

Configuratie van transparante omleiding met WCCP om inheems FTP-verkeer om te buigen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[WSA-configuratie](#)

[ASA-configuratie van monsters](#)

[Configuratie voorbeeldswitch \(c3560\)](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u de Web Security Appliance (WSA)/Cisco router kunt configureren om een transparante omleiding van HTTP, HTTPS en Native FTP-verkeer te ondersteunen met Web Cache Communication Protocol (WCCP).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco web security applicatie die AsyncOS versie 6.0 of hoger draait
- Native FTP-proxy ingeschakeld op WSA
- WCCPv2-compatibele Cisco router/switch voor ASA-firewall

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Wanneer het inheemse FTP-verkeer op transparante wijze wordt hergeleid naar de WSA, ontvangt de WSA doorgaans het verkeer op de standaard FTP poort 21. Vandaar dat de Native

FTP-proxy op de WSA op poort 21 moet luisteren (standaard is de native FTP-proxy 8021).
Selecteer in de GUI de optie **Security Services > FTP Proxy** ter verificatie.

WSA-configuratie

1. Maak een identiteit voor FTP-verkeer. In de GUI, kies **Web Security Manager > Identificaties** en zorg ervoor dat de authenticatie voor deze ID is uitgeschakeld.
2. Schep een toegangsbeleid. In de GUI, kies **Web Security Manager > Toegangsbeleid**, wat de identiteit in stap 1 verwijst.
3. Onder FTP proxy-instellingen wijzigt u de FTP passieve poorten om 1000-1006 te zijn, om er zeker van te zijn dat alle poorten in één servicegroep passen.
4. Maak deze WCCP-service-ID's:

Naamservice Poorten

web-cache 0 80 (*anders kunt u 98 op maat-web-cache gebruiken als u meerdere WSA's gebruikt*)

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

https-cache 70 443

In deze voorbeelden worden drie interne subnetten omgeleid terwijl de WCCP-omleiding wordt omzeild voor alle particuliere bestemmingen en één interne host.

ASA-configuratie van monsters

```
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
```

Configuratie voorbeeldswitch (c3560)

Dit zou ook op de meeste routers moeten werken.

```
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
```

Opmerking: Vanwege een technische beperking van WCCP kunnen maximaal acht poorten worden toegewezen per WCCP-service-ID.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.