APPLICATION NOTE

Dynamic VPN Tunnel Architecture

More and more customers are using broadband links (i.e., DSL & cable) to network all their business sites. Most of the broadband service providers issue IP addresses dynamically to their clients. As a result customers who secure their connections with VPN tunnels require the ability to establish IPSec tunnels over these links.

The existing Vanguard VPN tunnel architecture is based on the use of static addresses to identify the tunnel endpoints, however, the new dynamic tunnel address feature addresses the problem of establishing IPSec tunnels over links where the addresses may be assigned dynamically. The following figure illustrates a sample scenario of a VPN tunnel with the remote side using a dynamic address.

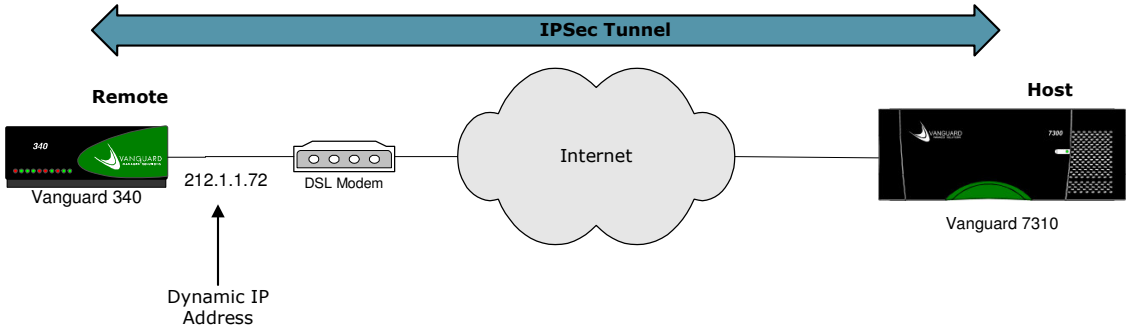

Figure 1 - Sample Tunnel Application

In this scenario:

- The remote side of the tunnel will be able to learn the dynamic address from the DSL service provider and use it to initiate an IPSec tunnel to the host.
- The host will be able to accept a connection from a remote tunnel for which the address is not known or may change over time.

This document will examine the functionality on both the remote and hosts nodes. All further references to the host and remote sides will be in the context of Figure 1. The remote side will refer to the node using the dynamic address and the host will refer the node using a static address.

Remote Node

Tunnels on nodes where the IP address is provided by a server or peer will be able to learn the IP address with little user configuration. Once the address has been learned on the link, the address will be installed in the tunnel and the IPSec negotiations will begin and continue similarly to when the using static addresses.

Host Node

Tunnels on host nodes where the destination address of the peer is not known are somewhat more complex and there are several issues associated with the dynamic tunnels where the endpoints are unknown.

Currently, when an incoming ISAKMP negotiation request is received, the ISAKMP module will identify which tunnel it is for by using the source and destination address of the packet. (The source and destination address uniquely identify the tunnel). In the dynamic address scenario the host side is not aware of the endpoint addresses. So it will be unable to determine which tunnel the ISAKMP requests are for. The solution is to match based on ISAKMP negotiation parameters rather than the IP addresses. So when an ISAKMP request is received, all the dynamic tunnels are examined to see whether they have any matching ISAKMP proposals. If there is a match, then that tunnel will be used to continue negotiations. However, a problem arises when multiple dynamic tunnels are configured. How do you distinguish the proposals on the tunnels? For this reason, the following restriction will exist. The ISAKMP policies on all the dynamic tunnels will have to be the same. Thus, the IPSec profile applied all the tunnels with dynamic destination addresses will need to use the same IPSec profile. So all dynamic tunnels on the host side must use the same profile.

Another reason for this restriction is that the pre-shared key is connected to the profile. If the dynamic tunnels are allowed to have different profiles, then even if the ISAKMP proposals match, the keys can be different and cause authentication failures. For example, in Figure 2, a node configured with two dynamic tunnels receives a request. The tunnels are examined for matching proposals, and it is possible that either one of the tunnels can match the request as they both have IKSAMP policy 1 as a match. Lets assume that the request is actually for establishing a connection with tunnel 2. If the tunnel 1 is chosen and used to continue negotiations, then there will be an authentication failure as the remote side will use the pre-shared key “alice” and tunnel 1 will use the key “bob”. So to avoid this problem, tunnel 1 and tunnel 2 must use the same profile so that the pre-shared keys are the same.

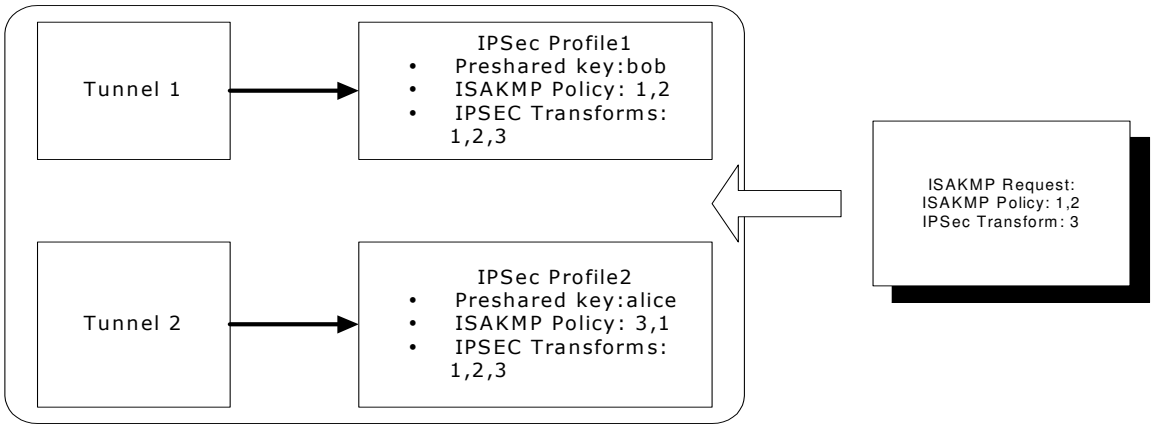

Figure 2 - ISAKMP Request Processing

Currently, the tunnels will try to establish as soon as there is connectivity to the peer. However, in the dynamic address scenario, the host side will not try to establish a tunnel connection as the remote address is not known. Instead it will only listen for incoming tunnel negotiation requests.

Supported Platforms

The Dynamic Tunnel Address feature will be supported on all existing platforms that support IPSec.

Limitations

- All dynamic tunnels on the host will have to use the same IPSec profile. Only one profile can be used to address the different policy schemes on various remote sites using dynamic addresses.
- All pre-shared keys used on the host for remotes with dynamic addresses will have to be the same.
- In scenario where Vanguard is the host node and the remotes are Cisco nodes, and the host wants to send data to the remote, it will not be able to do so as it cannot initiate a tunnel request. Cisco remotes will only negotiate a tunnel if it has data to send. So the tunnel will only be established if the remote wants to send data. In the case where the remote nodes are Vanguard, the problem does not exist; Vanguard will always try to negotiate a tunnel even if there is no data to send. So the tunnel will always be up.
- The Dynamic Address feature will only be supported on IPSec tunnels. SAM and GRE tunnels will continue to only work with static addresses.

Applications and Scenarios

The typical application scenario for this feature is targeted for the broadband connections such as DSL and cable. The figure below illustrates a sample application where the branch office sites are connected to the Internet via a DSL provider. For secure transmissions, VPN tunnels are used to connect to the central site.

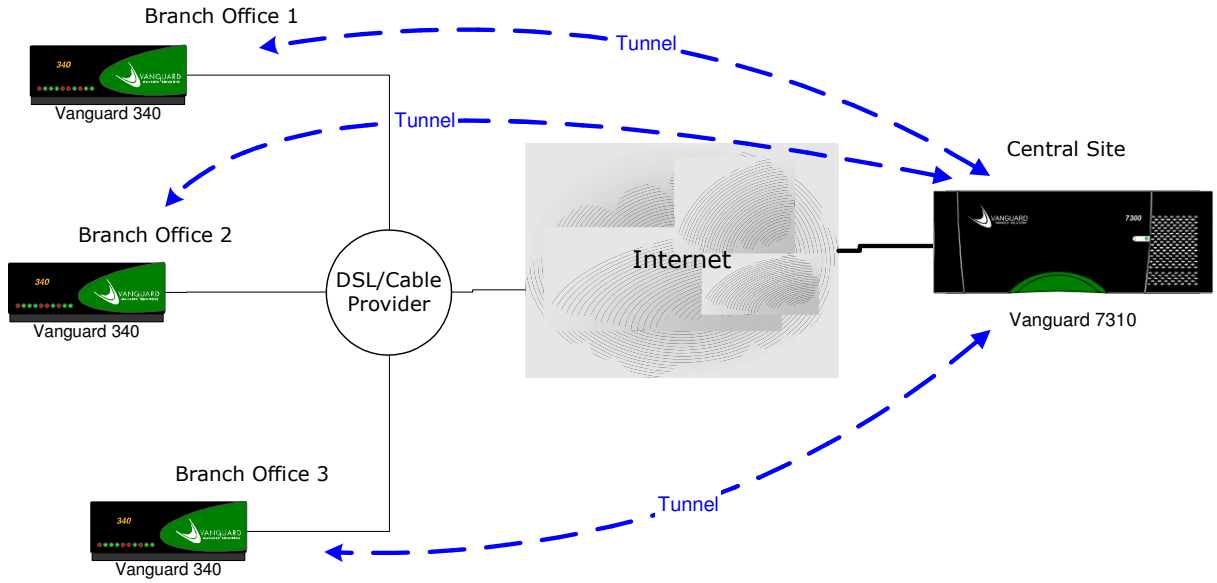

Figure 3

Vanguard Networks ♦ 25 Forbes Blvd. ♦ Foxboro MA 02035 ♦ USA
Phone +1 (508) 964 6200 ♦ Fax +1 (508) 543 0237
www.vanguardnetworks.com