同步(SYN)在300系列被管理的交换机的过滤器配置

客观

TCP是提供可靠的传输层协议，信息包被定购的发运并且允许错误的检测和丢失数据触发重新传输，直到数据正确和完全地接受。在客户端发送数据前，它请求与同步(SYN)信息包的连接与服务器开始连接。服务器然后发送一个SYN和确认(ACK)信息包到客户端，并且客户端发送一ACK数据包承认服务器响应。在客户端和服务器之间的此三通的握手连接以后，可以发送数据。

当中断时， SYN溢出攻击发生此TCP三次握手。一个有恶意的客户端充斥服务器与同步信息包，服务器回应所有有恶意的客户端的要求的SYN和ACK信息包，但是有恶意的客户端不发送ACK信息包。服务器等待不会到达，浪费服务器资源合法用户的和最终减少网络的ACK数据包。SYN过滤防止这些攻击。此条款说明如何配置过滤在300系列被管理的交换机的SYN。

可适用的设备

•SF/SG 300系列被管理的交换机

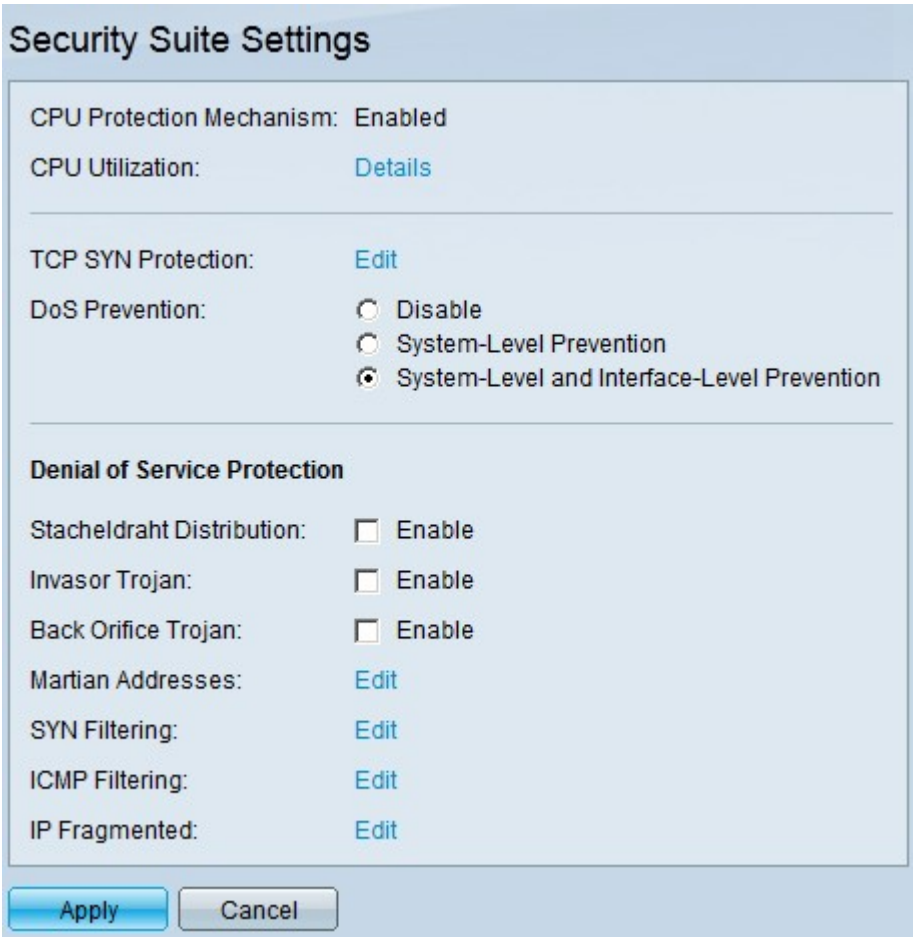
软件版本

•v1.2.7.76

Enable (event)拒绝服务级别预防

为了适用过滤，首先，您的SYN需要确定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**。此级别让您配置SYN过滤。

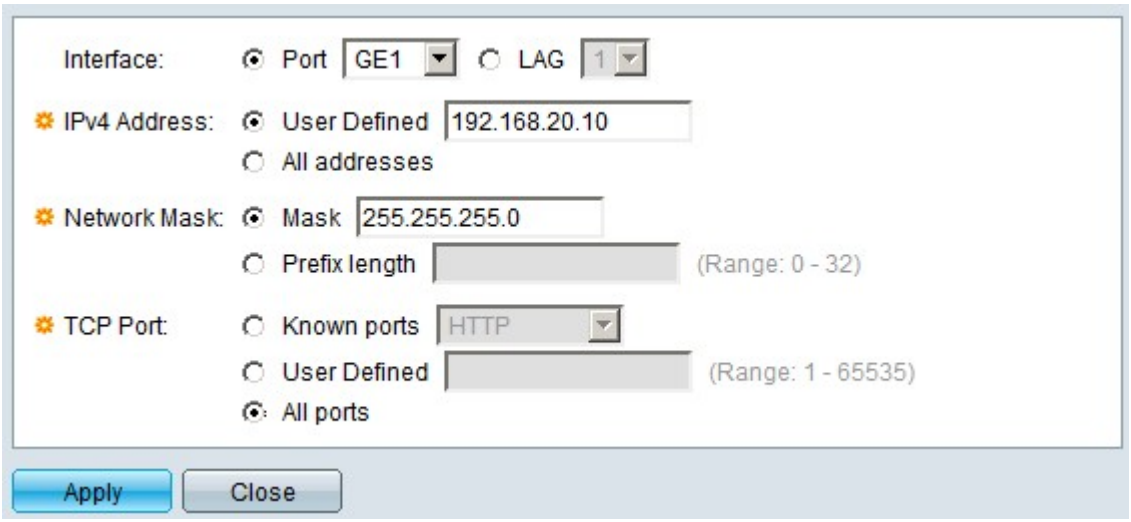
步骤3.点击**适用**保存您的配置。

过滤TCP Syn信息包

此部分说明如何配置过滤在300系列被管理的交换机的SYN。

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

步骤2.点击**添加**。*过滤*窗口的*添加SYN*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自端口下拉列表的同步信息包的端口。

•滞后—允许您选择您希望过滤自链路聚合组的滞后(滞后)下拉列表的同步信息包。滞后聚合多个端口到单个逻辑端口。

第 4 步：在IPv4地址域，请点击单选按钮其中一个可用的选项定义IPv4地址/地址过滤同步信息包从：

•用户定义—允许您输入同步信息包过滤器被定义的IPv4地址。

•所有地址—此选项过滤同步信息包的所有IPv4地址。

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—此选项让您输入IP地址的子网掩码。

•前缀长度—此选项在前缀格式让您输入子网掩码IP地址。

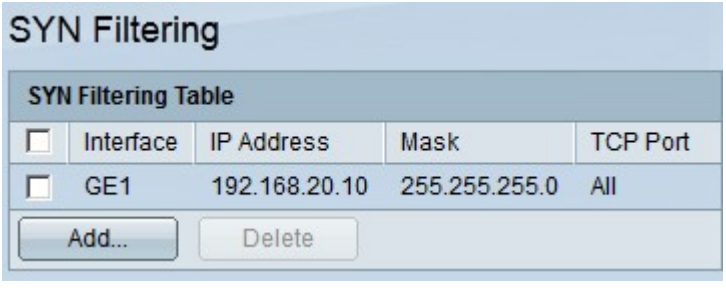
第 5 步：在TCP端口字段，请点击其中一个可用的选项确定TCP端口过滤：

•已知端口—此选项让您从已知端口下拉列表选择端口。例如HTTP是80，并且TELNET是23。

•用户定义—此选项让您输入TCP端口编号过滤。

•所有端口—此选项过滤所有TCP端口。

步骤6.点击**适用**保存您的配置。变动做对过滤表的SYN ：



第7.步(可选)删除一台SYN过滤器，在过滤表的SYN，检查您希望删除SYN过滤器的复选框。

然后请点击**删除**。