互联网控制消息协议(ICMP)在300系列被管理的交换机的过滤器配置

客观

互联网控制消息协议(ICMP)是用于的网络层协议报告和通知错误和网络发现的。有在网络可以进行与ICMP的许多攻击。例如， ICMP溢出拒绝服务攻击是利用ICMP协议弱点和不正确网络配置的攻击。ICMP过滤是防止攻击的这些类型的解决方案对网络。您能配置交换机过滤IP地址或端口您要阻拦ICMP信息包从。此条款说明如何配置在300系列被管理的交换机的ICMP过滤。

可适用的设备

•SF/SG 300系列被管理的交换机

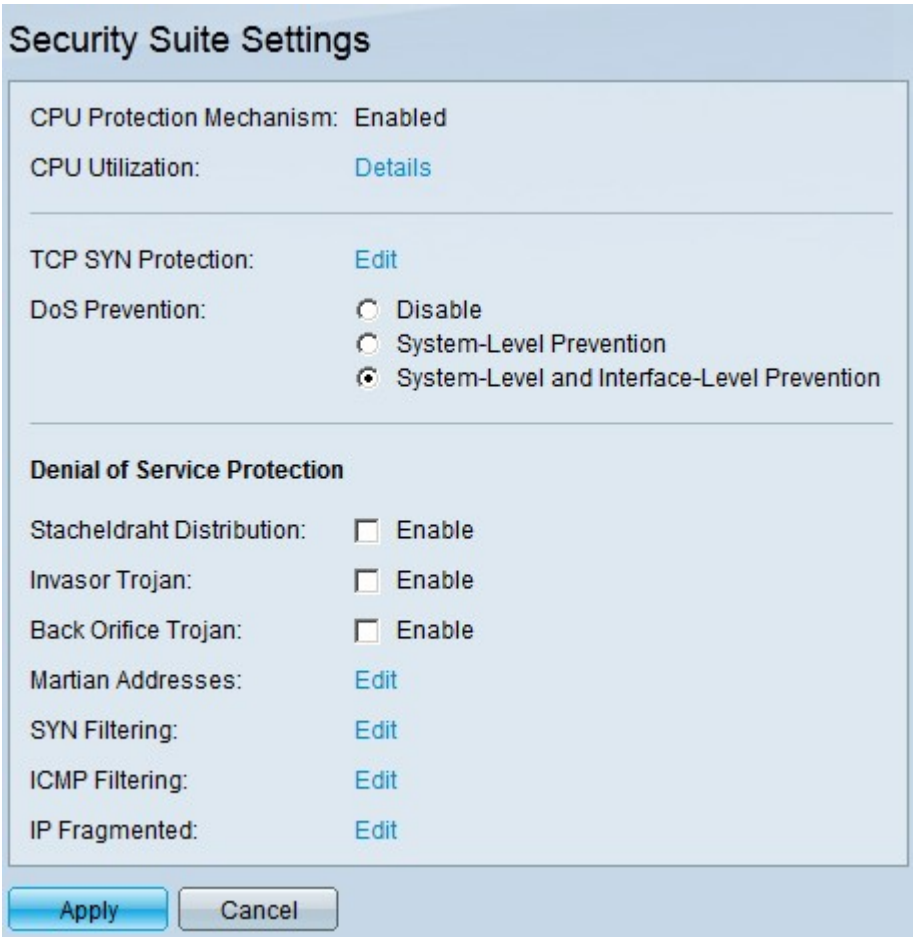
软件版本

•1.3.0.62

Enable (event)拒绝服务级别预防

为了施加ICMP过滤，您必须首先确信，交换机在正确的拒绝服务级别预防。此部分如何说明对enable (event)在300系列被管理的交换机的正确的预防级别。

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：



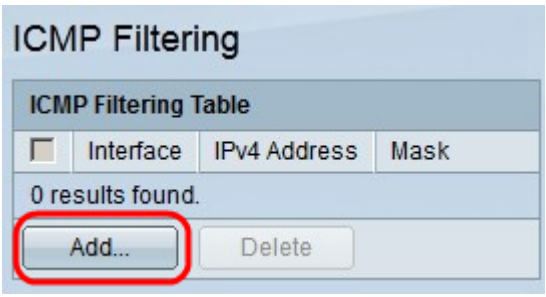
Step 2.在*DoS预防*字段，有预防的三个级别。点击**系统层和Interface-Level预防**单选按钮。此级别允许您配置ICMP过滤。

步骤3.点击**适用**保存您的配置。

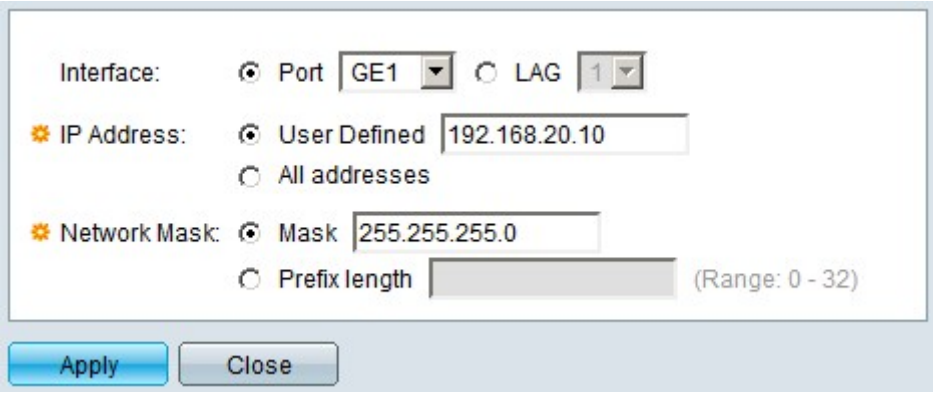
ICMP过滤配置

此部分说明如何配置在300系列被管理的交换机的ICMP过滤。

步骤1.登陆到Web配置工具并且选择**安全>拒绝服务预防> ICMP过滤。***ICMP过滤*页打开：



步骤2.Click**添加。***添加ICMP过滤*窗口出现。



第 3 步：在*接口*字段，请点击单选按钮其中一个可用接口选项：

•端口—允许您选择您希望过滤ICMP信息包从的端口。

•滞后—允许您选择您希望过滤ICMP信息包从的滞后。滞后聚合多个端口到单个逻辑端口。

第 4 步：在*IP Address字段*，请点击单选按钮其中一个可用的选项定义IP地址/地址过滤ICMP信息包从：

•用户定义—用户定义的ICMP信息包来源。

•所有地址— IP地址ICMP信息包来源的所有范围。

步骤5在*网络掩码*字段，请点击单选按钮其中一个可用的选项输入被配置的IP地址的网络掩码在第4步：

•掩码—子网掩码以点格式，例如， 255.255.255.0。

•前缀长度—子网掩码以斜线格式，例如， \24。

步骤6.点击**适用**保存您的配置。

下面的镜像在配置以后表示更改：

第7.步(可选)删除ICMP过滤器，检查您在ICMP过滤表里希望删除然后点击**删除**ICMP过滤器的复选框。