(m) F1000防火墙策略NAT开启自动生成安全策略后访问异常

NAT444 曾招维 2024-04-30 发表

组网及说明

设备型号F1000-AI-65,版本CMW710-R8860P43

组网:

PC (10.1.1.1) ---- (20.1.1.1:80) FW---- (30.1.1.1:8080) 服务器 需求:

PC通过访问防火墙接口地址20.1.1.1:80,实现访问内网服务器30.1.1.1:8080的需求。客户在防火墙新 建策略NAT实现nat server需求,为了减少配置工作量在高级设置中点击自动生成安全策略。

问题描述

安全域、路由正常,按下面步骤新建策略后发现访问服务器失败。





f建策略NAT		?×
启用规则		
统计		
高级设置		
转换前报文所属VRF	公网	
转换后报文所属VRF	公网	
自动生成安全策略	🗹 (更新) 🕐	
名称	GlobalPolicyRule_27_SecPolicy	*
源安全域	请选择安全域	[多选]
目的安全域	请选择安全域	[多选]
源IP地址	 ● 地址? ○ 地址对象组 	
	10.1.1.1	
目的IP地址	 ● 地址^⑦ ○ 地址対象组 	
	30.1.1.1	
服务	80	[多选]
VRF	公网 🗸	
	确定取消	

```
过程分析
```

ice 80.

```
1、确认web页面配置在命令行中的回显,如下:
#
object-group service 80
0 service tcp destination eq 80
#
#
nat global-policy
....
rule name GlobalPolicyRule_27
service 80
 source-ip host 10.1.1.1
destination-ip host 20.1.1.1
 action dnat ip-address 30.1.1.1 local-port 8080
#
#
security-policy ip
...
rule 6 name GlobalPolicyRule_27_SecPolicy
action pass
 source-ip-host 10.1.1.1
 destination-ip-host 30.1.1.1
 service 80
#
2、参考案例https://zhiliao.h3c.com/Theme/details/184124, 全局NAT先做目的NAT再进行安全策略的
匹配,防火墙新建策略NAT,在高级设置中点击自动生成安全策略,自动生成的安全策略放通的对应
源地址(10.1.1.1)和目的地址(30.1.1.1)是正确的,但是放通的服务 service 80 是nat转换之前的
端口。
3、再返回去看web上面配置,勾选"自动生成安全策略"后,默认的服务就是目的nat转换前的服务 serv
```

新建策略NAT			@×
启用规则			^
统计			
本保设管			
₩ 検強前招			
ACCOUNT OF A DESCRIPTION	公M	Ŧ	
转换后报文所属VRF	公网	$\overline{\mathbf{v}}$	
自动生成安全策略	☑ [更新] 🥐		
名称	GlobalPolicyRule_27_SecPolicy		*
源安全域	请选择安全域	Ŧ	[多选]
目的安全域	请选择安全域	~	[多选]
源IP地址	● 地址⑦ □ 地址对象组		
	10.1.1.1		
目的IP地址	◉ 地址 ⑦ 地址对象组		
	30.1.1.1		
		_	
版务	80	Ŧ	[多远]
VRF	公网	~	
			~
	确定取消		

解决方法

由于目的NAT转换前后对应的端口不同,开启自动生成安全策略后生成的服务无法匹配,导致无对应放通策略。通过新建一个service 8080,然后在安全策略中指定后正常。

```
#
```

object-group service 8080 0 service tcp destination eq 8080

```
#
```

security-policy ip

```
...
rule 6 name GlobalPolicyRule_27_SecPolicy
action pass
source-ip-host 10.1.1.1
destination-ip-host 30.1.1.1
service 8080
```

#