

ASA の WCCP : 概念、制限事項、および設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[WCCP と ASA の概要](#)

[WCCP リダイレクション](#)

[WCCP サービスグループ](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス (ASA) 上の Web Cache Coordination Protocol (WCCP) の概念、制限、および設定について説明します。WCCP は、ASA が Generic Routing Encapsulation (GRE) トンネル経由で WCCP キャッシュ エンジンにトラフィックをリダイレクトする手段です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Web Cache Communication Protocol (WCCP) バージョン 2 (v2)
- Cisco Adaptive Security Appliances (ASA)
- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア : 互換性については、コンフィギュレーション ガイドを参照
- プロキシ キャッシング
- リダイレクション

以下のドキュメントを読んで ASA 上の WCCP 設定の制限を理解することもお勧めします。

- [CLI 8.2 を使用した Cisco ASA 5500 シリーズ設定ガイド : WCCP による Web キャッシュ サービスの設定注意事項と制約事項](#)

- [Cisco ASA シリーズ CLI コンフィギュレーション ガイド 9.0 : WCCP を使用した Web キャッシュ サービスの設定](#)

使用するコンポーネント

このドキュメント内の情報は、Web Cache Communication Protocol (WCCP) バージョン 2 (V2) に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

WCCP と ASA の概要

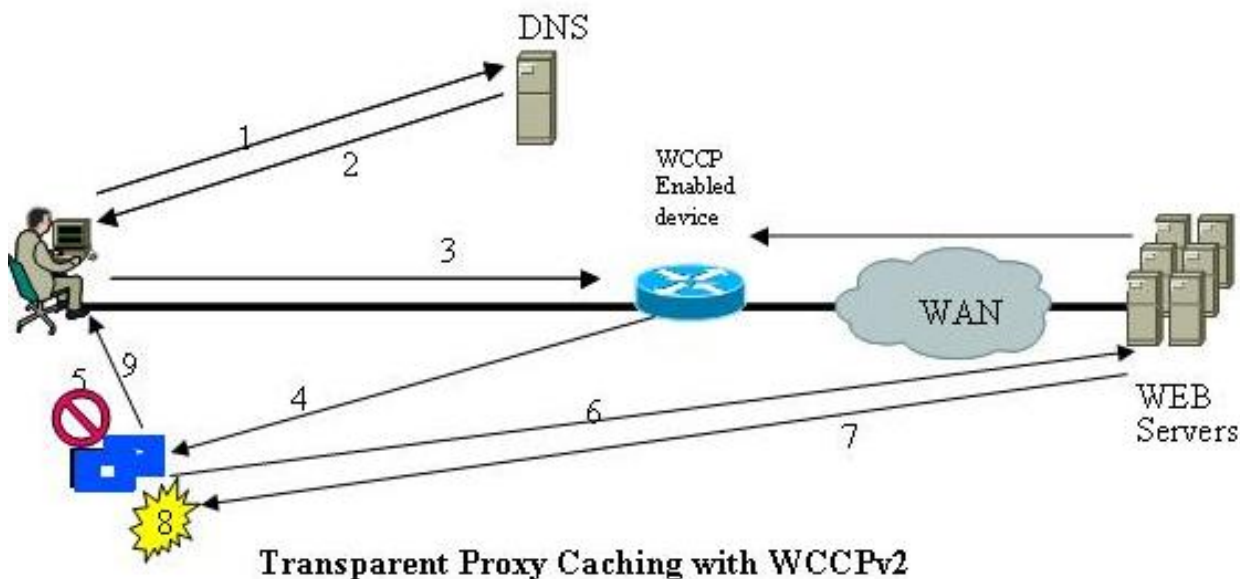
WCCP は、1 つ以上のルータと 1 つ以上の Web キャッシュ間の相互作用を規定しています。相互作用の目的は、ルータのグループを通過する選択されたトラフィックのタイプの透過的なリダイレクションを確立し、維持することです。選択されたトラフィックは、リソース使用率の最適化と応答時間の短縮のために Web キャッシュのグループにリダイレクトされます。

WCCP では、ASA がインターフェイス上に設定された最上位の IP アドレスを選択し、それをルータ ID として使用します。これは、Open Shortest Path First (OSPF) がルータ ID に関して従うプロセスとまったく同じです。ASA は、パケットをキャッシュ エンジン (CE) にリダイレクトするときに、ルータ ID IP アドレス (別のインターフェイスが起源でも) からリダイレクトを実行し、パケットを GRE ヘッダーにカプセル化します。

GRE 接続は単方向です。ASA は、リダイレクトするパケットを GRE にカプセル化し、それをキャッシュ エンジンに送信します。ASA は、CE からの GRE カプセル化応答を処理しません。CE は、内部ホストと直接通信する必要があります。

リダイレクションの作業フローには以下の手順が含まれます。

1. ホストが ASA のデフォルト ゲートウェイを使用して HTTP 接続を開きます。
2. ASA がパケット (GRE にカプセル化) を CE にリダイレクトします。
3. CE が要求されたサイトのキャッシュを検証または更新します。
4. CE がホストに直接応答します。ホストからのすべてのアウトバウンド パケットが ASA から CE にリダイレクトされます。サーバからホストへのすべてのインバウンド パケットが CE からホストに転送されます。



ASAはWCCP V2を実装します。サーバがWCCP V2をサポートしている場合は、互換性がある必要があります。

WCCP リダイレクション

WCCP V2 は、1 つ以上の Web キャッシュへの接続を検出、検証、およびアドバタイズするための透過的なリダイレクションに対して 1 つ以上のルータを有効にするメカニズムを定義しています。WCCP リダイレクションの手順を以下に示します。

1. ユーザが URL をブラウザに入力します。
2. URL がアドレス解決のためにドメイン ネーム システム (DNS) に転送されます。
3. URL が Web サーバの IP アドレスに解決されます。
4. クライアントが SYN 要求を使ってサーバへの接続を開始します。
5. アクティブ ルータでは、WCCP Web キャッシュ サービスが HTTP 要求 (TCP ポート 80) をインターセプトし、設定された負荷分散に基づいてその要求をキャッシュにリダイレクトします。キャッシュ ヒットが発生すると、CE が、要求されたコンテンツを使って元の GET に応答し、応答パック内の配信元サーバの送信元 IP アドレスを使用します。要求されたコンテンツがまだ CE 上に保存されていない場合は、キャッシュ ミスが発生します。CE が配信元サーバへの接続を確立して、それ自体の IP アドレスを送信元として使用し、HTTP GET を送信します。サーバがコンテンツを使って CE に応答します。CE がキャッシュ可能コンテンツのコピーをディスクに書き込みます。

WCCP サービス グループ

接続が確立されると、ルータと Web キャッシュがサービス グループを形成して、サービス グループ定義に特性が含まれているトラフィックのリダイレクションを処理します。

Web キャッシュは、HERE_I_AM_T (10) 秒間隔でグループ内の各ルータに WCCP2_HERE_I_AM メッセージを送信し、サービスグループに参加してそのメンバーシップを維持するように指示します。メッセージは、ユニキャストで各ルータに送信することも、マルチキャストで設定されたサービスグループのマルチキャストアドレスに送信することもできます。

- WCCP2_HERE_I_AM メッセージ内の Web-Cache Identity Info コンポーネントは、IP アドレスで Web キャッシュを識別します。
- WCCP2_HERE_I_AM メッセージの Service Info コンポーネントは、Web キャッシュが参加するサービスグループを識別して記述します。

サービスグループ	Type	説明
サービス 0	Web-cache	ASA に CE への HTTP トラフィックのリダイレクトを許可する Web キャッシュ サービス。
サービス 53	DNS	ASA にクライアント エンジンへの DNS クライアント要求の透過的なリダイレクトを許可する DNS キャッシング サービス。
サービス 60	FTP-native	ASA にコンテンツ エンジン上の単一ポートへの FTP ネイティブ要求のリダイレクトを許可するキャッシング サービス。
サービス 70	https-cache	ASA にポート 443 TCP トラフィックのインターセプトとコンテンツ エンジンへの HTTPS トラフィックのリダイレクトを許可するキャッシング サービス。
サービス 80	rtsp	ASA にコンテンツ エンジン上の単一ポートへの Real Time Streaming Protocol (RTSP) クライアント要求のリダイレクトを許可するメディアストリーミング サービス。
サービス 81	mmst	ASA に TCP ベースの Microsoft Media Server (MMST) リダイレクションを使用した、コンテンツ エンジン上の TCP ポート 1755 への Windows Media Technology (WMT) クライアント要求のルーティングを許可するメディアストリーミング サービス。
サービス 82	mmsu	ASA に User Datagram Protocol (UDP) ベースの Microsoft Media Server (MMSU) リダイレクションを使用した、コンテンツ エンジン上のポート 1755 への WMT クライアント要求のルーティングを許可するメディアストリーミング サービス。
サービス 83	wmt-rtsp	ASA に Windows Media サービス 9 クライアントから CE 上の UDP ポート 5005 への RTSP 要求のリダイレクトを許可するメディアストリーミング サービス。
サービス 90 ~ 97	user configurable	WCCP サービスごとに最大 8 つのポートをサポートするユーザ定義のサービス。このようなユーザ定義のサービスを設定する場合は、トラフィックを HTTP キャッシング アプリケーションにリダイレクトするのか、HTTPS キャッシング アプリケーションにリダイレクトするのか、コンテンツ エンジン上のストリーミング アプリケーションにリダイレクトするのかを指定する必要があります。
サービス 98	custom-web-cache	ASA にコンテンツ エンジン上のポート 80 以外の複数のポートへの HTTP トラフィックの透過的なリダイレクトを許可するキャッシング サービス。
サービス 99	reverse-proxy	ASA にポート 80 上のコンテンツ エンジンへの HTTP リバースプロキシのトラフィックのリダイレクトを許可するキャッシング サービス。

サービスグループは、サービスタイプとサービス ID で識別されます。次の 2 種類のサービスグループがあります。

- 既知のサービス
- ダイナミック サービス

既知のサービスは、ASA と Web キャッシュの両方で認識され、サービス ID 以外の記述を必要としません。

これに対して、ダイナミック サービスは ASA に対して記述する必要があります。ASA は、サービス グループに関連付けられたトラフィックの特性を知らなくても、サービス ID で識別される特定のダイナミック サービス グループに参加するように設定できます。トラフィック記述は、サービス グループに参加するための最初の Web キャッシュの WCCP2_HERE_I_AM メッセージで ASA に渡されます。Web キャッシュは、Service Info コンポーネントの Protocol、Service Flags、および Port の各フィールドを使用してダイナミック サービスを記述します。ダイナミック サービスが定義されると、ASA は矛盾した記述を含む後続の WCCP2_HERE_I_AM メッセージをすべて破棄します。また、まだ設定されていないサービス グループが記述された WCCP2_HERE_I_AM メッセージも破棄します。

0 ~ 254 の番号がダイナミック サービスで、Web キャッシュ サービスは標準サービス、つまり、既知のサービスです。これは、Web キャッシュ サービスが指定された場合は、WCCP V2 プロトコルで TCP 宛先ポート 80 トラフィックがリダイレクトされることが事前に定義されていることを意味します。0 ~ 254 の番号の場合は、それぞれがダイナミック サービス グループを表します。WCCP CE (Bluecoat など) がサービス グループごとにリダイレクトするプロトコルとポートのセットを定義します。次に、ASAが同じサービスグループ番号 (wccp 0 ...またはwccp 1 ...) で設定されている場合、ASAは指定されたプロトコルとポートでBluecoatデバイスの指示に従ってリダイレクションを実行します。

Web-Cache Identity Info の例を以下に示します。

```
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
```

Web キャッシュがサービス グループ 0 に属している例を以下に示します。

```
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-group=0, will show up as "Service ID:HTTP". On
    Service ID: HTTP ASA, web-cache is service-group 0
  Flags: 0x00000000
  web-cache Identity Info
  web-cache View Info
  Capabilities Info
```

カスタマー サービス グループ 91 に属している Web キャッシュ サーバとトラフィックがサーバにリダイレクトされるポートの例を以下に示します。

```
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) User-defined service-group. Hex 5b = 91 (Decimal)
    Priority: 0
    Protocol: 6
  Flags: 0x00000013
  Port 0: 80
  Port 1: 8080 Traffic of these ports will be redirected to this WCCP server.
  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
```

ASA は、WCCP2_I_SEE_YOU メッセージを使用して WCCP2_HERE_I_AM メッセージに回答します。

- WCCP2_HERE_I_AM メッセージがユニキャストだった場合、ルータはユニキャスト WCCP2_I_SEE_YOU メッセージを使用して即座に回答します。
- WCCP2_HERE_I_AM メッセージがマルチキャストだった場合、ルータはサービスグループに対してスケジューラされたマルチキャスト WCCP2_I_SEE_YOU メッセージを使用して回答します。

ルータ/ASA 'I See You' メッセージの例を以下に示します。この例では、ルータがサービスグループ 91 に参加して、ポート 80、8080、および 443 を Web キャッシュ サーバにリダイレクトします。

```
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
```

GRE パケットの例を以下に示します。

```
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
```

設定

注：リダイレクトリストでは、アクセスリストにネットワークアドレスだけが含まれている必要があります。ポート固有のエントリはサポートされていません。

注：wccp コマンドの詳細については、『[Cisco ASA 5500 シリーズ コマンド リファレンス 8.2](#)』を参照してください。

この手順では、ASA 上で WCCP を設定する方法について説明します。

1. wccp コマンドを入力して、リダイレクトするトラフィックを指定します。

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

2. wccp コマンドを入力して、トラフィック リダイレクションを実行するインターフェイスを指定します。

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

注：WCCP リダイレクトは、インターフェイスの入力側だけでサポートされています。

ASA 設定の例を以下に示します。

```
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]
```

注：このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \(登録ユーザ専用\)](#) を使用してください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

リダイレクトが想定どおりに動作しない場合は、次の出力を使用してトラブルシューティングします。この出力はすべて ASA に関するものです。

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

この3つのコマンドの出力が有効と判断した場合は、以下の手順を実行する必要があります。

- 該当する syslog を確認します。
- capture コマンドを使用して、ASA インターフェイスと Web キャッシュ サーバ IP 間のキャプチャと、クライアントとそれがアクセスしようとしている Web サーバ間のキャプチャを調査します。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

関連情報

- [Cisco ASA 5500 シリーズ次世代ファイアウォール レファレンスガイド](#)
- [Cisco ASA 5500 シリーズ次世代ファイアウォール設定ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)