

# WSA WCCP for ASA配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[組態概觀](#)

[組態範例](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本檔案介紹如何透過思科網路安全裝置(WSA)為思科調適型安全裝置(ASA)設定網路快取通訊協定(WCCP)。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco WSA
- Cisco ASA
- WCCP
- 透明代理部署

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco WSA版本7.x
- Cisco ASA版本8.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

# 設定

使用本節內容可為ASA配置WCCP。

## 組態概觀

在WSA上輸入以下命令，以便為ASA配置WCCP:

```
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
```

以下是此命令的條目說明：

- **service-number**:這是一個動態服務識別符號，這意味著服務定義由快取決定。動態服務編號的範圍可以是0到255。允許的最大數量是256，其中包括使用web-cache關鍵字指定的web-cache服務。
- **redirect-list**:這是一個可選條目。它與訪問控制清單一起使用，後者控制重定向到此服務組的流量。access-list引數是一個字串，它最多包含64個字元（名稱或數字），用於指定訪問清單。  
**附註**：ASA軟體8.1及更低版本不接受redirect-list中的TCP連線埠；只能使用網路地址。
- **group-list**:這是一個可選的訪問清單條目，用於確定允許參與服務組的Web快取。access-list引數是一個字串，它最多包含64個字元（名稱或數字），用於指定訪問清單。
- **密碼**:這是一個可選條目，它指定從服務組接收的消息的消息摘要5(MD5)身份驗證。身份驗證不接受的消息將被丟棄。

**附註**：標準服務是Web快取(服務ID 0)，它僅攔截TCP連線埠80(HTTP)流量。對於任何其他自定義服務，思科建議您使用介於90和97之間的服務ID。

## 組態範例

完成以下步驟，以便通過WSA為ASA配置WCCP:

1. 輸入以下命令可使用預設服務組Web-cache:

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

2. 輸入以下命令可對HTTP和HTTPS流量的重新導向使用動態服務組ID:

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

3. 輸入以下命令以使用WCCP安全性：

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

4. 可以配置訪問清單，使其拒絕傳送到ASA的流量作為目標IP地址並將其重定向到WSA。當ASA配置為將流量重定向到多個WSA時，這一點特別有用。例如，可以為WSA分配以下IP地址：

WSA1 IP地址= 10.0.0.1 WSA2 IP地址= 10.0.0.2

輸入以下命令可設定存取清單以拒絕流量：

```
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. 輸入以下命令可允許重新導向HTTP流量：

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

6. 輸入以下命令可允許重新導向HTTPS流量：

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

7. 輸入以下命令以定義允許參與WCCP通訊的WSA:

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

8. 如果不接受redirect-list命令，則可能需要擴展訪問清單。輸入以下命令以設定延伸存取清單：

```
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. 輸入以下命令以應用設定：

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

## 驗證

若要顯示與WCCP相關的全域性統計資訊，請在特權EXEC模式下輸入**show wccp**命令：

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

**附註：**重定向的流量型別(HTTP、HTTPS、FTP)由WSA WCCP配置定義。ASA只能使用redirect-list過濾重定向流量。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

## 相關資訊

- [使用WCCP配置Web快取服務](#)
- [技術支援與文件 - Cisco Systems](#)