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。

- aaa 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。此方法适用于 IPv4 和 IPv6 分配策略。
- 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。此方法适用于 IPv4 分配策略。
- **local** 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。如果选择 local，还必须使用 **ip-local-pool** 命令定义要使用的 IP 地址范围。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 ASA 不会强制执行延迟。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 IPv4 地址分配

过程

启用要供 ASA 在将 IPv4 地址分配给 VPN 连接时使用的地址分配方法。可用的方法是从 AAA 服务器、DHCP 服务器或本地地址池获取 IP 地址。默认情况下，这些方法均已启用。

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

示例：

例如，您可以将 IP 地址释放之后重新开始使用的时间配置为 0 至 480 分钟。

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

以下示例使用此命令的 no 形式禁用地址分配方法。

```
hostname(config)# no vpn-addr-assign dhcp
```

配置 IPv6 地址分配

过程

启用要供 ASA 在将 IPv6 地址分配给 VPN 连接时使用的地址分配方法。可用的方法是从 AAA 服务器或本地地址池获取 IP 地址。默认情况下，这两种方法均已启用。

ipv6-vpn-addr-assign {**aaa** | local}

示例：

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

以下示例使用此命令的 no 形式禁用地址分配方法。

```
hostname(config)# no ipv6-vpn-addr-assign local
```

查看地址分配方法

过程

使用以下方法之一查看在 ASA 上配置的地址分配方法：

- 查看 IPv4 地址分配

  显示已配置的地址分配方法。已配置的地址分配方法可能为 aaa、dhcp 或 local。

  ```
  show running-config all vpn-addr-assign
  vpn-addr-assign aaa
  vpn-addr-assign dhcp
  vpn-addr-assign local
  ```

- 查看 IPv6 地址分配

显示已配置的地址分配方法。已配置的地址分配方法可能为 aaa 或 local。

```
show running-config all ipv6-vpn-addr-assign
ipv6-vpn-addr-assign aaa
ipv6-vpn-addr-assign local reuse-delay 0
```

配置本地 IP 地址池

要配置用于 VPN 远程访问隧道的 IPv4 地址池，请在全局配置模式下输入 **ip local pool** 命令。如要删除地址池，请输入此命令的 **no** 形式。

要配置用于 VPN 远程访问隧道的 IPv6 地址池，请在全局配置模式下输入 **ipv6 local pool** 命令。如要删除地址池，请输入此命令的 **no** 形式。

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。

注释 在修改活动隧道组中当前正在使用的现有地址池（即，向最终用户开放连接）时，您必须在更改窗口中执行更改，并确保满足以下条件：

- 连接的用户已注销。
- 地址池将从隧道组中删除，并根据需要进行修改。
- 然后，修改后的地址池将被重新添加到隧道组下。

如果不以这种方式修改地址池，则可能会导致 ASA 的行为不一致。

配置本地 IPv4 地址池

注释 如果要在 CLI 上修改活动隧道组中当前正在使用的现有地址池（即向最终用户开放连接），则建议在更改窗口中执行此更改。应注销连接的用户，从隧道组中删除地址池，根据需要进行修改，然后重新添加到隧道组下。如果不以这种方式完成，则可能会导致 ASA 的行为不一致。

过程

步骤 1 将 IP 地址池配置为地址分配方法。输入参数为 **local** 的 **vpn-addr-assign** 命令。

示例：

```
hostname(config)# vpn-addr-assign local
```

步骤 2 配置地址池。此命令为地址池命名，并指定 IPv4 地址范围和子网掩码。

ip local pool*poolname first_address-last_address***mask***mask*

示例：

此示例配置名为 *firstpool* 的 IP 地址池。起始地址为 10.20.30.40，结束地址为 10.20.30.50。网络掩码为 255.255.255.0。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

此示例删除名为 **firstpool** 的 IP 地址池。

```
hostname(config)# no ip local pool firstpool
```

配置本地 IPv6 地址池

过程

步骤 1 将 IP 地址池配置为地址分配方法，输入参数为 **local** 的 ipv6-**vpn-addr-assign** 命令。

示例：

```
hostname(config)# ipv6-vpn-addr-assign local
```

步骤 2 配置地址池。此命令为地址池命名，并确定起始 IPv6 地址、前缀长度（位数）和要在相应地址范围中使用的地址数量。

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

示例：

此示例配置名为 *ipv6pool* 的 IP 地址池。起始地址为 2001:DB8::1，前缀长度为 32 位，要在地址池中使用的地址数量为 100。

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

此示例删除名为 *ipv6pool* 的 IP 地址池。

```
hostname(config)# no ipv6 local pool ipv6pool
```

配置 AAA 寻址

如要使用 AAA 服务器为 VPN 远程访问客户端分配地址，必须首先配置 AAA 服务器或服务器组。请参阅命令参考中的 **aaa-server protocol** 命令。

此外，用户必须匹配为 RADIUS 身份验证配置的连接配置文件。

以下示例说明如何为名为 firstgroup 的隧道组定义名为 RAD2 的 AAA 服务器组。此过程还包括一个必须执行的步骤，在该步骤中，您可能已经为隧道组命名并定义隧道组类型。该步骤在以下示例中显示为一则提醒，提示您只有先设置这些值，然后才有权访问后续 tunnel-group 命令。

这些示例创建的配置概述如下：

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)# authentication-server-group RAD2
```

如要配置用于 IP 寻址的 AAA，请执行以下步骤：

过程

步骤 1 如要将 AAA 配置为地址分配方法，请输入参数为 **aaa** 的 **vpn-addr-assign** 命令：

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

步骤 2 如要建立用作远程访问的名为 firstgroup 的隧道组或 LAN 间隧道组，请输入关键字为 **type** 的 **tunnel-group** 命令。以下示例配置远程访问隧道组。

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

步骤 3 如要进入通用属性配置模式，在该模式下可为名为 firstgroup 的隧道组定义 AAA 服务器组，请输入参数为 **general-attributes** 的 **tunnel-group** 命令。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

步骤 4 如要指定用于身份验证的 AAA 服务器组，请输入 **authentication-server-group** 命令。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

下一步做什么

此命令包含的参数比此示例中的参数要多。有关详情，请参阅命令参考。

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 将 IP 地址池配置为地址分配方法。

vpn-addr-assign dhcp

步骤 2 建立名为 **firstgroup** 的连接配置文件作为远程访问连接配置文件。

tunnel-group firstgroup type remote-access

步骤 3 进入连接配置文件的通用属性配置模式，以便配置 DHCP 服务器。

tunnel-group firstgroup general-attributes

步骤 4 按 IPv4 地址定义 DHCP 服务器，然后退出隧道组配置模式。

dhcp-server *IPv4_address_of_DHCP_server*

不能用 IPv6 地址定义 DHCP 服务器。可为连接配置文件指定多个 DHCP 服务器地址。输入 dhcp-server 命令。您可通过此命令将 ASA 配置为在其尝试获取 VPN 客户端的 IP 地址时向指定的 DHCP 服务器发送附加选项。

示例：

以下示例配置 IP 地址为 172.33.44.19 的 DHCP 服务器。然后，退出隧道组配置模式。

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)#
```

步骤 5 如果该组尚不存在，请创建一个名为 **remotegroup** 的内部组策略。

```
hostname(config)# group-policy remotegroup internal
```

步骤 6 （可选。）进入 group-policy attributes 配置模式并定义 DHCP 网络范围。

dhcp-network-scope *ip_address*

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。

注释
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。

示例：

以下是进入 remotegroup 的属性配置模式，并将 DHCP 范围设置为 10.100.10.1 的示例。

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

示例

这些示例创建的配置摘要如下：

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

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。