SecBlade防火墙单板IPSec的配置

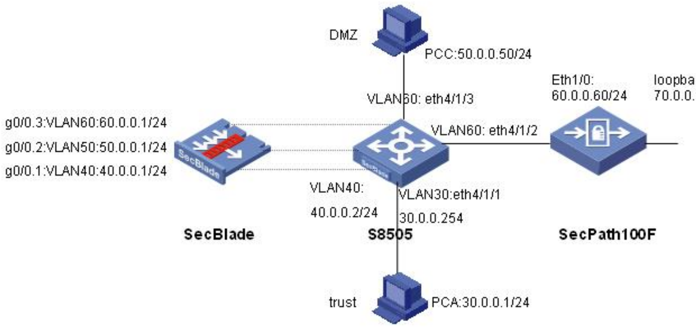
王思军 2006-10-08 发表

SecBlade防火墙单板IPSec的配置

一、 组网需求：

SecBlade防火墙单板与SecPath安全网关之间建立IPSec。

二、 组网图：



SecBlade单板和untrust区域的SecPath100F建立IPSec，保护数据流30.0.0.0/24<-->70.0.0.0/24。同时，trust区域用户能访问公网资源，DMZ区域的服务器能对外提供服务。

软件版本如下：
S8505: VRP310-R1271
SecBlade：VRP3.4-ESS1209
SecPath100F：VRP3.4-R1210

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，SecPath100F VRP3.4-E1209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(YaI!$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
#
 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
#
ike peer secpath                    //配置ike peer
 pre-shared-key 1234
 remote-address 60.0.0.60
#
ipsec proposal 1                    //配置ipsec  proposal
#
ipsec policy test 1 isakmp            //配置 ipsec policy
 security acl 3000
 ike-peer secpath
 proposal 1
#
acl number 3000                 //需要保护的数据流
 rule 0 permit ip source 30.0.0.0 0.0.0.255 destination 70.0.0.0 0.0.0.255
acl number 3001
 rule 0 deny ip source 30.0.0.0 0.0.0.255 destination 70.0.0.0 0.0.0.255//注意不要对ipsec保护的流做nat转换
 rule 1 permit ip source 40.0.0.0 0.255.255.255
 rule 2 permit ip source 30.0.0.0 0.255.255.255
#
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 3001                //做nat
 nat server protocol tcp global 60.0.0.2 ftp inside 50.0.0.50 ftp   //配置natserver
 ipsec policy test                //应用ipsec 策略
#
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                     //接口加入安全区域
 add interface GigabitEthernet0/0.1
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/0.2
 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
#
 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]
```

3、SecPath100F配置

```
<Quidway>dis cu
#
 sysname Quidway
#
 firewall packet-filter enable
 firewall packet-filter default permit        //包过滤缺省规则设置为permit
#
 insulate
#
 undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
ike peer secblade                  //配置ike peer
 pre-shared-key 1234
 remote-address 60.0.0.1
#
ipsec proposal 1                   //配置ipsec  proposal
#
ipsec policy test 1 isakmp           //配置ipsec policy
 security acl 3000
 ike-peer secblade
 proposal 1
#
acl number 3000                   //ipsec需要保护的数据流
 rule 0 permit ip source 70.0.0.0 0.0.0.255 destination 30.0.0.0 0.0.0.255
#
interface Aux0
 async mode flow
```

```
#
interface Ethernet0/0
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
 ip address 60.0.0.60 255.255.255.0
 ipsec policy test                    //应用ipsec 策略
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Encrypt2/0
#
interface NULL0
#
interface LoopBack1
 ip address 70.0.0.1 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 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
#
 ip route-static 0.0.0.0 0.0.0.0 60.0.0.1 preference 60        //到外网的缺省路由
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
<Quidway>
<Quidway>
```

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。

3、注意不要对ipsec保护的流做nat转换。