



CDRouter-IKE User Guide

Version 5.0



QA Cafe © 2009
support@qacafe.com

1.Introduction and Terminology

Introduction

CDRouter-IKE is an add-on module for CDRouter and CDRouter-MultiPort that adds IKE and IPSEC based VPN testing support to CDRouter. CDRouter-IKE is used to test CPE routers that contain VPN security gateway functionality based on IKE.

When CDRouter-IKE is enabled, CDRouter is able to establish IKE based VPN connections with the router under test by emulating IPSEC gateways and clients. Several automated functional test cases verify the behavior of IKE and verify that VPN connections are secure and robust. The CDRouter-IKE functionality can also be combined with CDRouter's existing application tests to allow application traffic to run over VPN connections.

CDRouter-IKE offers a blend of testing styles including conformance, functional, and negative. Many of the test cases focus on the underlying problems encountered during interoperability testing.

Since CDRouter-IKE is highly configurable, the number of VPN configurations that can be tested is unlimited. Test Engineers are encouraged to run their devices through as many different configurations as possible.

IKE/VPN Terminology

Before testing an IKE based gateway using CDRouter-IKE, it is helpful to review some terminology specific to IKE and VPNs. A good understanding of this terminology will assist the tester in reading log messages and diagnosing testing issues involving IKE. It is assumed the tester has some basic knowledge of IKE and VPN technologies.

The CDRouter-IKE test suite targets the testing of the IKE protocol (RFC 2409 Internet Key Exchange) and also the ESP protocol (RFC 2406 IP Encapsulating Security Payload). IKE is the keying protocol used to establish dynamic keys for IPSEC connections. The keys produced by IKE are used to encrypt and authenticate data traffic sent using ESP packets.

IKE is based on a general key management protocol called ISAKMP (RFC 2408). Some of the terminology used to test IKE comes from ISAKMP and some of the terminology comes from IKE. For simplicity, the test documentation generally refers to the protocol as IKE.

Key Exchange Modes

Phase 1 – When two IKE peers first attempt to communicate with each other, they must establish an IKE SA (Security Association). IKE supports two types of Phase 1 modes – “Main Mode” and “Aggressive Mode”. In test cases where the type of Phase 1 mode does not matter, the test case will refer to the general term “Phase 1”. A successful Phase 1 exchange will produce an IKE SA that is used to encrypt and authenticate all IKE traffic associated with a specific IKE SA.

Phase 2 – The actual IPSEC SAs (Security Associations) for ESP traffic are negotiated during the Phase 2 exchange. IKE only supports one type of Phase 2 exchange called “Quick Mode”. Test cases may refer to either Phase 2 or “Quick Mode”. A successful Phase 2 exchange will produce an IPSEC SA that is used to encrypt and authenticate all data traffic.

VPN Tunnels

A VPN Tunnel is the high level configuration provided by the user that describes the local and remote traffic that will be carried by IPSEC ESP packets. It also describes the type of encryption, authentication, and Diffie-Hellman modes for the Phase 1 and Phase 2 exchanges needed to produce the IKE SAs and IPSEC SAs.

2. Test Methodology

Initial Start-Up

CDRouter-IKE attempts to bring up any site-to-site tunnels defined in the CDRouter configuration file during the initial start-up phase. CDRouter-IKE first sends traffic on the LAN side that matches the tunnel. If the traffic matching the tunnel does not cause the tunnel to be established, CDRouter-IKE will initiate the Phase 1 exchange from the WAN.

For site-to-site tunnel testing, each test case assumes that one valid Phase 1 and Phase 2 SA exists before the test case starts. For some test cases, CDRouter will attempt to delete all existing Phase 1 and/or Phase 2 SAs. CDRouter does this by sending an Informational message with the DELETE payload.

Configuring Lifetime

CDRouter-IKE can test tunnels with various lifetime values for Phase 1 and Phase 2. However, in some situations, small tunnel lifetimes are recommended. There are a small number of test cases that will wait for Phase 1 and Phase 2 SAs initiated by the gateway to timeout. It may not always be practical to run these tests with the default SA lifetime.

Under normal operation, you should configure CDRouter with same Phase 1 and Phase 2 lifetimes as the gateway under test. In most situations the Phase 2 SA lifetime is usually shorter than the Phase 1 SA lifetime.

Not all IKE gateways all the configuration of short lifetimes. QA Cafe has found that the following sample values work well when running all the test cases in the ike.tcl module:

IKE SA Lifetime (Phase 1): 300
IPSEC SA Lifetime (Phase 2): 120

Longer lifetime values can still be used. However, the tester must be prepared to wait if the gateway initiated deletion test cases are included in the test run.

Minimum Lifetime

During some test cases, CDRouter-IKE will attempt to initiate IKE and IPSEC SAs with a very short lifetime. Some routers will not allow this and will actually set the lifetimes based on their configured values. The short lifetime values used by CDRouter can be configured using the testvars **ikeMinimumLifetime** and **ipsecMinimumLifetime**. If the

router does not support lifetimes shorter than its own configuration, these values should be set to the same values as the tunnel configuration.

Recovering IKE Tunnels

If a tunnel appears to be down, CDRouter will attempt to bring the tunnel back up using the following approach:

- Send traffic on the LAN with a destination IPv4 address that matches the tunnel
- If the tunnel is still down, attempt to initiate a new Phase 1 and Phase 2 exchange
- Include the INITIAL-CONTACT Notify Payload in the Phase 1 or Phase 2 exchange to encourage gateway to delete any existing Phase 1 and Phase 2 SAs

Switching IPSEC SAs

During several of the test cases, the IPSEC SA that is used for tunnel traffic will change. This may happen for several reasons:

- The IPSEC SA expires and the gateway under test initiates a new IPSEC SA
- CDRouter-IKE sends a DELETE payload for the IPSEC SA
- The INITIAL-CONTACT status message is sent to restart

After a Quick Mode exchange is completed, CDRouter-IKE can be configured to wait a specific amount of time before checking that a new IPSEC SA is being used. The testvar **ikeNewQuickModeDelay** should be configured with the amount of time to wait after a new Quick Mode exchange. The default value is 1000 milliseconds.

NAT-Traversal

CDRouter-IKE supports NAT-Traversal (NAT-T) based on RFC 3947 or NAT-T draft versions 00, 02, and 03. When NAT-T is enabled, CDRouter will report NAT Detection payloads that will not match either side of the IKE connection in order to force NAT-T to detect NAT and use UDP encapsulations. All of the existing test cases in the `ike.tcl` module may be run when NAT-T is enabled. There is also an additional `ike-natt.tcl` module that contains specific tests for NAT-T. These test cases may or may not force NAT to be detected. NAT-T may be enabled by selecting the NAT-T version that CDRouter-IKE will use.

Example:

```
testvar ikeNatTraversal draft-00
```

Valid values for `ikeNatTraversal` are `draft-00`, `draft-02`, `draft-03`, `rfc-3947`, and `no`.

You may test that your router interoperates with different versions of NAT-T by changing the version CDRouter-IKE will use. Some vendors support multiple versions at the same time in order to work with multiple products. CDRouter-IKE only recognizes one version of NAT-T at a time.

3.Requirements and License

In order to run CDRouter-IKE, you must have CDRouter 3.1, CDRouter-MultiPort 3.1 or newer versions installed on your CDRouter system. An update is required to your license file in order to enable the CDRouter-IKE functionality. Please follow the instructions from support@qacafe.com on how to install an updated license file that enables CDRouter-IKE.

CDRouter will report the status of IKE during its normal startup. If CDRouter-IKE is enabled, the line “IKE is enabled” will be displayed during the initial start up text.

```
Copyright (c) 2001-2007 by QA Cafe  
Built on 2007-11-05 on seagull, pktsrc version 4.0
```

```
Using license installed at: /etc/cdrouter.lic  
Registered to: qacafe  
Maintenance, Support and Upgrades until: 2008-11-01  
Licensed to run: cdrouter  
Buddyweb is enabled  
IKE is enabled  
TR69 is enabled
```

```
INFO(setup): Starting buddy Tue Nov 06 15:18:39 EST 2007  
INFO(setup): Loaded OS version Linux-2.6.22-14-generic  
INFO(setup): Loaded Tcl version 8.4.15
```

Using the buddy `-info` command, the status of IKE can also be quickly displayed:

```
# buddy -info
```

4.Configuration

Tunnel Configuration

The configuration of IKE based tunnels is similar to the existing CDRouter configuration for manual keyed IPSEC tunnels. Up to 4096 unique site-to-site IKE tunnels may be configured. Each testvar entry for a tunnel should end with the tunnel number. For example, ipsecTunnelEndPoint1, ipsecTunnelEndPoint2, ipsecTunnelEndPoint3, etc.

You can quickly comment out a tunnel in the CDRouter configuration file by commenting out the testvar ipsecTunnelEndPoint* for the tunnel. Not all of the other tunnel testvars need to be commented out to disable the tunnel.

The following table describes each entry.

| | |
|----------------------------------|--|
| ipsecTunnelEndPoint* | This value should be set to an IPv4 address that will be created by CDRouter-IKE to terminate the site-to-site tunnel. This is the same as the remote gateway value configured on the gateway under test. NOTE: This value should not be on the same network as the WAN. |
| ipsecTunnelRemoteNetwork* | This value should be set to an IPv4 network address that will be the remote end of the tunnel for the gateway under test. |
| ipsecTunnelRemoteMask* | This value should be set to the network mask for the ipsecTunnelRemoteNetwork* entry. |
| ipsecTunnelHost* | This value should be set to one example host that is contained inside of the ipsecTunnelRemoteNetwork range. The host cannot be the same as the ipsecTunnelEndPoint*. |
| ipsecTunnelKeyType* | This value should be set to 'ike' for IKE based tunnels. For a manual tunnel, this value should be set to 'manual'. Please see the CDRouter User Guide for more help with manual IPSEC tunnels. |

| | |
|--------------------------------|---|
| ipsecTunnelIkeEncrypt* | <p>This value is the Phase 1 encryption for Main Mode or Aggressive Mode. The following encryption suites are supported:</p> <ul style="list-style-type: none"> null des 3des aes-128 aes-196 aes-256 |
| ipsecTunnelIkeAuth* | <p>This value is the Phase 2 authentication type. The following authentication types are supported:</p> <ul style="list-style-type: none"> md5-hmac sha1-hmac |
| ipsecTunnelIkeGroup* | <p>This value is the Diffie-Hellman group for Phase 1. Valid group modes are:</p> <ul style="list-style-type: none"> 1 2 5 14 15 16 17 18 |
| ipsecTunnelIkeLifetime* | <p>This value is the Phase 1 SA lifetime in seconds. This value is normally longer than the Phase 2 lifetime.</p> |
| ipsecTunnelEncrypt* | <p>This value is Phase 2 encryption for Quick Mode. The following encryption suites are supported:</p> <ul style="list-style-type: none"> des 3des aes-128 aes-196 aes-256 |
| ipsecTunnelAuth* | <p>This value is the Phase 1 authentication type. The following authentication types are supported:</p> <ul style="list-style-type: none"> md5-hmac sha1-hmac |

| | |
|-----------------------------|---|
| ipsecTunnelPfsGroup* | This value is the Diffie-Hellman group for Phase 2 when PFS is enabled. Valid group modes are: 0 – no PFS 1 2 5 14 15 16 17 18 |
| ipsecTunnelLifetime* | This value is the Phase 2 SA lifetime in seconds. This value is normally shorter than the Phase 1 lifetime. |
| ipsecTunnelPsk* | This value is the pre-shared key for the site-to-site tunnel. |
| ipsecTunnelIkeMode* | This value is the Phase 1 mode, either ‘main’ or ‘aggressive’. |
| ipsecTunnelUsesNat* | Set to ‘yes’ if traffic for the tunnel is sent through NAT before being sent by IPSEC. Otherwise, set to ‘no’. |

Additional IKE Parameters

There are a few additional parameters that control the overall behavior of CDRouter-IKE.

| | |
|-----------------------------|---|
| ikeStatusInterval | This value can be used to configure the IKE status reporting interval. It defaults to 5 seconds. Set to 0 to disable the IKE status reports in the test log. |
| ikeDeadPeerDetection | Set this value to ‘yes’ if the gateway supports dead peer detection. Set to ‘no’ otherwise. |
| ikeNewQuickModeDelay | This value is the amount of time in milliseconds to wait for the gateway to switch to a new Phase 2 SA. The default is 1000 milliseconds. Under heavy loads it may be necessary to increase this value. |

| | |
|-----------------------------|--|
| ikeMinimumLifetime | This value should be configured with the minimum Phase 1 lifetime that CDRouter will attempt. It defaults to 20 seconds. Some gateways will not allow the creation of a new Phase 1 with a lifetime smaller than its own configured lifetime. In this case, the ikeMinimumLifetime should be set to be the same as the gateways normal Phase 1 lifetime. |
| ipsecMinimumLifetime | This value should be configured with the minimum Phase 2 lifetime that CDRouter will attempt. It defaults to 20 seconds. Some gateways will not allow the creation of a new Phase 2 with a lifetime smaller than its own configured lifetime. In this case, the ipsecMinimumLifetime should be set to be the same as the gateways normal Phase 2 lifetime. |
| ikePhase2DeleteDelay | This value should be configured with the number of milliseconds to wait in between deleting a list of Phase 2 SAs. The default is 100 milliseconds. This value can be adjusted if the gateway is unable to process multiple Informational DELETE messages. |
| ikeMaxTransforms | This value should be configured to the maximum number of Phase 1 Transforms that can be supported. |
| ikeMaxPhase2SA | The value should be configured to the maximum number of Phase 2 SAs that CDRouter-IKE should attempt on a single Phase 1 SA. |
| ikeInitialContact | <p>If the gateway deletes IKE and IPSEC SAs when the INITIAL-CONTACT message is received, the ikeInitialContact testvar should be set to 'yes'. Otherwise, this value should be set to 'no'. The default is 'yes'.</p> <p>When this setting in 'no' any tests that require INITIAL-CONTACT support are skipped.</p> |
| useSameIpsecTunnel | Set to 'yes' to prevent CDRouter-IKE from switching the VPN tunnel for each test case when multiple tunnels are defined. If set to 'yes', all test cases will run on the first tunnel although other tunnels may be defined. |

ikeNatTraversal

Enables CDRouter-IKE to use NAT-Traversal. This must be configured to the specific version of NAT-T to use or “no” if NAT-T should not be used. The following values are supported:

```
draft-00  
draft-02  
draft-03  
rfc-3947  
no
```

When NAT-T is enabled, CDRouter-IKE will also run the ike-natt.tcl module when selected. This module is skipped when ikeNatTraversal is set to no.

Example Configuration

```
testvar ipsecTunnelEndpoint1      5.0.0.1
testvar ipsecTunnelRemoteNetwork1 5.0.0.0
testvar ipsecTunnelRemoteMask1    255.255.255.0
testvar ipsecTunnelHost1          5.0.0.2
testvar ipsecTunnelKeyType1       ike
testvar ipsecTunnelIkeEncrypt1    des
testvar ipsecTunnelIkeAuth1       sha1-hmac
testvar ipsecTunnelIkeGroup1      1
testvar ipsecTunnelIkeLifetime1   150
testvar ipsecTunnelEncrypt1       des
testvar ipsecTunnelAuth1          sha1-hmac
testvar ipsecTunnelPfsGroup1      1
testvar ipsecTunnelLifetime1     120
testvar ipsecTunnelPsk1           qacafe123
testvar ipsecTunnelIkeModel       main
testvar ipsecTunnelUsesNat1       yes
```

Configuration of local subnet for site-to-site tunnels

When configuring site-to-site tunnels on the gateway under test, the local protected subnet should be the same as the local LAN network on the gateway under test. CDRouter-IKE will automatically create a security profile from the remote network to the local subnet on the LAN.

If NAT is also applied to the IPSEC tunnel, CDRouter will create a security protocol from the remote network to the assigned WAN IP address.

Log Messages

CDRouter-IKE protocol messages can be filtered out using the `--show` and `--hide` options from the command-line. The following protocols are specific to CDRouter-IKE:

| | |
|-------|--------------------------------------|
| IKE | All IKE protocol messages |
| DH | All Diffie-Hellman relaxed messages. |
| IPSEC | IPSEC messages and events |

IKE SA Status

By default, CDRouter-IKE will show the status of all IKE and IPSEC SAs for each tunnel every 5 seconds when protocol tracing is enabled (`-trace`). This interval can be configured

using the testvar `ikeStatusInterval`. Setting the `ikeStatusInterval` to 0 will completely disable the IKE status reports.

```
INFO (vpnServer) : 18:11:53 | ----- IKE status -----  
INFO (vpnServer) : 18:11:53 | IKE SA: 1: 9b0338d0ea406c33:cf5194d871a42523 (R)  
INFO (vpnServer) : 18:11:53 | tun_0: 60cdebb9 -> aa49ed3c:1150ca45 (R)  
INFO (vpnServer) : 18:11:53 | -----
```

The IKE status report shows all Phase 1 SAs (IKE SA) and all the Phase 2 SAs associated with it. If CDRouter-IKE initiated the SA the status is shown as (I). If the gateway under test initiated the SA the status is shown as (R).

5. Testing Exercises

The CDRouter-IKE test suite can be run through several different configurations. The following test scenarios are recommended.

Main Mode and Aggressive Mode

If the gateway under test supports both Main Mode and Aggressive Mode, we recommend running the test suite with a configuration for Main Mode and a configuration for Aggressive Mode. When running in Aggressive Mode, test cases that do not apply will be skipped. You may also consider running a configuration with multiple tunnels that includes both main mode and aggressive mode.

Wireless and Wired Interfaces

Both wired and wireless LAN interfaces should be used when running CDRouter-IKE. QA Cafe has seen issues where some routers send wireless traffic in the clear when IKE site-to-site tunnels are down.

Multiple Tunnels

Multiple tunnels can be configured on the gateway under test. When multiple tunnels exist, CDRouter-IKE will cycle through each tunnel when running each test case. For example, if 2 tunnels are defined and the user executes tests `ike_1`, `ike_2`, and `ike_4`, the first test (`ike_1`) will run using tunnel 1. The second test (`ike_2`) will be run using tunnel 2. The last test (`ike_4`) will be run using tunnel 3.

This behavior can be disabled by configuring the testvar `useSameIpssecTunnel` to yes. When testvars `useSameIpssecTunnel` is set to yes, all `ike.tcl` test cases will be run against the first tunnel in the configuration file. CDRouter will still respond to any IKE messages on the additional tunnels, but they will not be used for specific test cases.

Application Testing

If the gateway supports NAT over site-to-site tunnels, existing application tests may be run over the site-to-site tunnels by configuring the testvar `remoteHostIp` within the same range as the `ipsecTunnelRemoteNetwork`. The `remoteHostIp` must be different from the `ipsecTunnelEndPoint` and `ipsecTunnelHost`.

NOTE: When running any application modules over any IPSEC tunnel, you should check that the testvars **lanMtu** and testvar **mssClampingValue** are set to the expected values. If the gateway supports fragmentation of IPSEC packets, then the default value of lanMtu should be fine. IPSEC fragmentation can be minimized by dropping the value of lanMtu.

Multiple Transforms

By configuring multiple tunnels, multiple transforms can be run during a single test run. For example, tunnel 1 may be configured with AES-256+SHA1, tunnel 2 may be configured with 3DES+MD5, etc. CDRouter supports thousands of different tunnel configurations due to the number of encryption, authentication, and Diffie-Hellman groups that are supported.

Running the ESP test module (ipsec-esp.tcl)

The base version of CDRouter and CDRouter-MultiPort contain the ipsec-esp.tcl module which can also be run using IKE based tunnels. This test module includes tests specific to the ESP protocol. When IKE is enabled, some of the ipsec-esp.tcl test cases specific to Manual IPSEC tunnels are skipped.

Long duration testing

Aside running through the ike.tcl module one time per test run, it is recommended to set up long duration test runs of the ike.tcl module using the `-repeat` option or a BuddyWeb package with repeat enabled. Since many of the values used by IKE are random in nature, longer duration runs will verify that the gateway continues to operate correctly over time.

Frequent IKE Re-Keying

Another recommended exercise is to stress the number of IKE re-key attempts on the router. This can be done by running test case `ike_2` repeatedly. Another good candidate test case is `ike_14`.

Different NAT-T Versions

It is recommended to try all of the supported CDRouter-IKE NAT-T versions even if the device under test only supports a specific version. The main ike.tcl module should still run successfully even when NAT-T is not recognized. Unfortunately, several versions of NAT-T exist in the field and many are not backwards compatible with the first draft version.

6.Possible Problems

Certain IKE behavior issues can have a ripple effect on CDRouter-IKE testing. Rather than restarting the VPN gateway before each test, CDRouter-IKE brings the VPN gateway through a series of exercises. A failure in one of the test cases can lead to cascading failures. It can be difficult for CDRouter to recover if the active IKE and IPSEC SAs get out of sync between CDRouter and the gateway under test. The following examples mention some of the possible problems and possible work-arounds.

PROBLEM: IKE or IPSEC SAs not deleted with DELETE message

If a gateway does not correctly handle deleting IKE and IPSEC SAs using an Informational message, CDRouter-IKE and the VPN gateway will not agree on the SAs that exists. Unfortunately, some gateways incorrectly process a DELETE message for IKE SAs and occasionally drop IKE messages. If these problems occur SAs may not get deleted. This problem is usually easy to detect since CDRouter-IKE will delete all of its active IKE and IPSEC SAs, but the gateway may still initiate a new Quick Mode thinking it has a valid IKE SA. CDRouter will log a message that the IKE SA does not exist.

Work-around:

To work around this type of problem, try running each test one at a time after restarting the gateway. Another potential work around is to use a long delay in-between each test to let all SAs expire before each test starts. This can be done using the `-delay` option in buddy or when building a BuddyWeb test package.

If this problem is only experienced with a specific test case, it may be desirable to add a delay for a single test case. See the qacafe.com Knowledge Base note for more information: <http://www.qacafe.com/help/question.php?qstId=100>.

PROBLEM: Gateway reports MALFORMED-PAYLOAD

Often a problem with the encryption keys can lead to a MALFORMED-PAYLOAD error. This may only occur occasionally and disappear in the next Phase 1 or Phase 2 exchange.

Work-around:

Verify that the router correctly handles Diffie-Hellman keys with leading zeros using test cases ike_365 and ike_366. This is a common cause of mismatched encryption keys.

7. More Help

For more information on CDRouter and a listing of CDRouter-IKE test cases, please visit the CDRouter-IKE page at <http://www.qacafe.com/show/ike>.

For general help running CDRouter, please check the CDRouter User Guide on-line at <http://www.qacafe.com/cdrouter>

Additional support notes on IKE can be found in the QA Cafe knowledge base at <http://www.qacafe.com/help>

For additional help, contact support@qacafe.com