

一个规则的创建和配置IPv4的根据访问控制表(ACL) WAP121和WAP321接入点

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。ACL包含允许或对网络设备的拒绝访问的主机。QoS功能包含允许数据流被分类到流和特定某一QoS处理符合被定义的每跳跃工作情况的差异化服务(DiffServ)技术支持。

此条款说明如何创建和配置IPv4在WAP121和WAP321接入点(WAP)的基于ACL。

可适用的设备

- WAP121
- WAP321

软件版本

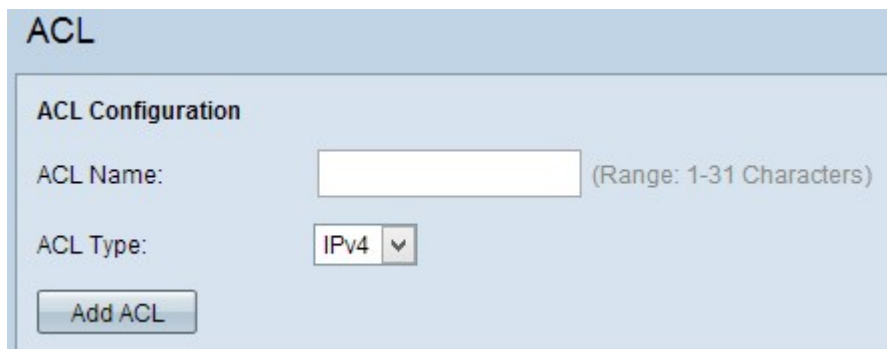
- v1.0.3.4

IPv4根据ACL配置

IP ACL分类第3层的数据流在IP栈。每个ACL是一套10个规则被运用于从无线客户端发送的数据流或将由无线客户端接受。每个规则指定是否应该用于容量对一个特定字段允许或拒绝对网络的访问。规则根据多种标准，并且可能适用于在一个信息包内的一个或更多字段，例如来源或目的地IP地址、源或目的地端口或者协议传送了信息包。

IPv4ACL的创建

步骤1.登陆到访问接入节点配置工具并且选择**客户端QoS > ACL**。ACL页打开：



ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4 ▼

Add ACL

步骤2.输入ACL的名字在ACL名称字段。

ACL

ACL Configuration

ACL Name: ExampleAllowSMTP

ACL Type: IPv4

Add ACL

步骤3.从ACL类型下拉列表选择ACL的IPv4类型。

ACL

ACL Configuration

ACL Name: ExampleAllowSTMP (Range: 1-31 Characters)

ACL Type: IPv4

Add ACL

步骤4.点击添加ACL创建一个新的IPv4ACL。

ACL

ACL Configuration

ACL Name: ExampleAllowSTMP (Range: 1-31 Characters)

ACL Type: IPv4

Add ACL

规则的配置IPv4ACL的

步骤1.从ACL NAME ACL类型规则必须被配置的下拉列表选择ACL。

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

Step 2.如果新规则必须为选择的ACL被配置，从规则下拉列表请选择新规则;否则，请选择其中一个从规则下拉列表的当前规则。

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4 ▾

Rule: **New Rule ▾**

Action: Deny ▾

Match Every Packet:

Note:最多10个规则可以为单个ACL被创建。

步骤3.从动作下拉列表选择ACL规则的动作。

ACL

ACL Configuration

ACL Name: ExampleAllowSMTP (Range: 1-31 Characters)

ACL Type: IPv4 ▾

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4 ▾

Rule: New Rule ▾

Action: **Deny ▾**

Match Every Packet:

Protocol: Select From List: ip ▾ Match to Value: (Range: 0-255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

可用的选项被描述如下：

- 拒绝—阻塞满足规则标准进入或退出WAP设备的所有数据流。
- 许可证—允许满足规则标准进入或退出WAP设备的所有数据流。

第 4 步：不管其内容，检查匹配每个信息包复选框匹配规则为每个帧或信息包。如果要配置特定匹配标准，则请不选定匹配每个信息包复选框。

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:)

Service Type

IP DSCP: Select From List: Match to Value: (Range:)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range:)

Delete ACL:

节时： 如果检查匹配每个信息包复选框然后跳到第13步。

第5步(可选)检查L3或L4协议根据IP Protocol字段的值的匹配情况的协议复选框在IPv4信息包的。如果协议复选框被检查，请点击这些单选按钮之一。

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:)

Service Type

IP DSCP: Select From List: Match to Value: (Range:)

选项被描述如下：

- 从列表挑选—从挑选选择协议从列表下拉列表。下拉列表有ip，icmp，igmp，tcp，

udp协议。

- 重视的匹配—在列表没提交的协议。输入标准IANA分配的协议ID发怒的从0到255。

来源IP Address复选框包括来源的IP地址的第6步(可选的)检查在匹配情况。输入来源的IP地址和通配符掩码在各自字段。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。

The screenshot shows the 'ACL Rule Configuration' interface. At the top, 'ACL Name - ACL Type' is set to 'User1 - IPv4' and 'Rule' is 'New Rule'. The 'Action' is 'Deny'. Under 'Match Every Packet', the checkbox is unchecked. The 'Protocol' is 'ip', selected from a list. The 'Source IP Address' field is checked and contains '192.168.10.0', with a 'Wild Card Mask' of '0.0.0.255'. Below this, 'Source Port', 'Destination IP Address', 'Destination Port', 'IP DSCP', 'IP Precedence', and 'IP TOS Bits' are all unchecked. A 'Delete ACL' checkbox is also unchecked. A 'Save' button is at the bottom.

第7步(可选的)检查包括源端口的源端口复选框在匹配情况。如果源端口复选框被检查，请点击这些单选按钮之一。

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:)

Service Type

IP DSCP: Select From List: Match to Value: (Range:)

IP Precedence: (Range: 0 - 7)

- 从列表挑选—从挑选选择源端口从列表下拉列表。下拉列表有ftp，ftpdata，http，smtp，snmp，telnet，tftp，www端口。

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:)

- 对端口的匹配—**在列表没提交的源端口。输入排列0到65535的端口号。**

目的地IP Address复选框包括目的地的IP地址的第8步(可选的)检查在匹配情况。输入目的地的IP地址和**通配符掩码**在他们的各自字段。通配符掩码让您指定到目的地IP地址的哪台主机此访问列表适用。

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

第9步(可选的)检查包括目的地端口的目的地Port复选框在匹配情况。如果目的地Port复选框被检查，请点击这些单选按钮之一。

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

•从列表挑选—从挑选选择目的地端口从列表下拉列表。下拉列表有ftp，ftpdata，http，smtp，snmp，telnet，tftp，www端口。

The screenshot shows a configuration window for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is unchecked. The 'Protocol' is set to 'ip'. The 'Source IP Address' is '192.168.10.0' with a 'Wild Card Mask' of '0.0.0.255'. The 'Source Port' is set to 'ftp'. The 'Destination IP Address' is '192.168.20.0' with a 'Wild Card Mask' of '0.0.0.255'. The 'Destination Port' is set to '80', which is highlighted with a red circle. The 'Service Type' section is empty. The 'Delete ACL' checkbox is unchecked. A 'Save' button is at the bottom.

•对端口的匹配—在列表没提交的目的地端口。输入范围自0到65535在匹配到Port字段的端口号。

Note:仅一服务从服务类型标准地区被挑选，并且可以为匹配情况被添加。

第10.步(可选的)检查匹配信息包的IP DSCP复选框根据IP DSCP重视。如果IP DSCP复选框被检查，请点击这些单选按钮之一。DSCP用于指定在帧的IP头的数据流优先级。这分类相关的数据流的所有信息包与您从列表挑选的IP DSCP值。关于在DSCP的更详细的资料，请参考得[这里](#)。

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: 192.168.10.0 Match to Value: (Range: 0 - 255) Wild Card Mask: 0.0.0.255

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: 192.168.20.0 Match to Value: (Range: 0 - 255) Wild Card Mask: 0.0.0.255

Destination Port: Select From List: Match to Port: 80 (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: af11 Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Save

•从列表挑选—从挑选选择IP DSCP值从列表下拉列表。下拉列表有DSCP保证的转发(AS)，业务类别(CS)或紧急转发(EF)值。

•重视的匹配—定制DSCP值。输入范围自0到63在匹配到值字段的DSCP值。

包括IP优先级值的第11步(可选)检查theIP优先次序复选框在匹配情况。如果IP优先级复选框被检查，请输入范围自0到7的IP优先级值。关于在IP优先级的更详细的资料，请参考得[这里](#)。

Service Type

IP DSCP: Select From List: Match to Value: 24 (Range: 0 - 63)

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: DF (Range: 00 - FF) IP TOS Mask: DE

Delete ACL:

Save

步骤12。(可选)请检查IP TOS位复选框使用信息包的服务类型位在IP头作为匹配标准。如果范围自00-FF和IP TOS掩码范围自在各自字段的00-FF的IP TOS位复选框被检查，请输入IP TOS位。

Service Type

IP DSCP: Select From List: Match to Value: (R)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask:

Delete ACL:

第13步。 (可选), 如果要然后删除被配置的ACL, 请检查删除ACL复选框。

Service Type

IP DSCP: Select From List: Match to Value: (R)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask:

Delete ACL:

步骤14。 点击“Save”保存设置。