DHCP サービスと DDNS サービス

この章では、ダイナミック DNS（DDNS）のアップデート方式のほか、DHCP サーバーまたは DHCP リレー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構成パラメータを DHCP クライアントに提供します。ASA は、ASA 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 サーバーを提供します。DHCP サーバは、ネットワーク設定パラメータを 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 でメッセージをリッスンし、DHCP サーバは UDP ポート 67 でメッセージをリッスンします。

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、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 サーバーおよび WINS サーバー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 サーバー名および WINS サーバー名とともに 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 サーバーについて

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、これらのクライアントが情報要求（IR）パケットを ASA に送信する際に（DNS サーバー、ドメイン名などの）情報を提供するように ASA を設定できます。ASA 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（ASA 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

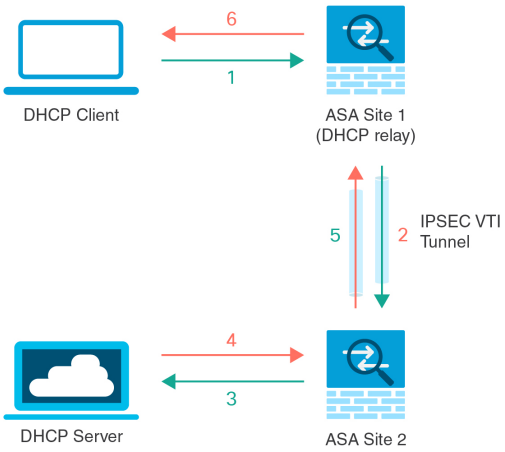
インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、ASA はブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェントを使用して、ブロードキャストを受信している ASA のインタ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

VTI での DHCP リレーサーバーのサポート

DHCP クライアントと DHCP サーバーの間で DHCP メッセージを受信して転送するように、ASA インターフェイスで DHCP リレーエージェントを設定できます。ただし、論理インターフェイスを介してメッセージを転送する DHCP リレーサーバーはサポートされていませんでした。

次の図は、VTI VPN 経由の DHCP リレーを使用した DHCP クライアントと DHCP サーバーの DISCOVER プロセスを示しています。ASA サイト 1 の VTI インターフェイスに設定された DHCP リレーエージェントは、DHCP クライアントから DHCPDISCOVER パケットを受信し、VTI トンネルを介してパケットを送信します。ASA サイト 2 は DHCPDISCOVER パケットを DHCP サーバーに転送します。DHCP サーバーは ASA サイト 2 に DHCPOFFER で応答します。この応答が ASA サイト 2 から DHCP リレー（ASA サイト 1）に転送され、そこから DHCP クライアントに転送されます。

図 *1 : VTI* を介した *DHCP* リレーサーバー



DHCPREQUEST および DHCPACK/NACK の要件についても同じ手順に従います。

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。

コンテキスト モード

- DHCPv6 ステートレス サーバは、マルチ コンテキスト モードではサポートされません。

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。
- DHCPv6 ステートレス サーバーは、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。

クラスタリング

- DHCPv6 ステートレス サーバは、クラスタリングではサポートされません。

IPv6

DHCP ステートレス サーバーの IPv6 と DHCP リレーをサポートします。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- 名前と IP アドレスを持つ任意のインターフェイス（物理インターフェイス、サブインターフェイス、ルーテッドモードの BVIなど）で DHCP サーバーを設定できます。
- 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。
- インターフェイスの DHCP アドレスを予約できます。ASA で、クライアントの MAC アドレスに基づいて、アドレスプールから DHCP クライアントに特定のアドレスが割り当てられます。
- ASA は、QIP DHCP サーバーと 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。

DHCPv6 サーバ

DHCPv6 ステートレス サーバは、DHCPv6 アドレス、プレフィックス委任クライアントまたは DHCPv6 リレーが設定されているインターフェイス上で設定できません。

DHCP リレー

- 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。
- 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、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利用できません。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 ASA 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 ASA 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、ASA 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、ASA 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。

DDNS サービス

ファイアウォールの DDNS は、DynDNS サービスのみをサポートします。したがって、DDNS が次のシンタックスの更新 URL で設定されていることを確認します。

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

DHCP サーバーの設定

ここでは、ASA の DHCP サーバーを設定する方法について説明します。

手順

ステップ 1 DHCPv4 サーバーの有効化 （6 ページ）。
ステップ 2 高度な DHCPv4 オプションの設定 （8 ページ）。
ステップ 3 DHCPv6 ステートレス サーバーの設定 （10 ページ）。

DHCPv4 サーバーの有効化

ASA のインターフェイスで DHCP サーバーをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 インターフェイスの DHCP アドレス プールを作成します。ASA は各クライアントにこのプールのアドレスを 1 つ割り当て、このアドレスを一定時間だけ使用できます。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。

dhcpd address *ip_address_start-ip_address_end if_name*

例：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

アドレス プールは、ASA 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。トランスペアレント モードでは、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、ルーテッド インターフェイスまたは 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。

ステップ 2 （任意）（ルーテッド モード）DHCP または PPPoE クライアントを実行するインターフェイスから、または VPN サーバーから取得される DNS、WINS、およびドメイン名の値を自動的に構成します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

例：

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

次のコマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定で取得されたパラメータが上書きされます。

ステップ 3 （任意）クライアントの DHCP アドレスを予約します。ASA で、クライアントの MAC アドレスに基づいて、設定されたアドレスプールから DHCP クライアントに特定のアドレスが割り当てられます。

dhcpd reserve-address *ip_address mac_address if_name*

例：

```
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

予約済みアドレスは設定済みのアドレスプールから取得する必要があり、アドレスプールは ASA インターフェイスと同じサブネット上にある必要があります。トランスペアレント モードでは、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、ルーテッドインターフェイスまたは 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。

ステップ 4 （オプション）DNS サーバーの IP アドレスを指定します。

dhcpd dns *dns1* [*dns2*]

例：

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

ステップ 5 （オプション）WINS サーバーの IP アドレスを指定します。WINS サーバーは最大 2 つまでです。

dhcpd wins *wins1* [*wins2*]

例：

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

ステップ 6 （任意）クライアントに許可するリース期間を変更します。リース期間とは、割り当てられた IP アドレスをクライアントが使用できる時間の長さ（秒）であり、この時間が経過するとリースは失効します。0 ～ 1,048,575 の範囲の数を入力してください。デフォルト値は 3600 秒です。

dhcpd lease *lease_length*

例：

```
ciscoasa(config)# dhcpd lease 3000
```

ステップ 7 （オプション）ドメイン名を設定します。

dhcpd domain *domain_name*

例：

```
ciscoasa(config)# dhcpd domain example.com
```

ステップ 8 （オプション）ICMP パケットの DHCP ping タイムアウト値を設定します。アドレスの競合を避けるために、ASA はアドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをそのアドレスに送信します。デフォルト値は 50 ミリ秒です。

dhcpd ping timeout *milliseconds*

例：

```
ciscoasa(config)# dhcpd ping timeout 20
```

ステップ 9 DHCP クライアントに送信するデフォルト ゲートウェイを定義します。ルーテッド モードで **dhcpd option 3 ip** コマンドを使用しない場合、ASA は、DHCP サーバーがイネーブルになっているインターフェイス IP アドレスをデフォルト ゲートウェイとして送信します。トランスペアレント モードでデフォルト ゲートウェイを設定する場合には **dhcpd option 3 ip** を設定する必要があります。ASA 自体はデフォルト ゲートウェイとして動作できません。

dhcpd option 3 ip *gateway_ip*

例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

ステップ 10 ASA 内の DHCP デーモンをイネーブルにし、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リッスンします。

dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd enable inside
```

dhcpd address 範囲と同じインターフェイスを指定します。

高度な DHCPv4 オプションの設定

ASA 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。

手順

ステップ 1 1 つまたは 2 つの IP アドレスを返す DHCP オプションを設定します。

dhcpd option *code* **ip** *addr_1* [*addr_2*]

例：

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

オプション 150 では、Cisco IP Phone で使用する 1 台または 2 台の TFTP サーバーの IP アドレスまたは名前を指定します。オプション 3 では、Cisco IP Phone のデフォルト ルートを設定します。

ステップ 2 テキスト文字列を返す DHCP オプションを設定します。

dhcpd option *code* **ascii** *text*

例：

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

オプション 66 では、Cisco IP Phone で使用する TFTP サーバーの IP アドレスまたは名前を指定します。

ステップ 3 16 進数値を返す DHCP オプションを設定します。

dhcpd option code hex *value*

例：

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

（注）
ASA 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** というコマンドを入力することは可能であり、ASA はこのコンフィギュレーションを受け入れますが、RFC 2132 の定義では、オプション 46 には 1 桁の 16 進数値を指定することになっています。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。

次の表に、**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 *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

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（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 ASA 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 ASA を設定できます。ASA は、IR パケットを受け取るだけでクライアントにアドレスを割り当てません。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（ASA 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。

始める前に

この機能は、シングル ルーテッド モードでのみサポートされます。この機能は、クラスタリングではサポートされていません。

手順

ステップ 1 DHCPv6 サーバーに提供させる情報が含まれる IPv6 DHCP プールを設定します。

ipv6 dhcp pool *pool_name*

例：

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

必要に応じてインターフェイスごとに個別のプールを設定できます。また、複数のインターフェイスで同じプールを使用することもできます。

ステップ 2 次のうち、IR メッセージに対する応答でクライアントに提供するパラメータを 1 つ以上設定します。

dns-server *dns_ipv6_address*

domain-name *domain_name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

import{[**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**]}

例：

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

import コマンドは、プレフィックス委任クライアント インターフェイスで ASA 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 **import** コマンドで設定することはできません。

ステップ 3 ASA に IR メッセージをリッスンさせるインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

ステップ 4 DHCPv6 サーバーをイネーブルにします。

ipv6 dhcp server *pool_name*

例：

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

ステップ 5 DHCPv6 サーバーに関する情報を SLAAC クライアントに提供するためのルータ アドバタイズメントを設定します。

ipv6 nd other-config-flag

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。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

DHCP リレー エージェントの設定

インターフェイスに DHCP 要求が届くと、ユーザーの設定に基づいて、ASA からその要求がリレーされる DHCP サーバーが決定されます。設定できるサーバーのタイプは次のとおりです。

- インターフェイス固有の DHCP サーバー：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバーにだけリレーします。
- グローバル DHCP サーバー：インターフェイス固有のサーバーが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバル サーバーは使用されません。

DHCPv4 リレー エージェントの設定

DHCP 要求がインターフェイスに届くと、ASA はその要求を DHCP サーバーにリレーします。

手順

ステップ 1 次のいずれかまたは両方を実行します。

- グローバル DHCP サーバーの IP アドレスおよびそのサーバーに到達可能なインターフェイスを指定します。

  dhcprelay server *ip_address if_name*

  例：

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- DHCP クライアント ネットワークに接続されているインターフェイス ID、およびそのインターフェイスで受信した DHCP 要求に対して使用される DHCP サーバーの IP アドレスを指定します。

```
interface interface_id
  dhcprelay server ip_address
```

  例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

  グローバル **dhcprelay server** コマンドとは異なり、要求の出力インターフェイスは指定しないことに注意してください。代わりに、ASA はルーティング テーブルを使用して出力インターフェイスを決定します。

ステップ 2 DHCP 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 サービスをイネーブルにします。複数のインターフェイス上で DHCP リレーをイネーブルにできます。

dhcprelay enable *interface*

例：

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

ステップ 3 （オプション）DHCP リレーのアドレス処理のために許容する時間を秒数で設定します。

dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# dhcprelay timeout 25
```

ステップ 4 （オプション）DHCP サーバーから送信されたパケットの最初のデフォルト ルータ アドレスを、ASA インターフェイスのアドレスに変更します。

dhcprelay setroute *interface_name*

例：

```
ciscoasa(config)# dhcprelay setroute inside
```

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、ASA 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、ASA 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。

ステップ 5 （オプション）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。次のいずれかを実行します。

- 信頼する DHCP クライアント インターフェイスを指定します。

```
interface interface_id
  dhcprelay information trusted
```

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

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、ASA 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、ASA 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。

- すべてのクライアント インターフェイスを信頼するインターフェイスとして設定します。

  dhcprelay information trust-all

  例：

```
ciscoasa(config)# dhcprelay information trust-all
```

DHCPv6 リレー エージェントの設定

インターフェイスに DHCPv6 要求が届くと、ASA はその要求をすべての DHCPv6 グローバル サーバーにリレーします。

手順

ステップ 1 クライアント メッセージの転送先となる IPv6 DHCP サーバーの宛先アドレスを指定します。

ipv6 dhcprelay server *ipv6_address* [*interface*]

例：

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 引数には、リンク スコープのユニキャスト、マルチキャスト、サイト スコープのユニキャスト、またはグローバル IPv6 アドレスを指定できます。リレー宛先の指定は必須です。ループバックやノードローカルのマルチキャストアドレスは指定できません。オプションの *interface* 引数では、宛先に対する出力インターフェイスを指定します。クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。指定したアドレスがリンク スコープのアドレスである場合は、インターフェイスを指定する必要があります。

ステップ 2 インターフェイス上で DHCPv6 リレー サービスをイネーブルにします。

ipv6 dhcprelay enable *interface*

例：

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

ステップ 3 （オプション）リレーアドレスの処理のために、リレーバインディングを通してDHCPv6サーバからの応答を DHCPv6 クライアントに渡すときに許容する時間を秒数で指定します。

ipv6 dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 引数の有効な値の範囲は 1 ～ 3600 です。デフォルトは 60 秒です。

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。

ASA 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、ASA と DHCP サーバーで DNS 要求を使用して DNS の RR を更新します。ASA 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、ASA 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。

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

    通常、ASA 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、ASA 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、ASA 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、ASA 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、スタティックアドレスの場合、ASA 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、ASA 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） 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

- **[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** で DNS サーバーを設定します。「DNS サーバーの設定」を参照してください。
- **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** でデバイスのホスト名とドメイン名を設定します。「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定」を参照してください。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。FQDN を指定しない場合、スタティックまたは PPPoE IP アドレッシングにおいては、システムのドメイン名または DNS サーバーのドメイン名がホスト名に追加されます。

手順

ステップ 1 標準の DDNS 方式：ASA 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) 更新方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns1
ciscoasa(DDNS-update-method)#
```

b) 標準の DDNS 方式を指定します。

ddns [**both**]

デフォルトでは、ASA は A RR のみを更新します。DHCP サーバーで PTR RR を更新する場合は、この設定を使用します。ASA で A RR と PTR RR の両方を更新する場合は、**both**

を指定します。スタティックまたは PPPoE IP アドレッシングには、**both** キーワードを使用します。

例：

```
ciscoasa(DDNS-update-method)# ddns
```

c) （任意） DNS 要求の更新間隔を設定します。

interval maximum *days hours minutes seconds*

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。

例：

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

d) この方式をインターフェイスに関連付けます。「ステップ 3 （19 ページ）」を参照してください。

ステップ 2 Web 方式：ASA 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) 更新方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method web1
ciscoasa(DDNS-update-method)#
```

b) DDNS サーバー証明書の ID を検証するための参照 ID 名を指定します。ASA は、ホスト名の一致を見つけようとします。ホストの解決に失敗するか一致するものが見つからない場合、接続は終了します。

例：

```
ciscoasa(DDNS-update-method)# web reference-identity dyndns
```

c) Web 方式と更新 URL を指定します。

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

疑問符（?）文字を入力する前に、キーボードの Ctrl キーと v キーを一緒に押します。これにより、? がソフトウェアでヘルプ照会と解釈されなくなり、? を入力できます。

例：

```
ciscoasa(DDNS-update-method)#
web update-url
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

d) （任意） 更新するアドレスタイプ（IPv4 または IPv6）を指定します。

デフォルトでは、ASA はすべての IPv4 アドレスと IPv6 アドレスを更新します。アドレスを制限する場合は、次のコマンドを入力します。

web update-type {**ipv4** | **ipv6** [**all**] | **both** [**all**]}

- **both all**：（デフォルト）すべての IPv4 アドレスと IPv6 アドレスを更新します。
- **both**：IPv4 アドレスと最新の IPv6 アドレスを更新します。
- **ipv4**：IPv4 アドレスのみを更新します。
- **ipv6**：最新の IPv6 アドレスのみを更新します。
- **ipv6 all**：すべての IPv6 アドレスを更新します。

例：

```
ciscoasa(DDNS-update-method)# web update-type ipv4
```

e) （任意） DNS 要求の更新間隔を設定します。

interval maximum *days hours minutes seconds*

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。

例：

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

f) この方式をインターフェイスに関連付けます。「ステップ 3 （19 ページ）」を参照してください。

g) 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 4 （21 ページ）を参照してください。

ステップ 3 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) インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)#
```

b) 更新方式を割り当てます。

ddns update *name*

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。 このコマンドは、Web アップデート方式の場合に必要です。

例：

```
ciscoasa(config-if)# ddns update ddns1
```

c) このインターフェイスのホスト名を割り当てます。

ddns update hostname *hostname*

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、システムのドメイン名または 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。

例：

```
ciscoasa(config-if)# ddns update hostname asa1.example.com
```

d) 標準の DDNS 方式：DHCP サーバーで更新するレコードを指定します。

dhcp client update dns [**server** {**both** | **none**}]

ASA 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）。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。

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、**dhcp-client update dns** コマンドを使用して、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。

- デフォルト（キーワードなし）：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、**ddns** で A レコードを有効にした DDNS 更新方式と連携して機能します。
- **server both**：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。
- **server none**：DHCP サーバで更新を実行しないように要求します。この設定は、**ddns both** で A レコードと PTR レコードを有効にした DDNS 更新方式と連携して機能します。

例：

```
ciscoasa(config-if)# ddns client update dns
```

ステップ 4 Web 方式の DDNS の場合は、HTTPS 接続用の DDNS サーバー証明書の検証のために DDNS サーバーのルート CA も識別する必要があります。「トラストポイントの設定」を参照してください。

例：

```
crypto ca trustpoint DDNS_Trustpoint
  enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

スタティック IP アドレスの標準の DDNS 方式

次に、スタティック IP アドレスで使用する標準の DDNS 方式を設定する例を示します。このシナリオでは、DHCP クライアント設定は設定しません。

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
 ddns both
interface gigabitethernet1/1
 ip address 209.165.200.225
! Associate the method with the interface:
 ddns update ddns-2
 ddns update hostname asa1.example.com
```

例：標準の DDNS 方式：ASA で A RR を更新し、DHCP サーバーで PTR RR を更新する

次に、ASA で A RR を更新し、DHCP サーバーで PTR RR を更新するように設定する例を示します。

```
! Define the DDNS method to update the A RR:
ddns update method ddns-1
 ddns
interface gigabitethernet1/1
  ip address dhcp
! Associate the method with the interface:
  ddns update ddns-1
  ddns update hostname asa
! Set the client to update the A RR, and the server to update the PTR RR:
  dhcp client update dns
```

例：標準の DDNS 方式：DHCP サーバーで RR を更新しない

次に、ASA で A RR と PTR RR の両方を更新するように設定し、DHCP サーバーで RR を更新しないように要求する例を示します。

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update ddns-2
  ddns update hostname asa1.example.com
! Set the client to update both RRs, and the server to update none:
  dhcp client update dns server none
```

例：標準の DDNS 方式：DHCP サーバーで両方の RR を更新する

次に、DHCP クライアントからの要求に応じて DHCP サーバーで A RR と PTR RR の両方を更新するように設定する例を示します。すべての更新をサーバーで実行するため、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。

```
interface gigabitethernet1/1
  ip address dhcp
  ddns update hostname asa
! Configure the DHCP server to update both RRs:
  dhcp client update dns server both
```

例：Web タイプ

次に、Web タイプ方式を設定する例を示します。

```
! Define the web type method:
ddns update method web-1
  web update-url
https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

DHCP および DDNS サービスのモニタリング

この項では、DHCPおよびDDNSの両方のサービスをモニターする手順について説明します。

DHCP サービスのモニタリング

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  このコマンドは、現在の DHCP サーバー クライアント バインディング、状態と統計情報を示します。

- **show dhcprelay** {**state** | **statistics**}

  このコマンドは、DHCP リレー ステータスと統計情報を表示します。

- **show ipv6 dhcprelay binding**

  このコマンドは、リレー エージェントによって作成されたリレー バインディング エントリを表示します。

- **show ipv6 dhcprelay statistics**

  このコマンドは、IPv6 の DHCP リレー エージェントの統計情報を表示します。

- **show ipv6 dhcp server statistics**

  このコマンドは、DHCPv6 ステートレス サーバーの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]
- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface コマンドは、すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバー構成用に設定されている場合（DHCPv6 ステートレス サーバーの設定 （10 ページ） を参照）、このコマンドはサーバーによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、このコマンドは各クライアントの状態とサーバーから受信した値を表示します。特定のインターフェイスについて、DHCP サーバーまたはクライアントのメッセージの統計情報を表示できます。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
```

```
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
```

```
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics コマンドは、DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバーユニット間のトランザクションの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

  アクティブ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  スタンドバイ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

VTI を介した DHCP リレーのトラブルシューティング

DHCP クライアントで IP アドレスを取得できない場合は、次の手順を実行します。

- 両方の ASA サイトのトンネルインターフェイス/VTI 設定を確認します。
- **show crypto ipsec sa** コマンドを使用して、サイト間で転送されたパケットを確認します。

  例

```
ciscoasa(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cmap, seq num: 10, local addr: 192.168.2.111
access-list CSM_IPSEC_ACL_0 extended permit ip any4 any4
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer: 192.168.2.110
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

デバッグコマンドの有効化

DHCP リレーのデバッグを有効にすると、DISCOVER/REQUEST パケットが DHCP リレーサーバーに転送されたかどうかを確認できます。

- **debug dhcprelay event 255**
- **debug dhcprelay packet 255**
- **debug dhcprelay error 255**

例

```
ciscoasa(config)# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
DHCP: Received a BOOTREQUEST from interface 2 (size = 548)
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPRA: setting giaddr to 192.168.1.111. dhcpd_forward_request: request from xxxx.xxxx.xxxx
forwarded to 192.168.3.112.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on vti interface
DHCP: Received a BOOTREPLY from relay interface 5 (size = 300, xid = xxxxxxxxx) at
04:40:52
UTC Tue Sep 10 2019
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPD/RA: creating ARP entry (192.168.1.88, xxxx.xxxx.xxxx).
DHCPRA: Adding rule to allow client to respond using offered address 192.168.1.95
DHCPRA: forwarding reply to client xxxx.xxxx.xxxx.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
```

DDNS ステータスのモニタリング

DDNS ステータスのモニタリングについては、次のコマンドを参照してください。

- **show ddns update** { **interface** *if_name* | **method** [*name*]}

  このコマンドは、DDNS 更新ステータスを表示します。

  次の例は、DDNS 更新方式の詳細を示しています。

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  次の例は、Web 更新方式の詳細を示しています。

```
ciscoasa# show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

次の例は、DDNS インターフェイスに関する情報を示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

次の例は、Web タイプの更新が成功したことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

次の例は、Web タイプの更新が失敗したことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

次の例は、DNS サーバーから Web タイプの更新のエラーが返されたことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

次の例は、IP アドレスが設定されていないか DHCP 要求が失敗したために、Web 更新がまだ試行されていないことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

DHCP および DDNS サービスの履歴

機能名	プラットフォーム リリース	説明
DDNS の Web 更新方式のサポート	9.15(1)	DDNS の Web 更新方式を使用するようにインターフェイスを設定できるようになりました。 新規/変更されたコマンド： **show ddns update interface**、**show ddns update method**、**web update-url**、**web update-type**
VTI での DHCP リレーサーバーのサポート	9.14(1)	VTI で DHCP リレーを有効にできるようになりました。 新規/変更されたコマンド： **dhcprelay server**
DHCP の予約	9.13(1)	ASA で DHCP の予約がサポートされます。DHCP サーバーで、クライアントの MAC アドレスに基づいて、定義されたアドレスプールから DHCP クライアントにスタティック IP アドレスが割り当てられます。 新規/変更されたコマンド： **dhcpd reserve-address**
IPv6 DHCP	9.6(2)	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバーから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバー：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次のコマンドが追加または変更されました。**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
DHCPv6 モニタリング	9.4(1)	IPv6 の DHCP 統計情報および IPv6 の DHCP バインディングをモニターできます。

機能名	プラットフォームリリース	説明
DHCP リレー サーバーは、応答用の DHCP サーバー識別子を確認します。	9.2(4)/ 9.3(3)	ASA DHCP リレー サーバーが不適切な DHCP サーバーから応答を受信すると、応答を処理する前に、その応答が適切なサーバーからのものであることを確認するようになりました。導入または変更されたコマンドはありません。変更された ASDM 画面はありません。 導入または変更されたコマンドはありません。
DHCP 再バインド機能	9.1(4)	DHCP 再バインド フェーズに、クライアントはトンネル グループ リスト内の他の DHCP サーバーへの再バインドを試みるようになりました。このリリース以前には、DHCP リースの更新に失敗した場合、クライアントは代替サーバーへ再バインドしませんでした。 導入または変更されたコマンドはありません。
DHCP の信頼できるインターフェイス	9.1(2)	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。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、ASA 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、ASA 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。 **dhcprelay information trusted**、**dhcprelay information trust-all**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
インターフェイスごとの DHCP リレー サーバー（IPv4 のみ）	9.1(2)	DHCP リレー サーバーをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサーバーに対してのみリレーされます。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。 **dhcprelay server**（インターフェイス設定モード）、**clear configure dhcprelay**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
DHCP relay for IPv6 (DHCPv6)	9.0(1)	DHCP リレーに IPv6 サポートが追加されました。 **ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics**、**clear ipv6 dhcprelay statistics** の各コマンドが導入されました。

機能名	プラットフォーム リリース	説明
DDNS	7.0(1)	この機能が導入されました。 **ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns**、および **show running-config dns server-group** の各コマンドが導入されました。
DHCP	7.0(1)	ASA は、DHCP サーバーまたは DHCP リレー サービスを ASA 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。 次のコマンドを導入しました。**dhcp client update dns**、 **dhcpd address**、 **dhcpd domain**、**dhcpd enable**、 **dhcpd lease**、**dhcpd option**、**dhcpd ping timeout**、**dhcpd update dns**、**dhcpd wins**、**dhcp-network-scope**、**dhcprelay enable**、**dhcprelay server**、**dhcprelay setroute**、**dhcp-server**、**show running-config dhcpd**、および **show running-config dhcprelay**。

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。