AR系列路由器野蛮IPSEC的典型配置

姚忆斌 2006-09-25 发表

AR系列路由器野蛮IPSEC的典型配置

【需求】

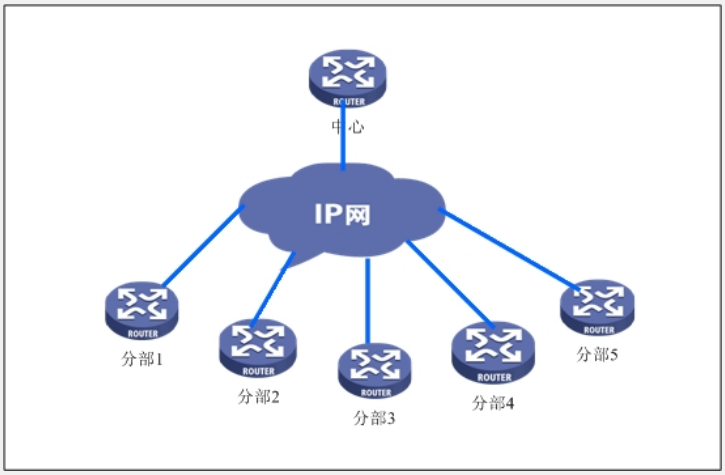
1、 除中心为固定IP外，其余各分部均不固定IP

2、 中心：支持VRP3.3 的R系列或AR系列路由器，内网网段192.168.0.0/24

3、 分部1 - 4：支持VRP3.3 的R系列或AR系列路由器，内网网段192.168.2~5.0/24

4、 分部5：Aolynk BR304 路由器，内网网段192.168.1.0/24

【组网图】



[中心配置]

下面的配置中省略了nat 的配置，省略了路由等配置，仅为突出VPN 的配置。

对中心配置简化的几点说明：

1、VRP3.3-0008 开始对VPN 的acl过滤的规则不像以前那样严格，所以acl 3009的配置完全可以。

2、ike仅配置一条即可，注意把max-connections配置为实际分部数量即可。

因为上述两点，中心路由器的配置大大简化。

中心配置	ike local-name center # 	
	ike proposal 1 authentication-algorithm md5 # 	
	ike peer 304 exchange-mode aggressive pre-shared-key huawei id-type name remote-name 304-1 max-connections **5** # 	
	ipsec proposal 1 # 	
	ipsec policy 1 1 isakmp security acl 3009 ike-peer 304 proposal 1 # 	
	interface Ethernet0/0 ip address 20.0.0.1 255.255.255.0 ipsec policy 1 # 	
	interface Ethernet1/0 ip address 192.168.0.1 255.255.255.0 # 	

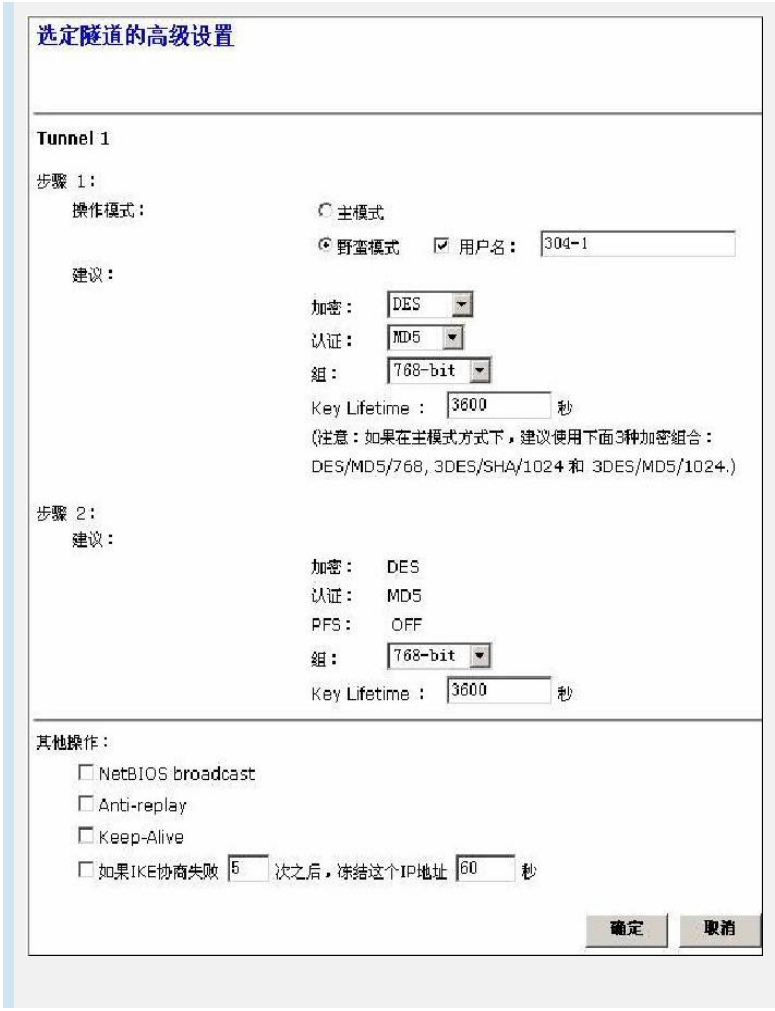
	acl number 3009 **rule 0 permit ip source 192.168.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255** rule 1 deny ip	

[分部1-4配置]

下面配置中，省略了adsl拨号或者以太口自动获取ip或者串口modem拨号，以串口固定ip代替；省略了nat的配置。

中心配置	ike local-name 304-1 #	
	ike proposal 1 authentication-algorithm md5 #	
	ike peer a exchange-mode aggressive pre-shared-key huawei id-type name remote-address 20.0.0.1 remote-name center #	
	ipsec proposal 1 #	
	ipsec policy 1 1 isakmp security acl 3000 ike-peer a proposal 1 #	
	interface Ethernet0/0 ip address 192.168.3.1 255.255.255.0 #	分部内网口地址依次为192.168.2～5.1/24
	interface Serial0/0 clock DTECLK1 link-protocol ppp ip address 20.0.0.2 255.255.255.0 ipsec policy 1 #	
	acl number 3000 rule 0 permit ip source 192.168.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255 rule 1 deny ip #	
	ip route-static 0.0.0.0 0.0.0.0 Serial 0/0 preference 60	

[分部5配置]


选定隧道的高级设置
Tunnel 1
步骤 1:
操作模式:
主模式
野蛮模式
用户名:
304-1
建议:
加密:
DES
认证:
MD5
组:
768-bit
Key Lifetime :
3600
秒
(注意:如果在主模式方式下,建议使用下面3种加密组合:
DES/MD5/768, 3DES/SHA/1024 和 3DES/MD5/1024.)
步骤 2:
建议:
加密:
DES
认证:
MD5
PFS:
OFF
组:
768-bit
Key Lifetime :
3600
秒
其他操作:
NetBIOS broadcast
Anti-replay
Keep-Alive
如果IKE协商失败
5
次之后,冻结这个IP地址
60
秒
确定
取消