

# Supernova 测试仪 防火墙转发策略检测配置手册

网测科技

2021/01/22



# 目



1.	文档说明	3
2.	网络拓扑图	3
3.	设置防火墙	4
	3.1 设置接口 ip 地址	4
	3.2 配置防火墙策略	5
4.	设置 Supernova 测试仪	6
	4.1 防火墙转发策略检测用例配置	6
	4.2 启动测试用例	7
	4.3 用例运行及查看报告	7





## 1. 文档说明

本文档介绍配置防火墙转发策略检测的配置过程,此文档使用一台简网防火 墙配置举例,不同品牌的防火墙操作配置存在差异性,而且随着系统版本升级和 接口变化,需要不断对配置用例进行修改和升级,所以有任何问题,请联系我们 的售前或售后支持人员。

# 2. 网络拓扑图

本次测试的网络拓扑图如下



策略判断方法:

测试仪模拟客户端与服务器,流量通过受测防火墙,模拟的客户端尝试与模拟的服务器打开指定的端口建立连接,客户端发送 syn 报文,通过接收服务器的 reset 或者 syn+ack 的回应报文,来判断流量通过的防火墙的策略是阻断还是通过。



# 3. 设置防火墙

## 3.1 设置接口 ip 地址

#### 进入防火墙系统网络接口配置页面

KFW 监控-	系统管理・	路由▼	防火墙+	病毒与攻击,	上网行为管理→	VPN-	设置用户▼	日志与报告	
系统管理 / 控制面板 / 状态	控制面板								
9 控件	网络	Þ	接口						
<ul> <li>系统信息</li> <li>客户名称</li> <li>序列号</li> <li>主机名</li> <li>持续运行时间</li> </ul>	DHCP服务器       配置       管理员设置       证书       维护	* * * * *	区 选项 DNS 服务 网络代理 7 小时 1 分钟				④ ③	(△ (3) (次)	
系统日期		Mon Ja	n 6 13:01:54	2020			[更]	改]	
AV特征值		33.156	5 (升级 2017-1	1-08)			[升约	级]	
IPS特征值		7.156	(升级 2017-11	-08)			[升]	段]	
警告信息窗口							000	00	
③ 2020-01-06 12:59:23 失败的管	管理员登录尝试 admir	n						×	
② 2019-12-30 20:00:29 系統重応	3							×	
© 2019-12-24 12:16:31 系统重点	3							×	
③ 2019-12-04 19:19:57 系统重点	3							×	
◎ 2019-11-26 16:45:58 失败的智	管理员登录尝试 APW1	1KMB001	000004 login		×				
◎ 2019-11-26 16:45:55 失败的智	管理员登录尝试 APW1	1KMB001	000004 login					×	

#### 我这里用的是 m1/1 和 m1/2 端口

KFW	监控▼	系统管理+	路由▼	防火墙▼	病毒与攻击•	上网行为管理+	VPN+	设置用户+	日志与报告・
系统管理 / 网络 /	接口								
○创建 /编辑	會删除								
	名称				IP/子网掩码				
	m1/1			81.1	.1.1 / 255.255.0.0	)			
	m1/2			82.1	.1.1 / 255.255.0.0				
	m1/3			117.1	.1.1 / 255.255.0.	0			
	m1/4			118.1	.1.1 / 255.255.0.	0			
	port1			192.168.1	.6.2 <mark>44</mark> / 255.255.	255.0			
	port2			8.8.8	.8 / 255.255.255.	0			
	port3			9.9.9	.9 / 255.255.255.	0			
	port4			10.20.9	2.1 / 255.255.25	5.0			
	port5			10.20.8	31.1 / 255.255.25	5. <mark>0</mark>			
	port6			10.20.9	91.1 / 255.255.25	5.0			
	port7			77.1	.1.1 / 255.255.0.0	)			
	port8			78.1	.1.1 / 255.255.0.0	)			



## 3.2 配置防火墙策略

#### 进入到防火墙策略配置界面:

KFW	监控▼	系统管理-	路由▼	防火増→	病毒与攻击	<ul> <li></li></ul>	VPN+	设置用户→	日志与报告
系统管理 / 控制面板	反/ 状态			策略		策略			
0 控件				地址	×.	显式NAT表			
-				服务	E.	DDoS策略			
系统信息				时刻表	E.	探测策略		00	00
客户名称			SN not	流量整形器	•	IPv6策略			
序列号			APW1K	-E-HITD		14.20024175			
主机名			APW1K	REPAIR		1974,20,256,444		更	改]
持续运行时间			6天17	负载均衡	•				
系统日期			Mon Jai	IPMAC绑定	≞ ▶			[更	改]
AV特征值			33.156	(升级 2017-11	08)			印	级]

#### 点击创建增加防火墙策略:

KFW	监控▼	系统管理・	路由▼	防火墙-	病毒与攻击・	上网行为管理•	VPN -	设置用户+	日志与报告+
防火墙 / 策略 / 策略									
◎创建 - 》编辑 -	自由除	11 移动到	•0 插入						

#### 配置策略内容:

KFW	监控+	系统管理-	路由- 防火	/墙→ 病毒与攻击→	上网行为管理-	VPN-	设置用户	日志与报告・
防火墙(策略)	策略							
								新建输出策略
源接口/区	m1/1							
源地址	all		* 3	<b>I</b> 多选				
目的接口/区	m1/2		~					
目的地址	all		* 2	1多选				
时刻表	always		~					
服务	[多选]		* 8	<b>多选</b>				
动作	DENY							选择多个服务
□ 记录拒绝流量					可用的服	务:		
注释 (最大63个字	符)							00
					成员:	各		
					FTP	550		
- <del>1</del>					SNMP			选择配置策略中的服务,
					· · · ·			此处选择了 FTP服务、HTTP服务、SNMP服
								劳
								~
								OV. BIDW
								UK UA

#### 最后的效果如下:

KFW	<b>1</b>	空- 系统1	ē理→ 路6	自- 防火	<b>培▼ 病毒</b> 与攻击▼	上网行为管理。	VPN-	设置用户,	日志与报告。					🛔 admin 🛛 🕞
防火墙 / 策略	/ 策略													
O (1)3≩ ∕ :	祖 - 自樹	e 11 移动至	り も 插入	■ 检査									[列设定]) 日 載	于接口查看 ④ 清单式查看
	序列	5	τi	枵	TΞ	て目的		て源地	tik 🛛	▼ 目的地址	▼ 副刻表	T 165	T 动作	▼ 状态
	1		2	i	m1/1	m1/2	0	all		o all	always	FTP     HTTP     SNMP	DENY	Ø



## 4. 设置 Supernova 测试仪

## 4.1 防火墙转发策略检测用例配置

新增防火墙转发策略检测测试用例:

<b>     阿测科技</b> netitest.com	шен [[]]	<b>0</b>	戸町線	金腔	派告	a Y Mile	admin					V20.12.06	Super	rnova-88D
E MXIGANIC O	转发算	明检测												
O (CHEIGRANILE O	专试与新	医多糖打开指闭	<b>走的绸口建立</b> 连	接,客户隅发;	送syn报文,通	过接收服务器	greset或者syn+ack的回	1应报文,来判断防火爆的)	#略是阻断还是通过。					
📓 алияла ө 🛛 🕄														
ti saapaat o	用例列													
⑦ 系统安全制品 Θ           由安全性制度	+ =		1850											
● DDoS映曲		编号	版行	任务列表	用户	ME-18 00 /	1201:175	\$1Q		565E	克隆	详细信息	母出	历史记录
C 吸出洗量量效	显示行的	<b>R:</b> 10 🗸	0 - 0 of 0			201年用15	125块							
> 转发田崎检测							IP/tx		1					
							党団役首奏							
K MIS201115 0 0							交对设置上行机	<ul> <li>EB由模式(NAT) @</li> </ul>	1					
							网络配	查 默认模板 ~	•					
								niz Riji						

#### 设置填写用例配置中 IP 地址: (此处 ip 地址与拓扑中一致)

基本信息(1	传发策略检测)							
	用例名称	FirewallPolicy_NA 合法字符类型: A-Z / a	T_admin_20210122-15:21:05 z / 0-9 / : / - / _ (不变持中文符号)					
网络	参数	记录						
保存网络设置 客户端 port1					服务端 port3	选择测试仪与防火墙连通的测试口		
◎ 禁用第口				MAC 90:e2:batee:92:50	⊘ 無用調口			MAC 90:e2:ba:ed:b5:74
子网 😡					子网 😡			
第1个子网					第1个子网			测试服务器端充当的测试
	2	list仪端口IP地址或范围	81.1.2.2	测试客户端充当的测试IP		测试仪端口IP地址成范围 82.1.1.100	0	IP
		测试仪跳口子网掩码	16 😡			测试仪端口子网掩码 16	0	
		测试仪跳口网关	81.1.1.1	客户端测试口连接防火墙端	口的IP	测试仪跳口网关 82.1.1.1	0 10	服务器端测试口连接防火 墙端口的IP

#### 设置用例扫描端口:

基本信息(转发策略检测)	
用例名称 日	FirewallPolicy_NAT_admin_20210122-15-21.05 生学符码型、A-27.a-27.0-97.1-7.(不变)中于文符号)
网络  参数	记录
用例参数 通用参数	
	(分類第二)         112250-45310           2010年7月1日、日本1271, 22, 80, 441, 102*           2010年7月1日、日本1211, 22, 80, 441, 102*           2010年7月1日、日本11, 122, 124, 240-1000, 10021-65535*           2010年7月1日日、日本11, 122           2010年7月1日日、日本11, 122           2010年8月1日、日本11, 122           2010年8月1日、日本11, 122           2010年8月1日           2010年8月1日           2010年8月1日           2010年8月1日           2010年8月1日           2010年8月1日           2010年8月1日           2010年8月1日           2010年8月1日           2011年8月1日           2011年8月1日           2011日           2011日 <tr< td=""></tr<>
	fina (947) Nois



### 4.2 启动测试用例

用例配置后,可点击【启动】直接运行测试用例:

基本信息(转	发羊畜检测)	F						
	用例名称	FirewallPolicy_NAT_adm 合法字符典型: A-Z / a-z / 0-5	nin_20210122-15:21:05					
网络 保存网络设置 客户端 port1	参数	记录			服务端 port5 port3			
◎ 禁用號口				MAC 68:91:d0:63:47:b4	◎ 禁用號□			MAC 68:91:d0:63:4b:54
子网 😡				•	子网 😧			
第1个子网		Rickand Patalan (1999) Rickand Paters Rickand Rickans	81.1.2.2 16 81.3.1.1	• • 2 •	<b>第</b> 1个子间	REFORMED FROM THE REF	82.11.100 16 62.11.1	0 0 20
				尼动	6877 4076			

# 4.3 用例运行及查看报告

用例启动后,正常运行界面如下:

用例名称 FirewallPolicy_NAT_admin_20200106-11:27:45	用例类型:转发策略检测	测试用户: admin		◎ 帶止
port1				
客户 <b>供</b> →服务器				
學近的100个结果:				
服务	端口ID		状态	协议
ftp	21		filtered	tcp
ssh	22		open	top
http	80		filtered	tcp
snmp	161		filtered	top
https	443		open	tcp

#### 用例运行结束,可点击【查看历史】查看运行报告:

用例名称: FirewallPolicy_NAT_admin_20200106-11:27:45	用例类型:转发集略检测	测试用户: admin	這行結果:●成功 [盘囊历史]			<b>考</b> 爾次還行
port1						
客户講=>服务器						
最近的100个结果:						
服务	端EIID			Ko	10-12	
ftp	21			filtered	tcp	
ssh	22			open	top	
http	80			filtered	tcp	
snmp	161			filtered	tcp	
https	443			open	tcp	

通过运行报告数据,查看防火墙转发策略是否生效:

★ 期次差行 22. 現象 団 神信 ○ 母出PDF										
pert										
■ 金融→服务器 数据流量访问方向										
最近的100	0个结果:									
编号	服务	端口ID	状态		协议					
1	ftp	21	filtered	filtered表示服务端口访问被过滤阻L	L <sub>tcp</sub>					
2	ssh	22	open		tcp					
3	http	80	filtered		tcp					
4	snmp	161	filtered		тср					
5	https	443	open	open表示服务端口访问正常允许	tcp					
显示行费	8: 10 ~ 1-5 of 5 测试扫描的服务及端					« 1 »				

可以看出防火墙设置的转发策略生效。