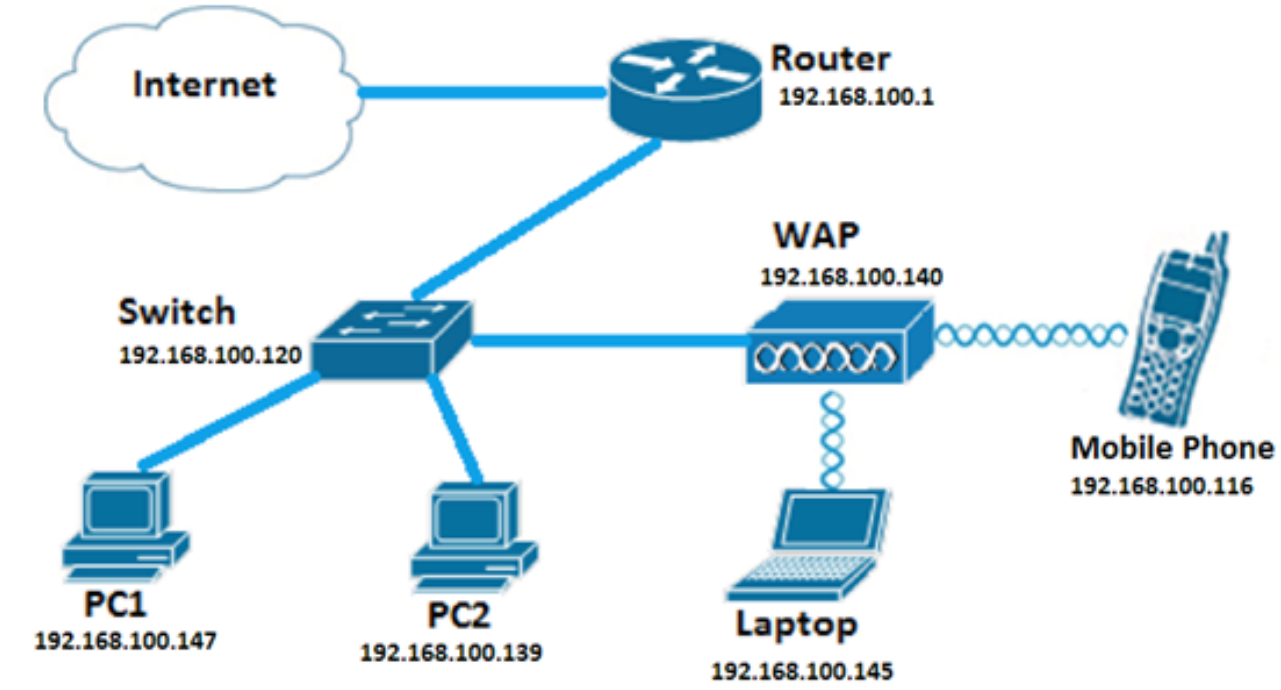
配置在WAP125和WAP581的IPv4ACL

Introduction

互联网协议版本4 (IPv4)和互联网协议版本6 (IPv6)访问控制列表(ACL)是一组规则被运用于无线访问访问接入点收到的信息包(WAP)。每个规则用于确定是否应该允许或拒绝对网络的访问。可以配置ACL检查一个帧的字段类似来源或目的地IP地址、虚拟局域网标识(ID)，或者业务类别(CoS)。当帧输入WAP设备端口时，检查帧并且根据帧的内容检查ACL规则。如果其中任一个规则匹配内容，许可证或在帧拒绝动作被采取。

配置IPv4 ACL典型地用于授权对网络资源的访问选择在网络的设备。

Note:有含蓄的拒绝在被创建的每个规则结束时。



Note:在此方案中，从PC2的所有数据流将允许访问网络。从其他主机的其他数据流将被否决。

客观

此条款打算显示您如何配置在WAP125和WAP581接入点的一IPv4ACL。

可适用的设备

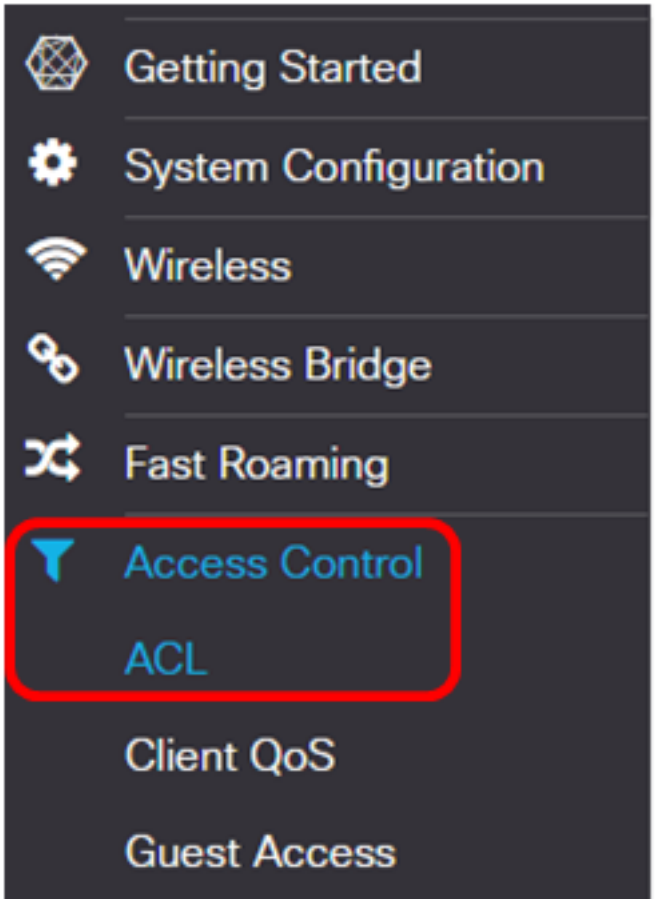
- WAP125
- WAP581

软件版本

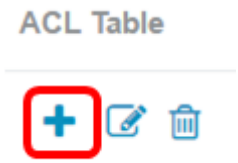
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

配置IPv4ACL

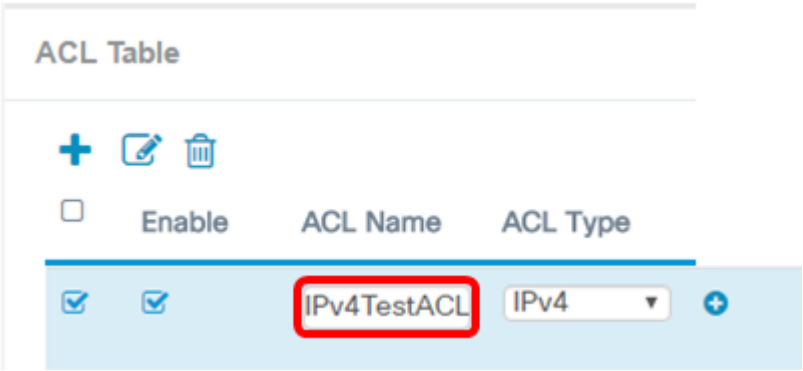
步骤1.登陆到WAP的基于Web的工具并且选择**访问控制> ACL**。



步骤2.点击 ✚ 按钮创建新的ACL。

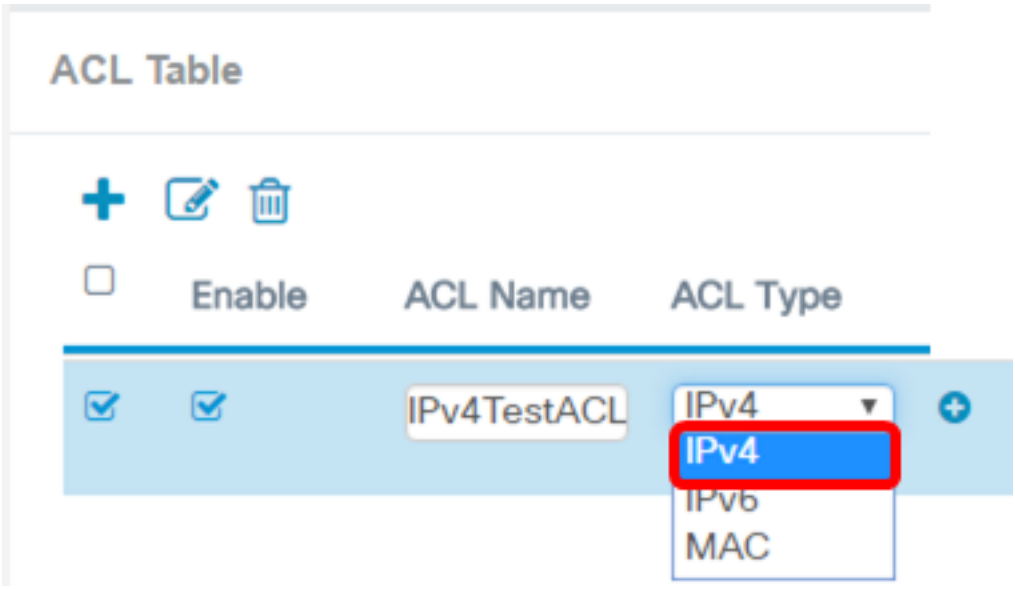


步骤3.输入一个名字对于ACL在*ACL名称*字段。



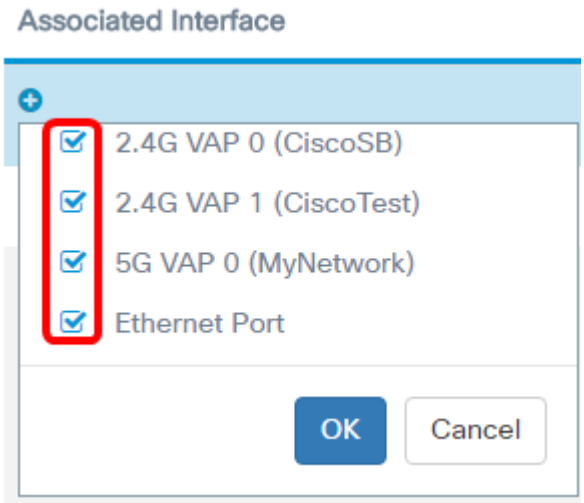
Note:在本例中， IPv4TestACL被输入。

步骤4.从ACL类型下拉列表选择IPv4。



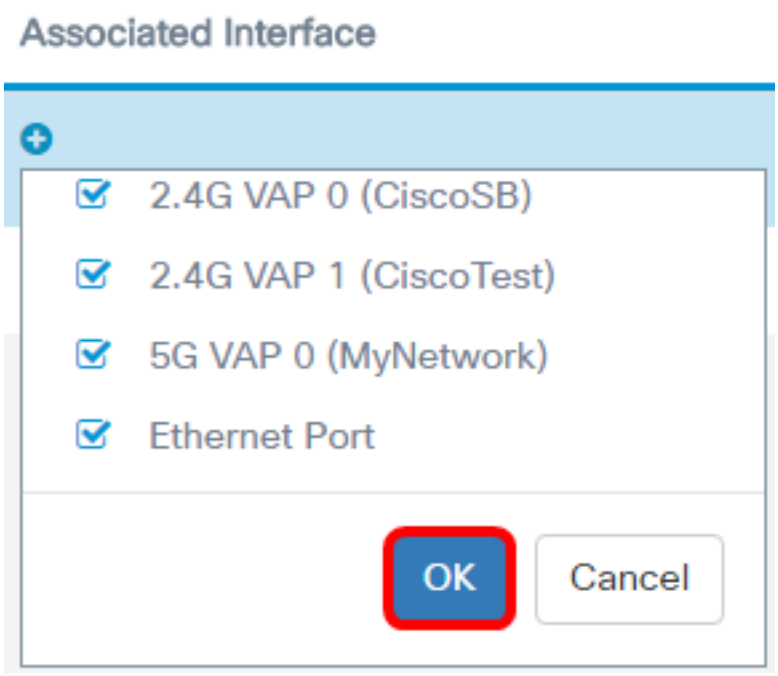
步骤5.点击 按钮并且从关联接口下拉列表选择接口。选项是：

- 2.4G VAP 0 (SSID名称) —此选项将适用MAC ACL于2.4千兆赫虚拟访问访问接入点(VAP)。SSID名称部分可能根据在WAP配置的SSID名称更改。
- 5G VAP0 (SSID名称) —此选项将适用MAC ACL于5个千兆赫VAP。
- 以太网端口—此选项将适用MAC ACL于WAP的以太网接口。



Note:多个接口可以被关联到ACL。然而，当已经被关联了对另一个ACL时，它不可能被关联到ACL。在本例中，所有接口被关联对IPv4TestACL。非选定机箱分离从ACL的接口。

步骤6.点击OK键。

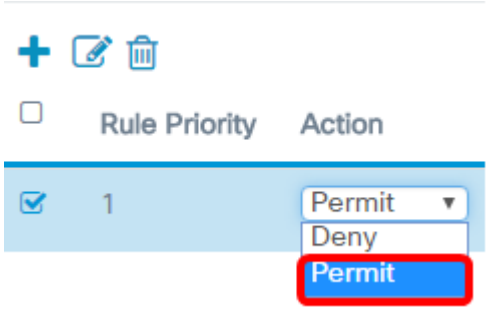


步骤7.点击**多...**按钮配置ACL的参数。

步骤8.点击 ✚ 按钮添加新规则。

步骤9.从动作下拉列表选择动作。选项是：

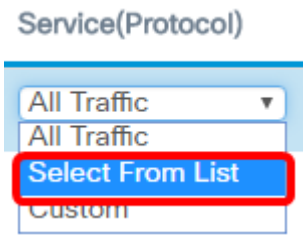
- 许可证—此选项将允许匹配ACL标准连接到网络。的信息包。
- 拒绝—此选项将防止匹配从连接的ACL标准到网络的信息包。



Note:在本例中，许可证被选择。

步骤10.选择从服务(协议)下拉列表或协议将过滤的服务。选项是：

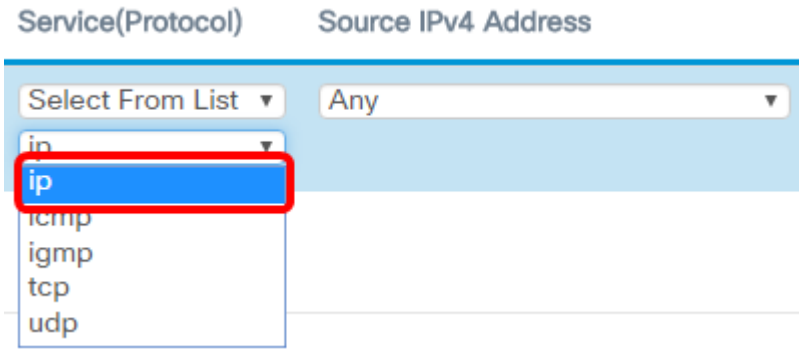
- 所有数据流—此选项将对待所有信息包作为匹配到ACL过滤器。
- 从列表挑选—此选项将允许您选择IP、ICMP、IGMP、TCP或者UDP作为ACL的过滤器。如果此选项被选择，请进行对第11.步。
- 自定义—此选项将允许您输入一个自定义协议标识符作为信息包的一台过滤器。值是一个四字节十六进制数字。范围是0到255。



Note:在本例中，请从列表挑选被选择。

步骤11.定义需要允许连接到网络的协议。选项是：

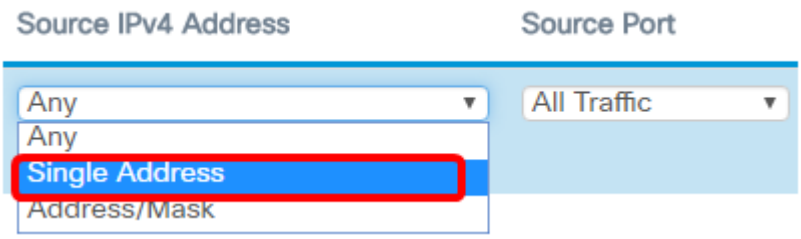
- ip —此选项将让接入点过滤访问网络的主机使用他们的IP地址作为过滤器。
- icmp —此选项将让接入点过滤进入网络的互联网控制消息协议(ICMP)信息包接入点。
- igmp —此选项将让接入点过滤进入网络的互联网组管理协议(IGMP)信息包接入点。
- tcp —此选项将让接入点过滤进入网络的传输控制协议(TCP)信息包接入点。
- udp —此选项将让接入点过滤进入网络的用户数据报协议(UDP)信息包接入点。



Note:在本例中， ip被选择。

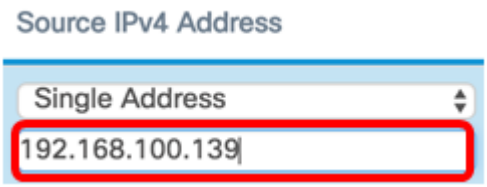
步骤12。定义从来源IPv4地址下拉列表的来源IPv4地址。选项是：

- 其中任一—此选项将让WAP应用过滤器于信息包从所有IP地址。
- 单个地址—此选项将让WAP应用过滤器于信息包从指定的IP地址。
- 地址/掩码—此选项将让WAP应用过滤器于信息包于IP地址和IP的掩码。



Note:在本例中，单个地址被选择。

第13步。输入需要允许，当访问网络时主机的IP地址。

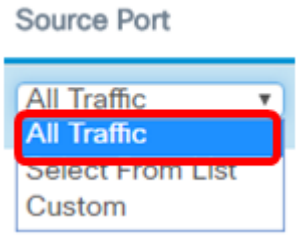


Note:在本例中， 192.168.100.139被输入。这是PC2的IP地址。

步骤14。选择情况的一个源端口。选项是：

- 所有数据流—此选项将允许自满足标准的源端口的所有信息包。
- 从列表挑选—此选项允许您选择ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。
- 自定义—此选项将允许您输入IANA端口号匹配在数据包报头识别的源端口。端口范围是从0到65535并且包括以下：

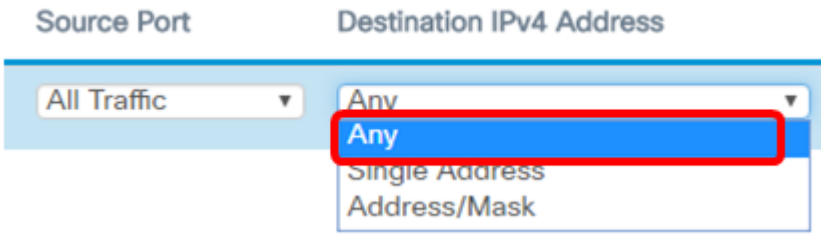
- 0到1023 —众所周知的端口
- 1024个— 49151 —注册的端口
- 49152 — 65535 —动态并且/或者专用的端口



Note:在本例中，所有数据流被选择。

第15步。从目的地IPv4地址下拉列表选择目的地地址。选项是：

- 其中任一—此选项对待所有IP地址作为匹配对ACL语句。
- 单个地址—此选项让您输入ACL情况的一个特定IP地址。
- 地址/掩码—此选项让您输入IP地址范围或掩码。



Note:在本例中，其中任一被选择。

第16步。从目的地端口下拉列表选择目的地端口。选项是：

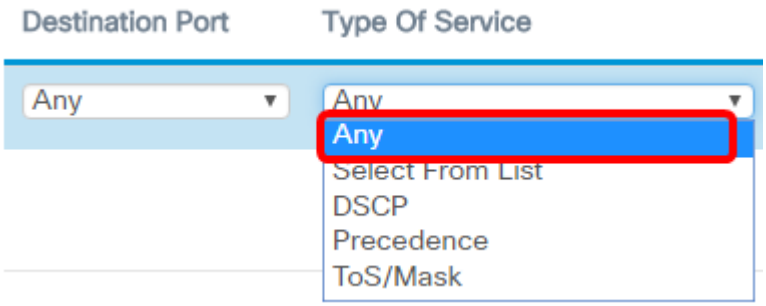
- 其中任一—此选项对待所有信息包的目的地端口作为匹配对在ACL的语句。
- 从列表挑选—此选项让您选择与目的地端口产生关联的关键字匹配。选项是：ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。这些关键字转换为他们的对应的端口编号。
- 自定义—此选项将允许您输入IANA端口号匹配在数据包报头识别的源端口。端口范围是从0到65535并且包括以下：

  - 0到1023 —众所周知的端口
  - 1024个— 49151 —注册的端口
  - 49152 — 65535 —动态并且/或者专用的端口

第17步。选择服务类型匹配从服务类型下拉列表的信息包类型。选项是：

- 其中任一—此选项对待所有服务作为信息包的匹配。
- 从列表挑选—此选项匹配根据他们的差分服务代码点，(DSCP)，业务类别(CoS)或者紧急转发(EF)值的信息包。

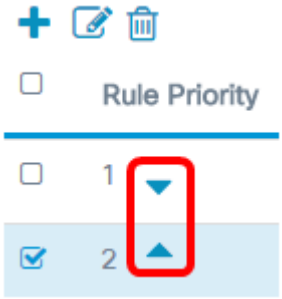
- DSCP —选项匹配根据他们的自定义DSCP值的信息包。当选择此选项时，从0请输入值到63在DSCP值字段。
- 优先次序—此选项匹配根据他们的IP优先级值的信息包。当此选项被选择时，从0请输入IP优先级值到7。
- Tos/掩码—此选项让您输入IP TOS掩码识别使用IP TOS字段的比较在信息包的比特位置按IP TOS比特值。



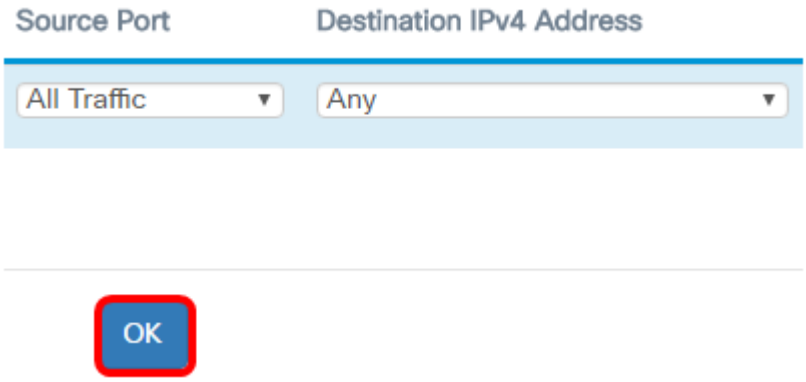
第18步。(可选)请重复第8步到第17步，直到ACL完成。

Note:因为有含蓄的请拒绝在被创建的每个规则结束时，那里是没有需要增加拒绝规则到ACL防止访问在网络的其它设备。

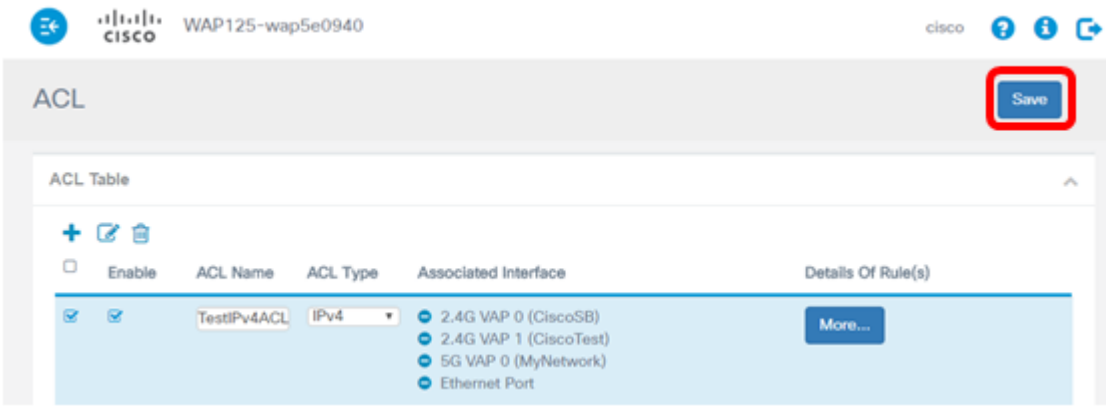
第19步。(可选)请通过上上下下点击按钮更改条件的命令在ACL的，直到他们按正确的顺序。



第20步。单击 **Ok**。



第21步。Click **Save**.



您应该当前完成设置只将允许一台主机访问网络，当连接到WAP的IPv4ACL。