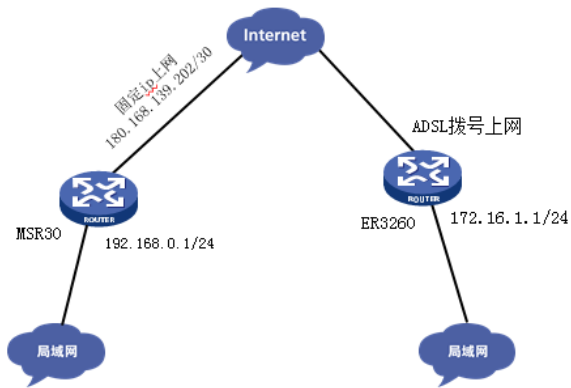


某公司总部使用H3C MSR30，分支使用H3C ER3260，ER3260上端运营商网络过了一个NAT设备，要实现分支与总部建立IPSEC VPN。组网图如下：



1、ER3260上的配置

1.1 接口设置—WAN设置—连接到因特网。

The screenshot shows the configuration page for the H3C ER3260 router, specifically the '连接到因特网' (Connect to Internet) section. The page title is 'H3C ER3260 Dual WAN Enterprise Router'. The left sidebar contains navigation options: 系统监控, 接口设置, WAN设置 (selected), LAN设置, VLAN设置, DHCP设置, 安全专区, VPN, QoS设置, 高级设置, 设备管理, and 用户FAQ. The main content area is titled '设置WAN口参数' (Set WAN port parameters) and contains two identical sections for WAN口1 and WAN口2. Each section has a dropdown menu set to '动态地址 (从DHCP服务器自动获取)', an MTU field set to 1500, and fields for primary and secondary DNS servers and hostnames, all with '应用' (Apply) buttons.

1.2 接口设置—LAN设置—局域网设置。配置lan口的ip地址

The screenshot shows the configuration page for the H3C ER3260 router, specifically the '局域网设置' (Local Area Network Settings) section. The page title is 'H3C ER3260 Dual WAN Enterprise Router'. The left sidebar contains navigation options: 系统监控, 接口设置, WAN设置, LAN设置 (selected), VLAN设置, DHCP设置, 安全专区, VPN, QoS设置, 高级设置, 设备管理, and 用户FAQ. The main content area is titled 'LAN(VLAN1)设置' (LAN(VLAN1) Settings) and contains fields for IP address (172.16.1.1) and subnet mask (255.255.255.0). Below this is the 'MAC克隆' (MAC Cloning) section, with radio buttons for '使用设备MAC' (selected) and '手工输入MAC', and a field for the MAC address (00:0F:E2:70:6E:1C). An '应用' (Apply) button is at the bottom.

1.3 VPN—VPN设置—虚接口。配置虚接口绑定wan1口。

H3C ER3260 Dual WAN Enterprise Router

我的网络我做主

虚接口 **IKE安全提议** IKE对等体 IPsec安全提议 IPsec安全策略

系统监控
接口设置
安全专区
VPN
VPN设置
VPN状态
QoS设置
高级设置
设备管理
用户FAQ

虚接口

按关键字过滤: 名称 关键字:

操作	序号	名称	绑定接口	描述
	1	ipsec0	WAN1	

第 1 页/共 1 页 共 1 条记录 每页 10 行

1.4 VPN—VPN设置—IKE安全提议。

H3C ER3260 Dual WAN Enterprise Router

我的网络我做主

虚接口 **IKE安全提议** IKE对等体 IPsec安全提议 IPsec安全策略

系统监控
接口设置
安全专区
VPN
VPN设置
VPN状态
QoS设置
高级设置
设备管理
用户FAQ

安全提议

按关键字过滤: 名称 关键字:

操作	序号	名称	认证算法	加密算法	DH组
	1	msr30	SHA1	3DES	DH2 modp1024

第 1 页/共 1 页 共 1 条记录 每页 10 行

1.5 VPN—VPN设置—IKE对等体。

H3C ER3260 Dual WAN Enterprise Router

我的网络我做主

虚接口 IKE安全提议 **IKE对等体** IPsec安全提议 IPsec安全策略

系统监控
接口设置
安全专区
VPN
VPN设置
VPN状态
QoS设置
高级设置
设备管理
用户FAQ

对等体

按关键字过滤: 名称 关键字:

操作	序号	名称	虚接口	对端地址	模式	ID类型	安全提议	DPD
	1	30	ipsec0	180.168.139.202	野蛮模式	NAME	msr30	关闭

第 1 页/共 1 页 共 1 条记录 每页 10 行

1.6 VPN—VPN设置—IPsec安全提议

H3C ER3260 Dual WAN Enterprise Router

我的网络我做主

虚接口 IKE安全提议 IKE对等体 **IPsec安全提议** IPsec安全策略

系统监控
接口设置
安全专区
VPN
VPN设置
VPN状态
QoS设置
高级设置
设备管理
用户FAQ

安全提议

按关键字过滤: 名称 关键字:

操作	序号	名称	安全协议	AH算法	ESP算法
	1	30	ESP	----	3DES-SHA1

第 1 页/共 1 页 共 1 条记录 每页 10 行

1.7 VPN—VPN设置—IPsec安全策略

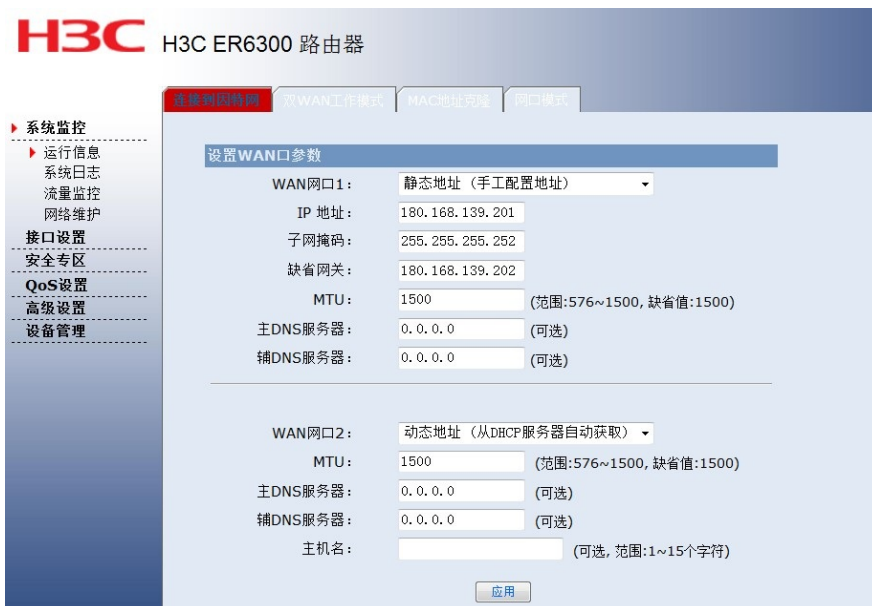


1.8 高级设置—路由设置—静态路由。设置一条指向虚接口的路由



2. ER6300的配置(NAT设置)

2.1 接口设置—wan设置—连接到因特网



2.2 接口设置—lan设置—局域网设置



3. MSR30的配置

3.1创建安全acl，匹配需要保护的数据流。

```
<H3C>sys
```

```
System View: return to User View with Ctrl+Z.
```

```
[H3C]acl number 3000
```

```
[H3C-acl-adv-3000]rule 1 per ip source 192.168.0.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
```

3.2建立ipsec提议30

```
[H3C-acl-adv-3000]ipsec prop 30
```

```
[H3C-ipsec-proposal-30]transform esp
```

```
[H3C-ipsec-proposal-30]esp encryption-algorithm 3des
```

```
[H3C-ipsec-proposal-30]esp authentication-algorithm sha1
```

```
[H3C-ipsec-proposal-30]quit
```

3.3配置ipsec安全策略，配置ike协商，绑定acl将策略应用到端口下。

```
[H3C]ipsec policy 30 10 is
```

```
[H3C-ipsec-policy-isakmp-30-10]security acl 3000
```

```
[H3C-ipsec-policy-isakmp-30-10]ike-peer 30
```

```
[H3C-ipsec-policy-isakmp-30-10]proposal 30
```

```
[H3C-ipsec-policy-isakmp-30-10]sa duration traffic-based 28800
```

```
[H3C-ipsec-policy-isakmp-30-10]int e5/0
```

```
[H3C-ipsec-policy-isakmp-30-10]quit
```

3.4建立ike提议

```
[H3C]ike proposal 30
```

```
[H3C-ike-proposal-30]encryption-algorithm 3des-cbc
```

```
[H3C-ike-proposal-30]authentication-method pre-share
```

```
[H3C-ike-proposal-30]authentication-algorithm sha
```

```
[H3C-ike-proposal-30]dh group2
```

```
[H3C-ike-proposal-30]sa duration 28800
```

```
[H3C-ike-proposal-30]quit
```

3.5配置ike对等体。

```
[H3C]ike peer 30
```

```
[H3C-ike-peer-30]exchange-mode agg
```

```
[H3C-ike-peer-30]pre-shared-key 123456
```

```
[H3C-ike-peer-30]id-type name
```

```
[H3C-ike-peer-30]remote-name 3260
```

```
[H3C-ike-peer-30]quit
```

```
[H3C]ike local-name 30
```

```
[H3C]ike peer 30
```

```
[H3C-ike-peer-30]nat traversal (nat穿越注意配置)
```

```
[H3C-ike-peer-30]ipsec policy 30 10 is
```

```
[H3C-Ethernet5/0]ipsec policy 30
```

```
[H3C-Ethernet5/0]ip add 180.168.139.202 24
```

```
[H3C-Ethernet5/0]int e5/1
```

```
[H3C-Ethernet5/1]ip add 191.168.0.1 24
```

```
[H3C-Ethernet5/1]quit
```

```
[H3C]ip route-static 0.0.0.0 0.0.0.0 180.168.139.201
```

4建立成功的日志

!	2000-01-01 00:50:41	Infor...	VPN	安全策略[30]: IPSEC SA建立完成 {ESP 出SPI=0xc10...
!	2000-01-01 00:50:41	Debug	VPN	安全策略[30]: 收到IPSEC_RESPONDER_LIFETIME消...
!	2000-01-01 00:50:41	Debug	VPN	安全策略[30]: 发起IPSEC SA协商。
!	2000-01-01 00:50:41	Debug	VPN	安全策略[30]:IPSEC SA 周期超时。
!	2000-01-01 00:00:46	Infor...	VPN	安全策略[30]: IPSEC SA建立完成 {ESP 出SPI=0x99...
!	2000-01-01 00:00:46	Debug	VPN	安全策略[30]: 收到IPSEC_RESPONDER_LIFETIME消...
!	2000-01-01 00:00:46	Debug	VPN	安全策略[30]: 发起IPSEC SA协商。
!	2000-01-01 00:00:46	Infor...	VPN	192.168.1.3<->180.168.139.202[30]: ISAKMP SA...
!	2000-01-01 00:00:45	Debug	VPN	192.168.1.3<->180.168.139.202[30]: 采用野蛮模...



H3C ER3260
Dual WAN Enterprise Router

我的网络我做主

系统监控

接口设置

安全专区

▶ VPN

▶ VPN设置

▶ VPN状态

QoS设置

高级设置

设备管理

用户FAQ

安全联盟

安全联盟SA

通过安全联盟SA，IPSec能够对不同的数据流提供不同级别的安全保护。在这里可以查询到相应隧道当前状态，了解隧道建立的各个参数。

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
30	out	192.168.1.3 =>180.168.139.202	----	----	0x99993b22	3DES_SHA1	172.16.1.0/24 =>192.168.0.0/24
30	in	180.168.139.202 =>192.168.1.3	----	----	0xa3295e7	3DES_SHA1	192.168.0.0/24 =>172.16.1.0/24

第 1 页 / 共 1 页 共 2 条记录 每页 10 行

[刷新](#)

经验证，通过该配置案例完全满足该公司客户需求，实现MSR路由器和ER3260路由器通过野蛮模式ipsec VPN穿越nat功能。