



DHCP および DDNS

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 \(1 ページ\)](#)
- [DHCP および DDNS の要件と前提条件 \(3 ページ\)](#)
- [DHCP サービスと DDNS サービスのガイドライン \(3 ページ\)](#)
- [DHCPv4 サーバーの設定 \(5 ページ\)](#)
- [DHCPv6 ステートレス サーバーの設定 \(7 ページ\)](#)
- [DHCP リレー エージェントの設定 \(12 ページ\)](#)
- [ダイナミック DNS の設定 \(14 ページ\)](#)
- [DHCP および DDNS の履歴 \(21 ページ\)](#)

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構成パラメータを DHCP クライアントに提供します。Threat Defense デバイスは、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、ネットワーク構成パラメータを 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 では、デフォルト ルートが設定されます。

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 オプションを使用すれば、DHCP クライアントに DNS、WINS、およびドメイン名の各パラメータを提供できます。DHCP オプション 15 は DNS ドメインのサフィックスに使用されます。DHCP 自動コンフィギュレーションの設定を使用して、これらの値を取得したり、これらを手動で定義したりできます。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 自動構成設定

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 自動構成を有効にできます。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。

DHCPv6 ステートレス サーバについて

ステートレスアドレス自動設定 (SLAAC) をプレフィックス委任機能と併せて使用するクライアント ([IPv6 プレフィックス委任クライアントの有効化](#)) については、DHCP IPv6 プールを定義して DHCPv6 サーバに割り当てることにより、これらのクライアントが情報要求 (IR) パケットを Threat Defense に送信する際に (DNS サーバ、ドメイン名などの) 情報を提供するように Threat Defense を設定できます。Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。クライアントが独自の IPv6 アドレスを生成するよう

に設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（Threat Defense がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

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、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 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。

DHCP および DDNS の要件と前提条件

モデルのサポート

Threat Defense

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

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が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 サーバーは、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 サーバーは 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 サーバー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 サーバー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 サーバー、ドメイン名、オプション、ping のタイムアウト、WINS サーバーなど他の 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 サーバーによって使用されます。
- インターフェイスで DHCP サーバーも有効になっている場合、そのインターフェイスを DHCP クライアントとして設定することはできません。スタティック IP アドレスを使用する必要があります。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- 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 サーバーは、BOOTP 要求をサポートしていません。

DHCP リレー

- 仮想ルータ、グローバルおよびインターフェイス固有のサーバーを合わせて 10 台までの DHCPv4 リレーサーバーを設定できます。インターフェイスごとには、4 台まで設定できます。
- 仮想ルータごとに 10 台までの DHCPv6 リレーサーバーを設定できます。IPv6 のインターフェイス固有のサーバーはサポートされません。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- 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 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

DHCP 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）に向かうサーバー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 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、Threat Defense デバイス は別のリレー サーバーからのパケットをサポートします。
- DHCP クライアントは、Threat Defense デバイス が要求をリレーする DHCP サーバー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 リレーは、仮想トンネルインターフェイス（VTI）ではサポートされていません。

DHCPv4 サーバーの設定

DHCPv4 サーバーを設定するには、次の手順を参照してください。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- ステップ 2** [DHCP] > [DHCP サーバー (DHCP Server)] を選択します。
- ステップ 3** 次の DHCP サーバーのオプションを設定します。
 - [Ping タイムアウト (Ping Timeout)] : 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、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。有効な値の範囲は、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)] : 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。仮想ルーティング機能を備えたデバイスの場合、このインターフェイスはグローバル仮想ルータインターフェイスにしかありません。

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 [サーバー (Server)] 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)] 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)] : 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) 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。

ステップ 10 DHCP バインディングを表示するには、次のコマンドを使用します。

show dhcpd binding

例 :

```
> show dhcpd binding
IP Address Client-id          Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds    automatic
```

DHCPv6 ステートレス サーバーの設定

ステートレスアドレス自動設定 (SLAAC) をプレフィックス委任機能と併せて使用するクライアントについては、これらのクライアントが情報要求 (IR) パケットを Threat Defense に送信する際に情報 (DNS サーバー、ドメイン名など) を提供するように Threat Defense を設定できます。

DHCP IPv6 プールの作成

DHCPv6 サーバーで使用する DHCP IPv6 プールを作成します。クライアントが Threat Defense に情報要求 (IR) パケットを送信すると、DHCPv6 サーバーは、DNS サーバー名やドメイン名などの情報を提供します。DHCP IPv6 プールは、IR メッセージで送信するパラメータを定義します。

この機能は、ルーテッドモードでのみサポートされます。この機能は、クラスタリングまたはハイアベイラビリティではサポートされません。

手順

ステップ1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

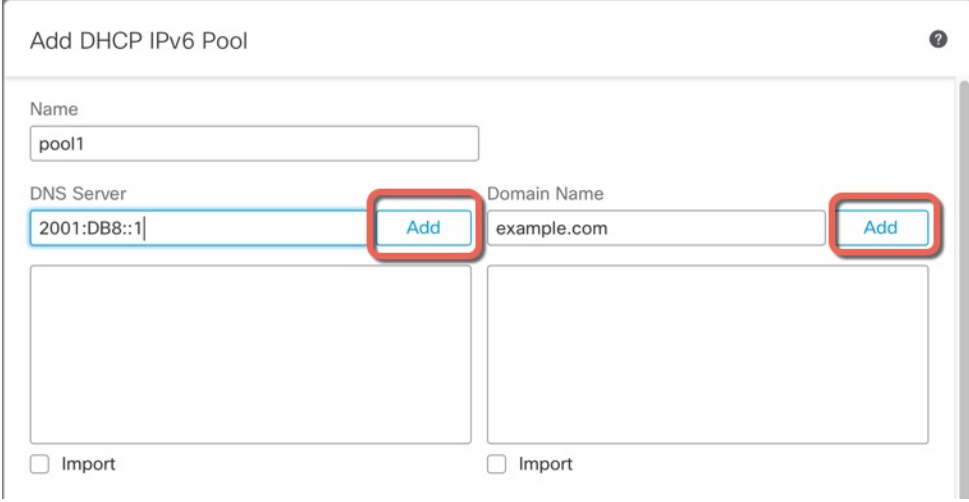
ステップ2 オブジェクトタイプのリストから [DHCP IPv6プール (DHCP IPv6 Pool)] を選択します。

ステップ3 Add () をクリックします。

ステップ4 DNS サーバーとドメイン名を設定します。

手動で値を定義して [追加 (Add)] をクリックするか、[インポート (Import)] をクリックして、プレフィックス委任クライアントインターフェイスで Threat Defense が DHCPv6 サーバーから取得した1つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせる使用できますが、同じパラメータを手動で設定し、かつ [インポート (Import)] を使用することはできません。

図 1: 手動での値の定義



Add DHCP IPv6 Pool

Name
pool1

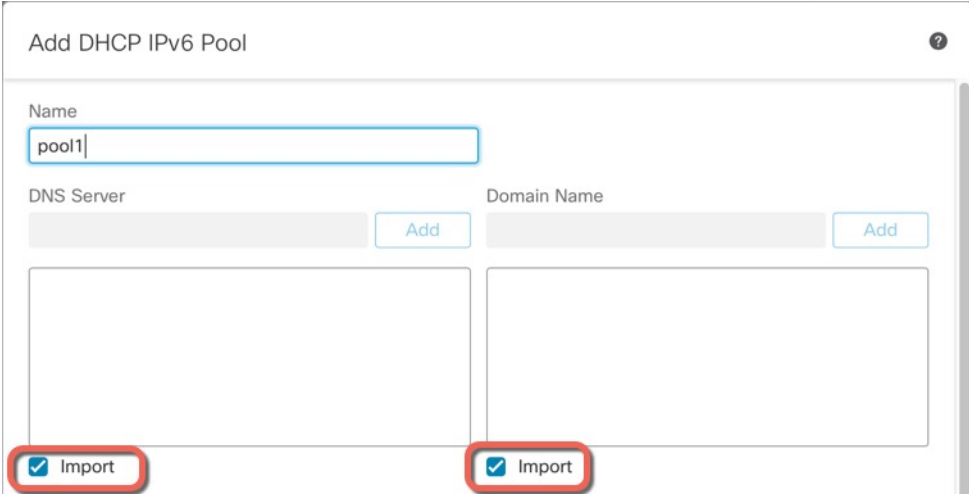
DNS Server
2001:DB8::1

Domain Name
example.com

Import

Import

図 2: 値のインポート



Add DHCP IPv6 Pool

Name
pool1

DNS Server

Domain Name

Import

Import

ステップ 5 その他のサーバーオプションを定義します。

次のサーバーのドメイン名と IP アドレスを定義できます。

- NIS
- NISP
- SIP
- SNTTP


- a) **Add** () をクリックします。

図 3: その他のサーバーオプション

Other Server Options



- b) [オプション (Option)] でサーバータイプを選択し、ドメイン名とアドレスを手動で定義するか、[インポート (Import)] をオンにします。

図 4: サーバーのドメイン名とアドレスの定義

[インポート (Import)] を指定すると、プレフィックス委任クライアントインターフェイスで Threat Defense が DHCPv6 サーバーから取得した 1 つ以上のパラメータが使用されます。手動で設定されたパラメータとインポートされたパラメータを組み合わせで使用できますが、同じパラメータを手動で設定し、かつ [インポート (Import)] を使用することはできません。

- c) [保存 (Save)] をクリックします。
- d) 各サーバータイプでこの手順を繰り返します。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 このプールは DHCPv6 サーバーで使用します。DHCPv6 ステートレスサーバーの有効化 (10 ページ) を参照してください。

DHCPv6 ステートレスサーバーの有効化

ステートレスアドレス自動設定 (SLAAC) をプレフィックス委任機能と併せて使用するクライアント (IPv6 プレフィックス委任クライアントの有効化) については、これらのクライア

トが情報要求 (IR) パケットを Threat Defense に送信する際に情報 (DNS サーバー、ドメイン名など) を提供するように Threat Defense を設定できます。Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス (Threat Defense がプレフィックス委任を使用して受信したプレフィックス) に基づいて IPv6 アドレスが設定されます。

この機能は、ルーテッドモードでのみサポートされます。この機能は、クラスタリングまたはハイアベイラビリティではサポートされません。

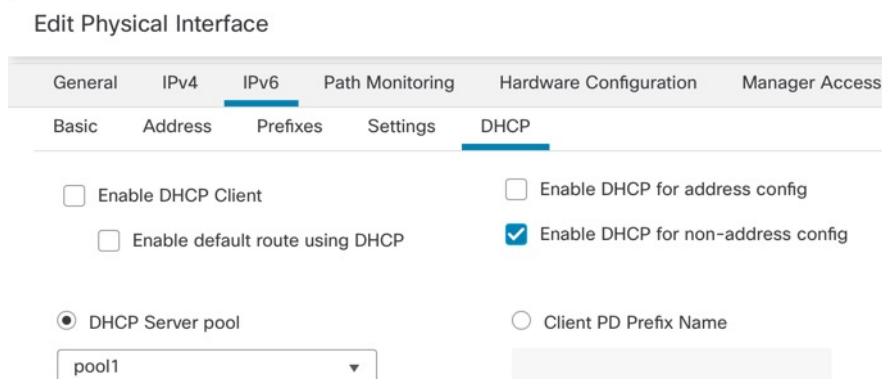
始める前に

DHCP IPv6 プールオブジェクトを追加します。[DHCP IPv6 プールの作成 \(7 ページ\)](#) を参照してください。このオブジェクトは、IR メッセージに含まれるサーバーパラメータを定義します。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイス [編集 (Edit)] (✎) をクリックします。[インターフェイス (Interfaces)] タブがデフォルトで選択されます。
- ステップ 2 編集するインターフェイス [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [IPv6] ページをクリックしてから、[DHCP] をクリックします。
- ステップ 4 [DHCPサーバープール (DHCP Server Pool)] をクリックし、前に作成したオブジェクトを選択します。

図 5: DHCPv6 サーバーの有効化



- ステップ 5 DHCPv6 サーバーについて SLAAC クライアントに通知するには、[アドレス以外の設定で DHCP を有効にする (Enable DHCP for non-address config)] をオンにします。

このフラグは、DHCPv6 から DNS サーバー アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

ステップ6 [OK] をクリックします。

ステップ7 [Save (保存)] をクリックします。

これで、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

DHCP リレー エージェントの設定

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、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 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) 透過型ファイアウォールモードでは DHCP リレーはサポートされていません。

手順

ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense 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 [IPv4リレータイムアウト (IPv4 Relay Timeout)] および [IPv6リレータイムアウト (IPv6 Relay Timeout)] フィールドでは、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 (任意) [すべての情報を信頼する (Trust All Information)] をオンにして、すべてのクライアント インターフェイスを信頼できるインターフェイスとして設定します。

DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、Threat Defense DHCP リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィー

ルド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合は、Threat Defense はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。

ステップ 5 [DHCPリレーエージェント (DHCP Relay Agent)] 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。
- [IPv4リレーを有効にする (Enable IPv4 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) サーバーからの 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 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サーバーで異なるルータが指定されている場合でも、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、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 6 [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 7 [DHCPサーバー (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 サーバーアドレスおよび IPv6 サーバー アドレスが同じサーバーに属していても、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 サーバー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 8 [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 9 DHCP ページで [保存 (Save)] をクリックして変更を保存します。

ダイナミック DNS の設定

インターフェイスで DHCP IP アドレッシングを使用している場合、DHCP リースが更新されると、割り当てられた IP アドレスが変更されることがあります。完全修飾ドメイン名 (FQDN) を使用してインターフェイスに到達できる必要がある場合、この IP アドレスの変更が原因で DNS サーバーのリソースレコード (RR) が古くなる可能性があります。ダイナミック DNS (DDNS) は、IP アドレスまたはホスト名が変更されるたびに DNS の RR を更新するメカニズムです。DDNS はスタティックまたは PPPoE IP アドレッシングにも使用できます。

DDNS では DNS サーバーの A RR と PTR RR を更新します。A RR には名前から IP アドレスへのマッピングが含まれ、PTR RR でアドレスが名前にマッピングされます。

Threat Defense では、次の DDNS 更新方式をサポートしています。

- 標準の DDNS : 標準の DDNS 更新方式は RFC 2136 で定義されています。

この方式では、Threat Defense と DHCP サーバーで DNS 要求を使用して DNS の RR を更新します。Threat Defense または DHCP サーバーは、ローカル DNS サーバーにホスト名に関する情報を求める DNS 要求を送信し、その応答に基づいて RR を所有するメイン DNS サーバーを特定します。その後、Threat Defense または DHCP サーバーからメイン DNS サーバーに更新要求が直接送信されます。一般的なシナリオを次に示します。

- Threat Defense で A RR を更新し、DHCP サーバーで PTR RR を更新する。

通常、Threat Defense が A RR を「所有」し、DHCP サーバーが PTR RR を「所有」するため、両方のエンティティで個別に更新を要求する必要があります。IP アドレスまたはホスト名が変更されると、Threat Defense から DHCP サーバーに DHCP 要求 (FQDN オプションを含む) が送信され、PTR RR の更新を要求する必要があることが通知されます。

- DHCP サーバーで A RR と PTR RR の両方を更新する。

このシナリオは、Threat Defense に A RR を更新する権限がない場合に使用します。IP アドレスまたはホスト名が変更されると、Threat Defense から DHCP サーバーに DHCP 要求 (FQDN オプションを含む) が送信され、A RR と PTR RR の更新を要求する必要があることが通知されます。

セキュリティのニーズやメイン DNS サーバーの要件に応じて、異なる所有権を設定できます。たとえば、静的アドレスの場合、Threat Defense で両方のレコードの更新を所有します。

- Web : Web 更新方式では、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用します。

この方式では、IP アドレスまたはホスト名が変更されると、Threat Defense からアカウントを持っている DNS プロバイダーに HTTP 要求が直接送信されます。



- (注) 外部インターフェイスからゼロタッチプロビジョニングを使用して登録されたデバイスの場合、DDNS は「fmcOnly」方式を使用して自動的に有効になります（Web 方式と同様）。このメソッドは、ゼロタッチプロビジョニングデバイスでのみ使用できます。この画面を使用して、この方式の一部のオプションを編集したり、方式を削除して別の方式を設定したりできます。ゼロタッチプロビジョニングの詳細については、[シリアル番号（ゼロタッチプロビジョニング）を使用した Management Center へのデバイスの追加](#)を参照してください。

[DDNS] ページは、DDNS に関連する DHCP サーバー設定の設定も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。

始める前に

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [DNS サーバーグループ (DNS Server Group)] で DNS サーバーグループを構成し、[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] > [DNS] でインターフェイスのグループを有効にします。DNS を参照してください。
- デバイスのホスト名を設定します。Threat Defense の初期セットアップを実行するとき、または `configure network hostname` コマンドを使用して、ホスト名を設定できます。インターフェイスごとにホスト名を指定しない場合は、デバイスのホスト名が使用されます。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。

ステップ 2 [DHCP] > [DDNS] を選択します。

ステップ 3 標準の DDNS 方式 : Threat Defense からの DNS 要求を有効にするように DDNS 更新方式を設定します。

すべての要求を DHCP サーバーで実行する場合は、DDNS 更新方式を設定する必要はありません。

- a) [DDNS更新方式 (DDNS Update Methods)] で、[追加 (Add)] をクリックします。
- b) [メソッド名 (Method Name)] を設定します。
- c) [DDNS] をクリックします。
- d) (任意) [Update Interval] で、DNS 要求の更新間隔を設定します。デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、[Days] (0 ~ 364)、[Hours]、[Minutes]、[Seconds] で間隔を設定します。
- e) Threat Defense が更新する [更新レコード (Update Records)] を設定します。

この設定は、Threat Defense から直接更新するレコードにのみ影響します。DHCP サーバーで更新するレコードを指定するには、インターフェイスごとまたはグローバルに DHCP クライアント設定を行います。ステップ 5 (16 ページ) を参照してください。

- [未定義 (Not Defined)] : Threat Defense からの DNS 更新を無効にします。
- [A および PTR の両レコード (Both A and PTR Records)] : Threat Defense で A RR と PTR RR の両方を更新するように設定します。スタティックまたは PPPoE IP アドレッシングには、このオプションを使用します。
- [A レコード (A Records)] : Threat Defense で A RR のみを更新するように設定します。DHCP サーバーで PTR RR を更新する場合は、このオプションを使用します。

- f) [OK] をクリックします。
- g) この方式を [ステップ 5 \(16 ページ\)](#) でインターフェイスに割り当てます。

ステップ 4 Web 方式 : Threat Defense からの HTTP 更新要求を有効にするように DDNS 更新方式を設定します。

- a) [DDNS 更新方式 (DDNS Update Methods)] で、[追加 (Add)] をクリックします。
- b) [メソッド名 (Method Name)] を設定します。
- c) [Web] をクリックします。
- d) [Web 更新タイプ (Web Update Type)] を、IPv4、IPv6、または両方のタイプのアドレスを更新するように設定します。
- e) [Web URL] を設定します。更新 URL を指定します。必要な URL については、DNS プロバイダーに問い合わせてください。

次の構文を使用します。

https://username:password@provider-domain/path?hostname=<h>&myip=<a>

例 :

https://jcrichon:pa\$\$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

- f) (任意) [Update Interval] で、DNS 要求の更新間隔を設定します。デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、[Days] (0 ~ 364)、[Hours]、[Minutes]、[Seconds] で間隔を設定します。
- g) [OK] をクリックします。
- h) この方式を [ステップ 5 \(16 ページ\)](#) でインターフェイスに割り当てます。
- i) Web タイプ方式の DDNS の場合は、HTTPS 接続用の DDNS サーバ証明書の検証のために DDNS サーバのルート CA も識別する必要があります。[ステップ 9 \(19 ページ\)](#) を参照してください。

ステップ 5 DDNS のインターフェイス設定として、このインターフェイスの更新方式、DHCP クライアント設定、ホスト名などを設定します。

- a) [DDNS インターフェイス設定 (DDNS Interface Settings)] で、[追加 (Add)] をクリックします。
- b) ドロップダウンリストから [Interface] を選択します。

- c) [DDNS更新方式 (DDNS Update Methods)] ページで作成した [メソッド名 (Method Name)] を選択します。

(標準の DDNS 方式) すべての更新を DHCP サーバーで実行する場合は、方式を割り当てる必要はありません。

- d) このインターフェイスの [ホスト名 (Host Name)] を設定します。

ホスト名を設定しない場合は、デバイスのホスト名が使用されます。FQDN を指定しない場合、DNS サーバーグループのデフォルトのドメイン (スタティックまたは PPPoE IP アドレッシングの場合)、または DHCP サーバーのドメイン名 (DHCP IP アドレッシングの場合) が追加されます。

- e) 標準の DDNS 方式 : [DHCP クライアントが更新要求を DHCP サーバーに要求 (DHCP Client requests DHCP server to update requests)] で、DHCP サーバーで更新するレコードを指定します。

Threat Defense から DHCP サーバーに DHCP クライアント要求が送信されます。DHCP サーバーも DDNS をサポートするように設定する必要があることに注意してください。サーバーはクライアント要求を受け入れるように設定できるほか、クライアントをオーバーライドすることもできます (この場合、サーバーで実行している更新をクライアントで実行しないようにクライアントに応答します)。

スタティックまたは PPPoE IP アドレッシングの場合、これらの設定は無視されます。

(注) これらの値は、[DDNS] ページで、すべてのインターフェイスに対してグローバルに設定することもできます。インターフェイスごとの設定は、グローバル設定よりも優先されます。

- [未選択 (Not Selected)] : DHCP サーバーへの DDNS 要求を無効にします。クライアントで DDNS 更新を要求しなくても、DHCP サーバーから更新を送信するように設定できます。
- [更新なし (No Update)] : DHCP サーバーで更新を実行しないように要求します。この設定は、[Both A and PTR Records] を有効にした DDNS 更新方式と連携して機能します。
- [PTRのみ (Only PTR)] : DHCP サーバーで PTR RR の更新を実行するように要求します。この設定は、[A Records] を有効にした DDNS 更新方式と連携して機能します。
- [AおよびPTRの両レコード (Both A and PTR Records)] : DHCP サーバーで A RR と PTR RR の両方の更新を実行するように要求します。この設定では、DDNS 更新方式をインターフェイスに関連付ける必要はありません。

- f) [OK] をクリックします。

(注) [ダイナミック DNS 更新 (Dynamic DNS Update)] 設定は、Threat Defense で DHCP サーバーを有効にするときの DHCP サーバー設定に関連します。詳細については、[ステップ 6 \(18 ページ\)](#) を参照してください。

ステップ 6 Threat Defense で DHCP サーバーを有効にすると、DDNS の DHCP サーバー設定を構成できません。

DHCP サーバーを有効にするには、[DHCPv4 サーバーの設定 \(5 ページ\)](#) を参照してください。DHCP クライアントが標準の DDNS 更新方式を使用する場合のサーバーの動作を構成できません。サーバーが更新を実行する場合に、クライアントのリースが期限切れになる（更新されない）場合、サーバーは、DNS サーバーが担当していた RR を削除するように要求します。

- a) サーバー設定は、グローバルに構成することも、インターフェイスごとに構成することもできます。グローバル設定については、メインの [DDNS] ページを参照してください。インターフェイスごとの設定については、[DDNS インターフェイス設定 (DDNS Interface Settings)] ページを参照してください。インターフェイス設定は、グローバル設定よりも優先されます。
- b) [ダイナミック DNS 更新 (Dynamic DNS Update)] で、DHCP サーバーが更新する DNS RR を構成します。

- [未選択 (Not Selected)] : クライアントが要求した場合でも、DDNS 更新は無効になっています。
- [PTR のみ (Only PTR)] : DDNS 更新を有効にします。[DHCP クライアント要求のオーバーライド (Override DHCP Client Requests)] 設定を有効にすると、サーバーは PTR RR のみを更新します。それ以外の場合、サーバーはクライアントが要求する RR を更新します。クライアントが FQDN オプションで更新要求を送信しない場合、サーバーは DHCP オプション 12 で検出されたホスト名を使用して、A RR と PTR RR の両方の更新を要求します。
- [A および PTR の両レコード (Both A and PTR Records)] : DDNS 更新を有効にします。[DHCP クライアント要求のオーバーライド (Override DHCP Client Requests)] 設定を有効にすると、サーバーは A RR と PTR RR の両方を更新します。それ以外の場合、サーバーはクライアントが要求する RR を更新します。クライアントが FQDN オプションで更新要求を送信しない場合、サーバーは DHCP オプション 12 で検出されたホスト名を使用して、A RR と PTR RR の両方の更新を要求します。

- c) 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には、[DHCP クライアント要求のオーバーライド (Override DHCP Client Requests)] をオンにします。

サーバーは、要求がオーバーライドされたので、サーバーで実行している更新をクライアントで実行しないようにクライアントに応答します。

ステップ 7 (任意) 一般的な DHCP クライアント設定を構成します。これらの設定は DDNS には関係ありませんが、DHCP クライアントの動作に関係しています。

- a) [DDNS] ページで、[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)] をオンにして、DHCP サーバーが DHCP 応答をブロードキャストするように要求します (DHCP オプション 1)。
- b) デフォルトの内部生成文字列ではなく、オプション 61 の DHCP 要求パケット内に保存された MAC アドレスを強制するには、[DDNS] > [DHCP クライアント ID インターフェイス (DHCP Client ID Interface)] 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、それを [選択したインターフェイス (Selected Interfaces)] リストに移動します。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。この設定は DDNS とは直接関係ありませんが、一般的な DHCP クライアントの設定です。

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

ステップ 9 Web 方式の DDNS の場合は、HTTPS 接続用の DDNS サーバ証明書の検証のために DDNS サーバのルート CA も識別する必要があります。

次に、DDNS サーバの CA をトラストポイントとして追加する例を示します。

- a) DDNS サーバの CA 証明書を取得します。この手順では、PEM 形式を使用した手動インポートを示していますが、PKCS12 を使用することもできます。
- b) Management Center で、[デバイス (Devices)] > [証明書 (Certificates)] を選択し、[追加 (Add)] をクリックします。
- c) [デバイス (Device)] を選択し、**Add (+)** をクリックします。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:
5516X-4

Cert Enrollment*:
Select a certificate enrollment object +

Cancel Add

[証明書の登録の追加 (Add Cert Enrollment)] ダイアログボックスが表示されます。

- d) 次のフィールドに入力し、[保存 (Save)] をクリックします。

Add Cert Enrollment

Name*
CiscoRootCA

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Only
Check this option if you do not require an identity certificate to be created from this CA

TkL4Eq1ZKR4O
fdX4lld
oXyB5DC2Ae/g

Allow Overrides

Cancel Save

- 名前を入力します。
 - [登録タイプ (Enrollment Type)] > [手動 (Manual)] を選択します。
 - [CAのみ (CA Only)] をクリックします。
 - ステップ 9.a (19 ページ) の CA テキストを貼り付けます。
- e) [保存 (Save)] をクリックします。

DHCP および DDNS の履歴

| 機能 | 最小 Management Center | 最小 Threat Defense | 詳細 |
|--|----------------------|-------------------|--|
| Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。 | 7.4.1 | いずれか | <p>アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。</p> <p>Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。</p> <p>DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、Option 82 がすでに設定されている DHCP パケットを Threat Defense DHCP リレーエージェントが受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合、Threat Defense のデフォルトではそのパケットはドロップされます。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。</p> <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[デバイスの追加/編集 (Add/Edit Device)]>[DHCP]>[DHCP リレー (DHCP Relay)]</p> <p>その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。サポートされていないバージョンにアップグレードする場合は、FlexConfig をやり直してください。</p> |

| 機能 | 最小 Management Center | 最小 Threat Defense | 詳細 |
|-------------------|----------------------|-------------------|--|
| DHCPv6 ステートレスサーバー | 7.3.0 | 7.3.0 | <p>Threat Defense は、DHCPv6 プレフィックス委任クライアントを使用するときに、軽量の DHCPv6 ステートレスサーバーをサポートするようになりました。SLAAC クライアントが Threat Defense に情報要求 (IR) パケットを送信すると、Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] > [インターフェイスの追加/編集 (Add/Edit Interfaces)] > [IPv6] > [DHCP] • [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [DHCP IPv6 プール (DHCP IPv6 Pool)] <p>新規/変更されたコマンド：<code>show ipv6 dhcp</code></p> |

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。