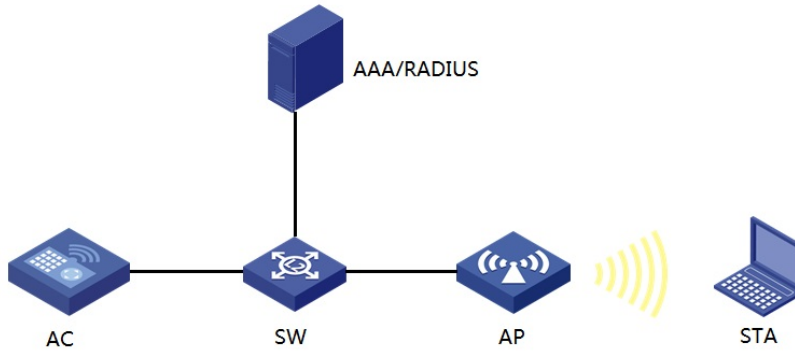


知 H3C无线控制器AC远程Portal下发ACL典型配置举例(V7)

ACL Portal 陈少华 2017-12-27 发表

- 1.AP通过交换机与AC相连,在AC开启DHCP server功能,为AP和客户端分配IP地址。
- 2.AP注册到AC上,业务网段属于vlan 161,需portal认证通过后才能访问网络资源,但是访问不能访问192.168.164.0段。

图1 AC启用portal认证对接imc实现用户接入认证



(1).AC主要配置:

```
#
portal server guest ip 192.168.21.15 port 2000 key simple portal url http://192.168.21.15:8080/portal/
server-type imc
#
acl number 3001 //下发acl的编号
description imc下发acl
rule 0 deny ip destination 192.168.164.0 0.0.0.255
rule 5 permit ip
#
vlan 161 //业务vlan
#
radius scheme 3245
server-type extended
primary authentication 192.168.21.15 key cipher $c$3$d2c4IKdo6KSApXrZLyzE9aN9Aeo/6lc=
primary accounting 192.168.21.15 key cipher $c$3$mgP$HtnU22ArZGNRyZZbGDFAA7rEjw=
user-name-format without-domain
nas-ip 192.168.160.2
domain portal
authentication portal radius-scheme 3245
authorization portal radius-scheme 3245
accounting portal radius-scheme 3245
access-limit disable
state active
idle-cut disable
self-service-url disable
#
dhcp server ip-pool 161
network 192.168.161.0 mask 255.255.255.0
gateway-list 192.168.161.1
dns-list 8.8.8.8
#
wlan service-template 10 crypto
ssid 2-portal
bind WLAN-ESS 10
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface161
```

```

ip address 192.168.161.1 255.255.255.0
portal server guest method direct
portal domain portal
portal nas-ip 192.168.161.1
#
interface WLAN-ESS10
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 161 untagged
port hybrid pvid vlan 161
mac-vlan enable
port-security port-mode psk
port-security tx-key-type 11key
port-security preshared-key pass-phrase simple 12345678
#
wlan ap wa4330-acn model WA4330-ACN id 1
serial-id 210235A1K6C161001123
radio 1
service-template 10
radio enable
#
dhcp enable
#
arp-snooping enable

```

(2). imc上主要配置

添加接入设备，密钥与设备radius方案中配置一致

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 修改接入设备

接入配置

认证端口 *	1812	计费端口 *	1813
业务类型	LAN接入业务	接入设备分组	无
接入设备类型	H3C (General)	确认共享密钥 *	****
共享密钥 *	****		

设备列表

设备名称	设备IP地址	设备型号	备注
wx5540e	192.168.160.2	H3C WX5540-WCM	

接入策略下发acl编号

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名 * portal

业务分组 * 未分组

描述

授权信息

接入时段 无

下行速率(Kbps)

优先级

普通CAP类型 EAP-MD5

EAP自协商 不启用

下发VLAN

下发User Profile

分配IP地址 * 否

上行速率(Kbps)

下发用户组

地址池

手工输入 3001

下发ACL

列表选择

接入ACL列表

创建接入服务，关联接入策略

用户 > 接入策略管理 > 接入服务管理 > 修改接入服务

基本信息

服务名 *	portal	服务后缀	
业务分组 *	未分组	缺省接入策略 *	portal
缺省安全策略 *	不使用	缺省内网外网策略 *	不使用
缺省私有属性下发策略 *	不使用	缺省单帐号最大绑定终端数 *	0
缺省单帐号最大绑定终端数 *	0	缺省单帐号在线数量限制 *	0
服务描述			
<input checked="" type="checkbox"/> 可申请	<input checked="" type="checkbox"/> 无感知认证		

创建接入用户

用户 > 接入用户 > 未分组 > 修改接入用户

接入信息

用户姓名 *	3245	帐号名 *	portal
密码 *	*****	密码确认 *	*****
<input checked="" type="checkbox"/> 允许用户修改密码	<input type="checkbox"/> 启用用户密码控制策略	<input type="checkbox"/> 下次登录须修改密码	
生效时间		失效时间	1
最大闲置时长(分钟)		在线数量限制	1
登录提示信息			
接入服务	选中相应接入服务		

portal服务器相关配置

ip地址组配置, 认证网段ip

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 修改IP地址组

修改IP地址组

IP地址组名 *	portal
起始地址 *	192.168.161.2
终止地址 *	192.168.161.254
业务分组	未分组
类型 *	普通

添加portal设备

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 修改设备信息

修改设备信息

设备名 *	5540e_portal	业务分组 *	未分组
版本 *	Portal 2.0	IP地址 *	192.168.161.1
监听端口 *	2000	本地Challenge *	否
认证重发次数 *	0	下线重发次数 *	1
支持逃生心跳 *	否	支持用户心跳 *	否
密码 *	*****	确认密码 *	*****
组网方式 *	直连		
设备描述			

vlan虚接口下的portal nas-ip

添加端口组

用户 > 接入策略管理 > Portal服务管理 > 设备配置

设备信息查询

设备名: 版本:

下发结果: 业务分组:

增加

设备名	版本	业务分组	IP地址	最近一次下发时间	下发结果	操作
yhyrp	Portal 2.0	未分组	192.168.10.1		未下发	
yhyrp20	Portal 2.0	未分组	192.168.20.1		未下发	
xhcdevice	Portal 2.0	未分组	20.1.1.1		未下发	
WAC365	Portal 2.0	未分组	192.168.21.10		未下发	
V7-PORTAL	Portal 2.0	未分组	192.168.21.7		未下发	
lan_portal	Portal 2.0	未分组	192.168.160.1		未下发	
jiangjihe_device	Portal 2.0	未分组	192.168.16.1		未下发	
fdfd	Portal 2.0	未分组	10.0.3.1		未下发	
5540e_portal	Portal 2.0	未分组	192.168.161.1		未下发	

点增加，绑定ip地址组

端口组名 *	<input type="text" value="portal"/>	提示语言 *	<input type="text" value="动态检测"/>
开始端口 *	<input type="text" value="0"/>	终止端口 *	<input type="text" value="22222"/>
协议类型 *	<input type="text" value="HTTP"/>	快速认证 *	<input type="text" value="否"/>
是否NAT *	<input type="text" value="否"/>	精英透传 *	<input type="text" value="是"/>
认证方式 *	<input type="text" value="CHAP认证"/>	IP地址组 *	<input type="text" value="portal"/>
心跳间隔(分钟) *	<input type="text" value="0"/>	心跳超时(分钟) *	<input type="text" value="0"/>
用户域名	<input type="text"/>	端口组描述	<input type="text"/>
无感知认证	<input type="text" value="不支持"/>	客户端破解 *	<input type="text" value="否"/>
页面推送策略	<input type="text"/>	融合认证页面	<input type="text"/>

验证配置:

(1).连接成功后，不能访问192.168.164.0段的ip

```
C:\Users\admin>ping 192.168.163.1
正在 Ping 192.168.163.1 具有 32 字节的数据:
来自 192.168.163.1 的回复: 字节=32 时间=1ms TTL=255

192.168.163.1 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 1ms, 最长 = 1ms, 平均 = 1ms
Control-C
^C
C:\Users\admin>ping 192.168.164.1
正在 Ping 192.168.164.1 具有 32 字节的数据:
请求超时。
```

(2).设备上显示，下发acl3001成功

```
<wx5540e>dis conn
Index=5321,Username=NGAOTksENy92TBsxdIZ5JiYWd9E= portal@portal
MAC=5C-E0-C5-AC-52-79
IP=192.168.161.2
IPv6=N/A
Online=00h07m16s
Total 1 connection(s) matched.
```

(3).通过索引查看具体信息:

```
<wx5540e>dis conn uc 5321
Index=5321, Username=NGAOTksENy92TBsxdIZ5JiYWd9E= portal@portal
MAC=5C-E0-C5-AC-52-79
IP=192.168.161.2
IPv6=N/A
Access=PORTAL ,AuthMethod=CHAP
Port Type=Wireless-802.11,Port Name=Vlan-interface161
Initial VLAN=161, Authorization VLAN=N/A
ACL Group=3001
```

User Profile=N/A

CAR=Disable

Traffic Statistic:

InputOctets =108961 OutputOctets =37550

InputGigawords=0 OutputGigawords=0

Priority=Disable

SessionTimeout=85953(s), Terminate-Action=Default

Start=2016-05-01 17:42:24 ,Current=2016-05-01 17:49:51 ,Online=00h07m27s

Total 1 connection matched.