

Full Crypto Cisco IPsec VPN Gateway With Software Client

Michael J. Martin

As with all full-crypto configurations, all of the traffic sent from the remote node is encrypted until it reaches the VPN gateway's inside interface. The gateway then sends the secured (now unencrypted) traffic on to the next local hop (172.30.40.33). In this case, we'll use the same networks we used in the "Old School" implementation: 172.30.40.0/24, 172.30.80.0/24 and 172.30.60.0/24. All other traffic is sent to the internal firewall interface. The firewall then processes the VPN client's external network requests in accordance with its policy rule base.

Getting all of this traffic to the right place does take a little effort. In order to support VPN client connections from non-explicitly defined networks, the VPN gateway's default route must point to the gateway router's DMZ interface (63.240.22.0.1). All of the secured networks must be explicitly defined and use the RS's 172.30.40.0/24 network interface (172.30.40.33) as the next hop. To get Internet traffic to the firewall's internal interface (172.30.40.1), we implement a route map that inspects the traffic and then forwards it to the appropriate gateway based on a traffic qualifier ACL. Much the same way the router decides what traffic to encrypt, it inspects the traffic against the ACL, and then processes it accordingly.

Now that we've overcome the secured traffic vs. Internet traffic processing issues associated with a full-crypto implementation on IOS routers, we can get to the New School VPN configuration. The difference between the New and Old School VPN configurations is largely the addition of the ISAKMP profile. In the Old School configuration, the VPN client authentication, authorization and IP address processing is configured as part of the static crypto map configuration.

In a single-client solution (where the user community all operates with a single network access, ISAKMP, and AAA policy), this does not present any limitation whatsoever. In a multi-client environment, where different AAA and network access policies need to be implemented, the Old School approach falls short. The ISAKMP profile offers the ability to build different ISAKMP profiles to be used in conjunction with different ISAKMP client configuration groups and, by extension, different dynamic crypto maps and/or map sequence entries.

To illustrate the difference, we will re-build split-tunneling and full-crypto VPN solutions using the New School approach. Like the Old-School approach, the VPN gateway configuration is comprised of two parts: the ISAKMP and crypto map configuration.

ISAKMP Configuration

1. Create ISAKMP policy: This configuration implements the ISAKMP Phase 1 policy, supporting both the default DES/SHA/DH-1 and the more secure, standard 3DES/MD5/DH-2 with support for pre-shared keys:

```
outlan-rt05(config)#crypto isakmp policy 10
outlan-rt05(config-isakmp)#encr 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
outlan-rt05(config)#crypto isakmp policy 20
outlan-rt05(config-isakmp)#hash sha
outlan-rt05(config-isakmp)#encryption des
```

Full Crypto Cisco IPsec VPN Gateway With Software Client

Michael J. Martin

```
outlan-rt05(config-isakmp)#authentication pre-share
outlan-rt05(config-isakmp)#group 1
```

2. Configure AAA user and group authentication, authorization, and accounting: The split-tunnel policy will use local sourced user authentication and group authorization. The full-crypto policy utilizes TACACS for user authentication and local sourced group authorization:

```
outlan-rt05(config)#aaa authentication login local-user-auth local
outlan-rt05(config)#aaa authorization network local-group-authz local
outlan-rt05(config)#aaa authentication login aaa-auth group tacacs+
outlan-rt05(config)#tacacs-server host 172.30.40.6
outlan-rt05(config)#tacacs-server key secretkey
```

3. Create IP address pools for both policies:

```
outlan-rt05(config)#ip local pool OS-VPN 172.30.90.2 172.30.90.14
outlan-rt05(config)#ip local pool FC-VPN 5.0.0.2 5.0.0.254
```

4. Create loopback interface associated with the address pool:

```
outlan-rt05(config)#interface loopback 90
outlan-rt05(config-if)#ip address 172.30.90.1 255.255.255.2
outlan-rt05(config-if)#exit
outlan-rt05(config)#interface loopback 5
outlan-rt05(config-if)#ip address 5.0.0.1 255.255.255.0
outlan-rt05(config-if)#exit
outlan-rt05(config)#
```

5. Create split-tunneling ACL:

```
outlan-rt05(config)#ip access-list extended SPLIT-TUNNEL
outlan-rt05(config-ext-nacl)#permit ip 172.30.40.0 0.0.0.255 172.30.90.0
0.0.0.15
outlan-rt05(config-ext-nacl)#permit ip 172.30.80.0 0.0.0.255 172.30.90.0
0.0.0.15
outlan-rt05(config-ext-nacl)#permit ip 172.30.60.0 0.0.0.255 172.30.90.0
0.0.0.15
outlan-rt05(config-ext-nacl)#exit
outlan-rt05(config)#
```

6. Create client configuration group(s): Separate ISAKMP groups for the split-tunnel and full-crypto policies must be created.

```
outlan-rt05(config)#crypto isakmp client configuration group split-tunnel
outlan-rt05(config-isakmp-group)#key secretkey
outlan-rt05(config-isakmp-group)#dns 172.30.40.2
outlan-rt05(config-isakmp-group)#domain outlan.net
outlan-rt05(config-isakmp-group)#pool OS-VPN
outlan-rt05(config-isakmp-group)#acl SPLIT-TUNNEL
```

Full Crypto Cisco IPsec VPN Gateway With Software Client

Michael J. Martin

```
outlan-rt05(config-isakmp-group)#max-logins 2
outlan-rt05(config-isakmp-group)#max-users 13
outlan-rt05(config-isakmp-group)#save-password
outlan-rt05(config-isakmp-group)#banner ^
Enter TEXT message. End with the character '^'.
You are connected to OUTLAN. All outlan traffic is secured.
^
outlan-rt05(config-isakmp-group)#exit
outlan-rt05(config)# crypto isakmp client configuration group full-crypto
outlan-rt05(config-isakmp-group)#key secretkey
outlan-rt05(config-isakmp-group)#dns 172.30.40.2
outlan-rt05(config-isakmp-group)#domain outlan.net
outlan-rt05(config-isakmp-group)#pool FC-VPN
outlan-rt05(config-isakmp-group)#save-password
outlan-rt05(config-isakmp-group)#include-local-lan
outlan-rt05(config-isakmp-group)#pfs
outlan-rt05(config-isakmp-group)#max-users 253
outlan-rt05(config-isakmp-group)#max-logins 1
outlan-rt05(config-isakmp-group)#banner ^
Enter TEXT message. End with the character '^'.
This is a full crypto VPN connection.
^
outlan-rt05(config-isakmp-group)#exit
```

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

8. Configure NAT transparency keepalive: NAT transparency is enabled by default, but you need to set a keepalive. However, if you only want to use CTCP you can disable NAT traversal:

```
outlan-rt05(config)#crypto isakmp nat keepalive 20
outlan-rt05(config)#no crypto ipsec nat-transparency udp-encaps
```

Configure ISAKMP profile: The ISAKMP profile is what makes this the New School configuration. Notice that the ISAKMP group name and ISAKMP policy names are the same. This is not a requirement, but it makes it easier to keep track if you have a number of different groups and profiles:

```
outlan-rt05(config)#crypto isakmp profile split-tunnel
% A profile is deemed incomplete until it has match identity statements
outlan-rt05(conf-isa-prof)#description ISAKMP for Split Tunneling Cisco Soft Clients
outlan-rt05(conf-isa-prof)#match identity group split-tunnel
outlan-rt05(conf-isa-prof)#client authentication list local-user-auth
outlan-rt05(conf-isa-prof)#isakmp authorization list local-group-authz
outlan-rt05(conf-isa-prof)#client configuration address respond
outlan-rt05(conf-isa-prof)#keepalive 20 retry 10
outlan-rt05(conf-isa-prof)#exit
```

Full Crypto Cisco IPsec VPN Gateway With Software Client

Michael J. Martin

```
outlan-rt05(config)#
outlan-rt05(config)# crypto isakmp profile full-crypto
% A profile is deemed incomplete until it has match identity statements
outlan-rt05(conf-isa-prof)#description ISAKMP for Full Crypto Cisco Soft Clients
outlan-rt05(conf-isa-prof)#match identity group full-crypto
outlan-rt05(conf-isa-prof)#client authentication list aaa-auth
outlan-rt05(conf-isa-prof)#isakmp authorization list local-group-authz
outlan-rt05(conf-isa-prof)#client configuration address respond
outlan-rt05(conf-isa-prof)#keepalive 20 retry 10
outlan-rt05(conf-isa-prof)#exit
outlan-rt05(config)#
```

Crypto Map Configuration

With the ISAKMP groups and profiles defined, we move onto the (far simpler) New School crypto map configuration.

1. Create transform set: Because we are supporting only the Cisco VPN software client we really only need one Phase 2 policy:

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

2. Create dynamic crypto map: Because we are supporting two different VPN policies, we have some options for implementing the dynamic crypto map. We can either implement two different maps or a single map with two sequences. Here is a single map example with two sequence entries:

```
outlan-rt05(config)#crypto dynamic-map Software-Client 10
outlan-rt05(config-crypto-map)#set security-association lifetime seconds 12000
outlan-rt05(config-crypto-map)#set transform-set 3DES-MD5-Z
outlan-rt05(config-crypto-map)#set isakmp-profile split-tunnel
outlan-rt05(config-crypto-map)#reverse-route
outlan-rt05(config-crypto-map)#exit
outlan-rt05(config-crypto-map)#crypto dynamic-map Software-Client 20
outlan-rt05(config-crypto-map)#set transform-set 3DES-MD5-Z
outlan-rt05(config-crypto-map)#set pfs group2
outlan-rt05(config-crypto-map)#set isakmp-profile full-crypto
outlan-rt05(config-crypto-map)#reverse-route
outlan-rt05(config-crypto-map)#exit
```

3. Create static crypto map:

```
outlan-rt05(config)#crypto map outlan-ipsec-gw05 10 ipsec-isakmp dynamic
Software-Client
```

4. Install the static crypto map: Once the crypto map is installed, it can support client connections. However, in order to support full crypto unsecured traffic handling, we need to implement policy routing:

Full Crypto Cisco IPsec VPN Gateway With Software Client

Michael J. Martin

```
outlan-rt05(config)#int fastEthernet 0/0
outlan-rt05(config-if)#crypto map outlan-ipsec-gw05
*Dec  8 04:32:00.479: %CRYPTO-6-ISA_KMP_ON_OFF: ISA_KMP is ON
outlan-rt05(config-if)#exit
```

5. Install the routing policy: As we reviewed above, in order handle off-network traffic, we need the router to ignore its default route when handling certain types of traffic. This trick is accomplished with the creation of a traffic-match ACL coupled with a simple route map that directs the matched traffic to another gateway:

```
outlan-rt05(config)#ip access-list extended redirect
outlan-rt05(config-ext-nacl)#permit tcp 5.0.0.0 0.0.0.255 any eq 80
outlan-rt05(config-ext-nacl)#permit tcp 5.0.0.0 0.0.0.255 any eq 443
outlan-rt05(config-ext-nacl)#permit tcp 5.0.0.0 0.0.0.255 any eq ftp
outlan-rt05(config)# route-map int-acc permit 10
outlan-rt05(config-route-map)#match ip address redirect
outlan-rt05(config-route-map)#set ip next-hop 172.30.40.1
outlan-rt05(config)#interface FastEthernet0/1
outlan-rt05(config-if)#ip policy route-map int-acc
outlan-rt05(config-if)#exit
outlan-rt05(config)#
```

The multi-policy VPN gateway is now configured. As for client profile configuration, an administrator would create a separate client profile for each ISA_KMP group. Below are the starter files for the split-tunnel and the full-crypto topologies.

```
[main]
Description= New_School_ST
Host=63.240.22.2
AuthType=1
GroupName=split-tunnel
GroupPwd=secretkey
TunnelingMode=1
TcpTunnelingPort=10000
```

```
[main]
Description=New_School_FC
Host=63.240.22.2
AuthType=1
GroupName=full-crypto
GroupPwd=secretkey
TunnelingMode=1
TcpTunnelingPort=443
```