加密可视性引擎

加密可视性引擎 (EVE) 用于识别使用 TLS 加密的客户端应用和进程。它支持可视性，并允许管理员在其环境中采取行动并实施策略。EVE 技术还可用于识别和阻止恶意软件。

加密可视性引擎概述

加密可视性引擎 (EVE)用于提供对加密会话的更多可视性，而无需对其进行解密。对 TLS 连接的见解源自思科的开源库，该库包含在思科的漏洞数据库 (VDB) 中。库指纹并分析传入的加密会话，并将其与一组已知指纹进行匹配。已知指纹的数据库在思科 VDB 中也可用。

注释 只有运行 Snort 3 的 防火墙管理中心管理的设备才支持加密可视性引擎功能。Snort 2 设备和防火墙设备管理器受管设备不支持此功能。

EVE 的一些重要功能如下：

- 您可以使用从 EVE 派生的信息对流量执行访问控制策略操作。
- Cisco Secure Firewall 中包含的 VDB 能够以高置信度值将应用分配给 EVE 检测到的某些进程。或者，您可以创建自定义应用检测器，以便：
  - 将 EVE 检测到的进程映射到用户定义的新应用。
  - 覆盖用于将应用分配给 EVE 检测到的进程的进程置信度的内置值。

请参阅 Cisco Secure Firewall Management Center 设备配置指南的**应用检测**一章中的**配置自定义应用检测器**和**指定 EVE 进程分配**部分。

- EVE 可以检测在加密流量中创建客户端 Hello 数据包的客户端的操作系统类型和版本。
- EVE 也支持快速 UDP 互联网连接 (QUIC) 流量的指纹识别和分析。来自客户端 Hello 数据包的服务器名称显示在 **连接事件** 页面的 URL 字段中。

注意 要在 防火墙管理中心上使用 EVE，您的设备上必须具有有效的 IPS 许可证。在没有 IPS 许可证的情况下，策略会显示警告，并且不允许部署。

注释

- EVE 可以检测 SSL 会话的操作系统类型和版本。操作系统的正常使用（例如运行应用、软件包管理软件等）可以触发操作系统检测。要查看客户端操作系统检测，除了启用 EVE 切换按钮，您还必须在 **策略 (Policies)** > **网络发现 (Network Discovery)** 下启用 **主机 (Hosts)** 。要查看主机 IP 地址上可能的操作系统的列表，请点击 **事件和日志** > **主机** > **网络映射**，然后选择所需的主机。
- 为访问控制策略启用 EVE 后，确保已为该策略中的访问控制规则开启日志记录，以便在满足任何特定规则条件时，能在 EVE 控制面板上显示预期结果。有关如何开启日志记录的详细信息，请参阅创建和编辑访问控制规则。
- 从 Cisco Secure Firewall 版本 10.0.0 开始，支持用于 Mercury 检测的 GRE 封装。

EVE 工作原理

加密可视性引擎 (EVE) 检查 TLS 握手的客户端 Hello 部分，以识别客户端进程。客户端 Hello 是发送到服务器的初始数据包。这可以很好地指示主机上的客户端进程。此指纹与其他数据（例如目的 IP 地址）相结合，为 EVE 的应用识别提供基础。通过识别 TLS 会话建立中的特定应用指纹，系统可以识别客户端进程并采取适当的操作（允许/阻止）。

EVE 可以识别 5,000 多个客户端进程。系统将许多此类进程映射到客户端应用，以用作访问控制规则中的条件。这使得系统能够在不启用 TLS 解密的情况下识别和控制这些应用。通过使用已知恶意进程的指纹，EVE 技术还可用于识别和阻止加密的恶意流量，而无需出站解密。

通过机器学习 (ML) 技术，思科每天要处理超过 10 亿个 TLS 指纹和超过 10000 个恶意软件样本，以创建和更新 EVE 指纹。然后，使用思科漏洞数据库 (VDB) 软件包将这些更新交付给客户。

如果 EVE 无法识别某个指纹，它会识别客户端应用，并使用目标详细信息（例如 IP 地址、端口和服务器名称）估算第一个数据流的威胁评分。此时，指纹的状态已随机化，可以在调试日志中查看状态。对于具有相同指纹的后续流，EVE 会跳过重新分析并将指纹状态标记为未标记。

危害事件表现

用于加密可视性引擎检测的主机危害表现(IoC)事件允许您检查恶意软件置信度非常高的连接事件，如 EVE 所报告的那样。使用恶意客户端从主机生成的加密会话会触发 IoC 事件。您可以查看恶意主机的 IP 地址、MAC 地址和操作系统信息等信息，以及可疑活动的时间戳。

如连接事件中所示，加密可视性威胁置信度评分为“非常高”的会话将 IoC 事件类型化。您必须从**策略** > **+ 显示更多** > **内容关联** > **网络发现**启用 **主机** 。在 防火墙管理中心中，您可以从以下位置查看 IoC 事件的存在情况：

- **分析** > **危害表现**。**事件和日志** > **+ 显示更多** > **主机** > **危害指标**
- **事件和日志** > **主机** > **网络映射** >选择必须检查的主机。

  您可以在**连接事件 (Connection Events)** 页面查看产生该 IoC 的会话的进程信息。点击**事件和日志** > **+ 显示更多** > **连接** > **事件**以访问**统一事件**页面。请注意，您必须从“**连接事件表视图**”选项卡中手动选择“加密可见性”字段和“IoC”字段。

  安全相关连接事件 (Security-Related Connection Events) 页面显示 EVE 阻止的连接，以及具有中、高和极高威胁置信度级别的恶意连接。点击 **事件和日志** > **+ 显示更多** > **连接** > **安全相关事件** 访问 “**安全相关的连接事件**” 页面。

EVE 中的 QUIC 指纹识别

Snort 可以根据 EVE 分析识别快速 UDP Internet 连接（QUIC 会话）中的客户端应用程序。QUIC 指纹识别可以：

- 通过 QUIC 检测应用而不启用解密。
- 在不启用解密的情况下识别恶意软件。
- 检测服务应用。您可以根据通过 QUIC 协议检测到的服务分配访问控制规则。

配置 EVE

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** (✎) 。

步骤 3 从数据包流行末尾的**更多**下拉箭头中选择**加密可视性引擎**。

步骤 4 在**加密可视性引擎 (Encrypted Visibility Engine)** 页面中，启用**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮。

步骤 5 选择**监控**模式或**保护**模式。

- 选择**监控**模式以检测客户端应用并监控加密流量。
- 选择**保护**模式可根据客户端进程的威胁置信度级别监控和阻止加密流量。您可以使用此模式在两个威胁置信度级别监控和阻止恶意连接：
  - **高**：使用此级别可阻止威胁置信度级别从高到极高的连接。
  - **非常高**：使用此级别可阻止威胁置信度级别归类为非常高的连接。

步骤 6 点击**保存**，然后部署访问控制策略。

注释
有关管理例外的信息，请参阅配置 EVE 例外规则， 第 6 页。

下一步做什么

部署配置更改。

查看 加密可视性引擎事件

启用**加密可视性引擎 (Encrypted Visibility Engine)** 并部署访问控制策略后，您可以开始通过系统发送实时流量。您可以在**统一事件**页面中查看记录的连接事件。

执行此过程以访问防火墙管理中心中的连接事件。

过程

步骤 1 请点击 **事件和日志** > **分析** > **统一事件**。

您也可以在**连接事件**页面中查看连接事件。点击**事件和日志** > **+ 显示更多** > **连接** > **事件**以访问**统一事件**页面。

此外，您可以使用**与安全相关的连接事件**页面（**分析** > **连接标题** > **安全相关的事件**）查看被 加密可视性引擎阻止的连接，以及具有中、高和非常高威胁置信度级别的恶意连接。

加密可视性引擎可以识别发起连接的客户端进程和客户端中的操作系统，并指示该进程是否包含恶意软件。

步骤 2 在**统一事件**页面上，显式启用为 加密可视性引擎添加的这些列：

- **EVE 指纹**
- **EVE 进程名称**
- **EVE 进程信心分数**

- **EVE 威胁信心**
- **EVE 威胁信心分数**
- **检测类型**

有关这些字段的信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的 连接和安全相关的连接事件字段。

注释
在**连接事件**页面上，如果进程被分配了应用程序，**检测类型**列会显示**加密可视性引擎**，表明客户端应用程序是由 加密可视性引擎识别的。如果没有为进程名称分配应用，**检测类型**列会显示**AppID**，表示识别客户端应用的引擎是 AppID。

查看 EVE 控制面板

您可以在以下控制面板中查看 EVE 分析信息：

开始之前

- 在访问控制策略中，必须在 **高级设置** 下启用 **加密可视性引擎（EVE）**。
- 要查看**检测到进程名称的连接**和**恶意进程**小组件，您的设备必须运行 Firewall Threat Defense 版本 7.7 或更高版本。
- 要查看**恶意进程响应器 IP**、**恶意进程联系的域**和**已阻止连接**数据，您的设备必须运行 Firewall Threat Defense 版本 10.0 或更高版本。

过程

步骤 1 转至**洞察和报告** > **控制面板**。

步骤 2 在 **摘要控制面板** 窗口中，点击 **加密可视性引擎 (Encrypted Visibility Engine)** 选项卡。

步骤 3 您可以查看以下控制面板：

- **发现的进程**：显示网络中使用的排名靠前的客户端进程和连接数。您可以点击表中的进程名称，查看 **连接事件** 页面的过滤视图，该视图按进程名称进行过滤。
- **威胁置信度**：按置信度（非常高、非常低等）显示连接。您可以点击表中的威胁置信度级别，查看 ”**连接事件**“ 页面的过滤视图，该视图按置信度级别进行过滤。
- **与检测到的进程的连接**：显示 EVE 在其中识别出客户端进程的连接总数。
- **恶意进程**：显示 EVE 识别的威胁置信度为高和极高的恶意客户端进程的计数。

- **恶意响应方 IP**：显示EVE识别为恶意的排名靠前的目标IP地址，按高或极高威胁置信度分类。点击构件中的任何响应方 IP 地址可导航至**连接事件**页面，该页面已按所选响应方 IP 地址进行过滤。
- **恶意域**：显示被EVE识别为恶意并归类为高或极高威胁置信度的域名的计数。点击构件中的任何域名可导航至按所选域名过滤的 **连接事件** 页面。
- **阻止的连接**：显示被 EVE 阻止的连接计数。

注释

- 如果管理中心使用的是 Cisco Secure Firewall 版本 10.0.0，并且没有运行 10.0.0 版本的设备，则不会填充 **恶意进程响应方 IP**、 **恶意进程联系的域**和 **受阻连接** 构件中的数据。
- 如果管理中心使用的是 Cisco Secure Firewall 版本 10.0.0，并且只有一台设备运行版本 10.0.0，则 **恶意进程响应方 IP**、 **恶意进程联系的域**和 **阻止的连接** 构件将仅从该设备填充。其他构件将显示使用较旧版本的设备的数据。

配置 EVE 例外规则

您可以创建加密可视性引擎 (EVE) 例外规则来绕过 EVE 的阻止操作，从而确保可信连接和服务的连续性。您可以将进程名称、源和目标IP地址/FQDN以及动态对象等属性添加到异常规则中。例如，您可能希望绕过受信任网络的EVE阻止判定。根据威胁置信度，绕过网络中的所有连接都免于执行 EVE 阻止判定。

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** (✎) 。

步骤 3 从数据包流行末尾的**更多**下拉箭头中选择**加密可视性引擎**。

步骤 4 在**加密可视性引擎 (Encrypted Visibility Engine)** 页面中，启用**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮。

步骤 5 选择**保护**模式可根据客户端进程的威胁置信度级别监控和阻止加密流量。您可以使用此模式在两个威胁置信度级别监控和阻止恶意连接：

- **高**：使用此级别可阻止威胁置信度级别从高到极高的连接。
- **非常高**：使用此级别可阻止威胁置信度级别归类为非常高的连接。

步骤 6 点击**管理例外**以查看和添加例外规则。

步骤 7 在**加密可视性引擎（EVE）例外列表**窗口中，点击 **+添加例外规则**，并添加所需属性。

注释

只能在全局域中配置 EVE 例外规则。在子域中，您只能查看 EVE 例外规则详细信息。您无法在子域中添加、编辑或删除 EVE 例外规则。

a) 在**进程名称**选项卡下，输入 EVE 识别的进程名称，然后点击窗口右侧的 **+添加**。

可以将多个进程名称添加到同一例外规则。基于进程名称的 EVE 例外列表仅适用于 EVE 识别的进程名称，这些进程名称区分大小写和空格。

b) 在**网络对象 (Network Objects)** 选项卡下，执行以下操作之一：

- 从**可用网络**列表中选择一个或多个网络对象，并将其添加到**选定源网络**或**选定目标网络**列表中。
- 在**选定源网络 (Selected Source Network)** 或**选定目标网络 (Selected Destination Network)** 下，手动输入 IP 地址，然后点击 **添加** (+) 图标以将其添加到所选网络列表中。
- 要创建新的网络对象，请点击 **+创建网络对象**。
  1. 输入**名称**和可选的**说明**。
  2. 选择所需的网络类型 - **主机**、**范围**、**网络**或 **FQDN**。如果选择**主机**、**范围**或**网络**，请输入相关的 IP 地址。如果选择 **FQDN**，请输入完全限定域名 (**FQDN**)，并从**查找**下拉列表中选择所需选项。
  3. 如果要允许配置覆盖，请选中**允许覆盖**复选框。
  4. 点击**添加 (Add)**。

c) 在**动态属性**选项卡下，从**可用动态属性**列表中选择所需的动态属性，并使用 > 按钮将其添加到**选定目标动态属性**列表中。

有关创建动态对象或使用动态对象的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的首次创建动态对象或使用动态对象部分。

d) 要创建新的动态属性，请点击 **+创建动态属性**。

1. 输入**名称**和可选的**说明**。
2. 点击**添加 (Add)**。可以使用思科安全动态属性连接器 (CSDAC) 或管理中心 API 配置此对象。

e) （可选）在所有选项卡的**注释**字段中，可以输入将所需网络对象和动态属性添加到 EVE 例外规则的原因。

步骤 8 点击**保存**，然后部署访问控制策略。

注释 当连接匹配例外规则时，它会绕过 EVE 的阻止判定。您可以在**连接事件**或**统一事件**页面中查看 EVE 的操作。**原因 (Reason)** 列标题显示 **EVE 已豁免 (EVE Exempted)**，用于识别此类绕过 EVE 的流量。

从统一事件添加例外规则

使用**统一事件**页面为被EVE阻止的连接添加例外规则。防火墙管理中心会将例外规则添加到**加密可视性引擎(EVE)例外列表**对象。请注意，添加到此列表的例外规则适用于所有启用了EVE的访问控制策略。

开始之前

仅 Threat Defense 版本 7.6.0 及更高版本支持例外列表。

过程

步骤 1 请点击 **事件和日志** > **分析** > **统一事件**。

步骤 2 在**原因**为“**加密可见性块**”的原因列中，点击单元格内的**省略号**( )图标。

步骤 3 从下拉列表中选择**添加 EVE 例外规则 (Add EVE Exception Rule)**。

注释
只能在全局域中配置 EVE 例外规则。在子域中，您只能查看 EVE 例外规则详细信息。您无法在子域中添加、编辑或删除 EVE 例外规则。

步骤 4 在显示的**加密可视性引擎 (Encrypted Visibility Engine)** 窗口中，规则会自动添加到例外列表的底部。您可以在保存和部署配置之前查看并更改添加的规则。

升级 EVE 例外规则

在 Cisco Secure Firewall 7.7 及更早版本上，为每个策略单独配置 EVE 例外规则。从 Cisco Secure Firewall版本10.0.0开始，EVE例外列表是全局域的一部分。因此，EVE例外规则在全局域中配置，并应用于启用 EVE 以阻止流量的所有策略。

当您将管理中心从版本 7.7 升级到 10.0.0 时，系统会识别并存储包含枝叶域网络对象的枝叶域的所有 EVE 例外规则。升级完成后：

- 全局域策略中的所有 EVE 例外规则，以及叶域策略中引用全局域对象或内联 IP 地址的规则，都会整合到单个全局 EVE 例外列表中。因此，某些策略现在可能包括升级前不存在的 EVE 例外规则。
- 包含 EVE 例外规则的所有策略都将被标记为过期。

如果枝叶域的例外规则包含枝叶域网络或动态对象，则在升级过程中这些规则将被删除。升级脚本日志文件包含所有合并和删除的例外规则的日志，以及每个规则源自的相应访问控制策略和域。日志文件位于 */var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade10.0.0/800_post/1114_eve_rules.pl.log*。

当您在升级后首次部署配置时，管理中心上的警告消息会列出所有已删除的EVE例外规则。警告消息还指出，如果未在全局EVE例外列表中重新配置规则，则可能会产生流量影响。请注意，只有在升级完成后首次部署配置时，才会显示警告消息。

对于映射到运行 10.0.0 版本的管理中心的运行 7.7 及更早版本的 Cisco Secure Firewall 设备，只有“**非常高**”威胁置信度连接事件才会发送到“**安全相关连接事件**”表。对于运行版本 10.0.0 的 Cisco Secure Firewall 设备，EVE **阻止** 和 **中+** EVE 威胁置信度连接事件将发送到 **安全相关连接事件** 表。

EVE 升级期间的更改管理支持

当您将管理中心升级到 10.0.0 版本时，包含启用了 EVE 的访问控制策略的所有活动更改管理故障单的 EVE 例外规则将自动与全局 EVE 例外列表合并。

无论通知单处于何种审批状态，EVE 例外规则都会与全局 EVE 例外列表合并。这可确保在升级期间不会丢失例外规则。

EVE 故障单预览生成行为

如果变更管理故障单包含锁定的策略，并且其中仅包含与 EVE 相关的修改（例如 EVE 设置或例外规则），则在升级后不会自动重新生成 EVE 故障单预览。如果除了与 EVE 相关的修改外，通知单还包含其他策略修改，则 EVE 通知单预览将正常生成。

事件扩充

Talos 分类法和加密可视性引擎 (EVE) 可丰富 MITRE ATT&CK 的情景。Talos 和 EVE 扩充都使用 Talos 分类法进行传达。启用 EVE 时，EVE 扩充有效。有关启用 EVE 的详细信息，请参阅配置 EVE，第 3 页。

在**连接事件 (Connection Events)** 页面上，可以查看作为扩充事件内容的一部分添加的以下列标题。您必须明确启用这些列。

- **MITRE ATT&CK**
- **其他扩充**

有关这些字段的信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的“连接和 中的“安全相关连接 事 件字段” 。

EVE 示例

关于加密可视性引擎

您可以使用加密可视性引擎 (EVE) 来识别使用传输层安全 (TLS) 加密的客户端应用和进程。EVE 无需解密即可提供对加密会话的更多可视性。根据 EVE 的调查结果，管理员可以对其环境中的流量实施策略操作。您还可以使用 EVE 识别和阻止恶意软件。

优势

管理员可以利用和调整EVE的威胁评分来阻止恶意加密流量。如果传入流量是恶意的，则可以根据威胁评分将 EVE 配置为阻止连接。

示例业务情景

一家大型企业网络使用 Snort 3 作为其主要的入侵检测和防御系统。在快速发展的威胁环境中，采用强大的网络安全措施是必要且重要的。安全团队使用加密可视性引擎 (EVE) 来增强加密流量检查，而无需实施完整的中间人 (MITM) 解密。EVE 技术使用已知恶意进程的指纹来识别和阻止恶意软件。网络管理员必须能够灵活地配置EVE的阻止流量阈值，以阻止基于其配置的阻止阈值的潜在恶意连接。

前提条件

- 您必须运行管理中心 7.4.0 或更高版本，并且托管威胁防御也必须是 7.4.0 或更高版本。
- 确保您拥有有效的入侵防御系统 (IPS) 许可证，并且 Snort 3 是检测引擎。

高级工作流程

1. EVE 分析传入流量，并判定传入流量是否为恶意软件的可能性。
2. 如果 EVE 以一定的置信度检测到传入流量为恶意软件，则可以将 EVE 配置为阻止该流量。
3. 首先检查数据包的恶意软件概率或威胁评分，然后将威胁评分与您设置的阻止阈值进行比较。
4. 如果威胁评分高于配置的阈值，EVE 将阻止流量。
5. 如果威胁评分低于配置的阈值，EVE 不采取任何措施。

在 EVE 中配置阻止阈值

此程序显示如何根据 90% 或更高的 EVE 威胁置信度分数阻止潜在的恶意流量。

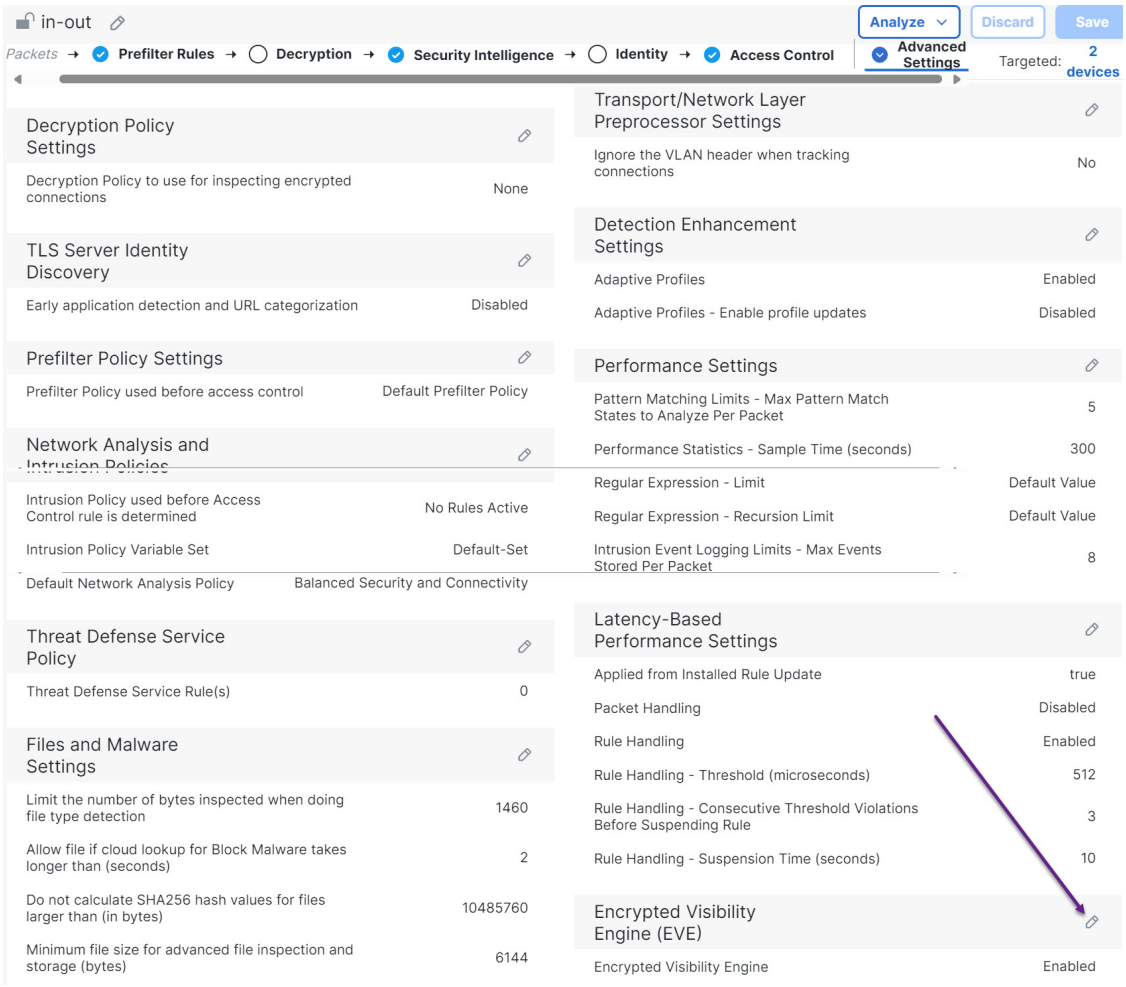
过程

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** (✎) 。

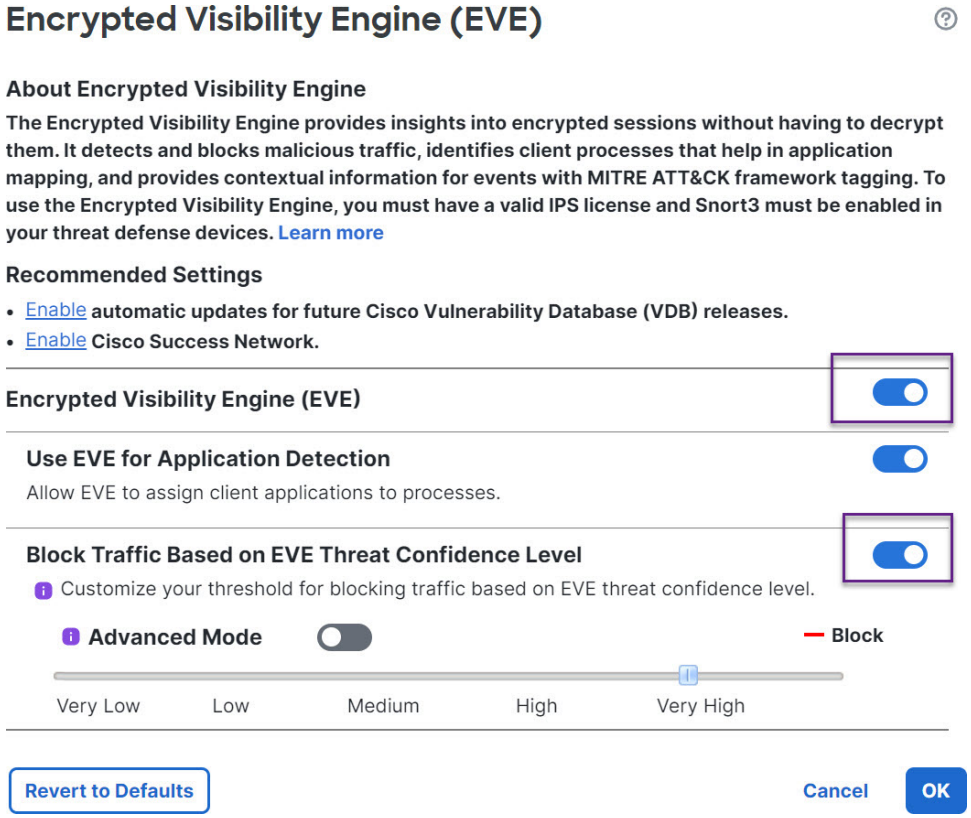
步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**加密可视性引擎 (Encrypted Visibility Engine)** 旁边的 **编辑** (✎)。



步骤 5 在 **加密可视性引擎** 页面中，启用 **加密可视性引擎 (EVE)** 切换按钮。

步骤 6 启用 **基于 EVE 分数阻止流量** 切换按钮。默认情况下，任何可能构成威胁的传入流量都会被阻止。

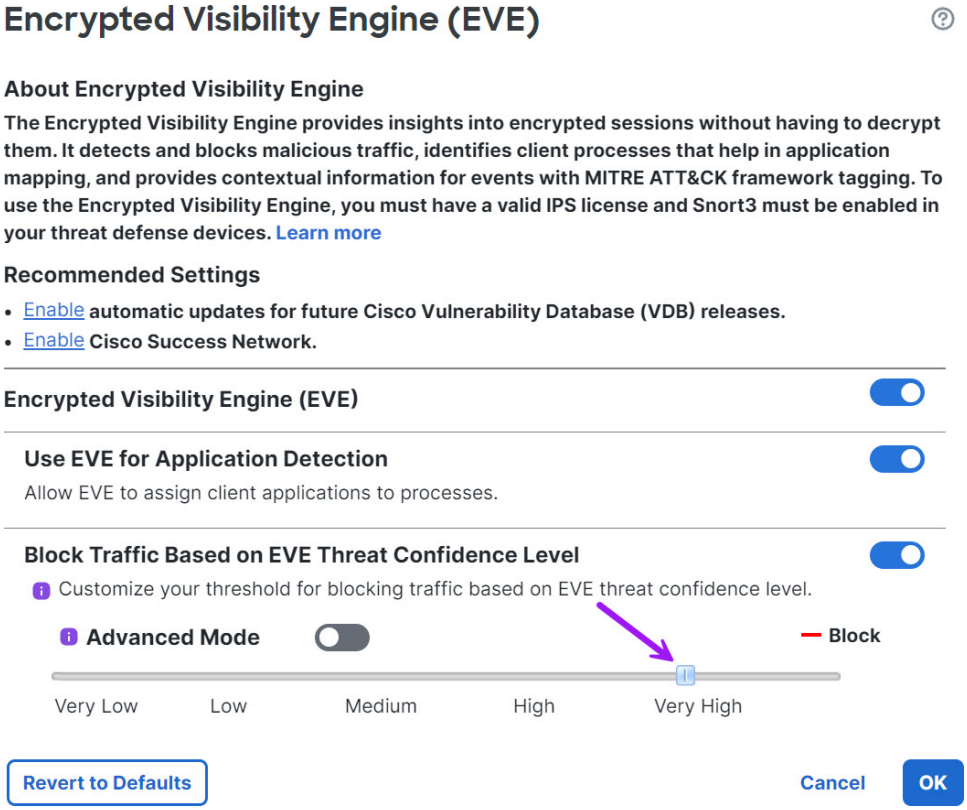


注释

默认情况下，阻止恶意软件的阈值为 99%，这意味着：

- 如果 EVE 检测到流量为恶意软件且置信度为 99% 或更高，则 EVE 会被阻止流量。
- 如果 EVE 检测到流量为恶意软件且其置信度低于 99%，则 EVE 不会采取任何措施。

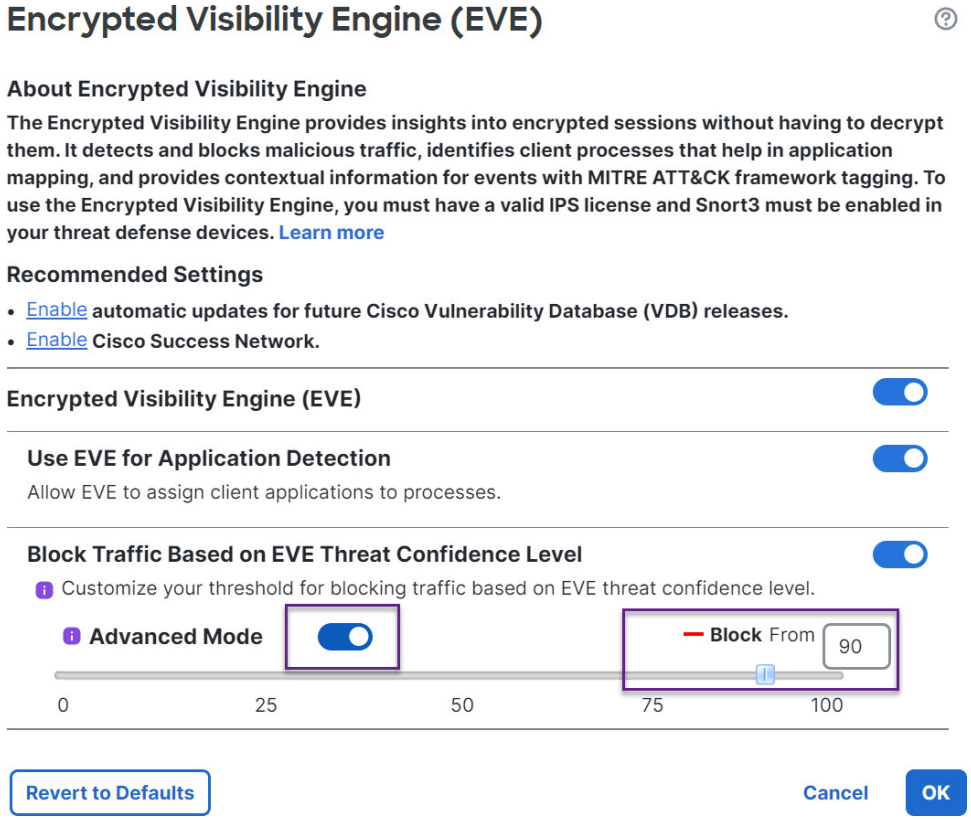
步骤 7 使用滑块根据 EVE 威胁置信度调整阻止阈值。范围从 **非常低** 到 **非常高**。在本例中，滑块设置为 **非常高**。



步骤 8 要进行进一步精细控制，请启用**高级模式 (Advanced Mode)** 切换按钮。现在，您可以为阻止流量分配特定的 EVE 威胁置信度评分。默认阈值为 99%。

步骤 9 在本例中，将阻止阈值更改为 **90**%。

注意
作为最佳实践，我们建议您不要将阻止阈值设置为低于 50%，以确保最佳性能。



步骤 10 点击**确定**。

步骤 11 点击**保存**。

下一步做什么

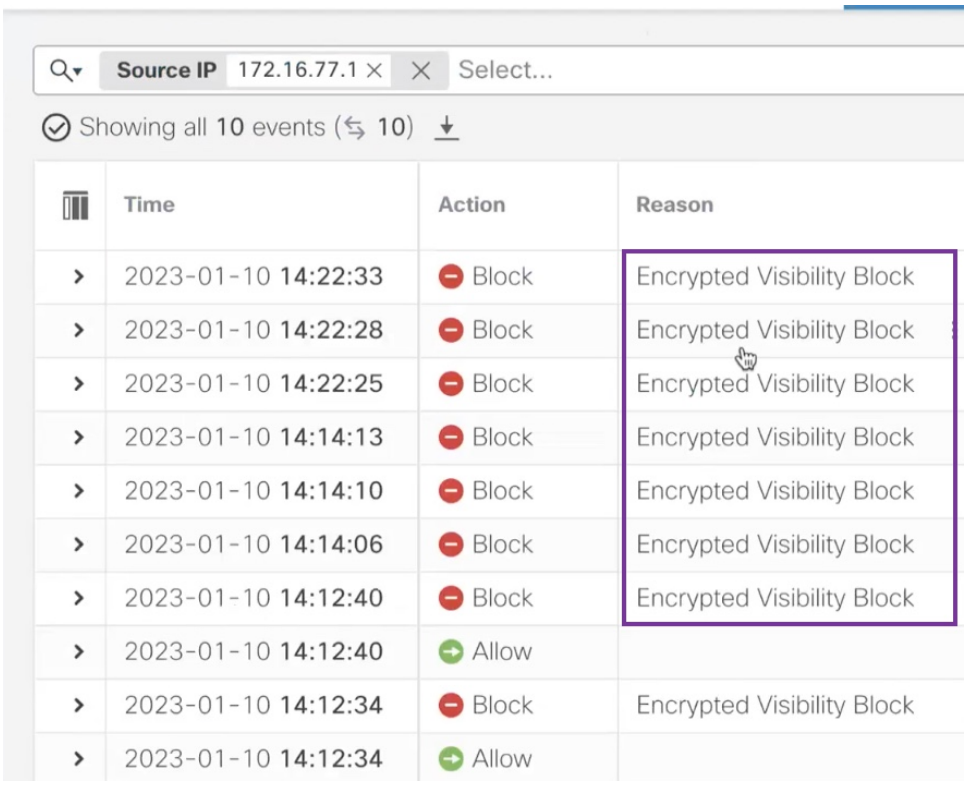
部署配置更改。

查看 EVE 事件

过程

步骤 1 要验证阻止操作，请选择 **事件和日志** > **+ 显示更多** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

步骤 2 如果您已将 EVE 配置为阻止流量，则 **原因** 字段将显示 **加密可视性阻止**。



步骤 3 以下是 **加密可视性进程名称** 为 **test_malware**、 **加密可视性威胁置信度** 为 **非常高**、 **加密可视性威胁置信度** 为 **90** % 的示例。

其他参考资料

有关详细的概念信息，请参阅本指南中的“Snort 3 加密可视性引擎”一章或以下链接中的内容：

加密可视性引擎

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。