拒绝服务预防技术(安全套件)的配置在Sx500系列可堆叠交换机

客观

拒绝服务或分布式拒绝服务(DDos)攻击限制有效用户使用网络。攻击者通过充斥网络进行一次DOS攻击与占去网络的所有带宽的许多多余的请求。DOS攻击能或者减速网络，或者完全地请中断网络几小时。 DoS保护是改进的网络安全主要功能;它发现异常数据流并且过滤它。

此条款说明拒绝服务的配置在安全用于拒绝服务预防和多种技术的套件设置。

Note: 如果选择的DoS预防是系统层和Interface-Level预防，则可以被编辑和配置军事地址，SYN过滤， SYN费率保护、ICMP过滤和IP段过滤。这些配置在此条款上也解释。

Note:在激活前DoS预防，解开被配置对端口的所有访问控制列表(ACL)或所有先进的QoS策略是必要的。一旦DoS保护在端口，被启用ACL和先进的QoS策略不是活跃的。

可适用的设备

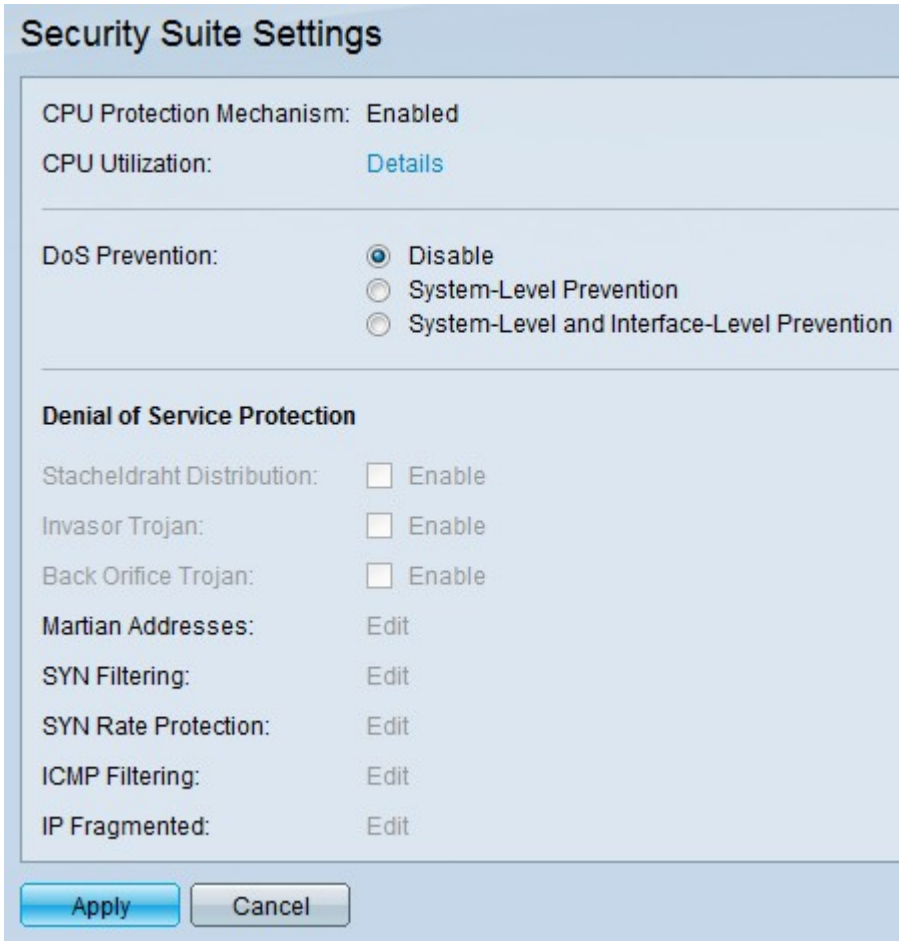
- Sx500系列可堆叠交换机

软件版本

- 1.3.0.62

拒绝服务的配置在安全套件设置的

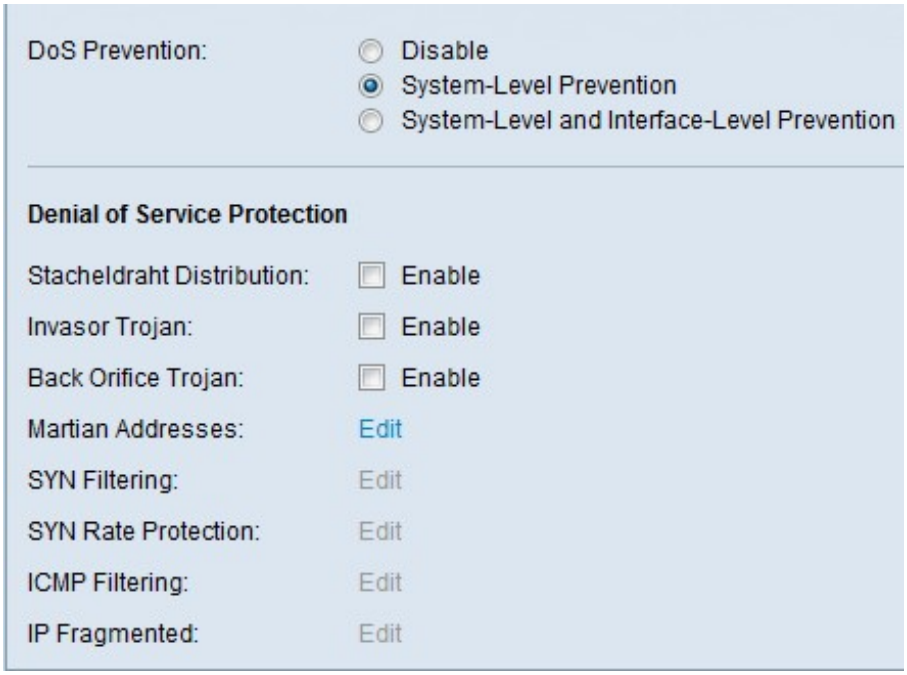
步骤1.登陆到Web配置工具，并且选择**安全>拒绝服务预防> Security套件设置**。*Settings页安全的套件*打开：



- CPU保护机制—这是
- **启用**。这表明安全转换工具(SCT)是启用的。
- CPU利用率—点击
- 在查看CPU资源利用率信息的CPU利用率旁边的**详细资料**。

步骤2.点击appropriate单选按钮在DoS预防字段下。

- 功能失效—禁用DoS预防。
- 系统层预防—这防止攻击Stacheldraht分配、Invasor特洛伊人和回到管口特洛伊人。
- 系统层和Interface-Level预防—这防止攻击每个接口对交换机。



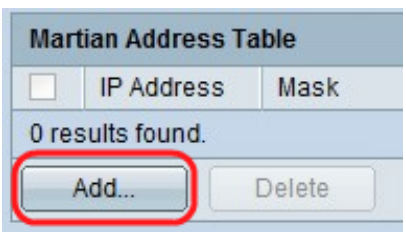
第 3 步：这些选项可以为拒绝服务保护被选择：

- Stacheldraht分配—这是的DDoS攻击示例攻击者使用一个客户端程序连接到计算机在网络里面。那些计算机然后派出多个登录请求到内部服务器并且开始DDoS攻击。
- Invasor特洛伊人—如果计算机由此攻击感染，TCP端口2140使用恶意活动。
- 回到管口特洛伊人—这丢弃使用与服务器和客户端程序联络DOS攻击的UDP信息包。

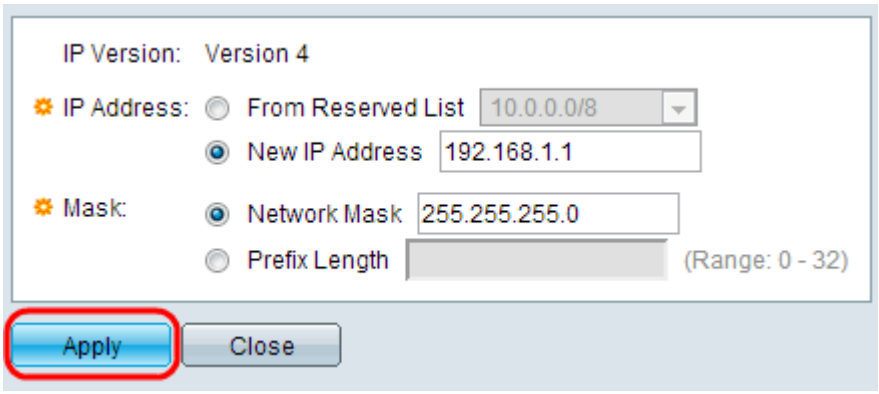
火星的地址的配置

步骤1.点击在火星Addresses字段**编辑***火星Addresses页*然后打开。火星的地址指示可以可能是一次攻击的原因对网络的IP地址。来自这些网络的信息包被丢弃。

Step 2.检查在后备的火星的地址**包括**并且点击**适用**添加在系统层预防列表的后备的火星的地址。



第 3 步：要添加一个火星的地址请点击**添加**。*添加火星Addresses页*显示。输入这些参数：



第 4 步：在IP Address字段请输入需要被拒绝的IP地址。

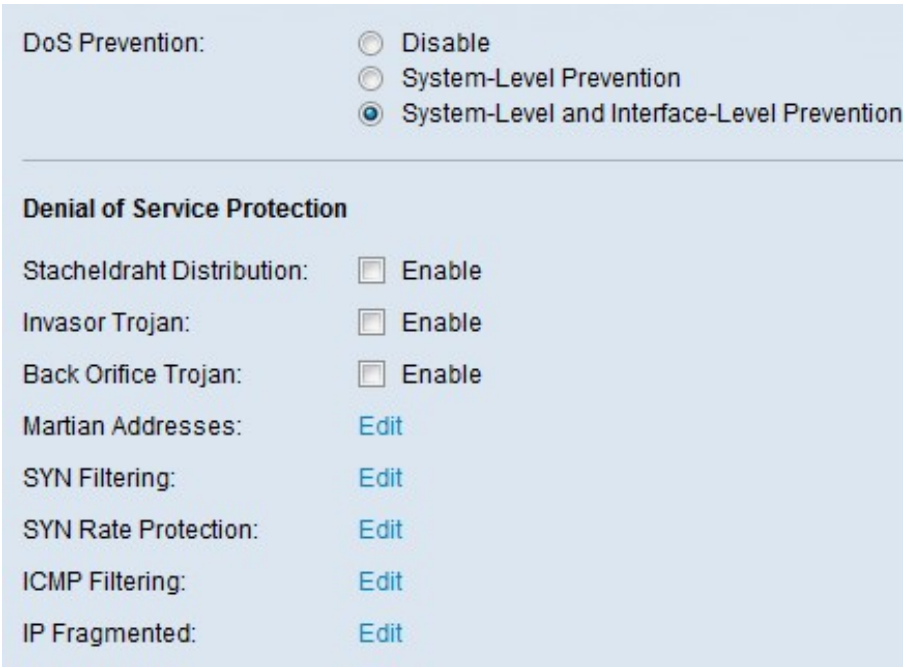
第 5 步：指示应该拒绝IP地址的范围的IP地址掩码。

- IP版本—支持的IP版本。当前，仅IPv4允许。
- 从储备名单—从储备名单选择已知IP地址。
- 新的IP地址—输入IP地址。
- 网络掩码—网络掩码以点分十进制格式。
- 前缀长度—定义拒绝服务预防是启用的IP地址的范围的IP地址前缀。

步骤6.点击**适用**做给运行配置文件将被写的火星的讲演。

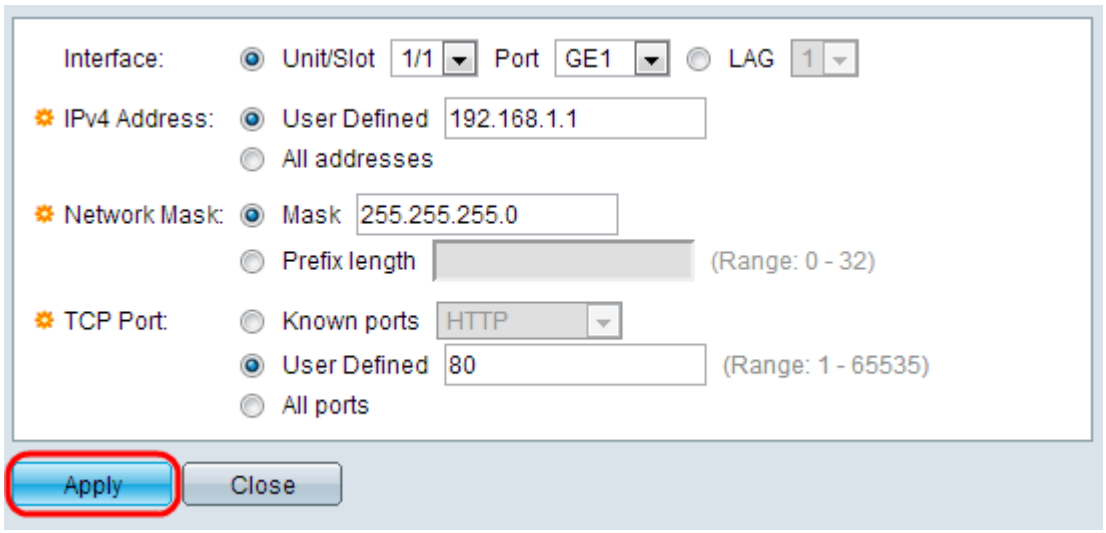
SYN过滤的配置

SYN过滤允许网络管理员丢弃与SYN标志位的非法TCP信息包。SYN端口过滤被定义得在每个端口。



第 1 步：要配置SYN过滤请点击**编辑**，并且*过滤*页的*SYN*打开：

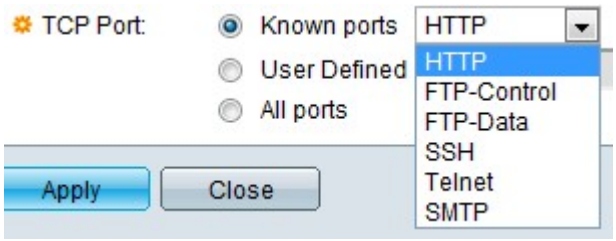
步骤2.点击**添加**。*过滤*页的*添加SYN*显示。输入这些参数在显示域：



步骤3.选择过滤器需要被定义的接口。

步骤4.点击**用户定义**产生过滤器被定义的IP地址或点击**所有地址**。

第 5 步： 过滤器是启用的网络掩码。点击**前缀长度**为了指定长度，其范围是从0到32或者点击**掩码**输入子网掩码正如在点分十进制表示方法。



步骤6.点击被过滤的目的地TCP端口。他们是类型：

- 已知端口—从列表选择端口。
- 用户定义—输入端口号。
- 所有端口—点击表明所有端口被过滤。

步骤7.点击**适用**做过滤的SYN给运行配置文件被写。

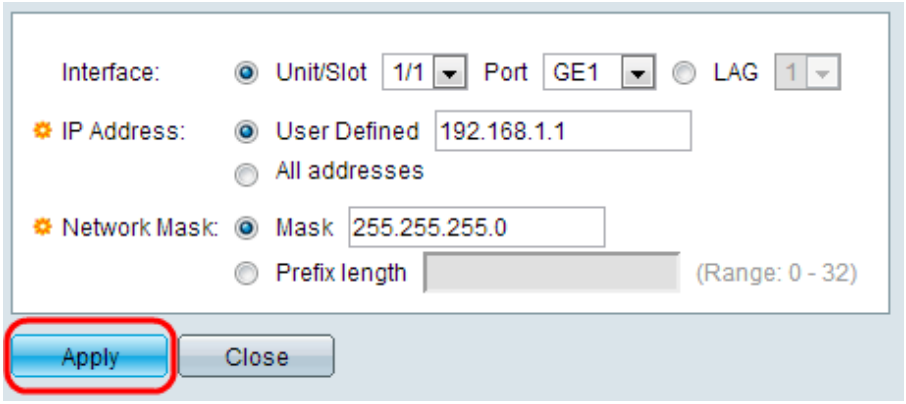
ICMP过滤的配置

互联网控制消息协议(ICMP)是其中一个最重要的互联网协议。它是网络层协议。操作系统用于ICMP发错误信息告诉服务哪些被请求不是可用的或一台特定主机不可能被到达。它也用于发诊断消息。ICMP不可能用于在系统之间的交换数据。他们通常生成以回应在IP数据包的一些错误。

ICMP数据流是非常重要网络数据流，但是可能也导致许多网络问题，如果使用网络由一名有恶意的攻击者。这带动对严格过滤来自互联网的ICMP数据流的需要。*ICMP过滤*页enable (event) ICMP信息包的过滤自特定来源的。如果有任何ICMP攻击，这使在网络的负荷减到最小，万一。

第 1 步：要配置ICMP过滤请点击**编辑，**并且*ICMP过滤*页打开。

步骤2.点击**添加**。*添加ICMP过滤*页显示。输入这些参数在显示域：



步骤3.选择ICMP过滤被定义的接口。

步骤4.输入ICMP信息包过滤是启用的IPv4地址或点击**所有地址**阻拦自所有源地址的ICMP信息包。如果IP地址被输入，请输入掩码或前缀长度。

第 5 步： 费率保护是启用的网络掩码。选择网络掩码的格式IP原地址的并且点击其中一个字段。

- 掩码—选择IP原地址属于对的子网并且输入子网掩码以点分十进制格式。
- 点击**前缀长度**为了指定长度，并且输入包括IP原地址前缀位的数量，其范围是从0到32。

步骤6.点击**适用**做给运行配置文件将被写的ICMP过滤。

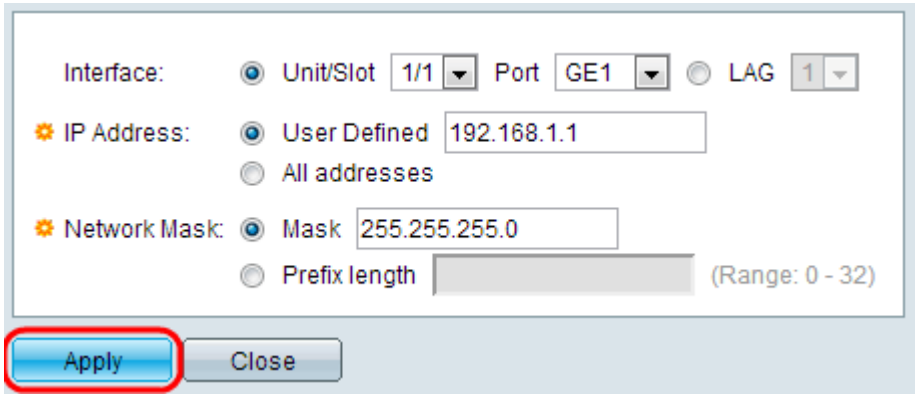
IP段过滤的配置

所有信息包有最大传输单元(MTU)大小。是的MTU网络能传输最大的信息包的大小。IP利用分段，以便比原始信息包大小能通过与更小的MTU的一条链路横断的信息包可以形成。所以，大小大于链路的可允许MTU必须分开的信息包成更小的信息包给他们通过链路横越。

另一方面，分段能也提出许多安全问题。因此，当他们可以有时是系统妥协的一个原因阻拦IP段变得必要。

第 1 步：要配置过滤点击的IP段请**编辑，**并且*过滤*页的*ICMP片段*打开。

步骤2.点击**添加**。*添加IP段过滤*页显示。输入这些参数在显示域：



步骤3.接口—选择IP分段被定义的接口。

步骤4. IP地址—输入IP分段是启用的IP地址或点击**所有地址**阻拦自所有源地址的IP分段的信息包。如果IP地址被输入，请输入掩码或前缀长度。

步骤5.网络掩码— IP分段被阻拦的网络掩码。选择网络掩码的格式IP原地址的并且点击其中一个字段。

- 掩码—选择IP原地址属于对的子网并且输入子网掩码以点分十进制格式。
- 点击**前缀长度**为了指定长度，并且输入包括IP原地址前缀位的数量，其范围是从0到32。

步骤6.点击**适用**做过滤的IP段给运行配置文件被写。