SSL VPN 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F1080、F1070、F5040、F5020等F10X0、F50X0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

V7防火墙设备作为出口设备,外网PC通过inode软件拨SSLVPN,认证成功后可以访问内网192.168.10.0网段的资源。IP地址及接口规划如下表所示:

,			
外网接口	公网地址/掩码	内网接口	内网地址/掩码
GE1/0/1	222.1.1.100/24	GE1/0/3	192.168.10.1/24

2 组网图



配置步骤

3 配置步骤

3.1 防火墙上网配置

防火墙上网配置请参考"2.2.2 防火墙外网使用固定IP地址上网配置方法"进行配置,本文只针对SSLVP N配置进行介绍。

3.2 配置SSL VPN网关

#选择 "网络">"SSL VPN">"网关"点击"新建", IP地址填写防火墙1口地址222.1.1.1.00, 端口号修改为4 433, 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

liti i	《 网关							
VRF	④ 新建		の刷新					
接口	□ 网关		工作状	\$		IP地址		HTTPSIR
安全域								
1625		新建网关					? X	
DNS								
IP		网关()	SSLVPNGW			*(1-31字符)		
IPv6		IP地址	● IPv4	O IPv6				
VPN			222.1.1.100	此处填写公网	IP地址	(缺省为0.0.0.0	1	
SSL VPN		HTTPSIR	4433	am to an an an	18	(1025-65535	89(875443.)	
- 访问实例		IDUTORRED	11	RE OCTOL CORE	1.9			
网关		THERITPACHECIER					Participant 1	
- 暮户調地址泡		HITPAL				(1025-05535	. 0(197300)	
- 护接入接口		SSL服务器跳绳略				*		
- 统计信息		VRF	公网			~		
路由		(19.82						
組織		1 CONT						
DHCP				确定	取消			

3.3 配置SSL VPN实例

#选择 "网络">"SSL VPN">"访问实例"中点击新",在"关联网关"中点击新建,下拉选择上一步创建的SSL VPN网关,确定后点击"下一步"

НЗС	SecPath F1000-C- G2	C] () () () () () () () () () () () () () () (見え	の数	<♪ 系统	
98	< 300年94							
- VRF 建設 - 安全城 電路路	· 新建 · 新時 · 林達 · 小日本 · · 小日本 · · · · · · · · · · · · ·	○ RMF 工作H本 访问案例(例	SSLVPNSL		* (1	1-31字符)	12.03	7 X
DNS	2 业务选择	关联网关	④ 新建 🗵] 444 📋 11 94				
IPv6	(3) 资源组		□ 网关	访问方式	城	主机名称	编辑	**
SSL VPN · 访问实例 · 网头	-	VRF ISPU(正統	公网	关联网关 访问方式	ss III	LVPNGW 腰访问网关	2 2] 下拉选择之前创建好的同关 。
- 編戸病地北方 - P接入接口 - 统计信息 ■ 路由 ■ 領題		开启检证码检证例 开启还书认证例 开启MC提倡认证例		NON				
DHCP		最大用户数	1048575		(1	1-1048575)		
■ 股外 ■ 採用工具		每用户在线控制()	最大会活数 开启强制下线	32	((0-1048575)		
		每会运量大连接限制。	 开启 最大连接数 上一步 	◎ 关闭 64 下一步	(1	10-1000)		

#勾选"IP业务",然后点击"下一步"

访问实例				
🕀 新建 i 副除 📿 刷新				
🔄 访问实例名称	工作状	あ	网关	服务器地址
新建访问实例				? X
1 基本配置	🥅 Web业务	配置外网用户可以访问的内网	Web资源	
2 业务选择	TCP业务	配置外网用户可以访问的基于1	「CP的内网资源	
	✓ IP业务	配置外网用户可以通过IP接入	客户端访问的内网资源	
ID TO B	I BYOD业务	配置移动客户请使用的服务器		
3 资源组				
		上一步下一步	取消	

#新建SSL VPN接口,接口编号为1,配置SSL VPN接口IP,IP地址不要和内网网段冲突,配置完成点击"确定"。

新建访问实例					,	× VRF			使起	196
1 基本配置	IPER入进口			新建炉接入接口		×1			7	×
2 业务选择	赛户跳地址池 主DNS服务器	XXXX	~	接口编导④	1			* (0-4095)		
1019 11 资源组	做DNS服务器	XXXX		描述				(0-255字符)		
	重WINS服务器	XXXX		VRF	公司					
	保活問期 IP接入把握	30		IPV4地址信息 从IP地址	10.10.10.1 ④新建 前 859	/ 255-255-2	55.0	(IPv42512/96666	EME1-31)	
	 ● 新建 ● 新建 ○ 協助列表 	10 HO 4	子网地址		□ 从IP地址	港 码长度	病情	1		
		上一步下	-9 R.H			执 空 取消				

2 业务选择 3 P25 3 P2	8户調地址池 EDNS服务器	XXXX		新建客户满地址池				,
P25 3	EDNS服务器	XXXX		新建赛户跳地址池				?
1	EDNCE24LBE	主DNS服务器 XXXX 名 愛DNS服务器 XXXX						
3.00105/03	晉DNS服务器			********	SCIVE	NJHORI-DO		• (1, 21 20 20)
B) MANE	EWINS服务器	XXXX		distants	10.10	10.2		
9	ewins服务器	XXXX		结束地址	10.10.	10.100		
é	彩舌周期	30						
(ⁿ	9接入资源			-		确定	取消	
6	●新建 2 4848	<u>iii</u> 2009						
1	3 路由列表		子网地址	掩码	世世	编辑		

#填写客户端地址掩码,主dns服务器地址(可选),在"IP接入资源"中新建路由列表,列表名称为"访问内网",路由列表中添加SSL VPN认证成功后需要访问的内网网段地址,确定后点击"下一步"

新建访问实例						? X	VRF
1 基本配置	IP接入接口	SSLVPN-AC1	~			^	
2 业务选择	客户读地址池	SSLVPN地址地	~				
IDJUST	客户跳地址掩码	24	(1-30)			
17-22.09	主DNS服务器	114.114.114.114	新建路由列表				?
3 资源组	备DNS服务器	XXXX	路由列表名	际 135	间内网	- (1-31字符)
	主WINS服务器	XXXX	路由列表表	Q			
	备WINS服务器	XXXX	⊕ 新建	1959 📸			
	保活問期	30	□ 子网地	址	掩码长度	关型	编辑
	[P摄入资源		新建路由男	项			? X
	⊕新建 ☑ 编辑	1 1959:	ANR1		① 包含 ①	指錄	
	四 路田列表	子网地址	子用地	· ()	192.168.10.0	VPN# A methi	·李要访问的内国网段排
			種研长的		24		(0-32)
						more	
					SHITE	40.0	
		4.5					
		上一步下一步用	8				
					确定	取消	

#新建资源组,组名称为"SSLVPN"资源组,指定路由接入VPN中选择"子网资源",子网资源引用之前 创建的IP路由列表"访问内网",新建IPV4 ACL 3999,只有通过ACL检查的报文才可以访问IP资源

					请输入
访问实例名称	工作状态		同关	服务器地址	VRF
新建访问实例				? X	
1 基本配置	· 资源组	and makes Protest			
2 业务选择	日 近際組名称	NOAL OCCOLUMNICATION		秋市 编辑	
IP业务	anaketeria			7 X	
3 资源组	资源组名称	SSLVPN资源组	* (1-31李符)		
	「PER入 - IPER入 - IPER入				
	指定器曲接入VPN	子网资源	*		
		法资本网	▶ 下位洗径之前的时	?的IP路由列表,名称为"认	前内网"
	子列资源	KUMPER INS	T Interior Activities	and the second descent of the second s	
	子阿贾源 IPv4 ACL	- Constana	* #FaltIPv4ACL		? :
	子利西源 IPv4 ACL IPv6 ACL	40/5/3P3	REEIPv4ACL ACL	3999	* (3000-3999)
	子利西源 IPv4 ACL IPv6 ACL	100000 1000	 新聞IPv4ACL ACL 税利匹配成年 	3999 ● 拉彩配置成序 ①	? (3000-3999) 自动相序
	子利西源 IPv4 ACL IPv6 ACL	() ()))))))	 新聞Pv4ACL ACL 取 成別匹配原序 飲以規則病号步长 	3999 ● 拉特配置信序 ① 5	7 (3000-3999) 回初起序 (1-20)
	子利西源 IPv4 ACL IPv6 ACL	神道	 ▼ 新聞Pv4ACL ▼ ACL 取 規則匹配標序 取以規則编号歩长 振送 	3999 ● 拉特配置初字 ① 5	7 * (3000-3999) 回初即年 (1-20) (1-127年時)
	子科武源 IPv4 ACL IPv6 ACL	(1992) 	 ・ ・	3999 ● 15州配置初序 ① 5	7 * (1000-1999) 回初期年 (1-20) (1-127年時)
	子科武源 IPv4 ACL IPv6 ACL	10-215	 新聞Pv4ACL ACL 規則匹配成序 脱以規則编号か长 振送 	3999 ● 她和政策的本 ① 5	* (3000-3999) 副初編年 (1-20) (1-127年符)
	子外回源 IPv4 ACL IPv6 ACL	(M2)	 ▼ 新聞P+4ACL ▲ ACL ■ 税利回勤前序 ■ 税利回勤前序 ■ 税利回勤満号か长 > 通送 	3999 ● 10%配置的字 ① 5 ② 回時高大の税約 (例	7 目前出来 (1-20) (1-127年符)

#IPV4 ACL 3999中IP协议类型中填写256,256代表任意IP,配置完IPV4 ACL 3999点击"确定",再点击" 完成"

1 10/04/01/01/01	Contractor					VIDE
	 ● 基本配置 ● 业务选择 ● 业务 	登房道 ● 新建	i 💼 804 925446 Roadey		22:00 MR(0)	
	3 20768	activities		REEIP-48ERACL	ADAGRI	*:
		変要総合称 P提入 強制扱入VPN 指定語由語入VPN 子可当源 IPv4 ACL IPv6 ACL	SSLVPN改要组 子和改產 访问内用	ACL編号 規則编号 描述 * * * * * * * * * * * * *	3999 2 回动発导 ● たi平 ① 拒绝 256	(3000-3999號 1-6)个体符) *(0-65534) (1-127字符) (1-127字符)
			<u>後日</u> 上一歩 完成 5	80.64 (F)	 このボアやなど意能対象時 このボアやなどを取ります。 この目がかなどがあります。 この目がかなりがあります。 この目のかないから。 この目のかないから。 この目のかないから。 この目のかないから。 この目のかないから、 この目のかないから、 この目のかないから、 この目のかないから、 この目のかないから、 この目のかないから、 この目のかないから、 この目のかないから、 この目のから、 こののから、 こののから、<	⊖ (CB⊄∰p)

#实例配置完成后勾选"使能"选项来生效配置

🕢 HER 🏥 HER 💭 RHE				這個人要要同的信息	Q, 2018 (C)	電波面:
I 访问案例名称	INKS	用关	服用器地址	VRF	(645	144
SSLVPNSL	● 生效	SSLVPNGW	直接访问同关	公開		

3.4 新建SSL VPN拨号用户,关联SSL VPN策略组

#选择 "对象">"用户">"用户管理">"本地用户"点击"新建", 来新建SSLVPN用户,配置用户名密码,可 用服务中选中SSL VPN

ñ	《 用户 用户组		
用户			
→ 用户管理	目前目的/JAAA865/M88A3767-244	- 1902-011 (1903) - 第995-02 第三人の1018023 555-114日。 描述 授权	用户组
身份识别用户	新建用户		?
■ 认证管理			
■ 接入管理	用户名 (教	userl	*(1-55字符)
应用安全	密码		(1-63字符)
ACL	确认密码		(1-63字符)
SSL	授权用户组 🕐		
公明管理	身份识别用户组(多		
PKI	可用服务 同时在线最大用户数	I ADVPN I IKE I IPoE Lan 扱入 Portal I PPF	SSL VPN
	描述		(1-127字符)
	✓ 授权属性 ACL类型	● IPv4 ACL ◎ 二层ACL	
	授权ACL		-

#点击"授权属性">"SSL VPN策略组"填写SSL VPN实例中创建的SSLVPN资源组,点击"确定"完成配置

与新	《 用户 用户组		
≥ 用户	●新建 前期除 書 与入	号出・	
踚 用户管理	当设备做为AAA服务器搞对用户进行	认证、授权和计费时,需要在设备上添加相应的用户值	0.
本地用户	□ 用户名	描述	授权用户组
身份识别用户	新建用户		? >
🖿 认证管理			
■ 扱入管理			
直用安全			
] 对象组	₩ 授权關性		
ACL	ACL类型	● IPv4 ACL ◎ 二层ACL	
SSL SSL	授权ACL		~
公明管理	用户闲置切断时间		分钟 (1-120)
PKI	授权VLAN		(1-4094)
	SSL VPN策略组	SSLVPN语源组	(1-31字符)
	☑ 绑定属性 (?)		
	用户接入的接口		~
	用户的IPv4地址		
	用户的MAC地址®		
	用户所屬的VLAN		(1-4094)
		take of a	
		98221 10210	

3.5 将SSL VPN端口加入安全域,放通对应安全策略

#选择"网络">"接口">"安全域"点击新建,安全域名称为"SSLVPN",三层成员列表中选中SSLVPN-AC1接口加入到此安全域

НЗС	SecPath F1000-C- G2	●	∞>
98	《 安全城		
VRF	●新建 前 100 m 投票	■豊示导出 🔘 刷新	
190	🔄 安全域名称	新建安全域	? X 10.
安全域	E Local		<u>^</u>
1638	Trust	PERMINIA 227AMA	G
DNS	E DMZ	VLAN成员列表 (1-4094)	
P IP	Untrust	0	G
IPv6	Management		G
VPN SSLVPN 通信 低語 OHCP SS F規工具		GELV0/4 GELV0/4 GELV0/5 GELV0/6 GELV0/7 Image: Control of the second seco	
	14 4 第 1 页,	三規成則列数 GEU/0/21 GEU/0/22 GEU/0/2 GEU/0/7 GEU/0/8 NULL0 SSUVPA-AC2 Tur0 VPPP1 VT1 単石 取画	

#选择"对象">"对象组>"服务对象组"点击"添加",对象组名称"SSLVPN",添加对象,类型为TCP,目的端口为SSL VPN端口4433

62			19575 88174		
	(+) /0.70 (0 (K))	THE STATE	24.0		443100
安全	日、対象組合称		大川間に		42517日
6組	BITALERSSYXJARAE			1.4	1 1 1
Pv4地址对象组	对象组名称	SSLVPN		*(1-31字符)	8
Pv6地址对象组	SELE			(1-127字符)	8
服务对象组					8
力间段	9				8
					8
		·9		1000	8
管理	(A		内容	9610	a
	20.50.75.90			? X	8
	对象(3)	• 协议类型(名称)	〕协议类型(数字)◎ 对象组		8
	美型	TCP		*	8
	夏 深洲口	0	- 65535	• (0-65535)	8
	目的時口	4433	- 4433	(0-65535)	8
				-	8
					a
	9		确定 取消		8
					8
	9				8
			御宗 取 演		8
	a				8
	Vrrp		IP协议号 112		8
	wais		UDP 遵調口0 - 65535,	目的調口210 - 210	Ť
	winframe		TCP 源)由口0 - 65535, 目	目的3月口1494 - 1494	8

#选择"策略">"安全策略">点击新建,策略名称为"Untrust-Local",源安全域为Untrust,目的安全域为Local ,服务引用之前创建好的服务对象"SSLVPN"

	cPath F1000-	C-	() () () () () () () () () () () () () (2 東路 対象	一网络 系统
981	<< > 全全部時				
10450	● 新建 👔	建安全策略			7 × 体张件 ○ 刷新 □ 列定制
安正规理	安全策略配				
SCHENDER	四 名称	名称	Untrust-Local	*(1-127字符)	_ 服务 用户
I NAT	12	源安全域	Untrust	▼ (#活)	
		目的安全城	Local	✓ (序选)	
	123	82	● IPv4 ◎ IPv6		
TO BRUTHIN		描述信息		(1-127字符)	
		动作	● 允许 ◎ 拒绝		
		191P1842	增达理成输入对象组	× (*3)	
		目的印地址	请选择或输入对象组	▼ [部造]	
		服务	SSLVPN	▼ [条选]	
		应用	请选择应用	~ [部造]	
		应用道	请选择应用组	~ (多法)	
		用户	请选择用户	~	
		时间段	确远非时间的	*	
		VRF	公网	~	
		内容安全			
		IPS頒略		*	
		政黨过滤策略		~	
		文件过滤质略	NONE	*	
		防病毒策略		~	
			通空 取消		

#新建安全策略,策略名称为"SSLVPN-Trust,源安全域为SSLVPN,目的安全域为Trust

安	全策略		
\oplus	新建 💼 删除 🏮 复制	◆移动 ② 统计 🚫 取消统计	- 📀 启用 🚫 禁用 💼 清空统计数据 💼 清除
安全	新建安全策略		? X
	名称	SSLVPN-Trust	* (1-127字符) ^
	源安全域	SSLVPN	▼ [多选]
	目的安全域	Trust	▼ [多选]
	类型		
	描述信息		(1-127字符)
	动作	④ 允许	
	源IP地址	请选择或输入对象组	▼ [多选]
	目的IP地址	请选择或输入对象组	▼ [多选]
	服务	请选择服务	▼ [多选]
	应用	请选择应用	▼ [多选]
	应用组	请选择应用组	✔ [多选]
	用户	请选择用户	~
	时间段	请选择时间段	~
	VRF	公网	~
	内容安全		
	IPS策略	NONE	~
	数据过滤策略	NONE	~
	文件过滤策略	NONE	~
	防病毒策略	NONE	·
	l:	-	
		确定取	2消
14			

3.6 配置验证, 查看拨号成功的用户

#输入SSLVPN网关地址加端口,输入用户名密码点击连接



拨号成功后获取到SSLVPN地址池中IP地址



#在"网络">"SSL VPN">"统计信息">中查看拨入成功的用户

导航			
- VRF	在成局内公款:1 □ 注明 型,但如下点 ○ 和新		
·安全城 ■ 1838	SSLVPN	1	
DNS IP			
IPv6			
SSL VPN 法间实例			
- 用关 - 要户供助证法			
统计信息			

#点击详细可以查看终端详细信息,如:拨号的用户名,分配到的IP地址等

5965	CILLER CILLER	PAR						
VRF	読得案例名 SSLVPN 島、福利下記 〇 刷新		▲ Q, 重用					-
HC	巴 用户名	191512	世界组	空闲超时时间(分钟)	上級的周	何時信息	SHEEDIPROLE	
安全地	E user1	222.1.1.99	SSLVPN资源组	30	2018-08-26 18:16:02	Windows	10.10.10.2	
■ 1838								
DNS D								
10								
19v6								
VPN								
SSL VPN								
法同类例								
周英								
香户课场让该								
22提入接口								
统计信息								

3.7 保存配置

#在设备右上角选择"保存"选项,点击"是"完成配置。

概题	→ 监控	策略	对象	一 网络	<⊅ 系统			admin v 👔 保存 修改密码
	_	_	\$	=0 0 ×	系统日志 时间 ~	级别	洋田信息	\$≡0 0 ×
1%			13%		没有可以显示的数据			
CPU	人提示				×			
	?	N定要保存设计	新的当前配置。	57				≈=0¢×
本统计		ł	5	否			最近一个小时(个)	

4 注意事项

- 1、本案例适应的是默认证书,不需要手工导入CA证书和本地正常
- 2、不需要配置SSL服务器端策略,SSLVPN网关不需要引用SSL服务器端策略

配置关键点