

Configurazione del reindirizzamento trasparente con WCCP per reindirizzare il traffico FTP nativo

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione WSA](#)

[Esempio di configurazione dell'ASA](#)

[Esempio di configurazione dello switch \(c3560\)](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Web Security Appliance (WSA) / Cisco Router per supportare il reindirizzamento trasparente del traffico HTTP, HTTPS e FTP nativo con il protocollo WCCP (Web Cache Communication Protocol).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Web Security Appliance con AsyncOS versione 6.0 o successive
- Proxy FTP nativo abilitato su WSA
- Router/switch Cisco compatibile WCCPv2 o firewall ASA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Quando il traffico FTP nativo viene reindirizzato in modo trasparente al server WSA, in genere il

server WSA riceve il traffico sulla porta FTP standard 21. Di conseguenza, il proxy FTP nativo del server WSA deve essere in ascolto sulla porta 21 (per impostazione predefinita il proxy FTP nativo è 8021). Dalla GUI, selezionare **Security Services > FTP Proxy** per la verifica.

Configurazione WSA

1. Crea un'identità per il traffico FTP. Nell'interfaccia utente, scegliere **Web Security Manager > Identities** (Identità) e verificare che l'autenticazione sia stata disabilitata per questo ID.
2. Creare un criterio di accesso. Nella GUI, selezionare **Web Security Manager > Access Policies** (Policy di accesso), che fa riferimento all'identità indicata nel passaggio 1.
3. In Impostazioni proxy FTP, modificare le porte FTP passive in 11000-11006 per garantire che tutte le porte rientrino in un unico gruppo di servizi.
4. Crea i seguenti ID servizio WCCP:

<u>Name Service</u>	<u>Porte</u>
---------------------	--------------

web-cache	0 80 <i>(in alternativa, è possibile utilizzare 98 custom-web-cache se si utilizzano più WSA)</i>
-----------	---

ftp nativo	60 21.1000,11001,11002,11003,11004,11005,11006
------------	--

https-cache	70-443
-------------	--------

In questi esempi vengono reindirizzate tre subnet interne evitando il reindirizzamento WCCP per tutte le destinazioni con indirizzo privato e per un singolo host interno.

Esempio di configurazione dell'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
```

Esempio di configurazione dello switch (c3560)

Questa operazione dovrebbe essere eseguita anche sulla maggior parte dei router.

```
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
```

Nota: A causa di un limite della tecnologia WCCP, è possibile assegnare un massimo di otto porte per ID servizio WCCP.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.