在Sx500系列可堆叠交换机的IP源防护配置

客观

IP源防护是能使用防止导致的数据流攻击的安全功能，当主机设法使用一台相邻的主机时的IP地址。当IP源防护是启用的时，交换机只传输客户端IP数据流对在DHCP监听的约束数据库包含的IP地址。如果主机发送匹配在数据库的一个条目的信息包，交换机转发信息包。如果信息包不匹配在数据库的一个条目被丢弃。

在一个实时方案中， IP源防护使用的一种方式将帮助防止不信任的第三方尝试化妆象一个真正用户的中间人攻击。 基于在IP源防护约束数据库被配置的地址，只有从客户端的数据流用该IP地址允许和信息包的其余丢弃。

Note: 监听的DHCP应该是启用的为了IP源防护能作用。为了获得关于怎样的更多详细资料对请监听enable (event)的DHCP请参见*在SX500系列可堆叠交换机的*条款*DHCP监听的配置*。配置约束数据库指定也是必要的哪些IP地址允许。在此的更多详细资料可以在*DHCP监听的约束数据库的*条款*配置在SX500系列可堆叠交换机的*找到。

此条款说明如何配置在Sx500系列可堆叠交换机的IP源防护。

可适用的设备

•Sx500系列可堆叠交换机

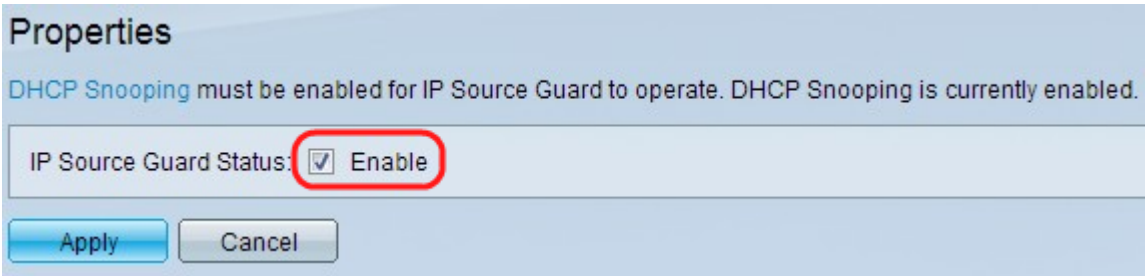
软件版本

•v1.2.7.76

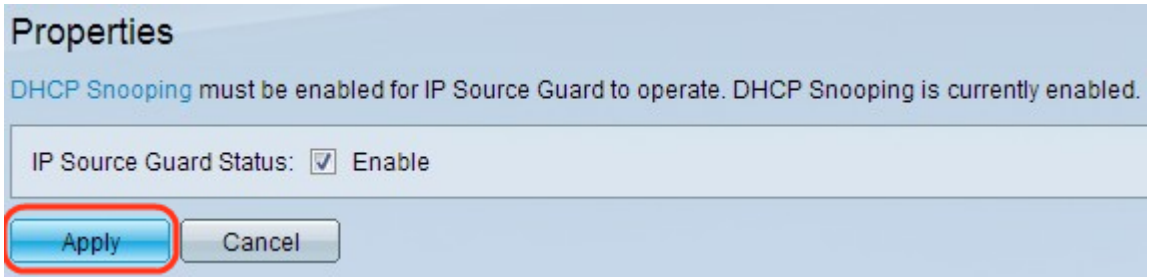
配置IP源防护设置

Enable (event)全局IP源防护设置

步骤1.登陆到Web配置工具并且选择**安全> IP源防护>Properties**。*Properties页的IP源防护*打开：



Step 2.检查**Enable复选框**对enable (event) IP源防护全局。



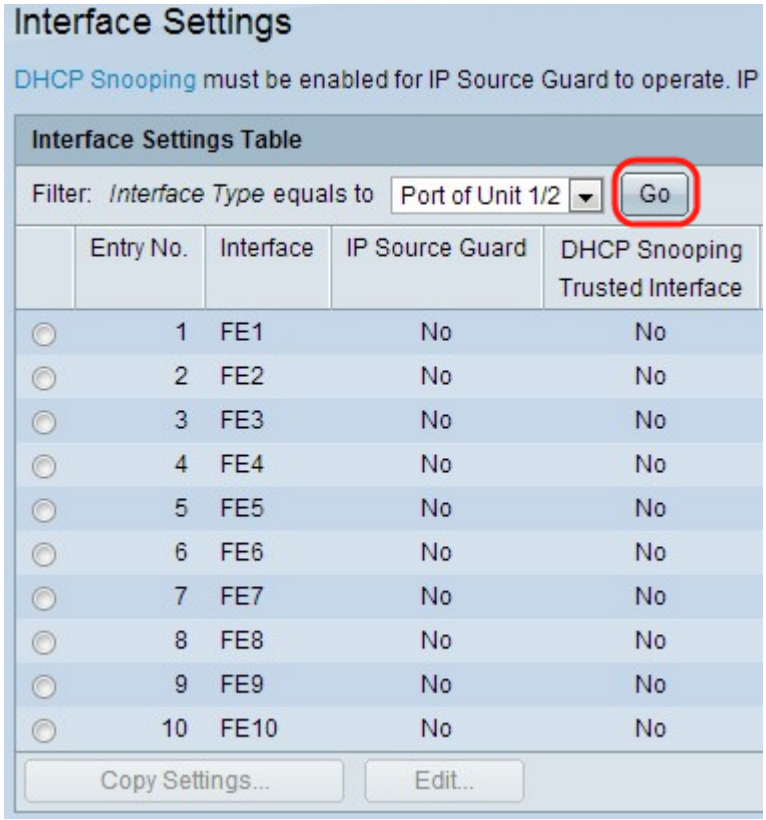
步骤3.点击**适用**应用设置。

编辑IP源防护的接口设置

如果IP源防护在不信任的端口或滞后允许，传输的DHCP信息包由DHCP监听的数据库允许。如果IP地址用过滤器允许那么信息包传输允许如下：

- IPv4数据流—与特定端口的IP原地址产生关联的IPv4数据流允许。
- 非IPv4数据流—所有non-IPv4数据流允许。

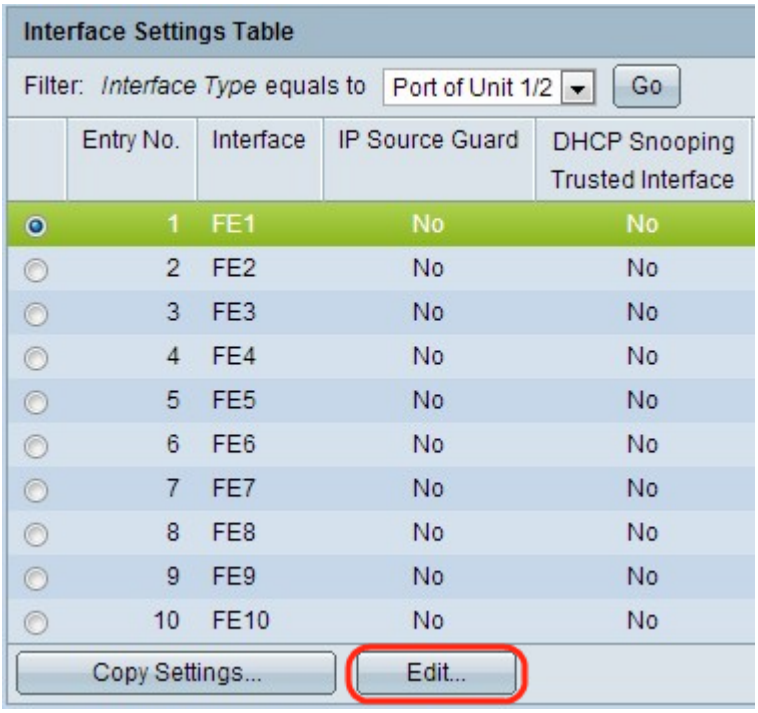
步骤1.登陆到Web配置工具并且选择**安全> IP源防护>接口设置**。*Settings页的接口*打开：



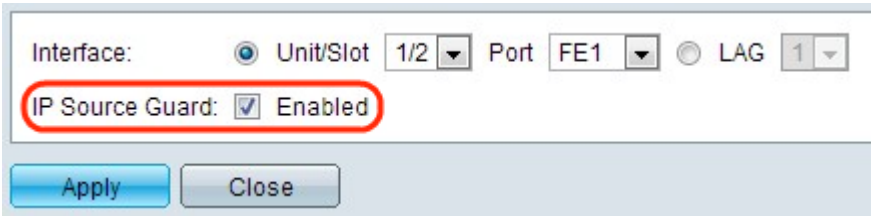
步骤2.从接口类型下拉列表选择接口类型并且点击**进来**在过滤器领域。

接口设置表包括以下参数。

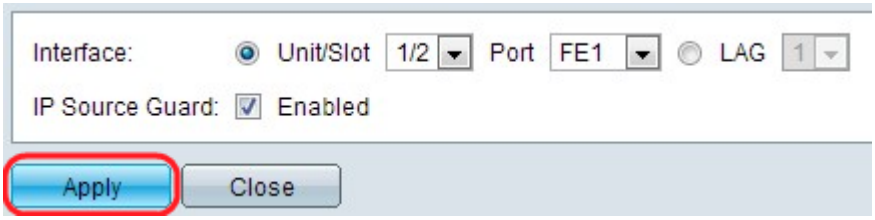
- 接口—显示IP源防护适用的接口。
- IP源防护—显示是否IP源防护是启用的。
- DHCP监听的受信接口—显示是否它是DHCP受信接口。委托的接口能仅收到数据流从网络的内部。 IP源防护在没有委托的DHCP接口通常被配置。不信任的接口是配置这样的接口能从网络外面收到消息。



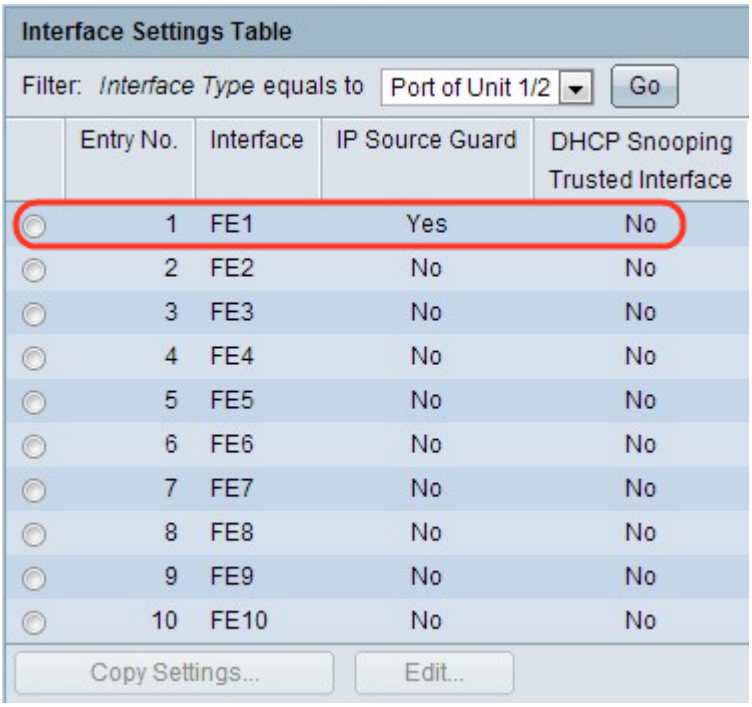
步骤3.点击对应于将被编辑的接口的单选按钮并且点击**编辑**在页底端。*Settings窗口编辑的接口*出现。



第 4 步：检查在IP源防护字段的**Enable (event)**对enable (event)在当前接口的IP源防护。

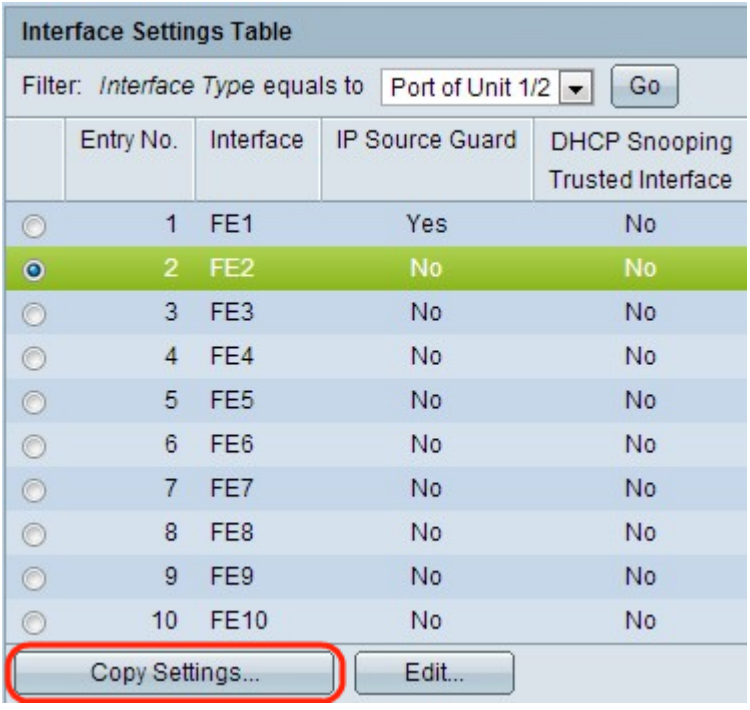


步骤5.点击**适用**。更改显示。

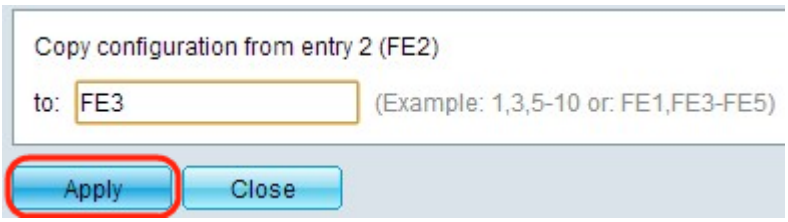


复制IP源防护的接口设置

步骤1.登陆到Web配置工具并且选择**安全> IP源防护>接口设置**。*Settings页的接口*打开：



步骤2.点击所需的接口的单选按钮并且点击**"Copy"设置**。*Settings窗口的复制*出现。



步骤3.进入接口或选择的条目需要被复制接口的范围和点击**适用**。设置适用。