

# Troubleshooting Guide: IKE IPSec VPN Initialization

02/2007

## Introduction

This guide will present the basic information required to troubleshoot problems in establishing an IKE IPSec VPN Tunnel. The guide will first present the basic premise of IKE negotiation, protocol support, and noteworthy configuration details. This guide will then provide a methodology to test and troubleshoot using the IKE log messages.

## IKE Negotiation

An IKE VPN tunnel is established by negotiations between two IPSec security devices. The VPN *Security Association* (SA) configured on each device defines the Security Policy settings proposed in the IKE negotiation. For negotiations to succeed, these Security Policies must be in agreement.

When a VPN/Firewall receives a packet (e.g. a PING) destined for a subnet located behind the remote peer VPN/Firewall and the tunnel is not established, it will initiate the IKE negotiations to establish the VPN tunnel.

The IPSec security devices negotiating an IKE VPN are referred to as an IKE Initiator and an IKE Responder. This distinction is evident in the logs. They are defined as follows:

- ☞ IKE Initiator: Device initiating the IKE VPN tunnel negotiation request.
- ☞ IKE Responder: Device receiving the request to establish an IKE VPN tunnel.

## IKE VPN Protocols

The IKE protocol is used during the entire negotiation phase. The negotiation defines policy settings and keys used by the IPSec tunnel protocol. The protocols used for the IKE negotiation and VPN tunnel are as follows:

### Standard

- TCP port 50 for IPSec Encapsulating Security Protocol (ESP) traffic
- TCP port 51 for IPSec Authentication Header (AH) traffic
- UDP port 500 for Internet Key Exchange (IKE) negotiation traffic

### With NAT Traversal (NAT-T) active

- UDP port 500 for Internet Key Exchange (IKE) negotiation traffic
- UDP port 4500 for IPSec Encapsulating Security Protocol (ESP) traffic

These protocols must not be blocked by any firewalls or the ISP networks between the two IPSec security devices attempting to establish the tunnel.

## NAT Traversal (NAT-T)

NAT Traversal (NAT-T) is a VPN option used on many IPSec security devices. It is typically enabled by default. With this option, a NAT discovery process runs after the IKE initiation request to determine if there are any NAT devices in the tunnel path. If a NAT device is detected in the tunnel path, the IPSec

security devices will use UDP encapsulated IPSec packets for the VPN tunnel. NAT discovery messages are displayed in the logs, but typically only in the IKE Responder log with Aggressive Mode.

### **Main Mode vs. Aggressive Mode**

There are two phases of the IKE negotiations, called Phase 1 and Phase 2. Phase 1 can be configured to use either Main Mode or Aggressive Mode. Main Mode is more secure in providing identity protection for the negotiating nodes. However, Main Mode requires a static IP address on both IPSec security devices negotiating the VPN tunnel.

Aggressive Mode is used when one IPSec security device has a dynamic WAN IP address (i.e., uses DHCP, PPPoE, PPPoA, PPTP, etc.). Aggressive Mode has more configuration requirements than Main Mode and may be difficult or impossible to achieve with some IPSec security device pairings.

### **IKE Access Rules**

Inbound and outbound IKE Access Rules may be required by any user controlled firewall device to allow IKE sessions. If one end of the VPN is a VPN/firewall combination device these rules are typically generated automatically when you setup or enable an IKE VPN SA.

Be sure not to disable the IKE rules in the firewall. Ideally, there should not be any other rules before the IKE access rule that would deny access for this service.

### **Routing Multiple Subnets Through a VPN (optional)**

The SA on each IPSec security device also defines the subnet behind the remote peer IPSec security device to which the VPN tunnel will route. In some cases, the IPSec security devices may support defining multiple subnets via a single SA. But this is device dependant and specific.

If there are multiple remote destination subnets defined in an SA, there will typically be a separate tunnel established for each subnet. Thus, a separate negotiation would occur for each subnet.

### **Central Gateway Configurations (optional)**

Some IPSec security devices support a Central Gateway configuration option and may sometimes be referred to as a Hub & Spoke configuration. Selecting an option entitled 'Use this SA as default route for all Internet traffic' allows you to configure a remote office or home installation to route all traffic including Internet traffic to a Central Gateway IPSec security devices.

This is to prevent 'Split Tunneling' and is often used in Hub and Spoke VPN configurations. Typically the configuration on the Central Gateway IPSec security device must define a 'Default LAN Gateway' IP address in the advanced configuration settings of the VPN SA. Traffic destined for the Internet will then route through the VPN and be forwarded to another firewall or router, defined as the 'Default LAN Gateway', which will route and control access to the Internet from the central site.

This option is useful for logging all Internet traffic or implementing content filtering, anti-virus, anti-spyware or other bulk security scans from the central site.

### **Testing The VPN Tunnel**

Initiating traffic through the VPN will start the IKE negotiation. Check the VPN Summary page of your IPSec security device to see the status of the VPN and any active tunnels. If a tunnel does not show as active after traffic for it has been generated, review the log messages on both IPSec security devices to determine the problem. The final sections of this document provide troubleshooting tips based on the error messages displayed.

Running a simple PING test will typically generate sufficient traffic to initiate the VPN.

Note: If a server is not responding to PING across a tunnel that appears to be active, verify that there is not a routing or connectivity problem between the server and the IPSec security device local to it. Also, verify the TCP/IP configurations of the server.

### **Troubleshooting IKE VPN Tunnel Establishment**

There are 3 basic scenarios to investigate if the IKE VPN tunnel fails to establish:

- 1) No Response to IKE Initiation Request
- 2) IKE Negotiation Fails
- 3) IKE Negotiation Completes, but No Traffic is Passing

The log messages generated during the IKE negotiations will show quickly which of the scenarios is occurring and where to focus the troubleshooting. The log entries in the Initiator log are different than those in the Responder log. In most cases, the responder will provide more precise information when there is an SA proposal mismatch during the negotiations. The logs of both the IKE Initiator and IKE Responder should be checked when troubleshooting establishment of a VPN.

### **Scenario 1: No Response to IKE Initiation Request**

Use the following table of log entries to determine troubleshooting steps to resolve a problem initiating the IKE negotiations.

| <b>IKE Initiator Log Messages</b>                                                                                                                                                                                                                                                                                                                                                                                        | <b>Troubleshooting Notes</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No IKE Initiator Start Negotiation message in log                                                                                                                                                                                                                                                                                                                                                                        | Check the following: <ul style="list-style-type: none"><li>✓ 'Disable this SA' box is not checked in SA of IKE Initiator.</li><li>✓ Destination subnet defined in SA of IKE Initiator.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>IKE Initiator: No response - Remote Peer Timeout<br/>IKE Initiator: No response - Remote Peer Timeout<br/>IKE Initiator: No response - Remote Peer Timeout<br/>IKE negotiation aborted due to timeout</p> <p><b>Note:</b> <i>If IKE Initiator Log only shows several timeout messages and negotiation aborted after a short delay, then there is a communication problem between the Initiator and Responder.</i></p> | Check the following: <ul style="list-style-type: none"><li>✓ Network connectivity between the units. (<b>Hint:</b> <i>Try to access remote unit HTTPS management console from a host behind the local unit</i>)</li><li>✓ 'Disable this SA' box is not checked in SA of IKE Responder.</li><li>✓ IPsec Gateway address in Initiator SA specifies WAN address of IKE Responder</li><li>✓ IPsec Gateway Name (if used) resolves to WAN address of IKE Responder</li><li>✓ IKE Access Rules are enabled on both IPsec security devices.</li><li>✓ No other firewalls in path blocking IKE (UDP 500) or IPsec (IP 50) protocols.</li><li>✓ Contact ISP to see if they are blocking IKE (UDP 500) or IPsec (IP 50) protocols.</li></ul> |

## Scenario 2: IKE Negotiation Failures

Use the following tables to identify pertinent log entries in the IKE Initiator and IKE Responder and appropriate troubleshooting steps to resolve the problem.

### Troubleshooting with IKE Initiator Log Messages

| IKE Initiator Log Messages                                                                                                                                                                                                                       | Troubleshooting Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Received notify: INVALID_ID_INFO                                                                                                                                                                                                                 | Aggressive Mode request error: <ul style="list-style-type: none"> <li>✓ Set SA security policy to use Aggressive Mode in both units.</li> <li>✓ SA name in local unit must be the same as the remote peer Unique Firewall Identifier (and vice-versa).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Received notify: PAYLOAD_MALFORMED                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>✓ Shared Secret mismatch error</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Received notify: NO_PROPOSAL_CHOSEN<br><br><b>Note:</b> <i>IKE Responder log will provide specifics of this error.</i>                                                                                                                           | SA Security Policy settings don't match or the destination network field in either SA is incorrect. <ul style="list-style-type: none"> <li>✓ <b>Check the IKE Responder log for specifics of the error.</b></li> </ul> Verify the following SA Security Policy settings match: <ul style="list-style-type: none"> <li>✓ Phase 1 DH Group</li> <li>✓ Phase 1 Encryption/Authentication</li> <li>✓ Phase 2 Encryption/Authentication</li> <li>✓ PFS should be either enabled or disabled on both units</li> <li>✓ Phase 2 DH Group, if PFS is enabled</li> </ul> If 'Specify destination networks' option is selected in VPN SA, verify the following: <ul style="list-style-type: none"> <li>✓ Destination network field in each SA is defined on remote peer LAN or has a static route on the remote peer.</li> <li>✓ If terminating on DMZ, destination network must be defined in DMZ.</li> <li>✓ If 'Apply NAT and firewall rules' enabled, destination addresses must be configured in NAT.</li> </ul> |
| IKE Responder: Received Aggressive Mode request (Phase 1)<br><br><b>Note:</b> <i>If this log message appears in the IKE Initiator log after initiating an Aggressive Mode request, check the IKE Responder log for an INVALID_ID_INFO error.</i> | Aggressive Mode request error: <ul style="list-style-type: none"> <li>✓ SA name in remote peer must be the same as the local unit's unique firewall identifier in the VPN settings (and vice-versa).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## **Scenario 2: IKE Negotiation Failures (continued)**

### **Troubleshooting with Responder Log Messages (Part 1)**

| <b>IKE Responder Log Messages (Basic)</b>                                                          | <b>Troubleshooting Notes</b>                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Received notify: INVALID_ID_INFO                                                                   | Aggressive Mode request error.<br><br>Check the following: <ul style="list-style-type: none"><li>✓ SA name in remote peer must be the same as the local unit's unique firewall identifier in the VPN settings (and vice-versa).</li></ul>                                              |
| Failed payload verification after decryption.<br>Possible preshare key mismatch.                   | ✓ Shared Secret mismatch                                                                                                                                                                                                                                                               |
| IKE Responder: IKE proposal does not match (Phase 1)                                               | ✓ Phase 1 Encryption/Authentication mismatch                                                                                                                                                                                                                                           |
| IKE Responder: Algorithms and/or keys do not match (Phase 2)                                       | ✓ Phase 2 Encryption/Authentication mismatch                                                                                                                                                                                                                                           |
| IKE Responder: ESP Perfect Forward Secrecy mismatch                                                | ✓ PFS should be either enabled or disabled on both devices<br>✓ Phase 2 Diffie-Hellman (DH) Group mismatch for PFS                                                                                                                                                                     |
| IKE Responder: No match for proposed remote network address                                        | ✓ Proposed source network from IKE Initiator is not defined in the destination network field on the IKE Responder SA.<br>✓ If 'Apply NAT and firewall rules' is enabled on IKE Initiator SA, destination field on IKE Responder needs to use the IKE Initiator public NAT address(es). |
| IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall | ✓ Destination network in IKE Initiator SA is not defined on LAN or static route on the IKE Responder.                                                                                                                                                                                  |

## **Scenario 2: IKE Negotiation Failures (continued)**

### **Troubleshooting with Responder Log Messages (Part 2)**

| <b>IKE Responder Log Messages (Advanced)</b>                                                           | <b>Troubleshooting Notes</b>                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IKE Responder: Tunnel terminates on DMZ but proposed local network is on LAN                           | Check the following: <ul style="list-style-type: none"><li>✓ IKE Responder SA is configured to terminate on DMZ, but the proposed destination network is on the LAN.</li></ul>                                                                           |
| IKE Responder: Tunnel terminates on LAN but proposed local network is on DMZ                           | <ul style="list-style-type: none"><li>✓ IKE Responder SA is configured to terminate on LAN, but the proposed destination network is on the DMZ.</li></ul>                                                                                                |
| IKE Responder: Tunnel terminates outside firewall but proposed local network is not NAT public address | <ul style="list-style-type: none"><li>✓ 'Apply NAT and firewall rules' option is enabled on the IKE Responder, but proposed destination network is not a public IP address on the IKE Responder.</li></ul>                                               |
| IKE Responder: Proposed local network is 0.0.0.0 but SA has no LAN Default Gateway                     | <ul style="list-style-type: none"><li>✓ The IKE Initiator SA is configured as default route for all Internet traffic but the IKE Responder has no 'Default LAN Gateway' address defined.</li></ul>                                                       |
| IKE Responder: Proposed remote network is 0.0.0.0 but not DHCP relay nor default route                 | <ul style="list-style-type: none"><li>✓ 'Default LAN Gateway' advanced option in IKE Initiator defines a gateway address, but the IKE Responder SA is not configured as default route for all Internet traffic (nor is DHCP relay configured).</li></ul> |
| IKE Responder: Default LAN gateway is set but peer is not proposing to use this SA as a default route  | <ul style="list-style-type: none"><li>✓ 'Default LAN Gateway' advanced option in IKE Responder defines a gateway address, but the IKE Initiator SA is not configured as default route for all Internet traffic.</li></ul>                                |

### **Scenario 3: IKE Negotiation Completes, but No Traffic is Passing**

If traffic will not pass through the VPN tunnel after the IKE negotiations successfully complete, then the VPN tunnel protocol is being blocked. The NAT discovery entries will determine which protocol, IPSec or encapsulated IPSec, is being used for the tunnel.

- ☞ If using Aggressive Mode, check the IKE Responder log to find the NAT Discovery messages. In Aggressive Mode, only the IKE Responder performs the NAT Discovery process.
- ☞ Be sure to verify the problem is with the VPN tunnel and not an external routing problem. The problem can be isolated by changing advanced configurations to ‘terminate on LAN’, including the remote LAN interface subnet as destination network, and running PING directly from the local IPSec security device to the remote IPSec security device LAN interface address.

### **Troubleshooting with NAT Discovery Messages**

| <b>NAT Discovery Log Messages</b>                                                                                                                               | <b>Troubleshooting Notes</b>                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAT Discovery: No NAT/NAPT device detected between IPSec Security gateways                                                                                      | Check the following: <ul style="list-style-type: none"><li>✓ Verify IPSec protocol (IP 50) is not being blocked by your ISP or another firewall</li></ul>                                                                                                                                                                                                                                 |
| NAT Discovery: Local IPSec Security Gateway behind a NAT/NAPT Device<br><br>- or -<br><br>NAT Discovery: Remote IPSec Security Gateway behind a NAT/NAPT Device | The NAT device may be blocking UDP encapsulated IPSec packets. <ul style="list-style-type: none"><li>✓ Check with the NAT device manufacturer to see if they know of a problem with blocking UDP encapsulated IPSec.</li><li>✓ Try disabling the NAT Traversal option if there are no other NAT devices in the tunnel path and the suspect NAT device supports IPSec pass-thru.</li></ul> |
| NAT Discovery: Peer IPSec Security Gateway doesn't support VPN NAT Traversal (NAT-T)                                                                            | <ul style="list-style-type: none"><li>✓ Verify there are no NAT devices in the tunnel path by enabling NAT Traversal on both units.</li><li>✓ Verify IPSec protocol (IP 50) is not being blocked by your ISP or another firewall.</li></ul>                                                                                                                                               |
| No NAT discovery messages found in either firewall log                                                                                                          | <ul style="list-style-type: none"><li>✓ Verify there are no NAT devices in the tunnel path by enabling NAT Traversal on both units.</li><li>✓ Verify IPSec protocol (IP 50) is not being blocked by your ISP or another firewall.</li></ul>                                                                                                                                               |

## **Additional Resources**

Here are some additional resources you find useful.

### **HomeNetHelp**

HomeNetHelp (<http://www.homenethelp.com/>) has various writings and White Papers on many manufacturers VPN devices and tips for achieving interoperability. They also host a user support forum on VPN Routers where users can post questions and get answers from their peers.

### **VPNC**

The VPN Consortium (<http://www.vpnc.org/>). VPNC has various writings and White Papers on many manufacturers VPN devices and tips for achieving interoperability.

### **SafeNet**

SafeNet (<http://www.safenet.biz/>) is one of the larger OEM providers of VPN client software to VPN/firewall manufacturers. SafeNet has a tech support area listing tech notes on their products with various VPN gateways including some individual interoperability examples.

### **SonicWALL**

The firewall manufacturer (<http://www.sonicwall.com/>) has several White Papers covering IPSec and VPN establishment and some tips for achieving interoperability. They also have a PDF called 'Troubleshooting Guide to IKE VPN Initialization' which was the inspiration for this document.

### **Netgear**

The network products manufacturer (<http://www.netgear.com/>) has some tech support notes and White Papers on their VPN/Firewall devices and some tips for achieving basic interoperability. They also host a user support forum on their various products where users can post questions and get answers from their peers.

### **Cisco**

The router manufacturer (<http://www.cisco.com/>) has several White Papers covering IPSec and VPN establishment and some tips for achieving interoperability.

### **Linksys**

The network products manufacturer (<http://www.linksys.com/>) has some tech support notes and White Papers on their VPN/Firewall devices and some tips for achieving basic interoperability. They also host a user support forum on their various products where users can post questions and get answers from their peers.

### **Intel**

The CPU manufacturer (<http://support.intel.com/>) has a White Paper covering VPN establishment and basic troubleshooting.