捆绑在一台被管理的交换机的入口或出口访问控制表(ACL)

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。它阻拦或允许用户访问特定资源。ACL包含允许或对网络设备的拒绝访问的主机。

ACL可以适用不仅于入口，而且于输出接口。入口(入站)和出口(outbound) ACL的目的将指定从在网络的设备允许或的网络类型数据流。此功能允许管理员过滤在网络的数据流到互联网，或者到组织防火墙。

此条款提供指令关于怎样配置和捆绑在您的交换机的入口或出口ACL。

可适用的设备

- Sx350系列
- SG350X系列
- Sx550X系列

软件版本

- 2.2.0.66

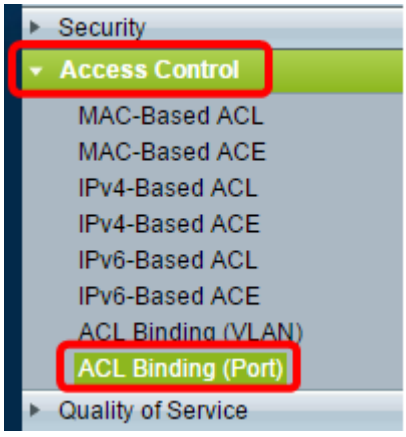
配置入口或出口ACL

重要信息：保证在您的交换机配置的您有ACL和访问控制项(ACE)。要配置IPv4-based ACL和ACE，为指令请点击此处。对于IPv6-based，请点击此处。要配置基于MAC的ACL和ACE，请点击此处。

配置在接口的入口ACL

步骤1.基于Web的工具的洛金然后选择**访问控制> ACL捆绑(端口)**。

Note:在此方案中，使用SG350-28MP交换机。

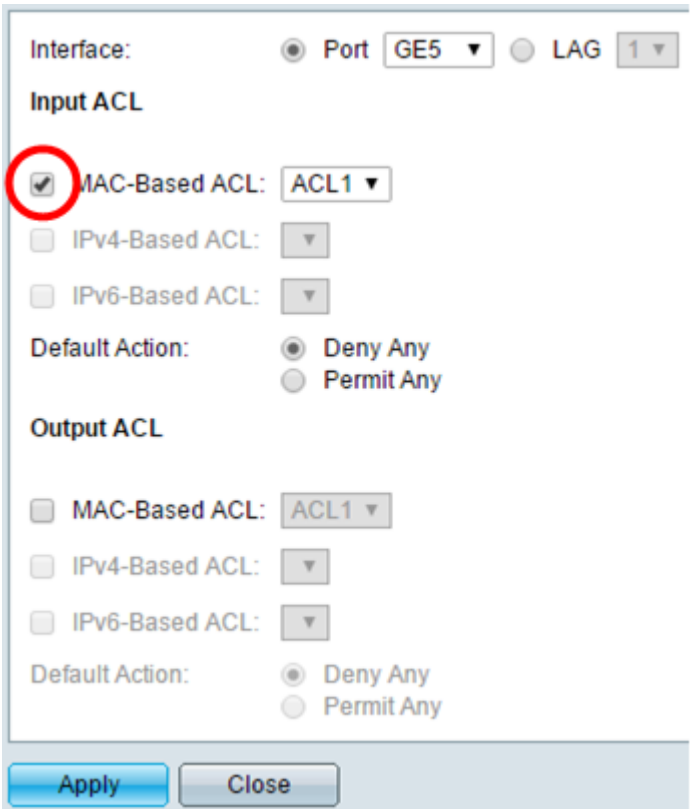


Step 2.在接口旁边检查复选框您要适用ACL对，然后点击**编辑**。

Note:在本例中， ACL将适用于GE5接口。

第3.步。要配置在接口的入口ACL，请检查期望输入ACL复选框。

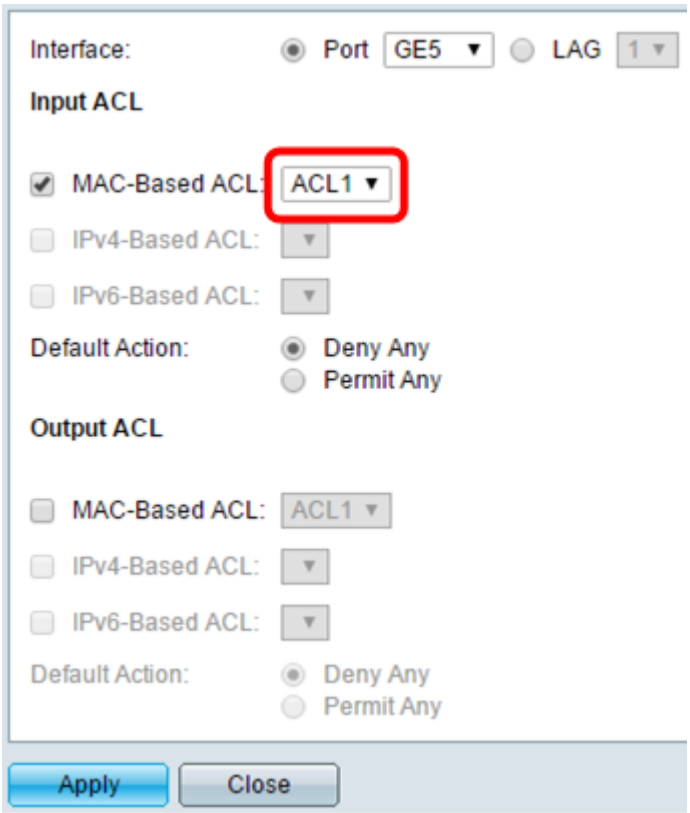
Note:在本例中，基于MAC的ACL被选择。



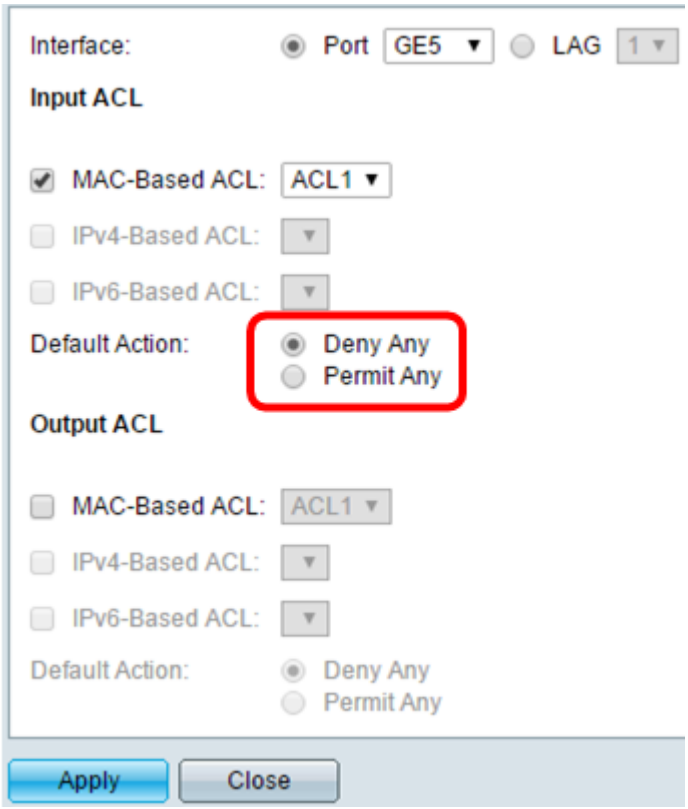
Note:如果要捆绑IPv4或IPv6-Based ACL，请点击相应地选择。

步骤4.从对应的下拉列表选择ACL。

Note:在本例中，预先配置的基于MAC的ACL ACL1被选择。



步骤5.点击默认动作单选按钮。

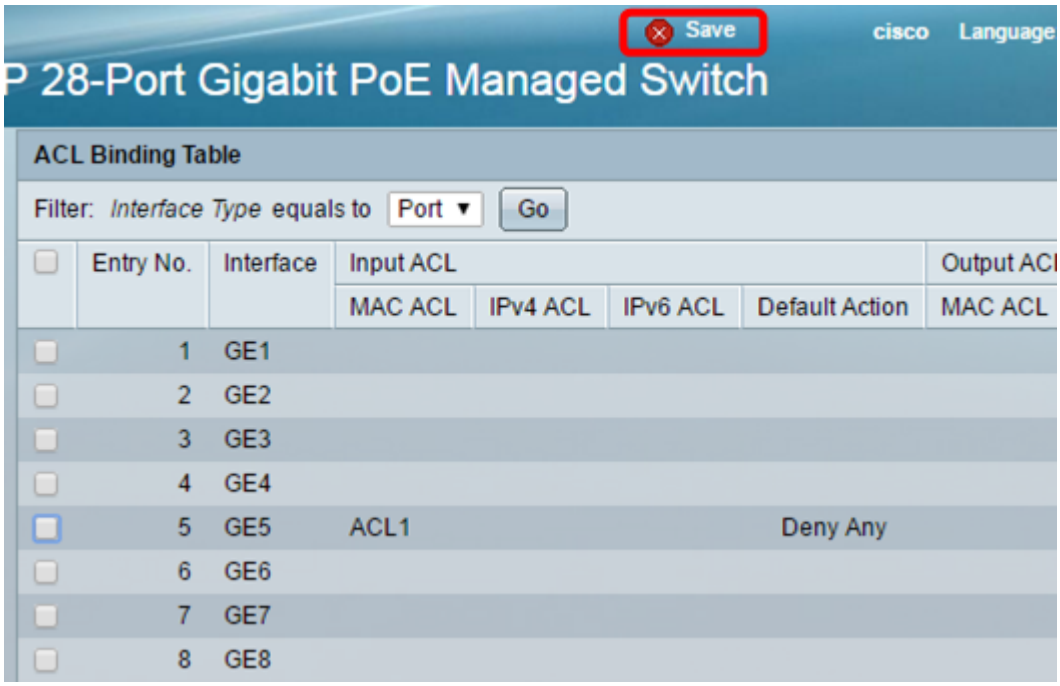


选项是：

- 拒绝其中任一—交换机丢弃不满足ACL的必需的标准的信息包。
- 允许其中任一—交换机转发满足ACL的必需的标准的信息包。

步骤6.点击**适用**保存对运行配置文件的更改然后点击**Close**。

第7.步。ACL绑定表应该显示在选择的接口的被配置的ACL。点击**"Save"**更新启动配置文件。

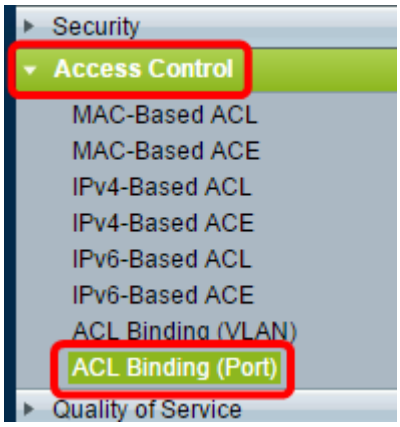


配置在接口的出口ACL

重要信息：在继续进行步骤前，请保证您已经创建了基于MAC的ACL和访问控制项(ACE)在您的交换机。对于详细指令，请点击此处。

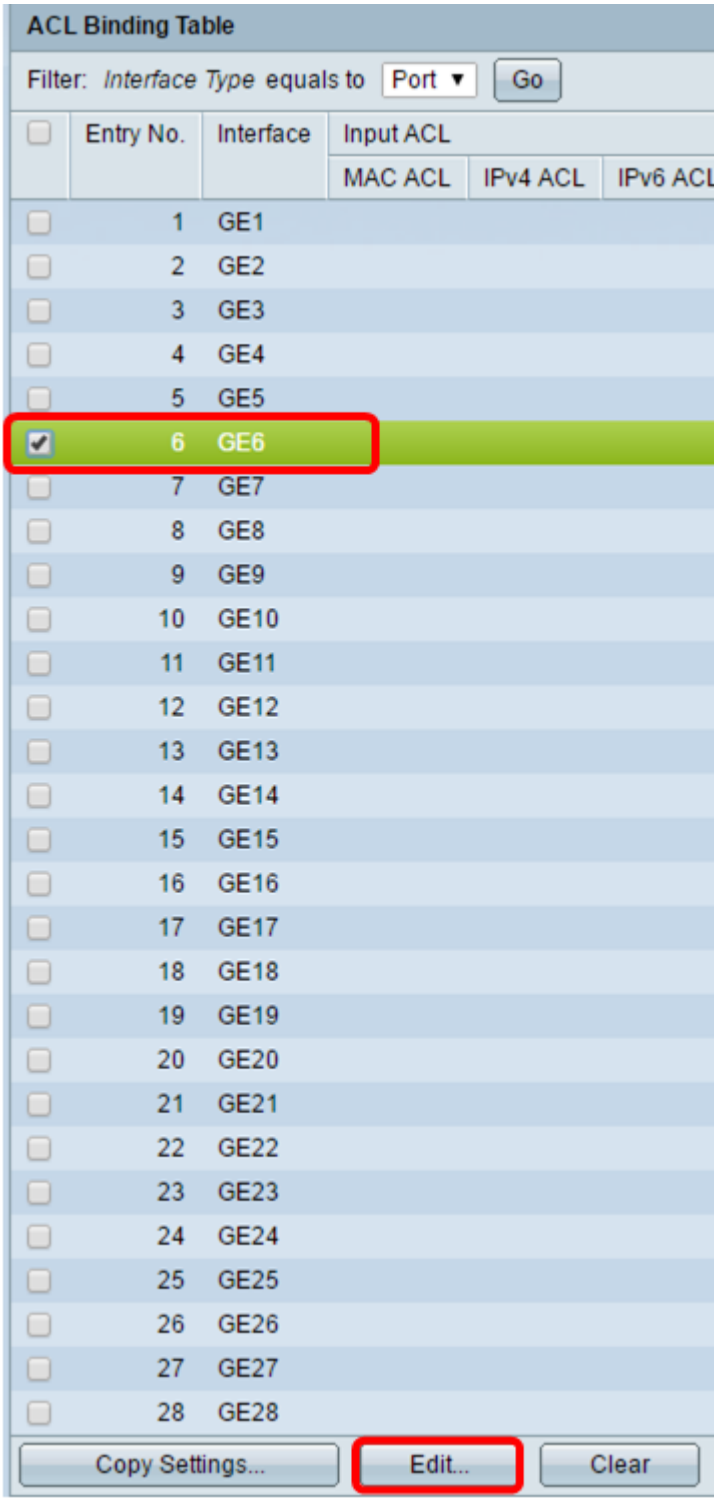
Step 1.在基于Web的工具中，请选择**访问控制> ACL捆绑(端口)**。

Note:在此方案中，使用SG350-28MP交换机。



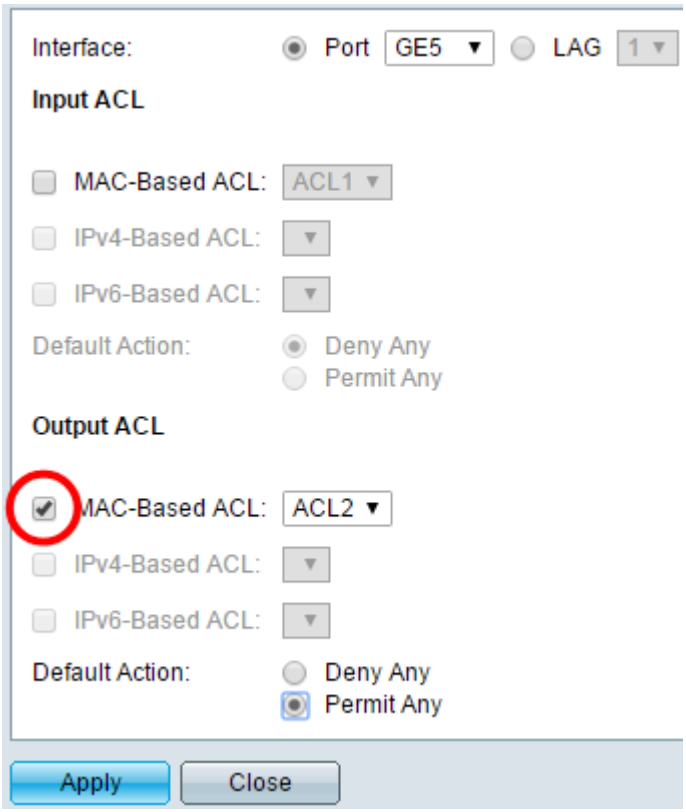
Step 2.在接口旁边检查复选框您要适用ACL对，然后点击**编辑**。

Note:在本例中， GE6被选择。



第3.步。要配置在接口的入口ACL，请检查期望输出ACL复选框。

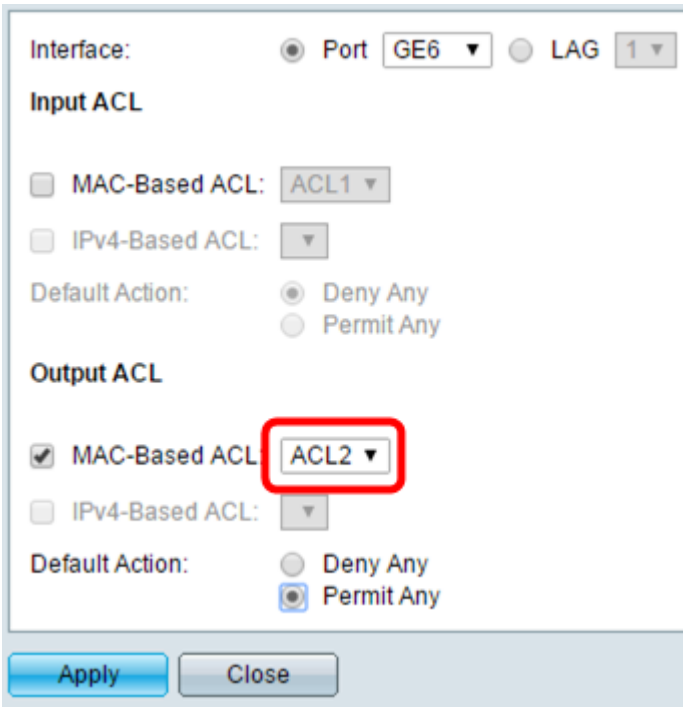
Note:在本例中，基于MAC的ACL被选择。



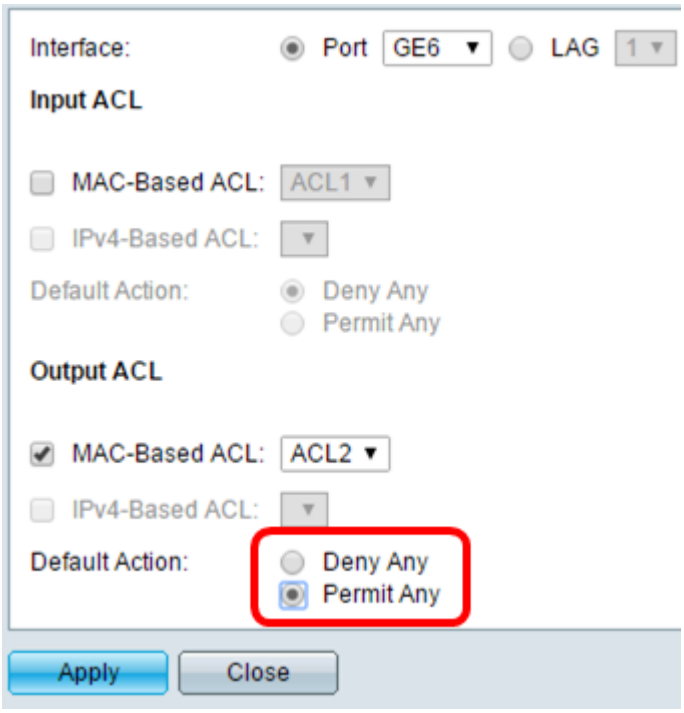
Note:如果要捆绑IPv4或IPv6-Based ACL，请点击相应地选择。

步骤4.从基于MAC的ACL下拉列表选择ACL。

Note:在本例中，预先配置的基于MAC的ACL ACL2被选择。



步骤5.点击默认动作单选按钮。

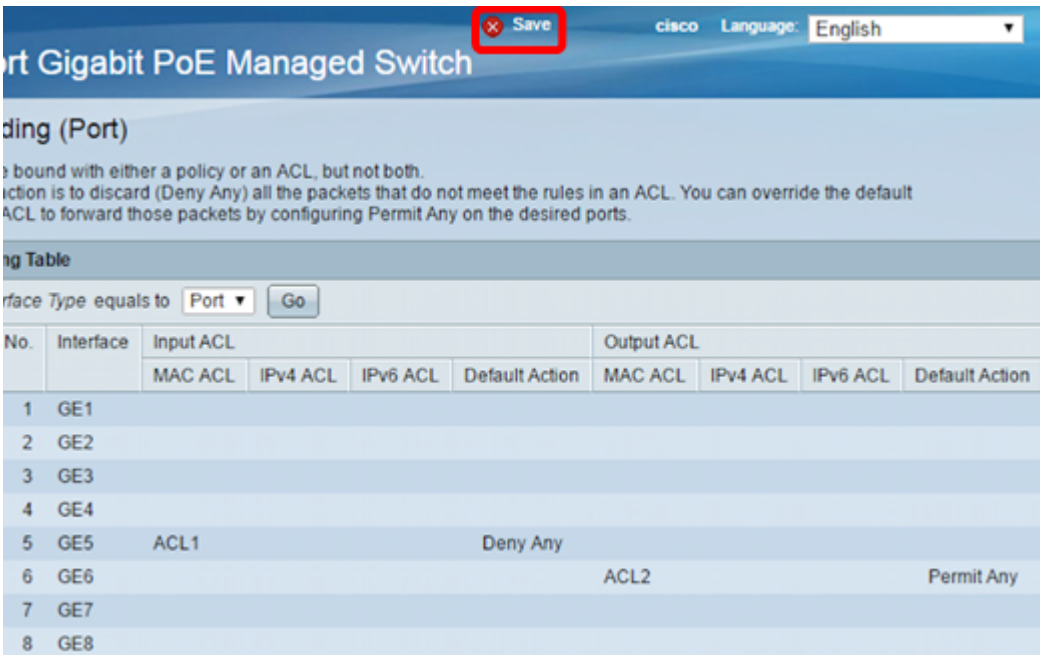


选项是：

- 拒绝其中任一—交换机丢弃不满足ACL的必需的标准的信息包。
- 允许其中任一—交换机转发满足ACL的必需的标准的信息包。

步骤6.点击**适用**保存对运行配置文件的更改然后点击**Close**。

第7.步。ACL绑定表应该显示在选择的接口的被配置的ACL。点击**"Save"**更新启动配置文件。



Note:如果希望同时配置出口和入口ACL，您可以通过配置输入ACL和输出ACL如此执行区域。

您应该当前配置了在您的交换机接口的出口和入口ACL。