

Configure la redirección transparente con el WCCP para reorientar el tráfico nativo FTP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de WSA](#)

[Configuración ASA de la muestra](#)

[Configuración del switch de la muestra \(c3560\)](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar el dispositivo de seguridad de la red (WSA)/al router de Cisco para utilizar la redirección transparente del HTTP, del HTTPS, y del tráfico nativo FTP con el protocolo web cache communication (WCCP).

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Dispositivo de seguridad de la red de Cisco que funciona con la versión 6.0 o posterior de AsyncOS
- Natural proxy FTP activado en WSA
- Router WCCPv2 Cisco/conmutador o Firewall compatible ASA

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.

Configurar

Cuando el tráfico nativo FTP se reorienta transparente al WSA, el WSA recibe típicamente el tráfico en el puerto estándar 21 FTP. Por lo tanto, el natural proxy FTP en el WSA debe escuchar en el puerto 21 (por abandono el natural proxy FTP es 8021). En el GUI, elija los **Servicios de seguridad > proxy FTP** para la verificación.

Configuración de WSA

1. Cree una identidad para el tráfico FTP. En el GUI, elija el **administrador de seguridad > las identidades de la red** y asegúrese de que la autenticación se ha inhabilitado para esta identificación.
2. Cree una política de acceso. En el GUI, elija el **administrador de seguridad > las políticas de acceso de la red**, que se refiere a la identidad al paso 1.
3. Bajo proxy FTP configuraciones, modifique los puertos pasivos FTP para ser 11000-11006 para asegurarse de que todos los puertos cabidos en un solo grupo de servicios.
4. Cree estos ID del servicio WCCP:

Puertos del servicio de nombre

caché Web 0 80 *(alternativamente, usted puede utilizar el aduana-red-caché 98 si usted utiliza WSAs múltiple)*

60 21,11000,11001,11002,11003,11004,11005,11006 ftp-nativos

https-caché 70 443

Estos ejemplos reorientan tres subredes internas mientras que desvían el redireccionamiento de WCCP para todos los destinos privado dirigidos así como un solo host interno.

Configuración ASA de la muestra

```
wccp web-cache redirect-list web-cache group-list group_acl
wccp 60 redirect-list ftp-native group-list group_acl
wccp 70 redirect-list https-cache group-list group_acl
```

```
wccp interface inside web-cache redirect in
wccp interface inside 60 redirect in
wccp interface inside 70 redirect in
```

```
access-list group_acl extended permit ip host 10.1.1.160 any
```

```
access-list ftp-native extended deny ip any 10.0.0.0 255.0.0.0
access-list ftp-native extended deny ip any 172.16.0.0 255.240.0.0
access-list ftp-native extended deny ip any 192.168.0.0 255.255.0.0
access-list ftp-native extended deny ip host 192.168.42.120 any
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any range 11000
11006
```

```
access-list https-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list https-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list https-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list https-cache extended deny ip host 192.168.42.120 any
```

```

access-list https-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq https

access-list web-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list web-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list web-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list web-cache extended deny ip host 192.168.42.120 any
access-list web-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq www

```

Configuración del switch de la muestra (c3560)

Esto debe trabajar en la mayoría del Routers también.

```

ip wccp web-cache redirect-list web-cache group-list group_acl
ip wccp 60 redirect-list ftp-native group-list group_acl
ip wccp 70 redirect-list https-cache group-list group_acl

interface Vlan99
ip address 192.168.99.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

interface Vlan100
ip address 192.168.100.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

interface Vlan420
ip address 192.168.42.1 255.255.255.0
ip helper-address 192.168.100.20
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

ip access-list extended ftp-native
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq ftp
permit tcp 192.168.42.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.99.0 0.0.0.255 any eq ftp
permit tcp 192.168.99.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.100.0 0.0.0.255 any eq ftp
permit tcp 192.168.100.0 0.0.0.255 any range 11000 11006

ip access-list extended https-cache
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq 443
permit tcp 192.168.99.0 0.0.0.255 any eq 443
permit tcp 192.168.100.0 0.0.0.255 any eq 443

ip access-list extended web-cache
deny ip any 10.0.0.0 0.255.255.255

```

```
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq www
permit tcp 192.168.99.0 0.0.0.255 any eq www
permit tcp 192.168.100.0 0.0.0.255 any eq www
```

```
ip access-list standard group_acl
permit 10.1.1.160
```

Note: Debido a una limitación de tecnología WCCP, un máximo de ocho puertos se puede asignar por el ID del servicio WCCP.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.