VPN 向导

VPN 概述

ASA 通过跨 TCP/IP 网络（如互联网）创建被用户视为专用连接的安全连接来创建虚拟专用网络。它可以创建单一用户到 LAN 连接和 LAN 到 LAN 连接。

这种安全连接被称为隧道，ASA 使用隧道协议来协商安全参数，创建并管理隧道，封装数据包，通过隧道收发数据包，然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。

通过 VPN 向导，可以配置基本 LAN 到 LAN 连接和远程访问 VPN 连接，并为身份验证分配预先共享的密钥或数字证书。使用 ASDM 编辑和配置高级功能。

本节中描述的四个 VPN 向导如下：

- Secure Client VPN 向导， 第 4 页

  Cisco Secure 客户端的 AnyConnect VPN 型号 通过企业资源的全 VPN 隧道来为远程用户提供到 ASA 的安全 SSL 或 IPsec (IKEv2) 连接。在先前未安装客户端的情况下，远程用户在其浏览器中输入配置为接受无客户端 VPN 连接的接口的 IP 地址。ASA 下载与远程计算机的操作系统匹配的客户端。下载后，客户端会自行进行安装和配置，建立安全连接，并在连接终止时自行保留或自行卸载（视 ASA 配置而定）。如果先前已安装客户端，当用户进行身份验证时，ASA 将检查客户端的修订版本并在必要情况下升级客户端。

  当 ASA 处于多情景模式下时，Secure Client VPN 向导仅在用户情景中可用。必须在系统情景中配置所需情景的存储和资源类。

  每个情景都需要存储来容纳思科 Secure Client 软件包文件和配置文件。每个情景的许可证分配都需要资源类。使用的许可证是 Secure Client 高级版许可证。

注释 此向导的其余配置部分与单情景模式相同。

- IPsec IKEv2 远程访问向导，第 10 页

  IKEv2 允许其他供应商的 VPN 客户端连接到 ASA。这可增强安全性并符合联邦和公共部门授权中定义的 IPsec 远程访问要求。

  当 ASA 处于多情景模式下时，IPSec IKEv2 远程访问向导仅在用户情景中可用。必须在系统情景中配置所需情景的资源类。使用的许可证是 Secure Client 高级版许可证。

注释 此向导的其余配置部分与单情景模式相同。

- IPsec IKEv1 远程访问向导，第 6 页
- IPsec 站点到站点 VPN 向导，第 2 页

  对于同时使用 IPv4 和 IPv6 寻址的 LAN 到 LAN 连接，如果两个对等体均为 ASA，并且双方的内部网络具有匹配的寻址方案（均为 IPv4 或均为 IPv6），则 ASA 支持 VPN 隧道。如果两个对等体在网络内部均为 IPv6 而网络外部为 IPv6，则此情况也成立。

IPsec 站点到站点 VPN 向导

两个 ASA 设备之间的隧道被称为站点到站点隧道，并且是双向的。站点到站点 VPN 隧道使用 IPsec 协议保护数据。

对等设备标识

- Peer IP Address - 配置另一个站点（对等设备）的 IP 地址。
- VPN Access Interface - 选择要用于站点到站点隧道的接口。
- Crypto Map Type - 指定将用于此对等体的映射类型为静态还是动态。

保护流量

通过此步骤可标识本地网络和远程网络。这些网络使用 IPsec 加密来保护流量。

- Local Networks - 标识 IPsec 隧道中使用的主机。
- Remote Networks - 标识 IPsec 隧道中使用的网络。

安全

通过此步骤可配置使用对等设备进行身份验证的方法。可以选择简单配置并提供预先共享的密钥。或者，也可以选择 Customized Configuration 以获取更多高级选项，如下所示：

- IKE Version - 根据要使用的版本选中 IKEv1 或 IKEv2 复选框。
- IKE 第 1 版身份验证方式
  - Pre-shared Key - 使用预先共享的密钥是设置与有限数量的远程对等体和稳定网络的通信的一种快捷方法。它在大型网络中可能会导致可扩展性问题，因为每个 IPSec 对等体需要与其建立安全连接的每个对等体的配置信息。

    每对 IPSec 对等体必须交换预先共享的密钥以建立安全隧道。请使用安全方法与远程站点的管理员交换预先共享的密钥。
  - Device Certificate - 点击以使用证书在本地 ASA 和远程 IPsec 对等体之间进行身份验证。

    可以高效地管理用于与数字证书建立 IPSec 隧道的安全密钥。数字证书包含用于标识用户或设备的信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包含公共密钥的副本。

    当两个对等体要通信时，它们交换证书和数字签名数据以相互进行身份验证。向网络中添加新的对等体时，该对等体会向 CA 注册，并且其他任何对等体都不需要额外配置。
- IKE 第 2 版身份验证方式
  - Local Pre-shared Key - 指定 IPsec IKEv2 身份验证方式和加密算法。
  - Local Device Certificate - 通过安全设备对 VPN 访问进行身份验证。
  - Remote Peer Pre-shared Key - 点击以使用预先共享的密钥在本地 ASA 和远程 IPsec 对等体之间进行身份验证。
  - Remote Peer Certificate Authentication - 如果选中，允许对等设备使用证书向此设备自行进行身份验证。
- Encryption Algorithms - 通过此选项卡可选择用于保护数据的加密算法的类型。
  - IKE Policy - 指定 IKEv1/IKEv2 身份验证方式。
  - IPsec Proposal - 指定 IPsec 加密算法。
- Perfect Forward Secrecy
  - Enable Perfect Forwarding Secrecy (PFS) - 指定在生成第 2 阶段 IPsec 密钥时是否使用完全向前保密以及要使用的数量规模。PFS 是一个加密概念，其中每个新密钥都与任何先前密钥无关。在 IPsec 协商中，除非启用 PFS，否则第 2 阶段密钥基于第 1 阶段密钥。PFS 使用 Diffie-Hellman 技术来生成密钥。

    PFS 确保在将来其中一个私钥被泄漏的情况下，从一组长期公共密钥和私钥派生的会话密钥不被泄漏。

    必须在连接的两端均启用 PFS。

- Diffie-Hellman Group - 选择 Diffie-Hellman 组标识符，供两个 IPsec 对等体用于派生共享密钥而不将其相互传输。默认组 14（2048 位 Diffie-Hellman）。

NAT 免除

- Exempt ASA side host/network from address translation - 使用下拉列表选择要从地址转换中排除的主机或网络。

Secure Client VPN 向导

使用此向导配置 ASA 以接受来自 Cisco 安全客户端 AnyConnect VPN 模块的 VPN 连接。此向导为完全网络访问配置 IPsec (IKEv2) 或 SSL VPN 协议。建立 VPN 连接后，ASA 将Cisco 安全客户端 AnyConnect VPN 模块自动上载到最终用户的设备。

连接配置文件标识

连接配置文件标识用于向远程访问用户标识 ASA：

- Connection Profile Name - 提供远程访问用户将对 VPN 连接进行访问的名称。
- VPN Access Interface - 选择远程访问用户将对 VPN 连接进行访问的接口。

VPN 协议

指定为此连接配置文件允许的 VPN 协议。

Secure Client 默认为 SSL。如果启用 IPsec 作为连接配置文件的 VPN 隧道协议，还必须从 ASDM 使用配置文件编辑器创建并部署启用了 IPsec 的客户端配置文件，然后部署该配置文件。

如果预先部署而不是 Web 启动 Secure Client，则第一个客户端连接将使用 SSL，并在会话期间从 ASA 接收客户端配置文件。对于后续连接，客户端使用配置文件中指定的协议（SSL 或 IPsec）。如果使用客户端预先部署指定了 IPsec 的配置文件，则第一个客户端连接将使用 IPsec。有关预先部署启用了 IPsec 的客户端配置文件的详细信息，请参阅安全客户端管理员指南。

- SSL
- IPsec (IKEv2)
- Device Certificate - 向远程访问客户端标识 ASA。一些 Secure Client 功能（例如“始终开启”和 IPsec/IKEv2）需要在 ASA 上具有有效的设备证书。
- Manage - 选择 **Manage** 将打开 Manage Identity Certificates 窗口。
  - Add - 选择 **Add** 以添加身份证书及其详细信息。
  - Show Details - 如果选择特定证书并点击 **Show Details**，则系统会显示 Certificate Details 窗口，其中提供将证书颁发给的人员和颁发者，以及指定其序列号、用途、关联信任点、有效时间范围等的有关信息。

- Delete - 突出显示要删除的证书并点击 **Delete**。
- Export - 突出显示证书并点击 **Export** 以将证书导出到具有或没有加密口令的文件。
- Enroll ASA SSL VPN with Entrust - 通过来自 Entrust 的 SSL Advantage 数字证书使思科 ASA SSL VPN 设备快速启动并运行。

客户端映像

ASA 可以在访问企业网络时自动将最新的 Secure Client 软件包上传到客户端设备。可以使用正则表达式将浏览器的用户代理与映像相匹配。您也可以通过将最常用的操作系统移至列表顶部来最小化连接设置时间。

认证方式

在此屏幕上指定身份验证信息。

- “AAA 服务器组”- 启用以使 ASA 能够联系远程 AAA 服务器组来对用户进行身份验证。从预先配置的组列表中选择 AAA 服务器组，或者点击 **New** 以创建新组。
- “本地用户数据库详细信息”- 将新用户添加到存储在 ASA 上的本地数据库。
  - Username - 为用户创建用户名。
  - Password - 为用户创建密码。
  - Confirm Password - 重新键入同一密码以确认。
  - Add/Delete - 从本地数据库添加或删除用户。

客户端地址分配

向远程 Secure Client 用户提供一系列 IP 地址。

- “IPv4 地址池”- SSL VPN 客户端在连接到 ASA 时接收新 IP 地址。无客户端连接不需要新 IP 地址。Address Pools 定义远程客户端可以接收的地址范围。请选择现有 IP 地址池，或者点击 **New** 以创建新池。

  如果选择 **New**，将必须提供开始和结束 IP 地址及子网掩码。

- IPv6 Address Pool - 选择现有 IP 地址池，或者点击 **New** 以创建新池。

注释 无法为 IKEv2 连接配置文件创建 IPv6 地址池。

网络名解析服务器

指定在访问内部网络时为远程用户解析了哪些域名。

- DNS Servers - 输入 DNS 服务器的 IP 地址。
- WINS Servers - 输入 WINS 服务器的 IP 地址。
- Domain Name - 键入默认域名。

NAT 免除

如果在 ASA 上启用了网络转换，则必须豁免 VPN 流量执行此转换。

Secure Client 部署

可以使用以下两种方法之一将 Secure Client 程序安装到客户端设备：

- Web launch - 使用 Web 浏览器访问 ASA 时， Secure Client 软件包自动进行安装。

注释 在多情景模式下不支持 Web 启动。

- Pre-deployment - 手动安装 Secure Client 软件包。

Allow Web Launch 是一项全局设置，可影响所有连接。如果取消选中（不允许），则 Secure Client SSL 连接和无客户端 SSL 连接不工作。

对于预先部署，disk0:/test2_client_profile.xml 配置文件捆绑包包含 .msi 文件，并且必须从 ASA 将此客户端配置文件包含在 Secure Client 软件包中，以确保 IPsec 连接按预期工作。

IPsec IKEv1 远程访问向导

注释 思科 VPN 客户端已停产并终止支持。必须升级到 Cisco Secure 客户端。

使用IKEv1 远程访问向导为 VPN 客户端（例如移动用户）配置安全远程访问权限，以及标识连接到远程 IPsec 对等体的接口。

- VPN Tunnel Interface - 选择要用于远程访问客户端的接口。如果 ASA 有多个接口，请立即停止并配置 ASA 上的接口，然后再运行此向导。
- “支持入站 IPsec 会话绕过接口访问列表”- 支持始终允许通过 IPsec 身份验证的入站会话经过 ASA（即，不检查接口访问列表语句）。请注意，入站会话只会绕过接口 ACL。配置的组策略、用户和下载的 ACL 仍然适用。

远程访问客户端

各种类型的远程访问用户可以打开到此 ASA 的 VPN 隧道。选择此隧道的 VPN 客户端类型。

- VPN 客户端类型

- Easy VPN Remote 产品。
- Microsoft Windows client using L2TP over IPsec - 指定 PPP 身份验证协议。选项包括 PAP、CHAP、MS-CHAP-V1、MS-CHAP-V2 和 EAP-PROXY：

  PAP - 在身份验证期间传递明文用户名和密码，并且不安全。

  CHAP - 为响应服务器质询，客户端使用明文用户名返回加密质询及密码。此协议比 PAP 更安全，但不加密数据。

  MS-CHAP, Version 1 - 与 CHAP 类似，但更安全，原因是服务器仅存储和比较加密密码，而不是像 CHAP 中存储和比较明文密码。

  MS-CHAP, Version 2 - 包含优于 MS-CHAP, Version 1 的安全增强功能。

  “EAP 代理”- 启用 EAP，它允许 ASA 代理面向外部 RADIUS 身份验证服务器的 PPP 身份验证过程。

  如果在远程客户端上未指定某协议，请勿指定该协议。
- 指定客户端是否将以 username@tunnelgroup 形式发送隧道组名。

VPN 客户端身份验证方式及隧道组名称

使用 VPN Client Authentication Method and Name 窗格配置身份验证方式和创建连接策略（隧道组）。

- Authentication Method - 远程站点对等体通过预先共享的密钥或证书进行身份验证。
  - “预共享密钥”- 点击以使用预先共享的密钥在本地 ASA 和远程 IPsec 对等体之间进行身份验证。

    使用预先共享的密钥是设置与有限数量的远程对等体和稳定网络的通信的一种快捷方法。它在大型网络中可能会导致可扩展性问题，因为每个 IPSec 对等体需要与其建立安全连接的每个对等体的配置信息。

    每对 IPSec 对等体必须交换预先共享的密钥以建立安全隧道。请使用安全方法与远程站点的管理员交换预先共享的密钥。
  - Pre-shared Key - 键入长度介于 1 到 128 个字符之间的字母数字字符串。
  - “证书”- 点击以使用证书在本地 ASA 和远程 IPsec 对等体之间进行身份验证。要完成此部分，必须先前已向 CA 注册并将一个或多个证书下载到 ASA。

    可以高效地管理用于与数字证书建立 IPSec 隧道的安全密钥。数字证书包含用于标识用户或设备的信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包含公共密钥的副本。

    要使用数字证书，每个对等体需要向负责颁发数字证书的证书颁发机构 (CA) 注册。CA 可以是受信任的供应商，或者是在组织内建立的私有 CA。

    当两个对等体要通信时，它们交换证书和数字签名数据以相互进行身份验证。向网络中添加新的对等体时，该对等体会向 CA 注册，并且其他任何对等体都不需要额外配置。

    Certificate Signing Algorithm - 显示用于为数字证书签名的算法，rsa-sig 对应于 RSA。

- Tunnel Group Name - 键入一个名称以创建包含此 IPsec 连接的隧道连接策略的记录。连接策略可以指定身份验证、授权和记账服务器、默认组策略及 IKE 属性。使用此 VPN 向导配置的连接策略会指定身份验证方法并使用 ASA 默认组策略。

客户端身份验证

使用“客户端身份验证”窗格选择 ASA 对远程用户进行身份验证的方法。选择以下选项之一：

- “使用本地用户数据库进行身份验证”- 点击以使用 ASA 内部身份验证。此方法用于用户数较少且稳定的环境。通过下一个窗格，可在 ASA 上为个人用户创建账户。
- Authenticate using an AAA server group - 点击以使用内部服务器组进行远程用户身份验证。
  - AAA Server Group Name - 选择先前配置的 AAA 服务器组。
  - New...- 点击以配置新的 AAA 服务器组。

用户账户

使用“用户账户”窗格将新用户添加到 ASA 内部用户数据库以进行身份验证。

地址池

使用“地址池”窗格配置 ASA 分配给远程 VPN 客户端的本地 IP 地址池。

- Tunnel Group Name - 显示此地址池应用到的连接配置文件（隧道组）的名称。可在 VPN Client and Authentication Method 窗格中设置此名称（步骤 3）。
- Pool Name - 为地址池选择描述性标识符。
- New...- 点击以配置新地址池。
- Range Start Address - 键入地址池中的开始 IP 地址。
- Range End Address - 键入地址吃中的结束 IP 地址。
- Subnet Mask -（可选）选择这些 IP 地址的子网掩码。

推送至客户端的属性（可选）

使用“推送至客户端的属性（可选）”窗格使 ASA 将有关 DNS 和 WINS 服务器及默认域名的信息传递到远程访问客户端。

- Tunnel Group - 显示地址池应用到的连接策略的名称。可在 VPN Client Name and Authentication Method 窗格中设置此名称。
- Primary DNS Server - 键入主 DNS 服务器的 IP 地址。
- Secondary DNS Server - 键入辅助 DNS 服务器的 IP 地址。
- Primary WINS Server - 键入主 WINS 服务器的 IP 地址。

- Secondary WINS Server - 键入辅助 WINS 服务器的 IP 地址。
- Default Domain Name - 键入默认域名。

IKE 策略

IKE，也称为互联网安全关联和密钥管理协议 (ISAKMP)，是让两台主机商定如何构建 IPSec 安全关联的一种协商协议。每个 IKE 协商分为两个部分，分别称为第 1 阶段和第 2 阶段。第 1 阶段创建第一条隧道，用于保护后来的 IKE 协商消息。第 2 阶段创建用于保护数据的隧道。

使用 IKE Policy 窗格设置第 1 阶段 IKE 协商的条款，其中包括保护数据和确保隐私的加密方法、确保对等体身份的身份验证方式，以及用于建立加密密钥确定算法强度的 Diffie-Hellman 组。ASA 使用此算法派生加密密钥和散列密钥。

- “加密”- 选择 ASA 用于建立保护第 2 阶段协商的第 1 阶段 SA 的对称加密算法。ASA 支持以下加密算法：

算法	说明
DES	数据加密标准。使用 56 位密钥。
3DES	三重 DES。使用 56 位密钥执行三次加密。
AES-128	高级加密标准。使用 128 位密钥。
AES-192	使用 192 位密钥的 AES。
AES-256	使用 256 位密钥的 AES。

  默认的 3DES 比 DES 更安全，但是需要对加密和解密进行更多处理。同样，AES 选项可提高安全性，但也需要增加处理。

- Authentication - 选择用于身份验证并确保数据完整性的散列算法。默认值为 SHA。MD5 具有比 SHA 更小的摘要并认为其比 SHA 稍快一些。已成功（但极其困难）演示过对 MD5 的攻击。不过，ASA 所使用的带密钥的散列消息认证码 (HMAC) 版本可防止此类攻击。
- Diffie-Hellman Group - 选择 Diffie-Hellman 组标识符，供两个 IPsec 对等体用于派生共享密钥而不将其相互传输。默认的 DH 组 14（2048 位）被认为比组 2 和组 5 更安全。

IPsec 设置（可选）

使用 IPsec Settings (Optional) 窗格标识无需地址转换的本地主机/网络。默认情况下，ASA 使用动态或静态网络地址转换 (NAT) 对外部主机隐藏内部主机和网络的真实 IP 地址。NAT 可将不受信任的外部主机的攻击风险降到最低，但是对于已由 VPN 进行身份验证和保护的主机可能不合适。

例如，使用动态 NAT 的内部主机通过将其 IP 地址与池中随机选择的地址相匹配来转换其 IP 地址。只有已转换的地址在外部才可见。除非配置 NAT 豁免规则，否则尝试通过将数据发送到其真实 IP 地址来到达这些主机的远程 VPN 客户端无法连接到这些主机。

注释 如果希望豁免所有主机和网络执行 NAT，不要在此窗格上进行任何配置。如果即使有一个条目，则所有其他主机和网络都要执行 NAT。

- Interface - 选择用于连接到选定的主机或网络的接口的名称。
- Exempt Networks - 选择要从所选接口网络中豁免的主机或网络的 IP 地址。
- Enable split tunneling - 选择以在未加密的情况下发送从远程访问客户端到公共互联网的流量。分割隧道会导致受保护网络的流量加密，而到未受保护网络的流量则未加密。启用分割隧道时，ASA 在身份验证后将 IP 地址列表推送到远程 VPN 客户端。远程 VPN 客户端会对发往 ASA 后的 IP 地址的流量加密。所有其他流量都在未加密的情况下直接传输到互联网而不涉及 ASA。
- Enable Perfect Forwarding Secrecy (PFS) - 指定在生成第 2 阶段 IPsec 密钥时是否使用完全向前保密以及要使用的数量规模。PFS 是一个加密概念，其中每个新密钥都与任何先前密钥无关。在 IPsec 协商中，除非启用 PFS，否则第 2 阶段密钥基于第 1 阶段密钥。PFS 使用 Diffie-Hellman 技术来生成密钥。

  PFS 确保在将来其中一个私钥被泄漏的情况下，从一组长期公共密钥和私钥派生的会话密钥不被泄漏。

  必须在连接的两端均启用 PFS。

  - Diffie-Hellman Group - 选择 Diffie-Hellman 组标识符，供两个 IPsec 对等体用于派生共享密钥而不将其相互传输。默认的 DH 组 14（2048 位）被认为比组 2 和组 5 更安全。

汇总

如果对配置满意，请点击 **Finish**。ASDM 将保存 LAN 到 LAN 配置。点击 **Finish** 后，无法再使用 VPN 向导对此配置进行更改。使用 ASDM 编辑和配置高级功能。

IPsec IKEv2 远程访问向导

使用IKEv2 远程访问向导为 VPN 客户端（如移动用户）配置安全远程访问权限，以及标识连接到远程 IPsec 对等体的接口。

连接配置文件标识

输入 **Connection Profile Name** 并选择将用于 IPsec IKEv2 远程访问的 **VPN Access Interface**。

- Connection Profile Name - 键入一个名称以创建包含此 IPsec 连接的隧道连接策略的记录。连接策略可以指定身份验证、授权和记账服务器、默认组策略及 IKE 属性。使用此 VPN 向导配置的连接策略会指定身份验证方法并使用 ASA 默认组策略。
- VPN Access Interface - 选择用于与远程 IPsec 对等体建立安全隧道的接口。如果 ASA 有多个接口，则需要在运行此向导之前规划 VPN 配置，标识要用于每个计划与其建立安全连接的远程 IPsec 对等体的接口。

“基于标准的 IPSec (IKEv2) 身份验证”页面

IKE 对等身份验证 - 远程站点对等体通过预先共享的密钥或证书或者使用 EAP 的对等身份验证来进行身份验证。

- Pre-shared Key - 键入长度介于 1 到 128 个字符之间的字母数字字符串。

  使用预先共享的密钥是设置与有限数量的远程对等体和稳定网络的通信的一种快捷方法。它在大型网络中可能会导致可扩展性问题，因为每个 IPSec 对等体需要与其建立安全连接的每个对等体的配置信息。

  每对 IPSec 对等体必须交换预先共享的密钥以建立安全隧道。请使用安全方法与远程站点的管理员交换预先共享的密钥。

- Enable Certificate Authentication - 如果选中，则允许使用证书进行身份验证。
- Enable peer authentication using EAP - 如果选中，则允许使用 EAP 进行身份验证。如果选中此复选框，则必须使用证书进行本地身份验证。
- Send an EAP identity request to the client - 支持向远程访问 VPN 客户端发送 EAP 身份验证请求。

MobIKE RRC

- “为 Mobike 启用返回路由能力检查”- 对已启用 MobIKE 的 IKE/IPSEC 安全关联中的动态 IP 地址更改启用返回路由能力检查。

IKE 本地身份验证

- 启用本地身份验证，然后选择预先共享的密钥或证书
  - Preshared Key - 键入长度介于 1 到 128 个字符之间的字母数字字符串。
  - “证书”- 点击以使用证书在本地 ASA 和远程 IPsec 对等体之间进行身份验证。要完成此部分，必须先前已向 CA 注册并将一个或多个证书下载到 ASA。

    可以高效地管理用于与数字证书建立 IPSec 隧道的安全密钥。数字证书包含用于标识用户或设备的信息，如名称、序列号、公司、部门或 IP 地址。数字证书还包含公共密钥的副本。

    要使用数字证书，每个对等体需要向负责颁发数字证书的证书颁发机构 (CA) 注册。CA 可以是受信任的供应商，或者是在组织内建立的私有 CA。

    当两个对等体要通信时，它们交换证书和数字签名数据以相互进行身份验证。向网络中添加新的对等体时，该对等体会向 CA 注册，并且其他任何对等体都不需要额外配置。

身份验证方式

IPsec IKEv2 远程访问仅支持 Radius 身份验证。

- AAA Server Group - 选择先前配置的 AAA 服务器组。
- New - 点击以配置新的 AAA 服务器组。
- AAA Server Group Details - 使用此区域修改 AAA 服务器组（如果需要）。

客户端地址分配

创建或选择 IPv4 和 IPv6 地址池。将为远程访问客户端分配来自 IPv4 或 IPv6 地址池中的地址。如果配置了两种地址，则 IPv4 地址优先。有关详细信息，请参阅配置本地 *IP* 地址池。

网络名解析服务器

指定在访问内部网络时如何为远程用户解析域名。

- DNS Servers - 键入 DNS 服务器的 IP 地址。
- WINS Servers - 键入 WINS 服务器的 IP 地址。
- Default Domain Name - 键入默认域名。

NAT 免除

- Exempt VPN traffic from Network Address Translation - 如果在 ASA 上启用了 NAT，则必须选中此项。

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。