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：

远程访问 VPN 身份源

安全客户端 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。

按照创建新的远程访问 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
远程访问 VPN 概述
VPN 基础知识
远程访问 VPN 功能
远程访问 VPN 的准则和限制
创建新的远程访问 VPN 策略

配置用户控制 RA VPN

开始之前

- 按创建 LDAP 领域或 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访问 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托管设备，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 。

远程访问 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。

- 如果遇到远程访问 VPN 问题，请检查 管理中心和托管设备之间的连接。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访问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。

- 托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。

未观察到 VPN 统计信息的正确设置

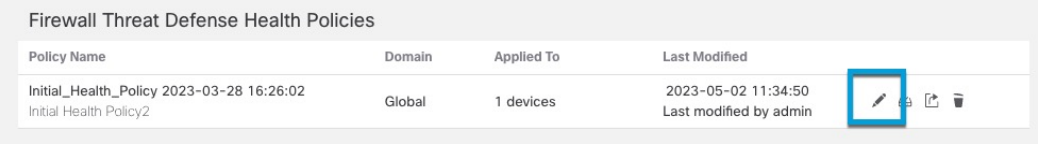
此任务讨论在运行状况策略中启用或禁用 **VPN 统计信息** 设置后必须执行的步骤。未能执行此任务意味着托管设备的运行状况策略设置不正确。

过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **系统** (⚙) > **运行状况 (Health)** > **策略 (Policy)** 。

步骤 3 在防火墙威胁防御运行状况策略下，点击要编辑的策略旁边的 **编辑** (✎) 。



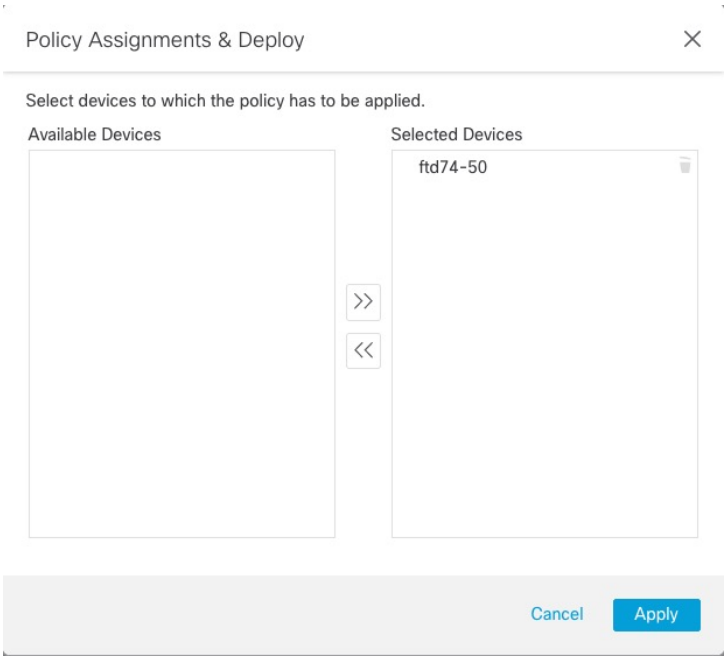
步骤 4 在 **运行状况** 模块选项卡页面上，向下滚动以找到 **VPN 统计信息**。

步骤 5 验证 VPN 统计信息设置是否正确，或根据需要进行更改。

步骤 6 如果您更改了设置，请点击 **保存**，然后点击 **取消** 以返回到运行状况策略。

步骤 7 在防火墙威胁防御运行状况策略下， **部署运行策略** (⬇) 点击以应用策略。

步骤 8 在 **策略分配和部署** 对话框中，将要部署运行状况策略的设备移至 **所选设备** 字段。



步骤 9 点击**应用 (Apply)**。
部署运行状况策略时，系统会显示一条消息。

步骤 10 运行状况策略完成部署后，点击 **策略** > **访问控制标题** > **访问控制** 以编辑访问控制策略。

步骤 11 点击策略旁边的 **编辑** (✎) 进行编辑。

步骤 12 对策略进行细微更改，例如更改其名称。

步骤 13 保存访问控制策略。

步骤 14 部署配置更改；请参阅 部署配置更改。。

远程接入 VPN 的历史记录

功能	管理中心最低版本	威胁防御最低版本	详细信息
远程接入 VPN	6.2.1	任意	引入的功能。远程接入 VPN 允许个人用户使用连接到互联网的笔记本电脑或台式计算机或者使用 Android 或 Apple iOS 移动设备，从远程位置连接到专用企业网络。远程用户使用对于通过共享介质和互联网传输的数据至关重要的加密技术，安全且自信地传输数据。

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。