

Configurar o redirecionamento transparente com WCCP a fim reorientar o tráfego nativo FTP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração WSA](#)

[Configuração da amostra ASA](#)

[Configuração de switch da amostra \(c3560\)](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como para configurar Web ferramenta de segurança) (WSA/roteador Cisco a fim apoiar o redirecionamento transparente do HTTP, do HTTPS, e do tráfego nativo FTP com Protocolo de Comunicação de Cache da Web (WCCP).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Ferramenta de segurança da Web de Cisco que executa a versão 6.0 ou mais recente de AsyncOS
- Proxy de FTP nativo permitido em WSA
- Roteador Cisco WCCPv2/interruptor ou Firewall compatível ASA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Quando o tráfego nativo FTP é reorientado transparentemente ao WSA, o WSA recebe

tipicamente o tráfego na porta 21 do padrão FTP. Daqui, o proxy de FTP nativo no WSA deve escutar na porta 21 (à revelia o proxy de FTP nativo é 8021). No GUI, escolha **Serviços de segurança > proxy de FTP** para a verificação.

Configuração WSA

1. Crie uma identidade para o tráfego FTP. No GUI, escolha o **gerenciador de segurança > as identidades da Web** e assegure-se de que a autenticação esteja desabilitada para este ID.
2. Crie uma política de acesso. No GUI, escolha o **gerenciador de segurança > as políticas de acesso da Web**, que provê a identidade em etapa 1.
3. Sob ajustes de proxy de FTP, altere as portas passivas FTP para ser 11000-11006 a fim assegurar-se de que todas as portas cabidas em um único grupo de serviço.
4. Crie este o serviço ID WCCP:

Portas do serviço de nome

cache de web 0 80 (*alternativamente, você pode usar o costume-Web-esconderijo 98 se você usa WSAs múltiplo*)

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

https-esconderijo 70 443

Estes exemplos reorientam três sub-redes internas quando contornarem o redirecionamento de WCCP para todos os destinos confidencialmente endereçados assim como um único host interno.

Configuração da amostra ASA

```
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
```

Configuração de switch da amostra (c3560)

Isto deve trabalhar na maioria de Roteadores demasiado.

```
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: Devido a uma limitação de tecnologia WCCP, um máximo de oito portas pode ser atribuído pelo ID de serviço WCCP.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.