SSL VPN 张新姿 2021-03-03 发表

## 组网及说明



## 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:本案例适用于如F5080、F5060、F5030、F 5000-M等F5000、F5000-X系列的防火墙。

注:本案例是在F1000-C-G2的Version 7.1.064, Release 9323P19版本上进行配置和验证的。

## 1.2 配置需求及实现的效果

路由器设备作为出口设备,防火墙旁挂,外网PC通过inode软件拨SSLVPN,认证成功后可以访问内网的资源。

# 2组网图



#### 配置步骤

# 1 配置步骤

## 1.1 路由器配置

设置路由器出0口地址222.1.1.100, 配置nat outbound,以及针对内部的提供服务的端口号修改为1443

3,缺省端口为443,443端口和https端口冲突,然后配置nat server映射对应的端口

[H3C]interface GigabitEthernet0/0

[H3C-GigabitEthernet0/0]ip address 222.1.1.100 255.255.255.0

[H3C-GigabitEthernet0/0] nat outbound [H3C-GigabitEthernet0/0] nat server protocol tcp global 222.1.1.100 14443 inside 192.168.40.2 14443

设置路由器内网接口地址为192.168.30.2

[H3C]interface GigabitEthernet0/1

[H3C-GigabitEthernet0/1] ip address 192.168.30.2 255.255.255.0 [H3C-GigabitEthernet0/1]

路由器设置针对内网的网段路由:

[H3C] ip route-static 0.0.0.0 0 222.1.1.200 [H3C] ip route-static 192.168.0.0 16 192.168.30.1

#### 1.2 配置交换机和防火墙以及路由器互联

#配置策略路由保证内网的数据可以上送到防火墙设备 [H3C]acl ad 3000 [H3C-acl-ipv4-adv-3000] rule 10 permit ip source 192.168.20.0 0.0.0.255 destination 10.10.10.0 0.0.0 .255 [H3C-acl-ipv4-adv-3000]quit [H3C]policy-based-route aaa permit node 10 [H3C-pbr-aaa-10] if-match acl 3000 [H3C-pbr-aaa-10] apply next-hop 192.168.40.2 [H3C-pbr-aaa-10]quit #配置对应的ip地址和调用策略路由 [H3C]interface Vlan-interface2 [H3C-Vlan-interface2] ip address 192.168.20.1 255.255.255.0 [H3C-Vlan-interface2] ip policy-based-route aaa [H3C-Vlan-interface2]quit [H3C]interface Vlan-interface3 [H3C-Vlan-interface3] ip address 192.168.30.1 255.255.255.0 [H3C-Vlan-interface3]quit [H3C]interface Vlan-interface4 [H3C-Vlan-interface4] ip address 192.168.40.1 255.255.255.0 [H3C-Vlan-interface4]quit #配置相应的路由 [H3C] ip route-static 0.0.0.0 0 192.168.30.2 1.3 配置静态路由

### #选择 "网络">"路由">"静态路由"点击"新建",目的IP地址填写0.0.0.0,掩码长度填写0,下一跳I P地址填写连接核心交换的对端的地址192.168.40.1,点击"确认"完成配置

HBC 50		0	0		•	Ð	() N 10				
1945	Pressa manage		_								
W VRF	98	(H (	DER XI	179			_		1846.5.8	18540903.8	Q RR E RERR
00 HCI	新闻和Pv4基本和由						0×	HMC .	DAVID	H.d.	10.0
♥ 安全城	C								0		۲
<ul> <li>✓ 6535</li> </ul>		524							0		1
BIDNS	E BROPRESE	0.0.0.0			-			661/0/0	0		8
0 Dip	C NECK					(0-32)			0		1
· El IPv6	¥-#.0	T-BARRENT									
O S VPN		C10825									
IN SSL VPN		102577									
*****		T-BPRX									
- BAR		192.168.40.1									
· MALING	四中23日 0	60				1-255. BPM(2660)					
- OSPF											
+ BGP	manua O	0				0-4294967295, 89	8(790)				
· RIP	84					(1-60913)					
© d' 11115											
· OHCP											
◎_2 服务		- 46	2 5	275							型目1-4条,共4条
		Copyright	MD 2004-2	020 8691710	-	NOTION OR	100281				

#选择 "网络">"SSL VPN">"网关"点击"新建",IP地址填写防火墙1口地址192.168.40.2,端口号 修改为14443,缺省端口为443,443端口和https端口冲突。勾选"使能"选项点击"确认" 完成配置

配置关键点				
HBC SecPath F1010		0 C		almin = Q.H @ C
1、本案例适应的是默认证于	, 不需要手上导	人CA证F	动和本地止常	V97 (256) 668
2、不需要配置SSL服务器端	策略, SSLVPN	网关不需	要引用SSL服务	5器端策略
3、交换机上需要将对应的流	量通过策略 <mark>路由</mark>	形式引到	防火墙进行处	理, 以免数据来回路径不一致
C IIPv6 C VPN	HTTPSUILE 4433	建议修改端口	- (1025-05515, M28(2)443)	
SSL VPN)	开启HTTP加速度已			
· CPSEM	HTTHREE 80		(1025-65515, \$P\$\$62980)	