使用集中 Web 报告和跟踪

本章包含以下部分：

集中 Web 报告和跟踪概述

思科安全邮件和Web管理器设备可以聚合来自多个网络安全设备上的安全功能的信息，并记录可用于监控网络流量模式和安全风险的数据。可以实时运行报告来查看特定时间段内系统活动的交互显示，也可以安排并定期运行报告。此外，报告功能还可将原始数据导出到文件。

集中Web报告功能不仅可生成概要报告，使管理员可以了解网络上发生的情况，而且还使管理员可以深入分析并查看特定域、用户或类别的流量详细信息。

域

对于域，Web报告功能可以将以下数据元素生成到域报告。例如，如果您在Facebook.com域上生成报告，则报告可能包含：

- 访问 Facebook.com 的排名靠前的用户的列表
- Facebook.com 内访问量排名靠前的 URL 的列表

用户

对于用户，Web 报告功能可以将数据元素生成到用户报告。例如，对于标题为“Jamie”的用户报告，报告可能包含：

- 用户“Jamie”访问的排名靠前的域的列表
- 具有恶意软件或病毒特征的排名靠前的 URL 的列表
- 用户“Jamie”访问的排名靠前的类别的列表

URL 类别

对于 URL 类别，Web 报告功能可以生成要包括在类别报告中的数据。例如，对于类别“Sports”，报告可能包含：

- 位于“Sports”类别中的排名靠前的域的列表
- 访问“Sports”类别的排名靠前的用户的列表

在上述所有这些示例中，这些报告旨在提供网络上特定项目的综合视图，以便管理员可以采取行动。

常规

有关记录页面与报告页面的详细说明，请参阅日志记录与报告。

Note 您可以检索用户访问的所有域信息，而不一定是用户访问的特定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) 页面上的搜索网络代理服务处理的事务 , on page 68。

Note 网络安全设备仅在使用本地报告时才存储数据。如果为网络安全设备启用了集中报告，则网络安全设备仅保留系统容量和系统状态数据。如果未启用集中 Web 报告，则仅会生成系统状态和系统容量报告。

有多种方式可用于查看有关安全管理设备的 Web 报告数据。

- 要查看交互式报告页面，请参阅Web 报告页面说明, on page 6。
- 要按需生成报告，请参阅按需生成 Web 报告 , on page 63。
- 要安排重复性地定期生成报告，请参阅关于计划的报告和按需 Web 报告, on page 58。
- 要查看以前运行的报告（已安排和按需生成）的存档版本，请参阅查看和管理存档的 Web 报告, on page 64。
- 要查看各个事务的信息，请参阅Web跟踪 , on page 67。

设置集中 Web 报告和跟踪

要设置集中 Web 报告和跟踪，请按顺序完成以下步骤：

在安全管理设备上启用集中 Web 报告

步骤 1 在启用集中 Web 报告之前，请确保已为该服务分配足够的磁盘空间。请参阅管理磁盘空间。

步骤 2 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 3 选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **网络 (Web)** > **集中报告 (Centralized Reporting)**。

步骤 4 如果您是在运行“系统设置向导”(System Setup Wizard) 后首次启用集中报告：

a) 点击**启用 (Enable)**。

b) 审查最终用户许可协议，然后点击**接受 (Accept)**。

步骤 5 如果您是在先前禁用集中报告后将其再次启用：

a) 点击**编辑设置 (Edit Settings)**。

b) 选中**启用集中 Web 报告服务 (Enable Centralized Web Report Services)** 复选框。

c) 可以现在或稍后访问在 Web 报告中让用户名保持匿名 , on page 4。

步骤 6 提交并确认更改。

在网络安全设备上启用集中 Web 报告

在启用集中报告之前，应配置所有网络安全设备并确保其按预期工作。

必须在将要使用集中报告的每个网络安全设备上启用集中报告。

请参阅《思科网络安全设备 AsyncOS 用户指南》中的“启用集中报告”部分。

将集中 Web 报告服务添加到每个托管网络安全设备

执行的步骤取决于是否已在配置其他集中管理功能时添加了设备。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 选择**管理设备 > 集中服务 > 安全设备**。

步骤 3 如果已将网络安全设备添加到列表，请执行以下操作：

a) 点击网络安全设备的名称。

b) 选择**集中报告 (Centralized Reporting)** 服务。

步骤 4 如果您尚未添加网络安全设备，请执行以下操作：

a) 点击“添加网络设备”(Add Web Appliance)。

b) 在“设备名称 (Appliance Name)”和“IP 地址 (IP Address)”文本字段，键入设备名称和网络安全设备管理接口的 IP 地址。

Note 可以在“IP 地址 (IP Address)”文本字段中输入 DNS 名称，但点击**提交**后，它将立即解析为 IP 地址。

c) 集中报告服务已预先选中。

d) 点击**建立连接 (Establish Connection)**。

e) 在要托管的设备上输入管理员账户的用户名和口令，然后点击**建立连接 (Establish Connection)**。

Note 输入登录凭证，以便将文件传输的公共 SSH 密钥从安全管理设备传递到远程设备。登录凭证不会存储在安全管理设备上。

f) 等待该页面表格上方显示成功消息。

g) 点击**测试连接 (Test Connection)**。

h) 阅读表格上方的测试结果。

步骤 5 点击**提交 (Submit)**。

步骤 6 为每个您要启用集中报告的网络安全设备重复此操作步骤。

步骤 7 确认您的更改。

在 Web 报告中让用户名保持匿名

默认情况下，用户名显示在报告页面上和 PDF 中。但是，为保护用户隐私，您可能希望在 Web 报告中令用户名无法识别。

Note 设备上具有管理员权限的用户在查看交互报告时可以始终查看用户名。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 网络 (Web) > 集中报告 (Centralized Reporting)**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 选中**在报告中让用户名保持匿名 (Anonymize usernames in reports)** 复选框。

步骤 5 提交并确认更改。

与网络安全报告一起使用

Web 报告页面支持监控有关系统中一个或所有托管网络安全设备上的信息。

要想	请参阅
访问和查看报告数据的视图选项	查看报告数据的各种方法
自定义交互报告页面的视图	自定义报告数据的视图
查找数据内特定事务的信息	Web跟踪 , on page 67
打印或导出报告信息	并导出报告和跟踪数据
了解各种交互报告页面	Web 报告页面说明, on page 6
按需生成报告	了解新 Web 界面上的“Web 报告”(Web Reporting) 页面, on page 33
安排报告，以便按指定的间隔和时间自动运行	关于计划的报告和按需 Web 报告, on page 58
查看按需存档的报告和已安排的报告	查看和管理存档的 Web 报告, on page 64
了解数据的收集方式	安全管理设备如何收集报告的数据

在新 Web 界面上使用网络安全报告

Web 报告页面支持监控有关系统中一个或所有托管网络安全设备上的信息。

收件人	请参阅
访问和查看报告数据的视图选项	查看报告数据的各种方法
自定义交互报告页面的视图	自定义报告数据的视图
查找数据内特定事务的信息	新 Web 界面上的 Web 跟踪， 第 73 页
打印或导出报告信息	并导出报告和跟踪数据
了解各种交互报告页面	了解新 Web 界面上的“Web 报告”(Web Reporting) 页面，第 33 页

Web 报告页面说明

Note 有关“Web 报告 (Web Reporting)”选项卡上哪些选项可用于按需或计划报告的信息，请参阅关于计划的报告和按需 Web 报告, on page 58。

Table 1:“Web 报告”(Web Reporting) 选项卡详细信息

“Web 报告”(Web Reporting) 菜单	操作
Web 报告概述 , on page 9	“概述”(Overview) 页面提供您的网络安全设备上的活动的概要。它包括传入和传出事务的图和摘要表。有关详细信息，请参阅Web报告概述 , on page 9。
用户报告 (Web) , on page 10	“用户”(Users) 页面提供多个 Web 跟踪链接，允许您查看各个用户的 Web 跟踪信息。 从**用户 (Users)** 页面中，可以查看系统上的一个或多个用户在互联网、特定站点或 URL 上花费的时间，以及用户使用多少带宽。 从**用户 (Users)** 页面中，可以点击交互式用户表格中的单个用户，以在“用户详细信息”(User Details) 页面上查看该特定用户的更多详细信息。 通过**用户详细信息 (User Details)** 页面，可以查看关于在**网络 (Web) > 报告 (Reporting) > 用户 (Users)** 页面的“用户”(Users) 表格中识别的用户的特定信息。从该页面您可以深入研究系统上各个用户的活动。如果您正在运行用户级调查，并且需要查找诸如用户正在访问哪些站点、他们遇到了哪些恶意软件威胁、正在访问哪些 URL 类别，以及特定用户在这些站点上花费了多少时间等信息，则此页面将非常有用。 有关详细信息，请参阅用户报告 (Web) , on page 10。有关您的系统中特定用户的信息，请参阅用户详细信息（Web 报告） , on page 11
用户计数报告 (Web)	“用户计数”(User Count) 页面提供有关启用了集中报告的网络安全设备的经过身份验证和未经身份验证的用户总数的信息。该页面列出最近 30 天、90 天和 180 天的唯一用户计数。 **Note** 系统每小时计算一次已经过身份验证和未经身份验证的用户总数。
网站报告 , on page 13	“网站”(Web Sites) 页面允许您查看托管设备上所发生的活动的汇聚情况。从该页面您可以监控特定时间范围内访问的高风险网站。有关详细信息，请参阅网站报告 , on page 13。

“Web 报告”(Web Reporting) 菜单	操作
URL 类别报告 , on page 14	利用“URL 类别”(URL Categories) 页面可以查看所访问的排名靠前的 URL 类别，包括： • 每个事务已触发阻止或警告操作发生的排名靠前的 URL。 • 已完成、已警告和已阻止事务在指定时间范围内的所有URL类别。这是一个交互表，具有交互列标题，您可以使用该列标题按需排序数据。 有关详细信息，请参阅URL 类别报告 , on page 14。
应用可视性报告 , on page 16	通过“应用可视性”(Application Visibility) 页面，可以应用和查看已用于安全管理设备和网络安全设备中特定应用类型的控件。有关详细信息，请参阅应用可视性报告 , on page 16。
防恶意软件报告 , on page 17	“防恶意软件”(Anti-Malware) 页面允许您查看在指定时间范围内防恶意软件扫描引擎检测到的恶意软件端口和恶意站点的信息。报告的上半部分显示每个排名靠前的恶意软件端口和网站的连接数量。报告的下半部分显示检测到的恶意软件端口和网站。有关详细信息，请参阅防恶意软件报告 , on page 17。
高级恶意软件防护（文件信誉和文件分析）报告 , on page 20	有三个显示文件信誉和分析数据的报告页面。 有关详细信息，请参阅高级恶意软件防护（文件信誉和文件分析）报告 , on page 20。
客户端恶意软件风险报告 , on page 25	“客户端恶意软件风险”(Client Malware Risk) 页面是一个安全相关的报告页面，可以用于确定那些正异常频繁地连接到恶意软件站点的各个客户端计算机。 有关详细信息，请参阅客户端恶意软件风险报告 , on page 25。
网络信誉过滤器报告 , on page 26	允许您查看指定时间范围内事务的网络信誉过滤报告。有关详细信息，请参阅网络信誉过滤器报告 , on page 26。
L4 流量监控器报告 , on page 28	允许您查看在指定时间范围内第 4 层流量监控器检测到的恶意软件端口和恶意站点的信息。有关详细信息，请参阅L4 流量监控器报告 , on page 28。
SOCKS 代理报告 , on page 30	允许您查看 SOCKS 代理事务的数据，包括目标和用户。 有关详细信息，请参阅SOCKS 代理报告 , on page 30。
按用户地点分类的报告 , on page 30	“按用户位置报告”(Reports by User Location) 页面允许您查看您的移动用户正在其本地或远程系统上执行哪些活动。 有关详细信息，请参阅按用户地点分类的报告 , on page 30。

“Web 报告”(Web Reporting) 菜单	操作
Web跟踪 , on page 67	“Web 跟踪”(Web Tracking) 页面允许您搜索以下类型的信息： • 通过搜索网络代理服务处理的事务 , on page 68，可以跟踪和查看与网络相关的基本信息，例如通过设备处理的网络流量类型。 这包括诸如时间范围、用户 ID 和客户端 IP 地址等信息，同时还包括特定 URL 类型、每个连接占用了多少带宽以及跟踪特定用户的网络使用情况等信息。 • 通过搜索 L4 流量监控器处理的事务 , on page 72，可以搜索 L4TM 数据以了解恶意软件传输活动涉及的站点、端口和客户端IP地址。 • 通过搜索 SOCKS 代理处理的事务 , on page 72，可以搜索 SOCKS 代理处理的事务。 有关详细信息，请参阅Web跟踪 , on page 67。
“系统容量”(System Capacity) 页面, on page 31	可用于查看将报告数据发送到安全管理设备的总体工作负载。 有关详细信息，请参阅“系统容量”(System Capacity) 页面, on page 31。
“数据可用性”(Data Availability) 页面, on page 33	可用于概括了解报告数据对每个设备上的安全管理设备的影响。有关详细信息，请参阅“数据可用性”(Data Availability) 页面, on page 33。
计划的报告	允许您为指定时间范围安排报告。有关详细信息，请参阅关于计划的报告和按需 Web 报告, on page 58。
存档的报告	允许您为指定时间范围存档报告。有关详细信息，请参阅查看和管理存档的 Web 报告, on page 64。

Note 您可以为大多数 Web 报告类别安排报告，包括扩展的排名靠前的 URL 类别和排名靠前的应用类型的附加报告。有关安排报告的更多信息，请参阅关于计划的报告和按需 Web 报告, on page 58

关于“所花费时间”(Time Spent)

各个表中“所花费时间”(Time Spent) 列表示用户在某个网页上所花费的时间。用户在每个 URL 类别上所花费的时间（为了用户调查）。当跟踪 URL 时，每个用户在该特定 URL 上所花费的时间。

一旦事务事件被标记“已查看”(viewed)，即用户访问特定 URL，将会开始计算一个“所花费时间”(Time Spent) 值，并将其添加为 Web 报告表中的一个字段。

为计算所花费时间，AsyncOS 针对一分钟期间内的活动为每个活动用户分配 60 秒时间。在这一分钟结束时，在用户访问的不同域之间将会均分每个用户所花费的时间。例如，如果用户在一个活动分钟内访问四个不同的域，则会认为该用户在每个域花费 15 秒。

对于所花费时间值，请注意以下事项：

- 活动用户定义为通过设备发送 HTTP 流量并访问 AsyncOS 视为一次“页面阅览”的网站的用户名或 IP 地址。
- AsyncOS 会将页面阅览定义为用户发起的 HTTP 请求，与客户端应用发起的请求相对。AsyncOS 使用启发式算法进行最佳猜测，以确定用户页面阅览量。

单位以小时：分钟格式显示。

Web 报告概述

网络 (Web) > 报告 (Reporting) > 概述 (Overview) 页面提供您的网络安全设备上的活动概要。它包括传入和传出事务的图和摘要表。

概述 (Overview) 页面概括地显示有关 URL 和用户使用、网络代理活动以及各种事务摘要的统计数据。事务摘要为诸如可疑事务等内容提供进一步的趋势详细信息，并且直接从此图中可以了解阻止了多少上述可疑事务，以及阻止的方式。

概述 (Overview) 页面的下半部分介绍使用情况。也就是查看的排名靠前的 URL 类别、排名靠前的应用类型以及被阻止的类别，生成这些阻止或警告的排名靠前的用户。

Table 2: *“Web 报告概述”页面详细信息*

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
查看以下项的数据 (View Data for)	选择要查看其概述数据的网络安全设备，或选择所有网络设备。 另请参阅查看设备或报告组的报告数据。
Web 代理活动总数	通过此部分可查看当前由安全管理设备管理的网络安全设备报告的网络代理活动。 此部分显示实际事务数（纵坐标）以及发生活动的大约日期（水平时间轴）。
网络代理摘要 (Web Proxy Summary)	本部分允许您查看可疑或正常的网络代理活动的百分比，包括事务总数。
L4 流量监控摘要	本部分报告当前由安全管理设备管理的网络安全设备所报告的任何 L4 流量。
可疑事务数	本部分允许您查看被管理员标记为可疑事务的网络事务。 本部分显示事务的实际数量（垂直标尺），以及活动发生的大约日期（水平时间线）。
可疑事务摘要 (Suspect Transactions Summary)	本部分允许您查看因可疑而被阻止或警告的事务的百分比。另外，您可以查看已被检测和阻止的事务的类型，以及此事务被阻止的实际次数。

部分	说明
按事务总数排名靠前的 URL 类别 (Top URL Categories by Total Transactions)	本部分显示被阻止的排名靠前 10 个 URL 类别，包括 URL 类别的类型（垂直标尺）以及已阻止的特定类型类别的实际次数（水平标尺）。 预定义的 URL 类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 , on page 15。
按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)	本部分显示正阻止的排名靠前的应用类型，包括实际应用类型的名称（垂直标尺）和已阻止的特定应用的次数（水平标尺）。
检测到的恶意软件类别总数 (Top Malware Categories Detected)	此部分显示检测到的所有恶意软件类别。
受阻或警告事务数排名靠前的用户 (Top Users Blocked or Warned Transactions)	本部分显示生成已阻止或已警告事务的实际用户。可以按 IP 地址或按用户名称来显示用户。要使用户名无法识别，请参阅在 Web 报告中让用户名保持匿名 , on page 4。
网络流量分流状态	以图形格式显示未分流和已分流流量的事务。
网络流量分流摘要	显示已分流和未使用流量事务以及总流量事务的摘要。
已分流 HTTP/HTTPS 流量	以图形格式显示已分流 HTTP 和 HTTPS 流量的事务。
已分流流量摘要	显示 HTTP 和 HTTPS 流量事务以及总 HTTP/HTTPS 流量事务的摘要。

用户报告 (Web)

网络 (Web) > 报告 (Reporting) > 用户 (Users) 页面提供了多个链接，可用于查看各个用户的 Web 报告信息。

从**用户 (Users)** 页面中，可以查看系统上的一个或多个用户在互联网、特定站点或 URL 上花费的时间，以及用户使用多少带宽。

从**用户 (Users)** 页面，可以查看有关系统中用户的以下信息：

Table 3: *“网络”(Web) > “报告”(Reporting) > “用户”(Users) 页面上的详细信息*

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
按受阻事务数排名靠前的用户 (Top Users by Transactions Blocked)	本部分的垂直标尺按 IP 地址或用户名列出排名靠前的用户，水平标尺列出针对该用户所阻止的事务数量。报告时可以将用户名或 IP 地址进行匿名。有关如何在此页或在已安排报告中令用户名无法无法识别的更多信息，请参阅在安全管理设备上启用集中 Web 报告 , on page 3。默认设置为所有用户名均显示。要隐藏用户名，请参阅在 Web 报告中让用户名保持匿名 , on page 4。

部分	说明
按使用的带宽排名靠前的用户 (Top Users by Bandwidth Used)	本部分的垂直标尺按 IP 地址或用户名列出系统上排名靠前的用户,水平标尺上以 GB 显示在系统上使用最多带宽的用户。
用户表 (Users Table)	您可以找到查找特定用户 ID 或客户端 IP 地址。在“用户”(User) 部分底部的文本字段中，请输入特定用户 ID 或客户端 IP 地址，并点击**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。 在“用户”(Users) 表，可以点击特定用户以找到更具体的信息。此信息显示在“用户详细信息”(User Details) 页面。有关“用户详细信息”(User Details) 页面的详细信息，请参阅用户详细信息（Web 报告） , on page 11。

Note 要查看用户 ID 而不是客户端 IP 地址，必须设置安全管理设备，以从 LDAP 服务器获取用户信息。有关详细信息，请参阅与 LDAP 集成章节中的创建 LDAP 服务器配置文件。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

要查看如何使用**用户 (Users)** 页面的示例，请参阅示例 1：调查用户。

Note 您可以为“用户”(Users) 页生成或安排报告。有关更多信息，请参阅关于计划的报告和按需 Web 报告, on page 58。

用户详细信息（Web 报告）

通过**用户详细信息 (User Details)** 页面，可以查看关于在**网络 (Web) > 报告 (Reporting) > 用户 (Users)** 页面上的交互式用户表中识别的用户的特定信息。

通过**用户详细信息 (User Details)** 页面，可以调查系统上各个用户的活动。如果您正在运行用户级调查，并且需要查找诸如用户正在访问哪些站点、他们遇到了哪些恶意软件威胁、正在访问哪些 URL 类别，以及特定用户在这些站点上花费了多少时间等信息，则此页面将非常有用。

要显示特定用户的**用户详细信息 (User Details)** 页面，请点击**网络 (Web) > 用户 (Users)** 页面上用户表中的特定用户。

从**用户详细信息 (User Details)** 页面，可以查看有关系统中各个用户的以下信息：

Table 4: *“网络”(Web) >“报告”(Reporting) >“用户”>“用户详细信息”(User Details)* 页面详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	该菜单允许您选择报告中所包含数据的时间范围。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。

部分	说明
按事务总数的 URL 类别 (URL Categories by Total Transactions)	本部分列出特定用户正在使用的特定 URL 类别。 预定义的URL类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 , on page 15。
按事务总数的趋势 (Trend by Total Transactions)	本图显示了用户访问网络的时间。 例如，此图将指示在一天的某些时段内是否存在网络流量激增以及这些激增发生的时间。使用“时间范围”(Time Range) 下拉列表，您可以扩展此图，以查看此用户在网络上的更为精细或粗略的时间范围。
匹配的 URL 类别 (URL Categories Matched)	“匹配的 URL 类别”(URL Categories Matched) 部分显示了已完成和已阻止事务的匹配类别。 从本部分您还可以找到特定的URL类别。在该部分底部的文本字段中，输入URL类别并点击**查找 URL 类别 (Find URL Category)**。该类别不需要是完全匹配。 预定义的URL类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 , on page 15。
匹配的域 (Domains Matched)	在本部分，您可以查看此用户已经访问的特定域或 IP 地址的相关信息。您还可以查看在这些类别上所花费的时间，以及您在列视图中设置的其他各类信息。在该部分底部的文本字段中，输入域或 IP 地址，并点击**查找域或 IP (Find Domain or IP)**。域或 IP 地址不必是完全匹配。
匹配的应用 (Applications Matched)	在此部分,可以找到特定用户正在使用的特定应用。例如，如果用户正在访问需要使用大量 Flash 视频的站点，您将在“应用”(Application) 列中看到此应用类型。 在该部分底部的文本字段中，输入应用名称，并点击**查找应用 (Find Application)**。应用的名称不必是完全匹配。
检测到的恶意软件威胁数 (Malware Threats Detected)	在此表中，您可以查看特定用户触发的排名靠前的恶意软件威胁。 您可以在“查找恶意软件威胁”(Find Malware Threat) 字段中搜索特定恶意软件威胁名称的数据。输入“恶意软件威胁”(Malware Threat) 名称并点击“查找恶意软件威胁”(Find Malware Threat)。恶意软件威胁的名称不必是完全匹配。
匹配的策略 (Policies Matched)	在此部分，可以找到当用户访问网络时适用于此用户的策略组。 在该部分底部的文本字段中，输入策略名称，并点击**查找策略 (Find Policy)**。策略的名称不必是完全匹配。

Note 在“客户端恶意软件风险详细信息”(Client Malware Risk Details) 表：客户端报告有时会在用户名的末尾显示星号 (*). 例如，客户端报告可能会同时为“jsmith”和“jsmith*”显示一个条目。带有星号 (*) 的用户名表示用户提供的用户名，但并未经身份验证服务器确认。当身份验证服务器不可用，并且设备配置为在身份验证服务不可用的情况下允许流量时，可能会出现上述情况。

要查看如何使用“用户详细信息”(User Details) 页面的示例，请参阅示例 1：调查用户。

用户计数报告 (Web)

网络 (Web) >报告 (Reporting) > 用户计数 (User Count) 页面显示有关启用了集中报告的网络安全设备的经过身份验证和未经身份验证的用户总数的信息。该页面列出最近 30 天、90 天和 180 天的唯一用户计数。

注释 系统每小时计算一次已经过身份验证和未经身份验证的用户总数。

网站报告

网络 (Web) > 报告 (Reporting) > 网站 (Web Sites) 页面汇聚了托管设备上所发生活动的整体情况。从该页面您可以监控特定时间范围内访问的高风险网站。

在**网站**页，您可以查看以下信息：

Table 5: *“网络” (Web) > “报告” (Reporting) > “网站” (Web Sites)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
按事务总数排名靠前的域 (Top Domains by Total Transactions)	本部分以图的形式站点上被访问量排名靠前的域。
按受阻事务数排名靠前的域 (Top Domains by Transactions Blocked)	本部分以图的形式按事务列出触发阻止操作的排名靠前的域。例如，用户访问了某特定域，并且由于布置了我拥有的一个特定策略，这触发了阻止操作。此域会在此图中以受阻止事务列出，并且列出触发了阻止操作的域站点。
匹配的域 (Domains Matched)	本部分在一个交互表中列出了该站点上正被访问的域。在此表中，通过点击特定域，您可以访问该特定域的更为详细的信息。在“Web 跟踪” (Web Tracking) 页面上的“代理服务” (Proxy Services) 选项中，您可以查看跟踪信息以及某些域被阻止的原因。 当您点击某个特定域时，您可以查看到该域的排名靠前的用户、该域上排名靠前的事务、匹配的 URL 类别以及检测到的恶意软件威胁。 要查看如何使用 Web 跟踪的示例，请参阅示例 2：跟踪 URL。 **Note** 如果您将此数据导出到 .csv 文件，则系统仅导出前 300000 个条目。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

Note 您可以在“网站”(Web Sites) 页面上生成或安排报告。有关更多信息，请参阅关于计划的报告和按需 Web 报告, on page 58。

URL 类别报告

网络 (Web) > 报告 (Reporting) > URL 类别 (URL Categories) 页面可用于查看系统中的用户正在访问的站点的 URL 类别。

在**URL 类别**页面中，您可以查看以下信息：

Table 6: “网络”>“报告”>“*URL* 类别”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
按事务总数排名靠前的 URL 类别 (Top URL Categories by Total Transactions)	本部分以图的形式列出站点上排名靠前的被访问 URL 类别。
按阻止和警告的事务数排名靠前的URL类别 (Top URL Categories by Blocked and Warned Transactions)	本部分以图的形式按事务列出触发阻止或警告操作的排名靠前的URL。例如，用户访问了某特定 URL，并且由于布置了一个特定策略，这触发了阻止操作或警告。然后此 URL 会作为受阻止的事务或警告在图中列出。
匹配的 URL 类别 (URL Categories Matched)	“匹配的 URL 类别”(URL Categories Matched) 部分按 URL 类别显示指定时间范围内的事务处理，以及使用的带宽和每个类别中所花费的时间。 如果有大量未分类的 URL，请参阅减少未分类的 URL , on page 15。
被绕过的 URL 过滤 (URL Filtering Bypassed)	表示在 URL 过滤前发生的策略、端口和管理用户代理阻止。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

Note 要生成比此页面提供信息更为详细的报告，请参阅URL 类别排行榜 - 扩展, on page 61。

- 如果在计划报告内为URL类别使用“数据可用性”，并且在任意设备之间存在着数据差异，则会在页面底部显示以下信息：“此时间范围内的某些数据不可用”。如果没有数据差异，则不会显示任何内容。

减少未分类的 URL

如果未分类的 URL 的百分比高于 15-20%，请考虑以下选项：

- 对于特定的本地化 URL，您可以创建自定义 URL 类别，并将其应用到特定用户或组策略。这些事务将改为包括在“被绕过的 URL 过滤”(URL Filtering Bypassed) 统计信息内。为此，请参阅有关适用于思科网络安全设备的 AsyncOS 用户指南的自定义 URL 类别的信息。
- 对于您认为应包括在现有或其他类别的站点，请参阅报告错误分类和未分类的 URL , on page 16。

URL 类别集更新和报告

预定义的 URL 类别集可能会在安全管理设备上定期更新，如准备和管理 URL 类别集更新中所述。

当发生这些更新时，旧类别的数据将继续显示在报告和 Web 跟踪结果中，直到数据因太旧而无法包括在其中。在类别集更新后生成的报告数据将使用新的类别，因此，您在同一报告中可以同时看到旧类别和新类别。

如果新旧类别的内容之间有重叠，则您可能需要仔细检查报告结果以获取有效的统计信息。例如，如果在所查看的时间段内“即时消息”和“基于网络的聊天”类别已合并到单个“聊天和即时消息”类别，则在合并之前对“即时消息”和“基于网络的聊天”类别中涵盖的站点进行的访问不会计入“聊天和即时消息”的总计中。类似地，在合并后对即时消息或基于网络的聊天站点的访问将会包括在“即时消息”(Instant Messaging) 或“基于网络的聊天”(Web-based Chat) 类别内。

将“URL 类别”页面与其他报告页面结合使用

“URL 类别”(URL Categories) 页面可以与“应用可视性”(Application Visibility) 页面, on page 37和“用户”(User) 页面, on page 45配合使用，以调查特定用户以及该特定用户尝试访问的应用或网站的类型。

例如，在“URL 类别”(URL Categories) 页面, on page 42中可以为人力资源部门生成高级别报告，其中详细说明站点访问的所有 URL 类别。在同一页面，您可以在“URL 类别”(URL Categories) 交互表中收集关于流媒体 (Streaming Media) URL 类别的更多详细信息。通过单击“流媒体”(Streaming Media) 类别链接，可以查看特定的 URL 类别报告页。此页面不仅显示访问流媒体站点的排名靠前的用户（在“按事务总数排名靠前的类别的用户”[Top Users by Category for Total Transactions] 部分），同时还显示所访问的域（在“匹配的域”[Domains Matched] 交互表中），例如，YouTube.com 或 QuickPlay.com。

此时，您会获得特定用户的越来越精准的信息。现在，让我们假设此特定用户因为其用量而显得尤为突出，则您可能想确切地找出他们正在访问什么内容。在这里，您可以在“用户”(Users) 交互表中单击用户。此操作会将您带到“用户”(User) 页面, on page 45，您可以在这里查看该用户的用户趋势，并准确地了解他们正在网络做什么。

如果您希望了解更多内容，现在可以单击交互表中的“已完成事务”(Transactions Completed) 链接，深入了解 Web 跟踪详细信息。这会在“Web 跟踪”(Web Tracking) 页面上显示搜索网络代理服务处理的事务 , on page 68，在此页面中可以查看有关用户访问站点的日期、完整 URL 以及在该 URL 上花费的时间等实际详细信息。

要查看如何使用“URL 类别”(URL Categories) 页面的其他示例，请参阅示例 3：调查受访问的排名靠前的 URL 类别。

报告错误分类和未分类的 URL

您可以在以下 URL 报告错误分类的和未分类的 URL：

https://talosintelligence.com/tickets。

会评价提交，以便包括在后续规则更新中。

要检查已提交的 URL 的状态，请单击此页面上的**有关已提交 URL 的状态 (Status on Submitted URLs)** 选项卡。

应用可视性报告

Note 有关应用可视性的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》的“了解应用可视性与可控性”一章。

通过**网络 (Web) > 报告 (Reporting) > 应用可视性 (Application Visibility)**页，可以将应用控制用于安全管理设备和网络安全设备中的特定应用类型。

应用控件不仅可以为您提供比只使用URL过滤更为精细的网络流量控制，同时它会为您提供对诸如以下应用类型的更多控制：

- 规避应用，例如匿名程序和加密隧道。
- 协作应用，例如 Cisco Webex、Facebook 和即时消息。
- 资源密集型应用，例如流媒体。

了解应用与应用类型之间的差异

了解应用和应用类型之间的差异以便可以控制报告涉及的应用，这一点至关重要。

- **应用类型**。包含一个或多个应用的类别。例如，**搜索引擎**是可包含搜索引擎（例如Google Search 和 Craigslist）的应用类型。即时消息是另一种应用类型类别，可能包含 Yahoo Instant Messenger 或 Cisco Webex。Facebook 也是一种应用类型。
- **应用**。属于某一应用类型的特定应用。例如，YouTube 是一种媒体 (Media) 应用类型的应用。
- **应用行为**。用户可以在应用中完成的特定操作或行为。例如，用户可以在使用某种应用（例如 Yahoo Messenger）时传输文件。并非所有应用均包括您可以配置的应用行为。

Note 要了解有关如何使用应用可视性与可控性 (AVC) 引擎以控制 Facebook 活动的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》中的“了解应用可视性与可控性”一章。

在**应用可视性**页面中，您可以查看以下信息：

Table 7: “*Web* 报告应用可视性”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)	本部分以图的形式列出站点上排名靠前的被访问应用类型。例如，像 Instant Messenger 这样的即时聊天工具、Facebook 和演示应用类型。
按受阻事务数排名靠前的应用 (Top Applications by Blocked Transactions)	本部分以图的形式按事务列出触发阻止操作的排名靠前的应用类型。例如，用户尝试启动某个应用类型，例如 Google Talk 或 Yahoo Instant Messenger，由于特定策略已就位，这触发了阻止操作。然后此应用会作为受阻止的事务或警告在图中列出。
匹配的应用类型 (Application Types Matched)	“匹配的应用类型”(Application Types Matched) 交互表允许您查看“按事务总数排名靠前的应用类型”(Top Applications Type by Total Transactions) 表中列出的应用类型。在“应用”(Applications) 列，您可以单击某个应用以查看详细信息
匹配的应用 (Applications Matched)	“匹配的应用”(Applications Matched) 部分显示在指定时间范围内的所有应用。这是一个交互表，具有交互列标题，您可以使用该列标题按需排序数据。 您可以配置您希望显示在“匹配的应用”(Applications Matched) 部分中的列。有关为本部分配置列的信息，请参阅与网络安全报告一起使用, on page 5。 选择要在“应用”(Applications) 表格中显示的特定项目后，可以从**显示的项目 (Items Displayed)** 下拉菜单中选择要显示的项目数。选项有：10、20、50 或 100。 此外，您可以在匹配的应用 (Applications Matched) 部分查找特定应用。在该部分底部的文本字段中，输入特定应用名称，并单击**查找应用 (Find Application)**。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

Note 您可以为“应用可视性”(Application Visibility) 页面上的信息生成已安排报告。有关安排报告的信息，请参阅关于计划的报告和按需 Web 报告, on page 58。

防恶意软件报告

网络 (Web) > 报告 (Reporting) > 防恶意软件 (Anti-Malware) 页面是一个与安全相关的报告页面，反映由启用的扫描引擎（Webroot、Sophos、McAfee 和/或自适应扫描）扫描的结果。

使用此页面可以帮助识别和监控基于网络的恶意软件威胁。

Note 要查看第 4 层流量监控器查找到的恶意软件的数据，请参阅L4 流量监控器报告 , on page 28。

在**防恶意软件**页面中，可以查看以下信息：

Table 8: *“网络”(Web) > “报告”(Reporting) > “防恶意软件”(Anti-Malware) 页面上的详细信息*

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
“排名靠前的恶意软件类别：受监控或受阻止”(Top Malware Categories: Monitored or Blocked)	本部分显示指定类别类型检测到的排名靠前的恶意软件类别。此信息以图的形式显示。有关有效恶意软件类别的详细信息，请参阅恶意软件类别说明, on page 19。
“排名靠前的恶意软件威胁：受监控或受阻止”(Top Malware Threats: Monitored or Blocked)	本部分显示排名靠前的恶意软件威胁。此信息以图的形式显示。
恶意软件类别 (Malware Categories)	“恶意软件类别”(Malware Categories) 交互表为在“排名靠前的恶意软件类别”(Top Malware Categories) 图表中显示的特定恶意软件类别显示详细信息。 点击“恶意软件类别”(Malware Categories) 交互表中的任意链接，您可以更为精细地查看各个恶意软件类别及其位于网络上哪个位置的详细信息。 例外：该表中的“病毒爆发启发式扫描”(Outbreak Heuristics) 链接，允许您查看一个图表，其中显示了何时出现此类别的事务。 有关有效恶意软件类别的详细信息，请参阅恶意软件类别说明, on page 19。
恶意软件威胁数 (Malware Threats)	“恶意软件威胁数”(Malware Threats) 交互表在为“排名靠前的恶意软件威胁”(Top Malware Threats) 部分中显示的特定恶意软件威胁显示详细信息。 以一个数字标记为“病毒爆发”(Outbreak) 的威胁是由 Adaptive Scanning 功能独立于其他扫描引擎标识的威胁。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

恶意软件类别报告 (Malware Category Report)

“恶意软件类别报告”(Malware Category Report) 页允许您查看单个恶意软件类别的详细，以及它在您的网络中正在执行哪些操作。

要访问“恶意软件类别报告”(Malware Category Report) 页，请执行以下操作

步骤 1 在安全管理设备中，从下拉列表中选择**网络 (Web)**。

步骤 2 选择**监控 (Monitoring)** > **防恶意软件 (Anti-Malware)**页面。

步骤 3 在“恶意软件类别 (Malware Categories)”交互式表格中，点击“恶意软件类别 (Malware Category)”列中的一个类别。

步骤 4 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

恶意软件威胁报告 (Malware Threat Report)

“恶意软件威胁报告”(Malware Threat Report) 页显示遭受特定威胁风险的客户端，显示可能受感染客户端的列表，以及指向“客户端详细信息”(Client Detail) 页的链接。报告顶部的趋势图显示在指定的时间范围内因某威胁受到监控和阻止的事务。底部的表显示在指定的时间范围内因某威胁受到监控和阻止的事务的实际数量。

要查看此报告，请在“防恶意软件报告”(Anti-Malware report) 页的“恶意软件类别”(Malware Category) 列中点击一个类别。

有关其他信息，请点击表格下方的**支持门户恶意软件详细信息 (Support Portal Malware Details)** 链接。

恶意软件类别说明

网络安全设备 可以阻止以下类型的恶意软件：

恶意软件类型	说明
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。某些广告软件应用具有并发运行并彼此监控的单独进程，确保修改是永久的。某些变体使得它们自己可以在每次计算机启动时自动运行。这些程序也可能更改安全设置，使得用户无法对其浏览器搜索选项、桌面和其他系统设置进行更改。
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供充分、明确且知情许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。

恶意软件类型	说明
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未提供充分、明确且知情许可的情况下，将用户引导至一个网站或运行一个程序。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
病毒爆发启发式扫描	此类别表示 Adaptive Scanning 独立于其他防恶意软件引擎发现的恶意软件。
网络钓鱼 URL	网络钓鱼 URL 显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。网络钓鱼是一种在线身份窃取形式，会使用社交工程和技术手段窃取个人身份数据和财务账户凭证。
PUA	可能不需要的应用。PUA 是非恶意应用，但可能被视为不想要的应用。
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： 公开地或隐蔽地记录系统进程和/或用户操作。 使这些记录可用于以后检索和审核。
特洛伊木马下载程序 (Trojan Downloader)	特洛伊木马下载程序是一种木马程序，在安装后，会与远程主机/站点联系，并安装来自远程主机的程序包或附属程序。这些安装通常会无需用户确认即可发生。此外，不同安装之间，特洛伊木马下载程序的有效载荷可能会不同，因为它是从远程主机/站点获取下载说明。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可能会扫描受感染的计算机来查找银行站点、拍卖站点或在线支付站点的用户名和口令。
病毒	病毒是未经您确认就加载到您的计算机上，并且违背您的意愿运行的程序或代码段。
蠕虫	蠕虫是一种程序或算法，会通过计算机网络进行自我复制，通常执行恶意操作。

高级恶意软件防护（文件信誉和文件分析）报告

• 关于 Web 跟踪和高级恶意软件防护功能 , on page 79

文件分析报告详细信息的要求

• （云文件分析）确保管理设备可以连接到文件分析服务器 , on page 21
• （云文件分析）配置管理设备以显示详细的文件分析结果 , on page 21
• （本地文件分析）激活文件分析账户 , on page 22
• 其它要求 , on page 22

（云文件分析）确保管理设备可以连接到文件分析服务器

要获取文件分析报告详细信息，设备必须能够通过端口 443 连接到文件分析服务器。请参阅防火墙资讯中的详细信息。

如果思科内容安全管理设备没有直接连接到互联网，请为此流量配置一个代理服务器（请参阅升级和更新设置。）如果已将设备配置为使用代理获取升级和服务更新，则会使用现有的设置。

如果您使用HTTPS代理，则代理不能将流量解密；请使用直通机制与文件分析服务器通信。代理服务器必须信任来自文件分析服务器的证书，但是不需要向文件分析服务器提供其自己的证书。

（云文件分析）配置管理设备以显示详细的文件分析结果

为了使组织中的所有内容安全设备都可以在云中显示有关从组织中的任何思科邮件安全设备或思科网络安全设备送交分析的文件的详细结果，您需要将所有设备加入到同一设备组。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 3 滚动至“文件分析”(File Analysis) 部分。

步骤 4 如果您管理的设备指向不同的文件分析云服务器，请选择从中显示结果详细信息的服务器。

将不提供由任何其他云服务器处理的文件的结果详细信息。

步骤 5 输入分析组 ID。

- 如果未正确输入组 ID 或出于任何其它原因需要对其进行更改，则必须向 Cisco TAC 提交请求。
- 此更改会立即生效；它不需要“确认”(Commit)。
- 建议将您的 CCOID 用于此值。
- 此值区分大小写。
- 在共享上传以供分析的文件的相关数据的所有设备上，此值必须是相同的。
- 一台设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。

步骤 6 点击**立即分组 (Group Now)**。

步骤 7 在将与此设备共享数据的每个网络安全设备上配置相同的组。

What to do next

相关主题

可以在云中查看哪些文件的详细文件分析结果？ , on page 24

（本地文件分析）激活文件分析账户

如果您已部署本地（私有云）的思科 AMP Threat Grid 设备，必须激活思科内容安全管理设备的文件分析账户，才能查看 Threat Grid 设备上提供的报告详细信息。您通常只需执行此操作一次。

Before you begin

确保您接收“严重”(Critical) 级别的系统警报。

步骤 1 首次尝试从 Threat Grid 设备访问文件分析报告详细信息时，请等待几分钟，然后您将收到包含一个链接的警报。

如果您没有收到此警报，请单击 图标加载旧 Web 界面，选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，然后单击**查看排名靠前的警报 (View Top Alerts)**。

步骤 2 单击警报消息中的链接。

步骤 3 如有必要，请登录到您的思科 AMP Threat Grid 设备。

步骤 4 激活您的管理设备账户。

其它要求

有关任何其他要求，请参阅安全管理设备版本的版本说明，位置：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，所有实例被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，文件按其 SHA-256 值列出（以缩写格式）。为了标识您的组织中与恶意软件实例相关联的文件名，请选择高级恶意软件保护 (Advanced Malware Protection) 报告页面，然后点击表格中的 SHA-256 链接。详细信息页面将显示了关联的文件名。

高级恶意软件防护（文件信誉和文件分析）报告页

报告	说明
高级恶意软件防护	显示由文件信誉服务识别的基于文件的威胁。 要查看尝试访问每个 SHA 的用户以及与该 SHA-256 关联的文件名，请单击表格中的 SHA-256。 单击“恶意软件威胁文件详细信息”(Malware Threat File Details) 报告页面底部的链接，会在网络跟踪中显示在最大可用时间范围内遇到的该文件的所有实例，不管为该报告选择什么时间范围都是如此。 有关判定已更改的文件，请参阅 AMP 判定更新报告。这些判定不会反映在“高级恶意软件防护”(Advanced Malware Protection) 报告中。 如果从某个已压缩或已存档的文件中提取的某个文件是恶意文件，则只有这个已压缩或已存档的文件的 SHA 值包括在“高级恶意软件防护”(Advanced Malware Protection) 报告中。 **按类别划分的恶意软件文件**部分显示从面向终端的 AMP 控制台所接收、归类为**自定义检测**且已列入阻止列表的文件 SHA 百分比 从面向终端的 AMP 控制台获取的已列入阻止列表的文件 SHA 百分比在报告的“恶意软件威胁文件”部分中显示为**简单自定义检测**。 要查看面向终端的 AMP 控制台中已列入阻止列表的文件 SHA 的文件轨迹详细信息，请执行以下步骤： **1.** 依次选择**报告 (Reporting)** > **高级恶意软件防护 (Advanced Malware Protection)**。 **2.** 单击要查看其轨迹详细信息的文件 SHA 链接。 **3.** 单击**更多详细信息 (More Details)** 部分中的 AMP 控制台链接。
文件分析 (File Analysis)	显示送交分析的每个文件的时间和判定（或临时判定）。设备每 30 分钟检查一次分析结果。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 对于采用现场思科 AMP Threat Grid 设备的部署：在思科 AMP Threat Grid 设备上包含在允许列表中的文件显示为“正常”(clean)。有关允许列表的信息，请参阅 AMP Threat Grid 联机帮助。 深入查看详细分析结果，包括威胁特征和每个文件的得分。 您还可以直接在执行分析的服务器上查看有关 SHA 目录的其他详细信息，方法是搜索 SHA 或单击文件分析详细信息页面底部的“思科 AMP Threat Grid”链接。 要在分析了文件的服务器上查看详细信息，请参阅文件分析报告详细信息的要求 , on page 21。 如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的 SHA 值包括在“文件分析”(File Analysis) 中。

报告	说明
AMP 判定更新 (AMP Verdict Updates)	列出由设备处理且在事务处理后已更改裁定的文件。有关此情况的详细信息，请参阅网络安全设备的相应文档。 要查看超过 1000 个裁定更新，请将数据导出为 .csv 文件。 如果单个 SHA-256 的判定多次发生变化，此报告仅显示最新的判定，而不显示判定历史记录。 如果多个网络安全设备对于同一文件具有不同的判定更新，则将显示具有最新时间戳的结果。 单击 SHA-256 链接会显示在最大可用时间范围内包括此 SHA-256 的所有事务的 Web 跟踪结果，不论为报告选择的是哪种时间范围。 要在最大可用时间范围内为特定 SHA-256 查看所有受影响的事务（不论为报告选择的是哪种时间范围），请单击“恶意软件威胁文件”(Malware Threat Files) 页面底部的链接

查看其他报告中的文件信誉过滤数据

用于文件信誉和分析的数据会在其他相关的报告中提供。默认情况下，设备报告中的“受高级恶意软件防护阻止”(Blocked by Advanced Malware Protection) 列处于隐藏状态。要显示其他列，请单击表格下方的“列“(Columns) 链接。

可以在云中查看哪些文件的详细文件分析结果？

如果您部署了公共云文件分析，则可以查看从已添加到文件分析设备组的任何受管设备上传的所有文件的详细结果。

如果您已将管理设备添加到该组，可以查看组中的受管设备列表，方法是依次单击**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页上的按钮。

分析组中的设备由文件分析客户端 ID 标识。要确定特定设备的此标识符，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 (Security Services > 文件信誉和分析 (File Reputation and Analysis)** 页面上的“文件分析的高级设置”(Advanced Settings for File Analysis) 部分。
网络安全设备	**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)** 页面上的“文件分析高级设置”(Advanced Settings for File Analysis) 部分。
思科内容安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

相关主题

（云文件分析）配置管理设备以显示详细的文件分析结果 , on page 21

客户端恶意软件风险报告

网络 (Web) > 报告 (Reporting) > 客户端恶意软件风险 (Client Malware Risk) 页面是一个安全相关报告页面，可用于监控客户端恶意软件风险活动。

在“客户端恶意软件风险”(Client Malware Risk) 页面，系统管理员可以查看哪些用户遇到了最多的阻止或警告。根据从此页面收集的信息，管理员可以点击用户链接，查看此用户在网络上执行了哪些操作导致受到如此多的阻止或警告，引发比网络上其他用户更多的检测。

此外，“客户端恶意软件风险”(Client Malware Risk) 页面还列出了常见恶意软件连接涉及的客户端 IP 地址，如第 4 层流量监控器 (L4TM) 所标识。经常连接到恶意站点的计算机可能感染了尝试连接到中央命令和控制服务器的恶意软件，应进行杀毒。

下表介绍有关“客户端恶意软件风险”页的信息。

Table 9: 客户端恶意软件风险报告组件

部分	说明
时间范围 (Time Range) （下拉列表）	该菜单允许您选择报告中所包含数据的时间范围。有关详细信息，请参阅选择报告的时间范围。
网络代理：排名靠前的受监控或阻止的客户端 (Web Proxy: Top Clients Monitored or Blocked)	此图表显示遇到恶意软件风险的排名前十的用户。
第 4 层流量监控器：检测到的恶意软件连接 (L4 Traffic Monitor: Malware Connections Detected)	此图表显示您的组织中最常连接到恶意站点的排名前十的计算机的 IP 地址。 此图表与L4 流量监控器报告 , on page 28上的“排名靠前的客户端 IP”图表相同。有关图表选项的更多信息，请参阅上述提及的部分。
网络代理：客户端恶意软件风险 (Web Proxy: Client Malware Risk)	网络代理：“客户端恶意软件风险”(Client Malware Risk) 表显示在“网络代理：按恶意软件风险排名靠前的客户端”部分中显示的特定客户端的详细信息。 您可以在此表中点击每个用户，以查看与该客户端相关联的“用户详细信息”(User Details) 页。有关该页的信息，请参阅用户详细信息（Web 报告） , on page 11。 点击该表中的任意链接，您可以更为精细地查看各个用户以及他们正在执行的哪些活动触发了恶意软件风险的详细信息。例如，点击“用户 ID/客户端 IP 地址”(User ID / Client IP Address) 列中的链接会将您带到该用户的“用户”(User) 页。

部分	说明
第 4 层流量监控器：按恶意软件风险排名的客户端 (L4 Traffic Monitor: Clients by Malware Risk)	此表显示您的组织中最常连接到恶意站点的计算机的IP地址。 该表与L4 流量监控器报告 , on page 28上的“客户端源IP”(Client Source IPs) 表相同。有关使用此表用的信息，请参阅此部分。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

网络信誉过滤器报告

网络 (Web) > 报告 (Reporting) > 网络信誉过滤器 (Web Reputation Filters) 可用于查看在指定的时间范围内为事务设置的网络信誉过滤器的结果。

什么是网络信誉过滤？

网络信誉过滤用于分析网络服务器行为并为 URL 分配一个信誉得分，从而确定其包含基于 URL 的恶意软件的可能性。它有助于防御会威胁最终用户隐私和敏感公司信息的基于URL的恶意软件。网络安全设备使用URL信誉分数来识别可疑活动并提前阻止恶意软件攻击，避免其发生。您可以使用同时具有访问和解密策略的网络信誉过滤。

网络信誉过滤器使用统计数据评估互联网域可靠性并对URL信誉进行评分。许多数据可用于判断给定URL的可信度，例如，特定域的注册时长，或网站的托管位置，或者网络服务器是否使用动态IP地址等。

网络信誉计算将URL与网络参数相关联，用于确定恶意软件存在的可能性。然后得出的恶意软件存在的综合可能性会映射为一个 -10 到 +10 之间的网络信誉分数，+10 为最不可能包含恶意软件。

示例参数包括：

- URL 类别数据
- 存在的可下载代码
- 存在的冗长且含混的最终用户许可协议 (EULA)
- 全局量和量的变化
- 网络所有者信息
- URL 的历史记录
- URL 的时长
- 是否存在于任何阻止列表上
- 是否存在于任何允许列表上
- 常用域的 URL 拼写错误
- 域注册商信息
- IP 地址信息

有关网络信誉过滤的详细信息，请参阅《网络 IronPort AsyncOS 用户指南》中的“网络信誉过滤器”。

在**网络信誉过滤器**页面中，您可以查看以下信息：

Table 10: *“Web 报告网络信誉过滤器”页面上的详细信息*

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
网络信誉操作（趋势）(Web Reputation Actions [Trend])	本部分以图的形式显示在指定的时间（水平）内网络信誉操作总数（垂直）。在这里，您可以看到随着时间推移网络信誉操作的潜在趋势。
网络信誉操作（容量）(Web Reputation Actions [Volume])	本部分按事务显示网络信誉操作量（以百分比表示）。
已由 WBRS 阻止的网络信誉威胁类型 (Web Reputation Threat Types Blocked by WBRS)	本部分显示事务中发现的已由网络信誉过滤阻止的威胁类型。 注：WBRS 不能始终识别出威胁类型。
在其他事务中检测到的威胁类型 (Threat Types Detected in Other Transactions)	本部分显示事务中发现的未由网络信誉过滤阻止的威胁类型。 这些威胁未被阻止的可能原因包括： • 并非所有威胁的得分均达到阻止阈值。但是，设备的其他功能可以捕获这些威胁。 • 可策略以允许配置威胁通过。 注：WBRS 不能始终识别出威胁类型。
Web 信誉操作（按分数分解）	如果未启用自适应扫描功能，此交互式表格会显示针对每项操作细分的网络信誉分数。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

“调整网络信誉设置”(Adjusting Web Reputation Settings)

基于您的报告结果，您可能希望调整已配置的网络信誉设置，例如调整阈值得分，或启用或禁用 Adaptive Scanning。有关配置网络信誉设置的具体信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

L4 流量监控器报告

网络 (Web) > 报告 (Reporting) > L4 流量监控器 (L4 Traffic Monitor) 页面会显示有关上网络安全设备的L4流量监控器在指定的时间范围内检测到的恶意软件端口和恶意软件站点的信息。它还会显示经常遇到恶意软件站点的客户端的 IP 地址。

L4 流量监视器会监听通过每个网络安全设备上的所有端口传入的网络流量,并且将域名称和 IP 地址与其自己的数据库表中的条目进行匹配，以确定是否允许传入和传出流量。

可以使用此报告中的数据来确定是阻止端口或站点，还是调查某个特定客户端 IP 地址反常地频繁连接到恶意软件站点的原因（例如，这可能是因为与该 IP 地址关联的计算机感染了尝试连接到一台集中命令和控制服务器的恶意软件）。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

***Table 11: L4* 流量监控器报告页组件**

部分	说明
时间范围 (Time Range)（下拉列表）	该菜单允许您选择要报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
“排名靠前的客户端 IP”(Top Client IPs)	本部分以图的形式显示您的组织中最常连接到恶意站点的计算机的IP地址。 点击图表下面的“图表选项”(Chart Options) 链接可以将显示从“检测到的恶意软件连接”(Malware Connections Detected) 总数更改为“监控到的恶意软件连接”(Malware Connections Monitored) 或“已阻止的恶意软件连接”(Malware Connections Blocked)。 此图表与客户端恶意软件风险报告 , on page 25上的“第 4 层流量监控器检测到的恶意连接”图表相同。
恶意软件最多的网站 (Top Malware Sites)	本部分以图的形式显示第4层流量监控器检测的排名靠前的恶意软件域名。 点击图表下面的“图表选项”(Chart Options) 链接可以将显示从“检测到的恶意软件连接”(Malware Connections Detected) 总数更改为“监控到的恶意软件连接”(Malware Connections Monitored) 或“已阻止的恶意软件连接”(Malware Connections Blocked)。

部分	说明
客户端源 IP (Client Source IPs)	本表显示您的组织中经常连接到恶意站点的计算机的 IP 地址。 要仅包括特定端口的数据，请在表底部的框中输入端口号，并点击“按端口过滤”(Filter by Port)。您可以使用此功能帮助确定那些将恶意软件站点“称为家”的恶意软件使用哪些端口。 要查看诸如每个连接的端口和目标域的详细信息，请点击表中的条目。例如，如果特定客户端 IP 地址具有大量已受阻止的恶意软件连接，请点击该列中的数字，查看每个受阻止连接的列表。该列表显示为“网络”(Web) >“报告”(Reporting) >“Web 跟踪”(Web Tracking) 页面中“第 4 层流量监控器”(L4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 , on page 72。 该表与客户端恶意软件风险报告 , on page 25上的“第 4 层流量监控器 - 按恶意软件风险排名的客户端”(L4 Traffic Monitor - Clients by Malware Risk) 表相同。
恶意软件端口 (Malware Ports)	此表显示第 4 层流量监控器最常检测到恶意软件的端口。 要查看详细信息，请点击表中的某个条目。例如，点击“检测到的恶意软件连接总数”(Total Malware Connections Detected) 可以查看该端口上每个连接的详细信息。该列表显示为“网络”(Web) >“报告”(Reporting) >“Web 跟踪”(Web Tracking) 页面中“第 4 层流量监控器”(L4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 , on page 72。
检测到的恶意软件站点数 (Malware Sites Detected)	此表显示第 4 层流量监控器最常检测到恶意软件的域。 要仅包括特定端口的数据，请在表底部的框中输入端口号，并点击“按端口过滤”(Filter by Port)。您可以使用此功能帮助确定是否阻止某个站点或端口。 要查看详细信息，请点击表中的某个条目。例如，点击“受阻止的恶意软件连接”(Malware Connections Blocked) 的数字可以查看特定站点的每个已阻止连接的列表。该列表显示为“网络”(Web) >“报告”(Reporting) >“Web 跟踪”(Web Tracking) 页面中“第 4 层流量监控器”(L4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 , on page 72。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

相关主题

- 解决第 4 层流量监控器报告问题 , on page 82

SOCKS 代理报告

网络 (Web) > 报告 (Reporting) > SOCKS 代理 (SOCKS Proxy) 页面允许您查看那些通过 SOCKS 代理处理的事务的数据和趋势，包括目标和用户的信息。

Note 报告中显示的目标是 SOCKS 客户端（通常是浏览器）发送到 SOCKS 代理的地址。

要更改 SOCKS 策略设置，请参阅思科网络安全设备 AsyncOS 用户指南。

相关主题

- 搜索 SOCKS 代理处理的事务 , on page 72

按用户地点分类的报告

网络 (Web) > 报告 (Reporting) > 按用户地点分类的报告 (Reports by User Location) 页面允许您查看您的移动用户正在其本地或远程系统上执行哪些活动。

具体活动包括：

- 本地和远程用户正访问的 URL 类别。
- 由本地和远程用户正访问的站点触发的防恶意软件活动。
- 本地和远程用户正访问的站点的网络信誉。
- 本地和远程用户正访问的应用。
- 用户（本地和远程）。
- 本地和远程用户访问的域。

从**按用户位置报告**页面，可查看下列信息：

Table 12: *“按用户位置 Web 报告” (Web Reporting Reports by User Location)* 页面的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
网络代理活动总数：远程用户 (Total Web Proxy Activity: Remote Users)	本部分以图的形式显示在指定时间内（水平）您的远程用户的活动（垂直）。
网络代理摘要 (Web Proxy Summary)	本部分显示您的系统上的本地和远程用户的活动的摘要。
网络代理活动总数：本地用户 (Total Web Proxy Activity: Local Users)	本部分以图的形式显示在指定时间内（水平）您的远程用户的活动（垂直）。
检测到的可疑事务数：远程用户 (Suspect Transactions Detected: Remote Users)	本部分以图的形式显示在指定的时间内（水平）由于为您的本地用户定义的访问策略而检测到的可疑事务（垂直）。

部分	说明
可疑事务摘要 (Suspect Transactions Summary)	本部分显示您的系统上的远程用户的可疑事务摘要。
检测到的可疑事务数：本地用户 (Suspect Transactions Detected: Local Users)	本部分以图的形式显示在指定的时间内（水平）由于为您的本地用户定义的访问策略而检测到的可疑事务（垂直）。
可疑事务摘要 (Suspect Transactions Summary)	本部分显示您的系统上的本地用户的可疑事务摘要。

在**按用户地点分类的报告 (Reports by User Location)** 页面中，可以生成显示本地和远程用户活动的报告。这允许您方便地比较您的用户的本地和远程活动。

Tip 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

Note 您可以为“按用户位置报告”(Reports by User Location) 页面上的信息生成一个已安排报告。有关安排报告的信息，请参阅关于计划的报告和按需 Web 报告, on page 58。

“系统容量”(System Capacity) 页面

通过**网络 (Web) > 报告 (Reporting) > 系统容量 (System Capacity)** 页面，可以查看网络安全设备在安全管理设备上施加的总体工作负载。最重要的是，您可以使用“系统容量”(System Capacity) 页面来跟踪随着时间的发展情况并针对系统容量进行规划。监控您的网络安全设备确保容量适合您的用量。邮件量将随着时间不可避免地增加；适当的监控可确保主动应用额外的容量或配置更改。

“系统容量”(System Capacity) 页面可用于确定以下信息：

- 发现网络安全设备何时超出了建议的 CPU 容量；这使得您可以确定何时需要配置优化或其他设备。
- 要进行故障排除，需确定系统的哪些部分使用大多数资源。
- 识别响应时间和代理缓冲内存。
- 识别每秒的事务数和未完成的任意连接。

查看系统容量报告

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 系统容量 (System Capacity)**。

步骤 2 要查看不同类型的数据，请单击**列 (Columns)** 并选择要查看的数据。

步骤 3 要查看单个设备的系统容量，请单击“平均使用和性能概述 (Overview of Averaged Usage and Performance)”表格中网络安全设备列中的设备。

将显示该设备的系统容量图。页面上的图会划分为两个部分：

- 系统容量 - 系统负载 , on page 32

• 系统容量 - 网络负载 , on page 32

如何解释您在“系统容量”(System Capacity) 页面上看到的数据

当选择时间范围来查看“系统容量”(System Capacity) 页面上的数据时，记住以下内容非常重要：

- 日报告 (Day Report) - 日报告查询小时表并显示设备在 24 小时内每小时收到的准确查询数量。此信息收集自小时表。
- 月报告 - 月报告查询 30 或 31 天（取决于该月份的实际天数）的日表，为您提供 30 或 31 天内查询数量的确切报告。再次重申，这是一个精确的数字。

“系统容量”(System Capacity) 页面上的“最大值”(Maximum) 值指示符是在指定时间段内看到的最高值。“平均值”(Average) 值是指定时间段内所有值的平均值。汇聚的时间取决于为该报告选择的时间间隔。例如，如果图表表示某个月时间段，您可以选择查看每天的“平均值”(Average) 和“最大值”(Maximum) 值。

Note 如果为其他报告的时间范围选择**是 (Yes)**，我们建议选择最大的时间范围，即 90 天。

系统容量 - 系统负载

“系统容量”(System Capacity) 窗口的前四个图形显示系统负载报告。这些报告显示设备上的整体 CPU 使用情况。AsyncOS 优化为使用空闲 CPU 资源提高事务吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高CPU使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。该页面还显示一个图，其中显示了不同功能使用的 CPU 量，包括网络安全设备报告的处理。按功能显示的CPU图表可指示产品的哪些部分占用系统上的大多数资源。如果需要优化设备，则此图形可以帮助确定哪些功能可能需要调整或禁用。

此外，“响应时间/延迟”(Response Time/Latency) 和“每秒事务数”(Transactions Per Second) 图显示“时间范围”(Time Range) 下拉菜单中指定的日期范围内的整体响应时间（毫秒）以及每秒事务数。

系统容量 - 网络负载

“系统容量”(System Capacity) 窗口的下个图显示传出连接、使用的带宽和代理缓冲区内存统计信息。您可以查看一天、一周、一月或一年的结果。了解环境中的正常量和激增量的趋势很重要。

代理缓冲区内存可能会指示正常操作期间的网络流量的激增，但是如果图形稳定地攀爬至最大值，则设备可能达到其最大容量，则您就考虑增加容量。

下面这些图表与系统容量 - 系统负载 , on page 32中介绍的图表相同。

有关代理缓冲内存交换的说明

系统设计为定期交换代理缓冲区内存，因此，某些代理缓冲区内存交换是在预期中，并不表示您的设备存在问题。除非系统持续大量交换代理缓冲内存，否则代理缓冲内存交换是正常的预期行为。

如果系统运行极高的负载量且由于高负载量而持续交换代理缓冲内存，则可能需要将网络安全设备添加到网络或调整配置以确保最大吞吐量，从而提高性能。

“数据可用性”(Data Availability) 页面

网络 (Web) > 报告 (Reporting) > 数据可用性 (Data Availability) 页面提供有关每个受管网络安全设备的安全管理设备上具有可用报告和 Web 跟踪数据的日期范围。

Note 如果禁用了 Web 报告，则不会从网络安全设备提取任何新数据，但是以前检索的数据仍存在于安全管理设备中。

如果 Web 报告的“从 (From)”和“到 (To)”列与 Web 报告和跟踪的“从 (From)”和“到 (To)”列之间具有不同的状态，则“状态 (Status)”列中会显示最严重的后果。

有关清除数据的信息，请参阅管理磁盘空间。

Note 如果在计划报告内为 URL 类别使用“数据可用性”(Data Availability)，并且在任意设备之间存在着数据差异，则会在页面底部显示以下信息：“Some data in this time range was unavailable”。如果没有数据差异，则不会显示任何内容。

了解新 Web 界面上的“Web 报告”(Web Reporting) 页面

下表列出了 Web 界面**报告**下拉列表中网络安全设备的 AsyncOS 最新支持版本中可用的报告。有关详细信息，请参阅使用交互式报告页面。如果您的网络安全设备运行的是早期版本的 AsyncOS，并非上述所有报告均可用。

表 *13: Web* 报告下拉选项

报告下拉选项	操作
一般报告	
“概述”(Overview) 页面	“概述”(Overview) 页面提供您的网络安全设备上的活动的概要。它包括传入和传出事务的图和摘要表。有关详细信息，请参阅“概述”(Overview) 页面，第 35 页。
“应用可视性”(Application Visibility) 页面	通过“应用可视性”(Application Visibility) 页面，可以应用和查看已用于安全管理设备和网络安全设备中特定应用类型的控件。有关详细信息，请参阅“应用可视性”(Application Visibility) 页面，第 37 页。

报告下拉选项	操作
“第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面	允许您查看在指定时间范围内第 4 层流量监控器检测到的恶意软件端口和恶意站点的信息。有关详细信息，请参阅“第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面，第 38 页。
“SOCKS 代理”(SOCKS Proxy) 页面	允许您查看 SOCKS 代理事务的数据，包括目标和用户。有关详细信息，请参阅“SOCKS 代理”(SOCKS Proxy) 页面，第 41 页。
“URL 类别”(URL Categories) 页面	利用“URL 类别”(URL Categories) 页面可以查看所访问的排名靠前的 URL 类别，包括： • 按事务触发阻止或警告操作的排名靠前的 URL。 • 在指定时间范围内，已完成、已警告和已阻止的事务对应的所有 URL 类别。这是一个交互表，具有交互列标题，您可以使用该列标题按需排序数据。 有关详细信息，请参阅“URL 类别”(URL Categories) 页面，第 42 页。
“用户”(User) 页面	“用户”(Users) 页面提供多个 Web 跟踪链接，允许您查看各个用户的 Web 跟踪信息。 从用户 (Users) 页面中，可以查看系统上的一个或多个用户在互联网、特定站点或 URL 上花费的时间，以及用户使用多少带宽。 从“用户”(Users) 页面中，可以点击交互式用户表格中的单个用户，以在“用户详细信息”(User Details) 页面上查看该特定用户的更多详细信息。 通过“用户详细信息”(User Details) 页面，可以查看关于在“用户”(Users) 页面的“用户”(Users) 表格中识别的用户的特定信息。从该页面您可以深入研究系统上各个用户的活动。如果您正在运行用户级调查，并且需要查找诸如用户正在访问哪些站点、他们遇到了哪些恶意软件威胁、正在访问哪些URL类别，以及特定用户在这些站点上花费了多少时间等信息，则此页面将非常有用。 有关详细信息，请参阅“用户”(User) 页面，第 45 页。 有关您的系统中特定用户的信息，请参阅“用户详细信息”页面（Web 报告），第 46 页。
“网站”(Web Sites) 页面	“网站”(Web Sites) 页面允许您查看托管设备上所发生的活动的汇聚情况。从该页面您可以监控特定时间范围内访问的高风险网站。有关详细信息，请参阅“网站”(Web Sites) 页面，第 48 页。

报告下拉选项	操作
HTTPS 报告	“HTTPS 报告”报告页面是托管设备上 HTTP/HTTPS 流量摘要（事务或带宽使用情况）的整体汇聚。有关详细信息，请参阅“HTTPS 报告”页面，第 49 页。
威胁报告	
“防恶意软件”(Anti-Malware) 页面	“防恶意软件”(Anti-Malware) 页面允许您查看在指定时间范围内防恶意软件扫描引擎检测到的恶意软件端口和恶意站点的信息。报告的上半部分显示每个排名靠前的恶意软件端口和网站的连接数量。报告的下半部分显示检测到的恶意软件端口和网站。有关详细信息，请参阅“防恶意软件”(Anti-Malware) 页面，第 50 页。
“客户端恶意软件风险”(Client Malware Risk) 页面	“客户端恶意软件风险”(Client Malware Risk) 页面是一个安全相关的报告页面，可以用于确定那些正异常频繁地连接到恶意软件站点的各个客户端计算机。 有关详细信息，请参阅客户端恶意软件风险报告，第 55 页。
网络信誉过滤器 (Web Reputation Filters) 页面	允许您查看指定时间范围内事务的网络信誉过滤报告。有关详细信息，请参阅网络信誉过滤器 (Web Reputation Filters) 页面，第 56 页。

关于“所花费时间”(Time Spent)

各个表中“所花费时间”(Time Spent) 列表示用户在某个网页上所花费的时间。用户在每个 URL 类别上所花费的时间（为了用户调查）。当跟踪 URL 时，每个用户在该特定 URL 上所花费的时间。

一旦事务事件被标记“已查看”(viewed)，即用户访问特定 URL，将会开始计算一个“所花费时间”(Time Spent) 值，并将其添加为 Web 报告表中的一个字段。

为计算所花费时间，AsyncOS 针对一分钟期间内的活动为每个活动用户分配 60 秒时间。在这一分钟结束时，在用户访问的不同域之间将会均分每个用户所花费的时间。例如，如果用户在一个活动分钟内访问四个不同的域，则会认为该用户在每个域花费 15 秒。

对于所花费时间值，请注意以下事项：

- 活动用户定义为通过设备发送 HTTP 流量并访问 AsyncOS 视为一次“页面阅览”的网站的用户名或 IP 地址。
- AsyncOS 会将页面阅览定义为用户发起的 HTTP 请求，与客户端应用发起的请求相对。AsyncOS 使用启发式算法进行最佳猜测，以确定用户页面阅览量。

单位以小时：分钟格式显示。

“概述”(Overview) 页面

概述报告页面提供网络安全设备上的活动概要。它包括传入和传出事务的图和摘要表。

要查看“概述”(Overview) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 概述 (Overview)**。有关详细信息，请参阅使用交互式报告页面。

概述报告页面概括地显示有关URL和用户使用、网络代理活动以及各种事务摘要的统计数据。事务摘要为诸如可疑事务等内容提供进一步的趋势详细信息，并且直接从此图中可以了解阻止了多少上述可疑事务，以及阻止的方式。

“概述”报告页面的下半部分介绍使用情况。也就是查看的排名靠前的URL类别、排名靠前的应用类型以及被阻止的类别，生成这些阻止或警告的排名靠前的用户。

表 *14*:“概述”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其概述数据的网络安全设备，或选择所有网络设备。 另请参阅查看设备或报告组的报告数据
Web 代理活动总数	您可以查看当前由安全管理设备管理的网络安全设备报告的网络代理活动。 此部分以图形格式显示实际事务数以及发生活动的大约日期。 您还可以查看可疑或正常的网络代理活动的百分比，包括事务总数。
可疑事务数	以图形格式查看被管理员标记为可疑事务的网络事务。 此部分以图形格式显示实际事务数以及发生活动的大约日期。 您也可以查看已阻止或警告的可疑事务的百分比。另外，您可以查看已被检测和阻止的事务的类型，以及此事务被阻止的实际次数。
L4 流量监控器摘要	您可以以图形格式查看当前由安全管理设备管理的网络安全设备所报告的任何 L4 流量。
排名靠前的 URL 类别：按事务总数排列	您可以以图形格式查看被阻止的排名靠前的 URL 类别，包括 URL 类别的类型以及已阻止的特定类型类别的实际次数。 预定义的URL类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 ， 第 15 页。
排名靠前的应用类型：按事务总数排列	您可以以图形格式查看被阻止的排名靠前的应用类型，包括实际应用类型的名称和已阻止的特定应用的次数。

部分	说明
排名靠前的恶意软件类别：受监控或受阻止	您可以以图形格式查看已检测到的所有恶意软件类别。
排名靠前的用户：按受阻或警告的事务数排列	您可以以图形格式查看生成阻止或警告的事务的实际用户。可以按 IP 地址或按用户名称来显示用户。要使用户名无法识别，请参阅在 Web 报告中让用户名保持匿名 ，第 4 页。

“应用可视性”(Application Visibility) 页面

注释 有关应用可视性的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》的“了解应用可视性与可控性”一章。

通过**应用可视性**报告页面，可以将控制应用于安全管理设备和网络安全设备中的特定应用类型。

要查看“应用可视性”(Application Visibility) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 应用可视性 (Application Visibility)**。有关详细信息，请参阅使用交互式报告页面。

应用控制不仅可以为您提供比只使用URL过滤更为精细的网络流量控制，同时它会为您提供对诸如以下应用类型的更多控制：

- 规避应用，例如匿名程序和加密隧道。
- 协作应用，例如 Cisco Webex、Facebook 和即时消息。
- 资源密集型应用，例如流媒体。

了解应用与应用类型之间的差异

了解应用和应用类型之间的差异以便可以控制报告涉及的应用，这一点至关重要。

- **应用类型**。包含一个或多个应用的类别。例如，搜索引擎是可包含搜索引擎（例如Google Search 和 Craigslist）的应用类型。即时消息是另一种应用类型类别，可能包含 Yahoo Instant Messenger 或 Cisco Webex。Facebook 也是一种应用类型。
- **应用**。属于某一应用类型的特定应用。例如，YouTube 是一种媒体 (Media) 应用类型的应用。
- **应用行为**。用户可以在应用中完成的特定操作或行为。例如，用户可以在使用某种应用（例如 Yahoo Messenger）时传输文件。并非所有应用均包括您可以配置的应用行为。

注释 有关了解如何使用应用可视性与可控性 (AVC) 引擎以控制 Facebook 活动的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》中的“了解应用可视性与可控性”一章。

在“应用可视性”(Application Visibility) 页面，您可以查看以下信息：

表 *15:*“应用可视性”*(Application Visibility)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)	以图形格式查看在站点上访问的排名靠前的应用类型。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。 例如，像 Instant Messenger 这样的即时聊天工具、Facebook 和演示应用类型。
按受阻事务数排名靠前的应用 (Top Applications by Blocked Transactions)	以图形格式查看根据事务触发阻止操作的排名靠前的应用类型。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。 例如，用户尝试启动某个应用类型，例如 Google Talk 或 Yahoo Instant Messenger，由于特定策略已就位，这触发了阻止操作。然后此应用会作为受阻止的事务或警告在图中列出。
匹配的应用类型 (Application Types Matched)	“匹配的应用类型”(Application Types Matched) 交互表允许您查看“按事务总数排名靠前的应用类型”(Top Applications Type by Total Transactions) 表中列出的应用类型。 在“应用”列，您可以点击某个应用以查看详细信息。
匹配的应用 (Applications Matched)	“匹配的应用”交互式表显示在指定时间范围内的所有应用。 此外，您可以在匹配的应用 (Applications Matched) 部分查找特定应用。在该部分底部的文本字段中，输入特定应用名称，并点击查找应用 (Find Application)。

注释 要自定义此报告的视图，请参阅与网络安全报告一起使用 ，第 5 页。

“第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面

第 4 层流量监控器报告页面显示有关网络安全设备上的第 4 层流量监控器在指定的时间范围内检测到的恶意软件端口和恶意软件站点的信息。它还显示经常遇到恶意站点的客户端的 IP 地址。

要查看“网站”(Web Sites) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 网站 (Web Sites)**。有关详细信息，请参阅使用交互式报告页面。

第 4 层流量监控器会侦听通过每个网络安全设备上的所有端口传入的网络流量，并且将域名称和 IP 地址与其自己的数据库表中的条目进行匹配，以确定是否允许传入和传出流量。

您可以使用此报告中的数据来决定是否阻止某个端口或站点，或研究某个特定客户端 IP 地址异常频繁地连接到恶意站点的原因（例如，这可能是因为与该 IP 地址相关联的计算机尝试连接到一台集中命令和控制服务器）。

表 *16:*“第 *4* 层流量监控器”*(Layer 4 Traffic Monitor)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
排名靠前的客户端 IP：按检测到的恶意软件连接数排列	以图形格式查看您的组织中最频繁连接到恶意软件站点的计算机的 IP 地址。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。 此图表与客户端恶意软件风险报告 ， 第 55 页上的“第 4 层流量监控器：检测到的恶意软件连接”图表相同。
排名靠前的恶意软件站点：按检测到的恶意软件连接数排列	以图形格式查看第 4 层流量监控器检测到的排名靠前的恶意软件域。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。

部分	说明
客户端源 IP (Client Source IPs)	可以使用本交互式表查看您的组织中频繁连接到恶意软件站点的计算机的 IP 地址。 要仅包括特定端口的数据，请在表底部的框中输入端口号，并点击“按客户端 IP 过滤”(Filter by Client IP)。您可以使用此功能帮助确定那些将恶意软件站点“称为家”的恶意软件使用哪些端口。 要查看诸如每个连接的端口和目标域的详细信息，请点击表中的条目。例如，如果特定客户端IP地址具有大量已受阻止的恶意软件连接，请点击该列中的数字，查看每个受阻止连接的列表。该列表显示为“Web 跟踪搜索”(Web Tracking Search) 页面中“第 4 层流量监控器”(Layer 4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 ，第 72 页。 此图表与客户端恶意软件风险报告 ，第 55 页上的“第 4 层流量监控器：检测到的恶意软件连接”图表相同。
恶意软件端口 (Malware Ports)	可以使用本交互式表查看第 4 层流量监控器最常检测到恶意软件的端口。 要查看详细信息，请点击表中的某个条目。例如，点击“检测到的恶意软件连接总数”(Total Malware Connections Detected) 可以查看该端口上每个连接的详细信息。该列表显示为“Web 跟踪搜索”(Web Tracking Search) 页面中“第 4 层流量监控器”(Layer 4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 ，第 72 页。
检测到的恶意软件站点数 (Malware Sites Detected)	可以使用本交互式表查看第 4 层流量监控器最常检测到恶意软件的域。 要仅包括特定端口的数据，请在表底部的框中输入端口号，并点击“按端口过滤”(Filter by Port)。您可以使用此功能帮助确定是否阻止某个站点或端口。 要查看详细信息，请点击表中的某个条目。例如，点击“受阻止的恶意软件连接”(Malware Connections Blocked) 的数字可以查看特定站点的每个已阻止连接的列表。该列表显示为“Web 跟踪搜索”(Web Tracking Search) 页面中“第 4 层流量监控器”(Layer 4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 ，第 72 页。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 ，第 5 页。

相关主题

解决第 4 层流量监控器报告问题 ，第 82 页

“SOCKS 代理”(SOCKS Proxy) 页面

通过“SOCKS 代理”报告页面，可以以图形和表格格式查看通过 SOCKS 代理处理的事务，其中包括目标和用户的相关信息。

要查看“SOCKS 代理”(SOCKS Proxy) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > SOCKS 代理 (SOCKS Proxy)**。有关详细信息，请参阅使用交互式报告页面。

注释 报告中显示的目标是 SOCKS 客户端（通常是浏览器）发送到 SOCKS 代理的地址。

要更改 SOCKS 策略设置，请参阅《思科网络安全设备 *AsyncOS* 用户指南》。

表 *17:* “*SOCKS* 代理”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
排名靠前的 SOCKS 目标：按事务总数排列	以图形格式查看 SOCKS 代理检测到的排名靠前的目标。 要自定义图表视图，请单击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
排名靠前的 SOCKS 用户：恶意软件事务	以图形格式查看 SOCKS 代理检测到的排名靠前的用户。 要自定义图表视图，请单击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
目的	您可以使用本交互式表查看通过 SOCKS 代理处理的目的域或 IP 地址的列表。 要仅包含特定目的的数据，请在表底部的框中输入域名或 IP 地址，然后单击**查找域或 IP (Find Domain or IP)**。

部分	说明
用户	您可以使用本交互式表查看通过 SOCKS 代理处理的用户或 IP 地址的列表。 要仅包含特定用户的数据，请在表底部的框中输入用户名或IP地址，然后单击**查找用户 ID/客户端 IP 地址 (Find User ID / Client IP Address)**。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 ，第 5 页。

相关主题

搜索 SOCKS 代理处理的事务 ，第 72 页

“URL 类别”(URL Categories) 页面

URL 类别报告页面可用于查看系统中的用户正在访问的站点的 URL 类别。

要查看“URL 类别”(URL Categories) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > URL 类别 (URL Categories)**。有关详细信息，请参阅使用交互式报告页面。

在“URL 类别”(URL Categories) 页面中，您可以查看以下信息：

表 *18: “URL 类别”(URL Categories)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
排名靠前的 URL 类别：按事务总数排列	以图形格式查看在站点上访问的排名靠前的 URL 类别。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
排名靠前的 URL 类别：按受阻和警告事务数排列	以图形格式查看按事务触发阻止或警告操作的排名靠前的 URL。例如，用户访问了某特定 URL，并且由于布置了一个特定策略，这触发了阻止操作或警告。然后此 URL 会作为受阻止的事务或警告在图中列出。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。

部分	说明
排名靠前的 Youtube 类别：按事务总数排列	以图形格式查看在站点上访问的排名靠前的 Youtube 类别。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
排名靠前的 Youtube 类别：按受阻止和警告事务数排列	以图形格式查看按事务触发阻止或警告操作的排名靠前的 Youtube URL。例如，用户访问了某特定 Youtube URL，并且由于布置了一个特定策略，这触发了阻止操作或警告。然后此 Youtube URL 会作为受阻止的事务或警告在图中列出。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
匹配的 URL 类别 (URL Categories Matched)	“匹配的 URL 类别”交互式表按 URL 类别显示指定时间范围内的事务处理，以及每个类别中使用的带宽和花费的时间。 如果有大量未分类的 URL，请参阅减少未分类的 URL ，第 15 页。
匹配的 Youtube 类别	“匹配的 Youtube 类别”交互式表按 Youtube 类别显示指定时间范围内的事务处理，以及每个类别中使用的带宽和花费的时间。 要查看匹配的 Youtube 类别交互式表，请选择**网络 (Web)** > **报告 (Reporting)** > **URL 类别 (URL Categories)**。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 ，第 5 页。

减少未分类的 URL

如果未分类的 URL 的百分比高于 15-20%，请考虑以下选项：

- 对于特定的本地化 URL，您可以创建自定义 URL 类别，并将其应用到特定用户或组策略。这些事务将改为包括在“被绕过的 URL 过滤”(URL Filtering Bypassed) 统计信息内。为此，请参阅有关适用于思科网络安全设备的 AsyncOS 用户指南的自定义 URL 类别的信息。
- 对于您认为应包括在现有或其他类别的站点，请参阅报告错误分类和未分类的 URL , on page 16。

URL 类别集更新和报告

预定义的 URL 类别集可能会在安全管理设备上定期更新，如准备和管理 URL 类别集更新中所述。

当发生这些更新时，旧类别的数据将继续显示在报告和 Web 跟踪结果中，直到数据因太旧而无法包括在其中。在类别集更新后生成的报告数据将使用新的类别，因此，您在同一报告中可以同时看到旧类别和新类别。

如果新旧类别的内容之间有重叠，则您可能需要仔细检查报告结果以获取有效的统计信息。例如，如果在所查看的时间段内“即时消息”和“基于网络的聊天”类别已合并到单个“聊天和即时消息”类别，则在合并之前对“即时消息”和“基于网络的聊天”类别中涵盖的站点进行的访问不会计入“聊天和即时消息”的总计中。类似地，在合并后对即时消息或基于网络的聊天站点的访问将会包括在“即时消息”(Instant Messaging) 或“基于网络的聊天”(Web-based Chat) 类别内。

将“URL 类别”页面与其他报告页面结合使用

“URL 类别”(URL Categories) 页面可以与“应用可视性”(Application Visibility) 页面, on page 37和“用户”(User) 页面, on page 45配合使用，以调查特定用户以及该特定用户尝试访问的应用或网站的类型。

例如，在“URL 类别”(URL Categories) 页面, on page 42中可以为人力资源部门生成高级别报告，其中详细说明站点访问的所有 URL 类别。在同一页面，您可以在“URL 类别”(URL Categories) 交互表中收集关于流媒体 (Streaming Media) URL 类别的更多详细信息。通过单击“流媒体”(Streaming Media) 类别链接，可以查看特定的 URL 类别报告页。此页面不仅显示访问流媒体站点的排名靠前的用户（在“按事务总数排名靠前的类别的用户”[Top Users by Category for Total Transactions] 部分），同时还显示所访问的域（在“匹配的域”[Domains Matched] 交互表中），例如，YouTube.com 或 QuickPlay.com。

此时，您会获得特定用户的越来越精准的信息。现在，让我们假设此特定用户因为其用量而显得尤为突出，则您可能想确切地找出他们正在访问什么内容。在这里，您可以在“用户”(Users) 交互表中单击用户。此操作会将您带到“用户”(User) 页面, on page 45，您可以在这里查看该用户的用户趋势，并准确地了解他们正在网络做什么。

如果您希望了解更多内容，现在可以单击交互表中的“已完成事务”(Transactions Completed) 链接，深入了解 Web 跟踪详细信息。这会在“Web 跟踪”(Web Tracking) 页面上显示搜索网络代理服务处理的事务 , on page 68，在此页面中可以查看有关用户访问站点的日期、完整 URL 以及在该 URL 上花费的时间等实际详细信息。

要查看如何使用“URL 类别”(URL Categories) 页面的其他示例，请参阅示例 3：调查受访问的排名靠前的 URL 类别。

报告错误分类和未分类的 URL

您可以在以下 URL 报告错误分类的和未分类的 URL：

https://talosintelligence.com/tickets。

会评价提交，以便包括在后续规则更新中。

要检查已提交的 URL 的状态，请单击此页面上的**有关已提交 URL 的状态 (Status on Submitted URLs)** 选项卡。

“用户”(User) 页面

用户报告页面提供了多个链接，可用于查看各个用户的 Web 报告信息。

要查看“用户”(Users) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring)** > **用户 (Users)**。有关详细信息，请参阅使用交互式报告页面。

从**用户 (Users)** 页面中，可以查看系统上的一个或多个用户在互联网、特定站点或 URL 上花费的时间，以及用户使用多少带宽。

注释 在网络安全设备上，安全管理设备可以支持的最大用户数为 500。

从**用户 (Users)** 页面，可以查看有关系统中用户的以下信息：

表 *19*:“用户”*(Users)* 页面上的详细信息

部分	说明
时间范围 (Time Range)（下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
排名靠前的用户：按受阻事务数排列	以图形格式按 IP 地址或用户名查看排名靠前的用户以及针对该用户阻止的事务的数量。报告时可以将用户名或 IP 地址进行匿名。有关如何在此页或在已安排报告中令用户名无法无法识别的更多信息，请参阅在安全管理设备上启用集中 Web 报告 ，第 3 页。默认设置为所有用户名均显示。要隐藏用户名，请参阅在 Web 报告中让用户名保持匿名 ，第 4 页。 要自定义图表视图，请点击图表上的。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
排名靠前的用户：使用的带宽	以图形格式按 IP 地址或用户名查看系统上使用最多带宽的排名靠前的用户。 要自定义图表视图，请点击图表上的。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
用户	您可以使用此交互式表搜索特定用户 ID 或客户端 IP 地址。在“用户”(User) 表底部的文本字段中，输入特定用户 ID 或客户端 IP 地址，然后点击“查找用户 ID /客户端 IP 地址”(Find User ID / Client IP Address)。IP 地址不需要是精确匹配项就可以返回结果。 您可以点击特定用户，查找更具体的信息。有关更多信息，请参阅 “用户详细信息”页面（Web 报告） ，第 46 页

注释 要查看用户 ID 而不是客户端 IP 地址，必须设置安全管理设备，以从 LDAP 服务器获取用户信息。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用，第 5 页。

“用户详细信息”页面（Web 报告）

通过**用户详细信息**页面，可以查看关于在“用户”报告页面上的交互式表中识别的用户的特定信息。

通过用户详细信息 (User Details) 页面，可以调查系统上各个用户的活动。如果您正在运行用户级调查，并且需要查找诸如用户正在访问哪些站点、他们遇到了哪些恶意软件威胁、正在访问哪些 URL 类别，以及特定用户在这些站点上花费了多少时间等信息，则此页面将非常有用。

要显示特定用户的“用户详细信息”页面，请单击**用户 (Users)** 报告页面上用户交互式表中的特定用户。

从用户详细信息 (User Details) 页面，可以查看有关系统中各个用户的以下信息：

表 *20*:“用户详细信息”页面上的详细信息

部分	说明
时间范围 (Time Range)（下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
URL 类别：按事务总数排列	以图形格式查看特定用户正在使用的特定 URL 类别。 要自定义图表视图，请单击图表上的 ✓。 预定义的 URL 类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告，第 15 页。
趋势：事务总数	您可以使用此趋势图查看特定用户的所有网络事务。 要自定义图表视图，请单击图表上的 ✓。 例如，此图将指示在一天的某些时段内是否存在网络流量激增以及这些激增发生的时间。使用“时间范围”(Time Range) 下拉列表，您可以扩展此图，以查看此用户在网络上的更为精细或粗略的时间范围。

部分	说明
匹配的 URL 类别 (URL Categories Matched)	“匹配的 URL 类别”交互式表显示了已完成和已阻止事务的匹配类别。 您可以在表底部的文本字段中搜索特定的 URL 类别，然后单击**查找 URL 类别 (Find URL Category)**。该类别不需要是完全匹配。 预定义的 URL 类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 ，第 15 页。
匹配的域 (Domains Matched)	“匹配的域”交互式表显示用户已访问的域或 IP 地址。您还可以查看在这些类别上所花费的时间，以及您在列视图中设置的其他各类信息。 您可以在表底部的文本字段中搜索特定的域或 IP 地址，然后单击**查找域或 IP (Find Domain or IP)**。域或 IP 地址不必是完全匹配。
匹配的应用 (Applications Matched)	“匹配的应用”交互式表显示特定用户使用的应用。例如，如果用户正在访问需要使用大量 Flash 视频的站点，您将在“应用”(Application) 列中看到此应用类型。 您可以在表底部的文本字段中搜索特定应用名称，然后单击**查找应用 (Find Application)**。应用的名称不必是完全匹配。
检测到的高级恶意软件防护威胁数	“检测到的高级恶意软件防护威胁数”交互式表显示高级恶意软件防护引擎检测到的恶意威胁文件。 您可以在表底部的文本框中搜索恶意威胁文件的特定 SHA 值的相关数据，然后单击**查找恶意软件威胁文件 SHA 256 (Find malware Threat File SHA 256)**。应用的名称不必是完全匹配。
检测到的恶意软件威胁数 (Malware Threats Detected)	“检测到的恶意软件威胁数”交互式表显示特定用户触发的排名靠前的恶意软件威胁。 您可以在表底部的文本字段中搜索特定恶意软件威胁名称的相关数据，然后单击**查找恶意软件威胁 (Find Malware Threat)**。恶意软件威胁的名称不必是完全匹配。
匹配的策略 (Policies Matched)	“匹配的策略”交互式表显示访问网络时应用到该用户的策略组。 您可以在表底部的文本字段中搜索特定策略名称，然后单击**查找策略 (Find Policy)**。策略的名称不必是完全匹配。

注释 在“客户端恶意软件风险详细信息”(Client Malware Risk Details) 表：客户端报告有时会在用户名的末尾显示星号 (*). 例如，客户端报告可能会同时为“jsmith”和“jsmith*”显示一个条目。带有星号 (*) 的用户名表示用户提供的用户名，但并未经身份验证服务器确认。当身份验证服务器不可用，并且设备配置为在身份验证服务不可用的情况下允许流量时，可能会出现上述情况。

“网站”(Web Sites) 页面

网站报告页面汇聚了托管设备上所发生活动的整体情况。您可以使用此报告页面监控特定时间范围内访问的高风险网站。

要查看“网站”(Web Sites) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 网站 (Web Sites)**。有关详细信息，请参阅使用交互式报告页面。

在网站 (Web Sites) 页面，您可以查看以下信息：

表 *21:*“网站”*(Web Sites)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
排名靠前的域：按事务总数排列	您可以以图形格式查看在网站上访问的排名靠前的域。 要自定义图表视图，请点击图表上的 ✓ 。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
排名靠前的域：按受阻事务数排列	您可以以图形格式查看根据事务触发阻止操作的排名靠前的域。 要自定义图表视图，请点击图表上的 ✓ 。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。 例如，用户访问了某特定域，并且由于布置了我拥有的一个特定策略，这触发了阻止操作。此域会在此图中以受阻止事务列出，并且列出触发了阻止操作的域站点。
匹配的域 (Domains Matched)	您可以使用此交互式表搜索正在网站上访问的域。您可以点击特定域，访问更加精细的信息。在“Web 跟踪”(Web Tracking) 页面上的“代理服务”(Proxy Services) 选项中，您可以查看跟踪信息以及某些域被阻止的原因。 当您点击某个特定域时，您可以查看到该域的排名靠前的用户、该域上排名靠前的事务、匹配的 URL 类别以及检测到的恶意软件威胁。 要查看如何使用 Web 跟踪的示例，请参阅示例 2：跟踪 URL。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用，第 5 页。

“HTTPS 报告”页面

“HTTPS 报告”报告页面是受管设备上 HTTP/HTTPS 流量摘要（事务或带宽使用情况）的整体汇聚。

您还可以根据客户端连接或服务器端连接，查看通过受管设备的单个 HTTP/HTTPS Web 流量所支持的密码摘要。

要查看“HTTPS 报告”(HTTPS Reports) 报告页面，请从**产品 (Product)**下拉列表中选择**网络 (Web)**，然后从 **报告 (Reports)** 下拉列表中选择**监控 (Monitoring) > HTTPS 报告 (HTTPS Reports)**。有关详细信息，请参阅使用交互式报告页面。

表 *22:* “*HTTPS* 报告”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
Web 流量摘要	您可以通过以下方式之一在设备上查看网络流量摘要： • **事务**：从下拉列表中选择此选项可根据 HTTP 或 https web 事务数以图形格式显示网络流量摘要，以表格格式显示 HTTP 或 https web 事务的百分比。 • **带宽使用情况**：从下拉列表中选择此选项可根据 HTTP 或 https 网络流量使用的带宽量以图形格式显示网络流量摘要，以图形格式显示 HTTP 或 https 带宽使用百分比（以表格形式）形式.
趋势： 网络流量	您可以通过以下方式之一根据所需的时间范围，在设备上查看网络流量的趋势图： • **网络流量趋势**：从下拉列表中选择此选项，以显示基于事务或带宽使用情况的 HTTP 和 HTTPS 网络流量的累积趋势。 • **HTTPS 趋势**：从下拉列表中选择此选项，以显示基于事务或带宽使用情况的 HTTPS 网络流量趋势。 • **HTTP 趋势**：从下拉列表中选择此选项，以显示基于事务或带宽使用情况的 HTTP 网络流量趋势。

部分	说明
密码	您可以通过以下方式之一查看密码摘要： • **按客户端连接**：从下拉列表中选择此选项，以图形格式显示 HTTP 或 HTTPS 网络流量的客户端上使用的密码摘要。 • **按服务器端连接**：从下拉列表中选择此选项，以图形格式显示 HTTP 或 HTTPS 网络流量的服务器端使用的密码摘要。

“防恶意软件”(Anti-Malware) 页面

防恶意软件报告页面是一个与安全相关的报告页面，反映由启用的扫描引擎（Webroot、Sophos、McAfee 和/或自适应扫描）扫描的结果。

要查看防恶意软件报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring)** > **防恶意软件 (Anti-Malware)**。有关详细信息，请参阅使用交互式报告页面。

使用此页面可以帮助识别和监控基于网络的恶意软件威胁。

注释 要查看第 4 层流量监控器发现的恶意软件的数据，请参阅 “第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面，第 38 页

在防恶意软件页面中，可以查看以下信息：

表 *23:*“防恶意软件”*(Anti-Malware)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
排名靠前的恶意软件类别	以图形格式查看按指定类别类型检测到的排名靠前的恶意软件类别。有关有效恶意软件类别的详细信息，请参阅恶意软件类别说明，第 19 页。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。
排名靠前的恶意软件威胁	以图形格式查看排名靠前的恶意软件威胁。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。

部分	说明
恶意软件类别数	“恶意软件类别”(Malware Categories) 交互表为在“排名靠前的恶意软件类别”(Top Malware Categories) 图表中显示的特定恶意软件类别显示详细信息。 点击“恶意软件类别”(Malware Categories) 交互表中的任意链接，您可以更为精细地查看各个恶意软件类别及其位于网络上哪个位置的详细信息。 例外：该表中的“病毒爆发启发式扫描”(Outbreak Heuristics) 链接，允许您查看一个图表，其中显示了何时出现此类别的事务。 有关有效恶意软件类别的详细信息，请参阅恶意软件类别说明，第 19 页。
恶意软件威胁数 (Malware Threats)	“恶意软件威胁数”(Malware Threats) 交互表在为“排名靠前的恶意软件威胁”(Top Malware Threats) 部分中显示的特定恶意软件威胁显示详细信息。 以一个数字标记为“病毒爆发”(Outbreak) 的威胁是由 Adaptive Scanning 功能独立于其他扫描引擎标识的威胁。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用，第 5 页。

恶意软件类别报告 (Malware Category Report)

“恶意软件类别报告”(Malware Category Report) 页允许您查看单个恶意软件类别的详细，以及它在您的网络中正在执行哪些操作。

要访问“恶意软件类别报告”(Malware Category Report) 页，请执行以下操作

步骤 1 在安全管理设备中，从下拉列表中选择**网络 (Web)**。

步骤 2 选择**监控 (Monitoring)** > **防恶意软件 (Anti-Malware)**页面。

步骤 3 在“恶意软件类别 (Malware Categories)”交互式表格中，点击“恶意软件类别 (Malware Category)”列中的一个类别。

步骤 4 要自定义此报告的视图，请参阅与网络安全报告一起使用, on page 5。

恶意软件威胁报告 (Malware Threat Report)

“恶意软件威胁报告”(Malware Threat Report) 页显示遭受特定威胁风险的客户端，显示可能受感染客户端的列表，以及指向“客户端详细信息”(Client Detail) 页的链接。报告顶部的趋势图显示在指定的时间范围内因某威胁受到监控和阻止的事务。底部的表显示在指定的时间范围内因某威胁受到监控和阻止的事务的实际数量。

要查看此报告，请在“防恶意软件报告”(Anti-Malware report) 页的“恶意软件类别”(Malware Category) 列中点击一个类别。

有关其他信息，请点击表格下方的**支持门户恶意软件详细信息 (Support Portal Malware Details)** 链接。

恶意软件类别说明

网络安全设备 可以阻止以下类型的恶意软件：

恶意软件类型	说明
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。某些广告软件应用具有并发运行并彼此监控的单独进程，确保修改是永久的。某些变体使得它们自己可以在每次计算机启动时自动运行。这些程序也可能更改安全设置，使得用户无法对其浏览器搜索选项、桌面和其他系统设置进行更改。
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供充分、明确且知情许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未提供充分、明确且知情许可的情况下，将用户引导至一个网站或运行一个程序。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
病毒爆发启发式扫描	此类别表示 Adaptive Scanning 独立于其他防恶意软件引擎发现的恶意软件。
网络钓鱼 URL	网络钓鱼 URL 显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。网络钓鱼是一种在线身份窃取形式，会使用社交工程和技术手段窃取个人身份数据和财务账户凭证。
PUA	可能不需要的应用。PUA 是非恶意应用，但可能被视为不想要的应用。

恶意软件类型	说明
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： 公开地或隐蔽地记录系统进程和/或用户操作。 使这些记录可用于以后检索和审核。
特洛伊木马下载程序 (Trojan Downloader)	特洛伊木马下载程序是一种木马程序，在安装后，会与远程主机/站点联系，并安装来自远程主机的程序包或附属程序。这些安装通常会无需用户确认即可发生。此外，不同安装之间，特洛伊木马下载程序的有效载荷可能会不同，因为它是从远程主机/站点获取下载说明。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可能会扫描受感染的计算机来查找银行站点、拍卖站点或在线支付站点的用户名和口令。
病毒	病毒是未经您确认就加载到您的计算机上，并且违背您的意愿运行的程序或代码段。
蠕虫	蠕虫是一种程序或算法，会通过计算机网络进行自我复制，通常执行恶意操作。

“高级恶意软件保护”页面

高级恶意软件防护通过如下方式防范零日威胁和基于文件的针对性威胁：

- 获取已知文件的信誉。
- 分析尚不为信誉服务所知的某些文件行为。
- 在获得新信息时评估新出现的威胁，并在确定为威胁的文件进入您的网络后通知您。

有关文件信誉过滤和文件分析的详细信息，请参阅用于网络安全设备的 *AsyncOS* 的用户指南或联机帮助。

要查看“高级恶意软件保护”(Advanced Malware Protection) 报告页面，请从“产品”(Product) 下拉列表中选择 **Web**，然后从“报告”(Product) 下拉列表中选择**监控 (Monitoring)** > **高级恶意软件保护 (Advanced Malware Protection)**。有关详细信息，请参阅 使用交互式报告页面。

“高级恶意软件保护”报告页面显示以下报告视图：

- 高级恶意软件防护 - AMP 摘要， 第 54 页
- 高级恶意软件保护 - 文件分析， 第 54 页

相关主题

- 文件分析报告详细信息的要求 ， 第 21 页
- 通过 SHA-256 散列标识文件 ， 第 22 页
- 查看其他报告中的文件信誉过滤数据 ， 第 24 页
- 关于 Web 跟踪和高级恶意软件防护功能 ， 第 79 页

高级恶意软件防护 - AMP 摘要

“高级恶意软件保护”(Advanced Malware Protection) 报告的“AMP 摘要”(AMP Summary) 部分显示了由文件信誉服务标识的基于文件的传入和传出威胁。

要查看尝试访问每个 SHA 的用户以及与该 SHA-256 关联的文件名，请点击表格中的 SHA-256。

您可以点击“恶意软件威胁文件”(Malware Threat Files) 交互式表中的链接，以便在网络跟踪中查看在最大可用时间范围内遇到的该文件的所有实例，不管为该报告选择什么时间范围都是如此。

如果从某个已压缩或已存档的文件中提取的某个文件是恶意文件，则只有这个已压缩或已存档的文件的 SHA 值包括在“高级恶意软件防护”(Advanced Malware Protection) 报告中。

您可以通过“高级恶意软件保护”(Advanced Malware Protection) 页面的“AMP 摘要”(AMP Summary) 部分来查看：

- 由高级恶意软件保护引擎的文件信誉服务标识的文件的摘要，以图形格式表示。
- 恶意软件威胁文件排行榜，以图形格式表示。
- 基于文件类型的威胁文件排行榜，以图形格式表示。
- 基于所选时间范围的所有恶意软件威胁文件的趋势图。
- 列出了恶意软件威胁文件排行榜的“恶意软件威胁文件”(Malware Threat Files) 交互式表。
- “具有追溯性判定更改的文件”(Files With Retrospective Verdict Change) 交互式表，其中列出了由设备处理且在事务处理后已更改裁定的文件。有关此情况的详细信息，请参阅网络安全设备的相应文档。

  如果单个 SHA-256 的判定多次发生变化，此报告仅显示最新的判定，而不显示判定历史记录。

  如果多个网络安全设备对于同一文件具有不同的判定更新，则将显示具有最新时间戳的结果。

  您可以点击 SHA-256 链接，以便查看在最大可用时间范围内包括此 SHA-256 的所有事务的 Web 跟踪结果，不论为报告选择的是哪种时间范围。

高级恶意软件保护 - 文件分析

“高级恶意软件保护”(Advanced Malware Protection) 报告页面的“文件分析”(File Analysis) 部分显示了发送以供分析的每个文件的时间和判定（或临时判定）。设备每 30 分钟检查一次分析结果。

对于采用现场思科 AMP Threat Grid 设备的部署：在思科 AMP Threat Grid 设备上包含在允许列表中的文件显示为“正常”(clean)。有关允许列表的信息，请参阅 AMP Threat Grid 联机帮助。

深入查看详细分析结果，包括威胁特征和每个文件的得分。

您还可以直接在执行分析的服务器上查看有关 SHA 目录的其他详细信息，方法是搜索 SHA 或点击文件分析详细信息页面底部的“思科 AMP Threat Grid”链接。

要在分析了文件的服务器上查看详细信息，请参阅文件分析报告详细信息的要求 ， 第 21 页。

如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的SHA值包括在“文件分析”(File Analysis) 中。

您可以使用“高级恶意软件保护报告”(Advanced Malware Protection) 页面中的“文件分析”(File Analysis) 部分进行查看：

- 由高级恶意软件保护引擎的分析服务上传以进行文件分析的文件的数量。
- 已完成文件分析请求的文件的列表。
- 待处理文件分析请求的文件的列表。

客户端恶意软件风险报告

客户端恶意软件风险报告页面是与安全相关的报告页面，可用于监控客户端恶意软件风险活动。

要查看“客户端恶意软件风险”(Client Malware Risk) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 客户端恶意软件风险 (Client Malware Risk)**。有关详细信息，请参阅使用交互式报告页面。

在“客户端恶意软件风险”报告页面，系统管理员可以查看哪些用户遇到了最多的阻止或警告。根据从此页面收集的信息，管理员可以点击用户链接，查看此用户在网络上执行了哪些操作导致受到如此多的阻止或警告，引发比网络上其他用户更多的检测。

此外，“客户端恶意软件风险”(Client Malware Risk) 页面还列出了常见恶意软件连接涉及的客户端 IP 地址，如第 4 层流量监控器 (L4TM) 所标识。经常连接到恶意站点的计算机可能感染了尝试连接到中央命令和控制服务器的恶意软件，应进行杀毒。

下表介绍有关“客户端恶意软件风险”页的信息。

表 *24:*“客户端恶意软件风险”*(Client Malware Risk)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
网络代理：排名靠前的受监控或阻止的客户端 (Web Proxy: Top Clients Monitored or Blocked)	以图形格式查看遇到了恶意软件风险的排名靠前的十个用户。 要自定义图表视图，请点击图表上的 ✓ 。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。

部分	说明
第 4 层流量监控器：检测到的恶意软件连接 (L4 Traffic Monitor: Malware Connections Detected)	以图形格式查看您的组织中最频繁连接到恶意软件站点的十台计算机的 IP 地址。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。 此图表与“第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面，第 38 页上的“排名靠前的客户端 IP”图表相同。
网络代理：客户端恶意软件风险 (Web Proxy: Client Malware Risk)	“网络代理：客户端恶意软件风险”交互式表显示在“网络代理：按恶意软件风险排名靠前的客户端”部分中显示的特定客户端的详细信息。 您可以在此表中点击每个用户，以查看与该客户端相关联的“用户详细信息”(User Details) 页。有关该页的信息，请参阅“用户详细信息”页面（Web 报告），第 46 页。 点击该表中的任意链接，您可以更为精细地查看各个用户以及他们正在执行的哪些活动触发了恶意软件风险的详细信息。
第 4 层流量监控器：按恶意软件风险排名的客户端 (L4 Traffic Monitor: Clients by Malware Risk)	“第4层流量监控器：按恶意软件风险排名的客户端”交互式表显示您的组织中频繁连接到恶意软件站点的计算机的 IP 地址。 该表与“第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面，第 38 页上的“客户端源 IP”(Client Source IPs) 表相同。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用，第 5 页。

网络信誉过滤器 (Web Reputation Filters) 页面

您可以使用**网络信誉过滤器**报告页面查看在指定的时间范围内为事务设置的网络信誉过滤器的结果。

要查看“网络信誉过滤器”(Web Reputation Filters) 报告页面，请从“产品”(Product) 下拉列表中选择**网络 (Web)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 网络信誉过滤器 (Web Reputation Filters)**。有关详细信息，请参阅使用交互式报告页面。

什么是网络信誉过滤？

网络信誉过滤用于分析网络服务器行为并为 URL 分配一个信誉得分，从而确定其包含基于 URL 的恶意软件的可能性。它有助于防御会威胁最终用户隐私和敏感公司信息的基于URL的恶意软件。网络安全设备使用URL信誉分数来识别可疑活动并提前阻止恶意软件攻击，避免其发生。您可以使用同时具有访问和解密策略的网络信誉过滤。

网络信誉过滤器使用统计数据评估互联网域可靠性并对URL信誉进行评分。许多数据可用于判断给定URL的可信度，例如，特定域的注册时长，或网站的托管位置，或者网络服务器是否使用动态IP地址等。

网络信誉计算将URL与网络参数相关联，用于确定恶意软件存在的可能性。然后得出的恶意软件存在的综合可能性会映射为一个 -10 到 +10 之间的网络信誉分数，+10 为最不可能包含恶意软件。

示例参数包括：

- URL 类别数据
- 存在的可下载代码
- 存在的冗长且含混的最终用户许可协议 (EULA)
- 全局量和量的变化
- 网络所有者信息
- URL 的历史记录
- URL 的时长
- 是否存在于任何阻止列表上
- 是否存在于任何允许列表上
- 常用域的 URL 拼写错误
- 域注册商信息
- IP 地址信息

有关网络信誉过滤的详细信息，请参阅《网络安全设备 *AsyncOS* 用户指南》中的“网络信誉过滤器”。

在网络信誉过滤 (Web Reputation Filters) 页面，您可以查看以下信息：

表 *25:*“网络信誉过滤器”*(Web Reputation Filters)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	选择报告的时间范围。有关详细信息，请参阅选择报告的时间范围。
网络信誉操作（趋势）(Web Reputation Actions [Trend])	您可以以图形格式查看指定时间内的网络信誉操作总数。在这里，您可以看到随着时间推移网络信誉操作的潜在趋势。
网络信誉操作（容量）(Web Reputation Actions [Volume])	您可以按事务以百分比的形式查看网络信誉操作数量。
已由WBRS阻止的网络信誉威胁类型 (Web Reputation Threat Types Blocked by WBRS)	您可以以图形格式查看事务中发现的已由网络信誉过滤阻止的威胁类型。 **注释** WBRS 不能始终识别出威胁类型。

部分	说明
在其他事务中检测到的威胁类型 (Threat Types Detected in Other Transactions)	您可以以图形格式查看事务中发现的已由网络信誉过滤阻止的威胁类型。 要自定义图表视图，请点击图表上的 ✓。有关详细信息，请参阅（仅限 Web 报告）选择要绘制哪些数据的图表。 这些威胁未被阻止的可能原因包括： • 并非所有威胁的得分均达到阻止阈值。但是，设备的其他功能可以捕获这些威胁。 • 可策略以允许配置威胁通过。 **注释** WBRS 不能始终识别出威胁类型。
Web 信誉操作（按分数分解）	如果未启用自适应扫描功能，此交互式表格会显示针对每项操作细分的网络信誉分数。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 ，第 5 页。

“调整网络信誉设置”(Adjusting Web Reputation Settings)

基于您的报告结果，您可能希望调整已配置的网络信誉设置，例如调整阈值得分，或启用或禁用 Adaptive Scanning。有关配置网络信誉设置的具体信息，请参阅《思科网络安全设备 *AsyncOS* 用户指南》。

关于计划的报告和按需 Web 报告

除非另有说明，否则您可以将以下网络安全报告生成为已安排报告或按需报告：

- “Web 报告概述”(Web Reporting Overview) - 要了解此页面上所包括内容的相关信息，请参阅Web 报告概述 , on page 9。
- “用户”(Users) - 要了解此页面上所包括内容的相关信息，请参阅用户报告 (Web) , on page 10。
- “网站”(Web Sites) - 要了解此页面上所包括内容的相关信息，请参阅网站报告 , on page 13。
- “URL 类别”(URL Categories) - 要了解此页面上所包括内容的相关信息，请参阅URL 类别报告 , on page 14。
- “排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended)：有关如何为“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 生成报告的信息，请参阅URL 类别排行榜 - 扩展, on page 61。

此报告不可作为按需报告。

- “应用可视性”(Application Visibility) - 要了解此页面上所包括内容的相关信息，请参阅应用可视性报告 , on page 16。
- “排名靠前的应用类型 - 扩展”(Top Application Types - Extended)：有关如何为“排名靠前的应用类型 - 扩展”(Top Application Types - Extended) 生成报告的信息，请参阅排名靠前的应用类型 - 扩展, on page 62。

此报告不可作为按需报告。

- “防恶意软件”(Anti-Malware) - 要了解此页面上所包括内容的相关信息，请参阅防恶意软件报告 , on page 17。
- “客户端恶意软件风险”(Client Malware Risk) - 要了解此页面上所包括内容的相关信息，请参阅客户端恶意软件风险报告 , on page 25。
- “网络信誉过滤”(Web Reputation Filters) - 要了解此页面上所包括内容的相关信息，请参阅网络信誉过滤器报告 , on page 26。
- “第 4 层流量监控器”(L4 Traffic Monitor) - 要了解此页面上所包括内容的相关信息，请参阅L4 流量监控器报告 , on page 28。
- “移动解决方案”(Mobile Secure Solution) - 要了解此页面上所包括内容的相关信息，请参阅按用户地点分类的报告 , on page 30。
- “系统容量”(System Capacity) - 要了解此页面上所包括内容的相关信息，请参阅“系统容量”(System Capacity) 页面, on page 31。

计划 Web 报告

本节包括以下主题：

Note 您可以选择让用户名在所有报告中无法识别。有关信息，请参阅在 Web 报告中让用户名保持匿名 , on page 4。

您可以安排报告每日、每周或每月运行。已安排报告可以配置为包括前一天、前七天、上个日历日（最多 250 天）以及上个日历月（最多 12 个月）的数据。或者，您可以包括自定义天数（从 2 天到 100 天）或自定义月数（从 2 个月到 12 个月）的数据。

无论您何时运行报告，均会从上一个时间时间间隔（小时、天、星期或月）返回数据。例如，如果您计划在凌晨 1 点运行每日报告，则该报告将包含前一天从午夜到午夜（00:00 到 23:59）的数据。

可以根据需要为报告定义任意数量的收件人，包括零个收件人。如果不指定邮件收件人，则系统仍会将报告存档。但是，如果您需要将报告发送到大量地址，则可能需要创建邮件列表，而不是逐个列出收件人。

“我的 Web 报告”是“计划的报告”菜单下的用户报告。用户报告只能由创建它们的用户查看。

计划的 Web 报告的存储

会保留其生成的最新报告 - 对于每个计划报告，可包含多达 30 个最近的实例，并且对于所有报告，可包含 1000 个总版本。

存档的报告会自动删除。在添加新的报告时，系统会删除较旧的报告以将数量保持在1000个。最多可将 30 个实例应用到具有相同名称和时间范围的各个计划报告。

已存档的报告存储在设备上的/periodic_reports目录。（有关详细信息，请参阅IP接口和访问设备。）

相关主题

- 查看和管理存档的 Web 报告, on page 64

添加已安排的 Web 报告

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 计划报告 (Scheduled Reports)**。

步骤 2 点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3 在**类型 (Type)** 旁边的下拉菜单中，选择您的报告类型。

步骤 4 在**标题 (Title)** 字段中，键入报告的标题。

为了避免创建多个使用相同名称的报告，我们建议使用说明性的标题。

步骤 5 从**时间范围 (Time Range)** 下拉菜单中，选择报告的时间范围。

步骤 6 选择所生成的报告的格式。

默认格式为 PDF。大多数报告还允许您将原始数据另存为 CSV 文件。

步骤 7 在**项目数 (Number of Items)** 旁边的下拉列表中，选择您要包括在已生成报告中的项目数。

有效值为 2 到 20。默认值为 5。

步骤 8 对于**图表 (Charts)**，请点击**要显示的数据 (Data to display)** 下的默认图表，然后选择要在报告的每个图表中显示的数据。

步骤 9 在**对列排序 (Sort Column)** 旁边的下拉列表中，选择对此报告的数据进行排序的列。这允许您按已安排报告中任意可用的列生成一个具有前“N”项的已安排报告。

步骤 10 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 11 在**电子邮件** 文本字段中，输入生成的报告将发送到的邮件地址。

如果不指定邮件地址，则仅存档该报告。

步骤 12 点击**提交 (Submit)**。

编辑计划的 Web 报告

要编辑报告，请转到**网络 (Web) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**，并选中您要编辑报告的相应复选框。修改设置，然后点击**提交 (Submit)** 以提交在页面上进行的更改，然后点击**确认更改 (Commit Changes)** 按钮以确认对设备进行的更改。

删除已安排的 Web 报告

要删除报告，请转到**网络 (Web) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**，并选中您要编辑报告的相应复选框。要删除所有计划报告，请选中**全部 (All)** 复选框，然后**删除**并**确认**更改。注意已删除报告的存档版本不会被删除。

更多扩展的 Web 报告

安全管理设备上还提供另外两个报告作为计划报告：

- URL 类别排行榜 - 扩展, on page 61
- 排名靠前的应用类型 - 扩展, on page 62

URL 类别排行榜 - 扩展

对于希望接收到的信息比 URL 类别报告中的信息更详细的管理员来说，“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 报告非常有用。

例如，在典型的 URL 类别报告中，您可以在较大的 URL 类别级别按特定员工收集评估带宽使用量的信息。要生成更为详细的报告，用于为每个 URL 类别监控前十个 URL 的带宽使用量，或者为每个 URL 类别监控前五位用户的带宽使用量，请使用“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 报告。

Note 使用此报告类型可以生成的最大报告数为 20。

- 预定义的URL类别列表会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 , on page 15。

要生成“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 报告，请执行以下操作：

步骤 1 在安全管理设备上，选择**网络 (Web) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2 点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3 在“类型”旁边的下拉菜单中，选择**URL 类别排行榜 - 扩展**。

步骤 4 在**标题 (Title)** 文本字段中，键入 URL 扩展报告的标题。

步骤 5 从**时间范围 (Time Range)** 下拉菜单中，选择报告的时间范围。

步骤 6 选择所生成的报告的格式。

默认格式为 PDF。

步骤 7 在**项目数 (Number of Items)** 旁边的下拉列表中，选择要包括在已生成报告中的 URL 类别数。

有效值为 2 到 20。默认值为 5。

步骤 8 在**对列排序 (Sort Column)** 旁边的下拉列表中，选择对此报告的数据进行排序的列。这允许您按已安排报告中任意可用的列生成一个具有前“N”项的已安排报告。

步骤 9 对于**图表 (Charts)**，请点击**要显示的数据 (Data to display)** 下的默认图表，然后选择要在报告的每个图表中显示的数据。

步骤 10 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 11 在**电子邮件** 文本字段中，输入生成的报告将发送到的邮件地址。

步骤 12 点击**提交 (Submit)**。

排名靠前的应用类型 - 扩展

要生成“排名靠前的应用类型 - 扩展”(Top Application Type—Extended) 报告，请执行以下操作：

步骤 1 在安全管理设备上，选择**网络 (Web) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2 单击**添加计划的报告 (Add Scheduled Report)**。

步骤 3 在“类型”(Type) 旁边的下拉菜单中，选择**排名靠前的应用类型 - 扩展 (Top Application Type—Extended)**。

页面上的选项将更改。

步骤 4 在**标题 (Title)** 文本字段中，键入报告的标题。

步骤 5 从**时间范围 (Time Range)** 下拉菜单中，选择报告的时间范围。

步骤 6 选择所生成的报告的格式。

默认格式为 PDF。

步骤 7 在**项目数 (Number of Items)** 旁边的下拉列表中，选择您要包括在已生成报告中的应用类型数。

有效值为 2 到 20。默认值为 **5**。

步骤 8 在**对列排序 (Sort Column)** 旁边的下拉列表中，选择要显示在表中的列类型。选项包括：“已完成事务”(Transactions Completed)、“已阻止事务”(Transactions Blocked)、“事务总数”(Transaction Totals)。

步骤 9 对于**图表 (Charts)**，请单击**要显示的数据 (Data to display)** 下的默认图表，然后选择要在报告的每个图表中显示的数据。

步骤 10 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 11 在**电子邮件** 文本字段中，输入生成的报告将发送到的邮件地址。

步骤 12 点击**提交**。

按需生成 Web 报告

您可以安排大多数报告，并且还可以按需生成报告。

Note 某些报告仅以“已安排报告”(Scheduled Reports) 的形式而不是按需报告的形式存在。请参阅更多扩展的 Web 报告, on page 61。

要按需生成报告，请执行以下操作：

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2 点击**立即生成报告 (Generate Report Now)**。

步骤 3 在**报告类型 (Report type)** 部分中，从下拉列表选择报告类型。

页面上的选项可能会变化

步骤 4 在“标题”(Title) 文本字段中，键入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 5 从**要包括的时间范围**下拉列表中，为报告数据选择一个时间范围。

步骤 6 在“格式”(Format) 部分中，选择报告的格式。

选项包括：

- PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件可包含多达 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。

步骤 7 根据报告可用的选项，请选择：

- **行数 (Number of rows)**：显示在表中的数据行数。
- **图表 (Charts)**：哪些数据显示在报告的图表中：
- 点击“要显示的数据”(Data to display) 下的默认选项。
- **对列排序 (Sort Column)**：对每个表进行排序所依据的列。

步骤 8 从“传送选项”(Delivery Option) 部分中，选择以下选项：

- 如果希望此报告显示在“存档的报告”(Archived Reports) 页面上，请选中**存档报告 (Archive Report)** 复选框。

Note 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 选中**立即通过邮件发送给收件人 (Email now to recipients)** 复选框，通过邮件发送该报告。

- 在文本字段中，请输入报告的收件人邮件地址。

步骤 9 点击**传送此报告 (Deliver This Report)** 生成报告。

“存档的 Web 报告”(Archived Web Reports) 页面

- 关于计划的报告和按需 Web 报告， 第 58 页
- 按需生成 Web 报告 ， 第 63 页
- 查看和管理存档的 Web 报告， 第 64 页

查看和管理存档的 Web 报告

使用本部分的信息可以处理生成为已安排报告的报告。

“存档”报告下的“我的 Web 报告”只能由创建计划报告的用户查看。

步骤 1 转到**网络 (Web) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2 要查看报告，请单击“报告标题”(Report Title) 列中的报告名称。“显示”(Show) 下拉菜单会过滤在**存档的报告 (Archived Reports)** 页面上列出的报告类型。

步骤 3 如果列表很长，要找到特定的报告，请通过从**显示 (Show)** 菜单中选择报告类型来过滤列表，或者单击某个列标题以按该列进行排序。

What to do next

相关主题

- 计划的 Web 报告的存储 , on page 60
- 添加已安排的 Web 报告, on page 60
- 按需生成 Web 报告 , on page 63

在新 Web 界面上计划和存档网络报告

“我的 Web 报告”是“计划的报告”菜单下的用户报告。用户报告只能由创建它们的用户查看。
“存档”报告下的“我的 Web 报告”只能由创建计划报告的用户查看。

- 在新 Web 界面上计划 Web 报告， 第 65 页
- 在新 Web 界面上存档 Web 报告， 第 66 页

在新 Web 界面上计划 Web 报告

本节包括以下主题：

注释　您可以选择让用户名在所有报告中无法识别。有关信息，请参阅在 Web 报告中让用户名保持匿名，第 4 页。

您可以安排报告每日、每周或每月运行。已安排报告可以配置为包括前一天、前七天、上个日历日（最多 250 天）以及上个日历月（最多 12 个月）的数据。或者，您可以包括自定义天数（从 2 天到 100 天）或自定义月数（从 2 个月到 12 个月）的数据。

无论您何时运行报告，均会从上一个时间时间间隔（小时、天、星期或月）返回数据。例如，如果您计划在凌晨 1 点运行每日报告，则该报告将包含前一天从午夜到午夜（00:00 到 23:59）的数据。

可以根据需要为报告定义任意数量的收件人，包括零个收件人。如果不指定邮件收件人，则系统仍会将报告存档。但是，如果您需要将报告发送到大量地址，则可能需要创建邮件列表，而不是逐个列出收件人。

在新 Web 界面上添加已计划的 Web 报告

步骤 1　在安全管理设备上，从“产品”(Product) 下拉列表中选择 **Web**。有关详细信息，请参阅 使用交互式报告页面。

步骤 2　选择**监控 > 计划和存档**。

步骤 3　在“已计划/已存档”(Schduled / Archived) 选项卡中，单击 + 按钮。

步骤 4　从**报告类型 (Report Type)** 下拉菜单选择报告类型。

步骤 5　在**报告标题 (Report Title)** 字段中，键入报告的标题。

为了避免创建多个使用相同名称的报告，我们建议使用说明性的标题。

步骤 6　从**要包括的时间范围**下拉菜单中选择报告的时间范围。

步骤 7　选择所生成的报告的格式。

默认格式为 PDF。

步骤 8　从“传送选项”(Delivery Option) 部分中，选择以下任一选项：

如果选择此选项，报告将在“已存档的报告”(Archived Reports) 页面上列出。

注释　无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 要存档报告，请选择**仅存档 (Only Archive)**。
- 要存档并通过邮件发送报告，请单击**存档并通过邮件发送至收件人 (Archive and Email to Recipients)**。

- 要通过邮件发送报告，请单击**仅发送邮件至收件人 (Only Email to Recipients)**。

在**邮件 ID** 字段中，输入收件人邮箱地址。

步骤 9 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 10 从**报告语言 (Report Language)** 下拉列表中选择必须生成报告的语言。

步骤 11 点击**提交**。

在新 Web 界面上编辑已计划网络报告

要在设备的新 Web 界面上编辑报告，请从“产品”(Product) 下拉列表中选择 **Web**，然后选择**监控 (Monitoring) > 计划和存档 (Scheduled & Archive)** 页面。单击与要编辑的报告的报告标题对应的链接。修改设置，然后单击**编辑 (Edit)** 以便在页面上提交更改。

在新 Web 界面上删除已计划的 Web 报告

要在设备的新 Web 界面上删除报告，请从“产品”(Product) 下拉列表中选择 **Web**，然后选择**监控 (Monitoring) > 已计划 (Scheduled) / 已存档 (Archived)** 页面。选中与要删除的报告对应的复选框，然后单击垃圾桶图标。

要删除所有计划的报告，请选中报告标题旁边的复选框。注意已删除报告的存档版本不会被删除。

在新 Web 界面上存档 Web 报告

- [新 Web 界面] 按需生成 Web 报告，第 66 页
- 在新 Web 界面上查看和管理存档的网络报告，第 67 页

[新 Web 界面] 按需生成 Web 报告

您可以安排大多数报告，并且还可以按需生成报告。

注释 某些报告仅以“已安排报告”(Scheduled Reports) 的形式而不是按需报告的形式存在。请参阅更多扩展的 Web 报告，第 61 页。

要按需生成报告，请执行以下操作：

步骤 1 在安全管理设备上，从“产品”(Product) 下拉列表中选择 **Web**，然后选择**监控 (Monitoring) > 计划和存档 (Schedule& Archive)**。

步骤 2 在“查看已存档”(View Archived) 选项卡中，单击 + 按钮。

步骤 3 在**报告类型 (Report Type)** 部分中，从下拉列表选择报告类型。

页面上的选项可能会变化

步骤 4 在**报告标题 (Report Title)** 部分中，输入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 5 从**要包括的时间范围**下拉列表中，为报告数据选择一个时间范围。

步骤 6 在**附件详细信息 (Attachment Details)** 部分中，选择报告的格式。

PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过单击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。

步骤 7 从**传送选项 (Delivery Option)** 部分中，选择以下任一选项：

如果选择此选项，报告将在“已存档的报告”(Archived Reports) 页面上列出。

注释 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 要存档报告，请选择**仅存档 (Only to Archive)**。
- 要存档并通过邮件发送报告，请单击**存档并通过邮件发送至收件人 (Archive and Email to Recipients)**。
- 要通过邮件发送报告，请单击**仅发送邮件至收件人 (Only Email to Recipients)**。

在**邮件 ID** 字段中，输入收件人邮箱地址。

步骤 8 从**报告语言 (Report Language)** 下拉列表中选择必须生成报告的语言。

步骤 9 单击**传送此报告 (Deliver This Report)** 生成报告。

在新 Web 界面上查看和管理存档的网络报告

使用本部分的信息可以处理生成为已安排报告的报告。

步骤 1 登录设备的新 Web 界面。

步骤 2 从“产品”(Product) 下拉列表中选择 **Web**，然后选择**监控 (Monitoring) > 计划和存档 (Schedule& Archive)**。

步骤 3 选择“查看已存档”(View Archived) 选项卡。

步骤 4 要查看报告，请单击“报告标题”(Report Title) 列中的报告名称。“报告类型”(Report Type) 下拉列表会过滤在“存档的报告”(Archived Reports) 选项卡中列出的报告类型。

步骤 5 您可以在搜索框中搜索特定报告。

Web跟踪

使用“Web 跟踪”(Web Tracking) 页面可以搜索和查看关于各个事务的详细信息，或者搜索和查看您关心的事务的模式。根据您的部署使用的服务，请在相关选项卡中搜索：

- 搜索网络代理服务处理的事务 , on page 68
- 搜索 L4 流量监控器处理的事务 , on page 72

- 搜索 SOCKS 代理处理的事务 , on page 72
- 处理 Web 跟踪搜索结果 , on page 78
- 查看 Web 跟踪搜索结果的事务详细信息 , on page 78

或者，在某些情况下（如透明传递）使用 FQDN 在“网络跟踪”(Web Tracking) 页面上搜索网站数据。

有关网络代理与 L4 流量监控器之间区别的更多信息，请参阅《思科网络安全设备 AsyncOS 用户指南》中的“了解网络安全设备如何工作”一节。

相关主题

- 关于 Web 跟踪和升级 , on page 80

搜索网络代理服务处理的事务

使用**网络 (Web) > 报告 (Reporting) > Web 跟踪 (Web Tracking)** 页面上的 **代理服务 (Proxy Services)** 选项卡搜索从各个安全组件和可接受的使用实施组件汇聚的 Web 跟踪数据。此数据不包括第 4 层流量监控数据或 SOCKS 代理处理的事务。

您可能希望使用它协助以下角色的工作：

- **HR 或法务经理**。在特定时段运行对某位员工的调查报告。

例如，您可以使用“代理服务”(Proxy Services) 选项卡检索用户正在访问的特定 URL、用户访问该 URL 的时间以及该 URL 是否被允许等信息。

- **网络安全管理员**。检查公司网络是否正通过员工的智能手机遭受恶意软件威胁。

您可以查看特定时段内已记录事务（包括已阻止、已监控、已警告和已完成）的搜索结果。您还可以使用多个条件（例如 URL 类别、恶意软件威胁和应用）来过滤数据结果。

Note 网络代理仅报告包括 ACL 决策标记（而非“OTHER-NONE”）的事务。

有关 Web 跟踪使用情况的示例，请参阅示例 1：调查用户。

有关“代理服务”(Proxy Services) 选项卡如何与其他 Web 报告页面配合使用的示例，请参阅将“URL 类别”页面与其他报告页面结合使用, on page 15。

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

步骤 2 点击**代理服务 (Proxy Services)** 选项卡。

步骤 3 要查看所有搜索和过滤选项，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件：

Table 26: *“代理服务”(Proxy Services)* 选项卡上的 *Web* 跟踪搜索条件

选项	说明
默认搜索条件	
时间范围 (Time Range)	选择要报告的时间范围。有关安全管理设备上可用的时间范围的信息，请参阅选择报告的时间范围。
用户/客户端 IPv4 或 IPv6 (User/Client IPv4 or IPv6)	当用户名显示在报告中时输入身份验证用户名，或输入您要跟踪的客户端 IP 地址，这是可选操作。您还可以输入 CIDR 格式的 IP 范围，例如 172.16.0.0/16。 当您将此字段留空时，搜索将为所有用户返回结果。
网站 (Website)	输入您要跟踪的网站，这是可选操作。当您将此字段留空时，搜索将为所有网站返回结果。
事务类型	选择您要跟踪的事务类型，可能是“所有事务”(All Transactions)、“已完成事务”(Completed)、“已阻止事务”(Blocked)、“已监控事务”(Monitored) 或“已警告事务”(Warned)。
高级搜索条件	
URL 类别	要按 URL 类别过滤，请选择**按 URL 类别过滤 (Filter by URL Category)**，并键入过滤所依据的自定义或预定义的 URL 类别的第一个字母。从显示的列表中选择类别. 如果 URL 类别集已更新，则某些类别可能标记为“已弃用 (Deprecated)”。已弃用的类别将不再用于新事务。但是，仍然可以搜索当该类别处于活动状态时发生的最近事务。有关 URL 类别集更新的更多信息，请参阅URL 类别集更新和报告 , on page 15。 将包括与类别名称匹配的所有最近事务，无论下拉列表中标明的是哪个引擎名称。
应用	要按应用进行过滤，请选择**按应用过滤 (Filter by Application)** 并选择要依据其进行过滤的应用。 要按应用类型进行过滤，请选择**按应用类型过滤 (Filter by Application)** 并选择要依据其进行过滤的应用类型。
策略 (Policy)	要按策略组进行过滤，请选择**按策略过滤 (Filter by Policy)** 并输入依据其进行过滤的策略组名称。 确保您已在网络安全设备上声明了该策略。
恶意软件威胁	要按特定恶意软件威胁进行过滤，请选择**按恶意软件威胁过滤 (Filter by Malware Threat)** 并输入要依据其进行过滤的恶意软件威胁名称。 要按恶意软件类别过滤，选择**按恶意软件类别过滤 (Filter by Malware Category)** 并选择按其过滤的恶意软件类别。有关说明，请参阅恶意软件类别说明, on page 19。

选项	说明
WBRS	在 WBRS 部分中，可以按基于网络的信誉分数和特定网络信誉威胁进行过滤。 • 要按网络信誉得分过滤，请选择**得分范围**，并选择过滤所依据的上限值和下限值。或者，您可以选择**无得分 (No Score)** 来过滤出那些没有得分的网站。 • 要按网络信誉威胁过滤，选择**按信誉威胁过滤 (Filter by Reputation Threat)** 并选择按其过滤的网络信誉威胁。 有关 WBRS 得分的详细信息，请参阅《适用于 Web 的 IronPort AsyncOS 用户指南》。
AnyConnect 安全移动	要按远程或本地访问进行过滤，请选择**按用户地点进行过滤 (Filter by User Location)** 并选择访问类型。要包括所有访问类型，请选择**禁用过滤 (Disable Filter)**。 （在以前的版本中，此选项被标记为“移动用户安全”(Mobile User Security)。）
网络设备 (Web Appliance)	要按特定网络设备过滤，请点击**按网络设备过滤 (Filter by Web Appliance)** 旁边的单选按钮，并在文本字段中输入网络设备名称。 如果选择**禁用过滤器 (Disable Filter)**，则搜索将包括与安全管理设备关联的所有网络安全设备。
用户请求	要按用户实际发起的事务过滤，请选择**按 Web 用户请求的事务过滤**。 **说明**：启用此过滤器后，搜索结果将包括“最佳猜测”事务。

步骤 5 点击**搜索 (Search)**。

What to do next

相关主题

- 显示更多 Web 跟踪搜索结果 , on page 78
- 了解 Web 跟踪搜索结果 , on page 78
- 查看 Web 跟踪搜索结果的事务详细信息 , on page 78
- 关于 Web 跟踪和高级恶意软件防护功能 , on page 79

恶意软件类别说明

网络安全设备 可以阻止以下类型的恶意软件：

恶意软件类型	说明
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。某些广告软件应用具有并发运行并彼此监控的单独进程，确保修改是永久的。某些变体使得它们自己可以在每次计算机启动时自动运行。这些程序也可能更改安全设置，使得用户无法对其浏览器搜索选项、桌面和其他系统设置进行更改。

恶意软件类型	说明
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供充分、明确且知情许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未提供充分、明确且知情许可的情况下，将用户引导至一个网站或运行一个程序。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
病毒爆发启发式扫描	此类别表示 Adaptive Scanning 独立于其他防恶意软件引擎发现的恶意软件。
网络钓鱼 URL	网络钓鱼 URL 显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。网络钓鱼是一种在线身份窃取形式，会使用社交工程和技术手段窃取个人身份数据和财务账户凭证。
PUA	可能不需要的应用。PUA 是非恶意应用，但可能被视为不想要的应用。
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： 公开地或隐蔽地记录系统进程和/或用户操作。 使这些记录可用于以后检索和审核。
特洛伊木马下载程序 (Trojan Downloader)	特洛伊木马下载程序是一种木马程序，在安装后，会与远程主机/站点联系，并安装来自远程主机的程序包或附属程序。这些安装通常会无需用户确认即可发生。此外，不同安装之间，特洛伊木马下载程序的有效载荷可能会不同，因为它是从远程主机/站点获取下载说明。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可能会扫描受感染的计算机来查找银行站点、拍卖站点或在线支付站点的用户名和口令。

恶意软件类型	说明
病毒	病毒是未经您确认就加载到您的计算机上，并且违背您的意愿运行的程序或代码段。
蠕虫	蠕虫是一种程序或算法，会通过计算机网络进行自我复制，通常执行恶意操作。

搜索 L4 流量监控器处理的事务

网络 (Web) > 报告 (Reporting) > Web 跟踪 (Web Tracking) 页面上的“L4 流量监控器”(L4 Traffic Monitor) 选项卡提供有关与恶意软件站点和端口的连接的详细信息。您可以通过以下信息类型搜索至恶意软件站点的连接：

- 时间范围
- 发起该事务的计算机的 IP 地址（IPv4 或 IPv6）
- 目标网站的域或 IP 地址（IPv4 或 IPv6）
- 端口
- 与组织中的计算机相关联的 IP 地址
- 连接类型
- 处理连接的网络安全设备

将会显示前 1000 个匹配的搜索结果。

查看有问题站点或处理事务的网络安全设备的主机名，请单击“目标 IP 地址 (Destination IP Address)”列标题中的“显示详细信息 (Display Details)”链接。

有关如何使用此信息的更多信息，请参阅L4 流量监控器报告 , on page 28。

搜索 SOCKS 代理处理的事务

您可以搜索符合多个条件的事务，包括已阻止事务或已完成事务；发起该事务的客户端计算机的 IP 地址；目标域、IP 地址或端口。您还可以按自定义 URL 类别、匹配的策略以及用户位置（本地或远程）来过滤结果。不支持 IPv4 和 IPv6 地址。

步骤 1 依次选择**网络 (Web) > 报告 (Reporting) > Web 跟踪 (Web Tracking)**。

步骤 2 点击 **SOCKS 代理 (SOCKS Proxy)** 选项卡。

步骤 3 要过滤结果，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件。

步骤 5 点击**搜索 (Search)**。

What to do next

相关主题

SOCKS 代理报告 , on page 30

新 Web 界面上的 Web 跟踪

您可以使用**Web 跟踪搜索**页面搜索和查看有关各个事务或可能有关的事务模式的详细信息。根据您的部署使用的服务，请在相关选项卡中搜索：

- 搜索网络代理服务处理的事务 ， 第 73 页
- 搜索 L4 流量监控器处理的事务 ， 第 72 页
- 搜索 SOCKS 代理处理的事务 ， 第 77 页
- 处理 Web 跟踪搜索结果 ， 第 78 页
- 查看 Web 跟踪搜索结果的事务详细信息 ， 第 78 页

有关网络代理与第4层流量监控器之间区别的更多信息，请参阅中的“《思科网络安全设备*AsyncOS*用户指南》中的“了解网络安全设备如何工作”一节。

搜索网络代理服务处理的事务

您可以使用**Web 跟踪搜索**页面上的**代理服务**选项卡搜索从各个安全组件和可接受的使用实施组件汇聚的 Web 跟踪数据。此数据不包括第 4 层流量监控数据或 SOCKS 代理处理的事务。

您可能希望使用它协助以下角色的工作：

- **HR 或法务经理**。在特定时段运行对某位员工的调查报告。

  例如，您可以使用“代理服务”(Proxy Services) 选项卡检索用户正在访问的特定 URL、用户访问该 URL 的时间以及该 URL 是否被允许等信息。

- **网络安全管理员**。检查公司网络是否正通过员工的智能手机遭受恶意软件威胁。

您可以查看特定时段内已记录事务（包括已阻止、已监控、已警告和已完成）的搜索结果。您还可以使用多个条件（例如 URL 类别、恶意软件威胁和应用）来过滤数据结果。

注释 网络代理仅报告包括 ACL 决策标记（而非“OTHER-NONE”）的事务。

有关 Web 跟踪使用情况的示例，请参阅示例 1：调查用户。

有关“代理服务”(Proxy Services) 选项卡如何与其他 Web 报告页面配合使用的示例，请参阅将“URL 类别”页面与其他报告页面结合使用 ， 第 15 页。

步骤 1 在安全管理设备上，从下拉列表中选择**网络 (Web)**。

步骤 2 选择**跟踪 > 代理服务**。

步骤 3 要查看所有搜索和过滤选项，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件：

表 27: “代理服务” *(Proxy Services)* 选项卡上的 *Web* 跟踪搜索条件

选项	说明
默认搜索条件	
时间范围 (Time Range)	选择要报告的时间范围。有关安全管理设备上可用的时间范围的信息，请参阅选择报告的时间范围。
用户/客户端 IPv4 或 IPv6	当用户名显示在报告中时输入身份验证用户名，或输入您要跟踪的客户端 IP 地址，这是可选操作。您还可以输入 CIDR 格式的 IP 范围，例如 172.16.0.0/16。 当您将此字段留空时，搜索将为所有用户返回结果。
网站 (Website)	输入您要跟踪的网站，这是可选操作。当您将此字段留空时，搜索将为所有网站返回结果。
事务类型	选择您要跟踪的事务类型，可能是“所有事务”(All Transactions)、“已完成事务”(Completed)、“已阻止事务”(Blocked)、“已监控事务”(Monitored) 或“已警告事务”(Warned)。
高级搜索条件	
URL 类别	要按 URL 类别过滤，请选择**按 URL 类别过滤 (Filter by URL Category)**，并键入过滤所依据的自定义或预定义的 URL 类别的第一个字母。从显示的列表中选择类别. 如果URL类别集已更新，则某些类别可能标记为“已弃用(Deprecated)”。已弃用的类别将不再用于新事务。但是，仍然可以搜索当该类别处于活动状态时发生的最近事务。有关 URL 类别集更新的更多信息，请参阅URL 类别集更新和报告 ，第 15 页。 将包括与类别名称匹配的所有最近事务，无论下拉列表中标明的是哪个引擎名称。
应用	要按应用进行过滤，请选择**按应用过滤 (Filter by Application)** 并选择要依据其进行过滤的应用。 要按应用类型进行过滤，请选择**按应用类型过滤 (Filter by Application)** 并选择要依据其进行过滤的应用类型。
Youtube (YT) 类别	要按特定的 YouTube 类别进行过滤，请展开 **YouTube 类别 (Youtube Category)** 部分，然后选择要查看的 YouTube 类别。

选项	说明
策略 (Policy)	要按策略组进行过滤，请选择**按策略过滤 (Filter by Policy)** 并输入依据其进行过滤的策略组名称。 确保您已在网络安全设备上声明了该策略。
恶意软件威胁	要按特定恶意软件威胁进行过滤，请选择**按恶意软件威胁过滤 (Filter by Malware Threat)** 并输入要依据其进行过滤的恶意软件威胁名称。 要按恶意软件类别过滤，选择**按恶意软件类别过滤 (Filter by Malware Category)** 并选择按其过滤的恶意软件类别。有关说明，请参阅恶意软件类别说明，第 19 页。
WBRS	在 WBRS 部分中，可以按基于网络的信誉分数和特定网络信誉威胁进行过滤。 • 要按网络信誉得分过滤，请选择**得分范围**，并选择过滤所依据的上限值和下限值。或者，您可以选择**无得分 (No Score)** 来过滤出那些没有得分的网站。 • 要按网络信誉威胁过滤，选择**按信誉威胁过滤 (Filter by Reputation Threat)** 并选择按其过滤的网络信誉威胁。 有关 WBRS 得分的详细信息，请参阅《适用于 Web 的 IronPort AsyncOS 用户指南》。
AnyConnect 安全移动	要按远程或本地访问进行过滤，请选择**按用户地点进行过滤 (Filter by User Location)** 并选择访问类型。要包括所有访问类型，请选择**禁用过滤 (Disable Filter)**。 （在以前的版本中，此选项被标记为“移动用户安全”(Mobile User Security)。）
网络设备 (Web Appliance)	要按特定网络设备过滤，请点击**按网络设备过滤 (Filter by Web Appliance)** 旁边的单选按钮，并在文本字段中输入网络设备名称。 如果选择**禁用过滤器 (Disable Filter)**，则搜索将包括与安全管理设备关联的所有网络安全设备。
用户请求	要按用户实际发起的事务过滤，请选择**按 Web 用户请求的事务过滤**。 **说明**：启用此过滤器后，搜索结果将包括“最佳猜测”事务。

恶意软件类别说明

网络安全设备 可以阻止以下类型的恶意软件：

恶意软件类型	说明
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。某些广告软件应用具有并发运行并彼此监控的单独进程，确保修改是永久的。某些变体使得它们自己可以在每次计算机启动时自动运行。这些程序也可能更改安全设置，使得用户无法对其浏览器搜索选项、桌面和其他系统设置进行更改。

恶意软件类型	说明
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供充分、明确且知情许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未提供充分、明确且知情许可的情况下，将用户引导至一个网站或运行一个程序。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
病毒爆发启发式扫描	此类别表示 Adaptive Scanning 独立于其他防恶意软件引擎发现的恶意软件。
网络钓鱼 URL	网络钓鱼 URL 显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。网络钓鱼是一种在线身份窃取形式，会使用社交工程和技术手段窃取个人身份数据和财务账户凭证。
PUA	可能不需要的应用。PUA 是非恶意应用，但可能被视为不想要的应用。
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： 公开地或隐蔽地记录系统进程和/或用户操作。 使这些记录可用于以后检索和审核。
特洛伊木马下载程序 (Trojan Downloader)	特洛伊木马下载程序是一种木马程序，在安装后，会与远程主机/站点联系，并安装来自远程主机的程序包或附属程序。这些安装通常会无需用户确认即可发生。此外，不同安装之间，特洛伊木马下载程序的有效载荷可能会不同，因为它是从远程主机/站点获取下载说明。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可能会扫描受感染的计算机来查找银行站点、拍卖站点或在线支付站点的用户名和口令。

恶意软件类型	说明
病毒	病毒是未经您确认就加载到您的计算机上，并且违背您的意愿运行的程序或代码段。
蠕虫	蠕虫是一种程序或算法，会通过计算机网络进行自我复制，通常执行恶意操作。

搜索第 4 层流量监控器处理的事务

Web 跟踪搜索 (Web Tracking Search) 页面上的“第 4 层流量监控器”(Layer 4 Traffic Monitor) 选项卡提供有关与恶意软件站点和端口连接的详细信息。您可以通过以下信息类型搜索至恶意软件站点的连接：

- 时间范围
- 发起该事务的计算机的 IP 地址（IPv4 或 IPv6）
- 目标网站的域或 IP 地址（IPv4 或 IPv6）
- 端口
- 与组织中的计算机相关联的 IP 地址
- 连接类型
- 处理连接的网络安全设备

查看有问题站点或处理事务的网络安全设备的主机名，请点击“目标 IP 地址 (Destination IP Address)”列标题中的“显示详细信息 (Display Details)”链接。

有关如何使用此信息的更多信息，请参阅“第 4 层流量监控器”(Layer 4 Traffic Monitor) 页面，第 38 页。

搜索 SOCKS 代理处理的事务

您可以搜索符合多个条件的事务，包括已阻止事务或已完成事务；发起该事务的客户端计算机的 IP 地址；目标域、IP 地址或端口。您还可以按自定义 URL 类别、匹配的策略以及用户位置（本地或远程）来过滤结果。不支持 IPv4 和 IPv6 地址。

步骤 1 在安全管理设备上，从下拉列表中选择**网络 (Web)**。

步骤 2 选择**跟踪 > SOCKS 代理**。

步骤 3 要查看所有搜索和过滤选项，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件。

步骤 5 点击**搜索 (Search)**。

下一步做什么

相关主题

SOCKS 代理报告 ， 第 30 页

处理 Web 跟踪搜索结果

显示更多 Web 跟踪搜索结果

步骤 1 请务必查看所返回结果的全部页面。

步骤 2 要在每页显示比当前数量更多的结果，请在**显示的项目数 (Items Displayed)** 菜单中选择一个选项。

步骤 3 如果与您的条件匹配的事务数多于“显示的项数”(Items Displayed) 菜单中提供的最大事务数，您可以单击**可打印的下载 (Printable Download)** 链接以获取一个包含所有匹配事务的 CSV 文件，从而可以查看全部结果。

此 CSV 文件包括原始数据的完整集合，不包括相关事务的详细信息。

了解 Web 跟踪搜索结果

默认情况下，结果是按时间戳排序，最近的结果显示在顶部。

搜索结果包括：

- 访问 URL 的时间。
- 用户发起的事务所引发的相关事务数，例如，加载的图像、JavaScript 运行和访问的辅助站点等。相关事务的数量会显示在列标题中“显示所有详细信息”(Display All Details) 链接下的每行中。
- 处理（事务的结果。如果适用，显示事务被阻止、被监控或被警告的原因。）

查看 Web 跟踪搜索结果的事务详细信息

要查看	相应操作
列表中被截断 URL 的完整的 URL	注意哪些主机网络安全设备处理了事务，然后检查该设备上的 Accesslog。

要查看	相应操作
单个事务的详细信息	点击“网站”(Website) 列中的 URL。
所有事务的详细信息	点击“网站”(Website) 列标题中的**显示所有详细信息... (Display All Details...)** 链接。
最多包含 500 个相关事务的列表	相关事务的数量会显示在搜索结果列表的列标题中的“显示详细信息”(Display Details) 链接下的括号中。 点击事务详细信息视图中的**相关事务 (Related Transactions)** 链接。

关于 Web 跟踪和高级恶意软件防护功能

当在“Web 跟踪”(Web Tracking) 中搜索文件威胁信息时，请记住以下要点：

- 要搜索文件信誉服务找到的恶意文件，请针对 Web 跟踪的“高级”(Advanced) 部分中恶意软件威胁区域的**按恶意软件类别过滤 (Filter by Malware Category)** 选项选择**已知恶意软件和高风险文件 (Known Malicious and High-Risk Files)**。
- Web 跟踪仅包括文件信誉处理以及在处理事务时返回的初始文件信誉判定的相关信息。例如，如果最初发现文件是干净文件，然后判定更新发现文件是恶意文件，则只有干净的判定显示跟踪结果中。

  搜索结果中的“阻止 - AMP”(Block - AMP) 意味着由于文件的信誉判定而阻止该事务。

  在跟踪详细信息中，“AMP 威胁评分”是当云信誉服务无法判定某个文件正常时所能提供的最佳得分。在这种情况下，得分介于 1 和 100 之间。（如果返回了 AMP 判定，或者得分为零，请忽略 AMP 威胁评分。）设备会将此得分与阈值得分（在“安全服务”[Security Services] > “防恶意软件和信誉”[Anti-Malware and Reputation] 页面上配置）进行比较，以确定所需采取的操作。默认情况下，得分介于 60 到 100 之间的文件会被视为恶意文件。思科不建议更改默认阈值得分。WBRS 得分是从中下载文件的站点的信誉；此得分与文件信誉无关。
- 判定更新仅在 AMP 判定更新报告中可用。Web 跟踪中的初始事务详细信息不会随判定更改而更新。要涉及特定文件的事务，请在判定更新报告中点击 SHA-256。
- 有关文件分析的信息（包括分析结果以及是否发送文件进行分析）仅在文件分析报告中可用。

  有关已分析的文件的其他信息，可从云端获取。要查看文件的任何可用的文件分析信息，请依次选择**报告 (Reporting) > 文件分析 (File Analysis)** 并输入 SHA-256 以搜索该文件，或点击 Web 跟踪详细信息中的 SHA-256 链接。如果文件分析服务已分析任何源中的文件，则可以查看详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了已发送的待分析文件的后续实例，则这些实例将显示在“Web 跟踪”(Web Tracking) 搜索结果中。

相关主题

- 通过 SHA-256 散列标识文件 , on page 22

关于 Web 跟踪和升级

新的 Web 跟踪功能可能不适用于在升级之前发生的事务，因为可能没有为这些事务保留所需的数据。有关与 Web 跟踪和升级相关的可能限制，请参阅您的版本的发行说明。

解决 Web 报告和跟踪问题

另请参阅对所有报告进行故障排除。

集中报告已正确启用，但不工作

问题

已按照指示启用了集中 Web 报告功能，但这不起作用。

解决方案

如果没有为报告分配磁盘空间，则集中 Web 报告不起作用，直到分配磁盘空间。只要您为 Web 报告和跟踪设置的配额大于当前使用的磁盘空间，您就不会丢失任何 Web 报告和跟踪数据。有关详细信息，请参阅管理磁盘空间。

高级恶意软件保护判定更新报告结果存在差异

问题

网络安全设备和邮件安全设备发送同一文件进行分析，而网络和邮件的 AMP 裁定更新报告针对该文件显示不同的裁定。

解决方案

这种情况是暂时的。下载了所有判定更新后，结果便会匹配。实现匹配最多需要 30 分钟。

查看文件分析报告详细信息的问题

文件分析报告详细信息不可用

问题

文件分析报告详细信息不可用。

解决方案

请参阅文件分析报告详细信息的要求 , on page 21。

查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”报告详细信息时，出现没有可用的云服务器配置错误。

解决方案

转到**管理设备** > **集中服务** > **安全设备**，然后添加至少一个启用了分析功能的网络安全设备。

使用私有云 Cisco AMP Threat Grid 设备查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”(File Analysis) 报告详细信息时，出现 API 密钥、注册或激活错误。

解决方案

如果您使用私有云（本地部署的）Cisco AMP Threat Grid 设备进行文件分析，请参阅（本地文件分析）激活文件分析账户 , on page 22。

如果 Threat Grid 设备主机名发生更改，您必须重复执行所引用操作程序中的流程。

在报告或跟踪结果中缺少预期的数据

问题

报告或跟踪结果中缺少预期数据。

解决方案

可能的原因：

- 确保您选择了所需的时间范围。
- 对于跟踪结果，请确保您正在查看所有匹配的结果。请参阅显示更多 Web 跟踪搜索结果 , on page 78。
- 网络安全设备和思科 安全邮件和 Web 管理器设备之间的数据传输可能已被中断，或者数据可能已被清除。请参阅“数据可用性”(Data Availability) 页面, on page 33。
- 如果升级更改了报告或跟踪信息的方式，则在升级前发生的事务可能不会按预期呈现。要查看您的版本是否具有此类更改，请参阅文档中指定的您的版本的发行说明。
- 对于网络代理服务跟踪搜索结果中缺少的结果，请参阅搜索网络代理服务处理的事务 , on page 68。

- 对于按用户请求的事务过滤时出现的意外结果，请参阅搜索网络代理服务处理的事务 , on page 68中表的“用户请求”(User Request) 行。

PDF 仅显示网络跟踪数据的子集

问题

PDF 仅显示在“Web 跟踪”(Web Tracking) 页面上可见的一些数据。

解决方案

有关要包含在 PDF 和 CSV 文件中以及从其中省略的数据的信息，请参阅并导出报告和跟踪数据中相应表格的网络跟踪信息。

解决第 4 层流量监控器报告问题

如果网络代理配置为转发代理，并且第 4 层流量监控器设置为监控所有端口，则代理的数据端口的 IP 地址会记录并显示为报告中的客户端 IP 地址。如果网络代理配置为透明的代理，请启用 IP 欺骗以正确地记录和显示客户端 IP 地址。为此，请参阅《IronPort AsyncOS for Web 用户指南》。

相关主题

- 客户端恶意软件风险报告 , on page 25
- 搜索 L4 流量监控器处理的事务 , on page 72

导出的 .CSV 文件与网络界面数据不同

问题

导出到 .csv 文件的“匹配的域”(Domains Matched) 数据与网络界面中显示的数据不同。

解决方案

出于性能原因，系统仅将前 300,000 个条目导出为 .csv。

导出 Web 跟踪搜索结果时的问题

问题

在同时运行多个大型搜索查询时，网络跟踪搜索结果会显示“内存不足”(Out of Memory) 错误。

解决方案

要解决此问题，您可以将内存的堆大小增加到 1024 MB 或更大，或者缩小搜索条件的时间范围。请记住，增加内存的堆大小可能会导致内存相关问题。

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。