连接日志记录

以下主题介绍如何配置 Firepower 系统以记录由受监控网络上的主机进行的连接：

关于连接日志记录

系统可以生成其托管设备检测到的连接的日志。这些日志称为连接事件。规则和策略中的设置可供您精细控制记录的连接、记录连接的时间以及存储数据的位置。特殊连接事件称为 安全相关的连接事件，代表被基于信誉的安全情报功能阻止的连接。

连接事件包含关于检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等
- 有关连接记录原因的元数据：哪个配置处理流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等

根据您的组织的安全和合规性需求记录连接。设置连接日志记录时，请记住：系统可能会因为多种原因记录连接，禁用某一处的日志记录并不意味着不会记录匹配连接。

连接事件中的信息取决于多种因素，包括流量特征、最终处理连接的配置等。

注释 您可以用导出的 NetFlow 记录生成的连接数据补充您的受管设备收集的连接日志。这在受管设备无法监控的网络上部署支持 NetFlow 的路由器或其他设备时尤为有用。

始终记录的连接

除非禁用连接事件存储，否则系统会将以下连接结束事件自动保存到 防火墙管理中心数据库，不考虑任何其他日志记录配置。

与入侵关联的连接

除非通过访问控制策略的默认操作来处理连接，否则系统会自动记录与入侵事件关联的连接。

当与访问控制默认操作关联的入侵策略生成入侵事件时，系统不会自动记录相关连接终止事件。相反，您必须明确启用默认操作连接日志记录。对于不想记录任何连接数据的仅入侵防御部署，这十分有用。

不过，如果您为默认操作启用连接开始日志记录，除了记录连接开始事件，系统会在关联的入侵策略触发时记录连接结束事件。

与文件和恶意软件事件关联的连接

系统会自动记录与文件和恶意软件事件关联的连接。

注释 检查 NetBIOS-SSN (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。

与智能应用绕行关联的连接

系统会自动记录与 IAB 关联的已绕行和将绕行的连接。

受监控连接

系统始终记录受监控流量的连接结束事件，即使流量与其他规则都不匹配且您没有启用默认操作日志记录。有关详细信息，请参阅受监控连接的日志记录，第 4 页。

您可以记录的其他连接

要仅记录关键连接，可以逐条规则启用连接日志记录。如果为某条规则启用连接日志记录，则系统会记录该规则处理的所有连接。

您还可以记录策略默认操作处理的连接。根据规则或默认策略操作（以及针对访问控制的规则检查配置），您的日志记录选项可能有所不同。

预过滤器策略：规则和默认操作

您可以记录您通过预过滤器策略使用快速路径或进行阻止的连接（包括整个明文、传递隧道）。

预过滤使用外部报头条件处理流量。对于您记录的隧道，生成的连接事件包含来自外部封装报头的信息。

对于需要接受进一步分析的流量，预缩率策略中的日志记录功能已禁用，但匹配连接可能仍然被其他配置记录下来。系统会使用内部报头执行所有进一步的分析，也就是说，系统单独处理并记录允许隧道内的每个连接。

解密策略：规则和默认操作

您可以记录匹配 解密规则或解密策略 默认操作的连接。

对于受阻连接，系统会立即结束会话并生成事件。对于受监控连接以及您将其传递到访问控制规则的连接，系统会在会话结束时生成事件。

访问控制策略：安全智能决策

只要基于信誉的安全智能功能阻止连接，您就可以对该连接进行日志记录。

或者，您可以像被动部署中建议的那样，使用仅监控设置进行安全智能过滤。这使得系统可以进一步分析本应被安全智能组织的连接，并仍将记录匹配项。安全智能监控还允许您使用安全智能信息创建流量配置文件。

当系统由于安全智能过滤而记录连接事件时，它也会记录匹配的安全智能事件，这是一种您可以单独查看和分析的特殊类型连接事件，而且可以单独存储和删除。因此，您可以确定连接中匹配的 IP 地址，列入受阻止和受监控的 IP 地址旁边的主机图标在**事件和日志** > **+ 显示更多** > **连接** > **事件**菜单下的页面上的表格中看上去稍有不同。

访问控制策略：规则和默认操作

您可以记录匹配访问控制规则或访问控制策略默认操作的连接。

相关主题

规则和策略操作如何影响日志记录 ，第 3 页

规则和策略操作如何影响日志记录

连接事件包含有关连接记录原因的元数据，包括哪些配置处理流量。配置连接日志记录时，规则操作和策略默认操作不仅可以确定系统如何检查和处理匹配流量，而且可以确定您何时及如何记录匹配流量的相关详细信息。

相关主题

连接和 安全相关连接 事件字段

快速路径连接的日志记录

您可以记录快速路径连接和非加密隧道，其包括与预过滤器策略中的以下规则和操作匹配的流量：

- 隧道规则 - **快速路径 (Fastpath)** 操作（记录外部会话）
- 预过滤器规则 - **快速路径 (Fastpath)** 操作

快速路径流量会绕过其余访问控制和 QoS，因此快速路径连接的连接事件包含的信息是有限的。

受监控连接的日志记录

系统始终记录与以下配置匹配的流量的连接结束事件，即使流量与其他规则都不匹配且您没有启用默认操作日志记录：

- 安全智能 - 阻止列表设为监控（也生成安全智能事件）
- SSL 规则 - **监控 (Monitor)** 操作
- 访问控制规则 - **监控 (Monitor)** 操作

系统不会在每次单个连接匹配“监控”(Monitor) 规则时都成一个单独的事件。由于单一连接可能与多条“监控”(Monitor) 规则相匹配，每个连接事件均可能包含和显示关于该连接匹配的前八条监控访问控制规则，以及第一条匹配的 SSL 监控规则的信息。

同样，如果您将连接事件发送至外部系统日志或 SNMP 陷阱服务器，则每当单一连接与监控规则相匹配时，系统均不会发送单独的警报。相反，系统在连接终止时发送的警报包含有关连接匹配的监控规则的信息。

受信任连接的日志记录

您可以记录受信任连接的开始和结束，包括匹配以下规则和操作的流量：

- 访问控制规则 - **信任 (Trust)** 操作
- 访问控制默认操作 - **信任所有流量 (Trust All Traffic)**

注释 虽然您可以记录受信任的连接，但是建议不要这样做，因为受信任的连接不会受到深入检查或发现，因此受信任连接的连接事件包含的信息有限。

信任规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统将在最终会话数据包发送完毕 1 小时后生成事件。

受阻连接的日志记录

您可以记录受阻连接，这包括与以下规则和操作匹配的流量：

- 隧道规则 - **阻止 (Block)**
- 预过滤器规则 - **阻止 (Block)**
- 预过滤器默认操作 - **阻止所有隧道流量 (Block all tunnel traffic)**
- 安全智能 - 阻止列表勿设为监控（也生成安全智能事件）
- 解密规则—**阻止** 和 **阻止并重置**
- SSL 默认操作 - **阻止 (Block)** 和**阻止并重置 (Block with reset)**
- 访问控制规则 - **阻止 (Block)**、**阻止并重置 (Block with reset)** 和**交互式阻止 (Interactive Block)**

- 访问控制默认操作 - **阻止所有流量 (Block All Traffic)**

仅内联部署的设备（即使用已路由、已交换或透明接口或内联接口对）可以阻止流量。因为阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。

注意 Firewall Threat Defense 设备会记录三向握手未完成的 TCP 连接的连接结束事件，包括仅 SYN、SYN-SYN/ACK（无 ACK）和 SYN-RST/ACK 场景（启用 TLS 身份时除外））。通过这些日志，可以了解不完整或可疑的连接尝试。但是，在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口上的流量。

受阻连接的连接开始和连接结束的日志记录

当您记录受阻连接时，系统如何进行记录该连接取决于其受阻原因；当根据连接日志配置关联规则时，必须记住这一点：

- 对于阻止已加密流量的 SSL 规则和 SSL 策略 默认操作，系统记录连接 **结束**事件。这是因为系统无法确定连接是否使用会话中的第一个数据包加密。
- 对于其他阻止操作，系统会记录连接**开始**的事件。匹配流量会被拒绝，无需进一步检测。

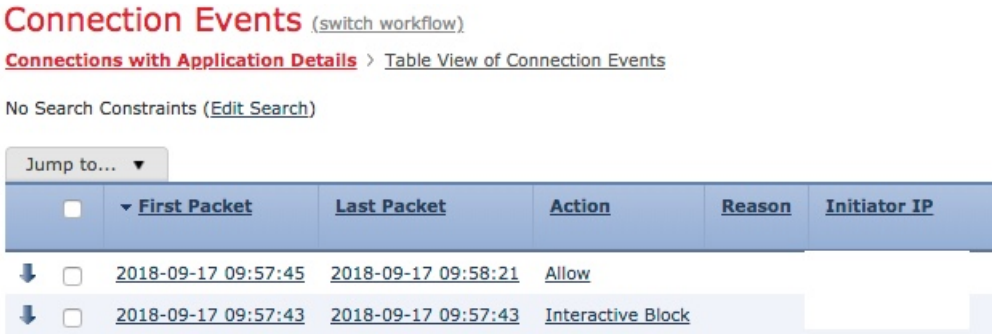
绕行交互式阻止的日志记录

当用户浏览受禁网站时，交互式阻止访问控制规则导致系统显示警告页面，该等规则可供您配置连接结束日志记录。这是因为，如果用户点击浏览警告页面，该连接会被视为系统可以监控和记录并且允许访问的新连接。

因此，对于与“交互式阻止”或“交互式阻止并重置”规则匹配的数据包而言，系统可以生成以下连接事件：

- 用户的请求最初被阻止且显示警告页面时的连接开始事件；该事件的关联操作为交互式阻止或交互式阻止并重置
- 当用户点击警告页面并加载最初请求的页面时生成的多个连接开始或连接结束事件；这些事件的关联操作为允许，原因为用户绕行

  下图显示交互式阻止以及允许操作的示例。



允许连接的日志记录

您可以记录允许连接，这包括与以下规则和操作匹配的流量：

- SSL 规则 - **解密 (Decrypt)** 操作
- SSL 规则 - **不解密 (Do not Decrypt)** 操作
- SSL 默认操作 - **不解密 (Do not Decrypt)**
- 访问控制规则 - **允许 (Allow)** 操作
- 访问控制默认操作 - **仅限网络发现 (Network Discovery Only)** 以及任何入侵防御选项

为这些配置启用日志记录可确保连接已记录，同时也允许（或指定）下一阶段的检查和流量处理。SSL 日志记录始终在连接结束时进行；访问控制配置也允许在连接开始时进行日志记录。

虽然隧道和预过滤器规则中的**分析 (Analyze)** 操作也允许连接继续进行访问控制，但禁用进行此操作的规则的日志记录。匹配连接仍然可由其他配置进行记录。允许的隧道可能会对封装会话进行单独评估和记录。

当您通过访问控制规则或默认操作允许流量时，可以使用相关入侵策略进一步检查流量和阻止入侵。对于访问控制规则，您也可以使用文件策略检测和阻止被禁止的文件，包括恶意软件。除非禁用连接事件存储，否则系统将自动记录大多数与入侵、文件和恶意软件事件关联的允许连接。有关详细信息，请参阅始终记录的连接，第 2 页。

具有加密负载的连接不进行深度检查，因此加密连接的连接事件包含的信息有限。

允许连接的文件和恶意软件事件日志记录

当文件策略检测或阻止文件时，它会将以下事件之一记录到 防火墙管理中心数据库：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件。
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件。
- 可追溯的恶意软件事件，在之前检测到的文件的恶意软件处置变更时生成。

您可以以每个访问控制规则为基础禁用此日志记录。您还可以完全禁用文件和恶意软件事件存储。

注释 建议您将文件和恶意软件事件日志记录保持启用状态。

连接开始和连接结束日志记录

您可以在连接开始或结束时记录该连接，对于受阻流量，下列情况除外：

- 受阻流量 - 由于会立即拒绝受阻流量而不进一步检查，因此通常您只能记录受阻流量的连接开始事件。没有要记录的唯一连接结束。

- 受阻加密流量 - 当在 解密策略中启用连接日志记录时，系统会记录连接结束而不是连接开始事件。这是因为，系统无法确定连接是否使用会话中第一个数据包加密，因此无法立即阻止已加密会话。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。出于任何原因监控连接都会强制执行连接结束日志记录。对于单个未被阻止的连接，连接终止事件包含连接开始事件中的所有信息，以及在会话期间收集到的信息。

下表详细列出了连接开始和连接终止事件之间的差异，包括相比于记录每种事件的优势。

表 *1:* 比较连接开始和连接结束事件

	连接开始事件	连接结束事件
生成时间…	当系统检测到连接开始（或者在前几个数据包之后，如果事件生成取决于应用或 URL 识别）。	当系统： • 检测到连接关闭。 • 在一段时间后未检测到连接结束。 • 由于内存限制，无法再跟踪会话。
记录对象...	除受到 解密策略阻止以外的所有连接。	大多数连接。
包含...	仅在第一个数据包中可以确定的信息（或者前几个数据包，如果事件生成取决于应用或 URL 识别）。	连接开始事件中的所有信息，以及通过在会话期间检查流量确定的信息；例如，传输的数据总量或连接中最后一个数据包的时间戳。 **注释** 如果威胁防御系统对连接返回 snort 判定，或者您对连接进行了快速路径连接，则连接事件不会计算传输的数据量。
十分有用…	如果您要记录： • 阻止的连接。 • 仅连接的开始，因为连接结束信息对您无关紧要。	如果要： • 被 解密策略处理的日志加密连接。 • 使用在会话期间收集的信息执行任何类型的详细分析或者触发关联规则。 • 查看自定义工作流程中的连接摘要（汇聚连接数据），查看图形格式的连接数据，或者创建并使用流量量变曲线。

Secure Firewall Management Center 与外部日志记录

如果您在 防火墙管理中心上存储连接和安全情报事件日志，则可以使用 Firepower 系统的报告、分析和数据关联功能。例如：

- 控制面板和情景管理器为您提供由系统记录的连接的图形化概览视图。
- 事件视图（大多数选项在“分析”菜单下提供）显示有关系统记录的连接的详细信息，您可以用图形或表格格式显示这些信息，也可以在报告中将其汇总。
- 流量分析使用连接数据创建正常网络流量的配置文件，然后您可以将其用作检测和跟踪异常行为的基准。
- 通过关联策略，您可以生成事件并触发对特定类型的连接或流量量变曲线更改的响应（例如警报或外部补救）。

防火墙管理中心可以存储的事件数取决于其型号。

注释 要使用这些功能，**必须**记录连接（而且在大多数情况下，必须记录连接结束而非开始事件）。这就是为什么系统自动记录关键连接，即与记录的入侵、受禁文件和恶意软件关联的那些链接。

您还可以使用以下工具将事件记录到外部系统日志或 SNMP 陷阱服务器或其他外部工具：

- 对于任何设备上的外部日志记录：

  您配置的连接称为 警报响应。

- 对于 Firewall Threat Defense 设备上的外部日志记录：

  请参阅了解配置系统日志和在*Cisco Secure Firewall Management Center* 设备配置指南中配置 *SNMP* 陷阱的相关信息。

- 有关与外部日志记录相关的其他选项：

  请参阅使用外部工具的事件分析。

相关主题

使用告警响应配置外部告警

连接日志记录的限制

无法记录：

- 其封装连接由访问控制检查的明文、传递隧道的外部会话。
- 未完成三次握手的 TCP 连接，以避免针对防火墙的拒绝服务攻击。要监控或调试失败的连接，可以使用 **show asp drops** CLI 命令或数据包捕获功能 (数据包捕获概述)。

如果某个连接事件不包含您认为其应包含的信息，请参阅填充连接事件字段的要求和连接事件字段中的可用信息。

当事件显示在事件查看器中时

以下几点适用于所有类型的事件：

- 如果您正在查看“分析”菜单下的页面，则必须刷新页面以显示新事件。
- 事件通常在检测到流量后几秒钟内即可查看。但是，在以下情况下可能会出现任意延迟：FMC 正在管理低带宽网络上的许多设备；或在暂停事件处理的操作（例如事件备份）期间。
- 根据定义的规则记录的所有连接事件都显示在事件查看器中。用于过滤事件的选项不适用于连接事件的统一日志记录。

连接日志记录最佳实践

使用以下最佳实践确保仅记录要记录的连接。

因此，仅记录关键连接，在每个访问控制规则的基础上启用连接日志记录。

始终记录的连接

系统将自动记录以下连接：

- 一些与检测到的文件、恶意软件、入侵和智能应用绕行 (IAB) 关联的连接。

  有关详细信息，请参阅始终记录的连接，第 2 页。

- 受监控连接。

  有关详细信息，请参阅受监控连接的日志记录，第 4 页。

永远不会记录的连接

请勿启用以下各项的日志记录：

- 访问控制规则与信任操作。

  受信任的连接不会受到深入检查或发现，因此受信任连接的连接事件包含的信息有限。

- 请勿在被动部署中启用“阻止”规则的日志记录。要记录在内联部署设备时系统将阻止的连接，请使用“监控”规则而不是“阻止”规则。

  仅内联部署的设备（即使用已路由、已交换或透明接口或内联接口对）可以阻止流量。因为阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。

- 不感兴趣的流量。示例如下：
  - 特定的允许流量，例如对可信 DNS 主机的 DNS 请求。
  - 与服务产品无关的基础设施流量。

  （如前所述，您仍然可以监控此流量是否存在威胁。）

如始终记录的连接，第 2 页中所讨论的，即使禁用了上述各项的日志记录，仍然会记录入侵事件、恶意软件和 IAB。

避免记录将在其他位置记录的内容

如果其他设备或服务正在记录网段的连接数据，请在 防火墙管理中心中禁用该网段数据的日志记录。示例如下：

- 如果路由器在与 防火墙管理中心相同的网段上记录连接事件，请避免记录 防火墙管理中心 上的相同连接，除非您需要将连接事件用于其他用途，例如关联策略或流量配置文件。

  有关关联策略的详细信息，请参阅关联策略和规则简介。有关流量配置文件的详细信息，请参阅流量量变曲线简介。

- 如果使用 Cisco Secure Network Analytics 以利用交换机和路由器报告的 NetFlow 记录来识别潜在的行为异常和可疑流量模式，则可以禁用监控这些网段的规则的连接日志记录，依靠Cisco Secure Network Analytics 对网络的这些部分进行行为分析。

  有关详细信息，请参阅Cisco Secure Network Analytics 文档。

记录连接的开始或结束（并非两者）

如果可以在连接开始或结束日志记录之间进行选择，请启用连接结束日志记录。这是因为连接结束记录连接开始事件的信息以及在会话期间收集的信息。

仅当要记录被阻止的连接或连接结束信息对您无关紧要时，才记录连接开始。

有关详细信息，请参阅连接开始和连接结束日志记录，第 6 页。

受阻流量的日志记录

因为受阻流量会被立即拒绝，无需进一步检查，因此您可以仅记录连接开始事件。

有关详细信息，请参阅受阻连接的日志记录，第 4 页。

将事件记录到外部位置

如果您的公司的安全策略允许，您可以使用以下任意一项将日志传输到外部源，从而节省 防火墙管理中心 的磁盘空间：

- eStreamer，可以让您将日志从 防火墙管理中心 传输到自定义开发的客户端应用。有关详细信息，请参阅《*Cisco Secure Firewall Management Center* 事件流传输器集成指南》《》。

  您可以集成 Splunk 服务器，以直接从 防火墙管理中心 或其受管设备接收事件。有关 Splunk 配置程序的详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南文档。

- 系统日志或 SNMP 陷阱，称为警报响应。有关详细信息，请参阅使用告警响应配置外部告警。

指定事件记录的最大数量

考虑可以存储在数据库中的最小和最大记录数量。例如，虚拟 防火墙管理中心 最多可以存储 5000 万个连接事件。此外，其他事件类型具有其各自的可配置限制。转到 **管理** > **配置** > **数据库** 调整这些限制，以满足您的存储和性能需求。

有关所有 防火墙管理中心 型号及其事件数据库大小的列表，请参阅数据库事件限制。

控制连接事件中显示的内容

要指定连接事件中显示的行数，请点击 防火墙管理中心 右上角的用户名，然后点击**用户首选项 (User Preferences)**事件视图设置 **(Event View Settings)**。 可以设置的最大值是每页 1000 个事件。

设置连接事件报告

为确保不会错过连接事件，可以设置 .csv 格式的自动报告，并可选择安排以固定的时间间隔生成报告。有关详细信息，请参阅：

- 要创建报告模板，请点击 **事件和日志** > **+ 显示更多** > **连接** > **事件** ，然后从事件视图页面中，点击 **创建报告 (Create Report)**。有关详细信息，请参阅从事件视图创建报告模板。
- 计划任务 (**管理** > **高级** > **计划**)：关于任务安排。

连接日志记录的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置连接日志记录

以下各部分介绍如何设置连接日志记录以匹配各种规则和条件。

使用隧道和预过滤器规则记录连接

预过滤器策略仅适用于 Cisco Secure Firewall Threat Defense 设备。

开始之前

- 将规则操作设置为**阻止 (Block)** 或**快速路径** （**Fastpath**）。对于**分析 (Analyze)** 操作，记录已被禁用，这可以让连接继续接受访问控制的检查，由其他配置来确定其处理和记录。
- 日志记录在内部流上执行，而不是在封装流上执行。

过程

步骤 1 在预过滤策略编辑器中，点击要在其中配置记录的规则旁边的 **编辑** ( ) 。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 点击**日志记录 (Logging)**。

步骤 3 指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。因为阻止的流量会被立即拒绝而无需进一步检查，所以只能记录“阻止”(Block) 规则的连接结束事件。

步骤 4 指定将连接事件发送至何处：

步骤 5 点击**保存** 保存规则。

步骤 6 点击**保存** 以保存预过滤策略。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

使用TLS/SSL解密规则记录可解密连接

过程

步骤 1 在 解密策略 编辑器中，点击要在其中配置记录的规则旁边的 **编辑** ( ) 。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 点击 **日志记录**。

步骤 3 选中**在连接结束时进行日志记录 (Log at End of Connection)** 复选框。

对于受监控流量，需要连接结束日志记录。

步骤 4 指定将连接事件发送至何处。

如果要对这些连接事件执行基于 防火墙管理中心的分析，请将事件发送到事件查看器。对于受监控流量，需要执行此操作。

步骤 5 点击**保存** 保存规则。

步骤 6 点击**保存**以保存解密策略。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

使用安全智能记录连接

安全智能策略需要威胁智能许可证。

过程

步骤 1 在访问控制策略编辑器中，点击**安全智能 (Security Intelligence)**。

步骤 2 点击 **日志记录**（ ） 图标以使用以下条件启用安全智能日志记录：

- 按 IP 地址 - 点击**网络 (Networks)** 旁边的日志记录图标。
- 按 URL - 点击 **URL** 旁边的日志记录图标。
- 按域名 - 点击 **DNS 策略 (DNS Policy)** 下拉列表旁边的日志记录图标。

如果日志记录图标被禁用，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 选中**记录连接 (Log Connections)** 复选框。

步骤 4 指定要将连接和 安全相关的连接事件发送到何处。

如果要执行基于 防火墙管理中心 的分析，或者如果要将列入阻止名单为仅监控，请将事件发送到事件查看器。

步骤 5 点击**确定** 以设置日志记录选项。

步骤 6 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

使用访问控制规则记录连接

根据您选择的规则操作和深度检查选项，您的日志记录选项会有所不同；请参阅规则和策略操作如何影响日志记录，第 3 页。

过程

步骤 1 在访问控制策略编辑器中，点击要配置日志记录的规则旁边的 **编辑** ( )。

如果显示**视图** ( )，则表明配置继承自祖先策略或属于祖先域，或者您没有修改配置的权限。

步骤 2 点击**日志记录 (Logging)**。

步骤 3 指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。

步骤 4 （可选）选中**记录文件 (Log Files)** 复选框以记录与连接关联的文件和恶意软件事件。

建议启用此选项。

步骤 5 指定将连接事件发送至何处：

- **事件查看器**：将事件发送到防火墙管理中心。使用云管理时，将事件发送到云交付防火墙管理中心 和本地 防火墙管理中心 （如果已将其配置为仅执行事件分析）。您可以在任一产品的事件查看器中查看事件。
- **系统日志服务器**：将连接事件发送到访问控制策略的“日志记录”选项卡中配置的系统日志服务器，除非被覆盖。

  显示覆盖：显示可覆盖访问控制策略中配置的设置的选项。

  - **覆盖严重性**：选择此选项并为规则选择严重性时，此规则的连接事件将具有所选择的严重性，而与在访问控制策略的“日志记录”选项卡中配置的严重性无关。
  - **覆盖默认系统日志目标**：将为此规则的连接事件生成的系统日志发送到此警报中指定的目标。

- **SNMP 陷阱**：连接事件发送到所选的 SNMP 陷阱。

步骤 6 点击 **Confirm**。

步骤 7 点击**应用**以保存规则。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

使用策略默认操作记录连接

策略的默认操作确定系统如何处理与策略中所有规则均不匹配的流量（访问控制和 解密策略中的“监控”规则除外，这些规则匹配和记录流量，但不处理或检测流量）。

解密策略 默认操作的记录设置还监管系统如何记录无法解密的会话。

开始之前

- 对于预过滤器默认操作日志记录，请将默认操作设置为**阻止所有隧道流量 (Block all tunnel traffic)**。对于**允许所有隧道流量 (Allow all tunnel traffic)** 操作，日志记录已被禁用，这可以让连接继续接受访问控制的检查，由其他配置来确定其处理和记录。

过程

步骤 1 在策略编辑器中，点击**默认操作 (Default Action)** 下拉列表旁边的 **默认日志记录和检查** 。

步骤 2 指定要记录匹配连接的时间：

- “在连接开始时记录”(Log at Beginning of Connection) - SSL 默认操作不支持。
- “在连接结束时记录”(Log at End of Connection) - 如果选择访问控制**阻止所有流量 (Block All Traffic)** 默认操作或预过滤**阻止所有隧道流量 (Block all tunnel traffic)** 默认操作，则不受支持。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。 在访问控制策略中，也可从祖先策略继承配置。

步骤 3 指定将连接事件发送至何处。

如果要对这些连接事件执行基于 防火墙管理中心的分析，请将事件发送到事件查看器。

步骤 4 点击**应用 (Apply)**。

步骤 5 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

限制长 URL 的日志记录

HTTP 流量的连接结束事件会记录受监控主机所请求的 URL。禁用或限制存储的 URL 字符数可提高系统性能。禁用 URL 日志记录（存储零字符）不会影响 URL 过滤。尽管系统不会记录流量，但会根据请求的 URL 过滤流量。

过程

步骤 1 在访问控制策略编辑器中，点击**更多 (More)** > **高级设置 (Advanced Settings)**，然后点击**常规设置 (General Settings)** 旁边的 **编辑** (✎)。

如果显示**视图** (👁)，则表明配置继承自祖先策略或属于祖先域，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 输入**要在连接事件中存储的最大 URL 字符数 (Maximum URL characters to store in connection events)**。

步骤 3 点击**确定**。

步骤 4 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

应用感知和协议感知系统日志

应用程序日志记录选项使您能够生成包含应用程序和协议特定流量数据的事件，并通过全面的数据收集提供增强的网络可视性。 Firewall Threat Defense 设备会在现有连接、入侵、文件和恶意软件事件旁边生成这些日志。您可以将这些日志作为系统日志发送到外部事件管理解决方案进行分析。应用日志记录使用 Snort 3 引擎的深度数据包检查功能来提取协议数据。它提供了一个可配置的解决方案，用于将这些日志从 Firewall Threat Defense 设备发送到目的地，例如 Splunk 或系统日志警报服务器。

高级日志记录协议

高级日志记录支持这些协议。

表 *2:* 高级日志记录的协议列表

协议 (Protocol)	说明
CONN	记录从连接结束事件收集的数据，包括传输协议、服务协议和会话持续时间。
DNS	记录从对 TCP 和 UDP DNS 会话的响应中收集的数据，包括命令、命令的参数以及应答代码和消息。
FTP	记录 FTP 会话期间交换的命令和数据，包括命令及其参数、应答代码和应答消息。

协议 (Protocol)	说明
HTTP	记录从 HTTP 响应收集的数据，包括 HTTP 方法、报头和状态代码。
通知	记录为入侵事件收集的数据，包括 GID:SID 对、规则消息和关联的引用。
异常	记录在流量中检测到的异常的相关数据。

有关应用程序事件字段的详细信息，请参阅高级日志记录系统日志字段。

高级日志记录的准则和限制

- 如果访问控制规则中没有过滤器，高级日志记录可能会降低网络性能。为减少日志量，请使用访问控制规则作为过滤器，过滤特定流量类型，并通过网络和端口设置将日志记录限制在特定网络配置范围内。
- 为所有协议启用高级日志记录可能会影响 Firewall Threat Defense 设备的性能。选择性地配置高级日志记录，以避免增加设备内存消耗。
- 只有运行 10.0 或更高版本的基于 Snort 3 的 Firewall Threat Defense 设备支持高级日志记录。
- 高级日志记录不支持将日志发送到在平台设置中配置的系统日志服务器。要将事件发送到访问控制策略中配置的默认日志记录目标，您必须将系统日志警报服务器配置为默认日志记录目标。
- 高级日志记录不支持使用数据接口将事件发送到 Splunk 的 Splunk 配置文件。要将事件发送至 Splunk，必须将 Splunk 配置文件配置为使用管理接口发送事件。有关配置 Splunk 配置文件的详细信息，请参阅Splunk 集成：直接从 防火墙管理中心 发送事件。

启用高级日志记录

配置 Firewall Threat Defense 设备，以生成包含应用和协议特定数据的事件日志，并将这些日志发送到事件管理解决方案进行分析。

注意 如果在访问控制规则中没有配置过滤器的情况下使用高级日志记录，则可能会导致网络中的性能下降。使用访问控制规则过滤特定流量类型，以减少记录的流量。使用访问控制规则中的网络和端口，将日志记录限制到特定网络配置。

开始之前

- 确保在访问控制策略中启用了连接日志记录。
- 确保您已配置日志记录目标，例如要向其发送日志的 Splunk 或本地系统日志服务器。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 在访问控制策略编辑器中，从数据包流行末尾的**更多**下拉箭头中选择**高级设置** 。

步骤 4 点击**高级日志记录**旁边的 **编辑** () 图标。

步骤 5 选中**启动高级日志记录**复选框以启用日志记录。

步骤 6 选择目的文件格式。默认情况下，选择 JSON 格式。

步骤 7 您可以将事件日志发送到访问控制策略的日志记录设置中配置的默认日志记录目标，或者发送到以下一个或多个目标：

- **所有 Splunk 配置文件**
- **系统日志**

注释

- 如果选择将事件日志发送到访问控制策略中配置的默认日志记录目标，请注意，高级日志记录不支持将日志发送到平台设置中配置的系统日志服务器。您必须将系统日志警报服务器配置为默认日志记录目标。
- 如果选择 **所有 Splunk 配置文件** 选项，请注意，高级日志会发送到为 Firewall Threat Defense 设备配置的所有 Splunk 配置文件。
- 高级日志记录不支持使用数据接口将事件发送到 Splunk 的 Splunk 配置文件。要将事件发送至 Splunk，必须将 Splunk 配置文件配置为使用管理接口发送事件。

注意
将高级日志记录系统日志发送到多个目标可能会影响设备的性能。

步骤 8 点击**保存**。

步骤 9 点击**保存** 保存策略。

下一步做什么

部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

配置高级日志记录的协议

开始之前

确保已为要修改的访问控制策略启用高级日志记录功能。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 在访问控制策略编辑器中，您有以下选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击 **编辑** (✎)。

步骤 4 点击**高级日志记录**。

步骤 5 选中要为其记录连接的应用协议旁边的复选框。

注意
在 Firewall Threat Defense 设备中为所有协议启用日志记录可能会影响其性能，因为设备必须提取数据、将其转换为目标格式并发送到配置的目的地。

步骤 6 点击 **Confirm**。

步骤 7 点击**应用 (Apply)** 保存规则。

步骤 8 点击**保存** 保存策略。

下一步做什么

部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

监控高级日志记录并排除故障

要收集高级日志记录事件的统计信息并获取运行状况警报，您必须在 Firewall Threat Defense 设备的运行状况策略 (**故障排除** > **+ 显示更多** > **运行状况** > **策略**) 中启用 **Snort 3 统计信息**模块。启用后，您可以监控一些指标，例如被丢弃、发送失败或成功发送的高级日志记录事件的数量。

要查看这些运行状况指标，请导航到 > **运行状况** > **监控器故障排除** ，然后通过从 **Snort 3 性能统计信息**组中选择这些指标来将其添加到控制面板中。

未能将高级日志记录事件传输到系统日志服务器

当系统日志消息由于系统日志服务器的连接问题或配置错误而无法传输时，会显示此警报。

- 检查系统日志服务器的状态，确保其正常运行且可访问。
- 验证 防火墙管理中心 中的系统日志配置是否有错误。

已丢弃到系统日志服务器的高级日志记录事件

当系统日志消息由于 Firewall Threat Defense 设备中的内存溢出而被丢弃时，系统会显示此警报，表明设备无法以当前速率处理日志。

查看您的高级日志记录配置。考虑在访问控制规则中应用更精细的过滤器，以减少生成的日志量，或有选择地为少数协议启用高级日志记录，以减少设备内存消耗。有关详细信息，请参阅高级日志记录的准则和限制，第 17 页。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

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。