

SecBlade IAG 配合 radius 服务器做 portal 认证典型配置

一、组网需求:

用户 PC 能够进行 portal 认证, 认证服务器为远程 radius 服务器, 认证通过后能够访问外网。

二、组网图:

//repository/38872.jpg

三、配置步骤:

IAG 版本:

H3C Comware Platform Software

Comware Software, Version 5.20, Ess 7504P13

Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.

H3C SecBlade FW uptime is 0 week, 0 day, 21 hours, 11 minutes

CPU type: RMI XLR732 1000MHz CPU

2048M bytes DDR2 SDRAM Memory

4M bytes Flash Memory

247M bytes CF0 Card

PCB Version: Ver.A

Logic Version: 3.0

Basic BootWare Version: 1.28

Extend BootWare Version: 1.29

[FIXED PORT] CON (Hardware) Ver.A, (Driver) 1.0, (Cpld) 3.0

[FIXED PORT] GE0/1 (Hardware) Ver.A, (Driver) 1.0, (Cpld) 3.0

[FIXED PORT] GE0/2 (Hardware) Ver.A, (Driver) 1.0, (Cpld) 3.0

[FIXED PORT] GE0/3 (Hardware) Ver.A, (Driver) 1.0, (Cpld) 3.0

[FIXED PORT] GE0/4 (Hardware) Ver.A, (Driver) 1.0, (Cpld) 3.0

[FIXED PORT] XGE0/0 (Hardware) Ver.A, (Driver) 1.0, (Cpld) 3.0

iMC 版本:

//repository/38877.jpg

主要配置步骤:

1. 配置 portal server;
2. 配置 radius 服务器;
3. 配置认证域;
4. 在接口下应用 portal;

? IAG 基本配置 (红色为关键配置) :

#

domain default enable system

#

portal server 8042 ip 192.168.100.12 key ccc

url http://192.168.100.12:8080/portal

portal free-rule 0 source any destination ip 121.7.0.1

```
mask 255.255.255.255
portal free-rule 1 source any destination ip 192.168.100.240
mask 255.255.255.255
#
radius scheme 8042
primary authentication 192.168.100.12 key ccc
primary accounting 192.168.100.12 key ccc
user-name-format without-domain
nas-ip 192.168.102.7
#
domain 8042
authentication portal radius-scheme 8042
authorization portal radius-scheme 8042
accounting portal radius-scheme 8042
access-limit disable
state active
idle-cut enable 10 102400
self-service-url disable
#
dhcp server ip-pool 1
network 121.7.0.0 mask 255.255.0.0
gateway-list 121.7.0.1
dns-list 192.168.100.240
expired day 0 hour 12
#
interface GigabitEthernet0/1
port link-mode route
ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/2
port link-mode route
#
interface GigabitEthernet0/3
port link-mode route
#
interface Ten-GigabitEthernet0/0
port link-mode route
#
interface Ten-GigabitEthernet0/0.2
vlan-type dot1q vid 248
ip address 121.7.0.1 255.255.0.0
arp authorized enable
dhcp update arp
portal server 8042 method direct
portal domain 8042
portal nas-ip 192.168.102.7
access-user detect type arp retransmit 2 interval 5
#
interface Ten-GigabitEthernet0/0.192
vlan-type dot1q vid 192
ip address 192.168.102.7 255.255.252.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.100.254
```

? **PC配置:**

PC IP地址无须配置，直接获取地址即可。

portal server 上首先配置到达网段121.7.0.0/16 的路由如下:

//repository/38882.jpg

? **iMC配置:**

//repository/38883.jpg

创建计费策略：

//repository/38870.jpg

创建服务（引用前面创建的计费策略）：

//repository/38874.jpg

用户及接入用户（绑定前面创建的服务）：

//repository/38876.jpg

//repository/38885.jpg



配置“业务”:

//repository/38881.jpg



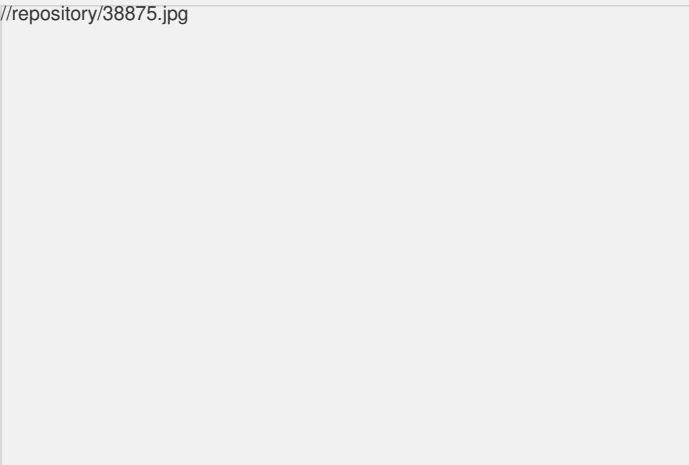
配置portal 服务器:

//repository/38878.jpg



“设备配置”, IP地址为portal nas-ip:

//repository/38875.jpg



配置“IP地址组”:

//repository/38879.jpg

在“设备配置”中指定该地址组：

//repository/38884.jpg

配置radius设备：

//repository/38871.jpg

iMC配置完成。

此时在PC机上打开IE浏览器（IE6.0以上，其它浏览器不保证功能生效），输入任意网址（若输入域名要保证该域名能够被正确解析），验证portal认证。

验证结果：

PC 浏览器弹出portal 认证页面：

//repository/38880.jpg

输入用户名和密码后，portal认证成功：

//repository/38873.jpg

在IE浏览器中再次输入正确的网址（或域名），此时能够正常访问外网。

四、配置关键点：

1. DNS服务器地址要加入到portal free-rule规则中，用户PC在认证通过之前才能够正确解析IP地址；
2. 网关地址加入到portal free-rule规则中，用户PC在认证通过之前才能够ping通网关。