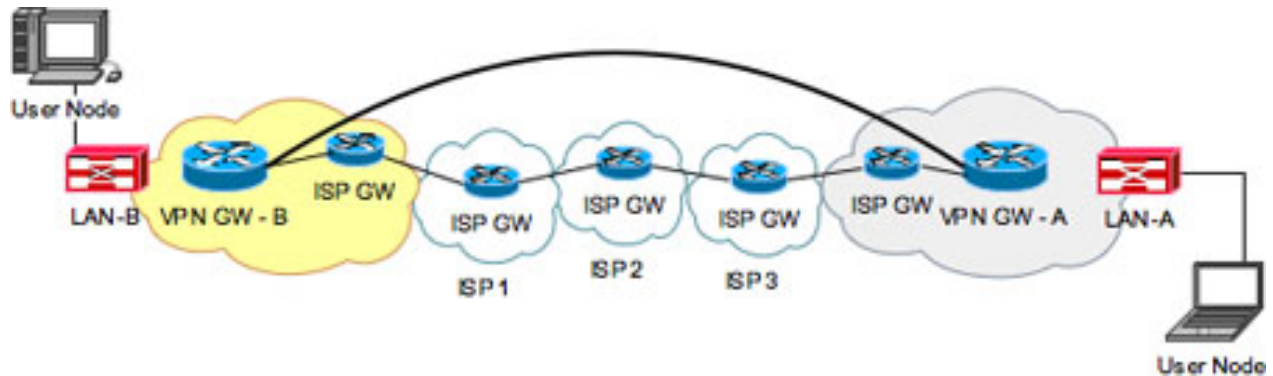


IPsec VPN Connection Models: Site-to-Site and Client-to-Site

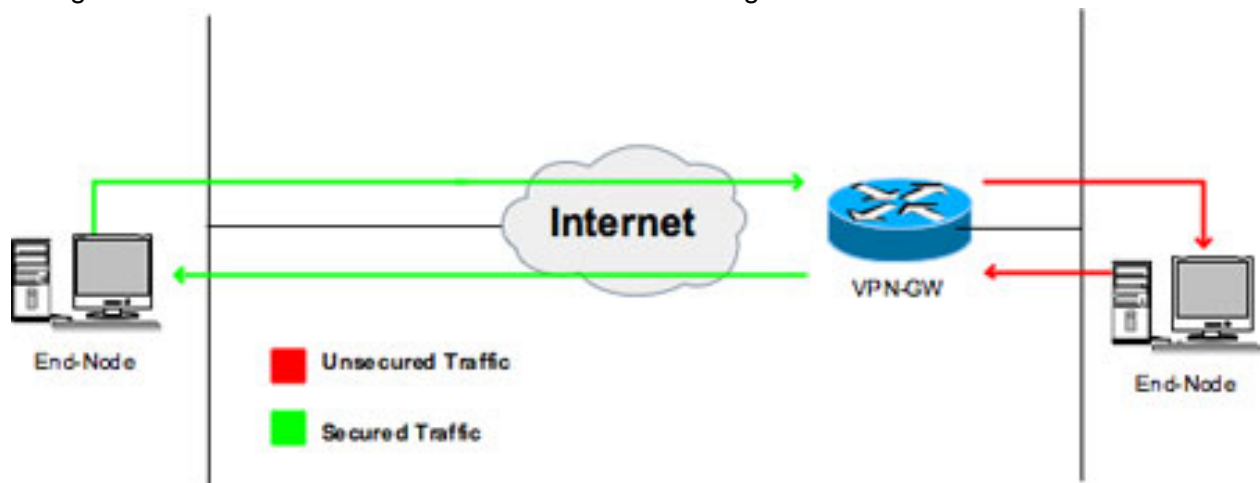
Michael J. Martin

In the first article in this series on implementing VPN gateways using Cisco routers, we reviewed the basic protocols and process involved with establishing an IPsec connection between two peers. Now let's take a look at the basic IPsec VPN connection models. While the IOS supports a variety of IPsec implementations, essentially all IPsec VPNs are implemented using one of two basic forms: site-to-site and client-to-site VPNs.



Site-to-site VPN

In the site-to-site VPN configuration above, each node is connected to a discrete network, separated by other unsecured or public networks. Depending on the security requirements for these network segments, it could be the case that end nodes on the networks are not able to exchange data unless the VPN is in place. This type of VPN configuration is known as a "closed" site-to-site network topology. Alternatively, the end nodes connected to the segments could have the ability to freely exchange data, utilizing other networks to relay the data back and forth. This data exchange, however, is unsecured. In this kind of network environment, IPsec can be employed to secure some or all of these data exchanges. This type of VPN configuration is known as an "open" site-to-site network design. The key point is that in either case, IPsec is implemented using gateways that secure the data exchanges. And, more importantly, the securing of the data exchanges is done without any knowledge of the end nodes connected to the networks being secured.



IPsec VPN Connection Models: Site-to-Site and Client-to-Site

Michael J. Martin

Client-to-site VPN

In the case of a client-to-site topology, the models "open" and "closed" still hold true. Connectivity between nodes separated by (or adjacent to) the IPsec gateway may or may not be restricted. In an open client-to-site topology, the network path between the end node and the IPsec gateway is secured. In a closed client-to-site topology, the path between the end node and gateway is secure. But data exchanges between the client node and nodes adjacent to (i.e., behind) the IPsec gateway is only possible if a connection to the IPsec gateway exists.

In both topologies, the relationship between the client node and the IPsec gateway is architecturally similar to a traditional PSTN remote-access dial network. The end node establishes a connection to the gateway and the two communicate as IPsec peers. Additionally, the gateway provides the end node an IP identity that gives the client node IP network access to other end nodes directly connected (via VPN) and adjacent to the IPsec gateway. The communications between the client end node and the gateway is secured with IPsec. Communications between the client end node and other end nodes adjacent to the IPsec gateway, however, are not secured.

When developing IPsec solutions, it is important to keep in mind that the IPsec protocol suite is geared to secure IP communications. The construct of the VPN is commonly perceived today as the connecting of private (secured) networks using public (unsecured) ones as the connectivity substrate. That is not solely what IPsec was developed to support. IPsec can also be used to enhance the security within private networks, using many of the same solution strategies used to secure data over public networks. That's a thought to keep in mind as we examine different IOS IPsec configurations, all of which start with the configuration of the router's ISAKMP policy using IKE.