SCADA 预处理器

以下主题介绍监控和数据采集 (SCADA) 协议的预处理器及其配置方法：

SCADA 预处理器简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。Firepower 系统为可作为网络分析策略一部分进行配置的 Modbus 、分布式网络协议 (DNP3)、通用工业协议 (CIP) 和 S7Commplus SCADA 协议提供预处理器。

如果 Modbus、DNP3、CIP 或 S7Commplus 预处理被禁用，而您启用并部署需要其中一种预处理器的入侵规则，则系统会自动使用所需的预处理器及其当前设置，尽管该预处理器在 Web 界面中对于相应的网络分析策略仍处于禁用状态。

SCADA 预处理器的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

SCADA 预处理器的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

Modbus 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

Modbus 协议由 Modicon 于 1979 年首次发布，是一种广泛使用的 SCADA 协议。Modbus 预处理器可检测 Modbus 流量中的异常，解码 Modbus 协议以供规则引擎进行处理（规则引擎使用 Modbus 关键字来访问某些协议字段）。

单一配置选项允许为预处理器进行 Modbus 流量检查的端口修改默认设置。

相关主题

SCADA 关键字

Modbus 预处理器端口选项

端口

指定预处理器检查 Modbus 流量的端口。使用逗号分隔多个端口。

配置 Modbus 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

如果您的网络不包含任何支持 Modbus 的设备，则不应该在应用于流量的网络分析策略中启用此预处理器。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 单击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**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 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **Modbus 配置 (Modbus Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **Modbus 配置 (Modbus Configuration)** 旁边的 **编辑**（）。

步骤 7 在**端口 (Ports)** 字段中输入值。

多个值之间用逗号隔开。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 Modbus 预处理器规则 (GID 144)。有关详细信息，请参阅设置入侵规则状态和Modbus 预处理器规则，第 4 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层

冲突和更改：网络分析和入侵策略

Modbus 预处理器规则

如果希望这些规则生成事件并在内联部署中丢弃攻击性数据包，则必须启用下表中的 Modbus 预处理器规则。

表 *1: Modbus* 预处理器规则

预处理器规则 GID:SID	说明
144:1	如果 Modbus 报头中的长度与 Modbus 函数代码所要求的长度不匹配，将会生成事件。 每个 Modbus 函数都有预期的请求和响应格式。如果消息长度与预期格式不匹配，将会生成此事件。
144:2	如果 Modbus 协议 ID 为非零值，将会生成事件。协议 ID 字段用于将其他协议与 Modbus 协议复用。由于预处理器并不处理此类其他协议，因此会生成此事件。
144:3	如果预处理器检测到保留的 Modbus 函数代码，将会生成事件。

DNP3 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

分布式网络协议 (DNP3) 是一种 SCADA 协议，最初开发是为了在发电站之间提供一致的通信。此外，DNP3 还在水务、废弃物、运输和很多其他行业中得到广泛使用。

DNP3 预处理器可检测到 DNP3 流量中的异常，并对 DNP3 协议进行解码以用于按规则引擎进行处理，这将使用 DNP3 关键字来访问某些协议字段。

相关主题

DNP3 关键字

DNP3 预处理器选项

端口

启用对每个指定端口的 DNP3 流量检查。可以指定单个端口或端口的逗号分隔列表。

记录错误 CRC

验证包含在 DNP3 链路层帧中的校验和。具有无效校验和的帧将被忽略。

可以启用规则 145:1，以便在检测到无效校验和时生成事件并在内联部署中丢弃攻击性数据包。

配置 DNP3 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

如果您的网络不包含任何支持 DNP3 的设备，则不应该在应用于流量的网络分析策略中启用此预处理器。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 单击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**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 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **DNP3 配置 (DNP3 Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **DNP3 配置 (DNP3 Configuration)** 旁边的 **编辑**（）。

步骤 7 为**端口数 (Ports)** 输入一个值。

多个值之间用逗号隔开。

步骤 8 选中或清除**记录不良 CRC (Log bad CRCs)** 复选框。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 DNP3 预处理器规则 (GID 145)。有关详细信息，请参阅设置入侵规则状态、DNP3 预处理器选项 ，第 4 页和DNP3 预处理器规则 ，第 6 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

管理层

冲突和更改：网络分析和入侵策略

DNP3 预处理器规则

如果希望下表中所列的 DNP3 预处理器规则生成事件并在内联部署中丢弃攻击性数据包，必须启用这些规则。

表 *2: DNP3* 预处理器规则

预处理器规则 GID:SID	说明
145:1	在**记录无效 CRC (Log bad CRC)** 已启用的情况下，如果预处理器检测到具有无效校验和的链路层帧，将会生成事件。
145:2	如果预处理器检测到具有无效长度的 DNP3 链路层帧，系统将会生成事件并阻止该数据包。
145:3	如果预处理器检测到具有无效序列号的传输层分段，系统将会生成事件并在重组期间阻止数据包。
145:4	如果需要清除 DNP3 重组缓冲区后才能重组完整的片段，系统将会生成事件。如果在其他分段已加入队列后出现带有 FIR 标志的分段，系统将会发生这种情况。
145:5	如果预处理器检测到使用保留地址的 DNP3 链路层帧，系统将会生成事件。
145:6	如果预处理器检测到使用保留函数代码的 DNP3 请求或响应，系统将会生成事件。

CIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

通用工业协议 (CIP) 是广泛使用的应用协议，支持工业自动化应用。EtherNet/IP (ENIP) 是基于以太网的网络中使用的 CIP 的实施。

CIP 预处理器检测 TCP 或 UDP 上运行的 CIP 和 ENIP 流量，并将其发送给入侵规则引擎。可以使用自定义入侵规则中的 CIP 和 ENIP 关键字检测 CIP 和 ENIP 流量中的攻击。请参阅 CIP 和 ENIP 关键字。此外，可以指定访问控制规则中的 CIP 和 ENIP 应用条件以控制流量。请参阅配置应用条件和过滤器。

CIP 预处理器选项

端口

指定用于检查 CIP 和 ENIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

注释 必须将默认的 CIP 检测端口 44818 和您列出的任何其他端口添加到 TCP 数据流**对两个端口执行数据流重组**列表。请参阅TCP 数据流预处理选项和创建自定义网络分析策略。

默认的无关联超时时间 (秒)

当 CIP 请求消息不包含协议特定超时值，并且达到**每个 TCP 连接上并发无关联请求的最大数 (Maximum number of concurrent unconnected requests per TCP connection)** 时，系统测定此选项指定的消息的秒数。如果计时器过期，则会删除此消息，以便腾出空间来存储未来的请求。可指定 0 到 360 之间的整数。如果指定 0，不具有协议特定超时值的所有流量会首先超时。

每个 TCP 连接上并发无关联请求的最大数

在系统关闭连接之前，可以不用理会的并发请求的数量。可指定 1 到 10000 之间的整数。

每个 TCP 连接上 CIP 连接的最大数

系统允许的每个 TCP 连接上的同步 CIP 连接的最大数。可指定 1 到 10000 之间的整数。

CIP 事件

根据设计，应用检测器检测并且事件查看器显示相同的应用，每个会话一次。CIP 会话可以在不同的数据包中包括多个应用，一个 CIP 数据包可以包含多个应用。CIP 预处理器根据相应的入侵规则处理所有 CIP 和 ENIP 流量。

下表展示在事件视图中显示的 CIP 值。

表 *3: CIP* 事件字段值

事件字段	显示的值
应用协议	CIP 或 ENIP

事件字段	显示的值
客户端	CIP 客户端或 ENIP 客户端
Web 应用	检测到的特定应用，即： • 对于允许或监控流量的访问控制规则，会话中检测到的最新应用协议。 配置为记录连接的访问控制规则可能不会为指定的 CIP 应用生成事件，而没 接的访问控制规则可能会为 CIP 应用生成事件。 • 对于阻止流量的访问控制规则，触发此阻止的应用协议。 当访问控制规则阻止 CIP 应用列表时，事件查看器显示检测到的第一个应用

GTP 预处理器规则

如果您希望下表中所列的 CIP 预处理器规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅设置入侵规则状态。

表 *4: GTP* 预处理器规则

GID:SID	Rule Message
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

配置 CIP 预处理器的准则

配置 CIP 预处理器时，请注意以下事项：

- 必须将默认的 CIP 检测端口 44818 和您列出的任何其他 CIP **端口**添加到 TCP 数据流**对两个端口执行数据流重组**列表。请参阅CIP 预处理器选项，第 7 页、创建自定义网络分析策略和TCP 数据流预处理选项。
- 事件查看器可对 CIP 应用进行特殊处理。请参阅CIP 事件，第 7 页。
- 我们建议您使用入侵防御操作作为访问控制策略的默认操作。
- CIP 预处理器不支持**访问控制：信任所有流量**的访问控制策略默认操作，此选项可能会产生不需要的行为，包括不丢弃由入侵规则和访问控制规则中所指定的 CIP 应用触发的流量。
- CIP 预处理器不支持**访问控制：阻止所有流量**的访问控制策略默认操作，此选项可能会产生不需要的行为，包括阻止并不想要阻止的 CIP 应用。
- CIP 预处理器不支持 CIP 应用的应用可视性，包括网络发现。

- 要检测 CIP 和 ENIP 应用并将其用在访问控制规则、入侵规则等规则中，必须手动启用相应自定义网络分析策略中的 CIP 预处理器。请参阅创建自定义网络分析策略、设置默认网络分析策略和配置网络分析规则。
- 要丢弃可触发 CIP 预处理器规则和 CIP 入侵规则的流量，请确保在相应入侵策略中已启用**内联时丢弃**。请参阅设置内联部署中的丢弃行为。
- 要使用访问控制规则阻止 CIP 或 ENIP 应用流量，请确保在相应的网络分析策略中已启用内联规范化预处理器及其**内联模式**选项（默认设置）。请参阅创建自定义网络分析策略、设置默认网络分析策略和内联部署中预处理器流量的修改。

配置 CIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

开始之前

- 必须将默认的 CIP 检测端口 44818 和任何其他您列出为 CIP **端口**的端口添加到 TCP 数据流**对两个端口执行数据流重组**列表。请参阅CIP 预处理器选项，第 7 页、创建自定义网络分析策略和TCP 数据流预处理选项。
- 熟悉配置 CIP 预处理器的准则，第 8 页。
- 威胁防御 设备不支持 CIP 预处理器。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 单击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**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 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器** 下的 **CIP 配置**已禁用，请点击**已启用**。

步骤 6 可以修改 CIP 预处理器选项，第 7 页中所述的任何选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果您要 生成事件并在内联部署中丢弃攻击性数据包，请启用 CIP 入侵规则，或者 CIP 预处理器规则 (GID 148)。有关详细信息，请参阅设置入侵规则状态、GTP 预处理器规则，第 8 页和 CIP 事件，第 7 页。
- 部署配置更改；请参阅 部署配置更改。

S7Commplus 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

S7Commplus 预处理器可检测 S7Commplus 流量。可以使用自定义入侵规则中的 S7Commplus 关键字检测 S7Commplus 流量中的攻击。请参阅S7Commplus 关键字。

配置 S7Commplus 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

所有 威胁防御 设备都支持 S7Commplus 预处理器。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 单击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**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 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **S7Commplus 配置 (S7Commplus Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 或者，点击 **S7Commplus 配置 (S7Commplus Configuration)** 旁边的 **编辑**（  ），然后修改 **s7commplus_ports** 以标识预处理器用于检查 S7Commplus 流量的端口。使用逗号分隔多个端口。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 S7Commplus 预处理器规则 (GID 149)。有关详细信息，请参阅设置入侵规则状态
- 部署配置更改；请参阅 部署配置更改。

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。