IPSec VPN IPv4 zhiliao\_5ilsv 2018-11-25 发表

#### 组网及说明

1 配置需求或说明

#### 1.1 适用产品系列

本案例适用于ER产品系列路由器: ER3260、ER3100、ER3200、ER5200等。 注意: ER6300、ER8300不支持IPSEC VPN。

#### 1.2 配置需求及实现的效果

Router A和Router B均使用ER系列路由器,在两者之间建立一个安全隧道,对客户分支机构A所在的子网(192.168.1.0/24)与客户分支机构B所在的子网(172.16.1.0/24)之间的数据流进行安全保护,实现2端子网终端通过IPsec VPN 隧道进行互访。

#### 2 组网图



## 配置步骤

### 3 配置步骤

### 3.1 基本连接

在路由器接口面板找到LAN接口,用网线将电脑和设备的任意一个LAN接口连在一起,电脑可以自动获取192.168.1.X/24网段的地址。电脑连接好路由器之后完成后打开浏览器,在浏览器地址栏中输入http://192.168.1.1登录设备管理界面。

### 3.2 登陆设备WEB界面

运行Web浏览器,在地址栏中输入http://192.168.1.1,如下图所示。



回车后跳转到Web登录页面,输入用户名、密码(缺省均为admin,区分大小写)以及验证码(不区分大小写),如下图所示。



单击【登录】按钮或直接回车后,您即可登录到路由器的Web设置页面,如下图所示。

нзс	
	基本信息 运行状态 性能温液 技术支持
▶ 运行信用	性能指数
	也影響被功能以折线器的方式提供过系统CPU以及內存使用僅充的实时當被,在當稅过程中意可以继续对页面通
	1987-
	ph.
	and a second
	开始呈现
高级装置	

注意:同一时间,路由器最多允许五个用户通过Web设置页面进行管理。

## 3.3 配置IPSEC VPN

# 3.3.1 配置IPSEC 虚接口

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

нзс						
EARD	虚接口 IKE安全	提议 IKE对等体	IPSec安全提议	IPSec安全策略	}	
未次面立 接口设置	虛接口	do the			- 201	
安全专区	按关键字过滤:	名称 ▼ 关键字:		「重印」「显示す	自部	
VPN VPN@#	援作 序号	名称	绑定接口		描述	
VPN状态		第1	页/共 1页 共 0 ;	条记录 每页 10	行! 4 1	Go * *
QoS设置 高级设置 设备管理 用户FAQ	全选		新井			
🩋 虚接口 网页改	话框					<b>—</b>
	整接口名称: 绑定接口: 描述:	ipsec0 、 VANI 、 增加 取消				

### 3.3.2 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。

H3C					
	虚接口 IKE安全提议	IKE对等体 IPSecg	全提议 IPS	ec安全策略	
系线监控 第日设置 安全考区 VPN改置 VPN改善 QoS设置 高敏设置 高敏设置 明存在AO	安全提议 扶关建夺过步: 名称 任作 序号 全法	▼ 美雄字: 名除 第 1		■ 显示全部 加倍排法 未记录 毎页 10 部除	DH组 行/н н 1 бо жи
IKE安全提议	网页对话框				×
	安全提议名称:	IKE	(i	范围:1~16个字	2符)
	IKE验证算法:	SHA1 👻			
	IKE加密算法:	3DES -			
	IKE DH组:	DH2 modp10:	<sup>24</sup> ▼ 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Router B的公网ip,即192.100.100.19、协商模式选择主模式、

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(可根据自己需求自行设置)、其 余选择默认即可。

对等体名称:	like	(范围:1~16个字符)
虚接口:	ipsec0 -	
对端地址:	192.100.100.19	(IP 或 博名)
协商模式:	● 主模式 ○ 野蛮根	ET.
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 ▼	
模共享密钥(PSK):	123456	(范围:1~128个字符)
生命周期:	28800 秒(范	團: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:

後监控 口设置	安全提议				
全专区	按关键字过滤:	名称 ▼ 关键字:	重調	显示全部	
N VPN设置	操作 序号	名称	安全协议	AH算法	ESP算法
VPN状态	1	IPSEC	ESP		JUES-SHA
S设置		-	第1页/共1页共1	条记录 每页 10	行HH H 1 GC
<u>設設置</u> 5.管理	全法	J	新增	部派	
PFAQ					
1000000分担約	的百对沃和				ſ
IPSec安全提议	网页对话框				(
IPSec安全提议	网页对话框				ĺ
IPSec安全提议	阿页对话框				
IPSec安全提议 安全提	网页对话框 议名称:	IPSEC		(范围:1-	(
IPSec安全提议 安全提 安全损	网页对话框 议名称: 议类型:	IPSEC		(范围:1~	-31个字符)
(PSec安全提议 安全提 安全协	网页对话框 议名称: 议类型:	IPSEC AH @ ESP	P O AH+ESP	(范围:1~	-31个字符)
IPSec安全提议 安全提 安全损 ESP验	网页对话框 议名称: 议类型: 证算法:	IPSEC AH ® ESP SHA1 •	P O AH+ESP	(范围:1~	-31个字符)
IPSec安全提议 安全提 安全协 ESP蜒 ESP加	<b>网页对话框</b> 议名称: 议类型: ;证算法: !密算法:	IPSEC AH © ESP SHA1 - 3DES -	P ⊙ AH+ESP	(范围:1^	-31个字符)

# 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172.16.1.0,子网掩码为255.255.255.0,出接口为ipsec0虚接口。

静态路由配置 网页对话框					
目的地址:	172.16.1.0				
子网掩码:	255.255.255.0				
下一跳地址:					
出接口:	ipsec0 👻				
描述:		(可选,范围:1~15个字符)			
	増加 取消				
http://10.88.26.33:21007/ 🤤 Internet   保护模式: 禁用					

在Router B上, IPSec VPN的相关配置与Router A是相互对应的, Router B上除了IKE对等体的对端地址 以及IPSEC安全策略中的本地子网、对端子网需要做相应修改外,其他的设置均一致, Router B的具体 配置参见Router A配置,此处不再赘述。

注意:修改了IPSEC相关参数,需要将启用IPsec功能勾去掉应用再重新勾上应用使能,否则IPsec VP N无法起来。

3.4 保存配置

设备默认会保存配置。

配置关键点