配置在200/300系列被管理的交换机的IPv4-Based访问列表

客观

访问列表是规定您能适用允许或拒绝在您的网络的特定的流量，添加更多安全并且增加在您的网络的整体性能。

本文目标将显示您如何配置在200/300系列被管理的交换机的IPv4-based访问列表。

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

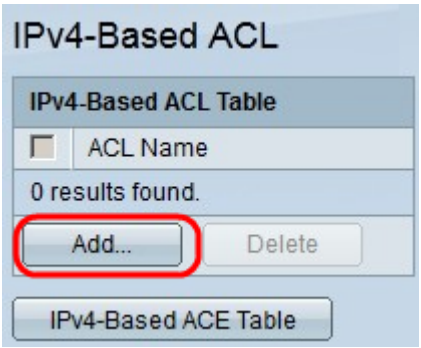
•1.3.0.62

IPv4-Based ACL和ACE的配置

IPv4-Based ACL

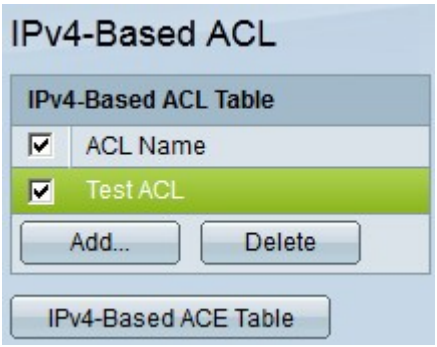
步骤1.登陆到Web配置工具并且选择**访问控制> IPv4-Based ACL**。*IPv4-Based ACL*页打开。

步骤2.点击**添加**添加一新的访问列表。



第 3 步：在*ACL名称*字段，请输入一个名字对于新的访问列表。

步骤4.点击**适用**保存访问列表。



第5.步(可选)删除访问列表，检查您希望删除访问列表的复选框，和点击**删除**。

IPv4-Based ACE

要管理ACE到ACL，以下步骤需要跟随。

步骤1.登陆到Web配置工具并且选择**访问控制> IPv4-Based ACE**。*IPv4-Based ACE*页打开。

Step 2.在*过滤器中：对*下拉列表的*ACL名称等于*，选择您希望分配访问规则的访问列表。

步骤3.点击**添加**。*添加基于IP的ACE*窗口出现。

步骤4.输入ACE的优先级在优先级字段。与最高优先级的ACE首先被处理。最高优先级是1。它有范围的1到2147483647。

第 5 步：在战场，请点击您希望此访问规则进行动作的单选按钮。可用的选项是：

- 许可证—转发当前ACE过滤的信息包。
- 拒绝—丢弃由当前ACE过滤的信息包。
- 关闭—丢弃由当前ACE过滤的信息包并且使端口无效从信息包收到。

第6.步。在*Protocol字段*，请点击您在ACE希望添加协议的单选按钮。当信息包穿过路由器，ACE为所有路由的网络协议被配置为了过滤信息包。可用的选项是：

- 其中任一—选择其中任一个IPv4-Based ACE协议。

•从列表挑选—从下拉列表选择期望协议。

•匹配的协议ID —此选项让您输入您要使用的协议ID。

第 7 步：在*IP Address字段的来源*，请点击其中一个可用的选项作为IP原地址：

•其中任一—此选项运用访问规则于任何IP地址可用在一个特定网段。

•用户定义—此选项让您输入一个特定IP地址。

- IP Address值的来源—在此字段，请输入IP原地址。

-来源IP通配符屏蔽—在此字段，请输入IP原地址的通配符屏蔽。通配符掩码让您指定到IP原地址的哪台主机此访问列表适用。

第8.步。在*IP Address字段的目的地*，请点击其中一个可用的选项作为目的地IP地址：

•其中任一—此选项运用访问规则于任何IP地址可用在一个特定网段。

•用户定义—此选项让您输入一个特定IP地址运用访问规则：

– IP Address值的目的地—在此字段，请输入目的地IP地址。

–目的地IP通配符屏蔽—在此字段，请输入目的地IP地址的通配符屏蔽。通配符掩码让您指定目的地IP地址的哪些主机此访问列表适用于。

第9.步。只有当您从第5.步选择TCP或UDP点击单选按钮其中一个可用的选项选择源端口时，*源端口*字段被启用：

•其中任一—此选项接受所有源端口。

•单一此选项让您输入单个源端口值。

•范围—此选项让您输入可用的源端口的范围。

第10.步。只有当您从第5.步选择TCP或UDP点击单选按钮其中一个可用的选项选择目的地端口时，*Port字段的目的地*被启用：

•其中任一—此选项接受所有目的地端口。

•单一此选项让您输入Port值的单个目的地。

•范围—此选项让您输入可用的目的地端口的范围。

第11.步。*TCP*标志字段只是启用的，如果从第5.步选择TCP点击其中一个每个标志位的单选按钮为了选择什么状态您希望触发访问规则：

•Urg —此标志位识别流入的数据如紧急。

•Ack —此标志位用于顺利地承认信息包收据。

•Psh —此标志位用于保证制定数据正确的优先级和被处理在发送或接收端。

•Rst —此标志位，当连接接受一个错误的分段时，使用。

•同步符—此标志位使用TCP通信。

•飞翅—此标志位，当通信或数据传输完成时，使用。

步骤12。在*服务字段类型*，请点击其中一个可用的单选按钮选择IP信息包的一种服务类型：

•其中任一—此选项选择任一种服务。

•匹配的DSCP —选择此选项实现差分服务代码点(DSCP)作为服务类型。DSCP是分类和管理网络流量的机制。输入您希望运用于访问规则的DSCP值。

•匹配的IP优先级—当前网络用于此种服务提供正确的服务质量(QoS)。输入您希望运用于访问规则的值。

第13步。*ICMP (互联网控制消息协议)*字段被启用，只有当您选择在第5.步ICMP的ICMP用于发错误信息，当服务不是可用的时时或测试连接。点击其中一个可用的单选按钮过滤ICMP信息类型：

•其中任一—它能是其中任一个错误信息或查询消息。

•从列表挑选—从下拉列表选择其中任一允许的控制消息。

•匹配的ICMP类型—此选项让您输入ICMP的编号键入您要过滤。

步骤14。只有当您从第5.步ICMP代码选择ICMP用于提供关于控制消息时的特定信息*ICMP代码*字段被启用。点击其中一个可用的选项：

•其中任一—它可以是匹配控制信息的所有值。

•用户定义—输入您希望过滤的ICMP代码。

第15步。*IGMP (互联网组管理协议)*字段被启用，只有当您从第5.步IGMP选择IGMP管理在IP组播组的主机会员在网段时。点击其中一个可用的单选按钮过滤IGMP信息类型：

•其中任一—此选项接受所有IGMP信息类型。

•从列表挑选—从下拉列表选择其中一个可用的选项过滤：

– DVMRP —它使用一个反向路径泛滥技术，通过除了那个的每个接口发送收到的信息包的复制信息包到达。

–主机查询—它周期地传送在每个连接的网络的一般主机查询信息对于信息

–主机回复—它回复查询。

– PIM —它用于在本地和远程组播路由器之间处理从组播服务器的组播数据流对许多组播客户端。

–跟踪—它提供信息参加和离开IGMP组播组。

•匹配的IGMP类型—此选项让您输入IGMP的数量键入您要过滤。

第16步。点击**适用**保存您的配置。

第17步。(可选)编辑一个当前访问规则，检查您希望编辑访问规则的复选框，和点击**编辑**。

第18步。(可选)删除一个当前访问规则，检查您希望删除访问规则的复选框，和点击**删除**。