Network Visibility Module

关于 Network Visibility Module

由于用户越来越多地在非托管设备上操作，因此企业管理员对网络内部和外部的可视性下降。Network Visibility Module (NVM) 可以从本地或外部终端收集丰富的流上下文信息；当与 Cisco Secure Cloud Analytics 等思科解决方案或 Splunk 等第三方解决方案配合使用时，它能够提供对网络连接设备和用户行为的可视性。然后，企业管理员可以执行容量和服务规划、审计、合规性检查和安全性分析。Network Visibility Module 提供以下服务：

- 通过监控应用的使用情况，更好地依据事实改进网络设计（对 nvzFlow 协议规范中的 IPFIX 收集器元素加以扩展：https://developer.cisco.com/site/network-visibility-module/）。
- 对应用、用户或终端进行逻辑分组。
- 通过查找潜在异常，帮助跟踪企业资产并规划迁移活动。

利用此功能，您可以选择是否不将整个基础设施部署作为遥测对象。Network Visibility Module 可收集终端遥测信息，提高以下内容的可视性：

- 设备 - 终端，不考虑其位置
- 用户 - 登录到终端的用户
- 应用 - 生成流量的应用
- 位置 - 生成流量的网络位置
- 目的地 - 流量发往地的实际域名 (FQDN)

在一个受信任的网络中，Cisco Secure Client Network Visibility Module 将流记录导出到收集器（例如 Cisco Secure Cloud Analytics）或第三方供应商（例如 Splunk），由其进行文件分析并提供 UI 接口和报告。流记录提供关于用户功能的信息，相关值按 ID 导出（例如 LoggedInUserAccountType 导出为 12361，ProcessUserAccountType 导出为 12362，ParentProcessUserAccountType 导出为 12363）。有关在 Splunk 上构建的思科终端安全分析 (CESA) 的详细信息，请参阅 http://www.cisco.com/go/cesa。由于大多数企业 IT 管理员可能需要利用该数据构建各自的可视化模板，因此我们通过 Splunk 应用插件提供了一些示例基础模板。

桌面 Cisco Secure Client 上的 NVM

过去，流量收集器提供相应功能来收集出入交换机或路由器的一个接口的 IP 网络流量。它可以确定网络中的拥塞来源、流量路径，但没有多少其他信息。通过终端上的 Network Visibility Module，可以通过丰富的终端上下文（例如设备类型、用户、应用等）来增强流。这使得流记录更具可操作性，具体取决于收集平台的功能。通过 IPFIX 发送的 Network Visibility Module 所提供的导出数据与思科 NetFlow 收集器以及其他第三方流收集平台（如 Splunk、IBM Qradar、LiveAction）兼容。有关其他信息，请参阅特定于平台的集成文档，例如，可访问以下网址了解 Splunk 集成的信息：https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html。

在版本 4.9 或更高版本中使用 Network Visibility Module 收集器时，您必须使用 Splunk 应用 3.x 查看其他参数。

如果启用此功能，则从 ISE 或 Cisco Secure Firewall ASA 头端推送 Network Visibility Module 的 Cisco Secure Client 配置文件。与您在网络访问管理器上的操作一样，在 ISE 头端，您可以使用独立配置文件编辑器，生成 Network Visibility Module 服务配置文件 XML，上传至 ISE 并对照新的 Network Visibility Module 模块进行映射。在 Cisco Secure Firewall ASA 头端，您可以使用独立配置文件编辑器或 ASDM 配置文件编辑器。

当 VPN 状态更改为已连接，或者当终端处于受信任的网络中时，Network Visibility Module 会收到提示。

注释 如果您将 Network Visibility Module 与 Linux 一起使用，请确保已完成在 Linux 上使用 Network Visibility Module中的预备步骤。

独立 NVM

对于没有 Cisco Secure Client 部署或正在使用其他 VPN 解决方案的用户，您可以安装 Network Visibility Module 独立软件包来满足 Network Visibility Module 的需求。此软件包独立运行，但它提供与现有 Cisco Secure Client Network Visibility Module 解决方案相同的流收集级别。如果安装独立 Network Visibility Module，活动进程（例如 macOS 上的活动监视器）指出其使用情况。

独立 Network Visibility Module 使用 Network Visibility Module 配置文件编辑器 进行配置，且值得信赖的网络检测 (TND) 配置为必填项。使用 TND 配置，Network Visibility Module 确定终端是否在企业网络上，然后应用适当的策略。

故障排除和日志记录仍通过 Cisco Secure Client DART （可从 Cisco Secure Client 软件包进行安装）完成。

部署模式

您可以使用 Cisco Secure Client 软件包部署 Network Visibility Module 1) 或 2) 使用独立 Network Visibility Module 软件包（仅在 Cisco Secure Client 桌面上）。有关将部署为 Cisco Secure Client 软件包的一部分的步骤，请参阅 "部署 *Cisco Secure Client* " 一章。否则，您最初可以通过下载以下软件包来安装独立 Network Visibility Module，而无需完整的 Cisco Secure Client 软件包：

- cisco-secure-client-win-[版本]-nvm-standalone-k9.msi（适用于 Windows）
- cisco-secure-client-macos-[版本]-nvm-standalone.dmg（适用于 macOS）
- cisco-secure-client-linux64-[版本]-nvm-standalone.tar.gz（适用于 Linux）

此外，Network Visibility Module 是思科 XDR 的核心部分。您可以通过在终端上安装 XDR 默认部署，将遥测直接发送到思科 XDR，而无需本地收集器。思科 XDR 使用此数据创建新的检测，将多个事件关联到单个事件中，并填补网络中的不可见性空白。在 XDR 中，您可以导航至“客户端管理”(Client Management) >“部署”(Deployments) 以查看思科 XDR 组织中所有安全客户端部署的列表，并允许用户定义必须在特定部署中的所有计算机上安装的所有软件包和相关配置文件的列表一个组织。有关详细信息，请参阅 XDR 文档。

独立 Network Visibility Module 的正常运行不依赖于 VPN；因此，您可以将其部署在终端上，而无需安装 VPN。

如果已安装独立 Network Visibility Module，则可以无缝地迁移到相同或更高版本的完整 Cisco Secure Client 安装，并且所有 Network Visibility Module 数据文件和配置文件都将保留。

要升级到 Network Visibility Module 独立配置，必须将带外方法（例如 SMS）用于 Network Visibility Module 配置文件。如果在终端上同时需要 VPN 和 Network Visibility Module 功能，我们建议您部署 Cisco Secure Client 软件包以安装 VPN 和 Network Visibility Module，因为不建议进行单独安装。在以下情况下，安装将失败：

- 降级独立 Network Visibility Module
- 安装较旧版本的 Cisco Secure Client Network Visibility Module，其中已存在较新版本的独立 Network Visibility Module。这种情况会导致卸载独立 Network Visibility Module。
- 安装任何版本的独立 Network Visibility Module，其中 Cisco Secure Client Network Visibility Module 已存在

移动 Cisco Secure Client 上的 NVM

Android 版 Cisco Secure Client 的最新版本（可通过 Google Play 商店获取）中包括 Network Visibility Module (NVM)。运行 Samsung Knox 版本 2.8 或更高版本的 Samsung 设备上支持 Network Visibility Module。目前不支持任何其他移动设备。

Android 上的 Network Visibility Module 是服务配置文件配置的一部分。要在 Android 上配置 Network Visibility Module，需使用 Cisco Secure Client Network Visibility Module 配置文件编辑器生成 Cisco

Secure Client Network Visibility Module 配置文件，然后再使用移动设备管理 (MDM) 将该配置文件推送到 Samsung 移动设备。

准则

- 运行 Samsung Knox 版本 3.0 或更高版本的 Samsung 设备上支持 Network Visibility Module。目前不支持任何其他移动设备。
- 在移动设备上，支持通过 IPv4 或 IPv6 连接到 Network Visibility Module 收集器。
- 不支持在基于 Java 的应用上收集数据流量。

如何使用 Network Visibility Module

您可以将 Network Visibility Module 用于以下场景：

- 在发生安全事件后，审核用户网络历史记录的潜在泄露。
- 查看系统或管理权限如何影响在用户的设备上正在运行且连接网络的进程。
- 获取运行旧版操作系统的所有设备的列表。
- 确定您的网络中的哪些应用正在占用最高的网络带宽。
- 确定您的网络中正在使用多少个 Firefox 版本。
- 确定您的网络中 IPv6 占 Chrome.exe 连接的百分比。

Network Visibility Module 的收集参数

在三个系统日志数据源：每一数据流、终端身份和接口信息中，唯一标识符 (UDID) 字段可用作关联这些源之间记录的方式。您可以使用 InterfaceInfoUDID 字段将每一数据流记录与接口信息记录相关联，以便收集有关该特定接口的详细信息。以下参数在终端收集并导出到收集器：

表 *1:* 终端身份

参数	说明/注释
虚拟站名称	在终端上配置的设备名称（例如，Boris-Macbook） 加入域的计算机将采用以下格式：<machinename>.<domainname>.<com>（例如，CESA-WIN10-1.mydomain.com） 对 Android 为空；Samsung 未提供。

参数	说明/注释
UDID	通用唯一标识符。唯一标识与每个流量对应的终端。此 UDID 值还通过桌面中的 Cisco Secure Firewall 终端安全评估 和移动设备中的 ACIDex 来报告。
操作系统名称	终端操作系统的名称（例如，WinNT）
OS 版本	终端操作系统的版本（例如，6.1.7601）
操作系统版本	操作系统版本，例如 Windows 8.1 Enterprise Edition
系统制造商	终端制造商（例如，联想、苹果等）
系统类型	针对 Android 设置为 `arm`。 针对其他平台，设置为 `x86` 或 `x64`。
代理版本	终端上运行的 Network Visibility Module 客户端软件的版本。格式通常为 major_v.minor_v.build_no
时间戳	终端数据的绝对时间戳（以毫秒为单位）。
AMP GUID	Cisco Secure Endpoint (AMP) 的唯一终端 ID

表 *2*: 接口信息

参数	说明/注释
终端 UDID	与 UDID 相同。
InterfaceInfoUID	接口元数据的唯一 ID。用于从 InterfaceInfo 记录查找接口元数据。
接口索引	操作系统报告的网络接口索引。
接口类型	接口类型，例如有线、无线、蜂窝、VPN 等。
接口名称	操作系统报告的网络接口/适配器名称。
接口详细信息列表	状态和 SSID，InterfaceDetailsList 的属性。表示接口的网络状态（受信任或不受信任），以及连接的 SSID。
接口 MAC 地址	接口的 MAC 地址。 仅限桌面。对 Android 为空（不受支持）。
时间戳	接口记录的绝对值（以毫秒为单位）。

表 *3:* 流信息

参数	说明/注释
源 IPv4 地址	终端上生成流的源接口的 IPv4 地址。
目的 IPv4 地址	终端上生成流的目标接口的 IPv4 地址。
源传输端口	终端上生成流的源端口号。
目标传输端口	终端上生成流的目标端口号。
流方向	在终端观察到的流的方向。它是从终端收集的强制性参数。这两个值是 0：入口流量或 1：出口流量。
源 IPv6 地址 (Source IPv6 Address)	终端上生成流的源接口的 IPv6 地址。 对 Android 为空（不受支持）。
目的 IPv6 地址 (Destination IPv6 Address)	终端上生成流的目标接口的 IPv6 地址。 对 Android 为空（不受支持）。
开始秒 结束秒	流量开始或结束的绝对时间戳（以秒为单位）。
开始（毫秒） 结束（毫秒）	流量开始或结束的绝对时间戳（以毫秒为单位）。
流量 UDID	与 UDID 相同。
当前登录用户	物理设备上登录的用户名，格式为“机构\主体” 对 Android 为空（不受支持）。
已登录用户帐户类型	已登录用户的帐户类型。 对 Android 为空（不受支持）。
进程 ID	发起网络流的进程的进程 ID。
进程名称	在终端上生成网络流的可执行文件名称。
进程散列	在终端上生成网络流的可执行文件的唯一 SHA256 哈希值。
进程帐户	在终端上生成网络流的应用执行情景所属的完全限定帐户，格式为“机构\主体”。 对 Android 为空（不受支持）。
进程帐户类型	进程帐户的帐户类型。 对 Android 为空（不受支持）。

参数	说明/注释
进程路径	发起网络流的进程的文件系统路径 对 Android 为空（不受支持）。
进程参数	发起网络流的进程的命令行参数，不包括进程路径。 对 Android 为空（不受支持）。
父进程 ID	发起网络流的进程的父进程 ID。
父进程名称	在终端上生成网络流的应用的父进程名称。
父进程哈希值	在终端上生成网络流的应用的父进程可执行文件的唯一 SHA256 哈希值。针对 Android 设置为 0。
父进程帐户	在终端上生成网络流的应用父进程执行情景所属的完全限定帐户，格式为“机构\主体”。 对 Android 为空（不受支持）。
父进程帐户类型	父进程帐户的帐户类型。 对 Android 为空（不受支持）。
父进程路径	发起网络流的进程父级的文件系统路径。 对 Android 为空（不受支持）。
父进程参数	发起网络流的进程父级的命令行参数，不包括父进程路径。 对 Android 为空（不受支持）。
DNS 后缀	在终端上与流量关联的接口上配置。
L4ByteCountIn	在第 4 层终端（不包括 L4 信头）上的给定流中下载的总字节数。
L4ByteCountOut	在第 4 层终端（不包括 L4 信头）上的给定流中上传的总字节数。
目标主机名	在终端上解析为目标 IP 的实际 FQDN
HTTP 主机	HTTP/1.1 流量的 HTTP 主机报头的内容。
接口 UID	与接口信息表中的接口 UID 相同。用于从连同 UDID 一起发送的接口记录中识别此流的接口信息。

参数	说明/注释
模块名称列表	生成流的进程托管的模块的名称（0个或更多）列表。其中可包括公共容器中的主要 DLL，例如 dllhost、svchost、rundll32 等。它还可以包含其他托管组件，例如 JVM 中 jar 文件的名称。 对 Android 为空（不受支持）。
模块哈希值列表	与模块名称列表关联的模块的 SHA256 哈希值（0 个或更多）列表。 对 Android 为空（不受支持）。
其他登录用户列表	（仅限 Windows）设备上的已登录用户列表（nzFlowLoggedInUser 除外），每个用户的格式为 SessionType:AccountType:Authority\Principal。例如，rdp:8001:ACME\JSmith console:0002:<machine>\Administrator 在升级过程中，默认情况下不报告该参数： 1) 如果 NVM 旧版本中的配置文件没有数据收集策略或包含数据收集策略 2) 如果 NVM 旧版本中的配置文件有不包含数据收集策略，且该配置文件是用4.10配置文件编辑器打开和保存的。 **注释** 对于非系统进程，此字段为空。
进程完整性级别	完整性级别定义进程与另一个对象（文件、进程或线程）之间的信任关系
父进程完整性级别	完整性级别定义父进程与另一个对象（文件、进程或线程）之间的信任关系
流报告阶段	流记录的阶段。0：结束流记录，1：开始流记录，2：定期/中间流记录。

Network Visibility Module 配置文件编辑器

在配置文件编辑器中，配置收集服务器的 IP 地址或 FQDN。您还可以自定义数据收集策略，用于选择要发送哪些类型数据，以及确定数据是否匿名。

Network Visibility Module 可以使用包含 IPv4 地址的单个堆栈 IPv4、包含 IPv6 地址的单个堆栈 IPv6 或双堆栈 IPv4/IPv6，建立与操作系统首选的 IP地址的连接。

移动 Network Visibility Module 仅可以使用 IPv4 建立连接。不支持 IPv6 连接。

注释 当 Network Visibility Module 在受信任网络中时，该模块发送流量信息。默认情况下，不收集任何数据。仅在配置文件中进行了相应配置时才会收集数据，且连接终端后，会继续收集数据。如果在一个不可信网络上进行收集，则会缓存数据，并在终端处于受信任的网络中时发送数据。如果您将收集数据发送到 Cisco Secure Cloud Analytics 7.3.1 及更低版本（或 Splunk 及类似 SIEM 工具之外的工具），则缓存数据会在受信任网络上发送一次，但不会进行处理。对于 Cisco Secure Cloud Analytics 应用程序，请参阅《Cisco Secure Cloud Analytics 企业终端许可证和 NVM 配置指南》。

如果已在 Network Visibility Module 配置文件中配置了 TND，则值得信赖的网络检测由 Network Visibility Module 完成，并且不依赖于 VPN 来确定终端是否位于受信任的网络中。此外，如果 VPN 为已连接状态，则会将终端视作处于受信任网络中，并会发送流信息。NVM 特定的系统日志会显示值得信赖的网络检测使用情况。

直接在 Network Visibility Module 配置文件中配置 TND 时，管理员定义的受信任服务器和证书散列将确定用户位于受信任还是不受信任的网络上。管理员为核心 VPN 配置文件配置值得信赖的网络检测会在核心 VPN 配置文件中另外配置受信任 DNS 域和受信任 DNS 服务器：Cisco Secure Client 配置文件编辑器，首选项（第 2 部分）。

- **桌面 (Desktop)** 或**移动 (Mobile)** - 确定是在桌面还是移动设备上设置 Network Visibility Module。**桌面 (Desktop)** 是默认值。
- **收集器配置**
  - **IP 地址/FQDN (IP Address/FQDN)** - 指定收集器的 IPv4 或 IPv6 IP 地址/FQDN。
  - **端口 (Port)** - 指定收集器正在侦听哪个端口号。
  - **安全 (Secure)** - 确定是否希望 Network Visibility Module 通过 DTLS 安全地将数据发送到收集器。选中此复选框后，Network Visibility Module 将使用 DTLS 进行传输。DTLS 连接要求终端信任 DTLS 服务器（收集器）证书。系统将以静默方式拒绝任何不受信任的证书。

    DTLS 支持需要收集器作为 CESA Splunk 应用 v3.1.0 的一部分，DTLS 1.2 是支持的最低版本。
- **缓存配置**
  - **最大大小 (Max Size)** - 指定该数据库可以达到的最大大小。以前对缓存大小有预设的限制，但您现在可在配置文件中配置它。缓存中的数据以加密格式存储，因此只有拥有根权限的进程可以解密数据。

    一旦达到大小限制，将从空间中丢弃最旧数据，将空间留给新数据。
  - **最大持续时间 (Max Duration)** - 指定您希望将数据存储多少天。如果您还设置了最大大小，则首先达到的限制优先。

    一旦达到天数限制，将从空间中丢弃日期最早的数据，将空间留给日期最近的数据。如果仅配置了“最大持续时间 (Max Duration)”，则没有大小上限；如果二者都被禁用，则大小上限为 50 MB。
- **定期模板 (Periodic Template)** - 指定从终端发出模板的时间间隔。默认值为 1440 分钟。

- **定期流量报告 (Periodic Flow Reporting)**（可选，仅应用于桌面）- 点击以启用定期流量报告。默认情况下，Network Visibility Module 发送连接结束时的流量相关信息 （当禁用此选项时）。如果需要定期的流量相关信息（甚至在这些流量被关闭之前），请在此处设置间隔（以秒为单位）。值为 0 表示在每个流量开始和结束时发送流量信息。如果值为 *n* ，则将在每个流量开始时、每隔 *n* 秒时和结束时发送流量信息。使用此设置跟踪长期运行的连接（甚至在这些连接被关闭之前）。

- **聚合时间间隔 (Aggregation Interval)** - 指定从端点导出数据流的时间间隔。使用 5 秒默认值时，一个数据包中将捕获不止一个数据流。如果时间间隔值为 0 秒，则每个数据包都有一个数据流。有效范围为 0 到 600 秒。

- **限制速率 (Throttle Rate)** - 限制控制以什么速率将数据从缓存发送到收集器，以便尽量减小对最终用户的影响。您可以对实时和缓存数据应用限制（只要存在缓存的数据）。以 Kbps 为单位，输入限制速率。默认值为 500 Kbps。

  在该固定时段后，缓存数据将被导出。输入 0 将禁用该功能。
- **收集模式 (Collection Mode)** - 通过选择收集模式关闭 (collection mode is off)、仅受信任网络 (trusted network only)、仅不受信任网络 (untrusted network only) 或所有网络 (all networks)，指定应从终端收集数据的时间。

- **收集标准 (Collection Criteria)** - 您可以在数据收集时减少不必要的广播，以便仅分析相关数据。通过以下选项控制数据搜集：

  - **广播数据包 (Broadcast packets)** 和**组播数据包 (Multicast packets)**（仅适用于桌面）- 默认情况下，为了提高效率，会关闭广播和组播数据包收集，以便缩短在后端资源上花费的时间。点击该复选框可启用对广播和组播数据包的收集并过滤数据。

  - **仅限 KNOX (KNOX only)**（可选且特定于移动设备）- 选中后，将仅从 KNOX 工作空间收集数据。默认情况下，未选中此字段，将会从工作空间内部和外部收集数据。

- **数据收集策略 (Data Collection Policy)** - 您可以添加数据收集策略，并将它们与网络类型或连接情形相关联。您可以将一种策略应用于 VPN，而将另一种策略应用于非 VPN 流量，因为多个接口可以同时处于活跃状态。

  在点击“添加”(Add) 时，系统显示“数据收集策略”(Data Collection Policy) 窗口。在创建策略时，请记住以下准则：

  - 默认情况下，如果未创建策略或未与网络类型相关联，则将报告和收集所有字段。

  - 每种数据收集策略必须与至少一种网络类型相关联，但您不能将两种策略与同一种网络类型相关联。

  - 具有更具体的网络类型的策略优先。例如，因为 VPN 是受信任网络的一部分，所以包含 VPN 网络类型的策略的优先级高于采用受信任网络为指定网络的策略。

  - 您只能基于所选的收集型号，为网络创建适用的数据收集策略。例如，如果**收集模式 (Collection Mode)** 设置为 **仅受信任网络 (Trusted Network Only)**，您无法为**不受信任网络类型 (Untrusted Network Type)** 创建**数据收集策略 (Data Collection Policy)**。

- 如果从较新版本的 Cisco Secure Client 打开来自较早版本 Cisco Secure Client 的配置文件，它会自动将该配置文件转换为较新的版本。转换过程中会为所有网络添加数据收集策略，用于排除先前匿名的字段。

- **名称 (Name)** - 为您要创建的策略指定名称。

- **网络类型 (Network Type)** - 通过选择 VPN、受信任或不受信任，来确定收集模式，或者应用数据收集策略的网络。如果您选择受信任网络，则策略也适用于 VPN 案例。

- **流过滤器规则 (Flow Filter Rule)** - 定义一组条件和一个操作，可以在满足所有条件时收集或忽略流。您最多可以配置 25 条规则，每条规则最多可以定义 25 个条件。使用“流过滤器规则”(Flow Filter Rule) 列表右侧的向上和向下按钮调整规则的优先级，并对后续规则给予更高的考虑。点击**添加 (Add)** 设置流过滤器规则的组成要素。

  - 名称 (Name) - 流过滤器规则的唯一名称。

  - 类型 (Type) - 每个过滤器规则都有“收集”或“忽略”类型。确定满足过滤器规则时要执行的操作（“收集”[Collect] 或“忽略”[Ignore]）。如果收集，则在满足条件时允许流。如果忽略，则丢弃流。

  - 条件 - 为要匹配的每个字段添加一个条目以及一个运算，以确定字段值对匹配项是否应相等或不相等。每个运算都有一个字段标识符和该字段的对应值。该字段区分大小写，除非您在设置过滤器引擎规则时对规则集应用了不区分大小写操作 (EqualsIgnoreCase)。启用后，规则中设置的 Value 字段中的输入不区分大小写。

- **包括/排除**

  - **类型 (Type)** - 确定要在数据收集策略中**包含 (Include)** 或**排除 (Exclude)** 的字段。默认值为**排除 (Exclude)**。所有未选中的字段都收集起来。未选中任何字段时，将收集所有字段。

  - **字段 (Fields)** - 确定要从终端接收哪些信息以及收集哪些字段的数据以满足策略要求。根据网络类型和包含或排除的字段，Network Visibility Module 将在终端上收集相应数据。

注释 升级期间，如果存在以下情况之一，默认从流信息的报告中排除 ProcessPath、ParentProcessPath、ProcessArgs 和 ParentProcessArgs：

- 如果较旧版本 Network Visibility Module 中的配置文件没有数据收集策略或有包含数据收集策略。
- 如果较旧版本 Network Visibility Module 中的配置文件有排除数据收集策略，并且该配置文件已使用更新版本的配置文件编辑器打开并保存。如果较旧版本 Network Visibility Module 中的配置文件有排除数据收集策略，但该配置文件未使用更新的 4.9 版本（或更高版本）配置文件编辑器打开和保存，则包含这四个字段。

如果 Network Visibility Module 无法计算父进程 ID，则值默认为 4294967295。

FlowStartMsec 和 FlowStopMsec 确定流的纪元时间戳（以毫秒为单位）。

您可以选择接口状态和 SSID，这将指定接口的网络状态为受信任还是不受信任。

- **可选匿名字段 (Optional Anonymization Fields)** - 如果要关联同一终端上的记录，同时保留隐私，请选择所需的字段进行匿名化。然后，它们将作为值的散列而不是实际值发送。字段的子集可用于匿名化。

  标记为包含或排除的字段不可用于匿名；同样，标记为匿名的字段不可用于包含或排除。

- **用于 Knox 的数据收集策略 (Data Collection Policy for Knox)**（**特定于移动设备**）- 该选项用于在选择移动配置文件时指定数据收集策略。要为 Knox 容器创建数据收集策略，请选择“范围”(Scope) 下的**仅 Knox (Knox-Only)** 复选框。除非指定单独的 Knox 容器数据收集策略，否则应用于 Knox 容器流量的设备范围内的数据收集策略也适用于 Knox 容器流量。要添加或删除数据收集策略，请参阅上面的数据收集策略说明。您可以为移动配置文件设置最多 6 个不同的数据收集策略：3 个用于设备，3 个用于 Knox。
- **可接受的使用策略 (Acceptable Use Policy)**（可选且特定于移动设备）- 点击**编辑 (Edit)**，在对话框中为移动设备定义可接受的使用策略。完成后，点击**确定 (OK)**。最多允许 4000 个字符。

  配置 Network Visibility Module 后，此消息会显示给用户。远程用户无法选择拒绝 Network Visibility Module 活动。网络管理员使用 MDM 工具控制 Network Visibility Module。
- **Export on Mobile Network**（**可选且特定于移动设备**）- 指定在设备使用移动网络时，是否允许导出 Network Visibility Module 流。如果启用（默认值），当显示或后续通过 Cisco Secure Client Android 应用中的 **设置 (Settings)** > **NVM-设置 (NVM-Settings)** > > **将移动数据用于 NVM (Use mobile data for NVM)** 复选框来显示“可接受的用户策略”(Acceptable User Policy) 窗口时，最终用户可以覆盖管理员 。如果取消选中**在移动网络上导出 (Export on Mobile Network)** 复选框，当设备使用移动网络时，不会导出 Network Visibility Module 流，最终用户无法对其进行更改。

- **值得信赖的网络检测 (Trusted Network Detection)** — 此功能可检测终端是否实际上位于企业网络中。Network Visibility Module 使用网络状态来确定何时导出数据并应用相应的数据收集策略。点击**配置 (Configure)** 以设置值得信赖的网络检测的配置。SSL 探测会发送到已配置的受信任前端，如果可访问，则前端会使用证书响应。然后，系统将根据配置文件编辑器中的散列设置提取指纹（SHA-256 散列）并将其与之匹配。成功匹配表明终端位于受信任的网络中；但是，如果前端无法访问，或者如果证书散列不匹配，则系统会将终端视为位于不受信任的网络中。

注释 从内部网络的外部进行操作时，值得信赖的网络检测会执行 DNS 请求并尝试与已配置服务器建立 SSL 连接。思科强烈建议使用别名，以确保在内部网络以外使用的机器不会通过这些请求泄露您组织的名称和内部结构。

1. **https://** — 输入每个受信任服务器的 URL （IP 地址、FQDN 或端口地址），然后点击**添加 (Add)**）。

注释 代理后的受信任服务器不受支持。

2. **证书散列 (SHA-256)** — 如果与受信任服务器的 SSL 连接成功，则系统会自动填充此字段。否则，您可以通过输入服务器证书的 SHA-256 散列并点击**设置 (Set)** 来手动对其进行设置。
3. **受信任服务器列表** — 通过此过程可以定义多个受信任服务器。（至多 10 个。）由于服务器会按已配置的顺序尝试值得信赖的网络检测，因此您可以使用**上移**和**移动 |向下**按钮来调整该顺序。如果终端无法连接到第一台服务器，它会尝试连接第二台服务器，依此类推。在对列表中的所有服务器进行尝试后，终端等待 10 秒后会再进行最后一次尝试。当服务器进行身份验证时，系统会视为终端在受信任的网络中。

将配置文件另存为 `NVM_ServiceProfile.xml`。您必须将配置文件准确保存为此名称，否则 Network Visibility Module 将无法收集和发送数据。

关于流过滤器

添加流过滤器会将当前数据收集策略扩展为仅以字段为中心，其中为每个流中的给定字段配置操作。通过“流过滤器”，您可以创建和应用规则以收集或忽略整个流（而不只是特定的字段），从而只监控感兴趣的流量，可能降低存储要求。

规则条件

- 只有在与流数据匹配时满足规则中指定的所有条件时，规则才匹配。
- 所满足的第一个规则会应用于流。
- 如果过滤策略允许，还会在流上应用其余的数据收集策略（包括/排除字段、匿名字段）。
- 使用多个规则的实例，

- 如果没有与流数据匹配的规则，不会对流执行任何操作。此时会遵循默认行为，即收集流。
- 如果规则与流数据匹配，则应用该流规则中指定的操作。不检查后续规则。“Network Visibility Module 配置文件编辑器流过滤器规则”(Flow Filter Rule) 参数中指定的规则顺序指示出现多个匹配时的优先级。

使用通配符、CIDR 和转义序列支持

输入规则条件时，对于 IP 地址，可以使用通配符或 CIDR 表示法定义更广泛的字段值。此外，还可以在字段值中使用某些转义序列。对于 IP 字段，CIDR/斜线符号可以指定规则应匹配的 IP 地址。例如，“192.30.250.00/16”将匹配有通过应用子网掩码“255.255.0.0”得到的路由前缀“192.30.0.0”的所有地址。对于文本字段，可以使用通配符（* 和 ?）和转义序列（*、\? 和 \\）捕获更广泛的输入。例如，登录用户“Jane*”将匹配以“Jane”开头的所有用户名。

实现流量过滤方案的示例配置

要丢弃特定端口（例如端口 53）上的所有 UDP 流量，请使用忽略 *(Ignore)* 类型和两个条件配置流过滤器规则：

- 条件 1：指定流协议等于 UDP。
- 条件 2：指定端口号等于 53。

要仅收集来自一个特定进程（例如 Tor 浏览器）的流量，请使用忽略类型配置过滤器规则，通过添加一个条件丢弃所有其他流：

- 条件 1：指定进程名称不等于 Tor 浏览器。

要仅收集源自子网中仅一个特定 IP 的流量，请配置两个规则：

- 规则 1：设置收集类型的规则，条件是 IPv4 源地址等于 192.168.30.14。
- 规则 2：设置忽略类型的第二个规则，条件是 IPv4 源等于 192.168.30.0/24。

客户反馈模块提供 NVM 状态

部分客户反馈模块集合可以提供关于是否已安装 Network Visibility Module、每日流量和数据库大小等的数据。

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。