网络安全管理示例

本章包含以下部分：

- 网络安全管理示例, on page 1

网络安全管理示例

本附录介绍和说明实施思科内容安全管理设备功能的许多常规方式，包括以下部分：

- 示例 1：调查用户 , on page 1
- 示例 2：跟踪 URL, on page 3
- 示例 3：调查受访问的排名靠前的 URL 类别, on page 3

网络安全设备示例

本部分介绍使用安全管理设备和网络安全设备的示例。

Note 所有这些示例场景均假设您已在安全管理设备和网络安全设备上启用 Web 报告和 Web 跟踪。有关如何启用 Web 跟踪和 Web 报告的信息，请参阅使用集中 Web 报告和跟踪

示例 1：调查用户

此示例演示了系统管理员将如何调查公司中的特定用户。

在此情景中，经理收到关于员工在工作时访问不当网站的投诉。为了调查此用户，系统管理员现在需要跟踪其网络活动的详细信息。

在跟踪网络活动后，就会生成一个 Web 报告，其中包含关于员工浏览历史记录的信息。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 用户 (Users)**。

步骤 2 在**用户 (Users)** 表中，点击要调查的**用户 ID (User ID)** 或**客户端 IP 地址 (Client IP address)**。

如果您不知道用户 ID 或客户端 IP 地址，请在文本字段中键入您能够想起的用户 ID 或客户端 IP 地址信息，然后点击**查找用户 ID 或客户端 IP 地址 (Find User ID or Client IP address)**。IP 地址不需要是精确匹配项就可以返回结果。您指定的用户 ID 和客户端 IP 地址会填充到“用户”(Users) 表中。在本示例中，我们将查找有关客户端 IP 地址 `10.251.60.24` 的信息。

步骤 3 点击 IP 地址 **`10.251.60.24`**。

此时将出现 `10.251.60.24` 的“用户详细信息”(User Details) 页面。

从“用户详细信息”(User Details) 页面中，您可以确定“按事务总数列出的 URL 类别”(URL Categories by Total Transactions)、“按事务总数列出的趋势”(Trend by Total Transaction)、“匹配的 URL 类别”(URL Categories Matched)、“匹配的域”(Domains Matched)、“匹配的应用”(Applications Matched)、“检测到的恶意软件威胁”(Malware Threats Detected) 和“匹配的策略”(Policies Matched)。

例如，这些类别使您可以了解用户 `10.251.60.24` 是否正在尝试访问被阻止的 URL，可在该页面的“域”部分下的“被阻止的事务”列中查看这些 URL。

步骤 4 点击“匹配的域”(Domains Matched) 表下的**导出 (Export)** 以查看用户尝试访问的域和 URL 的完整列表。

您可以在此处使用“Web 跟踪”(Web Tracking) 功能跟踪和查看此特定用户的网络使用情况。

Note 请务必注意，使用 Web 报告功能可以检索用户访问的所有域信息，但不一定可以检索用户访问的特定 URL。有关用户访问的特定 URL、用户访问 URL 的时间以及是否允许相应 URL 等信息，可使用“Web 跟踪”(Web Tracking) 页面上的“代理服务”(Proxy Services) 选项卡。

步骤 5 依次选择**网络 (Web) > 报告 (Reporting) > Web 跟踪 (Web Tracking)**。

步骤 6 点击**代理服务 (Proxy Services)** 选项卡。

步骤 7 在“用户/客户端 IP 地址”(User/Client IP Address) 文本字段中，键入用户名或 IP 地址。

在本示例中，我们将搜索用户 `10.251.60.24` 的 Web 跟踪信息。

屏幕上将显示搜索结果。

在此页面上，您可以查看分配了 IP 地址 `10.251.60.24` 的计算机的用户访问过的事务和 URL 的完整列表。

相关主题

下表列出了本示例中介绍的每个主题。点击链接可查看关于每个主题的详细信息。

Table 1: 调查用户的相关主题

功能名称	功能信息
用户页面	用户报告 (Web)
“用户详细信息”(User Details) 页面	用户详细信息（Web 报告）
导出报告数据	并导出报告和跟踪数据
“Web 跟踪”(Web Tracking) 页面上的“代理服务”(Proxy Services) 选项卡	搜索网络代理服务处理的事务

示例 2：跟踪 URL

在此情景中，销售经理希望了解其所在公司上星期访问量最高的前五个网站。此外，该经理希望了解哪些用户访问那些网站。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 网站 (Web Sites)**。

步骤 2 从“时间范围 (Time Range)”下拉列表中，选择**周 (Week)**。

步骤 3 向下滚动到“域”(Domains) 部分以查看访问过的域或网站。

访问过的前 25 个网站将显示在“匹配的域”(Domains Matched) 表中。在同一个表中，您可以点击“域”(Domain) 或“IP”列中的链接查看特定地址或用户实际访问的网站。

相关主题

下表列出了本示例中介绍的每个主题。点击链接可查看关于每个主题的详细信息。

Table 2: 跟踪 ***URL*** 的相关主题

功能名称	功能信息
网站页面	网站报告

示例 3：调查受访问的排名靠前的 URL 类别

在此情景中，人力资源经理希望了解其员工在 30 天内访问的前三种 URL 类别。此外，网络经理希望获得此信息以监控带宽使用量，从而了解哪些 URL 在其网络中占用最多带宽。

下面的示例旨在向您展示如何为多人收集涵盖多个关注点的数据，与此同时只需生成一个报告。

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > URL 类别 (URL Categories)**。

在本示例的“URL 类别”(URL Categories) 页面上，您可以看到，图形所显示的按事务总数列出的前 10 种 URL 类别中，访问过的“未分类 URL”(Uncategorized URLs) 有 28.2 万个，并且还访问了“即时消息”(Instant Messaging)、“仇恨言论”(Hate Speech) 和“纹身”(Tattoo) 等站点。

此时，您可以通过点击**导出 (Export)** 链接将这些原始数据导出到 Excel 电子表格，然后将此文件发送给人力资源经理。但是请记住，您的网络经理希望了解每个 URL 的带宽使用量。

步骤 2 需要新插图 - 跳过向下滚动到**匹配的 URL 类别**表以查看“使用的带宽”列。

从**匹配的 URL 类别 (URL Categories Matched)** 表中，您可以查看所有 URL 类别的带宽使用量。同样，您可以点击**导出 (Export)** 链接，然后将此文件发送给网络经理。但是，如需查看更精细的信息，请点击“即时消息”(Instant Messaging) 链接了解哪些用户占用带宽。此时将出现以下页面。

网络经理可以在此页面上查看“即时消息”(Instant Messaging) 站点访问量的前 10 名用户。

此页面显示，在过去 30 天里，用户 10.128.4.64 在即时消息网站上花了 19 小时 57 分钟，该时间的带宽使用量为 10.1 MB。

相关主题

下表列出了本示例中介绍的每个主题。点击链接可查看关于每个主题的详细信息。

Table 3: 调查前几项 ***URL*** 类别的相关主题

功能名称	功能信息
URL 类别页面	URL 类别报告
导出报告数据	并导出报告和跟踪数据

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。