SSL VPN 张新姿 2020-10-31 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙:本案例适用于如F1000-AK180、F1000-AK170等F 1000-AK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。

服务器系统: windows server 2012 R2

1.2 配置需求及实现的效果

V7防火墙部署在互联网出口,外网终端通过INode软件拨入SSL VPN,防火墙通过LDAP Server 对用 户进行远程认证和授权。认证成功后用户可以访问内网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	与LDAP互联口	LDAP服务器地址
GE1/0/1	222.1.1.100/24	GE1/0/3	192.168.10.1/24	GE1/0/8	10.88.142.171
2 组网图					



配置步骤

1.1 Windows server 2012镜像安装

请参考微软镜像安装手册或者百度自行解决,本文对Windows server 2012系统安装不做赘述。

1.2 LDAP服务器设置

1、在服务器界面点击"开始"旁边的服务器管理器按钮,调出管理器界面后点击"添加角色和功能选项"

la la		服务器管理器
● ● → 服务器管	理器・仪表板	• 🕲 🏲
■ 仪表板	欢迎使用服务器管理器	
 ▲地服务器 新有服务器 試 文件和存储服务 	1	配置此本地服务器
	9638/EW/(Q)	2 添加角色和功能
		3 添加要管理的其他服务器
	新增功能(W)	4 创建服务器组
🗄 占 🖉 🚞		

2、在出现的角色和功能向导中点击下一步。



3、安装类型选择"基于角色或基本功能的安装"后点击下一步。

战军安装类型	目标题务 KHXY-NET-IMC7
开始之前	选择安装类型。你可以在正在运行的物理计算机、虚拟机或脱机虚拟硬盘(VHD)上安装角色和功能。
安装类型 服务器洗择	 基于角色或基于功能的安装 通过添加角色、角色服务和功能未配置单个服务器。
服务體角色 功能 确认 结果	○ 远程桌面服务安装 为虚拟桌面基础结构(VDI)安装所需的角色服务以创建基于虚拟机或基于会活的桌面部署。
	<上一步(P) 下一步(N) > 安装(I) 取満

4、服务器选择显示为本机地址的服务器。

2	添加	加角色和功能向导		
选择目标服务	器			目标服务 KHXY-NET-IMC7
开始之前 安装类型 服务識选择 服务識角色 功能	选择要实装角色和功能的 ● 从服务器池中选择服务 ● 选择虚拟硬盘 服务器池	服务器或虚拟硬盘。 务器		
确认 结果	備透離: 名称 KHXY-NET-IMC7-1	IP 地址 10.88.142.171	操作系统 Microsoft Windows Se	rver 2012 R2 Datacenter
	找到 1 个计算机 此页显示了正在运行 Wir 醫 命令所质加的服务器。	ndows Server 2012 (脱机服务器和尚未完	的服务體以及那些已经在服	务器管理器中使用"添加服务 器将不会在此页中显示。
		< 上-	步(P) 下一步(N) >	安装(1) 取消

5、在服务器角色中点击Active Directory 域服务。





6、如果没有特殊需要不需要选择任何功能直接点击下一步即可。

6	添加角色和功能向导	
选择功能 ^{开始之前} 安装类型 服务器选择 服务器曲色	法得要会装在所选服务器上的一个或多个功能。 功能 ▶ ■ <u>NET Framework 3.5 功能(1 个已会装,共 3 へ)</u> ▶ ■ <u>NET Framework 4.5 功能(2 今日</u> 合装 共 3 へ)	目标被失器 KHOKY-NET-AMC7-1 描述 .NET Framework 3.5 结合了 .NET Framework 2.0 API 的功能和更于如
功能 AD DS 确认 结果	 ▶ 回 Xet Framework 4.3 Jinit (2 10 Sector 3.7 f) ■ BitLocker 预热操物 ■ BitLocker 网络操物 ■ BitLocker 网络操物 ■ DirectPlay ■ HTTP 代理上的 RPC □ IIS 可承載 Web 核心 □ Internet 打印客户端 □ IP 地址管理(IPAM)服务器 	建山田程序创建制化木,这起山田程 序可提供通购用于厚固,保护客户 个人身份信息,实现畅新市安全的通 信,以及提供为一系列业务进程建模 的功能。
	○ ISNS Server 服务 ○ LPR 第口盆祝器 ○ PS 客户時 ○ RAS 连报管理器管理工具包(CMAK) ○ CAN & A MERTE WHATHER (PD-544) ✓	

7、出现Active Directory 域服务点击下一步。



8、确认无误后点击安装Active Directory 域服务程序,安装成功后关闭向导。

E	添加角色和功能向导	_ _ ×
确认安装所选内	四容	目标级务器 KHXY-NET-iMC7-1
开始之前	若要在所远服务器上安装以下角色、角色服务或功能,请单击"安装"。	
安装类型	□ 如果需要,自动重新启动目标服务器	
服务器选择 服务器角色	可能会在此页面上显示可选功能(如管理工具),因为已自动选择这些功能。 能,请单击"上一步"以清除其复选框。	如果不希望安装这些可选功
功能	Active Directory 域服务	
AD DS	远程服务器管理工具	
确认	角色管理工具	
结果	AD US an AD US 上員 Windows PowerShell 的 Active Directory 標块 AD DS 工具 Active Directory 管理中心 AD DS 管理师元和命令行工具	
	組策幣管理 导出配置设置 指定备用原路径	
	<上一步(P) 下一步(N) >	安装(I) 取消

9、服务器部署成功后出现AD DS选项,点击"更多"打开域配置界面。

位表板		版务器 所有服务器 并	€1个				任务	*
本地服务器		A KHXY-NET-IM	C7-1 中的 Active	Directory 域服务 所需的	22		更多。	×
所有服务器	_	体进程		ρ ⊞ • (R) •				•
AD DS								
嵋 文件和存储服务	Þ	服务器名称	IPv4 地址	可管理性	上次更新	Windows 激活		
		KHXY-NET-IMC7-1	10.88.142.171	联机 · 未启动性能计数器	2020/4/19 15:49:35	未激活		

10、点击"将此服务器提升为域控制器"选项。

	所有服务器任务详细信息					
所有任	与服务器 个(⑻♯1↑	王务详细信》	息和通知			
192	58	۵ (۱	• (R) •		۲	
状态	任务名称	阶段	消息	操作	通知	
	部務局配置	未开始	KHXY-NET-IMC7-1 中的 Active Directory 域	将此服务器提升为域控制器	1	

11、选择添加新林并且将根域名设置为test.com。

b	Active Dire	ctory 域服务配置向导	_ _ X
部署配置 部署配置 城控制器选项 其他选项 路径	选择部署级作 外域控制器添加到现有机(等新述添加到现有机() ③ 添加解机(F)	(次(D) () ()	目标服务器 KHXY-NET-iMC7-1
查看选项 先决条件检查 安装 结果	描定此操作的域值思 模域名(R): 详细了解 部署配置	test.com	
		<上一步(P) 下一步(N) >	安装(I) 取消

12、创建目录服务还原密码后点击下一步。

6	Active Directory \$	或服务配置向导	= □ X
域控制器选项			目标服务器 KHXY-NET-iMC7-1
部署配置 域控制器选项 DNS 选项 其他选项 路径 查看选项 先决条件检查 安装 监架	 选择新林和根域的功能级别 林功能级别: 域功能级别: 描定域控制器功能 ✓ 域名系统(ONS)服务器(O) ✓ 全局環境(GC)(G) □ 尺域地控制器(ROC)(R) 輸入目型解除不開着式(DSRM)等差 	Windows Server 2012 R2 Windows Server 2012 R2	•
	密码(D): 确认密码(C): 详细了解 域控制器选项	•••••	
	[< 上一步(P) 下一步(N) >	安装(I) 取消

13、在DNS选项设置中会出现报错无法创建DNS服务器,可以忽略直接下一步即可。



14、设置NetBIOS域名,系统已经根据根域默认为TEST不用修改点击下一步。

雨7 NetRIOS 名			目标服务器 KHXY-NET-iMC7-1
記了 NetBIOS 名			
100 11010100 12	称,并在必要时更改该名称		
成名:	TEST		
电他选项			
	₹ 在 :	RE: [1251	RE: IESI

15、选择数据库、日志、SYSVOL文件夹的目录。

h	Active Director	y 域服务配置向导	_ 🗆 X
路径	城谷 とりつの 家福幸 日十寸を	HER EVELIAL 的計画	目标服务器 KHXY-NET-IMC7-1
域控制器选项	新派库文件夹(D);	C:\Windows\NTDS	
DNS 选项 其他选项	日志文件文件夹(L):	C:\Windows\NTDS	
路径	SYSVOL 文件夹(Y):	C:\Windows\SYSVOL	
呈有远坝 先决条件检查 安装 结果			
	详细了解 Active Directory 路	Æ	
		< 上一步(P) 下一步(N) > 安装	k(I) R iji

16、检查选项无误后选择下一步。

查看选项		目标服务 KHXY-NET-IMC7
部署配置 域控制證选项 DNS 透顶 其他选项 路径 查查选项 先决条件检查 安装 结果	检查你的选择: 将该服务器配置为新林中的第一个 Active Directory 域控制器。 新域名为"test.com"。这也是新林的名称。 该域的 NetBIOS 名称: TEST 林功能级别: Windows Server 2012 R2 域功能级别: Windows Server 2012 R2 其他选项: 全局编录: 是 DNS 服务器: 是	
	動通 DNS 要応: E 数据库文件央: C\Windows\NTDS 可以将这些设置导出到 Windows PowerShell 脚本以自动执行其他安装 注何了解 杂装洗透	- 查看脚本(V)

17、先决条件检查完成后选择安装,安装完成后点击关闭,关闭需要重启服务器后域名系统才能正常工作。



18、开启开启后选择管理工具。

服务器管理器	Windows PowerShell	桌面	a subuctore 2000
(1) しょうしょう しょう	任务管理 器	SHELA	
空間を	Internet Explorer		

19、点击Active Directory 用户和计算机

5 I 🖸 🛯 = I	管理工	具		
文件 主页 共享	查看			Ŷ
💿 💿 - 🕇 🗟 • 🗄	空制面板 → 系统和安全 → 管理工具 →	v 1	∪ 搜索"管理」	.具' A
☆ 收藏夹	名称	修改日期	类型	大小
🚺 下载	Terminal Services	2013/8/22 23:39	文件夹	
重 桌面	🛃 Active Directory 管理中心	2013/8/22 7:50	快捷方式	2 KB
19 最近访问的位置	🛃 Active Directory 用户和计算机	2013/8/22 14:55	快捷方式	2 KB
	Active Directory 域和信任关系	2013/8/22 14:55	快捷方式	2 KB
▲ 法公用院	Notive Directory 站点和服务	2013/8/22 14:55	快捷方式	2 KB
1 10 10 10 10 10 10 10 10 10 10 10 10 10	No ADSI 编辑器	2013/8/22 14:55	快捷方式	2 KB

20、新建一个SVPN的组织单位用来存储SSL VPN用户。



21、在SVPN组中添加用户

Active Direct	tory 用户和计算机 [名称	类型	描述		
 保存的会社 建 test.com Builtin Comp Doma Foreig Mana Users 	间 puters in Controllers gnSecurityPrincipal ged Service Accou			这里没有任何项目。		
SV ^{RAL}	委派控制(E) 移动(V) 查找(I)					
	新建(N)	 计算 	机			
	所有任务(K)	 联系 	人			
	查看(V)	, 组				
く川田	<u></u> 剪切(T) 删除(D) 重命名(M) 刷新(F) 島出列売(1)	Inet msIr MSM 组织 打印	OrgPerson maging-PSPs MQ 队列别名 单位 机			
	雇性(R)	用户			1	

22、添加用户为张三设置登录账号为zhangsan。

	新建对象 - 用户
🤱 éilte:	f: test.com/SVPN
姓(L):	<u>3</u> K
名(F):	三 英文缩写(1):
姓名(A):	张三
用户登录名(U):	
zhangsan	@test.com v
用户登录名(Wind	ows 2000 以前版本)(W):
TEST	zhangsan
	< 上一步(B) 下一步(N) > 取消

23、设置密码并设置密码为永不过期。

密码(P):	•••••	
确认密码(C):	•••••	
✔ 密码永不过期(W)		

24、设置完成后出现张三用户,至此LDAP服务器所有配置完成。



1.3 防火墙侧配置

#选择 "网络">"SSL VPN">"网关"点击"新建",IP地址填写防火墙GE1口地址222.1.1.100,端口号修改 为4433(缺省SSL VPN也是443端口与设备WEB登录端口冲突),勾选"使能"选项点击"确定"完成配置

网关⑦	SSLVPNGW		*(1-31字符)
IP地址⑦	● IPv4 □ IPv6		
	222.1.1.100		(缺省为0.0.0.0)
HTTPS端口	4433		(1025-65535,缺省为443)
开启HTTP流量重定 向			
HTTP端口	80		(1025-65535,缺省为80)
SSL服务器端策略		Ŧ	
VRF	公网	~	
使能	V		

1.3.2 增加SSL VPN接入接口

#点击 "网络">"SSL VPN">"IP接入接口"后新建IP接入接口,接口编号配置为1、IPV4地址配置为10.10. 10.1/24。

导航	◆ IP接入接口			
🖲 🎭 VPN	● 新建 × 删除	○ 刷新		
🖲 🐂 SSL VPN	新建IP接入接口			
 ・访问实例 ・ 网关 ・ 客户調地址地 	接口编号① 描述	1		• (0-4095) (0-2559255)
·安全引擎地址地 IP接入接口	VRF	公网		*
 ・ 全局配置 ・ 模板管理 	IPv4地址信息	10.10.10.1	/ 255.255.255.0	(IPv4地址/掩码长度1-31)
·统计信息	从IP地址	●新建 × 前除		
© ⑦ 路由		从IP地址	推码长度	编辑
・IP組織路由 ・PIM				

1.3.3 增加客户端地址池

#点击 "网络">"SSL VPN">"客户端地址池"新建客户端地址池,地址池名配置为"SSLPOOL"、起始地址 配置为10.10.10.2、结束地址配置为10.10.10.254,配置完成后点击确定。

导航	< 客户端地址池		
💿 🗺 VPN	< ● 新建 × 删除	○ 刷新	
🖲 强 SSL VPN	☑ 客户講地址	池名称	起始地址
·访问实例	编辑客户端地	逃池	®×
· 网关			
客户端地址池	地址地名称	SSLPOOL	*(1-31字符)
·安全引擎地址池	起始地址	10.10.10.2	•
 IP接入接口 ・ 全局配置 	结束地址	10.10.10.254	•
・模板管理		确定 取消	

1.3.4 配置SSL VPN访问实例

#点击 "网络">"SSL VPN">"访问实例"中新建访问实例,在"关联网关"中点击新建关联3.3.1创建的SSL VPN网关,在ISP域中添加ISP认证域,认证域名称配置为"svpn"其他选项全部为默认,配置完成后点击确定。

导航	• 访问实例				
₩. VRF	→ 新建 × 删				
◎□接口	编辑访问实例	9			@×
◎ 安全域	基本配置	Web <u>业务</u> TCP <u>业务</u>	IP业务 BY	/OD业务 资源组	页面配置
◎ ♥ 链路	访问实例⑦	SSLVPN	• (1-	31字符)	~
© DNS		- + 10 + 1010			
IP 🖸	关联网关	()新建 / 明雄	× 豊厚	A	
IPv6				67	
O VE VPN	9	·联网关 SSLVPNGW			
● N SSL VPN	VRF U	加方式 直接访问网关	÷		
· 网关	安全引	确定	取消		
· 客户端地址池	ISP认证域	svpn	v		
·安全引擎地址池	开启验证码验	HEO []			
·IP接入接口	开启证书认证	E ⁽²⁾			
·全局配置	开启iMC短信	以证⑦			
・模板管理	最大用户数	1048575	(1-	1048575)	
·统计信息			handle Dimitial		Ť.
添加ISP域					0×
ta 々			(1-2	55字符)	~
域名	svpn		(1-2	55字符)	^
域名 状态⑦	svpn 活动		(1-2 v	55字符)	^
城名 状态 ⑦ 接入方式	svpn 活动 登录用户	□ LAN接入	(1-2	55字符) □ ADVP	N
域名 状态 ⁽²⁾ 接入方式 登录用户AAA方案	svpn 活动 登录用户	□ LAN接入	(1-2 v Portal	55字符) □ ADVPI	N
域名 状态⑦ 接入方式 登录用户AAA方言 认证	svpn 活动 登录用户 RADIUS	□ LAN接入 □ 本地认证	(1-2	55字符) □ ADVPI	N
域名 状态 ⑦ 接入方式 登录用户AAA方室 认证 方案	svpn 活动 登录用户 RADIUS	□ LAN接入 □ 本地认证	(1-2 v Portal	55字符)	N
域名 状态 ⑦ 接入方式 登录用户AAA方案 认证 方案 授权	svpn 活动 登录用户 RADIUS	□LAN接入 □本地认证 □本地损权	(1-2 Portal	55字符)	N
域名 状态 ⁽²⁾ 接入方式 登录用户AAA方室 认证 方案 授权 方案	svpn 活动 登录用户 RADIUS	□ LAN接入 □ 本地认证 □ 本地授权	Portal	55字符) ADVPI 不认证 不误权	N
域名 状态⑦ 接入方式 登录用户AAA方案 认证 方案 授収 方案 计费	svpn 活动 登录用户 RADIUS RADIUS	 LAN接入 本地认证 本地送权 本地送权 本地试费 	(1-2 Portal	55字符) ADVP 不认证 不授权	N
域名 状态① 接入方式 登录用户AAA方室 认证 方室 授权 方案 计费 方案	svpn 活动 登录用户 RADIUS RADIUS	□ LAN接入 □ 本地认证 □ 本地授权	Portal	55字符) ADVPI 不认证 不送权 不送权	N
域名 状态⑦ 接入方式 登录用户AAA方案 认证 方案 授权 方案 计费 方案 上AN接入AAA方部	svpn 活动 登录用户 RADIUS RADIUS	 LAN接入 本地认证 本地运収 本地运収 本地计费 	Portal	SS字符) ADVP 不认证 不授权 不授权	N
域名 状态⑦ 接入方式 登录用户AAA方案 认证 方案 授权 方案 计费 方案 LAN接入AAA方题 认证	svpn 活动 登录用户 RADIUS RADIUS	LAN接入 本地认证 本地试版 本地试版 本地试版	Portal	55字符) ADVPI 不认证 不授权 不计费	N
域名 状态① 接入方式 登录用户AAA方案 认证 方案 授权 方案 计费 方案 LAN接入AAA方部 认证 方案	svpn 活动 登录用户 RADIUS RADIUS	 LAN接入 本地认证 本地提取 本地计费 本地计费 本地认证 	Portal	SS字符) ADVP 不认证 不授权 不计费 不计费	N

1.3.5 配置SSL VPN访问实例中的IP业务

#点击 "网络">"SSL VPN">"访问实例">"IP业务"IP接入接口选择3.3.2步骤添加的接口1(SSLVPN-AC1)、客户端地址池选择3.3.3步骤添加的"SSLPOOL"、配置客户端掩码及主DNS服务器地址分别为24和114.114.114.114后点击页面下方确定完成配置。

辑访问 实例			@×
基本配置 Web业务	TCP业务 IP业务	BYOD业务资源组页	面配置
IP接入接口	SSLVPN-AC1 v		
客户端地址池	SSLPOOL v		
客户端地址掩码	24	(1-30)	
主DNS服务器	114.114.114.114		
备DNS服务器	X.X.X.X		
主WINS服务器	XXXX		
备WINS服务器	XXXX		
保活周期	30	秒(0-600)	
开启IP客户端自启动⑦			
开启推送资源列表⑦			

新建组网地址为192.168.10.0/24的内网资源,当SSL VPN用尸拨入后可以直接访问该网段下的所有资源。

编辑访问实例				0×
基本配置 Web业务	TCP业务 IPy	BYOD业务	资源组页	面配置
开启IP客户端自启动⑦				^
开启推送资源列表⑦				
		2 201百		
	に接入	金源		a \
● 新建 ● 精構 ▲ 副味	编档面田列表			w>
NEIWANG	路由列表名称	NEIWANG	* (1-31字符	F)
		路由列表表	顼	
	分析建 × 删除	44x777 L4 ada	444 TU I	(det9)
	TMALAL	把好衣屋	<u>R</u> H	網視
	新建路由表项			$@\times$
	が担	●包含	除	
	子网地址⑦	192.168.10.0		
	海码长度	24	• (0-32)
	1.04.0 1.0702	24	× (0.32	
		确定	取消	

1.3.6 配置SSL VPN访问实例中的资源组

#点击 "对象">"ACL">"IPv4"中新建高级ACL编号为3999, 点击确定进入规则配置。

导航	◆ IPv4 ACL组		
目健康检测	● 新建 × 田玲		
🖲 🕹 用户	新建IPv4ACL		@×
② 〇 应用安全	类型	○ 基本ACL	
◎▲对象组	ACL ⑦	3999	(3000-3999或1-63个字符)
	规则匹配顺序	● 按照配置顺序 ○ 自动排序	
IPv4	默认规则编号步长	5	(1-20)
·	描述		(1-127字符)
© SSL			
◎ 🖧 公钥管理		☑ 继续添加规则⑦	
💿 者 PKI		确定取消	

进入规则配置界面后IP协议类型选择ip、取消继续添加下一条规则选项后点击确定完成配置。



1.3.7 配置SSL VPN访问实例中的资源组

#点击 "网络">"SSL VPN">"访问实例">"资源组"中新建名称为SSLVPNZIYUAN的资源组,

编辑访问实例				@×
基本配置 Web业务 TCP业务	IP业务	BYOD业务	资源组	页面配置
	资源组			
④ 新建 《编辑 × 删除 设为缺省	取消缺省			
☑ 资源组名称			缺省	编辑

在指定路由接入VPN中选择子网资源、子网资源选择3.3.5步骤创建的资源NEIWANG、IPV4 ACL用于 控制SSL VPN接入用户,选择3.3.6步骤创建IPv4 ACL 3999点击确定完成配置。

		IP接入	
强制接入VPN 🕐			
指定路由接入VPN	子网资源	~	
子网资源	NEIWANG	*	
客户端地址池	NONE	¥	
IPv4 ACL	3999	*	
IPv6 ACL		-	

1.3.8 配置SSL VPN访问实例中的资源组

#在 "网络">"SSL VPN">"访问实例"中点击使能开启SSL VPN实例。

1	別同英	例						
l	€ #R	E X BRE O REF				请输入要查询的信息 Q 查	19 🖻	\$8. # 3
		边间实例名称	Inks	用关	服务器地址	VRF *	使成	编辑
		SSLVPN	• 生效	SSLVPNGW	直接边间用关	公用	2 .	۲

1.3.9 创建SSL VPN用户组

#在 "对象">"用户">"用户管理">"本地用户">"用户组"中新建名称为svpn的用户组,在SSL VPN策略组 中将3.3.7步骤中创建的SSLVPNZIYUAN组调用在该用户组。

导航	◆ 用户 用户组	
🗑 💄 用户	④ 新建 ★ 删除	
◎ 用户管理	当设备作为AAA服务器满对用户进行认证、授权和计费时,需要在设备	上添加相应的用户信息。
本地用户	用户组 身份识别用户	身份识别用户组
修改用户组		$@\times$
用户组名称	svpn	(1-32字符)
		-
	身份识别成员⑦	
用户⑦		
日		
用户组	1	1
	授权属性	
ACL类型	● IPv4 ACL □二层ACL	
授权ACL		
用方语要把能计词		
用户内直切断时间		分钟(1-120)
授权VLAN		(1-4094)
SSL VPN策略组	SSLVPNZIYUAN	(1-31字符)
	704 also 700114/	
	佣定取消	

1.3.10 创建LDAP服务器

#在 "对象">"用户">"认证管理">"LDAP">"LDAP方案"新建名称为svpn的LDAP认证方案。



配置LDAP服务器名称为svpn、LDAP服务器地址为10.88.142.171、管理员DN为cn=administrator,cn= users,dc=test,dc=com、管理员密码为administrator用户密码、用户DN查询的起点为ou=svpn,dc=test, dc=com、用户名属性为samaccountname。对于上述所有参数的解释说明: login-dn是LDAP管理账号 的路径(要求此管理账号有读权限或者管理员权限)、管理员密码对应administrator账号的密码、sear ch-base-dn表示要查找的用户所在的目录、user-parameters samaccountname参数表示查找用户属性 samaccountname值,设备默认查询用户属性查询CN值。

名称	svpn	* (1-31字符)
属性映射表		*
	配置LDAP服务器	
名称	svpn	*(1-64字符)
VRF	公网 👻	
地址类型	● IPv4 □ IPv6	
服务器地址	10.88.142.171	\mathbf{F}
端口	389	(1-65535)
管理员DN	cn=administrator,cn=users,	(0-255字符)
管理员密码	•••••	(0-128字符)
LDAP版本号	○ V2	-
超时时间	10	秒(5-20)
用户DN查询的起始节点	ou=svpn,dc=test,dc=com	(0-255字符)
用户DN查询的范围?	 ● 所有子目录 ○ 下—级音 	- 子目录
用户名称属性	samaccountname	(0-64字符)
用户名称格式	○携带ISP域名 ● 不携带I	- SP域名
用户名称举型		(0-64字符)

1.3.11 创建LDAP方案 (需在命令行完成)

创建LDAP方案将LDAP认证和授权全部指向3.3.10步骤中创建的LDAP服务器。

[H3C]ldap scheme svpn

[H3C-Idap-svpn]authentication-server svpn

[H3C-ldap-svpn]authorization-server svpn

1.3.12 创建SSL VPN认证域 (需在命令行完成)

创建SSL VPN认证域,将认证授权全部改向3.3.11步骤创建的svpn方案,并且指定3.3.9步骤中创建的认证用户组svpn。

[H3C]domain svpn

[H3C-isp-svpn]authorization-attribute user-group svpn

[H3C-isp-svpn]authentication sslvpn ldap-scheme svpn

[H3C-isp-svpn]authorization sslvpn ldap-scheme svpn

1.3.13 配置与LDAP服务器互联端口

#在 "网络">"IP"找到1/0/8接口并配置1/0/8接口地址为10.88.142.1掩码配置为255.255.255.0。

导航	▲ IP	
WE VRF		alari
◎▽接口	修改IP配置	
● 安全域 ② ♂ 链路 ③ 目 DNS ③ 僅 IP - ARP ④ 쯭 IPv6	接口 状态 描述 保持上一跳 IP地址 IP地址/袖码长度 网关	GigabitEthernet1/0/8(GE1/0/8) down GigabitEthernet1/0/8 Interface ⑦ 开启 ● 关闭 ● 指定IP地址 通过DHCP自动获取IP地址 PPPoi 10.88.142.1 / 255.255.255.0
 ◎ ™ VPN ◎ N SSL VPN ◎ ♥ 路由 ◎ ♂ 組播 ◎ ◆ DHCP 		 新編ANP284E 人IP地址 挽切 編輯
◎ ♣ 服务	~	确定 取消

1.3.14 将SSL VPN端口加入安全域, 放通对应安全策略

#在 "策略">"安全域"中新建名称为SSLVPN的安全域,将步骤3.3.2添加的SSLVPN-AC1接口添加到SSLVPN域。

导航		◆ 安全域			
🗊 安全域		★ 新建 × 删除 [技	页面显示导出 🔷 刷新	
◎ 🔗 链路		安全域名称			成员个
I DNS		Local			
安全域名称	sslvpn		* (1-31字符)	
VLAN成员列表	E		(1-4094)	
0					
一巨成岛列夷	○ 篩洗			○篩洗	
	200 pp				
	接口列表 BAGG1			成员列表(0)	
	BAGG1 BAGG3		*>		
	BAGG4		+		
	BAGG10		+		
			*		
三层成员列表	Q筛选			Q筛选	
	接口列表			成员列表(1)	
	Loop2	~	*>	SSLVPN-AC1	
	Vlan2				

#在 "策略">"安全域"中新建名称为LDAP的安全域,将步骤3.3.13添加的与LDAP服务器互联接口GE1/0/8添加到LDAP域。

安全域名称	SSLVPN	* (1-31字符)
VLAN成员列表 ⑦	:		(1-4094)
二层成员列表	Q筛选		Q筛选
	接口列表		成员列表(0)
	BAGG1 BAGG3	*>	
	BAGG4 BAGG10	+	
	DAGGIO	+	
		*	
三层成员列表	Q筛选		Q筛选
	接口列表		成员列表(1)
	GE1/0/5	~ *	GE1/0/8

#在 "对象">"服务对象组"中新建名称为4433的对象组,点击页面中添加按钮后将目的端口设置起始端口和结束端口都设置为4433(3.3.1步骤中SSL VPN网关的端口)。

导航	< BR45734618			
王 健康检测	修改服务对象组			
💿 💄 用户	对象组名称 [4433		(1-31字符)
◎ 🗊 应用安全	描述			(1-127字符)
◎ 小 对象组				
· IPv4地址对象组				
· IPv6地址对象组		r.		
·MAC地址对象组	SPURYISK			@×
服务对象组	対象⑦	● 协议类型(名称) (协议类型(数字)) 対	教组
• 时间段	类型	TCP		w
🖲 🚍 ACL	源端口	0	- 65535	* (0-65535)
💿 🛢 SSL	目的端口	4433	- 4433	× (0-65535)
◎ 📌 公钥管理			20.45	
💿 者 PKI			PEAE ACT	

#在"策略">"安全策略"中将Untrust到Local域目的端口为TCP4433端口放通。

健安全策略				?×
夕 む (1)	0011/011			
白小小	SSLVPN			^
源安全域	Untrust	Ŧ	[多选]	
目的安全域	Local	Ŧ	[多选]	
类型	● IPv4 □ IPv6			
描述信息			(1-127字符)	
=h//=				
ал ғ				
服务				
服务对象组	4433	~	[多选]	
协议/端口号	请添加协议和端口号	~		
应用	请选择应用	Ŧ	[多选]	
用户	请选择或输入用户	Ŧ	[多选]	
时间段	请选择时间段	Ŧ		
VRF	公网	Ŧ		

皇安全策略			@>
名称⑦	SSLVPN1	* 目动命名	
源安全域	SSLVPN	👻 [多选]	
目的安全域	Trust	▼ [多选]	
美型	● IPv4 IPv6		
描述信息		(1-127字符)	
动作	 允许 拒绝 		

#配置配置安全策略,放通安全域为DMZ、Local域的数据流量。(点击多选按钮可以选择多个安全域)

建安全策略				@×
名称⑦	SSLVPN2	×	自动命名	~
源安全域	SSLVPN, Local	*	[多选]	
目的安全域	Trust, SSLVPN	*	[多选]	
类型	● IPv4 □ IPv6			
描述信息			(1-127字符)	
动作	● 允许 □ 拒绝			

1.4 保存配置

admin 🔫	⊂ .⊟	G

1.5 配置验证, 查看拨号成功的用户

可以在WEB界面SSL VPN统计信息中查看SSL VPN拨入信息,也可以在命令行通过dis sslvpn session verbose查看用户信息。

dis sslvpn session verbose

User : zhangsan

Context : SSLVPN

Policy group : SSLVPNZIYUAN

Idle timeout : 30 min

- Created at : 19:52:36 UTC Sun 04/19/2020
- Lastest : 19:52:36 UTC Sun 04/19/2020

User IPv4 address : 10.88.26.145

Alloced IP : 10.10.10.2

Session ID : 14

Web browser/OS : Windows

客户端使用INode登录截图:

INode智能容户	En ¥ - X		
SSL VPN连接			
同关	222.1.1.100		
当前用户	zhangsan		
域	无		
安全状态	未检查		
上线时间	2020-4-19 19:55:09		
Parta(\$18	¥.7. •		
Portagene	-		
	• 我的场景 »		
0	≣ ∿		

配置关键点

注意事项

1、安装Active Directory后服务器所在域会变更导致重启后无法使用原账号登录,登录时需要使用"域 名\用户名"的方式去登录。

2、因为设备默认查询用户属性是查询CN值,当LDAP服务器用户名与登录账号不一致情况下需要设备 查询samaccountname值来确定用户登录名,因此在设备LDAP Server下"user-parameters user-nameattribute samaccountname"命令是一定要添加的。