

WCCP sur ASA : Concepts, limitations et configuration

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Présentation de WCCP et ASA](#)

[Redirection WCCP](#)

[Groupes de services WCCP](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les concepts, les limites et la configuration du protocole WCCP (Web Cache Coordination Protocol) sur un appareil de sécurité adaptatif Cisco (ASA). WCCP est une méthode par laquelle l'ASA peut rediriger le trafic vers un moteur de mise en cache WCCP via un tunnel GRE (Generic Routing Encapsulation).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- WCCP (Web Cache Communications Protocol) version 2 (v2)
- Appareils de sécurité adaptatifs Cisco (ASA)
- Logiciel Cisco Adaptive Security Appliance (ASA); lire Guides de configuration pour la compatibilité
- Mise en cache du proxy
- Redirection

Cisco vous recommande également de comprendre les limites de la configuration WCCP sur l'ASA, comme expliqué dans ces documents :

- [Guide de configuration de la gamme Cisco ASA 5500 à l'aide de l'interface de ligne de commande, version 8.2 : Configuration des services de cache Web à l'aide de WCCP : Directives et limitations](#)
- [Guide de configuration de l'interface de ligne de commande de la gamme Cisco ASA, 9.0 : Configuration des services de cache web utilisant WCCP](#)

Components Used

Les informations de ce document sont basées sur le protocole WCCP (Web Cache Communications Protocol) version 2 (V2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Présentation de WCCP et ASA

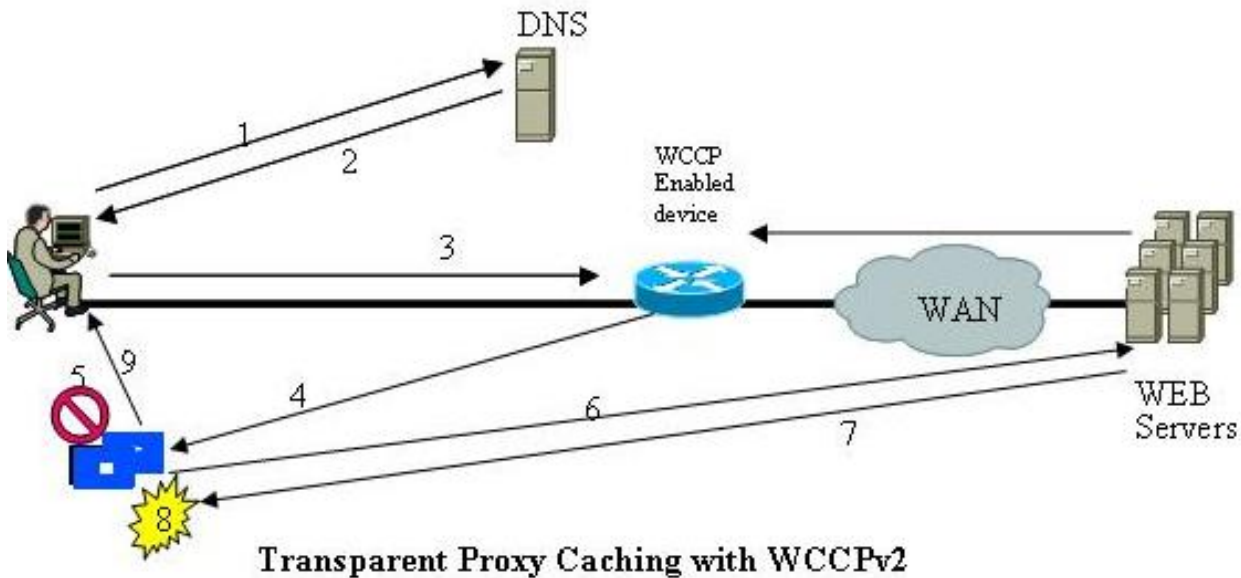
Le WCCP spécifie les interactions entre un ou plusieurs routeurs et un ou plusieurs caches Web. L'objectif de l'interaction est d'établir et de maintenir la redirection transparente de certains types de trafic qui transitent par un groupe de routeurs. Le trafic sélectionné est redirigé vers un groupe de caches Web afin d'optimiser l'utilisation des ressources et de réduire les temps de réponse.

Pour WCCP, l'ASA choisit l'adresse IP la plus élevée configurée sur une interface et l'utilise comme ID de routeur. Il s'agit exactement du même processus que celui suivi par le protocole OSPF (Open Shortest Path First) pour l'ID de routeur. Lorsque l'ASA redirige les paquets vers le moteur de cache (CE), l'ASA source la redirection à partir de l'adresse IP de l'ID de routeur (même si elle provient d'une autre interface) et encapsule le paquet dans un en-tête GRE.

La connexion GRE est unidirectionnelle. L'ASA encapsule les paquets redirigés dans GRE et les envoie au moteur de mise en cache. L'ASA ne traite aucune réponse encapsulée GRE du CE. Le CE doit communiquer directement avec l'hôte interne.

Le flux de travail pour la redirection comporte les étapes suivantes :

1. L'hôte utilise la passerelle par défaut de l'ASA afin d'ouvrir la connexion HTTP.
2. L'ASA redirige le paquet (encapsulé dans GRE) vers le CE.
3. Le CE vérifie ou met à jour le cache du site demandé.
4. Le CE répond directement à l'hôte. Tous les paquets sortants de l'hôte sont redirigés de l'ASA vers le CE. Tous les paquets entrants du serveur vers l'hôte sont dirigés du CE vers l'hôte.



L'ASA implémente WCCP V2. Si le serveur prend en charge WCCP V2, il doit être compatible.

Redirection WCCP

WCCP V2 définit des mécanismes qui permettent à un ou plusieurs routeurs activés pour la redirection transparente de détecter, vérifier et annoncer la connectivité à un ou plusieurs caches Web. Voici les étapes de la redirection WCCP :

1. L'utilisateur entre une URL dans un navigateur.
2. L'URL est transmise au système de noms de domaine (DNS) pour la résolution d'adresse.
3. L'URL est résolue en adresse IP du serveur Web.
4. Le client initie une connexion au serveur avec une requête SYN.
5. Sur le routeur actif, le service de cache Web WCCP intercepte la requête HTTP (port TCP 80) et redirige la requête vers les caches en fonction de la distribution de charge configurée : En cas d'accès au cache, le CE répond à l'GET d'origine avec le contenu demandé et utilise l'adresse IP source du serveur d'origine dans le pack de réponses. Si le contenu demandé n'est pas déjà stocké sur le CE, il manque un cache : Le CE établit une connexion au serveur d'origine, utilise sa propre adresse IP comme source et envoie le HTTP GET. Le serveur répond à CE avec du contenu. Le CE écrit une copie du contenu pouvant être mis en cache sur le disque.

Groupes de services WCCP

Une fois la connectivité établie, les routeurs et les caches Web forment des groupes de services afin de gérer la redirection du trafic dont les caractéristiques font partie de la définition du groupe de services.

Un cache Web transmet un message WCCP2_HERE_I_AM à chaque routeur du groupe à des intervalles de 10 secondes HERE_I_AM_T afin de rejoindre et de maintenir son appartenance à un groupe de services. Le message peut être transmis en monodiffusion à chaque routeur ou en multidiffusion à l'adresse de multidiffusion du groupe de services configuré.

- Le composant Informations d'identité du cache Web du message WCCP2_HERE_I_AM identifie le cache Web par adresse IP.
- Le composant Service Info du message WCCP2_HERE_I_AM identifie et décrit le groupe de services auquel le cache Web souhaite participer.

Groupe de services	Type	Description
Service 0	Cache Web	Service de mise en cache Web qui permet à l'ASA de rediriger le trafic HTTP vers le CE.
Service 53	DNS	Service de mise en cache DNS qui permet à l'ASA de rediriger les requêtes du client DNS de manière transparente vers le moteur du client.
Service 60	natif FTP	Service de mise en cache qui permet à l'ASA de rediriger les requêtes natives FTP de manière transparente vers un port unique sur le moteur de contenu.
Service 70	https-cache	Service de mise en cache qui permet à l'ASA d'intercepter le trafic TCP du port 443 et de rediriger ce trafic HTTPS vers le moteur de contenu.
Service 80	rtsp	Service de diffusion multimédia en continu qui permet à l'ASA de rediriger les requêtes client RTSP (Real Time Streaming Protocol) vers un port unique du moteur de contenu.
Service 81	mmst	Service de mise en cache de support qui permet à l'ASA d'utiliser la redirection Microsoft Media Server (MST) basée sur TCP afin d'acheminer les requêtes client de la technologie Windows Media (WMT) vers le port TCP 1755 sur le moteur de contenu.
Service 82	mmsu	Service de mise en cache de support qui permet à l'ASA d'utiliser la redirection MMSU (User Datagram Protocol) basée sur le protocole UDP (User Datagram Protocol) afin d'acheminer les requêtes client WMT vers le port UDP 1755 sur le moteur de contenu.
Service 83	wmt-rtsp	Service de diffusion multimédia en continu qui permet à l'ASA de rediriger les demandes RTSP des clients Windows Media Service 9 vers le port UDP 5005 sur le CE.
Service 90-97	configurable par l'utilisateur	Services WCCP définis par l'utilisateur qui prennent en charge jusqu'à huit ports pour chaque service WCCP. Lorsque vous configurez ces services définis par l'utilisateur, vous devez spécifier s'il faut rediriger le trafic vers l'application de mise en cache HTTP, vers l'application HTTPS ou vers l'application de diffusion en continu sur le moteur de contenu.
Service 98	custom-web-cache	Service de mise en cache qui permet à l'ASA de rediriger de manière transparente le trafic HTTP vers le moteur de contenu sur plusieurs ports autres que le port

		80.
Service 99	proxy inverse	Service de mise en cache qui permet à l'ASA de rediriger le trafic de proxy inverse HTTP vers le moteur de contenu sur le port 80.

Un groupe de services est identifié par le type de service et l'ID de service. Il existe deux types de groupes de services :

- Services connus
- Services dynamiques

Les services connus sont connus à la fois par les caches ASA et Web et ne nécessitent aucune description autre qu'un ID de service.

En revanche, les services dynamiques doivent être décrits comme ASA. L'ASA peut être configuré pour participer à un groupe de services dynamique particulier, identifié par l'ID de service, sans connaissance des caractéristiques du trafic associé à ce groupe de services. La description du trafic est communiquée à l'ASA dans le message WCCP2_HERE_I_AM du premier cache Web afin de rejoindre le groupe de services. Un cache Web utilise les champs Protocol, Service Flags et Port du composant Service Info afin de décrire un service dynamique. Une fois qu'un service dynamique a été défini, l'ASA rejette tout message WCCP2_HERE_I_AM ultérieur contenant une description conflictuelle. L'ASA rejette également un message WCCP2_HERE_I_AM qui décrit un groupe de services pour lequel il n'a pas été configuré.

Les numéros 0 à 254 sont des services dynamiques et le service de cache Web est un service standard, ou bien connu. Cela signifie que lorsque le service de cache Web est spécifié, le protocole WCCP V2 a prédéfini que le trafic du port de destination TCP 80 doit être redirigé. Pour les numéros 0 à 254, chaque numéro représente un groupe de services dynamique. Les CE WCCP (tels que Bluecoat) doivent définir un ensemble de protocoles et de ports qui doivent être redirigés pour chaque groupe de services. Ensuite, lorsque l'ASA est configuré avec le même numéro de groupe de services (wccp 0 ... ou wccp 1 ...), l'ASA effectue la redirection sur les protocoles et les ports spécifiés, comme indiqué par le périphérique Bluecoat.

Voici un exemple qui montre les informations d'identité du cache Web :

```

Frame 1 (170 bytes on wire, 170 bytes captured)
  Ethernet II, Src: Cisco_22:c3:41 (00:14:a9:22:c3:41), Dst: Cisco_d6:ae:63 (00:18:73:d6:ae:63)
  Internet Protocol, Src: 10.101.201.19 (10.101.201.19), Dst: 199.201.186.92 (199.201.186.92)
  User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
  Web Cache Coordination Protocol
    WCCP Message Type: 2.0 Here I am (10)
    WCCP Version: 2 (0x00000200)
    Length: 120
    Security Info
    Service Info
    web-cache Identity Info
      Type: web-cache Identity Info
      Length: 44
      web-cache Identity Element: IP address 10.101.201.19 Web-cache server Identity Info
    web-cache View Info
    Capabilities Info
  
```

Voici un exemple qui montre que le cache Web fait partie du groupe de services 0 :

```

+ Frame 1 (170 bytes on wire, 170 bytes captured)
+ Ethernet II, Src: Cisco_22:c3:41 (00:14:a9:22:c3:41), Dst: Cisco_d6:ae:63 (00:18:73:d6:ae:63)
+ Internet Protocol, Src: 10.101.201.19 (10.101.201.19), Dst: 199.201.186.92 (199.201.186.92)
+ User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
- Web Cache Coordination Protocol
  WCCP Message Type: 2.0 Here I am (10)
  WCCP Version: 2 (0x00000200)
  Length: 120
+ Security Info
- Service Info
  Type: Service Info
  Length: 24
  Service Type: well-known service
  Service ID: HTTP
+ Flags: 0x00000000
+ Web-Cache Identity Info
+ Web-Cache View Info
+ Capabilities Info

```

Service-group=0, will show up as "Service ID:HTTP". On ASA, web-cache is service-group 0

Voici un exemple qui montre un serveur de cache Web faisant partie du groupe de service client 91 et les ports dont le trafic est redirigé vers le serveur :

```

+ Frame 1 (166 bytes on wire, 166 bytes captured)
+ Ethernet II, Src: IntelCor_3a:d6:ef (00:15:17:3a:d6:ef), Dst: Cisco_80:f1:3f (00:13:c4:80:f1:3f)
+ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 990
+ Internet Protocol, Src: 10.99.0.10 (10.99.0.10), Dst: 10.99.0.1 (10.99.0.1)
+ User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
- Web Cache Coordination Protocol
  WCCP Message Type: 2.0 Here I am (10)
  WCCP Version: 2 (0x00000200)
  Length: 112
+ Security Info
- Service Info
  Type: Service Info
  Length: 24
  Service Type: dynamic service
  Service ID: Unknown (0x5b)
  Priority: 0
  Protocol: 6
+ Flags: 0x00000013
  Port 0: 80
  Port 1: 8080
  Port 2: 443
  Port 3: 0
  Port 4: 0
  Port 5: 0
  Port 6: 0
  Port 7: 0
+ Web-Cache Identity Info
+ Web-Cache View Info

```

User-defined service-group. Hex 5b = 91 (Decimal)

Traffic of these ports will be redirected to this WCCP server.

ASA répond à un message WCCP2_HERE_I_AM avec un message WCCP2_I_SEE_YOU.

- Si le message WCCP2_HERE_I_AM était monodiffusion, le routeur répond immédiatement avec un message WCCP2_I_SEE_YOU monodiffusion.
- Si le message WCCP2_HERE_I_AM était multidiffusion, le routeur répond avec le message de multidiffusion planifié WCCP2_I_SEE_YOU pour le groupe de services.

Voici un exemple du message router/ASA 'I See You', qui indique que le routeur rejoint le groupe de services 91 et redirige les ports 80, 8080 et 443 vers le serveur de cache Web :

```

# Frame 2 (186 bytes on wire, 186 bytes captured)
# Ethernet II, Src: Cisco_80:f1:3f (00:13:c4:80:f1:3f), Dst: IntelCor_3a:d6:ef (00:15:17:3a:d6:ef)
# 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 990
# Internet Protocol, Src: 10.99.0.1 (10.99.0.1), Dst: 10.99.0.10 (10.99.0.10)
# User Datagram Protocol, Src Port: dls-monitor (2048), Dst Port: dls-monitor (2048)
# Web Cache Coordination Protocol
  (WCCP Message Type: 2.0 I see you (11)) Sample message of Router "I See You"
  WCCP Version: 2 (0x00000200)
  Length: 132
# Security Info
# Service Info
  Type: Service Info
  Length: 24
  Service Type: Dynamic service
  (Service ID: unknown (0x5B)) Router is joining service-group 91
  Priority: 0
  Protocol: 6
# Flags: 0x00000013
  (Port 0: 80
  Port 1: 8080) These ports will be redirected by router for this service-group to the Web-cache server.
  Port 2: 443
  Port 3: 0
  Port 4: 0
  Port 5: 0
  Port 6: 0
  Port 7: 0
# Router Identity Info
# Router View Info

```

Voici un exemple de paquet GRE :

```

# Frame 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
# Ethernet II, Src: Cisco_17:ea:a1 (00:19:55:17:ea:a1), Dst: TyanComp_4e:c5:29 (00:e0:81:4e:c5:29)
# Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 10.0.127.3 (10.0.127.3)
# Generic Routing Encapsulation (WCCP)
# Internet Protocol Version 4, Src: 10.150.5.105 (10.150.5.105), Dst: 208.85.41.11 (208.85.41.11)
# Transmission Control Protocol, Src Port: vlsi-lm (1500), Dst Port: http (80), Seq: 2105048349, Ack: 3450412869, Len: 0

```

Configuration

Note: Dans la liste de redirection, la liste d'accès ne doit contenir que des adresses réseau. Les entrées spécifiques aux ports ne sont pas prises en charge.

Note: Pour plus d'informations sur la commande **wccp**, voir [Référence des commandes de la gamme Cisco ASA 5500, 8.2](#).

Cette procédure décrit comment configurer WCCP sur un ASA :

1. Entrez la commande **wccp** afin de spécifier le trafic à rediriger :

```
wccp {web-cache | service_number} [redirect-list access_list] [group-list access_list]
[password password]
```

2. Entrez la commande **wccp** afin de spécifier l'interface sur laquelle la redirection du trafic doit se produire :

```
wccp interface interface_name {web-cache | service_number} redirect in
```

Note: La redirection WCCP est prise en charge uniquement à l'entrée d'une interface.

Voici un exemple de configuration ASA :

```
access-list caching permit ip source_subnet mask any
wccp 90 redirect-list caching
wccp interface 90 redirect in
```

Helpful Commands:

```
show wccp
```

show wccp 90 service -> this should indicate the ports that are being serviced by this WCCP server. Without the 'service-flags ports-defined' in the Cache server configuration, the ports to be redirected are NOT passed to the ASA. Therefore, the traffic will never be redirected. This will result in 'Unassigned' increases with 'show wccp'.

```
ASA# show wccp 90 service
```

WCCP service information definition:

```
Type:          Dynamic
Id:            90
Priority:       0
Protocol:      6
Options:       0x00000013
```

```
Hash:          SrcIP DstIP
Alt Hash:      -none-
Ports:         Destination:: 80 8080 0 0 0 0 0 0
```

```
ASA# show wccp 90 view
```

WCCP Routers Informed of:

```
X.X.X.X [Higher IP address on the device will be seen here]
```

WCCP Cache Engines Visible:

```
Y.Y.Y.Y [IP address of the web-cache server in the service-group 91]
```

Note: Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\)](#) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Si la redirection ne fonctionne pas comme prévu, utilisez ces sorties afin de dépanner. Toutes ces sorties sont sur ASA.

- **show tech-support**
- **show wccp [service|view|hash|bucket|detail]**
- **show asp table classify**

Si le résultat de ces trois commandes semble valide, vous devrez peut-être :

- Examinez les Syslogs appropriés.
- Utilisez la commande **capture** afin d'examiner les captures entre l'interface ASA et l'IP du serveur de cache Web et les captures entre le client et le serveur Web auquel il tente d'accéder.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Informations connexes

- [Guides de référence des pare-feu de nouvelle génération Cisco ASA 5500](#)
- [Guides de configuration des pare-feu de nouvelle génération de la gamme Cisco ASA 5500](#)
- [Support et documentation techniques - Cisco Systems](#)