# 应用检测

以下主题介绍 Firepower 系统应用检测：



# 概述：应用检测

当 Firepower 系统分析 IP 流量时，它会尝试识别网络上的常用应用。应用感知对于应用控制至关重要。

系统检测的应用有三种类型：

- 应用协议（例如 HTTP 和 SSH），代表主机之间的通信
- 客户端（例如网络浏览器和邮件客户端），代表主机上运行的软件
- *Web* 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL

系统根据在检测器中指定的特征识别网络流量中的应用。例如，系统可以通过数据包报头中的ASCII模式识别应用。此外，安全套接字层(SSL)协议检测程序使用安全会话的信息来识别会话中的应用。

在 Firepower 系统中有两个应用检测器来源：

- 系统提供的检测器检测 Web 应用、客户端和应用协议。

系统提供的应用检测器（和操作系统）的可用性取决于 Firepower 系统的版本和已安装的 VDB 版本。版本说明和公告包含关于新的和更新的检测器的信息。也可以导入专业服务开发的各个检测器。

- 自定义应用协议检测器由用户创建并检测 Web 应用、客户端和应用协议。

您还可以通过隐含应用协议检测来检测应用协议，此检测根据对客户端的检测暗示应用协议的存在。

如在网络发现策略中所定义，系统仅识别受监控网络中的主机上运行的应用协议。例如，如果内部主机访问未受监控的远程站点的 FTP 服务器，系统不会将应用协议识别为 FTP。另一方面，如果远程或内部主机访问正受监控主机上的 FTP 服务器，系统能够正确识别应用协议。

如果系统可以识别受监控主机用于连接到未受监控服务器的客户端，则系统会识别客户端的对应应用协议，但是不将该协议添加到网络映射中。请注意，客户端会话必须包括来自要发生应用检测的服务器的响应。

系统会确定其检测到的每个应用的特征；请参阅应用特征。系统使用这些特征创建应用组，称为应用过滤器。应用过滤器用于执行访问控制以及限制报告和控制面板构件中使用的搜索结果和数据。

您还可以使用导出的 NetFlow 记录、Nmap 主动扫描和主机输入功能补充应用检测器数据。

**相关主题**

配置应用控制的最佳实践
应用检测器基础知识，第 2 页

# 应用检测器基础知识

Firepower 系统使用应用检测器来识别网络上的常用应用。使用“检测器”页面（**策略 > 应用检测器**）查看检测器列表和自定义检测功能。

是否能修改检测器或更改其状态（活动或非活动）取决于其类型。系统仅使用活动检测器来分析应用流量。

**注释** 思科提供的检测器可能会随 Firepower 系统和 VDB 更新而更改。有关已更新的检测器的信息，请参阅版本说明和咨询。

**注释** 对于Firepower应用标识，不会特意列出端口。不会为任何思科应用报告应用的关联端口，因为大多数应用都与端口无关。我们平台的检测功能可以识别在网络中的任何端口运行的服务。

### 思科提供的内部检测器

内部检测器是一种特殊类别的检测器，适用于客户端、Web 应用和应用协议流量。内部检测器随系统更新一起提供，并且永远在线。

如果应用与旨在检测客户端相关活动的内部检测器匹配且不存在特定客户端检测器，则可以报告通用客户端。

### 思科提供的客户端检测器

客户端检测器用于检测客户端流量，并且通过VDB或系统更新提供，或由思科专业服务提供用于导入。可以激活和停用客户端检测器。仅当导入客户端检测器后，才可以将其导出。

### 思科提供的 Web 应用检测器

*Web* 应用检测器用于检测 HTTP 流量负载中的 Web 应用，并且通过 VDB 或系统更新提供。Web 应用检测器永远在线。

### 思科提供的应用协议（端口）检测器

基于端口的应用协议检测器使用已知端口识别网络流量。此类检测器通过VDB或系统更新提供，或由思科专业服务提供用于导入。可以激活和停用应用协议检测器，还可查看检测器定义，以便将其用作自定义检测器的基础。

### 思科提供的应用协议 (Firepower) 检测器

基于 *Firepower* 的应用协议检测器用于使用 Firepower 应用指纹分析网络流量，并且通过 VDB 或系统更新提供。可以激活和停用应用协议检测器。

### 自定义应用检测器

自定义应用检测器基于模式。它们将检测来自客户端的数据包、Web应用或应用协议流量中的模式。对于已导入检测器和自定义检测器，您将拥有完全控制权。

# 在 Web 界面中识别应用协议

下表概述了系统如何识别检测到的应用协议：

**表 *1:* 系统识别应用协议**

| 标识 | 说明 |
| --- | --- |
| 应用协议名称 | 如果应用协议属于以下情况，管理中心将会使用应用协议名称来识别应用协议：<br>• 由系统正确识别出<br>• 使用 NetFlow 数据识别出，并且 `/etc/sf/services` 中有端口应用协议关联<br>• 使用主机输入功能手动识别出<br>• 由 Nmap 或其他活动源识别出 |

| 标识 | 说明 |
| --- | --- |
| pending | 如果系统既不能正确识别也不能错误识别应用，管理中心会将应用协议识别为 pending。<br>大多数情况下，系统需要收集和分析更多的连接数据才能识别待处理应用。<br>在应用详细信息表、服务器表和主机配置文件中，只会对在其中检测到（而不是由检测到的客户端或 Web 应用流量推断）特定应用协议流量的应用协议显示 pending 状态。 |
| unknown | 在以下情况下，管理中心会将应用协议识别为 unknown：<br>• 应用不匹配系统的任何检测器。<br>• 应用协议是使用 NetFlow 数据识别出的，但 /etc/sf/services 中没有端口应用协议关联。<br>• Snort 已关闭会话，但它仍存在于设备中。在这里，允许流量通过防火墙，但不会检测到应用。 |
| 空白 | 已检查检测到的所有可用数据，但没有识别出应用协议。在应用详细信息表、服务器表中和主机配置文件中，对于在其中没有检测到应用协议的非 HTTP 通用客户端数据流量，应用协议留空。 |

# 通过客户端检测进行隐含应用协议检测

如果系统可以识别受监控主机用于访问未受监控主机的客户端，管理中心会推断该连接使用与该客户端对应的应用协议。（由于系统仅跟踪监控网络上的应用，因此，连接日志通常不包含有关监控主机用于访问未受监控的服务器的连接的应用协议信息。）

此过程，或隐含应用协议检测，具有以下结果：

- 由于系统不会为这些服务器生成新的 TCP 端口或新的 UDP 端口事件，因此，服务器不会显示在服务器表中。此外，不能将对这些应用协议的检测作为条件来触发事件警报或关联规则。
- 由于应用协议未与主机关联，因此，不能查看主机配置文件中的详细信息，不能设置其服务器身份，也不能使用流量量变曲线或关联规则的主机配置文件限定条件中的信息。此外，系统不会根据此类检测将漏洞与主机关联。

但是，您可以触发有关连接中是否存在应用协议信息的关联事件。还可以使用连接日志中的应用协议信息创建连接跟踪程序和流量量变曲线。

# 主机限制和发现事件日志记录

如果系统检测到客户端、服务器或网络应用，它会生成发现事件，除非关联的主机已达到客户端、服务器或网络应用的最大数量。

主机配置文件最多为每个主机显示 16 个客户端、100 个服务器和 100 个网络应用。

请注意，依赖于客户端、服务器或网络应用检测的操作不受此限制的影响。例如，经配置要在服务器上触发的访问控制规则仍会记录连接事件。

# 应用检测的特殊注意事项

### SFTP

为了检测 SFTP 流量，同一规则还必须检测 SSH。

### Squid

在以下情况下，系统会积极识别 Squid 服务器流量：

- 系统检测从受监控网络上的主机到启用了代理身份验证的 Squid 服务器的连接；或
- 系统检测从受监控网络上的 Squid 代理服务器到目标系统（即，客户端正在其中请求信息或其他资源的目标服务器）的连接。

但是，在以下情况下，系统无法识别 Squid 服务流量：

- 受监控网络上的主机连接到已禁用代理身份验证的 Squid 服务器；或
- Squid 代理服务器被配置为从其 HTTP 响应中移除“通过：”报头字段

### SSL 应用检测

系统提供可以使用安全套接字层 (SSL) 会话中的会话信息识别会话中的应用协议、客户端应用或 Web 应用的应用检测器。

如果系统检测到加密连接，它会将该连接标记为通用 HTTPS 连接或更为具体的安全协议，例如 SMTPS（如果适用）。如果系统检测到 SSL 会话，它会将 `SSL client` 添加到该会话的连接事件中的 **客户端 (Client)** 字段。如果识别到会话的 Web 应用，系统会为该流量生成发现事件。

对于 SSL 应用流量，受管设备还可以检测服务器证书中的公用名并将其与 SSL 主机模式的客户端或 Web 应用比对。当系统识别到特定客户端时，会将 `SSL client` 替换为该客户端的名称。

由于 SSL 应用流量已加密，因此系统只能使用证书中的信息（而不是加密数据流中的应用数据）进行标识。为此，SSL 主机模式有时只能识别作为应用编写者的公司，因此同一公司开发的 SSL 应用可能有相同的标识。

在某些情况下，例如 HTTPS 会话是从 HTTP 会话内部发起时，受管设备会从客户端数据包中的客户端证书检测服务器名称。

要启用 SSL 应用标识，必须创建监控响应方流量的访问控制规则。这些规则必须包含适用于 SSL 应用的应用条件或者使用来自 SSL 证书的 URL 的 URL 条件。对于网络发现，响应方 IP 地址不必位于要在网络发现策略中监控的网络上；访问控制策略配置决定是否识别流量。要识别 SSL 应用的检测，您可以在应用检测器列表中或在访问控制规则中添加应用条件时按 `SSL protocol` 标记进行过滤。

### 推荐的 Web 应用

Web 服务器有时会将流量推荐到其他网站，这些网站通常是广告服务器。为帮助您更好地理解网络上出现的推荐流量的情景，系统在推荐会话的事件的 **Web 应用 (Web Application)** 字段中列出推荐流量的 Web 应用。VDB 包含已知被推荐站点的列表。如果系统检测到来自这些站点之一的流量，会将推荐站点连同该流量的事件一起存储。例如，如果通过Facebook访问的广告实际在Advertising.com上托管，则检测到的 Advertising.com 流量与 Facebook Web 应用关联。系统还可以检测到 HTTP 流量中的推荐 URL，例如当网站提供与另一站点的简单链接时；在这种情况下，推荐 URL 出现在 HTTP Referrer 事件字段。

在事件中，如果存在推荐应用，它将被列为流量的 Web 应用，而 URL 则是被推荐站点的 URL。在上述示例中，用于流量的连接事件的 Web 应用是 Facebook，但 URL 是 Advertising.com。在下列情况下，被推荐的应用可能显示为 Web 应用：未检测到推荐 Web 应用，主机推荐其本身，或者存在推荐链。在控制面板中，Web 应用的连接和字节数包括 Web 应用与该应用推荐的流量关联的会话数。

请注意，如果创建专门针对被推荐流量的规则，应该为被推荐应用（而不是推荐应用）添加条件。例如，要阻止从 Facebook 推荐的 Advertising.com 流量，可以向 Advertising.com 应用的访问控制规则添加应用条件。

## Snort 2 和 Snort 3 中的应用检测

在 Snort 2 中，您可以通过访问控制策略中的限制和网络发现策略中的网络过滤器来启用或禁用应用检测。但是，访问控制策略中的限制可以覆盖网络过滤器，同时启用应用检测。例如，如果您在网络发现策略中定义了网络过滤器，并且当访问控制策略具有需要应用检测的限制（例如 SSL、URL SI、DNS SI 等）时，则这些网络发现过滤器会被覆盖，并且所有网络会进行应用检测。Snort 3 不支持此 Snort 2 功能。

**注释** Snort 3 现在与 Snort 2 相同，如果 AC 策略中没有其他配置需要 AppID 来监控所有流量，则只会在网络发现策略过滤器中定义的特定网络子网上启用 AppID 检查。

在 Snort 3 中，默认情况下始终为所有网络启用应用检测。要禁用应用检测，请执行以下操作：

### 过程

**步骤 1** 选择**策略 (Policies)** > **访问控制 (Access Control)**，点击编辑策略并删除应用规则。

**步骤 2** 选择**策略 (Policies)** > **SSL**，点击删除以删除 SSL 策略。

**步骤 3** 选择**策略 (Policies)** > **网络发现 (Network Discovery)**，点击删除以删除网络发现策略。

**步骤 4** 选择 **策略** > **访问控制**，点击 **编辑**（✎），然后选择 **安全情报** > **URLs** 选项卡以删除 URL 允许或阻止列表。

**步骤 5** 由于您无法删除默认 DNS 规则，请选择**策略 (Policies)** > **DNS**，点击编辑并取消选中启用框以禁用 DNS 策略。

**步骤 6** 在访问控制策略的**高级 (Advanced)** 设置下，禁用启用威胁情报导向器 *(Enable Threat Intelligence Director)* 和对 *DNS* 流量启用信誉实施 *(Enable reputation enforcement on DNS traffic)* 选项。

**步骤 7** 保存并部署访问控制策略。

# 应用检测的要求和必备条件

**型号支持**

任意。

**支持的域**

任意

**用户角色**

- 管理员
- 发现管理员

# 自定义应用检测器

如果在网络上使用自定义应用，您可以创建自定义的 Web 应用、客户端或应用协议检测器，它们可向系统提供识别应用所需的信息。应用检测器的类型由您在**协议 (Protocol)**、**类型 (Type)** 和**方向 (Direction)** 字段中进行的选择确定。

只有客户端会话包含来自服务器的响应器数据包，系统才能开始检测和识别服务器流量中的应用协议。请注意，对于 UDP 流量，系统将响应器数据包的来源指定为服务器。

如果已经在另一管理中心上创建了检测器，可将其导出后，再导入至此管理中心。然后，可根据自己的需求编辑已导入的检测器。您可导出和导入自定义检测器以及思科专业服务提供的检测器。但是，您**无法**导出或导入思科提供的任何其他类型检测器。

## 自定义应用检测器和用户定义的应用字段

可以使用以下字段配置自定义应用检测器和用户定义的应用。

**自定义应用检测器字段：常规**

使用以下字段配置基本和高级自定义应用检测器。

**应用协议**

要检测的应用协议。这可以是系统提供的应用或用户定义的应用。

如果要让应用免于执行主动身份验证（在身份规则中配置），则必须选择或创建带**用户代理排除项 (User-Agent Exclusion)** 标记的应用协议。

**说明**

应用检测器的说明。

**名称**

应用检测器的名称。

**检测器类型 (Detector Type)**

检测器的类型，**基本 (Basic)** 或**高级 (Advanced)**。基本应用检测器是在 Web 界面中作为一系列字段而创建的。高级应用检测器是在外部创建并作为自定义 .lua 文件上传的。

### 自定义应用检测器字段：检测模式

使用以下字段配置基本自定义应用检测器的检测模式。

**方向**

检测器应当检查的流量源，包括**客户端 (Client)** 或**服务器 (Server)**。

**偏移**

以字节为单位表示的在数据包中的位置，从数据包负载起始位置（系统应开始搜索模式的位置）开始。

因为数据包负载从 0 字节开始，请按以下方法计算偏移：将想要从数据包负载起始位置前移的字节数减去 1。例如，要查找数据包的第 5 个位中的模式，请在**偏移 (Offset)** 字段键入 4。

**模式**

与您选择的**类型 (Type)** 相关联的模式字符串。

**端口**

检测器应检查流量的端口。

**协议**

要检测的协议。选择的协议将确定是显示**类型 (Type)** 还是 **URL** 字段。

该协议（以及在某些情况下，您在**类型 [Type]** 和**方向 [Direction]** 字段中的后续选择）将确定您创建的应用检测器类型：Web 应用、客户端或应用协议。

| 检测器类型 (Detector Type) | 协议 | 类型或方向 |
|---|---|---|
| Web 应用程序 | HTTP | **类型 (Type)** 为**内容类型 (Content Type)** 或 **URL** |
| | RTMP | Any |
| | SSL | Any |

| 检测器类型 (Detector Type) | 协议 | 类型或方向 |
|---|---|---|
| 客户端 | HTTP | 类型 (Type) 为用户代理 (User Agent) |
| | SIP | Any |
| | TCP 或 UDP | 方向 (Direction) 为客户端 (Client) |
| 应用协议 | TCP 或 UDP | 方向 (Direction) 为服务器 (Server) |

**类型**

输入的模式字符串类型。您看到的选项由您已选择的**协议 (Protocol)** 确定。如果已选择 **RTMP** 作为协议，则系统将显示 **URL** 字段而非**类型 (Type)** 字段。

**注释** 如果选择**用户代理 (User Agent)** 作为**类型 (Type)**，则系统自动将应用的**标记 (Tag)** 设为**用户代理排除项 (User-Agent Exclusion)**。

| 类型选择 | 字符串特征 |
|---|---|
| **Ascii** | 字符串使用 ASCII 编码。 |
| **公用名** | 字符串是服务器响应消息中 commonName 字段的值。 |
| **内容类型** | 字符串是服务器响应报头中 content-type 字段的值。 |
| **十六进制** | 字符串使用十六进制表示。 |
| **组织单位** | 字符串是服务器响应消息中 organizationName 字段的值。 |
| **SIP 服务器 (SIP Server)** | 字符串是消息报头中 From 字段的值。 |
| **SSL 主机 (SSL Host)** | 字符串是 ClientHello 消息中 server_name 字段的值。 |
| **URL** | 字符串是一个 URL。<br>**注释** 检测器假设输入的字符串是完整的 URL 部分。例如，输入 **cisco.com** 将匹配 **www.cisco.com/support** 和 **www.cisco.com**，但不匹配 **www.wearecisco.com**。 |
| **用户代理** | 字符串是 GET 请求报头中 user-agent 字段的值。它还可用于 SIP 协议，表示字符串是 SIP 消息报头中 user-agent 字段的值。 |

**URL**

来自 RTMP 数据包的 C2 消息内 swfURL 字段的完整 URL 或部分 URL。选择 **RTMP** 作为**协议 (Protocol)** 时，系统将显示此字段而非**类型 (Type)** 字段。

注释 检测器假设输入的字符串是完整的 URL 部分。例如，输入 **cisco.com** 将匹配 **www.cisco.com/support** 和 **www.cisco.com**，但不匹配 **www.wearecisco.com**。

**用户定义的应用字段**

使用以下字段在基本和高级自定义应用检测器内配置用户定义的应用。

**业务相关性**

应用被用于您的组织的业务运营中（而不是用于娱乐目的）的可能性：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 或**非常低 (Very Low)**。选择最能描述应用的选项。

**类别**

说明应用的最基本功能的应用通用分类。

**说明**

应用的说明。

**名称**

应用的名称。

**风险**

应用被用于违反您的组织安全策略的目的之可能性：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 或**非常低 (Very Low)**。选择最能描述应用的选项。

**标签**

提供有关应用的其他信息的一个或多个预定义标记。如果要让应用免于执行主动身份验证（在身份规则中配置），则必须为应用添加**用户代理排除项 (User-Agent Exclusion)** 标记。

# 配置自定义应用检测器

您可以配置基本或高级自定义应用检测器。

**过程**

**步骤 1** 选择**策略** > **应用检测器**。

**步骤 2** 点击**创建自定义检测器 (Create Custom Detector)**。

**步骤 3** 输入**名称 (Name)** 和**说明 (Description)**。

**步骤 4** 从应用下拉列表中选择**应用协议 (Application Protocol)**。您有以下选择：

- 如果是为现有应用协议创建检测器（例如，如果要检测非标准端口上的特定应用协议），请从下拉列表中选择应用协议。
- 如果是为用户定义的应用创建检测器，请按照创建用户定义的应用，第 11 页中概述的程序执行操作。

**步骤 5** 点击**检测器类型 (Detector Type)** 以选择**基本 (Basic)** 或 **高级 (Advanced)**。

**步骤 6** 点击 **OK**。

**步骤 7** 配置 **检测模式** 或 **检测标准** 或 **加密可视性引擎进程分配**：

- 如果配置的是基本检测器，请指定预设**检测模式 (Detection Patterns)**，如指定基本检测器中的检测模式，第 12 页中所述。
- 如果配置的是高级检测器，请指定自定义**检测条件 (Detection Criteria)**，如指定高级检测器中的检测条件，第 13 页中所述。
- 如果要配置加密可视性引擎（EVE）检测器，请指定自定义EVE进程分配，如本章指定 *EVE* 进程分配部分中所述。

  **注意** 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

**步骤 8** 或者，使用**数据包捕获 (Packet Captures)** 测试新检测器，如测试自定义应用协议检测器，第 15 页中所述。

**步骤 9** 点击**保存 (Save)**。

**注释** 如果在访问控制规则中包含该应用，则检测器会自动激活，并且在使用时不能停用。

### 下一步做什么

- 激活检测器，如激活和停用检测器，第 18 页中所述。

### 相关主题

自定义应用检测器和用户定义的应用字段，第 7 页

## 创建用户定义的应用

此处创建的应用、类别和标记在访问控制规则以及在应用过滤对象管理器中均可用。

**注意** 创建用户定义的应用会立即重启 Snort 进程，而无需执行部署过程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

### 开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。

### 过程

**步骤 1** 在**创建自定义应用检测器 (Create A Custom Application Detector)** 对话框中，点击**应用 (Application)** 字段旁边的 **添加**（+）。

**步骤 2** 键入**名称 (Name)**。

**步骤 3** 键入**说明 (Description)**。

**步骤 4** 选择**业务关联性**。

**步骤 5** 选择**风险**。

**步骤 6** 点击“类别”(Categories) 旁的**添加 (Add)** 以添加类别，并键入新的类别名称，或者从**类别 (Categories)** 下拉列表选择现有类别。

**步骤 7** 或者，也可以点击"标记"(Tags) 旁的**添加 (Add)** 以添加标记，并键入新的标记名称，或者从**标记 (Tags)** 下拉列表选择现有标记。

**步骤 8** 点击 **OK**。

### 下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

### 相关主题

自定义应用检测器和用户定义的应用字段，第 7 页

## 指定基本检测器中的检测模式

可以配置自定义应用协议检测器以搜索应用协议数据包报头中的特定模式字符串。也可配置检测器，使其搜索多个模式，在这种情况下，应用协议流量必须匹配所有模式，以便检测器主动识别应用协议。

应用协议检测器可使用任何偏移搜索 ASCII 或十六进制模式。

### 开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。

### 过程

**步骤 1** 在**创建检测器 (Create Detector)** 页面上的**检测模式 (Detection Patterns)** 部分中，点击**添加 (Add)**。

**步骤 2** 从**应用 (Application)** 下拉列表中选择协议类型。

**步骤 3** 从**类型 (Type)** 下拉列表中选择模式类型。

**步骤 4** 键入与指定的**类型**相匹配的**模式**字符串。

**步骤 5** 或者，键入**偏移 (Offset)**（以字节为单位）。

**步骤 6** 或者，要根据其使用的端口识别应用协议流量，请在**端口**字段中键入 1 到 65535 之间的端口。要使用多个端口，请用逗号分隔它们。

**步骤 7** 点击**方向 (Direction)**：**客户端 (Client)** 或**服务器 (Server)**。

**步骤 8** 点击 **OK**。

**提示** 如果要删除模式，请点击要删除的模式旁边的 **删除**（ ）。

### 下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

### 相关主题

指定高级检测器中的检测条件，第 13 页

## 指定高级检测器中的检测条件

**注意** 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

**注意** 不要上传来自不可信来源的 .lua 文件。

自定义 .lua 文件包含自定义应用检测器设置。创建自定义 .lua 文件需要具备 lua 编程语言的高级知识和思科的 C-lua API 经验。思科强烈建议使用以下材料来准备 .lua 文件：

- lua 编程语言的第三方说明和参考资料
- 开源检测器开发人员指南： https://www.snort.org/downloads
- OpenAppID Snort 社区资源： http://blog.snort.org/search/label/openappid

**注释** 系统不支持引用系统调用或文件 I/O 的 .lua 文件。

### 开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。

- 通过下载和学习类似检测器的 .lua 文件，为创建有效的 .lua 文件做准备。有关下载检测器文件的详细信息，请参阅查看或下载检测器详细信息，第 15 页。
- 创建包含自定义应用检测器设置的有效 .lua 文件。

### 过程

**步骤 1** 在高级自定义应用检测器的**创建检测器 (Create Detector)** 页面的**检测条件 (Detection Criteria)** 部分中，点击**添加 (Add)**。

**步骤 2** 点击**浏览...(Browse...)** 以导航至 **.lua** 文件并将其上传。

**步骤 3** 点击 **OK**。

### 下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

### 相关主题

指定基本检测器中的检测模式，第 12 页

## 指定 EVE 进程分配

您可以配置自己的自定义应用检测器，以将加密可视性引擎 (EVE) 检测到的进程映射到新应用或现有应用。

### 开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。

### 过程

**步骤 1** 在“创建检测器”(Create Detector) 页面上的“加密可视性引擎进程分配”(Encrypted Visibility Engine Process Assignments) 部分中，点击**添加 (Add)**。

**步骤 2** 输入 **进程名称** 和 **最小进程置信度** 值。

注释 您可以在 **进程名称** 字段中输入文本，这区分大小写。该值应与 EVE 检测到的确切进程名称匹配。 **最小进程置信度** 可以是 0 到 100 之间的任何数字。这是连接事件中 **加密可视化进程置信度得分** 字段中显示的数字。

有关 **加密可视化进程置信度得分** 字段的信息，请参阅 《Cisco Firepower 管理中心管理指南》中 “连接和安全情报事件字段” 的部分。

**步骤 3** 点击**保存 (Save)**。

**步骤 4** 在应用检测器列表页面中，激活您创建的检测器。有关详细信息，请参阅激活和停用检测器，第 18 页。当您激活检测器时，检测器文件会被推送到 管理中心上注册的所有 FTD。

### 下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

## 测试自定义应用协议检测器

如您拥有的数据包捕获 (pcap) 文件包含的数据包带有要检测的应用协议的流量，则可针对该 pcap 文件测试自定义的应用协议检测器。思科建议使用简单、干净的 pcap 文件，没有不必要的流量。

Pcap 文件必须为 256 KB 或更小；如果尝试针对较大的 pcap 文件测试检测器，管理中心会自动将其截断并测试不完整文件。在使用该文件测试检测器之前，必须修复 pcap 中无法确定的校验和。

### 开始之前

- 配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。

### 过程

**步骤 1** 在“创建检测器”(Create Detector) 页面上的“数据包捕获”(Packet Captures) 部分，点击**添加 (Add)**。

**步骤 2** 在弹出式窗口中浏览至 pcap 文件，然后点击**确定 (OK)**。

**步骤 3** 要针对 pcap 文件的内容测试检测器，点击 pcap 文件旁的评估。系统显示消息，指示测试是否成功。

**步骤 4** 或者，重复第 1至 3 步，针对额外的 pcap 文件测试检测器。

**提示** 要删除 pcap 文件，点击想要删除的文件旁的 **删除**（  ） 。

### 下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 10 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

# 查看或下载检测器详细信息

可以使用检测器列表来查看应用检测器详细信息（所有检测器）和下载检测器详细信息（仅自定义应用检测器）。

过程

步骤 1 要查看应用检测器详细信息，请执行以下任一操作：

- 参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html 上提供的相关 VDB 版本的思科 *Firepower* 应用检测器参考
- a. 选择**策略** > **应用检测器**。

  b. 过滤列表以查找特定检测器。

  c. 点击 **信息**（  ）

步骤 2 要下载自定义应用检测器的检测器详细信息，请点击 **下载**（  ）。

如果控件呈灰显状态，则表明配置属于祖先域，或者您没有必要的权限。

# 检测器列表排序

默认情况下，Detectors 页面将按名称以字母顺序列出检测器。列标题旁边的向上或向下箭头表示页面按该列升序或降序排序。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击相应的列标题。

# 过滤检测器列表

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 展开检测器列表的过滤器组，第 17 页中所述的其中一个过滤器组并选择过滤器旁边的复选框。要选择组中的所有过滤器，右键点击组名称，然后选择 **Check All**。

步骤 3 如果要移除某个过滤器，请点击 **删除**（  ）（位于**过滤器 [Filters]** 字段的过滤器名称中）或禁用过滤器列表中的过滤器。要移除组中的所有过滤器，右键点击组名称，然后选择 **Uncheck All**。

**步骤 4** 如果要移除所有过滤器，请点击已应用至检测器的过滤器列表旁边的**全部清除 (Clear alls)**。

# 检测器列表的过滤器组

可单独或组合使用多个过滤器组，以过滤检测器列表。

### 名称

查找名称或描述包含您键入的字符串的检测器。字符串可包含任何字母数字或特殊字符。

### 自定义过滤器 (Custom Filter)

查找与对象管理页面上创建的自定义应用过滤器匹配的检测器。

### 作者

按检测器的创建者查找检测器。可按以下内容过滤检测器：

- 创建或导入自定义检测器的任何个别用户
- 思科代表所有思科提供的检测器，单独导入的附加检测器除外（您是自己导入的任何检测器的作者）
- **任何用户 (Any User)**，代表非思科提供的所有检测器

### 状态

根据检测器的状态（即**活动 [Active]** 或**非活动 [Inactive]**）查找检测器。

### 类型

根据检测器类型查找检测器，如应用检测器基础知识，第 2 页中所述。

### 协议

根据检测器检查的流量协议查找检测器。

### 类别

根据分配至所检测应用的类别查找检测器。

### 标签

根据分配至所检测应用的类别查找检测器。

### 风险

根据分配到所检测应用的风险查找检测器：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 和**非常低 (Very Low)**。

**业务关联性 (Business Relevance)**

根据分配至所检测应用的业务关联性查找检测器：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 和**非常低 (Very Low)**。

# 导航至其他检测器页面

**过程**

**步骤 1** 选择**策略** > **应用检测器**。

**步骤 2** 如果要查看下一页，请点击 **右箭头**（ > ）。

**步骤 3** 如果要查看上一页，请点击 **左箭头**（ < ）。

**步骤 4** 如果要查看另一页，请键入页码并按 Enter 键。

**步骤 5** 如果要跳到最后一页，请点击 **右端箭头**（ >| ）。

**步骤 6** 如果要跳到第一页，请点击 **左端箭头**（ |< ）。

# 激活和停用检测器

必须激活检测器，然后才能将其用于分析网络流量。默认情况下，思科提供的所有检测器均已激活。

可为每个端口激活多个应用检测器，以补充系统的检测能力。

在策略的访问控制规则中包含应用并部署策略时，如果该应用没有活动检测器，一个或多个检测器将会自动激活。类似地，在已部署策略中使用应用时，如果停用检测器会使该应用没有活动检测器，则不能停用检测器。

**提示** 为提高性能，请停用任何您不打算使用的应用协议、客户端或 Web 应用检测器。

**注意** 激活或停用系统或自定义应用检测器会立即重启 Snort 进程，而不会执行部署过程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

过程

**步骤 1** 选择**策略** > **应用检测器**。

**步骤 2** 点击要激活或停用的检测器旁边的滑块。 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。

注释 其他检测器可能需要某些应用检测器。如果停用其中一个检测器，系统会显示警告表明依赖于它的检测器也已被禁用。

# 编辑自定义应用检测器

使用以下程序修改自定义应用检测器。

过程

**步骤 1** 选择**策略** > **应用检测器**。

**步骤 2** 点击要修改的检测器旁边的 **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** 对检测器进行更改，如配置自定义应用检测器，第 10 页中所述。

**步骤 4** 根据检测器的状态，您具有以下保存选择：

- 要保存非活动检测器，请点击**保存 (Save)**。
- 要将非活动检测器另存为新的非活动检测器，请点击**另存为新项目 (Save as New)**。
- 要保存活动检测器并立即开始使用，请点击**保存并重新激活 (Save and Reactivate)**。

  注意 保存和重新激活自定义应用检测器后，无需执行部署过程即可立即重启 Snort 进程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

- 要将活动检测器另存为新的非活动检测器，请点击**另存为新项目 (Save as New)**。

# 删除检测器

可以删除自定义检测器以及单独导入的由思科专业服务提供的附加检测器。不能删除思科提供的任何其他检测器，不过可以停用其中许多检测器。

**注释** 当检测器正在已部署的策略中使用时，不能删除该检测器。

**注意** 删除已激活的自定义应用检测器将立即重启 Snort 进程，而无需执行部署流程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

过程

**步骤 1** 选择**策略** > **应用检测器**。

**步骤 2** 点击要删除的检测器旁边的 **删除**（ ）。 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** 点击**确定 (OK)**。

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。