



天翼云·云下一代防火墙 应急预案

天翼云科技有限公司



目录

1 前言	1
1.1 编写目的	1
1.2 文档范围	1
1.3 目标读者	1
1.4 应急准备工作	1
2 日常巡检	1
2.1 并发会话检查	1
2.2 CPU 利用率及内存利用率检查	2
2.3 检查设备路由表	2
2.4 检查安全策略及 NAT 情况	4
2.5 检查日志情况	5
3 突发事件处理方法	6
3.1 配置错误或丢失处理方法	6
3.2 业务中断处理方法	6
3.3 业务访问慢处理方法	6
3.4 软件故障处理方法	7
3.5 HA 场景	7
4 应急处置	9
4.1 封堵恶意 IP 地址	9
4.2 回绑业务 IP	10

1 前言

1.1 编写目的

应急预案主要为最终用户所需操作的参考文档及针对云下一代防火墙运行过程中，或者操作过程中可能出现的紧急问题，如业务中断或系统性能严重下降等而制定的操作指导，其目的是缩短系统中断时间，降低业务损失。

1.2 文档范围

适用于最终用户的运维人员。

1.3 目标读者

最终用户

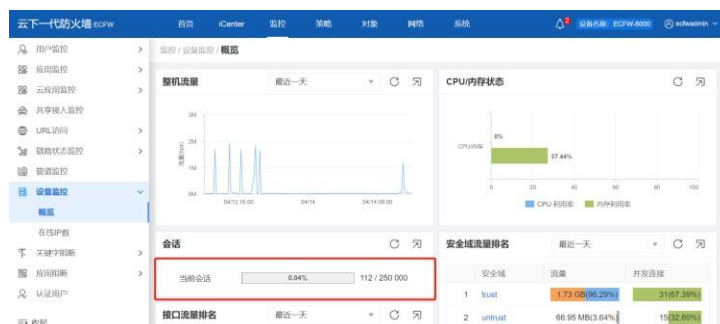
1.4 应急准备工作

人员保障，各区域提供云下一代防火墙技术支持，提前做好备用防火墙测试、主备切换测试，做好配置备份并导出至本地。如短时间无法解决，进行问题升级到资深天翼云安全专家处，尽快解决问题。

2 日常巡检

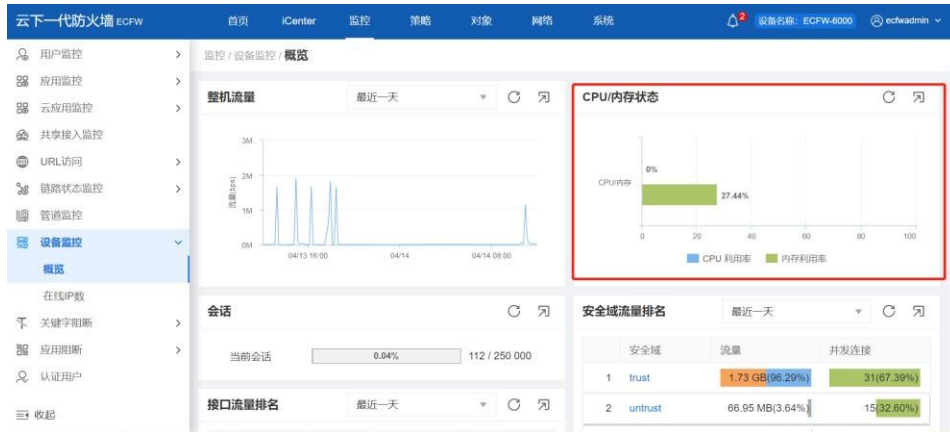
2.1 并发会话检查

- 1) Web 页面查看（监控-设备监控-概览-查看会话）：当 WEB 页面中的会话数值达到最大值，防火墙会话建立失败，从而影响到客户业务的稳定性。



2.2 CPU 利用率及内存利用率检查

- Web 页面查看（监控-设备监控-概览-CPU/内存状态）：CPU 及内存主要任务是执行功能、会话、日志等管理功能，其阈值为 90%，当长时间超过此阈值时影响到防火墙的处理性能。



2.3 检查设备路由表

- 查看目的路由（网络-路由-目的路由）：用于互联网访问内网业务



The screenshot shows the '目的路由' (Destination Routes) configuration page. It displays a table with columns for status, virtual router, IP address, next hop type, next hop gateway, next hop interface, protocol, and time table.

状态	所属虚拟路由	IP/掩码	下一跳类型	下一跳网关/虚拟路由器	下一跳接口	协议	时间表
<input type="checkbox"/>	trust-vr	0.0.0.0/0	接口	192.168.0.1	ethernet0/0	DHCP	
<input type="checkbox"/>	trust-vr	172.16.1.0/24	接口		tunnel1	直连	
<input type="checkbox"/>	trust-vr	172.16.1.1/32	接口		tunnel1	主机	
<input type="checkbox"/>	trust-vr	192.168.0.0/24	接口		ethernet0/0	直连	
<input type="checkbox"/>	trust-vr	192.168.0.191/32	接口		ethernet0/0	主机	
<input type="checkbox"/>	trust-vr	192.168.2.0/24	接口		ethernet0/1	直连	
<input type="checkbox"/>	trust-vr	192.168.2.1/32	接口		ethernet0/1	主机	

- 查看源接口路由（网络-路由-源路由/源接口路由）：用于云主机访问外网业务。



The screenshot shows the '源路由' (Source Routes) configuration page. It displays a table with columns for status, virtual router, IP address, next hop type, next hop gateway, next hop interface, protocol, and time table.

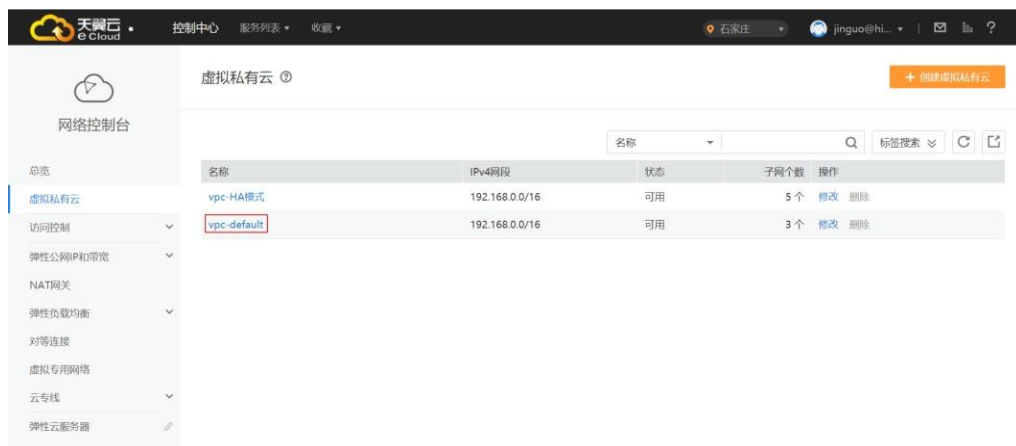
状态	所属虚拟路由	IP/掩码	下一跳类型	下一跳网关/虚拟路由器	下一跳接口	协议	时间表
<input type="checkbox"/>	trust-vr	10.0.0.0/16	网关	192.168.2.1	ethernet0/1	静态	
<input type="checkbox"/>	trust-vr	192.168.0.75/32	网关	192.168.2.1	ethernet0/1	静态	
<input type="checkbox"/>	trust-vr	192.168.0.103/32	网关	192.168.140.1	ethernet0/3	静态	

查看控制台的 VPC 默认路由是否指向云下一代防火墙：用于内外网互访，会影响到业务运行。

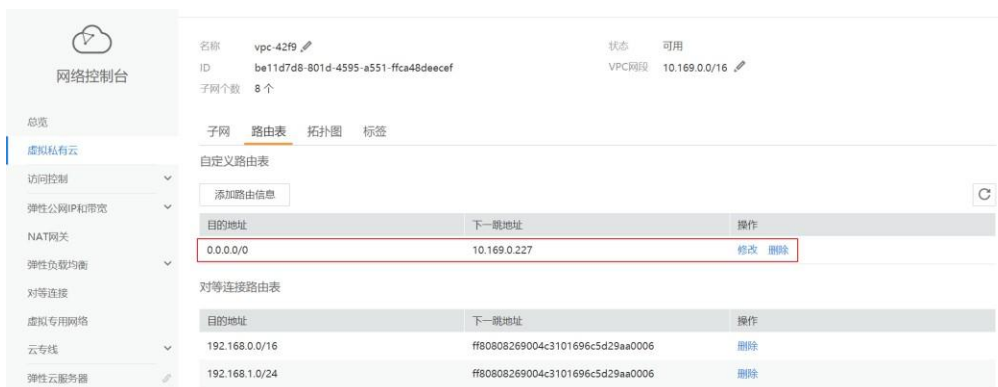
1) 服务列表



2) 点击业务 VPC

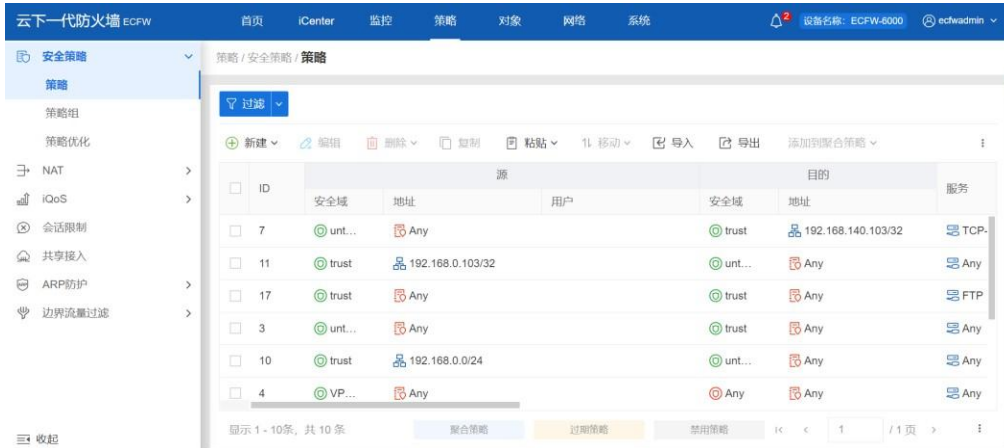


3) 点击业务 VPC，查看默认路由



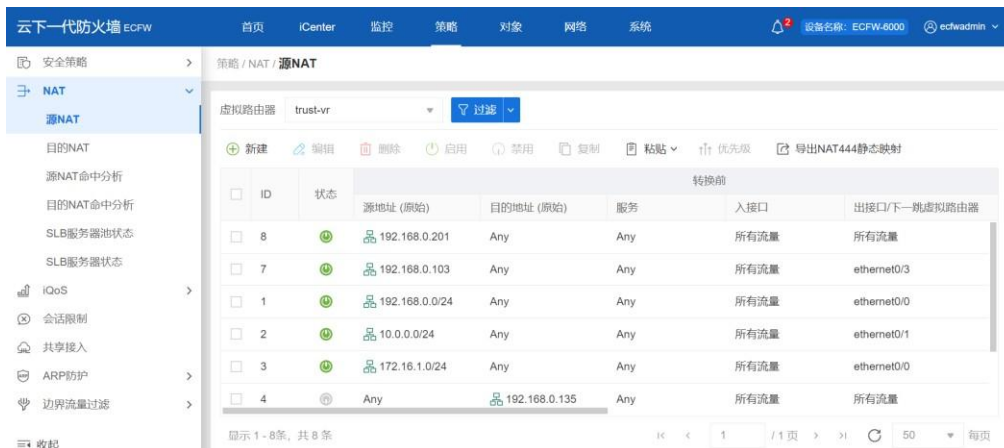
2.4 检查安全策略及 NAT 情况

6 查看已配置的安全策略（策略-安全策略-命中数）



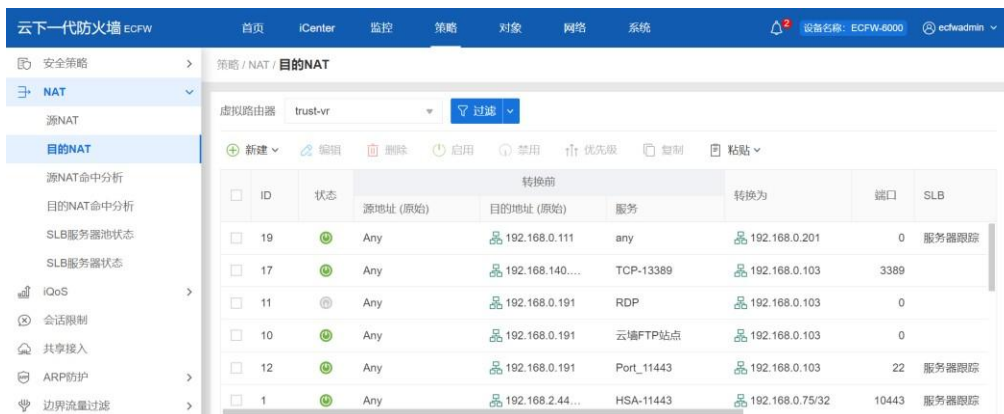
ID	安全域	地址	用户	安全域	地址	服务
7	unt...	Any		trust	192.168.140.103/32	TCP
11	trust	192.168.0.103/32		unt...	Any	Any
17	trust	Any		trust	Any	FTP
3	unt...	Any		trust	Any	Any
10	trust	192.168.0.0/24		unt...	Any	Any
4	VP...	Any		Any	Any	Any

7 查看已配置的源 NAT、目的 NAT（策略-NAT-源 NAT）



ID	状态	源地址(原始)	目的地址(原始)	服务	入接口	出接口/下一跳虚拟路由器
8	🟢	192.168.0.201	Any	Any	所有流量	所有流量
7	🟢	192.168.0.103	Any	Any	所有流量	ethernet0/3
1	🟢	192.168.0.0/24	Any	Any	所有流量	ethernet0/0
2	🟢	10.0.0.0/24	Any	Any	所有流量	ethernet0/1
3	🟢	172.16.1.0/24	Any	Any	所有流量	ethernet0/0
4	🟡	Any	192.168.0.135	Any	所有流量	所有流量

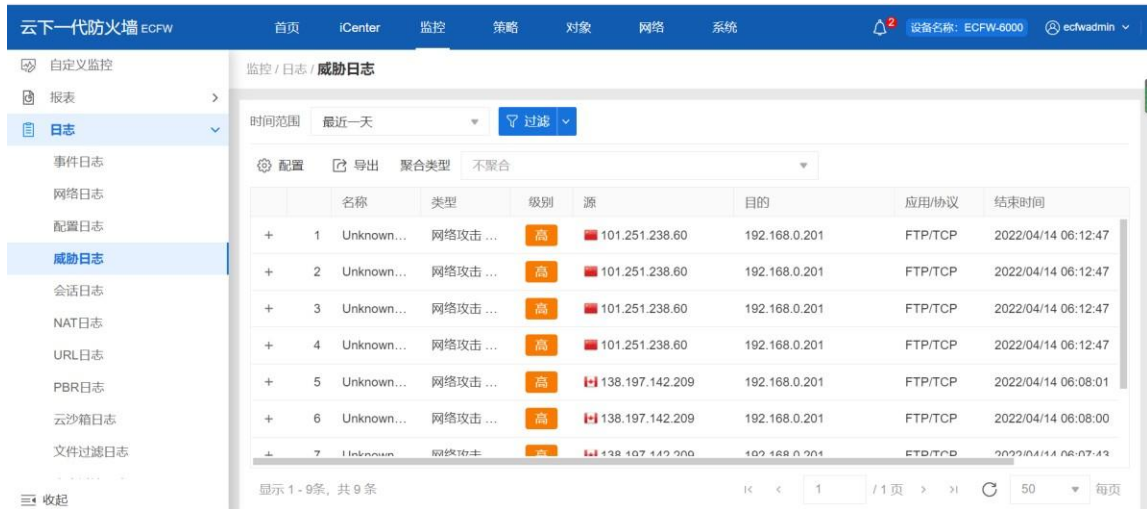
8 查看已配置的源 NAT、目的 NAT（策略-NAT-目的 NAT）



ID	状态	源地址(原始)	目的地址(原始)	服务	转换为	端口	SLB
19	🟢	Any	192.168.0.111	any	192.168.0.201	0	服务器跟踪
17	🟢	Any	192.168.140....	TCP-13389	192.168.0.103	3389	
11	🟡	Any	192.168.0.191	RDP	192.168.0.103	0	
10	🟢	Any	192.168.0.191	云端FTP站点	192.168.0.103	0	
12	🟢	Any	192.168.0.191	Port_11443	192.168.0.103	22	服务器跟踪
1	🟢	Any	192.168.2.44...	HSA-11443	192.168.0.75/32	10443	服务器跟踪

2.5 检查日志情况

⑨ WEB 页面查看日志：



	名称	类型	级别	源	目的	应用/协议	结束时间	
+	1	Unknown...	网络攻击 ...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
+	2	Unknown...	网络攻击 ...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
+	3	Unknown...	网络攻击 ...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
+	4	Unknown...	网络攻击 ...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
+	5	Unknown...	网络攻击 ...	高	138.197.142.209	192.168.0.201	FTP/TCP	2022/04/14 06:08:01
+	6	Unknown...	网络攻击 ...	高	138.197.142.209	192.168.0.201	FTP/TCP	2022/04/14 06:08:00
+	7	Unknown...	网络攻击 ...	高	138.197.142.209	192.168.0.201	FTP/TCP	2022/04/14 06:07:43

⑩ 日志级别如下：

监控系统事件和网络流量的事件日志便于系统管理员分析和跟踪设备各种问题情况，日志信息根据严重级别的不同，可分为 8 级别。

日志信息严重性级别分类：

- Emergency（紧急）级别 0：系统不可用信息。
- Alert（警示）级别 1：需要立即处理的信息，如设备受到攻击灯。
- Critical（关键）级别 2：危急信息，如硬件出错。
- Error（错误）级别 3：错误信息。
- Warning（警告）级别 4：报警信息。
- Notification（通知）级别 5：非错误信息，但需要特殊处理。
- Information（信息）级别 6：通知信息。
- Debugging（调试）级别 7：调试信息，包括正常的使用信息。

3 突发事件处理方法

3.1 配置错误或丢失处理方法

重新导入备份配置或者恢复之前一段时间配置。

3.2 业务中断处理方法

- 1 查看防火墙状态，各种资源使用率。
- 2 登录防火墙，将策略改成全通，然后测试业务是否正常。
- 3 如果无法解决，联系云墙技术支持。

3.3 业务访问慢处理方法

- 1 检查 CPU、内存、会话表。
- 2 show cpu detail (查看板卡 CPU core 的使用率)
- 3 show cpu-cntr (查看 CPU 丢包情况) 查看是不是有通道丢包情况
- 4 检查设备的 session、cpu、内存使用情况检查方法：命令行登陆防火墙或者通过 show session ge、show cpu、show memory 命令查看日志。
- 5 显示结果：
 - Show session ge 显示 free 数值不能等于 0。
 - Show cpu 不超过 80%
 - Show memory 不超过 80%
- 6 处理方法：show session ge 显示 free 数值等于 0，查看每 ip 会话个数，如果每个 ip 会话数都正常，联系技术工程师做性能评估。Show cpu 和 show memory 超过 80%，查看防火墙 security 日志，确认是否有攻击。可关闭相应统计集或对攻击源 IP 进行会话限制或者策略拒绝。如果确认两者都正常，联系技术工程师配合处理。

3.4 软件故障处理方法

- 1) 策略不生效问题：策略不生效可能引起业务故障，但出现策略不生效概率很小。原因可能和软件版本有关。
- 2) 包转发不正常：包转发不正常可能和接口 MTU 值以及其他接口参数有关，若出现包转发不正常情况，先通过 show interface 查看接口包收发数量查看具体原因。
- 3) 配置错误：检查防火墙的配置，例如接口地址、策略、路由 NAT 这些基本配置，确认是否有误，再进行配置调整。
- 4) 会话激增：会话激增最可能的原因为内部或外部攻击，此时需要在防火墙上进行抓包，参看异常 ip 连接，然后进行相应阻断或会话限制。
- 5) CPU 利用率和内存利用率过高：当业务异常时，可能和 CPU 利用率和内存利用率有关，技术工程师可通过查看设备 alarm 日志进行故障定位和原因分析。
- 6) VPC 互通路由异常：两个 Vrouter 间虚机互相 ping 不通或者单通，原因：vpc 互通路由缺失，排查：检查 neutron-server 日志，查看是否由于配置下发异常引起路由缺失。

3.5 HA 场景

- a) 检查防火墙主备状态，检查方法：web 登陆防火墙——系统——状态——HA 状态。
显示结果：两台设备分别显示主状态和备状态。
处理方法：如遇两台设备同时为主的情况，查看设备告警日志接口的状态，必须保证接口是 up 状态。
- b) 查看两台防火墙 alarm 日志 检查方法：web 登陆防火墙——日志报表——告警日志。
显示结果：无非正常 alarm 日志。
处理方法：如遇非人为因素导致 alarm 日志产生，请联系技术工程师配合分析具体



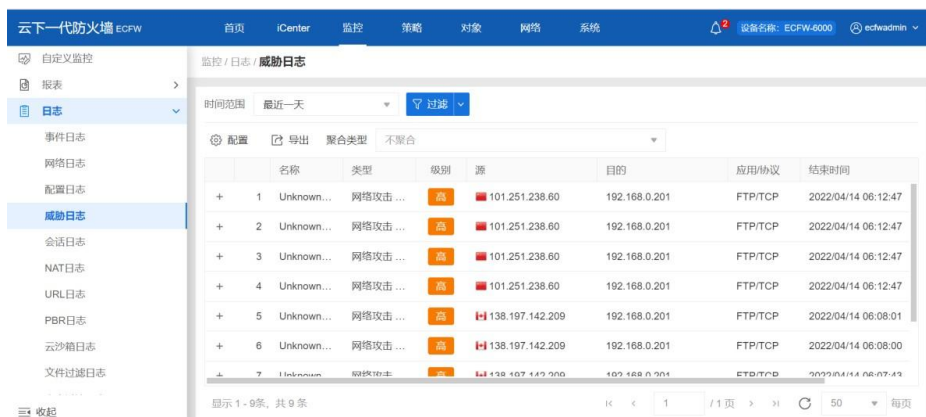
原因。

- c) HA 切换异常，HA 主备切换异常原因可能和 license、心跳线有关。针对 HA 切换异常故障，技术工程师会定期对云下一代防火墙进行查看，查看 license 期限，心跳接口等情况。

4 应急处置

4.1 封堵恶意 IP 地址

1. 查看威胁日志



名称	类型	级别	源	目的	应用协议	结束时间
1 Unknown...	网络攻击...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
2 Unknown...	网络攻击...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
3 Unknown...	网络攻击...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
4 Unknown...	网络攻击...	高	101.251.238.60	192.168.0.201	FTP/TCP	2022/04/14 06:12:47
5 Unknown...	网络攻击...	高	138.197.142.209	192.168.0.201	FTP/TCP	2022/04/14 06:08:01
6 Unknown...	网络攻击...	高	138.197.142.209	192.168.0.201	FTP/TCP	2022/04/14 06:08:00
7 Unknown...	网络攻击...	高	138.197.142.209	192.168.0.201	FTP/TCP	2022/04/14 06:07:43

2. 针对日志中的源地址进行 IP 封堵

1) 新建地址簿（对象-地址簿-新建）



名称	成员	排除成员	描述
Any	0.0.0.0/0		
111	1.1.1.1/32		
private_network	10.0.0.0/8, 172.16.0.0/12, 192...		
test-1	192.168.0.191/32		
test2	1.1.1.1/32		

2) 输入 IP 地址-添加-确认

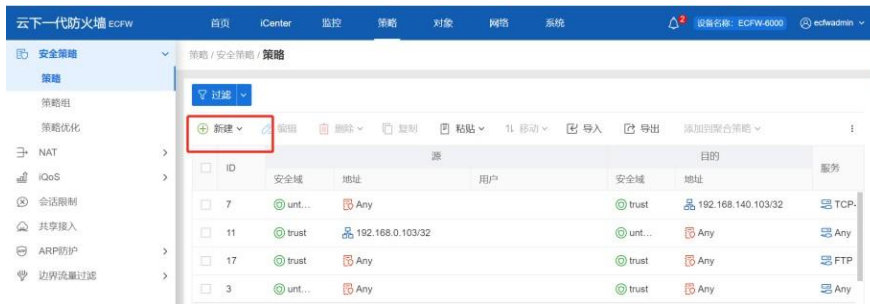


名称 * 封堵IP (1 - 95) 字符

地址成员	类型	成员
<input type="checkbox"/>	IP/掩码	138.197.142.209/32

新建 删除

3) 策略-安全策略-新建



4) 调整安全策略配置，其中源 IP 地址为第三步骤所创建的地址簿、动作修改为拒绝



4.2 回绑业务 IP

1. 点击服务列表中弹性 IP



2. 输入弹性 IP 119.96.125.38 并点击搜索，然后点击解绑并选择确认



3. 解绑成功之后选择弹性负载均衡点击绑定弹性 IP



4. 输入 119.96.125.38，然后点击确认

