

Split Tunnel Cisco IPsec VPN Gateway with Software Client

Michael J. Martin

The VPN gateway configuration above supports a split-tunneling traffic model in which only traffic to the secured networks is encrypted and all other traffic is forwarded unsecured. Many security professionals consider this model to be less secure than a "full-crypto" model. That's because when users are connected to the gateway, they are connected to two networks simultaneously. So there is a potential that any virus or security breach that originates from the unsecured network could breach the secured network through the connected host. Security concerns aside, this is a very popular model for most VPN gateway implementations. It secures the traffic that needs to be and does not require that the gateway have the bandwidth or take on the overhead of processing all of the connected users' traffic.

Split-tunnel (Old School) VPN Gateway Configuration

The configuration below will secure network communications between the VPN client pool address space 172.30.55.32/28 and the hosts and servers connected to the 172.30.40.0/24, 172.30.80.0/24 and 172.30.60.0/24 LAN subnets. The VPN gateway configuration is comprised of two parts: ISAKMP and crypto map configuration. Here are the steps:

ISAKMP Configuration

1. Create ISAKMP policy:

```
Create policy entries
Define Phase 1 encryption
Define Phase 1 hash
Define Phase 1 authentication
Define DH exchange key size

outlan-rt05(config)#crypto isakmp policy 10
outlan-rt05(config-isakmp)# encryption 3des
outlan-rt05(config-isakmp)# hash md5
outlan-rt05(config-isakmp)# authentication pre-share
outlan-rt05(config-isakmp)# group 2
outlan-rt05(config-isakmp)#exit
```

2. Configure AAA user and group authentication and accounting:

```
Enable AAA new model
Define VPN XAUTH user authentication
Define VPN XAUTH group authentication
Define VPN XAUTH group authorization
Create local accounts

outlan-rt05(config)#aaa new-model
outlan-rt05(config)#aaa authentication login default local
outlan-rt05(config)#aaa authentication login userauth local
outlan-rt05(config)#aaa authorization network groupauth local
outlan-rt05(config)#username root password root
```

Split Tunnel Cisco IPsec VPN Gateway with Software Client

Michael J. Martin

3. Create IP address pool:

```
outlan-rt05(config)# ip local pool OS-VPN 172.30.90.2 172.30.90.14
```

4. Create loopback interface associated with the address pool:

```
outlan-rt05(config)#interface loopback 90
outlan-rt05(config-if)#ip address 172.30.90.1 255.255.255.240
```

5. Create split-tunneling ACL:

```
outlan-rt05(config)# access-list 100 permit 172.30.40.0 0.0.0.255 172.30.90.0
0.0.0.15
```

```
outlan-rt05(config)# access-list 100 permit 172.30.80.0 0.0.0.255 172.30.90.0
0.0.0.15
```

```
outlan-rt05(config)# access-list 100 permit 172.30.60.0 0.0.0.255 172.30.90.0
0.0.0.15
```

6. Create client configuration group:

```
Define group name
Group key
DNS server
Netmask
ACL
Maximum logins
Maximum users
Address pool
Enable client to save XAUTH password
Connection banner
```

```
outlan-rt05(config)#crypto isakmp client configuration group Old-School
outlan-rt05(config-isakmp-group)# key secretkey
outlan-rt05(config-isakmp-group)#dns 172.30.40.2
outlan-rt05(config-isakmp-group)#netmask 255.255.255.240
outlan-rt05(config-isakmp-group)#backup-gateway 45.224.90.17
outlan-rt05(config-isakmp-group)#domain outlan.net
outlan-rt05(config-isakmp-group)#acl 100
outlan-rt05(config-isakmp-group)#max-login 1
outlan-rt05(config-isakmp-group)#max-users 13
outlan-rt05(config-isakmp-group)#pool OS-VPN
outlan-rt05(config-isakmp-group)#save-password
outlan-rt05(config-isakmp-group)#banner ^
```

Split Tunnel Cisco IPsec VPN Gateway with Software Client

Michael J. Martin

Enter TEXT message. End with the character '^'.

You are connected to outlan.net. All transactions are monitored.

^

```
outlan-rt05(config-isakmp-group)#
```

7. **Configure Compound TCP (CTCP) port definitions (and disable http and https services on the router):**

```
outlan-rt05(config)#crypto ctcp port 443 10000
```

```
outlan-rt05(config)#no ip http server
```

```
outlan-rt05(config)#no ip http secure-server
```

8. **Configure NAT transparency keepalive:**

```
outlan-rt05(config)#crypto isakmp nat keepalive 20
```

Crypto Map Configuration

1. **Create transform set:**

Define Phase 2 encryption

Define Phase 2 hash

Enable IP compression

```
outlan-rt05(config)# crypto transform-set 3DES-MD5-LZS esp-3des esp-  
md5-hmac comp-lzs
```

2. **Create dynamic crypto map:**

Define transform set

Define client route handling

```
outlan-rt05(config)#crypto dynamic-map OLD-SCHOOL 10
```

```
outlan-rt05(config-crypto-map)# set transform-set 3DES-MD5-LZS
```

```
outlan-rt05(config-crypto-map)# reverse-route
```

3. **Create static crypto map:**

Create static crypto map with authentication and dynamic crypto map reference

Define VPN client authentication list

Define client ISAKMP authorization list

Define VPN client IP address configuration

```
outlan-rt05(config)#crypto map SW-Client 10 ipsec-isakmp dynamic OLD-SCHOOL
```

```
outlan-rt05(config)#crypto map SW-Client client authentication list userauth
```

```
outlan-rt05(config)#crypto map SW-Client isakmp authorization list groupauth
```

```
outlan-rt05(config)#crypto map SW-Client client configuration address respond
```

Split Tunnel Cisco IPsec VPN Gateway with Software Client

Michael J. Martin

4. Create interface access ACL:

```
outlan-rt05(config)#access-list 101 permit tcp any host 172.30.80.45 eq 22
outlan-rt05(config)#access-list 101 permit tcp any host 172.30.80.45 eq 23
outlan-rt05(config)#access-list 101 permit tcp any host 172.30.80.45 eq telnet
outlan-rt05(config)#access-list 101 permit tcp any host 172.30.80.45 eq 443
outlan-rt05(config)#access-list 101 permit tcp any host 172.30.80.45 eq 10000

outlan-rt05(config)#access-list 101 permit tcp any host 172.30.80.45
established
```

5. Install crypto map:

Apply map to "unsecured" router interface
Install VPN access ACL
Configure IP routing

```
outlan-rt05(config)#interface FastEthernet0/0
outlan-rt05(config-if)#crypto map SW-Client
outlan-rt05(config-if)#ip access-group 101 in
outlan-rt05(config-if)#exit
outlan-rt05(config)#ip route 0.0.0.0 0.0.0.0 63.240.22.2
outlan-rt05(config)#ip route 172.30.80.0 0.0.0.255 172.30.40.33
outlan-rt05(config)#ip route 172.30.60.0 0.0.0.255 172.30.40.33
```

Create VPN Client Policy

With the VPN gateway completed, the last step is to create the VPN client policy. The Cisco VPN client software comes with all VPN licensed routers and with standalone hardware crypto modules (VAM and AIM hardware adapters). The software can also be downloaded from www.cisco.com. The client is available for Windows, Mac OS, and Linux. The Windows and Mac OS version has a GUI interface. There are two ways to build the profile. The first is to build a base configuration text file with the core connection variables defined, and then import the file into the client. Here is the profile for the Old School VPN gateway we configured above:

```
[main]
Host=63.240.22.2
AuthType=1
GroupName=Old-School
GroupPwd=secretkey
TunnelingMode=1
TcpTunnelingPort=443
```

To import the configuration, you launch the client GUI and click the "import" button. Once you connect to the VPN gateway, the client application will add the remaining client variables, including the group password in encrypted form.

Split Tunnel Cisco IPsec VPN Gateway with Software Client

Michael J. Martin

VPN Client | Create New VPN Connection Entry

Connection Entry: Old-School-VPN

Description:

Host: 63.240.22.2

Authentication Transport Backup Servers

Group Authentication Mutual Group Authentication

Name: Old-School

Password: *****

Confirm Password: *****

Certificate Authentication

Name: [Dropdown]

Send CA Certificate Chain

Erase User Password Save Cancel

The other approach is to build the profile for the client profile using the GUI. The build process begins by clicking the "New" button, which opens a profile configuration window:

When building the profile through the GUI, you need the following data points:

- VPN gateway IP address
- The ISAKMP client configuration group name
- The ISAKMP client configuration group key

Once the VPN gateway address and group authentication data has been configured, the "Transport" tab is next.

Split Tunnel Cisco IPsec VPN Gateway with Software Client

Michael J. Martin

VPN Client | Create New VPN Connection Entry

Connection Entry: Old-School-VPN

Description:

Host: 63.240.22.2

Authentication | Transport | Backup Servers

Enable Transparent Tunneling

IPSec over UDP (NAT / PAT)

IPSec over TCP TCP Port: 443

Allow Local LAN Access

Peer response timeout (seconds): 90

Erase User Password Save Cancel

The transport section provides the configuration interface for the CTCP or NAT traversal options for the client. The split-tunnel VPN configuration supports both NAT-T and CTCP, but only one tunneling option can be set for a profile. In the example above, the profile is configured to support CTCP listening on port 443. The last configuration step is to provision a backup VPN gateway by checking the "Enable Backup Servers" function on the "Backup Servers" tab.

Implementing a backup VPN gateway is a good idea if you're implementing a critical access service. If the backup server is defined as part of the ISAKMP group configuration, it will be pushed down to the VPN client profile when the initial connection is established. Alternatively, it can be configured as part of the VPN client profile build.