拒绝服务IP段在300系列被管理的交换机的过滤器配置

客观

网络流量利用称为数据包的多个信息包被发送。 每个传输方法(以太网、令牌环等等)有能处理数据包的最大大小。 如果数据包太大对于发射方法，被分裂成更小的片段。 此进程叫作IP分段。多数网络流量不必须被分段。实际上，被分段的数据流在拒绝服务攻击可以使用正如。 DOS攻击充斥网络与错误数据流并且减慢或者终止网络。300系列被管理的交换机能阻拦IP段，减少网络弱点对DOS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*IP段*设置。

Note:IP段过滤器，如果DoS预防是启用的，可能只使用。 请参见*在300系列被管理的交换机的*条款*安全套件设置*帮助的。

可适用的设备

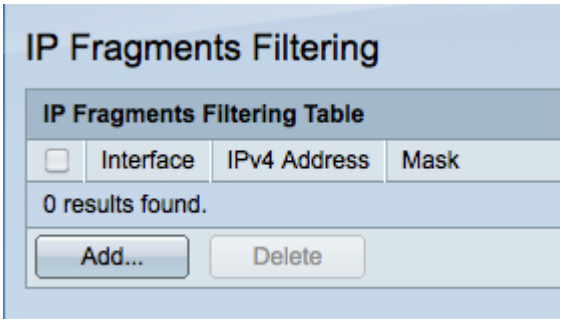
•SF/SG 300系列被管理的交换机

软件版本

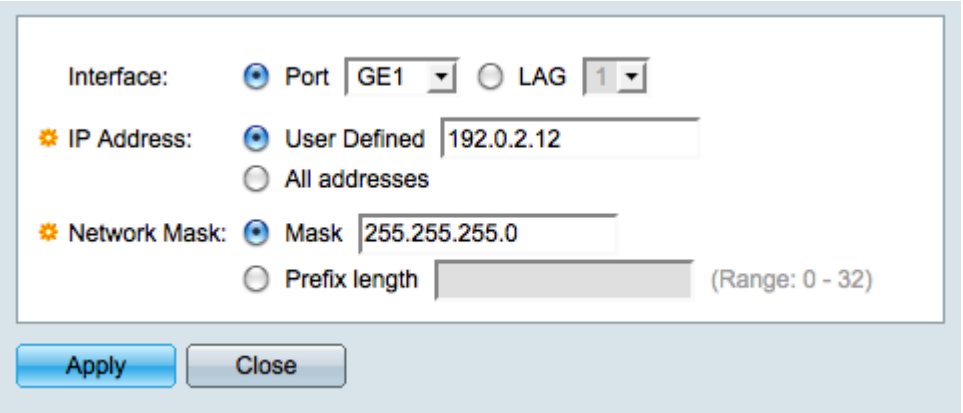
•1.3.0.62

添加IP段过滤器

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



步骤2.点击**添加**添加一台新的IP段过滤器。*过滤*窗口的*添加IP段*出现。



步骤3.点击对应与在接口字段的所需的接口的单选按钮。 这是物理位置过滤器将分配。

- 端口—在交换机的物理端口。 从端口下拉列表选择一个特定端口。
- 滞后—作为单个端口的一个端口组。 从滞后下拉列表选择特定滞后。

步骤4.点击对应与在IP Address字段将过滤的期望IPv4地址的单选按钮。

- 用户定义—输入将被过滤的IP地址。
- 所有地址—所有IPv4地址被过滤。

Note:如果选择了在第4步的所有地址，请跳到第6.步。

步骤5.点击对应与使用的方法定义IP地址子网掩码在网络掩码字段的单选按钮。

- 掩码—输入网络掩码在网络掩码字段。
- 前缀长度—输入前缀长度(在0到32范围内的整数)在前缀长度字段。

步骤6.点击**适用**救您更改然后点击**接近**close*过滤*窗口的*添加IP段*。