捆绑访问控制表(ACL)对在200/300系列被管理的交换机的一个接口

客观

访问控制表(ACL)是网络列表用于的数据流过滤器和关联的动作改进安全。ACL可以在三种方式之一中被定义：由MAC地址，由IPv4地址，或者由IPv6地址。当ACL一定对接口，到达该接口被匹配ACL的信息包和允许或丢弃。然而，仅一个ACL可以每个接口一定。

本文解释如何捆绑ACL到在200和300系列被管理的交换机的一个接口。

可适用的设备

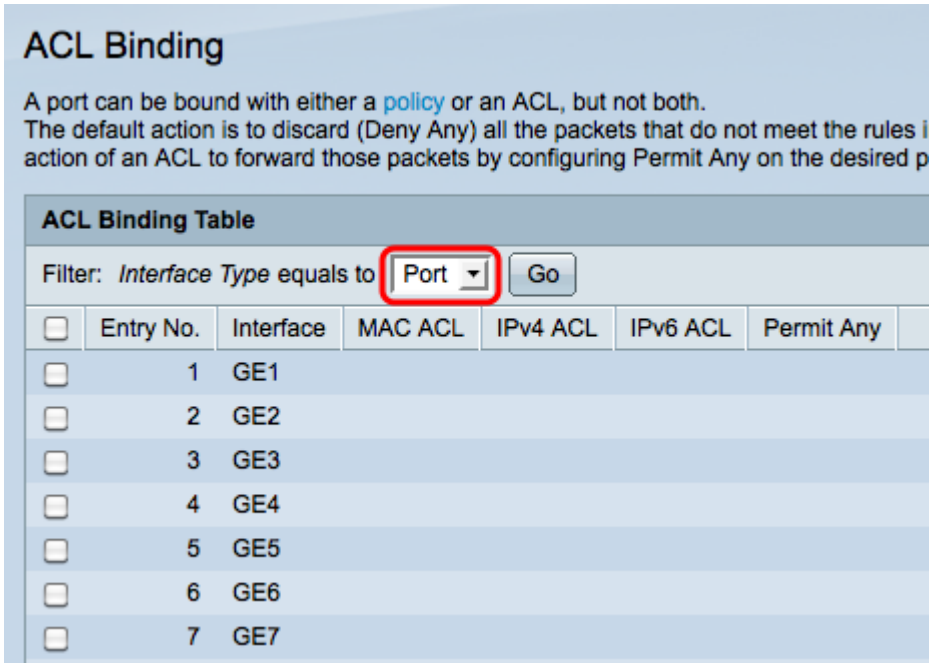
•SF/SG 200和SF/SG300系列被管理的交换机

软件版本

•1.3.0.62

对接口的捆绑访问控制表

步骤1.登陆到Web配置工具并且选择**访问控制> ACL捆绑**。*ACL约束*页打开：

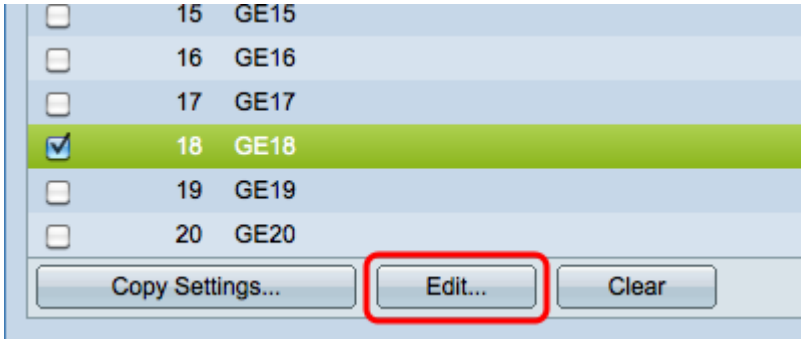


步骤2.从接口类型下拉列表选择了接口然后点击**去**。

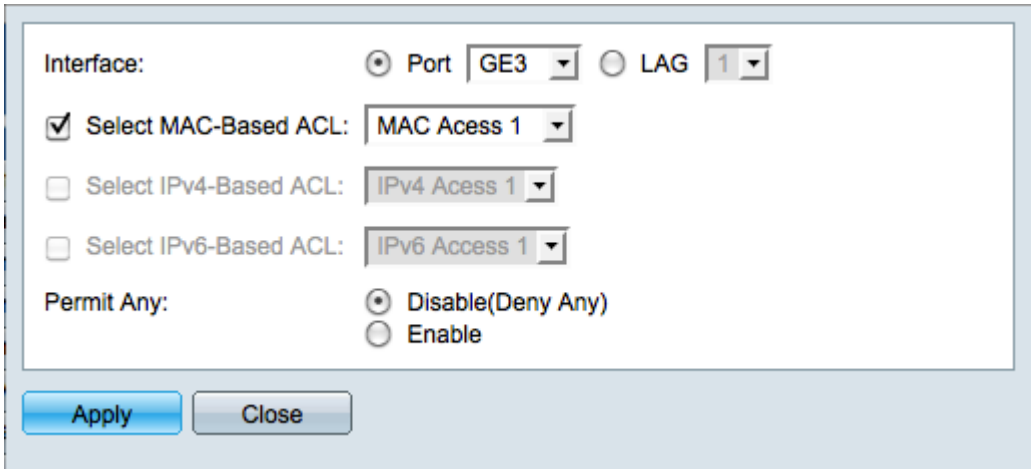
•端口—在交换机的单个物理端口。

•滞后—用于的一个端口组增加链路可靠性。

第 3 步：检查期望port/LAG的复选框并且点击编辑。



*编辑ACL约束*窗口出现。



第 4 步：检查您希望捆绑到选择的接口和从下拉列表选择ACL ACL类型的复选框。

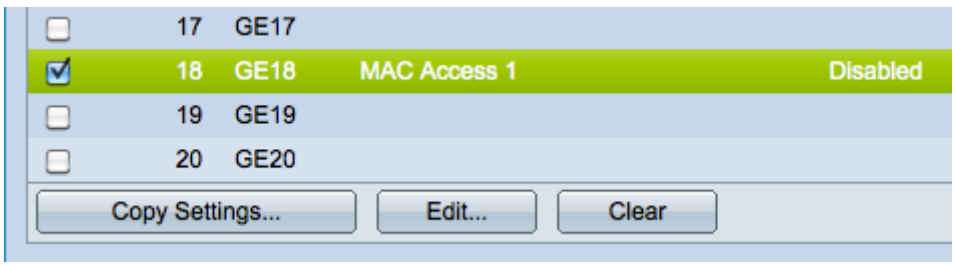
- •基于MAC的ACL —过滤流量根据帧标头的第2层字段。
- •IPv4-Based ACL —根据IPv4信息包的过滤流量。
- •IPv6-Based ACL —根据IPv6信息包的过滤流量。

Note:如果有可用的ACL以该格式的复选框任何ACL选项只将突出显示。

第 5 步：检查在许可证的appropriate单选按钮所有字段定义如何处理不匹配选择的ACL的信息包。

- •功能失效(请拒绝其中任一) —信息包被丢弃(拒绝)，如果他们不匹配ACL。
- •Enable (event) —转发信息包，即使他们不匹配ACL。

步骤6.点击**适用**捆绑选择的ACL到接口。*编辑ACL约束*窗口关闭。
第7.步(可选的)检查所需的接口的复选框和清楚点击解开从ACL的接口。



第8.步(可选的)检查所需的接口的复选框和点击**"Copy"设置**复制接口的设置到其他接口。
*Settings窗口的复制*出现：

步骤9.输入您希望复制选择的端口的设置端口的端口号或端口名。

步骤10.点击**适用**应用设置或点击**接近**取消设置。