网络发现概述

以下主题讨论网络发现：

主机、应用和用户数据的检测

主机、应用和用户数据的检测是一种网络监控功能

- 根据网络发现策略设置，使用主机身份源和应用检测器收集主机和应用数据；
- 根据网络发现和身份策略配置，通过用户身份源收集用户数据，以及
- 支持全面的网络资产映射、调查分析、行为分析、访问控制和漏洞缓解。

主机、应用和用户数据收集

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。系统分析发现和身份数据，以创建详细的网络资产映射、执行调查分析、行为剖析和访问控制，并对组织的潜在漏洞和危险做出响应。

系统会收集各种类型的数据，以增强网络安全和性能分析：

- 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。

  有关主机和应用数据的基础知识的详细信息，请参阅主机和应用检测基础知识，第 2 页

- 用户数据：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。使用这些数据获取用户感知和用户控制。

  有关用户身份的更多信息，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。

- 使用访问控制规则，结合应用条件、领域条件、用户条件、用户组条件和 ISE 属性条件，执行应用和用户控制。
- 查看受检测主机的完整配置文件。
- 通过控制面板监控网络资产和用户活动。
- 查看关于发现事件和用户活动的详细信息。

  记录和使用 NetFlow 连接（如果适用）。
- 将主机、服务器和客户端与易受漏洞攻击的主机、服务器和客户端关联，以识别和减少漏洞。

  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 陷阱或系统日志接收警报。
- 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。

主机和应用检测基础知识

网络发现策略是一项实现多种功能的功能。您可以执行以下操作：

- 启用设备标识，
- 监控网络设备和服务，以及
- 配置检测设置，以跟踪性能。

有关主机和应用检测的详细信息，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

被动检测是一种网络映射方法，

- 分析网络流量和任何导出的 NetFlow 数据以填充网络映射
- 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，以及
- 作为系统的默认检测方法。

操作系统确定过程

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

主动检测是一种网络发现功能，

- 将主动源收集的主机信息添加到网络映射，
- 使用 Nmap Scanner 等工具发现主机上的操作系统和应用，以及
- 允许将主机输入数据主动添加到网络映射中。

主机输入数据分类为：

- 用户输入数据 — 通过系统用户界面添加的数据，允许修改主机的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。

身份保留和优先级行为

系统将为每个主动源保留一个身份。例如，当您运行 Nmap 扫描实例时，先前的结果会用新的扫描数据进行更新。但是，如果用通过命令行导入的客户端数据替换扫描结果，系统将保留两者的身份信息。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。

用户输入无论来源如何，都会取代其他身份。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，则保留用户 B 设置的定义。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

当前身份是应用或操作系统的身份确定，

- 表示系统认为最有可能正确的身份，
- 用于漏洞分配和影响评估，以及
- 当同一主机存在多个身份时，由源优先级确定。

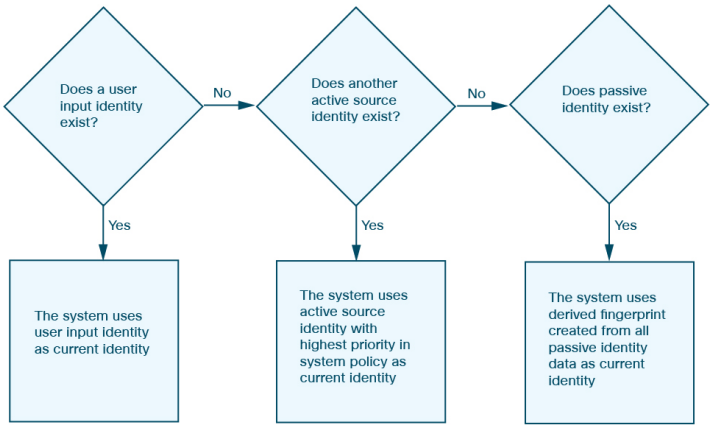
当前身份用户

系统会将操作系统或应用的当前身份用于这些用途：

- 分配漏洞至主机
- 评估影响
- 评估与操作系统标识、主机配置文件资格和合规性 allow 列表相关的关联规则
- 在工作流程的“主机”和“服务器”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”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。

图 *1:* 当前身份确定过程



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. 受管设备
4. NetFlow 记录

如果新的、优先级更高的应用标识比当前标识的细节更少，则不会覆盖当前应用标识。

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。

分配操作系统作为当前身份

例如，如果用户在一台主机上将操作系统设置为 Windows 2003 Server，则 Windows 2003 Server 成为当前身份，并且该主机上针对 Windows 2003 Server 漏洞的攻击将具有更高的影响。主机配置文件中针对该主机列出的漏洞包括 Windows 2003 Server 漏洞。

当前用户身份

当前用户身份由系统确定：

- 当多个用户登录到同一主机时，将最后的授权用户登录识别为当前用户
- 假定一次只能有一个用户登录到任何给定主机
- 记录用户在特定主机上的首次登录，但忽略同一用户的后续登录，并且
- 当多个用户通过远程会话登录时，向 防火墙管理中心 报告服务器检测到的最后一个用户。

用户登录跟踪行为

系统使用特定规则确定当前用户身份：

- 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

身份冲突是一种系统条件

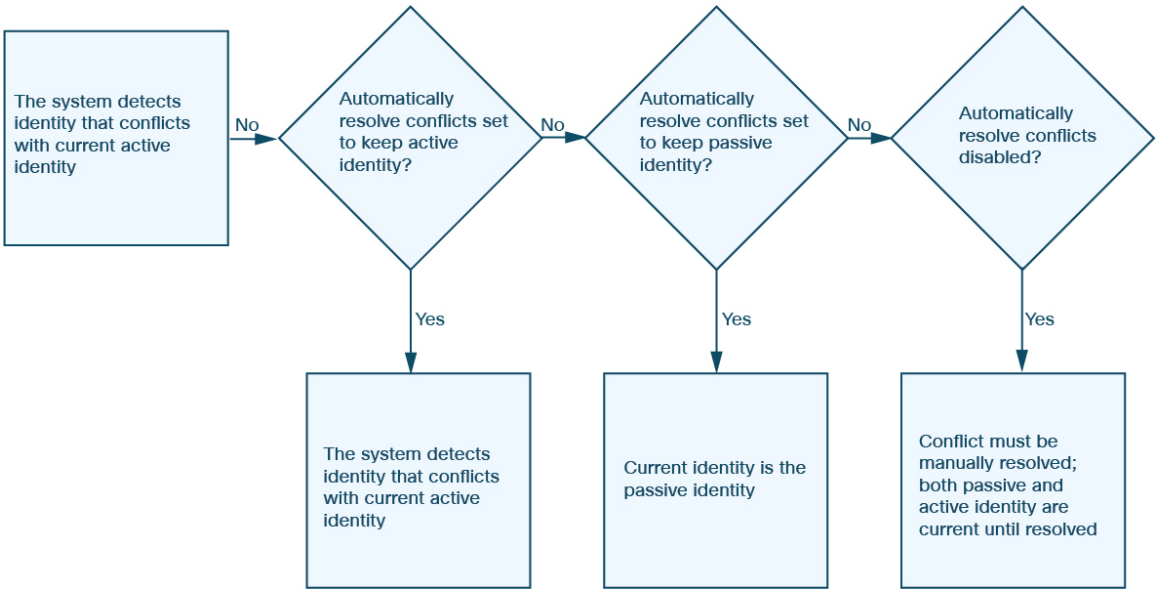
- 当系统报告新的被动身份与当前主动身份和先前报告的被动身份冲突时发生。
- 导致两个冲突的身份都被列为当前身份并用于影响评估，直到冲突得以解决，以及
- 通过选择始终使用被动身份或始终使用主动身份即可自动解决。

身份冲突行为和解决方法

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。



操作系统身份冲突场景

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。

NetFlow 数据

NetFlow 数据是网络流统计信息的集合，可以

- 通过 Cisco IOS 应用提供流经路由器的数据包统计信息
- 在思科网络设备可用，也可嵌入 Juniper、FreeBSD 和 OpenBSD 设备中，并且
- 在网络设备上启用 NetFlow 时，将流记录存储在设备上称为 NetFlow 缓存的数据库中。

NetFlow 数据处理与使用

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（原则）

要求：NetFlow 设备配置

在配置系统分析 NetFlow 数据前，**必须**在计划使用的路由器或其他支持 NetFlow 的网络设备上启用 NetFlow 功能。将设备配置为向托管设备传感接口所连接的网络广播 NetFlow 数据。

要求：NetFlow 版本与字段规范

系统可解析 NetFlow 版本 5 和版本 9 记录。若需导出数据，NetFlow 导出器**必须**使用上述版本之一。确保导出的 NetFlow 模板和记录包含特定字段，例如 IN_BYTES、IN_PKTS、PROTOCOL 等。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)

要求：托管设备部署

您的部署必须包含至少一台可监控 NetFlow 导出器的托管设备。将托管设备上的至少一个传感接口连接到网络，以收集导出的 NetFlow 数据。因传感接口缺乏 IP 地址，系统不支持直接收集。

注意：采样 NetFlow 注意事项

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。启用此功能虽可提升 CPU 利用率，但可能影响系统分析所用的 NetFlow 数据准确性。

NetFlow 与受管设备数据之间的差异

NetFlow 与受管设备数据的差异属于分析性差异，

- 源于将导出的 NetFlow 记录转换为连接日志以及主机和应用协议数据，而不是直接分析流量，

- 影响检测到的连接、操作系统信息和应用数据的统计信息，以及
- 影响连接发起方和响应方的识别。

数据收集和分析方面的主要差异

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 导出器会定期输出记录（即使连接仍在进行中），长时间运行的会话可能导致多个导出记录，每个记录都会生成一个连接事件。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，您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。

连接中的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，知名端口是指编号从 1 到 1023 的任何端口，或系统视为服务器端口的任何端口（无论其编号如何）。

NetFlow 字节计数

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。

仅 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。

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。

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。