

WSA WCCP für ASA-Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationsübersicht](#)

[Konfigurationsbeispiel](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie das Web Cache Communication Protocol (WCCP) für die Cisco Adaptive Security Appliance (ASA) über die Cisco Web Security Appliance (WSA) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco WSA
- Cisco ASA
- WCCP
- Transparente Proxy-Bereitstellungen

Verwendete Komponenten

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

- Cisco WSA Version 7.x
- Cisco ASA Version 8.x

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

In diesem Abschnitt können Sie das WCCP für die ASA konfigurieren.

Konfigurationsübersicht

Dies sind die Befehle, die in der WSA eingegeben werden, um das WCCP für die ASA zu konfigurieren:

```
hostname(config)# wccp {web-cache | service_number} [redirect-list access_list]
[group-list access_list] [password password]
```

```
hostname(config)# wccp interface interface_name {web-cache | service_number}
redirect in
```

Dies sind die Eintragsbeschreibungen für diesen Befehl:

- **Service-Nummer:** Dies ist eine dynamische Service-ID, d. h. die Dienstdefinition wird vom Cache vorgegeben. Die dynamische Servicenummer kann zwischen 0 und 255 liegen. Die maximal zulässige Zahl ist 256, die den Webcache-Dienst enthält, der mit dem web-cache-Schlüsselwort angegeben wird.
- **Umleitungsliste:** Dies ist ein optionaler Eintrag. Sie wird mit einer Zugriffsliste verwendet, die den an diese Servicegruppe umgeleiteten Datenverkehr steuert. Das access-list-Argument ist eine Zeichenfolge mit maximal 64 Zeichen (Name oder Nummer), die die Zugriffsliste angibt. **Hinweis:** Die ASA Software-Versionen 8.1 und früher akzeptieren den TCP-Port in der Redirect-Liste nicht. Es können nur Netzwerkadressen verwendet werden.
- **Gruppenliste:** Dieser optionale Zugriffslisteneintrag bestimmt die Webcaches, die zur Teilnahme an der Servicegruppe berechtigt sind. Das access-list-Argument ist eine Zeichenfolge mit maximal 64 Zeichen (Name oder Nummer), die die Zugriffsliste angibt.
- **Kennwort:** Dies ist ein optionaler Eintrag, der die MD5-Authentifizierung (Message Digest 5) für die Nachrichten angibt, die von der Servicegruppe empfangen werden. Die Nachrichten, die von der Authentifizierung nicht akzeptiert werden, werden verworfen.

Hinweis: Der Standarddienst ist der Web-Cache (Service-ID 0), der nur den TCP-Port 80 (HTTP)-Datenverkehr abfängt. Für alle anderen angepassten Services empfiehlt Cisco die Verwendung einer Service-ID zwischen 90 und 97.

Konfigurationsbeispiel

Gehen Sie wie folgt vor, um das WCCP für die ASA über die WSA zu konfigurieren:

1. Geben Sie diesen Befehl ein, um den Webcache der Standarddienstgruppe zu verwenden:

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

2. Geben Sie diesen Befehl ein, um eine dynamische Service-Gruppen-ID für die Umleitung von HTTP- und HTTPS-Datenverkehr zu verwenden:

```
wccp 90 redirect-list wccp-hosts group-list wccp-routers
```

3. Geben Sie den folgenden Befehl ein, um die WCCP-Sicherheit zu verwenden:

```
wccp 90 redirect-list wccp-hosts group-list wccp-routers password securewccp
```

4. Die Zugriffsliste kann so konfiguriert werden, dass sie den an die ASA als Ziel-IP-Adresse gesendeten Datenverkehr verweigert und an die WSA umleitet. Dies ist besonders dann nützlich, wenn die ASA so konfiguriert ist, dass der Datenverkehr an mehrere WSAs umgeleitet wird. Beispielsweise können den WSAs folgende IP-Adressen zugewiesen werden:

IP-Adresse WSA1 = 10.0.0.1 WSA2 IP-Adresse = 10.0.0.2

Geben Sie die folgenden Befehle ein, um die Zugriffsliste so zu konfigurieren, dass der Datenverkehr abgelehnt wird:

```
access-list wccp-hosts extended deny tcp any host 10.0.0.1  
access-list wccp-hosts extended deny tcp any host 10.0.0.2
```

5. Geben Sie diesen Befehl ein, um die Umleitung des HTTP-Datenverkehrs zu ermöglichen:

```
access-list wccp-hosts extended permit tcp any any eq www
```

6. Geben Sie diesen Befehl ein, um die Umleitung des HTTPS-Datenverkehrs zu ermöglichen:

```
access-list wccp-hosts extended permit tcp any any eq https
```

7. Geben Sie diese Befehle ein, um die WSAs zu definieren, die an der WCCP-Kommunikation teilnehmen dürfen:

```
access-list wccp-routers standard permit host 10.0.0.1  
access-list wccp-routers standard permit host 10.0.0.2
```

8. Wenn der Befehl redirect-list nicht akzeptiert wird, ist möglicherweise eine erweiterte Zugriffsliste erforderlich. Geben Sie die folgenden Befehle ein, um die erweiterte Zugriffsliste zu konfigurieren:

```
access-list wccp-routers extended permit ip host 10.0.0.1 any  
access-list wccp-routers extended permit ip host 10.0.0.2 any
```

9. Geben Sie den folgenden Befehl ein, um die Konfiguration anzuwenden:

```
wccp interface inside 90 redirect in
```

Überprüfen

Um die globalen Statistiken anzuzeigen, die sich auf WCCP beziehen, geben Sie den Befehl **show wccp** im privilegierten EXEC-Modus ein:

```
show wccp {web-cache | service-number}[detail | view]
show run | inc wccp
```

Hinweis: Der umgeleitete Datenverkehrstyp (HTTP, HTTPS, FTP) wird durch die WSA-WCCP-Konfiguration definiert. Die ASA kann den umgeleiteten Datenverkehr nur mithilfe der Umleitungsliste filtern.

Fehlerbehebung

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

Zugehörige Informationen

- [Konfigurieren von Webcache-Diensten mit WCCP](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)