策略路由 zhiliao\_FO3qD 2018-11-25 发表

#### 组网及说明

# 1 配置需求或说明

### 1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙: F100-X-G2、F1000-X-G2、F100-WiNet、F1000-AK、F10X0等

注:本案例是在F1000-C-G2的Version 7.1.064, Release 9323P1801版本上进行配置和验证的。

### 1.2 配置需求及实现的效果

防火墙作为网络出口设备,外网有移动和联通两条线路。内网有192.168.1.0和192.168.2.0两个网段, 需要实现192.168.1.0网段走移动线路,192.168.2.0网段走联通线路。当两条线路中的一条线路故障时 数据可以通过正常链路转发。

### 2 组网图



PC:192.168.2.0/24

### 配置步骤

## 3 配置步骤

### 3.1 上网配置

防火墙上网配置请参考"2.2.2 防火墙外网使用固定IP地址上网配置方法"进行配置,本文只针对策略路 由配置进行介绍。

### 3.2 创建IPV4策略路由

#在"网络"> "路由">"策略路由">"IPV4策略路由"中点击"新建",策略名称设置为"neiwang"应用于"GE1/0 /4"。



#### 3.3 新建策略节点匹配移动数据

#在策略节点中点击"新建", NodeID设置为"5", 勾选"匹配IPv4 ACL"后添加ACL策略。

建策略节点									?
NodeID	5					•	(0-65535)		
模式	<ul> <li>允许</li> </ul>		◎ 拒绝						
报文匹配规则									
🗐 匹配排	这长度								
							(1-65535)		
☑ 匹配1	Pv4 ACL								
	_					~	(2000-3999或)	63个字符)	
执行攝作 📑	添加ACL策略								
🔲 设 39	99								
📄 设置排	<b> </b>								
	Routine					~			
设置	P报文头中的分	片标志							
	允许分片操作					~			
📄 设置排	设在指定VRF <sup>®</sup>	中进行转发							
						~			
设置报文转发的	的下一跳地址								
④ 新建	删除								
VRF		IP地址			缺省	TrackI	直连下-	影编	ili,
设置报文转发的	的出接口								
⊕ 新建 前	删除								
				缺省		TrackJ	Ę	编	損
					-				
			确定		取消				

#类型选择"高级ACL", ACL编号设置为3000然后点击确定。

新建IPv4ACL		? X
类型 ACL (?)	◎ 基本ACL ③ 高级ACL 3000	*(3000-3999或1-63个字 符)
规则匹配顺序	◎ 按照配置顺序 ◎ 自动排序	
默认规则编号步长	5	(1-20)
描述		(1-127字符)
	開定 取消	

#在新弹窗中"IP协议类型选择"为IP,勾选匹配条件为"匹配源IP地址/通配符掩码"配置IP地址为192.168. 1.0,设置反掩码为0.0.0.255后点击确定。

键IPv4高级ACL的	匀规则	?
ACL编号	3000	(3000-3999或
		1-63个字符)
规则编号	☑ 自动编号	* (0-65534)
描述		(1-127字符)
动作	<ul> <li>允许</li> <li>⑦ 拒绝</li> </ul>	
IP协议类型	ip	▼* (0-256, 256)
		代表任意ip)
匹配条件 🕐	☑ 匹配源IP地址/通配符掩码	
	192.168.1.0 / 0.0.0.255	
	□ 匹配源地址对象组	
	匹配目的IP地址/通配符掩码	
	🔲 匹配目的地址对象组	
	■ 匹配TCP/UDP报文的源端口号	
	── 匹配TCP/UDP报文的目的端口号	
	确定 取消	

#在新弹窗中去勾选"继续添加下一条规则"点击确定。

f建IPv4高级ACL的	现则		?	×
	—— 一 匹配目的地址对象组			-
	■ 匹配TCP/UDP报文的源端口号			
	□ 匹配TCP/UDP报文的目的端口号			
	■ 匹配TCP报文的连接建立标识			
	匹配TCP报文标识			
	CI 匹配ICMP报文的消息类型和消息码			
	□ 匹配DSCP优先级			h
	□ 匹配IP优先级			
	□ 匹配ToS优先级			
规则生效时间段	请选择	~		
VRF	公网	~		1
分片报文 🕐	□ 仅对分片报文的非首个分片有效			
记录日志	🗐 对符合条件的报文记录日志信息			
匹配统计	□ 开启本规则的匹配统计功能			
	🔄 继续添加下一条规则			
	确定 取消			

#确认匹配IPv4 ACL已经有访问控制列表时,在"设置报文转发的下一条地址"中点击新建。

改策略节点						? X
NodeID 模式 报文匹配规则	5 ⑧ 允许	◎ 拒绝		•	(0-65535)	
[] 元香	报文长度	+			(1-65535)	
☑ 匹配	IPv4 ACL					
	3000			~	(2000-3999或63个字	符)
执行操作 () 设置 () 设置	后续节点 🕐 报文的IP优先级					
🔲 设置	0:Routine IP报文头中的分片标题	ī.		~		
🔲 设置	0:允许分片操作 报文在指定VRF中进行	转发		~		
				*		
设置报文转发 (十)新建	的下一跳地址					
VRF	IPtt	址	缺省	f Track项	直连下一跳	编辑
心黑 记 六 # # #	oo u ta D					
●新建 前						
	ARCE 121					100.00

#设置IP地址为移动外网线路的网关地址1.1.1.2后点击确定。

报文转发的下一题	化地址	? X
VRF	公网	*
IP地址	1.1.1.2	*
缺省	否	~
Track项 🕐		(1-1024)
直连下一跳	是	~
	确定取消	

#策略全部配置完成后点击确定完成对移动链路的配置。

建策略节点						?
NodeID	5			* ((	)-65535)	
模式 报文匹配规则	◉ 允许	◎ 拒绝				
	报文长度					
				(1	-65535)	
☑ 匹配	Pv4 ACL					
3	000			▼ (2)	2000-3999或63个	字符)
执行操作						
🔄 设置	后续节点 🕐					
📄 设置	设文的IP优先级					
	Routine			~		
🔄 设置	P报文头中的分片标志	ŧ.				
	):允许分片操作			~		
📄 设置	假文在指定VRF中进行	<b></b> 转发				
				~		
设置报文转发	的下一跳地址					
④新建	删除					
VRF	IP地	址	缺省	Track项	直连下一跳	编辑
□ 公网	1.1.	1.2	否		是	
设置报文转发	的出接口					
④新建	删除					
		9±	*	TrackID		(attrict)

## 3.4 新建策略节点匹配联通线路

.

#在策略节点中点击"新建",NodeID设置为"10",勾选"匹配IPv4 ACL"后添加ACL策略。

建策略节点						?
NodeID 模式 报文匹配规则	.0 ④ 允许	◎ 拒绝		•	(0-65535)	
□ 匹配报文	长度					
					(1-65535)	
▼ 匹配IPv4	ACL					
				~	(2000-3999或63个字	符)
执行操作 🕇 添	加ACL策略					
□设 3000						
回设 3999						
0:Roi	utine			~		
□ 设置IP报	之头中的分片标志					
0:分计	F分片操作			~		
□ 设置报文	<b>王指定VRF中进行转发</b>					
	Division 1.1			~		
设直接又转发的ト·						
	TOURLY		<b>Phylip</b>	7 1 12	= = + T N	1048
VKF	IPTER		設合	Track	直连トー跳	珊瑚
设置报文转发的出	接口					
→ 新建 前 副系	÷					

#类型选择"高级ACL", ACL编号设置为3001然后点击确定。

新建IPv4ACL		? X
类型 ACL (?)	<ul> <li>○ 基本ACL</li> <li>◎ 高级ACL</li> <li>3001</li> </ul>	*(3000-3999或1-63个字 符)
规则匹配顺序 默认规则编号步长	<ul> <li></li></ul>	(1-20)
描述		(1-127字符)
	<ul> <li>✓ 继续添加规则 ②</li> <li>确定</li> <li>取消</li> </ul>	

#在新弹窗中"IP协议类型选择"为IP,勾选匹配条件为"匹配源IP地址/通配符掩码"配置IP地址为192.168. 2.0,设置反掩码为0.0.0.255后点击确定。

新建IPv4高级ACL的规	则	?	×
ACL编号	3001	( 3000-3999或 L-63个字符 )	^
规则编号	☑ 自动编号	(0-65534)	
描述		(1-127字符)	н
动作	<ul> <li>允许</li> <li>⑦ 拒绝</li> </ul>		
IP协议类型	请选择	(0-256,256	
匹配条件 🕐	▼ 匹配源IP地址/通配符掩码	(交江高小方)	-
	192.168.2.0 / 0.0.0.255		
	🔲 匹配源地址对象组		
	匹配目的IP地址/通配符掩码		
	🗐 匹配目的地址对象组		
	□ 匹配TCP/UDP报文的源端口号		
	III 匹配TCP/UDP报文的目的端口号 确定 取消		*

新建IPv4高级ACL的	现则	? >
	── 匹配目的地址对象组	ŕ
	III 匹配TCP/UDP报文的源端口号	
	◎ 匹配TCP/UDP报文的目的端口号	
	III 匹配TCP报文的连接建立标识	
	III 匹配TCP报文标识	
	I 匹配ICMP报文的消息类型和消息码	
	I 匹配DSCP优先级	i i i
	III 匹配IP优先级	
	🔲 匹配ToS优先级	
规则生效时间段	请选择 💙	
VRF	公网 🖌	
分片报文 🕐	□ 仅对分片报文的非首个分片有效	
记录日志	□ 对符合条件的报文记录日志信息	
匹配统计	□ 开启本规则的匹配统计功能	
	2 继续添加下一条规则	
	WOAL HX/FB	

#确认匹配IPv4 ACL已经有访问控制列表时,在"设置报文转发的下一条地址"中点击新建。

<sup>#</sup>在新弹窗中去勾选"继续添加下一条规则"点击确定。

建策略节点							?
NodeID	10				*	(0-65535)	
模式 报文匹配规则	◎ 允许	◎ 拒绝					
	报文长度						
						(1-65535)	
☑ 匹配	IPv4 ACL						
3	3001				~	(2000-3999或63个与	\$符)
执行操作							
📄 设置	后续节点 🕐						
□ 设置	报文的IP优先级						
	):Routine				~		
🔄 设置	IP报文头中的分片标志	2					
	):允许分片操作				~		
📄 设置	报文在指定VRF中进行	转发					
					~		
设置报文转发	的下一跳地址						
① 新建	删除						
VRF	IP地	址		缺省	Track项	直连下一跳	编辑
设置报文转发	的出接口						
⊕ 新建	删除						
			缺省		Track	Į	编辑

#设置IP地址为联通外网线路的网关地址2.2.2.2后点击确定。

<b>员</b> 文转发的下一剧	地址		? X
VRF	公网	~	*
IP地址	2.2.2.2		*
缺省	否	*	
Track项 🕐			(1-1024)
直连下一跳	是	~	

#策略全部配置完成后点击确定完成对联通链路的配置。

<b>标建策略</b> 节点						?)	
NodeID	10			• ((	(0-65535)		
模式 报文匹配规则	◉ 允许	◎ 拒绝					
□ 匹配	报文长度						
				(1	-65535)		
☑ 匹配:	IPv4 ACL						
3	8001			▼ (2)	2000-3999或63个	字符)	
执行操作							
📄 设置	后续节点 🕐						
🔲 设置	报文的IP优先级						
	0:Routine			~			
📄 设置	IP报文头中的分片标志						
0:允许分片操作				~			
📄 设置	报文在指定VRF中进行:	转发					
				~			
设置报文转发	的下一跳地址						
<ul> <li>⊕ 新建</li> </ul>	删除						
VRF	IP地均	Ł	缺省	Track项	直连下一跳	编辑	
□ 公网	2.2.2.	2	否		是		
设置报文转发	的出接口						
④新建	删除					L	
□ 接口		缺	í	Track项		编辑	
		确定	取消				

#最后在IPv4策略中点击确定完成策略配置。

修改IPv4策略路由	4	? X
策略名称 应用于 策略节点	neiwang GE1/0/4	
⊕ 新建	删除	
NodeID		编辑
5		
10		
	确定 取消	

# 3.5 保存配置

系统					-	adm	in - 保存 修改密	<b>∂</b> [→
1據条件 📿 刷新	□ 列定制			请输入要查试	间的信息	Q, <u>1</u>	的 [	o <mark>]</mark> 高级查询
服务	用户	动作	内容安全	命中次数	流量	统计	启用	编辑
		允许					V	
		允许						
		允许					V	

配置关键点