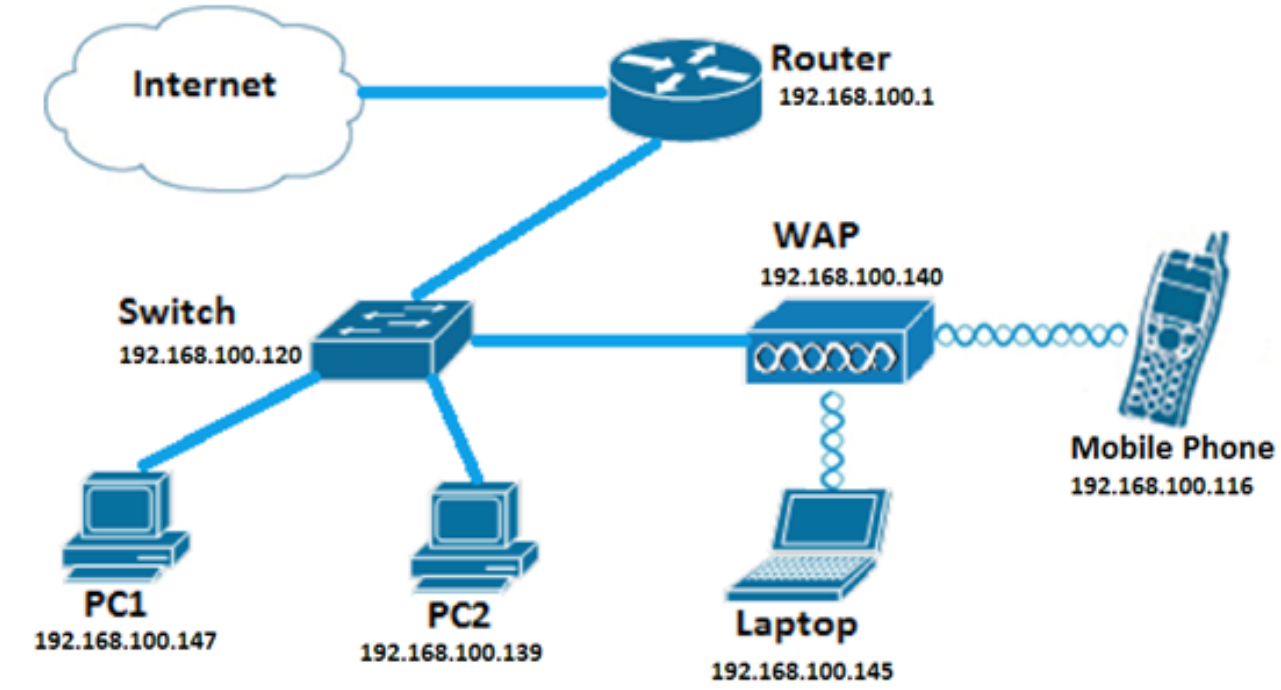
在WAP125和WAP581上配置IPv4 ACL

简介

Internet协议第4版(IPv4)和Internet协议第6版(IPv6)访问控制列表(ACL)是应用于无线接入点(WAP)接收的数据包的一组规则。 每条规则用于确定是允许还是拒绝访问网络。ACL可以配置为检查帧的字段，如源或目标IP地址、虚拟局域网(VLAN)标识符(ID)或服务类别(CoS)。 当帧进入WAP设备端口时，它会检查帧并根据帧的内容检查ACL规则。如果任何规则与内容匹配，则对帧执行允许或拒绝操作。

配置IPv4 ACL通常用于授权访问网络资源以选择网络中的设备。

注意：在创建的每条规则的末尾都有一个隐式拒绝。



注意：在此场景中，将允许来自PC2的所有流量访问网络。来自其他主机的所有其他流量将被拒绝。

目标

本文旨在向您展示如何在WAP125和WAP581接入点上配置IPv4 ACL。

适用设备

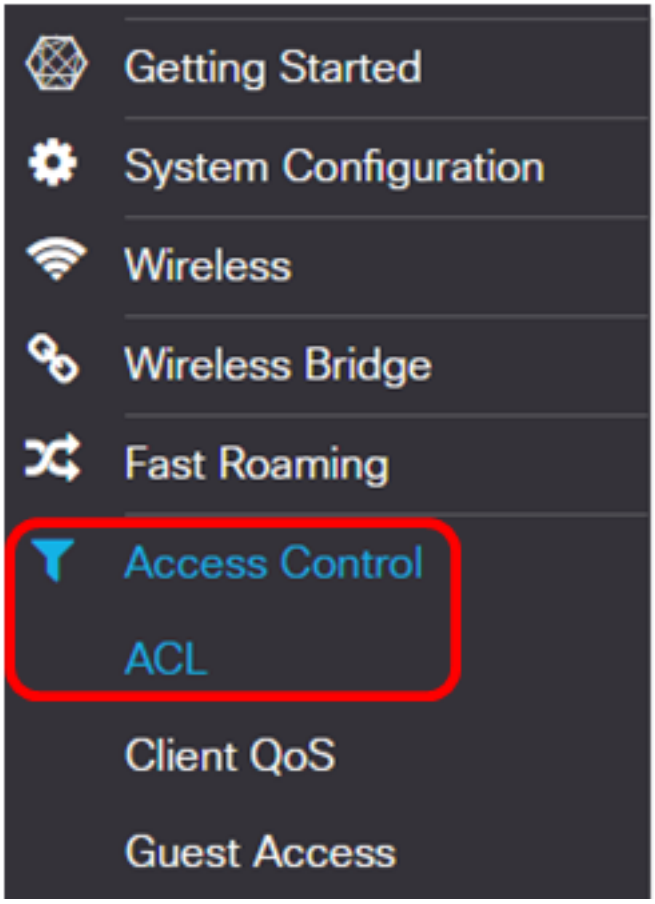
- WAP125
- WAP581

软件版本

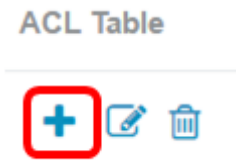
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

配置IPv4 ACL

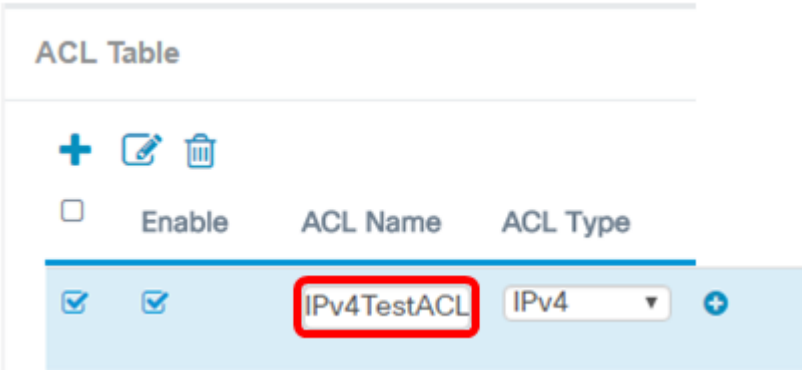
步骤1.登录WAP的基于Web的实用程序，然后选择**Access Control > ACL**。



步骤2.单击 ✚ 按钮创建新ACL。

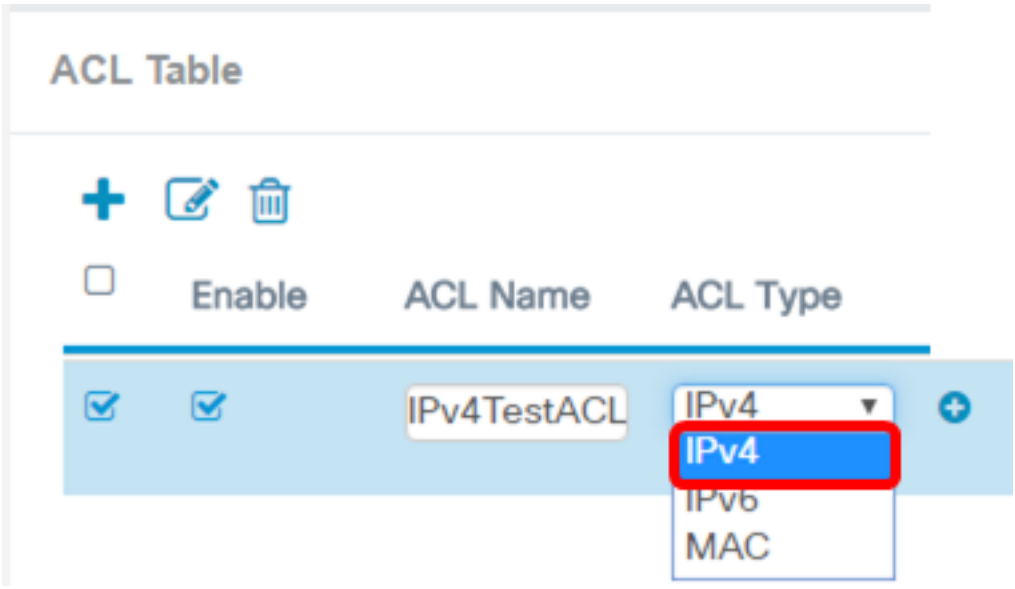


步骤3.在ACL Name字段中输入ACL*的名*称。



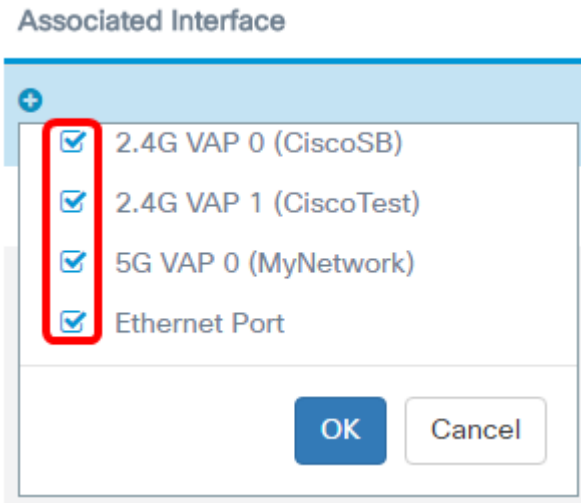
注意：在本例中，输入IPv4TestACL。

步骤4.从ACL Type下拉列表中选择IPv4。



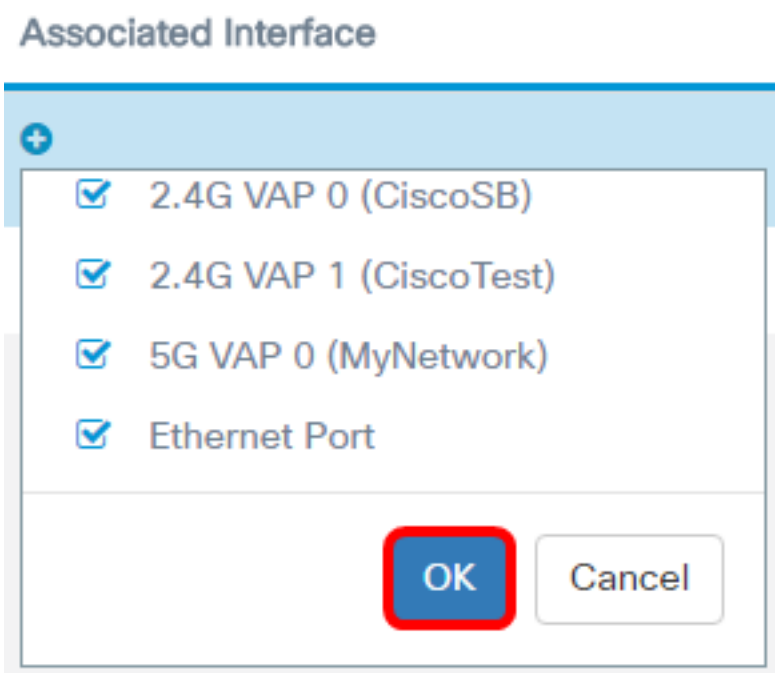
步骤5.单击按 钮，从Associated Interface下拉列表中选择接口。选项有：

- 2.4G VAP 0（SSID名称）— 此选项将MAC ACL应用于2.4 GHz虚拟接入点(VAP)。SSID Name部分可能会根据WAP上配置的SSID名称而更改。
- 5G VAP0（SSID名称）— 此选项将MAC ACL应用到5 GHz VAP。
- 以太网端口 — 此选项将MAC ACL应用到WAP的以太网接口。



注意：多个接口可以与ACL关联。但是，当它已关联到另一个ACL时，它不能与ACL关联。在本例中，所有接口都与IPv4TestACL关联。取消选中此框可取消接口与ACL的关联。

步骤6.单击**OK**。

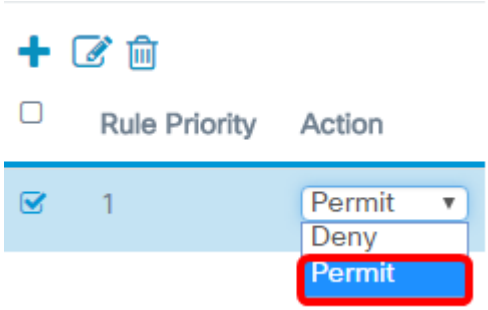


步骤7.单击**More...**按钮配置ACL的参数。

步骤8.单击 ✚ 按钮添加新规则。

步骤9.从Action下拉列表中选择操作。选项有：

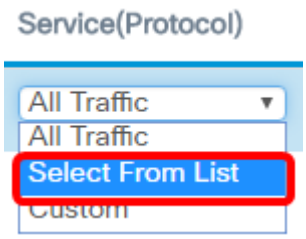
- 允许 — 此选项允许与ACL条件匹配的数据包连接到网络。
- 拒绝 — 此选项将阻止符合ACL条件的数据包连接到网络。



注意：在本例中，选择Permit。

步骤10.从Service(Protocol)下拉列表中选择要过滤的服务或协议。选项有：

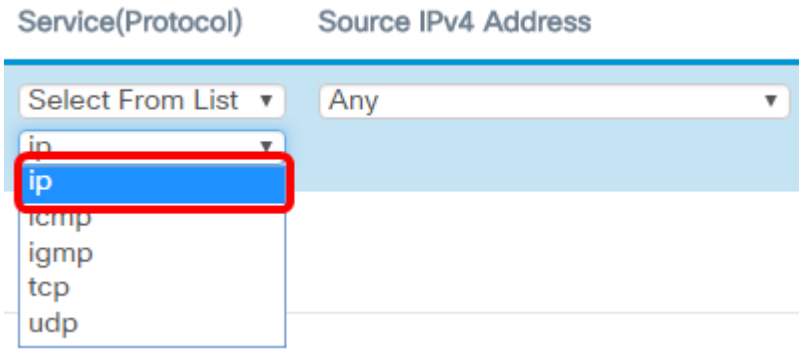
- 所有流量 — 此选项将所有数据包视为与ACL过滤器的匹配项。
- Select From List — 此选项允许您选择IP、ICMP、IGMP、TCP或UDP作为ACL的过滤器。如果选择此选项，请继续步骤11。
- 自定义 — 此选项允许您输入自定义协议标识符作为数据包的过滤器。该值是一个四位十六进制数。范围是0到255。



注意：在本例中，选择“从列表中选择”。

步骤11.定义需要允许连接到网络的协议。选项有：

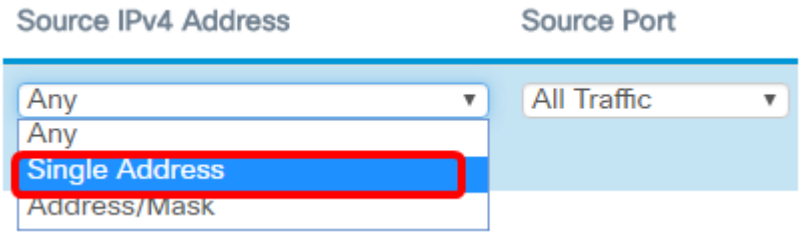
- ip — 此选项将允许接入点使用其IP地址作为过滤器过滤访问网络的主机。
- icmp — 此选项将让接入点过滤通过接入点进入网络的互联网控制消息协议(ICMP)数据包。
- igmp — 此选项将允许接入点过滤通过接入点进入网络的互联网组管理协议(IGMP)数据包。
- tcp — 此选项将允许接入点过滤通过接入点进入网络的传输控制协议(TCP)数据包。
- udp — 此选项将允许接入点过滤通过接入点进入网络的用户数据报协议(UDP)数据包。



注意：在本例中，选择ip。

步骤12.从Source IPv4 Address下拉列表定义Source IPv4 Address。选项有：

- Any — 此选项将允许WAP将过滤器应用于来自任何IP地址的数据包。
- Single Address — 此选项将允许WAP将过滤器应用于来自指定IP地址的数据包。
- 地址/掩码 — 此选项将允许WAP将过滤器应用于数据包的IP地址和IP掩码。



注意：在本例中，选择了Single Address。

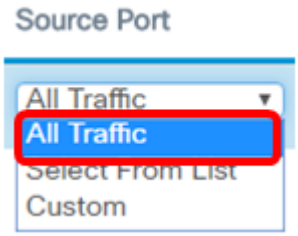
步骤13.输入访问网络时需要允许的主机的IP地址。

注意：在本例中，输入192.168.100.139。这是PC2的IP地址。

步骤14.为条件选择源端口。选项有：

- 所有流量 — 此选项将允许来自符合条件的源端口的所有数据包。
- Select From List — 此选项允许您选择ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。
- 自定义 — 此选项允许您输入IANA端口号，以匹配数据报报头中标识的源端口。端口范围为0到65535，包括以下内容：

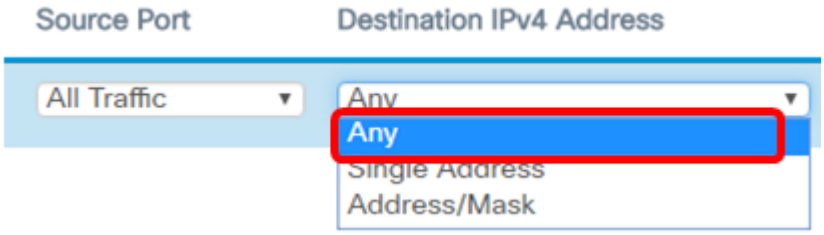
- 0到1023 — 公认端口
- 1024 — 49151 — 注册端口
- 49152 — 65535 — 动态和/或专用端口



注意：在本例中，选择All Traffic。

步骤15.从Destination IPv4 Address下拉列表中选择目标地址。选项有：

- Any — 此选项将任何IP地址视为与ACL语句匹配。
- Single Address — 此选项允许您为ACL条件输入特定IP地址。
- 地址/掩码 — 此选项允许您输入IP地址范围或掩码。



注意：在本例中，选择Any。

步骤16.从Destination Port下拉列表中选择目标端口。选项有：

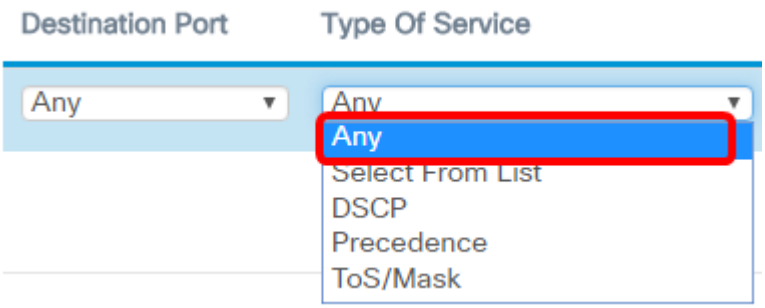
- Any — 此选项将数据包的所有目的端口视为与ACL中的语句匹配。
- 从列表中选择 — 此选项允许您选择与要匹配的目标端口关联的关键字。选项有：ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。这些关键字转换为相应的端口号。
- 自定义 — 此选项允许您输入IANA端口号，以匹配数据报报头中标识的源端口。端口范围为0到65535，包括以下内容：

  - 0到1023 — 公认端口
  - 1024 — 49151 — 注册端口
  - 49152 — 65535 — 动态和/或专用端口

步骤17.从Type of Service下拉列表中选择与数据包类型匹配的服务类型。选项有：

- Any — 此选项将任何服务视为数据包的匹配项。
- 从列表中选择 — 此选项根据其差分服务代码点、(DSCP)、服务类别(CoS)或加速转发(EF)值匹配数据包。

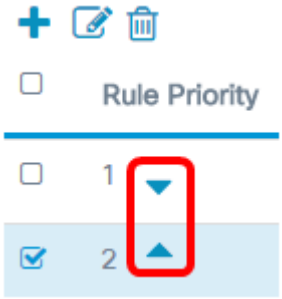
- DSCP — 选项根据数据包的自定义DSCP值匹配数据包。选择此选项时，在DSCP值字段中输入0到63之间的值。
- 优先级 — 此选项根据数据包的IP优先级值匹配数据包。选择此选项后，输入0到7之间的IP优先级值。
- ToS/Mask — 此选项允许您输入IP ToS掩码，以标识IP Tos Bits值中的位位置，该值用于与数据包中的IP ToS字段进行比较。



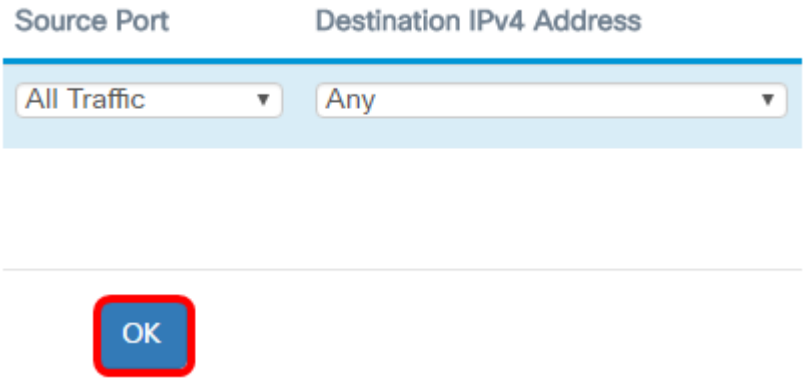
步骤18.（可选）重复步骤8到步骤17，直到ACL完成。

注意：由于在创建的每条规则末尾都存在隐式拒绝，因此无需向ACL添加拒绝规则来阻止从网络中的其他设备访问。

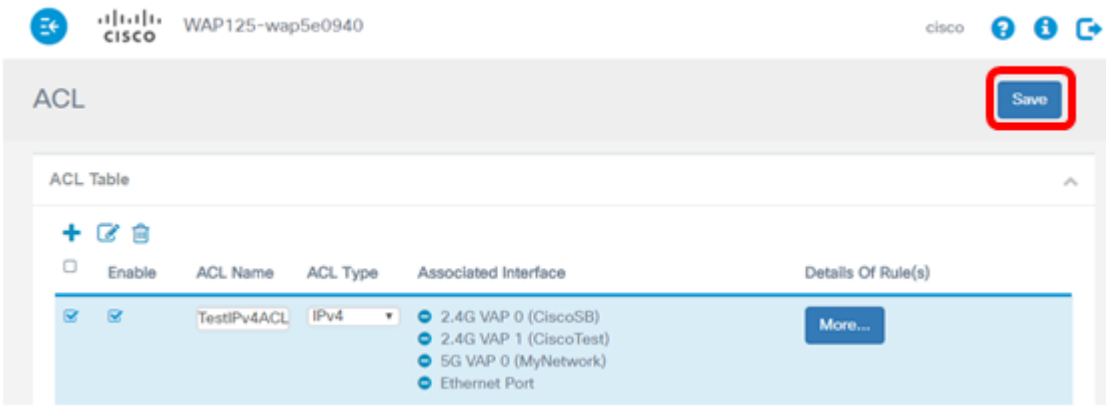
步骤19.（可选）通过单击上下按钮更改ACL上条件的顺序，直到它们按正确顺序排列。



步骤20.单击**OK**。



步骤21.单击“**保存**”。



现在，您应该已经完成IPv4 ACL的设置，该ACL在连接到WAP时仅允许一台主机访问网络。