



通过远程接入 VPN 的用户控制

以下主题讨论如何通过远程接入 VPN 执行用户感知和用户控制：

- [远程接入 VPN 身份源，第 1 页](#)
- [配置用户控制 RA VPN，第 2 页](#)
- [远程接入 VPN 身份源故障排除，第 2 页](#)

远程接入 VPN 身份源

AnyConnect 是终端设备上通过远程 VPN 连接 威胁防御 设备的唯一受支持客户端。

按照[创建新的远程接入 VPN 策略](#)中的描述设置安全 VPN 网关时，您可以为这些用户设置一个身份策略，并将该身份策略与访问控制策略关联，前提是您的用户位于 Active Directory 存储库中。



注释 如果使用具有用户身份和 RADIUS 作为身份源的远程访问 VPN，则必须配置领域（**对象 (Objects) > 对象管理 (Object Management) > AAA 服务器 (AAA Server) > RADIUS 服务器组 (RADIUS Server Group)**）。

远程用户提供的登录信息由 LDAP 或 AD 领域或 RADIUS 服务器组进行验证。这些实体与 Cisco Secure Firewall Threat Defense 安全网关相集成。



注释 如果用户使用 Active Directory 作为身份验证源通过远程访问 VPN 进行身份验证，则用户必须使用其用户名登录；domain\username 或 username@domain 格式无效。（Active Directory 将此用户名视为 logon 名称，有时也视为 sAMAccountName。）有关详细信息，请参阅 MSDN 上的[用户命名属性](#)。

如果使用 Radius 进行身份验证，用户可以使用上述任何一种格式登录。

通过 VPN 连接进行身份验证后，远程用户将接受 VPN 身份。Cisco Secure Firewall Threat Defense 安全网关上的身份策略将使用此 VPN 身份来识别和过滤属于此远程用户的网络流量。

身份策略与访问控制策略相关联，后者用于确定哪些人有权访问网络资源。使用访问控制策略可阻止或允许远程用户访问您的网络资源。

相关主题

[VPN 概述](#)

[Cisco Secure Firewall Threat Defense 远程接入 VPN 概述](#)

[VPN 基础知识](#)

[远程接入 VPN 功能](#)

[远程接入 VPN 的准则和限制](#)

[创建新的远程接入 VPN 策略](#)

配置用户控制 RA VPN

开始之前

- 按[创建 Active Directory 领域和领域目录](#)中所述创建领域。
- 要使用身份验证、授权和审核 (AAA)，请按照[添加 RADIUS 服务器组](#)中的讨论设置 RADIUS 服务器组。

过程

步骤 1 登录管理中心。

步骤 2 点击设备 > VPN > 远程访问。

步骤 3 请参阅[创建新的远程接入 VPN 策略](#)。

下一步做什么

- 使用[创建身份策略](#)中所述的身份策略指定要控制的用户和其他选项。
- 按[将其他策略与访问控制相关联](#)中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到受管设备，如[部署配置更改](#)中所述。
- 按[VPN 会话和用户信息](#)中所述，监视 VPN 用户流量。

远程接入 VPN 身份源故障排除

- 有关其他相关故障排除信息，请参阅[领域和用户下载故障排除](#)和[用户控制故障排除](#)和[VPN 故障排除](#)。

- 如果遇到远程接入 VPN 问题，请检查管理中心和受管设备之间的连接。如果连接失败，则无法在停机期间识别设备报告的所有远程接入 VPN 登录，除非以前查看过这些用户并已将他们下载到管理中心。

无法识别的用户在管理中心上记录为未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”用户。

- 受管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。
- 活动 FTP 会话在事件中显示为 **Unknown** 用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 [RFC 959](#)。

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。