WSA WCCP-voorbeeld voor ASA-configuratie

Inhoud

Inleiding

Dit document beschrijft hoe u het Web Cache Communication Protocol (WCCP) voor de Cisco adaptieve security applicatie (ASA) moet configureren via de Cisco Web Security Appliance (WSA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco WSA
- Cisco ASA
- WCCP
- Transparante proxy-implementaties

Gebruikte componenten

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

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

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

Gebruik dit gedeelte om de WCCP voor de ASA te configureren.

Overzicht van configuratie

Dit zijn de opdrachten die op de WSA zijn ingevoerd om de WCCP voor de ASA te configureren:

```
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
```

Dit zijn de invoerbeschrijvingen voor deze opdracht:

- servicenummer: Dit is een dynamische service identifier, wat betekent dat de service definitie wordt gedicteerd door de cache. Het dynamische servicenummer kan variëren van 0 tot 255. Het maximaal toegestane nummer is 256, dat de web-cache service omvat die wordt gespecificeerd met het web-cache sleutelwoord.

- vervolgkeuzelijst: Dit is een optionele vermelding. Het wordt gebruikt met een toegangslijst die het verkeer controleert dat naar deze servicegroep wordt verstuurd. Het access-list argument is een string van niet meer dan 64 tekens (naam of nummer) die de toegangslijst specificeert. Opmerking: De ASA-softwareversies 8.1 en eerder aanvaarden de TCP-poort in de vervolgkeuzelijst niet. alleen netwerkadressen kunnen worden gebruikt .
- groepslijst: Dit is een optionele access list die bepaalt welke webcaches mogen deelnemen aan de servicegroep. Het access-list argument is een string van niet meer dan 64 tekens (naam of nummer) die de toegangslijst specificeert.

- wachtwoord: Dit is een optionele ingang die de Message Digest 5 (MD5) verificatie specificeert voor de berichten die van de servicegroep worden ontvangen. De berichten die niet door de authenticatie worden geaccepteerd, worden weggegooid.

  Opmerking: De standaardservice is web-cache (Service ID 0), die alleen TCP Port 80 (HTTP)-verkeer onderschept. Voor andere aangepaste services raadt Cisco u aan een Service-ID tussen 90 en 97 te gebruiken.

Configuratievoorbeeld

Voltooi deze stappen om de WCCP voor de ASA te configureren via de WSA:

1. Voer deze opdracht in om de standaard servicegroep web-cache te gebruiken:

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

2. Typ deze opdracht om een dynamische servicegroep-ID te gebruiken voor de omleiding van HTTP- en HTTPS-verkeer:

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

3. Typ deze opdracht om WCCP-beveiliging te gebruiken:

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

4. De toegangslijst kan zo worden geconfigureerd dat deze het verkeer ontkent dat naar de ASA wordt verzonden als een IP-adres van de bestemming en deze naar de WSA doorstuurt. Dit is in het bijzonder nuttig wanneer de ASA is geconfigureerd om het verkeer naar meerdere WSA's te richten. Bijvoorbeeld, WSAs zou deze IP adressen kunnen worden toegewezen:

   WSA1 IP-adres = 10.0.0.1WSA2 IP-adres = 10.0.0.2

   Voer deze opdrachten in om de toegangslijst te configureren om het verkeer te ontkennen:

```
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. Voer deze opdracht in om het HTTP-verkeer opnieuw te kunnen sturen:

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

6. Typ deze opdracht om HTTPS-verkeer opnieuw te sturen:

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

7. Voer deze opdrachten in om de WSA's te definiëren die mogen deelnemen aan de WCCP-communicatie:

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

8. Als de opdracht opnieuw direct-list niet wordt geaccepteerd dan kan een uitgebreide toegangslijst nodig zijn. Voer deze opdrachten in om de uitgebreide toegangslijst te configureren:

```
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. Typ deze opdracht om de configuratie toe te passen:

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

Verifiëren

Om de mondiale statistieken die met WCCP verband houden weer te geven, voert u de opdracht **WCCP** in bevoorrechte EXEC-modus **in**:

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

> Opmerking: Het type verkeer (HTTP, HTTPS, FTP) dat wordt omgeleid wordt gedefinieerd door de WSA WCCP-configuratie. ASA kan alleen het geregisseerde verkeer filteren met het gebruik van de vervolgkeuzelijst.

Problemen oplossen

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

Gerelateerde informatie

- Web cacheservices configureren met WCCP
- Technische ondersteuning en documentatie – Cisco Systems