```
Cisco1751(config-isakmp-group)#pool dynpool
Cisco1751(config)#crypto isakmp client configuration address-pool local dynpool !---指定在组配置中要推送的本地地址池名为 dynpool
Cisco1751(config)#ip local pool dynpool 30.30.30.20 30.30.30.30  !---配置用于为 Easy VPN 客户端推送的内部全局 IP 地址池
```

（5）应用模式配置和 Xauth 认证。

```
Cisco1751(config)#crypto map dynmap client authentication list userlist
Cisco1751(config)#crypto map dynmap isakmp authorization list hw-client-groupname
Cisco1751(config)#crypto map dynmap client configuration address respond
Cisco1751(config)#crypto map dynmap 1 ipsec-isakmp dynamic dynmap
Cisco1751(config)#interface Ethernet0/0
Cisco1751(config-if)#description connected to INTERNET
Cisco1751(config-if)#ip address 20.20.20.2 255.255.255.0
Cisco1751(config-if)#half-duplex
Cisco1751(config-if)#no cdp enable
Cisco1751(config-if)#crypto map dynmap  !---应用前面在 IKE 策略中创建的名为 dynmap 的动态加密映射
Cisco1751(config-if)#exit
Cisco1751(config)#interface FastEthernet0/0
Cisco1751(config-if)#description connected to HQ LAN
Cisco1751(config-if)#ip address 30.30.30.1 255.255.255.0
Cisco1751(config-if)#speed auto
Cisco1751(config-if)#no cdp enable
Cisco1751(config-if)#exit
```

同样可以通过命令查看 Easy VPN 服务器端的 IPSec SA 协商所用的配置。总体上与在 Easy VPN 远端查看的 IPSec SA 协商配置差不多。

```
Cisco1751#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: dynmap, local addr. 20.20.20.2
protected vrf:
local ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (30.30.30.20/255.255.255.255/0/0)
current_peer: 20.20.20.1:500
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 13, #pkts decrypt: 13, #pkts verify 13
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 20.20.20.2, remote crypto endpt.: 20.20.20.1
path mtu 1500, media mtu 1500
current outbound spi: 239C766E
inbound esp sas:
spi: 0xE89E6649(3902694985)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: dynmap
sa timing: remaining key lifetime (k/sec): (4458452/3335)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x239C766E(597456494)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: dynmap
sa timing: remaining key lifetime (k/sec): (4458454/3335)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

可以使用 **show crypto engine connections active** 命令显示加密引擎活动的连接汇总。最前面的数字是指对应的连接 ID。

```
Cisco1751#show crypto engine connections active
ID Interface IP-Address State Algorithm Encrypt Decrypt
1 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 0
200 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 538
201 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 133 0
```

15.8.4　Cisco VPN 客户端 PC 的 Easy VPN 配置示例

本示例拓扑结构如图 15-16 所示，Cisco 1751 路由器作为 Easy VPN 服务器，Cisco VPN 客户端是使用 Cisco VPN Client 软件 PC 机。Easy VPN 服务器的 WAN 接口采用静态公网 IP 地址，PC 机的 WAN 接口可以是静态或者动态 WAN 接入，即可以是动态或静态公网 IP 地址。同样，Cisco VPN 客户端 PC 机工作在 Client 模式，采用 NAT 或者 PAT 进行 IP 地址转换，其内部全局 IP 地址是 Easy VPN 服务器推送得到。

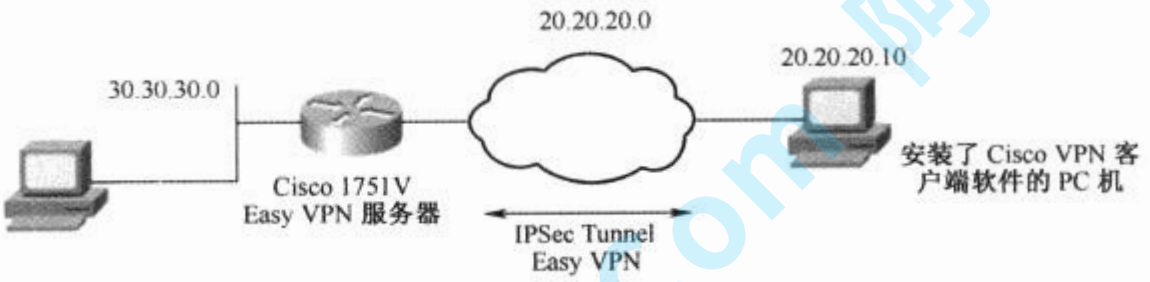

图 15-16　Cisco VPN 客户端 PC 的 Easy VPN 配置示例拓扑结构

本示例中 Easy VPN 客户端仅是安装好 Cisco VPN Client 软件的 PC 机，所以无需额外的配置，仅需在打开的界面中输入 Easy VPN 服务器的 WAN 接口 IP 地址即可进行 Easy VPN 连接。本示例的关键是担当 Easy VPN 服务器的 Cisco 1751 路由器配置。具体如下：

（1）基本全局配置。

```
Router(config)#hostname Cisco1751
Cisco1751(config)#ip subnet-zero
Cisco1751(config)#no ip source-route
Cisco1751(config)#ip domain-name cisco.com
Cisco1751(config)#ip classless
Cisco1751(config)#ip route 0.0.0.0 0.0.0.0 Ethernet0/0
Cisco1751(config)#no ip http server
Cisco1751(config)#ip pim bidir-enable
Cisco1751(config)#no cdp run
Cisco1751(config)#line vty 0 4
Cisco1751(config-line)#password cisco
Cisco1751(config-line)#login
```

（2）启用 AAA 策略查找。

```
Cisco1751(config)#aaa new-model
Cisco1751(config)#aaa authorization network hw-client-groupname local
Cisco1751(config)#aaa session-id common
Cisco1751(config)#enable password cisco
```

（3）创建 IKE 策略。

```
Cisco1751(config)#crypto isakmp policy 1
Cisco1751(config-isakmp)# encryption 3des
Cisco1751(config-isakmp)#authentication pre-share
Cisco1751(config-isakmp)#group 2
Cisco1751(config-isakmp)#exit
Cisco1751(config)#crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
```

```
Cisco1751(config-crypto-tran)#exit
Cisco1751(config)#crypto dynamic-map dynmap 1
Cisco1751(config-crypto-map)#set transform-set transform-1
Cisco1751(config-crypto-map)#reverse-route
Cisco1751(config-crypto-map)#exit
```

（4）配置模式配置组策略信息。

```
Cisco1751(config)#crypto isakmp client configuration group hw-client-groupname
Cisco1751(config-isakmp-group)#key hw-client-password
Cisco1751(config-isakmp-group)#dns 30.30.30.10 30.30.30.11
Cisco1751(config-isakmp-group)#wins 30.30.30.12 30.30.30.13
Cisco1751(config-isakmp-group)#domain cisco.com
Cisco1751(config-isakmp-group)#pool dynpool
Cisco1751(config)#crypto isakmp client configuration address-pool local dynpool
Cisco1751(config)#ip local pool dynpool 30.30.30.20 30.30.30.30
```

（5）应用模式配置和 Xauth 认证。

```
Cisco1751(config)#crypto map dynmap isakmp authorization list hw-client-groupname
Cisco1751(config)#crypto map dynmap client configuration address respond
Cisco1751(config)#crypto map dynmap 1 ipsec-isakmp dynamic dynmap
Cisco1751(config)#interface Ethernet0/0
Cisco1751(config-if)#description connected to INTERNET
Cisco1751(config-if)#ip address 20.20.20.2 255.255.255.0
Cisco1751(config-if)#half-duplex
Cisco1751(config-if)#no cdp enable
Cisco1751(config-if)#crypto map dynmap
Cisco1751(config-if)#exit
Cisco1751(config)#interface FastEthernet0/0
Cisco1751(config-if)#description connected to HQ LAN
Cisco1751(config-if)#ip address 30.30.30.1 255.255.255.0
Cisco1751(config-if)#speed auto
Cisco1751(config-if)#no cdp enable
Cisco1751(config-if)#end
```

在 Cisco 1751 路由器上执行 **show crypto ipsec sa** 命令可以查看本示例中用于 IPSec SA 协商的详细配置信息。

```
Cisco1751#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: dynmap, local addr. 20.20.20.2
protected vrf:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (30.30.30.20/255.255.255.255/0/0)
current_peer: 20.20.20.10:500
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 260, #pkts decrypt: 260, #pkts verify 260
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 20.20.20.2, remote crypto endpt.: 20.20.20.10
path mtu 1500, media mtu 1500
current outbound spi: C1E4231E
inbound esp sas:
spi: 0xEC89E882(3968460930)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 202, flow_id: 3, crypto map: dynmap
sa timing: remaining key lifetime (k/sec): (4511772/3455)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
```

```
inbound pcp sas:
outbound esp sas:
spi: 0xC1E4231E(3252953886)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 203, flow_id: 4, crypto map: dynmap
sa timing: remaining key lifetime (k/sec): (4511804/3455)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
protected vrf:
local ident (addr/mask/prot/port): (20.20.20.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (30.30.30.20/255.255.255.255/0/0)
current_peer: 20.20.20.10:500
PERMIT, flags={}
#pkts encaps: 50, #pkts encrypt: 50, #pkts digest 50
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 20.20.20.2, remote crypto endpt.: 20.20.20.10
path mtu 1500, media mtu 1500
current outbound spi: 86EA4824
inbound esp sas:
spi: 0x28231BBA(673389498)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: dynmap
sa timing: remaining key lifetime (k/sec): (4462296/3451)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x86EA4824(2263500836)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: dynmap
sa timing: remaining key lifetime (k/sec): (4462290/3450)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

同样可用 **show crypto engine connections active** 命令查看当前活跃的加密引擎连接。

```
Cisco1751#show crypto engine connections active
ID Interface IP-Address State Algorithm Encrypt Decrypt
1 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 0
200 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 0
201 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 134 0
202 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 770
203 Ethernet0/0 20.20.20.2 set HMAC_SHA+3DES_56_C 0 0
```