[2012-08-06]H3C S7500E+SecBlade FW LB IPS典型配置

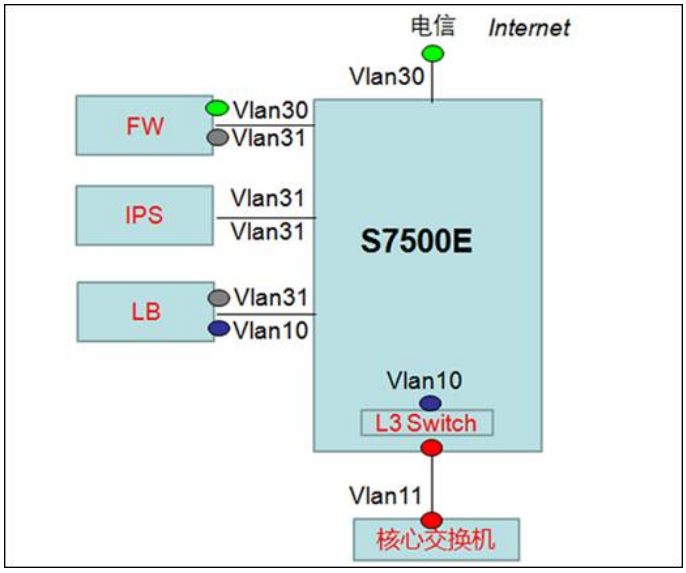
金山 2012-08-06 发表

H3C S7500E+SecBlade FW/LB/IPS典型配置

一、 组网需求：

某高校客户在校园网互联网出口区域计划部署FW、LB、IPS设备，为实现策略控制、攻击防范、链路负载分担、网络安全一体化等，采用了以S7500E交换机为载体，扩展SecBlade FW、SecBlade LB、SecBlade IPS为安全板卡的方案。在前期的具体部署上，实施了LB在外网侧，IPS在中间，FW在内网侧的拓扑结构，经过一段时间试运行，发现由于来自Internet的攻击流量频繁造成LB会话表项数量大、内存占用率高进而引起网络不稳定。为解决试行过程中发现的问题，决定变更组网拓扑为FW在外网侧、IPS在中间、LB在内网侧。在新的部署方案中，FW负责执行策略控制、NAT转换及网络层攻击防范，LB负责在多条运营商线路间为内网用户执行负载分担，IPS负责执行应用层攻击防范与病毒防范。特别地，由于LB并不与运营商线路直连，为保持LB的链路分担决策不受FW影响，处于外网侧的FW需要划分为多台虚拟防火墙，每台虚拟防火墙包含一个内网接口和一个公网接口，实现与各条运营商线路一一对应。

二、 组网图：



如上图所示：主体为一台S7500E交换机作为校园网互联网出口设备。交换机上除了一块GP12SC业务板外，还安装有SecBlade FW、SecBlade LB、SecBlade IPS安全板卡各一块。校园网内部核心交换机与S7500E通过VLAN 11三层互联，S7500E通过VLAN 10与LB内网口三层互联。FW划分四台虚拟防火墙，与四条运营商线路连接：电信400M、电信1000M、联通200M、教育网200M，虚拟防火墙的外网接口分别对应FW的VLAN 30、VLAN 40、VLAN 50、VLAN 60，内网接口分别对应FW的VLAN 31、VLAN 41、VLAN 51、VLAN 61，与LB互联（图上仅标出VLAN 30和VLAN 31示意）。IPS以OAA方式部署在FW和LB之间，对应四个互联VLAN创建4个段，对内网与外网之间互访流量执行安全检查。

交换机版本：Comware Software, Version 5.20, Release 6635
防火墙插卡版本：Comware Software, Version 5.20, Release 3166P06
LB插卡版本：Comware Software, Version 5.20, Feature 3206P02
IPS插卡版本：i-Ware software, Version 1.10, Ess 2110P10

三、 配置步骤：

S7500E交换机关键配置：

```
#
 acfp server enable                          //OAA引流必配项，使能交换机ACFP协议。
#
 acsei server enable                         //OAA引流必配项，使能交换机ACSEI协议。
#
switch-mode l2-enhanced                      //OAA引流必配项，使能主控板二层增强模式。
switch-mode normal slot 3
switch-mode normal slot 4
switch-mode normal slot 5
switch-mode normal slot 6
#
vlan 1
#
```

```
vlan 10                                    //S7500E与LB互联VLAN。
 description To_LB
#
vlan 11                                    //S7500E与核心交换机互联VLAN。
 description To_S12508
#
vlan 30
 description To_CTC400M                     //电信400M与对应虚拟防火墙互联VLAN。
#
vlan 31                                    //电信400M虚拟防火墙与LB互联VLAN。
#
vlan 40                                    //电信1000M与对应虚拟防火墙互联VLAN。
 description To_CTC1000M
#
vlan 41                                    //电信1000M虚拟防火墙与LB互联VLAN。
#
vlan 50
 description To_CNC200M                     //联通200M与对应虚拟防火墙互联VLAN。
#
vlan 51                                    //联通200M虚拟防火墙与LB互联VLAN。
#
vlan 60                                    //教育网100M与对应虚拟防火墙互联VLAN。
 description To_EDU200M
#
vlan 61                                    //教育网100M虚拟防火墙与LB互联VLAN。
#
vlan 1113                                   //OAA Server VLAN。
 description IPS_OAA
#
interface Vlan-interface10                  //与LB互联VLAN接口。
 description To_LB
 ip address 10.255.255.18 255.255.255.252
#
interface Vlan-interface11                  //与内网核心交换机互联VLAN接口。
 description To_S12508
 ip address 172.16.150.42 255.255.255.252
#
interface Vlan-interface1113                //OAA Server VLAN接口，与IPS交互ACFP协议。
 description OAA_Server
 ip address 172.16.150.45 255.255.255.252
#
interface GigabitEthernet3/0/1              //S7500E与内网核心交换机互联物理接口。
 port link-mode bridge
 description to_S12508
 port access vlan 11
#
interface GigabitEthernet3/0/9              //S7500E电信1000M线路物理接口。
 port link-mode bridge
 description To_CTC1000M
 port access vlan 40
 speed 1000
 duplex full
#
interface GigabitEthernet3/0/10             //S7500E电信400M线路物理接口。
 port link-mode bridge
 description To_CTC400M
 port access vlan 30
 speed 1000
 duplex full
#
interface GigabitEthernet3/0/11             //S7500E联通200M线路物理接口。
 port link-mode bridge
 description To_CNC200M
 port access vlan 50
```

```
 speed 1000
 duplex full
#
interface GigabitEthernet3/0/12                 //S7500E教育网100M线路物理接口。
 port link-mode bridge
 description To_EDU200M
 port access vlan 60
 speed 1000
 duplex full
#
interface Ten-GigabitEthernet4/0/1                  // S7500E与LB互联接口。
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 31 41 51 61
#
interface Ten-GigabitEthernet4/0/2
 port link-mode bridge
#
interface Ten-GigabitEthernet5/0/1                  // S7500E与IPS互联接口。
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 31 41 51 61 1113    //允许IPS监控的VLAN和OAA VLAN通过。
 port trunk pvid vlan 1113                  //设置PVID为OAA Server所在VLAN。
 port connection-mode extend                //设置端口为扩展连接模式。
 stp disable                                //禁用STP功能。
 mac-address mac-learning disable           //禁用端口MAC地址学习功能。
#
interface Ten-GigabitEthernet5/0/2
 port link-mode bridge
#
interface Ten-GigabitEthernet6/0/1                  // S7500E与FW互联接口。
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 to 31 40 to 41 50 to 51 60 to 61
#
interface Ten-GigabitEthernet6/0/2
 port link-mode bridge
#
 ip route-static 0.0.0.0 0.0.0.0 10.255.255.17              //配置Internet的缺省路由指向LB。
 ip route-static 172.16.0.0 255.255.128.0 172.16.150.41    //各个内网的明细路由指向核心。
 ip route-static 172.16.109.0 255.255.255.0 172.16.150.41
 ip route-static 172.16.192.0 255.255.224.0 172.16.150.41
 ip route-static 172.16.227.0 255.255.255.0 172.16.150.41
 ip route-static 172.17.0.0 255.255.0.0 172.16.150.41
 ip route-static 172.18.0.0 255.255.0.0 172.16.150.41
 ip route-static 210.28.84.0 255.255.252.0 172.16.150.41
 ip route-static 211.87.65.0 255.255.255.224 172.16.150.41
 ip route-static 211.87.72.0 255.255.255.0 172.16.150.41
 ip route-static 219.219.180.0 255.255.255.0 172.16.150.41
 ip route-static 219.219.188.0 255.255.252.0 172.16.150.41
#
 snmp-agent                                 //配置SNMP V3用户，OAA引流必配。
 snmp-agent local-engineid 800063A203C4CAD935069E
 snmp-agent community read wang
 snmp-agent community write wangwang
 snmp-agent sys-info version all
 snmp-agent group v3 v3group_no read-view iso write-view iso
 snmp-agent mib-view included iso iso
 snmp-agent usm-user v3 v3user_no v3group_no
#
 ip urpf strict                             //选配交换机URPF，防止源地址欺骗攻击。
```

#
交换机作为出口互联设备，既提供了连接核心交换机、互联网出口线路的物理接口，也提供了安全板卡的工作平台，在网络安全一体化中扮演网络部分的角色。

SecBlade LB CLI关键配置：

```
#
 undo alg all                                  //LB不执行NAT，关闭ALG提高转发性能。
#
 acl number 3100                    //配置固定走联通线路的目的地址，与虚服务ACL配合。
 description to_CNC
 rule 5 permit ip destination 1.24.0.0 0.7.255.255
 rule 10 permit ip destination 1.56.0.0 0.7.255.255
 rule 15 permit ip destination 1.188.0.0 0.3.255.255
 rule 20 permit ip destination 27.8.0.0 0.7.255.255
acl number 3200                    //配置固定走电信线路的目的地址，与虚服务ACL配合。
 description to_CTC1000
 rule 5 permit ip destination 1.12.0.0 0.3.255.255
 rule 10 permit ip destination 1.48.0.0 0.1.255.255
 rule 15 permit ip destination 1.68.0.0 0.3.255.255
 rule 20 permit ip destination 1.180.0.0 0.3.255.255
acl number 3201                    //配置固定走电信线路的目的地址，与虚服务ACL配合。
 description to_CTC400
 rule 5 permit ip destination 1.12.0.0 0.3.255.255
 rule 10 permit ip destination 1.48.0.0 0.1.255.255
 rule 15 permit ip destination 1.68.0.0 0.3.255.255
 rule 20 permit ip destination 1.180.0.0 0.3.255.255
acl number 3300                    //配置固定走教育网线路的源地址，与虚服务ACL配合。
 description to_EDU
 rule 5 permit ip source 210.28.80.0 0.0.0.255
 rule 10 permit ip source 210.28.81.0 0.0.0.255
 rule 15 permit ip source 210.28.82.0 0.0.0.255
 rule 20 permit ip source 210.28.83.0 0.0.0.255
#
interface Ten-GigabitEthernet0/0
 port link-mode route
 sub-interface rate-statistic               //万兆内联口使用路由模式，并启用子接口统计功能。
#
interface Ten-GigabitEthernet0/0.10        //与S7500E互联子端口。
 description to_S7500E_XBOX
 vlan-type dot1q vid 10
 ip address 10.255.255.17 255.255.255.252
#
interface Ten-GigabitEthernet0/0.31        //与电信400M虚拟防火墙互联子端口。
 description CTC400
 vlan-type dot1q vid 31
 ip address 10.255.255.2 255.255.255.252
#
interface Ten-GigabitEthernet0/0.41        //与电信1000M虚拟防火墙互联子端口。
 description CTC1000
 vlan-type dot1q vid 41
 ip address 10.255.255.6 255.255.255.252
#
interface Ten-GigabitEthernet0/0.51        //与联通200M虚拟防火墙互联子端口。
 description CNC
 vlan-type dot1q vid 51
 ip address 10.255.255.10 255.255.255.252
#
interface Ten-GigabitEthernet0/0.61        //与教育网100M虚拟防火墙互联子端口。
 description EDU
 vlan-type dot1q vid 61
 ip address 10.255.255.14 255.255.255.252
#
 ip route-static 0.0.0.0 0.0.0.0 10.255.255.1
```

```
 ip route-static 0.0.0.0 0.0.0.0 10.255.255.5
 ip route-static 0.0.0.0 0.0.0.0 10.255.255.9
 ip route-static 0.0.0.0 0.0.0.0 10.255.255.13
 ip route-static 10.255.255.20 255.255.255.252 10.255.255.13
 ip route-static 60.191.123.0 255.255.255.0 10.255.255.5 description H3C_Hangzhou
 ip route-static 65.55.21.15 255.255.255.255 10.255.255.5 description NTP_Server
 ip route-static 122.96.93.145 255.255.255.255 10.255.255.9 description CNC
 ip route-static 172.16.0.0 255.255.128.0 10.255.255.18
 ip route-static 172.16.138.0 255.255.255.0 10.255.255.18
 ip route-static 172.16.139.0 255.255.255.0 10.255.255.18
 ip route-static 172.16.150.0 255.255.255.0 10.255.255.18
 ip route-static 172.16.192.0 255.255.224.0 10.255.255.18
 ip route-static 172.16.255.81 255.255.255.255 10.255.255.13 description EDU
 ip route-static 172.17.0.0 255.255.0.0 10.255.255.18
 ip route-static 172.18.0.0 255.255.0.0 10.255.255.18
 ip route-static 210.28.80.0 255.255.248.0 10.255.255.18
 ip route-static 211.87.65.0 255.255.255.224 10.255.255.18
 ip route-static 211.87.72.128 255.255.255.128 10.255.255.18
 ip route-static 218.94.28.81 255.255.255.255 10.255.255.1 description CTC400
 ip route-static 218.94.119.225 255.255.255.255 10.255.255.5 description CTC1000
 ip route-static 219.219.180.0 255.255.255.0 10.255.255.18
 ip route-static 219.219.188.0 255.255.252.0 10.255.255.18
#
 ntp-service unicast-server 65.55.21.15
#
 arp static 10.255.255.1 3822-d629-103f                  //绑定静态ARP，提升快转性能。
 arp static 10.255.255.5 3822-d629-103f
 arp static 10.255.255.9 3822-d629-103f
 arp static 10.255.255.13 3822-d629-103f
 arp static 10.255.255.18 c4ca-d935-069e
```

SecBlade LB命令行部分的配置主要包括基本的接口及路由配置。
在接口配置方面，出方向链路负载均衡虚服务通常希望启用“链路带宽繁忙保护”功能，因此必须将LB的业务接口配置为三层万兆子接口，并启用子接口统计功能。
路由配置方面，由于LB位于公网出口位置，路由信息相对比较简单，建议采用静态配置方式。缺省路由指向公网下一跳，在本案例中即4个虚拟防火墙的内网接口地址；将内网网段聚合后，配置聚合路由指向内网，下一跳为核心交换机。准确完成路由配置，一方面可以保证LB正常转发报文，另一方面可以指导后续出方向链路负载均衡的配置。
ARP配置方面，由于LB内网方向下一跳和公网方向下一跳设备分别为核心交换机和防火墙，网络结构相对稳定，建议将ARP条目全部绑定为静态表项，除可以避免ARP震荡外，更重要的是可以提升设备快转性能。

SecBlade LB Web关键配置：
为实现出方向链路负载均衡，首先应配置物理链路。

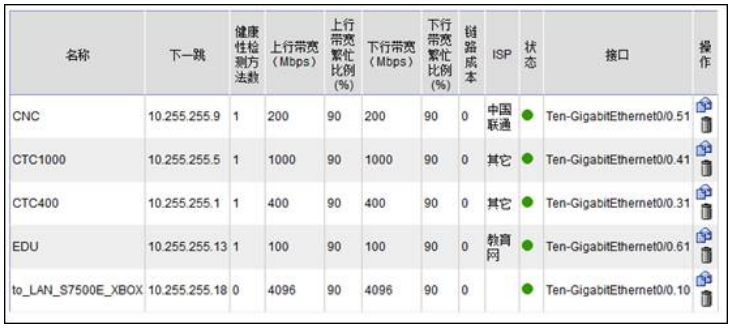
以电信400M线路为例，对应的与LB直连的防火墙地址为10.255.255.1/30。由于这个地址不是运营商设备出口地址，因此在选择健康性检测方法时，需要配置一个自定义的健康性检测方法，检测的地址为电信400M虚拟防火墙外侧的运营商地址。通过之前的配置可以看到，LB向Internet方向配置有四条缺省路由，而LB本地发出的报文是根据路由表逐包分担的，因此必须为4个运营商的出口下一跳地址配置4条精确路由，保证健康性检测的报文不会被分担到其他线路上造成探测失效。
以下是电信400M线路的健康性检测项目配置：

检测类型选择为ICMP检测，为避免线路拥塞、临时ping失败而引起的检测结果失败，造成线路状态反复震荡、不稳定，建议将检测参数值调整一下。以本案例为例，两次ping探测的检测时间间隔保持默认的5秒，超过1秒钟不响应认为本次探测失败，连续10次失败则认定健康性检测失败，进而将本条物理链路的状态设置为“红灯”。这样的设置相对于默认配置，物理线路状态出现不稳定，反复“红灯”、“绿灯”的可能性被大大降低了。

以下是静态路由的配置，CLI和Web均可以操作。其中的4条指向运营商出口下一跳地址的精确路由保证了本地发出的健康性检测报文可以按正确的一跳发送至4台虚拟报文墙上。

目的IP地址	掩码	协议	优先级	下一跳	出接口	操作
0.0.0.0	0.0.0.0	Static	60	10.255.255.1		
0.0.0.0	0.0.0.0	Static	60	10.255.255.5		
0.0.0.0	0.0.0.0	Static	60	10.255.255.9		
0.0.0.0	0.0.0.0	Static	60	10.255.255.13		
10.255.255.20	255.255.255.252	Static	60	10.255.255.13		
60.191.123.0	255.255.255.0	Static	60	10.255.255.5		
65.55.21.15	255.255.255.255	Static	60	10.255.255.5		
122.96.93.145	255.255.255.255	Static	60	10.255.255.9		
172.16.0.0	255.255.128.0	Static	60	10.255.255.18		
172.16.138.0	255.255.255.0	Static	60	10.255.255.18		
172.16.139.0	255.255.255.0	Static	60	10.255.255.18		
172.16.150.0	255.255.255.0	Static	60	10.255.255.18		
172.16.192.0	255.255.224.0	Static	60	10.255.255.18		
172.16.255.81	255.255.255.255	Static	60	10.255.255.13		

以下是完成物理线路配置后的总体情况。



名称	下一跳	健康性检测方法数	上行带宽（Mbps）	上行带宽繁忙比例（%）	下行带宽（Mbps）	下行带宽繁忙比例（%）	链路成本	ISP	状态	接口	操作
CNC	10.255.255.9	1	200	90	200	90	0	中国联通	●	Ten-GigabitEthernet0/0.51	
CTC1000	10.255.255.5	1	1000	90	1000	90	0	其它	●	Ten-GigabitEthernet0/0.41	
CTC400	10.255.255.1	1	400	90	400	90	0	其它	●	Ten-GigabitEthernet0/0.31	
EDU	10.255.255.13	1	100	90	100	90	0	教育网	●	Ten-GigabitEthernet0/0.61	
to_LAN_S7500E_XBOX	10.255.255.18	0	4096	90	4096	90	0		●	Ten-GigabitEthernet0/0.10	

在LB设备上导入运营商内置表项后，LB支持在进行流量调度时，根据会话的目的地址，直接将会话调度至相应的物理链路上。在本案例中，联通200M和教育网100M线路分别配置了对应的运营商属性，当LB收到会话首包进行选路时，便可以直接将访问中国联通和教育网的流量分发到对应的物理线路上。电信线路的带宽比较大，客户希望由电信线路多承担业务流量，可以将电信线路的运营商属性配置为其它，其含义是当LB收到会话首包后进行选路时，如果报文的目的地址既不是联通，也不是教育网，那么就通过两条电信的线路转发出去。4条公网方向的物理链路都需要配置实际带宽大小和链路繁忙比例，为后续的链路带宽繁忙保护功能做准备。

指向内网的物理链路对应着LB与S7500E之间的连接，且仅有一条，不配置健康性检测和运营商属性，带宽值保持默认的10G即可。

物理链路配置完成后，进行逻辑链路组的配置。

在出方向负载均衡配置中，一条逻辑链路组对应一个虚服务，我们以指向公网和指向内网的两个逻辑链路组为例。

上面是指向公网的逻辑链路组，为保证同一个内网用户访问Internet的资源时不会出现NAT转换后源地址忽而电信、忽而联通的情况，通常建议选择调度算法为源地址散列。逻辑链路故障处理建议选择保持已有连接，在这种配置下，LB进行报文转发时可以启用快转，大大提升转发性能。如果选择另外两种方式，LB只能通过慢转进行报文转发，性能有下降。除非特殊情况，不要选择其他两种方式。在高级配置中有温暖上线功能，该功能主要用于服务器负载均衡，在链路负载均衡中不必使能。

上面是一条指向内网的逻辑链路组，由于指向内网的物理链路只有一条，因此调度算法选择性能较好的轮转即可。建议在配置逻辑链路组时，名称和其对应的目标网段一致，后期维护或修改配置时会十分方便。

以下是完成逻辑链路组配置后的总体情况。从下图中我们不难看到，客户的组网中，在LB内侧，也包括一些配置有公网地址的网段，通常是服务器区。

逻辑链路组配置完成后，进行逻辑链路的配置，仍然以电信400M线路为例。

配置选择本逻辑链路对应的逻辑链路组，即“Internet”，选择对应的物理链路，即“CTC400”。支持配置ACL，在本例中为ACL 3201，其作用是使满足ACL 3201的新建会话由LB调度至电信400M线路。权值可以起到反映链路状态、调节调度决策的作用，两条电信线路带宽大小不同，为使流量根据带宽比进行分担，可以为每条线路配置不同的权值大小。本案例中，电信400M线路的权值配置为80，而电信1000M线路的权值配置为200，这样LB在调度时可以实现2：5的比例关系。

使用同样的方法，配置指向内网的逻辑链路组所包含的逻辑链路。由于一个虚服务只能对应一个逻辑链路组，因此必须为每个虚服务创建相应的逻辑链路。在新建逻辑链路时，物理链路可以重复“利用”。在本案例中，每一条指向内网的逻辑链路都关联了指向S7500E的物理链路。和逻辑链路组类似，建议将逻辑链路名配置与对应的目前网络相关，方便后续的维护。

全部逻辑链路配置完成后如下图所示，当逻辑链路对应的虚服务UP（亮绿灯）后，逻辑链路的状态也才会UP（亮绿灯）。

当逻辑链路组和逻辑链路都配置完成后，便可以进行虚服务的配置了。

虚服务的具体配置如下例。

上图所示为指向公网的虚服务，匹配方式为IP地址方式，除特殊需求外建议以IP地址方式进行配置。虚服务地址为全零，掩码为零，协议任意，端口号为零。这条需服务与路由表中的缺省路由类似，当LB收到会话首包后，如果不能命中掩码更长的虚服务，便会以这条虚服务对报文进行处理。

在本案例中，虚服务与“Internet”逻辑链路组对应，勾选使能虚服务、使能ISP选路、使能链路繁忙保护。就近性功能由于性能方面的原因，不推荐开启。当虚服务使能后，LB将按照由高到低的顺序对收到的会话首包进行负载均衡决策：持续性、ACL、ISP、就近性、调度算法。当某条链路带宽值达到繁忙比后，链路带宽繁忙保护功能可以影响ISP、就近性、调度算法，避免新的会话被调度到这条链路进一步加重拥塞。

上图是一个指向内网的虚服务，配置时仅需指定虚服务IP地址、掩码、协议、端口、对应的逻辑链路组和使能虚服务即可，其他功能都不必配置。指向内网的虚服务主要是为由外网主动发起的会话而准备的，在本案例中，由于外网侧的防火墙配置有NAT Server和NAT Static，公网侧用户需要访问内网服务器，如果不配置指向内网的虚服务，当防火墙执行NAT Server后将报文转发至LB，该报文会匹配全零的虚服务而被“弹”回公网。如果局点并没有从外至内的访问业务，全部都是从内网发起访问外网的，那么不配置指向内网的虚服务也是可以的。

新建会话的首包到达LB后，LB在全部虚服务中按最长匹配原则进行匹配，然后再根据相应的虚服务配置进行负载均衡决策。不难看到，虚服务配置完成后，与LB上的路由表项是一致的。虚服务配置完成后如下图所示：

LB上线运行后，可以通过统计信息查看每条虚服务的工作情况：

虚服务名	总连接数	活动连接数/连接数峰值	连接速率/速率峰值（个/秒）	入方向转发/忽略报文数	出方向转发报文数	操作
Internet	9434374861	55751 / 847466	1048 / 28001	324126928106 / 0	309878048801	
to_10.255.255.1	275378	5 / 123	0 / 46	9778605 / 0	9940450	
to_10.255.255.13	9322	0 / 5	0 / 2	330986 / 0	331316	
To_10.255.255.20_IPS	2546371	3 / 30	0 / 16	12300534 / 0	12792573	
to_10.255.255.5	35930	0 / 63	0 / 44	67419 / 0	69078	
to_10.255.255.9	162264	0 / 26	0 / 18	241332 / 4473	241310	
to_172.16.0.0	954515	53 / 635	0 / 196	1206467603 / 0	171936470	
to_172.16.138.0	0	0 / 0	0 / 0	0 / 0	0	
to_172.16.139.0	0	0 / 0	0 / 0	0 / 0	0	
to_172.16.150.0	258971	1 / 279	0 / 213	22358792 / 0	15460835	
to_172.16.192.0	160730	1 / 99	0 / 33	17589653 / 0	14211821	
to_172.17.0.0	207985	9 / 131	0 / 112	29184522 / 0	23065084	
to_172.18.0.0	0	0 / 0	0 / 0	0 / 0	0	
to_210.28.80.0	1316886536	5496 / 45767	135 / 39656	5766703112 / 0	7520405735	

也可以详细查看每一个虚服务的负载分担情况：

虚服务名	总连接数	活动连接数/连接数峰值	连接速率/速率峰值（个/秒）	入方向转发/忽略报文数	出方向转发报文数	操作
Internet	9434444501	56313 / 847466	988 / 28001	324130636475 / 0	309881956487	

逻辑链路名	总连接数	活动连接数/连接数峰值	连接速率/速率峰值（个/秒）	接收报文数	发送报文数	入方向速率（kbps）	出方向速率（kbps）
Internet_CNC	383394260	3765 / 669911	63 / 27077	42704953917	42711496996	34146	25854
Internet_CTC1000	2122264729	35404 / 834488	652 / 27633	147970980556	141989607063	212932	419359
Internet_CTC400	638082764	4897 / 24499	99 / 4882	47475144079	46560925810	47809	27591
Internet_EDU	6090391174	12248 / 583714	174 / 27182	61571191584	55289336925	907	2152

在LB配置部分的最后，推荐一个配置技巧。为了在查看LB处理的每条会话的具体分发情况，可以先为LB的每个接口加入不同的安全区域，然后在查看会话表详细信息时就可以直接了解到LB将这条会话分担至哪条运营商线路了。

下图显示了在LB上新建4个以运营商线路命令的安全区域后，为每个公网接口和内网接口加入了不同的安全区域：

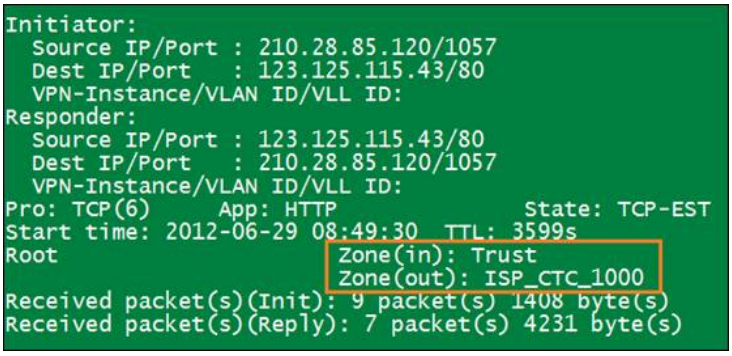
名称	IP地址	网络掩码	安全域	状态	操作
GigabitEthernet0/1			-		
GigabitEthernet0/2			-		
GigabitEthernet0/3			-		
GigabitEthernet0/4			-		
NULL0			-		
Ten-GigabitEthernet0/0			-		
Ten-GigabitEthernet0/0.10	10.255.255.17	255.255.255.252	Trust		
Ten-GigabitEthernet0/0.31	10.255.255.2	255.255.255.252	ISP_CTC_400		
Ten-GigabitEthernet0/0.41	10.255.255.6	255.255.255.252	ISP_CTC_1000		
Ten-GigabitEthernet0/0.51	10.255.255.10	255.255.255.252	ISP_CNC_100		
Ten-GigabitEthernet0/0.61	10.255.255.14	255.255.255.252	ISP_EDU_100		

共11条，每页 30 条 | 当前：1/1页，1-11条 | 首页 上一页 下一页 尾页 1 跳转

新建

然后在查看LB会话时，便可以在会话详细信息中，根据会话的入区域和出区域确认报文的来源以及报文被分担至哪条线路。

会话表详细信息如下图所示。



```
Initiator:
  Source IP/Port : 210.28.85.120/1057
  Dest IP/Port   : 123.125.115.43/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 123.125.115.43/80
  Dest IP/Port   : 210.28.85.120/1057
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: HTTP                  State: TCP-EST
Start time: 2012-06-29 08:49:30  TTL: 3599s
Root                          Zone(in): Trust
                              Zone(out): ISP_CTC_1000
Received packet(s)(Init): 9 packet(s) 1408 byte(s)
Received packet(s)(Reply): 7 packet(s) 4231 byte(s)
```

SecBlade FW CLI关键配置：

```
#
 nat address-group 0 218.94.128.105 218.94.128.110 level 1          //NAT地址池配置。
 nat address-group 1 58.213.14.66 58.213.14.110 level 1
 nat address-group 2 122.96.93.129 122.96.93.133 level 1
 nat address-group 3 211.87.71.2 211.87.71.125 level 1
#
```

```
 userlog flow export version 3                                          //Userlog版本配置。
 userlog flow export vpn-instance CTC400 host 172.16.109.51 30017      //Userlog日志主机。
#
 undo alg dns                                          //关闭除FTP协议外的其他协议ALG功能。
 undo alg rtsp
 undo alg h323
 undo alg sip
 undo alg sqlnet
 undo alg pptp
 undo alg ils
 undo alg nbt
 undo alg msn
 undo alg qq
 undo alg tftp
 undo alg sccp
 undo alg gtp
#
ip vpn-instance CTC400                                 //VPN实例实现路由隔离，配合虚拟防火墙。
 route-distinguisher 65001:1
#
ip vpn-instance CTC1000
 route-distinguisher 65001:2
#
ip vpn-instance CNC
 route-distinguisher 65001:3
#
ip vpn-instance EDU
 route-distinguisher 65001:4
#
acl number 2001                                          //VPN实例内NAT ACL配置。
 description NAT_ACL_CTC400
 rule 5 permit vpn-instance CTC400 source 211.87.72.128 0.0.0.127
 rule 15 permit vpn-instance CTC400 source 172.16.0.0 0.0.255.255
 rule 20 permit vpn-instance CTC400 source 172.17.0.0 0.0.255.255
 rule 25 permit vpn-instance CTC400 source 172.18.0.0 0.0.255.255
 rule 30 permit vpn-instance CTC400 source 210.28.84.0 0.0.3.255
 rule 35 permit vpn-instance CTC400 source 219.219.180.0 0.0.0.255
 rule 40 permit vpn-instance CTC400 source 219.219.188.0 0.0.3.255
 rule 1005 permit vpn-instance CTC400 source 10.255.255.2 0
acl number 2002
 description NAT_ACL_CTC1000
 rule 5 permit vpn-instance CTC1000 source 211.87.72.128 0.0.0.127
 rule 15 permit vpn-instance CTC1000 source 172.16.0.0 0.0.255.255
 rule 20 permit vpn-instance CTC1000 source 172.17.0.0 0.0.255.255
 rule 25 permit vpn-instance CTC1000 source 172.18.0.0 0.0.255.255
 rule 30 permit vpn-instance CTC1000 source 210.28.84.0 0.0.3.255
 rule 1005 permit vpn-instance CTC1000 source 10.255.255.6 0
acl number 2003
 description NAT_ACL_CNC
 rule 10 permit vpn-instance CNC source 211.87.72.128 0.0.0.127
 rule 15 permit vpn-instance CNC source 172.16.0.0 0.0.255.255
 rule 20 permit vpn-instance CNC source 172.17.0.0 0.0.255.255
 rule 25 permit vpn-instance CNC source 172.18.0.0 0.0.255.255
 rule 30 permit vpn-instance CNC source 210.28.84.0 0.0.3.255
 rule 1005 permit vpn-instance CNC source 10.255.255.10 0
acl number 2004
 description NAT_ACL_EDU
 rule 10 permit vpn-instance EDU source 211.87.72.128 0.0.0.127
 rule 15 permit vpn-instance EDU source 172.16.0.0 0.0.255.255
 rule 20 permit vpn-instance EDU source 172.17.0.0 0.0.255.255
 rule 25 permit vpn-instance EDU source 172.18.0.0 0.0.255.255
 rule 30 permit vpn-instance EDU source 210.28.84.0 0.0.3.255
 rule 1005 permit vpn-instance EDU source 10.255.255.14 0
 rule 1010 permit vpn-instance EDU source 10.255.255.22 0
```

```
#
connection-limit policy 0                                    //连接数限制配置。
 limit 0 source ip 210.28.80.0 24 source-vpn EDU destination ip any destination-vpn EDU protocol ip
max-connections 2000 per-source
#
interface GigabitEthernet0/3                    //交换机无千兆接口，利用防火墙面板口连接IPS。
 port link-mode route
 description EDU_IPS
 ip binding vpn-instance EDU
 ip address 10.255.255.21 255.255.255.252
#
interface Ten-GigabitEthernet0/0
 port link-mode route
#
interface Ten-GigabitEthernet0/0.30          //电信400M虚拟防火墙外网接口。
 description CTC400
 vlan-type dot1q vid 30
 nat outbound 2001 address-group 0 vpn-instance CTC400
 ip binding vpn-instance CTC400
 ip address 218.94.28.82 255.255.255.252
#
interface Ten-GigabitEthernet0/0.31          //电信400M虚拟防火墙内网接口。
 description CTC400_LAN
 vlan-type dot1q vid 31
 ip binding vpn-instance CTC400
 ip address 10.255.255.1 255.255.255.252
#
interface Ten-GigabitEthernet0/0.40          //电信1000M虚拟防火墙外网接口。
 description CTC1000
 vlan-type dot1q vid 40
 nat outbound 3992 address-group 1 vpn-instance CTC1000
 nat outbound 2002 address-group 1 vpn-instance CTC1000
 nat server protocol tcp global 58.213.14.111 443 vpn-instance CTC1000 inside 172.16.150.113 443
vpn-instance CTC1000
 nat server protocol tcp global 58.213.14.111 20443 vpn-instance CTC1000 inside 10.255.255.6 www
vpn-instance CTC1000
 nat server protocol tcp global 58.213.14.111 10443 vpn-instance CTC1000 inside 10.255.255.22 ww
w vpn-instance CTC1000
 nat server protocol tcp global 58.213.14.111 10023 vpn-instance CTC1000 inside 10.255.255.22 teln
et vpn-instance CTC1000
 nat server protocol tcp global 58.213.14.111 35715 vpn-instance CTC1000 inside 10.255.255.22 357
15 vpn-instance CTC1000
 ip binding vpn-instance CTC1000
 ip address 218.94.119.226 255.255.255.252
#
interface Ten-GigabitEthernet0/0.41          //电信1000M虚拟防火墙内网接口。
 description CTC1000_LAN
 vlan-type dot1q vid 41
 nat outbound 3993
 ip binding vpn-instance CTC1000
 ip address 10.255.255.5 255.255.255.252
#
interface Ten-GigabitEthernet0/0.50          //联通200M虚拟防火墙外网接口。
 description CNC
 vlan-type dot1q vid 50
 nat outbound 2003 address-group 2 vpn-instance CNC
 ip binding vpn-instance CNC
 ip address 122.96.93.146 255.255.255.252
#
interface Ten-GigabitEthernet0/0.51          //联通200M虚拟防火墙内网接口。
 description CNC_LAN
 vlan-type dot1q vid 51
 ip binding vpn-instance CNC
 ip address 10.255.255.9 255.255.255.252
```

```
#
interface Ten-GigabitEthernet0/0.60          //教育网100M虚拟防火墙外网接口。
 description EDU
 vlan-type dot1q vid 60
 nat outbound 2004 address-group 3 vpn-instance EDU
 ip binding vpn-instance EDU
 ip address 172.16.255.82 255.255.255.252
#
interface Ten-GigabitEthernet0/0.61          //教育网100M虚拟防火墙内网接口。
 description EDU_LAN
 vlan-type dot1q vid 61
 ip binding vpn-instance EDU
 ip address 10.255.255.13 255.255.255.252
#
 ip route-static vpn-instance CTC400 0.0.0.0 0.0.0.0 218.94.28.81    //各虚墙路由配置。
 ip route-static vpn-instance CTC400 172.16.0.0 255.255.0.0 10.255.255.2
 ip route-static vpn-instance CTC400 172.17.0.0 255.255.0.0 10.255.255.2
 ip route-static vpn-instance CTC400 172.18.0.0 255.255.0.0 10.255.255.2
 ip route-static vpn-instance CTC400 210.28.84.0 255.255.252.0 10.255.255.2
 ip route-static vpn-instance CTC400 211.87.72.0 255.255.255.0 10.255.255.2
 ip route-static vpn-instance CTC400 219.219.180.0 255.255.255.0 10.255.255.2
 ip route-static vpn-instance CTC400 219.219.188.0 255.255.252.0 10.255.255.2
 ip route-static vpn-instance CTC1000 0.0.0.0 0.0.0.0 218.94.119.225
 ip route-static vpn-instance CTC1000 10.255.255.22 255.255.255.255 10.255.255.6
 ip route-static vpn-instance CTC1000 172.16.0.0 255.255.0.0 10.255.255.6
 ip route-static vpn-instance CTC1000 172.17.0.0 255.255.0.0 10.255.255.6
 ip route-static vpn-instance CTC1000 172.18.0.0 255.255.0.0 10.255.255.6
 ip route-static vpn-instance CTC1000 210.28.84.0 255.255.252.0 10.255.255.6
 ip route-static vpn-instance CTC1000 211.87.72.128 255.255.255.128 10.255.255.6
 ip route-static vpn-instance CTC1000 219.219.180.0 255.255.255.0 10.255.255.6
 ip route-static vpn-instance CTC1000 219.219.188.0 255.255.252.0 10.255.255.6
 ip route-static vpn-instance CNC 0.0.0.0 0.0.0.0 122.96.93.145
 ip route-static vpn-instance CNC 172.16.0.0 255.255.0.0 10.255.255.10
 ip route-static vpn-instance CNC 172.17.0.0 255.255.0.0 10.255.255.10
 ip route-static vpn-instance CNC 172.18.0.0 255.255.0.0 10.255.255.10
 ip route-static vpn-instance CNC 210.28.84.0 255.255.252.0 10.255.255.10
 ip route-static vpn-instance CNC 211.87.72.0 255.255.255.0 10.255.255.10
 ip route-static vpn-instance CNC 219.219.180.0 255.255.255.0 10.255.255.10
 ip route-static vpn-instance CNC 219.219.188.0 255.255.252.0 10.255.255.10
 ip route-static vpn-instance EDU 0.0.0.0 0.0.0.0 172.16.255.81
 ip route-static vpn-instance EDU 10.255.255.5 255.255.255.255 10.255.255.14
 ip route-static vpn-instance EDU 172.16.0.0 255.255.0.0 10.255.255.14
 ip route-static vpn-instance EDU 172.16.138.0 255.255.255.0 10.255.255.14
 ip route-static vpn-instance EDU 172.16.139.0 255.255.255.0 10.255.255.14
 ip route-static vpn-instance EDU 172.16.150.0 255.255.255.0 10.255.255.14
 ip route-static vpn-instance EDU 172.16.192.0 255.255.224.0 10.255.255.14
 ip route-static vpn-instance EDU 172.17.0.0 255.255.0.0 10.255.255.14
 ip route-static vpn-instance EDU 172.18.0.0 255.255.0.0 10.255.255.14
 ip route-static vpn-instance EDU 210.28.80.0 255.255.248.0 10.255.255.14
 ip route-static vpn-instance EDU 211.87.65.0 255.255.255.224 10.255.255.14
 ip route-static vpn-instance EDU 211.87.72.0 255.255.255.0 10.255.255.14
 ip route-static vpn-instance EDU 219.219.180.0 255.255.255.0 10.255.255.14
 ip route-static vpn-instance EDU 219.219.188.0 255.255.252.0 10.255.255.14
#
 info-center loghost vpn-instance CTC400 172.16.109.51 port 30514      //日志服务器配置。
#
 snmp-agent                                          //启用SNMP，配合SecCenter。
 snmp-agent local-engineid 800063A2033822D629103A
 snmp-agent community read wang
 snmp-agent community read public
 snmp-agent sys-info version all
#
 ntp-service unicast-server vpn-instance CTC1000 65.55.21.15 //启用NTP，保证日志时间准确。
#
```

```
 arp static 10.255.255.2 3822-d69c-fdba vpn-instance CTC400 //对内网设备绑定ARP表项。
 arp static 10.255.255.6 3822-d69c-fdba vpn-instance CTC1000
 arp static 10.255.255.10 3822-d69c-fdba vpn-instance CNC
 arp static 10.255.255.14 3822-d69c-fdba vpn-instance EDU
 arp static 10.255.255.22 c4ca-d935-4c56 vpn-instance EDU
#
```

防火墙命令行部分的配置，最主要的工作是配置VPN实例，实现防火墙上4对内外网接口的路由隔离。通过配合虚拟防火墙功能，将1台物理防火墙虚拟成4台虚拟防火墙，可以实现防火墙可以保持LB对链路负载分担的决策，避免LB将流量分担至某条运营商线路后，防火墙却将其转稳至另一条线路上。在命令行中可以配置的大部分功能，如创建接口、配置ACL、启用NAT等功能，在Web管理页面也可以配置，配置时可根据熟练程度，选择其中一种配置方式。

由于防火墙上配置了VPN实例，因此须注意所有的配置命令，如NAT、ACL、ARP、Userlog、Info-center、路由条目等等，则是需要配置VPN实例参数的，都必须准确配置，否则配置无法正常生效。

具体配置方面，可以为对应各条运营商线路的NAT命令，分别关联不同的ACL。每个虚拟防火墙都需要分别配置不同的地址池、路由信息等。为提高设备快转性能，防火墙配置静态路由，并将与内网设备有关的ARP表项绑定为静态表项，由于公网运营商设备有时会有切换，ARP对应的MAC地址可能会随时变化，因此在防火墙上不建议绑定公网下一跳地址的ARP表项。日志输出相关配置，如Userlog日志输出、Info-Center日志输出，仅配置由某一个VPN实例始发即可，不必在各个VPN实例中分别配置。

SecBlade FW Web关键配置：

首先在虚拟设备管理中添加4个虚拟防火墙，名称自拟。

在最新版本中，每个防火墙能够建立的会话表项数都与整机相同，为防止某个虚拟防火墙受攻击后会话表项高，继而导致内存占用率高并引发其他问题，在本例中，我们为每个虚墙分配50万。如果各个虚墙上正常运行期间会话表项数相差较多，还可以进行调整。

虚拟防火墙创建好以后，将防火墙的三层接口加入相应的虚拟防火墙中。在本例中，防火墙通过三层接口与其他设备互联，因此可以直接将三层接口划分至不同的虚拟防火墙中。如果防火墙工作在二层模式，则不能直接划分接口，而是将不同的VLAN划分至不同的虚拟防火墙中。

虚拟防火墙配置完成后，需要在“虚拟设备选择”中进行登录。在新版本中，如果登录用户账号是属于某个虚墙的，那么当网络管理员访问设备IP地址的Web页面时，输入虚拟防火墙的账号密码，则可以直接进入相应虚拟防火墙的管理页面。

登录虚拟防火墙以后，需要创建安全区域，并将划归至本防火墙的接口加入相应的安全区域。

将接口添加至安全区域后，在接口管理中可以进行检查。

安全区域配置完成后，便可以进行域间策略的配置。针对电信400M虚拟防火墙而言，该墙上只有内网用户访问外网的业务（NAT Outbound），并无外网主动通过电信400M虚拟防火墙访问内网的业务（NAT Server、NAT Static）。因此防火墙默认规则（高优先级可以主动访问低优先级安全区域）即可满足要求。

但本案例中，防火墙上线以后，我们通过观察防火墙收发报文情况，发现由于运营商及内网存在地址欺骗攻击，导致防火墙从公网口或内网口收到报文后，经查询路由表，发现该报文仍然要从原接口发送出去。这种地址欺骗造成的路由环路问题，不仅仅浪费设备性能，更重要的是它造成防火墙创建了大量的无有会话表项，进而造成内存占用率高，设备性能不稳定。为避免该问题，我们配置了两条域间策略，一条是Untrust至Untrust区域全禁止，另一条是Trust区域至Trust区域全禁止。当防火墙从公网接口收到报文，查路由表后发现该报文仍要发送加公网侧时，便会根据域间策略将其丢弃并且不创建会话表项。

经过一段时间观察，防火墙丢弃了大量的攻击性质的异常报文，保证了防火墙及业务的正常运行。

在另一台虚拟防火墙电信1000M上，由于存在外网主动防火墙内网的业务，因此需要配置从Untrust区域至Trust区域允许的策略。在配置时，注意允许访问的目标地址是NAT Server命令的inside地址，即防火墙从外网接口收到匹配NAT Server命令的会话首个报文后，先执行NAT转换，然后再将报文送至域间策略模块处理。

如果实际业务流量中三层分片报文较多，防火墙中有大量的分片泛洪攻击日志，可以适当调整虚拟分片重组功能的配置。常见方式是将分片队列数调整至最大。在某些应用场景中，由于同一个IP报文的不同三层分片到达防火墙时间差较大，还需要将分片队列老化时间适当调长。

防火墙需要输出Userlog日志，即NAT日志。如何输出至服务器在命令行配置中已经介绍过。该配置是全局的，先择从一个虚拟防火墙发出即可，该虚拟防火墙的IP地址应该是SecCenter FW Manager添加设备时的IP地址。除此之外，要真正输出Userlog日志，须在每个虚拟防火墙上配置日志输出策略，该配置不是全局的。如果仅希望观注部分业务的日志信息，可以配置ACL进行过滤。

SecBlade IPS Web关键配置：

当LB和FW配置完成后，网络的主体框架便完成了。此时即使没有部署IPS，业务也可以正常使用。因此推荐先完成LB和FW的部署和测试，然后再将IPS部署上线。

在本案例中，按规划应将IPS部署在FW和LB之间，由于上下行流量的报文在交换机上携带的是相同的VLAN Tag，且交换机没有配置IRF，是单机环境，因此使用OAA引流方案。为保证IPS不影响网络业务，选择旁路部署模式。

登录IPS Web管理页面后先检查设备版本、系统时间等。SecBlade IPS的系统时间是通过ACSEI系统由交换机同步而来的。在SecCenter IPS Manager中添加IPS设备时，如果SecCenter服务器的系统时间是当前时间，时区是GMT+8，IPS设备的系统时间是当前时间，时区是GMT，那么SecCenter的时间纠正方式必须选择“以格林威治时间处理”；如果SecCenter服务器的系统时间是当前时间，时区是GMT+8，IPS设备的系统时间是当前时间，时区也是GMT+8，那么SecCenter的时间纠正方式必须选择“以本地时间处理”。

在配置IPS安全策略前，必须先配置安全区域和段。由于本例采用OAA方式引流，因此需先配置ACFP参数。

在“OAA设置”界面，配置使能ACFP Client功能。在“OAA Client配置”中，“用户名”即交换机上配置的SNMP用户名，“OAA Server地址”即交换机上用于ACFP协议交互的VLAN虚接口地址。在内联接口配置中，“VLAN ID”为交换机内联口PVID，“IP地址/掩码”为ACFP互联时IPS的IP地址/掩码。配置完成后，通过单击“连通性测试”按钮进行配置检查。

OAA配置完成后，进行安全区域的配置时，在SecBlade IPS上便可以直接选择交换机接口作为安全区域的物理接口。在本案例中，LB与FW之间共有4条二层连接，为区分流量，共配置8个安全区域，外部安全区域选择交换机与FW互联万兆口+相应VLAN ID，内部安全区域先择交换机与LB互联万兆口+相应VLAN ID。

每两个安全区域组合形成一个段。联动策略优先级是多块IPS插卡环境，决定引流策略优先级的配置，本例中只有一块IPS插卡，可以不考虑。

以上介绍的是IPS B31平台软件的安全区域、段及引流配置，在E2113系列B35平台的软件版本中，安全区域、段和引流配置是各自独立的，配置上会有区别，具体实施时需要参考相应的配置文档指导。段配置完成后，安全策略的配置方式与盒式设备相同。直接在相应的段上下发策略即可，注意配置完成后必须激活才能生效。

SecBlade IPS默认配置为在线模式，策略下发后，交换机执行的OAA动作为重定向，此时IPS可以实现在线阻断攻击等功能。在本案例中，由于IPS设备在线处理报文会增加业务流量的时延，当IPS设备负载较高时对业务会有影响，因此采用旁路模式部署。当IPS工作在旁路模式时，交换机执行的OAA动作为镜像，此时业务报文在交换机上是直接转发的，仅仅镜像一份流量给IPS，IPS可以实现IDS的功能，输出监控日志。

建议当IPS工作在旁路模式时，修改阻断动作为不发送RST报文，默认配置下是发送的。这样可以避免当IPS检测到阻断事件时，发送的RST报文影响业务。

SecBlade IPS部署上线后，可以在系统状态页直接观察到设备运行情况。

四、 配置关键点：

详见配置过程说明。