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 **分析 (Analysis)** > **主机 (Hosts)** > **网络映射 (Network Map)**，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。
- EVE 无法提供对封装流量的可视性或洞察力。

相关链接

配置 EVE，第 3 页

配置 EVE 例外规则，第 6 页

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。如果您打算

基于 EVE 的“低”或“非常低”分数阈值阻止流量，应阻止初始流。但是，一旦应用的指纹被缓存，将允许以后的流。

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** > **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**。
- **分析** > **网络映射** > **危害表现** > 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 **分析** > **连接 信头** > **事件** 以访问 “**连接事件**” 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。

EVE 中的 QUIC 指纹识别

Snort 可以根据 EVE 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 依次选择**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 (EVE) (Encrypted Visibility Engine [EVE])**旁边的 **编辑** (✎)。

步骤 5 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 6 **使用 EVE 进行应用检测 (Use EVE for Application Detection)** - 默认情况下启用此切换开关，这意味着允许 EVE 将客户端应用分配给进程。

将在连接事件或统一事件的**加密可视性指纹 (Encrypted Visibility Fingerprint)** 列标题中添加 EVE 的指纹信息。要对收集的 EVE 数据进行进一步分析，可以右键点击指纹信息以打开下拉菜单。在菜单中，点击**查看加密可视性引擎进程分析 (View Encrypted Visibility Engine Process Analysis)** 以转至 Cisco Secure Firewall 应用检测器站点，然后查看详细信息，例如指纹、VDB 版本等。系统将显示具有相同指纹字符串的不同行，以及与其关联的潜在进程名称及其普遍性。普遍性表示与数据收集系统中的特定指纹关联的进程的频率。您可以选择进程名称，然后点击 **提交请求 (Submit Request)**，以提供有关 EVE 进程检测中任何差异的反馈。例如，如果检测到的进程名称与正在发送的流量不匹配，或者根本没有检测到特定指纹的进程名称，则可以提交请求。

具有非思科电子邮件地址的用户当前无法访问 Cisco Secure Firewall 应用检测器 (Secure Firewall Application Detectors) 页面上查看其他详细信息的权限。

如果禁用 **使用 EVE 进行应用检测** 切换按钮：

- AppID 识别的客户端将分配给进程，您可以看到 EVE 进程和分数，但没有将 EVE 检测到的进程映射到应用，也不会执行任何操作。您可以在**连接事件 (Connection Events)** 或**统一事件 (Unified Events)** 下查看事件的详细信息。要查看连接事件的差异（有和没有应用分配），请参阅**客户端应用 (Client Application)** 列标题。
- 连接事件或统一事件中的 **已加密可视性指纹 (Encrypted Visibility Fingerprint)** 字段为空。

步骤 7 启用**基于威胁置信度阻止恶意软件进程 (Block Malware Processes Based on Threat Confidence Level)** 切换按钮，以根据 EVE 的威胁置信度阻止前缀为 *Malware_* 的恶意客户端进程。

默认阻止阈值为 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，则流量会被阻止。
- 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。

注释
如果 EVE 已阻止流量，则在**连接事件 (Connection Events)** 页面中，**原因 (Reason)** 列标题会显示**加密可视性阻止 (Encrypted Visiblity Block)**。

步骤 8 使用滑块根据 EVE 的威胁置信度调整阻止阈值，范围从 **非常低** 到 **非常高**。

步骤 9 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。默认阻止阈值为 99%。

注意
为了获得最佳性能，我们建议不要将阈值设置为低于 50%。

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 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“连接事件”**页面或**“统一事件”**页面查看已记录的连接事件。

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 依次点击 **分析 (Analysis)** > **连接 (Connections)** > **事件 (Events)**。

步骤 2 点击**连接事件的表视图 (Table View of Connection Events)** 选项卡。

您也可以在**统一事件**页面中查看连接事件。点击**分析** > **统一事件**以访问**统一事件**页面。

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。

在**连接事件**页面上，您必须显式启用为 加密可视性引擎添加的这些列：

- **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**与检测到的进程的连接**和**恶意进程**构件，设备必须运行版本 7.7 及更高版本。

过程

步骤 1 前往**概述 (Overview)** > **控制面板 (Dashboards)**，然后点击**控制面板 (Dashboard)**。

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。

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 依次选择**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**下拉箭头选择**高级设置 (Advanced Settings)**。

步骤 4 在**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 旁边，点击 **编辑** (✎)。

步骤 5 在**加密可视性引擎 (Encrypted Visibility Engine)** 页面中，点击**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮以启用 EVE。

步骤 6 启用**根据 EVE 置信度阻止流量 (Block based on EVE threat confidence level)** 开关来根据 EVE 的威胁置信度来阻止流量。

步骤 7 点击**添加例外规则 (Add Exception Rule)** 并添加以下一个或多个属性。

a) 在**进程名称 (Process Name)** 选项卡下，输入 EVE 识别的进程名称，然后点击窗口右侧的**添加到进程 (Add to Process)**。

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：

- 从列表中选择一个或多个 IP 地址或 FQDN，然后点击**添加到源网络 (Add to Source Network)** 或**添加到目标网络 (Add to Destination Network)**。
- 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。

c) 在**动态属性 (Dynamic Attributes)** 选项卡下，选择动态对象并将其添加到**选定的动态对象 (Selected Dynamic Objects)** 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) （可选）在所有选项卡上提供的**注释 (Comment)** 字段中，您可以输入将所需属性添加到 EVE 例外规则的原因。

步骤 8 点击**保存**保存 EVE 例外规则。

步骤 9 在设备上保存并部署访问控制策略。

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。

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 **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)**。

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。

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” 。

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。