

知 SecBladeIAG作为NAT网关时Portal认证典型配置

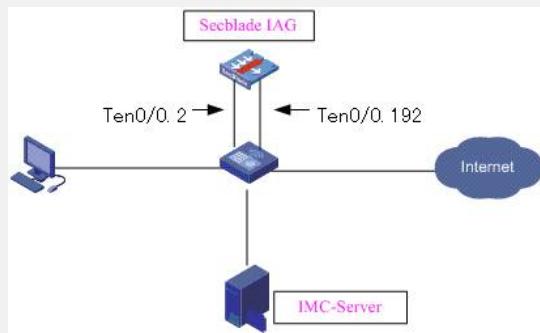
Portal NAT 张红飞 2012-05-31 发表

SecBladeIAG作为NAT网关时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，IAG上同时启用nat，用户认证通过后能够访问外网。

二、组网图:



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:



配置步骤:

1. 配置nat;

```
2. 配置认证域;
3. 配置radius 服务器;
4. 配置portal server;
5. 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
#
acl number 3000
rule 0 permit ip
#
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
nat outbound 3000
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。

? iMC配置：



创建计费策略：

创建服务（引用前面创建的计费策略）：

业务 >> 接入业务 >> 蓝牙配置管理 >> 修改服务配置

修改服务配置

基本信息

- 服务名: portal_dmn
- 服务后缀:
- 业务分组: 未分组
- 安全策略: 不使用安全策略
- 计费策略: accounting_dmn
- 服务描述:
- LDAP优先级: 1
- 可申请

授权信息

- 准入时段: 无
- 下行速率: Kbps
- 上行速率: Kbps
- 优先级:
- 启用RSA认证
- 证书认证: 不启用
- EAP证书认证: WPA证书认证
- 认证证书类型: EAP-TLS/U2F
- 分配IP地址: 否
- 下发VLAN

版权所有 © 2007-2010 杭州华三通信技术有限公司，保留一切权利。

用户及接入用户（绑定前面创建的服务）：

用户管理 >> 用户 >> 修改接入用户

接入用户

接入信息

- 用户名: 0001
- 帐号名: 0001
- 密码: *****, 密码确认: *****
- 允许用户修改密码
- 启用用户密码控制策略
- 下次登录修改密码
- 失效日期: 2010-01-01
- 最大闲置时长: 分钟
- 在线数量限制: 1
- 帐号类型: 预付货号
- 预付金额: 9999999.00 元
- 自动充值: 允许
- 登录提示信息:

接入服务

服务名	服务后缀	安全策略	状态	计费策略	用户的地址
portal_dmn		可申请	accounting_dmn		

版权所有 © 2007-2010 杭州华三通信技术有限公司，保留一切权利。

H3C Intelligent Management Center

我的快捷

首页 **资源** **用户** **业务** **告警** **报表** **系统管理** **帮助**

用户管理 >> 所有接入用户

接入用户查询

帐号名	用户名	用户分组	服务名	查询	设置
0001	0001	未分组	portal_dmn		

接入用户列表

帐号名	用户名	用户分组	帐号类型	当余额(元)	失效日期	状态	修改
0001	0001	未分组	预付费	9999997.51	正常		
0002	0002	未分组	预付费	9999999.00	正常		
0003	0003	未分组	预付费	9999999.00	正常		
0004	0004	未分组	预付费	9999999.00	正常		
0005	0005	未分组	预付费	9999999.00	正常		
0006	0006	未分组	预付费	9999999.00	正常		
0007	0007	未分组	预付费	9999999.00	正常		

共有5,000条记录, 当前第1-50, 第1/100页。 每页显示: 8 15 [50] 100 200

版权所有 © 2007-2010 杭州华三通信技术有限公司，保留一切权利。

配置“业务”：

H3C Intelligent Management Center

我的快捷

首页 **资源** **用户** **业务** **告警** **报表** **系统管理** **帮助**

业务 >> 接入业务 >> Portal服务管理

Portal服务管理简介

Portal是一种认证客户机和BAS设备之间的信息交互协议，主要应用于基于WEB的宽带接入认证系统中，完成用户的认证和授权。Portal服务器通过实现Portal协议来控制Portal客户端与设备之间的交互来进行用户认证，用户只有认证通过后才能在运营商的管理下访问网络资源。

基础配置 为保证Portal服务器能正常运行而设置系统参数。

设备配置 在Portal服务器中配置的用户上网接入设备信息，Portal服务器通过这些信息与设备交互。配置Portal设备首先要配置IP地址组。

IP地址组配置 IP地址对用户进行分组，Portal服务器通过用户所在的IP地址组来定位接入用户所在的设备和端口。

认证页面配置 配置用户属性与认证页面的关系，用户访问Portal服务器将重定向到认证页面。

IP地址组配置 → 设备配置 → 端口号配置

版权所有 © 2007-2010 杭州华三通信技术有限公司，保留一切权利。

配置portal 服务器：

Portal设备配置

基本信息

- 服务器IP: 192.168.100.12
- 监听端口: 50100
- 日志级别: 警告
- 丢包检测间隔: 20 秒
- 丢文请求超时: 5 秒
- 用户心跳间隔: 5 分钟
- Portal主页: http://192.168.100.12:8080/portal

高级信息

服务类型列表

服务类型标识	服务类型
	阶段

共有0条记录。

确定 刷新

“设备配置”，IP地址为portal nas-ip：

修改设备信息

设备信息

- 设备名: 192.168.102.7
- IP地址: 192.168.102.7
- 版本: Portal 2.0
- 监听端口: 2000
- 密钥: CCC
- 认证重发次数: 2
- 本地Challenge: 否
- 二次地址分配: 否
- 下线重发次数: 4
- 支持逃生心跳: 否
- 支持用户心跳: 否
- 业务分组: 未分组
- 设备描述:

确定 取消

配置“IP地址组”，启用NAT：

修改IP地址组

- IP地址组名: client_cdm
- 起始地址: 121.7.0.1
- 终止地址: 121.7.255.255
- 业务分组: 未分组
- 是否NAT: 是
- 起始NAT地址: 192.168.102.7
- 终止NAT地址: 192.168.102.7

确定 取消

在“设备配置—端口组”中指定该IP地址组：



配置radius设备：



iMC配置完成。

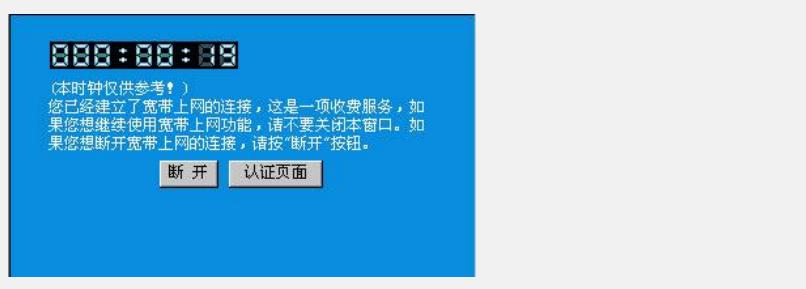
此时在PC机上打开IE浏览器（IE6.0以上，其它浏览器不保证功能生效），输入任意网址（若输入域名要保证该域名能够被正确解析），验证portal认证。

验证结果

PC浏览器弹出portal认证页面：



输入用户名和密码后，portal认证成功：



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；
3. Portal nas-ip要配置为私网网段地址。