使用 Cisco Secure Firewall Management Center 在威胁防御上配置 Cisco Secure 客户端模块

首次发布日期: 2023 年 7 月 31 日

使用 Cisco Secure Firewall Management Center 在威胁防御上配置 Cisco Secure 客户端模块

简介

Cisco Secure 客户端可以与各种 Cisco 终端安全解决方案集成，并使用不同的安全客户端模块提供增强的安全性。

您可以使用受管前端威胁防御向终端分发和管理安全客户端模块。当用户连接到威胁防御时，它会在终端上下载并安装安全客户端和所需的模块。

优势

使用威胁防御系统向终端分发和管理安全客户端模块具有显著的优势，因为它消除了以下管理组织网络的手动操作需求：

- 在每个终端上下载或升级安全客户端。
- 分发和管理每个终端上的安全客户端模块和配置文件。

本指南适用对象

本用例适用于使用管理中心为使用远程访问 VPN 连接到组织网络的远程员工配置安全客户端模块的网络管理员。

系统要求

下表列出了该功能支持的平台。

产品	版本	本文档使用的版本
Cisco Secure Firewall Threat Defense（之前的 Firepower 威胁防御/FTD）	6.3 及更高版本	7.3

产品	版本	本文档使用的版本
Cisco Secure Firewall Management Center（之前的 Firepower 管理中心/FMC）	6.7 及更高版本	7.3
Cisco Secure 客户端（之前的 AnyConnect）	4.0 及更高版本	5.0

注释 在 FMC 版本 6.4 到 6.6 中，您可以使用 FlexConfig 在 FTD 上启用这些模块和配置文件。有关详细信息，请参阅使用 FlexConfig 配置 AnyConnect 模块和配置文件。

如何使用托管威胁防御来安装安全客户端模块

1. 管理员可为所需的安全客户端模块创建配置文件。
2. 管理员可使用管理中心执行以下操作：
   1. 配置模块并在 RA VPN 组策略中添加配置文件。
   2. 在威胁防御上部署配置。
3. 用户使用安全客户端来启动到威胁防御的 VPN 连接。
4. 威胁防御对用户进行身份验证。
5. 安全客户端会检查更新。
6. 威胁防御在终端上分发安全客户端模块和配置文件。

有哪些不同的安全客户端模块？

模块	说明
AMP 启用程序	在终端上部署 Cisco Secure Endpoint（以前称为面向终端的 AMP）。 它可以检测网络中可能发生的潜在恶意软件威胁、删除这些威胁并保护企业免受危害。
ISE 终端安全评估	使用 Cisco Identity Services Engine (ISE) 执行安全状态检查，以评估终端的合规性。
网络可视性	监控终端应用使用情况。 可将使用情况数据与 NetFlow 分析工具共享。
Umbrella 漫游安全	通过 Cisco Umbrella 漫游安全服务实现 DNS 层安全。

模块	说明
网络访问管理器	提供安全的第2层网络，并执行设备身份验证以访问有线和无线网络。
登录前启动 (SBL)	允许用户在登录 Windows 之前建立与企业基础设施的 VPN 连接。
网络安全	将 HTTP 流量路由到思科 Cloud Web Security 扫描代理。
诊断和报告工具 (DART)	整理系统日志和其他诊断信息，以排除安全客户端安装和连接问题。
反馈	提供有关您使用和启用的功能和模块的信息。 此信息使思科能够提高 Cisco Secure 客户端的质量、可靠性、性能和用户体验。

有关部署这些模块的详细信息，请参阅《Cisco Secure 客户端（包括 AnyConnect）管理指南，版本5》。

前提条件

- 根据您要使用的模块配置关联的产品。
- 从 Cisco 软件下载中心将以下安全客户端相关软件包下载到本地主机。
  - 适用于所需平台的 Cisco Secure 客户端前端部署包。

    此软件包适用于前端，包含所有安全客户端模块。对于 Windows，文件名为 cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg。
  - 配置文件编辑器：为需要配置文件的模块创建配置文件。

    安全客户端需要某些模块的安全客户端配置文件。配置文件包含用于启用模块和连接到相应安全服务的配置。配置文件编辑器仅支持 Windows。

    如果模块需要客户端配置文件，请参阅以下列表：

Secure Client 模块	需要客户端配置文件
AMP 启用程序	是
ISE 终端安全评估	是
网络访问管理器	是
网络可视性模块	是
Umbrella 漫游安全模块	是

Secure Client 模块	需要客户端配置文件
反馈	是
诊断和报告工具 (DART)	否
登录前开始	否

许可证

- 您需要以下安全客户端许可证之一：Cisco Secure Client Premier、Cisco Secure Client Advantage 或 Cisco Secure Client VPN Only。
- 您的管理中心 Essentials（以前称为 Base）许可证必须允许导出控制功能。

  依次选择**系统 (System)** > **许可证 (Licenses)** > **智能许可证 (Smart Licenses)** 以在管理中心验证此功能。

指南、最佳实践和限制

- 不同的模块支持具有不同文件扩展名的配置文件。

  确保选择正确的文件扩展名，如下表所示：

模块名称	文件扩展名
AMP 启用程序	*.xml、*.asp
客户体验反馈	*.xml
ISE 终端安全评估	*.xml、*.isp
网络访问管理器	*.xml、*.nsp
网络可视性	*.xml、*.nvmsp
Umbrella 漫游安全	*.xml、*.json
网络安全	*.xml、*.wsp、*.wso

- 使用 DART 整理故障排除数据和日志，并在需要时与思科 TAC 共享。

  默认情况下，6.7 及更高版本的新远程访问 VPN 组策略中未启用 DART。在 6.6 及更早版本中，默认情况下启用 DART。

- 如果在 Windows 操作系统上使用 ISE 态势模块，则必须在使用 ISE 态势模块前安装网络访问管理器。
- 思科 ISE 3.0 及更高版本支持无代理终端安全评估。

- 如果启用 Umbrella 漫游安全模块，请确保禁用 RA VPN 组策略中的分割隧道下的**始终通过隧道发送 DNS 请求 (Always send DNS requests over tunnel)** 选项。
- 您必须在安全客户端 VPN 配置文件中启用 SBL，并将其添加到管理中心的 RA VPN 组策略中。

  要在组策略中添加安全客户端 VPN 配置文件，请执行以下操作：

  1. 编辑 RA VPN 组策略。
  2. 点击**安全客户端 (Secure Client)** 选项卡并点击**配置文件 (Profile)**。
  3. 点击 + 以添加安全客户端 VPN 配置文件。
  4. 点击**保存 (Save)**。

限制

- 对于组策略，每个客户端模块只能添加一个条目。您可以编辑或删除模块的条目。
- AMP 启用程序仅适用于 Cisco Secure 客户端 5.0 中的 macOS，因为适用于 Windows 的 Cisco Secure 客户端提供与 Cisco Secure Endpoint 的完全集成。
- 网络访问管理器不支持 macOS 或 Linux。

使用安全客户端模块配置远程接入 VPN 组策略

开始之前

在管理中心配置远程接入 VPN 策略。

过程

步骤 1 登录管理中心 Web 接口。

步骤 2 选择**设备 (Devices)** > **远程访问 (Remote Access)**。

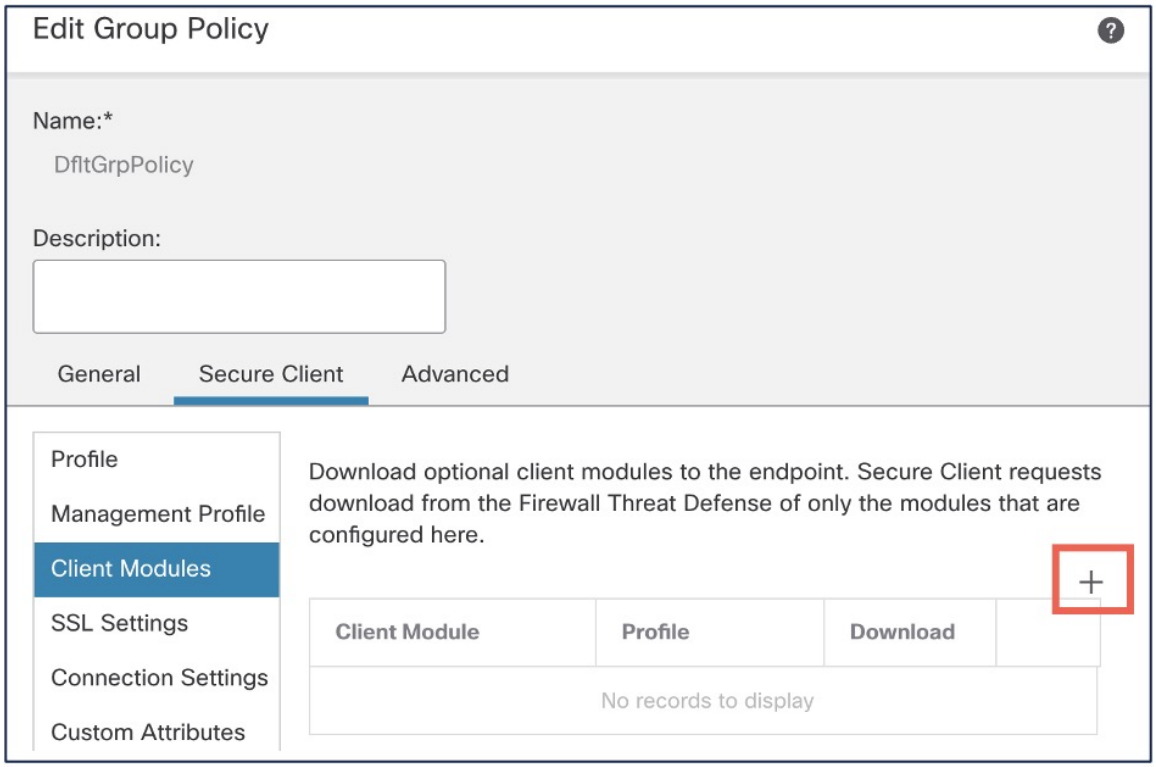
步骤 3 选择远程访问 VPN 策略，然后点击**编辑 (Edit)**。

步骤 4 选择连接配置文件，然后点击**编辑 (Edit)**。

步骤 5 点击**编辑组策略 (Edit Group Policy)**。

步骤 6 点击**安全客户端 (Secure Client)** 选项卡。

步骤 7 点击**客户端模块 (Client Modules)**，然后点击 +。



步骤 8 从客户端模块 **(Client Module)** 下拉列表中选择一个模块。

步骤 9 从要下载的配置文件 **(Profile to download)** 下拉列表中选择模块的配置文件，或点击 + 添加配置文件。

步骤 10 选中启用模块下载 **(Enable module download)** 复选框。

步骤 11 点击添加 **(Add)**。

步骤 12 点击保存 **(Save)**。

下一步做什么

1. 在威胁防御上部署配置。
2. 使用安全客户端建立与威胁防御的 VPN 连接。
3. 验证安全客户端配置。

验证安全客户端模块配置

在威胁防御上

在威胁防御 CLI 上使用以下命令查看安全客户端模块配置：

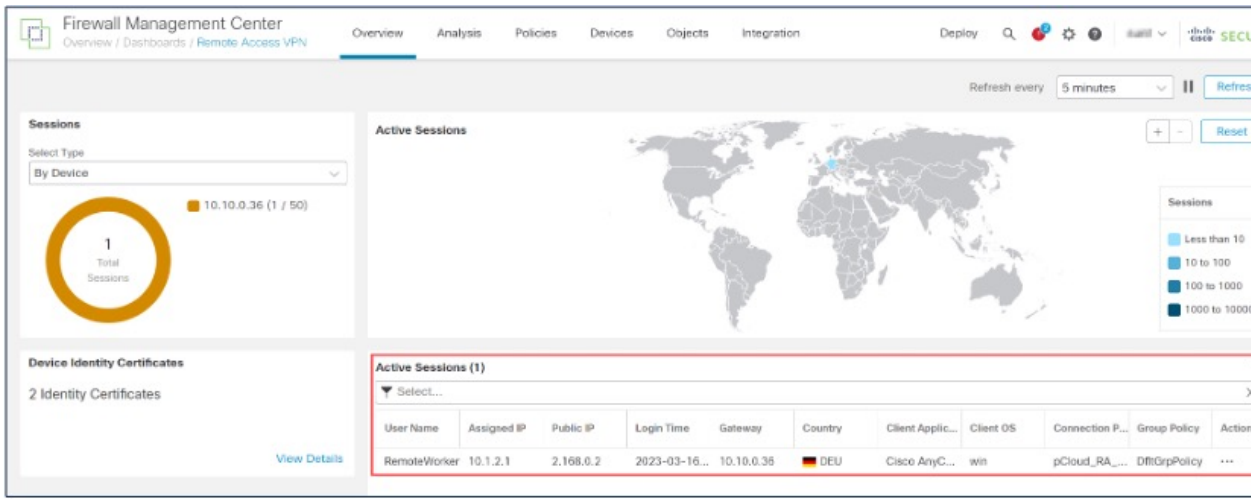
命令	说明
show disk0:	查看配置文件及其配置。
show run webvpn	查看安全客户端配置的详细信息。
show run group-policy <group_policy_name>	查看安全客户端的远程访问 VPN 组策略的详细信息。
show vpn-sessiondb anyconnect	查看活动安全客户端 VPN 会话的详细信息。

在终端上

1. 使用安全客户端建立与威胁防御的 VPN 连接。
2. 验证已配置的模块是否已作为安全客户端的一部分下载并安装。
3. 验证所有操作系统的配置文件位置中指定的位置是否有配置文件。

在管理中心上

您可以使用远程访问 VPN 控制面板（**概述 (Overview)** > **远程访问 (Remote Access)** > **VPN**）来监控管理中心的活动远程访问VPN会话。您可以确定与用户会话相关的问题，同时规避网络和用户的问题。



配置安全客户端模块的示例

- 使用安全客户端 Umbrella 模块和管理中心为终端提供 DNS 层安全性， 第 8 页
- 在终端上配置 DART 模块
- 使用 Cisco Secure 客户端 ISE 安全评估模块和 Cisco Secure Firewall Management Center 来评估终端合规性

使用安全客户端 Umbrella 模块和管理中心为终端提供 DNS 层安全性

准备工作

确保：

- 访问 Umbrella 控制面板。
- 已将安全客户端软件包下载到本地主机。
- 已在管理中心配置远程接入 VPN。
- 管理中心上的安全客户端版本高于终端上的版本。
- 禁用 RA VPN 组策略中的分割隧道下的**始终通过隧道发送 DNS 请求 (Always send DNS requests over tunnel)** 选项。

程序

步骤	任务	更多信息
1	从 Umbrella 控制面板将安全客户端 Umbrella 模块配置文件下载到本地主机。	从 Umbrella 控制面板下载安全客户端 Umbrella 模块配置文件，第 8 页
2	在管理中心的远程访问 VPN 组策略中配置 Umbrella 模块和配置文件。	使用安全客户端模块配置远程接入 VPN 组策略，第 5 页
3	在威胁防御上部署配置。	在管理中心菜单栏中，点击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

从 Umbrella 控制面板下载安全客户端 Umbrella 模块配置文件

Umbrella 配置文件 (OrgInfo.json) 文件包含关于您的 Cisco Umbrella 服务订用的具体信息，可让安全漫游模块了解向哪里报告，以及需要实施哪些策略。

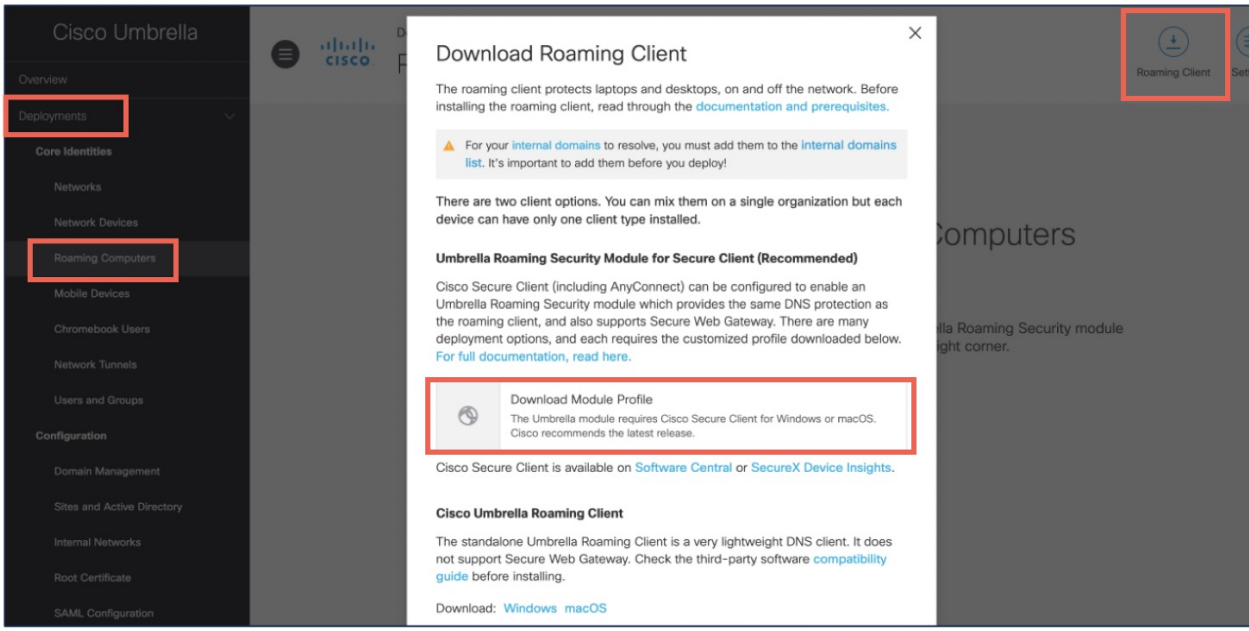
过程

步骤 1 登录 Cisco Umbrella。

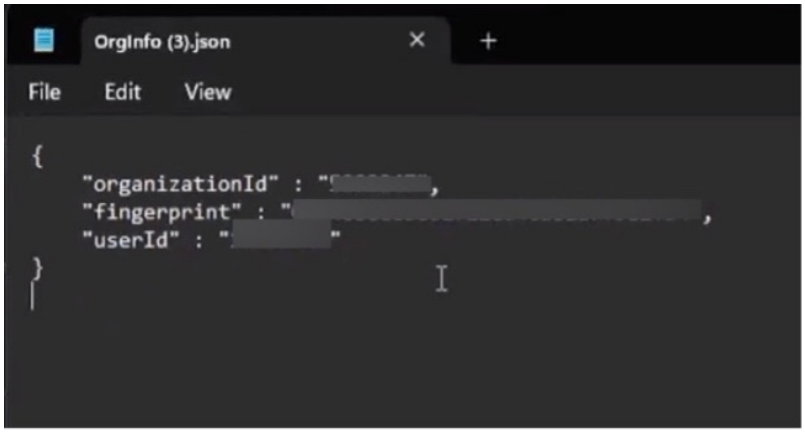
步骤 2 选择**部署 (Deployments)** > **漫游计算机 (Roaming Computers)**。

步骤 3 点击**漫游客户端 (Roaming Client)** 图标。

步骤 4 点击**下载模块配置文件 (Download Module Profile)**。



下面给出了 **OrgInfo.json** 文件的示例：



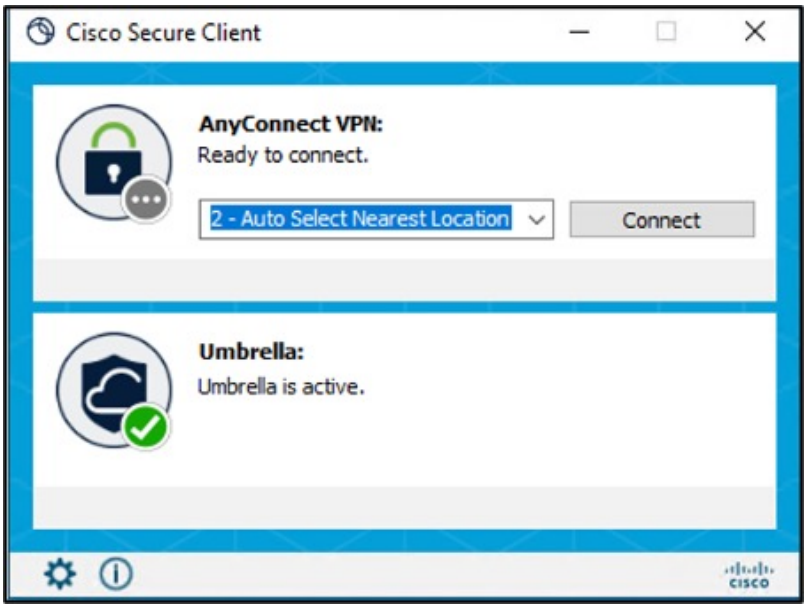
验证 Umbrella 模块配置

在威胁防御上

- 使用 **sh vpn-sessiondb anyconnect** 命令确认安全客户端连接成功。
- 使用 **sh run group-policy** 命令查看远程接入 VPN 组策略的详细信息。

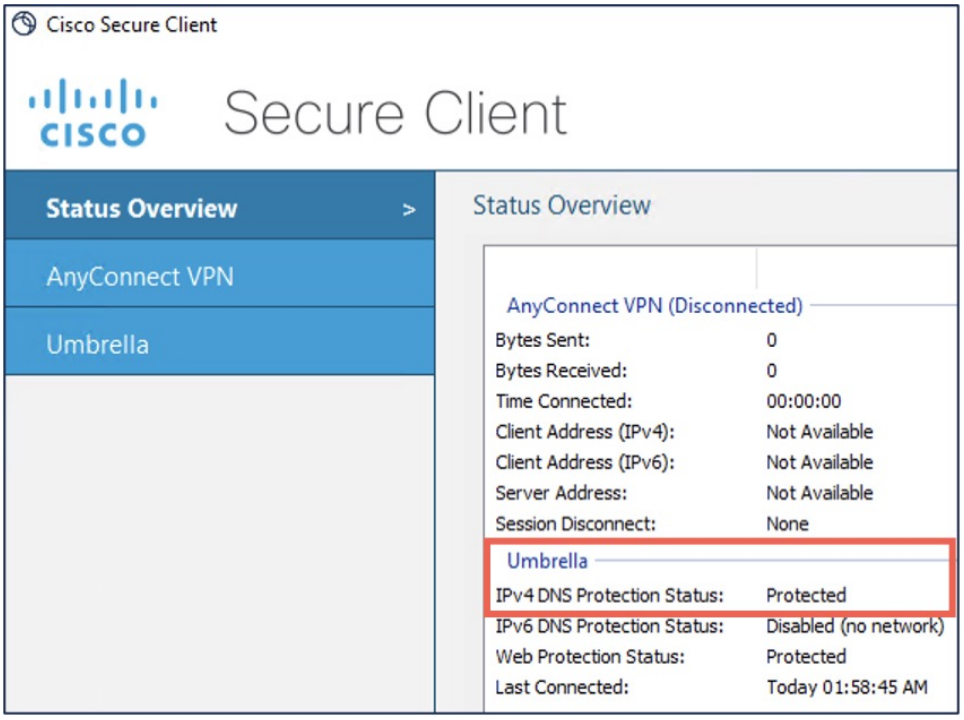
在终端上

1. 验证 VPN 连接是否成功，以及 Umbrella 模块是否已下载到终端。



2. 点击**统计信息 (Statistics)** 图标，然后点击**状态概述 (Status Overview)** 选项卡。

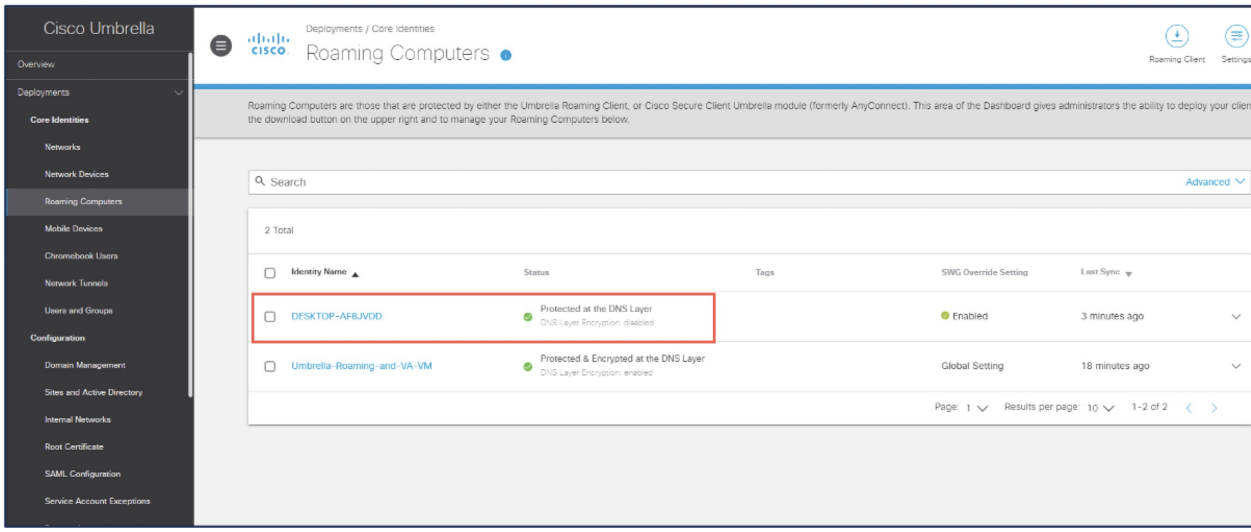
   IPv4/IPv6 DNS 保护状态为“受保护”(Protected)。



在 Cisco Umbrella 上

选择**部署 (Deployments)** > **漫游计算机 (Roaming Computers)**。

终端的状态为“在 DNS 层受保护”(Protected at the DNS Layer)。



在终端上配置 DART 模块

过程

步骤 1 将安全客户端软件包下载到本地主机，请参阅 Cisco 软件下载中心。

步骤 2 在管理中心配置远程接入 VPN。

步骤 3 在管理中心的 RA VPN 组策略中配置 DART 模块，请参阅使用安全客户端模块配置远程接入 VPN 组策略。

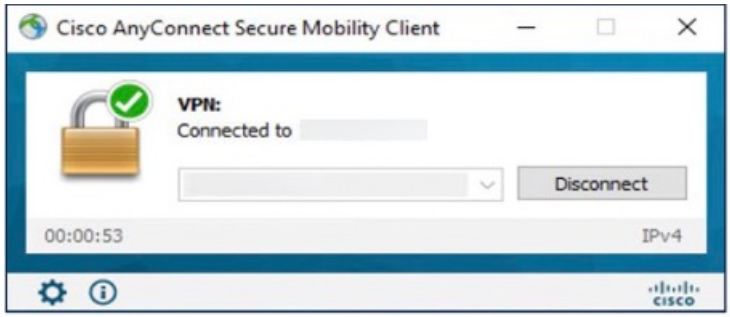
步骤 4 在威胁防御上部署配置。

在管理中心菜单栏中，点击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

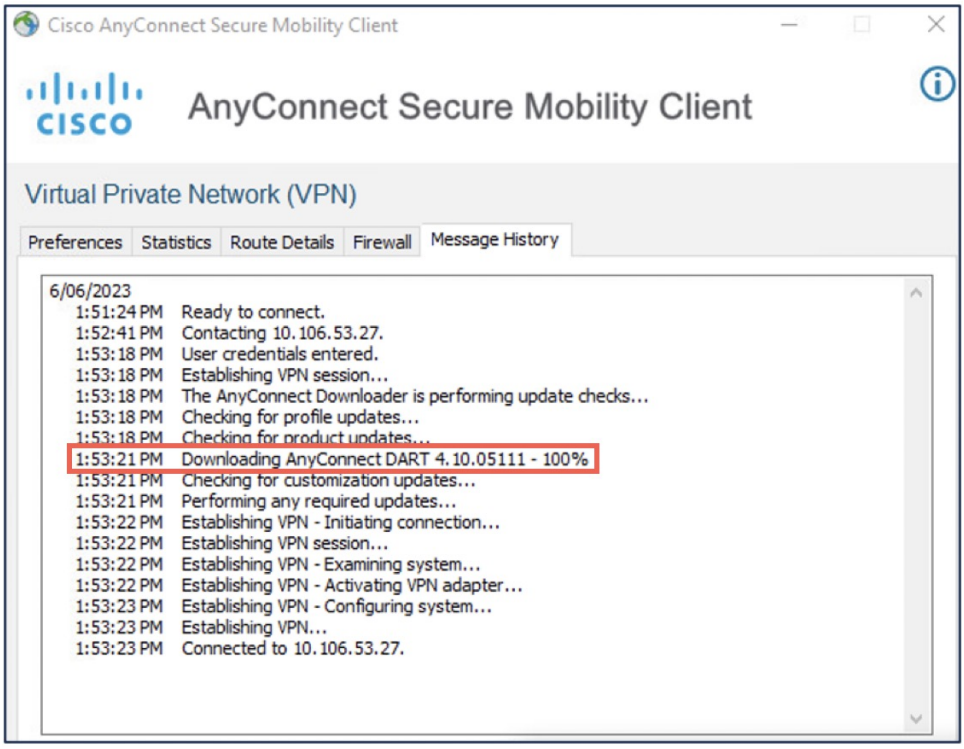
验证 DART 配置

在终端上

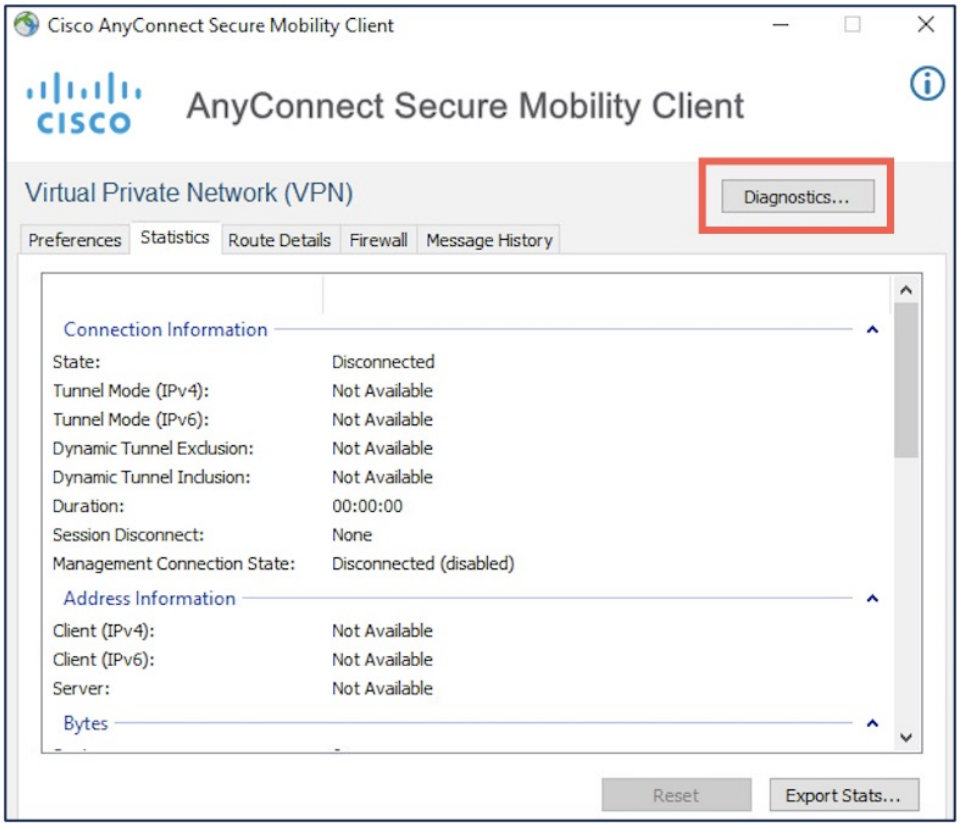
1. 验证 VPN 连接是否成功。



2. 验证是否已在终端上下载 DART 模块。



3. 成功下载后，重新启动 AnyConnect 客户端。
4. 点击**统计信息 (Statistics)** 图标。
5. 点击**诊断 (Diagnostics)**。



6. 使用 DART 向导来使用 DART 模块。

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。