Threat Defense 用の DHCP および DDNS サービス

次のトピックでは、DHCP サービスと DDNS サービスについて、および Threat Defense デバイスでこれらを設定する方法について説明します。

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

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。Firepower Threat Defense デバイスはFirepower Threat Defense デバイスインターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。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。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

IPv6 の DHCP サーバはサポートされていません。ただし、IPv6 トラフィックの DHCP リレーを有効にできます。

DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたアイテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。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。
- DHCP オプション 3 はデフォルト ルートを設定します。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションにより、DNS、WINS、ドメインネームパラメータを DHCP クライアントに提供できます。DNS ドメインサフィックスは DHCP オプション 15 を使用します。これらの値は DHCP 自動設定により、または手動で設定できます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動コンフィギュレーションの設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動コンフィギュレーションをイネーブルにできます。DHCP 自動構成によって、DNS サーバおよび WINS サーバとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバ名および WINS サーバ名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、Firepower Threat Defense デバイスはブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェ

ントを使用して、ブロードキャストを受信している Firepower Threat Defense デバイス のインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定できます。

DDNS の概要

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。

DDNS の名前とアドレスのマッピングは、DHCP サーバ上で 2 つのリソース レコード（RR）で行われます。A RR では、名前から IP アドレスへのマッピングが保持され、PTR RR では、アドレスから名前へのマッピングが行われます。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 標準規格、および一般的な HTTP 方式）のうち、Firepower Threat Defense デバイス では、IETF 方式をサポートしています。

（注） DDNS は BVI またはブリッジ グループのメンバー インターフェイスではサポートされません。

DDNS アップデート コンフィギュレーション

2 つの最も一般的な 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。DHCP サーバは、PTR RR をアップデートするクライアントの完全修飾ドメイン名（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。

UDP パケット サイズ

DDNS は、DNS 要求者が UDP パケットのサイズをアドバタイズできるようにし、512 オクテットより大きいパケットの転送を容易にします。DNS サーバは UDP 上で要求を受信すると、OPT RR から UDP パケット サイズを識別し、要求者により指定された最大 UDP パケット サイズにできるだけ多くのリソース レコードを含めることができるよう、応答のサイズを調整します。

DNS パケットのサイズは、BIND の場合は最大 4096 バイト、Windows 2003 DNS サーバの場合は 1280 バイトです。

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCP および DDNS サービスを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジグループ メンバー インターフェイスではサポートされません。
- DHCP サーバは、ブリッジグループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。 ルーテッド モードでは、DHCP サーバは BVI インターフェイスでサポートされますが、ブリッジ グループ メンバー インターフェイスではサポートされません。DHCP サーバを動作させるために、BVI には名前が必要です。
- DDNS は、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジグループ メンバー インターフェイスではサポートされません。

IPv6

DHCP サーバでサポートされます。 DHCP リレーの IPv6 はサポートされます。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。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 クライアントや DHCP リレー サービスは、サーバがイネーブルになっているインターフェイス上では設定できません。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。
- Firepower Threat Defense デバイス は、QIP DHCP サーバと DHCP プロキシ サービスとの併用をサポートしません。
- 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することはできません。
- DHCP サーバは、BOOTP 要求をサポートしません。

DHCP リレー

- グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。
- 10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバはサポートされません。
- 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。
- 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。ただし、アクセス ルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答がFirepower Threat Defenseデバイスを通過できるようにするには、2 つのアクセス ルール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（UDP 宛先ポート 67）への DCHP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 Firepower Threat Defense デバイス 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ません。IPv6 の場合、Firepower Threat Defense デバイス は別のリレー サーバからのパケットをサポートします。
- DHCP クライアントは、Firepower Threat Defense デバイス が要求をリレーする DHCP サーバとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DHCP サーバの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [DHCP] > [DHCP サーバ（DHCP Server）] を選択します。

ステップ 3 次の DHCP サーバのオプションを設定します。

- [Ping タイムアウト（Ping Timeout）]：Firepower Threat Defense デバイスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。

  アドレスの衝突を避けるために、Firepower Threat Defense デバイスは、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。

- [リース長（Lease Length）]：リースの期間が終了する前に、割り当てIPアドレスをクライアントが使用できる秒単位の時間。有効値の範囲は 300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。
- （ルーテッド モード）[自動設定（Auto-configuration）]：Firepower Threat Defense デバイスで DHCP 自動設定を有効にします。自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動設定にしない場合は、自動設定を無効にして、手順 4 で値を追加することもできます。
- （ルーテッドモード）[インターフェイス（Interface）]：自動設定に使用されるインターフェイスを指定します。

ステップ 4 自動設定をオーバーライドするには、以下を実行します。

- インターフェイスのドメイン名を入力します。たとえば、デバイスは Your_Company ドメインにあるかもしれません。
- ドロップダウン リストから、インターフェイスに設定された DNS サーバ（プライマリおよびセカンダリ）を選択します。DNS サーバを新たに追加する手順については、ネットワーク オブジェクトの作成を参照してください。
- ドロップダウン リストから、インターフェイスに設定された WINS サーバ（プライマリおよびセカンダリ）を選択します。WINS サーバを新たに追加する手順については、ネットワーク オブジェクトの作成を参照してください。

ステップ 5 [サーバ（Server）] タブを選択して [追加（Add）] をクリックし、次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストからインターフェイスを選択します。トランスペアレント モードでは、名前付きブリッジ グループ メンバー インターフェイスを指定します。ルーテッド モードでは、名前付きルーテッド インターフェイスまたは名前付き BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。DHCP サーバが動作するためには、BVI の各ブリッジ グループ メンバー インターフェイスにも名前を付ける必要があることに注意してください。
- [アドレス プール（Address Pool）]：DHCP サーバが使用する IP アドレスの最下位から最上位の間の範囲です。IPアドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCP サーバを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバを有効にします。

ステップ 6 [OK] をクリックして、DHCP サーバの設定を保存します。

ステップ 7 （オプション）[詳細（Advanced）] タブを選択して、[追加（Add）] をクリックし、DHCP クライアントに戻すオプションの情報のタイプを指定します。

- [オプション コード（Option Code）]：Firepower Threat Defense デバイスは、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（1 ～ 255）がサポート

されています。DHCP オプション コードの詳細については、DHCPv4 サーバについて （1 ページ）を参照してください。

（注） Firepower Threat Defense デバイスは、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。オプション コードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

- [タイプ（Type）]：DHCP のオプションのタイプ。使用できるオプションには、IP、ASCII、および HEX が含まれます。IP を選択する場合、[IP アドレス（IP Address）] フィールドに IP アドレスを追加する必要があります。ASCII を選択する場合、[ASCII] フィールドに [ASCII] 値を追加する必要があります。HEX を選択する場合、[HEX] フィールドに [HEX] 値を追加する必要があります。
- [IP アドレス 1（IP Address 1）] および [IP アドレス 2（IP Address 2）]：このオプションコードで戻る IP アドレス。IP アドレスを新たに追加する手順については、ネットワーク オブジェクトの作成を参照してください。
- [ASCII]：DHCP クライアントに戻る ASCII 値。文字列にスペースを含めることはできません。
- [HEX]：DHCP クライアントに戻る HEX 値。文字列はスペースなしの偶数でなければなりません。0x プレフィックスを使用する必要はありません。

ステップ 8 [OK] をクリックして、オプション コードの設定を保存します。

ステップ 9 DHCP ページで [保存（Save）] をクリックして変更を保存します。

DHCP リレー エージェントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、Firepower Threat Defense デバイスはブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。

ブロードキャストを受信している Firepower Threat Defense デバイスのインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定すると、この状況を改善できます。

（注） DHCP リレーは、トランスペアレント ファイアウォール モードまたは では、サポートされません。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [DHCP] > [DHCP リレー（DHCP Relay）] を選択します。

ステップ 3 [タイムアウト（Timeout）] フィールドでは、Firepower Threat Defense デバイスが DHCP リレー エージェントのタイムアウトを待つ時間を秒単位で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

タイムアウトは、ローカル DHCP リレー エージェントを介すアドレス ネゴシエーション用です。

ステップ 4 [DHCP リレー エージェント（DHCP Relay Agent）] タブで、[追加（Add）] をクリックして、以下のオプションを設定します。

- [インターフェイス（Interface）]：DHCP クライアントに接続されているインターフェイス。
- [DHCP リレーを有効にする（Enable DHCP Relay）]：このインターフェイスで IPv4 DHCP リレーを有効にします。
- [ルート設定（Set Route）]：（IPv4 用）サーバからの DHCP メッセージのデフォルト ゲートウェイ アドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い Firepower Threat Defense デバイスのインターフェイスのアドレスに変更します。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、Firepower Threat Defense デバイ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、Firepower Threat Defense デバイスは、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。
- [IPv6 リレーを有効にする（Enable IPv6 Relay）]：このインターフェイスで IPv6 DHCP リレーを有効にします。

ステップ 5 [OK] をクリックして、DHCP リレー エージェントの変更を保存します。

ステップ 6 [DHCP サーバ（DHCP Servers）] タブで、[追加（Add）] をクリックして、以下のオプションを設定します。

IPv4 サーバ アドレスおよび IPv6 サーバ アドレスが同じサーバに属していても、個別のエントリとして追加します。

- [サーバ（Server）]：DHCP サーバの IP アドレス。ドロップダウン リストから IP アドレスを選択します。新たに加えるには、次を参照してください。 ネットワーク オブジェクトの作成
- [インターフェイス（Interface）]：指定の DHCP サーバが接続されるインターフェイス。DHCP リレー エージェントと DHCP サーバを、同じインターフェイスに設定することはできません。

ステップ 7 [OK] をクリックして、DHCP サーバの変更を保存します。

ステップ 8 DHCP ページで [保存（Save）] をクリックして変更を保存します。

DDNS の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ダイナミック DNS（DDNS）アップデートにより、DNS を DHCP に組み込みます。DDNS 更新プログラムは割り当て済み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、頻繁に変更されるアドレスとホスト名間のアソシエーションを効果的に更新できるようにします。

始める前に

- 概要については、DDNS の概要 （3 ページ）を参照してください。
- DDNS は、トランスペアレント ファイアウォール モードでサポートされていません。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[DHCP]** > **[DDNS]**を選択して、次の DDNS オプションを設定します。

- [DHCP クライアントが記録更新を DHCP サーバに要求（DHCP Client Requests DHCP Server to update Records）]：DHCP サーバによる指定の記録の更新を DHCP クライアントが要求するよう設定します。使用可能なオプションは、[選択なし（Not Selected）]、[更新なし（No Update）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。A および PTR 記録の説明については、DDNS の概要 （3 ページ）を参照してください。
- [DHCP クライアント ブロードキャストを有効にする（Enable DHCP Client Broadcast）]：DHCP クライアントが DHCP サーバに到達するためにブロードキャスト アドレスを使用することを有効にします。
- [ダイナミック DNS 更新（Dynamic DNS Update）]：DHCP サーバの DDNS 更新に使用する記録を選択します。使用可能なオプションは、[選択なし（Not Selected）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。
- [DHCP クライアント要求のオーバーライド（Override DHCP Client Requests）]：DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションをオーバーライドするよう指定します。

ステップ 3 [DHCP クライアント ID インターフェイス（DHCP Client ID Interface）] タブで、[使用可能なインターフェイス（Available Interfaces）] リストからインターフェイスを選択し、[追加（Add）] をクリックして、インターフェイスを [選択されたインターフェイス（Selected Interfaces）] リストに移動します。

ステップ 4 [DDNS インターフェイス設定（DDNS Interface Settings）] タブで、[追加（Add）] をクリックし、以下のオプションを設定します。

- [インターフェイス（Interface）]：設定済みのそれぞれのインターフェイスに DDNS 設定を追加するには、ドロップダウン リストからインターフェイスを選択します。
- [方法名（Method Name）]：インターフェイスに割り当てられた DDNS 更新方法。
- [ホスト名（Host Name）]：DDNS クライアントのホスト名。
- [DHCP クライアントが更新要求を DHCP サーバに要求（DHCP Client requests DHCP server to update requests）]：DHCP サーバによる指定の記録の更新を DHCP クライアントが要求するよう設定します。使用可能なオプションは、[選択なし（Not Selected）]、[更新なし（No Update）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。A および PTR 記録の説明については、DDNS の概要 （3 ページ）を参照してください。
- [ダイナミック DNS 更新（Dynamic DNS Update）]：DHCP サーバの DDNS 更新に使用する記録を選択します。使用可能なオプションは、[選択なし（Not Selected）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。
- [DHCP クライアント要求のオーバーライド（Override DHCP Client Requests）]：DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションをオーバーライドするよう指定します。

ステップ 5 [OK] をクリックして、DDNS のインターフェイスの変更を保存します。

ステップ 6 [DDNS 更新方法（DDNS Update Methods）] タブで、[追加（Add）] をクリックし、以下のオプションを設定します。

- [方法名（Method Name）]：インターフェイスに割り当てられた DDNS 更新方法。
- [更新間隔（Update Interval）]：日（0 ～ 364）、時（0 ～ 23）、分（0 ～ 59）、秒（0 ～ 59）で設定される DNS の更新試行の整数の更新間隔。これらの単位は、追加式です。つまり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、このアップデート方式がアクティブである限り、5 分 15 秒ごとに更新が試行されます。
- [更新記録（Update Records）]：DNS クライアントによるサーバ リソース記録の更新を保存します。使用可能なオプションは、[定義なし（Not Defined]、[A と PTR 記録（Both A and PTR Records）]、[A 記録（A Records）] です。

ステップ 7 [OK] をクリックして、DDNS の更新方法の変更を保存します。

ステップ 8 DHCP ページで [保存（Save）] をクリックして変更を保存します。