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 V	
Add ACL		

步骤2.在ACL Name字段中输入ACL的名称。

ACL	
ACL Configuration	
ACL Name:	ExampleAllowSMTP
ACL Type:	IPv4 V
Add ACL	

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 💌	
Add ACL	IPv4 IPv6 MAC	

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 💌	
Add ACL		

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:	v

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
Add ACL	
ACL Rule Configuration	n
ACL Name - ACL Type:	User1 - IPv4 💌
Rule:	New Rule
Action:	
Match Every Packet:	Permit
Protocol:	Select From List: ip V Match to Value: (Range: (Range:)
Source IP Address:	(xooccooccoocc) 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:	(XOC.XOC.XOC.XOX) Wild Card Mask:
Source Port:	O Select From List: Vatch to Port: (Ran
Destination IP Address:	(XOC.XOC.XOC.XOX) Wild Card Mask:
Destination Port:	O Select From List: ✓ Match to Port: (Ran
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: (
Delete ACL:	
Save	

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:	icmp xcx.xxxx) Wild Card Mask:
Source Port:	C Select From List: tcp U Match to Port: (Range
Destination IP Address:	Wild Card Mask:
Destination Port:	C Select From List:
Service Type	
IP DSCP:	C Select From List:

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	1
ACL Name - ACL Type:	User1 - IPv4
Rule:	New Rule 💌
Action:	Deny 💌
Match Every Packet:	
Protocol:	Select From List: ip Select From List: ip Match to Value: 0 (Range: 0 - 2)
Source IP Address:	Image: 192.168.10.0 (xox.xox.xox.xox) Wild Card Mask: 0.0.0.255 (xox.xox.xox)
Source Port:	C Select From List: Match to Port: (Range: 0 - 6
Destination IP Address:	(xox.xox.xox.xox) Wild Card Mask: (xox
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:	
Save	

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 Select From List: ip Match to Value: (Range:
Source IP Address:	☑ 192.168.10.0 (x00000000000) Wild Card Mask: 0.0.0.255
Source Port:	Select From Lis: ftp Match to Port: (Range:
Destination IP Address:	ftp xboox.coox) Wild Card Mask:
Destination Port:	C Select From Lis: http Match to Port: (Range:
Service Type	snmp
IP DSCP:	Select From Lis: tftp UMatch to Value: (Range: WWW)
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:	Image: 192.168.10.0 (x000.x000.x000) Wild Card Mask: 0.0.0.255
Source Port:	Select From List: Natch to Port 80 (Range:
Destination IP Address:	(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 C Match to Value: (Range: 0 - 25)
Source IP Address:	☑ 192.168.10.0 (xoc:xoc:xoc:xoc) Wild Card Mask: 0.0.0.255 (xoc.
Source Port:	Select From List: ftp Match to Port: (Range: 0 - 6)
Destination IP Address:	▼ 192.168.20.0 (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Destination Port:	C Select From List: V 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:	
Save	

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 (xox.xox.xoxx) Wild Card Mask: 0.0.0.255
Source Port:	Select From List: ftp Select From List: ftp Match to Port: (Range:
Destination IP Address:	V 192.168.20.0 (xooc.xooc.xooc) Wild Card Mask: 0.0.0.255
Destination Port:	Select From List: http Match to Port: (Range:
Service Type	ftp
IP DSCP:	C Select From List: http Match to Value: (Range:
IP Precedence:	smp snmp talaat
IP TOS Bits:	tftp 00 - FF) IP TOS Mask: (Ran
Delete ACL:	
Save	

·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: Content of
Source IP Address:	☑ 192.168.10.0 (x0x.x0x.x0x.x0x) Wild Card Mask: 0.0.0.255
Source Port:	Select From List: ftp Select From List: ftp Match to Port: (Range:
Destination IP Address:	☑ 192.168.20.0 (x000.x000.x000.x000) Wild Card Mask: 0.0.0.255
Destination Port:	🖉 🛇 Select From List: 🔍 🔍 Match to Port 80 (Range:
Service Type	
IP DSCP:	C Select From List: Match to Value: (Range: (
IP Precedence:	(Range: 0 - 7)
IP TOS Bits:	(Range: 00 - FF) IP TOS Mask: (Range
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<u>阅此处</u>。

ACL Rule Configuration	
ACL Name - ACL Type:	User1 - IPv4 💌
Rule:	
Action:	Deny af12 af13 af21
Match Every Packet:	af22 af23
Protocol:	Select From Lis: af31 af32 A Match to Value: (Range: 0
Source IP Address:	Image: Wild Card Mask: 0.0.0.255 ()
Source Port:	Image: Weight of the second secon
Destination IP Address:	▼ 192.168.20.0 cs1 xopcooccoox) Wild Card Mask: 0.0.0.255 (
Destination Port:	Select From Lis: Cs3 cs4 Match to Port: 80 (Range: 1
Service Type	cs5 cs6 🔻
IP DSCP:	O Select From Lis: af11 Match to Value: (Range: 0
IP Precedence:	(Range: 0 - 7)
IP TOS Bits:	(Range: 00 - FF) IP TOS Mask: (Rang
Delete ACL:	
Save	

·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<u>阅此处</u>

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:	
Save	

o

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 (R
IP Precedence:	✓ 5 (Range: 0 - 7)
IP TOS Bits:	DF (Range: 00 - FF) IP TOS Mask: DE
Delete ACL:	
Save	

<u>步骤13</u>.(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 (F
IP Precedence:	✓ 5 (Range: 0 - 7)
IP TOS Bits:	DF (Range: 00 - FF) IP TOS Mask: DE
Delete ACL:)
Save	

步骤14.单击"**保存**"以保存设置。