SX500系列堆叠式交换机上的IP源防护配置

目标

IP源防护是一种安全功能，可用于防止主机尝试使用相邻主机的IP地址时引起的流量攻击。启用IP源防护后，交换机仅将客户端IP流量传输到DHCP监听绑定数据库中包含的IP地址。如果主机发送的数据包与数据库中的条目匹配，交换机将转发该数据包。如果数据包与数据库中的条目不匹配，则会丢弃该数据包。

在实时场景中，使用IP源防护的一种方式是帮助防止不受信任的第三方试图伪装成正版用户的中间人攻击。根据在IP源防护绑定数据库中配置的地址，仅允许来自具有该IP地址的客户端的流量，并丢弃其余数据包。

注意：应启用DHCP监听，IP源防护才能正常工作。要获取有关如何启用DHCP监听的更多详细信息，请参阅SX500系列可堆叠交换*机上的DHCP监听配置文章*。还需要配置绑定数据库以指定允许哪些IP地址。有关此项的更多详细信息，请参阅SX500系*列堆叠式交换机上DHCP监听绑定数据库的配置文章。*

本文介绍如何在Sx500系列堆叠式交换机上配置IP源防护。

适用设备

·Sx500系列堆叠式交换机

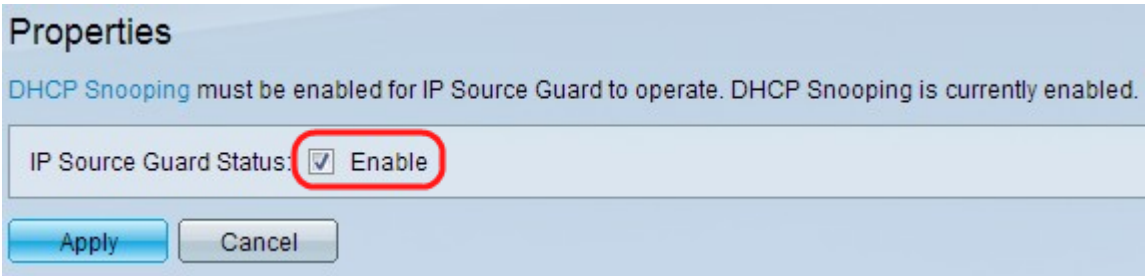
软件版本

•v1.2.7.76

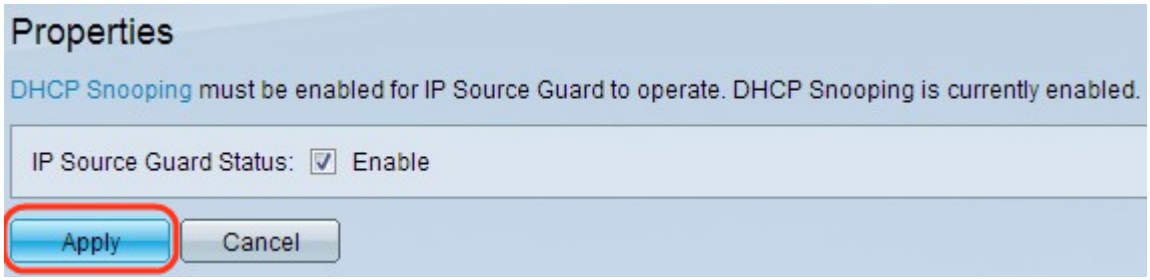
配置IP源防护设置

全局启用IP源防护设置

步骤1.登录到Web配置实用程序，然后选择**Security > IP Source Guard > Properties**。“IP*源防护属性*”页打开：



步骤2.选中**Enable**复选框以全局启用IP源防护。



步骤3.单击“**应用**”以应用设置。

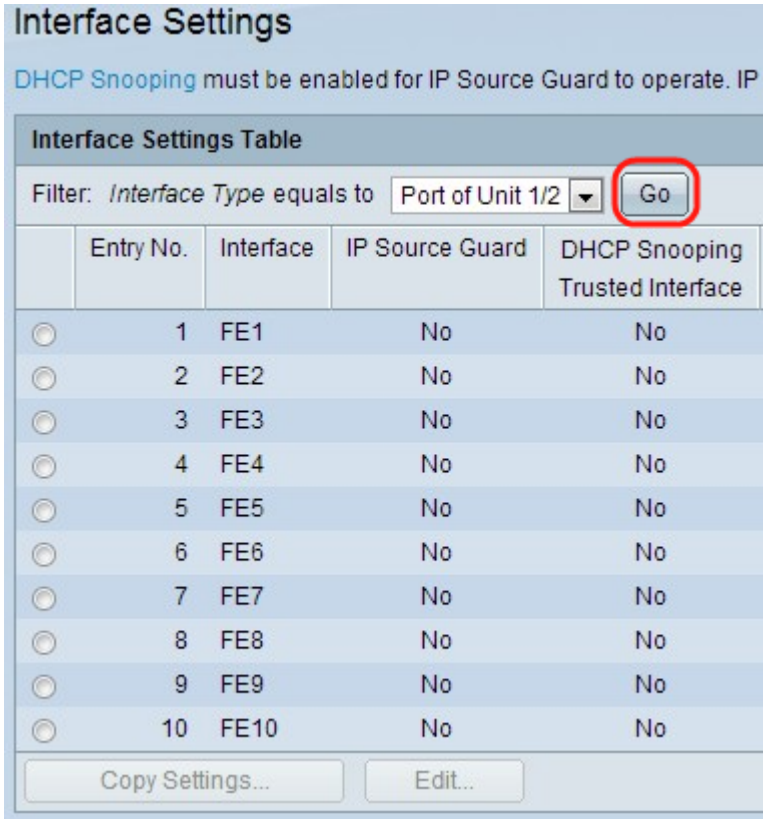
编辑IP源防护的接口设置

如果在不受信任的端口或LAG上启用IP源防护，则DHCP监听数据库允许传输的DHCP数据包。如果IP地址启用了过滤器，则允许数据包传输，如下所示：

·IPv4流量 — 允许与特定端口的源IP地址关联的IPv4流量。

·非IPv4流量 — 允许所有非IPv4流量。

步骤1.登录到Web配置实用程序，然后选择**Security > IP Source Guard > Interface Settings**。“接口 *设置*”页面打开：



步骤2.从Interface Type下拉列表中选择接口类型，然后在Filter字段**中单**击Go。

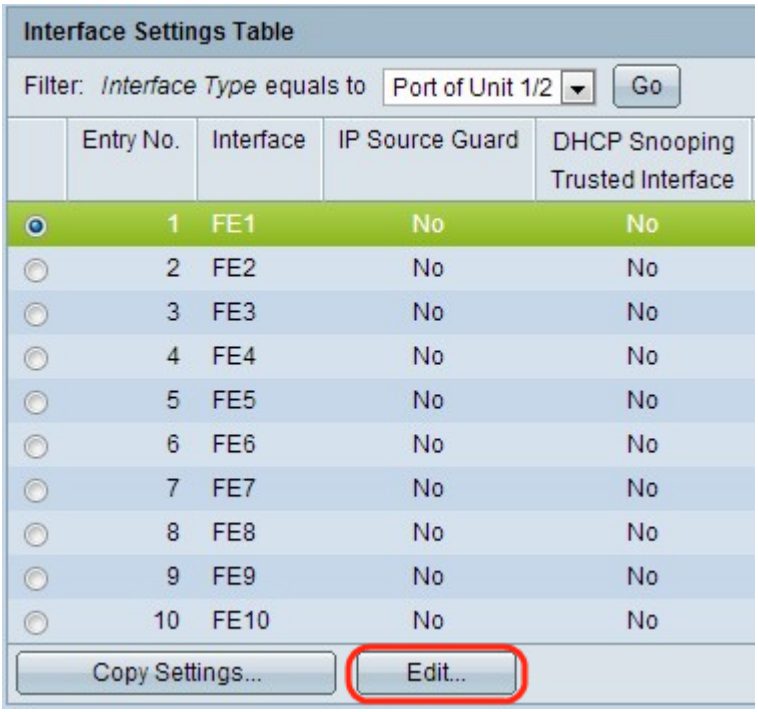
接口设置表包含以下参数。

·接口 — 显示应用IP源防护的接口。

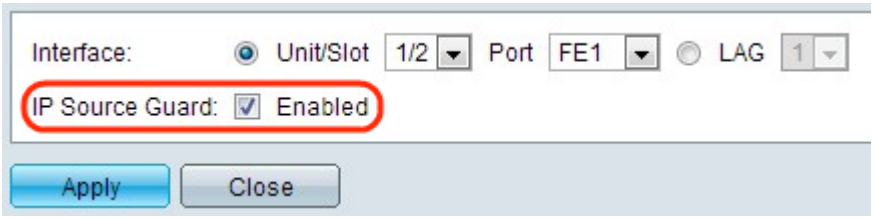
·IP Source Guard — 显示是否启用IP Source Guard。

·DHCP监听受信任接口 — 显示它是否是DHCP受信任接口。受信任接口只能从网络内接收流量。 IP源防护通常在不受信任的DHCP接口上配置。不可信接口是配置为能够从网络外部

接收消息的接口。

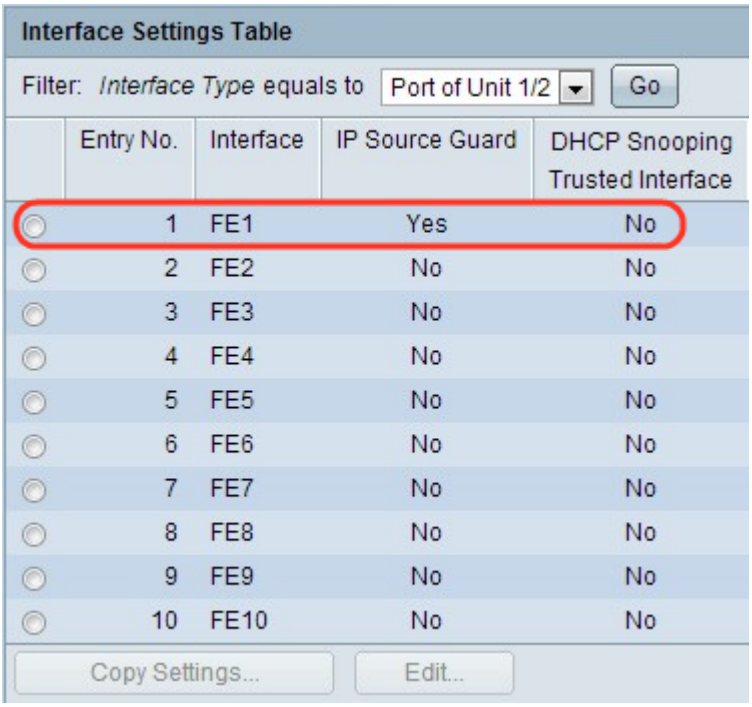


步骤3.点击与要编辑的接口对应的单选按钮，然后点**击页**面底部的编辑。系统将显示*"编辑接口设置"*窗口。



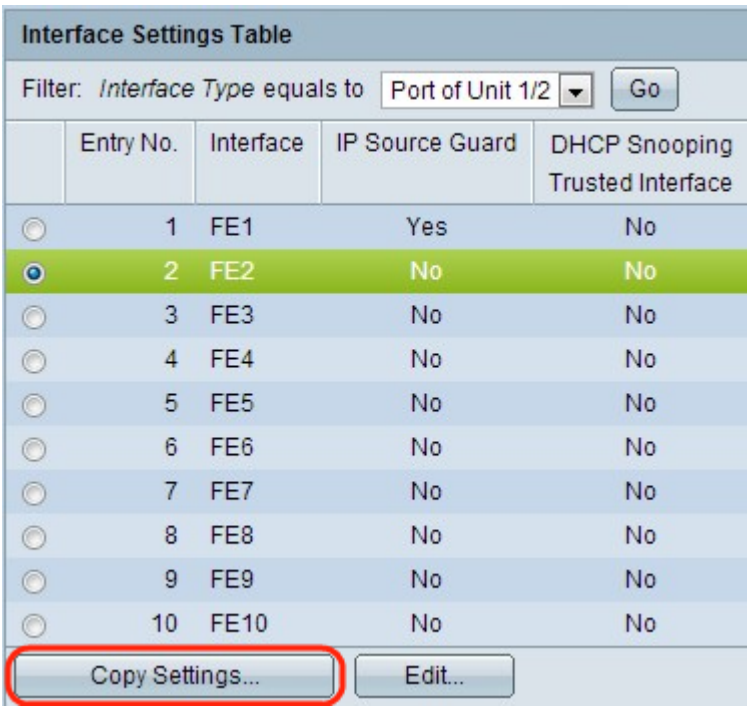
步骤4.在IP Source Guard字段中选中**Enable**，以在当前接口上启用IP Source Guard。

步骤5.单击**"应用"**。将显示更改。

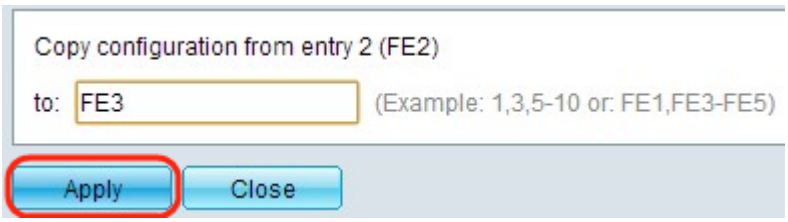


复制IP源防护的接口设置

步骤1.登录到Web配置实用程序，然后选择**Security > IP Source Guard > Interface Settings**。"接口*设置*"页面打开：



步骤2.单击所需接口的单选按钮，然后单击"复制设**置**"。系统将显示"*复制设*置"窗口。



步骤3.输入需要将所选条目复制到的接口或接口范围，然后单击"应**用**"。将应用设置。