DHCP 和 DDNS

以下主题介绍 DHCP 和 DDNS 服务以及如何在威胁防御设备上配置这些服务。

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。Firewall 威胁防御设备 可以为连接到 Firewall 威胁防御设备 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 上已配置这两个选项，则 Firewall 威胁防御 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，可以通过定义 DHCP IPv6 池并将其分配给 DHCPv6 服务器来配置 Firewall Threat Defense，以便在它们向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall 威胁防御设备 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 Firewall 威胁防御设备 的接口，以将 DHCP 请求转发至另一接口上的 DHCP 服务器。

DHCP 和 DDNS 的要求和前提条件

型号支持

Firewall Threat Defense

用户角色

- 管理员
- 访问管理员
- 网络管理员

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。

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。
- 您可以在具有名称和 IP 地址的任何接口（例如物理接口、子接口或路由模式下的 BVI）上配置 DHCP 服务器。
- 对于使用 DHCP 或 PPPoE 获取其地址的接口，请勿选择作为 DHCP 服务器接口。
- 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。

- Firewall Threat Defense 不支持 DHCP 中继服务器背后的 DHCP 客户端；客户端必须直接连接到 Firewall Threat Defense。
- 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

- 每个虚拟路由最多可以配置 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。
- 每个虚拟路由 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。
- 对于使用 DHCP 或 PPPoE 获取其地址的接口，请勿选择作为 DHCP 中继接口。
- 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 Firewall Threat Defense，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 DCHP 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 Firewall Threat Defense 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，Firewall Threat Defense支持来自另一个中继服务器的数据包。
- DHCP 客户端必须与 Firewall Threat Defense 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。

DDNS 服务

防火墙的 DDNS 仅支持 DynDNS 服务。因此，请确保使用以下语法中的更新 URL 配置 DDNS：

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

配置 DHCPv4 服务器

请参阅以下步骤来配置 DHCPv4 服务器。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择 **DHCP > DHCP 服务器**。

步骤 3 配置以下 DHCP 服务器选项：

- **Ping 超时** - Firewall Threat Defense设备等待 DHCP ping 尝试超时的时间量（以毫秒为单位）。值的范围为 10 到 10000 毫秒。默认值为 50 毫秒。

  为避免地址冲突，Firewall Threat Defense设备会向一个地址发动两个 ICMP ping 数据包，然后再将该地址分配给 DHCP 客户端。

- **租赁时长** - 客户端在租赁到期前可以使用其已分配的 IP 地址的时间量（以秒为单位）。值的范围为 300 到 1048575 秒。默认值为 3600 秒（1 小时）。

- （路由模式）**自动配置** - 在 Firewall Threat Defense设备上启用 DHCP 自动配置。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。否则，可以禁用自动配置，并在第 4 步自行添加值。

- （路由模式）**接口** - 指定用于自动配置的接口。 对于具有虚拟路由功能的设备，此接口只能是全局虚拟路由器接口。

步骤 4 要覆盖自动配置的设置，请进行以下操作：

- 输入接口的域名：例如，您的设备可能位于 Your_Company 域中。
- 从下拉列表中，选择为该接口配置的 DNS 服务器（主服务器和辅助服务器）。要添加新的 DNS 服务器，请参阅创建网络对象。
- 从下拉列表中，选择为该接口配置的 WINS 服务器（主服务器和辅助服务器）。要添加新的 WINS 服务器，请参阅创建网络对象。

步骤 5 选择 **服务器**，点击 **添加**，然后配置以下选项：

- **接口** -- 从下拉列表中选择接口。在透明模式下，指定命名桥接组成员接口。 在路由模式下，请指定一个命名路由接口或命名 BVI；请勿指定桥接组成员接口。请注意，还必须指定 BVI 每个桥接组成员接口才能使 DHCP 服务器运行。
- **地址池** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。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。
- **启用 DHCP 服务器** - 在所选接口上启用 DHCP 服务器。

步骤 6 点击**确定** 以保存 DHCP 服务器配置。

步骤 7 （可选）选择 **高级**，点击 **添加**，然后指定希望该选项返回到 DHCP 客户端的信息的类型：

- **选项代码** - Firewall Threat Defense设备支持 RFC 2132、RFC 2562 和 RFC 5510 中列出的 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。有关 DHCP 选项代码的更多信息，请参阅关于 DHCPv4 服务器 ， 第 1 页。

  注释
  Firewall Threat Defense设备不会验证您提供的选项类型和值是否与 RFC 2132 中定义的选项代码的预期类型和值匹配。有关选项代码及其关联的类型和期望值的详细信息，请参阅 RFC 2132。

- **类型** - DHCP 选项类型。可用选项包括 **IP**、**ASCII** 和 **十六进制**。如果选择了“IP”，则必须在“IP 地址”字段中添加 IP 地址。如果选择了“ASCII”，则必须在“ASCII”字段中添加 ASCII 值。如果选择了“十六进制”，则必须在“十六进制”字段中添加十六进制值。
- **IP 地址 1** 和 **IP 地址 2** - 要通过此选项代码返回的 IP 地址。要添加新的 IP 地址，请参阅创建网络对象。
- **ASCII** - 将返回到 DHCP 客户端的 ASCII 值。字符串不能包含空格。
- **十六进制** - 将返回到 DHCP 客户端的十六进制值。该字符串的位数必须是偶数，并且不含空格。您无需使用 0x 前缀。

步骤 8 点击**确定** 以保存选项代码配置。

步骤 9 在“DHCP”页面上点击**保存**，以保存更改。

步骤 10 要查看 DHCP 绑定，请使用以下命令。

show dhcpd binding

示例：

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

配置 DHCPv6 无状态服务器

对于结合前缀授权功能使用无状态地址自动配置 (SLAAC) 的客户端，可以配置 Firewall Threat Defense 以在它们向 Firewall Threat Defense发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。

创建 DHCP IPv6 池

创建用于 DHCPv6 服务器的 DHCP IPv6 池。DHCPv6 服务器会在向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器和域名等信息。DHCP IPv6 池会定义要在 IR 消息中发送的参数。

此功能仅支持路由模式。此功能不支持集群或高可用性。

过程

步骤 1 选择**对象 (Objects)** > **DHCP IPv6 池 (DHCP IPv6 Pool)**。

步骤 2 请点击 添加 ()。

步骤 3 配置 **DNS 服务器 (DNS Server)** 和**域名 (Domain Name)**。

您可以手动定义值并点击**添加 (Add)**，或者您可以选中**导入 (Import)** 使用 Firewall Threat Defense 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使用**导入 (Import)** 配置的参数不能相同。

图 *1:* 手动定义值

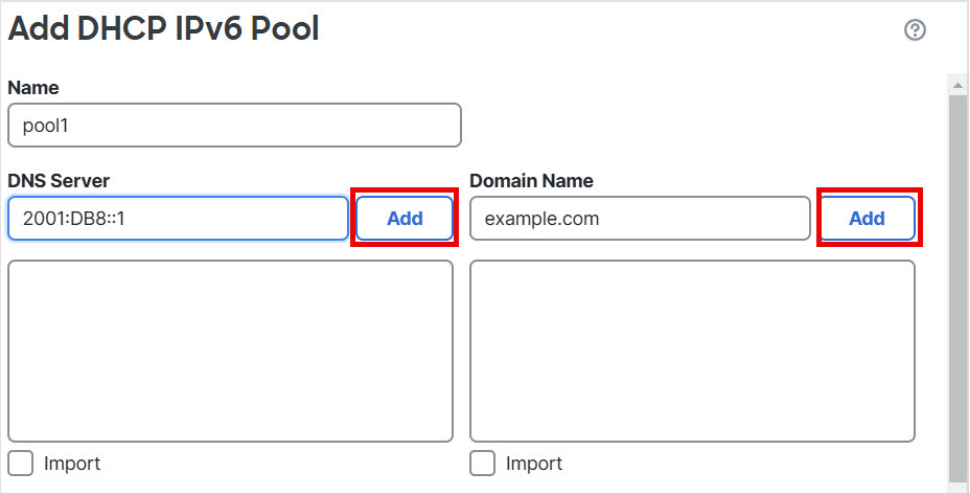
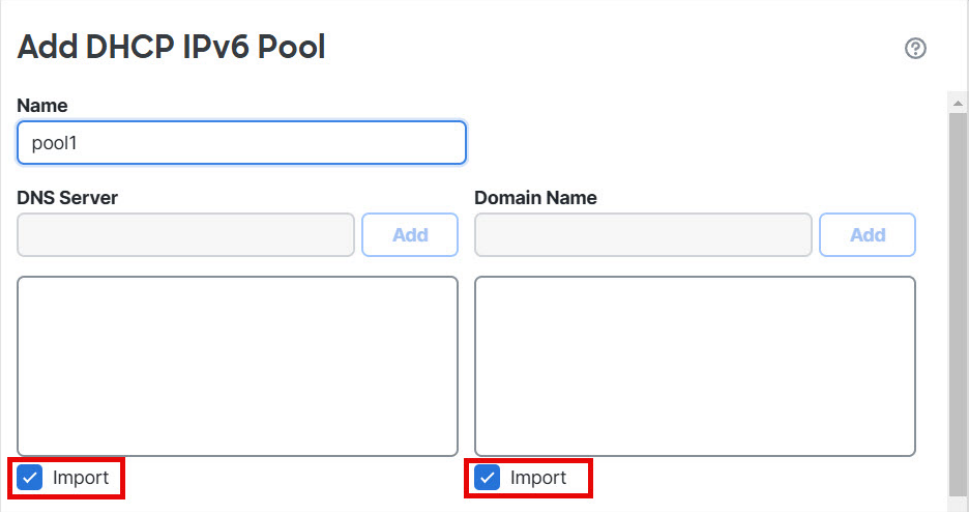


图 *2:* 导入值



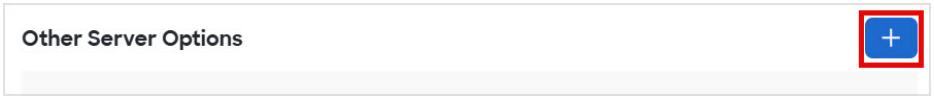
步骤 4 定义**其他服务器选项 (Other Server Options)**。

您可以为以下服务器定义域名和 IP 地址：

- NIS
- NISP
- SIP
- SNTP

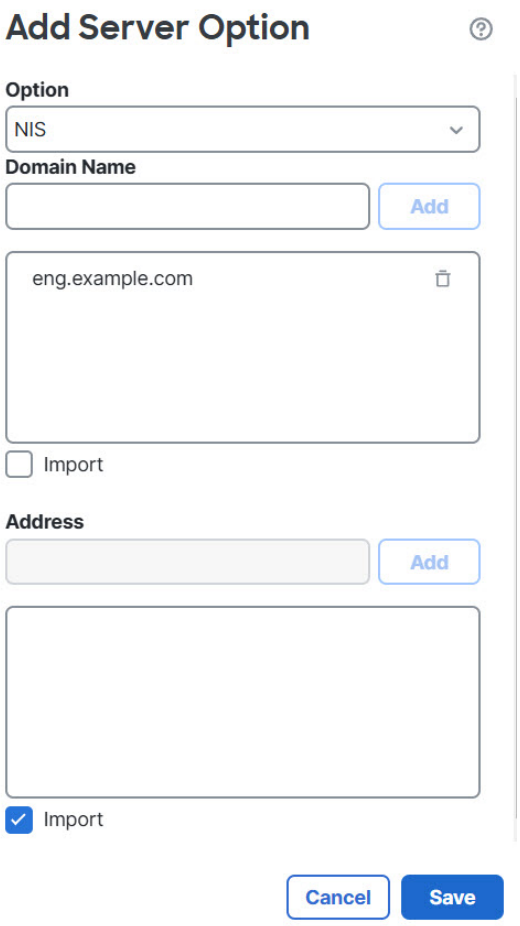
a) 请点击 添加 (+)。

图 3: 其他服务器选项



b) 在选项 (Option) 下选择服务器类型，然后手动定义域名 (Domain Name) 和地址 (Address)，或者选中导入 (Import)。

图 4: 定义服务器域名和地址



导入 (Import) 使用 Firewall Threat Defense 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使用导入 (Import) 配置的参数不能相同。

c) 点击保存。

d) 对每个服务器类型重复上述步骤。

步骤 5 点击保存。

步骤 6 将此池与 DHCPv6 服务器配合使用。请参阅启用 DHCPv6 无状态服务器，第 9 页。

启用 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，可以配置 Firewall Threat Defense 以在它们向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。Firewall Threat Defense 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 Firewall Threat Defense 的前缀。

此功能仅支持路由模式。此功能不支持集群或高可用性。

开始之前

添加 DHCP IPv6 池对象。请参阅创建 DHCP IPv6 池，第 6 页。此对象定义 IR 消息中包含的服务器参数。

过程

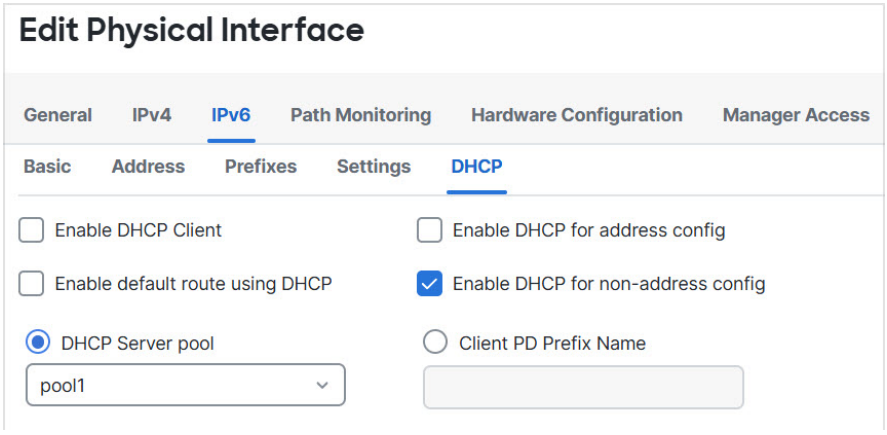
步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6** 页面，然后点击 **DHCP**。

步骤 4 点击 **DHCP 服务器池 (DHCP Server Pool)**，然后选择您之前创建的对象。

图 *5:* 启用 ***DHCPv6*** 服务器



步骤 5 选中**为非地址配置启用 DHCP (Enable DHCP for non-address config)** 以通知 SLAAC 客户端有关 DHCPv6 服务器的信息。

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 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 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 Firewall Threat Defense 设备进行转发，因为它不转发广播流量。

您可以通过配置接收广播来将 DHCP 请求转发到另一个接口上 DHCP 服务器的 Firewall Threat Defense 设备接口来对此情况做出补救。

注释 在透明防火墙模式下不支持 DHCP 中继。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **DHCP** > **DHCP 中继**。

步骤 3 在 **IPv4 中继超时 IPv6 中继超时** 字段中，输入 Firewall Threat Defense 设备等待 DHCP 中继代理超时的时间（以秒为单位）。值的范围为 1 到 3600 秒。默认值为 60 秒。

超时用于通过本地 DHCP 中继代理进行的地址协商。

步骤 4 （可选） 选中 **信任所有信息** ，将所有客户端接口设置为受信任。

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 Firewall Threat Defense DHCP 中继代理接收到一个已设置选项 82 的 DHCP 数据包，但是 giaddr 字段（在将数据包转发到服务器之前，指定由中继代理设置的 DHCP 中继代理地址）设置为 0，则 Firewall Threat Defense 默认丢弃该数据包。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。

步骤 5 在 **DHCP 中继代理**上，点击**添加**，并配置以下选项：

- **接口** - 连接到 DHCP 客户端的接口。
- **启用 IPv4 中继** - 为该接口启用 IPv4 DHCP 中继。

- **设置路由** - （对于 IPv4）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 Firewall Threat Defense设备接口的地址，该客户端中继原始 DHCP 请求。通过此操作，客户端可以将其默认路由设置为指向 Firewall Threat Defense设备，即使 DHCP 服务器指定了另一个路由器也如此。如果数据包内无默认路由器选项，则 Firewall Threat Defense设备将添加一个包含接口地址的选项。
- **启用 IPv6 中继** - 为该接口启用 IPv6 DHCP 中继。

步骤 6 点击**确定**，保存 DHCP 中继代理更改。

步骤 7 在 **DHCP 服务器 (DHCP Servers)** 上，点击**添加 (Add)**，并配置以下选项：

将 IPv4 和 IPv6 服务器地址添加为单独的条目，即使它们属于同一台服务器亦是如此。

- **服务器** - DHCP 服务器的 IP 地址。从该下拉列表中选择一个 IP 地址。要添加新的 IP 地址，请参阅 创建网络对象
- **接口** - 指定的 DHCP 服务器连接到的接口。DHCP 中继代理和 DHCP 服务器不能配置在同一接口上。

步骤 8 点击**确定**，保存 DHCP 服务器更改。

步骤 9 在“DHCP”页面上点击**保存**，以保存更改。

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。

Firewall Threat Defense 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，Firewall Threat Defense 和 DHCP 服务器使用 DNS 请求更新 DNS RR。Firewall Threat Defense 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，Firewall Threat Defense 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。

  - Firewall Threat Defense 更新 A RR，而 DHCP 服务器更新 PTR RR。

    通常情况下，Firewall Threat Defense“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，Firewall Threat Defense 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 Firewall Threat Defense 无权更新 A RR，请使用此场景。当 IP 地址或主机名更改时，Firewall Threat Defense 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，Firewall Threat Defense 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，Firewall Threat Defense 会直接向您拥有帐户的 DNS 提供商发送 HTTP 请求。

注释 对于从外部接口使用 零接触调配 注册的设备，使用“fmcOnly”方法自动启用 DDNS，该方法类似于 Web 方法。此方法仅适用于 零接触调配 设备。您可以使用此屏幕编辑此方法的某些选项，或删除该方法并配置其他方法。有关 零接触调配 的详细信息，请参阅使用序列号添加设备（零接触调配） - 基本配置。

DDNS 页面还支持设置与 DDNS 相关的 DHCP 服务器设置。

注释 BVI 或网桥组成员接口上不支持使用 DDNS。

开始之前

- 在 **对象** > **DNS 服务器组**上配置 DNS 服务器组，然后为 **设备** > **平台设置**上的接口启用该组，创建或编辑威胁防御策略并点击 **DNS**。请参阅DNS。
- 配置设备主机名。您可以在执行 Firewall Threat Defense 初始设置时配置主机名，也可以使用 **configure network hostname** 命令配置主机名。如果未指定每个接口的主机名，则使用设备主机名。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **DHCP** > **DDNS**.

步骤 3 标准 DDNS 方法： 配置 DDNS 更新方法以启用来自 Firewall Threat Defense 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。

a) 在 **DDNS 更新方法**上，点击 **添加**。
b) 设置 **方法名称**。
c) 点击 **DDNS**。

d) （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**。

e) 设置您希望 Firewall Threat Defense 更新的**更新记录**。

此设置仅影响您要直接从 Firewall Threat Defense 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。请参阅步骤 5，第 13 页。

- **未定义 (Not Defined)** - 未从 Firewall Threat Defense 禁用 DNS 更新。
- **A 和 PTR 两者记录 (Both A and PTR Records)** - 将 Firewall Threat Defense 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。
- **A 记录 (A Records)** - 将 Firewall Threat Defense 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。

f) 点击**确定**。

g) 将此方法分配在 步骤 5，第 13 页 中的接口。

步骤 4 Web 方法：配置 DDNS 更新方法，启用来自 Firewall Threat Defense 的 HTTP 更新请求。

a) 在 **DDNS 更新方法**上，点击 **添加**。

b) 设置 **方法名称**。

c) 点击 **Web**。

d) 设置 **Web 更新类型** 以更新 IPv4 和/或 IPv6 地址类型。

e) 设置 **Web URL**。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://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) （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**。

g) 点击**确定**。

h) 将此方法分配在 步骤 5，第 13 页 中的接口。

i) 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。请参阅步骤 9，第 15 页。

步骤 5 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 **DDNS 接口设置**上，点击 **添加**。

b) 从下拉列表中选择**接口**。

c) 选择在 **DDNS 更新方法** 页面中创建的 **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) 设置此接口的 **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 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 客户端请求 DHCP 服务器以更新请求**，以确定希望 DHCP 服务器更新哪些记录。

Firewall Threat Defense 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）。

静态或 PPPoE IP 寻址，请忽略这些设置。

注释
还可以在 **DDNS** 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。

- **未选择**-禁用对 DHCP 服务器的 DDNS 请求。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。
- **无更新**-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。
- **仅 PTR**-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。使用此设置启用 DHCP 选项 81。
- **A 和 PTR 两者记录**-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。

f) 点击**确定**。

注释
当您在 Firewall Threat Defense 上启用 DHCP 服务器时， **动态 DNS 更新 (Dynamic DNS Update)** 设置与 DHCP 服务器设置相关。有关详细信息，请参阅步骤 6，第 14 页。

步骤 6 如果在 Firewall Threat Defense 上启用 DHCP 服务器，则可以为 DDNS 配置 DHCP 服务器设置。

要启用 DHCP 服务器，请参阅 配置 DHCPv4 服务器，第 4 页）。您可以配置 DHCP 客户端使用标准 DDNS 更新方法时的服务器行为。如果服务器执行任何更新，则如果客户端租约到期（且未续约），则服务器将请求 DNS 服务器删除其负责的 RR。

a) 您可以全局或按接口配置服务器设置。有关全局设置，请参阅 **DDNS** 主页。有关每个接口的设置，请参阅 **DDNS接口设置** 页面。接口的设置优先于全局设置。
b) 配置您希望 DHCP 服务器在 **动态 DNS 更新**下更新的 DNS RR。

- **未选定**-未禁用 DDNS 更新，即使客户端请求也是如此。
- **仅 PTR**-启用 DDNS 更新。如果启用 **覆盖 DHCP 客户端请求** 设置，则服务器将仅更新 PTR RR。否则，服务器将更新客户端请求的 RR。如果客户端未使用 FQDN 选项发送更新请求，则服务器将使用 DHCP 选项 12 中发现的主机名请求 A 和 PTR RR 的更新。
- **A 和 PTR 两者记录**-启用 DDNS 更新。如果启用 **覆盖 DHCP 客户端请求** 设置，则服务器将同时更新 A 和 PTR RR。否则，服务器将更新客户端请求的 RR。如果客户端未使用 FQDN 选项发送更新请求，则服务器将使用 DHCP 选项 12 中发现的主机名请求 A 和 PTR RR 的更新。

c) 要覆盖 DHCP 客户端请求的更新操作，请选中 **覆盖 DHCP 客户端请求**。

服务器会回复客户端，表示请求被覆盖了，所以客户端不会同时尝试执行服务器正在执行的更新。

步骤 7 （可选）配置常规 DHCP 客户端设置。这些设置与 DDNS 不相关，但与 DHCP 客户端的行为相关。

a) 在 **DDNS** 页面上，选中 **启用 DHCP 客户端广播** 以请求 DHCP 服务器广播 DHCP 应答（DHCP 选项 1）。

b) 要强制将 MAC 地址存储在选项 61 的 DHCP 请求数据包中而不是默认内部生成的字符串中，请在 **DDNS** > **DHCP 客户端 ID 接口**，从 **可用接口** 列表中选择接口，然后点击 **添加** 将其移动到 **选定的接口** 列表。

某些 ISP 期望选项 61 成为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。此设置与 DDNS 不直接相关，而是常规 DHCP 客户端设置。

步骤 8 点击设备页面上的 **保存** 以保存更改。

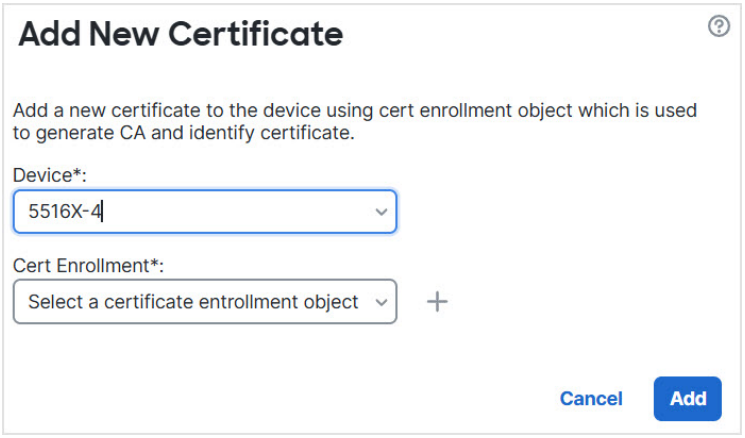
步骤 9 DDNS 的 Web 方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。

以下示例显示如何将 DDNS 服务器的证书添加为信任点。

a) 获取 DDNS 服务器 CA 证书。此程序显示使用 PEM 格式的手动导入，但您也可以使用 PKCS12。

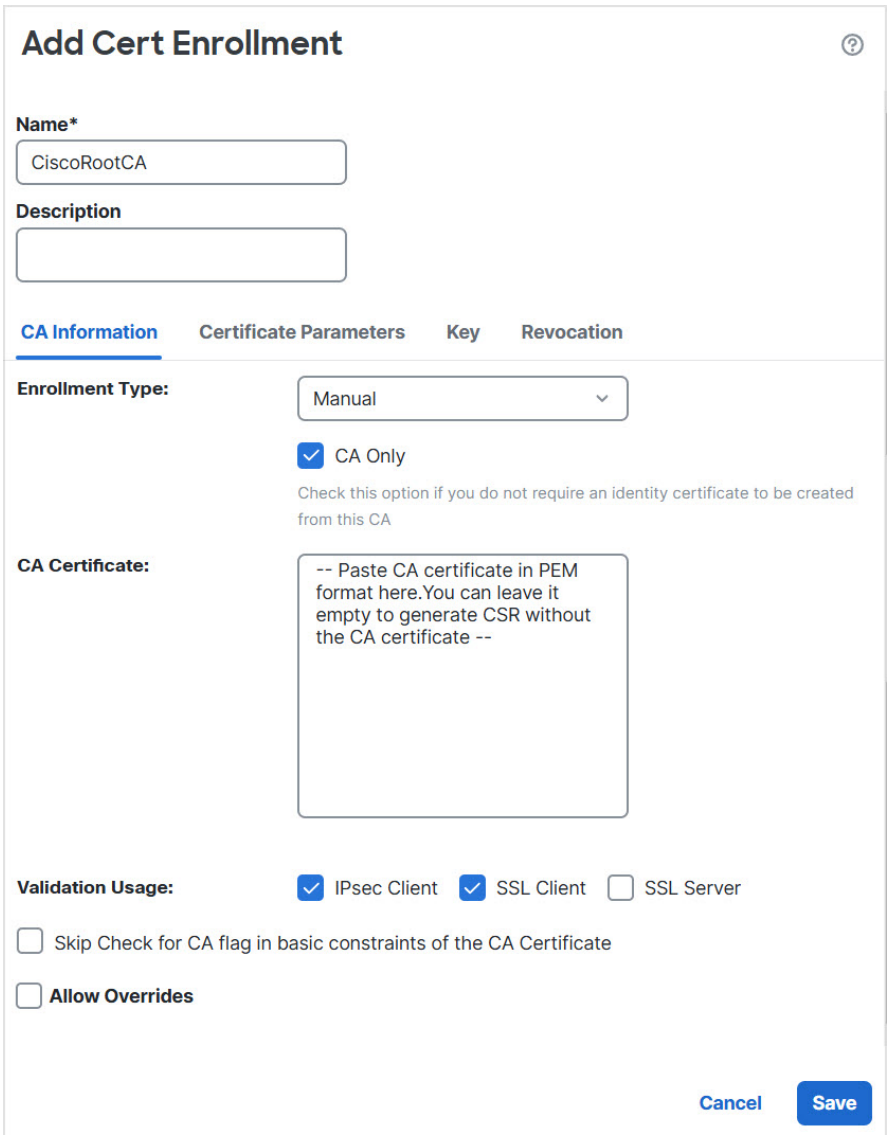
b) 在防火墙管理中心，选择**设备** > **证书**，然后点击**添加**。

c) 选择 **设备**，点击 **添加** (+)。



系统将显示**添加证书注册 (Add Cert Enrollment)** 对话框。

d) 输入以下字段值，然后点击 **保存**。



- 输入 **Name**。
- 选择 **注册类型** > **手动**。
- 点击 **仅 CA**。
- 从步骤 9.a，第 15 页粘贴 CA 文本。

e) 点击**保存**。

DHCP 和 DDNS 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
从防火墙管理中心 Web 界面配置 DHCP 中继受信任接口。	7.2.6/7.4.1	任意	**升级影响。升级后重新设置任何相关的 FlexConfig。** 现在，您可以使用防火墙管理中心 Web 界面将接口配置为受信任接口，以保留 DHCP 选项 82。如果执行此操作，这些设置将覆盖任何现有的 FlexConfig，但您应将其删除。 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 Firewall Threat Defense DHCP 中继代理接收到一个已设置选项 82 的 DHCP 数据包，但是 giaddr 字段（在将数据包转发到服务器之前，指定由中继代理设置的 DHCP 中继代理地址）设置为 0，则 Firewall Threat Defense 默认丢弃该数据包。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。 新增/修改的菜单项：**设备 (Devices)** > **设备管理 (Device Management)** > **添加/编辑设备 (Add/Edit Device)** > **DHCP** > **DHCP 中继 (DHCP Relay)**
DHCPv6 无状态服务器	7.3.0	7.3.0	使用 DHCPv6 前缀委派客户端时，Firewall Threat Defense 现在支持轻型 DHCPv6 无状态服务器。当 SLAAC 客户端向 Firewall Threat Defense 发送信息请求 (IR) 数据包时，Firewall Threat Defense 会向它们提供域名等其他信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加/编辑接口 (Add/Edit Interfaces)** > **IPv6** > **DHCP** • **对象 (Objects)** > **对象管理 (Object Management)** > **DHCP IPv6 池 (DHCP IPv6 Pool)** 新增/修改的命令：**show ipv6 dhcp**

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。

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。

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。