ASA 8.3 y posterior: El permiso FTP/TFTP mantiene el ejemplo de configuración

Contenido

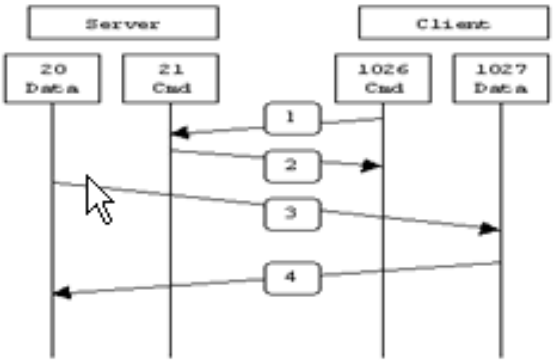
Introducción

Este documento explica los pasos necesarios para los usuarios fuera de su red para acceder a los servicios FTP y TFTP en su red DMZ.

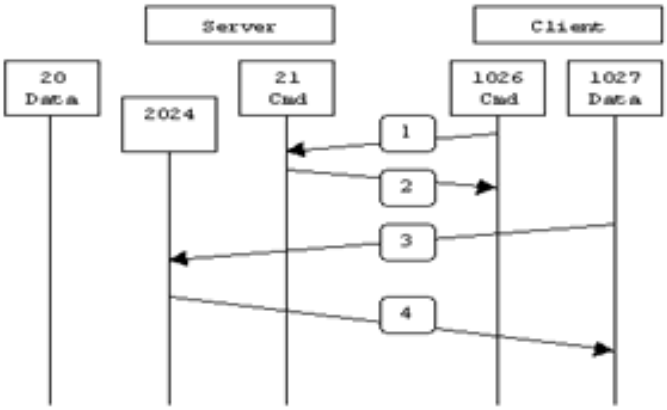
File Transfer Protocol (FTP)

Hay dos formas de FTP:

- Modo activo
- Modo pasivo



Active FTP



Passive FTP

Active FTP :
command : client >1023 -> server 21
data : client >1023 <- server 20

Passive FTP :
command : client >1023 -> server 21
data : client >1023 -> server >1023

En el modo FTP activo, el cliente conecta de un puerto no privilegiado al azar (N>1023) con el comando port (21) del servidor FTP. Después el cliente comienza a escuchar para virar el N+1 hacia el lado de babor y envía el puerto N+1 del comando ftp al servidor FTP. El servidor entonces conecta de nuevo a los puertos especificados de los datos del cliente de su puerto de los datos locales, que es el puerto 20.

En el modo del FTP pasivo, el cliente inicia ambas conexiones al servidor, que soluciona el problema de un Firewall que filtre la conexión del puerto de datos entrantes al cliente del servidor. Cuando se abre una conexión FTP, el cliente abre dos puertos no privilegiados al azar localmente (N>1023 y N+1). El primer puerto entra en contacto el servidor en el puerto 21. Pero en vez después de publicar un **comando port** y de permitir que el servidor conecte de nuevo a sus datos vire hacia el lado de babor, los problemas de cliente el **comando pasv**. El resultado de esto es que el servidor después abre un puerto no privilegiado al azar (P>1023) y envía el **comando P del puerto** de nuevo al cliente. El cliente entonces inicia la conexión del puerto N+1 para virar P hacia el lado de babor en el servidor para transferir los datos. Sin el comando configuration del **examen** en el dispositivo de seguridad, el FTP por dentro de los usuarios dirigió los trabajos salientes solamente en el modo pasivo. También, entrante dirigido exterior de los usuarios a su servidor FTP se niega el acceso.

Consulte PIX/ASA 7.x: Habilite el ejemplo de configuración de los servicios FTP/TFTP para la misma configuración en el dispositivo de seguridad adaptante de Cisco (ASA) con las versiones 8.2 y anterior.

Trivial File Transfer Protocol (TFTP)

El TFTP, según lo descrito en el RFC 1350, es un protocolo sencillo para leer y para escribir los archivos entre un servidor TFTP y un cliente. El TFTP utiliza el puerto 69 UDP.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Hay comunicación básica entre las interfaces necesarias.
- Usted tiene configurado el servidor FTP situado en su red DMZ.

Componentes Utilizados

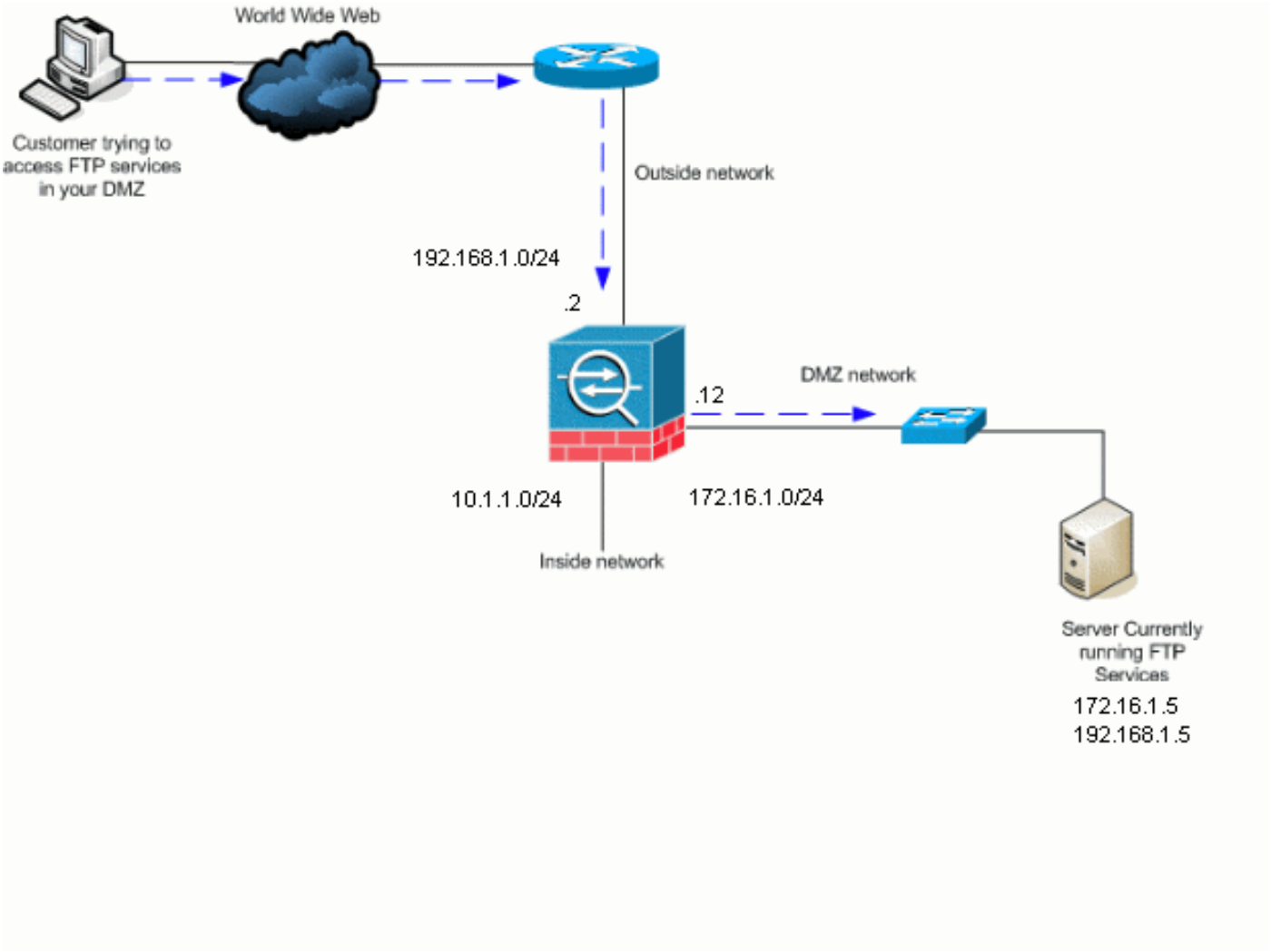
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad adaptante de las 5500 Series ASA que funciona con 8.4(1) la imagen del software
- Servidor de Windows 2003 que dirige los servicios FTP
- Servidor de Windows 2003 que dirige los servicios TFTP
- PC del cliente localizado en el exterior de la red

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Productos Relacionados

Esta configuración se puede también utilizar con el dispositivo de seguridad adaptante 8.3 de Cisco y posterior.

Convenciones

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

Antecedentes

El dispositivo de seguridad soporta la Inspección de la aplicación con la función del algoritmo de seguridad adaptable. Con la Inspección de la aplicación stateful usada por el algoritmo de seguridad adaptable, el dispositivo de seguridad sigue cada conexión que atraviese el Firewall y se asegura de que son válidos. El Firewall, con la inspección con estado, también monitorea el estado de la conexión para compilar la información para colocar en una tabla de estado. Con el uso de la tabla de estado además de las reglas administrador-definidas, las decisiones de filtración se basan en el contexto que es establecido por los paquetes pasajeros previamente con

el Firewall. La implementación de las Inspecciones de la aplicación consiste en estas acciones:

- Identifique el tráfico.
- Aplique los exámenes al tráfico.
- Active los exámenes en una interfaz.

Dirección avanzada del protocolo

FTP

Algunas aplicaciones requieren la dirección especial por la función de las Inspecciones de la aplicación del dispositivo del Cisco Security. Estos tipos de aplicaciones integran típicamente la información del IP Addressing en el paquete de datos del usuario o los canales secundarios abiertos en los puertos dinámicamente asignados. Los trabajos de la función de la Inspección de la aplicación con el Network Address Translation (NAT) a ayudar a identificar la ubicación de la información de direccionamiento integrada.

Además de la identificación de la información de direccionamiento integrada, las sesiones de monitores de la función de la Inspección de la aplicación para determinar los números del puerto para los canales secundarios. Muchos protocolos abren los puertos secundarios TCP o UDP para mejorar el funcionamiento. La sesión inicial sobre un puerto conocido se utiliza para negociar los números del puerto dinámicamente asignados. La función de la Inspección de la aplicación monitorea estas sesiones, identifica las asignaciones de puerto dinámico y permite el intercambio de datos en estos puertos para la duración de las sesiones específicas. Las multimedias y las aplicaciones FTP exhiben a este tipo de conducta.

El protocolo FTP requiere una cierta dirección del special debido a su uso de dos puertos por la sesión FTP. El protocolo FTP utiliza dos puertos cuando está activado para los datos de transferencia: un canal de control y un canal de datos que utiliza el puerto 21 y 20, respectivamente. El usuario, que inicia a la sesión FTP sobre el canal de control, hace todos los pedidos de datos a través de ese canal. El servidor FTP entonces inicia una petición de abrir un puerto del puerto de servidor 20 en el equipo del usuario. El FTP utiliza siempre el puerto 20 para las comunicaciones de canal de datos. Si el examen FTP no se ha habilitado en el dispositivo de seguridad, se desecha esta petición y las sesiones FTP no transmiten ningunos datos pedidos. Si el examen FTP se habilita en el dispositivo de seguridad, el dispositivo de seguridad monitorea el canal de control e intenta reconocer una petición de abrir el canal de datos. El protocolo FTP integra las especificaciones de puerto del canal de datos en el tráfico del canal de control, requiriendo el dispositivo de seguridad examinar el canal de control para saber si hay cambios del DATA-puerto. Si el dispositivo de seguridad reconoce una petición, crea temporalmente una apertura para el tráfico del canal de datos que dura para la vida de la sesión. De esta manera, la función del examen FTP monitorea el canal de control, identifica una asignación del DATA-puerto, y permite que los datos sean intercambiados en el puerto de los datos para la longitud de la sesión.

El dispositivo de seguridad examina las conexiones del puerto 21 para el tráfico FTP por abandono a través del clase-mapa del global-examen. El dispositivo de seguridad también reconoce la diferencia entre un active y una sesión del FTP pasivo. Si las sesiones FTP soportan la Transferencia de datos del FTP pasivo, el dispositivo de seguridad, a través del **comando ftp de la inspección**, reconoce la petición del puerto de los datos del usuario y abre un nuevo puerto de los datos mayor de 1023.

El examen de la aplicación FTP examina a las sesiones FTP y realiza la tarea cuatro:

- Prepara una conexión de datos secundaria dinámica
- Sigue la secuencia de comando response FTP
- Genera un rastro de auditoría
- Traduce el IP Address incluido usando el NAT

El examen de la aplicación FTP prepara los canales secundarios para la transferencia de datos FTP. Los canales se afectan un aparato en respuesta al File Upload (Subir archivo), a una descarga del archivo, o a un evento del listado del directorio, y deben PRE-ser negociados. El puerto se negocia con los 227) comandos del **PUERTO** o **PASV** (.

TFTP

El examen TFTP se habilita por abandono.

El dispositivo de seguridad examina el tráfico TFTP y crea dinámicamente las conexiones y las traducciones en caso necesario, para permitir la transferencia de archivos entre un cliente TFTP y un servidor. Específicamente, el motor del examen examina las peticiones leídas TFTP (RRQ), escribe las peticiones (WRQ), y las notificaciones de error (ERROR).

Un canal secundario dinámico y una traducción de la PALMADITA en caso necesario, se afectan un aparato en una recepción de un RRQ o de un WRQ válido. Este canal secundario es utilizado posteriormente por el TFTP para la transferencia de archivos o la notificación de error.

Solamente el servidor TFTP puede iniciar el tráfico sobre el canal secundario, y a lo más un canal secundario incompleto puede existir entre el cliente TFTP y el servidor. Una notificación de error del servidor cierra el canal secundario.

El examen TFTP debe ser habilitado si el PAT estático se utiliza para reorientar el tráfico TFTP.

Examen básico de la aplicación FTP de la configuración

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique el examen al tráfico en todas las interfaces (una política global). El tráfico del examen de la aplicación predeterminada incluye el tráfico a los puertos predeterminados para cada protocolo. Usted puede aplicar solamente una política global, así que si usted quiere alterar la política global, por ejemplo, para aplicar el examen a los puertos no estándar, o agregar los exámenes que no se habilitan por abandono, usted necesita editar la política predeterminada o inhabilitarla y aplicar un nuevo. Para una lista de todos los puertos predeterminados, refiera a la directiva predeterminada del examen.

1. Publique el comando policy-map global_policy.`ASA(config)#policy-map global_policy`
2. Publique el comando class inspection_default.`ASA(config-pmap)#class inspection_default`
3. Publique el comando ftp de la inspección.`ASA(config-pmap-c)#inspect FTP` Hay una opción para utilizar el comando estricto de la inspección FTP. Este comando aumenta la Seguridad de las redes protegidas evitando que un buscador Web envíe los comandos integrados en los pedidos de FTP.Después de que usted habilite la opción *estricta* en una interfaz, el examen FTP aplica este comportamiento:Un comando ftp debe ser reconocido antes de que el dispositivo de seguridad permita un comando new.El dispositivo de seguridad cae una conexión que envíe los comandos integrados.Marcan los **227** y a los **comandos port** de asegurarse que no aparecen en una secuencia de comandos de error.**Advertencia:** El uso de la opción *estricta* pudo causar el error de FTP cliente que no son estrictamente

obedientes con FTP RFC. Refiérase usando la opción estricta para más información sobre el uso de la opción *estricta*.

Ejemplo de configuración

Nombre del dispositivo 1
ASA(config)#**show running-config** ASA Version 8.4(1) ! hostname ASA domain-name corp.com enable password WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 192.168.1.2 255.255.255.0 ! interface Ethernet0/1 nameif Inside security-level 100 ip address 10.1.1.1 255.255.255.0 ! interface Ethernet0/2 nameif DMZ security-level 50 ip address 172.16.1.12 255.255.255.0 ! interface Ethernet0/3 no nameif no security-level no ip address ! interface Management0/0 no nameif no security-level no ip address ! *!--- Output is suppressed. !--- Permit inbound FTP control traffic.* **access-list 100 extended permit tcp any host 192.168.1.5 eq ftp** *!--- Permit inbound FTP data traffic.* **access-list 100 extended permit tcp any host 192.168.1.5 eq ftp-data** ! *!--- Object groups are created to define the hosts.* **object network DMZ host 172.16.1.5 object network DMZ-out host 192.168.1.5** ***!--- Configure manual NAT*** **nat (DMZ,outside) source static DMZ DMZ-out access-group 100 in interface outside** 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 ! *!--- This command tells the device to !--- use the "global_policy" policy-map on all interfaces.* **service-policy global_policy global** prompt hostname context Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end ASA(config)#

Examen del protocolo FTP de la configuración en el puerto TCP no estándar

Usted puede configurar el examen del protocolo FTP para los puertos TCP no estándar con estas líneas de configuración (substituya el por el nuevo número del puerto):

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
   inspect ftp
```

Configure el examen básico de la aplicación TFTP

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de

la aplicación predeterminada y aplique el examen al tráfico en todas las interfaces (una política global). El tráfico del examen de la aplicación predeterminada incluye el tráfico a los puertos predeterminados para cada protocolo. Usted puede aplicar solamente una política global. Tan si usted quiere alterar la política global, por ejemplo, para aplicar el examen a los puertos no estándar, o agregar los exámenes que no se habilitan por abandono, usted necesita editar la política predeterminada o inhabilitarla y aplicar un nuevo. Para una lista de todos los puertos predeterminados, refiera a la directiva predeterminada del examen.

1. Publique el comando policy-map global_policy.`ASA(config)#policy-map global_policy`
2. Publique el comando class inspection_default.`ASA(config-pmap)#class inspection_default`
3. Publique el comando tftp de la inspección.`ASA(config-pmap-c)#inspect TFTP`

Ejemplo de configuración

Nombre del dispositivo 1

```
ASA(config)#show running-config ASA Version 8.4(1) !
hostname ASA domain-name corp.com enable password
WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0
nameif Outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! interface Ethernet0/1 nameif Inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/2 nameif DMZ security-level 50 ip
address 172.16.1.12 255.255.255.0 ! interface
Ethernet0/3 no nameif no security-level no ip address !
interface Management0/0 no nameif no security-level no
ip address ! !--- Output is suppressed. !--- Permit
inbound TFTP traffic. access-list 100 extended permit
udp any host 192.168.1.5 eq tftp ! !--- Object groups
are created to define the hosts. object network DMZ host
172.16.1.5 object network DMZ-out host 192.168.1.5 !---
Configure manual NAT nat (DMZ,outside) source static DMZ
DMZ-out access-group 100 in interface outside 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 ! !--- This command tells the device
to !--- use the "global_policy" policy-map on all
interfaces. service-policy global_policy global prompt
hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA(config)#
```

Verificación

Para asegurar la configuración ha tomado, utiliza con éxito el **comando service-policy de la demostración**. También, limite la salida al examen FTP solamente usando la servicio-directiva de la demostración examinan el comando ftp.

```
ASA#show service-policy inspect ftp Global Policy: Service-policy: global_policy Class-map:
inspection_default Inspect: ftp, packet 0, drop 0, reste-drop 0 ASA#
```

Troubleshooting

No hay actualmente información específica acerca de Troubleshooting disponible para esta configuración

Información Relacionada

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems