入侵策略

以下主题说明了入侵策略和密切相关的网络分析策略 (NAP)。入侵策略包括用于检查流量中的威胁并阻止看似为攻击的流量的规则。网络分析策略控制流量预处理，通过规范化流量和识别协议异常来准备要进一步检查的流量。

由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略必须相互补充。

关于入侵和网络分析策略

网络分析和入侵策略配合使用，以检测和防止入侵威胁。

- 网络分析策略 (NAP) 监管流量如何解码和预处理，以便可以进一步对其进行评估，尤其是对于可能指示入侵尝试的异常流量。
- 入侵策略使用入侵和预处理器规则（统称为入侵规则），根据模式检测已解码数据包是否存在攻击。入侵规则可防止（丢弃）有威胁的流量并生成事件，或直接检测（警告）有威胁流量并仅生成事件。

在系统分析流量时，进行解码和预处理的网络分析阶段发生在入侵防御阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

系统定义的网络分析和入侵策略

系统包括几对相辅相成的同名网络分析和入侵策略。例如，名称同为“平衡安全和连接”的NAP策略和入侵策略要一起使用。系统提供的策略由思科 Talos 智能小组 (Talos) 配置。对于这些策略，Talos设置入侵和预处理器规则状态，并提供预处理器和其他高级设置的初始配置。

随着新的漏洞被发现，Talos会发布入侵规则更新。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理器规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

您可以手动更新规则数据库，或配置定期更新计划。更新必须部署，才能生效。有关更新系统数据库的更多信息，请参阅更新系统数据库。

以下是系统提供的策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。系统默认使用“平衡安全和连接”网络分析策略。

“连接优先于安全”网络分析和入侵策略

这些策略专为连接（即能够获取所有资源）优先于网络基础设施安全的网络而构建。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测”网络分析和入侵策略

此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

检测模式：预防与检测

默认情况下，所有入侵策略在防御模式下运行，以实施入侵防御系统(IPS)。在防御检测模式下，如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

如果想要测试入侵策略对网络的影响，则可以更改为“检测”模式，从而实施入侵检测系统 (IDS)。在此检测模式下，丢弃规则的处理方式类似于报警规则，在这种情况下，系统会通知您匹配的连接，但操作结果变为“将被阻止”，而事实上绝不会阻止连接。

您可以更改每个入侵策略的检测模式，以便组合使用防御与检测功能。

Snort 3 网络分析策略 (NAP) 也有检测模式。与入侵策略不同，NAP 策略是全局策略，因此您必须在防御或检测模式下运行所有NAP处理。您应使用为入侵策略使用的相同模式。如果您混合使用防御和检测策略，请选择“防御”以匹配最严格的入侵策略。

入侵和预处理器规则

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

系统包含思科 Talos 智能小组 (Talos) 创建的以下类型的规则：

- 入侵规则，可细分为共享对象规则和标准文本规则
- 预处理器规则，是指与网络分析策略中的预处理器和数据包解码器检测选项关联的规则。默认情况下禁用大多数预处理器规则。

以下主题更深入地介绍入侵规则。

入侵规则属性

当您查看入侵策略时，可以看到可用于识别威胁的所有入侵规则的列表。

每个策略的规则列表都是相同的。不同的是为每个规则配置的操作。由于规则数量在 30,000 条以上，所以滚动列表需要时间。滚动列表时会显示规则。

以下是定义每个规则的属性：

>（签名说明）

点击左列的 > 按钮可打开签名说明。说明内容是 Snort 检测引擎用来根据规则匹配流量的实际代码。代码介绍不在本文范围之内，有关详细信息，请参阅 管理中心配置指南；请从 http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html中选择适合您的软件版本的书籍。查找入侵规则编辑的相关信息。

签名包含某些项目的变量。有关详细信息，请参阅默认入侵变量集，第 4 页。

GID

生成器标识符 (ID)。此数字指示评估规则并生成事件的系统组件。1 表示标准文本入侵规则，3 表示共享对象入侵规则。（对于 设备管理器用户，这些规则类型差异没有意义。）这些是在配置入侵策略时主要关注的规则。有关其他 GID 的信息，请参阅生成器标识符，第 5 页。

SID

Snort 标识符 (ID)，也称为签名 ID。低于 1000000 的 Snort ID 由思科 Talos 智能小组 (Talos) 创建。

操作

此规则在所选入侵策略中的状态。此策略内每个规则的默认操作后面会添加“（默认）”。要使规则返回其默认设置，请选择此操作。可能的操作包括：

- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
- **禁用** - 不针对此规则匹配流量。不生成事件。

状态

对于Snort 2规则，“状态”为单独的一列。如果更改规则的默认操作，此列将显示“已覆盖”。否则，该列为空。

对于 Snort 3 规则，“覆盖”状态显示在“操作”属性的底部（如果您已更改）。

消息

这是规则的名称，规则触发的事件中也会显示该名称。消息通常标识签名匹配的威胁。通过互联网可搜索每个威胁的详细信息。

默认入侵变量集

入侵规则签名包含某些项目的变量。以下是这些变量的默认值，其中最常用的变量是 $HOME_NET 和 $EXTERNAL_NET。请注意，协议与端口号分开指定，所以端口变量只是数字。

- $DNS_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $EXTERNAL_NET = 任何 IP 地址。
- $FILE_DATA_PORTS = $HTTP_PORTS、143、110。
- $FTP_PORTS = 21、2100、3535。
- $GTP_PORTS = 3386、2123、2152。
- $HOME_NET = 任何 IP 地址。
- $HTTP_PORTS = 144 个端口号：36、80-90、311、383、443、555、591、593、631、666、801、808、818、901、972、1158、1212、1220、1414、1422、1533、1741、1830、1942、2231、2301、2381、2578、2809、2980、3029、3037、3057、3128、3443、3507、3702、4000、4343、4848、5000、5117、5222、5250、5450、5600、5814、6080、6173、6767、6988、7000、7001、7005、7071、7080、7144、7145、7510、7770、7777-7779、8000、8001、8008、8014、8015、8020、8028、8040、8060、8080-8082、8085、8088、8118、8123、8161、8180-8182、8222、8243、8280、8300、8333、8344、8400、8443、8500、8509、8787、8800、8888、8899、8983、9000、9002、9060、9080、9090、9091、9111、9290、9443、9447、9710、9788、9999、10000、11371、12601、13014、15489、19980、23472、29991、33300、34412、34443、34444、40007、41080、44449、50000、50002、51423、53331、55252、55555、56712。
- $HTTP_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $ORACLE_PORTS = 任何
- $SHELLCODE_PORTS = 180。
- $SIP_PORTS = 5060、5061、5600
- $SIP_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $SMTP_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $SNMP_SERVERS = $HOME_NET（表示任何 IP 地址）。

- $SQL_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $SSH_PORTS = 22。
- $SSH_SERVERS = $HOME_NET（表示任何 IP 地址）。
- $TELNET_SERVERS = $HOME_NET（表示任何 IP 地址）。

生成器标识符

生成器标识符 (GID) 标识评估入侵规则并生成事件的子系统。标准文本入侵规则的生成器 ID 为 1，共享对象入侵规则的生成器 ID 为 3。对于各种预处理器也有几套规则。下表解释了 GID。

表 *1:* 生成器 *ID*

ID	组件
1	标准文本规则。
2	标记的数据包。 （标记生成器规则，根据标记会话生成数据包。）
3	共享对象规则。
102	HTTP 解码器。
105	Back Orifice 检测器。
106	RPC 解码器。
116	数据包解码器。
119、120	HTTP 检查预处理器。 （GID 120 规则与服务器特定 HTTP 流量相关。）
122	Portscan 检测器。
123	IP 分片重组器。
124	SMTP 解码器。 （针对 SMTP 动词的攻击）
125	FTP 解码器。
126	Telnet 解码器。
128	SSH 预处理器。
129	流预处理器。

ID	组件
131	DNS 预处理器。
133	DCE/RPC 预处理器。
134	规则延迟，数据包延迟。 （规则延迟暂停 (SID 1) 或重新启用 (SID 2) 一组入侵规则，或系统由于超出数据包延迟阈值 (SID 3) 而停止检查数据包时，生成这些规则的事件。）
135	基于速率的攻击检测器。 （与网络上主机的连接过多。）
137	SSL 预处理器。
138、139	敏感数据预处理器。
140	SIP 预处理器。
141	IMAP 预处理器。
142	POP 预处理器。
143	GTP 预处理器。
144	Modbus 预处理器。
145	DNP3 预处理器。

网络分析策略

网络分析策略控制流量预处理。预处理器通过规范化流量和标识协议异常，准备要进行进一步检查的流量。网络分析相关预处理发生在安全智能丢弃和 SSL 解密之后进行，但在访问控制和入侵或文件检测开始之前进行。

默认情况下，系统使用“平衡安全和连接”网络分析策略预处理由访问控制策略处理的所有流量。但是，如果在任何访问控制规则上配置入侵策略，系统将使用与所应用的最严格入侵策略匹配的网络分析策略。例如，如果在访问控制规则中同时使用“安全优先于连接”策略和“平衡”策略，则系统将对所有流量使用“安全优先于连接”NAP。对于 Snort 3 自定义入侵策略，此分配根据分配给入侵策略的基本模板策略完成。

使用 Snort 3 时，您可以明确选择一个策略，并选择性地自定义其设置。建议您选择名称与用于通过设备的大多数流量的入侵策略匹配的策略，无论是直接使用入侵策略，还是将其用作自定义入侵策略中的基本策略。然后，您可以更改检测模式，或调整特定检查器或绑定程序设置，以考虑网络中的流量。

此外，请考虑您是否在入侵策略中启用了预处理器规则。如果您启用需要预处理器的规则，请确保同时在 NAP 中启用相应检查器。对于每个检查器，您还可以调整检查器的属性，包括检查的端口（绑定程序），以自定义网络的检查器行为。

注释 如果您使用的是 Snort 2，系统将使用同名的 NAP 策略作为您在任何访问控制规则中应用的最严格的入侵策略，并且您无法编辑检查器或绑定程序设置。

入侵策略的许可证要求

只有启用**IPS** 许可证，才能在访问控制规则中应用入侵策略。有关配置许可证的信息，请参阅启用或禁用可选许可证。

网络分析策略无需额外的许可证。

在访问控制规则中应用入侵策略

要将入侵策略应用于网络流量，请在允许流量的访问控制规则中选择该策略。不得直接分配入侵策略。

可以根据所保护网络的相对风险分配不同的入侵策略，以提供可变的入侵保护。例如，可以对内部网络与外部网络之间的流量使用更严格的“安全优先于连接”策略。另一方面，可以对内部网络之间的流量应用更宽松的“连接优于安全”策略。

此外，还可以通过对所有网络使用相同的策略来简化配置。例如，“平衡安全和连接”策略用于提供良好的保护，且不会对连接产生过多的影响。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 创建新规则或编辑**允许**流量的现有规则。

如果允许默认操作，还可在默认操作中指定入侵策略。

不得将入侵策略应用于信任或阻止流量的规则。

步骤 3 点击**入侵策略**选项卡。

步骤 4 依次选择**入侵策略** > **开**，然后选择要在匹配流量中使用的入侵检测策略。

在 Snort 2 和 Snort 3 之间切换

Snort 是产品的主要检测引擎。虽然可以自由切换 Snort 版本，但 Snort 2.0 中的某些入侵规则未在 Snort 3.0 中提供，反之亦然。如果对其中一项规则更改了规则操作，则在从 Snort 3 切换到 Snort 2 或再次切换回 Snort 3 时，不会保留该更改。您对两个版本中现有规则的规则操作更改都将被保留。请注意，Snort 3 与 Snort 2 中的规则之间的映射可以是一对一或一对多的，因此系统将尽可能保留更改。

如果更改Snort版本，系统将执行自动部署以实施更改。您可以在任务列表中查看进度。这些任务是 Snort 版本更改和自动部署 - Snort 版本切换。由于部署以及必须停止并重新启动 Snort 的事实，所有现有连接（包括 VPN）都将被丢弃并必须重新建立，这将导致瞬时流量丢失。

注释 如果您尝试切换Snort版本但切换失败，您将无法放弃待处理的更改，并且系统不允许进行后续切换尝试。如果发生这种情况，您必须使用 ToggleInspectionEngine API 完成切换，您可以在 API Explorer 中使用该 API。您必须将 bypassPendingChangeValidation 属性设置为 TRUE。

开始之前

要确定当前启用的 Snort 版本，请使用此程序，或依次选择**策略** > **入侵**。查看表上方的 **Snort 版本**行。当前版本是完整版本号中的第一个数字。例如，2.9.17-95 是 Snort 2 版本。

如果设备位于气隙网络中，请考虑在切换之前手动上传新版本的最新规则包。

如果降级到2.0，您创建的所有自定义入侵策略都将转换为自定义策略中使用的基本策略。尽可能保留“覆盖”规则操作。如果多个自定义策略使用相同的基本策略，则系统将保留大多数访问控制策略中使用的自定义策略“覆盖”操作，而其他自定义策略的“覆盖”操作将丢失。现在，使用这些“复制”策略的访问控制规则将使用根据最常用自定义策略创建的基本策略。所有自定义策略都将被删除。如果要保留自定义策略以便稍后导入，请在切换回 Snort 3 后使用 威胁防御 API 导出配置。

此外，降级到 2.0 会删除所有 NAP 自定义，并且系统会根据访问控制规则中使用的入侵策略切换为使用最合适的 NAP。

主动身份验证中的主机名重定向也需要 Snort 3，如果您切换到 Snort 2，它将被删除。

您必须部署所有待处理更改，然后才能切换 Snort 版本。

过程

步骤 1 选择**设备**，然后点击“更新”摘要中的**查看配置**。

查看**入侵规则**组。系统会显示当前的 Snort 版本。

步骤 2 在**入侵规则**组中，您可以通过点击**升级到 Snort 3.0** 或**降级到 Snort 2.0** 来更改 Snort 版本。

步骤 3 当系统提示您确认操作时，请选择获取最新入侵规则包的选项，然后点击**是**。

我们建议您获取最新的规则包。系统仅下载活动 Snort 版本的包，因此无法安装您要切换到的 Snort 版本的最新包。

您必须等到切换版本的任务完成后，才能编辑入侵策略。

为入侵事件配置系统日志

可以为入侵策略配置外部系统日志服务器，从而将入侵事件发送至系统日志服务器。必须根据入侵策略配置系统日志服务器，从而将入侵事件发送到服务器。根据访问规则配置系统日志服务器只可将连接事件（而不是入侵事件）发送到系统日志服务器。

如果选择多个系统日志服务器，事件将发送到每个服务器。

入侵事件的消息 ID 为 430001。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击**入侵策略设置**按钮 (⚙) 来配置系统日志。

步骤 3 点击**将入侵事件发送到**字段下的 **+**，然后选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建相应对象。

步骤 4 点击**确定 (OK)**。

配置网络分析策略 (Snort 3)

网络分析策略 (NAP) 应用于设备上所有允许的连接。NAP 确定启用了哪些检查器，以及检查器使用的属性值。绑定程度确定应与各种检查器关联的端口和协议。

协调 NAP 与您在访问控制规则中应用的入侵策略：

- 如果您在访问控制规则中使用单个入侵策略，请选择同名的 NAP。然后，根据入侵策略中的设置对检查器和属性进行调整。例如，如果您为某个特定检查器（例如 CIP）启用入侵规则，请确保在 NAP 中启用该检查器。
- 如果您使用多个入侵策略，请选择与您使用的最严格的入侵策略匹配的 NAP。
- 如果您使用自定义入侵策略，请根据自定义入侵策略的基本入侵策略选择 NAP。
- 如果不需要自定义任何检查器或绑定程序，请考虑将系统配置为根据您的入侵策略使用情况自动选择最合适的 NAP。这是默认选项。

开始之前

除非您阻止，否则系统会定期将 LSP 更新下载到检测规则中。这些更新可以添加或删除检查器和属性，以及更改属性的默认设置。如果对已删除的检查器进行了覆盖，则会保留这些覆盖，并且您将看到不再支持检查器的警告。在这种情况下，请删除检查器并进行任何其他标记调整，以确保您的 NAP 完全有效。

过程

步骤 1 依次选择**策略** > **入侵**。

验证表上方显示的 Snort 版本是否为 3.x。

步骤 2 点击**入侵策略设置按钮** (⚙)。

步骤 3 在**默认网络分析策略**中，选择以下选项之一：

- **自动** - 自动选择与访问控制规则中应用的最常用入侵策略（或自定义规则的基本策略）相匹配的NAP。如果不应用任何入侵策略，则会使用“安全性和连接性均衡”NAP。NAP在防御模式下运行，您无法自定义入侵或绑定程序设置。在自动模式下运行时，此程序的其余部分不适用。
- **自定义** - 明确选择应当使用的 NAP。点击策略名称旁边的**编辑**链接可选择不同的策略。然后，您可以选择检测模式，并自定义检查器和绑定程序设置，如以下步骤所述。

步骤 4 在“编辑网络分析策略”对话框中，选择策略并配置其设置。

a) 在**网络分析策略**中，选择应全局应用于所有允许连接的策略。

b) 选择**检测模式**。

检测模式决定了如何处理不合规的流量。为了获得最佳效果，请使用与入侵策略所用模式相同的检测模式。

- **防御** - 根据策略中的设置阻止所有解码器异常、规范化异常或协议异常。如果启用SSL解密策略，或者在访问控制策略设置中启用了 **TLS 服务器身份发现** 选项，则必须使用此选项。
- **检测** - 只会就解码器异常、规范化异常或协议异常发出警报。不会阻止任何流量。

c) （可选。）配置并管理对检查器和绑定程序的覆盖：

- 要编辑覆盖，请参阅配置检查器和绑定程序覆盖 ， 第 11 页。
- 要下载架构或覆盖，请参阅下载覆盖和架构 ， 第 12 页。
- 要上传覆盖，请参阅上传覆盖 ， 第 13 页。
- 要重置所有覆盖，请点击NAP文件上方的**重置检查器/绑定程序覆盖**链接。系统会要求您确认重置。如命令名称所示，只能对检查器或绑定程序执行删除操作。例如，删除所有绑定程序覆盖不会改变检查器覆盖。
- 要撤销对选定检查器的所有更改，请点击**将检查器重置为默认值**。

- 要过滤视图以仅查看具有覆盖的检查器，请点击**仅显示覆盖**。点击**显示所有检查器**可删除过滤器

d) 点击**确定 (OK)**。

配置检查器和绑定程序覆盖

当您选择基本NAP时，您选择的是该基准策略中包含的检查器设置。大多数情况下，这些是适当的设置。

但是，您可以覆盖所选NAP中的设置。例如，您可以启用或禁用单个检查器，或者更改属性或绑定程序的值。

以下程序介绍了如何直接配置覆盖。或者，您也可以下载架构，离线进行更改，然后上传您的覆盖。您还可以上传从另一台设备下载的覆盖。

开始之前

说明每个检查器、绑定程序和属性不在本文档范围之内。有关详细信息（包括示例），请参阅 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference.html 上提供的 *Snort 3* 检查器参考。

过程

步骤 1 依次选择**策略** > **入侵**，点击**入侵策略设置**按钮 ( )，为 NAP 设置选择**自定义**，然后点击策略名称旁边的**编辑**链接。

步骤 2 点击包含您要更改的设置的选项卡：

- **检查器** - 检查器检查特定类型的流量（例如 FTP）是否存在协议异常。
- **绑定程序** - 绑定程序检查器确定何时需要使用服务检查器来检查流量。绑定程序检查器中的配置包括端口、主机、CIDR 以及定义网络分析策略中的另一个检查器何时需要检查流量的服务。

步骤 3 根据需要编辑设置。

- 使用以下项控制 JSON 编辑器中的视图：
  - 使用**过滤器**编辑框对 JSON 文件执行全文搜索。
  - 点击**展开所有字段 (Expand All Fields)** 按钮 ( )，打开 JSON 文件中的所有文件夹。
  - 点击**折叠所有字段**按钮 ( )，关闭 JSON 文件中的所有文件夹。
  - 点击**撤销上次操作**按钮 ( )，撤销最近的更改。
  - 点击**重做**按钮 ( )，重做上次撤销的更改。

- 选择**树**，查看 JSON 文件的格式化视图，其中包括操作菜单、错误标志和其他可指导您进行编辑的功能。
- 选择**代码**，查看原始 JSON 文件。

- 在“树”视图中，点击**菜单**按钮 (▮) 可操作文件的内容。您可以执行以下操作：
  - **插入**属性。使用“自动”选项可允许编辑器确定适当的数据类型。否则，请添加数组、对象或字符串。如果您添加无效属性，系统会将检查器或绑定程序标记为存在必须解决的问题。
  - **附加**属性。此操作与“插入”的作用相同，但会将属性放在相应部分的末尾。
  - **复制**所选属性。
  - **移除**（删除）所选属性。编辑属性时，弹出消息也可能提供**删除**命令。
- 要启用当前禁用的检查器，或更改任何布尔属性的设置，请点击属性值前面的复选框。例如，要启用检查器，请将 **enabled : false** 属性更改为：

- 要更改字符串或数字属性的值，请点击相应属性并根据需要编辑值。如果您输入的内容违反了相应字段的规则，错误消息会解释不符之处。例如，如果您输入的值超出范围，则数值会指示值的有效范围。
- 要重置覆盖，请执行以下操作：
  - 点击**重置检查器/绑定程序覆盖**可删除您对所有检查器或绑定程序所做的所有更改，并返回默认值。如命令名称所示，只能对检查器或绑定程序执行删除操作。例如，删除所有绑定程序覆盖不会改变检查器覆盖。
  - 点击**将检查器重置为默认值**可仅撤销对所选检查器所做的所有更改。
- 要过滤视图以仅查看具有覆盖的检查器，请点击**仅显示覆盖**。点击**显示所有检查器**可删除过滤器
- 如果某个检查器不再受支持，则系统会用一条消息标记该检查器。点击消息中的**删除检查器**链接可删除该检查器。

步骤 4 完成后点击**确定**。

下载覆盖和架构

您可以下载 NAP 架构，或下载您为策略配置的覆盖。

每当您更改基本NAP时，建议下载覆盖，以防您想返回到之前的设置。此外，您可以在一台设备上使用 JSON 编辑器来实施要在所有设备上使用的覆盖，下载覆盖，然后将该覆盖文件上传到其他设备。

如果您想离线编辑文件，然后将覆盖上传到此设备或多台设备，则下载架构非常有用。您应该只复制/粘贴您需要更改的部分，而不是上传整个文件，以确保只有您所做的更改才被视为覆盖。

过程

步骤 1 依次选择**策略** > **入侵**，点击**入侵策略设置**按钮 ( )，为 NAP 设置选择**自定义**，然后点击策略名称旁边的**编辑**链接。

步骤 2 执行以下操作之一：

- 要下载当前选择的 NAP 的架构，请点击齿轮图标 ( ) 并选择**下载** > **策略架构**。
- 要下载已保存的覆盖集，因为它们在当前编辑会话之前就已存在，请点击齿轮图标 ( ) 并选择**下载** > **上次保存的覆盖**。该文件包括覆盖的属性及其包含的对象。
- 要下载您在当前编辑会话中创建的覆盖，请点击齿轮图标 ( ) 并选择**下载** > **当前未保存的覆盖**。该文件包括覆盖的属性及其包含的对象。

上传覆盖

您可以下载 NAP 策略架构，离线编辑文件，然后上传文件，而不是使用嵌入式 JSON 编辑器编辑属性。然后，在上传的文件中配置的所有覆盖都将应用于选定的 NAP。

您还可以上传在另一台设备上配置覆盖后下载的文件。

通过上传覆盖，您可以将同一文件上传到多台设备，并轻松应用相同的覆盖。

开始之前

要覆盖网络分析策略中的检查器配置，您应只上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认值或配置的任何后续更改作为 LSP 更新的一部分。确保上传的覆盖仅专注于您想要更改的属性。

过程

步骤 1 依次选择**策略** > **入侵**，点击**入侵策略设置**按钮 ( )，为 NAP 设置选择**自定义**，然后点击策略名称旁边的**编辑**链接。

步骤 2 点击齿轮图标 ( ) 并选择**上传** > **覆盖**。

步骤 3 （可选。）点击其中一个**下载**链接，以保存现有覆盖的副本。

您可以下载上次保存的覆盖（在当前编辑会话之前创建的覆盖）或当前未保存的覆盖（在当前编辑会话期间创建的覆盖）。

步骤 4 点击“确认上传覆盖”对话框上的**是**，以确认您要继续。

步骤 5 点击**浏览**或拖放以选择包含覆盖的 JSON 文件，然后点击**确定**。

管理入侵策略 (Snort 3)

当您使用 Snort 3 作为检测引擎时，您可以创建自己的入侵策略，并根据自己的目的对其进行自定义。系统随附基于同名思科 Talos 智能小组 (Talos) 定义的策略的预定义策略。虽然可以编辑这些策略，但最好根据基础 Talos 策略创建自己的策略，并在需要调整规则操作时进行更改。

其中每个预定义策略包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于启用状态，但在另一个策略中可能被禁用。

如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

相反，如果您知道自己需要防御特定的攻击，但相关规则在您所选的入侵策略中被禁用，可以启用该规则而不必更改为更安全的策略。

使用与入侵相关的控制面板和事件查看器（两者均在**监控 (Monitoring)** 页面）可评估入侵规则对流量的影响。请记住，仅将匹配入侵规则的流量设为警告或丢弃时，才会看到入侵事件和入侵数据；系统不评估禁用的规则。

注释 如果切换到 Snort 2，则无法创建自定义策略，并且入侵策略的使用略有不同。请不要参阅此主题，而是参阅管理入侵策略 (Snort 2)，第 26 页。

过程

步骤 1 依次选择**策略** > **入侵**。

验证表上方显示的 Snort 版本是否为 3.x。

步骤 2 执行以下任一操作：

- 使用**搜索/过滤器**框查找策略。您只能按名称搜索。
- 点击齿轮图标 (⚙) 可启用将日志记录发送至系统日志服务器。请参阅为入侵事件配置系统日志，第 9 页。
- 点击齿轮图标 (⚙) 可配置网络分析策略 (NAP)。请参阅配置网络分析策略 (Snort 3)，第 9 页。
- 点击 + 可创建新的策略。请参阅配置自定义入侵策略 (Snort 3)，第 15 页。
- 点击编辑图标 (✎) 可查看策略中的属性和规则，并进行编辑。请参阅查看或编辑入侵策略属性 (Snort 3)，第 16 页。

- 点击删除图标 ( ) 可删除策略。

配置自定义入侵策略 (Snort 3)

如果预定义策略不符合您的需求，您可以创建新的入侵策略以自定义规则行为。通常，最好根据预定义策略创建自定义策略，而不是修改这些策略。如果您发现自定义无法实现所需的结果，这样可以确保您轻松实施 Cisco Talos 定义的策略之一。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 执行以下操作之一：

- 要创建新策略，请点击 **+**。
- 要编辑某个现有策略，请点击该策略的编辑图标 ( )。当显示策略详细信息时，点击页面顶部策略属性部分中的**编辑 (Edit)** 链接。

步骤 3 为该策略输入**名称**和说明（后者为可选项）。

步骤 4 为策略配置**检测模式**。

- **防御** - 始终应用入侵规则操作。匹配丢弃规则的连接将被阻止。
- **检测** - 入侵规则仅生成警报。匹配丢弃规则的连接将生成警报消息，但不会阻止连接。

步骤 5 为策略选择**基本模板**。

基本模板由 Cisco Talos 提供。点击每个模板的信息图标可查看有关策略的详细信息。请注意，在安装新的规则包时，策略名称可以更改，并且会显示新策略。

- **最大限度检测 (Cisco Talos)** - 此策略只强调安全性。不保证网络连接性和吞吐量，也可能出现误报。此策略应仅用于高安全性区域，并且必须配备安全监控器来调查警报，以确定其有效性。
- **安全优先于连接 (Cisco Talos)** - 此策略可能以牺牲网络连接和吞吐量为代价而强调安全。对流量进行更深入的检测，评估更多的规则，并且预期会出现误报以及延迟增加，但都在合理的范围内。
- **平衡安全和连接 (Cisco Talos)** -（默认设置。）此策略试图在网络连接性和吞吐量与安全性需求之间达到精细均衡。虽然不像“安全优先于连接”那样严格，但此策略试图在保持用户安全的同时降低对正常流量的干扰。
- **连接优先于安全 (Cisco Talos)** - 此策略可能以牺牲安全为代价而强调网络连接和吞吐量。对流量的检测不够深入，评估的规则也较少。

- **无活动规则 (Cisco Talos)** - 此策略是配置典型预处理器设置但未启用任何规则或内置警报的基本策略。如果要确保仅启用要应用的策略，请使用此策略作为基础策略。

步骤 6 点击**确定**。

系统会将您返回到入侵策略列表。现在，您可以查看新策略并根据需要调整规则操作。

查看或编辑入侵策略属性 (Snort 3)

“入侵策略”(Intrusion Policy) 页面显示策略列表，包括预定义和用户定义的策略及其说明。要编辑策略，必须先查看策略的属性。

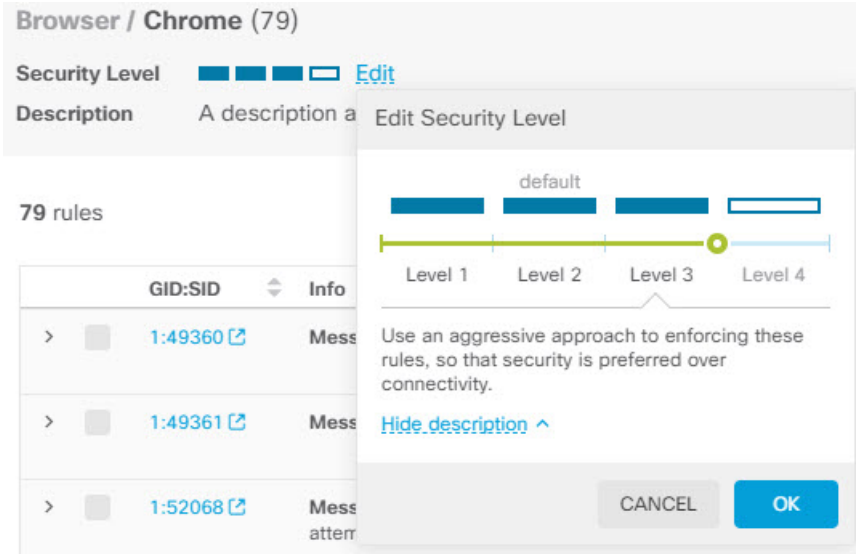
过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ( )。

策略包含以下部分：

- **策略名称**下拉列表。
  - 您可以通过从下拉列表中选择策略轻松切换到其他策略，也可以通过点击后退按钮 ( ) 返回到策略列表。
  - 您可以通过点击策略名称 ( ) 旁边的删除图标来删除此策略。
- **常规属性**。此部分显示入侵模式、基本策略和说明。点击**编辑**以更改这些属性或策略名称。
- **规则组**目录。此列表显示策略中具有活动规则的所有规则组。这些组具有层次结构，其中父组包含子组，子组将较大的父组内的规则划分为不同子集。每个组都是规则的逻辑集合，一个规则可以出现在多个组中。
  - 要添加当前在策略中没有活动规则的组，请点击 + > **添加现有规则组**并选择该组。请参阅在入侵策略中添加或删除规则组 (Snort 3)，第 18 页。
  - 要更改组的安全级别，请在列表中选择子组。规则列表改为在顶部显示安全级别，下面列出组中的规则。点击安全级别旁边的**编辑**链接并选择新级别。编辑时，点击**查看说明**可获取有关每个安全级别的信息。请注意，更改级别可以更改哪些规则处于活动状态，也可以更改给定规则的操作，安全级别越多，活动规则往往就越多，而且具有“丢弃”操作的规则也越多。点击**确定**，确认更改。（安全级别不适用于自定义规则组。）



- 要删除组中的所有规则，请在列表中选择子组。然后，点击组名称最右侧的**排除**链接，并确认要排除该组。排除组仅会禁用组中的所有规则，而不会删除组。

  但是，如果组包含与其他已启用组共享的规则，则共享规则会保留仍处于活动状态的组应用的所有操作。在所有情况下，无论组成员身份如何，我们都会为单个规则保留最严格的设置。

- 要添加自定义规则的新自定义规则组，请点击 + > **上传自定义规则**。有关详细信息，请参阅上传自定义入侵规则，第 22 页。

- 要更改自定义规则组的名称或说明，请点击**编辑**。

- 要删除自定义规则组，请点击**删除**。有关详细信息，请参阅管理自定义入侵规则和规则组，第 21 页。

- 要在自定义规则组中添加新的自定义规则，请点击规则表上方的 +。请参阅配置单独自定义入侵规则，第 24 页。

- 要编辑、复制、删除或管理自定义规则的组成员身份，请将鼠标悬停在规则右侧，然后点击相应的按钮或命令。有关详细信息，请参阅配置单独自定义入侵规则，第 24 页。

- **规则列表**。您可以使用搜索字段来帮助您使用全文搜索查找规则。您还可以选择过滤项目来对 GID 或 SID 的任意组合进行搜索， 仅显示用户定义的规则（您添加的规则）， 仅显示操作被覆盖的规则，或者仅根据其操作（禁用、警报、丢弃）显示规则。规则是延迟加载的，因此滚动浏览整个未过滤的列表需要相当长的时间。过滤列表时，点击刷新按钮可重新加载已过滤的视图。

  - 要更改规则的操作，请点击规则的**操作**单元格，然后选择以下新操作：仅生成**警报**，**阻止**匹配规则的流量，或**禁用**规则。系统会指示每个规则的默认操作。

  - 要一次更改多个规则的操作，请点击要更改的规则左列中的复选框，然后从规则表上方的**操作**下拉列表中选择新操作。点击 GID:SID 表标题中的复选框以选择列表中的所有规则。一次最多可以更改 5000 条规则。

- 要更新自定义规则组中的规则，请点击**上传规则文件**。有关详细信息，请参阅上传自定义入侵规则，第 22 页。
- 要获取有关规则的更多信息，请点击 **GID:SID** 单元格中的链接。该链接会将您引导至 Snort.org。
- 要更改列出的规则，您可以点击规则组目录中的子组（而不是父组）。您可以通过点击规则组列表顶部的**全部规则**返回到全部规则列表。
- 要更改排列顺序，请点击列的表标题。规则的默认排序方式是首先为覆盖规则，然后是丢弃规则，然后是警报规则。
- 要查看入侵规则 (LSP) 更新中进行了哪些更改，请在过滤器字段中选择 **LSP 更新**，然后选择要查看其更改的更新，并指定是要查看所有更改，还是仅查看规则添加或更改。

在入侵策略中添加或删除规则组 (Snort 3)

入侵规则划分为多个本地组。组具有层次结构，其中父组包含相关的子组。规则本身仅显示在子组中：父组只是一个组织结构。给定规则可以出现在多个组中。

您创建的任何自定义规则组都位于“用户定义的组”文件夹中。自定义规则组没有层次结构。

在入侵策略中添加或删除规则的最简单方法是添加或删除组。由于组中的规则在逻辑上是关联的，因此您很可能希望使用给定组中的大多数（如果不是全部）规则。

以下程序介绍如何添加组和更改组的安全级别。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击要更改的策略的编辑图标 ( )。

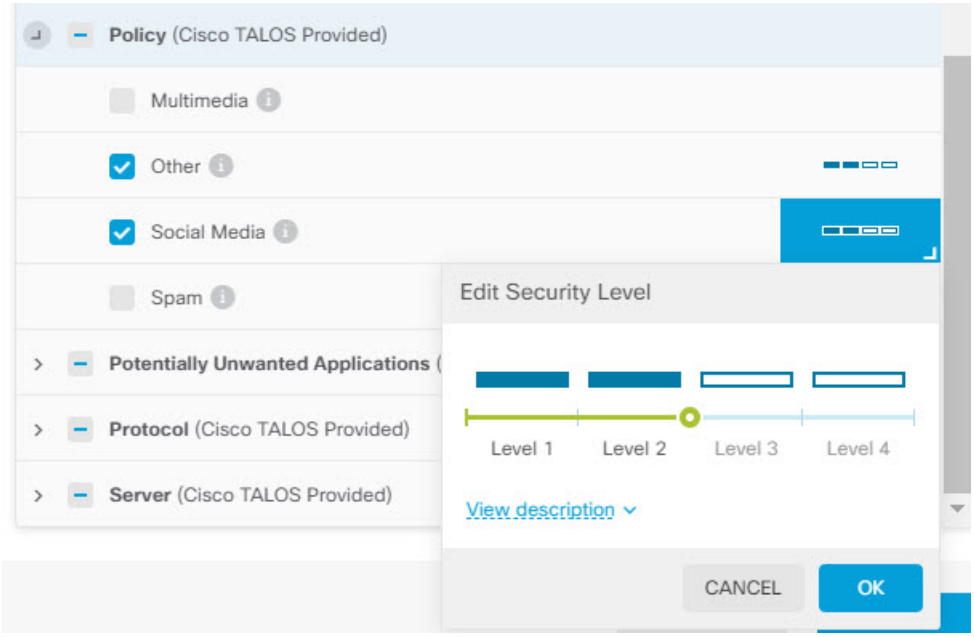
步骤 3 （添加组。）如果规则组列表中未显示该组，请点击 + > **添加现有规则组**并执行以下操作：

a) 查找子组。
   - 父组名称旁边的复选标记表示已选择父组中的所有子组。
   - 父组名称旁边的减号表示一个或多个子组没有为此策略启用规则。可以添加这些组。
   - 子组名称旁边的复选标记表示该组已被选中。

b) 选择要添加的组（即，选中其复选框）。

c) （可选，不适用于自定义规则组。）每个组都有一个默认安全级别，具体取决于自定义策略所用的基本策略。如果要更改它，请点击安全级别图标，选择新级别，然后点击**确定**。

级别 1 是最不安全的状态，强调连接优先于安全，而级别 4 是最严格的状态，提供最高级别的安全。您可以点击**查看说明**，在选择每个级别时查看其说明。



d) 继续选择（或取消选择）组，直到完成所有更改。

e) 点击**确定**。

步骤 4 （删除组。）如果要禁用组中的所有规则，可以使用以下任一方法：

- 选择组，然后点击规则列表上方组名称最右侧的**排除**链接。
- 使用添加组的方法，但取消选择不需要的组（即，取消选中其复选框），然后点击**确定**。
- 您可以删除自定义规则组，以将其从系统和使用该规则组的所有入侵策略中完全删除。选择组，然后点击**删除**。

更改入侵规则操作 (Snort 3)

每个入侵策略包含相同的规则。不同的是针对每个规则所采取的操作因策略而异。

通过更改规则操作，可以禁用为您提供过多误报的规则，也可以将规则更改为针对匹配流量发出警报或丢弃该流量。您还可以启用已禁用的规则，以警告或丢弃匹配的流量。

更改规则操作的最简单方法是更改规则组的安全级别。当您更改组的安全级别时，组内规则的操作也会更改。这可能意味着某些规则会启用（或禁用），或者操作可以根据您选择的安全状态评估在警报和丢弃之间切换。但是，如果需要，可以更改单个规则操作。

注释 给定规则的默认操作基于组和严重性的整体选择。更改组的严重性或排除组可以更改规则的默认操作。

开始之前

自定义规则组没有安全级别。不能使用安全级别技术更改自定义规则的规则操作。

过程

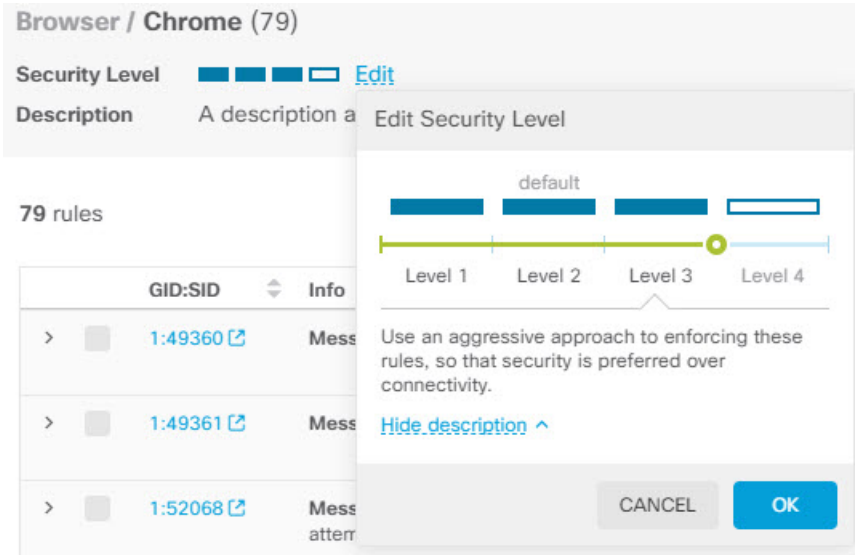
步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击您要更改其规则操作的策略的查看图标 ( )。

步骤 3 （这是建议方法。）更改规则组的安全级别。

a) 点击规则组列表中的子规则组。

b) 在规则列表上方，点击组安全级别旁边的**编辑**。



注释
如果要禁用组中的所有规则，请勿点击**编辑**。相反，请点击**排除**并确认要排除组。系统不会删除该组，而只是禁用其规则。跳过其余步骤。

c) 为组选择新级别。点击**查看说明**，查看您所选择的每个级别的说明。

级别 1 是最不安全的状态，强调连接优先于安全，而级别 4 是最严格的状态，提供最高级别的安全。

d) 点击**确定**。

步骤 4 （手动方法。）更改一个或多个规则的操作。

a) 查找您要更改其操作的规则。

使用**搜索/过滤器**框搜索规则信息中的字符串。您还可以选择过滤项目以对 GID 或 SID 的任意组合进行搜索，或者仅根据其操作（禁用、警报、丢弃）显示规则。规则是延迟加载的，因此滚动浏览整个未过滤的列表需要相当长的时间。过滤列表时，点击刷新按钮可重新加载已过滤的视图。

如果您正在与思科技术支持部门合力解决某个问题，最好可以从事件中或通过该部门获取 Snort 标识符 (SID) 和生成器标识符 (ID)。然后，您可以精确搜索规则。

b) 要更改操作，请执行以下操作之一：

- 一次更改一个规则 - 点击规则的**操作**列，选择所需的操作：
  - **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
  - **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
  - **禁用** - 不针对此规则匹配流量。不生成事件。
- 一次更改多个规则 - 点击要更改的规则的复选框，然后点击表上方的**批量**下拉列表并选择所需操作。点击 GID:SID 表标题中的复选框以选择列表中的所有规则。一次最多可以更改 5000 条规则。

管理自定义入侵规则和规则组

系统中附带思科 Talos 智能小组 (Talos) 定义的数千条入侵规则。如果您知道其他攻击，则可以创建和上传自定义入侵规则来过滤这些攻击，并发出警报或丢弃这些攻击。您也可以一次创建、编辑和删除一个规则。

对于上传的规则，您可以使用文本编辑器离线创建规则。建议您在上传的每个文本文件中包含一组自定义规则。然后，您可以轻松上传对规则的更改，将新规则合并到自定义规则组中，或将规则替换为新的已编辑副本规则。

介绍如何创建这些规则不属于本文档的范围。有关如何为 Snort 编写入侵规则（包括如何将 Snort 2 规则转换为 Snort 3 格式）的详细信息，请参阅 https://snort.org/documents 上的指南。例如，https://snort.org/documents/rules-writers-guide-to-snort-3-rules 上提供的面向规则编写者的 *Snort 3* 规则编写简介。

开始之前

您可以在上传自定义规则的过程中创建自定义规则组，如上传自定义入侵规则，第 22 页中所述，也可以在创建单个规则或管理规则成员时创建。创建组后，您可以管理组及其内容。

请注意，自定义组可用于所有入侵策略，而不仅仅是创建组时编辑的策略。因此，对组所做的更改会应用于所有策略。例如，如果删除某个自定义规则组，该规则组将从所有策略中删除，并且不再对其中任何策略可用。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ( )。

建议您将自定义规则添加到自定义入侵策略，而不是添加到其中一个内置策略。

步骤 3 执行以下任一操作：

- 要创建组，请点击 + > **上传自定义规则**。请参阅上传自定义入侵规则，第 22 页。
- 要编辑某个组的名称或说明，请在“用户定义的组”文件夹的组目录中选择该组。然后，您可以点击**编辑**并进行更改。
- 要从策略中排除该组及其规则，请在“用户定义的组”文件夹的组目录中选择该组。然后，您可以点击**排除**来删除该组。
- 要从系统及使用该组的所有策略中删除该组，请在“用户定义的组”文件夹的组目录中选择该组。然后，点击**删除**。请注意，如果某个规则仅存在于已删除的组中，那么该规则也会从系统中删除。但是，如果某个规则也存在于您不会删除的其他自定义规则组中，则该规则将保留在这些组中。
- 要批量替换或更新某个组中的规则，请在“用户定义的组”文件夹的组目录中选择该组。然后，点击该组的规则表上方“操作”下拉列表旁边的**上传规则文件**。流程与上传自定义入侵规则，第 22 页中介绍的流程相同。
- 要创建和管理单个规则及其向规则组的分配，请参阅配置单独自定义入侵规则，第 24 页。

上传自定义入侵规则

如果您知道其他规则当前未涵盖的攻击，则可以创建和上传自定义入侵规则来过滤这些攻击，并发出警报或丢弃这些攻击。导入规则的操作必须是 alert 或 drop，并且规则的默认操作由导入文件中的操作定义。导入后，您可以更改规则操作并根据需要禁用规则。

您必须离线创建这些规则。在 设备管理器中，您只需上传规则文件，而不是直接配置规则。规则文件应为文本文件。您可以使用换行符将规则设置为可读格式，或将规则放在一行中，并且允许使用空行。规则格式在 snort.org 中进行了说明。

例如，包含三个规则的上传文件可能如下所示：

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
```

```
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
   rev:1;
)
```

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ( )。

建议您将自定义规则添加到自定义入侵策略，而不是添加到其中一个内置策略。

步骤 3 执行以下操作之一：

- 在组列表上方，点击**+** > **上传自定义规则 (Action)**。
- 如果要将规则上传到某个已创建的自定义规则组，您可以选择该自定义规则组，然后点击该组的规则表上方**操作 (Action)** 下拉列表旁边的**上传规则文件 (Upload Rule File)**。

步骤 4 点击**浏览 (Browse)** 并选择自定义规则文件，或将文件拖放到“上传文件”对话框中。

等待上传完成。

步骤 5 选择处理冲突的方式：

当您添加的规则与系统中已有的规则相同时，会发生冲突。仅当您上传的规则或编辑的规则版本与之前上传的规则或规则版本相同时，才会出现这种情况。

选择以下选项之一：

注释
合并和**替换**基本相同。上传的规则的修订版本号必须高于已上传的修订版本号，才能对现有规则进行任何更改。唯一的区别是，如果上传文件缺少目标自定义规则组中的规则，**替换**选项将从规则组中删除这些规则。**合并**选项将保留这些“缺失”规则。

- **合并** - 如果上传文件中的规则具有更高的修订版本号，则上传文件中也存在于所选组中的任何已更改规则都将合并这些更改。任何未更改的规则或组中在上传中没有对应规则的规则将保持不变。系统将添加上传中的任何新规则。这是默认选项。
- **替换** - 如果上传的规则的修订版本号更高，则上传文件中的规则将替换所选组中的规则。任何不在上传文件中的现有规则都将从组中删除。上传版本的修订版本号相同或更低的现有规则将保持不变。系统将添加上传中的任何新规则。

步骤 6 点击 **+**，然后为上传的规则选择自定义规则组。

如果您想使用的自定义规则组尚不存在，请点击**创建新组 (Create New Group)** 立即创建组。新组需要名称和说明（后者为可选项）。然后，您可以选择该新组。

如果要替换规则，则只能选择单个组。如果要合并规则，则可以选择多个组。

步骤 7 点击**确定 (OK)**。

文件将上传并放置在该新组中。您应该会看到一个摘要，说明上传了多少规则以及更新、删除或忽略了多少规则。

如果文件中有错误，上传将失败。您可以点击**下载错误文件 (Download Error File)** 链接，获取有关错误的更多信息。

该组在此入侵策略中自动激活。可以将该组和新规则添加到其他策略，但不会在任何其他策略中自动启用该组和规则。有关将组添加到其他策略的信息，请参阅在入侵策略中添加或删除规则组 (Snort 3)，第 18 页。

配置单独自定义入侵规则

您可以一次配置一个自定义入侵规则，而不是通过文件上传批量配置。当您需要快速调整某个规则，或者需要一次只创建或修改几个规则时，此方法十分有效。

配置入侵规则时，请记住以下几点：

- 所有自定义规则的 GID 都应为 1。
- 规则的 SID 在系统中的所有规则中必须是唯一的。它的值还必须等于或高于一百万 (1000000)。
- 如果您编辑某个规则，必须更改该规则的版本。通常情况下，版本号每次递增 1。
- 您可以复制思科 Talos 智能小组 (Talos) 规则来创建自己的规则版本，但仍必须更改复制规则的 SID 以确保其唯一性。

系统会执行一些有效性检查，以确保规则的格式正确，并且您会看到有关任何问题的错误消息。但是，系统无法确定规则是否合理。

有关如何为 Snort 编写入侵规则（包括如何将 Snort 2 规则转换为 Snort 3 格式）的详细信息，请参阅 https://snort.org/documents 上的指南。例如，https://snort.org/documents/rules-writers-guide-to-snort-3-rules 上提供的面向规则编写者的 *Snort 3* 规则编写简介。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击策略的编辑图标 ( )。

建议您将自定义规则添加到自定义入侵策略，而不是添加到其中一个内置策略。

步骤 3 执行以下操作之一：

- 要添加入侵规则，请点击规则表上方的**添加新的入侵规则**按钮 (+)。添加规则时，您必须选择一个或多个自定义规则组以包含新规则。如有必要，您可以在添加规则时创建新组。
- 要通过复制和编辑某个现有规则来添加规则，请将鼠标悬停在该规则的右端，然后点击复制 ( ) 按钮。该按钮仅在鼠标悬停时才会显示。对于自定义规则，**复制**命令位于更多选项 (**...**) 按钮下。
- 要编辑某个自定义规则，请在自定义规则组中找到该规则，然后点击该规则的编辑 ( ) 按钮。您所做的编辑将应用于该规则所在的所有组。在进行更改时，确保规则版本号每次至少递增 1。
- 要删除某个自定义规则，请点击该规则的删除 ( ) 按钮。该规则将从包含该规则的所有规则组中删除。如果您只想从组中删除某个规则，请使用**管理组分配**选项，而不是删除该规则。
- 要更改包含规则的组，请点击更多选项 (**...**) 按钮，然后选择**管理组分配**。随后即可添加或删除组。您所做的更改只会影响组成员身份，不会更改或删除规则。

步骤 4 对于新规则和组，请将规则添加到策略。

如果您在创建新规则或编辑现有规则时创建新组，该组不会自动添加到您的策略，规则也不会自动启用。系统会提示您将该组添加到正在编辑的策略。如果在添加或编辑规则时未添加该组，您可以稍后按照以下流程添加该组：

a) 点击组目录上方的 + > **添加现有规则组**。
b) 在“用户定义的组”文件夹下找到该组，选中，然后点击**确定**。
c) 在目录中选择该组，并验证新规则是否在该组中并具有所需操作。

管理入侵策略 (Snort 2)

您可以应用预定义的任何入侵策略。其中每个策略包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于活动状态，但在另一个策略中可能被禁用。

如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

相反，如果您知道自己需要防御特定的攻击，但相关规则在您所选的入侵策略中被禁用，可以启用该规则而不必更改为更安全的策略。

使用与入侵相关的控制面板和事件查看器（两者均在**监控 (Monitoring)** 页面）可评估入侵规则对流量的影响。请记住，仅将匹配入侵规则的流量设为警告或丢弃时，才会看到入侵事件和入侵数据；系统不评估禁用的规则。

以下主题详细介绍入侵策略和规则调整。

配置入侵策略的检测模式 (Snort 2)

默认情况下，所有入侵策略在防御模式下运行，以实施入侵防御系统 (IPS)。在防御检测模式下，如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

如果想要测试入侵策略对网络的影响，则可以更改为“检测”模式，从而实施入侵检测系统 (IDS)。在此检测模式下，丢弃规则的处理方式类似于报警规则，在这种情况下，系统会通知您匹配的连接，但操作结果变为“将被阻止”，而事实上绝不会阻止连接。

您可以更改每个入侵策略的检测模式，以便组合使用防御与检测功能。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击您要更改其检测模式的入侵策略选项卡。

规则表上方指示**检测模式**。

步骤 3 点击检测模式旁边的**编辑**链接，更改策略的模式，然后点击**确定**。

选项包括：

- **防御** - 始终应用入侵规则操作。匹配丢弃规则的连接将被阻止。
- **检测** - 入侵规则仅生成警报。匹配丢弃规则的连接将生成警报消息，但不会阻止连接。

更改入侵规则操作 (Snort 2)

每个预定义的入侵策略包含相同的规则。不同的是针对每个规则所采取的操作因策略而异。

通过更改规则操作，可以禁用为您提供过多误报的规则，也可以将规则更改为针对匹配流量发出警报或丢弃该流量。您还可以启用已禁用的规则，以警告或丢弃匹配的流量。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击您要更改其规则操作的“入侵策略”选项卡。

预定义的策略包括：

- 连接优先于安全
- 平衡安全和连接
- 安全优先于连接
- 最大检测数

步骤 3 查找您要更改其操作的规则。

这些规则首先根据所列的已覆盖规则进行排序，并在已覆盖规则组中根据操作进行排序。否则，这些规则将先后根据 GID 和 SID 进行排序。

使用搜索框查找希望更改的规则。如果您正在与思科技术支持部门合力解决某个问题，最好可以从事件中或通过该部门获取 Snort 标识符 (SID) 和生成器标识符 (ID)。

有关每个规则的元素的详细信息，请参阅入侵规则属性，第 3 页。

要搜索列表，请执行以下操作：

a) 点击**搜索**框，打开“搜索属性”对话框。
b) 输入生成器 ID 的组合 (**GID**)、Snort ID (**SID**) 或规则**操作**，然后点击**搜索**。

例如，您可以选择**操作=丢弃**来查看丢弃匹配连接的策略中的所有规则。搜索框旁边的文本表示与您的条件匹配的规则数量，例如“找到 9416 条规则中的 8937 条”。

要清除搜索条件，请点击搜索框中条件的 x。

步骤 4 点击规则的**操作**列，选择所需的操作：

- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
- **禁用** - 不针对此规则匹配流量。不生成事件。

规则的默认操作用操作后面附加“（默认）”表示。如果更改了默认设置，状态列会针对该规则指示“已覆盖”。

监控入侵策略

可以在**监控 (Monitoring)** 页面上的**攻击者 (Attackers)** 和**目标 (Targets)** 控制面板找到入侵策略统计信息。必须将入侵策略应用于至少一个访问控制规则，才能在这些控制面板上看到任何信息。请参阅监控流量和系统控制面板。

要查看入侵事件，请依次选择**监控** > **事件**，然后点击**入侵**选项卡。将鼠标悬停在某个事件上方，点击**查看详细信息**链接以获取更多信息。在详细信息页面中，点击**查看 IPS 规则 (View IPS Rule)** 转至相关入侵策略中的规则（您可以在此页面更改规则操作）。如果规则阻止过多安全连接，则可通过将操作从丢弃更改为警告减少误报带来的影响。相反，如果对于某条规则看到的是大量攻击流量，则可将警告规则更改为丢弃规则。

如果为入侵策略配置系统日志服务器，入侵事件的消息 ID 则为 430001。

入侵策略示例

使用案例章节涵盖以下实施入侵策略的示例。

- 如何阻止威胁
- 如何被动监控网络上的流量

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。