在Sx500系列堆叠式交换机上配置拒绝服务防御技术（安全套件）

目标

拒绝服务(DoS)或分布式拒绝服务(DDoS)攻击限制有效用户使用网络。攻击者通过泛洪网络来执行DOS攻击，这些网络包含许多不必要的请求，占用了网络的所有带宽。DoS攻击可能会减缓网络运行速度，也可能导致网络瘫痪数小时。它会检测异常流量并对其进行过滤。

本文介绍在安全套件设置上配置拒绝服务以及用于拒绝服务防御的各种技术。

注意：如果选择的DoS防御是系统级和接口级防御，则可以编辑和配置军事地址、SYN过滤、SYN速率保护、ICMP过滤和IP分段过滤。本文也对这些配置进行了说明。

注意：在激活DoS防御之前，必须解除所有访问控制列表(ACL)或配置到端口的任何高级QoS策略的绑定。在端口上启用DoS保护后，ACL和高级QoS策略将不处于活动状态。

适用设备

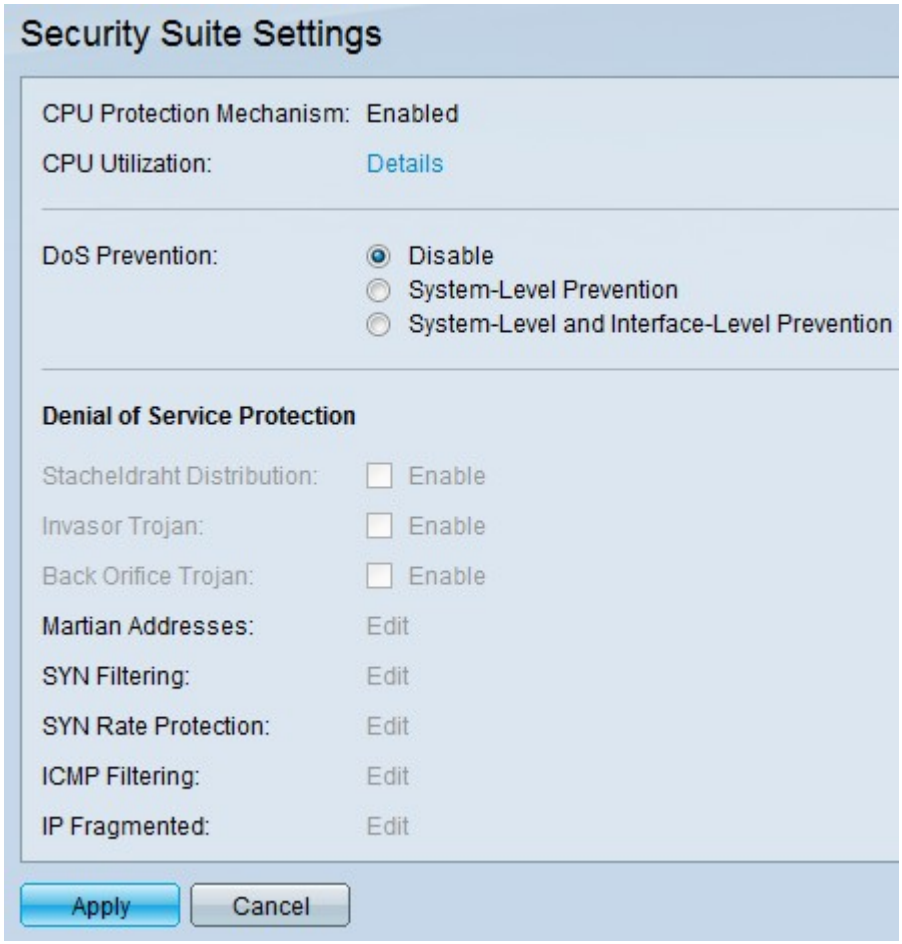
- SX500系列堆叠式交换机

软件版本

- 1.3.0.62

在安全套件设置上配置拒绝服务

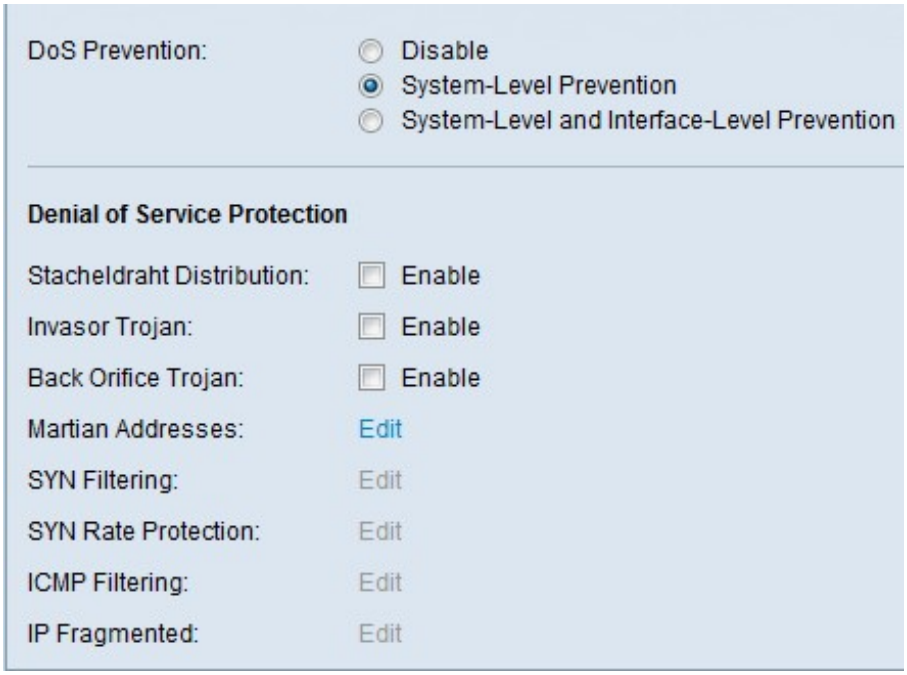
步骤1.登录Web配置实用程序，然后选择**Security > Denial of Service Prevention > Security Suite Settings**。“安全*套件设置*”页面打开：



- CPU保护机制 — 这是
- **启用**.这表示已启用安全转换工具(SCT)。
- CPU利用率 — 单击
- **CPU利**用率旁边的详细信息，用于查看CPU资源利用率信息。

步骤2.点击DoS Prevention字段下的相应单选按钮。

- 禁用 — 禁用DoS防御。
- System-Level Prevention — 这可防止来自Stacheldraht Distribution、Invasor特洛伊木马和Back Orifice特洛伊木马的攻击。
- 系统级和接口级防御 — 可防止交换机上每个接口的攻击。



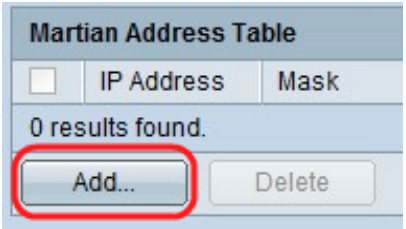
步骤3.可以为拒绝服务保护选择以下选项：

- Stacheldraht Distribution — 这是DDoS攻击的示例，其中攻击者使用客户端程序连接到网络内的计算机。然后，这些计算机向内部服务器发出多个登录请求并发起DDoS攻击。
- Invasor特洛伊木马 — 如果计算机受到此攻击的感染，则TCP端口2140用于恶意活动。
- Back Orifice特洛伊木马 — 这会丢弃用于与服务器和客户端程序通信以进行DoS攻击的UDP数据包。

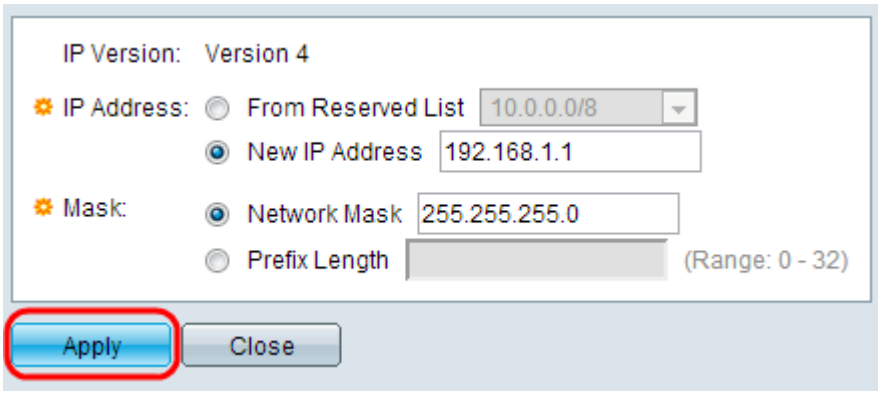
配置Martian地址

步骤1.在“火星地**址**”字段中单击“编辑”，然后*打开“火星*地址”页。Martian Addresses表示可能是网络攻击原因的IP地址。来自这些网络的数据包将被丢弃。

步骤2.选中**Include in the Reserved Martian Addresses**，然后单击**Apply**，在System Level Prevention列表中添加Reserved Martian Addresses。



步骤3.要添加Martian Address，请单击**Add**。系统将*显示"添加*火星地址"页。输入以下参数：



步骤4.在IP Address字段中，输入需要拒绝的IP地址。

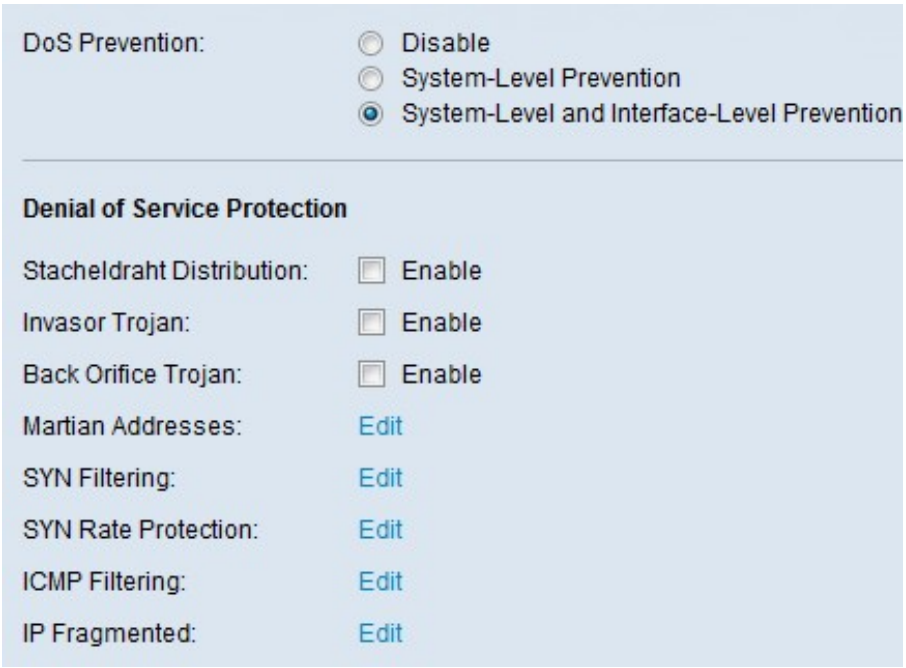
步骤5. IP地址的掩码，表示应拒绝的IP地址范围。

- IP版本 — 支持的IP版本。目前，仅允许IPv4。
- 从保留列表 — 从保留列表中选择已知IP地址。
- 新IP地址 — 输入IP地址。
- 网络掩码 — 点分十进制格式的网络掩码。
- 前缀长度 — IP地址的前缀，用于定义启用拒绝服务防御的IP地址范围。

步骤6.单击**Apply**，使Martian Address写入Running Configuration文件。

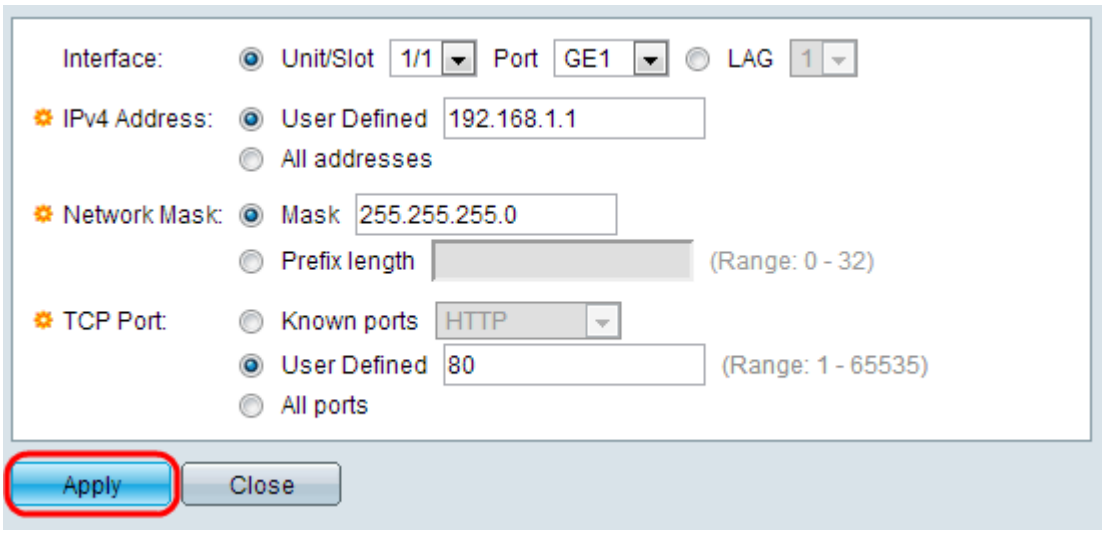
配置SYN过滤

SYN过滤允许网络管理员丢弃带有SYN标志的非法TCP数据包。SYN端口过滤是按端口定义的。



步骤1.要配置SYN过滤，请单击**编辑**，然后*打开SYN过*滤页面：

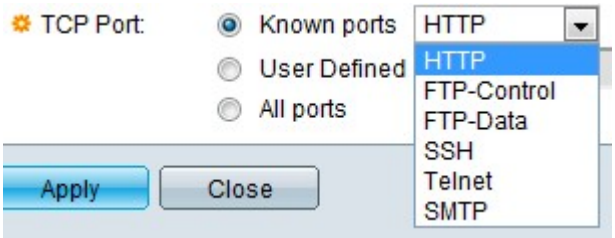
步骤2.单击“添**加**”。将显示*Add SYN过滤*页面。在显示的字段中输入以下参数：



步骤3.选择需要定义过滤器的接口。

步骤4.单击**User Defined**（用户定义）以提供为其定义过滤器的IP地址，或单击**All Addresses(所有地**址)。

步骤5.启用过滤器的网络掩码。单击**Prefix Length**以指定长度，其范围为0到32，或单击**Mask**以点分十进制记法输入子网掩码。



步骤6.点击要过滤的目的TCP端口。这些类型包括：

- 已知端口(Known Ports) — 从列表中选择端口。
- 用户定义 — 输入端口号。
- 所有端口(All Ports) — 点击以指示已过滤所有端口。

步骤7.单击**Apply**，使SYN过滤写入运行配置文件。

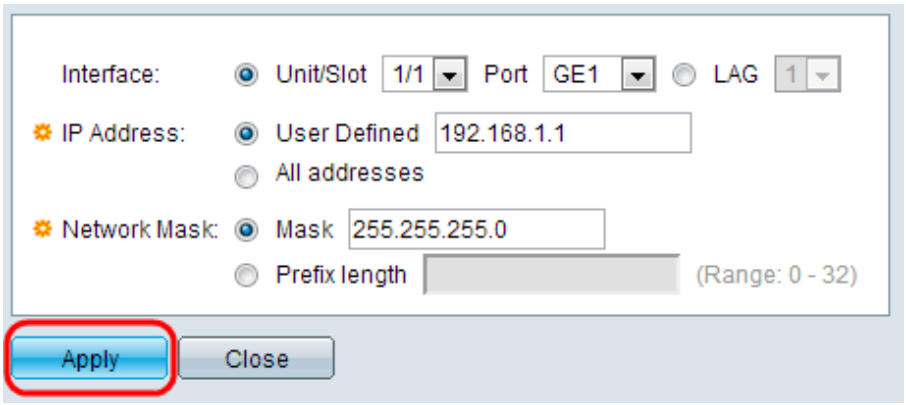
配置ICMP过滤

互联网控制消息协议(ICMP)是最重要的互联网协议之一。它是网络层协议。操作系统使用ICMP发送错误消息，以告知请求的服务不可用或无法访问特定主机。它还用于发送诊断消息。ICMP不能用于在系统之间交换数据。它们通常是为了响应IP数据报中的某些错误而生成的。

ICMP流量是非常关键的网络流量，但如果恶意攻击者对网络使用ICMP流量，也会导致许多网络问题。这就需要严格过滤来自Internet的ICMP流量。*ICMP过滤*页启用对来自特定源的ICMP数据包的过滤。这可以最大限度地减少网络负载，以防发生任何ICMP攻击。

步骤1.要配置ICMP过滤，请单击**编辑**，然后*打开ICMP过滤*页面。

步骤2.单击“添**加**”。此时将显示“*添加ICMP过滤*”页。在显示的字段中输入以下参数：



步骤3.选择定义ICMP过滤的接口。

步骤4.输入启用ICMP数据包过滤的IPv4地址，或点击All Addresses以阻止来自所有源**地址的**ICMP数据包。如果输入了IP地址，请输入掩码或前缀长度。

步骤5.启用速率保护的网络掩码。选择源IP地址的网络掩码格式，然后单击其中一个字段。

- 掩码 — 选择源IP地址所属的子网，并以点分十进制格式输入子网掩码。
- 单击**Prefix Length**以指定长度并输入由源IP地址前缀组成的位数，其范围为0到32。

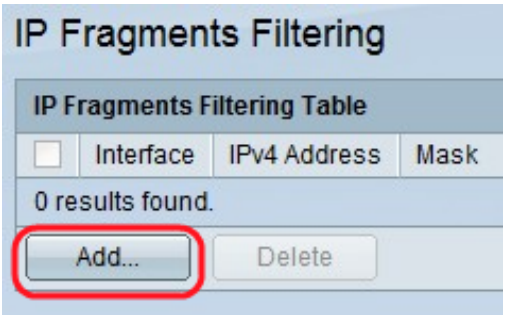
步骤6.单击**Apply**，使ICMP过滤写入运行配置文件。

配置IP分段过滤

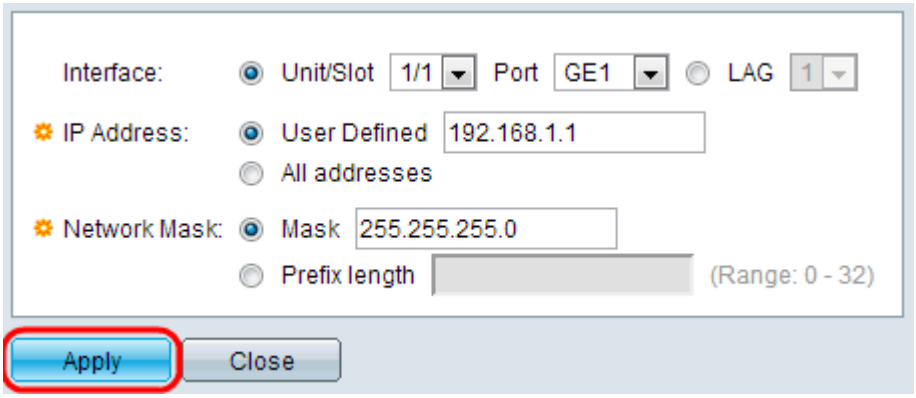
所有数据包都具有最大传输单位(MTU)大小。MTU是网络可以传输的最大数据包的大小。IP利用分段的优势，以便形成数据包，该数据包可以通过MTU小于原始数据包大小的链路传输。因此，其大小大于链路允许的MTU的数据包必须划分成更小的数据包，以允许其通过链路。

另一方面，碎片也可能带来许多安全问题。因此，有时IP分段可能是造成系统危害的原因，因此有必要对其进行阻止。

步骤1.要配置IP分段过滤，请单击“编辑”**，然后**打开“*ICMP分段过滤*”页面。



步骤2.单击“添**加**”。此时将显示“*添加IP分片过滤*”页。在显示的字段中输入以下参数：



步骤3.接口 — 选择定义IP分段的接口。

步骤4. IP Address — 输入启用IP分段的IP Address，或单击All Addresses**以阻**止来自所有源地址的IP分段数据包。如果输入了IP地址，请输入掩码或前缀长度。

步骤5. Network Mask — 阻止IP分段的网络掩码。选择源IP地址的网络掩码格式，然后单击其中一个字段。

- 掩码 — 选择源IP地址所属的子网，并以点分十进制格式输入子网掩码。
- 单击**Prefix Length**以指定长度并输入由源IP地址前缀组成的位数，其范围为0到32。

步骤6.单击**Apply**，使IP分段过滤写入运行配置文件。