Konfigurieren der transparenten Umleitung mit WCCP für die Umleitung des nativen FTP-Datenverkehrs

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Web Security Appliance (WSA)/der Cisco Router konfiguriert wird, um die transparente Umleitung von HTTP-, HTTPS- und nativem FTP-Datenverkehr mit Web Cache Communication Protocol (WCCP) zu unterstützen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Web Security Appliance, die AsyncOS Version 6.0 oder höher ausführt
- Nativer FTP-Proxy auf WSA aktiviert
- WCCPv2-kompatibler Cisco Router/Switch oder ASA-Firewall

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Wenn nativer FTP-Datenverkehr transparent an die WSA umgeleitet wird, empfängt die WSA in der Regel den Datenverkehr auf dem Standard-FTP-Port 21. Daher sollte der Native FTP-Proxy auf der WSA Port 21 überwachen (standardmäßig ist der native FTP-Proxy 8021). Wählen Sie in der GUI **Sicherheitsdienste > FTP-Proxy** zur Überprüfung aus.

WSA-Konfiguration

1. Erstellen Sie eine Identität für FTP-Datenverkehr. Wählen Sie in der GUI **Web Security Manager > Identities aus,** und stellen Sie sicher, dass die Authentifizierung für diese ID deaktiviert wurde.
2. Erstellen Sie eine Zugriffsrichtlinie. Wählen Sie in der GUI **Web Security Manager > Access Policies (Websicherheits-Manager > Zugriffsrichtlinien)** aus, die auf die Identität in Schritt 1 verweisen.
3. Ändern Sie unter FTP-Proxy-Einstellungen die FTP-Ports Passive (Passiv) auf 11000-11006, um sicherzustellen, dass alle Ports zu einer Servicegruppe gehören.
4. Erstellen Sie folgende WCCP-Dienst-IDs:

   Name Service Ports
   web-cache 0 80 *(alternativ können Sie 98 benutzerdefinierten Web-cache verwenden, wenn Sie mehrere WSAs verwenden)*
   ftp-nativ 60 21,1000,11001,11002,11003,11004,11005,11006
   HTTPS-Cache 70 443

In diesen Beispielen werden drei interne Subnetze umgeleitet, während sie die WCCP-Umleitung für alle privat adressierten Ziele sowie für einen einzelnen internen Host umgehen.

ASA-Beispielkonfiguration

```
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
```

Switch-Beispielkonfiguration (c3560)

Dies sollte auch auf den meisten Routern funktionieren.

```
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
```

> **Hinweis**: Aufgrund einer Beschränkung der WCCP-Technologie können maximal acht Ports pro WCCP-Dienst-ID zugewiesen werden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.