

Network to Network VPN Gateway Configuration for Cisco EzVPN

Michael J. Martin

Previous articles in this series on Cisco IPsec VPN configuration covered building a VPN gateway and implementing clients using a Cisco router as the gateway and Cisco's software VPN client. Now we will examine Cisco's EzVPN ability to support network-to-network VPN topologies using the Cisco router as the VPN gateway and the Cisco router hardware client. We will use both full-crypto and split-tunneling architectures. Where software client solutions are limited, hardware client solutions provide flexibility. Both of our examples can be used to provide primary support for remote office connections or with a leased line or other VPN links to provide backup or secondary connectivity.

Interoperability is a benefit of products based on IPsec standards, but what makes some products superior is the technology developed on top of IPsec. Traditional network-to-network interoperability means that two known IPsec peers, each running a different vendor's IPsec solution, can achieve IKE authentication, exchange Keys, establish SAs, and qualify, transmit, and receive secured traffic. These basic elements do not make an enterprise VPN solution. High availability, routing protocol support, broad authentication options, and packet fragmentation processing, to name just a few, are the elements that make up an enterprise-class VPN solution. After you waste a day in the lab making two different vendors IPsec-based VPNs interoperate, you quickly learn that it's not supporting the IPsec standards that make a given vendor's solution attractive, it's what the vendor has built on top of those standards that makes it great.

Although the existence of Cisco's EzVPN is an anathema to many IPsec traditionalists, EzVPN is an excellent example of building on top of IPsec to make IPsec VPNs work for the enterprise. The premise behind the EzVPN model is that the VPN gateway or core device should be smart, with the ability to control the peer connection parameters, at least as much as is viable. The VPN client or edge device, in contrast, should be simple, having just enough information to get connected to the core without hurting itself. It could be said that this model is quite contrary to traditional IPsec dogma, which is based on the idea that IPsec peers are supposed to be, well... peers.

Cisco accomplishes this non-traditional IPsec peer configuration using its Unity Client Protocol (UCP) to facilitate communications between the gateway and the client, enabling the VPN gateway to push the tunnel parameters, SA lifetimes, authentication, etc., to the client and in turn allow the client to push information about the networks it is securing. The gateway and client push configuration data, no static crypto maps, and XAUTH authentication.

The EzVPN hardware client is supported on the Cisco 8xx, 176x, 18xx, 26xx, 37xx, and 38xx platforms. The EzVPN gateway is typically implemented on a 38xx or 72xx platform. The EzVPN hardware client supports two modes: Client and Network Extension. In Client Mode (EZ-CM), the router is assigned an IP address out of the VPN gateway's client address pool. The VPN address is dynamically configured on the router and bound to a loopback interface. Once the VPN connection is established, all traffic is forwarded using Port Address Translation (PAT). This is essentially how the Cisco VPN client operates. Like the software client, split-tunnel or full-crypto security models are supported. EZ-CM has limited value except perhaps in a home office environment, where you could more easily use a software client.

Network Extension Mode (EZ-NEM) allows the remote router to establish IPsec peering with the VPN gateway for directly and indirectly connected networks, thus supporting a "routed" communication

Network to Network VPN Gateway Configuration for Cisco EzVPN

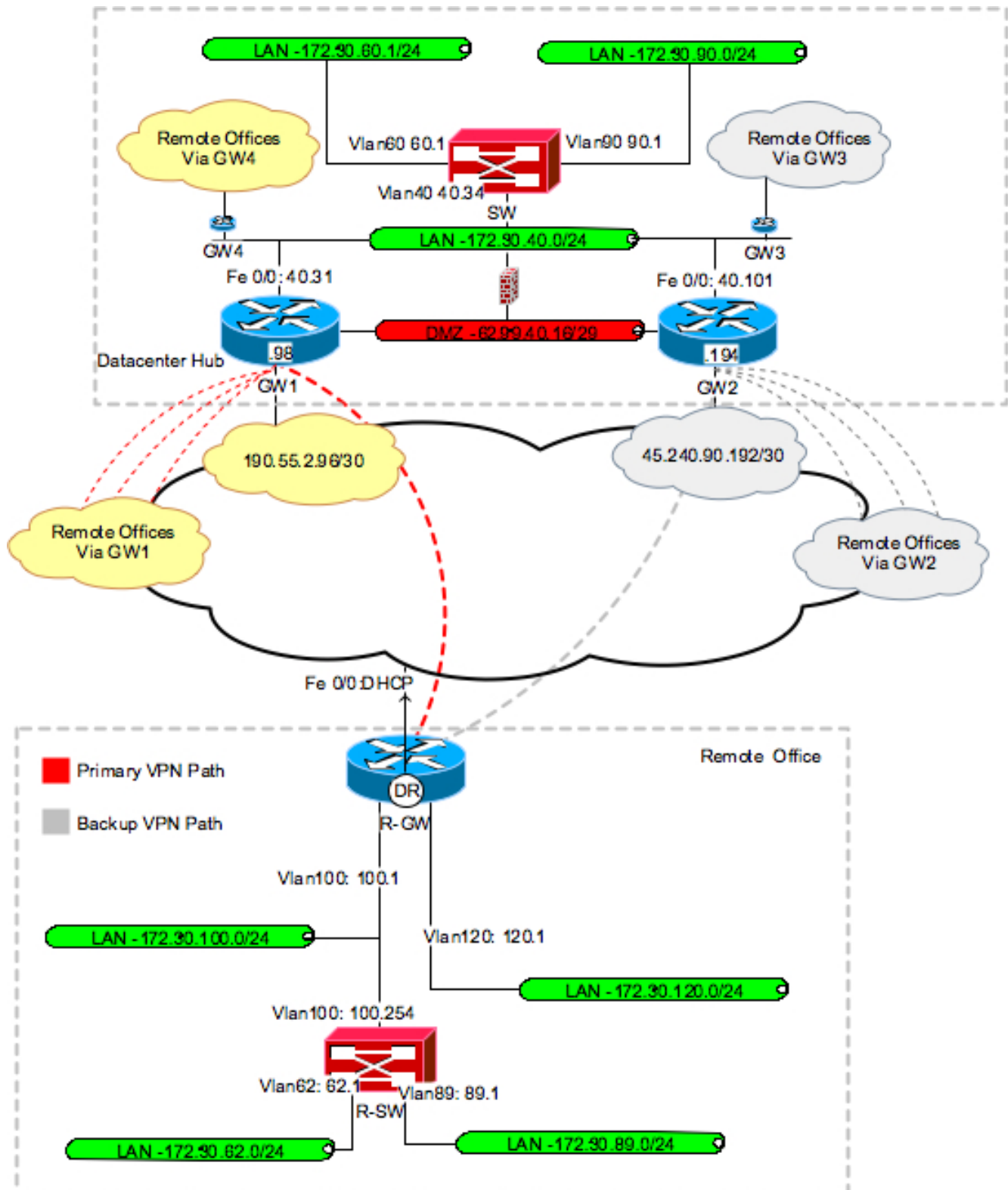
Michael J. Martin

model that is completely dynamic. The VPN gateway does not require an IP network or even the remote peer's IP address to establish the IPsec policy. The hardware client uses the designations "outside" for the public or unsecured network interface and "inside" for the router interfaces that are connected to networks that should be secured, in addition to the defined networks that are not directly connected but reachable through a gateway connected to one of the designated secure segments and can be included in the EZ-NEM policy using an ACL. The EZ-NEM client also supports gateway redundancy and dynamic routing.

In our first hardware client design scenario, a small local office needs reliable connectivity to the corporate data network and other remote offices. The company uses a VPN because it provides cost-effective network connectivity. The company also monitors Internet usage so all external Internet access must flow out of the corporate firewall. The office has one broadband Internet connection. We will be implementing a redundant VPN gateway core solution using a full-crypto client policy that provides access to core server LAN segments, remote office networks and the Internet.

Network to Network VPN Gateway Configuration for Cisco EzVPN

Michael J. Martin



Network to Network VPN Gateway Configuration for Cisco EzVPN

Michael J. Martin

Below is the VPN gateway configuration that supports both of the hardware client examples (the second example elements are in red) we are implementing:

I. AAA configuration:

GW 1 (Used for topology example 1 and 2)	GW 2 (Used for topology example 1 only)
<pre>aaa new-model aaa authentication login default local aaa authentication login userauth local aaa authorization network groupauth local ! username outlan-rtr1 password 0 outlan-rtr1</pre>	<pre>aaa new-model aaa authentication login default local aaa authentication login userauth local aaa authorization network groupauth local ! username outlan-rtr1 password 0 outlan-rtr1</pre>

II. ISAKMP Phase I configuration:

GW 1 (Used for topology example 1 and 2)	GW 2 (Used for topology example 1 only)
<pre>crypto isakmp policy 10 encr 3des hash md5 authentication pre-share group 2</pre>	<pre>crypto isakmp policy 10 encr 3des hash md5 authentication pre-share group 2</pre>
<pre>crypto isakmp client configuration group hard-client-fc key supersecret save-password pfs backup-gateway 45.240.90.2 max-users 1 max-logins 1 ! crypto isakmp client configuration group hard-client-st key supersecret acl hard-client-nets save-password pfs backup-gateway 45.240.90.2 max-users 1 max-logins 1</pre>	<pre>crypto isakmp client configuration group hard-client-fc key supersecret save-password pfs backup-gateway 190.55.2.98 max-users 1 max-logins 1</pre>
<pre>crypto isakmp profile hard-client description ISAKMP for Cisco Soft Clients match identity group hard-client client authentication list userauth isakmp authorization list groupauth client configuration address respond keepalive 20 retry 10</pre>	<pre>crypto isakmp profile hard-client description ISAKMP for Cisco Soft Clients match identity group hard-client client authentication list userauth isakmp authorization list groupauth client configuration address respond keepalive 20 retry 10</pre>

Network to Network VPN Gateway Configuration for Cisco EzVPN Michael J. Martin

```

ip access-list extended hard-client-nets
permit ip 172.30.40.0 0.0.0.255 1.1.1.0
0.0.0.255
permit ip 172.30.40.0 0.0.0.255
172.30.62.0 0.0.0.255
permit ip 172.30.40.0 0.0.0.255
172.30.89.0 0.0.0.255
permit ip 172.30.60.0 0.0.0.255 1.1.1.0
0.0.0.255
permit ip 172.30.60.0 0.0.0.255
172.30.62.0 0.0.0.255
permit ip 172.30.60.0 0.0.0.255
172.30.89.0 0.0.0.255
permit ip 172.30.131.0 0.0.0.255 1.1.1.0
0.0.0.255
permit ip 172.30.131.0 0.0.0.255
172.30.62.0 0.0.0.255
permit ip 172.30.131.0 0.0.0.255
172.30.89.0 0.0.0.255
permit ip 172.30.50.0 0.0.0.255 1.1.1.0
0.0.0.255
permit ip 172.30.50.0 0.0.0.255
172.30.62.0 0.0.0.255
permit ip 172.30.50.0 0.0.0.255
172.30.89.0 0.0.0.255
permit ip 172.30.132.0 0.0.0.255 1.1.1.0
0.0.0.255
permit ip 172.30.132.0 0.0.0.255
172.30.62.0 0.0.0.255
permit ip 172.30.132.0 0.0.0.255
172.30.89.0 0.0.0.255

```

III. ISAKMP Phase II configuration:

GW 1 (Used for topology example 1 and 2)	GW 2 (Used for topology example 1 only)
crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac	crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map hard-vpn-gateway 15 set security-association lifetime seconds 12000 set transform-set DES-MD5 set pfs group2 set isakmp-profile hard-client reverse-route	crypto dynamic-map hard-vpn-gateway 15 set security-association lifetime seconds 12000 set transform-set DES-MD5 set pfs group2 set isakmp-profile hard-client reverse-route
crypto map secure-client 10 ipsec- isakmp dynamic hard-vpn-gateway	crypto map secure-client 10 ipsec- isakmp dynamic hard-vpn-gateway

Network to Network VPN Gateway Configuration for Cisco EzVPN Michael J. Martin

IV. Crypto map installation interfaces, Internet policy route and IP routing configuration:

GW 1 (Used for topology example 1 and 2)	GW 2 (Used for topology example 1 only)
<pre>interface FastEthernet0/0 ip address 190.55.2.98 255.255.255.252 crypto map secure-client ! interface FastEthernet0/1 ip address 172.30.40.31 255.255.255.0</pre>	<pre>interface FastEthernet0/0 ip address 45.240.90.194 255.255.255.252 ip policy route-map int-acc crypto map secure-client ! interface FastEthernet0/1 ip address 172.30.40.101 255.255.255.0</pre>
<pre>router ospf 20 log-adjacency-changes redistribute static metric 200 subnets network 172.30.40.0 0.0.0.255 area 0.0.0.0</pre>	<pre>router ospf 20 log-adjacency-changes redistribute static metric 200 subnets network 172.30.40.0 0.0.0.255 area 0.0.0.0</pre>
<pre>ip route 0.0.0.0 0.0.0.0 190.55.2.97</pre>	<pre>ip route 0.0.0.0 0.0.0.0 45.240.90.193</pre>

In order for the remote offices to communicate with each other, the core routers must utilize a dynamic routing protocol to announce the remote networks they have established peering relationships with. This is accomplished using a combination of a dynamic routing protocol, static route redistribution and Reverse Route Injection (RRI). RRI is enabled as one of the crypto map policy options using the configuration command <reverse-route>. With RRI enabled, after the client and gateway establish IPsec peering the gateway device dynamically adds static routes to its routing table for the secured network and its associated remote tunnel endpoint. These static routes can then be redistributed via a routing protocol such as OSPF or BGP. In the example above, OSPF redistributes the remote networks.