

Troubleshooting NetScreen Remote from Log Viewer

Introduction

This document describes the messages that appear in the NetScreen Remote (NSR) Log Viewer. The Log Viewer messages enable users to troubleshoot problems with establishing IPSec communications. The Log Viewer must be enabled before logging will occur. You can print and save log files.

Log Viewer Message Format

Two types of messages can appear in the Log Viewer: error messages and IKE messages. For error messages, see *IKE Messages*.

This is the format of IKE messages:

message time connection name transmit direction IKE message

For example, this is a typical message logged in the Log Viewer:

01:38:02.570 Balt Corporate Access - SENDING>>>> ISAKMP OAK MM (SA)

Log Viewer Field	Field Definition	Message Segment
Message time	Time that message is written to log	01:38:02.570
Connection name	Security Policy Editor connection name associated with the IKE activity	Balt Corporate Access
Transmit direction	Direction of IKE message: sending or receiving	SENDING>>>>
IKE message	IKE message indicating type of ISAKMP message being processed. IKE messages are defined in the NSR Log Viewer IKE message table.	ISAKMP OAK MM (SA)

Troubleshooting with the Log Viewer

This table lists different scenarios and the accompanying debug messages. Use this information as a reference for interpreting the Log Viewer file in conjunction with the NetScreen Remote (NSR) Log Viewer IKE message table.

Successful IKE Establishment

Description and Result	Debug Messages
<p>Successful Main Mode (MM) Negotiation (Pre-share) Successful SA established. Yellow key appears in NSR icon.</p>	<pre>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)</pre>
<p>Successful Aggressive Mode negotiation (pre-shared key) Successful SA established. Yellow key appears in NSR icon.</p>	<pre>Pre-share - Initiating IKE Phase 1 (IP ADDR= IPSec peer) Pre-share - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID) Pre-share - RECEIVED<<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH) Pre-share - SENDING>>>> ISAKMP OAK AG *(HASH) Pre-share - Established IKE SA MY COOKIE 73 9c 76 19 4f 5e 35 c8 HIS COOKIE e9 94 9c 82 64 b2 fa 44 Pre-share - Initiating IKE Phase 2 with Client IDs (message id: 99F08C75) 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 = 99F08C75 OUTBOUND SPI = 189 INBOUND SPI = BA78A2CD)</pre>

Failed IKE Establishment

Description and Possible Cause	Debug Messages
<p>IPSec peer not responding; no key appears in NSR icon.</p> <p>Remote peer is either unreachable or not responding to SA request. Verify that IP connectivity exists to the local router and then to the IPSec peer.</p>	<pre>Demo - Initiating IKE Phase 1 (IP ADDR= IPSec peer) Demo - SENDING>>>> ISAKMP OAK MM (SA) Demo - message not received! Retransmitting! Demo - SENDING>>>> ISAKMP OAK MM (Retransmission) Demo - message not received! Retransmitting! Demo - SENDING>>>> ISAKMP OAK MM (Retransmission) Demo - message not received! Retransmitting! Demo - SENDING>>>> ISAKMP OAK MM (Retransmission) Demo - Exceeded 3 IKE SA negotiation attemptsx</pre>
<p>Failed Quick Mode (QM) negotiation</p> <p>Improper IPSec peer configuration. NSR was configured for three retransmissions to establish SA.</p>	<pre>Demo - Initiating IKE Phase 1 (IP ADDR=IPSec peer) Demo - SENDING>>>> ISAKMP OAK MM (SA) Demo - RECEIVED<<<< ISAKMP OAK MM (SA) Demo - SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID) Demo - RECEIVED<<<< ISAKMP OAK MM (KE, NON) Demo - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT) Demo - RECEIVED<<<< ISAKMP OAK MM *(ID, HASH) Demo - Established IKE SA MY COOKIE 1f f5 e4 d 84 30 f9 5c HIS COOKIE 4c af 1f 2c 20 16 d0 ec Demo - 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 Demo - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) Demo - RECEIVED<<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Demo - SENDING>>>> ISAKMP OAK QM *(Retransmission) Demo - RECEIVED<<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Demo - SENDING>>>> ISAKMP OAK QM *(Retransmission) Demo - RECEIVED<<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Demo - SENDING>>>> ISAKMP OAK QM *(Retransmission) Demo - RECEIVED<<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Exceeded retry attempts - deleting IPSec Security Association</pre>

IKE Messages

IKE Message	Description and Explanation
ISAKMP OAK MM (SA)	<p>Message containing proposed parameters that will be used to secure sensitive exchange messages.</p> <p>ISAKMP proposal list exchange. Each proposal has a setting for encryption algorithm, hash algorithm, and Diffie-Hellman group. The agreed-on settings will be used to protect the final messages of MM and all of QM. Should the settings not be compatible, a NO PROPOSAL message will appear.</p>
ISAKMP OAK MM (KE, NON)	<p>The Diffie-Hellman exchanged and nonce used as key material for securing sensitive exchange messages.</p> <p>ISAKMP Diffie-Hellman key exchange with nonce. The key, KE, is created by each party using an agreed-on formula, plugging values in the formula, and raising the result of the formula to the power of a secret value. As each party knows its secret exponent, it can take the KE received from the other party and raise that by its own exponent. If each party performs this procedure, both get a shared secret key. The nonce, NON, is a nonsense random value used in the calculation to add randomness to the KE.</p>
ISAKMP OAK MM *(ID, HASH)	<p>The party's identity used as authentication and a calculated hash as assurance of identification.</p> <p>ISAKMP message containing the identity that one party is using as identification to the other. This can be its IP address, domain name, e-mail address, or distinguished name. That identity must be accepted by the receiving party for a positive identification. The hash, HASH, is created by selecting bits of the message as samples, then sending these selected bits through an algorithm. The pattern for selection and the algorithm are agreed on in the MM proposal exchange as the hash algorithm setting. The asterisk indicates that this message is one of the final MM messages and is protected, encrypted, and hashed.</p>

<p>ISAKMP OAK QM *(HASH, SA, NON, ID, ID)</p>	<p>Proposed parameters to be used when securing the IP data, the two parties identification and nonces for a non-PFS exchange.</p> <p>IPSec exchange message containing a hash of the message contents, HASH, a list of the proposed parameters to be used on the user's data, SA, each party's nonce, and the identity of each party's identification, ID. The parameters agreed on will be IPSec protocol, ESP or AH; encryption algorithm, if ESP is to be used; hash algorithm; and if tunneling is to be performed. Hash algorithms and tunneling settings are for either ESP or AH. The responder in an IKE that did not use Perfect Forward Secrecy (PFS), because there were no KEs, sent this message. This means that the parties will reuse some of the agreed-on key when calculating the IPSec key. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.</p>
<p>ISAKMP OAK QM *(HASH)</p>	<p>The conclusion of the Quick Mode exchange containing a hash of the agreed-on key, protocol, the responder's SPI, and the two nonces.</p> <p>IPSec message used to finalize the entire exchange. This also provides a form of verification as the hash is calculated using the IPSec key, IPSec protocol agreed on, the other party's Security Parameter Index (SPI), and the two nonces each party used. The SPI is a reference number each party uses to keep track of the parameters and keys to be used for the traffic that is sent and received. For example, I would tell you my SPI so when you transmit a protected message to me, I know how to handle the message properly, and vice versa. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.</p>
<p>ISAKMP OAK MM (KE, NON, VID)</p>	<p>The Diffie-Hellman exchanged and nonce used as key material for securing sensitive exchange messages and the product vendor ID.</p> <p>ISAKMP message containing a Diffie-Hellman key, KE, nonce used to add randomness to the key, and a Vendor ID used to notify the receiver of the transmitting party's vendor. This can be used to associate what the transmitter's capabilities are and allow parameter preferences to be made as well as determining if the connection should be established.</p>
<p>ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN)</p>	<p>Message indicating that the QM exchange parameters were incompatible, so the exchange failed.</p> <p>IPSec message viewed when the list of proposed parameters did not have any common settings for the transmitter. This means the IPSec parameters for each party must be verified. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.</p>

ISAKMP OAK QM *(Retransmission)	<p>Message indicating a previously sent message was sent again because no response was received in the allotted time.</p> <p>IPSec message sent when a previous message was not responded to in the configured time period. This indicates that one of the parties may not be available to complete the exchange. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.</p>
------------------------------------	--

Sample Messages

Device A

Device B

Phase 1—Authentication

1. MM ----->
SA(Security Association) DES/SHA-1/DHG1; TDES/SHA-1/DHG2
2. <----- MM
SA: TDES/SHA-1/DHG2
3. MM ----->
KE (Diffie-Hellman a^x), NON (nonsense, random number)
4. <----- MM
KE (Diffie-Hellman a^y), NON (nonsense, random number)
5. MM ----->
ID (the identification of one party), HASH
6. <----- MM
ID, HASH

***** Phase 1 Completed *****

Phase 2—Key Exchange with Perfect Forward Secrecy (PFS)

1. QM ----->
SA: ESP/DES/SHA-1; ESP/TDES/SHA-1; AH/MD5, KE, NON
2. <----- QM
SA: ESP/TDES/SHA-1, KE, NON
3. QM ----->
HASH

Message Explanations

Phase 1

During Phase 1, IDs and parameters for protecting Phase 2 are established.

1. Device A sends a list of proposed parameters to protect the Phase 2 key exchange and the level of key strength it wants to use for Phase 1's key exchange, not necessarily for both phases.
2. Device B selects the proposed parameters it prefers over the other proposals and send its selection to Device A. If none of the proposals fit its requirements, it sends a NO PROPOSAL message and the exchange ends. The two parties must be reconfigured to work.
3. Should the exchange continue, Device A calculates a number " a raised to x " where a is known by each device and x is a random number known only by Device A. The NON is a random number added to the calculation to add randomness.
4. Device B receives that message and performs a similar calculation.
5. Both sides exchange Identification. Alternate subject fields—IP address, e-mail address

and domain name—can be used as IDs. The ID is a field containing the information the party is using to identify itself.

6. If either side fails to accept the other's ID, the exchange ends. The two parties must be reconfigured to work.

If both sides are satisfied up to this point, Phase 1 completes and Phase 2 begins.

Phase 2

Phase 2 combines several Phase 1 steps.

1. Device A sends a list of proposed parameters using the new key material established in Phase 1.
2. Phase 2 concludes with a HASH—the IDs and NON's of each party and the responder's (Device B's) SPI to use when sending packets.

This concludes the key exchange. The two parties can now exchange data securely.