访问配置文件在200/300系列被管理的交换机的规则配置

目标

访问配置文件作为安全另一个层交换机的。 访问配置文件能包含128个规则强化安全。每个规则包含一个动作和标准。如果接入方式不匹配管理方法，用户被阻拦并且不能访问交换机。

此条款说明如何配置在200/300系列被管理的交换机的配置文件规则。

可适用的设备

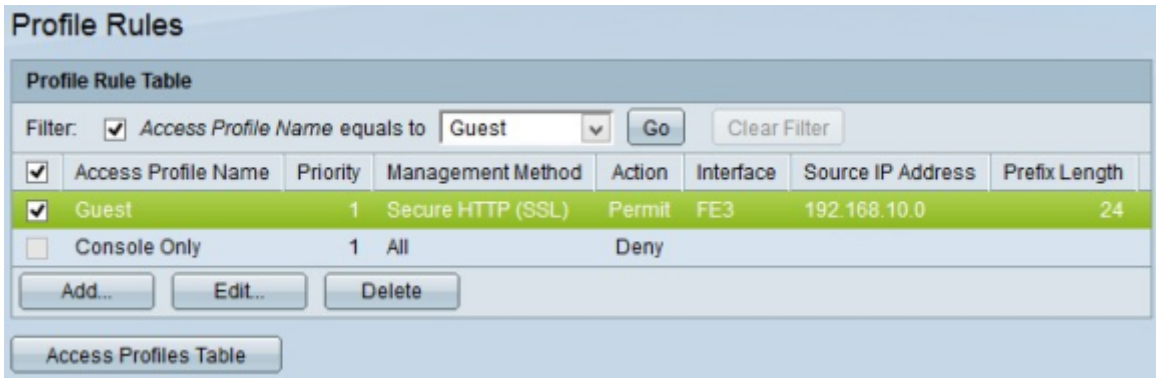
•SF/SG 200和SF/SG 300系列被管理的交换机

软件版本

•v1.2.7.76

访问配置文件配置

步骤1.登陆到Web配置工具并且选择**安全> Mgmt接入方式>配置文件规则**。*配置文件规则*页打开：



Step 2.检查**过滤器**复选框显示在*访问配置文件*页被创建了的访问配置文件名字。

步骤3.从访问配置文件名字等于选择期望访问配置文件到下拉列表。

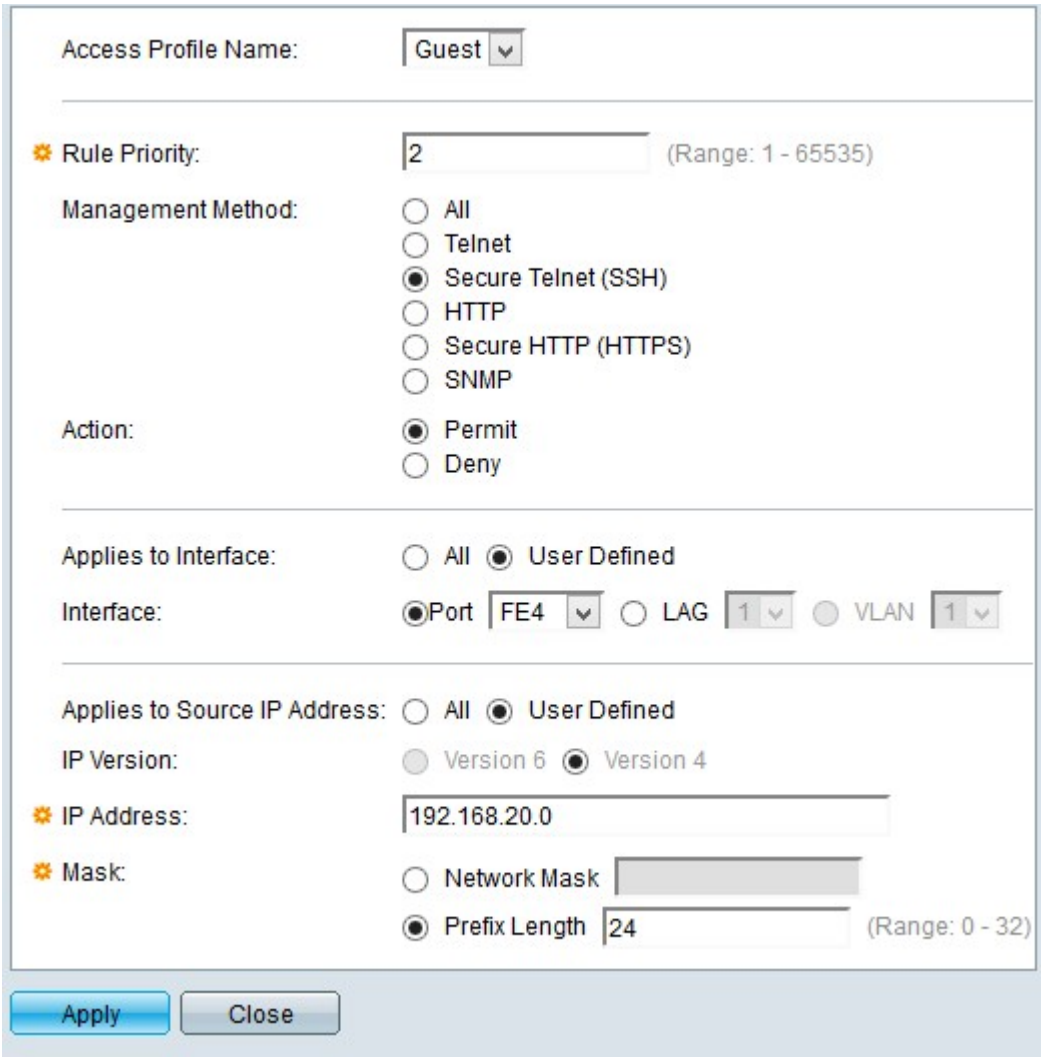
步骤4.点击**去**显示期望访问配置文件。

第5.步(可选)开始新的搜索，点击**清楚的过滤器**。

增加配置文件规则

第 1 步：检查对应于访问配置文件您希望增加规则的复选框。

步骤2.点击**添加**。*添加配置文件规则*窗口出现。



第3.步(可选)增加配置文件规则到不同的数据图表名字，从访问配置文件名字下拉列表选择不同的数据图表名字。

步骤4.输入规则的优先级在规则优先级字段。规则优先级匹配信息包以规则。与更加低优先级的规则首先被检查。如果信息包匹配一个规则所需的动作进行。

步骤5.点击对应于在管理方法字段的期望管理方法的单选按钮。用户使用的接入方式必须匹配将执行的动作的管理方法。

•全所有管理方法分配到访问配置文件。

•Telnet — Telnet管理方法分配到规则。有Telnet会议访问配置文件方法的只有用户访问设备。

•安全的Telnet (SSH) — SSH管理方法分配到配置文件。有安全的Telnet会议访问配置文件的只有用户访问设备。

•HTTP — HTTP管理方法分配到配置文件。仅用户有HTTP会议访问配置文件方法的访问设备。

•安全HTTP (SSL) — HTTPS管理方法分配到配置文件。仅用户有HTTPS会议访问配置文件方法的访问设备。

•SNMP — SNMP管理方法分配到配置文件。仅用户有满足访问配置文件方法的SNMP的访问设备。

步骤6.选择将附有的动作从动作单选按钮的规则。可能行动值是：

•许可证—对交换机的访问允许。

•拒绝—对交换机的访问被拒绝。

步骤7.点击对应于所需的接口键入适用建立接口字段定义访问配置文件的接口的期望单选按钮。

•全包括所有接口例如端口， VLAN和滞后。

Note:滞后是组合多条物理链路为了提供更多带宽的逻辑链接。

•用户定义—仅适用于用户的所需的接口。

–端口—从访问配置文件将被定义的端口下拉列表选择端口。

–滞后—从访问配置文件将从滞后下拉列表被定义的滞后下拉列表选择滞后。

– VLAN —从访问配置文件将从VLAN下拉列表被定义的VLAN下拉列表选择VLAN。

步骤8.点击**来源IP Address单选按钮**对enable (event)接口IP原地址。有两可能的值：

•全包括所有IP地址。

•用户定义—仅适用于用户的所需的IP地址。

–版本6 — IP版本6 (IPv6)地址。

–版本4 — IP版本4地址。

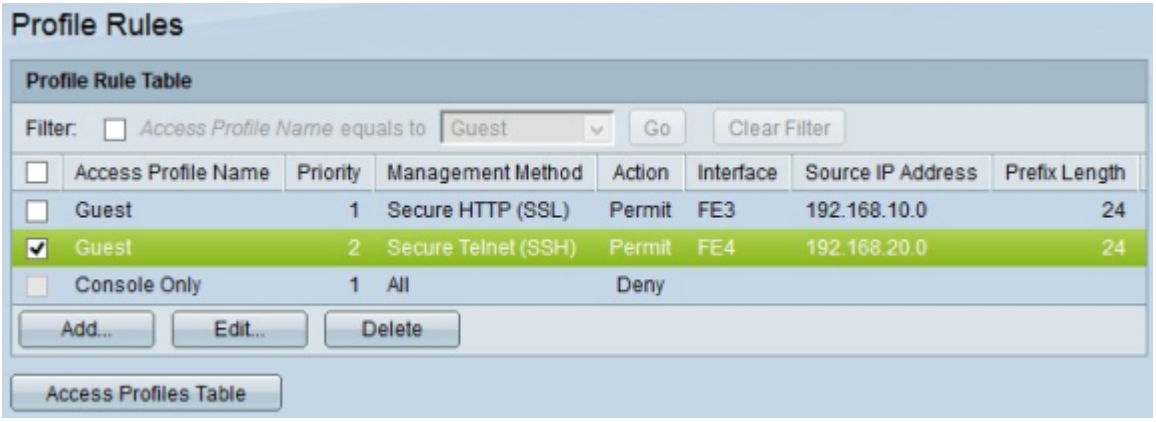
第9.步。如果选择了用户定义在第7步，请在IP Address字段输入设备的IP地址。

步骤10.点击在掩码字段的一个单选按钮的其中一个选项定义网络掩码。可用的选项是：

•网络掩码—输入对应于IP地址以点分十进制格式的子网掩码。

•前缀长度—输入对应于IP地址的子网掩码前缀长度。

步骤11.点击**适用**。



步骤12。(可选)编辑一个当前访问配置文件，检查您希望编辑访问配置文件名字的复选框，和点击**编辑**。

第13步。(可选)删除访问配置文件，检查您希望删除访问配置文件的复选框，和点击**删除**。