What do the messages mean in the SoftRemote Log Viewer?

A: The SoftRemote Log Viewer displays the IKE and IPSec negotiation between the SoftRemote client and the peer encryptor, such as a VPN gateway. This negotiation establishes the VPN tunnel.

Here is a sample of a successful log using Main Mode for Phase 1:

Pre-share - Initiating IKE Phase 1 (IP ADDR=IPSec peer)
Pre-share - SENDING>>>> ISAKMP OAK MM (SA)
Pre-share - RECEIVED<<< ISAKMP OAK MM (SA)
Pre-share - SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID)
Pre-share - RECEIVED<<< ISAKMP OAK MM (KE, NON)
Pre-share - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
Pre-share - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
Pre-share - Established IKE SA
MY COOKIE 1f f5 e4 d 84 30 f9 5c
HIS COOKIE 4c af 1f 2c 20 16 d0 ec
Pre-share - Initiating IKE Phase 2 with Client IDs (message id: 61965C8D)
Initiator = IP ADDR= your_address, prot = 0 port = 0
Responder = IP ADDR= IPSec peer, prot = 0 port = 0
Pre-share - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID)
Pre-share - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NOTIFY:STATUS_RESP_LIFETIME, NON, ID, ID)
Pre-share - SENDING>>>> ISAKMP OAK QM *(HASH)
Pre-share - RECEIVED<<< ISAKMP OAK QM *(HASH, NOTIFY:NOTIFY_CONNECTED)
Pre-share - Loading IPSec SA (Message ID = 61965C8D OUTBOUND SPI = 405 INBOUND SPI = 493B30CC)

Here are some common error messages and troubleshooting suggestions:

Message Not Received! Retransmitting!
Message Not Received! indicates that SafeNet SoftRemote sent an IPSec packet to a peer encryptor, such as a VPN client or VPN gateway, and expected a response, but did not get one.

There are many reasons why a response was not received from the VPN peer. Here are the most common causes:

1) SoftRemote and the VPN peer do not have matching security policies.

Suggestions:
Check the configurations of the security policies settings to make sure they match. View the log of the VPN peer for more information on why it did not respond to the IPSec packet.

2) Packet was blocked along the path from the SoftRemote client to VPN gateway.

Suggestions:
a) Check the connection by sending a ping to the peer VPN client or VPN gateway. b) A personal firewall may be blocking the traffic. Make sure it is open to UDP port 500 and ESP protocol 50 and AH protocol 51.

3) SoftRemote client may have a private IP address assigned to it, which cannot be routed back to over the public Internet. Network Address Translation (NAT) is not supported within the VPN tunnel unless the user has installed SoftRemote version 8 or later and the peer encryptor is NAT-T compatible.

Suggestions:
a) Obtain a public IP address from the ISP.
b) Disable NAT on the local gateway.

Incorrect Phase 1 ID type
Expected FQDN, received IP address 0.0.0.0, or Expected ID_IPV4_ADDR, received FQDN

Incorrect Phase 1 ID type indicates that SafeNet SoftRemote was configured to expect a specific ID type from the peer encryptor but got a different ID type than the one configured in the Security Policy Editor. The resolution is to set the Secure Gateway ID Type to the expected ID Type (IP Address, Domain Name, or Distinguished Name) or change the ID Type to ANY.

FQDN = Fully Qualified Domain Name, or Domain Name
IPV4_ADDR = IP address

Pre-share - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT) Pre-share - SENDING>>>> ISAKMP OAK MM * (Retransmitting)
The asterisk (*) in this message indicates that this packet is encrypted, and is subject to an integrity check by the peer VPN encryptor. There are 2 common reasons for failure at this point in the negotiation:
1) NAT is being performed within the VPN tunnel and the peer VPN encryptor does not support NAT-T. See the FAQ regarding NAT.
2) The pre-shared key does not match the pre-shared key, or shared secret, in the peer VPN encryptor. Re-enter the pre-shared key exactly as it is entered in the security policy of the peer VPN encryptor.