CHAPTER 10

DHCP、DDNS、および WCCP サービスの設定

この章では、DHCP サーバ、Dynamic DNS（DDNS; ダイナミック DNS）のアップデート方式、およびセキュリティ アプライアンスでの WCCP の設定方法について説明します。DHCP は、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。セキュリティ アプライアンスは、DHCP サーバまたは DHCP リレー サービスをセキュリティ アプライアンスのインターフェイスに接続されている DHCP クライアントに提供することができます。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。DHCP リレーでは、1 つのインターフェイスで受信した DHCP 要求を、別のインターフェイスの背後に位置する外部 DHCP サーバに渡します。

DDNS アップデートでは、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に変わるアドレスとホスト名のアソシエーションを頻繁にアップデートできるようにします。これにより、たとえばモバイル ホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。DDNS は、DNS サーバ上で、名前からアドレスへのマッピングと、アドレスから名前へのマッピングをダイナミックにアップデートして、同期化します。

WCCP では、1 つ以上のルータ、レイヤ 3 スイッチ、またはセキュリティ アプライアンスと、1 つ以上の Web キャッシュの間の相互作用を指定します。この機能は、選択したタイプのトラフィックを Web キャッシュ エンジンのグループに透過的にリダイレクトして、リソースの使用状況を最適化し、応答時間を短縮します。

この章は、次の項で構成されています。

DHCP サーバの設定

ここでは、セキュリティ アプライアンス の DHCP サーバを設定する方法について説明します。この項では、次のトピックについて取り上げます。

DHCP サーバのイネーブル化

セキュリティ アプライアンスは DHCP サーバとして動作することができます。DHCP は、ホスト IP アドレス、デフォルト ゲートウェイ、DNS サーバなどのネットワーク設定値をホストに供給するプロトコルです。

（注）　セキュリティ アプライアンス DHCP サーバは、BOOTP 要求をサポートしていません。

マルチ コンテキスト モードでは、DHCP サーバまたは DHCP リレーは、複数のコンテキストで使用されるインターフェイス上ではイネーブルにはできません。

DHCP サーバは、セキュリティ アプライアンスの各インターフェイスに設定することができます。各インターフェイスには、それ自体のアドレス プールがあり、利用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。

DHCP クライアントまたは DHCP リレー サービスを、サーバがイネーブル化されたインターフェイス上で設定することはできません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。

特定の セキュリティ アプライアンス インターフェイス上で DHCP サーバをイネーブルにする手順は、次のとおりです。

ステップ 1　DHCP アドレス プールを作成します。次のコマンドを入力して、アドレス プールを定義します。

```
hostname(config)# dhcpd address ip_address-ip_address interface_name
```

セキュリティ アプライアンスは、1 つのクライアントに対して一定時間だけ使用可能なアドレスを 1 つ、このプールから割り当てます。これらのアドレスは、直接接続されているネットワークのための、変換されていないローカル アドレスです。

アドレス プールは、セキュリティ アプライアンス インターフェイスと同じサブネット内にある必要があります。

ステップ 2　（任意）次のコマンドを入力して、クライアントに使用させる DNS サーバ（複数可）の IP アドレス（複数可）を指定します。

```
hostname(config)# dhcpd dns dns1 [dns2]
```

DNS サーバを 2 つまで指定できます。

ステップ 3　（任意）次のコマンドを入力して、クライアントに使用させる WINS サーバ（複数可）の IP アドレス（複数可）を指定します。

```
hostname(config)# dhcpd wins wins1 [wins2]
```

WINS サーバは最大 2 つまで指定できます。

ステップ 4　（任意）次のコマンドを入力して、クライアントに付与するリース期間を変更します。

```
hostname(config)# dhcpd lease lease_length
```

リース期間は、その期間が終了するまでクライアントがその割り当て IP アドレスを使用できる時間（秒）のことです。300 ～ 1,048,575 の間の値を入力します。デフォルト値は 3600 秒です。

ステップ 5　（任意）次のコマンドを入力して、クライアントが使用するドメイン名を設定します。

```
hostname(config)# dhcpd domain domain_name
```

ステップ 6　（任意）次のコマンドを入力して、DHCP の ping タイムアウト値を設定します。

```
hostname(config)# dhcpd ping_timeout milliseconds
```

アドレスの衝突を避けるために、セキュリティ アプライアンスは、1 つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。このコマンドは、これらのパケットのタイムアウト値を指定します。

ステップ 7　（トランスペアレント ファイアウォール モード）デフォルト ゲートウェイを定義します。DHCP クライアントに送信するデフォルトのゲートウェイを定義するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option 3 ip gateway_ip
```

DHCP のオプション 3 を使用せずにデフォルトのゲートウェイを定義する場合、DHCP クライアントは管理インターフェイスの IP アドレスを使用します。管理インターフェイスは、トラフィックをルーティングしません。

ステップ 8　次のコマンドを入力して、セキュリティ アプライアンス 内の DHCP デーモンがイネーブルになったインターフェイス上で DHCP クライアント要求を待ち受けるようにします。

```
hostname(config)# dhcpd enable interface_name
```

たとえば、内部インターフェイスに接続されたホストに 10.0.1.101 ～ 10.0.1.110 の範囲を割り当てる場合、次のコマンドを入力します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 209.165.201.2 209.165.202.129
hostname(config)# dhcpd wins 209.165.201.5
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

DHCP オプションの設定

セキュリティ アプライアンスは、RFC 2132 に記載されている DHCP オプションの情報を送信するように設定できます。DHCP オプションは次の 3 つのいずれかのカテゴリに属します。

- IP アドレスを返すオプション
- テキスト文字列を返すオプション
- 16 進数値を返すオプション

セキュリティ アプライアンス は、DHCP オプションの 3 つのカテゴリすべてをサポートします。DHCP オプションを設定するには、次のいずれかを実行します。

- 1 つまたは 2 つの IP アドレスを返す DHCP オプションを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option code ip addr_1 [addr_2]
  ```

- テキスト文字列を返す DHCP オプションを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option code ascii text
  ```

- 16 進数値を返す DHCP オプションを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option code hex value
  ```

（注）　セキュリティ アプライアンスは、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、**dhcpd option 46 ascii hello** コマンドを入力することは可能であり、セキュリティ アプライアンスはこのコンフィギュレーションを受け入れますが、RFC 2132 では、オプション 46 には 1 桁の 16 進数値が期待値として定義されています。オプション コードとオプション コードに対応付けられたタイプおよび予測値の詳細については、RFC 2132 を参照してください。

表 10-1 に、**dhcpd option** コマンドでサポートされていない DHCP オプションを示します。

表 10-1　サポートされていない DHCP オプション

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

特定オプション（DHCP オプション 3、66、150）を使用して Cisco IP Phone を設定します。これらのオプションの設定については、「DHCP サーバを利用する Cisco IP Phone の使用」（P.10-4）を参照してください。

DHCP サーバを利用する Cisco IP Phone の使用

Cisco IP テレフォニー VoIP ソリューションを実装する小規模な支社を持つ企業では、一般に本社で Cisco CallManager を実装し、支社の Cisco IP Phone を制御します。この実装により中央集中型のコール プロセッシングが可能となり、必要な装置を少なく抑え、支店側で Cisco CallManager およびその他のサーバを管理する必要がなくなります。

Cisco IP Phone では、コンフィギュレーションを TFTP サーバからダウンロードします。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。

Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

Cisco IP Phone は、1 つの要求にオプション 150 と 66 の両方を含めることがあります。この場合、セキュリティ アプライアンス DHCP サーバは、セキュリティ アプライアンス 上で値が設定されていれば、両方のオプションに対応する値を応答として提供します。

RFC 2132 に記載されているオプションの大部分の情報を送信するようにセキュリティ アプライアンスを設定できます。次の例は、任意のオプション番号の構文と、一般的に使用されているオプション 66、150、および 3 の構文を示しています。

- RFC-2132 に指定されているオプション番号を含む DHCP 要求の情報を提供するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option number value
  ```

- 次のコマンドを入力して、オプション 66 に対応する TFTP サーバの IP アドレスまたは名前を提供します。

  ```
  hostname(config)# dhcpd option 66 ascii server_name
  ```

- 次のコマンドを入力して、オプション 150 に対応する 1 つまたは 2 つの TFTP サーバの IP アドレスまたは名前を提供します。

  ```
  hostname(config)# dhcpd option 150 ip server_ip1 [server_ip2]
  ```

  server_ip1 には、プライマリ TFTP サーバの IP アドレスまたは名前を、*server_ip2* には、セカンダリ TFTP サーバの IP アドレスまたは名前を指定します。オプション 150 を使用すると、最大 2 つの TFTP サーバが指定できます。

- デフォルト ルートを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option 3 ip router_ip1
  ```

DHCP リレー サービスの設定

DHCP リレー エージェントを使用すると、セキュリティ アプライアンスを介して DHCP 要求をクライアントから別のインターフェイスに接続されているルータに転送することができます。

DHCP リレー エージェントを使用する場合、次の制限が適用されます。

- DHCP サーバもイネーブルになっている場合、リレー エージェントをイネーブルにできません。
- クライアントは直接セキュリティ アプライアンスに接続する必要があり、他のリレー エージェントやルータを介して要求を送信できない。
- マルチ コンテキスト モードでは、複数のコンテキストによって使用されるインターフェイス上で DHCP リレーをイネーブルにできません。

（注） DHCP リレー サービスはトランスペアレント ファイアウォール モードでは使用できません。トランスペアレント ファイアウォール モードの場合、セキュリティ アプライアンスは ARP トラフィックだけ通過を許可します。他のトラフィックはすべてアクセス リストが必要です。トランスペアレント モードで DHCP 要求と応答がセキュリティ アプライアンスを通過できるようにするには、2 つのアクセス リストを設定する必要があります。1 つは内部インターフェイスから外部への DCHP 要求を許可するもので、もう 1 つは逆方向に向かうサーバからの応答を許可するためのものです。

（注） DHCP リレーがイネーブルになっていて、複数の DHCP リレー サーバが定義されている場合、セキュリティ アプライアンスは定義された各 DHCP リレー サーバにクライアントの要求を転送する。また、クライアントの DHCP リレー バインディングが削除されるまで、サーバからの応答もクライアントに転送されます。セキュリティ アプライアンスが ACK、NACK、または拒否のいずれかの DHCP メッセージを受け取ると、バインディングは削除されます。

DHCP リレーをイネーブルにするには、次の手順を実行します。

ステップ 1　DHCP クライアントとは異なるインターフェイス上の DHCP サーバの IP アドレスを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcprelay server ip_address if_name
```

このコマンドを使用して 4 つまでのサーバを 4 回まで設定できます。

ステップ 2　次のコマンドを入力して、クライアントに接続されたインターフェイス上で DHCP リレーをイネーブルにします。

```
hostname(config)# dhcprelay enable interface
```

ステップ 3　（任意）次のコマンドを入力して、リレー アドレス ネゴシエーションが可能な秒数を設定します。

```
hostname(config)# dhcprelay timeout seconds
```

ステップ 4　（任意）次のコマンドを入力して、DHCP サーバから セキュリティ アプライアンス インターフェイスのアドレスに送信されるパケットに組み込む、最初のデフォルト ルータ アドレスを変更します。

```
hostname(config)# dhcprelay setroute interface_name
```

このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、セキュリティ アプライアンスをポイントすることができます。

パケット内にデフォルトのルータ オプションがなければ、セキュリティ アプライアンスは、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。

次の例では、セキュリティ アプライアンスは、内部インターフェイスに接続されているクライアントからの DHCP 要求を、外部インターフェイス上の DHCP サーバに転送することができるようになります。

```
hostname(config)# dhcprelay server 201.168.200.4
hostname(config)# dhcprelay enable inside
hostname(config)# dhcprelay setroute inside
```

ダイナミック DNS（DDNS）の設定

この項では、ダイナミック DNS をセキュリティ アプライアンスサポートするためのの設定例について説明します。DDNS アップデートでは、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。つまり、DHCP は、IP アドレス割り当てを集中化および自動化し、ダイナミック DNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを自動的に記録します。DHCP とダイナミック DNS アップデートを使用する場合、ホストが IP ネットワークに接続するときに、必ずそのホストのネットワーク アクセスを自動的に設定します。永続的で固有の DNS ホスト名を使用してホストを検索し、そこに到達できます。たとえば、モバイル ホストは、ユーザや管理者の介入なしで、自由に移動できるようになります。

DDNS は、アドレスとドメイン名のマッピングを提供して、各ホストの DHCP 割り当てによる IP アドレスが頻繁に変化しても、ホスト同士が互いに検索できるようにします。DDNS の名前とアドレスのマッピングは、2 つのリソース レコードの DHCP サーバ上で行われます。A RR は名前から IP アドレスへのマッピングを保持し、PTR RR はアドレスから名前へのマッピングを行います。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

2 つの最も共通の DDNS アップデート コンフィギュレーションは次のとおりです。

- DHCP クライアントは A RR をアップデートし、DHCP サーバは PTR RR をアップデートします。
- DHCP サーバは、A RR と PTR RR の両方をアップデートします。

通常、DHCP サーバはクライアントの代わりに DNS PTR RR を保持します。クライアントは、必要なすべての DNS アップデートを実行するように設定できます。サーバは、これらのアップデートを実行するかどうかを設定できます。PTR RR をアップデートするには、DHCP サーバがクライアントの FQDN を認識している必要があります。クライアントは Client FQDN と呼ばれる DHCP オプションを使用して、サーバに FQDN を提供します。

次に、一般的な事例を示します。

- 「例 1：クライアントが A RR と PTR RR の両方をスタティック IP アドレス用にアップデートする」（P.10-7）
- 「例 2：クライアントが A RR と PTR RR の両方をアップデートし、DHCP サーバがクライアント アップデート要求を実行し、コンフィギュレーションを介して FQDN が取得される」（P.10-8）
- 「例 3：クライアントに含まれる FQDN オプションがいずれの RR もアップデートしないようにサーバに要求し、サーバはクライアントを上書きして RR を両方ともアップデートする」（P.10-8）
- 「例 4：クライアントはサーバに両方のアップデートの実行を要求し、サーバは PTR RR だけをアップデートするように設定されている。クライアントの要求が実行され、A RR と PTR RR の両方がアップデートされる」（P.10-9）
- 「例 5：クライアントは A RR をアップデートし、サーバは PTR RR をアップデートする」（P.10-9）

例 1：クライアントが A RR と PTR RR の両方をスタティック IP アドレス用にアップデートする

次の例では、クライアントを設定して A リソース レコードと PTR リソース レコードの両方をスタティック IP アドレス用にアップデートすることを要求するように設定します。この例を設定するには、次の手順を実行します。

ステップ 1　クライアントに A RR と PTR RR の両方をアップデートするように要求する DDNS アップデート方式（ddns-2 と呼ばれる）を定義するには、次のコマンドを入力します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

ステップ 2　方式 ddns-2 を eth1 インターフェイスに関連付けるには、次のコマンドを入力します。

```
hostname(DDNS-update-method)# interface eth1
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname asa.example.com
```

ステップ 3　eth1 のスタティック IP アドレスを設定するには、次のコマンドを入力します。

```
hostname(config-if)# ip address 10.0.0.40 255.255.255.0
```

例 2：クライアントが A RR と PTR RR の両方をアップデートし、DHCP サーバがクライアント アップデート要求を実行し、コンフィギュレーションを介して FQDN が取得される

次の例では、（1）DHCP クライアントに A RR と PTR RR の両方をアップデートすることを要求し、（2）DHCP サーバがその要求を実行するように設定します。この例を設定するには、次の手順を実行します。

ステップ 1　DHCP サーバがアップデートを行わないように DHCP クライアントを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcp-client update dns server none
```

ステップ 2　DHCP クライアントで、クライアントに A と PTR の両方のアップデートを実行するように指示する ddns-2 という名前の DDNS アップデート方式を作成するには、次のコマンドを入力します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

ステップ 3　ddns-2 という名前の方式を Ethernet0 という名前のセキュリティ アプライアンス インターフェイスに関連付け、インターフェイス上で DHCP をイネーブルにするには、次のコマンドを入力します。

```
hostname(DDNS-update-method)# interface Ethernet0
hostname(if-config)# ddns update ddns-2
hostname(if-config)# ddns update hostname asa.example.com
hostname(if-config)# ip address dhcp
```

ステップ 4　DHCP サーバを設定するには、次のコマンドを入力します。

```
hostname(if-config)# dhcpd update dns
```

例 3：クライアントに含まれる FQDN オプションがいずれの RR もアップデートしないようにサーバに要求し、サーバはクライアントを上書きして RR を両方ともアップデートする

次の例では、A と PTR のいずれもアップデートしないように DHCP サーバに指示する FQDN オプションを含めるように、DHCP クライアントを設定します。また、クライアントの要求を上書きするようにサーバを設定します。その結果、クライアントはアップデートを行わずにバックオフします。

この事例を設定するには、次の手順を実行します。

ステップ 1　ddns-2 という名前のアップデート方式を、A RR と PTR RR の両方のアップデートを要求するように設定するには、次のコマンドを入力します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

ステップ 2　インターフェイス Ethernet0 で ddns-2 という名前の DDNS アップデート方式を割り当て、クライアント ホスト名（asa）を付与するには、次のコマンドを入力します。

```
hostname(DDNS-update-method)# interface Ethernet0
hostname(if-config)# ddns update ddns-2
hostname(if-config)# ddns update hostname asa.example.com
```

ステップ 3　インターフェイスで DHCP クライアント機能をイネーブルにするには、次のコマンドを入力します。

```
hostname(if-config)# dhcp client update dns server none
hostname(if-config)# ip address dhcp
```

ステップ 4　クライアントのアップデート要求を上書きするように DHCP サーバを設定するには、次のコマンドを入力します。

```
hostname(if-config)# dhcpd update dns both override
```

例 4：クライアントはサーバに両方のアップデートの実行を要求し、サーバは PTR RR だけをアップデートするように設定されている。クライアントの要求が実行され、A RR と PTR RR の両方がアップデートされる

次の例では、デフォルトで PTR RR アップデートだけを実行するようにサーバを設定します。ただしサーバは、A と PTR の両方をアップデートするクライアントの要求を実行します。また、サーバは、クライアントが提供するホスト名（asa）にドメイン名（example.com）を追加することで FQDN を形成します。

この事例を設定するには、次の手順を実行します。

ステップ 1　インターフェイス Ethernet0 で DHCP クライアントを設定するには、次のコマンドを入力します。

```
hostname(config)# interface Ethernet0
hostname(config-if)# dhcp client update dns both
hostname(config-if)# ddns update hostname asa
```

ステップ 2　DHCP サーバを設定するには、次のコマンドを入力します。

```
hostname(config-if)# dhcpd update dns
hostname(config-if)# dhcpd domain example.com
```

例 5：クライアントは A RR をアップデートし、サーバは PTR RR をアップデートする

次の例では、クライアントが A リソース レコードをアップデートし、サーバが PTR レコードをアップデートするように設定します。また、クライアントは DHCP サーバからのドメイン名を使用して、FQDN を形成します。

この事例を設定するには、次の手順を実行します。

ステップ 1　ddns-2 という名前の DDNS アップデート方式を定義するには、次のコマンドを入力します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns
```

ステップ 2　インターフェイス Ethernet0 の DHCP クライアントを設定し、アップデート方式をインターフェイスに割り当てるには、次のコマンドを入力します。

```
hostname(DDNS-update-method)# interface Ethernet0
hostname(config-if)# dhcp client update dns
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname asa
```

ステップ 3　DHCP サーバを設定するには、次のコマンドを入力します。

```
hostname(config-if)# dhcpd update dns
hostname(config-if)# dhcpd domain example.com
```

WCCP を使用する Web キャッシュ サービスの設定

Web キャッシングの目的は、遅延とネットワーク トラフィックを減らすことです。以前アクセスした Web ページがキャッシュ バッファに保存されているため、ページが再度必要になったときに、ユーザは Web サーバではなくキャッシュから取得できます。

WCCP は、セキュリティ アプライアンスと外部 Web キャッシュの間の相互作用を指定します。この機能は、選択したタイプのトラフィックを Web キャッシュ エンジンのグループに透過的にリダイレクトして、リソースの使用状況を最適化し、応答時間を短縮します。セキュリティ アプライアンスは、WCCP バージョン 2 だけをサポートしています。

セキュリティ アプライアンスを仲介役として使用すると、WCCP リダイレクトを行うために個別のルータが不要になります。これは、セキュリティ アプライアンスがキャッシュ エンジンへのリダイレクト要求を処理できるためです。セキュリティ アプライアンスは、パケットにリダイレクトが必要な時期を認識すると、TCP ステート トラッキング、TCP シーケンス番号のランダム化、およびトラフィック フローでの NAT をスキップします。

この項では、次のトピックについて取り上げます。

- 「WCCP 機能のサポート」（P.10-10）
- 「WCCP とその他の機能との相互作用」（P.10-10）
- 「WCCP リダイレクションのイネーブル化」（P.10-11）

WCCP 機能のサポート

セキュリティ アプライアンスでは、次の WCCPv2 機能がサポートされています。

- TCP/UDP ポート宛ての複数のトラフィックのリダイレクション
- サービス グループ内のキャッシュ エンジンのための認証

次の WCCPv2 機能は、セキュリティ アプライアンスでサポートされていません。

- サービス グループ内の複数のルータはサポートされていません。それでも、サービス グループ内の複数のキャッシュ エンジンはサポートされています。
- マルチキャスト WCCP はサポートされていません。
- レイヤ 2 リダイレクト方式はサポートされていません。GRE カプセル化だけがサポートされています。
- WCCP 送信元アドレス スプーフィング

WCCP とその他の機能との相互作用

セキュリティ アプライアンスの WCCP の実装では、プロトコルと他の設定可能な機能との相互作用に次の点が適用されます。

- 入力アクセス リスト エントリの優先度は常に WCCP よりも上です。たとえば、アクセス リストでサーバとの通信をクライアントに許可していない場合、トラフィックはキャッシュ エンジンにリダイレクトされません。入力インターフェイス アクセス リストと出力インターフェイス アクセス リストの両方が適用されます。
- TCP 代行受信、許可、URL フィルタリング、インスペクション エンジン、および IPS 機能は、トラフィックのリダイレクト フローに適用されません。
- キャッシュ エンジンが要求に対してサービスを行わずパケットが戻された場合、またはキャッシュ エンジンでキャッシュ ミスが生じて Web サーバからデータを要求した場合、トラフィック フローの内容がセキュリティ アプライアンスのその他すべての設定機能に反映されます。
- フェールオーバーでは、WCCP リダイレクト テーブルはスタンバイ装置に複製されません。フェールオーバー後、テーブルが再構築されるまでパケットはリダイレクトされません。フェールオーバー前にリダイレクトされたセッションは、多くの場合、Web サーバからリセットされます。
- 2 つの WCCP サービスを使用していて、それらが同じパケット（deny または permit アクション）が一致する、重複する 2 つのリダイレクション ACL を別個に使用している場合、最初に見つかったサービス グループとインストールされているルールに基づいて動作します。パケットは、一部のサービス グループには渡されません。

WCCP リダイレクションのイネーブル化

セキュリティ アプライアンスで WCCP リダイレクションを設定するには、2 つの手順があります。まず **wccp** コマンドでリダイレクトするサービスを特定し、次に **wccp redirect** コマンドでリダイレクションを行うインターフェイスを定義します。また、**wccp** コマンドはオプションで、サービス グループに参加するキャッシュ エンジンや、そのキャッシュ エンジンにリダイレクトされる必要のあるトラフィックを定義することもできます。

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。セキュリティ アプライアンスでサポートされている唯一のトポロジは、クライアントとキャッシュ エンジンがセキュリティ アプライアンスの同じインターフェイスの背後にあり、キャッシュ エンジンがセキュリティ アプライアンスを介さずに直接クライアントと通信を行う場合です。

次のコンフィギュレーション タスクは、ネットワークに含めるキャッシュ エンジンがすでにインストールおよび設定されていることを前提としています。

WCCP リダイレクションを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、WCCP サービス グループをイネーブルにします。

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

標準サービスは **web-cache** で、TCP ポート 80（HTTP）トラフィックを代行受信してキャッシュ エンジンにリダイレクトします。ただし、必要に応じて、0 ～ 254 のサービス番号を特定できます。たとえば、ネイティブの FTP トラフィックをキャッシュ エンジンに透過的にリダイレクトするには、WCCP サービス 60 を使用します。このコマンドは、イネーブルにするサービス グループごとに何度も入力できます。

redirect-list *access_list* 引数は、このサービス グループにリダイレクトするトラフィックを制御します。*access-list* 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。

group-list *access_list* 引数は、サービス グループに参加が許可される Web キャッシュ IP アドレスを判別します。*access-list* 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。

password *password* 引数は、サービス グループから受け取るメッセージの MD5 認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。

ステップ 2　インターフェイスで WCCP リダイレクションをイネーブルにするには、次のコマンドを入力します。

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

標準サービスは **web-cache** で、TCP ポート 80（HTTP）トラフィックを代行受信してキャッシュ エンジンにリダイレクトします。ただし、必要に応じて、0 ～ 254 のサービス番号を特定できます。たとえば、ネイティブの FTP トラフィックをキャッシュ エンジンに透過的にリダイレクトするには、WCCP サービス 60 を使用します。このコマンドは、参加するサービス グループごとに何度も入力できます。

たとえば、標準 **web-cache** サービスをイネーブルにして、内部インターフェイスに入る HTTP トラフィックを Web キャッシュにリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# wccp web-cache
hostname(config)# wccp interface inside web-cache redirect in
```

たとえば、WCCP がサービス グループに参加できるようにするには、次のコマンドを入力します。

```
hostname(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```