



DHCP 和 DDNS 服务

本章介绍如何配置 DHCP 服务器和 DHCP 中继以及动态 DNS (DDNS) 更新方法。

- [关于 DHCP 和 DDNS 服务，第 1 页](#)
- [DHCP 和 DDNS 服务准则，第 3 页](#)
- [配置 DHCP 服务器，第 5 页](#)
- [配置 DHCP 中继代理，第 8 页](#)
- [配置动态 DNS，第 10 页](#)
- [监控 DHCP 和 DDNS 服务，第 13 页](#)
- [DHCP 和 DDNS 服务的历史记录，第 16 页](#)

关于 DHCP 和 DDNS 服务

以下主题介绍 DHCP 服务器、DHCP 中继代理和 DDNS 更新。

关于 DHCPv4 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。ASA 可以为连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器。DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

DHCP 选项

DHCP 提供用于将配置信息传递至 TCP/IP 网络中主机的标准。配置参数在存储于 DHCP 消息的 Options 字段中的标记项目中携带，数据也称为选项。供应商信息也存储在 Options 中，并且所有供应商信息扩展均可用作 DHCP 选项。

例如，思科 IP 电话从 TFTP 服务器下载其配置。当思科 IP 电话启动时，如果其不让 IP 地址和 TFTP 服务器 IP 地址均得以预配置，则其将向 DHCP 服务器发送带有选项 150 或 66 的请求以获取此信息。

- DHCP 选项 150 提供 TFTP 服务器列表的 IP 地址。
- DHCP 选项 66 提供单一 TFTP 服务器的 IP 地址或主机名。

- DHCP 选项 3 设置默认路由。

单一请求可能同时包括选项 150 和 66。在此情况下，如在 ASA 上已配置这两个选项，则 ASA DHCP 服务器将在响应中为两个选项提供值。

您可以使用高级 DHCP 选项向 DHCP 客户端提供 DNS、WINS 和域名参数；DHCP 选项 15 用于 DNS 域名后缀。也可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器来发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

关于 DHCPv6 无状态服务器

对于结合前缀授权功能 ([启用 IPv6 前缀授权客户端](#)) 使用无状态地址自动配置 (SLAAC) 的客户端，可以来配置 ASA，以便在它们向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

关于 DHCP 中继代理

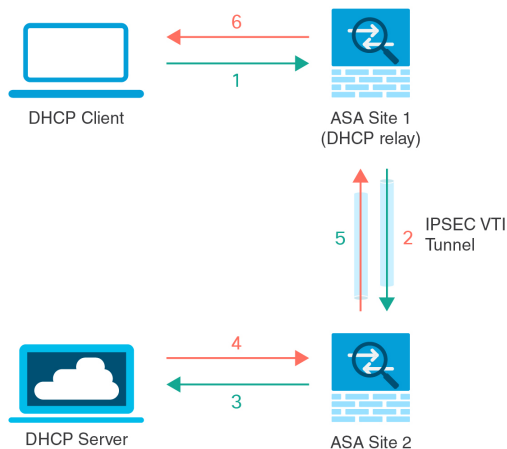
您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 ASA 进行转发，因为它不转发广播流量。DHCP 中继代理可用于配置用来接收广播的 ASA 的接口，以将 DHCP 请求转发至另一接口上的 DHCP 服务器。

VTI 上的 DHCP 中继服务器支持

您可以在 ASA 接口上配置 DHCP 中继代理，以在 DHCP 客户端和 DHCP 服务器之间接收和转发 DHCP 消息。但是，不支持通过逻辑接口转发消息的 DHCP 中继服务器。

下图显示了通过 VTI VPN 使用 DHCP 中继的 DHCP 客户端和 DHCP 服务器的发现过程。在 ASA 站点 1 的 VTI 接口上配置的 DHCP 中继代理从 DHCP 客户端接收 DHCPDISCOVER 数据包，并通过 VTI 隧道发送数据包。ASA 站点 2 将 DHCPDISCOVER 数据包转发到 DHCP 服务器。DHCP 服务器使用 DHCP OFFER 向 ASA 站点 2 进行回复。ASA 站点 2 将其转发到 DHCP 中继 (ASA 站点 1)，后者将其转发到 DHCP 客户端。

图 1: 通过 VTI 的 DHCP 中继服务器



DHCPREQUEST 和 DHCPACK/NACK 要求遵循相同的程序。

DHCP 和 DDNS 服务准则

本节介绍在配置 DHCP 和 DDNS 服务之前应检查的准则和限制。

情景模式

- 多情景模式下不支持 DHCPv6 无状态服务器。

防火墙模式

- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCP 中继。
- 在网桥组成员接口上的透明防火墙模式下，支持 DHCP 服务器。在路由模式下，在 BVI 接口（而非网桥组成员接口）上支持 DHCP 服务器。BVI 必须具有名称，DHCP 服务器才能运行。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DDNS。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCPv6 无状态服务器。

集群

- 集群不支持 DHCPv6 无状态服务。

IPv6

支持 IPv6 用于 DHCP 无状态服务器和 DHCP 中继。

DHCPv4 服务器

- 最大可用 DHCP 池为 256 个地址。
- 只能在每个接口上配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置（如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 如果某个接口也启用了 DHCP 服务器，则不能将该接口配置为 DHCP 客户端；您必须使用静态 IP 地址。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 您可以为接口保留 DHCP 地址。根据客户端的 MAC 地址，ASA 从地址池中将一个具体的 IP 地址分配给 DHCP 客户端。
- ASA 不支持 QIP DHCP 服务器与 DHCP 代理服务一起使用。
- DHCP 服务器不支持 BOOTP 请求。

DHCPv6 服务器

在已配置 DHCPv6 地址、前缀委派客户端或 DHCPv6 中继的接口上，无法配置 DHCPv6 无状态服务器。

DHCP 中继

- 在单一模式和每个情景中 最多可以配置 10 台 DHCPv4 中继服务器，这些服务器为全局和接口专用服务器的组合，其中每个接口最多允许 4 台服务器。
- 在单一模式和每个情景中 最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的接口专用服务器。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下 DHCP 中继服务不可用。但是，可以通过使用访问规则允许 DHCP 流量通过。要允许 DHCP 请求和回复通过 ASA，需要配置两条访问规则，一条允许从内部接口到外部接口（UDP 目标端口 67）的 DHCP 请求，另一条允许来自其他方向（UDP 目标端口 68）的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 ASA 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，ASA 支持来自另一个中继服务器的数据包。
- DHCP 客户端必须与 ASA 中继请求的 DHCP 服务器位于不同接口。
- 不能在流量区域内的接口上启用 DHCP 中继。

配置 DHCP 服务器

本部分介绍如何配置 ASA 提供的 DHCP 服务器。

过程

-
- 步骤 1 启用 DHCPv4 服务器，第 5 页。
 - 步骤 2 配置高级 DHCPv4 选项，第 7 页。
 - 步骤 3 配置 DHCPv6 无状态服务器，第 7 页。
-

启用 DHCPv4 服务器

要在 ASA 接口上启用 DHCP 服务器，请执行以下步骤：

过程

-
- 步骤 1 依次选择配置 > 设备管理 > DHCP > DHCP 服务器。
 - 步骤 2 选择接口，然后点击编辑 (Edit)。

在透明模式下，请选择网桥组成员接口。在路由模式下，请选择一个路由接口或 BVI；不要选择网桥组成员接口。

- a) 选中 **Enable DHCP Server** 复选框以启用选定接口上的 DHCP 服务器。
- b) 在 **DHCP Address Pool** 字段中，输入 DHCP 服务器使用的从最低到最高的 IP 地址范围。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- c) 在 **Optional Parameters** 区域内设置以下参数：
 - 为接口配置的 DNS 服务器（1 和 2）。
 - 为接口配置的 WINS 服务器（主服务器和次要服务器）。
 - 接口的域名
 - ASA 将在接口上等待 ICMP ping 响应的的时间（单位：毫秒）。
 - 接口上配置的 DHCP 服务器允许 DHCP 客户端使用所分配的 IP 地址的持续时间。
 - 如果 ASA 用作指定接口（通常为外部）上的 DHCP 客户端，为向自动配置提供 DNS、WINS 和域名信息的 DHCP 客户端上的接口。
 - 点击高级 (Advanced) 以显示高级 DHCP 选项 (Advanced DHCP Options) 对话框，从而配置多个 DHCP 选项。有关详细信息，请参阅配置高级 DHCPv4 选项，第 7 页。

- d) 在 **Dynamic Settings for DHCP Server** 区域中，选中 **Update DNS Clients** 复选框以指定，除更新客户端 PTR 资源记录的默认操作之外，所选的 DHCP 服务器也应执行以下更新操作：
- 选中 **Update Both Records** 复选框，以指定 DHCP 服务器应同时更新 A RR 和 PTR RR。
 - 选中 **Override Client Settings** 复选框，以指定 DHCP 服务器操作应覆盖 DHCP 客户端请求的任何更新操作。

e) 点击 **确定 (OK)** 以关闭 **编辑 DHCP 服务器 (Edit DHCP Server)** 对话框。

步骤 3 (可选) (路由模式) 在 DHCP 服务器表下的 **Global DHCP Options** 区域中，选中 **Enable Auto-configuration from interface** 复选框以仅在 ASA 用作指定接口 (通常为外部) 上的 DHCP 客户端时启用 DHCP 自动配置。

DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。如果在 **Global DHCP Options** 区域内还手动指定通过自动配置获取的信息，则手动指定的信息优先于发现的信息。

步骤 4 从下拉列表中选择自动配置接口。

步骤 5 选中 **Allow VPN Override** 复选框，以使用 VPN 客户端参数覆盖 DHCP 或 PPPoE 客户端参数。

步骤 6 在 **DNS Server 1** 字段中，为 DHCP 客户端输入 DNS 主服务器的 IP 地址。

步骤 7 在 **DNS Server 2** 字段中，为 DHCP 客户端输入 DNS 备选服务器的 IP 地址。

步骤 8 在 **Domain Name** 字段中，输入 DHCP 客户端的 DNS 域名 (例如，example.com)。

步骤 9 在 **Lease Length** 字段中，输入在租赁到期之前客户端可使用向其分配的 IP 地址的时间 (以秒为单位)。值的范围为 300 到 1048575 秒。默认值为 3600 秒 (1 小时)。

步骤 10 在 **Primary WINS Server** 字段中，为 DHCP 客户端输入 WINS 主服务器的 IP 地址。

步骤 11 在 **Secondary WINS Server** 字段中，为 DHCP 客户端输入 WINS 备选服务器的 IP 地址。

步骤 12 为了避免地址冲突，ASA 会在将某个地址分配至 DHCP 客户端之前向该地址发送两个 ICMP ping 数据包。在 **Ping Timeout** 字段中输入 ASA 等待 DHCP ping 尝试超时的时长 (单位：毫秒)。值的范围为 10 到 10000 毫秒。默认值为 50 毫秒。

步骤 13 点击 **高级 (Advanced)** 选项卡，以显示配置 **高级 DHCP 选项 (Configuring Advanced DHCP Options)** 对话框，从而在其中指定其他 DHCP 选项及其参数。有关详细信息，请参阅 [配置高级 DHCPv4 选项](#)，第 7 页。

步骤 14 为 **Dynamic DNS Settings for DHCP Server** 区域内的 DHCP 服务器配置 DDNS 更新设置。选中 **Update DNS Clients** 复选框，以指定除了更新客户端 PTR 资源记录这一默认操作外，选定 DHCP 服务器还应执行以下更新操作：

- 选中 **Update Both Records** 复选框，以指定 DHCP 服务器应同时更新 A RR 和 PTR RR。
- 选中 **Override Client Settings** 复选框，以指定 DHCP 服务器操作应覆盖 DHCP 客户端请求的任何更新操作。

步骤 15 点击 **Apply** 保存更改。

配置高级 DHCPv4 选项

ASA 支持 RFC 2132、RFC 2562 和 RFC 5510 中所列的 DHCP 选项以发送信息。所有 DHCP 选项 (1-255) 均受支持，但 1、12、50 - 54、58 - 59、61、67 和 82 除外。

过程

步骤 1 依次选择配置 > 设备管理 > DHCP > DHCP 服务器，然后点击高级。

步骤 2 从下拉列表中选择选项代码。

步骤 3 选择要配置的选项。某些选项属于标准选项。对于标准选项，选项名称显示在选项编号之后并用括号括起来，选项参数限定于那些受该选项支持的参数。对于所有其他选项，仅显示选项编号，您必须选择要随该选项提供的适当参数。例如，如果选择 DHCP 选项 2（时间偏移量），则只能输入该选项的十六进制值。对于所有其他 DHCP 选项，所有选项值类型均可用，必须选择适当的一个。

步骤 4 指定选项向 **Option Data** 区域内 DHCP 客户端返回的信息的类型。对于标准 DHCP 选项，仅支持的选项值类型可用。对于所有其他 DHCP 选项，所有选项值类型均可用。点击 **Add** 以将选项添加到 DHCP 选项列表。点击 **Delete** 以将选项从 DHCP 选项列表中删除。

- 点击 **IP Address** 以表明已向 DHCP 客户端返回一个 IP 地址。最多可以指定两个 IP 地址。IP 地址 1 和 IP 地址 2 以点分十进制表示法显示 IP 地址。

注释 关联 IP 地址字段的名称可能随选择的 DHCP 选项改变。例如，如果选择 DHCP 选项 3（路由器），则字段名将更改为 Router 1 和 Router 2。

- 点击 **ASCII** 以指定已向 DHCP 客户端返回一个 ASCII 值。在 **Data** 字段中，输入一个 ASCII 字符串。字符串不能包含空格。

注释 关联 Data 字段的名称可能随选择的 DHCP 选项改变。例如，如果选择 DHCP 选项 14（Merit Dump File），则关联 Data 字段将更改为 File Name。

- 点击 **Hex** 以指定已向 DHCP 客户端返回一个十六进制值。在 **Data** 字段中，输入一个偶数位且无空格的十六进制字符串。您无需使用 0x 前缀。

注释 关联 Data 字段的名称可能随选择的 DHCP 选项改变。例如，如果选择 DHCP 选项 2（时间偏移量），则关联 Data 字段变为 Offset 字段。

步骤 5 点击 **OK** 以关闭 **Advanced DHCP Options** 对话框。

步骤 6 点击 **Apply** 保存更改。

配置 DHCPv6 无状态服务器

对于配合使用无状态地址自动配置 (SLAAC) 及前缀代理功能 ([启用 IPv6 前缀授权客户端](#)) 的客户端，可以将 ASA 配置为在客户端向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户

端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

开始之前

此功能仅支持单一路由模式。此功能不支持集群。

过程

步骤 1 配置包含您希望 DHCPv6 服务器提供的信息的 IPv6 DHCP 池：

- a) 依次选择配置 > 设备管理 > DHCP > DHCP 池，然后点击添加。
- b) 在 **DHCP Pool Name** 字段中输入名称。
- c) 对于每个选项卡上的各个参数，选中 **Import** 复选框或手动在该字段中输入值，再点击 **Add**。

Import 选项使用 ASA 在前缀代理客户端接口上从 DHCPv6 服务器获取的一个或多个参数。您可以混合搭配手动配置的参数与导入的参数；但是，手动配置相同的参数与指定 **import** 配置的参数不能相同。

- d) 点击 **OK**，然后点击 **Apply**。

步骤 2 依次选择配置 > 设备设置 > 接口设置 > 接口。

步骤 3 选择接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

步骤 4 点击 **IPv6** 选项卡。

步骤 5 在 **Interface IPv6 DHCP** 区域中，点击 **Server DHCP Pool Name** 单选按钮，并输入 IPv6 DHCP 池名称。

步骤 6 选中 **Hosts should use DHCP for address config** 复选框以在 IPv6 路由器通告数据包中设置其他地址配置标志。

此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

步骤 7 点击确定 (**OK**)。

系统将返回到 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。

步骤 8 点击应用。

配置 DHCP 中继代理

在 DHCP 请求进入接口后，ASA 中继将请求转发到的 DHCP 服务器取决于您的配置。您可以配置以下类型的服务器：

- 接口专用 DHCP 服务器 - DHCP 请求进入特定接口后，ASA 仅向接口专用服务器中继请求。

- 全局 DHCP 服务器 - DHCP 请求进入未让接口专用服务器得以配置的接口后，ASA 将向所有全局服务器中继请求。如果接口有接口专用服务器，则将不使用全局服务器。

过程

步骤 1 依次选择配置 > 设备管理 > DHCP > DHCP 中继。

步骤 2 在 **DHCP Relay Agent** 区域选中，为每个接口所需服务选择对应的复选框。

- **IPv4 > DHCP Relay Enabled**。
- **IPv4 > Set Route** - 将来自服务器的 DHCP 消息中默认网关地址更改为最接近 DHCP 客户端的 ASA 接口的地址，该客户端中继原始 DHCP 请求。此操作允许客户端将其默认路由器设置为指向 ASA，即使 DHCP 服务器指定了其他路由器亦是如此。如果数据包中没有默认的路由器选项，则 ASA 会添加一个包含接口地址的路由器选项。
- **IPv6 > DHCP Relay Enabled**。
- **Trusted Interface** - 指定要信任的 DHCP 客户端接口。您可以将接口配置为受信任接口以保留 DHCP Option 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 `giaddr` 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。另外，可通过选中 **Set dhcp relay information as trusted on all interfaces** 复选框信任所有接口。

步骤 3 在 **Global DHCP Relay Servers** 区域中，添加一个或多个要将 DHCP 请求中继到的 DHCP 服务器。

- a) 点击 **Add**。系统将显示 **Add Global DHCP Relay Server** 对话框。
- b) 在 **DHCP Server** 字段中，输入 DHCP 服务器的 IPv4 或 IPv6 地址。
- c) 从 **Interface** 下拉列表中，选择指定 DHCP 服务器要连接的接口。
- d) 点击 **OK**。

Global DHCP Relay Servers 列表中将显示新添加的全局 DHCP 中继服务器。

步骤 4 （可选）在 **IPv4 Timeout** 字段中，输入为 DHCPv4 地址处理预留的时间量（以秒为单位）。值的范围为 1 到 3600 秒。默认值为 60 秒。

步骤 5 （可选）在 **IPv6 Timeout** 字段中，输入为 DHCPv6 地址处理预留的时间量（以秒为单位）。值的范围为 1 到 3600 秒。默认值为 60 秒。

步骤 6 在 **DHCP Relay Interface Servers** 区域中，添加要将给定接口上 DHCP 请求中继到的一个或多个接口专用 DHCP 服务器。

- a) 点击 **Add**。系统将显示 **Add DHCP Relay Server** 对话框。
- b) 从 **Interface** 下拉列表中，选择连接到 DHCP 客户端的接口。请注意，如同在全局 DHCP 服务器中，您未为请求指定输出接口；相反，ASA 将使用路由表确定输出接口。
- c) 在 **Server to** 字段中，输入 DHCP 服务器的 IPv4 地址，然后点击 **Add**。服务器已成功添加到右侧列表。添加多达 4 台服务器（如未超过服务器总数上限）。接口专用服务器不支持 IPv6。
- d) 点击 **OK**。

新添加的接口 DHCP 中继服务器将显示在 **DHCP Relay Interface Servers** 列表中。

步骤 7 要将所有接口配置为受信任接口，请选中 **Set dhcp relay information as trusted on all interfaces** 复选框。您也可以选择信任单个接口。

步骤 8 点击应用保存设置。

配置动态 DNS

当接口使用 DHCP IP 寻址时，分配的 IP 地址可以在续约 DHCP 租用时间更改。当需要使用完全限定域名 (FQDN) 访问接口时，更改 IP 地址可能导致 DNS 服务器资源记录 (RR) 失效。动态 DNS (DDNS) 提供一种机制，会在 IP 地址或主机名更改时更新 DNS RR。您还可以将 DDNS 用于静态或 PPPoE IP 寻址。

DDNS 在 DNS 服务器上更新以下 RR：A RR 包括名称到 IP 地址的映射，而 PTR RR 将地址映射到名称。

ASA 支持以下 DDNS 更新方法：

- 标准 DDNS，即标准 DDNS 更新方法由 RFC 2136 定义。

通过此方法，ASA 和 DHCP 服务器使用 DNS 请求更新 DNS RR。ASA 或 DHCP 服务器向其本地 DNS 服务器发送 DNS 请求以获取有关主机名的信息，并根据响应确定拥有 RR 的主 DNS 服务器。然后，ASA 或 DHCP 服务器直接向主 DNS 服务器发送更新请求。请参阅以下典型场景。

- ASA 更新 A RR，而 DHCP 服务器更新 PTR RR。

通常情况下，ASA “拥有” A RR，而 DHCP 服务器 “拥有” PTR RR，因此两个实体需要单独请求更新。当 IP 地址或主机名更改时，ASA 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 PTR RR 更新。

- DHCP 服务器既更新 A，也更新 PTR RR。

如果 ASA 无权更新 A RR，请使用此场景。当 IP 地址或主机名更改时，ASA 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 A 和 PTR RR 更新。

您可以根据安全需求和主 DNS 服务器的要求配置不同的所有权。例如，对于静态地址，ASA 应拥有两个记录的更新。

- Web - Web 更新方法使用使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。

使用此方法，当 IP 地址或主机名更改时，ASA 会直接向您拥有帐户的 DNS 提供商发送 HTTP 请求。



注释 BVI 或网桥组成员接口上不支持使用 DDNS。

开始之前

- 依次选择配置 > 设备管理 > DNS > DNS 客户端 配置 DNS 服务器。请参阅 [配置 DNS 服务器](#)。
- 依次选择配置 > 设备设置 > 设备名称/密码，配置设备主机名和域名。请参阅 [设置主机名、域名及启用密码和 Telnet 密码](#)。如果未指定每个接口的主机名，则使用设备主机名。如果未指定 FQDN，则对于静态或 PPPoE IP 寻址，系统域名或 DNS 服务器域名将附加到主机名之前。

过程

步骤 1 依次选择配置 > 设备管理 > DNS > 动态 DNS。

步骤 2 标准 DDNS 方法：配置 DDNS 更新方法以启用来自 ASA 的 DNS 请求。

如果 DHCP 服务器将执行所有请求，则无需配置 DDNS 更新方法。

- 在更新方法区域中，点击添加。
- 为此方法指定一个名称。
- （可选）配置 DNS 请求之间的更新间隔。默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置天数(0-364)、小时、分钟和秒。
- 依次选择 **DDNS 记录类型 > 标准 DDNS**。
- 在要更新的记录下，指定要 ASA 更新的标准 DDNS 记录。

此设置仅影响您要直接从 ASA 更新的记录；要确定您希望 DHCP 服务器更新的记录，请按接口或全局配置 DHCP 客户端设置。请参见第 [步骤 4](#)，第 [12 页](#) 步。

- **两者（PTR 和 A 记录）**- 将 ASA 设置为同时更新 A 和 PTR RR。使用此选项进行静态或 PPPoE IP 寻址。
- **仅 A 记录**- 将 ASA 设置为仅更新 A RR。如果您希望 DHCP 服务器更新 PTR RR，请使用此选项。

- 点击“确定”。
- 将此方法分配到第 [步骤 4](#)，第 [12 页](#) 步中的接口。

步骤 3 Web 方法：配置 DDNS 更新方法，启用来自 ASA 的 HTTP 更新请求。

- 在更新方法区域中，点击添加。
- 为此方法指定一个名称。
- （可选）配置 DNS 请求之间的更新间隔。默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置天数(0-364)、小时、分钟和秒。
- 依次选择 **DDNS 记录类型 > Web**。
- 在 **Web** 字段中，指定更新 URL。请咨询您的 DNS 提供商，获取所需的 URL。

使用以下语法：

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

示例：

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

- f) 对于 **Web 更新类型**，请指定要更新的地址类型（IPv4 或 IPv6）。
- **两种全部** - (默认) 更新所有 IPv4 和 IPv6 地址。
 - **两者** - 更新 IPv4 地址和最新的 IPv6 地址。
 - **IPv4** - 仅更新 IPv4 地址。
 - **IPv6** - 仅更新最新的 IPv6 地址。
 - **IPv6 全部** - 更新所有 IPv6 地址。
- g) 在引用身份名称中，输入配置用于验证服务器证书身份的引用身份名称。
- h) 点击“确定”。
- i) 将此方法分配到第 [步骤 4，第 12 页](#) 步中的接口。
- j) DDNS 的 Web 类型方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参见第 [步骤 6，第 13 页](#) 步。

步骤 4 配置 DDNS 的接口设置，包括为此接口设置更新方法、DHCP 客户端设置和主机名。

- a) 在动态 **DNS 接口设置** 区域中，点击“添加”。
- b) 从下拉列表中选择接口。
- c) 选择在“更新方法”区域中创建的“方法名称”。
(标准 DDNS 方法) 如果您希望 DHCP 服务器执行所有更新，则无需分配方法。
- d) 为此接口设置主机名。

如果未设置主机名，则会使用设备主机名。如果未指定 FQDN，则会附加系统域名或 DNS 服务器组中的默认域（用于静态或 PPPoE IP 寻址），或附加来自 DHCP 服务器的域名（用于 DHCP IP 寻址）。

- e) 标准 DDNS 方法：配置 **DHCP 服务器记录更新**，以确定希望 DHCP 服务器更新哪些记录。

ASA 将 DHCP 客户端请求发送到 DHCP 服务器。请注意，还必须将 DHCP 服务器配置为支持 DDNS。可以将该服务器配置为满足客户端请求，也可以覆盖客户端（在这种情况下，它将回复客户端，因此客户端也不会尝试执行服务器正在执行的更新）。即使客户端不请求 DDNS 更新，也可以将 DHCP 服务器配置为始终发送更新。

静态或 PPPoE IP 寻址，请忽略这些设置。

注释 还可以在 **动态 DNS** 主页面上为所有接口全局设置这些值。每个接口的设置优先于全局设置。

- **默认 (PTR 记录)** - 请求 DHCP 服务器执行 PTR RR 更新。此设置与启用 **A 记录** 的 DDNS 更新方法配合使用。
- **两者 (PTR 记录和 A 记录)** - 请求 DHCP 服务器同时执行 A 和 PTR RR 更新。此设置不需要将 DDNS 更新方法与接口关联。

- 无 - 请求 DHCP 服务器不执行更新。此设置与同时启用了 **A** 和 **PTR** 记录的 DDNS 更新方法配合一起使用。

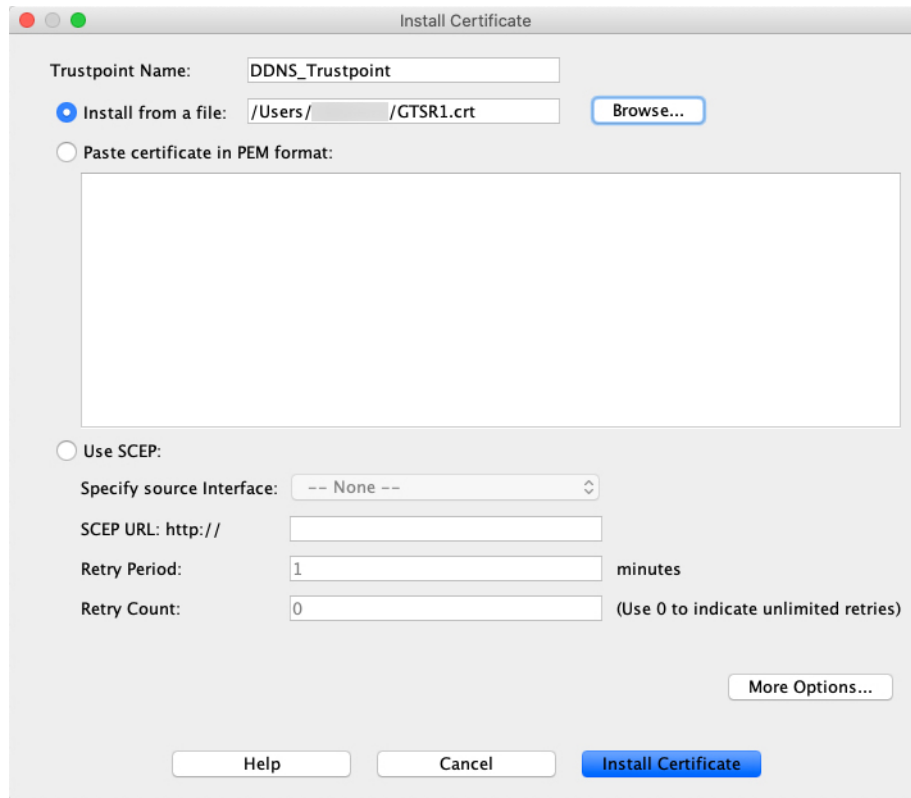
f) 点击“确定”。

步骤 5 点击“应用”保存更改，或点击“重置”放弃更改并输入新的更改。

步骤 6 DDNS 的 Web 方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。

以下示例显示如何将 DDNS 服务器的证书添加为信任点。

- 获取 DDNS 服务器 CA 证书。此程序显示文件导入，但您也可以将其粘贴为 PEM 格式。
- 依次选择配置 > 设备管理 > 证书管理 > CA 证书，然后点击添加。



- 输入信任点名称。
- 点击从文件进行安装，浏览至证书文件。
- 点击 **Install Certificate**。

监控 DHCP 和 DDNS 服务

本节介绍监控 DHCP 和 DDNS 服务的程序。

监控 DHCP 服务

- **监控 > 接口 > DHCP > DHCP 客户端租用信息。**
此窗格显示已配置的 DHCP 客户端 IP 地址。
- **Monitoring > Interfaces > DHCP > DHCP Server Table**
此窗格显示已配置的动态 DHCP 客户端 IP 地址。
- **Monitoring > Interfaces > DHCP > DHCP Statistics**
此窗格显示 DHCPv4 消息类型、计数器、值、方向、接收的消息和发送的消息。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP Relay Statistics**
此窗格显示 DHCPv6 中继消息类型、计数器、值、方向、接收的消息和发送的消息。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP Relay Binding**
此窗格显示 DHCPv6 中继绑定。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP Interface Statistics**
此屏幕显示所有接口的 DHCPv6 信息。如果接口配置用于 DHCPv6 无状态服务器配置（请参阅 [配置 DHCPv6 无状态服务器，第 7 页](#)），则此屏幕将列出该服务器正在使用的 DHCPv6 池。如果接口包含 DHCPv6 地址客户端或前缀委派客户端配置，则此屏幕显示各个客户端的状态，以及从该服务器收到的值。此屏幕还将显示 DHCP 服务器或客户端的消息统计信息。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP HA Statistics**
此屏幕显示故障转移设备之间的事务处理统计信息，包括在 DUID 信息各个设备之间的同步次数。
- **Monitoring > Interfaces > DHCP > IPV6 DHCP Server Statistics**
此屏幕显示 DHCPv6 无状态服务器统计信息。

监控 DDNS 状态

请参阅以下用于监控 DDNS 状态的命令。在 **Tools > Command LineInterface** 上输入命令。

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

此命令显示 DDNS 更新状态。

以下示例显示有关 DDNS 更新方法的详细信息：

```
ciscoasa# show ddns update method ddns1

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

以下示例显示有关 Web 更新方法的详细信息：

```
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>
```

以下示例显示有关 DDNS 接口的信息:

```
ciscoasa# show ddns update interface outside

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

以下示例显示 Web 类型更新成功:

```
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 : asal.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

以下示例显示 Web 类型故障:

```
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
```

以下示例显示 DNS 服务器返回 Web 类型更新错误:

```
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)
```

以下示例显示, 由于 IP 地址未配置或 DHCP 请求失败, 尚未尝试 Web 更新, 例如:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
```

test

not available

Last Update Not attempted

DHCP 和 DDNS 服务的历史记录

功能名称	平台版本	说明
DDNS 支持 Web 更新方法	9.15(1)	您现在可以将接口配置为使用支持 Web 更新方法的 DDNS。 新增/修改的屏幕： 配置 > 设备管理 > DNS > 动态 DNS
VTI 上的 DHCP 中继服务器支持	9.14(1)	ASA 支持将 VTI 接口配置为 DHCP 中继服务器连接接口。 我们修改了以下屏幕，为 DHCP 中继选择 VTI 接口： 配置 > 设备管理 > DHCP > DHCP 中继 > DHCP 中继接口服务器
DHCP 预留	9.13(1)	ASA 支持 DHCP 预留。根据客户端的 MAC 地址从定义的地址池中将一个静态 IP 地址分配给 DHCP 客户端。 我们未修改任何 ASDM 屏幕。
IPv6 DHCP	9.6(2)	ASA 现在支持 IPv6 寻址的以下功能： <ul style="list-style-type: none"> • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - ASA 从 DHCPv6 服务器获取指定的前缀。然后，ASA 可使用这些前缀来配置其他 ASA 接口地址，以使无状态地址自动配置 (SLAAC) 客户端可在同一网络上自动配置 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会向它们提供域名等其他信息。ASA 仅接受 IR 数据包，不向客户端分配地址。 <p>引入或修改了以下菜单项：</p> <p>配置 > 设备设置 > 接口设置 > 接口 > 添加接口 > IPv6</p> <p>配置 > 设备管理 > DHCP > DHCP 池</p> <p>配置 > 设备设置 > 路由 > BGP > IPv6 系列 > 网络</p> <p>监控 > 接口 > DHCP</p>
DHCPv6 监控	9.4(1)	现在，可以监控适用于 IPv6 的 DHCP 统计信息和适用于 IPv6 的 DHCP 绑定。 引入了以下屏幕： DHCPv6 monitoring Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics ; Monitoring > Interfaces > DHCP > IPV6 DHCP Binding 。

功能名称	平台版本	说明
DHCP 中继服务器验证 DHCP 服务器标识符是否存在应答	9.2(4) 9.3(3)	如果 ASA DHCP 中继服务器收到来自错误的 DHCP 服务器的应答，现在它会验证该应答是否来自正确的服务器，然后对应答做出反应。未引入或修改任何命令。未修改任何 ASDM 屏幕。 未修改任何 ASDM 屏幕。
DHCP 重新绑定功能	9.1(4)	在 DHCP 重新绑定阶段，客户端会尝试重新绑定到隧道组列表中的其他 DHCP 服务器。在此版本之前，当 DHCP 租约未能更新时，客户端不会重新绑定到备用服务器。 未修改任何 ASDM 屏幕。
DHCP 受信任接口	9.1(2)	现可将接口配置为受信任接口，以保留 DHCP 选项 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探测和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 giaddr 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。 修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
每个接口的 DHCP 中继服务器（仅限 IPv4）	9.1(2)	现在可以配置单个接口的 DHCP 中继服务器，因此仅将进入指定接口的请求中继给为该接口指定的服务器。每接口 DHCP 中继不支持 IPv6。 我们修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
适用于 IPv6 的 DHCP 中继 (DHCPv6)	9.0(1)	添加了 DHCP 中继对 IPv6 的支持。 我们修改了以下屏幕：Configuration > Device Management > DHCP > DHCP Relay。
DDNS	7.0(1)	引入了此功能。 引入了以下屏幕： Configuration > Device Management > DNS > DNS Client。配置 > 设备管理 > DNS > 动态 DNS。
DHCP	7.0(1)	ASA 可向连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器或 DHCP 中继服务。 我们引入了以下屏幕： Configuration > Device Management > DHCP > DHCP Relay。 Configuration > Device Management > DHCP > DHCP Server。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。