网络发现策略

以下主题介绍如何创建、配置和管理网络发现策略：

概述：网络发现策略

防火墙管理中心上的网络发现策略控制系统如何收集有关组织网络资产以及哪些网段和端口受监控的数据。

策略中的发现规则指定系统监控哪些网络和端口来根据流量中的网络数据生成发现数据，以及指定策略部署到的区域。在规则中，您可以配置是否发现主机、应用和非管理用户。可以创建规则来将网络和区域排除在发现范围外。您可以从 NetFlow 导出器配置数据发现，并且限制在网络上发现了用户数据的流量的协议。

网络发现策略包含一个配置为从观察到的所有流量发现应用的默认规则。该规则不排除任何网络、区域或端口，未配置主机和用户发现，并且规则未配置为监控 NetFlow 导出器。当托管设备注册到防火墙管理中心时，此策略默认部署到任何托管设备。要开始收集主机或用户数据，必须添加或修改发现规则并将策略重新部署到设备。

如果要调整网络发现范围，可以创建其他发现规则，并修改或移除默认规则。

请记住，每个托管设备的访问控制策略都定义面向该设备允许的流量，以及因此可使用网络发现监控的流量。如果使用访问控制阻止某些流量，则系统无法检查主机、用户和应用活动的该流量。例如，如果访问控制策略阻止对社交网络应用的访问，则系统无法在这些应用上提供任何发现数据。

如果在发现规则中启用基于流量的用户检测，则可以通过使用一组应用协议的流量中的用户登录活动来检测非管理用户。如有需要，可以禁用用于所有规则的特定协议中的发现。禁用某些协议有助于避免达到与 防火墙管理中心型号关联的用户限制，从而为来自其他协议的用户保留可用用户计数。

借助高级网络发现设置，可以管理记录哪些数据、如何存储发现数据、哪些危害表现 (IOC) 规则处于活动状态、哪些漏洞映射用于影响评估，以及如果源提供冲突发现数据将会发生什么情况。您还可以添加要监控的主机输入和 NetFlow 导出器的源。

网络发现策略的要求和前提条件

型号支持

任意。

支持的域

枝叶

用户角色

- 管理员
- 发现管理员

网络发现自定义

Firepower 系统收集的有关网络流量的信息对您最有价值，因为系统可以参考该信息来识别网络上最易受攻击和最重要的主机。

例如，如果网络上有多个运行自定义版本的 SuSE Linux 的设备，则系统无法识别操作系统，因此无法将漏洞映射至主机。不过，如果知道系统拥有 SuSE Linux 的漏洞列表，您可能想要为某个主机创建自定义的指纹，以便随后可使用该指纹来识别运行相同操作系统的其他主机。可将 SuSE Linux 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

系统还允许使用主机输入功能，将来自第三方系统的主机数据直接输入至网络映射。不过，第三方操作系统或应用数据不会自动映射至漏洞信息。如果想要为使用第三方操作系统、服务器和应用协议数据的主机查看漏洞并执行影响关联，必须将来自第三方系统的供应商和版本信息映射至漏洞数据库 (VDB) 中列出的供应商和版本。您也可能想要持续维护主机输入数据。请注意，即使将应用数据映射到 Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

如果系统无法识别网络主机上运行的应用协议，则可创建用户定义的应用协议检测器以便系统根据端口或模式识别应用。您还可以导入、激活和停用某些应用检测器，以便进一步自定义 Firepower 系统的应用检测功能。

还可使用 Nmap 主动扫描器的扫描结果替换操作系统和应用数据的检测结果，或者使用第三方漏洞来扩充漏洞列表。系统可以协调来自多个源的数据，从而确定应用的身份。

配置网络发现策略

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 配置策略的以下组件：

- 发现规则 - 请参阅配置网络发现规则，第 3 页。
- 基于流量的用户检测 - 请参阅配置基于流量的用户检测，第 11 页。
- 高级网络发现选项 - 请参阅配置高级网络发现选项，第 12 页。
- 自定义操作系统定义（指纹） - 请参阅为客户端创建自定义指纹和为服务器创建自定义指纹。

网络发现规则

通过网络发现规则，您可以将为网络映射发现的信息定制为仅包含所需的特定数据。网络发现策略中的规则按顺序接受评估。您可以使用重叠的监控条件创建规则，但这样做可能会影响系统性能。

将主机或网络排除在监控范围外之后，被排除的主机或网络将不会显示在网络映射中，系统也不会为其报告事件。但是，在禁用本地 IP 的主机发现规则时，检测引擎实例会受到更高处理负载的影响，因为它会从每个流重新构建数据，而不是使用现有主机数据。

我们建议将负载均衡器（或负载均衡器上的特定端口）和NAT设备排除在监控范围外。这些设备可能会创建过量并有误导性的事件，从而填充数据库并使防火墙管理中心过载。例如，受监控的NAT设备可能会在短时间内显示其操作系统的多个更新。如果知道负载均衡器和 NAT 设备的 IP 地址，可以将它们排除在监控范围外。

提示 系统可通过检查网络流量识别许多负载均衡器和 NAT 设备。

此外，如果需要创建自定义服务器指纹，应暂时禁止监控用于与正在创建指纹的主机通信的 IP 地址。否则，网络映射和发现事件视图中将会出现大量关于该IP地址代表的主机的不准确信息。创建指纹后，可以配置策略，以便再次监控该 IP 地址。

思科还建议 **不** 监控 NetFlow 导出器和托管设备的相同网段。尽管在理想情况下应使用不重叠的规则来配置网络发现政策，但系统不会丢弃托管设备生成的重复连接日志。但是，**不能**丢弃托管设备和 NetFlow 导出器均检测到的连接的重复连接日志。

配置网络发现规则

可以配置发现规则，以根据自身需求定制主机和应用数据的发现。

提示 在大多数情况下，我们建议将发现限制在 RFC 1918 中的地址。

开始之前

- 确保正在为要在其中发现网络数据的流量记录连接；请参阅《Cisco Secure Firewall Management Center 管理指南》中的连接日志记录最佳实践。
- 如果要收集导出的 NetFlow 记录，请按照将 NetFlow 导出器添加到网络发现策略，第 17 页中所述添加 NetFlow Exporter。
- 如果要查看发现性能图，必须在发现规则中启用主机，用户和应用。请注意，这可能会影响性能。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**添加规则**。

步骤 3 如操作和发现的资产，第 4 页中所述，为规则设置**操作 (Action)**。

步骤 4 设置可选的发现参数：

- 将规则操作限定于特定网络；请参阅限制受监控网络，第 5 页。
- 将规则操作限定于特定区域中的流量；请参阅配置网络发现规则中的区域，第 9 页。
- 将端口排除在监控范围外；请参阅排除网络发现规则中的端口，第 8 页。
- 为 NetFlow 数据发现配置规则；请参阅配置用于 NetFlow 数据发现的规则，第 6 页。

步骤 5 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

操作和发现的资产

配置发现规则时，必须为规则选择操作。规则操作的影响取决于规则是用于从托管设备还是NetFlow导出器发现数据。

下表说明了规则使用这两种方案中指定的操作设置发现的资产。

表 *1:* 发现规则操作

操作	选项	托管设备	NetFlow 导出器
排除	--	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。
发现	主机数	根据发现事件将主机添加到网络映射。（可选操作；如果启用了用户发现，则为必要操作。）	根据 NetFlow 记录将主机添加到网络映射并记录连接。（必需）
发现	应用	根据应用检测程序将应用添加到网络映射。请注意，在没有发现应用的情况下，无法发现规则中的主机或用户。（必需）	根据 NetFlow 记录和 `/etc/sf/services` 中的端口应用协议关联将应用协议添加到网络映射。（可选）
发现	用户	将用户添加到用户表，并根据对网络发现策略中配置的用户协议进行的基于流量的检测记录用户活动。（可选）	n/a
记录 NetFlow 连接	--	n/a	仅记录 NetFlow 连接。不发现主机或应用。

如果要让规则监控托管设备流量，则应用日志记录为必要操作。如果要让规则监控用户，则主机日志记录为必要操作。如果要让规则监控导出的 NetFlow 记录，则您无法将其配置为记录用户，并且记录应用为可选操作。

注释 系统根据网络发现策略中的**操作 (Action)** 设置检测 NetFlow 记录中的连接。系统根据访问控制策略设置检测托管设备中的连接。

受监控网络

发现规则仅可发现流量中发向和来自指定网络中主机的受监控资产。发现规则执行发现的对象是至少有一个 IP 地址在指定网络范围内的连接，并仅对位于受监控网络范围内的 IP 地址生成事件。默认发现规则从所有观察到的流量中发现应用（`0.0.0.0/0` 表示所有 IPv4 流量，`::/0` 表示所有 IPv6 流量）。

如果将规则配置为处理 NetFlow 发现并仅记录连接数据，则系统还会记录发向和来自指定网络中 IP 地址的连接。请注意，网络发现规则是记录 NetFlow 网络连接的唯一方式。

另外，您也可以使用网络对象或对象组指定要监控的网络。

限制受监控网络

每个发现规则必须至少包含一个网络。

过程

步骤 1 选择策略 > 网络发现。

步骤 2 点击添加规则。

步骤 3 如果还未打开，请点击 网络。

步骤 4 （可选）将网络对象添加到“可用网络”(Available Networks) 列表，如在配置发现规则期间创建网络对象，第 7 页中所述。

如果修改网络发现策略中使用的网络对象，则更改对于发现不会生效，直至部署配置更改为止。

步骤 5 指定网络：

- 从可用网络 **(Available Networks)** 列表中选择网络。如果网络没有立即显示在列表中，请点击重新加载 ()。
- 将 IP 地址输入到“可用网络”(Available Networks) 标签下方的文本框中。

步骤 6 点击添加 **(Add)**。

步骤 7 点击保存。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

配置用于 NetFlow 数据发现的规则

系统可以使用来自 NetFlow 导出器的数据生成连接和发现事件，并将主机和应用数据添加到网络映射。

如果选择某个发现规则中的 NetFlow 导出器，该规则将被限制为为指定网络发现 NetFlow 数据。应先选择要监控的 NetFlow 设备，然后再配置规则行为的其他方面，因为在选择 NetFlow 设备时可用规则操作会变化。不能为监控 NetFlow 导出器配置端口排除。

开始之前

- 将支持 NetFlow 的设备添加到网络发现策略；请参阅将 NetFlow 导出器添加到网络发现策略，第 17 页。

过程

步骤 1 选择策略 > 网络发现。

步骤 2 点击添加规则。

步骤 3 选择 **NetFlow 设备**。

步骤 4 从 **NetFlow 设备 (NetFlow Device)** 下拉列表中，选择要监控的 NetFlow 导出器的 IP 地址。

步骤 5 指定要让系统托管设备收集的 NetFlow 数据类型：

- 仅连接 - 从操作 (Action) 下拉列表中选择 **Log NetFlow Connections**。
- 主机、应用和连接 - 从操作 (Action) 下拉列表中选择 **Discover**。系统会自动选中**主机 (Hosts)** 复选框并启用连接数据的收集。或者，可以选中**应用 (Application)** 复选框以收集应用数据。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

在配置发现规则期间创建网络对象

将新的网络对象添加到可重用网络对象和组列表中，即可将其添加到发现规则中显示的可用网络列表中。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 在**网络**中，点击**添加规则**。

步骤 3 点击**可用网络 (Available Networks)** 旁边的 **添加** (+)。

步骤 4 按照创建网络对象中所述创建网络对象。

步骤 5 按照配置网络发现规则，第 3 页中所述完成添加网络发现规则。

端口排除

可以将特定端口排除在监控范围外，就像将主机排除在监控范围外一样。例如：

- 负载均衡器可在短时间内报告同一端口上的多个应用。可以配置网络发现规则，以便将该端口排除在监控范围外，例如排除处理 Web 场的负载均衡器上的端口 80。
- 组织可以使用采用特定端口范围的自定义客户端。如果来自该客户端的流量生成过多有误导性的事件，可以排除对这些端口的监控。同样，可以决定是否要监控DNS流量。在这种情况下，可以配置规则，使发现策略不监控端口 53。

添加要排除的端口时，可以决定是使用 Available Ports 列表中的可重用端口对象，将端口直接添加到源或目标排除列表，还是创建新的可重用端口然后将其移至排除列表。

注释 不能排除处理 NetFlow 数据发现的规则中的端口。

排除网络发现规则中的端口

不能排除处理 NetFlow 数据发现的规则中的端口。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**添加规则**。

步骤 3 点击 **Port Exclusions**。

步骤 4 或者，将端口对象添加到“可用端口”(Available Ports) 列表，如在配置发现规则期间创建端口对象，第 8 页中所述。

步骤 5 使用以下任一方法将特定源端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到源 (Add to Source)**。
- 要排除来自特定源端口的流量而不添加端口对象，请在**所选源端口 (Selected Source Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号（从 1 到 65535 的值），然后点击**添加 (Add)**。

步骤 6 使用以下任一方法将特定目标端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到目标 (Add to Destination)**。
- 要排除来自特定目标端口的流量而不添加端口对象，请在**所选目标端口 (Selected Destination Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号，然后点击**添加 (Add)**。

步骤 7 点击**保存**以保存所做的更改。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

在配置发现规则期间创建端口对象

将新的端口对象添加到可在系统中任意位置使用的可重用端口对象和对象组列表，即可将其添加到发现规则中显示的可用端口列表中。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 在“网络”中，点击**添加规则**。

步骤 3 点击 **Port Exclusions**。

步骤 4 要将端口添加到可用端口列表，请点击 **添加** (+)。

步骤 5 输入**名称**。

步骤 6 在 **Protocol** 字段中，指定要排除的流量协议。

步骤 7 在**端口 (Port)** 字段中，输入要排除在监控范围外的端口。

可以指定单个端口、用破折线(-)分隔的一系列端口或者用逗号分隔的端口和端口范围列表。允许的端口值介于 1 到 65535 之间。

步骤 8 点击**保存**。

步骤 9 如果添加的端口没有立即显示在列表中，请点击 **刷新**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

网络发现规则中的区域

要提高性能，可以配置发现规则，以便规则中的区域包含物理连接到规则中的待监控网络的托管设备上的传感接口。

但是，系统可能并不总是告知您网络配置的更改情况。网络管理员可以通过路由或主机更改修改网络配置而无需告知您，这可能会导致您难以随时了解正确的网络发现策略配置。如果您不知道托管设备上的传感接口如何物理连接到您的网络，请将区域配置保留为默认设置。此默认设置会导致系统将发现规则部署到您的部署中的所有区域。（如果未排除任何区域，则系统会将发现策略部署到所有区域。）

配置网络发现规则中的区域

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**添加规则**。

步骤 3 点击 **区域**。

步骤 4 从**可用区域 (Available Zones)** 列表中选择一个或多个区域。

步骤 5 点击**保存**以保存所做的更改。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

基于流量的检测身份源

基于流量的检测是系统唯一支持的未授权身份源。进行配置后，托管设备会检测您指定的网络上的 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录。从基于流量的检测获取的数据仅可用于用户感知。与授权身份源不同，您可在网络发现策略中配置基于流量的检测，如配置基于流量的用户检测，第 11 页中所述。

请注意以下限制：

- 基于流量的检测仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。托管设备无法检测使用协议（例如 SSL 或 TLS）的加密 LDAP 身份验证。
- 基于流量的检测只能检测使用 OSCAR 协议的 AIM 登录。无法检测使用 TOC2 的 AIM 登录。
- 基于流量的检测无法限制 SMTP 日志记录。这是因为未根据 SMTP 登录将用户添加到数据库；虽然系统会检测 SMTP 登录，这些登录不会被记录下来，除非数据库中包含已具有匹配邮件地址的用户。

基于流量的检测还会记录失败的登录尝试。如果登录尝试失败，不会将新用户添加到数据库的用户列表中。基于流量的检测功能检测到的登录失败活动的用户活动类型是**登录失败的用户 (Failed User Login)**。

注释 系统无法区分失败和成功的 HTTP 登录。要查看 HTTP 用户信息，您必须在基于流量的检测配置中启用**捕获登录失败尝试 (Capture Failed Login Attempts)**。

注意 使用网络发现策略 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。 在 HTTP、FTP 或 MDNS 协议上启用或禁用基于流量的非授权用户检测

基于流量的检测数据

设备使用基于流量的检测功能检测到登录时，它会将以下信息发送到 防火墙管理中心（这些信息将被记录为用户活动）：

- 识别出的登录用户名。
- 登录时间。
- 登录使用的 IP 地址，可能是用户的主机（用于 LDAP、POP3、IMAP 和 AIM 登录）、服务器（用于 HTTP、MDNS、FTP、SMTP 和 Oracle 登录）或会话发起方（用于 SIP 登录）的 IP 地址。
- 用户的邮件地址（用于 POP3、IMAP 和 SMTP 登录）。
- 检测到登录的设备名称。

如果之前已检测到该用户，防火墙管理中心会更新该用户的登录历史记录。请注意，防火墙管理中心可以使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 用户 关联。举例来说，这意味着如果 防火墙管理中心检测到新的 IMAP 登录，且 IMAP 登录中的邮件地址与某个现有 LDAP 用户的邮件地址匹配，则 IMAP 登录不会创建新用户，而是会更新该 LDAP 用户的历史记录。

如果之前从未检测到该用户，防火墙管理中心会将该用户添加到用户数据库。唯一的 AIM、SIP 和 Oracle 登录始终会创建新用户记录，因为这些登录事件中没有 防火墙管理中心可与其他登录类型关联的数据。

在以下情况下，防火墙管理中心**不**会记录用户活动或用户身份：

- 网络发现策略被配置为忽略该登录类型
- 托管设备检测到 SMTP 登录，但用户数据库不包含之前使用匹配的邮件地址检测到的 LDAP、POP3 或 IMAP 用户

用户数据将被添加到用户表中。

基于流量的检测策略

可以限制在其中发现用户活动的协议，以减少检测到的用户的总数，以便将重点放在可能提供最完整用户信息的用户。限制协议检测有助于最大程度地减少用户名混乱以及预留 防火墙管理中心上的存储空间。

当选择基于流量的检测协议时，请注意以下事项：

- 如果通过协议（例如 AIM、POP3 和 IMAP）获取用户名，可能会由于承包商、访客及其他访客的网络访问而引入与组织无关的用户名。
- AIM、Oracle 和 SIP 登录可能会创建外来用户记录。之所以会发生这种情况，是因为这些登录类型没有与系统从 LDAP 服务器获取的任何用户元数据关联，也没有与托管设备会检测的其他类型登录中包含的任何信息关联。因此，防火墙管理中心无法将这些用户与其他类型的用户关联。

配置基于流量的用户检测

在网络发现规则中启用基于流量的用户检测时，将会自动启用主机发现。有关基于流量的检测的详细信息，请参阅基于流量的检测身份源，第 10 页。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**用户**。

步骤 3 请点击 **编辑** ()。

步骤 4 选中要检测登录的协议的复选框，或取消选中不希望检测登录的协议的复选框，然后选择是否**捕获失败的登录尝试**。

步骤 5 点击**保存**。

下一步做什么

注意 使用网络发现策略 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。 在 HTTP、FTP 或 MDNS 协议上启用或禁用基于流量的非授权用户检测

- 配置网络发现规则以发现用户，如配置网络发现规则，第 3 页中所述。
- 部署配置更改；请参阅 部署配置更改。

配置高级网络发现选项

可以使用网络发现策略的”高级“(Advanced) 来配置策略范围的设置，以指定要检测的事件、发现数据的保留时间长度和更新频率、用于影响关联的漏洞映射，以及如何解决操作系统和服务器身份冲突。此外，还可以添加主机输入源和 NetFlow 导出器，以允许从其他源导入数据。

注释 发现和用户活动事件的数据库事件限制是在系统配置中设置。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击要修改的设置旁边的 **编辑** (✎) 或 **添加** (+)：

- “数据存储设置”(Data Storage Settings) - 更新设置，如配置网络发现数据存储，第 19 页中所述。
- “事件日志记录设置”(Event Logging Settings) - 更新设置，如配置网络发现事件日志记录，第 19 页中所述。
- “常规设置”(General Settings) - 更新设置，如配置网络发现常规设置，第 13 页中所述。
- “身份冲突设置”(Identity Conflict Settings) - 更新设置，如配置网络发现身份冲突解决方法，第 14 页中所述。
- “危害表现设置”(Indications of Compromise Settings) - 更新设置，如启用危害表现规则，第 16 页中所述。
- “NetFlow 导出器”(NetFlow Exporters) - 更新设置，如将 NetFlow 导出器添加到网络发现策略，第 17 页中所述。

- “操作系统和服务器身份源”(OS and Server Identity Sources) - 更新设置，如添加网络发现操作系统和服务器身份源，第 19 页中所述。
- “用于影响评估的漏洞”(Vulnerabilities to use for Impact Assessment) - 更新设置，如启用网络发现漏洞影响评估，第 15 页中所述。

步骤 4 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

网络发现常规设置

常规设置控制系统更新网络映射的频率以及是否在发现过程中捕获服务器横幅。

捕获横幅

如果希望系统存储来自通告服务器供应商和版本的网络流量的报头信息（“横幅”），请选中此复选框。这些信息可提供有关收集的信息的其他上下文。可以通过访问服务器详细信息来访问为主机收集的服务器横幅。

更新间隔

系统更新信息（例如，上一次显示任何主机的 IP 地址的时间、使用应用的时间或应用的点击次数）的时间间隔。默认设置为 3600 秒（1 小时）。

请注意，为更新超时设置较小的时间间隔可在主机显示中提供更准确的信息，但会增加生成的网络事件数量。

配置网络发现常规设置

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**常规设置 (General Settings)** 旁边的 **编辑** (✎)。

步骤 4 更新设置，如网络发现常规设置，第 13 页中所述。

步骤 5 点击**保存**以保存常规设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

网络发现身份冲突设置

系统通过将操作系统和服务器的指纹与流量模式进行匹配，从而确定在主机上运行的操作系统和应用。为了提供最可靠的操作系统和服务器身份信息，系统会核对来自多个源的指纹信息。

系统使用所有被动数据来推导操作系统身份并分配置信度值。

默认情况下，除非存在身份冲突，否则由扫描工具或第三方应用添加的身份数据会覆盖 Firepower 系统检测到的身份数据。可以使用 Identity Sources 设置按优先级对扫描程序和第三方应用指纹源进行评级。系统为每个源保留一个身份，但只有优先级最高的第三方应用或扫描程序源中的数据可用作当前身份。但请注意，用户输入数据会覆盖扫描程序和第三方应用数据，无论后者的优先级如何。

身份冲突是指系统检测到某个身份与来自“身份源”(Identity Sources) 设置中列出的活动扫描工具或第三方应用源或者来自 Firepower 系统用户的现有身份相冲突。默认情况下，身份冲突不会自动解决，必须通过主机配置文件，或者通过重新扫描主机或重新添加新的身份数据覆盖被动身份来解决冲突。但是，可以将系统设置为通过保留被动身份或主动身份来自动解决冲突。

生成身份冲突事件

指定在发生身份冲突时系统是否生成事件。

自动解决冲突

从**自动解决冲突 (Automatically Resolve Conflicts)** 下拉列表中，选择以下选项之一：

- **已禁用 (Disabled)**，如果要强制手动解决身份冲突
- **身份**，如果要在发生身份冲突时让系统使用被动指纹
- **保留主动身份 (Keep Active)**，如果要在发生身份冲突时让系统使用来自最高优先级主动源的当前身份

配置网络发现身份冲突解决方法

过程

步骤 1 选择**策略 > 网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**身份冲突设置 (Identity Conflict Settings)** 旁边的 **编辑** (✎)。

步骤 4 更新“编辑身份冲突设置”(Edit Identity Conflict Settings) 弹出窗口中的设置，如网络发现身份冲突设置，第 14 页中所述。

步骤 5 点击**保存**以保存身份冲突设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

网络发现漏洞影响评估选项

可以配置系统如何对入侵事件执行关联影响。您具有以下选择：

- 如果要使用基于系统的漏洞信息执行影响关联，请选中**使用网络发现漏洞映射 (Use Network Discovery Vulnerability Mappings)** 复选框。
- 如果要使用第三方漏洞参考执行影响关联，请选中**使用第三方漏洞映射 (Use Third-Party Vulnerability Mappings)** 复选框。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

可以同时选中这两个复选框或选中其中之一。如果系统生成入侵事件，且该事件涉及的主机所拥有的服务器或操作系统包含所选漏洞映射集中的漏洞，则该入侵事件将带有 Vulnerable（级别 1：红色）影响图标。对于没有供应商或版本信息的任何服务器，需要在 防火墙管理中心配置中启用漏洞映射。

如果取消选中这两个复选框，入侵事件将**不会**带有 Vulnerable（级别 1：红色）影响图标。

相关主题

映射第三方漏洞

启用网络发现漏洞影响评估

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**用于影响评估的漏洞 (Vulnerabilities to use for Impact Assessment)** 旁边的 **编辑** (✎)。

步骤 4 更新“编辑漏洞设置”(Edit Vulnerability Settings) 弹出窗口中的设置，如网络发现漏洞影响评估选项，第 15 页中所述。

步骤 5 点击**保存**保存漏洞设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

危害表现

系统使用网络发现策略中的 IOC 规则，以确定主机是否可能被恶意手段损害。当主机满足这些系统提供的规则中指定的条件时，系统将使用危害表现 (IOC) 进行标记。相关规则被称为 *IOC* 规则。每条 IOC 规则对应于一种类型的 IOC 标记。*IOC* 标记用于指定可能发生的危害的性质。

当发生以下情况时，防火墙管理中心可以标记涉及的主机和用户：

- 通过使用入侵、连接、安全智能和文件或恶意软件事件，系统将收集到的关于受监控网络及其流量的数据相关联，并确定潜在 IOC 已发生。
- 防火墙管理中心 可以通过 AMP 云从您的 Cisco Secure Endpoint 部署导入 IOC 数据。由于这些数据检查主机本身上的活动（例如，单个程序执行的操作），因此，通过这些数据可了解到纯网络数据无法洞察到的可能威胁。为了方便起见，防火墙管理中心会自动获取思科从 AMP 云开发的任何新 IOC 标记。

要配置此功能，请参阅启用危害表现规则，第 16 页。

您还可以针对主机 IOC 数据和合规 allow 名单（决定 IOC 标记的主机）。

要调查和使用标记的 IOC，请参阅《Cisco Secure Firewall Management Center 管理指南》。

启用危害表现规则

要使系统检测和标记危害表现 (IOC)，必须先在网络发现策略中至少激活一个 IOC 规则。每个 IOC 规则对应于一种类型的 IOC 标记，所有 IOC 规则均由思科预定义；您不能创建原始规则。可根据网络和组织需要启用任何或全部规则。例如，如果使用诸如 Microsoft Excel 等软件的主机从未出现在监控网络上，可决定不启用与基于 Excel 的威胁相关的 IOC 标记。

提示 要禁用个别主机或其关联用户的 IOC 规则，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 发现事件。

开始之前

由于 IOC 规则根据系统的其他组件以及Cisco Secure Endpoint 提供的数据触发，因此必须为要设置 IOC 标记的 IOC 规则正确许可并配置这些组件。启用与您将启用的 IOC 规则相关联的系统功能，例如入侵检测和防御 (IPS) 及高级恶意软件防护 (AMP)。如果未启用 IOC 规则的关联功能，将不会收集相关数据，规则也将无法触发。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**危害表现设置 (Indications of Compromise Settings)** 旁边的 **编辑** ()。

步骤 4 要关闭或关闭整个 IOC 功能，请点击 **Enable IOC** 旁边的滑块。

步骤 5 要全局启用或禁用个别 IOC 规则，请点击相应规则的**启用 (Enabled)** 列中的滑块。

步骤 6 点击**保存**以保存 IOC 规则设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

将 NetFlow 导出器添加到网络发现策略

使用此程序添加NetFlow导出器。请注意，如果导出器当前正在发现规则中使用，则无法将其删除。

开始之前

- 查看前提条件：使用 NetFlow 数据的要求
- 配置 NetFlow 导出器：NetFlow 数据

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **NetFlow 设备**旁边的 **添加** (+) 。

步骤 4 输入导出器的 **IP 地址**。

步骤 5 点击**保存**。

下一步做什么

- 配置网络发现规则以监控 NetFlow 流量：配置网络发现规则， 第 3 页
- 部署配置更改；请参阅 部署配置更改。

网络发现数据存储设置

发现数据存储设置包括主机限制和超时设置。

当达到主机限制时 (When Host Limit Reached)

Cisco Secure Firewall Management Center可以监控因而存储在网络映射中的主机数取决于其型号。**当达到主机限制时 (When Host Limit Reached)** 选项控制在达到主机限制后检测到新主机时发生的情况。您可以执行以下操作：

丢弃主机

系统丢弃保持非活动状态时间最长的主机，然后添加新主机。这是默认设置。

不插入新主机

系统不跟踪任何新发现的主机。系统仅在主机计数降至低于限制后跟踪新主机，例如，在管理员增大域的主机限制或从网络映射中手动删除主机后，或者，如果系统因主机不活动而将其识别为已超时。

表 *2:* 达到多租户的主机限制

设置	已设置域主机限制？	已达到域主机限制	已达到祖先域主机限制
丢弃主机	是	丢弃受限制域中的最旧主机。	丢弃配置为丢弃主机的所有后代分叶域中的最旧主机。 如果无法丢弃任何主机，则不添加主机。
	否	不适用	丢弃配置为丢弃主机以及共享常规池的所有后代分叶域中的最旧主机。
不插入新主机	是/否	不添加主机。	不添加主机。

主机超时

系统因网络映射中的某一主机不活动而丢弃该主机之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。单个主机 IP 和 MAC 地址可以单独超时，但是，除非主机的所有关联地址都超时，否则该主机不会从网络映射中消失。

要避免主机提前超时，请确保主机超时值大于网络发现策略常规设置中的更新间隔。

服务器超时

系统因网络映射中的某一服务器不活动而丢弃该服务器之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

要避免服务器提前超时，请确保服务超时值大于网络发现策略常规设置中的更新间隔。

客户端应用超时

系统因网络映射中的某一客户端不活动而丢弃该客户端之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

确保客户端超时值大于网络发现策略常规设置中的更新间隔。

相关主题

主机限制

配置网络发现数据存储

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **网络发现数据存储设置**旁的 **编辑** (✎) 。

步骤 4 更新“数据存储设置”(Data Storage Settings) 对话框中的设置，如网络发现数据存储设置 ，第 17 页中所述。

步骤 5 点击**保存**以保存数据存储设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

配置网络发现事件日志记录

事件日志记录设置控制是否记录发现和主机输入事件。如果不记录事件，则无法在事件视图中检索事件，也不能将事件用于触发关联规则。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **事件日志记录设置**旁边的 **编辑** (✎) 。

步骤 4 选中或取消选中要在数据库中记录的发现和主机输入事件类型旁边的复选框，如在发现事件类型和主机输入事件类型 《Cisco Secure Firewall Management Center 管理指南》 的发现事件一节所述。

步骤 5 点击**保存**以保存事件日志记录设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

添加网络发现操作系统和服务器身份源

在网络发现策略的“高级”中，可以添加新的主动源，或更改现有源的优先级或超时设置。

将扫描工具添加到此页面不会添加 Nmap 扫描工具已有的完整集成功能，但允许集成导入的第三方应用或扫描结果。

如果从第三方应用或扫描工具导入数据，请确保将源中的漏洞映射到网络中检测到的漏洞。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **操作系统和服务器身份源** 旁边的 **编辑** (✎) 。

步骤 4 要添加新源，请点击 **Add Source**。

步骤 5 输入 **Name**。

步骤 6 从下拉列表中选择输入源**类型 (Type)**：

- 如果打算使用 AddScanResult 函数导入扫描结果，请选择**扫描工具 (Scanner)**。
- 如果不打算导入扫描结果，请选择**应用 (Application)**。

步骤 7 要指示从此源将某个身份添加到网络映射到删除该身份之间的持续时间，请从**超时**下拉列表中选择**小时数**、**天数**或**周数**，并输入适当的持续时间。

步骤 8 或者：

- 要升级某个源并使用操作系统和应用身份以支持列表中该源下面的源，请选择该源并点击向上箭头。
- 要降级某个源并且只有列表中该源上面的源没有提供身份时才会使用操作系统和应用身份，请选择改源并点击向下箭头。
- 要删除某个源，请点击该源旁边的 **删除** (🗑) 。

步骤 9 点击**保存**以保存身份源设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

相关主题

映射第三方漏洞

对网络发现策略进行故障排除

在对系统的默认检测功能进行任何更改之前，应分析哪些主机未被正确地识别以及原因，以便可以决定实施哪些解决方案。

托管设备是否正确布置？

如果诸如负载均衡器、代理服务器或NAT设备的网络设备位于托管设备和未识别或错误识别的主机之间，请将托管设备布置在更靠近错误识别的主机的位置，而不是使用自定义指纹技术。思科不建议在这种情况下使用自定义指纹技术。

未识别的操作系统是否拥有唯一的 TCP 堆栈？

如果系统识别的主机错误，应调查主机为何被错误地识别，以便帮助您决定：是创建和激活自定义指纹，还是用 Nmap 或主机输入数据替代发现数据。

⚠

注意 如果遇到错误识别的主机，请在创建自定义指纹之前联系支持代表。

如果主机正在运行的操作系统未被系统默认检测到，并且该操作系统不与检测到的现有操作系统共享识别性 TCP 堆栈特征，则应创建自定义指纹。

例如，如您拥有的 Linux 自定义版本带有系统无法识别的唯一 TCP 堆叠，则创建自定义指纹将让您受益，因为这可使系统识别并继续监控主机，而不必使用扫描结果或第三方数据，进而无需持续自行主动更新这些数据。

请注意，许多开源Linux发行版本使用相同的内核，同样，系统将使用Linux内核名称来识别它们。如为 Red Hat Linux 系统创建自定义指纹，可能会看到识别为 Red Hat Linux 的其他操作系统（如 Debian Linux、Mandrake Linux、Knoppix 等），因为相同的指纹与多个 Linux 发行版本匹配。

不应在每种情况下都使用指纹。例如，可能对主机的 TCP 堆叠做出了修改，以使其与另一操作系统类似或相同。例如，Apple Mac OS X 主机已修改，使其指纹与 Linux 2.4 主机相同，从而导致系统将其识别为 Linux 2.4 而不是 Mac OS X。如果为 Mac OS X 主机创建自定义指纹，可能会导致所有合法的 Linux 2.4 主机被错误地识别为 Mac OS X 主机。在这种情况下，如果 Nmap 正确地识别主机，应为该主机安排定期的 Nmap 扫描。

如果使用主机输入从第三方系统导入数据，则必须将第三方用于描述服务器和应用协议的供应商、产品和版本字符串映射到这些产品的思科定义。请注意，即使将应用数据映射到Firepower系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

系统可以协调来自多个源的数据，以便确定操作系统或应用的当前标识。

对于 Nmap 数据，可安排定期 Nmap 扫描。对于主机输入数据，可定期运行用于导入的 Perl 脚本或命令行实用程序。然而，请注意，主动扫描数据和主机输入数据可能不会随发现数据的频率进行更新。

Firepower 系统能否识别所有应用？

如果主机已由系统正确识别，但有未识别的应用，则可创建用户定义的检测器来向系统提供端口和模式匹配信息以帮助识别应用。

是否已应用可修复漏洞的修补程序？

如果系统已正确识别主机，但未反映已应用的修补，则可使用主机输入功能导入修补程序信息。导入修补程序信息时，必须将修补程序的名称映射至数据库中的修补程序。

是否要跟踪第三方漏洞？

如果拥有要用于影响关联的第三方系统的漏洞信息，则可将服务器和应用协议的第三方漏洞标识符映射到思科数据库中的漏洞标识符，然后使用主机输入功能导入漏洞。有关使用主机输入功能的详细信息，请参阅《《*Firepower* 系统主机输入 *API* 指南》》。请注意，即使将应用数据映射到Firepower系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

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。