ASA 8.3 y posterior: Ejemplo de Configuración de Habilitar Servicios FTP/TFTP

Contenido

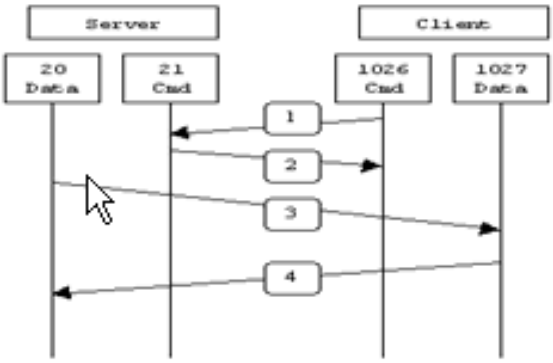
Introducción

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.

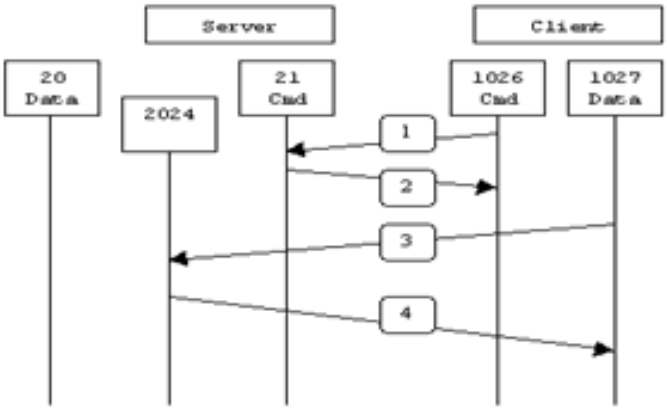
Protocolo de transferencia de archivos (FTP)

Existen 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 se conecta desde un puerto aleatorio no privilegiado (N>1023) al puerto de comando (21) del servidor FTP. A continuación, el cliente comienza a escuchar el puerto N+1 y envía el puerto de comando FTP N+1 al servidor FTP. A continuación, el servidor se vuelve a conectar a los puertos de datos especificados del cliente desde su puerto de datos local, que es el puerto 20.

En el modo FTP pasivo, el cliente inicia ambas conexiones al servidor, lo que resuelve el problema de un firewall que filtra la conexión del puerto de datos entrante al cliente desde el servidor. Cuando se abre una conexión FTP, el cliente abre dos puertos aleatorios no privilegiados localmente (N>1023 y N+1). El primer puerto entra en contacto con el servidor en el puerto 21. Pero en lugar de ejecutar un comando **port** y permitir que el servidor se conecte nuevamente a su puerto de datos, el cliente ejecuta el comando **PASV**. El resultado de esto es que el servidor abre un puerto aleatorio no privilegiado (P>1023) y envía el comando **port P** nuevamente al cliente. A continuación, el cliente inicia la conexión del puerto N+1 al puerto P del servidor para transferir datos. Sin la configuración del comando **inspection** en el dispositivo de seguridad, el FTP de los usuarios internos que se dirigen a la salida funciona sólo en modo pasivo. Además, se deniega el acceso a los usuarios externos que se dirigen al servidor FTP.

Consulte PIX/ASA 7.x: Ejemplo de Configuración de Habilitar FTP/TFTP Services para la misma configuración en Cisco Adaptive Security Appliance (ASA) con las versiones 8.2 y anteriores.

Protocolo trivial de transferencia de archivos (TFTP)

El TFTP, como se describe en RFC 1350, es un protocolo simple para leer y escribir archivos entre un servidor TFTP y un cliente. TFTP utiliza el puerto UDP 69.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Hay una comunicación básica entre las interfaces necesarias.
- Ha configurado un servidor FTP ubicado en la red DMZ.

Componentes Utilizados

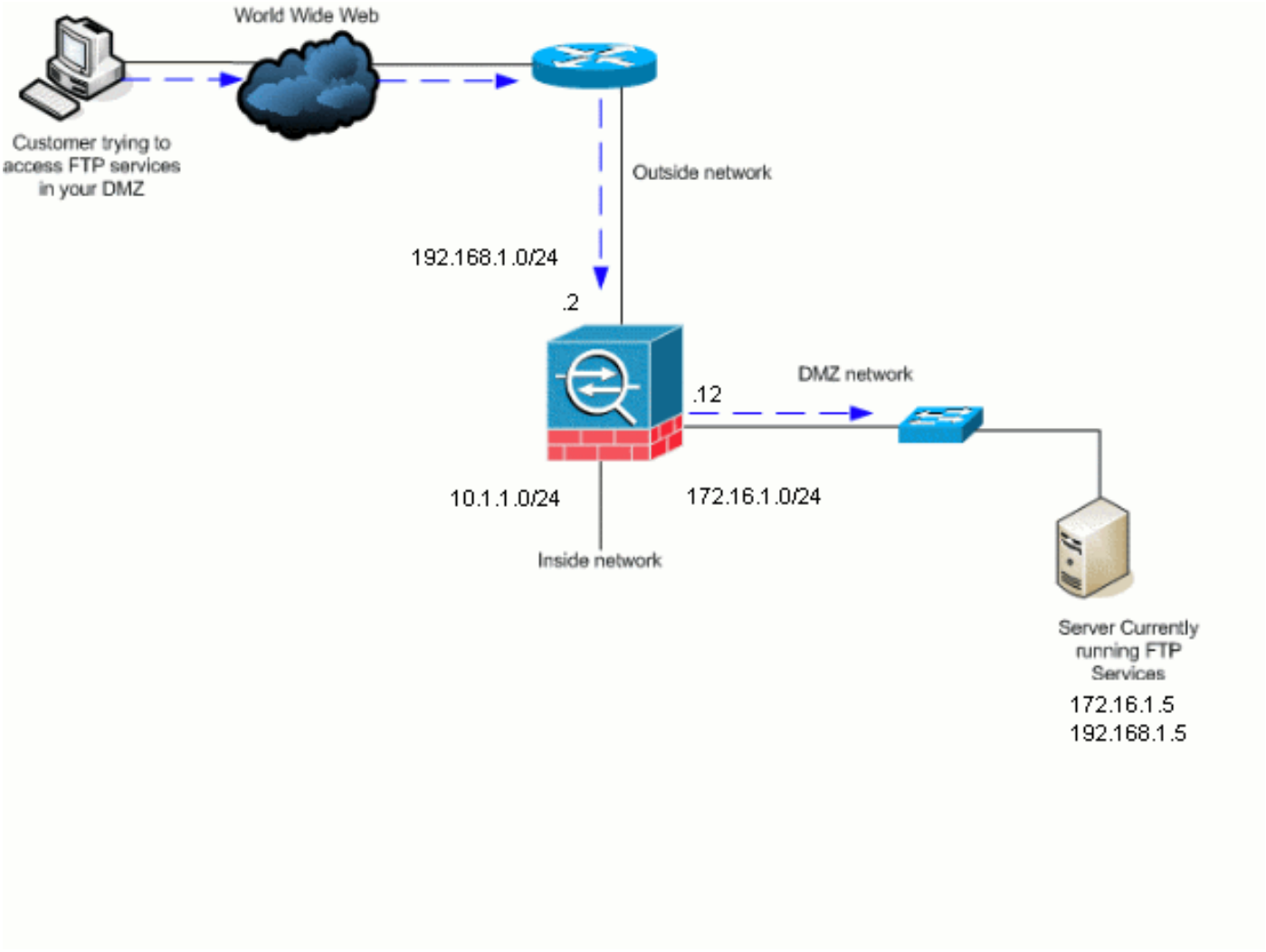
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad adaptable ASA serie 5500 que ejecuta la imagen de software 8.4(1)
- Windows 2003 Server que ejecuta servicios FTP
- Windows 2003 Server que ejecuta servicios TFTP
- PC cliente ubicado en el exterior de la red

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP utilizados 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 también se puede utilizar con Cisco Adaptive Security Appliance 8.3 y posteriores.

Convenciones

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

Antecedentes

El dispositivo de seguridad admite la inspección de aplicaciones mediante la función Adaptive Security Algorithm. A través de la inspección de estado de la aplicación utilizada por el algoritmo de seguridad adaptable, el dispositivo de seguridad realiza un seguimiento de cada conexión que atraviesa el firewall y asegura que sean válidas. El firewall, a través de la inspección activa (stateful), también supervisa el estado de la conexión para compilar información para colocarla en una tabla de estado. Con el uso de la tabla de estado además de las reglas definidas por el administrador, las decisiones de filtrado se basan en el contexto establecido por los paquetes previamente pasados a través del firewall. La ejecución de las inspecciones de aplicación consiste en las siguientes acciones:

- Identifique el tráfico.
- Aplicar inspecciones al tráfico.
- Active las inspecciones en una interfaz.

Gestión avanzada de protocolos

FTP

Algunas aplicaciones requieren un manejo especial por parte de la función de inspección de aplicaciones de Cisco Security Appliance. Estos tipos de aplicaciones normalmente incrustan información de direccionamiento IP en el paquete de datos del usuario o abren canales secundarios en puertos asignados dinámicamente. La función de inspección de aplicaciones funciona con la traducción de direcciones de red (NAT) para ayudar a identificar la ubicación de la información de direccionamiento integrada.

Además de la identificación de la información de direccionamiento integrada, la función de inspección de aplicaciones monitorea las sesiones para determinar los números de puerto para los canales secundarios. Muchos protocolos abren puertos TCP o UDP secundarios para mejorar el rendimiento. La sesión inicial en un puerto conocido se utiliza para negociar números de puerto asignados dinámicamente. La función de inspección de aplicaciones monitorea estas sesiones, identifica las asignaciones de puertos dinámicos y permite el intercambio de datos en estos puertos durante la duración de las sesiones específicas. Las aplicaciones multimedia y FTP muestran este tipo de comportamiento.

El protocolo FTP requiere cierta gestión especial debido al uso de dos puertos por sesión FTP. El protocolo FTP utiliza dos puertos cuando se activa para transferir datos: un canal de control y un canal de datos que utiliza los puertos 21 y 20, respectivamente. El usuario, que inicia la sesión FTP sobre el canal de control, realiza todas las solicitudes de datos a través de ese canal. A continuación, el servidor FTP inicia una solicitud para abrir un puerto desde el puerto del servidor 20 al equipo del usuario. FTP siempre utiliza el puerto 20 para las comunicaciones del canal de datos. Si la inspección FTP no se ha habilitado en el dispositivo de seguridad, esta solicitud se descarta y las sesiones FTP no transmiten los datos solicitados. Si se habilita la inspección FTP en el dispositivo de seguridad, el dispositivo de seguridad monitorea el canal de control e intenta reconocer una solicitud para abrir el canal de datos. El protocolo FTP incrusta las especificaciones del puerto del canal de datos en el tráfico del canal de control, lo que requiere que el dispositivo de seguridad inspeccione el canal de control para ver los cambios del puerto de datos. Si el dispositivo de seguridad reconoce una solicitud, crea temporalmente una apertura para el tráfico del canal de datos que dura toda la vida de la sesión. De esta manera, la función de inspección FTP monitorea el canal de control, identifica una asignación de puerto de datos y permite intercambiar datos en el puerto de datos durante la duración de la sesión.

El dispositivo de seguridad inspecciona de forma predeterminada las conexiones del puerto 21 para el tráfico FTP a través del mapa de clase de inspección global. El dispositivo de seguridad también reconoce la diferencia entre una sesión FTP activa y una sesión FTP pasiva. Si las sesiones FTP soportan la transferencia pasiva de datos FTP, el dispositivo de seguridad, a través del comando **inspect ftp**, reconoce la solicitud del puerto de datos del usuario y abre un nuevo puerto de datos mayor que 1023.

La inspección de la aplicación FTP inspecciona las sesiones FTP y realiza cuatro tareas:

- Prepara una conexión de datos secundaria dinámica
- Realiza un seguimiento de la secuencia de respuesta de comandos FTP
- Genera una pista de auditoría
- Traduce la dirección IP incrustada mediante NAT

La inspección de aplicaciones FTP prepara canales secundarios para la transferencia de datos FTP. Los canales se asignan en respuesta a un evento de carga de archivos, descarga de archivos o listado de directorios, y deben negociarse previamente. El puerto se negocia a través de los comandos **PORT** o **PASV** (227).

TFTP

La inspección TFTP está habilitada de forma predeterminada.

El dispositivo de seguridad inspecciona el tráfico TFTP y crea dinámicamente conexiones y traducciones, si es necesario, para permitir la transferencia de archivos entre un cliente TFTP y un servidor. Específicamente, el motor de inspección inspecciona las solicitudes de lectura TFTP (RRQ), las solicitudes de escritura (WRQ) y las notificaciones de error (ERROR).

Un canal secundario dinámico y una traducción PAT, si es necesario, se asignan en la recepción de una RRQ o WRQ válida. Este canal secundario es utilizado posteriormente por TFTP para la transferencia de archivos o la notificación de errores.

Sólo el servidor TFTP puede iniciar el tráfico a través del canal secundario, y al menos un canal secundario incompleto puede existir entre el cliente TFTP y el servidor. Una notificación de error del servidor cierra el canal secundario.

La inspección TFTP se debe habilitar si se utiliza PAT estática para redirigir el tráfico TFTP.

Configuración de la Inspección Básica de la Aplicación FTP

De forma predeterminada, la configuración incluye una política que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica la inspección al tráfico en todas las interfaces (una política global). El tráfico de inspección de aplicaciones predeterminado incluye el tráfico a los puertos predeterminados para cada protocolo. Sólo puede aplicar una política global, por lo que si desea modificar la política global, por ejemplo, para aplicar la inspección a los puertos no estándar o para agregar inspecciones que no están habilitadas de forma predeterminada, debe editar la política predeterminada o desactivarla y aplicar una nueva. Para ver una lista de todos los puertos predeterminados, consulte la Política de inspección predeterminada.

1. Ejecute el comando policy-map global_policy.
   ```
   ASA(config)#policy-map global_policy
   ```

2. Ejecute el comando class inspection_default.
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. Ejecute el comando inspect FTP.
   ```
   ASA(config-pmap-c)#inspect FTP
   ```

   Hay una opción para utilizar el comando inspect FTP strict. Este comando aumenta la seguridad de las redes protegidas al impedir que un navegador web envíe comandos incrustados en las solicitudes FTP.Después de habilitar la opción *estricta* en una interfaz, la inspección FTP aplica este comportamiento:Se debe reconocer un comando FTP antes de que el dispositivo de seguridad permita un nuevo comando.El dispositivo de seguridad descarta una conexión que envía comandos incrustados.Los comandos 227 y PORT se verifican para asegurarse de que no aparezcan en una cadena de error.**Advertencia:** El uso de la opción *estricta* puede causar la falla de los clientes FTP que no cumplen estrictamente con los RFC FTP. Refiérase a Uso de la Opción estricta para obtener 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)#
```

Configuración de la Inspección del Protocolo FTP en un Puerto TCP No Estándar

Puede configurar la inspección de protocolo FTP para puertos TCP no estándar con estas líneas de configuración (reemplace XXXX por el nuevo número de 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
```

Configuración de la Inspección Básica de la Aplicación TFTP

De forma predeterminada, la configuración incluye una política que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica la inspección al tráfico en todas las interfaces (una política global). El tráfico de inspección de aplicaciones predeterminado incluye el tráfico a los puertos predeterminados para cada protocolo. Sólo puede aplicar una política global. Por lo tanto, si desea modificar la política global, por ejemplo, para aplicar la inspección a puertos no estándar o para agregar inspecciones que no están habilitadas de forma predeterminada, debe editar la política predeterminada o desactivarla y aplicar una nueva. Para ver una lista de todos los puertos predeterminados, consulte la Política de inspección predeterminada.

1. Ejecute el comando policy-map global_policy.
   ```
   ASA(config)#policy-map global_policy
   ```
2. Ejecute el comando class inspection_default.
   ```
   ASA(config-pmap)#class inspection_default
   ```
3. Ejecute el comando inspect TFTP.
   ```
   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 asegurarse de que la configuración se ha realizado correctamente, utilice el comando **show service-policy**. Además, limite el resultado a la inspección de FTP sólo mediante el comando show service-policy inspect 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#
```

Troubleshoot

Actualmente, no hay información específica 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