VPN 的 IP 地址

配置 IP 地址分配策略

ASA 可使用以下一种或多种方法将 IP 地址分配给远程访问客户端。如已配置多种地址分配方法，则 ASA 将搜索每一个选项，直到找到一个 IP 地址为止。默认情况下，所有方法均已启用。

- 使用身份验证服务器 - 从外部身份验证、授权和记账服务器逐个用户检索 IP 地址。如果使用已配置 IP 地址的身份验证服务器，建议使用此方法。您可以在“配置”>“AAA 设置”窗格中配置 AAA 服务器。此方法适用于 IPv4 和 IPv6 分配策略。
- 使用 DHCP - 从 DHCP 服务器获取 IP 地址。如要使用 DHCP，则必须配置 DHCP 服务器。还必须定义 DHCP 服务器可使用的 IP 地址范围。如果使用 DHCP，请在 Configuration > Remote Access VPN > DHCP Server 窗格中配置服务器。此方法适用于 IPv4 分配策略。
- **使用内部地址池** - 内部配置的地址池是分配地址池以进行配置的最简单方法。如果使用此方法，请在 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools 窗格中配置 IP 地址池。此方法适用于 IPv4 和 IPv6 分配策略。
  - 允许释放 IP 地址一段时间之后对其重新使用 - 在 IP 地址返回到地址池之后，延迟一段时间方可重新使用。增加延迟有助于防止防火墙在快速重新分配 IP 地址时遇到的问题。默认情况下，已取消选中该选项，表示 ASA 不会强制执行延迟。如果需要延迟，请选中此框并输入取值范围为 1 至 480 的分钟数，以便延迟 IP 地址重新分配。此配置元素适用于 IPv4 分配策略。

使用以下方法之一指定将 IP 地址分配给远程访问客户端的方法。

配置 IP 地址分配选项

过程

步骤 1 依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址分配 (Address Assignment)** > **分配策略 (Assignment Policy)**

步骤 2 在 IPv4 Policy 区域中，选中相应地址分配方法即表示启用，取消选中即表示禁用。默认情况下，这些方法已启用：

- Use Authentication server。启用已配置的身份验证、授权和记帐 (AAA) 服务器，以提供 IP 地址。
- Use DHCP。启用已配置的动态主机配置协议 (DHCP) 服务器，以提供 IP 地址。
- 使用内部地址池：启用在 ASA 上配置的本地地址池。

如果启用 **Use internal address pools**，则也可在释放 IPv4 地址之后对其重新使用。可指定 0 至 480 分钟的时间范围，经过此时间范围，就可重新使用 IPv4 地址。

步骤 3 在 IPv6 Policy 区域中，选中相应地址分配方法即表示启用，取消选中即表示禁用。默认情况下，这些方法已启用：

- Use Authentication server。启用已配置的身份验证、授权和记帐 (AAA) 服务器，以提供 IP 地址。
- 使用内部地址池：启用在 ASA 上配置的本地地址池。

步骤 4 单击**应用 (Apply)**。

步骤 5 点击**确定 (OK)**。

查看地址分配方法

过程

依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址分配 (Address Assignment)** > **分配策略 (Assignment Policy)**。

配置本地 IP 地址池

如要配置 VPN 远程访问隧道的 IPv4 或 IPv6 地址池，请打开 ASDM 并依次选择 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址管理 (Address Management)** > **地址池 (Address Pools)** > **添加/编辑 IP 池 (Add/Edit IP Pool)**。如要删除地址池，请打开 ASDM 并依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络**

（客户端）访问 **(Network [Client] Access) > 地址管理 (Address Management) > 地址池 (Address Pools)**。选择要删除的地址池，然后点击**删除 (Delete)**。

ASA 根据连接配置文件或连接的组策略使用地址池。地址池的指定顺序非常重要。如果为连接配置文件或组策略配置了多个地址池，则 ASA 将按您向 ASA 添加地址池的顺序使用地址池。

如果从非本地子网分配地址，我们建议添加位于子网边界的地址池，从而可更轻松地添加这些网络的路由。

配置本地 IPv4 地址池

IP Pool 区域按名称显示已配置的地址池及其 IP 地址范围，例如：10.10.147.100 至 10.10.147.177。如果地址池不存在，该区域为空。ASA 按所列顺序使用这些地址池：如果第一个地址池中的所有地址已分配，则使用下一个地址池，以此类推。

如果从非本地子网分配地址，我们建议添加位于子网边界的地址池，从而可更轻松地添加这些网络的路由。

过程

步骤 1 依次选择**配置 (Select Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 地址分配 (Address Assignment) > 地址池 (Address Pools)**。

步骤 2 要添加 IPv4 地址，请依次点击**添加 (Add) > IPv4 地址池 (IPv4 Address pool)**。如要编辑现有地址池，请选择地址池表中的地址池，然后点击**编辑 (Edit)**。

步骤 3 在 Add/Edit IP Pool 对话框中输入以下信息：

- Pool Name - 输入地址池的名称。最多可包含 64 个字符
- Starting Address - 输入每个已配置地址池中可用的第一个 IP 地址。使用点分十进制表示法，例如：10.10.147.100。
- Ending Address - 输入每个已配置地址池中可用的最后一个 IP 地址。使用点分十进制表示法，例如：10.10.147.177。
- Subnet Mask - 标识此 IP 地址池所属的子网。

步骤 4 单击**应用 (Apply)**。

步骤 5 点击**确定 (OK)**。

配置本地 IPv6 地址池

IP Pool 区域按名称显示已配置的地址池，及其起始 IP 地址范围、地址前缀和可在地址池中配置的地址数量。如果地址池不存在，该区域为空。ASA 按所列顺序使用这些地址池：如果第一个地址池中的所有地址已分配，则使用下一个地址池，以此类推。

如果从非本地子网分配地址，我们建议添加位于子网边界的地址池，从而可更轻松地添加这些网络的路由。

过程

步骤 1 依次选择**配置 (Select Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **地址分配 (Address Assignment)** > **地址池 (Address Pools)**。

步骤 2 要添加 IPv6 地址，请依次点击**添加 (Add)** > **IPv6 地址池 (IPv6 Address pool)**。如要编辑现有地址池，请选择地址池表中的地址池，然后点击**编辑 (Edit)**。

步骤 3 在 Add/Edit IP Pool 对话框中输入以下信息：

- Name - 显示每个已配置地址池的名称。

  Starting IP Address - 输入已配置地址池中可用的第一个 IP 地址。例如：2001:DB8::1。

- Prefix Length - 输入 IP 地址前缀长度（位数）。例如，32 代表 CIDR 表示法中的 /32。前缀长度定义 IP 地址池所属的子网。

- Number of Addresses — 标识地址池中从起始 IP 地址开始的 IPv6 地址的数量。

步骤 4 单击**应用 (Apply)**。

步骤 5 点击**确定 (OK)**。

将内部地址池分配给组策略

在 Add or Edit Group Policy 对话框中，可为正在添加或修改的内部网络（客户端）访问组策略指定地址池、隧道协议、过滤器、连接设置和服务器。对于此对话框中的每一个字段，如果选中 Inherit 复选框，则相应的设置将从默认组策略获取其值。Inherit 是此对话框中所有属性的默认值。

可为同一个组策略同时配置 IPv4 和 IPv6 地址池。如果在同一个组策略中配置了两个版本的 IP 地址，则配置了 IPv4 的客户端将获得 IPv4 地址，配置了 IPv6 的客户端将获得 IPv6 地址，而同时配置了 IPv4 和 IPv6 地址的客户端将获得 IPv4 和 IPv6 地址。

过程

步骤 1 使用 ASDM 连接至 ASA，并依次选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 组策略 (Group Policies)**。

步骤 2 创建新的组策略或要使用内部地址池配置的组策略，然后点击 Edit。

默认情况下，会在“组策略”(Group Policy) 对话框中选择“常规属性”(General attributes) 窗格。

步骤 3 使用 Address Pools 字段指定该组策略的 IPv4 地址池。点击“选择”(Select) 以添加或编辑 IPv4 地址池。

步骤 4 使用 IPv6 Address Pools 字段指定要用于此组策略的 IPv6 地址池。点击“选择”(Select) 以添加或编辑 IPv6 地址池。

步骤 5 点击**确定**。

步骤 6 点击**应用**。

配置 DHCP 寻址

如要使用 DHCP 为 VPN 客户端分配地址，必须首先配置 DHCP 服务器和 DHCP 服务器可使用的 IP 地址范围。然后根据连接配置文件定义 DHCP 服务器。或者，也可在与连接配置文件或用户名关联的组策略中定义 DHCP 网络范围。

以下示例为名为 **firstgroup** 的连接配置文件定义为 172.33.44.19 的 DHCP 服务器。该示例还为名为 **remotegroup** 的组策略将 DHCP 网络范围定义为 10.100.10.1。（名为 remotegroup 的组策略与名为 firstgroup 的连接配置文件关联）。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

开始之前

您只能使用 IPv4 地址标识要分配客户端地址的 DHCP 服务器。此外，DHCP 选项不会转发给用户，他们只会收到地址分配。

过程

步骤 1 配置 DHCP 服务器。

无法使用 DHCP 服务器将 IPv6 地址分配给 Secure Client。

a) 确认已在**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > > **地址分配 (Address Assignment)** > **分配策略 (Assignment Policy)** 中启用 DHCP。

b) 通过选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **DHCP 服务器 (DHCP Server)** 来配置 DHCP 服务器。

步骤 2 在连接配置文件中定义 DHCP 服务器。

a) 选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **安全客户端 (Secure Client) 连接配置文件 (Connection Profiles)**。

b) 在“连接配置文件”(Connection Profiles) 区域中，点击**添加 (Add)** 或**编辑 (Edit)**。

c) 在连接配置文件的配置树中，点击**基本 (Basic)**。

d) 在 Client Address Assignment 区域中，输入要用于向客户端分配 IP 地址的 DHCP 服务器的 IPv4 地址。例如：**172.33.44.19**。

步骤 3 编辑与连接配置文件关联的组策略，以定义 DHCP 范围。

a) 选择**配置 (Configuration**） > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

b) 双击要编辑的组策略。
c) 在配置树中点击**服务器 (Server)**。
d) 通过点击向下箭头，展开**更多选项 (More Options)** 区域。
e) 取消选中 DHCP 范围**继承**并定义 DHCP 范围。

如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。

如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

要指定范围，请输入与所需池位于同一子网上但不在池内的可路由地址。DHCP 服务器确定此 IP 地址所属的子网并从该地址池分配 IP 地址。

建议尽可能将接口的 IP 地址用于路由目的。例如，如果池为 10.100.10.2-10.100.10.254，接口地址为 10.100.10.1/24，则使用 10.100.10.1 作为 DHCP 范围。请不要使用网络编号。DHCP 仅可用于 IPv4 寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

f) 点击**确定**。
g) 点击**应用**。

将 IP 地址分配给本地用户

可将本地用户账户配置为使用组策略，还可配置某些 Secure Client 属性。当 IP 地址的其他源出现故障时，这些用户账户将提供回退，以便管理员仍然可以访问。

开始之前

要添加或编辑用户，请依次选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > AAA/本地用户 (AAA/Local Users) > 本地用户 (Local Users)**，然后点击**添加 (Add)** 或**编辑 (Edit)**。

默认情况下，“编辑用户帐户”(Edit User Account) 屏幕上的每项设置均将选中**继承 (Inherit)** 复选框，这表明用户账户从默认组策略 DfltGrpPolicy 继承该设置的值。

要覆盖每项设置，请取消选中**继承 (Inherit)** 复选框，并输入新值。接下来的详细步骤介绍 IP 地址设置。有关完整的配置详情，请参阅为本地用户配置 VPN 策略属性。

过程

步骤 1 启动 ASDM 并依次选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > AAA/本地用户 (AAA/Local Users) > 本地用户 (Local Users)**。
步骤 2 选择要配置的用户，然后点击**编辑 (Edit)**。
步骤 3 在左侧窗格中，点击 **VPN 策略 (VPN Policy)**。
步骤 4 要为此用户设置专用 IPv4 地址，请在**专用 IPv4 地址（可选）**区域中输入 IPv4 地址和子网掩码。

步骤 5 要为此用户设置专用 IPv6 地址，请在**专用 IPv6 地址**（**可选**）区域中输入带 IPv6 前缀的 IPv6 地址。IPv6 前缀表示 IPv6 地址所属的子网。

步骤 6 点击**应用 (Apply)**，将更改保存到运行配置。

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。