安全在300系列被管理的交换机的套件设置

客观

Cisco 300系列管理的交换机提供保护的安全套件免受拒绝服务攻击。DOS攻击充斥网络与错误数据流，使网络服务器资源未提供或无答复对合法用户。通常，有DOS攻击的两种类型。暴力DOS攻击充斥服务器并且使用服务器和网络带宽。系统的攻击操作协议弱点类似TCP SYN消息失败系统。此条款说明设置可用在300系列被管理的交换机的安全套件。

Note:当DOS攻击保护是启用的时，访问控制列表(ACL)和先进的QoS策略不是活跃的在端口。

可适用的设备

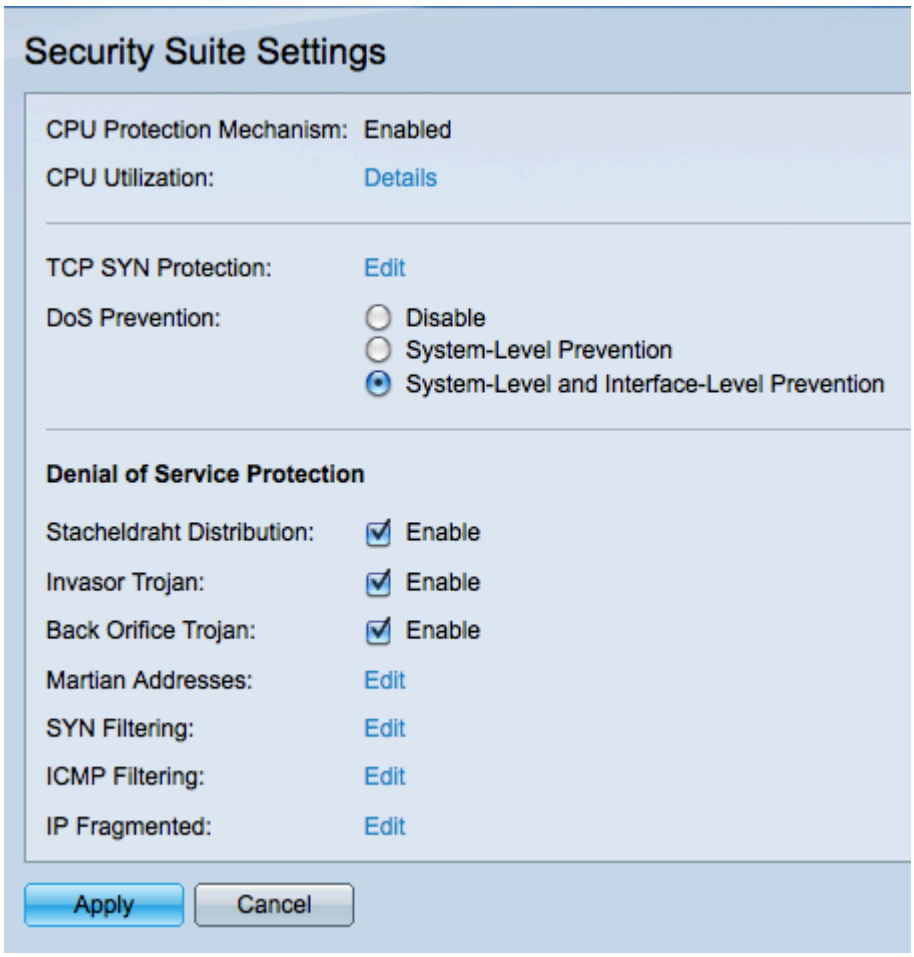
•SF/SG 300系列被管理的交换机

软件版本

•1.3.0.62

安全套件设置配置

步骤1.登陆到Web配置工具并且选择**安全>拒绝服务预防> Security套件设置**。*Settings页安全的套件*打开：



Note:默认情况下CPU保护机制在300系列被管理的交换机被启用，并且不可以是失效的。交换机使用安全的核心技术(SCT)，允许交换机处理管理和协议数据流，无论总流量收到。

第2.步(可选)点击在CPU利用率字段的**详情**查看CPU利用率。请参见*在200/300系列被管理的交换机的*条款*CPU利用率*欲知更多信息。

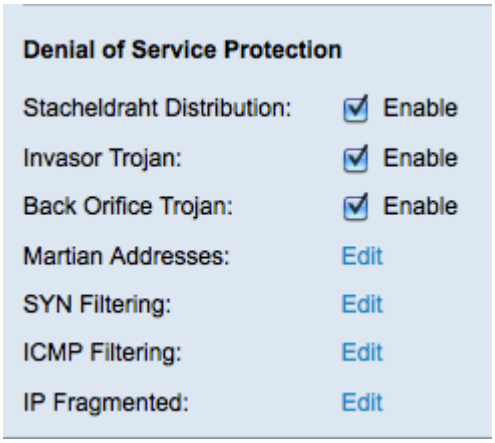
第3.步(可选)在TCP SYN保护字段点击**编辑**编辑TCP SYN保护设置。请参见条款*同步(SYN)在300系列被管理的交换机的过滤器配置*欲知更多信息。

第 4 步：在DoS预防字段，请点击对应于DoS预防方法您希望使用的单选按钮。可用的选项是：

•功能失效—功能失效DoS保护特点。如果功能失效被选择，请跳到第13步。

•系统-级别预防— Enable (event) DoS保护免受Invasor特洛伊人、Stacheldraht分配、回到管口特洛伊人和火星地址的保护特点。

•系统-级别预防和Interface-Level保护— Enable (event)在拒绝服务保护地区定义的所有安全措施。



第 5 步：检查在Stacheldraht分配字段的**Enable复选框**丢弃与来源TCP端口编号的TCP信息包的16660。

第6.步。检查在Invasor特洛伊字段的**Enable复选框**丢弃与目的地TCP端口2140和来源TCP端口的TCP信息包1024。

第 7 步：检查在回到管口特洛伊领域的**Enable复选框**丢弃与目的地UDP端口相等到31337和来源UDP端口的UDP信息包1024。

Note:当有数百DOS攻击时，以上提到的端口为恶意活动通常被使用。然而，他们也使用合法数据流。 如果有使用以上任何一个端口的一个设备，该信息将被阻拦。

步骤8.点击**编辑**在Addresses字段的火星编辑火星地址表。火星地址表丢弃信息包从选择IP地址。要编辑火星地址列表，请参见*在300系列被管理的交换机的条款拒绝服务火星的地址配置*。

Note:步骤9-12要求系统层，并且Interface-Level预防被选择在第4.步跳到第13步，如果选择了另一种DoS预防类型。

步骤9.点击**编辑**在过滤字段的SYN允许管理员阻拦某些TCP端口。要配置过滤的SYN，请参见*在300系列被管理的交换机的条款拒绝服务SYN过滤器配置。*

步骤10.点击**编辑**在SYN费率保护字段限制同步信息包的数量收到的。要配置SYN费率保护，请参见*在300系列被管理的交换机的条款SYN费率保护*。

步骤11.点击**编辑**在ICMP过滤字段允许自某些来源的ICMP信息包被阻拦。要配置ICMP过滤，请参见*在300系列被管理的交换机的条款互联网控制消息协议(ICMP)过滤器配置。*

步骤12。点击**编辑**在IP被分段的字段阻拦被分段的IP信息包。要配置过滤的IP段，请参见*在300系列被管理的交换机的条款拒绝服务IP段过滤器配置。*

第13步。点击**适用**保存更改或点击**取消**取消您的更改。