PIX/ASA 7.x: Comunicación del permiso/de la neutralización entre las interfaces

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Productos Relacionados
Convenciones
Antecedentes
NAT
Niveles de seguridad
ACL
Configurar
Diagrama de la red
Configuración inicial
DMZ ante el interior
Internet al DMZ
Inside/DMZ a Internet
La misma comunicación del nivel de seguridad
Troubleshooting
Información Relacionada

Introducción

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

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- IP Addresses y asignación del default gateway
- Conectividad de la red física entre los dispositivos

Componentes Utilizados

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

- Dispositivo de seguridad adaptante que funciona con la versión de software 7.x y posterior
- Windows 2003 servidores
- Puestos de trabajo de Windows XP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

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

- PIX 500 Series Firewall que ejecutan 7.x y posterior

Convenciones

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

Antecedentes

Este documento delinea los pasos obligatorios para permitir que la comunicación fluya entre diversas interfaces. Las formas de comunicación tales como éstos se discuten:

1. La comunicación de los host que están situados en el exterior que requiere el acceso al recurso localizó en el DMZ
2. La comunicación de los host en la red interna que requieren el acceso a los recursos localizó en el DMZ
3. Comunicación de los host en el interior y la red DMZ que requieren el acceso a los recursos en el exterior

NAT

En nuestro ejemplo, utilizamos el Network Address Translation (NAT) y el Port Address Translation (PAT) en nuestra configuración. La traducción de la dirección substituye a la dirección real (local) en un paquete con un direccionamiento asociado que (global) sea routable en la red de destino. El NAT se comprende de dos pasos: el proceso en el cual traducen a una dirección real a un direccionamiento asociado y entonces el proceso para deshacer la traducción para el tráfico que vuelve. Hay dos formas de traducción de la dirección que utilizamos en esta guía de configuración: Estático y dinámico.

Las traducciones dinámicas permiten que cada host utilice un diverso direccionamiento o vire hacia el lado de babor para cada traducción subsiguiente. Las traducciones dinámicas pueden ser utilizadas cuando los host locales comparten o “oculte detrás” de una o más direcciones globales comunes. En este modo, una dirección local no puede reservar permanentemente a una dirección global para la traducción. En lugar, la traducción de la dirección ocurre en a mucho-a-uno o la

base múltiple, y se crean las entradas de traducción solamente mientras que son necesarias. Tan pronto como una entrada de traducción esté libre del uso, se borra y se pone a disposición otros host locales. Este tipo de traducción es el más útil para las conexiones salientes, en las cuales los host interiores se asignan una dirección dinámica o un número del puerto solamente mientras que se hacen las conexiones. Hay dos formas de traducción de la dirección dinámica:

- NAT dinámico - Traducen a las direcciones locales a la dirección global disponible siguiente en un pool. La traducción ocurre en un de a uno a uno, así que es posible agotar a la agrupación de direcciones globales si un mayor número de host locales requiere la traducción en un momento dado.
- Sobrecarga NAT (PALMADITA) - Traducen a las direcciones locales a una sola dirección global; cada conexión se hace única cuando asignan el número del puerto de alto nivel disponible siguiente de la dirección global como la fuente de la conexión. La traducción ocurre en a mucho--uno a la base porque muchos host locales comparten a una dirección global común.

La traducción estática crea una traducción fija de la dirección real al direccionamiento asociado. Una configuración del NAT estático asocia el mismo direccionamiento para cada conexión por un host y es una regla de traducción persistente. Se utilizan las traducciones de dirección estática cuando un interno o un host local necesita tener la misma dirección global para cada conexión. La traducción de la dirección ocurre en un de a uno a uno. Las traducciones estáticas se pueden definir para un solo host o para todos los direccionamientos contenidos en una subred IP.

La diferencia principal entre el NAT dinámico y un rango de direcciones para el NAT estático es que el NAT estático permite que un host remoto inicie una conexión a un host traducido (si hay una lista de acceso que lo permite), mientras que no lo hace el NAT dinámico. Usted también necesita un mismo número de direccionamientos asociados con el NAT estático.

El dispositivo de seguridad traduce un direccionamiento cuando una regla NAT hace juego el tráfico. Si ninguna regla NAT hace juego, el proceso para el paquete continúa. La excepción es cuando usted habilita el control NAT. El control NAT requiere que los paquetes que transversal de una interfaz de mayor seguridad (dentro) a una coincidencia más baja del nivel de seguridad (afuera) una regla NAT, o bien el proceso para el paquete para. Para ver la información de configuración común, refiera al documento del PIX/ASA 7.x NAT y de la PALMADITA. Para una comprensión más profunda de cómo el NAT trabaja, refiera a cómo el NAT trabaja la guía.

Consejo: Siempre que usted cambie la configuración del NAT, se recomienda que usted borra las Traducciones NAT actuales. Usted puede borrar la tabla de traducción con el **comando clear xlate**. **Sin embargo, precaución de la toma cuando usted hace esto** puesto que borrar la tabla de traducción desconecta todas las conexiones actuales que utilicen las traducciones. El alternativo borrando la tabla de traducción es esperar las traducciones actuales para medir el tiempo hacia fuera, pero esto no se recomienda porque la conducta inesperada puede resultar mientras que las nuevas conexiones se crean con las nuevas reglas.

Niveles de seguridad

Los controles de valor del nivel de seguridad cómo los host/los dispositivos en las diversas interfaces obran recíprocamente con uno a. Por abandono, los host/los dispositivos conectados con las interfaces con los mayores niveles de seguridad pueden acceder los host/los dispositivos conectados para interconectar con los niveles de la bajo-Seguridad. Los host/los dispositivos conectados con las interfaces con las interfaces de menor seguridad no pueden acceder los host/los dispositivos conectan con las interfaces con las interfaces de mayor seguridad sin el

permiso de las Listas de acceso.

El comando del **nivel de seguridad** es nuevo a la versión 7.0 y substituye a la porción del **comando nameif** que asignó el nivel de seguridad para una interfaz. Dos interfaces, “el interior” y el “exterior” interconecta, tiene niveles de seguridad predeterminados, pero éstos se pueden reemplazar con el comando del **nivel de seguridad**. Si usted nombra una interfaz “dentro,” se da un nivel de seguridad predeterminado de 100; una interfaz nombrada “exterior” se da a un nivel de seguridad predeterminado de 0. El resto de las interfaces nuevamente agregadas reciben un nivel de seguridad predeterminado de 0. para asignar un nuevo nivel de seguridad a una interfaz, utilizan el comando del **nivel de seguridad** en el modo de comando interface. Los niveles de seguridad se extienden a partir de la 1-100.

Nota: Los niveles de seguridad se utilizan para determinar solamente cómo el Firewall examina y maneja el tráfico. Por ejemplo, trafique que los pasos de una interfaz de mayor seguridad hacia más baja están remitidos con las políticas predeterminadas menos rigurosas que el tráfico que viene de una interfaz de menor seguridad hacia una mayor seguridad una. Para más información sobre los niveles de seguridad, refiera ASA/PIX al guía de referencia de comandos 7.x.

ASA/PIX 7.x también introdujo la capacidad de configurar las interfaces múltiples con el mismo nivel de seguridad. Por ejemplo, las interfaces múltiples conectaron con los Partners u otros DMZ se pueden todos dar un nivel de seguridad de 50. Por abandono, estas mismas interfaces de seguridad no pueden comunicar el uno con el otro. Para trabajar alrededor de esto, el comando de la inter-**interfaz del permiso del trafico de seguridad igual** fue introducido. Este comando permite la comunicación entre las interfaces del mismo nivel de seguridad. Para más información sobre la mismo-Seguridad entre las interfaces, refiera a los parámetros guideConfiguring de la interfaz de la referencia de comandos, y vea este ejemplo.

ACL

Las listas de control de acceso consisten en típicamente las entradas de control de acceso múltiples (ACE) ordenadas internamente por el dispositivo de seguridad en una lista enlazada. Los ACE describen un conjunto de tráfico tal como eso de un host o de una red y enumeran una acción para aplicarse a ese tráfico, generalmente permit or deny. Cuando un paquete se sujeta al control de la lista de acceso, el dispositivo del Cisco Security busca esta lista enlazada de aces para encontrar uno que haga juego el paquete. **Primer ACE que hace juego el dispositivo de seguridad es el que se aplica al paquete.** La coincidencia se encuentra una vez, la acción en que ACE (permit or deny) está aplicado al paquete.

Solamente una lista de acceso se permite por la interfaz, por la dirección. Esto significa que usted puede solamente tener una lista de acceso que se aplique para traficar entrante en una interfaz y una lista de acceso que se aplique para traficar saliente en una interfaz. Las Listas de acceso que no se aplican a las interfaces, tales como NAT ACL, son ilimitadas.

Nota: Por abandono, todas las listas de acceso tienen un ACE implícito en el extremo que niega todo el tráfico, tan todo el tráfico que no corresponda con ningún ACE que usted ingrese en la lista de acceso corresponda con el implícito niegue en el extremo y se caiga. Usted debe tener por lo menos una declaración del permiso en una lista de acceso de la interfaz para que el tráfico fluya. Sin una declaración del permiso, se niega todo el tráfico.

Nota: La lista de acceso se implementa con los **comandos access-list y access-group**. Estos comandos se utilizan en vez del **conducto** y de los **comandos outbound**, que fueron utilizados en las versiones anteriores del Software PIX Firewall. Para más información sobre los ACL, refiera a

configurar la lista de acceso por IP.

Configurar

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

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

Diagrama de la red

Este documento utiliza la esta configuración de la red:

Configuración inicial

En este documento, se utilizan estas configuraciones:

- Con esta configuración de escudo de protección básica, no hay actualmente declaraciones NAT/STATIC.
- No hay ACL aplicados, así que ACE implícito de `niega cualquier ninguno` 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 ante el interior

Para permitir la comunicación del DMZ a los host de la red interna, utilice estos comandos. En este ejemplo, un servidor Web en el DMZ necesita acceder un AD y a un servidor DNS en el interior.

1. Cree una entrada NAT estática para el servidor AD/DNS en el DMZ. El NAT estático crea una traducción fija de una dirección real a un direccionamiento asociado. Este direccionamiento asociado es un direccionamiento que los host DMZ pueden utilizar para acceder el servidor en el interior sin la necesidad de conocer a la dirección real del servidor. Este comando asocia el direccionamiento 192.168.2.20 DMZ a la dirección interna real 172.20.1.5.`Netmask estático 255.255.255.255 ASA-AIP-CLI(config)# (dentro, DMZ) 192.168.2.20 172.20.1.5`
2. Los ACL se requieren para permitir que una interfaz con un nivel de seguridad más bajo tenga acceso a un mayor nivel de seguridad. En este ejemplo, damos al servidor Web que se sienta en el acceso DMZ (Seguridad 50) al servidor AD/DNS en el interior (Seguridad 100) con estos puertos específicos del servicio: DNS, Kerberos, y LDAP.`Dominio ampliado DMZtoInside del eq de 192.168.2.20 del host de 192.168.1.10 del host UDP del permiso de la lista de acceso ASA-AIP-CLI(config)#Eq ampliado DMZtoInside 88 de 192.168.2.20 del host de 192.168.1.10 del host tcp del permiso de la lista de acceso ASA-AIP-CLI(config)#Eq ampliado DMZtoInside 389 de 192.168.2.20 del host de 192.168.1.10 del host UDP del permiso de la lista de acceso ASA-AIP-CLI(config)#`**Nota:** El acceso del permiso ACL al direccionamiento asociado del servidor AD/DNS que fue creado en este ejemplo y no la dirección interna real.
3. En este paso, usted aplica el ACL a la interfaz DMZ en la dirección entrante con este comando:`ASA-AIP-CLI(config)# acceso-grupo DMZtoInside en la interfaz DMZ`**Nota:** Si usted quiere bloquear o inhabilitar el puerto 88, el tráfico del DMZ a dentro, por ejemplo, utiliza esto:`ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88`**Consejo:** Siempre que usted cambie la configuración del NAT, se recomienda que usted borra las Traducciones NAT actuales. Usted puede borrar la tabla de traducción con el **comando clear xlate**. **Ejercite la precaución cuando usted hace esto** puesto que borrar la tabla de traducción desconecta todas las conexiones actuales que utilicen las traducciones. El alternativo borrando la tabla de traducción es esperar las traducciones actuales para medir el tiempo hacia fuera, pero esto no se recomienda porque la conducta inesperada puede resultar mientras que las nuevas conexiones se crean con las nuevas reglas.Otras configuraciones comunes incluyen éstos:Servidores del correo en el DMZAcceso de SSH dentro y afueraSesiones de escritorio remoto permitidas a través de los dispositivos del PIX/ASAOtras soluciones DNS cuando está utilizado en el DMZ

Internet al DMZ

Para permitir la comunicación de los usuarios en Internet, o la interfaz exterior (Seguridad 0), a un servidor Web que esté situado en el DMZ (Seguridad 50), utiliza estos comandos:

1. Cree una traducción estática para el servidor Web en el DMZ al exterior. El NAT estático crea una traducción fija de una dirección real a un direccionamiento asociado. Este direccionamiento asociado es un direccionamiento que los host en Internet pueden utilizar para acceder al servidor Web en el DMZ sin la necesidad de conocer a la dirección real del servidor. Este comando asocia a la dirección externa 172.22.1.25 al direccionamiento real 192.168.1.10 DMZ.`Netmask estático 255.255.255.255 ASA-AIP-CLI(config)# (DMZ, afuera) 172.22.1.25 192.168.1.10`
2. Cree un ACL que permita que los usuarios del exterior accedan al servidor Web con el direccionamiento asociado. Observe que el servidor Web también recibe el FTP.`ASA-AIP-CLI(config)# la lista de acceso OutsidetoDMZ extendió el permiso tcp cualquier eq WWW de 172.22.1.25 del hostASA-AIP-CLI(config)# la lista de acceso OutsidetoDMZ extendió el permiso tcp cualquier ftp del eq de 172.22.1.25 del host`
3. El paso más reciente de esta configuración es aplicar el ACL a la interfaz exterior para el tráfico en la dirección entrante.`ASA-AIP-CLI(config)# acceso-grupo OutsidetoDMZ en la interfaz afuera`**Nota:** Recuerde, usted puede aplicar solamente una lista de acceso por la interfaz, por la dirección. Si usted tiene ya un ACL entrante aplicado a la interfaz exterior, usted no puede aplicar este ejemplo ACL a él. En lugar agregue los ACE en este ejemplo en el ACL actual que se aplica a la interfaz.**Nota:** Si usted quiere bloquear o inhabilitar el tráfico FTP de Internet al DMZ, por ejemplo, utiliza esto:`ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit`
   `tcp any host 172.22.1.25 eq ftp`**Consejo:** Siempre que usted cambie la configuración del NAT, se recomienda que usted borra las Traducciones NAT actuales. Usted puede borrar la tabla de traducción con el **comando clear xlate**. **Ejercite la precaución cuando usted hace esto** puesto que borrar la tabla de traducción desconecta todas las conexiones actuales que utilicen las traducciones. El alternativo borrando la tabla de traducción es esperar las traducciones actuales para medir el tiempo hacia fuera, pero esto no se recomienda porque la conducta inesperada puede resultar mientras que las nuevas conexiones se crean con las nuevas reglas.

Inside/DMZ a Internet

En este escenario, los host situados en la interfaz interior (Seguridad 100) del dispositivo de seguridad se proporcionan el acceso a Internet en la interfaz exterior (Seguridad 0). Esto se alcanza con la sobrecarga de la PALMADITA, o NAT, forma de NAT dinámico. A diferencia de los otros escenarios, un ACL no se requiere en este caso porque los host en los host de alta seguridad de un acceso de la interfaz en una bajo-Seguridad interconectan.

1. Especifique las fuentes del tráfico que debe ser traducido. Aquí la regla número **1** NAT se define, y se permite todo el tráfico desde adentro y los host DMZ.`ASA-AIP-CLI(config)# (dentro) 1 172.20.1.0 nacional 255.255.255.0ASA-AIP-CLI(config)# (dentro) 1 192.168.1.0 nacional 255.255.255.0`
2. Especifique qué direccionamiento, interconecta la agrupación de direcciones, o el tráfico del NATed debe utilizar cuando accede la interfaz exterior. En este caso, la PALMADITA se realiza con la dirección de interfaz externa. Esto es especialmente útil cuando no conocen a la dirección de interfaz externa de antemano, por ejemplo adentro una configuración DHCP. Aquí, publican el comando global con la misma IDENTIFICACIÓN NAT de **1**, que la ata a las reglas NAT del mismo ID.`(Afuera) 1 interfaz global ASA-AIP-CLI(config)#`

Consejo: Siempre que usted cambie la configuración del NAT, se recomienda que usted borra las Traducciones NAT actuales. Usted puede borrar la tabla de traducción con el **comando clear xlate**. **Ejercite la precaución cuando usted hace esto** puesto que borrar la tabla de traducción

desconecta todas las conexiones actuales que utilicen las traducciones. El alternativo borrando la tabla de traducción es esperar las traducciones actuales para medir el tiempo hacia fuera, pero esto no se recomienda porque la conducta inesperada puede resultar mientras que las nuevas conexiones se crean con las nuevas reglas.

Nota: Si usted quiere bloquear el tráfico de la zona de mayor seguridad (dentro) a la zona de Seguridad más baja (internet/DMZ), cree un ACL y apliqúelo a la interfaz interior 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
```

La misma comunicación del nivel de seguridad

La configuración inicial muestra que las interfaces “DMZ” y el "DMZ-2-testing" están configuradas con el nivel de seguridad (50); por abandono, estas dos interfaces no pueden hablar. Aquí permitimos que estas interfaces hablen con este comando:

```
Inter-interfaz del permiso del trafico de seguridad igual ASA-AIP-CLI(config)#
```

Nota: Aunque “la inter-interfaz del permiso del tráfico de la mismo-Seguridad” se ha configurado para las mismas interfaces del nivel de seguridad (“DMZ” y el "DMZ-2-testing"), todavía necesita una regla de traducción (estática/dinámica) para acceder los recursos puestos en esas interfaces.

Troubleshooting

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

- Resolver problemas las conexiones con el PIX y el ASA
- NAT ConfigurationsVerify NAT y troubleshooting

Información Relacionada

- Referencia de comandos de Cisco ASA
- Referencia de comandos del Cisco PIX
- Error de Cisco ASA y mensajes de sistemas
- Error del Cisco PIX y mensajes de sistemas
- Soporte Técnico y Documentación - Cisco Systems