PIX/ASA 7.x: Activar/desactivar la comunicación entre interfaces

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de las diversas formas de comunicación entre las interfaces en el dispositivo de seguridad ASA/PIX.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Direcciones IP y asignación de gateway predeterminada
- Conectividad de red física entre dispositivos
- Puerto de comunicación # identificado para el servicio implementado

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Adaptive Security Appliance que ejecuta la versión de software 7.x y posteriores
- Servidores Windows 2003
- Estaciones de trabajo de Windows XP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- Firewalls PIX de la serie 500 que ejecutan 7.x y versiones posteriores

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Este documento describe los pasos necesarios para permitir que la comunicación fluya entre diferentes interfaces. Se discuten formas de comunicación como estas:

1. Comunicación de los hosts ubicados en el exterior que requieren acceso a los recursos ubicados en la DMZ
2. Comunicación de los hosts de la red interna que requieren acceso a los recursos ubicados en la DMZ
3. Comunicación de los hosts en el interior y la red DMZ que requieren acceso a los recursos en el exterior

NAT

En nuestro ejemplo, utilizamos Traducción de direcciones de red (NAT) y Traducción de direcciones de puerto (PAT) en nuestra configuración. La traducción de direcciones sustituye la dirección real (local) en un paquete con una dirección asignada (global) que se puede enrutar en la red de destino. NAT consta de dos pasos: el proceso en el que una dirección real se traduce en una dirección asignada y luego el proceso para deshacer la traducción para el tráfico que devuelve. Hay dos formas de traducción de direcciones que utilizamos en esta guía de configuración: Estático y dinámico.

Las traducciones dinámicas permiten que cada host utilice una dirección o puerto diferente para cada traducción posterior. Las traducciones dinámicas se pueden utilizar cuando los hosts locales comparten o "ocultan detrás" una o más direcciones globales comunes. En este modo, una dirección local no puede reservar permanentemente una dirección global para la traducción. En su lugar, la traducción de direcciones se realiza en una base de varios a uno o de muchos a muchos, y las entradas de traducción se crean sólo cuando se necesitan. En cuanto una entrada

de traducción no se utiliza, se elimina y se pone a disposición de otros hosts locales. Este tipo de traducción es más útil para las conexiones salientes, en las que a los hosts internos se les asigna una dirección dinámica o un número de puerto solamente a medida que se realizan las conexiones. Hay dos formas de traducción dinámica de direcciones:

- NAT dinámica: las direcciones locales se traducen a la siguiente dirección global disponible en un conjunto. La traducción se realiza de uno a uno, por lo que es posible agotar el conjunto de direcciones globales si un mayor número de hosts locales requieren traducción en un momento dado.
- Sobrecarga NAT (PAT): las direcciones locales se traducen en una única dirección global; cada conexión se hace única cuando el siguiente número de puerto de orden superior disponible de la dirección global se asigna como origen de la conexión. La traducción se realiza de forma múltiple porque muchos hosts locales comparten una dirección global común.

La traducción estática crea una traducción fija de las direcciones reales a las direcciones asignadas. Una configuración NAT estática asigna la misma dirección para cada conexión por un host y es una regla de traducción persistente. Las traducciones de direcciones estáticas se utilizan cuando un host interno o local necesita tener la misma dirección global para cada conexión. La traducción de direcciones se realiza de forma individual. Las traducciones estáticas se pueden definir para un solo host o para todas las direcciones contenidas en una subred IP.

La diferencia principal entre NAT dinámica y un rango de direcciones para NAT estática es que NAT estática permite que un host remoto inicie una conexión con un host traducido (si hay una lista de acceso que lo permite), mientras que NAT dinámica no. También necesita un número igual de direcciones asignadas con NAT estática.

El dispositivo de seguridad traduce una dirección cuando una regla NAT coincide con el tráfico. Si no coincide ninguna regla NAT, el procesamiento del paquete continúa. La excepción es cuando se habilita el control NAT. El control NAT requiere que los paquetes que atraviesan desde una interfaz de seguridad más alta (interna) a un nivel de seguridad inferior (externa) coincidan con una regla NAT, o bien el procesamiento para el paquete se detiene. Para ver la información de configuración común, consulte el documento PIX/ASA 7.x NAT y PAT. Para entender mejor cómo funciona NAT, consulte la guía Cómo funciona NAT.

Sugerencia: Siempre que cambie la configuración de NAT, se recomienda borrar las traducciones NAT actuales. Puede borrar la tabla de traducción con el comando **clear xlate**. **Sin embargo, tenga cuidado al hacer esto** ya que borrar la tabla de traducción desconecta todas las conexiones actuales que usan traducciones. La alternativa a borrar la tabla de traducción es esperar a que las traducciones actuales se agote el tiempo de espera, pero esto no se recomienda porque se puede producir un comportamiento inesperado, ya que se crean nuevas conexiones con las nuevas reglas.

Niveles de seguridad

El valor de nivel de seguridad controla cómo los hosts/dispositivos en las diferentes interfaces interactúan entre sí. De forma predeterminada, los hosts/dispositivos conectados a interfaces con niveles de mayor seguridad pueden acceder a los hosts/dispositivos conectados a la interfaz con niveles de menor seguridad. Los hosts/dispositivos conectados a interfaces con interfaces de menor seguridad no pueden acceder a los hosts/dispositivos que se conectan a interfaces con interfaces de mayor seguridad sin el permiso de las listas de acceso.

El comando **security-level** es nuevo en la versión 7.0 y reemplaza la parte del comando **nameif** que asignó el nivel de seguridad para una interfaz. Dos interfaces, las interfaces "interna" y "externa", tienen niveles de seguridad predeterminados, pero se pueden reemplazar con el comando **security-level**. Si nombra una interfaz "interna", se le da un nivel de seguridad predeterminado de 100; una interfaz denominada "outside" recibe un nivel de seguridad predeterminado de 0. Todas las demás interfaces recién agregadas reciben un nivel de seguridad predeterminado de 0. Para asignar un nuevo nivel de seguridad a una interfaz, utilice el comando **security-level** en el modo de comando interface. Los niveles de seguridad varían entre 1 y 100.

Nota: Los niveles de seguridad sólo se utilizan para determinar cómo inspecciona y gestiona el tráfico el firewall. Por ejemplo, el tráfico que pasa de una interfaz de mayor seguridad a una más baja se reenvía con políticas predeterminadas menos estrictas que el tráfico que proviene de una interfaz de menor seguridad hacia una de mayor seguridad. Para obtener más información sobre los niveles de seguridad, consulte la guía de referencia de comandos ASA/PIX 7.x.

ASA/PIX 7.x también introdujo la capacidad de configurar varias interfaces con el mismo nivel de seguridad. Por ejemplo, se puede dar a varias interfaces conectadas a partners u otras DMZ un nivel de seguridad de 50. De forma predeterminada, estas mismas interfaces de seguridad no pueden comunicarse entre sí. Para solucionar esto, se introdujo el comando **same-security-traffic permit inter-interface**. Este comando permite la comunicación entre interfaces del mismo nivel de seguridad. Para obtener más información sobre la misma seguridad entre interfaces, consulte la guía Referencia de Comandos Configuración de Parámetros de Interfaz y vea este ejemplo.

ACL

Las listas de control de acceso suelen constar de varias entradas de control de acceso (ACE) organizadas internamente por el dispositivo de seguridad en una lista vinculada. Las ACE describen un conjunto de tráfico como el de un host o red y enumeran una acción que se debe aplicar a ese tráfico, generalmente permiten o niegan. Cuando un paquete se somete al control de lista de acceso, Cisco Security Appliance busca esta lista vinculada de ACE para encontrar una que coincida con el paquete. **La primera ACE que coincide con el dispositivo de seguridad es la que se aplica al paquete.** Una vez que se encuentra la coincidencia, la acción en esa ACE (permit o deny) se aplica al paquete.

Sólo se permite una lista de acceso por interfaz, por dirección. Esto significa que sólo puede tener una lista de acceso que se aplica al tráfico entrante en una interfaz y una lista de acceso que se aplica al tráfico saliente en una interfaz. Las listas de acceso que no se aplican a las interfaces, como las ACL NAT, son ilimitadas.

Nota: De forma predeterminada, todas las listas de acceso tienen una ACE implícita al final que deniega todo el tráfico, de modo que todo el tráfico que no coincide con ninguna ACE que introduzca en la lista de acceso coincida con la denegación implícita al final y se descarte. Debe tener al menos una sentencia permit en una lista de acceso de interfaz para que el tráfico fluya. Sin una sentencia permit, todo el tráfico se niega.

Nota: La lista de acceso se implementa con los comandos **access-list** y **access-group**. Estos comandos se utilizan en lugar de los comandos **conduit** y **outbound**, que se utilizaron en versiones anteriores del software de firewall PIX. Para obtener más información sobre las ACL, consulte Configuración de la Lista de Acceso IP.

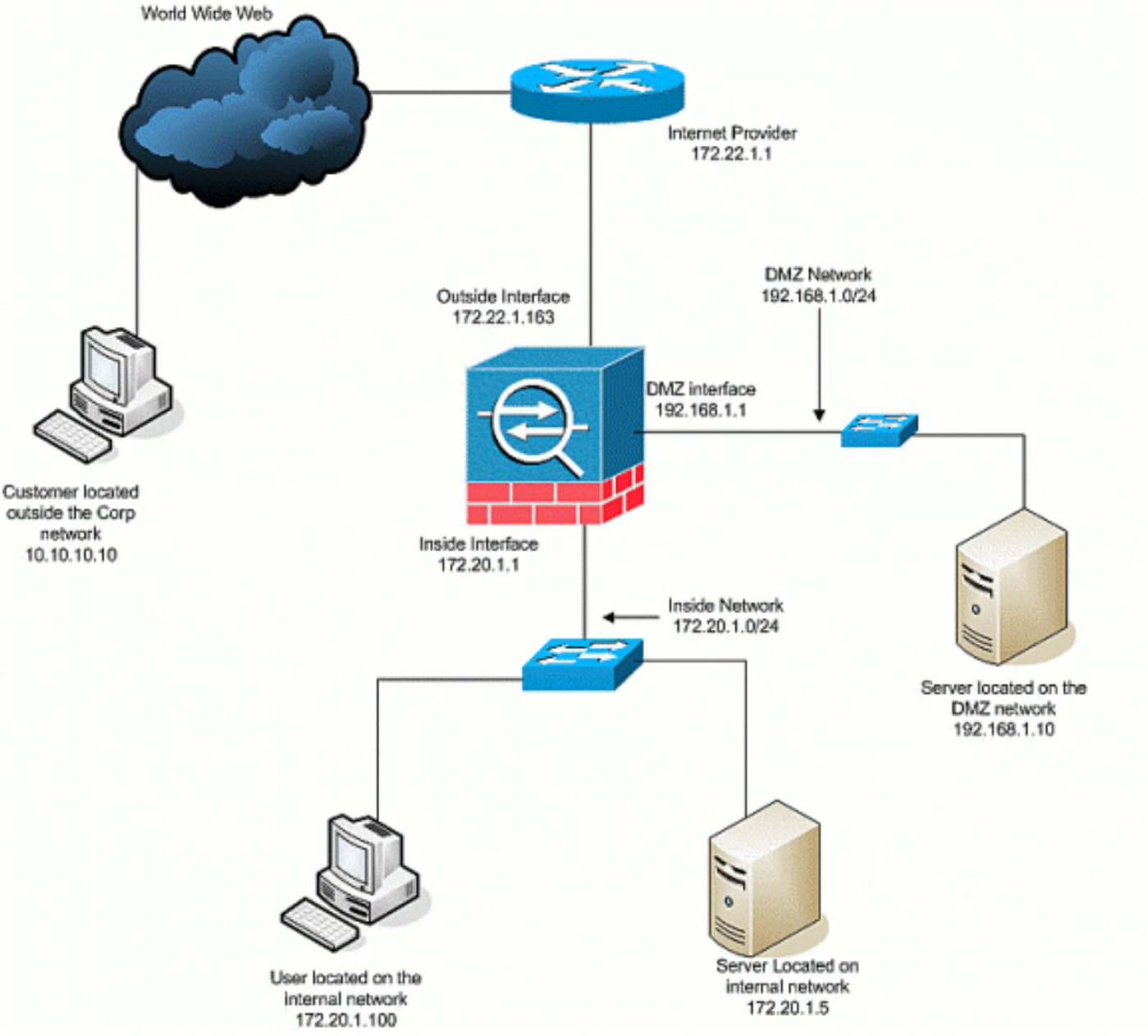
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuración inicial

En este documento, se utilizan estas configuraciones:

- Con esta configuración básica del firewall, actualmente no hay sentencias NAT/STATIC.
- No hay ACL aplicadas, por lo que la ACE implícita de `negar cualquier` se utiliza actualmente.

Nombre del dispositivo 1

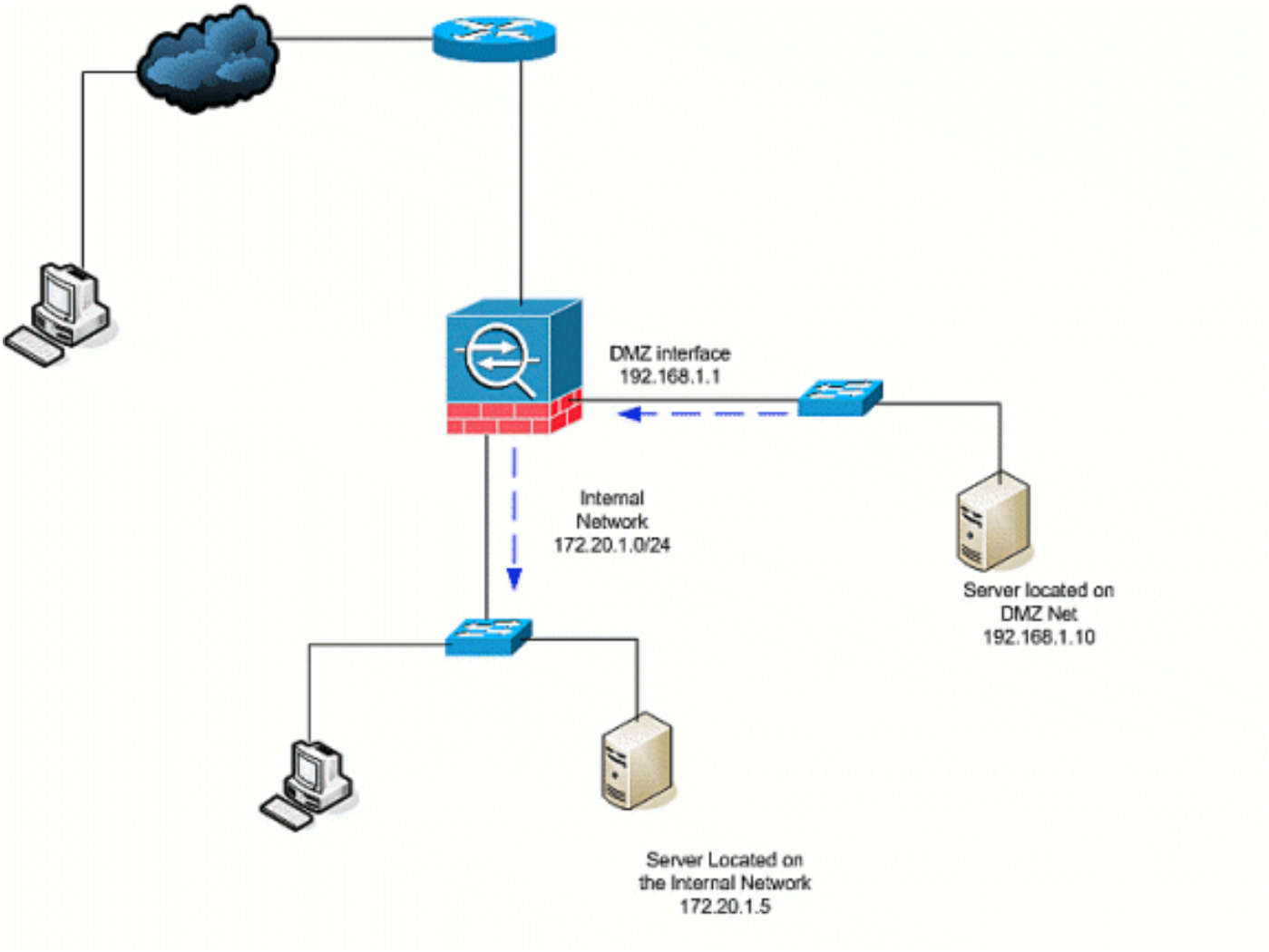
```
ASA-AIP-CLI(config)#show running-config

 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 a interno

Para permitir la comunicación de la DMZ a los hosts de red internos, utilice estos comandos. En este ejemplo, un servidor web en la DMZ necesita acceder a un servidor AD y DNS en el interior.

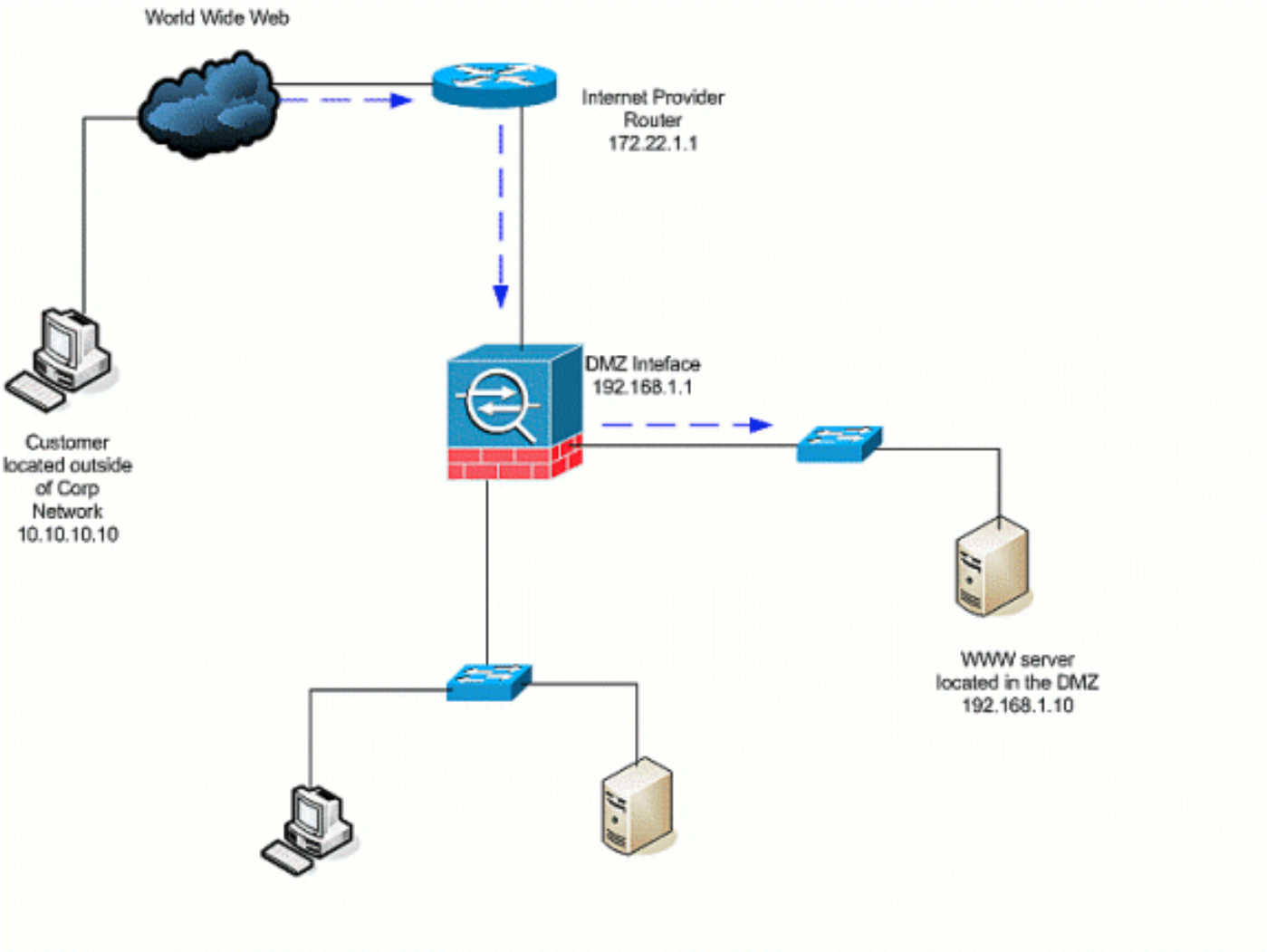


1. Cree una entrada NAT estática para el servidor AD/DNS en la DMZ. La NAT estática crea una traducción fija de una dirección real a una dirección asignada. Esta dirección asignada es una dirección que los hosts DMZ pueden utilizar para acceder al servidor en el interior sin necesidad de conocer la dirección real del servidor. Este comando mapea la dirección DMZ 192.168.2.20 a la dirección interna real 172.20.1.5.`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. Las ACL son necesarias para permitir que una interfaz con un nivel de seguridad inferior tenga acceso a un nivel de seguridad superior. En este ejemplo, damos al servidor web que se encuentra en la DMZ (Seguridad 50) acceso al servidor AD/DNS en el interior (Seguridad 100) con estos puertos de servicio específicos: DNS, Kerberos y LDAP.`ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host dominio 192.168.2.20 eqASA-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`**Nota:** Las ACL permiten el acceso a la dirección asignada del servidor AD/DNS que se creó en este ejemplo y no a la dirección interna real.
3. En este paso, aplica la ACL a la interfaz DMZ en la dirección entrante con este comando:`DMZtoInside del grupo de acceso ASA-AIP-CLI(config)# en la interfaz DMZ`**Nota:** Si desea bloquear o inhabilitar el puerto 88, el tráfico de DMZ al interior, por ejemplo, utilice lo siguiente:
   ```
   ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
   tcp host 192.168.1.10 host 192.168.2.20 eq 88
   ```
   Sugerencia: Siempre que cambie la configuración de NAT, se recomienda borrar las traducciones NAT actuales. Puede borrar la tabla de traducción con el comando **clear xlate**. **Tenga cuidado al hacer esto** ya que borrar la tabla de traducción desconecta todas las

conexiones actuales que usan traducciones. La alternativa a borrar la tabla de traducción es esperar a que las traducciones actuales se agote el tiempo de espera, pero esto no se recomienda porque se puede producir un comportamiento inesperado, ya que se crean nuevas conexiones con las nuevas reglas.Otras configuraciones comunes son las siguientes:Servidores de correo en la DMZAcceso SSH dentro y fueraSesiones permitidas de Escritorio remoto a través de dispositivos PIX/ASAOtras soluciones DNS cuando se utilizan en la DMZ

Internet a DMZ

Para permitir la comunicación de los usuarios en Internet o en la interfaz externa (Seguridad 0) a un servidor web ubicado en la DMZ (Seguridad 50), utilice estos comandos:

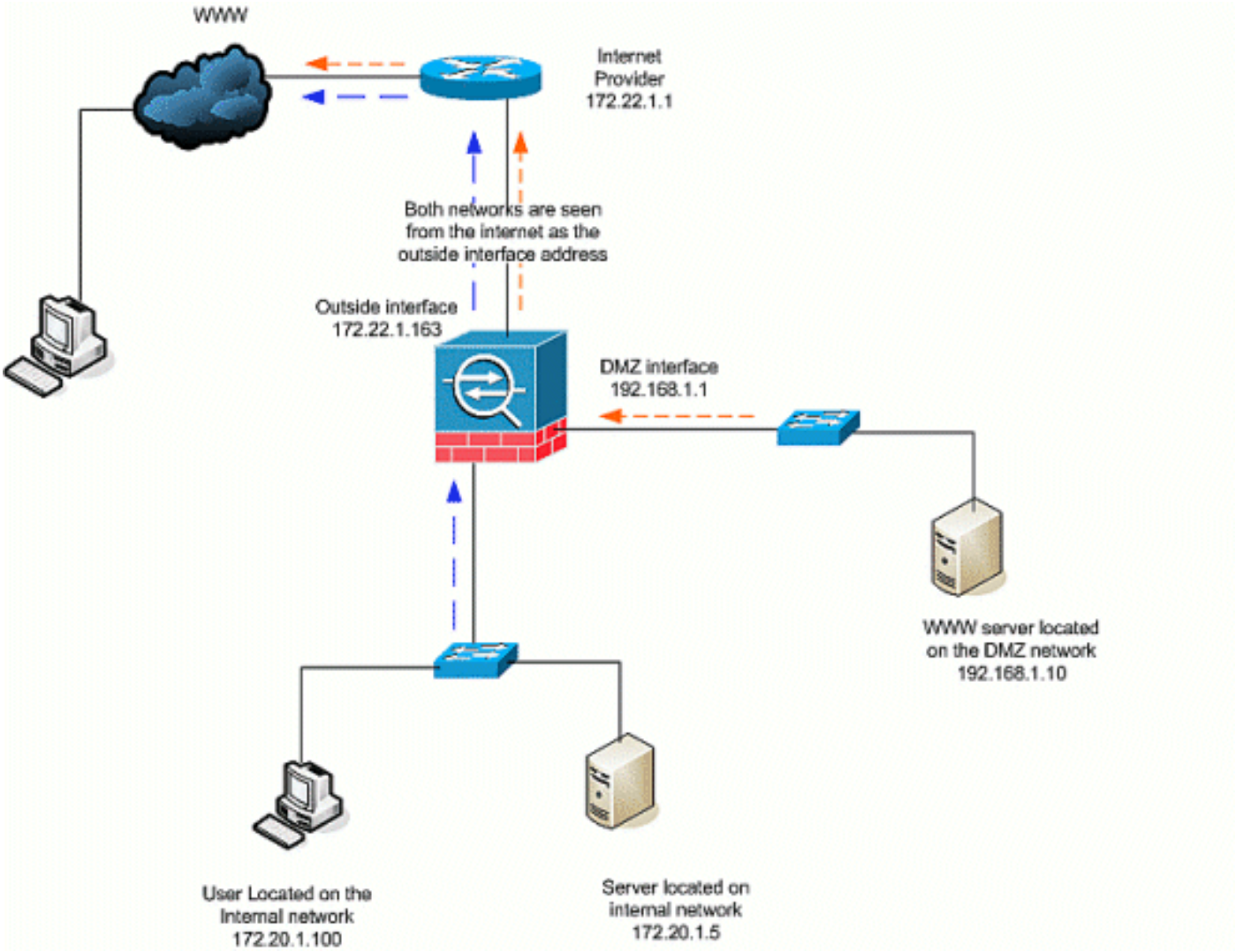


1. Cree una traducción estática para el servidor web en la DMZ al exterior. La NAT estática crea una traducción fija de una dirección real a una dirección asignada. Esta dirección asignada es una dirección que los hosts en Internet pueden utilizar para acceder al servidor web en la DMZ sin necesidad de conocer la dirección real del servidor. Este comando asigna la dirección externa 172.22.1.25 a la dirección DMZ real 192.168.1.10.`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. Cree una ACL que permita a los usuarios externos acceder al servidor web a través de la dirección asignada. Tenga en cuenta que el servidor web también aloja el FTP.`ASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`

3. El último paso en esta configuración es aplicar la ACL a la interfaz exterior para el tráfico en la dirección entrante.`ASA-AIP-CLI(config)# access-group OutsidetoDMZ en la interfaz externa`**Nota:** Recuerde que sólo puede aplicar una lista de acceso por interfaz, por dirección. Si ya tiene una ACL entrante aplicada a la interfaz exterior, no puede aplicar esta ACL de ejemplo a ella. En su lugar, agregue las ACE en este ejemplo a la ACL actual que se aplica a la interfaz.**Nota:** Si desea bloquear o deshabilitar el tráfico FTP de Internet a DMZ, por ejemplo, utilice lo siguiente:
```
ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
tcp any host 172.22.1.25 eq ftp
```
Sugerencia: Siempre que cambie la configuración de NAT, se recomienda borrar las traducciones NAT actuales. Puede borrar la tabla de traducción con el comando **clear xlate**. **Tenga cuidado al hacer esto** ya que borrar la tabla de traducción desconecta todas las conexiones actuales que usan traducciones. La alternativa a borrar la tabla de traducción es esperar a que las traducciones actuales se agote el tiempo de espera, pero esto no se recomienda porque se puede producir un comportamiento inesperado, ya que se crean nuevas conexiones con las nuevas reglas.

Dentro/DMZ a Internet

En este escenario, los hosts ubicados en la interfaz interna (Security 100) del dispositivo de seguridad reciben acceso a Internet en la interfaz exterior (Security 0). Esto se logra con la forma PAT, o sobrecarga NAT, de NAT dinámica. A diferencia de otros escenarios, no se requiere una ACL en este caso porque los hosts en una interfaz de acceso de alta seguridad en hosts en una interfaz de baja seguridad.



1. Especifique los orígenes del tráfico que se debe traducir. Aquí se define la regla NAT número **1**, y se permite todo el tráfico de los hosts internos y DMZ.`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. Especifique qué dirección, conjunto de direcciones o interfaz debe utilizar el tráfico NATed cuando accede a la interfaz externa. En este caso, PAT se realiza con la dirección de la interfaz externa. Esto es especialmente útil cuando la dirección de la interfaz externa no se conoce de antemano, como en una configuración DHCP. Aquí, el comando global se ejecuta con el mismo ID de NAT de **1**, que lo vincula a las reglas de NAT del mismo ID.`Interfaz ASA-AIP-CLI(config)# global (externa) 1`

Sugerencia: Siempre que cambie la configuración de NAT, se recomienda borrar las traducciones NAT actuales. Puede borrar la tabla de traducción con el comando **clear xlate**. **Tenga cuidado al hacer esto** ya que borrar la tabla de traducción desconecta todas las conexiones actuales que usan traducciones. La alternativa a borrar la tabla de traducción es esperar a que las traducciones actuales se agote el tiempo de espera, pero esto no se recomienda porque se puede producir un comportamiento inesperado, ya que se crean nuevas conexiones con las nuevas reglas.

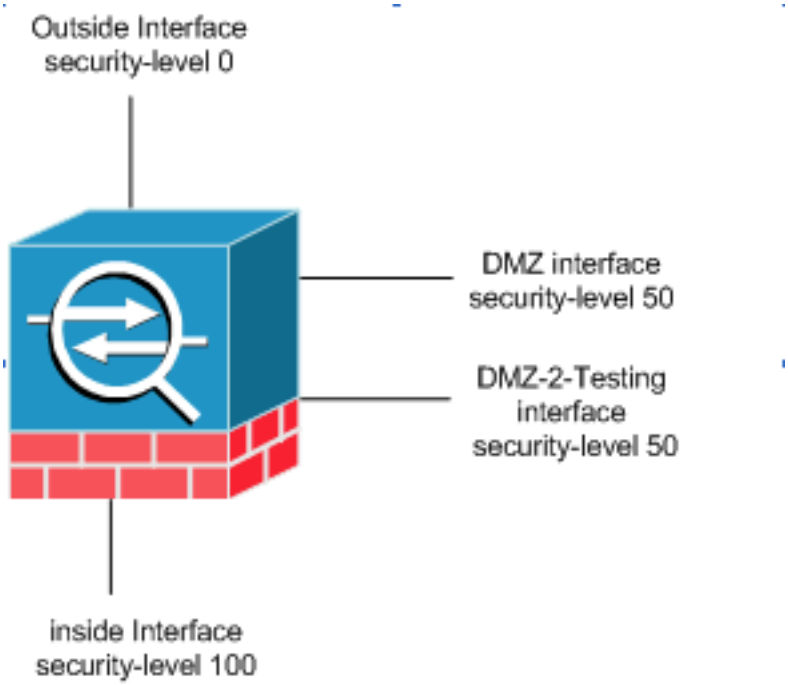
Nota: Si desea bloquear el tráfico de la zona de seguridad más alta (interna) a la zona de seguridad más baja (Internet/DMZ), cree una ACL y aplíquela a la interfaz interna del PIX/ASA como entrante.

Nota: Ejemplo: Para bloquear el tráfico del puerto 80 del host 172.20.1.100 en la red interna a Internet, utilice esto:

```
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
```

Misma comunicación de nivel de seguridad

La configuración inicial muestra que las interfaces "DMZ" y "DMZ-2-testing" se configuran con el nivel de seguridad (50); de forma predeterminada, estas dos interfaces no pueden hablar. Aquí permitimos que estas interfaces hablen con este comando:




```
ASA-AIP-CLI(config)# same-security-traffic permit inter-interface
```

Nota: Aunque se ha configurado el "permiso de tráfico de la misma seguridad entre interfaces" para las mismas interfaces de nivel de seguridad ("DMZ" y "pruebas de DMZ-2"), todavía necesita una regla de traducción (estática/dinámica) para acceder a los recursos ubicados en esas interfaces.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Resolución de problemas de conexiones a través de PIX y ASA
- Configuraciones NAT Verificación de NAT y resolución de problemas

Información Relacionada

- Referencia de Comandos de Cisco ASA
- Referencia de Comandos de Cisco PIX
- Mensajes de sistemas y errores de Cisco ASA
- Mensajes de Sistemas y Error PIX de Cisco

- Soporte Técnico y Documentación - Cisco Systems