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。

About DHCP and DDNS Services

The following topics describe the DHCP server, DHCP relay agent, and DDNS update.

About the DHCPv4 Server

DHCP provides network configuration parameters, such as IP addresses, to DHCP clients. The Firewall Threat Defense device can provide a DHCP server to DHCP clients attached to Firewall Threat Defense device interfaces. The DHCP server provides network configuration parameters directly to DHCP clients.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68; the DHCP server listens for messages on UDP port 67.

DHCP Options

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. The configuration parameters are carried in tagged items that are stored in the Options field of the DHCP message and the data are also called options. Vendor information is also stored in Options, and all of the vendor information extensions can be used as DHCP options.

For example, Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers.
- DHCP option 66 gives the IP address or the hostname of a single TFTP server.
- DHCP option 3 sets the default route.

A single request might include both options 150 and 66. In this case, the DHCP server provides values for both options in the response if they are already configured on the Firewall Threat Defense.

You can use advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients; DHCP option 15 is used for the DNS domain suffix. You can also use the DHCP automatic configuration setting to obtain these values or define them manually. When you use more than one method to define this information, it is passed to DHCP clients in the following sequence:

1. Manually configured settings.
2. Advanced DHCP options settings.
3. DHCP automatic configuration settings.

For example, you can manually define the domain name that you want the DHCP clients to receive and then enable DHCP automatic configuration. Although DHCP automatic configuration discovers the domain together with the DNS and WINS servers, the manually defined domain name is passed to DHCP clients with the discovered DNS and WINS server names, because the domain name discovered by the DHCP automatic configuration process is superseded by the manually defined domain name.

About the DHCPv6 Stateless Server

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (IPv6 プレフィックス委任クライアントの有効化), you can configure the Firewall Threat Defense to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the Firewall Threat Defense by defining a DHCP IPv6 Pool and assigning it to the DHCPv6 server. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages; in other words, based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

About the DHCP Relay Agent

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers. DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the Firewall Threat Defense device because it does not forward broadcast traffic. The DHCP relay agent lets you configure the interface of the Firewall Threat Defense device that is receiving the broadcasts to forward DHCP requests to a DHCP server on another device.

DHCP および DDNS の要件と前提条件

Model support

Firewall Threat Defense

User roles

- Admin
- Access Admin
- Network Admin

Guidelines for DHCP and DDNS Services

This section includes guidelines and limitations that you should check before configuring DHCP and DDNS services.

Firewall Mode

- DHCP Relay is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.
- DHCP Server is supported in transparent firewall mode on a bridge group member interface. In routed mode, the DHCP server is supported on the BVI interface, not the bridge group member interface. The BVI must have a name for the DHCP server to operate.
- DDNS is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.
- DHCPv6 stateless server is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.

Clustering

- DHCPv6 stateless server is not supported with clustering.

IPv6

Supports IPv6 for DHCP stateless server and DHCP Relay.

DHCPv4 Server

- The maximum available DHCP pool is 256 addresses.
- You can configure a DHCP server on any interface with a name and IP address, such as a physical interface, a subinterface, or a BVI in routed mode.
- Do not select an interface that uses DHCP or PPPoE to obtain it’s address as a DHCP server interface.

- You can configure only one DHCP server on each interface. Each interface can have its own pool of addresses to use. However the other DHCP settings, such as DNS servers, domain name, options, ping timeout, and WINS servers, are configured globally and used by the DHCP server on all interfaces.
- You cannot configure an interface as a DHCP client if that interface also has DHCP server enabled; you must use a static IP address.
- You cannot configure both a DHCP server and DHCP relay on the same device, even if you want to enable them on different interfaces; you can only configure one type of service.
- The Firewall Threat Defense does not support DHCP clients behind DHCP relay servers; the client must be directly connected to the Firewall Threat Defense.
- The DHCP server does not support BOOTP requests.

DHCPv6 Server

The DHCPv6 Stateless server cannot be configured on an interface where the DHCPv6 address, Prefix Delegation client, or DHCPv6 relay is configured.

DHCP Relay

- You can configure a maximum of 10 DHCPv4 relay servers per virtual router, global (VRF) and interface-specific servers combined, with a maximum of 4 servers per interface.
- You can configure a maximum of 10 DHCPv6 relay servers per virtual router. Interface-specific servers for IPv6 are not supported.
- You cannot configure both a DHCP server and DHCP relay on the same device, even if you want to enable them on different interfaces; you can only configure one type of service.
- Do not select an interface that uses DHCP or PPPoE to obtain it’s address as a DHCP relay interface.
- DHCP relay services are not available in transparent firewall mode or in routed mode on the BVI or bridge group member interface. You can, however, allow DHCP traffic through using an access rule. To allow DHCP requests and replies through the Firewall Threat Defense, you need to configure two access rules, one that allows DCHP requests from the inside interface to the outside (UDP destination port 67), and one that allows the replies from the server in the other direction (UDP destination port 68).
- For IPv4, clients must be directly-connected to the Firewall Threat Defense and cannot send requests through another relay agent or a router. For IPv6, the Firewall Threat Defense supports packets from another relay server.
- The DHCP clients must be on different interfaces from the DHCP servers to which the Firewall Threat Defense relays requests.
- You cannot enable DHCP Relay on an interface in a traffic zone.

DDNS Service

The firewall's DDNS supports only DynDNS service. Hence, ensure that the DDNS is configured with update URL in the following syntax:

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

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 [**Devices** > **Device Management**] を選択し、Firewall 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）]：Firewall 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、Firewall 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）]：Firewall 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なれません。

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 サーバー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 サーバー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 サーバーが使用する 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 サーバー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）]：Firewall 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、About the DHCPv4 Server （1 ページ）を参照してください。

  （注）
  Firewall 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 Firewall 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 Firewall 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 Firewall 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 **Objects** > **Object Management** > **DHCP IPv6 Pool**を選択します。

ステップ 2 **Add** ( ) をクリックします。

ステップ 3 **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 Firewall 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て使用できますが、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

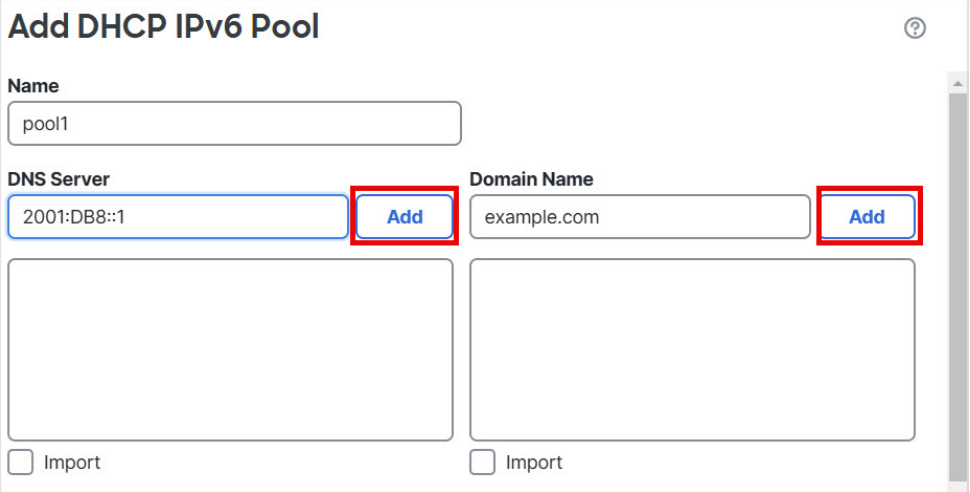
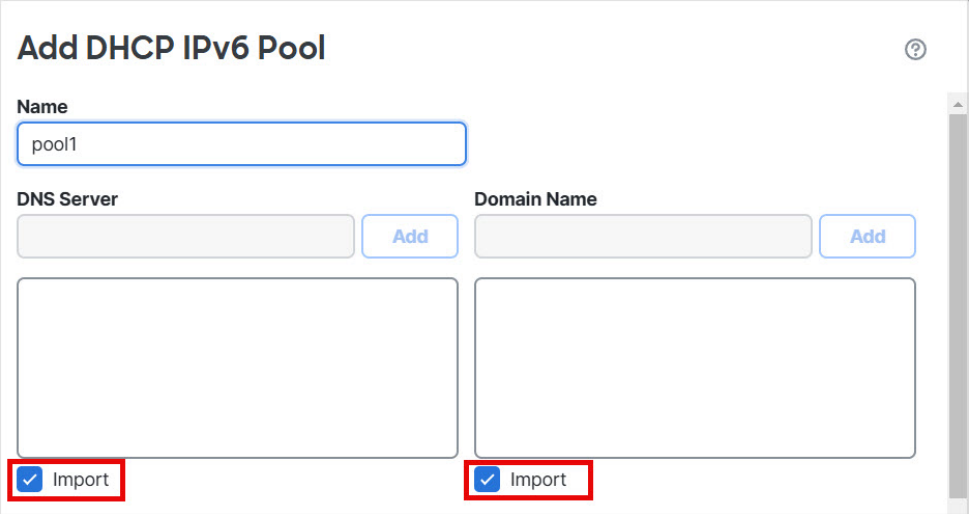


図 *2*: 値のインポート



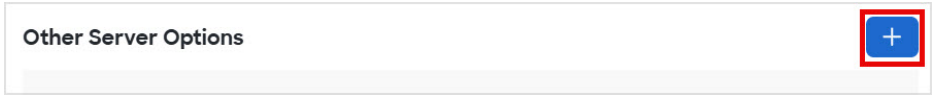
ステップ 4 **その他のサーバーオプション**を定義します。

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
- SNTP

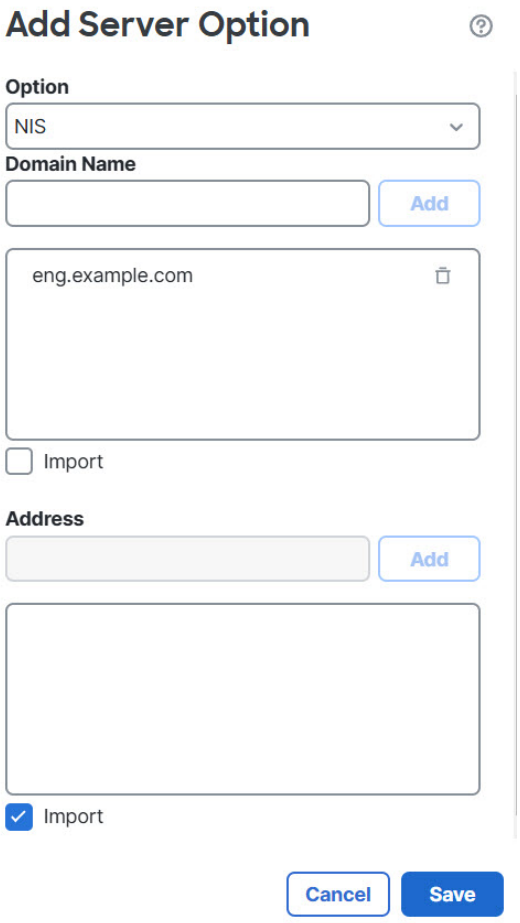
a) **Add** ( ) をクリックします。

図 *3*: その他のサーバーオプション



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 Firewall 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て使用できますが、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 5 **[保存（Save）]** をクリックします。

ステップ 6 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、これらのクライアントが情報要求（IR）パケットを Firewall 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 Firewall Threat Defense を設定できます。Firewall 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（Firewall 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

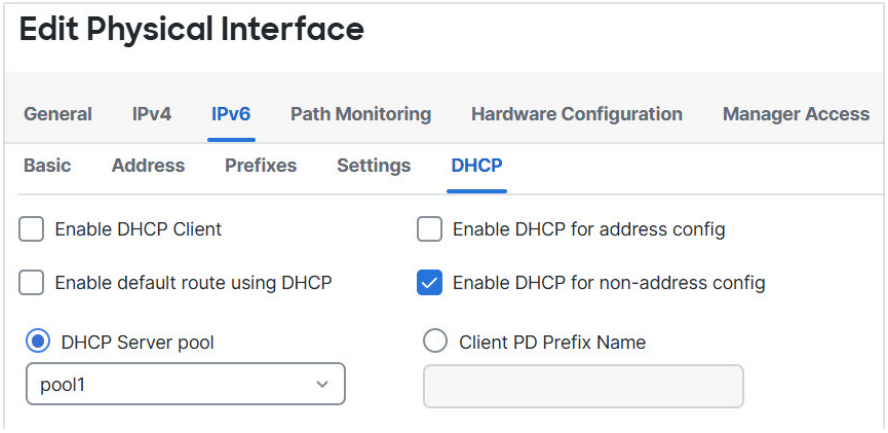
ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **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、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

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、Firewall 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 Firewall 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 サーバー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 [**Devices** > **Device Management**] を選択し、Firewall 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、Firewall 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、Firewall 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、Firewall 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 Firewall 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、Firewall 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、Firewall 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。

- [サーバー（Server）]：DHCP サーバーの 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 サーバーを、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 サーバー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。

Firewall 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、Firewall 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。Firewall 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、Firewall 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。

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

    通常、Firewall 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、Firewall 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、Firewall 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、Firewall 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、Firewall 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、Firewall 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 zero-touch provisioning 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）。この方式は、zero-touch provisioning 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。zero-touch provisioning の詳細については、シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）：基本設定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

- **Objects** > **Object Management** > **DNS Server Group** で DNS サーバーグループを構成し、**Devices** > **Platform Settings** のインターフェイスに対してグループを有効にし、Threat Defense ポリシーを作成または編集して、**[DNS]** をクリックします。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。Firewall 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 [**Devices** > **Device Management**] を選択し、Firewall 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：Firewall 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) Firewall 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、Firewall 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）]：Firewall 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）]：Firewall 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）]：Firewall 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：Firewall 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://jcrichton: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 （18 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。

Firewall 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、Firewall 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（17 ページ）を参照してください。

ステップ 6 Firewall 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す。

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す。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。

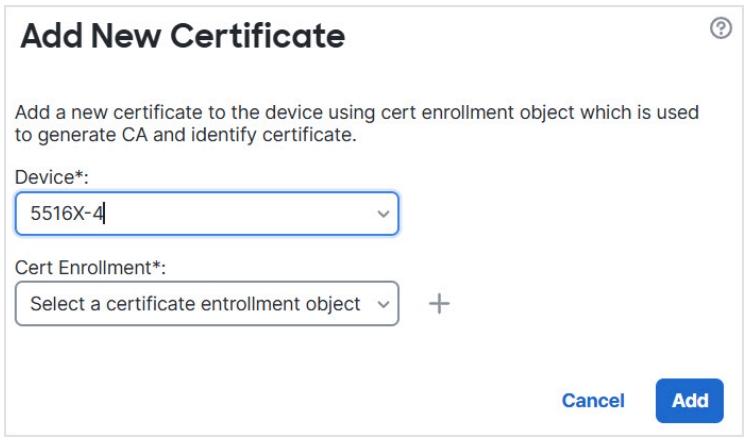
ステップ 9 Web 方式の DDNS の場合は、HTTPS 接続用の DDNS サーバ証明書の検証のために DDNS サーバのルート CA も識別する必要があります。

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 サーバーの 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。

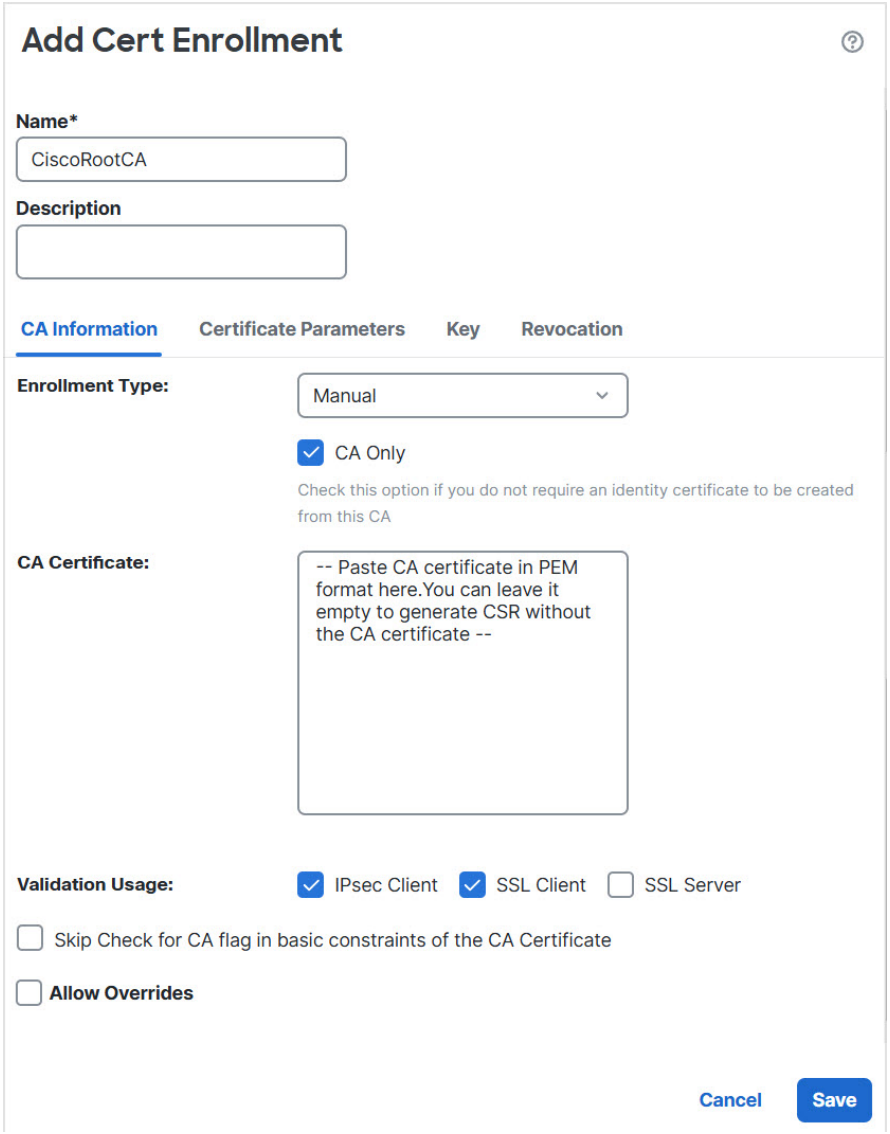
b) Firewall Management Center で、[**Devices** > **Certificates**]、**[追加（Add）]** の順に選択します。

c) [デバイス（Device）] を選択し、**Add** (＋) をクリックします。



[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。



- 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 （18 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	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Configure DHCP relay trusted interfaces from the Firewall Management Center web interface.	7.2.6/7.4.1	いずれか	**Upgrade impact. Redo any related FlexConfigs after upgrade.** You can now use the Firewall Management Center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the Firewall Threat Defense DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then Firewall Threat Defense will drop that packet by default. You can preserve Option 82 and forward the packet by identifying an interface as a trusted interface. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **DHCP** > **DHCP Relay**
DHCPv6 ステートレスサーバー	7.3.0	7.3.0	Firewall 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 Firewall Threat Defense に情報要求（IR）パケットを送信すると、Firewall 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。Firewall 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。 新規/変更された画面： • **[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）]** 新規/変更されたコマンド：**show ipv6 dhcp**

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。