L2TP over IPSec VP 吴昊A 2020-03-11 发表

组网及说明

1. 组网需求:

Comware V7防火墙设备作为VPN总部,电脑客户、移动终端通过中间跨越运营商网络拨入L2TP over IPSec VPN实现访问内网服务器的需求。

2. 组网图:



如图所示,外网终端通过防火墙的接口2地址192.168.1.1拨号L2TP over IPSec VPN访问内网web服务器的资源。

配置步骤

1. 防火墙接口配置如下。

```
interface GigabitEthernet1/0/2
   port link-mode route
   ip address 192.168.1.1 255.255.255.0
   ipsec apply policy 1
2. F1030 L2TP/IPSec相关配置.
  #
   ip pool pool 10.1.1.2 10.1.1.10
                                       //地址池
  #
   interface Virtual-Template1
   ppp authentication-mode pap
   remote address pool pool
   ip address 10.1.1.1 255.255.255.0
   #
   local-user client class network
   password simple client
   service-type ppp
   authorization-attribute user-role network-operato
   #
   ipsec transform-set 1
   encapsulation-mode transport
   esp encryption-algorithm 3des-cbc
   esp authentication-algorithm md5
   #
   ipsec transform-set 2
   encapsulation-mode transport
   esp encryption-algorithm aes-cbc-128
   esp authentication-algorithm sha1
   #
   ipsec transform-set 3
   encapsulation-mode transport
   esp encryption-algorithm aes-cbc-256
   esp authentication-algorithm sha1
   #
   ipsec transform-set 4
   encapsulation-mode transport
   esp encryption-algorithm des-cbc
```

```
esp authentication-algorithm sha1
  #
  ipsec transform-set 5
   encapsulation-mode transport
   esp encryption-algorithm 3des-cbc
   esp authentication-algorithm sha1
  #
  ipsec transform-set 6
   encapsulation-mode transport
   esp encryption-algorithm aes-cbc-192
   esp authentication-algorithm sha1
  #
  ipsec policy-template 1 1
   transform-set 1 2 3 4 5 6 //不确定终端的提议类型, 这里设置多个
   ike-profile 1
  #
  ipsec policy 1 1 isakmp template 1
  #
  l2tp-group 1 mode Ins
   allow l2tp virtual-template 1
   undo tunnel authentication
  #
   l2tp enable
  #
  ike profile 1
   keychain 1
   local-identity address 192.168.1.1
   match remote identity address 0.0.0.0 0.0.0.0
   proposal 1 2 3 4 5 6
  #
  ike proposal 1
   encryption-algorithm aes-cbc-128
   dh group2
   authentication-algorithm md5
  #
  ike proposal 2
   encryption-algorithm 3des-cbc
   dh group2
   authentication-algorithm md5
  #
  ike proposal 3
   encryption-algorithm 3des-cbc
   dh group2
  #
  ike proposal 4
   encryption-algorithm aes-cbc-256
   dh group2
  #
  ike proposal 5
   dh group2
  #
  ike proposal 6
   encryption-algorithm aes-cbc-192
   dh group2
  ike keychain 1
   pre-shared-key address 0.0.0.0 0.0.0.0 key simple test
  #
3. 物理口、Virtual-Template1接口加入安全区域,并放通域间策略。对于G1/0/2接口需要注意开放U
  ntrust到Local的策略。对于Virtual-Template1接口,假设虚拟接口加入的是Untrust安全域,如果要
  访问内网资源,开放Untrust到Trust的安全策略。
4. window10电脑终端的配置
```

```
前面的步骤和W7一样,可以参考: <u>https://zhiliao.h3c.com/theme/details/104211</u>
```

控制調販主页 管理无线网络 更改造配器设置 更改高级共享设置	直看基本网络信息开设置连接 2000 W182198 h3croot.huswei-3com.com 加引用 1000 建香志网络 近球点影开选择 動加用 1000 地図路 25点接到 Internet 通用 1000 並用 1000 東京大阪大学会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会
	更改网络设置 全型 设置新的注意或网络 设置无线 宽带、按号、能对或 VPN 连接;或设置独由器或访问点。 这 建用网络 通用网络 通用用网络 通用用网络 通用用网络 通用用网络 通用用网络 通用用网络 通用用网络 如果 如
另请参阅 Internet 选项 Windows 防火墙 家庭组	20年終年 分報升移复列組问题,或改得訪婚期除信息。

■ VPN 海塘 履性

...

和 近映 安王 阿塔 共享 /PN 操型(T):	
使用 IPsec 的第 2 层隧道协议(L2TP/IPsec)	
電磁设置(S	L2TP
不允许加密(如果它需要加密,服务器将新开连接)	使用预共享的密钥作身份验证(P)
身份验证	密明(K):
○使用可扩展的身份验证协议(EAP)(E)	
	○ Weit to by Brothaue(C) ▽ 验证服务器证书的"名称"和"用法"属性(V)
/唯代王(R)	
(● 允许使用这些协议(P)	
☑ 未加密的密码(PAP)(U)	
□ 医词握手身份验证协议(CHAP)(H)	确定 取消
Microsoft CHAP Version 2 (MS-CHAP v2)	
自动使用我的 Windows 登录名称和密码(及域、如果 有)(A)	t i i

記 売 Ln	削的网络 ternet			
www.vpn	连接			
			连接	
WLA に 已关 网络和 Inte	N 闭 ernet 设置	论本泉注曲		
G.		((1))		
WLAN	飞行模式	移动热点		
	へ 宮 歩 🕬	中 💈 20	16:53 20/3/11	3

或者点击网络和internet设置,从这里连接VPN





命 主页	VPN
査技设置	+ 添加 VPN 连接
网络科 Internet	VPN 连接
伊 状态	<u> </u>
<i>候</i> WLAN	ipsec 「完成连接
P 以太网	
命 拨号	取消
% VPN	高级选项
∲→ 飞行模式	允许通过按流量计费的网络进行 VPN 连接
(l) 移动热点	 关 允许漫游时进行 VPN 连接
④ 数据使用量	★
⊕ 代理	

配置关键点

有点电脑注册表没有自动生成,这时候尽量都先新建下注册表

修改注册表

- 1、在"开始 > 运行"中,输入regedit命令,单击"确定",进入注册表编辑器。
- 2、在"注册表编辑器"页面的左侧导航树中,选择"HKEY_LOCAL_MACHINE > SYSTEM >CurrentCont rolSet > Services > Rasman > Parameters"。
- 3、在菜单栏上选择"编辑 > 新建 > DWORD值"。
- 4、键入ProhibitIpSec, 然后按"ENTER"。
- 5、右键单击ProhibitIpSec,选择"修改",进入修改界面。
- 6、在"数值数据"框中键入1。
- 7、单击"确定",并退出注册表编辑器。
- 8、重新启动该PC,使修改生效。

件(F)编辑(E)查看(V) 算机\HKEY_LOCAL_MACHIN	tertterte (a) ter Dis (a)				
算机\HKEY_LOCAL_MACHIN	X藏兴(A) 帮助(H)				
	VE\SYSTEM\CurrentCont	trolSet\Services\RasMan	Parameters		
Y Paran	heters	▲ 名称	类型	数据	
~ <u></u> (折登	all all result	DEC 07	(数值未设置)	
	新建(N)	> 项(K)	RY	00 00 00 00	
> PPP	查找(F)	字符串值(S)	RD	0x00000000 (0)	
- Seci	删除(D)	二进制值(B)	RD	0x00000000 (0)	
🕂 🔤 Thir	重命 (R)	DWORD (32 (th)	信(D) RD	0x00000000 (0)	
> 🔤 RasPp			(C) I S7	rastani	
> 🔤 RasSst	导出(E)		BD	0x0000ffff (65535)	
- 📙 rdbss	权限(P)	多子符串值(M)	RD	0-0000001 (1)	
- RDMA	信制(雨夕谷(C))	可扩充字符甲值(a) 10 c⁻¹	0.00000001(1)	
> 📙 rdpbu	20039042104(C)	ServiceDil	REG_EXPAND_SZ	%SystemRoot%\System32\rasmans.dll	
- RDPDR		ing ServiceDilUnic	REG_DWORD	0x0000001(1)	
> RDPNP					
> RDPUDE)				
> 📙 RdpVide	oMiniport				
> 📙 rdyboos	t				
- ReFS					
- ReFSv1					
> 📙 Remote	Access				
> 📙 Remotel	Registry				
> 🔤 RetailDe	mo				
> 📙 RFCOM	N				
- rhproxy					
> 🔤 RmSvc					
- rpcapd					
> RpcEptN	/lapper	~			
		>			
注册违治编辑					
(4)(1)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)	ホ (A) 部時(1)				
(+(F) SHEE(C) 三日(V) 10380	火(A) 和印(II)	\Services\RasMan\Paramet	ters		
Paramete	h h	(25) (25) (25) (25) (25) (25) (25) (25)	****		
Paramete		合价 哭望	5335		
Contig			0.77 (00.107.00.0)		
Vortig	CostedNetworkSetting	(鉄认) REG_	SZ (数值未)	段置)	
Vpr	CostedNetworkSetting	●(鉄込) REG_ 認AllocatedLuids REG_	SZ (数值未: BINARY 00 00 0	段置) 0 00	
> _ Config	CostedNetworkSettin	 ●(鉄込) REG_ ● AllocatedLuids REG_ ● AllowL2TPWea REG_ 	SZ (数值未) BINARY 00 00 0 DWORD 编辑(段面) 0 00 DWORD (32 位)值 ×	
Config PPP Security ThirdPart	nCostedNetworkSetting	(読み) REG」 認AllocatedLuids REG」 認AllowL2TPWea REG」 AllowPPTPWea REG」	SZ (数值未i BINARY 00 00 0 DWORD (編輯 1 DWORD (新聞	2回) 0 00 DWORD (32 位)值 ×	
Config PPP Provide the security Result of the security Result of the security Result of the security Result of the security	nCostedNetworkSetting y	 ● (新込) REG_ ● AllocatedLuids REG_ ● AllowL2TPWea REG_ ● AllowPPTPWea REG_ ● AllowPATIPWea REG_ ● Medias PEG 	SZ (数值未i BINARY 00 00 0 DWORD 编辑 (DWORD (数值者) DWORD (数值者)	2回) 0.00 DWORD (32.05)嬗 X 玄称(N):	
Config Config PP Security RasPppoe RasSstp	iCostedNetworkSetting	 (武以) REG」 AllocatedLuids REG」 AllowL2TPWea REG」 AllowPPTPWea REG」 CeepRasConn REG」 Midias REG」 Minortelestal 	SZ (数值未) BINARY 00 00 0 DWORD 编辑 (DWORD 数据3 MULTI_SZ Proh	9章) 0 00 0 WORD (32 位)值 × 室祭(N): ibitipSee	
 Contig PpP Security ThirdPart RasPpoe RasSstp rdbss 	iCostedNetworkSetting	AllocatedLuids REG_ AllocatedLuids REG_ Allowt2TPWea REG_ AllowtPTTWea REG_ teepRasConn REG_ MiniportsInstal REG_ MiniportsInstal REG_ ProhibitoSer PEG	SZ (数值未) BINARY 00 00 0 DWORD 编辑 (DWORD 数据 MULTI_SZ Prob DWORD 2 DWORD 2 DWORD 2 DWORD 2 DWORD 2 2014	8월) 0.00 DWORD (32 位)值 X 名称(N): biblitpSec	
Contig PPP Security RasPppoe RasStp RasStp RabMANDK	iCostedNetworkSetting	AllocatedLuids REG_ AllocatedLuids REG_ AllowL2TPWea REG_ AllowPTPWea REG_ Modias REG_ MiniportsInstal REG_ MiniportsInstal REG_ ProhibitipSec REG_ Sparical PEGC	SZ (数值未) BINARY 00 00 0 DWORD 编辑 [DWORD 0 DWORD 0 DW	8回) 0 00 WORD (3 位)値 × 名称(N): ibitipSec 数類(V): 基数	
Contig PPP Security ThirdPart ResPippoe ResStp rdbss RoMANDK Contig PPP Security ThirdPart ResPippoe Contig ThirdPart Contig PPP Security ThirdPart Contig ThirdPart Contig Contig PPP Security ThirdPart Contig Contig PPP Security ThirdPart Contig	nCostedNetworkSetting	AllocatedLuids REG_ AllocatedLuids REG_ AllowL2TPWea REG_ AllowPPTPWea REG_ Moreproteinstal REG_ Moreportsinstal REG_ ProhibitipSec REG_ SepriceDII REG_ SepriceDII REG_	SZ (数值未) BINARY 00 00 0 DWORD 编辑 (DWORD 5 DWORD 5 DWORD 5 DWORD 5 EXPAND_SZ 1 DWORD 1 EXPAND_SZ 1	9回) 0 00 2 00 2 00/06 (22 位)値 X 2 際(N): 2 際(N): 2 (1) 2 (1	
Contig Ver Security ResPippoe RasStp rdbss RDMANDK RDPDR	nCostedNetworkSetting	AllocatedLuids REG_ AllocatedLuids REG_ MalowL2TPWea REG_ MalowL2TPWea REG_ MalowPPTPWea REG_ MinportsInstal REG_ MinportsInstal REG_ ServiceDII REG_ ServiceDII REG_	SZ (数值集) BINARY 00 000 DWORD 9%備 U DWORD 9%備 U DWORD 9%6 DWORD 9%6 EXPAND_SZ 9 DWORD 4 EXPAND_SZ 9 DWORD 4	8回) 0.00 DWORD (32 位)値 X 名称(N): ibithpSee 助旗(V): 磁数 の小正朝(H) 〇十正朝(D)	
 Contig PPP Security RasPppoe RasStp rdbss rdbss rdpbus ROPON ROPON 	CostedNetworkSetting	الله المراجع ال مراجع المراجع ال مراجع المراجع ال	SZ (数值年) BINARY 00 00 00 DWORD 编辑 I DWORD 0 数值 DWORD 0 00 DWORD 0 00 DWORD 0 00 EXPAND_SZ 0 00 DWORD 0 00000 0 00000000000000000000000000	9回) 0 00 5 00 5 和(N): 5 (N): 5 (
Company C	CostedNetworkSetting	الالله المحالية ال محالية محالية المحالية م محالية محالية محالية المحالية محالية محالية محالية المحالية المحالي محالي محالية مح محالي محالي محالي محالي محالية محالية محالية محالية محالية محالية محالية محالية محاليمان محاليمان محاليمان محالي محالي محالي	SZ (数值来) BINARY 00 00 00 00 DWORD (数值) DWORD (数值) DWORD (数值) DWORD (数值) DWORD (数值) DWORD (数值) DWORD (数值) DWORD (数值)	8回) 0 00 DWORD (22 位)値 名称(N): 立成(V): 日十近朝(P)	
Company C	(CostedNetworkSetting y	الله المرابق المراب	SZ (武備書) BINARY 00 00 0 DWORD 9 DWORD 1 DWORD	8월) 0 00 WORD (32 位)値 X SKNI: ibiblipSec 故道(V): 図+六进時(H) 〇・十进時(C) [換定 取済 取済	
Comparing	CostedNetworkSetting	الله المراجع ا المراجع المراجع ا مراجع المراجع ال مراجع المراجع ال مراجع المراجع ا	SZ (改值年 BINARY 00 000 DWORD (如何的) DWORD (如何的) DWORD (如何的) DWORD (如何的) DWORD (如何的) DWORD (如何的) DWORD (如何的)	8월) 0 00 50WORD (32 位)値 X 客所(N): 51bbfbeec 数度(V): 0 十六世制(0) () 十世制(0) () 十世制(0) () 第二 取消	
Company C	(CostedNetworkSetting	관 (RFU) FREG	SZ (改通来 BINARY 00 00 (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	8週) 0 00 DWORD (22 位)通 × 名称(N): はbittpSee 数数(V): ③ 十六世制(P) 〇 十世制(D) 横電 取済	
 Company Per Per Per ResPppce ResStap Robanna Robond Robord Robord Robord Robord Robord Robord Refs Refs Refs Refs Refs Refs 	y iniport	관(해사) FREG Allocateduids REG Mallocateduids REG Mallocateduids REG Mallocateduids REG Mangotassan REG Mangotassan REG ProhibitpSec REG ProhibitpSec REG 양 serviceDII Unio REG	52 (708%) BINARY 00 000 DWORD (%%) DWORD (%%) DWORD (%%) BWORD (%%) DWORD (%%) EXCAND 52 (%) DWORD (%%) EXCAND 52 (%)	9回) 0 00 5 00 2 00 文字のRD (32 位)値 文字 (21) (21) (21) (21) (21) (21) (21) (21)	
Company C	y iniport iss isty	الله المرابق المراب	SZ (7038) BINARY 00.00.0 DWGRD (9000 WWGRD (9000) DWGRD (9000) DWGRD (9000) DWGRD (9000) DWGRD (9000) DWGRD (9000)	8世) 0 00 DWORD (32 位)値 × 度称(N): (2年(N): (2年(大正明(H) 〇十正明(D) 〇十正明(D) 〇十正明(D)	
 Company Per Per Security Trividant Ras/Pope Ras/Stp dbss RobNANCK rdpuss ROPDR ROPND ROPND ROPND ROPND RoPNDD RoPNDD Refsi Refsi RemoteRegsi RemoteRegsi RemoteRegsi RemoteRegsi RemoteRegsion 	y y iniport iss istry	관(해신) FREG Allocateduids REG (제Allocateduids REG (제Allocateduids REG) (제AllowPTPWea REG (MalowPTPWea REG (제AllowPTPWea REG) 에 Miniportaintal REG 에 Miniportaintal REG 에 ProhibitipSes REG 아이아 REG ServiceDIUnio REG	SZ (7084) BINARY 00 00 00 00 00 00 00 00 00 00 00 00 00	8월) 0 00 DWORD (32 位)値 X 家族(N): NibhtpSec 取属(V): 日本語朝(H) 〇十混朝(D) 〇十混朝(D)	
Comparing	y iniport 155 istry	الله المراجع ا المراجع الم المم المراجع المراجع المراجع المراجع المراجع المراجع المراجع المراجع	SZ (7088) BINARY 00000 DWCRD 0000 DWCRD 00000 DWCRD 00000 DWCRD 00000 DWCRD 00000 DWCRD 00000 DWCRD 00000 DWCRD 00000 DWCRD 00000 DWCRD 00000	8世) 0 00 2 00 2 00 2 00 2 00 2 00 2 00 2 0	
Constant Constant	(CostedNetworkSetting y iniport iss istry	الالله المحالية ال محالية المحالية المحالي محالية محالية المحالية محالية المحالية المحالية المحالية المحالية ال محالية محالية محالي محالية محالية محالية محالية محالية محالية محالية مح	SZ (7038) BINARY 00 00 00 DWORD (90000 DWORD (2000) DWORD (2000) DWORD (2000) DWORD (2000) DWORD (2000) DWORD (2000)	8월) 0 00 DWORD (32 位)値 また(N): : : : : : : : : : : : : : : : : : :	
 Company PP Security RasPppce RasSrap RobNANICK RobPN ROPN ROPND ROPND ROPND RoPVDD Refsi Refsi<td>CostedNetworkSetting y iniport :ss istry</td><td>ها (اللابل) الحقق المالي المالي الم المالي المالي المالي المالي المالي المالي</td><td>SZ (7088) BINARY 00 000 DWORD (988) DWORD (988) DWORD (988) DWORD (988) EXPAND SZ (988) DWORD (988)</td><td>9回) 0 00 2 00 2 00 文字(N): 2 (次): 2 (文): 2 ((文): 2 (文): 2 (文): 2 ((文): 2 ((文): 2 ((文): 2 ((文): 2 (((x))))) 2 ((x)): 2 ((x))) 2 ((x)): 2 ((x))) 2 ((x)): 2 ((x))) 2 ((</td><td></td>	CostedNetworkSetting y iniport :ss istry	ها (اللابل) الحقق المالي المالي الم المالي المالي المالي المالي المالي	SZ (7088) BINARY 00 000 DWORD (988) DWORD (988) DWORD (988) DWORD (988) EXPAND SZ (988) DWORD (988)	9回) 0 00 2 00 2 00 文字(N): 2 (次): 2 (文): 2 ((文): 2 (文): 2 (文): 2 ((文): 2 ((文): 2 ((文): 2 ((文): 2 (((x))))) 2 ((x)): 2 ((x))) 2 ((x)): 2 ((x))) 2 ((x)): 2 ((x))) 2 ((
 Company Prevent Prevent Reservity Thriddatt RasSep RDMANDK RDMANDK RDPDR RDPDR RDPDR RDPDR RDPUDD RdpVideott RefS RefS RefSit RefSit RemotReg RefSit RemotReg RefSit Re	y iniport 155 istry	관 (RFU) FREG Allocated Luids REG (제 Allocated Luids REG) 에 Allow 27PWeas. REG 에 Allow 20PWeas. REG 에 Miniportinatal. REG 에 Miniportinatal. REG 에 Prohibitip Sec REG 와 Service DIUnio REG	SZ (7084) BINARY 00000 DWORD (1994) DWORD (1994) WUCHS (1994) DWORD (1994) DWORD (1994) DWORD (1994) DWORD (1994)	8월) 0 00 DWORD (32 位)値 文字(N): (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	
Constant Constant	CostedNetworkSetting y iniport iss istry per v	관(RKU) FEG	SZ (7088) BINARY 00 00 00 DWORD 00 00 00 DWORD 00 00 DWORD 00 00 BWORD 00 00 DWORD 00 00 EXPAND SZ 1 DWORD 00000	9回) 0 00 2 00 2 00 文字 2 (小):	

附件下载: W10拨号截图.rar