802.1X AAA ACL **宋斌** 2012-03-14 发表



本配置举例中的AP使用的是WA2200系列无线局域网接入点设备,AC使用的是WX6103 系列无线控制器。Radius server的IP地址为8.1.45.67/24。Client和AP通过DHCP服务器 获取IP地址。

Client通过认证后允许访问网络8.1.0.0/16即VLAN210,其他网络资源不允许访问。

三、特性介绍:

下发ACL是接入设备与Radius服务器配合来对用户访问网络的权限进行控制。用户认证 通过后根据Radius服务器报文中的ACL内容,对用户可以访问哪些网络资源,不可以访 问哪些网络资源进行控制。

网络管理员可以通过下发ACL对用户访问网络的权限进行控制,具有很强的灵活性和适应性。

四、主要配置步骤:

在Dot1x接入端配置802.1x和认证。

启用端口安全port-security, 配置Dot1x认证方式为CHAP。

[AC] port-security enable

[AC] dot1x authentication-method chap

#配置认证策略。

[AC] radius scheme radius

[AC-radius-radius] primary authentication 8.1.45.67

[AC-radius-radius] primary accounting 8.1.45.67

[AC-radius-radius] key authentication radius

[AC-radius-radius] key accounting radius

[AC-radius-radius] nas-ip 8.1.61.3

[AC-radius-radius] accounting-on enable

[AC-radius-radius] quit

#配置认证域。

[AC] domain radius

[AC-isp-radius] authentication lan-access radius-scheme radius [AC-isp-radius] authorization lan-access radius-scheme radius

[AC-isp-radius] accounting lan-access radius-scheme radius [AC-isp-radius] quit

#把配置的认证域cams设置为系统缺省域。

[AC] domain default enable radius

配置ACL。

[AC] acl number 3000[AC-acl-adv-3000] rule 0 permit ip destination 8.1.0.0 0.0.255.255[AC-acl-adv-3000] rule 1 deny ip

#配置无线口,并在无线口启用端口安全(802.1x认证)。

[AC] vlan 10
[AC-vlan10] quit
[AC] interface WLAN-ESS10
[AC-WLAN-ESS10] port access vlan 210
[AC-WLAN-ESS10] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS10] quit

#配置无线服务模板。

[AC] wlan service-template 10 clear [AC-wlan-st-10] ssid radius [AC-wlan-st-10] bind WLAN-ESS 10 [AC-wlan-st-10] service-template enable [AC-wlan-st-10] quit

#配置AP模板并绑定无线服务模板。

[AC] wlan ap wa2220x model WA2220X-AGP
[AC-wlan-ap-wa2220x] serial-id 210235A29E007C000009
[AC-wlan-ap-wa2220x] radio 2
[AC-wlan-ap-wa2220x-radio-2] channel 3
[AC-wlan-ap-wa2220x-radio-2] max-power 6
[AC-wlan-ap-wa2220x-radio-2] service-template 10
[AC-wlan-ap-wa2220x-radio-2] radio enable

#配置VLAN虚接口

[AC] vlan 210
[AC] quit
[AC] interface vlan 210
[AC-Vlan-interface210] ip address 8.1.61.3 24
[AC] interface Vlan-interface 1
[AC-Vlan-interface210] ip address 7.0.0.61 24
[AC-Vlan-interface1] dhcp select relay
[AC-Vlan-interface1] dhcp relay server-select 1

Windows IAS配置

在Windows IAS上配置ACL下发,需要在用户使用的"远程访问策略"中添加Filter-ID属性,配置方法如下:

(1) 进入Internet 验证服务的远程访问策略,双击选取用户所使用的访问策略,点击<编辑配置文件>按钮,弹出"编辑拨入配置文件"窗口。

			1
1912年後1度家心须儿配的条件。			
11次に120日からの人に日は15次(11) 筆取社)日 (2)・			
NAS-IP-Address 匹配 "8.1.61.3"			
添加の) 编辑の) 冊降(R)		
		ᆕᆆᇔᄀᅖᆕᅷᄱᆄᄼ	
如未注按请求和此来略于指定的来件但	689143 • 48/	athice vite	
WATCH THE TO WE			
编辑配查文件(2)			
除非在用户配置文件中指定了访问权限。	,否则本策	客控制对网络的	访问。
如果一个连接请求匹配指定条件:			
() 拒绝远程访问权限(图)			
● 授予远程访问权限 (G)			
	确定	取消	应用 (A)

(2) 在"编辑拨入配置文件"窗口中选取"高级"页签,点击<添加>按钮,弹出"添加属性" 窗口。

名称 ervice-Type	供应商 RADIUS Stan	值 Framed	
Etmon) (cete	a) 1 mile a)	1	

(3) 在"添加属性"中选取Filter-ID选项,双击Filter-ID,弹出"多值属性信息"对话框。

新性 (B):		
名称	供应商	描述
Acct-Interim-Interval	RADIUS Standard	指定每次 NAS 所传送的暂时更新之间的间
Callback-Number	RADIUS Standard	指定回拔电话号码。
Class	RADIUS Standard	指定记帐记录分类。
Filter-Id	RADIUS Standard	指定请求身份验证的用户的筛选器列表名称
Framed-AppleTalk-Link	RADIUS Standard	指定链接到用户的 AppleTalk 网络号。只
Framed-AppleTalk-Network	RADIUS Standard	指定 NAS 必须查询来分配用户的 AppleTa
Framed-AppleTalk-Zone	RADIUS Standard	指定用户的 AppleTalk 默认区域。
Framed-Compression	RADIUS Standard	指定使用的压缩协议。
Framed-IP-Netmask	RADIUS Standard	指定为用户配置的 IP 子网掩码。
Framed-IPX-Network	RADIUS Standard	指定在 NAS 上为用户配置的 IPX 网络编号
Framed-MTU	RADIUS Standard	指定为用户配置的最大传输单位(MTV)。
Framed-Pool	RADIUS Standard	指定应该用来指派地址给用户的指派地址注
Framed-Protocol	RADIUS Standard	指定使用的协议。
Framed-Route	RADIUS Standard	指定在 NAS 上为用户配置的路由信息。
Framed-Routing	RADIUS Standard	指定用户使用的路由方法。
Login-IP-Host	RADIUS Standard	指定用户应该连接到的主机的 IP 地址。
Login-LAT-Group	RADIUS Standard	指定用户身份验证的本地传输 (LAT)组编码
Login-LAT-Node	RADIUS Standard	指定被本地传输(LAT)服务把用户连接到的
Login-LAT-Port	RADIUS Standard	指定被本地传输(LAT)连接到用户的端口。
r , r r r r r	DIDTIG (1 1 1	きりしゃうきょうできょう。そうできょう日本では、

(4) 在"多值属性信息"对话框中点击<添加>按钮,弹出"属性信息"窗口。

【性名:		
/ilter-Id		
醒生号 :		
1		
酮性格式:		
OctetString		
属性值 (I):		
供应商	值	上移の
		下移(世)
		(添加(A)
		删除(医)
		编辑(E)
•		•

(5) 在"属性信息"窗口中配置Fileter-ID属性值,我司字符串和十六进制格式均支持。FileterID属性数字表示ACL NUMBER。

1 设置输入属性值所用的格式为以字符串形式下发,下发的格式类型需要接入 设备端支持。

Filter-Id		
属性号:		
11		
属性格式:		
OctetString		
输入属性值所用的格式 (2):	● 字符串 (S)	○ 十六进制 (년)
3000		

1 设置输入属性值所用的格式为以十六进制数的形式下发,下发的格式类型需要接入设备端支持。

属性名:			
Filter-Id			
属性号:			
11			
属性格式:			
OctetString			
输入属性值所用的格式(2)	○ 字符串	© • -	十六进制(H)
0xBB8			

完后点击<确定>按钮,完成属性添加。

(6) 完成属性添加后如下,点击<应用>按钮,然后确定完成。

1010	供应商	值	
Service-Type Filter-Id	RADIUS Stan RADIUS Stan	Framed 3000	
15 AP			
<u>d</u>			Þ
4 () () () () () () () () () () () () ()	(7) 日明全(7)	1	×

五、结果验证:

(1) Client连接 SSID, 输入用户名和密码, 上线成功。

(2) 在AC上执行display connection可以看到有对应的Client的MAC地址,且ACL正确下发。

display connection ucibindex 1174 Index=1174, Username=test@radius MAC=0810-742d-a88d IP=N/A Access=8021X ,AuthMethod=CHAP Port Type=Wireless-802.11,Port Name=WLAN-DBSS10:78 Initial VLAN=10, Authorization VLAN=N/A ACL Group=3000 User Profile=N/A CAR=Disable Priority=Disable Start=2008-09-14 17:05:38 ,Current=2008-09-14 17:05:51 ,Online=00h00m13s Total 1 connection matched. (3) Client可以访问网络8.1.0.0/16即VLAN210,其他网络资源不能访问。