IPSec VPN 程咪 2019-09-23 发表

# 组网及说明

# 1 配置需求或说明

#### 1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

ERG2 产品系列路由器: ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等。

注: 本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

#### 1.2 配置需求及实现的效果

总部有一台防火墙,分支有一台ERG2路由器部署在互联网出口,因业务需要两端内网需要通过VP N相互访问。IP地址及接口规划如下表所示:

公司名称	外网接口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部	1/0/3	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部	WAN1	动态获取		LAN1	192.168.20.0/24

#### 2 组网图



# 配置步骤

# 3 配置步骤

# 3.1 总部防火墙侧配置

# 3.1.1 创建IPSEC安全提议

#加密类型设置为3des-cbc,认证类型设置为sha1。

#### [H3C]ipsec transform-set 1

[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc

[H3C-ipsec-transform-set-1]esp authentication-algorithm sha1

[H3C-ipsec-transform-set-1]quit

## 3.1.2 创建IKE安全提议

#配置IKE安全提议默认的认证类型为sha1,加密类型为3DES-CBC,DH组为DH2

# [H3C]ike proposal 1

[H3C-ike-proposal-1] encryption-algorithm 3des-cbc

[H3C-ike-proposal-1] authentication-algorithm sha1

[H3C-ike-proposal-1] dh group2

### [H3C-ike-proposal-1]quit

### 3.1.3 创建IKE安全密钥

#创建IKE密钥,分部侧设备的公网IP地址不固定,这边的地址就写为0.0.0.0,密码设置为123456。

[H3C]ike keychain 1

[H3C-ike-keychain-1]pre-shared-key address 0.0.0.0 key simple 123456

[H3C-ike-keychain-1]quit

### 3.1.4 配置标识本端身份的FQDN名称

[H3C] ike identity fqdn F100

#### 3.1.5 创建IKE安全框架

#创建IKE安全框架,将本端名称、对端名称、keychain、proposal关联起来。

- [H3C]ike profile 1
- [H3C-ike-profile-1]keychain 1
- [H3C-ike-profile-1]exchange-mode aggressive
- [H3C-ike-profile-1] local-identity fqdn F100
- [H3C-ike-profile-1] match remote identity fqdn ER
- [H3C-ike-profile-1]proposal 1
- [H3C-ike-profile-1]quit

#创建IKE安全策略模板GE1/0/3将transform-set、ike-profile关联起来。 [H3C]ipsec policy-template GE1/0/3 1 [H3C-ipsec-policy-template-GE1/0/3-1]transform-set 1 [H3C-ipsec-policy-template-GE1/0/3-1]ike-profile 1 [H3C-ipsec-policy-template-GE1/0/3-1]quit #创建一个IPsec安全策略引用策略模板 [H3C]ipsec policy GE1/0/3 1 isakmp template GE1/0/3 3.1.7 创建ACL拒绝IPSEC兴趣流的数据 #创建acl 3888调用在外网接口用于排除IPSEC兴趣流不做NAT。 [H3C]acl advanced 3888 [H3C-acl-ipv4-adv-3888]rule deny ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255 [H3C-acl-ipv4-adv-3888]rule permit ip source any [H3C-acl-ipv4-adv-3888]quit 3.1.8 外网接口调用IPSEC策略和NAT动态转换策略 [H3C]interface GigabitEthernet 1/0/3 [H3C-GigabitEthernet1/0/3]ipsec apply policy GE1/0/3 [H3C-GigabitEthernet1/0/3]nat outbound 3888 [H3C-GigabitEthernet1/0/3]quit 3.1.9 配置安全策略放通IPSEC数据 #创建对象组,组名称为192.168.10.0 [H3C]object-group ip address 192.168.10.0 [H3C-obj-grp-ip-192.168.10.0]0 network subnet 192.168.10.0 255.255.255.0 [H3C-obj-grp-ip-192.168.10.0]quit #创建对象组,名称为192.168.20.0 [H3C]object-group ip address 192.168.20.0 [H3C-obj-grp-ip-192.168.20.0]0 network subnet 192.168.20.0 255.255.255.0 [H3C-obj-grp-ip-192.168.20.0]quit #创建对象策略,策略名称为Untrust-Trust [H3C]object-policy ip Untrust-Trust [H3C-object-policy-ip- Untrust-Trust] rule 0 pass source-ip 192.168.20.0 destination-ip 192.168.10.0 [H3C-object-policy-ip- Untrust-Trust]quit #创建Untrust到Tust域的域间策略调用Untrust-Trust策略 [H3C]zone-pair security source Untrust destination Trust [H3C-zone-pair-security-Untrust-Trust]object-policy apply ip Untrust-Trust [H3C-zone-pair-security-Untrust-Trust]quit 3.1.10 配置安全策略, 放通Untrust到Local, 以及Local到Utrust的策略, 用于建立IPSEC 隧道 #创建对象策略,策略名称为Untrust-Local [H3C]object-policy ip Untrust-Local [H3C-object-policy-ip-Untrust-Local] rule 0 pass [H3C-object-policy-ip-Untrust-Local]quit #创建Untrust到Local域的域间策略调用Untrust-Local策略 [H3C]zone-pair security source Untrust destination Local [H3C-zone-pair-security-Untrust-Local]object-policy apply ip Untrust-Local [H3C-zone-pair-security-Untrust-Local]quit #创建对象策略,策略名称为Local-Untrust [H3C]object-policy ip Local-Untrust [H3C-object-policy-ip-Local-Untrust] rule 0 pass [H3C-object-policy-ip-Local-Untrust]guit #创建Local到Untrust域的域间策略调用Local-Untrust策略 [H3C]zone-pair security source Local destination Untrust [H3C-zone-pair-security-Local-Untrust]object-policy apply ip Local-Untrust [H3C-zone-pair-security-Local-Untrust]quit 3.1.11 保存配置 [H3C]save force 3.2 分部ERG2路由器侧配置 3.2.1 配置IPSec 虚接口

3.1.6 创建IPSEC安全策略模板

单击【VPN】--【VPN设置】--【虚接口】, 点击【新增】, 绑定对应的WAN口, 比如WAN1:

нас								
▶ 系统导航	安全联盟	E掛口 IKES	b全權說 IKE别	等体 IPSec安	全變说 IPS	lec安全策略		
▶ 系统监控								
≫ 推口管理	安全部	2SA						
▶ 上同管理	通过安	全联盟SA, IPS	ec能够对不同的数据	·高提供不同级别的!	安全保护。在这	里可以查询到相同	<b>白隧道当前状态</b> ,	了解隧道建立的谷小香
> 安全考区	RT +							
V 178	*	春 方向	能道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	教師流
L2TP VPH					W 17	5/#1西#0;	中記录 御西 10	
> Q+++2/2								
▶ 高级设置								
≥ 设备管理								
> Mitan								
新增虚接口列表								×
虚接口名	称:	ipsec	•0 🔻					
绑定接	<b>[</b> ]:	WAN1	•					
摧	i述:							
		増加	取消					

#### 3.2.2 配置IKE安全提议

单击【VPN】--【VPN设置】--【IKE安全提议】,点击【新增】,配置IKE安全提议的各个参数:安全 提议名称、IKE验证算法、IKE加密算法、IKE DH组,如下图配置。

	安全寡想 击折	TRE BOR	KE21第年 IPSec安全	君设 IPSec安全議論	
≥ 系统导航	× ± •0.46 14 19	INEXABLE I	NEED IN DECK T	TE K IF OCCULANT	
▶ 系統监控	安全提议				
▶ 推口管理	安全提议的配置修改	と后,需要重新启用(先禁用	再启用)引用该安全提议的1	PSEC安全策略或重新使能II	PSEC功能,新的配置才能生效。
> 加管理	金通新規	開発化	关键字:	名称 •	査询 显示全部
上月管理	操作 序号	名称	认证算法	加密算法	DH组
Z#iPi	/ 1	IKE	SHA1	3DES	DH2 modp1024
安全专区	-		第1页/#	1页共1条记录每页 1	0 17 H 4 1 Go H 1
用相IKE安当	E提取刘表				×
÷	今世议之称,	TEE		(#E) 4 464	
安	全提议名称:	IKE		(范围:1~16个	字符)
安 I	全提议名称: KE验证算法:	IKE SHA1 ·	•	(范围:1~16个	字符)
安 II II	全提议名称: KE验证算法: KE加密算法:	IKE SHA1 · 3DES	•	(范围:1~16个	字符)

修改 取消

### 3.2.3 配置IKE对等体

单击【VPN】--【VPN设置】--【IKE对等体】,点击【新增】,配置IKE对等体: 对等体名称为IKE、绑定虚接口为ipsec0(前面已经创建)、对端地址为总部的公网ip,即101.88.26.3 4;协商模式选择野蛮模式,ID类型为name类型并配置本段的ID为ER对端的ID为F100;安全提议选择 ike(前面已经创建)、配置预共享秘钥,此处配置为123456,其余选择默认即可。

安全联盟	业接口 IKES	安全提议 IKE3	1等体 IPSec安全	注提家 IPSec安全部	16		
		_	_				
对等体							
对等体的配置给	改后,需要重新	启用(先禁用再 启用	)引用该对等体的IPSB	EC安全策略派重新使能II	PSEC功能	5,新的配置才能生	效*
金达 新燈	1078		关键字:	名称 *		<b>童词 显示</b> 全	85
操作 序号	名称	虚推口	对调地址	21.29	ID类型	安全覆谈	DPD
1 1	IKE	ipsec0	101.88.26.34	野窯模式	NAME	IKE	关闭
			第1页/	具1页具1条记录每页	10	र्गिम्स <b>स</b> 1	Go # #
1							
	安全职盟 对等体 对等体的截置给 全选 航程 發作 序号	安全联盟 金融口 IKE5 対導体 対導体的動置的次后・電景重額 全人 NU2 操作 序号 余務 1 IKE	安全联盟         金橋口         IKE 安全景空         IKE           対導体         対撃         対撃         対撃         対撃 </td <td>安全発還 曲線口 IKE安全管设 IKE31等称 IPSec安立 対等称 対等称的設置的次后, 電簧整新高用(先展用再高用)5(用收引等体約IPSi 法, 50° 新計 关键字: 重命 序号 各称 虚像口 対端地址 1 IKE Space 101.85.25.34 第 1 页/</td> <td>安全報道         曲線口         IKE 安全報道         IKE 刻等身         IPSec 安全報道         IPSec 安全報道           対導路         対導路         対導路         大雄字:         高原         新規         世界         日         &lt;</td> <td>安全和型 曲線口         IKE安全指染         IPSec安全指染         IPSec安全指染         IPSec安全指染           対等体         対等体         対等体         対等体         対等体           対导体的記述並次后・電景委員由用(先見用再品用)引用收引等体約1PSEC安全推測或量量検索1PSEC安全推測或量量検索1PSEC安全推測         大量字: 名称・            液体         建橡口         対端地址         構成         ID 先生           操作・厚心         内         機像口         対端地址         構成         ID 先生           1         IKE         ipsec0         101.85.26.34         野菜 成         NAME           第         IKE         ipsec0         101.85.26.34         野菜 成         NAME           第         IKE         ipsec0         101.85.26.34         野菜 成         10</td> <td>安全和型 曲線口         IKE安全置較         IPSec安全置較         IPSec安全置較           対等体         対等体         対等体         対等体           対等体         対等体         メ業         会報           対等体         共建字: 会称・         夏田         東京           原作 序号         会称         虚管口         対端地址         概式         ID 長型         安全保定           1         IKE         lpsec0         101.48.26.14         野菜 (KR)         NAME         IKE           第 1 同川県 1 原にでの         101.48.26.14         野菜 (KR)         IKE         IE         IE</td>	安全発還 曲線口 IKE安全管设 IKE31等称 IPSec安立 対等称 対等称的設置的次后, 電簧整新高用(先展用再高用)5(用收引等体約IPSi 法, 50° 新計 关键字: 重命 序号 各称 虚像口 対端地址 1 IKE Space 101.85.25.34 第 1 页/	安全報道         曲線口         IKE 安全報道         IKE 刻等身         IPSec 安全報道         IPSec 安全報道           対導路         対導路         対導路         大雄字:         高原         新規         世界         日         <	安全和型 曲線口         IKE安全指染         IPSec安全指染         IPSec安全指染         IPSec安全指染           対等体         対等体         対等体         対等体         対等体           対导体的記述並次后・電景委員由用(先見用再品用)引用收引等体約1PSEC安全推測或量量検索1PSEC安全推測或量量検索1PSEC安全推測         大量字: 名称・            液体         建橡口         対端地址         構成         ID 先生           操作・厚心         内         機像口         対端地址         構成         ID 先生           1         IKE         ipsec0         101.85.26.34         野菜 成         NAME           第         IKE         ipsec0         101.85.26.34         野菜 成         NAME           第         IKE         ipsec0         101.85.26.34         野菜 成         10	安全和型 曲線口         IKE安全置較         IPSec安全置較         IPSec安全置較           対等体         対等体         対等体         対等体           対等体         対等体         メ業         会報           対等体         共建字: 会称・         夏田         東京           原作 序号         会称         虚管口         対端地址         概式         ID 長型         安全保定           1         IKE         lpsec0         101.48.26.14         野菜 (KR)         NAME         IKE           第 1 同川県 1 原にでの         101.48.26.14         野菜 (KR)         IKE         IE         IE

编辑IKE对等体			×
	-		
对等体名称:	IKE	(范围:1~16个字符)	
虚接口:	ipsec0 🔻		
对端地址:	101.88.26.34	(IP 或 域名)	
协商模式:	◎ 主模式 ⑧ 野蛮様	莫式	
ID类型:	◎ IP类型 ④ NAME	5类型	
本端ID:	ER	(范围:1~32个字符)	
对端ID:	F100	(范围:1~32个字符)	
安全提议一:	IKE 👻		
安全提议二:	请选择 ▼		
安全提议三:	请选择 ▼		
安全提议四:	请选择 ▼		
预共享密钥(PSK):	123456	(范围:1~128个字符)	
生命周期:	28800 秒位	围:60~604800秒,缺省值:28800)	
DPD:	◎ 开启    关闭		
DPD周期:	10	]秒(范围:1~60秒,缺省值:10)	
DPD超时时间:	30	]秒(范围:1~300秒,缺省值:30)	
	修改 取消		

## 3.2.4 配置IPSec安全提议

单击【VPN】--【VPN设置】--【IPSec安全提议】,点击【新增】,配置IPSEC安全提议:安全提议 名称、安全协议类型、ESP验证算法、ESP加密算法配置如下图:

▶ 系统导航	安全联盟 虚	推口 IKE安全提议	IKE对等体 IPSec安	全權说 IPSec安全策略	
▶ 系统监控					
≫ 推口管理	安全提	ŵ.			
≽ AF管理	安全提议的	配置総改后・需要重新启	用(先慧用再启用)引用该安全	權效的IPSEC安全策略或重新使	临IPSEC功能,新的配置才能生效。
▶ 上阿德理	22	#18 P.12		关键字: 名称 -	24 AF±6
⇒ ±¥iFi	操作 序4	1	安全协议	AHBA	ESPILĂ
> 安全有区	1.1	Psec	659		3DES-SHA1
W VIN				第1页/共1页共	1条记录 編页 10 行HH H 1 Ga H HH
S LICEL VIS					
,	/夕称:	IPsor			(范围:1~31个字符)
× ± 11 %		11 300			()300,1.21(-74)
	/类刑:	O AH @	ESP AH+	ECD.	
安全协议			LOF PATT	ESP	
安全协议 ESP验证	算法:	SHA1 T	Lor - Aitt	ESP	
安全协议 ESP验证 ESP加密	算法: 算法:	SHA1 T	]	ESP	

# 3.2.5 配置IPSec安全策略

单击【VPN】--【VPN设置】--【IPSec安全策略】,勾选启【用IPSec功能】,点击【新增】,配置IP Sec安全策略:本地子网IP即为分支内网网段,此处配置为192.168.20.0/24,对端子网IP即为总部内网 网段,此处配置为192.168.10.0/24,其余参数按照下图所示配置:

5400 to 10			0.00	ment of ht da	INFO CROWN	THE OCTO DE DE		
● 未限可能	2.4.M. 12.10	IR	A SC T HE RC	THE XI IF IF	Inser%X#K	These 2 The		
→ 株口管理	IDEa-20							
≽ AT管理	IP-Sec (t)				T omm	Courte Million		
> 上同管理					E MHIP	Section		
» <del>⊼1</del> 171								
>> 安全考区	安全業業	- 410-	TAXED IN A	merch è filiz	en an an an an an an an an an	□●東美公司/未知		CRAME-INF
V VZN	IPSEC功能一	次,新的	配置就能主效	另外, 能改IP:	SEC安全策略的截置也能	能使新的配置生效。	na ma walina / nationali ser a	CXIM-AN
LITE VEN	22 B	<b>1</b>	8		关键字:	名称 •	皇년	重导金将
▶ 9+s设置	操作 序号		名称	状态	本诸子同同段	对端子阿阿段	协商类型	<b>邦</b> 它
≥ 高级设置	1 1		lpsec	启用	192.168.20.0/ 255.255.255.0	192.168.10.0/ 255.255.255.0	182协商	对等体: NE
▶ 设备管理						第1页/共1页 #	+ 1 亲记录 每页	5 (9H H 1
安全策略名称:	ipse			(范围:1	~16个字符)			
安全策略名称:	ipse			(范围:1	~16个字符)			
安全策略名称: 是否启用:	ipse 启用	•		(范围:1	~16个字符)			
安全策略名称: 是否启用: 本地子网IP/指码:	ipse 启用 192.	° ▼ 168. 2	0.0	(范围:1- / 255.2	~16个字符) 55.255.0			
安全策略名称: 是否启用: 本地子网IP/指码: 对满子网IP/指码:	ipse 启用 192. 192.	- • 168. 2 168. 1	0.0	(范围:1- / 255.25 / 255.25	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地子网IP/摧码: 对骥子网IP/摧码: 协商类型:	ipse 倉用 192. 192. ● IK	。 ▼ 168,2 168,1 E协商	0.0 0.0 ① 手道	(范围:1- / 255.25 / 255.25 加模式	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地于阿IP/报码: 对谋于阿IP/报码: 协商类型: 对等体:	ipse 启用 192. 192. ◎ IK IKE	。 168.2 168.1 E协商	0.0 0.0 ① 手衣	(范围:1- / 255.25 / 255.25 助模式	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地子网IP/搅码: 对端子网IP/搅码: 协商类型: 对等体: 安全提议一:	ipse 倉用 192. 192. ● IK IKE IPse	。 168.2 168.1 E协商 •	0.0 0.0 ① 手名	(范围:1- / 255.25 / 255.25 b模式	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地子网IP/搅码: 对端子网IP/搅码: 协商类型: 对等体: 安全提议一: 安全提议二:	ipse 倉用 192. 192. ◎ IK IKE IPse 请选	<ul> <li>▼</li> <li>168.2</li> <li>168.1</li> <li>正协商</li> <li>∞</li> <li>∞</li> <li>∓</li> <li>¥</li> </ul>	0.0 0.0 ① 手式	(范国:1- / 255.2 / 255.25 b模式	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地子网IP/搅码: 对端子阿IP/搅码: 协商类型: 对等体: 安全提议二: 安全提议二:	ipse 启用 192. 192. 9 IK IVse 请选 请选	□ ■ 168.2 168.1 E协商 ■ 定 平 择 ■	0.0 0.0 ② 手a	(范围:1- / 255.2 / 255.25 b模式	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地子网IP/搅码: 对端子网IP/搅码: 协商类型: 对等体: 安全提议一: 安全提视议二: 安全提议汉:	ipse 启用 192. 192. 第 E KE 译 透 请 选 请 选 请 选	<ul> <li>▼</li> <li>1168.2</li> <li>1168.1</li> <li>1168.1</li> <li>1168.4</li> <li>1168.4</li></ul>	0.0 0.0 ② 手车	(范围:1- / 255.2 / 255.25 / 255.25	~16个字符) 55.255.0 55.255.0			
安全策略名称: 是否启用: 本地子网IP/ 搅码: 功端子网IP/ 搅码: 协商类型: 对等体: 安全提视问: 安全提视问: 安全提视问: 安全提视问: 安全提视问:	ipse 启用 192. 9 IK IKE 请选 请选 请述	<ul> <li>▼</li> <li>168.2</li> <li>168.1</li> <li>Eb南</li> <li>▼</li> <li></li> <li></li></ul>	0.0 0.0 ① 手走	(范围:1- / 255.2 / 255.25 / 255.25	~16个字符) 55.255.0 ;5.255.0			
安全策略名称: 是否面用: 本地子网IP/ 代码: 功端子网IP/ 代码: 协第子网IP/ 代码: 功等承型: 安全建提议二: 安全建提议二: 安全建提议二: 安全建提议二: 安全是提议二: 安全是提议二: 安全是提议二: 安全是提议二: 安全是提议二: 安全策略名称:	ipse 启用 192. 9 IK IKE 译选 请选 请选 某止 2880	c ▼ 168.2 168.1 168.1 1 日 時 南 マ ▼ ▼	0.0 0.0 ●手a 秒 (页	(范围:1- / 255.25 / 255.25 / 旗式 頭:120~	~16个字符) 55. 255. 0 i5. 255. 0	<u>#</u> :28800)		

## 3.2.6 配置去往对端子网的静态路由

单击【高级设置】--【路由设置】--【静态路由】,目的地址配置成对端子网,即192.168.10.0,子网 掩码为255.255.255.0,出接口为ipsec0虚接口。

> X49K	志路由 策略站	in in in its second				
▶ 系统监控						
▶ 推口管理	静态路由表	_				
» AF管理	2.2 810		18.0	共建学: 新过	•	Ra Afta
▶ 上阿管理	操作 序号	目的地址	子同推码	下一跳地址	出售口	願述
> ± ₹171	1.1	192.168.10.0	255.255.255.0		ipsec0	
> RE415				第 1 页/共 1 3	5 共 1 条记录 每页	10 17 en en 1 Go e 1
> 0+x102						
▽ 高田夜園						
地址转换						
> 第由设置						
编辑静态路由列	表					
目的地址:	1	92.168.1	0.0			
HH)/G/H						
子网掩码:	2	55.255.2	55.0			
下一跳抽扯。						
1. 19030311.	_					
出接口:	i	psec0 🔻				
描述。					* ***	
"田儿二・				(中))	选, 氾围:1,	~15个字付)
			修改 取	浦		
3 测试VPN是否通	<u> </u>					

# 3.3.1 数据访问触发IPsec建立

在分部内网中任意找一台电脑访问对端网络资源。

举例:在分支侧电脑ping总部侧电脑, IPSEC初始建立时会丢1-2个包, 建立后通信正常。

C:\Users\sfw1081>ping 192.168.10.3
正在 Ping 192.168.10.3 具有 32 字节的数据: 请求超时。 诗文超时
頃か起4)。 来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=255 来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=255
192.168.10.3 的 Ping 统计信息: 数据句·已发送 = 4 已接收 = 2 毛牛 = 2 (50) 毛牛 )
往返行程的估计时间<以毫秒为单位>: 最短 = Oms,最长 = Oms,平均 = Oms

#### 3.3.2 查看IPSEC监控信息

#V7防火墙通过命令行查看display ike sa可以看到隧道状态为RD状态表示ike建立完成。

[H3C]dis ike sa Connection-ID Remote Flag DOI 29 198.76.26.90 RD IPsec Flags: RD--READY RL--REPLACED FD-FADING RK-REKEY #V7防火墙通过display ipsec sa可以看到IPSEC SA基本状态。 [H3C]dis ipsec sa Interface: GigabitEthernet1/0/3 IPsec policy: GE1/0/3 Sequence number: 1 Mode: Template Tunnel id: 0 Encapsulation mode: tunnel Perfect Forward Secrecy: Inside VPN: Extended Sequence Numbers enable: N Traffic Flow Confidentiality enable: N Path MTU: 1444 Tunnel: local address: 101.88.26.34 remote address: 198.76.26.90 Flow: \*: sour addr: 192.168.10.0/255.255.255.0 port: 0 protocol: ip dest addr: 192.168.20.0/255.255.255.0 port: 0 protocol: ip [Inbound ESP SAs] SPI: 4032357769 (0xf058e589) Connection ID: 158913789952 Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1 SA duration (kilobytes/sec): 1843200/3600 SA remaining duration (kilobytes/sec): 1843199/3545 Max received sequence-number: 8 Anti-replay check enable: Y Anti-replay window size: 64 UDP encapsulation used for NAT traversal: N Status: Active [Outbound ESP SAs] SPI: 1786751150 (0x6a7fa8ae) Connection ID: 64424509441 Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1 SA duration (kilobytes/sec): 1843200/3600 SA remaining duration (kilobytes/sec): 1843199/3545 Max sent sequence-number: 8 UDP encapsulation used for NAT traversal: N Status: Active ERG2侧:

在【VPN】--【VPN设置】--【IPSec安全策略】--【安全联盟】里查看隧道建立情况

安全联盟SA									
通过安全联盟SA+ IPS	iec戰移对不同的數據流提	供不同级别	的安全保护。在这里;	可以重调到相应	羅繼治前状态。	了解隨邊建立的	9音个鬱歡。		
etat	48	-the the	PR 26 46 10	AU CD7		560 CDT	ren 1824		
	ipsec	in	101.88.26.34 =>198.76.26.90			0x6a7fa8ae	JDES_SHAT	192.168.10.0/24 =>192.168.20.0/24	
	lpsec	out	198.76.26.90 =>101.88.26.34			0xf058e589	3DES_SHA1	192.168.20.0/24 =>192.168.10.0/24	
							第13	5/共1页共2条记录每页	10