Umbrella 漫游安全

Umbrella 漫游安全模块要求订用思科 Umbrella 漫游服务（包含 Professional、Insights、Platform 或 MSP 软件包）。Cisco Umbrella Roaming 在没有 VPN 活动时提供 DNS 层安全保护，而 Cisco Umbrella 订用添加了智能代理。此外，思科 Umbrella 订用还将提供内容过滤、多重策略、稳健性报告、Active Directory 集成等更多功能。无论订用情况如何，都将使用相同的 Umbrella 漫游安全模块。

Umbrella 漫游模块配置文件 (OrgInfo.json) 会将各种部署与相对应的服务关联起来，并将自动启用相对应的保护功能。

可以通过 Umbrella 控制面板实时查看源自漫游安全模块的所有互联网活动。策略和报告中的精细度级别取决于 Umbrella 订用情况。

有关各个服务级别订用中包含哪些功能的详细对比，请参阅 https://umbrella.cisco.com/products/packages。

适用于 Android 操作系统的 AnyConnect Umbrella 模块

适用于 Android 操作系统的 AnyConnect Umbrella 模块是托管的 Android 设备的漫游客户端，它提供 DNS 层保护，这种保护延伸到 Android 工作配置文件所涵盖的应用和浏览。

要将此客户端部署到 Android 设备并将 Umbrella 配置推送到 Android 设备，需要有移动设备管理系统 (MDM)。有关支持的 MDM 和其他前提条件的列表，请参阅在 Android 操作系统上部署 AnyConnect Umbrella 模块的前提条件 。

在 Android 上，某些 AnyConnect 功能在配合 Umbrella 使用时可能功能受限：

- 由于操作系统限制，Per-App VPN 不能与 Umbrella 模块配合使用。如果远程访问 VPN 处于活动状态，Umbrella 只能保护通过 VPN 隧道截获的 DNS 流量。如果为 Per-App VPN 配置了远程访问，则 Umbrella 只能保护隧道应用的 DNS 流量。
- 不应将永远在线 VPN 与锁定 (Fail Close) 选项配合使用。当 VPN 服务器无法接通时，它将停止互联网访问。请参阅您的 MDM 指南，了解如何在永远在线 VPN 设置为“开”时关闭锁定设置。

有关完整的 Umbrella 功能集的说明，请参阅 AnyConnect Umbrella 模块（Android 操作系统）文档。

在 Android 操作系统上部署 AnyConnect Umbrella 模块的前提条件

部署的前提条件：

注释 AnyConnect 监控在 MDM 中创建的工作配置文件内应用和浏览器生成的流量，并相应地阻止或允许浏览。不监控应用和/或浏览器在工作配置文件外生成的任何流量。

- 用于部署软件并将 Umbrella 配置推送到移动设备的移动设备管理系统 (MDM)。当前测试的版本有 Mobile Iron、Meraki、VMWare workspace 1 (Airwatch) 或 Microsoft Intune。
- 安装有 Android OS 6.0.1 及更高版本的 Android (Samsung/Google Pixel) 移动设备。
- 用于配置 DNS 策略、管理注册的 Android 设备以及报告用途的 Umbrella 许可证。
- 用于启用该功能的 Umbrella 组织 ID。
- 对于可信网络检测 (TND)：
  - 如果 Umbrella 模块检测到启用了 HTTPS 的虚拟设备 (VA)，它将自行停用；但是，如果 VA 不支持 HTTPS，则 Umbrella 模块将继续。
  - 必须启用 umbrella_va_fqdns 中的所有 VA FQDN。

适用于 Windows 或 macOS 的 AnyConnect Umbrella 模块

Umbrella 漫游客户端与 Umbrella 漫游安全模块不兼容

Umbrella 漫游安全模块与 Umbrella 漫游客户端不兼容。如果您要部署 Umbrella 漫游安全模块，在安装漫游安全模块过程中将检测任何现已安装的 Umbrella 漫游客户端并自动删除，以防止冲突。如果现已安装的 Umbrella 漫游客户端与某项 Umbrella 服务订用相关联，会将该项服务订用自动迁移至 Umbrella 漫游安全模块，除非 OrgInfo.json 文件与配置用于网络部署或预部署的 AnyConnect 安装程序处于 Umbrella 模块目录中的同一位置。您也可能希望在部署 Umbrella 漫游安全模块之前手动卸载 Umbrella 漫游客户端。

获得思科 Umbrella 帐户

Umbrella 控制面板 (http://dashboard.umbrella.com/) 是登录页面，您可在此获得用于要包括在您的部署中的 AnyConnect Umbrella 漫游安全模块的配置文件 (OrgInfo.json)。您还可以在此对漫游客户端活动的策略和报告进行管理。

从控制面板下载 OrgInfo 文件

OrgInfo.json 文件包含关于您的 Umbrella 控制面板实例的具体信息，可让漫游安全模块了解向哪里报告，以及需要实施哪些策略。

要为部署 AnyConnect Umbrella 漫游安全模块做好准备，请从 Umbrella 控制面板获取 OrgInfo.json 文件 (https://dashboard.umbrella.com)。

单击“身份 (Identities)”菜单结构中的**漫游计算机 (Roaming Computers)**，然后单击页面左上角的 + 符号。向下滚动到 AnyConnect Umbrella 漫游安全模块并单击**模块配置文件 (Module Profile)**。有关具体说明/部署步骤以及软件包和文件的具体信息，请参阅 AnyConnect 部署概述。

注释 在首次部署 OrgInfo.json 文件时，会将该文件复制到数据子目录 (/umbrella/data) 中，还会在该子目录中创建几个其他注册文件。因此，如果您需要部署替代 OrgInfo.json 文件，则必须删除该数据子目录。或者，您也可以卸载 Umbrella 漫游安全模块（这将删除该数据子目录），然后使用新 OrgInfo.json 文件重新安装。

安装和运行 Umbrella 漫游安全

在部署 AnyConnect 时，Umbrella 漫游安全模块是您可以引入以启用额外功能的众多可选模块之一。

要解释 Umbrella 安全模块的状态和条件，请参阅 AnyConnect 插件：Umbrella 漫游安全客户端管理员指南。

对于 Windows 7 SP1 用户，我们建议您在安装和首次使用之前安装 Microsoft .NET framework 4.0。在启动时，Umbrella 服务将检查是否已安装了 .NET framework 4.0（或更高版本）。如果未检测到，则不会激活 Umbrella 漫游安全模块，并将显示一条消息。下载然后安装 .NET Framework，必须重新启动才能激活 Umbrella 漫游安全模块。

配置 OrgInfo.json 文件

OrgInfo.json 文件包含关于您的 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。可以使用 CLI 或 GUI 从 ASA 或 ISE 来部署 OrgInfo.json 文件并启用 Umbrella 漫游安全模块。下面的步骤首先描述了如何从 ASA 启用，然后描述了如何从 ISE 启用：

ASA CLI

1. 将您从 Umbrella 控制面板 (https://dashboard.umbrella.com) 获得的 OrgInfo.json 上传到 ASA 文件系统。
2. 发布以下命令，针对您的配置根据需要调整组策略名称。

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. 导航到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。
2. 选择 **Add**。
3. 为简档命名。
4. 从 Profile Usage 下拉菜单中选择 Umbrella 安全漫游客户端类型。OrgInfo.json 文件将填充在 Profile Location 字段中。
5. 单击**上传 (Upload)**，然后浏览到您从控制面板下载的 OrgInfo.json 文件的位置。
6. 将其与 Group Policy 下拉菜单上的 DfltGrpPolicy 关联起来。请参阅启用其他 AnyConnect 模块以在组策略中指定新模块名称。

ISE

按照以下步骤操作，以从 ISE 启用：

1. 上传来自 Umbrella 控制面板 https://dashboard.umbrella.com 的 OrgInfo.json。
2. 重命名文件 OrgInfo.xml。
3. 按照配置 ISE 以部署 AnyConnect中的步骤操作。

云更新

Umbrella 漫游安全模块可从 Umbrella 云基础设施为所有已安装的 AnyConnect 模块提供自动更新。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。

默认情况下，将禁用通过云更新进行自动更新。要为 Umbrella 漫游安全和 AnyConnect 的其余模块启用云更新，请登录到 Umbrella 控制面板。在**身份 (Identities) > 漫游计算机 (Roaming Computers)** > 设置图标（齿轮图标）下，选中**无论何时发布新版本，都自动更新 AnyConnect，包括 VPN 模块 (Automatically update AnyConnect, including VPN module, whenever new versions are released)**。更新将在 VPN 处于活动状态时进行。默认情况下，不会选择此选项。

需要考虑以下有关云更新的情况：

- 只会更新当前安装的软件模块。
- 不支持定制、本地化和任何其他部署类型。
- 更新仅在登录到桌面时才会进行，如果建立了 VPN，则不会进行更新。
- 当禁用更新时，最新软件功能和更新将不可用。
- 禁用云更新对其他更新机制或设置（例如网络部署、延迟更新等）没有影响。
- 云更新将忽略装有较新、未发布的版本（例如临时版本和修补版本）AnyConnect 的设备。

配置安全策略以及审核报告

您必须有思科 Umbrella 漫游帐户，才能接受保护、查看报告信息以及配置策略。请访问 https://docs.umbrella.com/product/umbrella/ 以了解深入说明，或请访问 https://support.umbrella.com 以了解更多信息。

在安装后，可在 90 分钟至 2 小时后在您的 Umbrella 控制面板中看到漫游计算机。导航到 https://dashboard.umbrella.com 进行身份验证，然后转到**身份 (Identities) > 漫游计算机 (Roaming Computers)**，将显示漫游客户端的列表（包括处于活动状态和非活动状态的漫游客户端），以及关于每个已安装客户端的详情。

最初将为您的漫游计算机应用包含基本安全筛选级别的默认策略。此默认策略可在控制面板的“策略”(Policies) 部分（或“配置”(Configuration) > “思科 Umbrella 帐户的策略”(Policy for Cisco Umbrella accounts)）中找到。

可在 Policies 部分下找到漫游客户端的报告。选中 Activity Search 报告以查看来自装有 Umbrella 漫游安全模块并已关闭 VPN 的计算机的 DNS 流量。

对诊断进行解读

您应运行 DART 报告，以诊断任何思科 Umbrella 漫游安全模块问题。有关 Umbrella 的问题和故障排除详情，请参阅 https://docs.umbrella.com/umbrella-user-guide/docs/appendix-c-troubleshooting。

AnyConnect Umbrella 安全 Web 网关模块

AnyConnect Umbrella Roaming Security 模块提供 DNS 层的安全保护，而 AnyConnect Umbrella Secure Web Gateway (SWG) Agent 模块则在终端上提供了一层安全保护，提高了更多部署场景的灵活性和可能性。Umbrella SWG 允许您在非预期和预期两种情况上安全地对 Web 流量进行身份验证和重定向。此实施需要从 Umbrella 增订 SIG Essentials 或 SIG。

SWG 客户端将加密信头插入 HTTP 请求，头端提取信头，对其进行解密，并使用其用户数据进行身份和策略的确定和实施。同样，对于 HTTPS 流量，SWG 客户端使用 SWG 头端发起 HTTP 连接请求，而连接请求会传输加密报头，这些信头会被提取、解密并用于身份/策略确定和实施。

默认情况下，SWG 在端口 80 和 443 上拦截 HTTP 或 HTTPS 流量。可以使用 Umbrella 云配置添加非标准端口（除 80 和 44 之外）。配置后，除默认标准端口外，SWG 还会在这些额外端口上侦听 HTTP/HTTPS 流量。

通过值得信赖的网络检测，用户可以选择在值得信赖的网络上停用 SWG。在 Umbrella 云中配置此设置后，如果 AnyConnect VPN 隧道处于活动状态，则 SWG 功能将在值得信赖的网络上禁用。“UI 统计信息”(UI Statistics) 窗口中显示的网络保护状态反映了状态的任何更改。

注释 配置此设置后，还会在出现由 Umbrella 的 DNS 保护状态导致的某些错误（例如 Umbrella 解析器无法访问）时停用 SWG。

任何不应代理的域或 IP 地址可在 Umbrella 控制面板的“部署”>“域管理”下定义。不支持通配符，但 Umbrella 将匹配父级域下属的任何子域；例如，如果 example.com 进入域管理列表，则 www.example.com 也将匹配并被跳过。以无类域间路由 (CIDR) 表示法输入 IP 地址。目前仅支持 IPv4 地址。

如果 AnyConnect 无法打开与 Umbrella 代理的连接，则默认情况下 AnyConnect 会打开失败，从而允许直接访问用户。您不能配置这种硬编码行为。

有关这些 Umbrella UI 配置的其他信息，请参阅《思科 Umbrella SIG 用户指南》 。

SWG 的局限性

- 如果安装了 AnyConnect 的本地主机也配置了代理自动配置 (PAC) 文件，PAC 文件优先于 AnyConnect。
- 当前仅支持 IPv4。
- 本地代理不受支持。
- 安装后，Umbrella SWG Agent 可能需要长达 50 分钟的时间与 Umbrella 云同步并接收其配置。不过，默认网络策略应一直应用到同步发生。

Umbrella SWG 的安装和升级

AnyConnect Umbrella SWG 模块仅适用于 Windows 或 macOS，不需要 AnyConnect 核心 (VPN)。但是，如果 AnyConnect 核心 (VPN) 与 AnyConnect Umbrella SWG Agent 一起安装，必须在 VPN 配置文件中启用 *AllowLocalProxyConnections* 设置。

系统支持通过 ASA 或 ISE 进行预部署和 Web 部署。

通过伞云支持云升级。

Umbrella SWG 日志文件和消息

Umbrella 漫游客户端以 SWGConfig.json 文件格式将配置信息发送到 AnyConnect。SWGConfig 的日志文件和消息存储在以下位置：

- Windows—C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG
- macOS-/opt/cisco/anyconnect/umbrella/swg/

漫游安全磁贴中的状态

您可以在“高级统计信息”窗口中验证 SWG 的状态。在该窗口的漫游安全磁贴中，Web 保护状态表示以下其中一项：

- 已禁用 - Umbrella 服务已关闭
- 受保护 — acswgagent 正在运行
- 未受保护 — acswgagent 未运行

- 配置错误 — SWGConfig.json 中的值不正确
- 云服务不可用-无法访问伞代理

有关 Umbrella SWG Agent 的详细统计信息，请打开 AnyConnect UI 并导航到漫游安全分支，以查看重定向到 Umbrella 代理的 HTTP 请求数、重定向到 Umbrella 代理的 HTTPS 请求数、无法重定向到代理的请求数以及 AnyConnect 连接到的 Umbrella 代理。错误和信息性消息记录在邮件历史记录中。

Umbrella SWG 故障排除

如果您在“日志文件选择”窗口中选中“Cisco AnyConnect Umbrella 漫游安全模块”，则运行 DART 捆绑包时，它将包括 SWGConfig.json 和 SWG 相关的日志。转到 http://httpbin.org/ip 以检查流量是否到达 Umbrella 代理。如果您遇到连接重置，请发送 HTTP 请求以查看响应代码：

- 如果 HTTP 响应代码为 452，请检查客户端的时钟是否同步或者时间戳是否不正确。恶意用户可能正在尝试重放信头。
- 如果 HTTP 响应代码为 401，则密钥不是最新的。在 "伞控制面板" 上检查设备的上次同步时间。