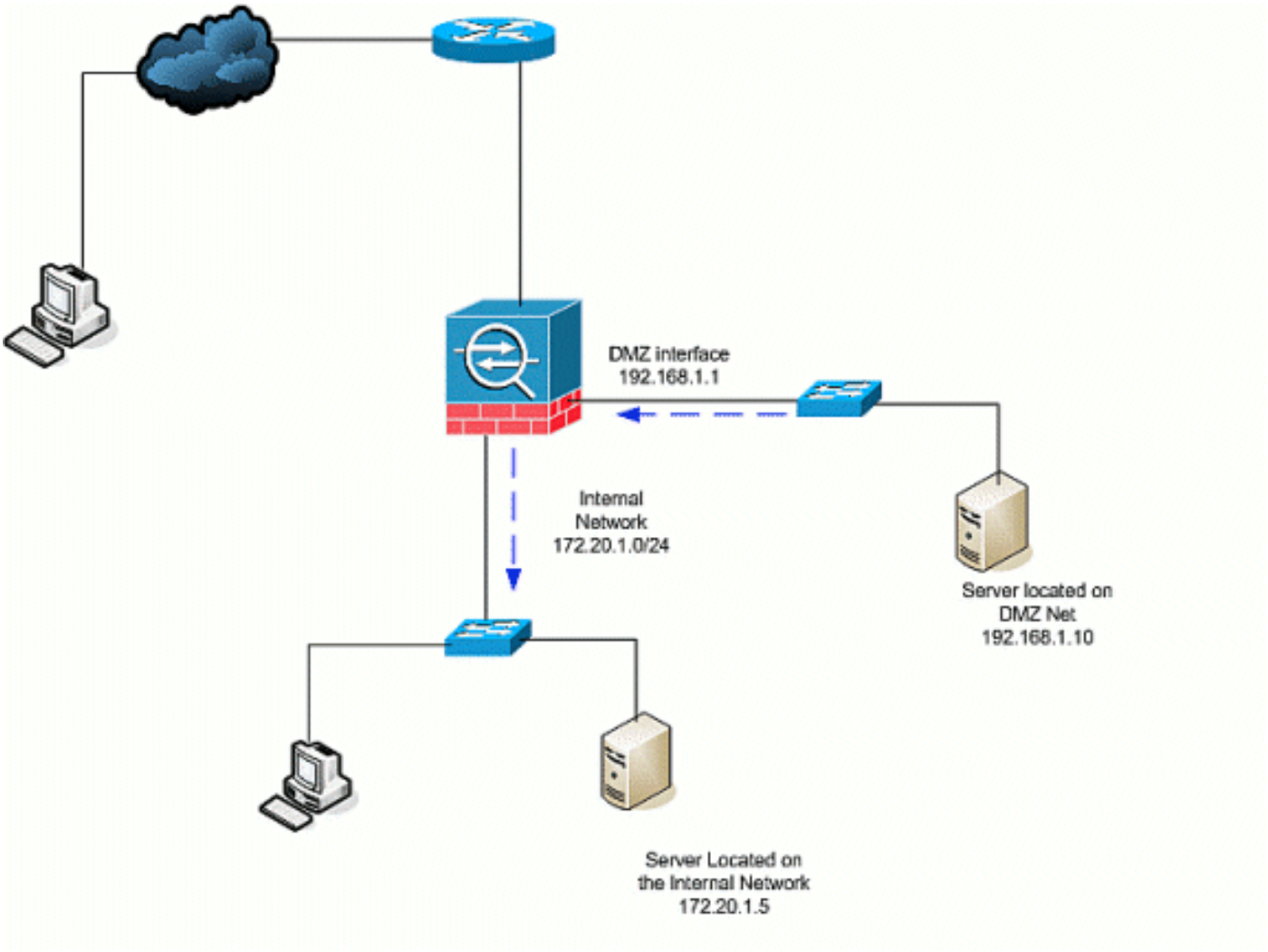
```
ASA-AIP-CLI(config)#show running-config

 ASA Version 7.2(2)
!
hostname ASA-AIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 172.22.1.163 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.20.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/3
 nameif DMZ-2-testing
 security-level 50
 ip address 192.168.10.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu inside 1500
mtu Outside 1500
mtu DMZ 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat-control
route Outside 0.0.0.0 0.0.0.0 172.22.1.1 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 uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
```

```
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  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 netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA-AIP-CLI(config)#
```

DMZ naar binnen

Gebruik deze opdrachten om communicatie van de DMZ naar interne netwerkhosts toe te staan. In dit voorbeeld moet een webserver op de DMZ toegang hebben tot een AD- en DNS-server binnenin.

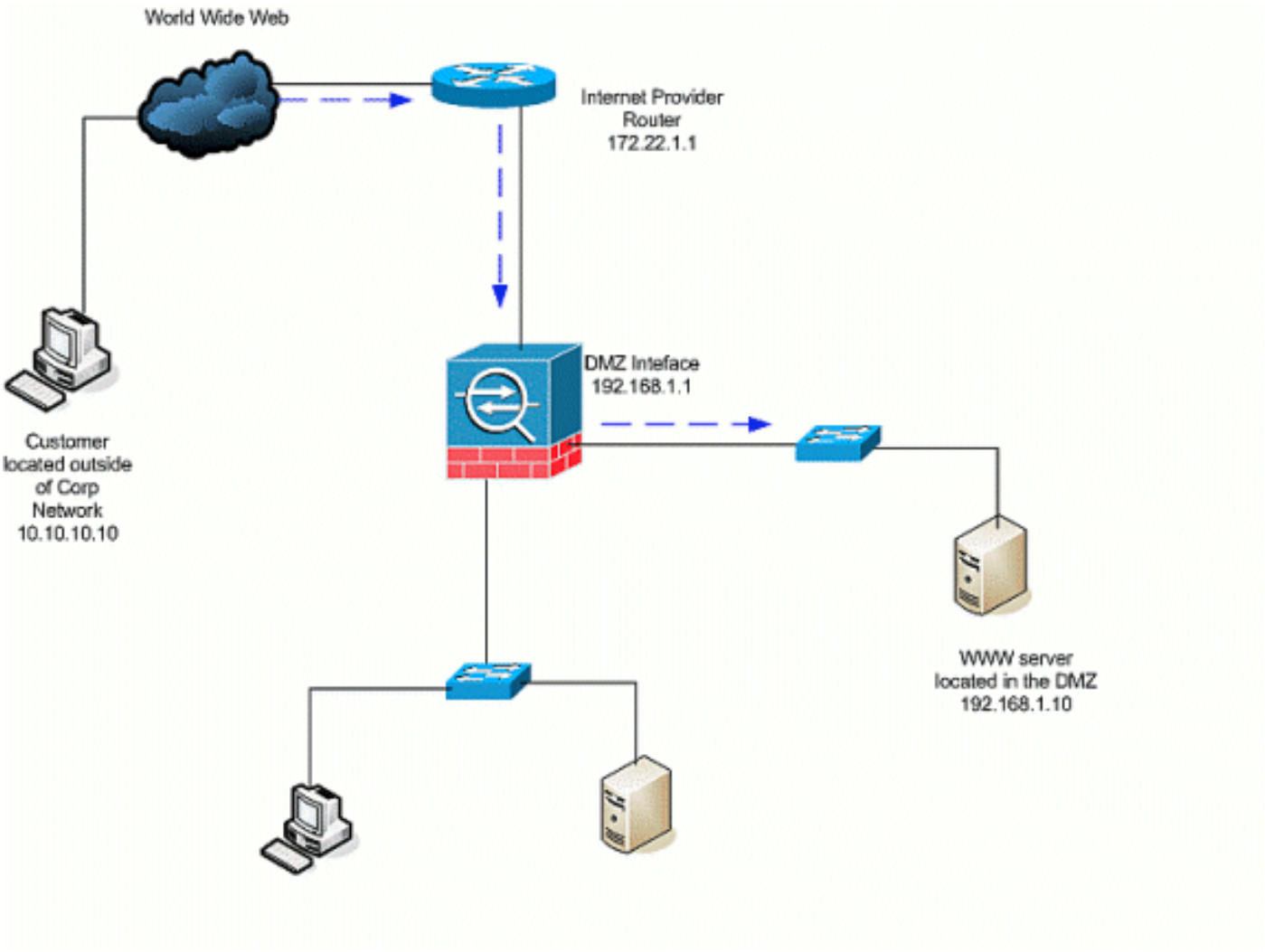


1. Maak een statische NAT-ingang voor de AD/DNS-server op de DMZ. Statische NAT maakt een vaste vertaling van een reëel adres naar een in kaart gebracht adres. Dit in kaart gebrachte adres is een adres dat de DMZ-hosts kunnen gebruiken om toegang te krijgen tot de server binnen zonder dat zij het echte adres van de server moeten kennen. Deze opdracht brengt het DMZ-adres 192.168.2.20 in kaart naar het echte binnenadres 172.20.1.5.`ASA-AIP-CLI (configuratie)# statisch (binnenin, DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. ACL's zijn vereist om een interface met een lager veiligheidsniveau toe te staan om toegang tot een hoger veiligheidsniveau te krijgen. In dit voorbeeld geven we de webserver die op de DMZ (Security 50) toegang heeft tot de AD/DNS server aan de binnenkant (Security 100) met deze specifieke servicepoorten: DNS, Kerberos en LDAP.`ASA-AIP-CLI (configuratie)# access-list DMZtoInside Extended Hedp host 192.168.1.10 host 192.168.2.20 eq-domeinASA 192.168.1.10 host 192.168.2.20 eq 88ASA-AIP-CLI (configuratie)# access-list DMZtoInside Extended Hedp host 192.168.1.10 host 192.168.2.20 eq 389`**Opmerking:** De ACL's staan toegang toe tot het in kaart gebrachte adres van de AD/DNS-server die in dit voorbeeld is gemaakt en niet het echte interne adres.
3. In deze stap, past u ACL op de interface DMZ in de inkomende richting met deze opdracht toe:`ASA 5500-AIP-CLI (configuratie)# access-group DMZtoInside in interface-DMZ`**Opmerking:** Als u poort 88 wilt blokkeren of uitschakelen, gebruikt u bijvoorbeeld dit voor verkeer van DMZ naar binnen:
   ```
   ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
   tcp host 192.168.1.10 host 192.168.2.20 eq 88
   ```
   Tip: Als u de NAT-configuratie wijzigt, wordt u aangeraden de huidige NAT-vertalingen te verwijderen. U kunt de vertaaltabel wissen met de **duidelijke** opdracht. **Wees voorzichtig als u**

dit doet omdat het verwijderen van de vertaaltabel alle huidige verbindingen die vertalingen gebruiken, koppelt. Het alternatief voor het wegwerken van de vertaaltabel is om te wachten op de huidige vertalingen voordat deze zijn beëindigd, maar dit wordt niet aanbevolen, omdat onverwacht gedrag kan resulteren in het aanleggen van nieuwe verbindingen met de nieuwe regels.Andere gemeenschappelijke formaties omvatten:Mail Server in DMZSSH-toegang binnen en buitenToegestane Remote-desktopsessies via PIX/ASA-apparatenAndere DNS-oplossingen bij gebruik in de DMZ

Internet naar DMZ

Gebruik deze opdrachten om communicatie van gebruikers via het internet of externe interface (Security 0) naar een webserver mogelijk te maken die zich in de DMZ bevindt (Security 50):



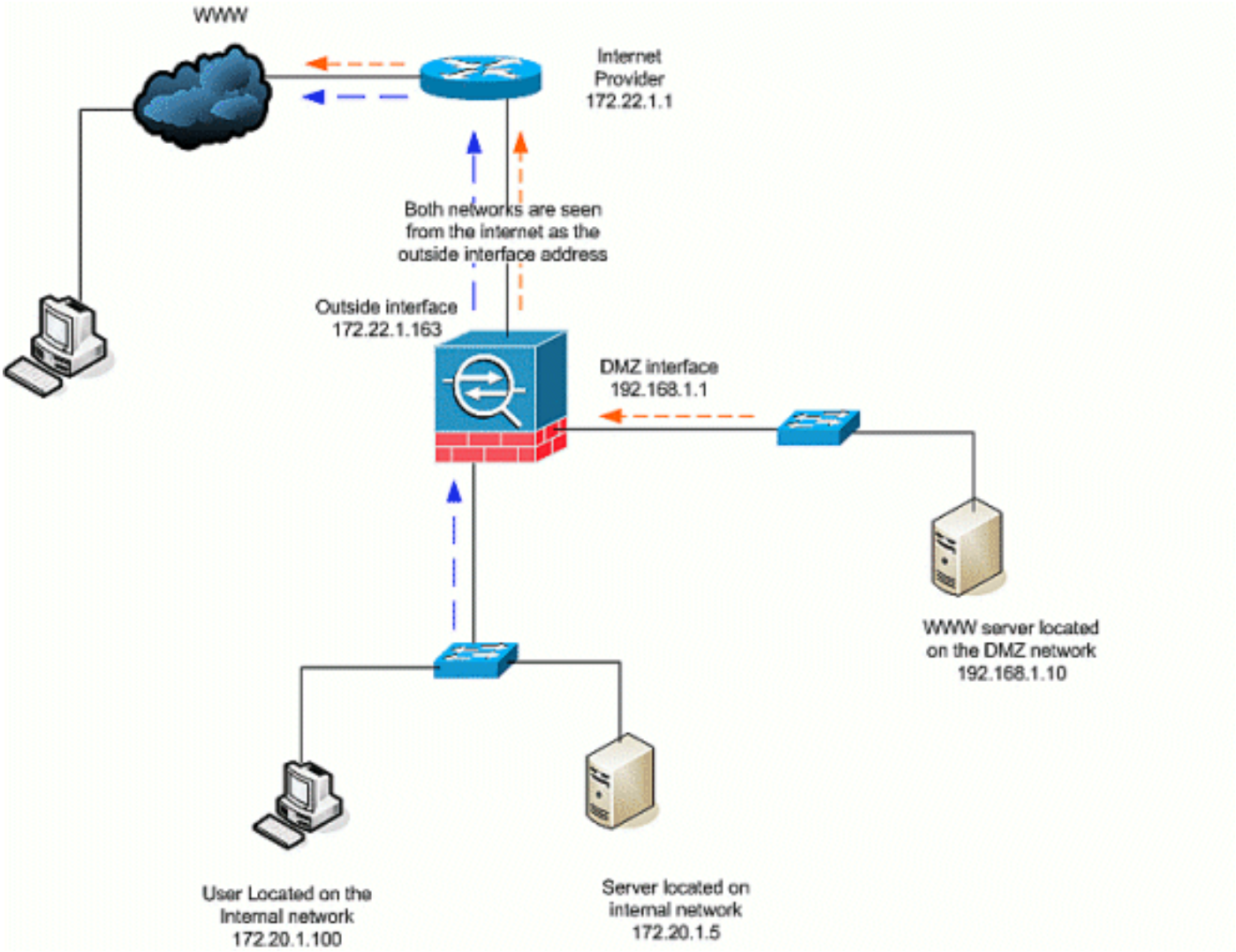
1. Maak een statische vertaling voor de webserver in de DMZ naar buiten. Statische NAT maakt een vaste vertaling van een reëel adres naar een in kaart gebracht adres. Dit in kaart gebrachte adres is een adres dat de hosts op het internet kunnen gebruiken om toegang te krijgen tot de webserver op de DMZ zonder dat het echte adres van de server moet worden gehoord. Deze opdracht geeft het externe adres 172.22.1.25 in kaart aan het echte DMZ-adres 192.168.1.10.`ASA 172.22.1.25 192.168.1.10 (configuratie)# statisch (DMZ, buiten) 25.25.25.255.255.255`
2. Maak een ACL die gebruikers van de buitenkant toestaat om de webserver door het in kaart gebrachte adres te gebruiken. Merk op dat de webserver ook de FTP-server gastheer is.`ASA-AIP-CLI (configuratie)# access-list OutsidetoDMZ uitgebreide vergunning TCP van elke host`

```
172.2.1.25 eq wwwASA-AIP-CLI (configuratie)# access-list OutsidetoDMZ uitgebreide
vergunning TCP van elke host 172.2.1.25 eq ftp
```

3. De laatste stap in deze configuratie is om ACL op de buiteninterface voor verkeer in de inkomende richting toe te passen.`ASA 5500-AIP-CLI (configuratie)# access-group Outside-toDMZ in interface buiten`**Opmerking:** Onthoud, u kunt slechts één toegangslijst per interface, per richting toepassen. Als u al een inkomende ACL hebt die op de buiteninterface wordt toegepast, kunt u dit voorbeeld ACL op het toepassen. In plaats daarvan voegt u ACE's toe in dit voorbeeld in de huidige ACL die op de interface wordt toegepast.**Opmerking:** Als u het FTP-verkeer van internet naar DMZ wilt blokkeren of uitschakelen, gebruikt u bijvoorbeeld dit:
```
ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
tcp any host 172.22.1.25 eq ftp
```
Tip: Als u de NAT-configuratie wijzigt, wordt u aangeraden de huidige NAT-vertalingen te verwijderen. U kunt de vertaaltabel wissen met de **duidelijke** opdracht. **Wees voorzichtig als u dit doet** omdat het verwijderen van de vertaaltabel alle huidige verbindingen die vertalingen gebruiken, koppelt. Het alternatief voor het wegwerken van de vertaaltabel is om op de huidige vertalingen te wachten tot de tijd is verstreken, maar dit wordt niet aanbevolen, omdat onverwacht gedrag kan resulteren in het aanleggen van nieuwe verbindingen met de nieuwe regels.

Binnenin/DMZ naar internet

In dit scenario worden hosts op de binneninterface (security applicatie 100) van het security apparaat geboden met toegang tot het internet op de externe interface (beveiliging 0). Dit wordt bereikt met de PAT- of NAT-overload dynamische NAT-modus. In tegenstelling tot de andere scenario's, wordt ACL in dit geval niet vereist omdat de gastheren op een hoge veiligheidsinterface gehuurd op een laag veiligheidsinterface.



1. Specificeer de bron(nen) van het verkeer die moet worden vertaald. Hier wordt NAT regel nummer **1** gedefinieerd en al verkeer van binnen en DMZ hosts toegestaan.`ASA-AIP-CLI (configuratie)# nat (binnenkant) 1 172.20.1.0 255.255.255.0ASA-AIP-CLI (configuratie)# nat (binnenkant) 1 192.168.1.0 255.255.255.0`
2. Specificeer welk adres, adrespool of interface het NATed-verkeer moet gebruiken wanneer het de externe interface betreedt. In dit geval wordt PAT uitgevoerd met het externe interfaceadres. Dit is vooral handig wanneer het externe interfaceadres niet van tevoren bekend is, zoals in een DHCP-configuratie. Hier wordt het algemene commando uitgegeven met dezelfde NAT-ID van **1**, dat gekoppeld is aan de NAT-regels van hetzelfde ID.`ASA 5500-AIP-CLI (configuratie)# mondiaal (Buiten) 1 interface`

Tip: Als u de NAT-configuratie wijzigt, wordt u aangeraden de huidige NAT-vertalingen te verwijderen. U kunt de vertaaltabel wissen met de **duidelijke** opdracht. **Wees voorzichtig als u dit doet** omdat het verwijderen van de vertaaltabel alle huidige verbindingen die vertalingen gebruiken, koppelt. Het alternatief voor het wegwerken van de vertaaltabel is om op de huidige vertalingen te wachten tot de tijd is verstreken, maar dit wordt niet aanbevolen, omdat onverwacht gedrag kan resulteren in het aanleggen van nieuwe verbindingen met de nieuwe regels.

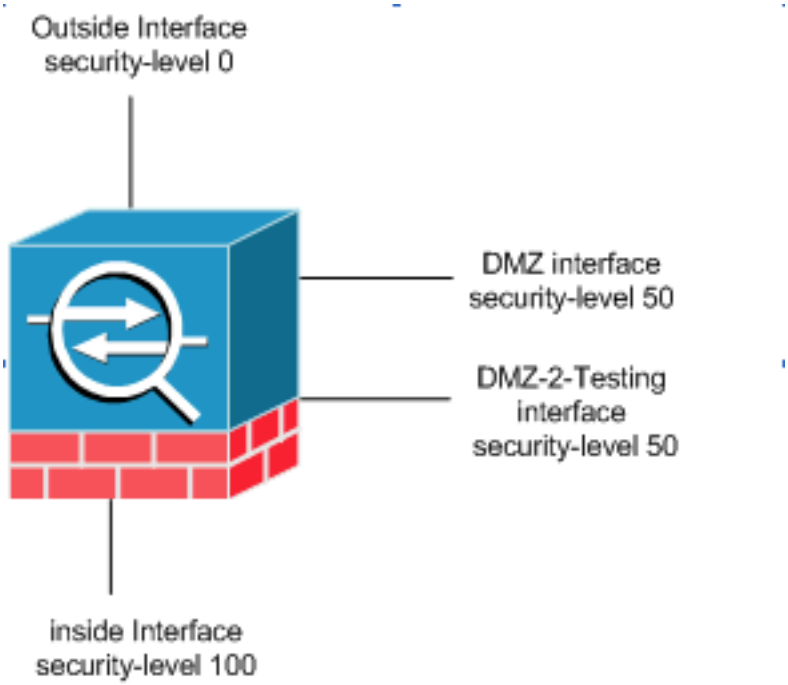
Opmerking: Als u het verkeer wilt blokkeren van de hogere veiligheidszone (binnenin) naar de lagere veiligheidszone (internet/DMZ), maak dan een ACL en pas deze toe op de interne interface van de PIX/ASA als inkomende.

OPMERKING: Voorbeeld: Om het port 80 verkeer van de gastheer 172.20.1.100 op het binnennetwerk aan het internet te blokkeren, gebruik dit:

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

Communicatie op hetzelfde beveiligingsniveau

De eerste configuratie laat zien dat de interfaces "DMZ" en "DMZ-2-testen" zijn ingesteld op veiligheidsniveau (50); deze twee interfaces kunnen normaal gesproken niet praten . Hier staan we deze interfaces toe om met deze opdracht te praten:




```
ASA 5500-AIP-CLI (configuratie)# verkeer met dezelfde beveiliging en tussen interfaces
```

Opmerking: Ook al is de "Dezelfde security traffic vergunningen inter-interface" ingesteld voor dezelfde security level interfaces (DMZ en "DMZ-2-tests"), toch heeft het nog een vertaalregel (statische/dynamische) nodig om toegang te krijgen tot de middelen die in die interfaces zijn geplaatst.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- Aansluitingen voor probleemoplossing via PIX en ASA
- NAT-configuratiesControleer NAT en probleemoplossing

Gerelateerde informatie

- Cisco ASA-opdracht
- Cisco PIX-opdracht Referentie
- Cisco ASA fout- en systeemmeldingen
- Cisco PIX-fout- en systeemmeldingen
- Technische ondersteuning en documentatie – Cisco Systems