文章编号：2096-1618(2022)06-0651-05

# 安全资源池在省级气象网络中的部署及优化

方国强[1,2]， 刘一谦[1,2]， 张常亮[1,2]

(1.高原与盆地暴雨旱涝灾害四川省重点实验室，四川 成都 610072；2.四川省气象探测数据中心，四川 成都 610072)

**摘要**：传统南北向网络安全防御已经无法满足新形势下网络安全需求，强化东西向网络安全是目前需要着力解决的一大问题。面对省级气象部门这种复杂网络环境，四川省气象部门采用安全资源池这一面向中小企业的安全服务系统，在省级气象业务网络上线部署方案，上线部署中遇到的交换机物理资源 IFP ACL 耗尽导致策略路由下发失败问题解决方法。系统部署上线后，有效提升了气象业务内网横向防护能力，完成了省级关键业务区域边界防护。为省级气象部门强化东西向网络安全提供了一种较廉价解决方案。

**关 键 词**：安全资源池；VAF；策略路由；ACL

**中图分类号**：TP393 **文献标志码**：A

**doi**：10.16836/j.cnki.jcuit.2022.06.006

## 0 引言

多年来，安全专家一直在争论网络安全威胁究竟是外部人员还是内部人员带来更大的风险，表明网络安全威胁来自于南北向、东西向网络安全威胁同样严重[1]。

气象部门是高度依赖信息化的公众服务型事业单位，网络建设起步较早，随着业务的发展，网络基础架构和业务系统布局越来越复杂。四川省气象局作为省级气象部门，网络结构相对也较复杂，网络安全建设由于多方面原因侧重南北向防御、东西向防御建设长期处于空白。面对省级气象部门这种复杂网络环境，如何在有限经费投入情况下，使东西向网络安全防御建设达到较理想的效果，是西部等欠发达地区气象部门面临的一大难题。基于云架构的安全资源池系统出现，较好地解决了此困境。但系统部署涉及现有资源整合，不可避免地会出现一些问题，需要根据实际情况针对性地优化解决。

## 1 相关技术介绍

### 1.1 安全资源池

安全资源池是云计算平台中提供安全服务的资源集合[2-3]。本文应用的深信服安全资源池架构基于软件虚拟化技术，建立能够为最终用户提供方便快捷的网络安全自动编排服务的云安全服务平台(cloud security service platform，CSSP)。平台主要包括下一代防火墙、入侵防御、Web 应用防火墙、堡垒机、漏洞扫描、数据库审计、上网行为管理、日志审计、终端安全(EDR)等组件。

云安全架构(图1)从下往上分为三层[4]：

基础硬件架构层：由服务器、交换机和存储系统构成。

虚拟化架构层：基于底层基础硬件架构，将计算、网络和存储进行软件虚拟化，为上层安全资源池架构提供其所需的资源单元。

安全资源池架构层：利用虚拟化架构层提供的资源单元，将各类安全组件进行统一部署和管理，对内利用安全服务链可以将任意安全组件进行自由组合，对外提供自由的安全编排服务能力。

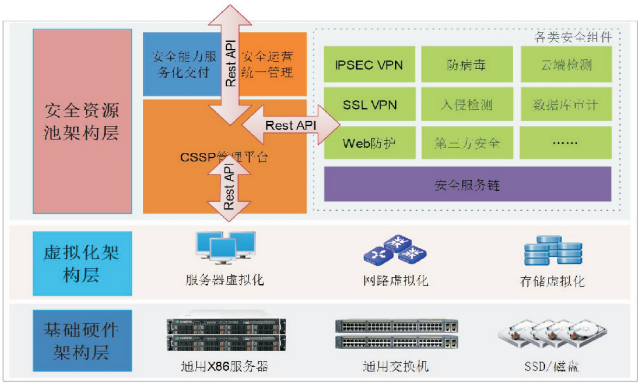


图1 安全资源池架构图

### 1.2 策略路由

策略路由(policy-based-route)是一种依据用户制定的策略进行路由选择的机制[5]，策略路由通过数据包

收稿日期：2021-12-23

源、目的地址、长度等信息匹配进行定制化的路由选择。

通常策略路由的优先级要高于普通路由，数据包到达端口后先匹配策略路由，如无匹配项再按照普通路由进行转发[6]。但不同厂商、不同类型的产品，路由优先级各有不同。总的来说，策略路由一般有强弱两种模式。弱策略路由的下一跳如果不可达，则返回继续查找路由表[7-8]；强策略路由，不管下一跳是否可达，都会按照策略路由进行转发，如果下一跳不可达，则直接丢弃报文。

## 2 网络现状及存在的问题

四川省气象局局域网络为典型的核心、汇聚和接入三层架构，汇聚交换机超过 20 台，可管理接入交换机超过 90 台。根据业务需要，核心与汇聚之间有三层和二层两种互联方式，整个网络中 VLAN 超过 100 个，重要业务系统分别部署于 16 个 C 类网段。其中，7 个为数据支撑系统专用网段，物理上为独立区域，其余 9 个网段网关全部位于核心交换机，散乱分布于机房内，接入不同的交换机。所有重要业务系统网段都需要进行边界安全防护，以提升整个网络东西向安全，但由于内部数据交换量大，如使用传统硬件安全设备，则一方面高性能设备经费投入太高，另一方面设备性能无法根据业务发展动态调整。

## 3 安全资源池部署及上线应用测试

### 3.1 安全资源池部署规划

如何将散乱分布于机房内的服务器纳入安全设备后端进行保护，是安全系统部署首要面临的问题。通过策略路由引流，实现气象业务数据流经安全设备是一种可行的方式。

本文应用测试的安全资源池单臂部署在核心交换机上，为保证安全资源池宕机等离线情况对网络通信不造成影响，采用弱策略路由将指定地址段的流量引流到安全资源池，以此实现 9 个分散部署的业务系统网段东西向网络边界防护。安全资源池全部选择下一代防火墙（VAF）[9]组件，实现东西向边界应用控制、WEB 应用防护、入侵防御等安全防护需求[10-11]。

根据业务系统数据流量，将 9 个业务网段安全防护分配到 7 个 VAF，安全资源池可以购买不同的 VAF 处理性能授权，灵活搭配，底层硬件服务器资源不足可以平滑扩容，满足业务发展需求。安全资源池的部署示意图如图 2 所示。

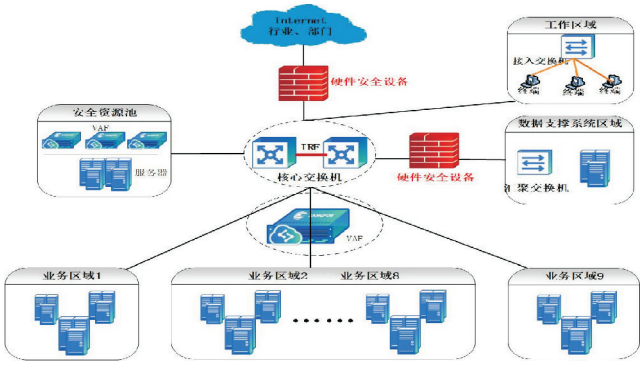


图 2 安全资源池部署示意图

安全资源池内部虚拟网络中，VAF 同样单臂部署在虚拟核心路由器上，通过策略路由将数据流量分发到不同 VAF，能够避免因 VAF 故障导致的网络中断，安全资源池内部结构如图 3 所示。

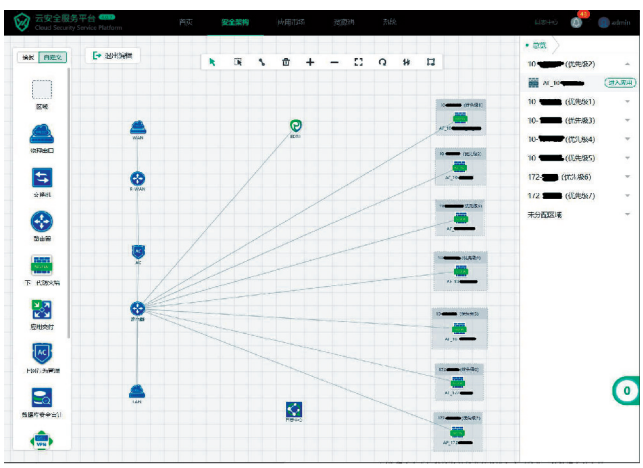

图 3 安全资源池内部结构

### 3.2 核心交换机策略路由配置

安全资源池单臂部署，通过在核心交换机上配置策略路由进行引流，保证访问重要业务系统网段的请求数据包和返回数据包都通过安全资源池。

#### 3.2.1 ACL 配置

对于防火墙来说，只有请求数据包和返回数据包都通过防火墙，才能准确发挥应用控制策略的作用。确保请求数据包和返回数据包都通过安全资源池的关键是策略路由 ACL 配置准确性[12]。本次部署测试中，业务系统网段的三层接口设计匹配指定源地址的 ACL，其他三层接口设计匹配指定目的的 ACL。

指定目的地址配置示例：

```
acl number 3000
  rule 0 permit ip source any destination X.X.X.0 0.0.0.255
```

指定源地址配置示例：

```
acl number 3001
```

rule 0 permit ip source X. X. X. 0 0. 0. 0. 255 destination any

3.2.2　策略路由配置

业务系统网段中有部分 NAS、ISCSI 等存储业务,一方面数据量过大,另一方面针对存储系统的安全威胁相对较小,这部分数据考虑不通过安全资源池。核心交换机配置策略路由时,需要将这部分 IP 排除,其方法是对这部分 IP 地址配置指定目的地址和源地址的两条 ACL,策略路由中匹配 ACL 后不进行任何后续动作,并将该部分配置在节点 node-number 最小的位置优先执行。

策略路由配置示例:

```
policy-based-route aqzyc permit node 10
  if-match acl 3002
policy-based-route aqzyc permit node 20
  if-match acl 3001
  apply next-hop X. X. 1. 2
policy-based-route aqzyc permit node 30
  if-match acl 3000
  apply next-hop X. X. 2. 2
```

策略路由应用下发示例:

```
interface Vlan-interface1
  ip policy-based-route aqzyc
```

3.2.3　策略路由下发效果

通过策略路由进行引流后,实现访问业务网段的数据通过 VAF 进行安全过滤,通过 TRACERT 命令进行路由跟踪,数据流量通过核心交换、安全资源池虚拟路由器、虚拟防火墙等设备地址后,最终到达目标服务器。

# 4　安全资源池上线异常分析及优化

交换机和安全资源池是比较成熟的网络及安全产品,在生产业务中单独部署时,基本不存在问题。但在本次部署测试中,在核心交换机的三层接口下发策略路由到最后阶段时,出现策略路由下发响应缓慢,策略路由下发后不生效的问题。

交换机其他操作运行正常,只有在下发策略路由配置操作时响应缓慢,应该是策略路由相关的资源不足,策略路由主要消耗 ACL 资源,从 ACL 资源进行问题分析处理。

## 4.1　ACL 资源分析

华三交换机可以通过 display qos-acl resource 命令查看 QoS 和 ACL 的资源使用情况,详细命令及命令结果如图 4 所示,图中各字段含义如表 1 所示。

```
<核心12510X>display qos-acl resource
Interfaces: XGE1/3/0/1 to XGE1/3/0/12
```

| Type | Total | Reserved | Configured | Remaining | Usage |
|---|---|---|---|---|---|
| VFP ACL | 2048 | 1536 | 0 | 512 | 75% |
| IFP ACL | 8192 | 2048 | 782 | 5362 | 34% |
| IFP Meter | 4096 | 1024 | 0 | 3072 | 25% |
| IFP Counter | 4096 | 1024 | 0 | 3072 | 25% |
| EFP ACL | 1024 | 0 | 0 | 1024 | 0% |
| EFP Meter | 512 | 0 | 0 | 512 | 0% |
| EFP Counter | 512 | 0 | 0 | 512 | 0% |

图 4　交换机 QoS 和 ACL 的资源使用情况

表 1　字段含义表

| 字段 | 描述 |
|---|---|
| Interfaces | 资源对应的接口范围 |
| Type | VFP ACL 表示二层转发前的,用于重标记 QoS 本地 ID 值功能的 ACL 资源<br>IFP ACL 表示入方向的 ACL 资源<br>IFP Meter 表示入方向的流量监管资源<br>IFP Counter 表示入方向的流量统计资源<br>EFP ACL 表示出方向的 ACL 资源<br>EFP Counter 表示出方向的流量统计资源 |
| Total | 资源总数 |
| Reserved | 预留的资源数 |
| Configured | 已经使用的资源数 |
| Remaining | 剩余可用的资源数 |
| Usage | 预留的资源数与已配置的资源数之和占资源总数的百分比,分子按实际计算结果的整数部分显示。 |

## 4.2　异常原因分析

通过在核心交换机上输入 display qos-acl resource 命令,发现交换机 7 号槽位板卡 IFP ACL 项 Usage 值超过了 90%,而 3 号槽位板卡仅只有 40%,同时发现 3 号槽位板卡的 IFP ACL 资源总数是 7 号槽位板卡的 3 倍。通过查看交换机物理设备信息发现,3 号槽位和 7 号槽位板卡分别是 EB 和 EA 两种类型的万兆电口板,EB 性能优于 EA。因此,初步判断策略路由下发后不生效的原因是 7 号槽位板卡物理性能不足,必须优化配置降低板卡物理资源消耗。异常时交换机资源使用情况如图 5 所示。

```
<核心12510X>dis qos-acl resource
Interfaces: XGE1/3/0/1 to XGE1/3/0/12
```

| Type | Total | Reserved | Configured | Remaining | Usage |
|---|---|---|---|---|---|
| VFP ACL | 2048 | 1536 | 0 | 512 | 75% |
| IFP ACL | 8192 | 2048 | 1232 | 4912 | 40% |
| IFP Meter | 4096 | 1024 | 0 | 3072 | 25% |
| IFP Counter | 4096 | 1024 | 0 | 3072 | 25% |
| EFP ACL | 1024 | 0 | 0 | 1024 | 0% |
| EFP Meter | 512 | 0 | 0 | 512 | 0% |
| EFP Counter | 512 | 0 | 0 | 512 | 0% |

```
Interfaces: XGE1/3/0/13 to XGE1/3/0/24
```

| Type | Total | Reserved | Configured | Remaining | Usage |
|---|---|---|---|---|---|
| VFP ACL | 2048 | 1024 | 0 | 1024 | 50% |
| IFP ACL | 8192 | 2048 | 1232 | 4912 | 40% |
| IFP Meter | 4096 | 1024 | 0 | 3072 | 25% |
| IFP Counter | 4096 | 1024 | 0 | 3072 | 25% |
| EFP ACL | 1024 | 0 | 0 | 1024 | 0% |
| EFP Meter | 512 | 0 | 0 | 512 | 0% |
| EFP Counter | 512 | 0 | 0 | 512 | 0% |

```
Interfaces: XGE1/7/0/1 to XGE1/7/0/24
```

| Type | Total | Reserved | Configured | Remaining | Usage |
|---|---|---|---|---|---|
| VFP ACL | 1024 | 512 | 0 | 512 | 50% |
| IFP ACL | 2048 | 768 | 1140 | 140 | 93% |
| IFP Meter | 1024 | 384 | 0 | 640 | 37% |
| IFP Counter | 1024 | 384 | 0 | 640 | 37% |
| EFP ACL | 1024 | 0 | 0 | 1024 | 0% |
| EFP Meter | 512 | 0 | 0 | 512 | 0% |
| EFP Counter | 512 | 0 | 0 | 512 | 0% |

```
Interfaces: XGE1/7/0/25 to XGE1/7/0/48
```

图 5　异常时交换机资源使用情况

### 4.3 优化处理

策略路由不生效的原因是板卡 ACL 资源消耗超过阈值,需要优化减少 ACL 匹配条数。从配置分析来看,ACL 数量过多,主要是在排除 NAS、ISCSI 等存储业务地址时,由于 IP 地址零散,每条规则只匹配一个地址,导致 ACL 规则条数过多。优化该 ACL 采用多个 IP 汇总为网段和调整设备地址到网络存储专用网段等方式,将原 22 条规则优化为 3 条规则。

优化前 ACL 配置:

```
acl number 3002 name aqzyc
  rule 0 permit ip destination 192.168.2.169 0
  rule 5 permit ip destination 192.168.2.170 0
  rule 10 permit ip destination 192.168.2.171 0
  rule 15 permit ip destination 192.168.2.172 0
  rule 20 permit ip destination 192.168.2.173 0
  rule 25 permit ip source 192.168.2.169 0
  rule 30 permit ip source 192.168.2.170 0
  rule 35 permit ip source 192.168.2.171 0
  rule 40 permit ip source 192.168.2.172 0
  rule 45 permit ip source 192.168.2.173 0
  rule 60 permit ip destination 192.168.2.76 0
  ……
  rule 130 permit ip source 192.168.2.115 0
  rule 135 permit ip destination 192.168.2.115 0
```

优化后 ACL 配置:

```
acl number 3002 name aqzyc
  rule 0 permit ip source 192.168.2.168 0.0.0.7
  rule 5 permit ip destination 192.168.2.168 0.0.0.7
  rule 10 permit ip source 192.168.20.0 0.0.0.255
  rule 15 permit ip destination 192.168.20.0 0.0.0.255
```

### 4.4 优化效果

通过对 ACL 优化后,板卡 ACL 资源消耗明显下降,交换机策略路由运行正常,安全资源池各 VAF 均有数量流量正常通过,应用控制策略功能正常。优化配置后的交换机资源使用情况如图 6 所示。

```
<核心12510X>dis qos-acl resource
Interfaces: XGE1/3/0/1 to XGE1/3/0/12
 Type            Total     Reserved    Configured Remaining   Usage
 VFP ACL         2048      1536        0          512         75%
 IFP ACL         8192      2048        782        5362        34%
 IFP Meter       4096      1024        0          3072        25%
 IFP Counter     4096      1024        0          3072        25%
 EFP ACL         1024      0           0          1024        0%
 EFP Meter       512       0           0          512         0%
 EFP Counter     512       0           0          512         0%
Interfaces: XGE1/3/0/13 to XGE1/3/0/24
 Type            Total     Reserved    Configured Remaining   Usage
 VFP ACL         2048      1024        0          1024        50%
 IFP ACL         8192      2048        782        5362        34%
 IFP Meter       4096      1024        0          3072        25%
 IFP Counter     4096      1024        0          3072        25%
 EFP ACL         1024      0           0          1024        0%
 EFP Meter       512       0           0          512         0%
 EFP Counter     512       0           0          512         0%
Interfaces: XGE1/7/0/1 to XGE1/7/0/24
 Type            Total     Reserved    Configured Remaining   Usage
 VFP ACL         1024      512         0          512         50%
 IFP ACL         2048      768         782        498         75%
 IFP Meter       1024      384         0          640         37%
 IFP Counter     1024      384         0          640         37%
 EFP ACL         1024      0           0          1024        0%
 EFP Meter       512       0           0          512         0%
 EFP Counter     512       0           0          512         0%
Interfaces: XGE1/7/0/25 to XGE1/7/0/48
```

图 6 优化配置后交换机资源使用情况

框式交换机业务模块配置时,不仅需要考虑端口配置,同时需要根据业务需求考虑模块自身物理性能,以免出现类似本文中将模块物理性能耗尽的情况。

## 5 结束语

安全资源池是一种较经济实惠的网络内部边界云安全系统,但对网络策略配置和网络设备协同要求较高,部署模式也导致应用中存在一些瑕疵。安全资源池内部策略路由全部在虚拟核心路由器上配置,网络通信时会按照策略路由配置先后顺序将数据流量分配到匹配的第一条 ACL 对应的 VAF,不会同时通过相应的两台 VAF。因此,安全资源池中的 VAF 之间存在优先级,业务网段之间的安全策略配置需要根据优先级确定对应的 VAF。单臂部署模式下,通过 VAF 防护的业务网段和没有应用策略路由的一般网段之间通信时,由于数据流量只单向经过 VAF,某些应用控制策略可能会造成误判,需要针对性地进行策略配置优化调整。

上线新的业务系统,尤其是网络安全方面的系统,上线运行只是开始,还需要在未来不断根据业务发展进行完善和调优,才能充分发挥系统作用,促进业务发展。

## 参考文献:


[1] 王莹. 计算机网络安全威胁分析及防护体系架构研究[J]. 数字技术与应用,2020,38(6):180-181.

[2] 张华,岳皓. 基于 SDN 的港口安全资源池建设[J]. 网络空间安全,2020,11(3):39-43.

[3] 袁文韬. 软件定义安全中安全资源池化技术研究及应用[D]. 北京:北京邮电大学,2018.

[4] 乔延臣,张结辉,陈晓帆. 基于安全资源池的云安全解决方案[J]. 信息技术与标准化,2018(9):57-62.

[5] 刘鑫,宁学武,徐天成. PBR+ACL 技术在取消高速公路省界收费站网络安全改造中的应用[J]. 工程技术研究,2020,5(24):24-26.

[6] 王献宏. 浅析策略路由的实现[J]. 电脑知识与技术,2020,16(22):67-68+73.

[7] 饶险峰,孙丽. 内部网关协议中精细路由调整方法简介[J]. 硅谷,2012(6):119+58.

[8] 孟金,陈澍. 基于 MSTP 的省市气象宽带网的设计与实现[J]. 中国新通信,2020,22(10):38-40.

[9] 王扣武,张珺铭,王婧如. 基于下一代防火墙的

企业网络安全设计与实现[J]. 信息技术与信息化,2019(6):123-126.
[10] 郑传德. 下一代防火墙在网络安全防护中的应用[J]. 网络安全技术与应用,2021(6):12-13.
[11] 陈博. 基于下一代防火墙技术在医院网络安全中的应用[J]. 网络安全技术与应用,2022(1):118-119.
[12] 陈一峰,陈颖. 一种访问控制列表 ACL 的检测方法及网络设备[P]. 中国:CN112565167A,2021-03-26.

# Deployment and Optimization of the Security Resources Pool in Provincial Meteorological Network

FANG Guoqiang[1,2], LIU Yiqian[1,2], ZHANG Changliang[1,2]
(1. Heavy Rain and Drought-Flood Disasters in Plateau and Basin Key Laboratory of Sichuan Province, Chengdu 610072, China; 2. Sichuan Meteorological Observation and Data Center, Chengdu 610072, China)

**Abstract**: Traditional north-south-traffic network security defense has been unable to can't meet the requirement for network security in the new era. Enhancing the east-west-traffic network security defense ability is an urgent issue for us to settle down at the moment. Facing a complex network environment, Sichuan Meteorological Administration used the security resources pool, a security service system oriented to the small and middle-sized enterprise, to enhance provincial key business area network border security defense capability. This article introduces deployment of the security resources pool in the Sichuan Meteorological Network System. After the failure of the first arrangement, we analyzed the reason and solved the fatal problem that the exhaustion of the physical switch IFP ACL resources caused the failure of policy distribution. After the operationalization of the system, the network border security defense capability of Sichuan Meteorological Bureau has raised effectively. Also the resolution is an economical plan for most provincial meteorological departments to improve the east-west-traffic network security defense ability.

**Keywords**: security resources pool; VAF; policy-based-route; ACL