在公司网络上配置Umbrella漫游客户端

目录

简介

本文档介绍贵公司网络上的Umbrella漫游客户端的配置。

概述

Umbrella漫游客户端是保护远程用户的理想工具，但它也可以保护企业网络上的用户，从而增加另一层安全性。根据业务需求，有些管理员希望继续保护企业网络上的Umbrella漫游客户端，而其他管理员则希望让Umbrella漫游客户端“后退”以利于其他Umbrella策略。

Umbrella为Umbrella漫游客户端进入网络时的操作方式提供了灵活性。本文概述了这些不同的方法。

目标

问： 为什么要在公司网络上禁用Umbrella漫游客户端？

通常无需禁用Umbrella漫游客户端即可使内部和外部DNS正常工作。Umbrella漫游客户端使用域管理功能将您的内部DNS流量定向到您的普通DNS服务器。这样，当Umbrella漫游客户端在网络中的终端上运行时，您可以同时保持保护和连接。

但是，有时会有理由考虑禁用漫游客户端保护……

- 为离开网络的漫游用户提供不同的“网内”和“网外”策略。
- 在公司网络上使用内部DNS服务器在缓存和减少传出DNS流量方面有一些优势。
- Umbrella漫游客户端定期发送探测消息以验证与Umbrella的连接。当您拥有大量客户端时，可能不需要额外的流量。

问：我为什么要让Umbrella漫游客户端在我的公司网络上保持启用状态？

另一方面，始终启用漫游客户端也有很好的理由：

- 确保Umbrella漫游客户端计算机始终使用相同的策略。
- 始终在报告中可识别Umbrella漫游客户端的主机名（而不是网络身份）— 用于精细报告。
- 漫游客户端使用“加密DNS”流量增强隐私
- 对于安全Web网关用户（使用AnyConnect），客户端必须保持启用状态以提供SWG Web过滤。

操作模式

始终在线

即使在公司网络中使用，Umbrella漫游客户端也可以保持打开。在此模式下，使用Umbrella漫游客户端身份配置策略，并且此身份显示在报告中。

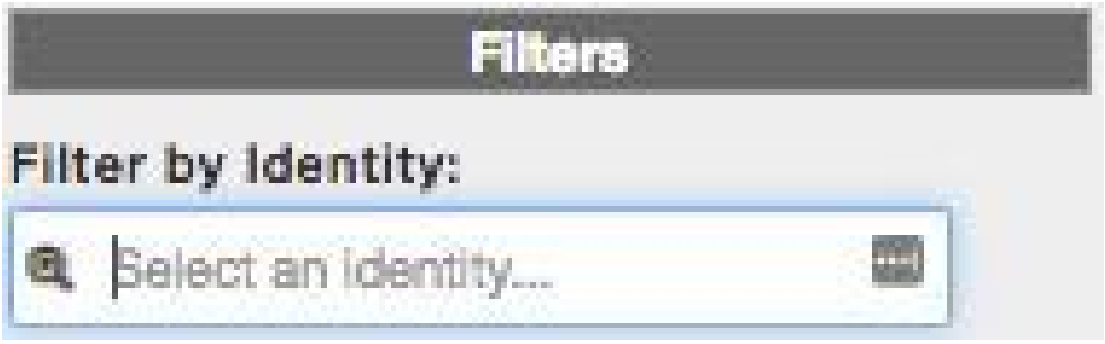
策略	始终使用Umbrella漫游客户端身份。
报告	Umbrella漫游客户端身份始终显示在提供每计算机粒度的报告中
DNS流量	• Umbrella漫游客户端继续将DNS查询直接发送到Umbrella，即使在公司网络中也是如此。 • 发送到Umbrella的查询经过加密，提供额外的安全性。 • 对“内部域”的查询将路由到您的普通DNS服务器，而不会发送到Umbrella。
探测消息	Umbrella漫游客户端继续发送探测消息以确定Umbrella的可用性。

如何配置“Always ON”模式：

1. 导航到身份 > 漫游计算机。
2. 点击(漫游客户端设置)图标。
3. 清除Disable DNS redirection while on an Umbrella Protected Network，然后单击Save。
4. 为Umbrella漫游客户端创建单独的策略，并确保它是最高优先级（位于列表顶部）。Umbrella漫游客户端策略的优先级必须高于任何基于网络身份的策略。

使用常规网络策略

Umbrella漫游客户端已启用并继续直接与Umbrella通信，但是，网络身份用于策略和报告目的。只需将网络策略设置为比Umbrella漫游客户端策略更高的优先级即可激活此模式。

策略	在受保护的网络上使用网络策略。这允许不同的开/关网络策略。
报告	• 报告与作为主要身份的网络身份相关联。 • 报告仍允许您通过Umbrella漫游客户端主机名进行搜索，以便仅过滤该客户端的结果。 
DNS流量	• Umbrella漫游客户端继续将DNS查询直接发送到Umbrella，即使在公司网络中也是如此。 • 发送到Umbrella的查询经过加密，提供额外的安全性。 • 对“内部域”的查询将路由到您的普通DNS服务器，而不会发送到Umbrella。
探测消息	Umbrella漫游客户端继续发送探测消息以确定Umbrella的可用性。

如何“使用常规网络策略”:

1. 导航到身份 > 漫游计算机。
2. 点击(漫游客户端设置)图标。
3. 清除Disable DNS redirection while on an Umbrella Protected Network，然后单击Save。
4. 为您的网络创建单独的策略。 确保您的网络策略的优先级高于任何基于漫游客户端的策略。

在受保护网络后禁用（适用于小型网络）
当Umbrella漫游客户端检测到它位于受保护的网络时，它可以“后退”。这意味着网络身份用于策略和报告目的。

此模式的行为类似于“使用常规网络策略”模式，不同之处在于Umbrella漫游客户端实际上会禁用自身，并且不会干扰DNS流量。

策略	在受保护的网络上使用网络策略。这允许不同的开/关网络策略。
报告	当在受保护网络上时，不存在对报告的每台计算机粒度。报告仅与网络身份相关联。
DNS流量	当在受保护网络上时，Umbrella漫游客户端不会干扰DNS查询，它们会转到正常的内部DNS服务器。
探测消息	Umbrella漫游客户端继续发送探测消息，以确定它是否处于受保护的网络上。

如何在受保护网络后面配置Disable:

1. 导航到身份 > 漫游计算机。
2. 点击(漫游客户端设置)图标。
3. 选择Disable DNS redirection while on an Umbrella Protected Network，然后单击Save。
4. 导航到Policies > Policies List。
5. 为您的网络创建单独的策略。 确保您的网络策略的优先级高于任何基于Umbrella漫游客户端的策略。
6. 您的本地DNS服务器必须转发到Umbrella解析程序，并且必须在Umbrella控制面板中正确注册。
7. 要使用此功能，客户端工作站使用的出口IP必须与内部DNS服务器使用的出口IP注册到相同的网络身份。有关完整详细信息，请参阅本文。

在受信任网络域后禁用（适用于大型网络）

现在可以选择客户配置的“受信任网络域”。 客户端尝试解析此DNS域（A记录），并在域成功解析时禁用保护。 这是仅供内部使用的DNS记录，仅当客户端位于公司网络时才解析。

策略	只要检测到受信任域，客户端就会回退，但不一定接收Umbrella策略或过滤。 我们建议添加其他伞状功能(例如，网络保护)，确保策略仍应用于公司网络。

报告	只要检测到受信任域，客户端就会回退，但不一定接收Umbrella策略或过滤。 如果网络受其他Umbrella功能(例如网络保护)，则流量会出现在网络身份下的报告中。
DNS流量	当在受信任网络上时，Umbrella漫游客户端不会干扰DNS查询，它们会转到正常的内部DNS服务器。
探测消息	Umbrella漫游客户端在此状态下禁用其大部分DNS“探测”测试，从而大大减少了漫游客户端生成的流量。

如何配置受信任网络域：

1. 在内部DNS服务器上创建DNS A记录(例如，magic.mydomain.tld)。
    1. 记录必须是“子域”（最少3个DNS标签）
    2. 记录必须解析为内部RFC-1918地址
    3. 请注意确保记录不公开存在
2. 导航到身份 > 漫游计算机。
3. 点击(漫游客户端设置)图标。
4. 选择Trusted Network Domain选项并输入域名(例如magic.mydomain.tld)。 Click Save.

将Umbrella漫游客户端与Umbrella虚拟设备配合使用

作为Umbrella“Insights”产品的一部分(在Platform and Insights产品包中)，我们提供在网络中充当DNS转发器的虚拟设备(VA)。此VA是了解网络中DNS请求源的关键，也是我们的Active Directory集成所必需的。

默认情况下，如果Umbrella漫游客户端检测到VA正用于DNS转发，则它会禁用自身。如果VA已分配为DNS服务器（使用DHCP或静态设置），则Umbrella漫游客户端会检测到此情况并禁用自身。

VA回退

策略	启用VA回退后，VA身份用于决定所选策略。可以基于以下身份创建策略： • AD用户（仅当启用AD集成时） • AD计算机（仅当启用AD集成时） • 内部网络 • Umbrella站点名称。

	有关策略优先级的详细信息，请单击此处。
报告	启用VA回退后，Umbrella漫游客户端在VA后面被禁用，并且不在报告中显示。报告记录为： • AD用户（仅当启用AD集成时） • AD计算机（仅当启用AD集成时） • 内部网络 • Umbrella站点名称。 此外，还会记录每个请求的内部客户端IP地址。 
DNS流量	• Umbrella漫游客户端不会干扰DNS查询，它们会转到虚拟设备。 • VA将外部DNS查询转发到Umbrella（加密）。 • VA会根据情况路由内部DNS查询，并将查询转发到已配置的内部DNS服务器。
探测消息	Umbrella漫游客户端仍然向Umbrella发送探测消息，但速度有所降低。

如何配置VA回退：

1. 此功能默认启用，但您可以检查其状态（或者将其禁用）
2. 导航到身份 > 漫游计算机。
3. 点击(漫游客户端设置)图标。
4. 选择VA回退选项

Cisco Umbrella AnyConnect漫游安全模块

Cisco AnyConnect的Umbrella模块支持上述所有相同的工作模式。 还提供另外两种特定的AnyConnect模式。 在Identities > Roaming Computers页面上的Umbrella Dashboard中可启用这两种模式，但是，AnyConnect VPN配置文件中需要其他配置。

- 请遵守AnyConnect受信任网络检测。
  当Cisco AnyConnect确定Umbrella Security模块位于受信任网络时，此功能会将其禁用。 这依赖AnyConnect的受信任网络检测功能来识别网络。 可信域、DNS服务器和URL可用于识别您的公司网络。 有关详细信息，请参阅AnyConnect文档。
- 当全通道VPN会话处于活动状态时，禁用漫游客户端
  启用此功能后，当AnyConnect连接到全通道（或全通道DNS）VPN时，Umbrella模块被禁用。

禁用后，漫游客户端不会过滤DNS流量，因此必须确保您的网络受其他安全功能（如我们的网络保护功能）的保护。

更多信息

如果您希望在公司网络上禁用漫游客户端，但需要更多控制，或者希望讨论其他选项，请联系Cisco Umbrella支持。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。