网络发现概述

以下主题讨论网络发现：

关于主机、应用和用户数据的检测

系统使用 网络发现和 身份 策略收集网络上流量的主机、应用和用户数据。您可以使用特定类型的发现和身份数据构建全面的网络资产映射，执行调查分析、行为剖析和访问控制并缓解和应对组织最易遭受的漏洞和攻击。

主机和应用数据

主机和应用数据由主机身份源和应用检测器根据网络发现策略中的设置进行收集。托管设备会观察指定网段上的流量。

有关详细信息，请参阅主机和应用检测基础知识， 第 2 页。

用户数据

用户数据由用户身份源根据网络发现和身份策略中的设置进行收集。您可以使用这些数据获取用户感知和用户控制。

有关详细信息，请参阅关于用户身份。

通过日志记录发现和身份数据，您可以利用系统中的许多功能，包括：

- 查看网络映射，网络映射是对网络资产和拓扑的详细表示，可通过对主机和网络设备、主机属性、应用协议或漏洞进行分组来查看。
- 执行应用和用户控制，即，使用应用、领域、用户、用户组和ISE属性条件编写访问控制规则。
- 查看主机配置文件，配置文件可完整展示检测到的主机的所有可用信息。
- 查看控制面板，控制面板提供有关网络资产和用户活动的概览及其他功能。
- 查看关于系统记录的发现事件和用户活动的详细信息。
- 将主机及其运行的任何服务器或客户端与它们易受攻击的漏洞关联起来。

这使您能够识别和减少漏洞，评估入侵事件对您的网络的影响，并优化入侵规则状态，以便它们为您的网络资产提供最大的保护

- 在系统生成具有特定影响标志的入侵事件或特定类型的发现事件时，通过邮件、SNMP 陷阱或系统日志向您发出警报
- 监控组织是否遵守允许的 allow操作系统、客户端、应用协议和协议的列表
- 在系统生成发现事件或检测用户活动时，创建具有会触发和生成关联事件的规则的关联策略
- 记录和使用 NetFlow 连接（如果适用）。

主机和应用检测基础知识

您可以配置网络发现策略，以执行主机和应用检测。

有关详细信息，请参阅概述：主机数据收集和概述：应用检测。

操作系统和主机数据被动检测

被动检测是通过分析网络通信量（以及任何导出的NetFlow数据）来填充网络映射的系统默认方法。被动检测提供有关您的网络资产（如操作系统和正在运行的应用）的情景信息。

如果来自受监控主机的流量不提供主机操作系统的确凿证据，则网络映射将显示最有可能的操作系统。例如，由于在 NAT 设备“后面”的主机，NAT 设备可能看起来正在运行多个操作系统。为了做出最可能的决定，系统使用其为每个检测到的操作系统分配的置信值，以及检测到的操作系统之间的确认数据量。

注释 系统在确定时不考虑报告的“unknown”应用和操作系统。

如果被动检测不准确地识别您的网络资产，请考虑更换托管设备。您还可以使用自定义操作系统指纹和自定义应用检测器来增强系统的被动检测功能。或者，您可以使用主用检测，它不基于流量分析，而是允许您使用扫描结果或其他信息源直接更新网络映射。

操作系统和主机数据主动检测

主动检测会将主动源收集的主机信息添加到网络映射。例如，可使用 Nmap 扫描程序主动扫描网络上的目标主机。Nmap 可发现主机上的操作系统和应用。

此外，主机输入功能可用于将主机输入数据主动添加到网络映射。有两种不同类别的主机输入数据：

- 用户输入数据 - 通过 FirePOWER 系统用户界面添加数据。您可以通过此界面修改主机操作系统或应用身份。
- 托管导入输入数据 - 使用命令行实用程序导入的数据。

系统将为每个主动源保留一个身份。如果运行 Nmap 扫描实例，例如，先前的扫描结果将替代为新的扫描结果。然而，如果运行 Nmap 扫描，然后用结果通过命令行导入的客户端的数据替代这些结果，系统将同时保留来自 Nmap 结果的身份以及来自导入客户端的身份。然后，系统会使用网络发现策略中设置的优先级来确定用作当前身份的主动身份。

请注意，用户输入视为一个源，即使其来自不同的源。例如，如果用户 A 通过主机配置文件设置操作系统，然后用户 B 通过主机配置文件更改该定义，用户 B 设置的定义将保留，而用户 A 设置的定义将丢弃。此外，请注意，用户输入会覆盖所有其他的主动源，并会用作当前身份（如果其存在）。

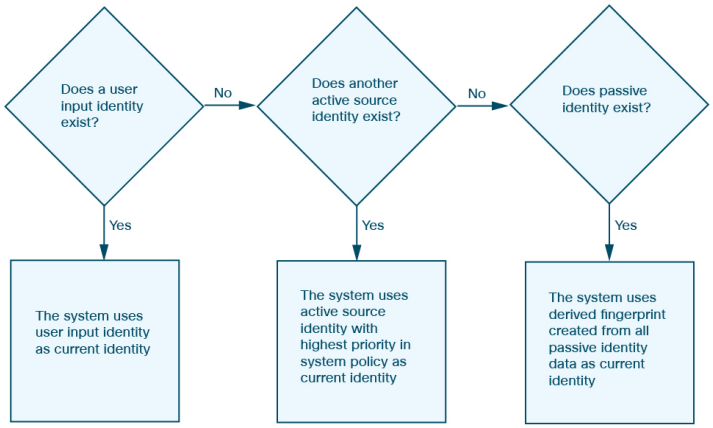
应用和操作系统的当前身份

主机上的应用或操作系统的当前身份是系统发现最有可能正确的身份。

系统会将操作系统或应用的当前身份用于以下用途：

- 分配漏洞至主机
- 影响评估
- 评估针对操作系统标识、主机配置文件合格性以及合规 allow 名单写入的关联规则
- 在工作流程的“主机”(Hosts) 和“服务器”(Servers) 表格视图中进行显示
- 在主机配置文件中进行显示
- 在“发现统计信息”(Discovery Statistics) 页面上计算操作系统和应用统计信息

系统会使用源优先级来确定哪个主动身份应该用作应用或操作系统的当前身份。



例如，如果用户在主机上将操作系统设置为 Windows 2003 Server，则 Windows 2003 Server 为当前身份。针对该主机上的 Windows 2003 Server 漏洞的攻击将被赋予更高的影响，而主机配置文件中为该主机列出的漏洞包括 Windows 2003 Server 漏洞。

对于主机上的操作系统或特定应用，数据库可能保留来自多个源的信息。

如果数据的源拥有最高的源优先级，系统会将操作系统或应用身份视作当前身份。可能的源的优先级顺序如下：

1. 用户

2. 扫描程序和应用（在网络发现策略中设置）

3. 托管设备

4. NetFlow 记录

如果优先级更高的新应用身份拥有的详细信息比当前身份少，则不会覆盖当前应用身份。

此外，如果出现身份冲突，冲突的解决取决于网络发现策略中的设置或者手动解决。

当前用户身份

当系统检测到不同用户多次登录同一主机时，系统将假设某一时刻只有一个用户登录到了某给定主机，并且一个主机的当前用户是最后授权的用户登录。如果只有非授权用户登录用户登录主机，则最后的非授权用户登录用户将被视为当前用户。如果有多个用户通过远程会话登录，则服务器报告的最后用户是报告给 防火墙管理中心的用户。

当系统检测到同一用户多次登录到同一主机时，系统会记录用户在特定主机的首次登录并忽略后续的登录。如果单个用户是唯一登录到特定主机的人员，则系统唯一记录的登录为原始登录。

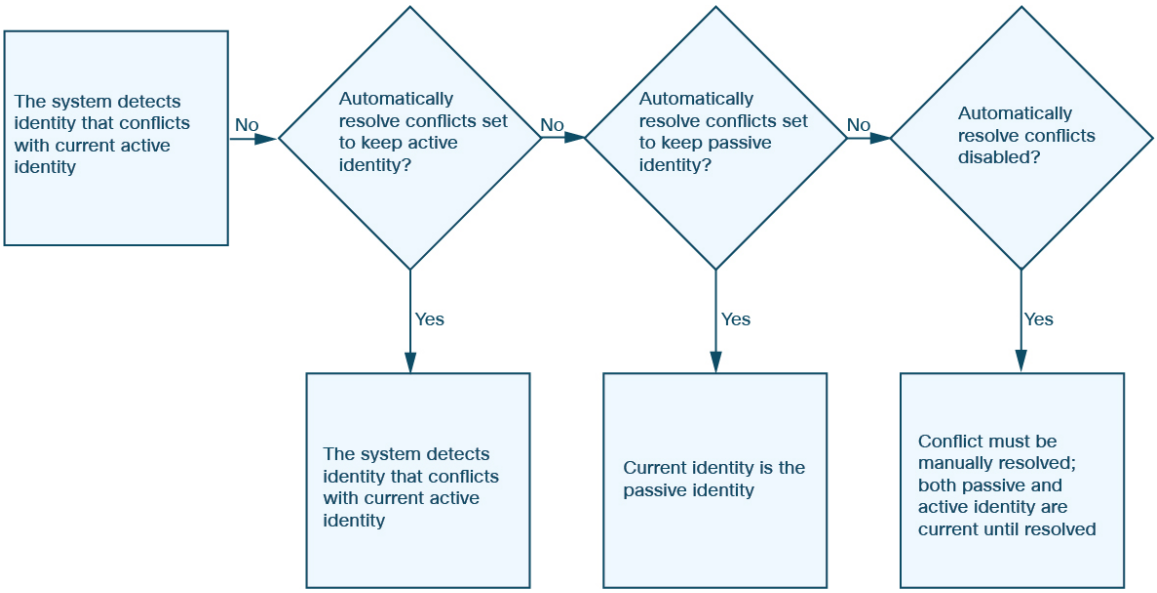
但是，如果另一用户登录到该主机，则系统会记录新的登录。如果原始用户再次登录，系统会记录其新的登录。

应用和操作系统的身份冲突

如果系统报告新的被动身份与当前主动身份和先前报告的被动身份冲突，就会发生身份冲突。例如，如将操作系统先前的被动身份报告为 Windows 2000，则主动身份 Windows XP 成为当前身份。接下来，系统检测到新的被动身份 Ubuntu Linux 8.04.1。身份 Windows XP 和 Ubuntu Linux 发生冲突。

如果主机的操作系统或主机上的某个应用存在身份冲突，系统会将两个冲突的身份均列为当前身份，并将二者用于影响评估，直到冲突解决。

有管理员权限的用户可自动解决身份冲突，只需选择始终使用被动身份或始终使用主动身份。除非禁用身份冲突的自动解决，否则身份冲突始终会自动解决。



有管理员权限的用户还可配置系统，从而在身份冲突发生时生成事件。然后，该用户可设置带有相关性规则的相关策略，规则将Nmap扫描用作相关性响应。如果事件发生，Nmap会扫描主机以获取经过更新的主机操作系统和应用数据。

NetFlow 数据

NetFlow 是一款思科 IOS 应用，可以提供有关流经路由器的数据包的统计信息。它在思科网络设备上可用，还可以嵌入到 Juniper、FreeBSD 和 OpenBSD 设备中。

在网络设备上启用 NetFlow 时，设备（NetFlow 缓存）上的数据库会存储通过路由器的数据流的记录。数据流（在系统中称为连接）是数据包序列，代表使用特定端口、协议和应用协议的源主机和目标主机之间的会话。可以将网络设备配置为导出此 NetFlow 数据。在本文档中，通过此方式配置的网络设备称为 *NetFlow* 导出器。

托管设备可以配置为从 NetFlow 导出器收集记录，根据这些记录中的数据生成单向连接结束事件，最后将这些事件发送到 防火墙管理中心以记录在连接事件数据库中。您还可以配置网络发现策略，以根据 NetFlow 连接中的信息将主机和应用协议信息添加到数据库。

可以使用这些发现和连接数据补充托管设备直接收集到的数据。这在让 NetFlow 导出器监控托管设备无法监控的网络时尤为有用。

使用 NetFlow 数据的要求

在配置 Firepower 系统以分析 NetFlow 数据之前，必须在计划使用的路由器或其他支持 NetFlow 的设备上启用 NetFlow 功能，并且配置设备以将 NetFlow 数据广播到连接了托管设备传感接口的目标网络。

Firepower 系统可以分析 NetFlow 版本 5 和 NetFlow 版本 9 记录。如果要将数据导出到 Firepower 系统，则 NetFlow 导出器**必须**使用这些版本之一。此外，系统还要求在已导出的 NetFlow 模板和记录

中存在特定字段。如果 NetFlow 导出器使用的是可以自定义的版本 9，则**必须**确保已导出的模板和记录按任意顺序包含以下字段：

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

由于 Firepower 系统使用托管设备分析 NetFlow 数据，因此，部署必须至少包括一个可监控 NetFlow 导出器的托管设备。该托管设备上的至少一个传感接口必须连接到可以收集已导出的 NetFlow 数据的网络。由于托管设备上的感应接口通常不具有 IP 地址，因此系统不支持直接收集 NetFlow 记录。

请注意，在某些网络设备上可用的采样 NetFlow 功能只会收集有关经过设备的数据包子集的 NetFlow 统计信息。尽管启用此功能可以提高网络设备上的 CPU 利用率，但可能会影响收集以供 Firepower 系统分析的 NetFlow 数据。

NetFlow 和托管设备数据之间的差异

NetFlow 数据代表的流量不会被直接分析 。相反，系统会将导出的 NetFlow 记录转换为连接日志以及主机和应用协议数据。

因此，转换后的 NetFlow 数据与托管设备直接收集到的发现数据和连接数据之间存在一些差异。在执行需要以下信息的分析时，应记住这些差异：

- 已检测的连接数量的统计信息
- 操作系统信息以及其他主机相关信息（包括漏洞）
- 应用数据，包括客户端信息、Web 应用信息，以及供应商和版本服务器信息
- 知道连接中哪个主机是发起方，哪个主机是响应方

网络发现策略与访问控制策略

可以使用网络发现策略中的规则来配置 NetFlow 数据收集（包括连接日志记录）。可以将这种数据收集与托管设备（根据访问控制规则进行配置）检测到的连接的连接日志记录进行比较。

连接事件的类型

由于 NetFlow 数据收集与网络而不是访问控制规则相关联，因此您不能非常精细地控制系统记录的 NetFlow 连接。

NetFlow 数据无法生成安全智能事件。

基于 NetFlow 的连接事件只能存储在连接事件数据库中；无法将这些事件发送到系统日志或 SNMP 陷阱服务器。

每个受监控会话生成的连接事件的数量

对于托管设备直接检测到的连接，可将访问控制规则配置为在连接开始和/或结束时记录双向连接事件。

相反，由于导出的 NetFlow 记录包含单向连接数据，因此系统会为其处理的每个 NetFlow 记录生成至少两个连接事件。这也意味着，对于基于 NetFlow 数据的每次连接，摘要的连接数会每次递增 2，从而提供网络上实际发生的快速增长的连接数量。

由于 NetFlow 导出器会以固定间隔输出记录（即使连接仍在继续），因此长期运行的会话可能会导致多个导出的记录，每个记录生成一个连接事件。例如，如果 NetFlow 导出器每 5 分钟导出一次，且特定连接持续 12 分钟，那么系统将会为该会话生成 6 个连接事件：

- 前 5 分钟生成一对事件
- 第二个 5 分钟生成一对事件
- 连接终止时生成最后一对事件

主机和操作系统数据

从 NetFlow 数据添加到网络映射的主机不具有操作系统、NetBIOS 或主机类型（主机与网络设备）信息。但是，可以使用主机输入功能手动设置主机的操作系统身份。

应用数据

对于托管设备直接检测到的连接，系统可以通过检查连接中的数据包来识别应用协议、客户端和 Web 应用。

系统处理 NetFlow 记录时，会使用 `/etc/sf/services` 中的端口关联来推断应用协议身份。不过，这些应用协议不包含供应商或供应商信息，而且连接日志不包含关于会话中使用的客户端或 Web 应用的信息。但是，可以使用主机输入功能手动提供这些信息。

请注意，简单端口关联意味着在非标准端口上运行的应用协议可能不会被识别或被错误识别。此外，如果不存在关联，系统会在连接日志中将应用协议标记为 `unknown`。

漏洞映射

系统无法将漏洞映射到 NetFlow 导出器监控的主机，除非使用主机输入功能手动设置主机操作系统的身份或应用协议身份。请注意，由于 NetFlow 连接中没有客户端信息，因此您无法将客户端漏洞与根据 NetFlow 数据创建的主机相关联。

连接中发起方和响应方信息

对于托管设备直接检测到的连接，系统可确定哪个主机是发起方（即“源”），哪个主机是响应方（即“目标”）。但是，NetFlow 数据不包含发起方或响应方信息。

当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。

- 如果使用的两个端口都是或都不是公认端口，系统会将端口号较小的那个主机视为响应方。
- 如果只有一个主机在使用公认端口，系统会将该主机视为响应方。

为此，公认端口是编号为 1 到 1023 的任意端口，或包含托管设备上 `/etc/sf/services` 中应用协议信息的任意端口。

此外，对于由托管设备直接检测到的连接，系统会在对应的连接事件中记录两个字节计数：

- **发起方字节数**字段记录发送的字节数。
- **响应方字节数**字段记录接收的字节数。

基于单向 NetFlow 记录的连接事件只包含一个字节计数（系统分配到**发起方字节数 [Initiator Bytes]** 或**响应方字节数 [Responder Bytes]**），具体取决于基于端口的算法。系统将另一个字段设置为 0。请注意，如果查看 NetFlow 记录的连接摘要（汇聚的连接数据），则这两个字段都可能会填充。

纯 NetFlow 连接事件字段

从 NetFlow 记录生成的连接事件中只存在少量字段；请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的连接时间字段中可用信息。

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。