NAT zhiliao_FO3qD 2018-11-25 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于如F5080、F5060、F5030、F5000-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 9323P1801版本上进行配置和验证的。

1.2 配置需求及实现的效果

将防火墙部署在公司核心网络下为财务部门提供网络安全防护,要求防火墙使用3接口自动获取公司内 网地址,4接口连接财务部为财务部用户动态下发192.168.10.0网段地址。在对公司原有网络影响最小 的情况下实现财务部电脑可以访问防火墙以外的网络,防火墙以外的网络不能访问财务部电脑的需求





配置步骤

3 配置步骤

3.1 基本登录

#在防火墙接口面板找到0接口,用网线将电脑和设备的0接口连在一起,电脑配置与设备管理IP相同网段的地址192.168.0.2/24,下面是电脑IP地址配置方法:

点击电脑右下角电脑图标,选择"打开网络和共享中心"选项。





更改网络设置

#鼠标双击"Internet协议版本4"打开属性菜单,按照下面图片内容配置电脑IP地址。



#电脑IP地址配置完成后打开浏览器,在浏览器地址栏中输入<u>https://192.168.0.1</u>登录设备管理界面。设备默认用户名密码均为admin。



3.2 配置外网接口

#在"网络">"IP"选项中选择1/0/3接口并点击此接口最后面的"编辑"按钮。

НЗС	SecPath F1000-C-G2	() 概览 监控 策	
导航	« IP		
- VRF	●新建 前時除 ○ 粉新 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	往杰	TPidelub
🎦 接口	227 H	1/25	TI JEJE
- 接口	GigabitEthernet1/0/1	down	
- 接口对	GigabitEthernet1/0/2	down	
链路聚合	GigabitEthernet1/0/3	up	
- 安全域	GigabitEthernet1/0/4	up	
■ 链路	GigabitEthernet1/0/5	down	
DNS	GigabitEthernet1/0/7	down	
P IP	GigabitEthernet1/0/8	down	
TP	GigabitEthernet1/0.9	down	**
APP	GigabitEthernet1/0/10	down	
AN	GigabitEthernet1/0/11	down	192.168.199.1/255.255.2

#"IP地址"选择"通过DHCP自动获取IP地址",并点击"确定"按钮。

修改IP配置		
接口 状态	GigabitEthernet1/0/3 (GE1/0/3) down	
描述 IP地址	GigabitEthernet1/0/3 Interface ② 指定IP地址 ③ 通过DHCP自动获取IP地址	O PPPoE
	确定取消	

3.3 配置内网接口

#在 "网络">"IP" 选项中选择1/0/4接口并点击此接口最后面的 "编辑"按钮。

H3C SecPath	F1000-C-G2	▼	対象の経	
导航 《				
UPE	④新建 m ※※ ○ 刷新			
後日	授	状态	IP地址	
- 接口	GigabitEthernet1/0/1	down	-	
- 接口对	GigabitEthernet1/0/2	down		
销路聚合	GigabitEthernet1/0/3	up	-	
- 安全抵	GigabitEthernet1/0/4	up	-	
1:492	GigabitEthernet1/0/5	down		
DNS	GigabitEthernet1/0/7	down		
	GigabitEthernet1/0/8	down		
TP	GigabitEthernet1/0/9	down	-	
100	GigabitEthernet1/0/10	down		
AKP	GigabitEthernet1/0/11	down	192.168.199.1/255.255.2	

#"IP地址"填写规划的内网地址192.168.10.1, 掩码为255.255.255.0。

修改IP配置				
接口 状态 描述 IP地址 IP地址/描码长度	GigabitEthernet1/0/4(GE) up GigabitEthernet1/0/4 Interfi ④ 指定IP地址 192.168.10.1	1/0/4) ace 通过DHCP自动 / 255.25	获取IP地址 5.255.0	PPPoE
	 ● 新建从IP地址 □ 从IP地址 	· 前 道 前 前 前 一	删除从IP地址 编辑 取消	

3.4 配置NAT地址转换

#在"策略">"NA"T>"NAT动态转换">"策略配置"选项中点击"新建"。



#"接口"选择外网接口1/0/3,转换后源地址选择"接口IP地址"并点击"确定"。



3.5 配置外网接口加入Untrust安全区域

#在 "网络">"接口">"安全域" 中选择Untrust区域点击"编辑"按钮。

HBC SecPar G2	th F	〒1000-C- 〇〇 一 戦策 高校			
导航 《	安	全域			
VRF	€	新建 🧰 删除 📭 按页面显示导出 📿 刷新			
■ :8□		安全域名称	成员个数		
- 安全城		Local			
■ 链路	-		4		
DNS		Trust			
IP IP		DMZ	0		
IPv6		Untrust	0		
VPN		Management	0		

#在"三层成员列表"中将1/0/1接口加入成员列表。

修改安全域			?
安全域名称	Untrust	• (1-31字符)	
VLAN成员列表 ⑦		(1-4094)	
二层成员列表	接口列表	成员列表	
		*	
		•	
		•	
		*	
三层成员列表	接口列表	成员列表	
	Dia0 GE1/0/10	GE1/0/3	
	GE1/0/12	*	

3.6 配置内网接口加入Trust安全区域

#在 "网络">"接口">"安全域" 中选择Trust区域点击"编辑"按钮。

HBC s	ecPat	n F1000-C-	→ 监控	策略	对象	國的
导航		安全域				
VRF		🕣 新建 🧰 删除 👔 按页面显示导出 🂭 刷新				
= :#□		🗇 安全域名称		成员个数		
安全域		Cocal				
葡萄路						
DNS		Trust		4		

#在"三层成员列表"中将1/0/4口加入成员列表。

安全域名称	Trust	* (1-31字符)
VLAN成员列表 ②		(1-4094)
二层成员列表	接口列表 GE1/0/6	成员列表 → ← 後
三层成员列表	接口列表 GE1/0/20	成员列表 GE1/0/4

3.7 配置安全策略将Trust到Untrust域内网数据放通

#在"安全策略"中点击"新建"。

НЗС	SecPath G2	n F	100	0-C-		() 競	★ 监控	策略
导航	*	安全	論略						
安全策略			听建		(1) ↓ 移动 (1) ↓ 移动	○ 统计	0 W	尚统计 ⊘ №	明 〇 新
安全防护		安全	策略配	查受更之后(?)	需要 立即加速	才能生效。	内容安全	自能宣受更之后	(?),需要
NAT			名称	源安全域	目的安全域	类型	ID	描述	源地址
➡ 应用审计			ljs			IPv4	3		
■ 帯宽管理			2			IPv4	1		

#"源安全域"选择Trust, "目的安全域"选择Untrust, 在源IP地址中选择"添加 IPV4地址对象组"。

名称		*(1-127字符)
原安全域	Trust	▼ [多选]
目的安全域	Untrust	▼ [多选]
世辺	● IPv4 ◎ IPv6	
苗述信息		(1-127字符)
动作	 允许 ⑦ 拒绝 	
原IP地址	请选择或输入对象组	▼ [多选]
	▲ 法fmTPv4批批对条组	[名进]

#对象组名称输入内网,点击"添加"按钮添加地址对象,添加内网192.168.10.0网段。点击"确定"完成策略配置。

新建IPv4地址对	象组			? X
对象组名称 描述	内网			*(1-31字符) (1-127字符)
安全域	Trust			•
⑦ 添加 前 一 ※刑 添加对象	删除	山谷	北瓜	dittetis ? X
对象 🕐	网段		~	
	192.168.10.0	/ 255.255.255.0	* ([IPv4地址/掩码长度0-32)
排除地址 📀				
		确定 取消		
		确定 取消		

3.8 配置安全策略将Trust到Local域、Local到Trust域数据全放通策略

#在"安全策略"中点击新建。

HBC SecPat	h F1	1000-	C-		(D IR	★ 监控	日 策略
导航 《	安全	策略						
安全策略	 新 			○利 ◆ 移动 売売 ☆ BD bo はあ	 ○ 统计 		院计 ⊘ ⋒	
 安全防护 NAT 	TE 1	名称	源安全域	新安 立即加速 目的安全域	为能生xx。 类型	ID	描述	源地址
■ 应用审计		ljs			IPv4	3		
➡ 带宽管理		2			IPv4	1		

#创建策略名称为互通,源安全域、目的安全域选择多选,并选中Local、Trust。

新建安全策略					?
名称	互通			*(1-127字符)	^
源安全域	请选择源安	全域	*	[多选]	
目的安全域	请选择目的	安全域	*	[多选]	
类型	● IPv4	© IPv6			
描述信息				(1-127字符)	
动作	◎ 允许	◎ 拒绝			
源IP地址	请选择或输	认对象组	*	[多选]	
#配置成功显示结果,点	京击"确定"完	成策略配置。			

互通	=符)
◉ 允许 ◎ 拒绝	
请选择或输入对象组 🖌 [多选]	
请选择或输入对象组 🗸 [多选]	
请选择服务 🛛 🗸 [多选]	
请选择应用	
请选择应用组 🛛 🖌 [多选]	
请选择用户	
请选择时间段	
公网 🗸	
2011 a	
NONE	
NONE	
NONE	
	互通 * (1-127号 Trust, Local 「多法」 Local, Trust 「「多法」 ● IPv4 ● IPv6 ① IPv4 ● IPv6 「1-127字 (1-127字) ● 允许 ● 拒绝 请选择或输入对象组 「多选」 「清选择服务 「多选」 「清选择服务 「多选」 「清选择应用組 「多选」 「清选择可用組 「多选」 「清选择可用組 「多选」

3.9 配置安全策略将Untrust到Local域、Local到Untrust域DHCP数据放通策略

#在"安全策略"中点击"新建"按钮创建安全策略,"源安全区域"选择Local、Untrust区域,"目的安全域"选择Local、Untrust区域。"服务"选择DHCP-client、DHCP-server。

:主東哨			
马称	放通DHCP	* (1-127字	符) 1
原安全域	Local, Untrust	▼ [多选]	
目的安全域	Local, Untrust	▼ [多选]	
世世	● IPv4 ◎ IPv6		
苗述信息		(1-127字符	夺)
动作	● 允许 ◎ 拒绝	xx	
动作	● 允许 ◎ 拒绝	xx	
动作 原IP地址	 允许 拒绝 36:22 请选择或输入对象组 	▼ [多选]	
动作 原IP地址 目的IP地址	 ① 允许 ② 拒绝 ③6:22 ③请选择或输入对象组 ·请选择或输入对象组 	xxx × [多选] × [多选]	
动作 原IP地址 目的IP地址 服务	 ⑥ 允许 ⑦ 拒绝 ③ 请选择或输入对象组 ③ 请选择或输入对象组 dhcp-client, dhcp-server 	 ✓ (多选) ✓ (多选) ✓ (多选) 	
的作 東IP地址 目的IP地址 長务 立用	 ① 抗许 ② 抗许 ② 拒绝 ③ 清选择或输入对象组 ③ 请选择或输入对象组 dhcp-client, dhcp-server 请选择应用 	xx × [序遗] × [序遗] × [序遗] × [序遗]	
动作 頭IP地址 目的IP地址 反务 立用 立用组	 分许 ● 拒绝 ^{36:22} ·请选择或输入对象组 ·请选择或输入对象组 dhcp-client, dhcp-server ·请选择应用 ·请选择应用组 	xx × [多遗] × [多遗] × [多遗] × [多遗] × [多遗] × [多遗]	
动作 頭IP地址 目的IP地址 長务 立用 组 刊 用 日	 分许 ● 拒绝 奇选择或输入对象组 奇选择或输入对象组 奇选择或输入对象组 dhcp-client, dhcp-server 请选择应用 请选择应用组 请选择用户 	xx × (多速) × (多速) × (多速) × (多速) × (多速) × (多速) ×	
动作 mpr 地址 目的IP地址 极务 立用 组 刊 时 向殿	 允许 ● 拒绝 36:22 请选择或输入对象组 请选择或输入对象组 dhcp-client, dhcp-server 请选择应用 请选择应用组 请选择应用组 请选择时间段 	xx × (多速) × (多速) × (多速) × (多速) × (多速) × (多速) × (多速) × (多速) × (多速)	

3.10 配置DHCP服务

#在"网络">"DHCP">"服务"中开启DHCP服务。

HBC SecPat	h F1000-C-
导航 《	DHCP
- VRF	
	DHCP(Dynamic Host Configuration Protocol,如此主机配置而及)用来为两倍设置和态地分配PP起近电机
安全域	
■ 链路	DHCP服务 III 开启
DNS	
IP IP	
IPv6	
VPN	
SSL VPN	
2 路由	
■ 組織	
DHCP	
- 服务	
地址池	

#在 "网络">"DHCP">"地址池"中新建地址池,名称设定为内网。

H3C SecPat	h F1000-C-	対象 网络
986 «	地址地	
VRF	1	▼ 葡 删除 → 新建地址池
■ 接口	地址分配 地址池选项 已分配地址	
安全域	新建DHCP服务器地址泡	? X
■ 槌路		(1.5)
DNS	地址记名称 内网	(1-03-9-14)
Ib Ib	takin Dick	
IPv6	PRAE AURI	硬件地址/1
VPN		
SSL VPN		
DHCP		
- 服务		
地址池		

#设置"地址分配"的地址段为192.168.10.0后点击"确定"。

也址池				
内网			▼ 💼 删除	⊕ 新建地址池
地址分配 地址池选项 已分	配地址			
动态分配的地址段 🕢	192.168.10.0	/ 255.255.255.0		
静态绑定的地址列表				
⊕ 新建 前 删除				
IP地址	掩码		英型	硬件地址/客户端ID

#选择"地址池选项"配置"网关"地址为192.168.10.1点击"确定"按钮,"DNS服务器"地址优先设置当地运 营商提供的DNS服务器地址,如果没有提供可以设置114.114.114.114或8.8.8.8等DNS服务器地址,配 置完成后点击确定。

地址池				
内网		 iii 	删除	⊕ 新建地址池
地址分配	地址池选项	已分配地址		
租约	的有效期限	◎ 无限制 ● 1 天 0 小时 0 分	0	秒
域名	3后缀 🕐			(1-50字符)
网关	¢?	(→ 新建 前 删除		
		网关	编辑	
		192.168.10.1		
		确定取消		
DNS服务器 🕑		 → 新建 前 删除 		
		DNS服务器	编辑	
		114.114.114		
		确定取消		

3.11 保存配置

在设备右上角选择保存选项,点击"是"按钮完成配置。

A 网络	>系统				admin 🔻 🥻
				请输入要查询的信息	
		确认提示		IRF端口状态 ×	
		?	确定要保存设备的当前配置吗? 是 否		

3.12 注意事项

防火墙缺省管理地址为192.168.0.0网段,如果核心网下发给防火墙外网接口也是192.168.0.0网段需要防火墙修改0接口管理地址。

