

ERG2 系列路由器 IPSEC VPN 配置

目录

ERG2 系列路由器 IPSEC VPN 配置.....	1
1 配置需求或说明.....	1
1.1 适用产品系列.....	1
1.2 配置需求及实现的效果.....	1
2 组网图.....	2
3 配置步骤.....	2
3.1 基本连接.....	2
3.2 登陆设备 WEB 界面.....	2
3.3 配置 IPSEC VPN.....	3
3.3.1 配置 IPSEC 虚接口.....	3
3.3.2 配置 IKE 安全提议.....	3
3.2.3 配置 IKE 对等体.....	4
3.2.4 配置 IPSEC 安全提议.....	5
3.2.5 配置 IPSEC 安全策略.....	6
3.2.6 配置去往对端子网的静态路由.....	6
3.4 保存配置.....	7

1 配置需求或说明

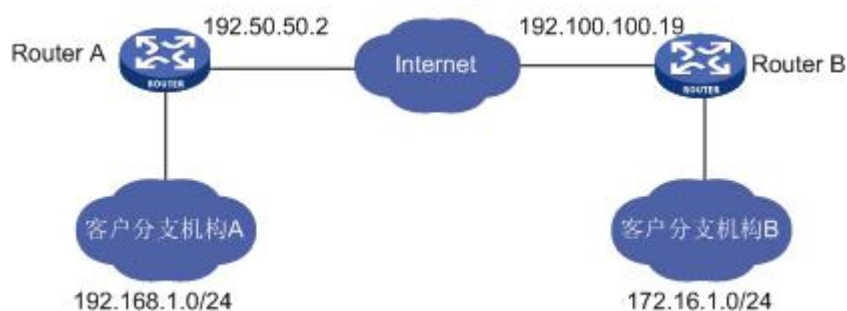
1.1 适用产品系列

本案例适用于 ERG2 产品系列路由器：ER8300G2-X、ER6300G2、ER3260G2、ER3200G2 等。

1.2 配置需求及实现的效果

Router A 和 Router B 均使用 ERG2 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



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）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。



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：



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。



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）、配置预共享密钥，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。



IKE对等体 -- 网页对话框

对等体名称: (范围:1~16个字符)

虚接口:

对端地址: (IP 或 域名)

协商模式: ☒ 主模式 ☐ 野蛮模式

安全提议一:

安全提议二:

安全提议三:

安全提议四:

预共享密钥(PSK): (范围:1~128个字符)

生命周期: 秒(范围:60~604800秒, 缺省值:28800)

DPD: ☐ 开启 ☒ 关闭

DPD周期: 秒(范围:1~60秒, 缺省值:10)

DPD超时时间: 秒(范围:1~300秒, 缺省值:30)

http://10.88.18.34:21007/ike_peer_config.asp?data Internet | 保护模式: 启用

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：

H3C

系统导航

系统监控

接口管理

上网管理

安全专区

VPN

IPSec VPN

L2TP VPN

Qos设置

高级设置

设备管理

用户FAQ

安全联盟 虚接口 IKE安全提议 IKE对等体 **IPSec安全提议** IPSec安全策略

安全提议

安全提议的配置修改后，需要重新启用(先禁用再启用)引用该安全提议的IPSEC安全策略或重新使能IPSEC功能，新的配置才能生效。

关键字: 名称

操作	序号	名称	安全协议	AH算法	ESP算法
编辑	1	bj	ESP	----	3DES-MD5

第 1 页/共 1 页 共 1 条记录 每页 10 行 << 1 >> Go >>

IPSec安全提议 -- 网页对话框

安全提议名称: (范围:1~31个字符)

安全协议类型: ☐ AH ☒ ESP ☐ AH+ESP

ESP验证算法:

ESP加密算法:

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 IPSEC 安全策略：本地子网 IP 即为 Router A 内网网段，此处配置为 192.168.1.0/24，对端子网 IP 即为 Router B 内网网段，此处配置为 172.16.1.0/24，其余参数按照下图所示配置：



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。

H3C

系统导航
系统监控
接口管理
上网管理
安全专区
VPN
Qos设置
高级设置
地址转换
路由设置
应用服务
设备管理
用户FAQ

静态路由 策略路由

静态路由表

全选 新增 删除 查看路由信息表 关键字: 描述 查询 显示全部

操作	序号	目的地址	子网掩码	下一跳地址	出接口	描述
	1	0.0.0.0	0.0.0.0	192.168.1.254	VLAN1	
	2	192.168.2.0	255.255.255.0	192.168.1.3	VLAN1	

第 1 页/共 1 页 共 2 条记录 每页 10 行 << 1 Go >>

新增静态路由列表

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)

增加 取消

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 VPN 无法起来。

3.4 保存配置

设备默认会保存配置。