PIX/ASA 7.x: Aktivieren/Deaktivieren der Kommunikation zwischen Schnittstellen

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für verschiedene Formen der Kommunikation zwischen den Schnittstellen der ASA/PIX Security Appliance.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- IP-Adressen und Standard-Gateway-Zuweisung
- Physische Netzwerkverbindungen zwischen Geräten
- Kommunikations-Port # für implementierten Service identifiziert

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Adaptive Security Appliance mit Softwareversion 7.x und höher
- Windows 2003-Server
- Windows XP-Workstations

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- Firewalls der Serie PIX 500 mit 7.x und höher

Konventionen

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

Hintergrundinformationen

Dieses Dokument beschreibt die erforderlichen Schritte, um die Kommunikation zwischen verschiedenen Schnittstellen zu ermöglichen. So genannte Kommunikationsformen werden behandelt:

1. Kommunikation von Hosts außerhalb, die Zugriff auf Ressourcen in der DMZ benötigen
2. Kommunikation von Hosts im internen Netzwerk, die Zugriff auf Ressourcen im DMZ benötigen
3. Kommunikation von Hosts im Innen- und DMZ-Netzwerk, die Zugriff auf Ressourcen im Außenbereich benötigen

NAT

In unserem Beispiel verwenden wir Network Address Translation (NAT) und Port Address Translation (PAT) in unserer Konfiguration. Bei der Adressumwandlung wird die tatsächliche Adresse (lokal) in einem Paket durch eine zugeordnete Adresse (global) ersetzt, die im Zielnetzwerk routbar ist. NAT besteht aus zwei Schritten: der Prozess, bei dem eine echte Adresse in eine zugeordnete Adresse übersetzt wird, und der Prozess zum Rückgängigmachen der Übersetzung für den zurückgegebenen Datenverkehr. In diesem Konfigurationsleitfaden werden zwei Formen der Adressübersetzung verwendet: Statisch und dynamisch.

Bei dynamischen Übersetzungen kann jeder Host für jede nachfolgende Übersetzung eine andere Adresse oder einen anderen Port verwenden. Dynamische Übersetzungen können verwendet

werden, wenn lokale Hosts eine oder mehrere gängige globale Adressen freigeben oder "verstecken". In diesem Modus kann eine lokale Adresse keine globale Adresse dauerhaft für die Übersetzung reservieren. Stattdessen wird die Adressenübersetzung auf einer Many-to-One- oder Many-to-Many-Basis durchgeführt, und die Übersetzungseinträge werden nur so erstellt, wie sie benötigt werden. Sobald ein Übersetzungseintrag frei von Verwendung ist, wird er gelöscht und anderen lokalen Hosts zur Verfügung gestellt. Diese Art der Übersetzung eignet sich vor allem für ausgehende Verbindungen, bei denen internen Hosts nur bei Herstellung von Verbindungen eine dynamische Adresse oder Portnummer zugewiesen wird. Es gibt zwei Arten der dynamischen Adressübersetzung:

- Dynamische NAT - Lokale Adressen werden in die nächste verfügbare globale Adresse in einem Pool übersetzt. Die Übersetzung findet auf Eins-zu-Eins-Basis statt, sodass der Pool globaler Adressen ausgefüllt werden kann, wenn eine größere Anzahl lokaler Hosts gleichzeitig eine Übersetzung benötigen.
- NAT Overload (PAT) - Lokale Adressen werden in eine einzige globale Adresse übersetzt. Jede Verbindung wird eindeutig festgelegt, wenn die nächste verfügbare, hochgeordnete Portnummer der globalen Adresse als Verbindungsquelle zugewiesen wird. Die Übersetzung findet auf Basis von "Many-to-One" statt, da viele lokale Hosts eine gemeinsame globale Adresse verwenden.

Bei der statischen Übersetzung wird eine feste Übersetzung der richtigen Adresse(n) in zugeordnete Adressen erstellt. Eine statische NAT-Konfiguration weist jeder Verbindung eines Hosts dieselbe Adresse zu und ist eine persistente Übersetzungsregel. Übersetzungen statischer Adressen werden verwendet, wenn ein interner oder lokaler Host für jede Verbindung dieselbe globale Adresse haben muss. Die Adressumwandlung findet auf Einzelbasis statt. Statische Übersetzungen können für einen einzelnen Host oder für alle Adressen in einem IP-Subnetz definiert werden.

Der Hauptunterschied zwischen dynamischer NAT und einem Adressbereich für statische NAT besteht darin, dass ein Remote-Host eine Verbindung zu einem übersetzten Host initiieren kann (wenn eine Zugriffsliste vorhanden ist, die dies zulässt), während dies bei dynamischer NAT nicht der Fall ist. Außerdem benötigen Sie eine identische Anzahl zugeordneter Adressen mit statischer NAT.

Die Sicherheits-Appliance übersetzt eine Adresse, wenn eine NAT-Regel mit dem Datenverkehr übereinstimmt. Wenn keine NAT-Regel übereinstimmt, wird die Verarbeitung für das Paket fortgesetzt. Die Ausnahme ist, wenn Sie NAT-Steuerelement aktivieren. Bei der NAT-Kontrolle müssen Pakete, die von einer höheren Sicherheitsschnittstelle (innen) zu einer niedrigeren Sicherheitsstufe (außen) übertragen werden, einer NAT-Regel entsprechen, oder die Verarbeitung für die Pakete wird unterbrochen. Informationen zur allgemeinen Konfiguration finden Sie im PIX/ASA 7.x NAT- und PAT-Dokument. Weitere Informationen zur Funktionsweise von NAT finden Sie im Leitfaden Funktionsweise von NAT.

Tipp: Wenn Sie die NAT-Konfiguration ändern, sollten Sie die aktuellen NAT-Übersetzungen löschen. Sie können die Übersetzungstabelle mit dem Befehl **clear xlate** löschen. **Seien Sie jedoch vorsichtig, wenn Sie dies tun**, da beim Löschen der Übersetzungstabelle alle aktuell vorhandenen Verbindungen, die Übersetzungen verwenden, getrennt werden. Die Alternative zum Löschen der Übersetzungstabelle besteht darin, auf eine Zeitüberschreitung der aktuellen Übersetzungen zu warten. Dies wird jedoch nicht empfohlen, da ein unerwartetes Verhalten bei der Erstellung neuer Verbindungen mit den neuen Regeln auftreten kann.

Sicherheitsstufen

Der Wert auf Sicherheitsebene steuert, wie Hosts/Geräte an den verschiedenen Schnittstellen miteinander interagieren. Standardmäßig können Hosts/Geräte, die mit Schnittstellen mit höheren Sicherheitsstufen verbunden sind, auf Hosts/Geräte zugreifen, die mit Schnittstellen mit niedrigeren Sicherheitsstufen verbunden sind. Hosts/Geräte, die mit Schnittstellen mit Schnittstellen mit Schnittstellen mit niedriger Sicherheit verbunden sind, können ohne die Erlaubnis von Zugriffslisten nicht auf Hosts/Geräte zugreifen, die mit Schnittstellen mit Schnittstellen mit Schnittstellen mit höherem Sicherheitsgrad verbunden sind.

Der Befehl **auf Sicherheitsebene** ist neu in Version 7.0 und ersetzt den Teil des Befehls **name**, dem die Sicherheitsstufe für eine Schnittstelle zugewiesen wurde. Zwei Schnittstellen, "die Innen"- und "Außen"-Schnittstellen, haben standardmäßige Sicherheitsstufen, die jedoch mit dem Befehl **auf Sicherheitsebene** überschrieben werden können. Wenn Sie eine Schnittstelle "inside" nennen, erhalten Sie eine Standardsicherheitsstufe von 100; Eine Schnittstelle mit dem Namen "outside" erhält die Standardsicherheitsstufe 0. Alle anderen neu hinzugefügten Schnittstellen erhalten die Standardsicherheitsstufe 0. Um einer Schnittstelle eine neue Sicherheitsstufe zuzuweisen, verwenden Sie im Schnittstellenbefehlsmodus den Befehl **Sicherheitsstufe**. Die Sicherheitsstufen liegen zwischen 1 und 100.

Hinweis: Sicherheitsstufen werden nur verwendet, um zu bestimmen, wie die Firewall den Datenverkehr überprüft und behandelt. Datenverkehr, der von einer Schnittstelle mit höherer Sicherheit an eine Schnittstelle mit niedrigerer Sicherheit weitergeleitet wird, wird beispielsweise mit weniger strengen Standardrichtlinien weitergeleitet als Datenverkehr, der von einer Schnittstelle mit niedrigerer Sicherheit zu einer Schnittstelle mit höherer Sicherheit führt. Weitere Informationen zu Sicherheitsstufen finden Sie im Referenzhandbuch zum ASA/PIX 7.x-Befehl.

Mit ASA/PIX 7.x können außerdem mehrere Schnittstellen mit demselben Sicherheitsgrad konfiguriert werden. Beispielsweise können mehrere Schnittstellen, die mit Partnern oder anderen DMZs verbunden sind, jeweils eine Sicherheitsstufe von 50 erhalten. Standardmäßig können dieselben Sicherheitsschnittstellen nicht miteinander kommunizieren. Um dieses Problem zu umgehen, wurde der Befehl **für die** Berechtigung **des Datenverkehrs zwischen den Schnittstellen** eingeführt. Dieser Befehl ermöglicht die Kommunikation zwischen Schnittstellen derselben Sicherheitsstufe. Weitere Informationen zur gleichen Sicherheit zwischen den Schnittstellen finden Sie im Leitfaden Befehlsreferenz Konfigurieren von Schnittstellenparametern und in diesem Beispiel.

ACL

Zugriffskontrolllisten bestehen in der Regel aus mehreren Zugriffskontrolleinträgen (ACEs), die intern von der Sicherheits-Appliance in einer verknüpften Liste organisiert werden. ACEs beschreiben eine Gruppe von Datenverkehr, wie z. B. von einem Host oder Netzwerk, und listen eine Aktion auf, die auf diesen Datenverkehr angewendet werden soll. Diese Aktion wird im Allgemeinen zugelassen oder verweigert. Wenn ein Paket der Zugriffslistenkontrolle unterliegt, durchsucht die Cisco Security Appliance die verknüpfte Liste von ACEs, um eine zu finden, die dem Paket entspricht. **Der erste ACE, der mit der Sicherheits-Appliance übereinstimmt, wird auf das Paket angewendet.** Sobald die Übereinstimmung gefunden wurde, wird die Aktion in diesem ACE (Zulassen oder Ablehnen) auf das Paket angewendet.

Pro Schnittstelle und Richtung ist nur eine Zugriffsliste zulässig. Das bedeutet, dass Sie nur eine Zugriffsliste für eingehenden Datenverkehr an einer Schnittstelle und eine Zugriffsliste für ausgehenden Datenverkehr an einer Schnittstelle haben können. Zugriffslisten, die nicht auf Schnittstellen angewendet werden, z. B. NAT-ACLs, sind unbegrenzt.

Hinweis: Standardmäßig verfügen alle Zugriffslisten am Ende über einen impliziten ACE, der den gesamten Datenverkehr blockiert. Daher entspricht der gesamte Datenverkehr, der nicht mit einem ACE übereinstimmt, den Sie in der Zugriffsliste eingeben, der impliziten Ablehnung am Ende und wird verworfen. Sie müssen über mindestens eine permit-Anweisung in einer Schnittstellenzugriffsliste verfügen, damit der Datenverkehr fließen kann. Ohne eine Genehmigungserklärung wird der gesamte Datenverkehr abgelehnt.

Hinweis: Zugriffslisten werden mit den Befehlen **access-list** und **access-group** implementiert. Diese Befehle werden anstelle der **Kanäle** und **ausgehenden** Befehle verwendet, die in früheren Versionen der PIX-Firewall-Software verwendet wurden. Weitere Informationen zu ACLs finden Sie unter Konfigurieren der IP-Zugriffsliste.

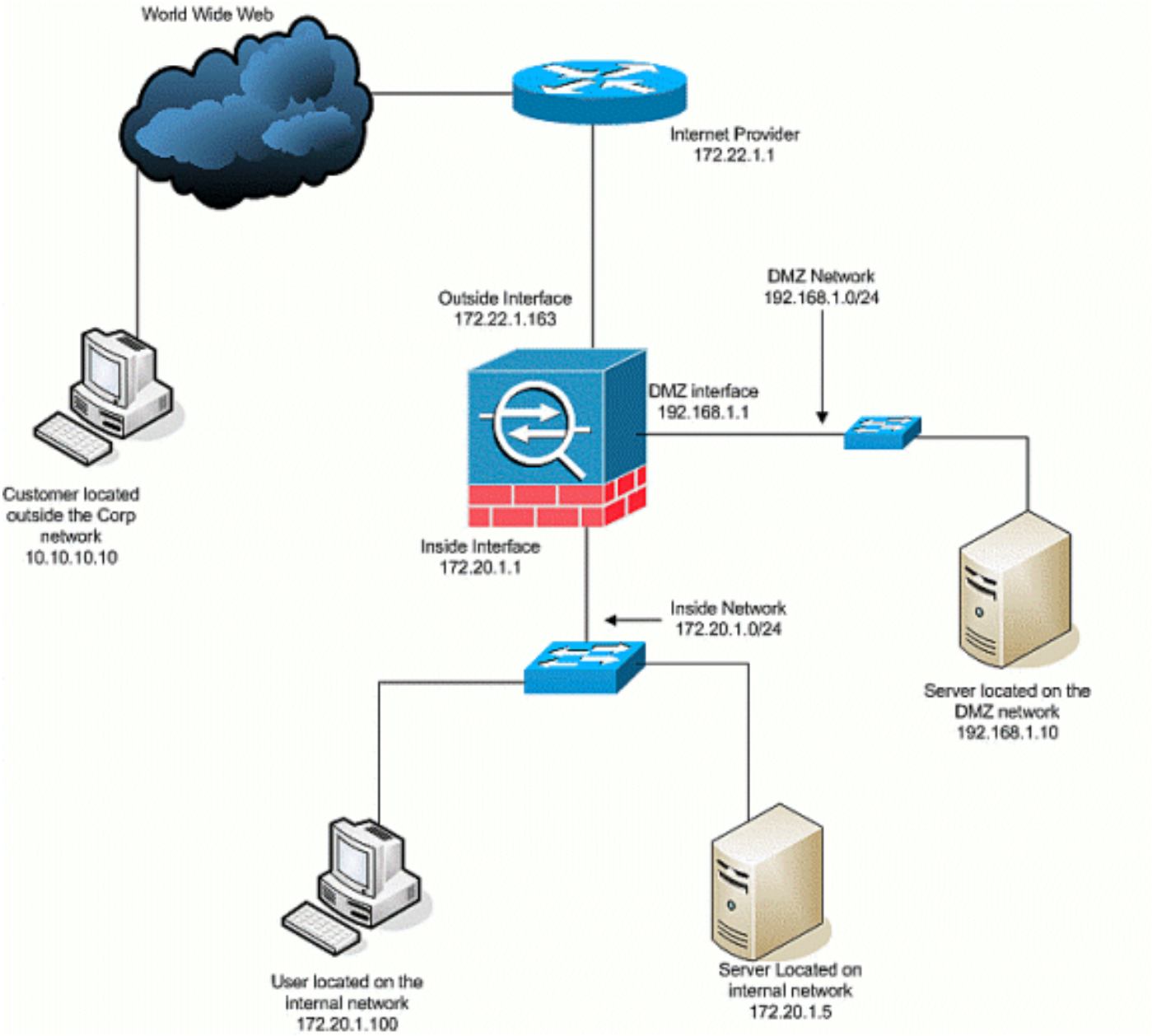
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Erstkonfiguration

In diesem Dokument werden folgende Konfigurationen verwendet:

- Bei dieser grundlegenden Firewall-Konfiguration gibt es derzeit keine NAT/STATIC-Anweisungen.
- Da keine ACLs angewendet werden, wird der implizite ACE, `keine` Zugriffskontrolllisten `zu verweigern`, verwendet.

Gerätename 1

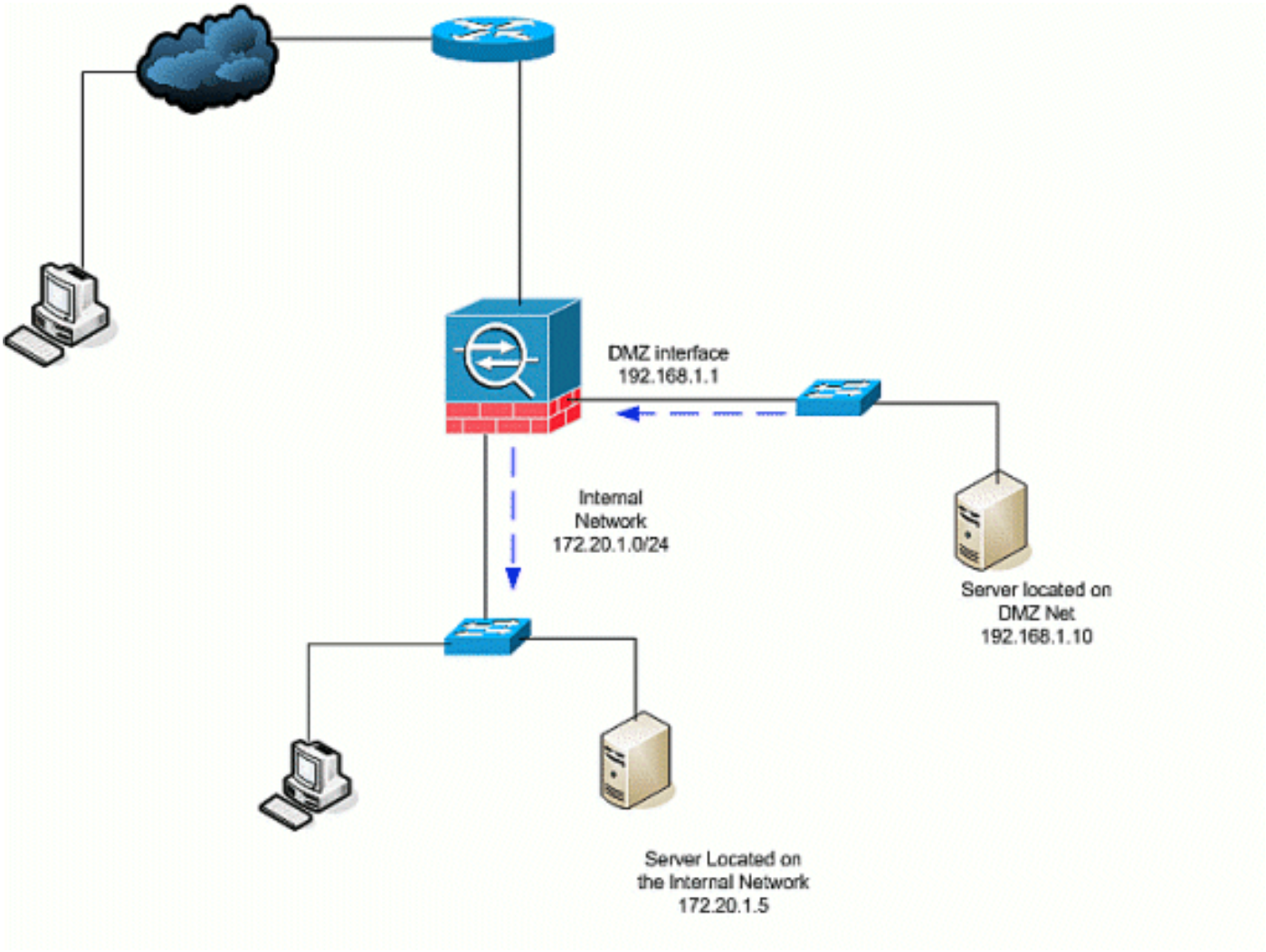
`ASA-AIP-CLI(config)#show running-config`
 	
`ASA Version 7.2(2)`
`!`
`hostname ASA-AIP-CLI`
`domain-name corp.com`
`enable password WwXYvtKrnjXqGbu1 encrypted`
`names`
`!`

```
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 zu innen

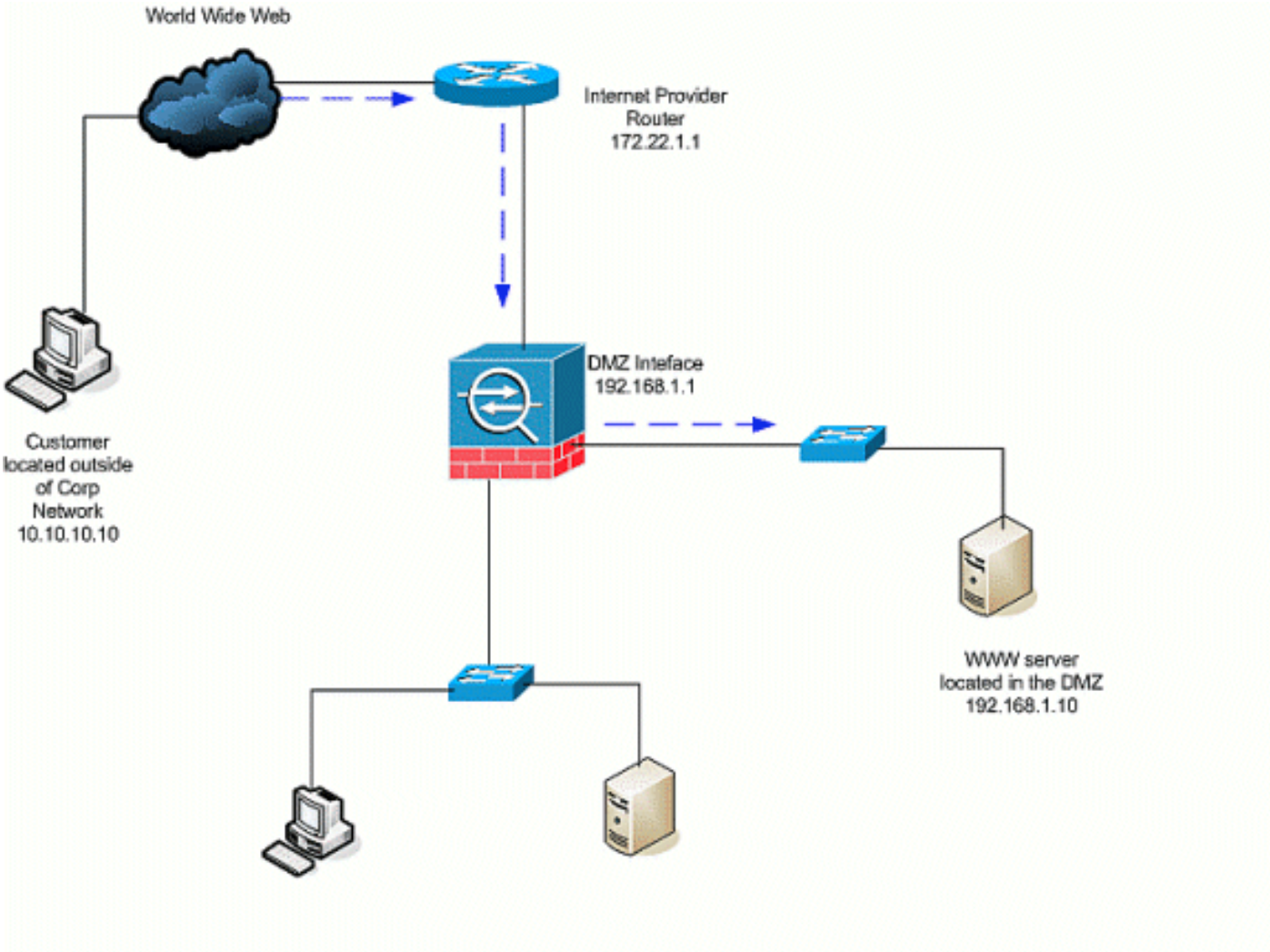
Verwenden Sie diese Befehle, um die Kommunikation von der DMZ zu internen Netzwerk-Hosts zu ermöglichen. In diesem Beispiel muss ein Webserver in der DMZ auf einen AD- und DNS-Server im Inneren zugreifen.



1. Erstellen Sie einen statischen NAT-Eintrag für den AD/DNS-Server in der DMZ. Static NAT erstellt eine feste Übersetzung einer echten Adresse in eine zugeordnete Adresse. Diese zugeordnete Adresse ist eine Adresse, die DMZ-Hosts verwenden können, um auf den internen Server zuzugreifen, ohne dass die tatsächliche Adresse des Servers bekannt sein muss. Mit diesem Befehl wird die DMZ-Adresse 192.168.2.20 der echten internen Adresse 172.20.1.5 zugeordnet.`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. ACLs sind erforderlich, damit eine Schnittstelle mit einer niedrigeren Sicherheitsstufe Zugriff auf eine höhere Sicherheitsstufe haben kann. In diesem Beispiel gewähren wir dem Webserver, der sich in der DMZ (Security 50) befindet, Zugriff auf den AD/DNS-Server im Inneren (Security 100) mit den folgenden spezifischen Service-Ports: DNS, Kerberos und LDAP.`ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq domainASA-AIP-CLI(config)# access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq 389`**Hinweis:** Die ACLs ermöglichen den Zugriff auf die zugeordnete Adresse des in diesem Beispiel erstellten AD/DNS-Servers und nicht auf die tatsächliche interne Adresse.
3. In diesem Schritt wenden Sie die ACL mit dem folgenden Befehl auf die DMZ-Schnittstelle in Eingangsrichtung an:`ASA-AIP-CLI(config)# Access-Group DMZtoInside in der DMZ der Schnittstelle`**Hinweis:** Wenn Sie Port 88 blockieren oder deaktivieren möchten, verwenden Sie z. B. Folgendes:
   ```
   ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
   tcp host 192.168.1.10 host 192.168.2.20 eq 88
   ```
   Tipp: Wenn Sie die NAT-Konfiguration ändern, sollten Sie die aktuellen NAT-Übersetzungen löschen. Sie können die Übersetzungstabelle mit dem Befehl **clear xlate** löschen. **Seien Sie vorsichtig, wenn Sie dies tun**, da beim Löschen der Übersetzungstabelle alle aktuell vorhandenen Verbindungen, die Übersetzungen verwenden, getrennt werden. Die Alternative zum Löschen der Übersetzungstabelle besteht darin, auf eine Zeitüberschreitung der aktuellen Übersetzungen zu warten. Dies wird jedoch nicht empfohlen, da ein unerwartetes Verhalten bei der Erstellung neuer Verbindungen mit den neuen Regeln auftreten kann.Weitere gängige Konfigurationen sind:Mailserver in der DMZSSH-Zugang innen und außenZulässige Remote-Desktop-Sitzungen über PIX-/ASA-GeräteAndere DNS-Lösungen bei Verwendung in der DMZ

Internet zu DMZ

Um die Kommunikation von Benutzern über das Internet oder die externe Schnittstelle (Security 0) mit einem Webserver in der DMZ (Security 50) zu ermöglichen, verwenden Sie die folgenden Befehle:

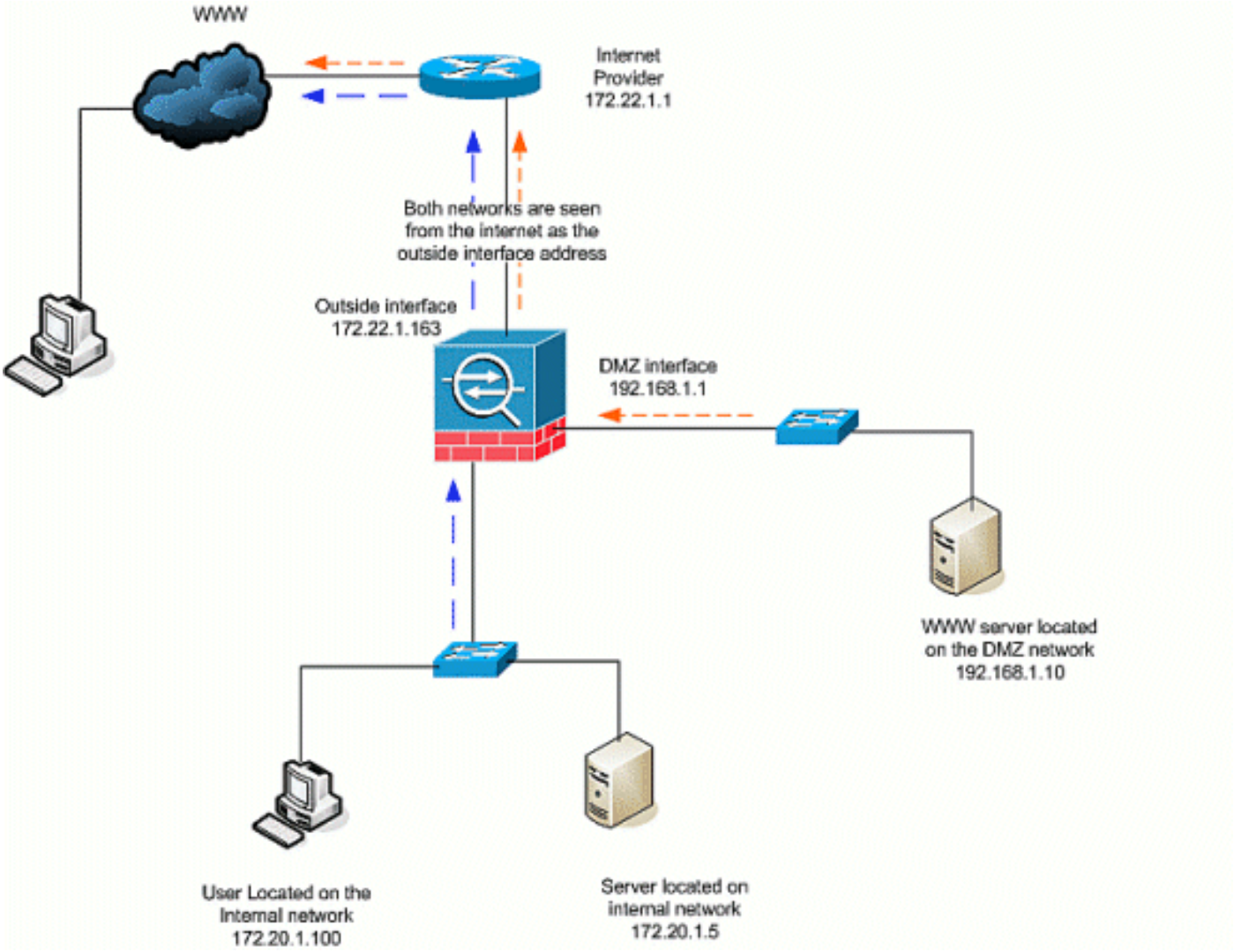


1. Erstellen Sie eine statische Übersetzung für den Webserver in der DMZ nach außen. Static NAT erstellt eine feste Übersetzung einer echten Adresse in eine zugeordnete Adresse. Diese zugeordnete Adresse ist eine Adresse, die Hosts im Internet verwenden können, um auf den Webserver der DMZ zuzugreifen, ohne dass die tatsächliche Adresse des Servers bekannt sein muss. Mit diesem Befehl wird die externe Adresse 172.22.1.25 der echten DMZ-Adresse 192.168.1.10 zugeordnet.`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. Erstellen Sie eine ACL, mit der Benutzer von außen über die zugeordnete Adresse auf den Webserver zugreifen können. Beachten Sie, dass der Webserver auch das FTP hostet.`ASA-AIP-CLI(config)# access-list OutsideDMZ extended permit tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsideDMZ extended permit tcp any host 172.22.1.25 eq ftp`
3. Der letzte Schritt dieser Konfiguration besteht darin, die ACL für den Datenverkehr in Eingangsrichtung auf die externe Schnittstelle anzuwenden.`ASA-AIP-CLI(config)# Access-Group OutsideDMZ in Schnittstelle Outside`**Hinweis:** Beachten Sie, dass Sie pro Schnittstelle und Richtung nur eine Zugriffsliste anwenden können. Wenn Sie bereits eine eingehende ACL auf die externe Schnittstelle angewendet haben, können Sie diese Beispiel-ACL nicht auf diese anwenden. Fügen Sie stattdessen die ACEs in diesem Beispiel zur aktuellen ACL hinzu, die auf die Schnittstelle angewendet wird.**Hinweis:** Wenn Sie beispielsweise den FTP-Datenverkehr vom Internet zur DMZ blockieren oder deaktivieren möchten, verwenden Sie Folgendes:
   ```
   ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
   tcp any host 172.22.1.25 eq ftp
   ```
   Tipp: Wenn Sie die NAT-Konfiguration ändern, sollten Sie die aktuellen NAT-Übersetzungen löschen. Sie können die Übersetzungstabelle mit dem Befehl **clear xlate** löschen. **Seien Sie**

vorsichtig, wenn Sie dies tun, da beim Löschen der Übersetzungstabelle alle aktuell vorhandenen Verbindungen, die Übersetzungen verwenden, getrennt werden. Die Alternative zum Löschen der Übersetzungstabelle besteht darin, auf eine Zeitüberschreitung der aktuellen Übersetzungen zu warten. Dies wird jedoch nicht empfohlen, da ein unerwartetes Verhalten bei der Erstellung neuer Verbindungen mit den neuen Regeln auftreten kann.

Inside/DMZ zum Internet

In diesem Szenario erhalten Hosts, die sich an der inneren Schnittstelle (Security 100) der Sicherheits-Appliance befinden, Zugriff auf das Internet über die externe Schnittstelle (Security 0). Dies wird durch die Form der PAT- oder NAT-Überladung (Dynamic NAT) erreicht. Im Gegensatz zu anderen Szenarien ist in diesem Fall keine ACL erforderlich, da Hosts mit einer Hochsicherheitsschnittstelle auf Hosts mit niedriger Sicherheitsstufe zugreifen.



1. Geben Sie die Quelle(n) des Datenverkehrs an, der übersetzt werden soll. Hier wird die NAT-Regel Nr. 1 definiert, und der gesamte Datenverkehr von internen und DMZ-Hosts ist zulässig.`ASA-AIP-CLI(config)# nat (inside) 1 172.20.1.0 255.255.255.0ASA-AIP-CLI(config)# nat (inside) 1 192.168.1.0 255.255.255.0`
2. Geben Sie an, welche Adresse, welchen Adresspool oder welche Schnittstelle der NAT-Verkehr verwenden muss, wenn er auf die externe Schnittstelle zugreift. In diesem Fall wird die PAT mit der externen Schnittstellenadresse durchgeführt. Dies ist besonders dann

nützlich, wenn die externe Schnittstellenadresse nicht im Voraus bekannt ist, z. B. in einer DHCP-Konfiguration. Hier wird der globale Befehl mit derselben NAT-ID von **1** ausgegeben, die mit den NAT-Regeln derselben ID verknüpft ist.`ASA-AIP-CLI(config)# global (extern) 1 Schnittstelle`

Tipp: Wenn Sie die NAT-Konfiguration ändern, sollten Sie die aktuellen NAT-Übersetzungen löschen. Sie können die Übersetzungstabelle mit dem Befehl **clear xlate** löschen. **Seien Sie vorsichtig, wenn Sie dies tun**, da beim Löschen der Übersetzungstabelle alle aktuell vorhandenen Verbindungen, die Übersetzungen verwenden, getrennt werden. Die Alternative zum Löschen der Übersetzungstabelle besteht darin, auf eine Zeitüberschreitung der aktuellen Übersetzungen zu warten. Dies wird jedoch nicht empfohlen, da ein unerwartetes Verhalten bei der Erstellung neuer Verbindungen mit den neuen Regeln auftreten kann.

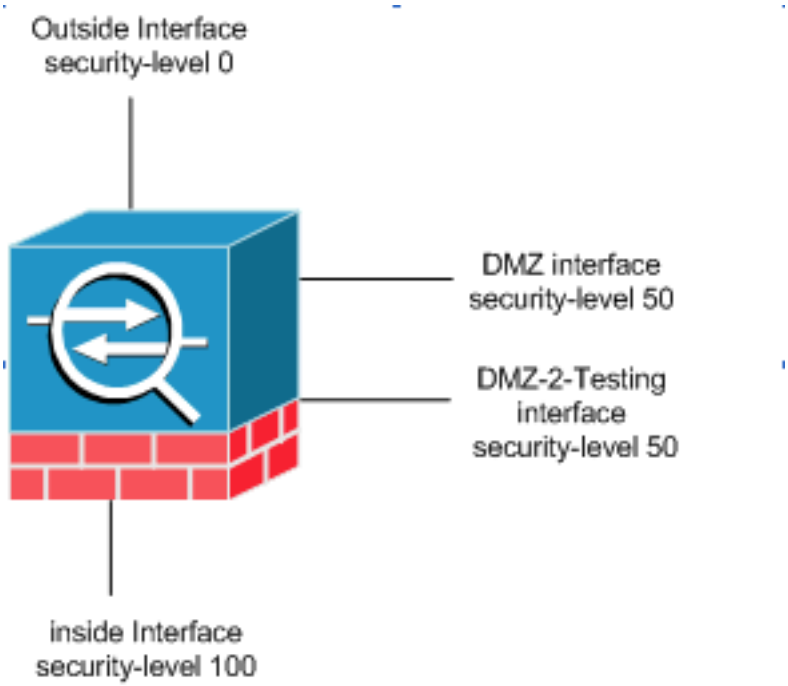
Hinweis: Wenn Sie den Datenverkehr von der höheren Sicherheitszone (innen) zur unteren Sicherheitszone (Internet/DMZ) blockieren möchten, erstellen Sie eine ACL und wenden ihn als eingehenden Datenverkehr auf die interne Schnittstelle von PIX/ASA an.

Hinweis: Beispiel: Um den Port 80-Datenverkehr vom Host 172.20.1.100 im internen Netzwerk zum Internet zu blockieren, verwenden Sie Folgendes:

```
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
```

Kommunikation auf Sicherheitsebene

Die Erstkonfiguration zeigt, dass die Schnittstellen "DMZ" und "DMZ-2-testing" mit der Sicherheitsstufe (50) konfiguriert sind. Standardmäßig können diese beiden Schnittstellen nicht sprechen. Hier können diese Schnittstellen mit dem folgenden Befehl kommunizieren:




```
ASA-AIP-CLI(config)#-Datenverkehr mit identischer Sicherheitsstufe erlaubt die
Schnittstellenverbindung
```

Hinweis: Obwohl der "Datenverkehr, der die Schnittstelle zwischen zwei Sicherheitsstufen zulässt" für dieselben Sicherheitsschnittstellen konfiguriert wurde ("DMZ" und "DMZ-2-testing"), ist für den

Zugriff auf die Ressourcen dieser Schnittstellen immer noch eine Übersetzungsregel (statisch/dynamisch) erforderlich.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Fehlerbehebung bei Verbindungen über PIX und ASA
- NAT-KonfigurationenNAT und Fehlerbehebung überprüfen

Zugehörige Informationen

- Cisco ASA-Befehlsreferenz
- Cisco PIX-Befehlsreferenz
- Fehler- und Systemmeldungen der Cisco ASA
- Cisco PIX-Fehler- und Systemmeldungen
- Technischer Support und Dokumentation - Cisco Systems