

Full Crypto VPN Hardware Client Configuration for Cisco EzVPN

Michael J. Martin

In the last article in our series on building router-based VPN gateways, we learned how to support network-to-network IPsec VPN topologies by building a gateway with Cisco EzVPN. Now we'll move on to the hardware client configuration that will support a full-crypto peering relationship for the EzVPN gateway.

The typical hardware client device build has four configuration elements: the DHCP/DNS server configuration, the hardware client configuration, the interface configuration, and the IP routing configuration.

Unlike other IOS IPsec configurations, the hardware client requires no ISAKMP policy, transform set or crypto map definition. Only the client configuration is needed to establish the IPsec link with the gateway. Hardware client configurations utilize "built-in" ISAKMP and transform set definitions. EzVPN supports 20 different ISAKMP policies utilizing AES, DES, 3DES for encryption and SHA and MD5 for authentication, but only supports Diffie-Hellman Group 2 (1024-bit) key lengths. This gives administrators flexibility in terms of encryption and authentication, but DH Group 2 must be used or ISAKMP Phase 1 negotiation will fail.

Transform set support also offers diverse authentication and encryption selection, with minor restrictions. This translates to only transform sets that support ESP with encryption and authentication being available. That means there is no AH support, and no transform sets using ESP with encryption and without authentication, or ESP with authentication and without encryption can be configured on the VPN gateway, at least if you expect to have a successful Phase 2 negotiations. The VPN gateway configuration in the previous article takes these rules into account, but a number of other ISAKMP and transform set configurations can be implemented and supported by the hardware client. Now on to the client configuration:

DHCP/DNS Services Configuration

With an EZ-NEM remote office configuration, the router (or the LAN routing switch) is typically configured to provide DHCP and DNS services. Alternatively a local server could be configured to provide these services. But the idea with this type of solution is to consolidate services to make support and replacement (if needed) easy. Here is the basic configuration for two directly connected networks' DHCP scopes and DNS proxy services with the core DNS server (172.30.40.101) and four Internet root DNS server definitions:

```
outlan-VPN-RTR(config)#ip dhcp pool vlan-100
outlan-VPN-RTR(dhcp-config)#network 172.30.100.0 255.255.255.0
outlan-VPN-RTR(dhcp-config)#default-router 172.30.100.1
outlan-VPN-RTR(dhcp-config)#dns-server 1.1.1.1
outlan-VPN-RTR(dhcp-config)#domain-name usr.outlan.net
outlan-VPN-RTR(dhcp-config)#exit
outlan-VPN-RTR(config)#ip dhcp excluded-address 172.30.100.1
outlan-VPN-RTR(config)#ip dhcp pool vlan-120
outlan-VPN-RTR(dhcp-config)#network 172.30.120.0 255.255.255.0
outlan-VPN-RTR(dhcp-config)#default-router 172.30.100.1
outlan-VPN-RTR(dhcp-config)#dns-server 1.1.1.1
outlan-VPN-RTR(dhcp-config)#domain-name usr.outlan.net
```

Full Crypto VPN Hardware Client Configuration for Cisco EzVPN

Michael J. Martin

```
outlan-VPN-RTR(dhcp-config)#exit
outlan-VPN-RTR(config)# ip dhcp excluded-address 172.30.120.1

outlan-VPN-RTR(config)#ip domain-name outlan.net
outlan-VPN-RTR(config)#ip dns server
outlan-VPN-RTR(config)#ip name-server 172.30.40.101
outlan-VPN-RTR(config)#ip name-server 192.36.148.17
outlan-VPN-RTR(config)#ip name-server 192.112.36.4
outlan-VPN-RTR(config)#ip name-server 193.0.14.129
outlan-VPN-RTR(config)#ip name-server 198.32.64.12
```

Hardware Client Configuration

The hardware client definition follows a format quite similar to the software client definition. The basic client definition requires the following attributes:

- EzVPN client connection definition name is set with the command <crypto ipsec client ezvpn {client name}>
- ISAKMP group authentication is set with the command <group {group-name} key {key string}>
- Connection mode definition, for full-time remote location connections, is set with the command <connect {auto | manual | acl {acl}}>
- Client mode definition is set with the command <mode {client network-extension}>
- Host (peer) definition allows multiple definitions to be defined. The client connects to the peers in descending order and is set with the command <peer {ip address | hostname}>
- XAUTH user and password definition is set with the command <username {name} password {passwd}>
- XAUTH authentication trigger definition sets up the authentication process. Once the connection has been triggered, the XAUTH credentials need to be sent. This is set with the command <xauth userid mode {interactive | http-intercept | local}>

Below is a syntax example detailing the hardware client connection definition configuration:

```
outlan-VPN-RTR(config)#crypto ipsec client ezvpn hard-client
outlan-VPN-RTR(config-crypto-ezvpn)#connect auto
outlan-VPN-RTR(config-crypto-ezvpn)#group hard-client-fc key supersecret
outlan-VPN-RTR(config-crypto-ezvpn)#username outlan-rtr1 password outlan-rtr1
outlan-VPN-RTR(config-crypto-ezvpn)#xauth userid mode local
outlan-VPN-RTR(config-crypto-ezvpn)#mode network-extension
outlan-VPN-RTR(config-crypto-ezvpn)#peer 190.55.2.98
outlan-VPN-RTR(config-crypto-ezvpn)#peer 45.240.90.194
```

Full Crypto VPN Hardware Client Configuration for Cisco EzVPN

Michael J. Martin

Traffic qualifier ACL is an optional client definition for use in scenarios in which the hardware client router does not have directly connected interfaces on all of the IP subnets that must be secured. The client hardware has a provision for including such subnets using a traffic qualifier ACL. The ACL follows the same format that a "gateway" traffic ACL uses: Local Network -> Remote Network (any), where the local networks are those adjacent to the hardware client router and the remote networks are reachable through the VPN gateway. Here is the ACL for our example network:

```
outlan-VPN-RTR(config)#access-list 140 permit ip 172.30.89.0 0.0.0.255 any
outlan-VPN-RTR(config)#access-list 140 permit ip 172.30.62.0 0.0.0.255 any
```

Once the ACL is defined, it is referenced within the client definition using client configuration sub-command <acl {acl name}>.

Interface Creation and Designation

With the hardware client profile definition in place, next we must configure the interface addressing and local subnet crypto client designations. Like NAT, the hardware client interface configuration uses "inside" and "outside" designations. There can be only one outside interface and there must be at least one inside interface in order for the policy to be enabled:

```
outlan-VPN-RTR(config)#ip access-list extended VPN-IN
outlan-VPN-RTR(config-ext-nacl)# remark permit DHCP Client Traffic
outlan-VPN-RTR(config-ext-nacl)# permit udp any any eq bootpc
outlan-VPN-RTR(config-ext-nacl)# remark permit IPSEC Phase 1 Phase 2 traffic
outlan-VPN-RTR(config-ext-nacl)# permit esp host 190.55.2.98 any
outlan-VPN-RTR(config-ext-nacl)# permit udp host 190.55.2.98 any eq isakmp
outlan-VPN-RTR(config-ext-nacl)# permit esp host 45.240.90.194 any
outlan-VPN-RTR(config-ext-nacl)# permit udp host 45.240.90.194 any eq isakmp
outlan-VPN-RTR(config-ext-nacl)#exit
outlan-VPN-RTR(config)# interface FastEthernet0/0
outlan-VPN-RTR(config-if)#ip address dhcp
outlan-VPN-RTR(config-if)#ip access-group VPN-IN in
outlan-VPN-RTR(config-if)#crypto ipsec client ezvpn hard-client outside
outlan-VPN-RTR(config-if)#exit
outlan-VPN-RTR(config)# interface Vlan100
outlan-VPN-RTR(config-if)#ip address 172.30.100.1 255.255.255.0
outlan-VPN-RTR(config-if)#crypto ipsec client ezvpn hard-client inside
outlan-VPN-RTR(config-if)#exit
outlan-VPN-RTR(config)# interface Vlan120
outlan-VPN-RTR(config-if)#ip address 172.30.120.1 255.255.255.0
outlan-VPN-RTR(config-if)#crypto ipsec client ezvpn hard-client inside
outlan-VPN-RTR(config-if)#exit
```

IP Routing Configuration

The routing configuration for this example is very simple. There is no default route configuration, because the outside interface is configured with DHCP and the default route will be provided as part of the DHCP lease from the ISP. For aesthetic purposes we could set the DR to the physical interface Fa0/0, but it is not required. It's also simple because all traffic to one of the inside interfaces is

Full Crypto VPN Hardware Client Configuration for Cisco EzVPN

Michael J. Martin

encrypted and sent to the VPN gateway. We do, however, need to provide some routing logic for the adjacent subnets that the client will also be securing. This can be handled with some static routes:

```
outlan-VPN-RTR(config)# ip route 172.30.62.0 255.255.255.0 1.1.1.254
outlan-VPN-RTR(config)# ip route 172.30.89.0 255.255.255.0 1.1.1.254
```

With "connect auto" set in the hardware client profile, the client will open negotiations with the VPN gateway as soon as the interface designations have been set and the interfaces are up. If you have been building along on your own network, your client and VPN gateway should now be connected and able to pass secured traffic.