网络相关 韦家宁 2024-09-14 发表

组网及说明



组网说明:

本案例采用ENSP模拟器的防火墙来部署Basic NAT,安全域和内网、外网在网络拓扑图中已经有了明确的标识,FW1作为出口设备与外网连接,某局点申请到了202.1.100.2-202.1.100.4的公网地址,通过Basic NAT的方式,实现内网访问外网。

配置思路:

- 1、按照网络拓扑图配置IP地址。
- 2、配置FW1的安全策略。
- 3、配置FW1的Basic NAT。

配置步骤

R1: <Huawei>u t m Info: Current terminal monitor is off. <Huawei>u t d Info: Current terminal debugging is off. <Huawei>system Enter system view, return user view with Ctrl+Z. [Huawei]sysname R1 [R1]int gi 0/0/0 [R1-GigabitEthernet0/0/0]ip address 202.103.224.1 24 [R1-GigabitEthernet0/0/0]quit [R1]int gi 0/0/1 [R1-GigabitEthernet0/0/1]ip address 202.1.100.1 29 [R1-GigabitEthernet0/0/1]quit

FW1:

<USG6000V1>u t m Info: Current terminal monitor is off. <USG6000V1>u t d Info: Current terminal debugging is off. <USG6000V1>system Enter system view, return user view with Ctrl+Z. [USG6000V1]sysname FW1 [FW1]int gi 1/0/2 [FW1-GigabitEthernet1/0/2]ip address 192.168.10.1 24 [FW1-GigabitEthernet1/0/2]quit [FW1]int gi 1/0/1 [FW1-GigabitEthernet1/0/1]ip address 202.1.100.2 29 [FW1-GigabitEthernet1/0/1]quit [FW1]ip route-static 0.0.00 0.0.0 202.1.100.1 [FW1-zone-trust]add int gi 1/0/2 [FW1-zone-trust]quit [FW1]firewall zone untrust [FW1-zone-untrust]add int gi 1/0/1 [FW1-zone-untrust]quit

[FW1]security-policy [FW1-policy-security]rule name 1 [FW1-policy-security-rule-1]action permit [FW1-policy-security-rule-1]source-address 192.168.10.0 24 [FW1-policy-security-rule-1]source-zone trust [FW1-policy-security-rule-1]destination-zone untrust [FW1-policy-security-rule-1]quit [FW1-policy-security]quit

[FW1]nat address-group 1 10 [FW1-address-group-1]section 202.1.100.3 202.1.100.4 [FW1-address-group-1]quit [FW1]nat statistics enable

[FW1]nat-policy [FW1-policy-nat]rule name 1 [FW1-policy-nat-rule-1]source-address 192.168.10.0 24 [FW1-policy-nat-rule-1]action source-nat address-group 1 [FW1-policy-nat-rule-1]source-zone trust [FW1-policy-nat-rule-1]destination-zone untrust [FW1-policy-nat-rule-1]enable

内网的PC和外网的PC分别填写IP地址,内网的PC能PING通外网的PC,但是外网的PC无法PING通内网的PC,说明NAT已经生效。

基础配置 命	令行 组播	UDP发包工具	串口		
主机名:					
MAC 地址:	54-89-98-F6-3D-11				
IPv4 配置					
○ 静态	ODHOP		🗌 自动获	取 DNS 服务器地址	
IP 地址:	192 . 168 . 10	. 2	DNS1:	0.0.0.0	
子阿摘码:	255 . 255 . 255	5.0	DNS2:	0 . 0 . 0 . 0	
网关:	192 . 168 . 10	. 1			
IPv6 配置					
○静态	O DHCPv6				
IPv6 地址:	::				
前缀长度:	128]			
IPv6 网关:	::				

E PC2			_ 🗆 X
基础配置命令	令行 組織 UDP发包工	串口	
主机名:			
MAC 地址:	54-89-98-C8-4F-04		
IPv4 配置			
○静态	ODHCP	□ 自动获取 DNS 服务器地址	
IP 地址:	202 . 103 . 224 . 68	DNS1: 0 . 0 . 0 . 0	
子网攬码:	255 . 255 . 255 . 0	DNS2: 0 . 0 . 0 . 0	
网关:	202 . 103 . 224 . 1		
IPv6 配置			
○ 静态	O DHCPv6		
IPv6 地址:			
前缀长度:	128		
IPv6 网关:			
			应用

E PC1



E PC2

基础配置 命令行 组播 UDP发包工具 串口 Welcome to use PC Simulator! PC>ping 192.168.10.2 Ping 192.168.10.2: 32 data bytes, Press Ctrl_C to break Request timeout! Request timeout! Request timeout! Request timeout! Request timeout! -- 192.168.10.2 ping statistics ---5 packet(s) transmitted 0 packet(s) received 100.00% packet loss

查看NAT地址组的状态是激活的。

```
[FW1]dis nat address-group
2024-09-14 04:13:54.020
NAT address-group information:
Total 1 address-group(s)
nat address-group 1 10
reference count: 1
mode pat
status active
section 0 202.1.100.3 202.1.100.4
[FW1]
```

查看防火墙的会话表,发现会话表的源地址已经转换后访问外网。

[FW1]dis firewall session table								
2024-09-14 (04:15:31.670							
Current Tot	tal Sessions :	19						
icmp VPN:	public> pub	lic 192.168.	10.2:53005[202.1.	.100.4:2556]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:51981[202.1.	.100.4:2552]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:51725[202.1.	.100.4:2551]	> 202.103.			
224.68:2048		14- 100 100	10.0.40/2020.0	100 4-05401	> 000 100			
1Cmp VPN:	public> pur	11C 192.168.	10.2:48653[202.1.	.100.4:2540]	> 202.103.			
224.00:2040	public> pub	110 102 169	10 2:490001202 1	100 4+25411	> 202 103			
224 68 2048	public> pu	110 192.100.	10.2.10505[202.1.	.100.4.2541]	> 202.103.			
icmp VPN:	public> pub	lic 192,168.	10.2:52493[202.1.	100.4:25541	> 202.103.			
224.68:2048	passing pass							
icmp VPN:	public> pub	lic 192.168.	10.2:50701[202.1.	.100.4:2547]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:51469[202.1.	.100.4:2550]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:53261[202.1.	.100.4:2557]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:49165[202.1.	.100.4:2542]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:49933[202.1.	.100.4:2545]	> 202.103.			
224.68:2048								
1cmp VPN:	public> pub	11C 192.168.	10.2:52237[202.1.	.100.4:2553]	> 202.103.			
224.68:2048		14- 100 100		100 4-05401				
1Cmp VPN:	public> pur	11C 192.168.	10.2:49421[202.1.	.100.4:2543]	> 202.103.			
icmp VPN.	public> pub	lic 192 168	10 2:496771202 1	100 4+25441	> 202 103			
224.68:2048	public> pu	110 152.100.	10121120011[20211]	.100.1.2011]	> 20212001			
icmp VPN:	public> pub	lic 192.168.	10.2:50445[202.1.	.100.4:25461	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:53517[202.1.	.100.4:2558]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:51213[202.1.	.100.4:2549]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:50957[202.1.	.100.4:2548]	> 202.103.			
224.68:2048								
icmp VPN:	public> pub	lic 192.168.	10.2:52749[202.1.	.100.4:2555]	> 202.103.			
224.68:2048								
[FW1]								

至此,华为防火墙Basic NAT典型组网配置案例已完成!