

知 SecBlade防火墙单板作为LNS接受SecPoint L2TP 拨入的配置

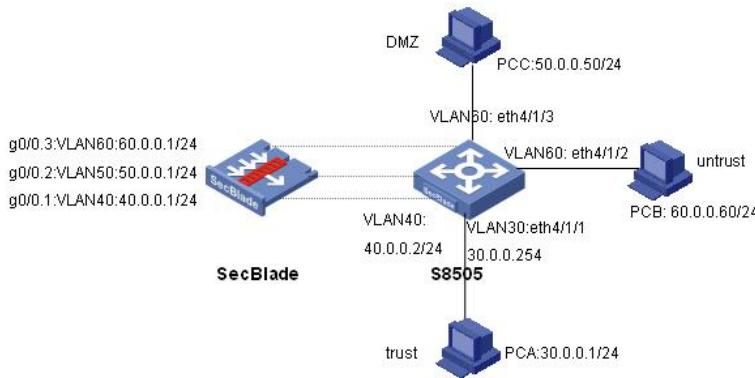
王思军 2006-09-17 发表

SecBlade防火墙单板作为LNS接受SecPoint L2TP 拨入的配置

一、组网需求：

SecBlade防火墙单板作为LNS，接受SecPoint L2TP拨入。

二、组网图：



要做LNS，SecBlade板只能工作在路由模式，S8505创建三层接口int Vlan-interface 40，作为与SecBlade的内部接口，内网PCA的网关在S8500上。PCB上安装L2TP客户端软件，通过L2TP方式拨入SecBlade，访问内部资源。

软件版本如下：

S8505: VRP310-R1271

SecBlade: VRP3.4-ESS1209

SecPoint: 5.05

三、配置步骤：

本配置适用于S8500VRP3.1-R1271及以后版本，SecBlade VRP3.4-E1209及以后版本，SecPoint3.08及以后版本。

```
1、S8500配置
<S8505>dis cu
#
config-version S8500-VRP310-r1271
#
sysname S8505
#
super password level 1 cipher O5(Yal!$LR+Q=^Q`MAF4<1!
#
local-server nas-ip 127.0.0.1 key huawei
#
Xbar load-single
#
router route-limit 128K
router VRF-limit 256
#
secblade aggregation slot 2      //配置内部端口聚合，增大带宽
#
radius scheme system
server-type huawei
primary authentication 127.0.0.1 1645
primary accounting 127.0.0.1 1646
user-name-format without-domain
#
```

```

domain system
vlan-assignment-mode integer
access-limit disable
state active
idle-cut disable
self-service-url disable

domain default enable system
#
vlan 1
#
vlan 30          //创建vlan30、vlan40、vlan50、vlan60
#
vlan 40
#
vlan 50
#
vlan 60
#
interface Vlan-interface30      //内网网关
ip address 30.0.0.254 255.255.255.0
#
interface Vlan-interface40      //与SecBlade内部三层接口
ip address 40.0.0.2 255.255.255.0
#
interface Aux0/0/1
#
interface M-Ethernet0/0/0
#
interface Ethernet4/1/1      //eth4/1/1接内网
port access vlan 30
#
interface Ethernet4/1/2      //eth4/1/2接外网
port access vlan 60
#
interface Ethernet4/1/3      //eth4/1/3接DMZ服务器
port access vlan 50
#
.... ...
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 40.0.0.1 preference 60 //通过路由，将来自内网的数据送给Secblade
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
secblade module secblade
security-vlan 50 60 //vlan50、60作为security-vlan，将来自外网和DMZ的数据送到SecBlade

secblade-interface Vlan-interface40 //vlan40为S8500与SecBlade的内部三层接口
map to slot 2      //SecBlade板在2号槽位
#
return

```

2、 SecBlade配置：
<SecBlade_FW>dis cu

sysname SecBlade_FW

```
#  
l2tp enable  
#  
firewall packet-filter enable  
firewall packet-filter default permit //包过滤缺省规则设置为permit  
#  
firewall statistic system enable  
#  
radius scheme system  
#  
domain system //注意在域下配置地址池，而不是全局下  
ip pool 1 1.1.1.2 1.1.1.254  
#  
local-user l2tp //创建l2tp用户  
password simple l2tp  
level 3  
service-type ppp  
#  
acl number 2000  
rule 0 permit source 40.0.0.0 0.255.255.255  
rule 1 permit source 30.0.0.0 0.255.255.255  
#  
interface Virtual-Template0 //创建L2TP虚模板  
ppp authentication-mode pap  
ip address 1.1.1.1 255.255.255.0  
remote address pool 1  
#  
interface Aux0  
async mode flow  
#  
interface Ethernet0/1  
#  
interface Ethernet0/2  
#  
interface Ethernet0/3  
#  
interface GigabitEthernet0/0  
#  
interface GigabitEthernet0/0.1 //与S8500的内部接口  
ip address 40.0.0.1 255.255.255.0  
vlan-type dot1q vid 40  
#  
interface GigabitEthernet0/0.2 //外网接口  
ip address 60.0.0.1 255.255.255.0  
vlan-type dot1q vid 60  
nat outbound 2000 //做nat  
nat server protocol tcp global 60.0.0.2 ftp inside 50.0.0.50 ftp //做natserver  
#  
interface GigabitEthernet0/0.3 //DMZ区域SERVER的网关  
ip address 50.0.0.1 255.255.255.0  
vlan-type dot1q vid 50  
#  
interface NULL0  
#  
firewall zone local  
set priority 100  
#  
firewall zone trust //内网接口加入trust域  
add interface GigabitEthernet0/0.1  
set priority 85  
#  
firewall zone untrust  
add interface GigabitEthernet0/0.2  
add interface Virtual-Template0 //注意将虚模板也加入untrust域
```

```

set priority 5
#
firewall zone DMZ
add interface GigabitEthernet0/0.3
set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
l2tp-group 1          //建立l2tp组
undo tunnel authentication
allow l2tp virtual-template 0
#
ip route-static 0.0.0.0 0.0.0.0 60.0.0.60 preference 60    //到公网的缺省路由
ip route-static 30.0.0.0 255.255.255.0 40.0.0.2 preference 60 //到内网的路由
#
user-interface con 0
user-interface aux 0
authentication-mode password
user-interface vty 0 4
authentication-mode scheme
#
return
<SecBlade_FW>
<SecBlade_FW>

```

3、 SecPoint的配置：

设置LNS地址：



L2TP相关设置：



因为前面选择的是“连接成功后不允许访问internet”，因此不用设置路由，否则要设置到要访问的内网网段的路由：



四、配置关键点：

- 1、SecBlade上要有到内网和外网的路由；S8500上要有到外网的路由，下一跳指向SecBlade。
- 2、注意将SecBlade子接口加入安全域，虚模板也要加入安全域。
- 3、注意在domain下配置ip pool，而不是全局下。