300系列托管交换机上的拒绝服务(DoS)SYN过滤配置

目标

拒绝服务(DoS)攻击使网络泛洪错误流量。这会使网络服务器资源远离合法用户。SYN泛洪特别针对TCP协议。TCP协议需要三个步骤才能运行。首先，用户将其IP地址发送到服务器并请求连接。然后，服务器响应请求并等待确认。最后，用户确认服务器已打开连接。TCP SYN攻击使用多个IP地址请求连接，但连接打开后，永远不会向服务器发回确认。服务器在开始丢弃TCP请求之前只能打开有限数量的连接，即使来自合法用户也是如此。

TCP流量在多个虚拟端口上发送。这些端口是将网络流量拆分为通用组的一种方式。SYN过滤器可配置为阻止来自特定虚拟端口的流量。此外，SYN过滤是在交换机的实际物理端口或LAG上配置的。本文介绍如何在300系列托管交换机上配置SYN过滤。

注意：仅当启用DoS防御时，才可使用同步过滤器。有关帮助，请参*阅"300系列托管交换机上的安全套件设*置"一文。

适用设备

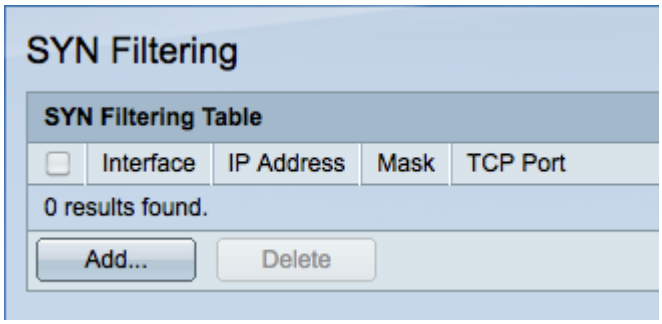
·SF/SG 300系列托管交换机

软件版本

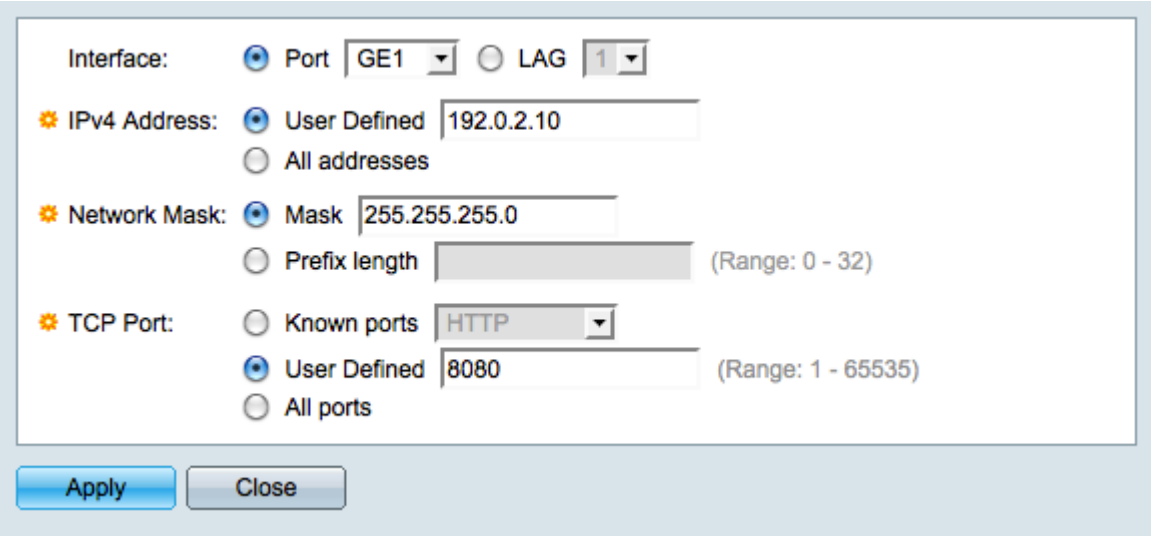
•v1.2.7.76

SYN过滤配置

步骤1.登录Web配置实用程序并选择**Security > Denial of Service Prevention > SYN Filtering**。"SYN过*滤"(SYN Filtering*)页面打开：



步骤2.单击**Add**添加新的SYN过滤器。系统将*显示Add Syn Filtering*窗口。



步骤3.在Interface字段中，点击与所需接口对应的单选按钮。这是过滤器将分配给的物理位置。

·端口 — 交换机上的物理端口。从Port下拉列表中选择特定端口。

·LAG — 充当单个端口的一组端口。从LAG下拉列表中选择特定LAG。

步骤4.在IPv4 Address字段中，点击与所需IPv4地址对应的单选按钮。

·用户定义 — 输入要针对TCP流量过滤的IP地址。

·所有地址 — 所有IPv4地址都针对TCP流量进行过滤。如果选择了“所有地址”，请跳至步骤6。

步骤5.在Network Mask字段中，点击与用于定义IP地址的子网掩码的方法对应的单选按钮。

·掩码 — 在网络掩码字段中输入网络掩码。

·前缀长度(Prefix Length) — 在前缀长度(Prefix length)字段中输入前缀长度（范围为0到32的整数）。

步骤6.点击与要在TCP Port字段中过滤的所需TCP端口对应的单选按钮。这些是网络流量被划分为的虚拟端口。

·Known Ports — 从Known Ports下拉列表中选择要过滤的TCP端口。

·用户定义 — 输入要过滤的TCP端口。

·所有端口 — 所有TCP端口都经过过滤。

步骤7.单击**Apply**保存更改，然后单击**Close**退出*Add Syn Filtering*窗口。