在WAP121和WAP321接入点上创建和配置基于IPv4的访问控制列表(ACL)规则

目标

访问控制列表(ACL)是用于提高安全性的网络流量过滤器和相关操作的列表。ACL包含允许或拒绝访问网络设备的主机。QoS功能包含差分服务(DiffServ)支持，允许将流量分类为流并根据定义的每跳行为进行特定QoS处理。

本文介绍如何在WAP121和WAP321接入点(WAP)上创建和配置基于IPv4的ACL。

适用设备

·WAP121
· WAP321

软件版本

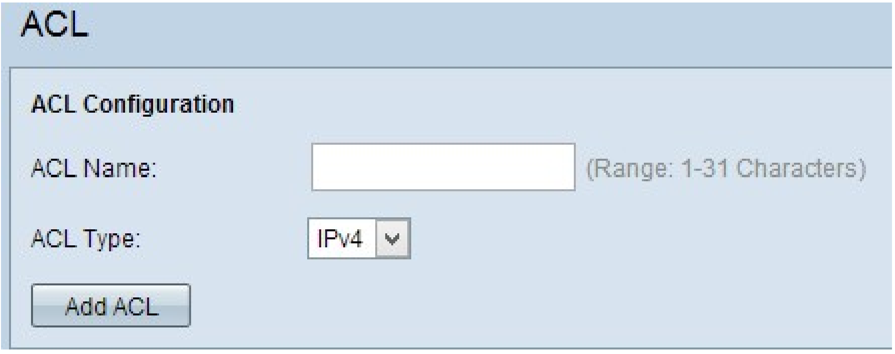
•v1.0.3.4

基于IPv4的ACL配置

IP ACL对IP堆栈中第3层的流量进行分类。每个ACL是一组最多10条规则，这些规则应用于从无线客户端发送或由无线客户端接收的流量。每条规则指定应使用给定字段的内容来允许还是拒绝对网络的访问。规则可以基于各种标准，并且可以应用于数据包中的一个或多个字段，例如源或目标IP地址、源或目标端口或数据包中承载的协议。

创建IPv4 ACL

步骤1.登录接入点配置实用程序并选择**Client QoS > ACL**。ACL*页面*打开：



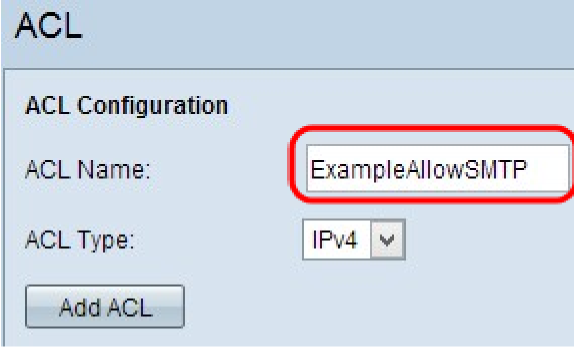
ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4

步骤2.在ACL Name字段中输入ACL*的名称*。



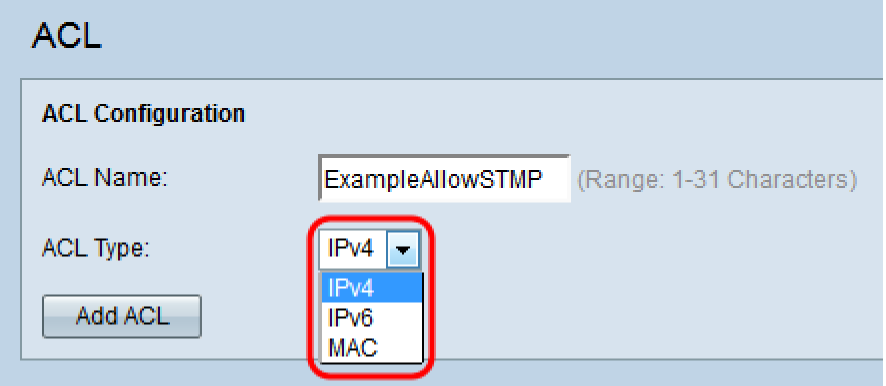
ACL

ACL Configuration

ACL Name: ExampleAllowSMTP

ACL Type: IPv4

步骤3.从ACL Type下**拉列**表中选择ACL*的IPv4*类型。



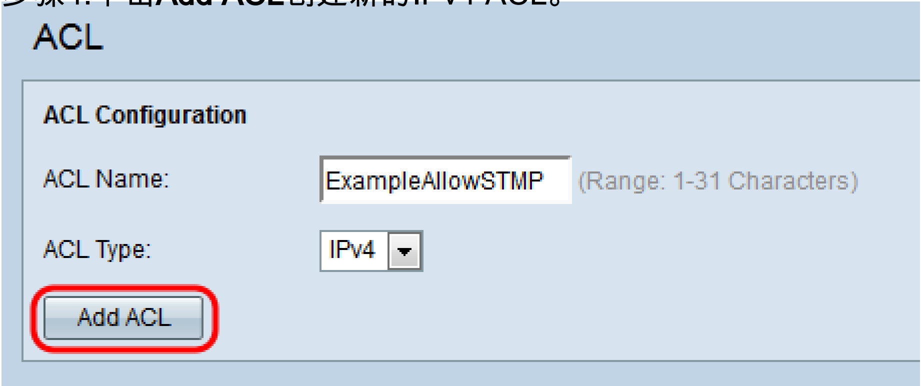
ACL

ACL Configuration

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

ACL Type: IPv4

步骤4.单击**Add ACL**创建新的IPv4 ACL。



ACL

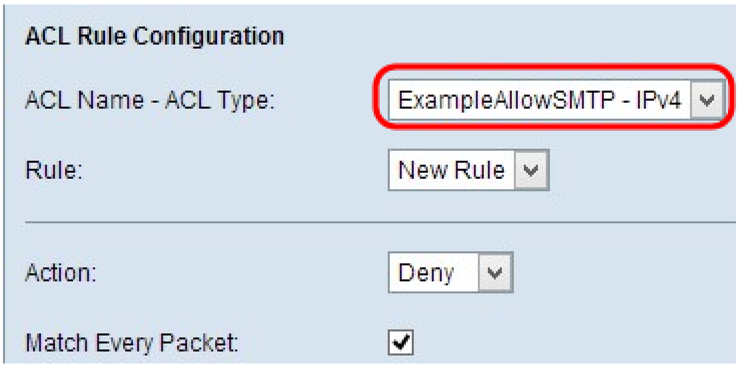
ACL Configuration

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

ACL Type: IPv4

IPv4 ACL规则的配置

步骤1.从ACL Name-ACL Type下拉列*表中选择*ACL，为其配置规则。



ACL Rule Configuration

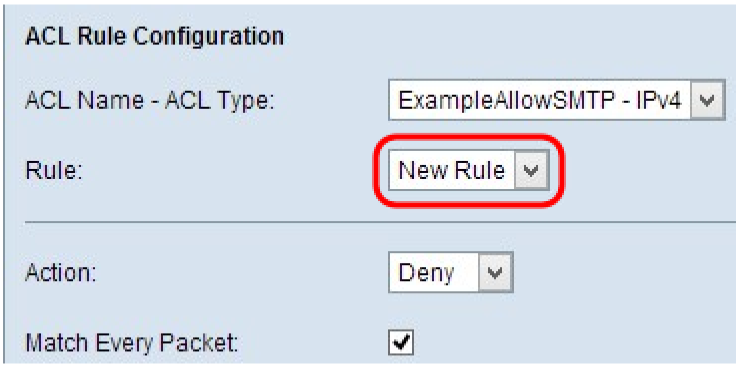
ACL Name - ACL Type: ExampleAllowSMTP - IPv4

Rule: New Rule

Action: Deny

Match Every Packet: ☑

步骤2.如果必须为所选ACL配置新规则，请从*Rule*下拉列**表中选**择New *Rule*;否则，从“规则”(Rule)下拉列*表中*选择一个当前规则。



ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4

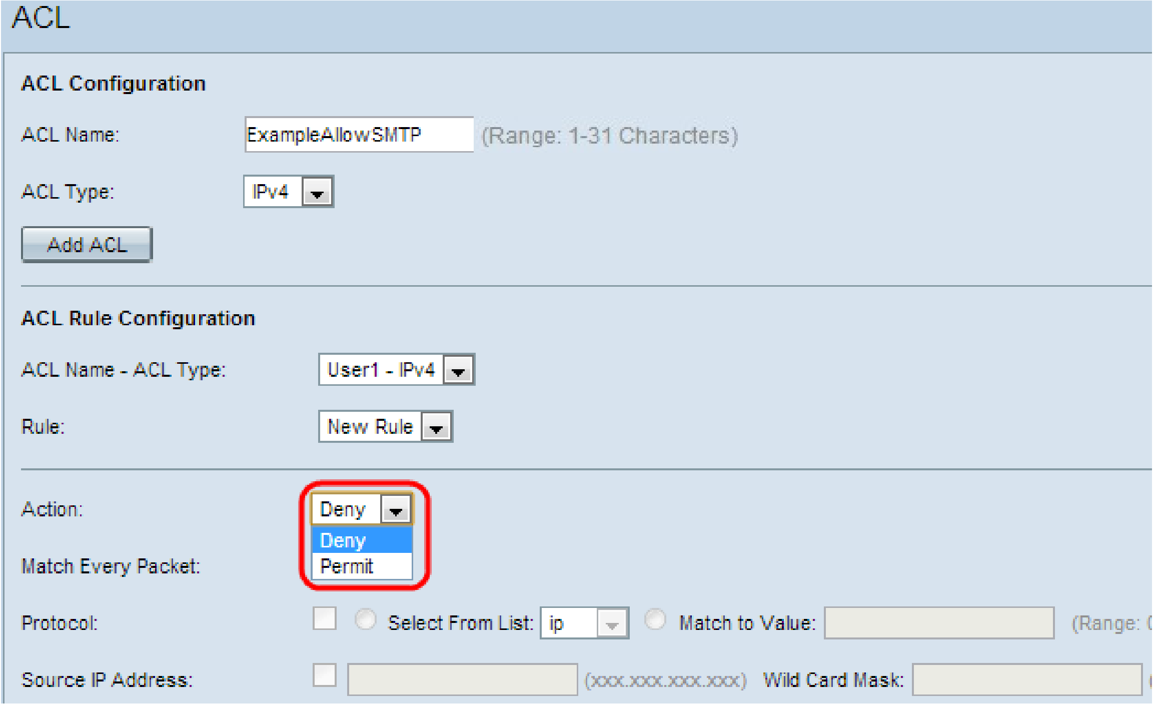
Rule: New Rule

Action: Deny

Match Every Packet: ☑

注意：一个ACL最多可创建10个规则。

步骤3.从Action下拉列表中选择ACL规则的操作。



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:

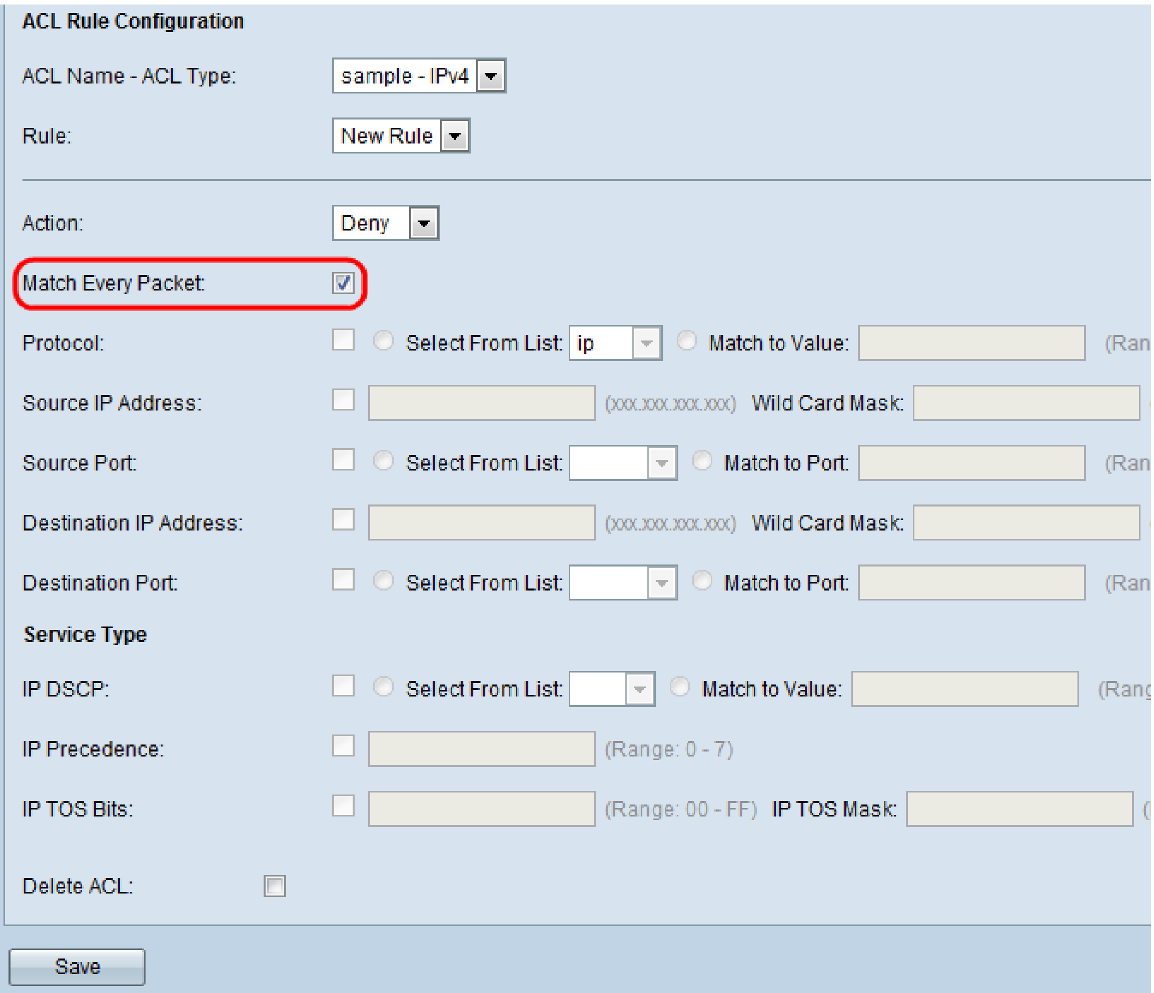
Source IP Address: □ (xxx.xxx.xxx.xxx) Wild Card Mask:

可用选项如下所述：

·拒绝 — 阻止符合规则条件的所有流量进入或退出WAP设备。

·允许 — 允许符合规则条件的所有流量进入或退出WAP设备。

步骤4.选中Match Every Packet*复选框*，以匹配每个帧或数据包的规则，而不考虑其内容。如果要配置特定匹配条件，请取消选中“匹配每个数据*包”复选*框。



ACL Rule Configuration

ACL Name - ACL Type: sample - IPv4

Rule: New Rule

Action: Deny

Match Every Packet: ☑

Protocol: □ ○ Select From List: ip ○ Match to Value: (Ran

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

Source Port: □ ○ Select From List: ○ Match to Port: (Ran

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

Destination Port: □ ○ Select From List: ○ Match to Port: (Ran

Service Type

IP DSCP: □ ○ Select From List: ○ Match to Value: (Rang

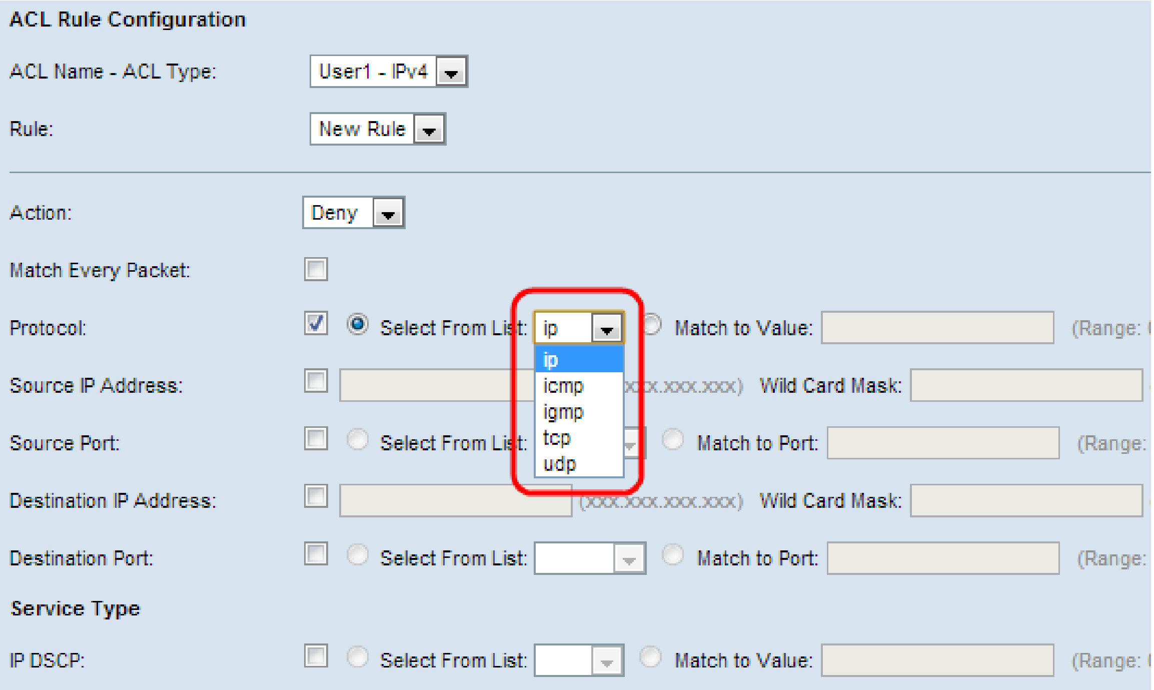
IP Precedence: □ (Range: 0 - 7)

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

Delete ACL: □

节省时间：如果选中Match *Every Packet复选*框，则跳至步骤13。

步骤5.（可选）根据IPv4数据包中IP协议字段的值，选中L3或L4协议匹配条件的*Protocol*复选框。如果选中*Protocol* 复选框，请单击其中一个单选按钮。



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:

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

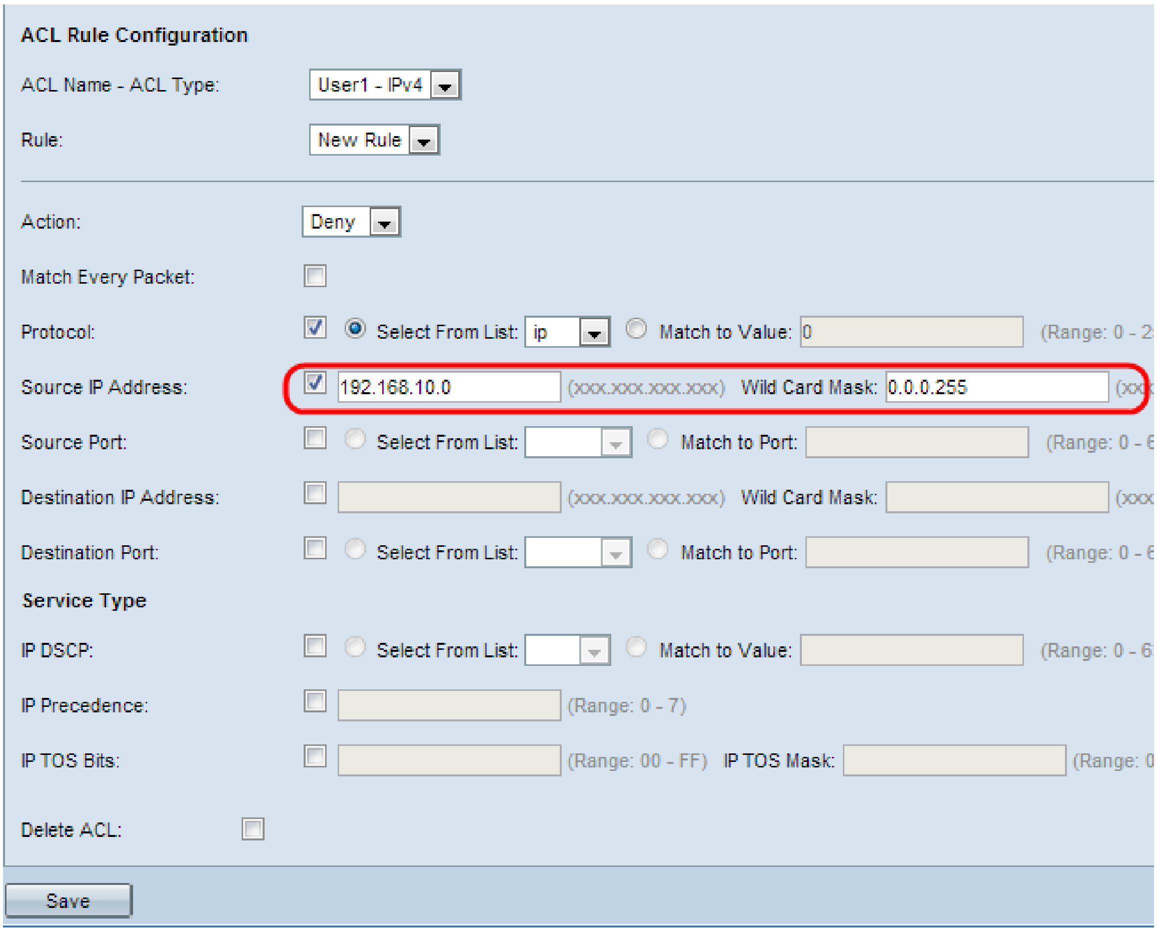
IP DSCP: □ ○ Select From List: ○ Match to Value: (Range:

选项描述如下：

·从列表中选择 — 从从列表中选择 *下拉列*表中选择协议。下拉列表包含ip、icmp、igmp、 tcp、udp协议。

·与值匹配 — 用于列表中未显示的协议。输入从0到255的标准IANA分配协议ID。

步骤6.（可选）选中Source IP Address*复选框*，以在匹配条件中包含源的IP地址。在相应字段中*输入源*的IP地址和通配符掩码。通配符掩码允许您指定此访问列表应用到源IP地址的主机。



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: 0 (Range: 0 - 2

Source IP Address: ☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255 (xx

Source Port: □ ○ Select From List: ○ Match to Port: (Range: 0 - 6

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

Destination Port: □ ○ Select From List: ○ Match to Port: (Range: 0 - 6

Service Type

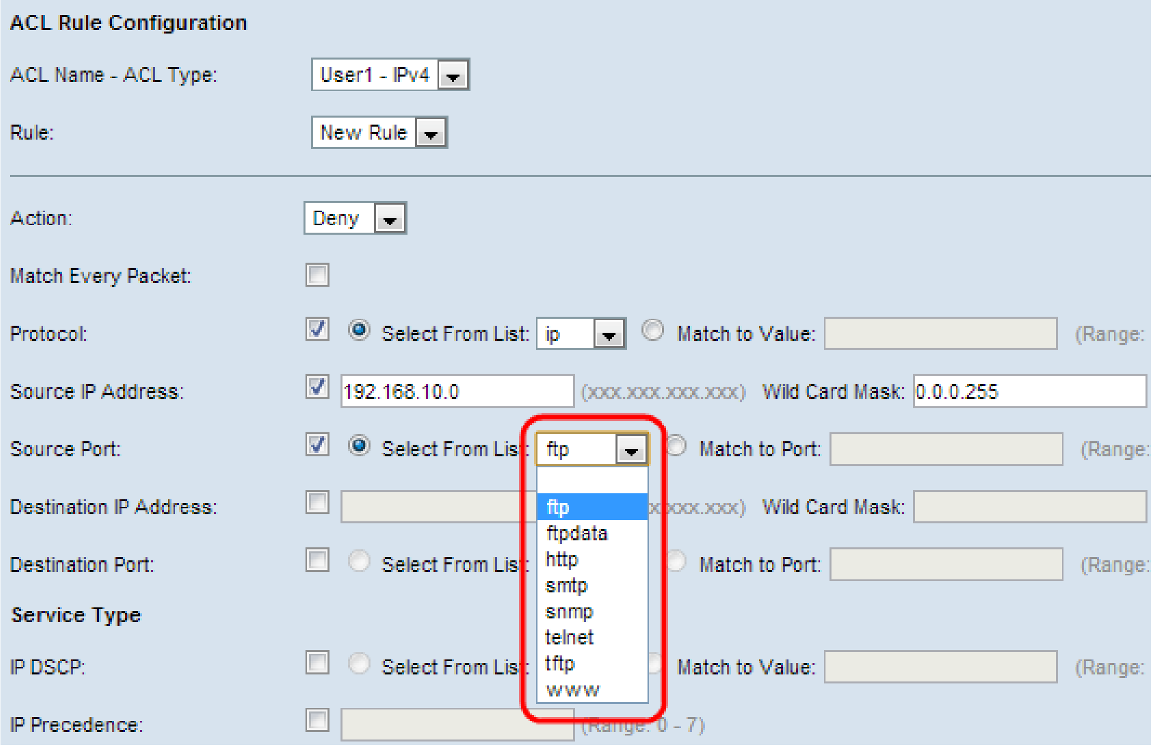
IP DSCP: □ ○ Select From List: ○ Match to Value: (Range: 0 - 6

IP Precedence: □ (Range: 0 - 7)

IP TOS Bits: □ (Range: 00 - FF) IP TOS Mask: (Range: 0

Delete ACL: □

步骤7.（可选）选中Source Port**复选框**，以在匹配条件中包含源端口。如果选中*Source Port(源端口*)复选框，请单击其中一个单选按钮。



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:

Source IP Address: ☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: ☑ ● Select From List: ftp ○ Match to Port: (Range:

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

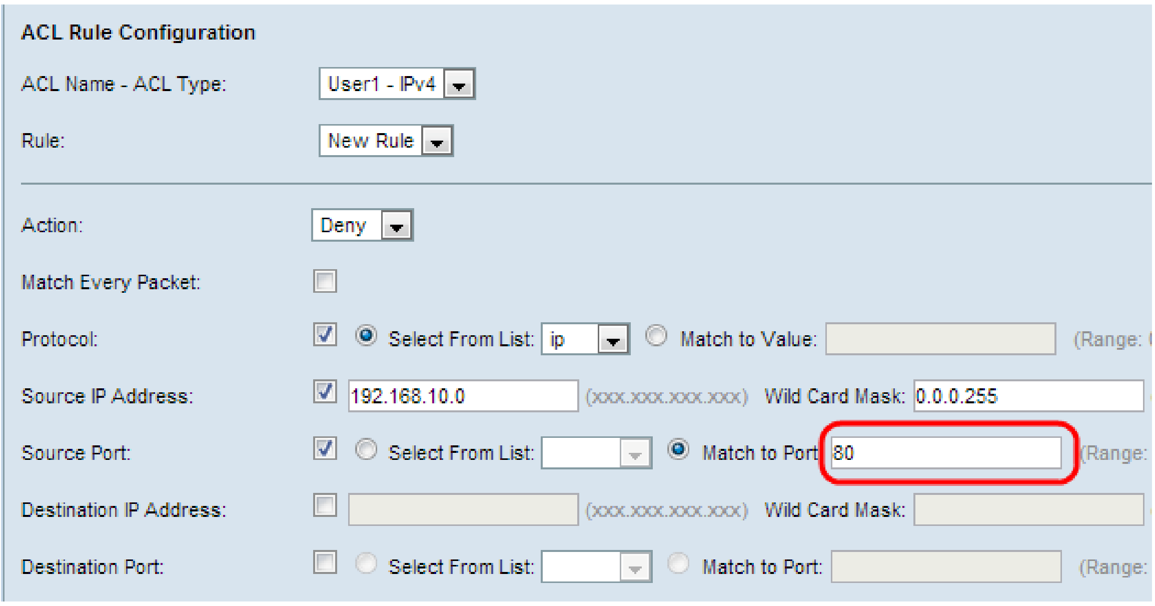
Destination Port: □ ○ Select From List ○ Match to Port: (Range:

Service Type

IP DSCP: □ ○ Select From List ○ Match to Value: (Range:

IP Precedence: □ (Range: 0 - 7)

·从列表中选择 — 从从列表中选择下*拉列表*中选择源端口。下拉列表包含ftp、ftpdata、http、smtp、snmp、telnet、tftp、www端口。



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:

Source IP Address: ☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

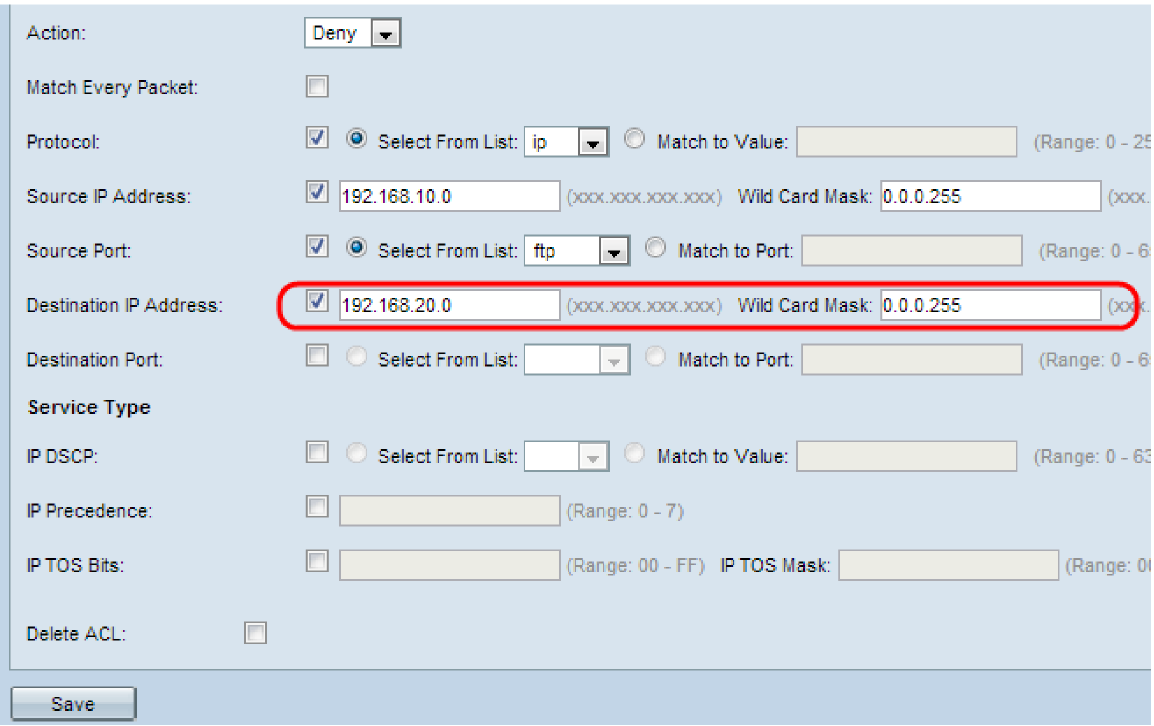
Source Port: ☑ ○ Select From List: ● Match to Port: 80 (Range:

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

Destination Port: □ ○ Select From List: ○ Match to Port: (Range:

·与端口匹配 — 用于列表中未显示的源端口。输入端口号，范围为0到65535。

步骤8.（可选）选中Destination IP Address复选*框，将目*标的IP地址包括在匹配条件中。在目标的IP地*址和通配符*掩码各自的字段中输入。通配符掩码允许您指定此访问列表应用于目标IP地址的主机。



Action: Deny

Match Every Packet: □

Protocol: ☑ ● Select From List: ip ○ Match to Value: (Range: 0 - 25

Source IP Address: ☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255 (xxx.

Source Port: ☑ ● Select From List: ftp ○ Match to Port: (Range: 0 - 6

Destination IP Address: ☑ 192.168.20.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255 (xx

Destination Port: □ ○ Select From List: ○ Match to Port: (Range: 0 - 6

Service Type

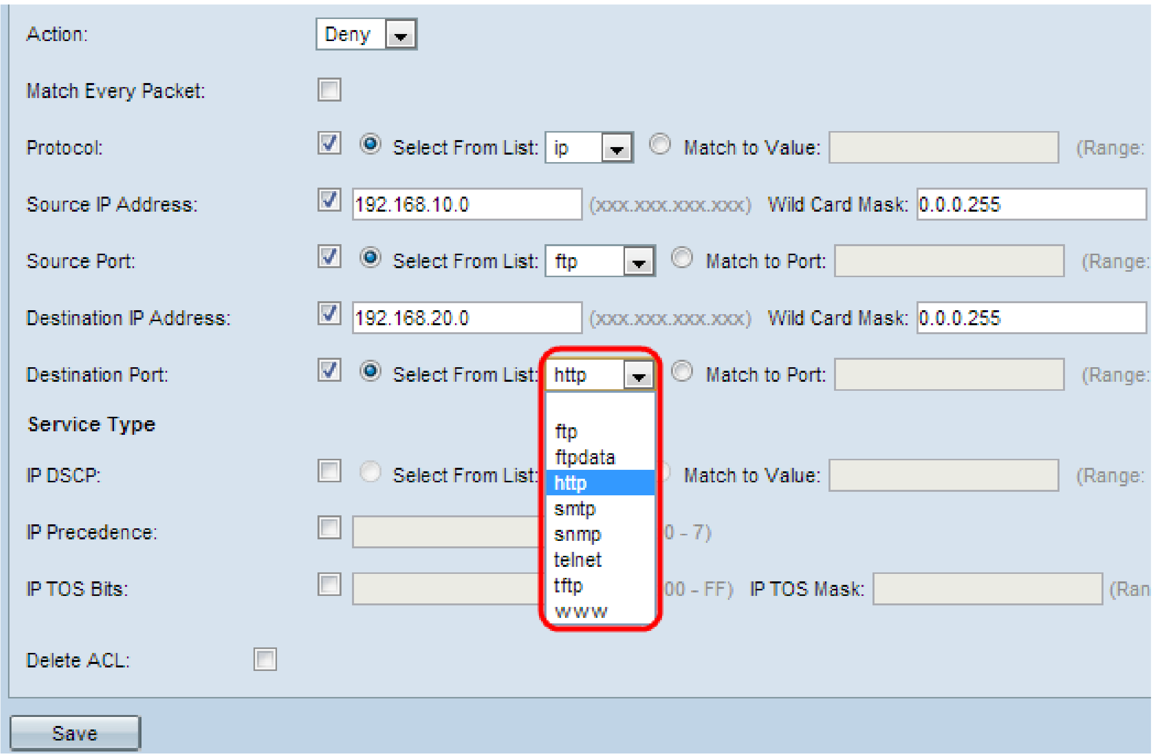
IP DSCP: □ ○ Select From List: ○ Match to Value: (Range: 0 - 63

IP Precedence: □ (Range: 0 - 7)

IP TOS Bits: □ (Range: 00 - FF) IP TOS Mask: (Range: 0(

Delete ACL: □

步骤9.（可选）选中Destination Port复**选框**，将目标端口包括在匹配条件中。如果选中*Destination Port（目标端口）*复选框，请单击其中一个单选按钮。



Action: Deny

Match Every Packet: □

Protocol: ☑ ● Select From List: ip ○ Match to Value: (Range:

Source IP Address: ☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: ☑ ● Select From List: ftp ○ Match to Port: (Range:

Destination IP Address: ☑ 192.168.20.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Destination Port: ☑ ● Select From List: http ○ Match to Port: (Range:

Service Type

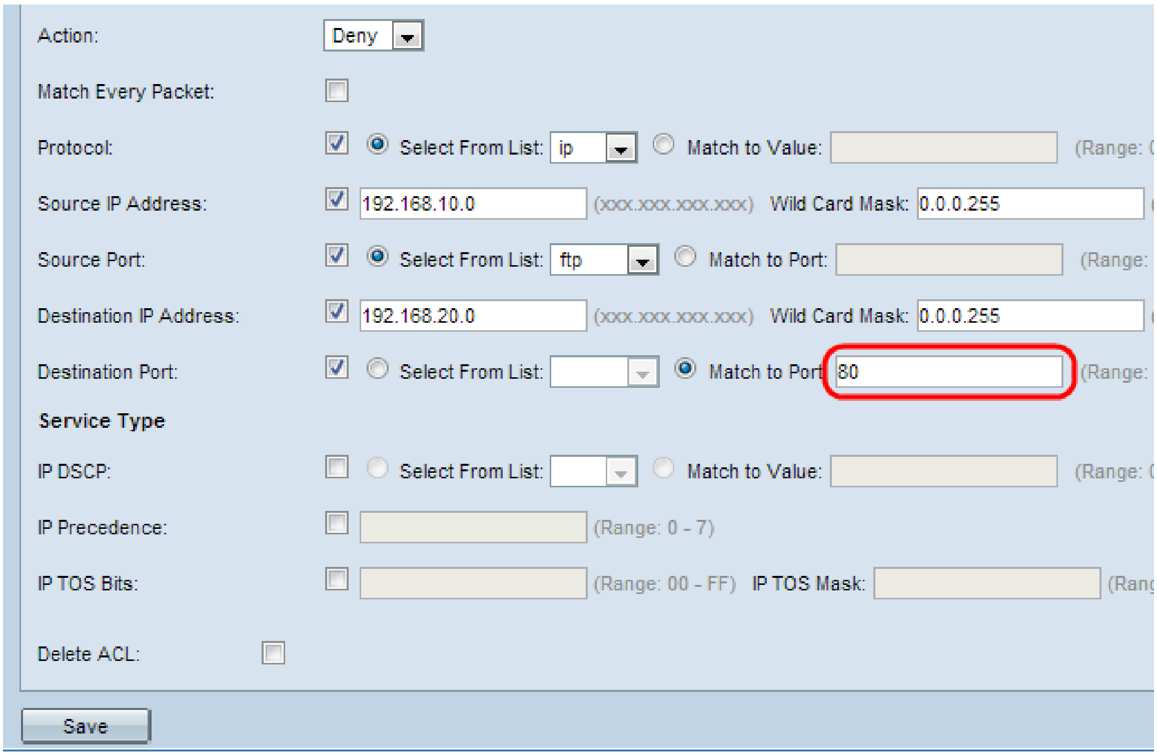
IP DSCP: □ ○ Select From List: Match to Value: (Range:

IP Precedence: □ 0 - 7)

IP TOS Bits: □ 00 - FF) IP TOS Mask: (Ran

Delete ACL: □

·从列表中选择 — 从从列表中选择下*拉列表*中选择目标端口。下拉列表包含ftp、ftpdata、http、smtp、snmp、telnet、tftp、www端口。



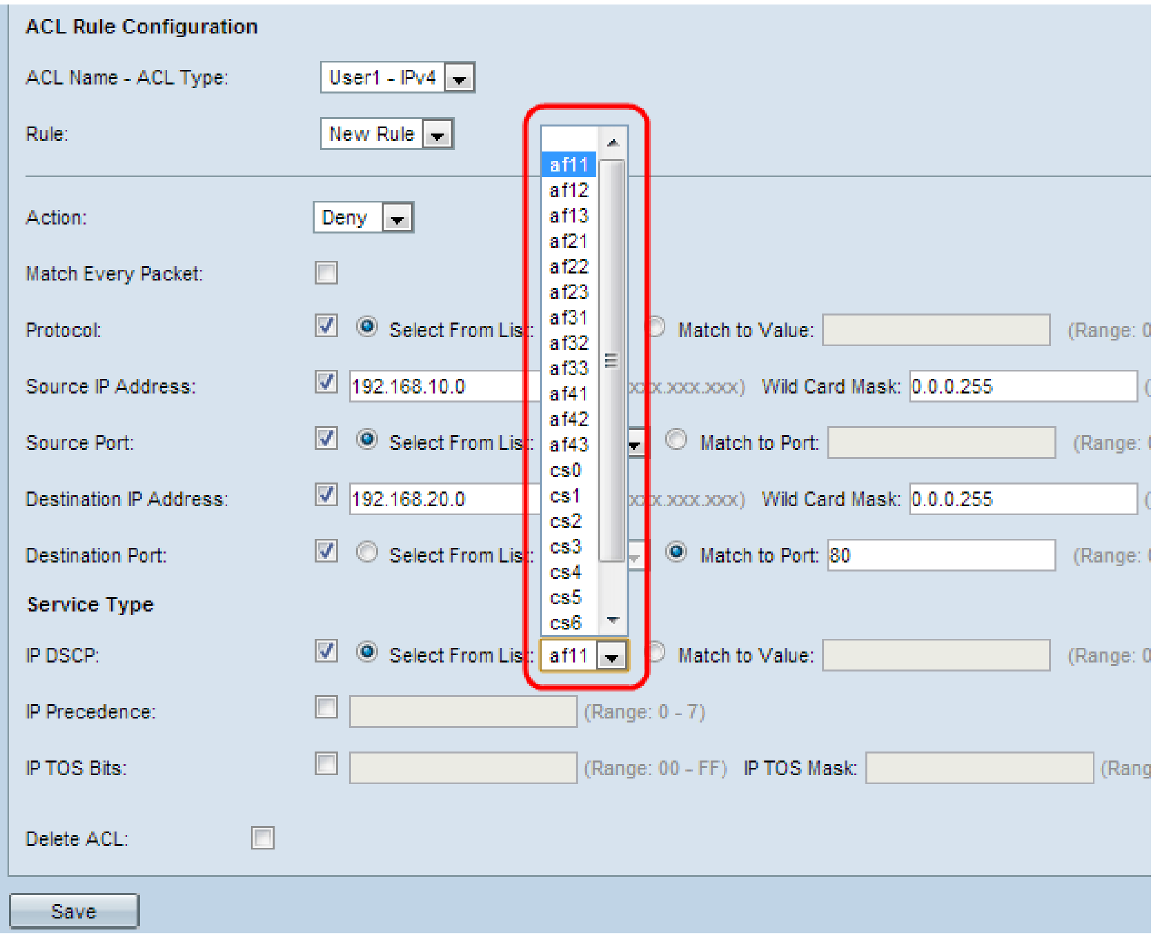
Action:	Deny
Match Every Packet:	□
Protocol:	☑ ● Select From List: ip ○ Match to Value: (Range: (
Source IP Address:	☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255 (
Source Port:	☑ ● Select From List: ftp ○ Match to Port: (Range:
Destination IP Address:	☑ 192.168.20.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255 (
Destination Port:	☑ ○ Select From List: ● Match to Port 80 (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: (Rang
Delete ACL:	□

Save

·与端口匹配 — 用于列表中未显示的目标端口。在Match to Port字段中输入范围为0到65535的端口号。

注意：只能从“服务类型”区域选择其中一*项服务*，并且可以为匹配条件添加这些服务。

步骤10.（可选）选中*IP DSCP*复选框，以根据IP DSCP值匹配数据包。如果选中*了IP DSCP*复选框，请单击其中一个单选按钮。DSCP用于指定帧的IP报头上的流量优先级。这会将关联流量流的所有数据包与您从列表中选择的IP DSCP值进行分类。有关DSCP的更多详细信息，请参阅此处。



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

Source IP Address: ☑ 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: ☑ ● Select From List ○ Match to Port: (Range:

Destination IP Address: ☑ 192.168.20.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Destination Port: ☑ ○ Select From List ● Match to Port: 80 (Range:

Service Type

IP DSCP: ☑ ● Select From List: af11 ○ Match to Value: (Range: 0

IP Precedence: □ (Range: 0 - 7)

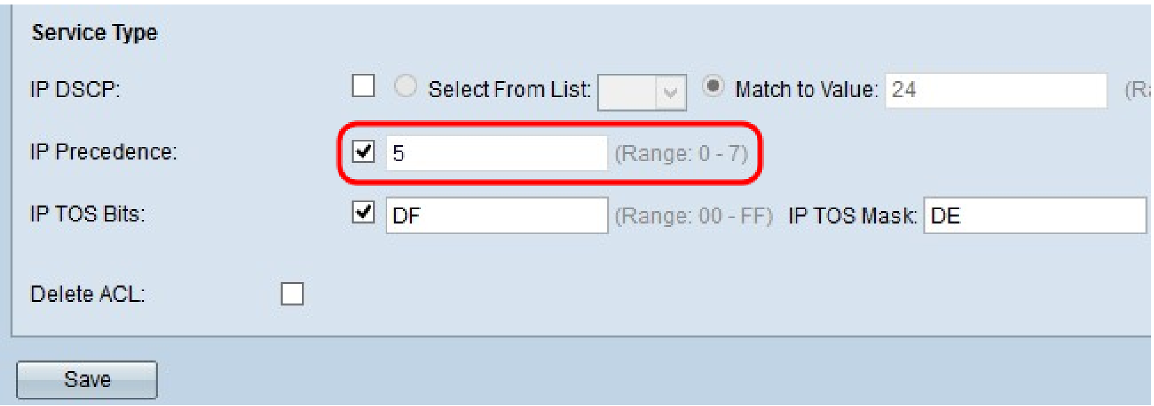
IP TOS Bits: □ (Range: 00 - FF) IP TOS Mask: (Rang

Delete ACL: □

·从列表中选择 — 从从列表中选择下拉列*表中选择*IP DSCP值。下拉列表具有DSCP保证转发(AS)、服务类别(CS)或加速转发(EF)值。

·与值匹配 — 自定义DSCP值。在Match to Value字段中输入范围为0到63的DSCP值。

第11步。（可选）选中*IP Precedence复选*框，在匹配条件中包含IP Precedence值。如果选中IP优先级复选框，请输入IP优先级值，范围为0到7。有关IP优先级的详细信息，请参阅此处。



Service Type

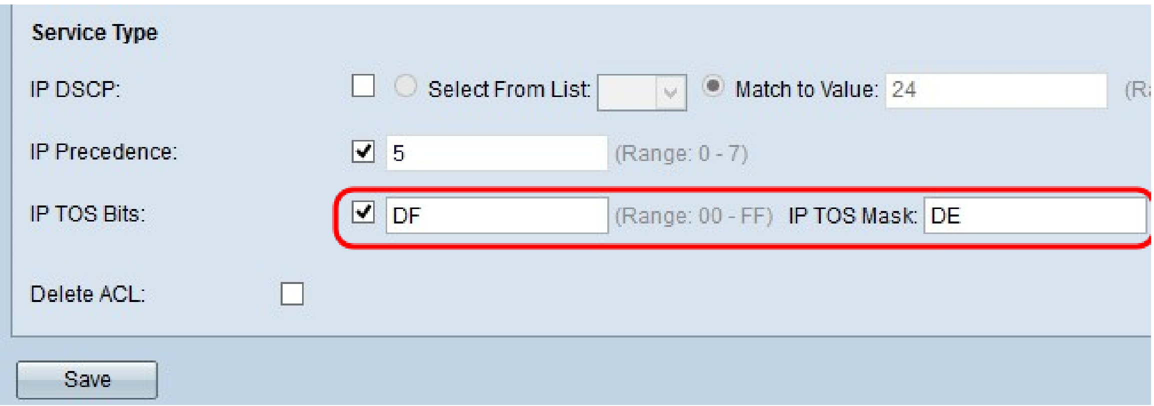
IP DSCP: □ ○ Select From List ● Match to Value: 24 (R

IP Precedence: ☑ 5 (Range: 0 - 7)

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

Delete ACL: □

步骤12.（可选）选中*IP TOS Bits*复选框，以将数据包的IP报头中的Type of Service bits用作匹配条件。如果选中IP TOS Bits复选框，请在相应字段中输入IP TOS位，范围为00-FF，IP TOS掩码范围为00-FF。



Service Type

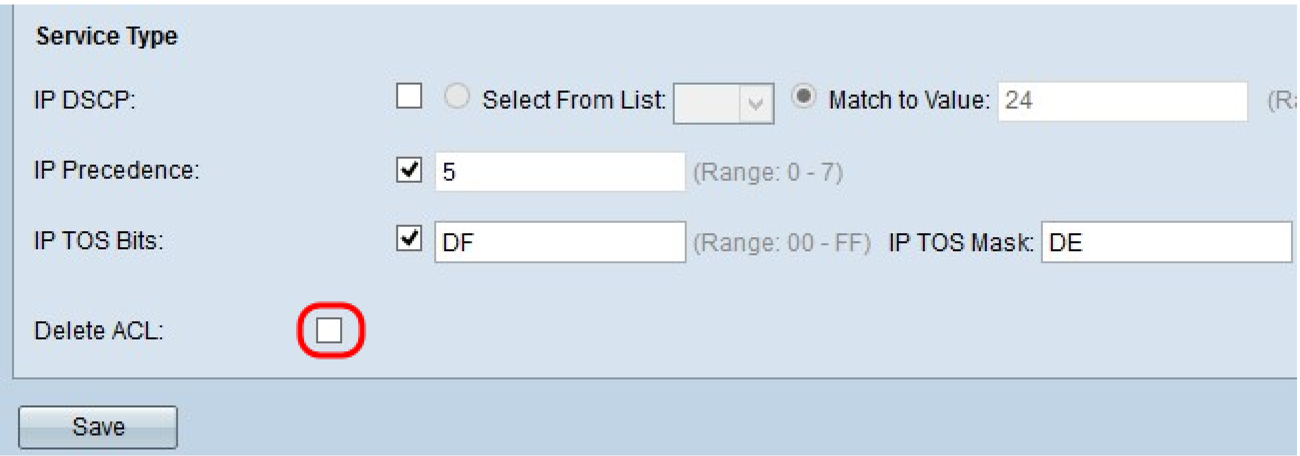
IP DSCP: □ ○ Select From List: ● Match to Value: 24 (Ra

IP Precedence: ☑ 5 (Range: 0 - 7)

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

Delete ACL: □

步骤13.（可选）如果要删除已配置的ACL，请选中Delete ACL复选框。



Service Type

IP DSCP: □ ○ Select From List: ● Match to Value: 24 (Ra

IP Precedence: ☑ 5 (Range: 0 - 7)

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

Delete ACL: □

步骤14.单击“**保存**”以保存设置。