# M9000多业务板卡部署配置指导-单框(IPS+ACG+LB+FW)

张泷文 2014-08-13 发表

M9000产品多业务板卡配置案例

单框（IPS+ACG+LB+FW)

一、组网需求：

在本案例组网设计中， M9000和安全插卡都为单机部署，使用静态路由协议。LB插卡与上游设备建立三层连接关系，提供出方向的链路负载均衡功能。FW插卡与M9000和LB建立三层连接关系，M9000对下再与园区核心或数据中心核心连接。插卡组合顺序为经过防火墙->LLB—>ACG—>IPS—>内部网络。该组网特点为外网出入方向的流量全部都经过LB和FW，防火墙可以在前端保护LB设备，防止攻击流量到LB上。

**流量走向**

在本案例组网设计中，根据测试环境需要，LB内部使用明细路由，LB外部使用默认路由。IPS和ACG流量通过MQC方式重定向。FW由于有多出口，使用虚拟防火墙隔离并三层转发。内网网段为172.16.0.0/16，下行内网网关为10.1.1.3.

实际应用时，防火墙如在LB后方，可以直接走三层转发。在LB前方，可以每个物理FW或者虚拟FW转发一个出口。

**实验版本列表**

开局时,除M9000必须使用9105版本外，其他产品请使用总部推荐的最新版本。

| 设备 | 版本 |
| --- | --- |
| M9000 | Comware Software, Version 7.1.045, Demo 9105 |
| SecBlade FW Enhanced | Comware software, Version 5.20, Release 3819P05 |
| SecBlade LB | Comware software, Version 5.20, Feature 3226 |
| SecBlade IPS Enhanced | i-Ware software, Version 1.10, Release 3807P01 |
| SecBlade ACG | i-Ware software, Version 1.10, E6119P03 |

二、组网图：

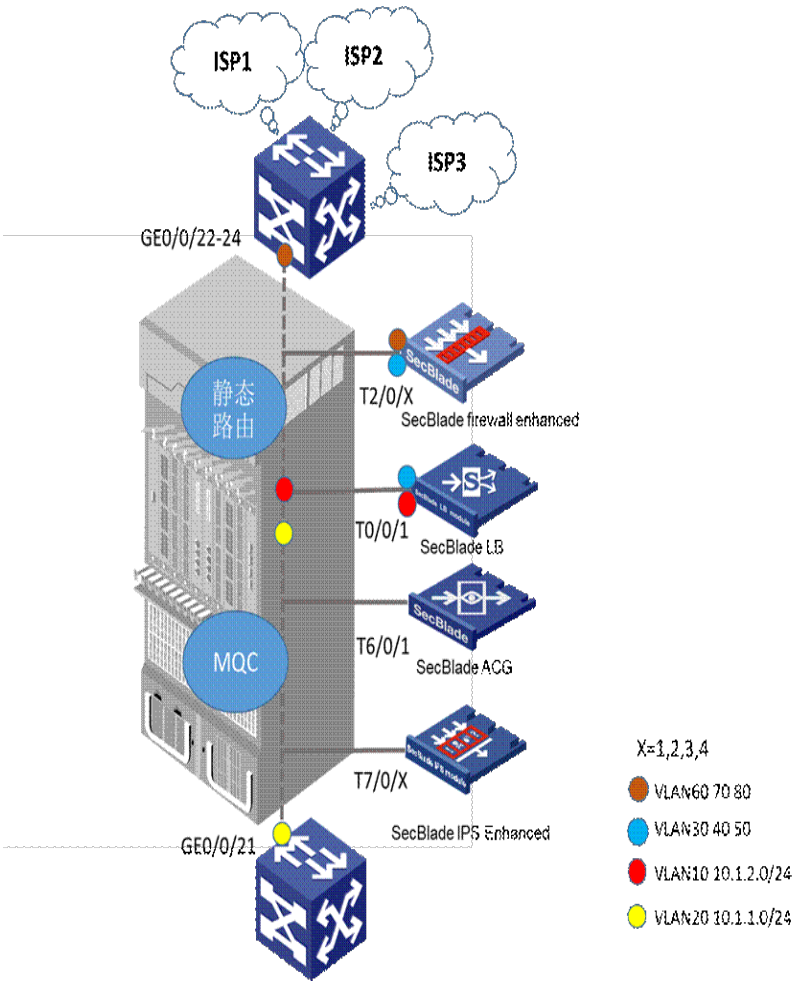



图1 案例组网网络结构图

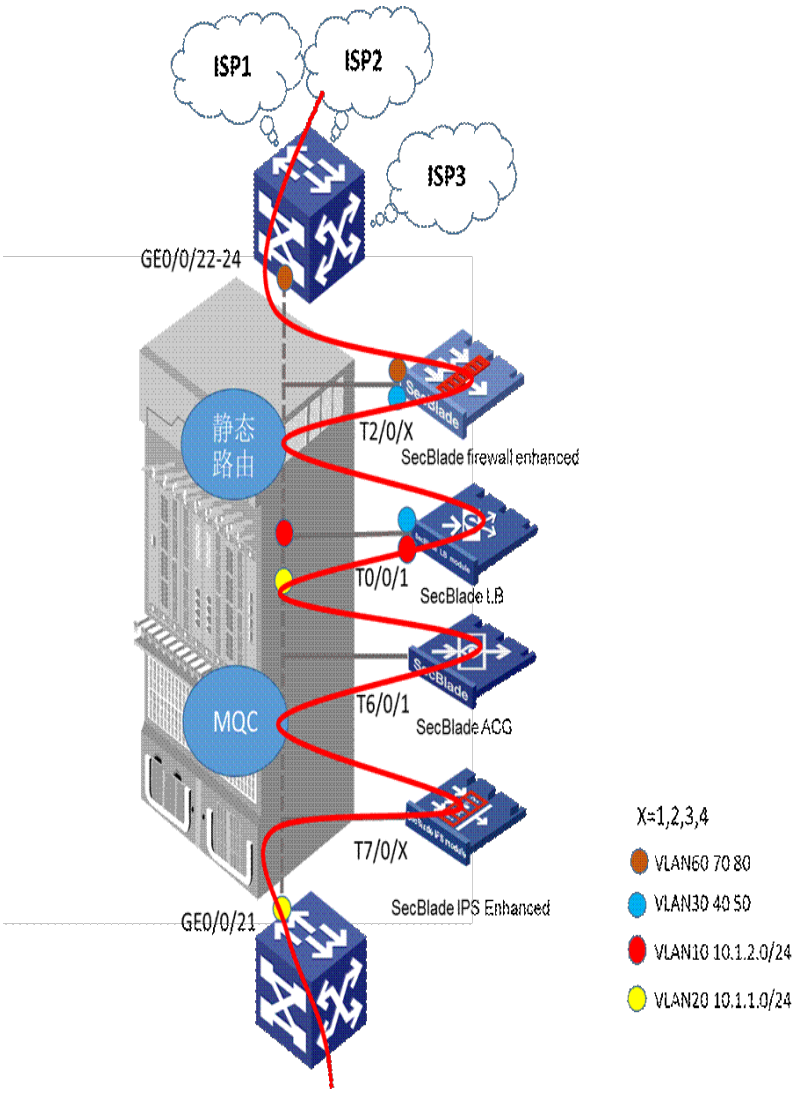



图2 流量走向图

三、配置步骤：

**M9000组网设计部署说明**

**vlan与接口部署**

vlan 10
 description UpStream
—— 配置上行至出口Vlan
vlan 20
 description DownStream
—— 配置下行至内网Vlan
vlan 30
 description ISP-1
—— 配置运营商1出口
vlan 40
 description ISP-2
—— 配置运营商2出口
vlan 50
 description ISP-3
—— 配置运营商3出口
vlan 100
 description pvid
—— 用于pvid的vlan创建
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
—— 配置上行vlan接口地址
#
interface Vlan-interface20
 ip address 10.1.2.1 255.255.255.0

—— 配置下行vlan接口地址
#

interface GigabitEthernet0/0/21
 port link-mode bridge
 description upstream
 port access vlan 10
 combo enable copper
 qos apply policy up_IPS inbound
—— 配置与下游设备相连接口，下发上行流量重定向到IPS的QoS
#
interface GigabitEthernet0/0/22
 port link-mode bridge
 description china_telecom
 port access vlan 30
 combo enable copper
#
interface GigabitEthernet0/0/23
 port link-mode bridge
 description china_unicom
 port access vlan 40
 combo enable copper
#
interface GigabitEthernet0/0/24
 port link-mode bridge
 description china_mobile
 port access vlan 50
 combo enable copper
—— 配置与上游设备相连接口

**路由部署**
在本案例组网中，M9000使用静态路由方式与其它设备相连。
ip route-static 0.0.0.0 0 10.1.2.2　　—— 上行重定向后走默认路由到LB
ip route-static 172.16.0.0 16 10.1.1.3
—— 下行重定向后走明细路由到内部网络，10.1.1.3为内网网关

上行流量进入M9000，QoS重定向至IPS和ACG，通过默认路由上送至LB，再转发给FW。下行从LB处理后出来重定向至IPS和ACG，再通过明细路由转发给下游设备。

**时间同步**
vlan 200　　——创建用于同步NTP的vlan
#
interface vlan200
ip address 200.0.0.1 255.255.255.0
#
ntp-service refclock-master 2　　——设置本地时钟作为参考时钟，层数为2

若需要从其他设备同步本地时钟，可以通过服务器/客户端模式，对等体模式，广播模式或者组播模式配置，可参考产品配置手册。

**SecBlade FW插卡设计部署**

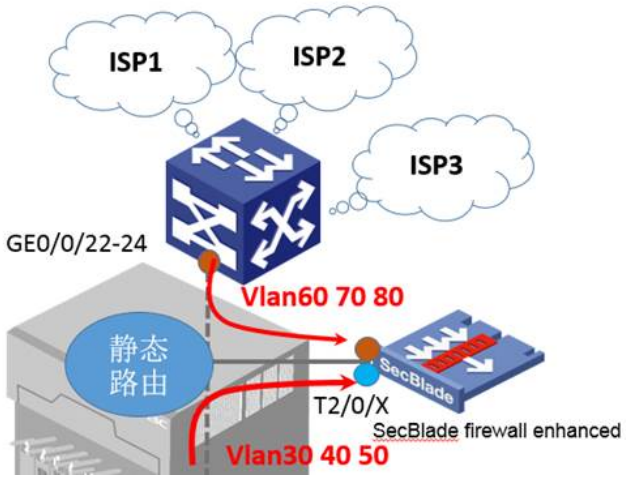



图3 SecBlade FW组网一部署结构图

**部署说明**

在本最佳实践案例中FW板卡主要保护外网用户访问数据中心内部的业务安全。外部用户经过防火墙转发到LB，内部流量从LB转发出去时需要经过FW。由于LB有多出口，前方防火墙为了简化配置，需要做虚拟防火墙，隔离不同的出口路由。上行流量由vlan30转换成vlan60出去，vlan40转换成vlan70出去，vlan50转换成vlan80出去。

**M9000侧配置**

```
interface Ten-GigabitEthernet2/0/1
 port link-mode bridge
port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
```

—— M9000对应的FW内联口有四个，推荐方式为四个内联口做聚合，允许相应vlan。
vlan200为ntp时间同步vlan。

**FW侧配置**

```
interface Bridge-Aggregation1     ——防火墙内联口作聚合口
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 30 40 50 60 70 80 200
#
interface Ten-GigabitEthernet0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Ten-GigabitEthernet0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Ten-GigabitEthernet0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
#
interface Ten-GigabitEthernet0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30 40 50 60 70 80 200
 port link-aggregation group 1
```

**时间同步**

```
vlan 200                          ——创建用于同步NTP的vlan
#
interface vlan200
ip address 200.0.0.2 255.255.255.0
#
ntp-service unicast-server 200.0.0.1      ——设置M9000为NTP服务器
```

**虚拟防火墙配置**

```
acl number 3001                ——— NAT转换匹配ACL
 rule 0 permit ip
#
ip vpn-instance vpn1            ——— 创建VPN实例，隔离路由
 route-distinguisher 1:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
ip vpn-instance vpn2
 route-distinguisher 2:2
 vpn-target 2:2 export-extcommunity
 vpn-target 2:2 import-extcommunity
#
ip vpn-instance vpn3
 route-distinguisher 3:3
 vpn-target 3:3 export-extcommunity
 vpn-target 3:3 import-extcommunity
#
interface vlan 30              ——— 创建三层虚接口，和VPN实例绑定
 ip binding vpn-instance vpn1
 ip address 10.1.3.2 255.255.255.0
#
interface vlan 40
 ip binding vpn-instance vpn2
 ip address 10.1.4.2 255.255.255.0
#
interface vlan 50
 ip binding vpn-instance vpn3
 ip address 10.1.5.2 255.255.255.0
#
```

```
interface Vlan-interface60        —— 出接口做NAT
 nat outbound 3001
 ip binding vpn-instance vpn1
 ip address 3.3.3.3 255.255.255.0
#
interface Vlan-interface70
 nat outbound 3001
 ip binding vpn-instance vpn2
 ip address 4.4.4.4 255.255.255.0
#
interface vlan 80
nat outbound 3001
 ip binding vpn-instance vpn3
 ip address 5.5.5.5 255.255.255.0
#
vd vda id 2            ——创建名称为vda、编号为1的VD，并进入该VD视图
allocate interface vlan30  ——为vda分配接口
allocate interface vlan60
allocate vlan 30 60        ——为vda分配vlan
limit-resource session max-entries 500000  ——为vda分配的最大会话数为500000
#
vd vdb id 3
allocate interface vlan40
allocate interface vlan70
allocate vlan 40 70
limit-resource session max-entries 500000
#
vd vdc id 4
allocate interface vlan50
allocate interface vlan80
allocate vlan 50 80
limit-resource session max-entries 500000
#
 ip route-static vpn-instance vpn1 0.0.0.0 0.0.0.0 3.3.3.4
 ip route-static vpn-instance vpn2 0.0.0.0 0.0.0.0 4.4.4.5
ip route-static vpn-instance vpn3 0.0.0.0 0.0.0.0 5.5.5.6
ip route-static vpn-instance vpn1 172.16.0.0 255.255.0.0 10.1.3.1
ip route-static vpn-instance vpn2 172.16.0.0 255.255.0.0 10.1.4.1
ip route-static vpn-instance vpn3 172.16.0.0 255.255.0.0 10.1.5.1
—— 每个虚拟防火墙都需要一条上行默认路由和下行明细路由，分别绑定不同的VPN实例
```

**FW域间策略配置**

```
switchto vd vda
 zone name Trust id 1
  priority 85
  import interface Vlan-interface30
 zone name Untrust id 2
  priority 15
  import interface Vlan-interface60
—— 进入虚拟防火墙，将相应接口计入安全域
#
switchto vd vdb
 zone name Trust id 1
  priority 85
  import interface Vlan-interface40
 zone name Untrust id 2
  priority 15
  import interface Vlan-interface70
    #
switchto vd vdc
 zone name Trust id 1
  priority 85
```

```
 import interface Vlan-interface50
 zone name Untrust id 2
  priority 15
  import interface Vlan-interface80
#
switchto vd vda          —— 进入虚拟防火墙，配置域间策略
 zone name Trust id 1
 ip virtual-reassembly
 zone name Untrust id 2
 ip virtual-reassembly
 interzone source Trust destination Untrust
  rule 0 permit
#
switchto vd vdb
 zone name Trust id 1
 ip virtual-reassembly
 zone name Utrust id 2
 ip virtual-reassembly
 interzone source Trust destination Untrust
  rule 0 permit
#
switchto vd vdc
 zone name Trust id 1
 ip virtual-reassembly
 zone name Utrust id 2
 ip virtual-reassembly
 interzone source Trust destination Untrust
  rule 0 permit
```

**SecBlade LB设计部署**

**部署说明**

LB对内部采用1个逻辑三层接口（vlan20），通过静态路由协议与M9000互连。对外部为3条出口三层链路（VLAN30,40,50），部署出方向负载均衡达到流量分担的目的。

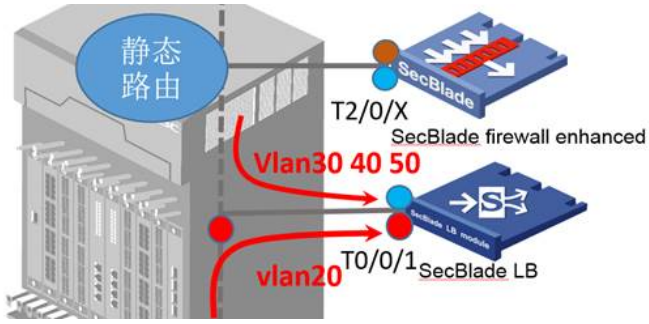



图4 SecBlade LB典型组网一结构图

**LB命令行配置**

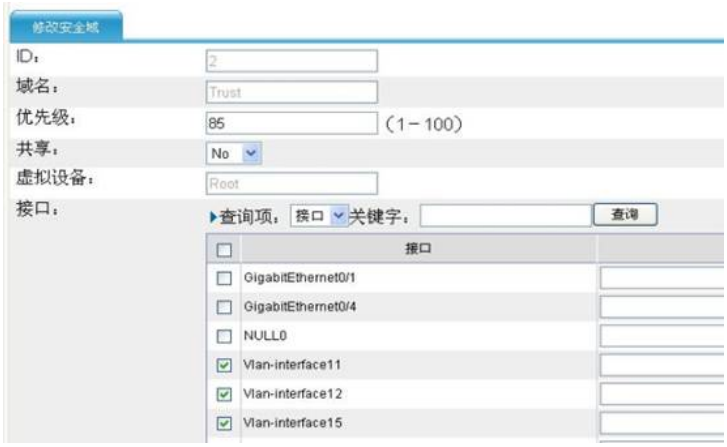
```
interface Vlan-interface20
ip address 10.1.2.2 255.255.255.0
#
interface Vlan-interface30                    ——配置出口方向地址
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface40
ip address 10.1.4.1 255.255.255.0
#
interface Vlan-interface50
ip address 10.1.5.1 255.255.255.0
#
interface Ten-GigabitEthernet0/0
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30 40 50
#
```

ip route-static 0.0.0.0 0.0.0.0 10.1.3.2
ip route-static 0.0.0.0 0.0.0.0 10.1.4.2 preference 100
ip route-static 10.1.1.0 255.255.255.0 10.1.2.1
——不走虚服务的流量可以根据静态路由转发，增加一条高优先级静态路由作为备份路由。
#
vlan 200　　——创建用于同步NTP的vlan
#
interface vlan200
ip address 200.0.0.3 255.255.255.0

#
ntp-service unicast-server 200.0.0.1　　——设置M9000为NTP服务器

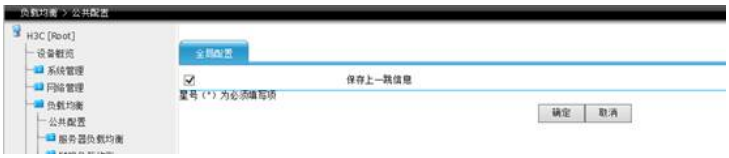
**LB的WEB配置**

在LB双机部署且配置NAT特性时，应注意需要将接口加入安全域，热备过程中需要同步安全域信息，通常部署时都建议添加安全域，避免出现配置疏忽。




**开启保存上一跳**

若有从外到内首先发起的流量，比如配置了nat server，要从外部映射到内部服务器，在多出口的情况下需要开启“保存上一跳”功能，保证流量从某个出口进来再从某个出口回去。




**配置逻辑链路组**

配置逻辑链路组，ISP选路优先，因此算法优先级较低不起作用，可以选择最小链接。逻辑链路故障可以选择“重定向已有链接”，选择“保持已有链接”可能导致上网持续不通。

**配置逻辑链路**

**配置物理链路**

配置outbound负载均衡，设定物理链路，关联ISP，保证健康型检测通过。假设电信IP为10.1.3.1，网关为10.1.3.2，按此配置。其他运营商链路假设:联通10.1.4.1，移动10.1.5.1，暂不举例。报文在防火墙做NAT转换出去。

**配置虚服务**

设置虚服务，开启虚服务功能和ISP选路功能

LB在收到TCP首个报文时，会先匹配虚服务，如果目的IP命中虚服务就按链路负载均衡流程转发报文。如果出口为公网，目的IP范围很大，可以用0.0.0.0的确省地址匹配所有网段流量，但另需要添加一个返回流量的虚服务，通过精确匹配原则将返回流量转发至内网，防止回程流量被转发会公网，部署时需注意。

**SecBlade ACG设计部署**

SecBlade ACG在本案例设计中使用在线部署方式，需要对上下行流量进行双向引流重定向上ACG板卡处理。在M9000对应接口入方向做流量重定向，使流量上ACG板卡，ACG板卡根据策略做允许、拒绝和记录等动作，不会对报文内容做任何修改。随后流量从ACG板卡转出时还是在同一Vlan中，再到三层Vlan接口做路由转发去下一跳。

由于ACG在整个网络中属于2层透明转发设备，不会对报文进行任何修改，整个网络从连通性上看加入ACG后不会产生任何变化影响。因此建议实施的时候将其放在最后进行上线配置，即其他设备都调试OK，流量转发与HA设计都以正常实现情况下再进行ACG的部署实施。

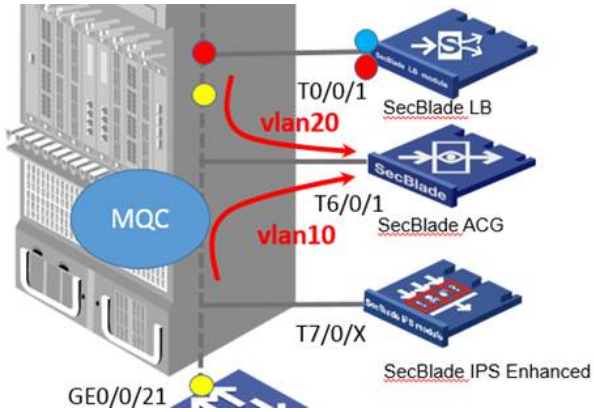



图5 SecBlade ACG典型组网一结构流量图

本案例中M9000的ACG插卡采用了传统的QoS重定向策略实现引流。

**M9000 SecBlade ACG部署说明**

**M9000交换机侧部署说明**

**流量重定向与接口配置**

traffic classifier down_ACG operator and ——下行流量从LB出来重定向到ACG
 if-match acl 3002
 if-match service-vlan-id 20 ——匹配下行vlan
 if-match destination-mac *0cda-41b6-41d8* ——匹配目的mac
#
traffic classifier up_ACG operator and ——上行流量从IPS出来重定向到ACG
 if-match service-vlan-id 10 ——匹配上行vlan
 if-match destination-mac *0cda-41b6-41d8*

```
 if-match acl 3001
#
traffic behavior down_ACG                ——设定重定向动作，注意track oap联动
 redirect interface Ten-GigabitEthernet6/0/1 track-oap
#
traffic behavior up_ACG
 redirect interface Ten-GigabitEthernet6/0/1 track-oap
#
qos policy down_ACG                  ——创建mqc策略，关联流量和动作
 classifier down_ACG behavior down_ACG
#
qos policy up_ACG
 classifier up_ACG behavior up_ACG
#
acl number 3001                      ——上行流量匹配
 description up_IPS
 rule 0 permit ip source 10.1.1.0 0.0.0.255
#
acl number 3002                      ——下行流量匹配
 description down_ACG
 rule 0 permit ip destination 10.1.1.0 0.0.0.255
#
interface Ten-GigabitEthernet6/0/1
 port link-mode bridge
 description to_ACG
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 undo stp enable
 undo mac-address mac-learning enable
 packet-filter 4000 outbound
 qos apply policy down_IPS inbound
 oap enable                                  ——使能oap协议
```

IPS和ACG插卡需要使用QoS引流，如果插卡故障，重定向动作通过OAP协议检测到后策略失效，流量不再重定向至插卡。

**二层报文过滤配置**

需要将常见的二层报文（如广播、组播、ARP）在IPS内部接口上进行过滤防止二层环路导致广播风暴，同时还需配置IPS所在接口禁止学习MAC地址。

```
acl number 4000
 description filter
 rule 0 permit type 0800 ffff dest-mac 0cda-41b6-41d8 ffff-ffff-ffff ——允许三层引流报文
 rule 50 permit type 88a7 ffff        ——允许oap协议报文
 rule 100 deny
    #
interface Ten-GigabitEthernet6/0/1
 port link-mode bridge
 description to_ACG
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 undo stp enable
 undo mac-address mac-learning enable
 packet-filter 4000 outbound
 qos apply policy down_IPS inbound  ——下行流量经过ACG处理后重定向至IPS
oap enable
```

**ACG侧Web部署说明**

**去使能OAA**

去使能OAA  ACFP Client。在本方案中，不使能acfp功能。

安全区域配置

段配置

**SecBlade IPS设计部署**

SecBlade IPS在本案例设计中使用在线部署方式，需要对上下行流量进行双向引流重定向上IPS板卡处理。在M9000对应接口入方向做流量重定向，使流量上IPS板卡，IPS板卡根据策略做允许、拒绝和记录等动作，不会对报文内容做任何修改。随后流量从IPS板卡转出时还是在同一Vlan中，再到三层Vlan接口做路由转发去下一跳。

由于IPS在整个网络中属于2层透明转发设备，不会对报文进行任何修改，整个网络从连通性上看加入IPS后不会产生任何变化影响。因此建议实施的时候将其放在最后进行上线配置，即其他设备都调试OK，流量转发与HA设计都以正常实现情况下再进行IPS的部署实施。

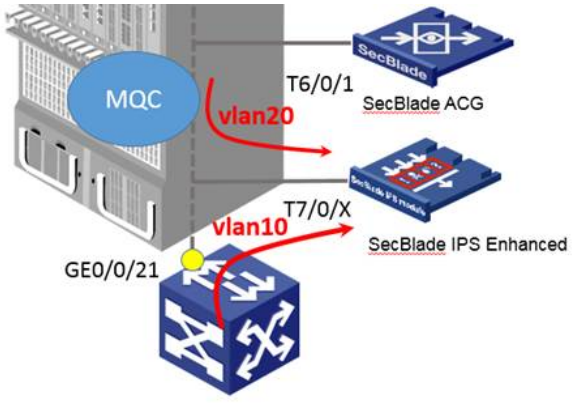



图6 SecBlade IPS典型组网一结构流量图

本案例中M9000的IPS插卡采用了传统的Qos重定向策略实现引流。

**M9000 SecBlade IPS部署说明**

**M9000交换机侧部署说明**

**流量重定向与接口配置**

```
traffic classifier down_IPS operator and      ——下行流量重定向到IPS
 if-match acl 3002                    ——匹配三层流量
 if-match service-vlan-id 20          ——匹配报文vlan
 if-match destination-mac 0cda-41b6-41d8 ——匹配目的mac，为本地vlan虚接口mac地址
#
traffic classifier up_IPS operator and        ——上行流量重定向到IPS
 if-match acl 3001
 if-match service-vlan-id 10
 if-match destination-mac 0cda-41b6-41d8
#
traffic behavior down_IPS
 redirect interface Ten-GigabitEthernet7/0/2 track-oap  ——OAP协议联动检测插卡状态
#
traffic behavior up_IPS
 redirect interface Ten-GigabitEthernet7/0/1 track-oap
#
qos policy down_IPS
 classifier down_IPS behavior down_IPS
#
qos policy up_IPS
 classifier up_IPS behavior up_IPS
#
acl number 3001                    ——上行流量匹配
 description up_IPS
 rule 0 permit ip source 10.1.1.0 0.0.0.255
#
acl number 3002                    ——下行流量匹配
 description down_IPS
 rule 0 permit ip destination 10.1.1.0 0.0.0.255
#
interface Ten-GigabitEthernet7/0/1
 port link-mode bridge
 description to_IPS
 port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 10 20 100
 port trunk permit pvid vlan 100
 undo stp enable                    ——关闭stp功能
 undo mac-address mac-learning enable      ——关闭mac地址学习功能，防止环路
 qos apply policy up_ACG inbound          ——上行重定向至ACG
packet-filter 4000 outbound     ——过滤非法报文
 port link-aggregation group 3
#
interface Ten-GigabitEthernet7/0/2
 port link-mode bridge
 description to_IPS
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 100
 port trunk permit pvid vlan 100
 undo stp enable
 undo mac-address mac-learning enable
qos apply policy up_ACG inbound
packet-filter 4000 outbound
port link-aggregation group 3
#
interface Ten-GigabitEthernet7/0/3
port link-mode bridge
description to_IPS
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 100
port trunk permit pvid vlan 100
undo stp enable
```

undo mac-address mac-learning enable
packet-filter 4000 outbound
port link-aggregation group 3
#
interface Ten-GigabitEthernet7/0/4
port link-mode bridge
description to_IPS
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 100
port trunk permit pvid vlan 100
undo stp enable
undo mac-address mac-learning enable
packet-filter 4000 outbound
port link-aggregation group 3
——四个内联口，分两对，12口一对，34口一对。
如果暂时使用12口，34口不使用，IPS侧可以shutdown，不要关闭M9000侧内联口
#
interface Bridge-Aggregation3
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 100
port trunk permit pvid vlan 100
link-aggregation selected-port minimum 4
——最小选择端口数为4，当4个接口中任意一个接口down，聚合口就down.(实际上任何一个接口down都说明插卡出现了问题)
undo stp enable
undo mac-address mac-learning enable
——聚合口必须配置，加入聚合的物理口推荐配置
oap enable
——IPS Enhanced插卡做OAP检测必须创建聚合口，将内联口加入聚合口，并在聚合口使能oap协议注册插卡。
内联口必须修改pvid，并本地创建pvid相应vlan。

IPS和ACG插卡需要使用QoS引流，如果插卡故障，重定向动作通过OAP协议检测到后策略失效，流量不再重定向至插卡。

**二层报文过滤配置**

需要将常见的二层报文（如广播、组播、ARP）在IPS内部接口上进行过滤防止二层环路导致广播风暴，同时还需配置IPS所在接口禁止学习MAC地址。

acl number 4000
description filter
rule 0 permit type 0800 ffff dest-mac *0cda-41b6-41d8* ffff-ffff-ffff
rule 50 permit type 88a7 ffff ——允许oap协议报文
rule 100 deny
#
interface Ten-GigabitEthernet7/0/1
port link-mode bridge
description to_IPS
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
port trunk permit pvid vlan 100
undo stp enable
undo mac-address mac-learning enable
packet-filter 4000 outbound ——物理接口下发，注意方向
qos apply policy up_ACG inbound

**IPS侧Web部署说明**

**去使能OAA**

去使能OAA ACFP Client。在本方案中，不使能acfp功能。

**安全区域配置**

**段配置**

**整网双机HA设计部署**

**整网双机HA部署**

前面的各设备板卡配置说明中已经涵盖了部分HA设计部署，此处对整网HA做统一说明，并对各种故障下的流量路径切换进行描述，对重点配置进行说明。

单框典型组网中，HA考虑点不多，主要针对以下故障切换：

板卡故障切换；

**板卡故障切换**

**LB和FW设备故障**

当LB和FW故障时，由于是单框单插卡，无法备份切换。

单框下，多LB和多FW插卡可以实现互相备份切换。

**IPS/ACG板卡故障切换**

IPS/ACG板卡与M9000配置oap协议，这样当IPS/ACG板卡故障时，重定向功能失效，M9000经过短暂中断后可以直接转发流量，不会发生主备机之间的切换，但流量将失去IPS/ACG的安全保护和审计

。

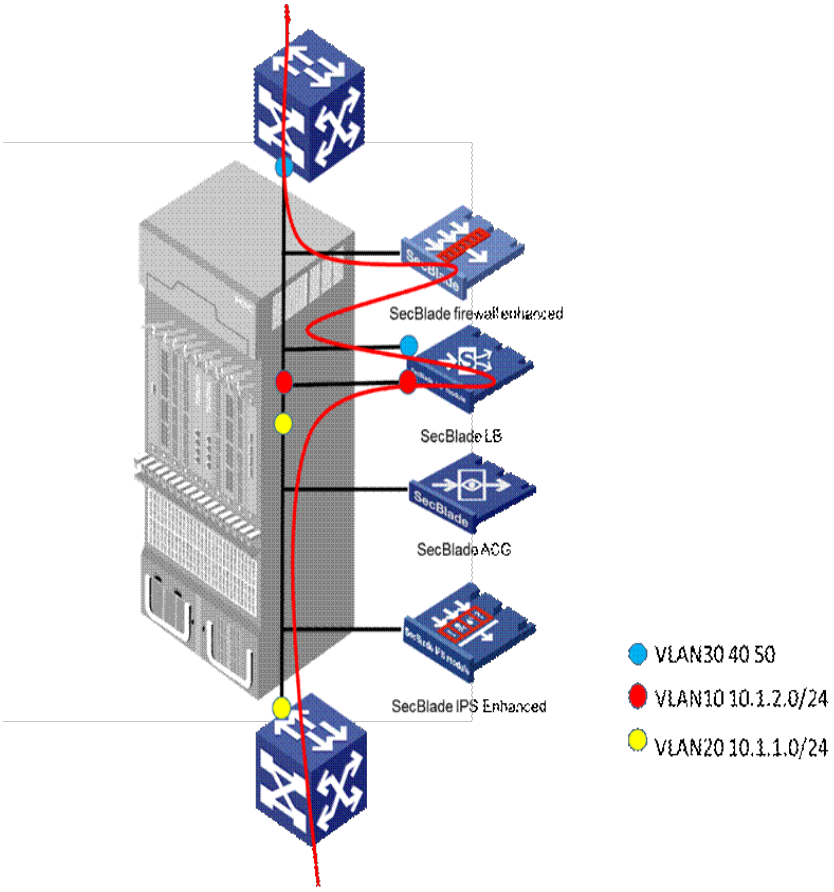



图7 IPS/ACG板卡故障切换示意图