Lobotomo
Software

IPSecuritas 3.x

Configuration Instructions

for

Netgear FVS114
Netgear FVS328
Netgear FVX538

June 17, 2009

Legal Disclaimer

Contents
Lobotomo Software (subsequently called "Author") reserves the right not to be responsible for the topicality, correctness, completeness or quality of the information provided. Liability claims regarding damage caused by the use of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected. All offers are not-binding and without obligation. Parts of the document or the complete publication including all offers and information might be extended, changed or partly or completely deleted by the author without separate announcement.

Referrals
The author is not responsible for any contents referred to or any links to pages of the World Wide Web in this document. If any damage occurs by the use of information presented there, only the author of the respective documents or pages might be liable, not the one who has referred or linked to these documents or pages.

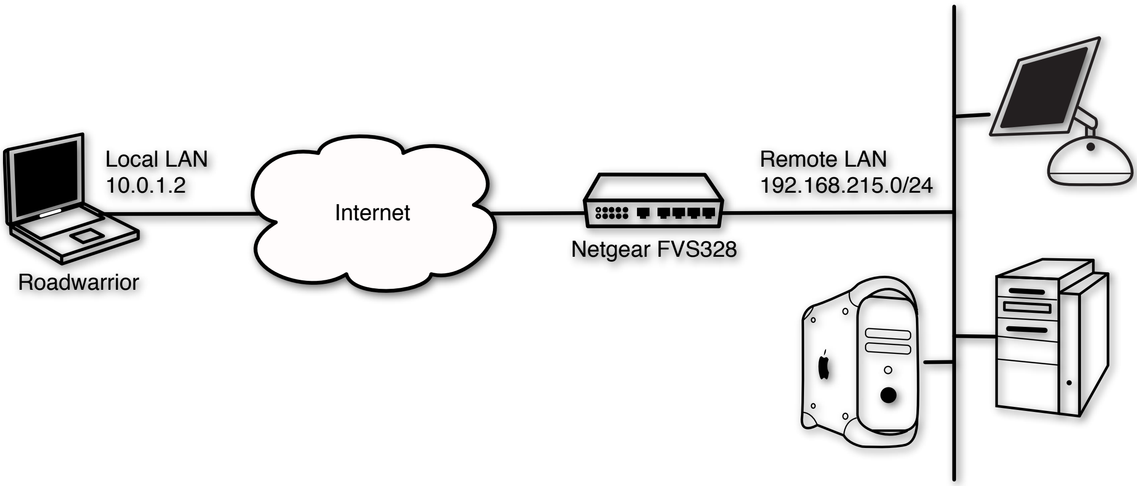
Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic or printed publications is not permitted without the author's agreement.

Legal force of this disclaimer
This disclaimer is to be regarded as part of this document. If sections or individual formulations of this text are not legal or correct, the content or validity of the other parts remain uninfluenced by this fact.

Table of contents

Introduction

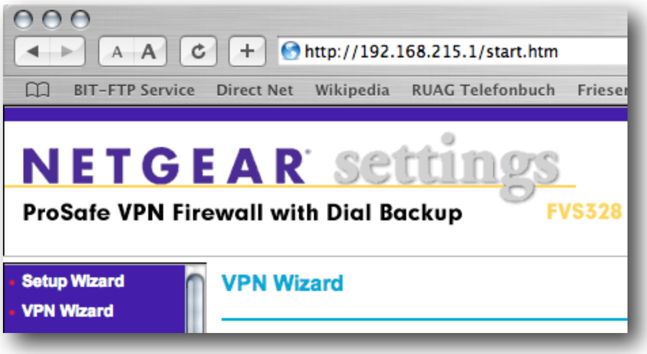
This document describes the steps necessary to establish a protected VPN connection between a Mac client and a Netgear FVS328 router/firewall. All information in this document is based on the following assumed network.



- Netgear FVS328 Wizard Setup

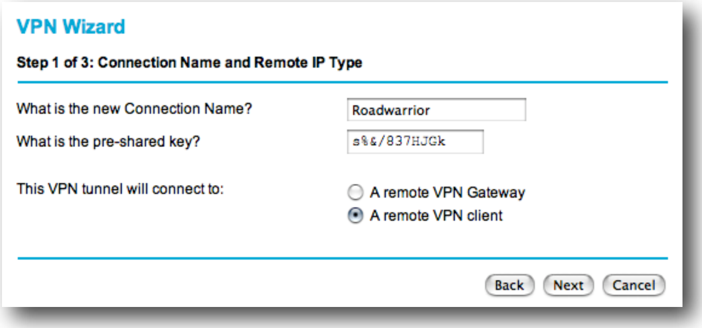
This section describes the necessary steps to setup the FVS328 to accept incoming connections.

Start VPN Wizard



Open a web browser and connect to your Netgear router. Enter the administrator's user name (usually admin) and password. On the left side, select **VPN Wizard**. Click on the **Next** button.

Enter Name and Preshared Key



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name? Roadwarrior

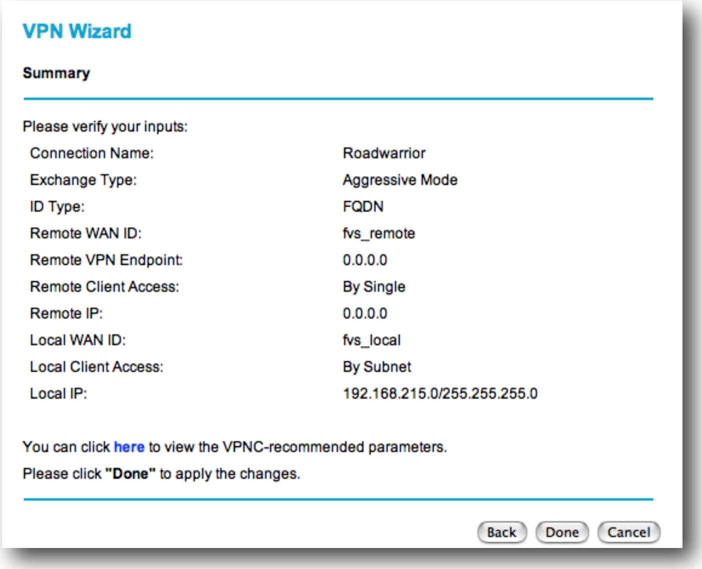
What is the pre-shared key? s%&/837HJGk

This VPN tunnel will connect to:
○ A remote VPN Gateway
● A remote VPN client

Enter a name (any arbitrary name) and the preshared key. The preshared key is used to encrypt the messages in the connection negotiations. Please choose a safe key (don't use the example on the left).
Set the connection endpoint to **A remote VPN client**.

Click on **Next**.

Finish the Wizard



VPN Wizard

Summary

Please verify your inputs:

Connection Name:	Roadwarrior
Exchange Type:	Aggressive Mode
ID Type:	FQDN
Remote WAN ID:	fvs_remote
Remote VPN Endpoint:	0.0.0.0
Remote Client Access:	By Single
Remote IP:	0.0.0.0
Local WAN ID:	fvs_local
Local Client Access:	By Subnet
Local IP:	192.168.215.0/255.255.255.0

You can click here to view the VPNC-recommended parameters.

Please click **"Done"** to apply the changes.

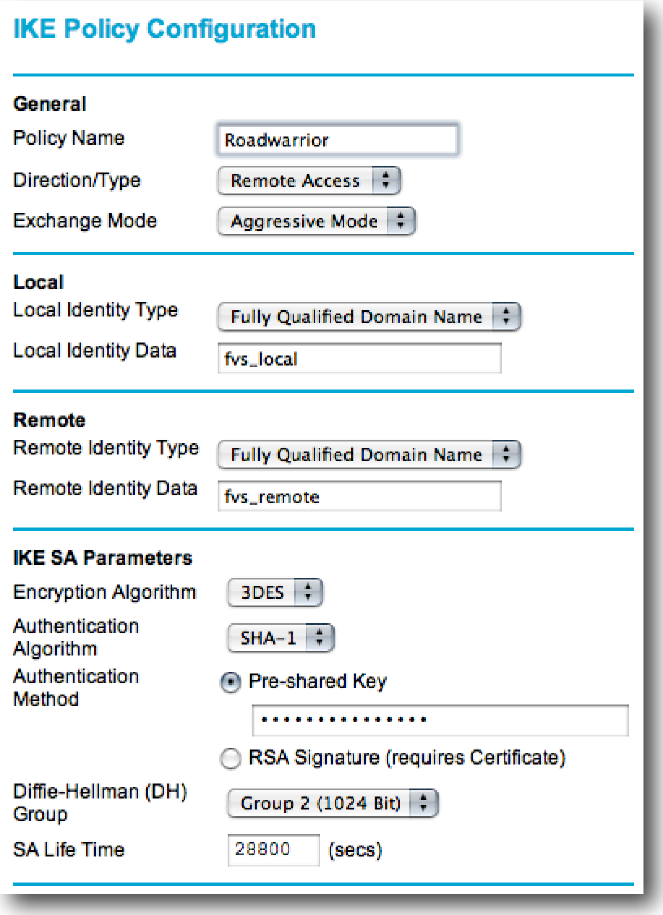
Check if all of your information is correct. The Local IP should correspond to your local LAN address.

Click on **Done** if all settings are correct.

Netgear FVS328 Manual Setup

This section describes the manual setup of the FVS328 in case you don‘t want to use the VPN wizard. Please keep in mind that the seetings in IPSecuritas also need to be adjusted in case your manual settings differ from the one described here.

IKE Policy



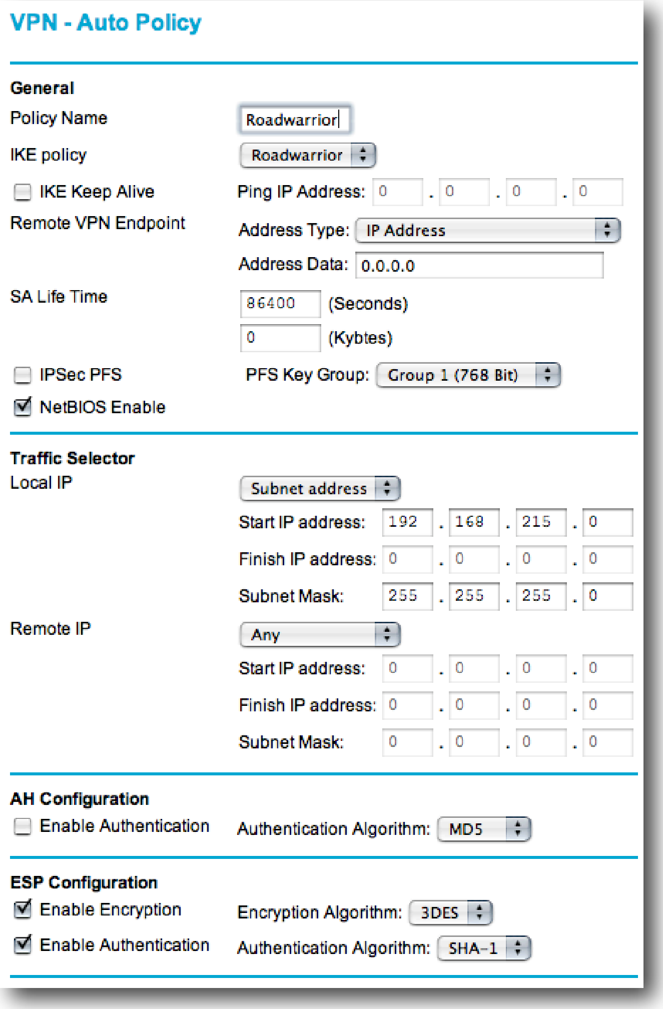
IKE Policy Configuration

General	
Policy Name	Roadwarrior
Direction/Type	Remote Access
Exchange Mode	Aggressive Mode
Local	
Local Identity Type	Fully Qualified Domain Name
Local Identity Data	fvs_local
Remote	
Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	fvs_remote
IKE SA Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	● Pre-shared Key ••••••••••••••• ○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	28800 (secs)

Create a new IKE Policy and enter the information shown on the left side (please choose a safe preshared key that is hard to guess).

Click on **Apply** to save the settings.

VPN Policy



VPN - Auto Policy

General

Policy Name: Roadwarrior

IKE policy: Roadwarrior

□ IKE Keep Alive — Ping IP Address: 0 . 0 . 0 . 0

Remote VPN Endpoint — Address Type: IP Address; Address Data: 0.0.0.0

SA Life Time: 86400 (Seconds); 0 (Kybtes)

□ IPSec PFS — PFS Key Group: Group 1 (768 Bit)

☑ NetBIOS Enable

Traffic Selector

Local IP: Subnet address
Start IP address: 192 . 168 . 215 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0

Remote IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

□ Enable Authentication — Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption — Encryption Algorithm: 3DES

☑ Enable Authentication — Authentication Algorithm: SHA-1

Create a new VPN Policy and enter the information shown on the left side. Adjust the **Local IP** to match your local IP network address and netmask.

Click on **Apply** to save the settings.

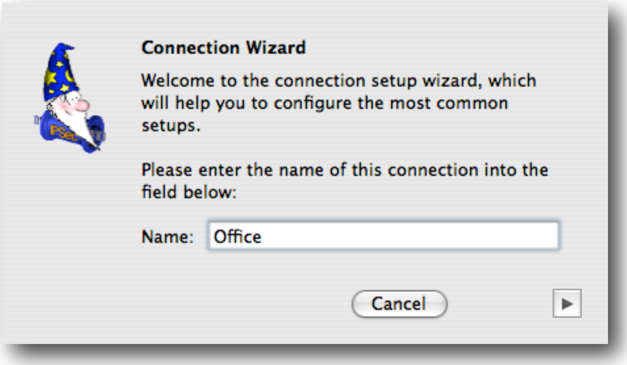
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the FVS328 router.

Start Wizard

Unless it is already running, you should start IPSecuritas now. Change to **Connections** menu and select **Edit Connections** (or press ⌘-E). Start the Wizard by clicking on the following symbol:

Enter Name of New Connection



Connection Wizard

Welcome to the connection setup wizard, which will help you to configure the most common setups.

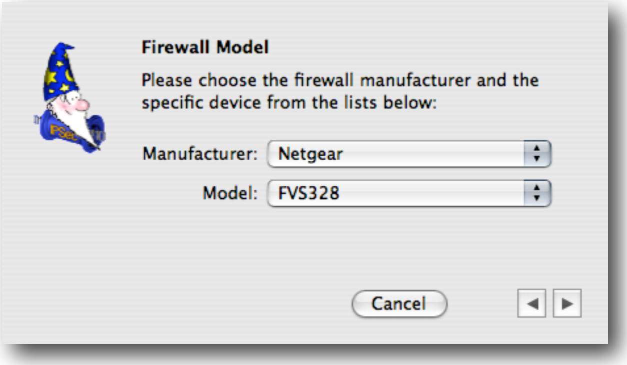
Please enter the name of this connection into the field below:

Name: Office

Enter a name for the connection (any arbitrary name).

Click on the right arrow to continue with the next step.

Select Router Model



Firewall Model

Please choose the firewall manufacturer and the specific device from the lists below:

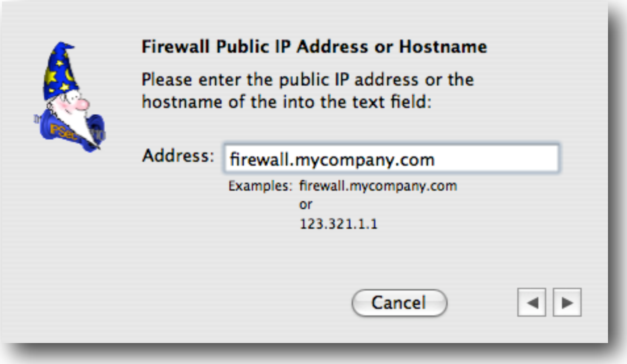
Manufacturer: Netgear

Model: FVS328

Select **Netgear** from the manufacturer list and **FVS328** (or **FVS114**) from the model list.

Click on the right arrow to continue with the next step.

Enter Router's Public IP Address



Firewall Public IP Address or Hostname

Please enter the public IP address or the hostname of the into the text field:

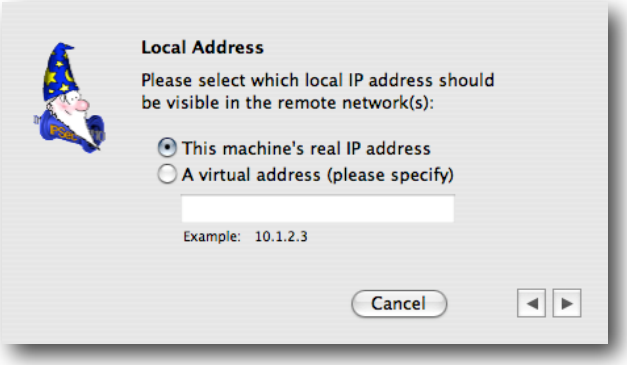
Address: firewall.mycompany.com

Examples: firewall.mycompany.com
or
123.321.1.1

Enter the public IP address or hostname of your Netgear FVS328 router. In case your ISP assigned you a dynamic IP address, you should register with a dynamic IP DNS service (like http://www.dyndns.org).

Click on the right arrow to continue with the next step.

Enter a Virtual IP Address



Local Address

Please select which local IP address should be visible in the remote network(s):

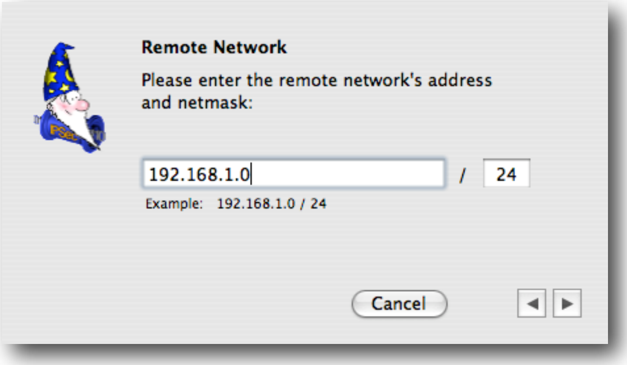
● This machine's real IP address
○ A virtual address (please specify)

Example: 10.1.2.3

Enter a virtual local IP address. This address appears as the source address of any packet going through the tunnel. If no address is specified, the real local IP address is used instead.
In order to prevent address collisions between the local network and the remote network, it is recommended to use an address from one the ranges reserved for private network (see **RFC 1918**).

Click on the right arrow to continue with the next step.

Enter Remote Network



Remote Network

Please enter the remote network's address and netmask:

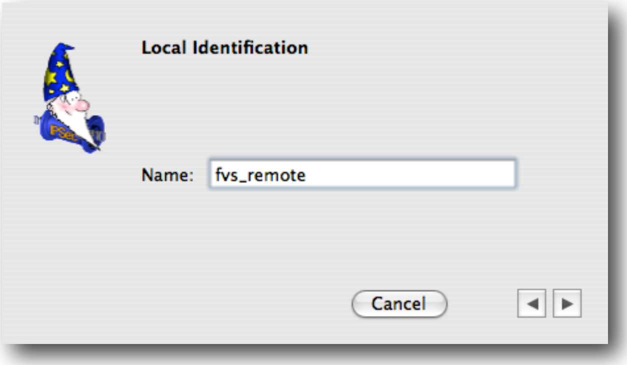
192.168.1.0 / 24

Example: 192.168.1.0 / 24

Enter the remote network address and netmask (please note that the netmask needs to be entered in **CIDR** format). This has to match with the settings of the FVS328.

Click on the right arrow to continue with the next step.

Enter Local Identification



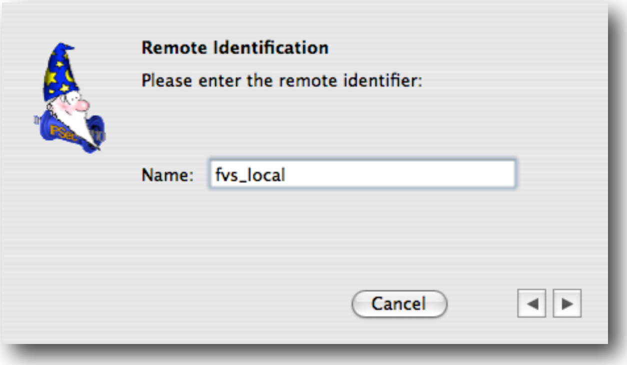
Local Identification

Name: fvs_remote

Enter the FVS328's local identification (which is **fvs_remote** by default if you used the FVS328's wizard).

Click on the right arrow to continue with the next step.

Enter Remote Identification


Remote Identification

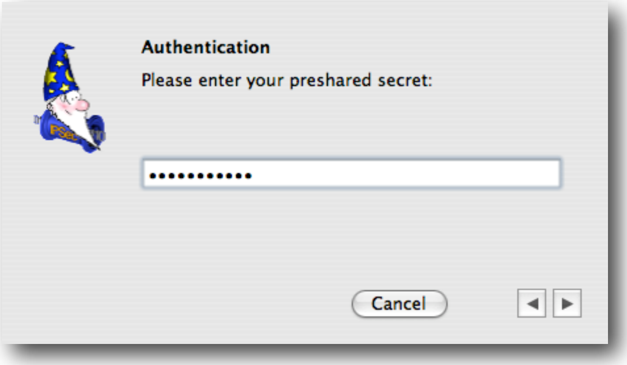
Please enter the remote identifier:

Name: fvs_local

Enter the FVS328's remote identification (which is **fvs_local** by default if you used the FVS328's wizard).

Click on the right arrow to continue with the next step.

Enter Preshared Key


Authentication

Please enter your preshared secret:

•••••••••••

Enter the same **Preshared Key** that you used for the FVS328.

Click on the right arrow to finish the connection setup.

Diagnosis

Reachability Test

To test reachability of the remote host, open an **Terminal Window** (Utilities -> Terminal) and enter the command **ping**, followed by the FVS328 **local IP address**. If the tunnel works correctly, a similar output is displayed:

```
[MacBook:~] root# ping 192.168.215.1
PING 192.168.215.1 (192.168.215.1): 56 data bytes
64 bytes from 192.168.215.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 192.168.215.1: icmp_seq=1 ttl=64 time=19.290 ms
64 bytes from 192.168.215.1: icmp_seq=2 ttl=64 time=12.823 ms
```

Sample FVS328 Log Output

The following is a sample log file from IPSecuritas after a successful connection establishment:

```
[2007-01-02 01:47:36][==== IKE PHASE 1(from 80.218.148.110) START (responder) ====]
[2007-01-02 01:47:36]**** RECEIVED  FIRST MESSAGE OF AGGR MODE ****
[2007-01-02 01:47:36]<POLICY: > PAYLOADS: SA,PROP,TRANS,KE,NONCE,ID,VID
[2007-01-02 01:47:36]<LocalRID> Type=ID_FQDN,ID Data=fvs_remote
[2007-01-02 01:47:36]<RemoteLID> Type=ID_FQDN,ID Data=fvs_remote
[2007-01-02 01:47:37]<POLICY: Roadwarrior> PAYLOADS: SA,PROP,TRANS,KE,NONCE,ID,HASH
[2007-01-02 01:47:37]**** SENT OUT SECOND MESSAGE OF AGGR MODE ****
[2007-01-02 01:47:37]**** RECEIVED  THIRD MESSAGE OF AGGR MODE ****
[2007-01-02 01:47:37]<POLICY: Roadwarrior> PAYLOADS: HASH
[2007-01-02 01:47:37]**** AGGR MODE COMPLETED ****
```

```
[2007-01-02 01:47:37][==== IKE PHASE 1 ESTABLISHED====]
[2007-01-02 01:47:37]**** SENT OUT INFORMATIONAL EXCHANGE MESSAGE(DELETE_PAYLOAD) ****
[2007-01-02 01:47:38][==== IKE PHASE 2(from 80.218.148.110) START (responder) ====]
[2007-01-02 01:47:38]**** RECEIVED  FIRST MESSAGE OF QUICK MODE ****
[2007-01-02 01:47:38]**** FOUND IDs,EXTRACE ID INFO ****
[2007-01-02 01:47:38]<Initiator IPADDR=10.0.1.2>
[2007-01-02 01:47:38]<Responder IPADDR=192.168.215.0 MASK=255.255.255.0>
[2007-01-02 01:47:38]**** SENT OUT SECOND MESSAGE OF QUICK MODE ****
[2007-01-02 01:47:38]**** RECEIVED  THIRD MESSAGE OF QUICK MODE ****
[2007-01-02 01:47:39]<POLICY: Roadwarrior> PAYLOADS: HASH
[2007-01-02 01:47:39]**** QUICK MODE COMPLETED ****
[2007-01-02 01:47:39][==== IKE PHASE 2 ESTABLISHED====]
```

Sample IPSecuritas Log Output

The following is a sample log file from the FVS328 after a successful connection establishment (with log level set to **Debug**):

```
IPSecuritas 3.0rc build 1046, Thu Dec 21 23:28:29 CET 2006, nadig
Darwin 8.8.3 Darwin Kernel Version 8.8.3: Wed Oct 18 21:57:10 PDT 2006; root:xnu-792.15.4.obj~4/RELEASE_I386 i386

Jan 02, 01:41:18  Info     APP  IKE daemon started
Jan 02, 01:41:18  Info     APP  IPSec started
Jan 02, 01:41:18  Debug    APP  State change from IDLE to RUNNING after event START
Jan 02, 01:41:18  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Jan 02, 01:41:18  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Jan 02, 01:41:18  Info     IKE  Foreground mode.
Jan 02, 01:41:18  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
Jan 02, 01:41:18  Info     IKE  @(#)This product linked OpenSSL 0.9.7i 14 Oct 2005 (http://www.openssl.org/)
Jan 02, 01:41:18  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
Jan 02, 01:41:18  Info     IKE  Resize address pool from 0 to 255
Jan 02, 01:41:18  Debug    IKE  lifetime = 12960000
Jan 02, 01:41:18  Debug    IKE  lifebyte = 0
Jan 02, 01:41:18  Debug    IKE  encklen=0
Jan 02, 01:41:18  Debug    IKE  p:1 t:1
Jan 02, 01:41:18  Debug    IKE  3DES-CBC(5)
Jan 02, 01:41:18  Debug    IKE  SHA(2)
Jan 02, 01:41:18  Debug    IKE  1024-bit MODP group(2)
Jan 02, 01:41:18  Debug    IKE  pre-shared key(1)
Jan 02, 01:41:18  Debug    IKE
Jan 02, 01:41:18  Debug    IKE  hmac(modp1024)
Jan 02, 01:41:18  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
Jan 02, 01:41:18  Debug    IKE  parse successed.
Jan 02, 01:41:18  Info     IKE  10.0.1.2[4500] used as isakmp port (fd=6)
Jan 02, 01:41:18  Info     IKE  10.0.1.2[500] used as isakmp port (fd=7)
Jan 02, 01:41:18  Debug    IKE  get pfkey X_SPDDUMP message
Jan 02, 01:41:18  Debug    IKE
Jan 02, 01:41:18  Debug    IKE  02120000 0f000100 01000000 7f0e0000 03000500 ff180000 10020000 c0a8d700
Jan 02, 01:41:18  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 0a000102 00000000 00000000
Jan 02, 01:41:18  Debug    IKE  07001200 02000100 d6000000 00000000 28003200 02020000 10020000 544a5a6e
Jan 02, 01:41:18  Debug    IKE  00000000 00000000 10020000 0a000102 00000000 00000000
Jan 02, 01:41:18  Debug    IKE  get pfkey X_SPDDUMP message
Jan 02, 01:41:18  Debug    IKE
Jan 02, 01:41:18  Debug    IKE  02120000 0f000100 00000000 7f0e0000 03000500 ff200000 10020000 0a000102
Jan 02, 01:41:18  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 c0a8d700 00000000 00000000
Jan 02, 01:41:18  Debug    IKE  07001200 02000200 d5000000 00000000 28003200 02020000 10020000 0a000102
Jan 02, 01:41:18  Debug    IKE  00000000 00000000 10020000 544a5a6e 00000000 00000000
Jan 02, 01:41:18  Debug    IKE  sub:0xbffff5d4: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 02, 01:41:18  Debug    IKE  db :0x308c88: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 02, 01:41:19  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netgear FVS328
Jan 02, 01:41:19  Debug    IKE  get pfkey ACQUIRE message
Jan 02, 01:41:19  Debug    IKE
Jan 02, 01:41:19  Debug    IKE  02060003 26000000 6a000000 00000000 03000500 ff200000 10020000 0a000102
Jan 02, 01:41:19  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 544a5a6e 00000000 00000000
Jan 02, 01:41:19  Debug    IKE  02001200 02000200 d5000000 00000000 1c000d00 20000000 00030000 00000000
Jan 02, 01:41:19  Debug    IKE  00010008 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Jan 02, 01:41:19  Debug    IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
Jan 02, 01:41:19  Debug    IKE  00040000 00000000 0001c001 00000000 01000000 01000000 00000000 00000000
Jan 02, 01:41:19  Debug    IKE  00000000 00000000 00000000 00000000 80510100 00000000 80700000 00000000
Jan 02, 01:41:19  Debug    IKE  00000000 00000000 000c0000 00000000 00010001 00000000 01000000 01000000
Jan 02, 01:41:19  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Jan 02, 01:41:19  Debug    IKE  80700000 00000000 00000000 00000000
Jan 02, 01:41:19  Debug    IKE  suitable outbound SP found: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out.
Jan 02, 01:41:19  Debug    IKE  sub:0xbffff5c0: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 02, 01:41:19  Debug    IKE  db :0x308c88: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 02, 01:41:19  Debug    IKE  suitable inbound SP found: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in.
Jan 02, 01:41:19  Debug    IKE  new acquire 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 02, 01:41:19  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 02, 01:41:19  Debug    IKE  (trns_id=DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:19  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:19  Debug    IKE  in post_acquire
Jan 02, 01:41:19  Debug    IKE  configuration found for 84.74.90.110.
Jan 02, 01:41:19  Info     IKE  IPsec-SA request for 84.74.90.110 queued due to no phase1 found.
Jan 02, 01:41:19  Debug    IKE  ===
Jan 02, 01:41:19  Info     IKE  initiate new phase 1 negotiation: 10.0.1.2[500]<=>84.74.90.110[500]
Jan 02, 01:41:19  Info     IKE  begin Aggressive mode.
Jan 02, 01:41:19  Debug    IKE  new cookie:
Jan 02, 01:41:19  Debug    IKE  378e09d248e961b0
Jan 02, 01:41:19  Debug    IKE  use ID type of FQDN
Jan 02, 01:41:19  Debug    IKE  compute DH's private.
Jan 02, 01:41:19  Debug    IKE
Jan 02, 01:41:19  Debug    IKE  4c85c4b9 4aaa12ef 97484236 12de4331 806e60ab 762aaf19 7f16f264 f257bce7
Jan 02, 01:41:19  Debug    IKE  8fd547c0 1e967320 72de82c1 4d8a94f7 05e4f44d 91bcb6bf 247f90b3 c40503ea
Jan 02, 01:41:19  Debug    IKE  2c9e8da5 a799385e 3225c66f 7a88024c 4da78234 9d106522 b931cb31 bc59ad6d
Jan 02, 01:41:19  Debug    IKE  8aecc2bf 4a0e1c10 7eac7eeb 2a993036 e7206164 cd6f1bee 4a2301a9 dec29fc1
Jan 02, 01:41:19  Debug    IKE  compute DH's public.
Jan 02, 01:41:19  Debug    IKE
Jan 02, 01:41:19  Debug    IKE  26ad23d7 8827b03f b3f4c5f3 8f231b96 57c93193 2c5dc991 a94e1d6d 0363ffb3
Jan 02, 01:41:19  Debug    IKE  e03cb46e a7a0de25 5c068566 5e6b89da f717e8d6 fa7f5451 a2bb96e3 4e023827
Jan 02, 01:41:19  Debug    IKE  25ee8e37 61deb1c9 f89f47ca fbc67ea0 4cd216a7 ba041abd 721dcd87 10af7920
Jan 02, 01:41:19  Debug    IKE  a415a472 218c5c27 85fafbb2 3a351705 9ad8c308 60d10eeb c8c31c22 978c2f66
Jan 02, 01:41:19  Debug    IKE  authmethod is pre-shared key
Jan 02, 01:41:19  Debug    IKE  add payload of len 52, next type 4
Jan 02, 01:41:19  Debug    IKE  add payload of len 128, next type 10
Jan 02, 01:41:19  Debug    IKE  add payload of len 16, next type 5
Jan 02, 01:41:19  Debug    IKE  add payload of len 14, next type 13
Jan 02, 01:41:19  Debug    IKE  add payload of len 16, next type 0
Jan 02, 01:41:19  Debug    IKE  274 bytes from 10.0.1.2[500] to 84.74.90.110[500]
Jan 02, 01:41:19  Debug    IKE  sockname 10.0.1.2[500]
Jan 02, 01:41:19  Debug    IKE  send packet from 10.0.1.2[500]
Jan 02, 01:41:19  Debug    IKE  send packet to 84.74.90.110[500]
Jan 02, 01:41:19  Debug    IKE  1 times of 274 bytes message will be sent to 84.74.90.110[500]
Jan 02, 01:41:19  Debug    IKE
Jan 02, 01:41:19  Debug    IKE  378e09d2 48e961b0 00000000 00000000 01100400 00000000 00000112 04000038
Jan 02, 01:41:19  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Jan 02, 01:41:19  Debug    IKE  00c5c100 80010005 80030001 80020002 80040002 0a000084 26ad23d7 8827b03f
Jan 02, 01:41:19  Debug    IKE  b3f4c5f3 8f231b96 57c93193 2c5dc991 a94e1d6d 0363ffb3 e03cb46e a7a0de25
Jan 02, 01:41:19  Debug    IKE  5c068566 5e6b89da f717e8d6 fa7f5451 a2bb96e3 4e023827 25ee8e37 61deb1c9
Jan 02, 01:41:19  Debug    IKE  f89f47ca fbc67ea0 4cd216a7 ba041abd 721dcd87 10af7920 a415a472 218c5c27
Jan 02, 01:41:19  Debug    IKE  85fafbb2 3a351705 9ad8c308 60d10eeb c8c31c22 978c2f66 05000014 b17b8482
Jan 02, 01:41:19  Debug    IKE  1afbd802 960e7bf2 59bd6cc6 0d000012 02000000 6676735f 72656d6f 74650000
Jan 02, 01:41:19  Debug    IKE  0014afca d71368a1 f1c96b86 96fc7757 0100
Jan 02, 01:41:19  Debug    IKE  resend phase1 packet 378e09d248e961b0:0000000000000000
Jan 02, 01:41:20  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netgear FVS328
Jan 02, 01:41:20  Debug    IKE  ===
Jan 02, 01:41:20  Debug    IKE  269 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 01100400 00000000 0000010d 04000038
Jan 02, 01:41:20  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Jan 02, 01:41:20  Debug    IKE  00c5c100 80010005 80030001 80020002 80040002 0a000084 19bd2774 8455d533
Jan 02, 01:41:20  Debug    IKE  45b6a9ff 6594dc0b 74c100c2 5b04712e 2515164a dee2a011 47399961 3b1de1a1
Jan 02, 01:41:20  Debug    IKE  14e9fd0e 3cb07a05 02d220a9 0d9862a0 2c42adb3 71359c52 04dbe3f3 99d4a3fd
Jan 02, 01:41:20  Debug    IKE  39ed2352 1db6b0e3 d4d19ed7 3698fdd1 7a8fc0b5 a93d01ec 40f6fd53 47459ed2
Jan 02, 01:41:20  Debug    IKE  bffd8804 f23c5461 e49da47a 0176b3d9 f8e0ba3e 8ae31c52 0500000c e7873f8f
Jan 02, 01:41:20  Debug    IKE  75038989 08000011 02000000 6676735f 6c6f6361 6c000000 1866bbd8 f9259d17
Jan 02, 01:41:20  Debug    IKE  c6829af2 9e148eeb 601b55da 98
Jan 02, 01:41:20  Debug    IKE  begin.
Jan 02, 01:41:20  Debug    IKE  seen nptype=1(sa)
Jan 02, 01:41:20  Debug    IKE  seen nptype=4(ke)
Jan 02, 01:41:20  Debug    IKE  seen nptype=10(nonce)
Jan 02, 01:41:20  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:20  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:20  Debug    IKE  succeed.
Jan 02, 01:41:20  Debug    IKE  total SA len=52
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Jan 02, 01:41:20  Debug    IKE  00c5c100 80010005 80030001 80020002 80040002
Jan 02, 01:41:20  Debug    IKE  begin.
Jan 02, 01:41:20  Debug    IKE  seen nptype=2(prop)
Jan 02, 01:41:20  Debug    IKE  succeed.
Jan 02, 01:41:20  Debug    IKE  proposal #1 len=44
Jan 02, 01:41:20  Debug    IKE  begin.
Jan 02, 01:41:20  Debug    IKE  seen nptype=3(trns)
Jan 02, 01:41:20  Debug    IKE  succeed.
Jan 02, 01:41:20  Debug    IKE  transform #1 len=36
Jan 02, 01:41:20  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:20  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Jan 02, 01:41:20  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Jan 02, 01:41:20  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Jan 02, 01:41:20  Debug    IKE  hash(sha1)
Jan 02, 01:41:20  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Jan 02, 01:41:20  Debug    IKE  hmac(modp1024)
Jan 02, 01:41:20  Debug    IKE  pair 1:
Jan 02, 01:41:20  Debug    IKE  0x308c40: next=0x0 tnext=0x0
Jan 02, 01:41:20  Debug    IKE  proposal #1: 1 transform
Jan 02, 01:41:20  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
Jan 02, 01:41:20  Debug    IKE  trns#=1, trns-id=IKE
Jan 02, 01:41:20  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:20  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Jan 02, 01:41:20  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Jan 02, 01:41:20  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Jan 02, 01:41:20  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Jan 02, 01:41:20  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Jan 02, 01:41:20  Debug    IKE  Compared: DB:Peer
Jan 02, 01:41:20  Debug    IKE  (lifetime = 12960000:12960000)
Jan 02, 01:41:20  Debug    IKE  (lifebyte = 0:0)
Jan 02, 01:41:20  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
Jan 02, 01:41:20  Debug    IKE  (encklen = 0:0)
Jan 02, 01:41:20  Debug    IKE  hashtype = SHA:SHA
Jan 02, 01:41:20  Debug    IKE  authmethod = pre-shared key:pre-shared key
Jan 02, 01:41:20  Debug    IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
Jan 02, 01:41:20  Debug    IKE  an acceptable proposal found.
Jan 02, 01:41:20  Debug    IKE  hmac(modp1024)
Jan 02, 01:41:20  Debug    IKE  agreed on pre-shared key auth.
Jan 02, 01:41:20  Debug    IKE  compute DH's shared.
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  4e000c8d f8b74330 fa11cf03 502a745e 59fb980d 49e14645 cd9882f2 caa9dbfa
Jan 02, 01:41:20  Debug    IKE  13ea1105 713b66de 3d02a3f8 e28931e7 512d1bd4 78ac673b 0cf4e919 c0558bbc
Jan 02, 01:41:20  Debug    IKE  78de62be 831f0788 9f331565 cb38fc0b a73c72f6 ce407a76 edd34964 921a1ba0
Jan 02, 01:41:20  Debug    IKE  ea85f940 65b4d12e 593d8036 2fc79cfe 9d4319c6 8cc87ce4 91554069 f934a57a
Jan 02, 01:41:20  Debug    IKE  the psk found.
Jan 02, 01:41:20  Debug    IKE  psk: 2007-01-02 01:41:20: DEBUG2:
Jan 02, 01:41:20  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
Jan 02, 01:41:20  Debug    IKE  nonce 1: 2007-01-02 01:41:20: DEBUG:
Jan 02, 01:41:20  Debug    IKE  b17b8482 1afbd802 960e7bf2 59bd6cc6
Jan 02, 01:41:20  Debug    IKE  nonce 2: 2007-01-02 01:41:20: DEBUG:
Jan 02, 01:41:20  Debug    IKE  e7873f8f 75038989
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  SKEYID computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  c66e3258 322a9796 0080aba4 7562e72d 3465bc65
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  SKEYID_d computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  485932da 86899f43 7b9ede54 d898fd51 e5c9f731
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  SKEYID_a computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  22b66a14 52bbb718 ea165da8 46642452 48fdb33d
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  SKEYID_e computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  a9c2fb1c 6f83518d 22d83d91 0c19512e 3c1b1535
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  hash(sha1)
Jan 02, 01:41:20  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  compute intermediate encryption key K1
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  00
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  compute intermediate encryption key K2
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  32e36485 896dc605 15af3b14 e6fd2baf 142cbc5e
Jan 02, 01:41:20  Debug    IKE  final encryption key computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:20  Debug    IKE  hash(sha1)
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  IV computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  31e5576d 297bbda3
Jan 02, 01:41:20  Debug    IKE  HASH received:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  66bbd8f9 259d17c6 829af29e 148eeb60 1b55da98
Jan 02, 01:41:20  Debug    IKE  HASH with:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  19bd2774 8455d533 45b6a9ff 6594dc0b 74c100c2 5b04712e 2515164a dee2a011
Jan 02, 01:41:20  Debug    IKE  47399961 3b1de1a1 14e9fd0e 3cb07a05 02d220a9 0d9862a0 2c42adb3 71359c52
Jan 02, 01:41:20  Debug    IKE  04dbe3f3 99d4a3fd 39ed2352 1db6b0e3 d4d19ed7 3698fdd1 7a8fc0b5 a93d01ec
Jan 02, 01:41:20  Debug    IKE  40f6fd53 47459ed2 bffd8804 f23c5461 e49da47a 0176b3d9 f8e0ba3e 8ae31c52
Jan 02, 01:41:20  Debug    IKE  26ad23d7 8827b03f b3f4c5f3 8f231b96 57c93193 2c5dc991 a94e1d6d 0363ffb3
Jan 02, 01:41:20  Debug    IKE  e03cb46e a7a0de25 5c068566 5e6b89da f717e8d6 fa7f5451 a2bb96e3 4e023827
Jan 02, 01:41:20  Debug    IKE  25ee8e37 61deb1c9 f89f47ca fbc67ea0 4cd216a7 ba041abd 721dcd87 10af7920
Jan 02, 01:41:20  Debug    IKE  a415a472 218c5c27 85fafbb2 3a351705 9ad8c308 60d10eeb c8c31c22 978c2f66
Jan 02, 01:41:20  Debug    IKE  aa3a595c a68ccd61 378e09d2 48e961b0 00000001 00000001 0000002c 01010001
Jan 02, 01:41:20  Debug    IKE  00000024 01010000 800b0001 000c0004 00c5c100 80010005 80030001 80020002
Jan 02, 01:41:20  Debug    IKE  80040002 02000000 6676735f 6c6f6361 6c
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  HASH (init) computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  66bbd8f9 259d17c6 829af29e 148eeb60 1b55da98
Jan 02, 01:41:20  Debug    IKE  HASH for PSK validated.
Jan 02, 01:41:20  Debug    IKE  ===
Jan 02, 01:41:20  Debug    IKE  generate HASH_I
Jan 02, 01:41:20  Debug    IKE  HASH with:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  26ad23d7 8827b03f b3f4c5f3 8f231b96 57c93193 2c5dc991 a94e1d6d 0363ffb3
Jan 02, 01:41:20  Debug    IKE  e03cb46e a7a0de25 5c068566 5e6b89da f717e8d6 fa7f5451 a2bb96e3 4e023827
Jan 02, 01:41:20  Debug    IKE  25ee8e37 61deb1c9 f89f47ca fbc67ea0 4cd216a7 ba041abd 721dcd87 10af7920
Jan 02, 01:41:20  Debug    IKE  a415a472 218c5c27 85fafbb2 3a351705 9ad8c308 60d10eeb c8c31c22 978c2f66
Jan 02, 01:41:20  Debug    IKE  19bd2774 8455d533 45b6a9ff 6594dc0b 74c100c2 5b04712e 2515164a dee2a011
Jan 02, 01:41:20  Debug    IKE  47399961 3b1de1a1 14e9fd0e 3cb07a05 02d220a9 0d9862a0 2c42adb3 71359c52
Jan 02, 01:41:20  Debug    IKE  04dbe3f3 99d4a3fd 39ed2352 1db6b0e3 d4d19ed7 3698fdd1 7a8fc0b5 a93d01ec
Jan 02, 01:41:20  Debug    IKE  40f6fd53 47459ed2 bffd8804 f23c5461 e49da47a 0176b3d9 f8e0ba3e 8ae31c52
Jan 02, 01:41:20  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 00000001 00000001 0000002c 01010001
Jan 02, 01:41:20  Debug    IKE  00000024 01010000 800b0001 000c0004 00c5c100 80010005 80030001 80020002
Jan 02, 01:41:20  Debug    IKE  80040002 02000000 6676735f 72656d6f 7465
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  HASH (init) computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  df25f85b 2e446b7c 7ea72809 cd90b8b4 91dc0331
Jan 02, 01:41:20  Debug    IKE  add payload of len 20, next type 0
Jan 02, 01:41:20  Debug    IKE  52 bytes from 10.0.1.2[500] to 84.74.90.110[500]
Jan 02, 01:41:20  Debug    IKE  sockname 10.0.1.2[500]
Jan 02, 01:41:20  Debug    IKE  send packet from 10.0.1.2[500]
Jan 02, 01:41:20  Debug    IKE  send packet to 84.74.90.110[500]
Jan 02, 01:41:20  Debug    IKE  1 times of 52 bytes message will be sent to 84.74.90.110[500]
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08100400 00000000 00000034 00000018
Jan 02, 01:41:20  Debug    IKE  df25f85b 2e446b7c 7ea72809 cd90b8b4 91dc0331
Jan 02, 01:41:20  Debug    IKE  compute IV for phase2
Jan 02, 01:41:20  Debug    IKE  phase1 last IV:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  31e5576d 297bbda3 ebc55b2d
Jan 02, 01:41:20  Debug    IKE  hash(sha1)
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  phase2 IV computed:
```

```
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  d9feeee9 52088a2a
Jan 02, 01:41:20  Debug    IKE  HASH with:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  ebc55b2d 0000001c 00000001 01106002 378e09d2 48e961b0 aa3a595c a68ccd61
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  HASH computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  8da97b63 0b160ce3 e516acae ea936dec 882c256c
Jan 02, 01:41:20  Debug    IKE  begin encryption.
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  pad length = 4
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  0b000018 8da97b63 0b160ce3 e516acae ea936dec 882c256c 0000001c 00000001
Jan 02, 01:41:20  Debug    IKE  01106002 378e09d2 48e961b0 aa3a595c a68ccd61 00000004
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  with key:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:20  Debug    IKE  encrypted payload by IV:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  d9feeee9 52088a2a
Jan 02, 01:41:20  Debug    IKE  save IV for next:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  f4e8f73d 5e82f58e
Jan 02, 01:41:20  Debug    IKE  encrypted.
Jan 02, 01:41:20  Debug    IKE  84 bytes from 10.0.1.2[500] to 84.74.90.110[500]
Jan 02, 01:41:20  Debug    IKE  sockname 10.0.1.2[500]
Jan 02, 01:41:20  Debug    IKE  send packet from 10.0.1.2[500]
Jan 02, 01:41:20  Debug    IKE  send packet to 84.74.90.110[500]
Jan 02, 01:41:20  Debug    IKE  1 times of 84 bytes message will be sent to 84.74.90.110[500]
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08100501 ebc55b2d 00000054 cf307ac4
Jan 02, 01:41:20  Debug    IKE  fe6c04fc 24df4401 b3761977 8e5aa881 5ee0de22 d19f4816 a0ee7d45 2eb17665
Jan 02, 01:41:20  Debug    IKE  d436d0e2 1268f013 c2ce6666 f4e8f73d 5e82f58e
Jan 02, 01:41:20  Debug    IKE  sendto Information notify.
Jan 02, 01:41:20  Debug    IKE  IV freed
Jan 02, 01:41:20  Info     IKE  ISAKMP-SA established 10.0.1.2[500]-84.74.90.110[500] spi:
378e09d248e961b0:aa3a595ca68ccd61
Jan 02, 01:41:20  Debug    IKE  ===
Jan 02, 01:41:20  Debug    IKE  ===
Jan 02, 01:41:20  Debug    IKE  68 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08100501 ab7a9782 00000044 cf8a04b6
Jan 02, 01:41:20  Debug    IKE  ff81c39b 0a2d29a6 ff22ca01 40024afb a8ef46b9 1b9e320a ac44dfae fa0bc4d5
Jan 02, 01:41:20  Debug    IKE  6e1a893f
Jan 02, 01:41:20  Debug    IKE  receive Information.
Jan 02, 01:41:20  Debug    IKE  compute IV for phase2
Jan 02, 01:41:20  Debug    IKE  phase1 last IV:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  31e5576d 297bbda3 ab7a9782
Jan 02, 01:41:20  Debug    IKE  hash(sha1)
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  phase2 IV computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  d6a8ad0a 178984c9
Jan 02, 01:41:20  Debug    IKE  begin decryption.
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  IV was saved for next processing:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  fa0bc4d5 6e1a893f
Jan 02, 01:41:20  Debug    IKE  encryption(3des)
Jan 02, 01:41:20  Debug    IKE  with key:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:20  Debug    IKE  decrypted payload by IV:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  d6a8ad0a 178984c9
Jan 02, 01:41:20  Debug    IKE  decrypted payload, but not trimed.
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  0c000018 2493bf59 bf5824d3 268bc07f 5f42e155 3c298f23 00000010 00000001
Jan 02, 01:41:20  Debug    IKE  03040001 8ba98062
Jan 02, 01:41:20  Debug    IKE  padding len=98
Jan 02, 01:41:20  Debug    IKE  skip to trim padding.
Jan 02, 01:41:20  Debug    IKE  decrypted.
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08100501 ab7a9782 00000044 0c000018
Jan 02, 01:41:20  Debug    IKE  2493bf59 bf5824d3 268bc07f 5f42e155 3c298f23 00000010 00000001 03040001
Jan 02, 01:41:20  Debug    IKE  8ba98062
Jan 02, 01:41:20  Debug    IKE  IV freed
Jan 02, 01:41:20  Debug    IKE  HASH with:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  ab7a9782 00000010 00000001 03040001 8ba98062
Jan 02, 01:41:20  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:20  Debug    IKE  HASH computed:
Jan 02, 01:41:20  Debug    IKE
Jan 02, 01:41:20  Debug    IKE  2493bf59 bf5824d3 268bc07f 5f42e155 3c298f23
Jan 02, 01:41:20  Debug    IKE  hash validated.
Jan 02, 01:41:20  Debug    IKE  begin.
Jan 02, 01:41:20  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:20  Debug    IKE  seen nptype=12(delete)
Jan 02, 01:41:20  Debug    IKE  succeed.
Jan 02, 01:41:20  Debug    IKE  delete payload for protocol ESP
Jan 02, 01:41:20  Debug    IKE  call pfkey_send_dump
Jan 02, 01:41:20  Debug    IKE  purged SAs.
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  148 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 b70df248 00000094 85b19347
Jan 02, 01:41:21  Debug    IKE  448eabb3 1f275a75 8c653bdb ca173649 b7c91bb1 3bdaf5b3 33c92614 23b3d409
Jan 02, 01:41:21  Debug    IKE  76e3a34f e75f71a4 0089389c 3035774b e91e7559 1a58ea15 dcd1a27b 7894515c
Jan 02, 01:41:21  Debug    IKE  3e2ab690 ae303212 a9da0638 5ab2df3a f01b75ce c72a51f9 f4f53fbb 12d3747d
Jan 02, 01:41:21  Debug    IKE  27fb9c43 0683cc71 5b2426fc d3e3dca1 26a39058
Jan 02, 01:41:21  Debug    IKE  compute IV for phase2
Jan 02, 01:41:21  Debug    IKE  phase1 last IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  31e5576d 297bbda3 b70df248
Jan 02, 01:41:21  Debug    IKE  hash(sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  phase2 IV computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  273c832c f29c2a54
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Info     IKE  respond new phase 2 negotiation: 10.0.1.2[500]<=>84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  begin decryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  IV was saved for next processing:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  d3e3dca1 26a39058
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  decrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  273c832c f29c2a54
Jan 02, 01:41:21  Debug    IKE  decrypted payload, but not trimed.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000018 497d6ace 8422b641 5130e179 b0a677ba f27f70e9 0a000034 00000001
Jan 02, 01:41:21  Debug    IKE  00000001 00000028 01030401 c8907f68 0000001c 01030000 80050002 80040001
Jan 02, 01:41:21  Debug    IKE  80010001 00020004 00015180 0500000c eb6c2ece 11b11e70 05000010 04000000
Jan 02, 01:41:21  Debug    IKE  c0a8d700 ffffff00 0000000c 01000000 14010101 00000000
Jan 02, 01:41:21  Debug    IKE  padding len=0
Jan 02, 01:41:21  Debug    IKE  skip to trim padding.
Jan 02, 01:41:21  Debug    IKE  decrypted.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 b70df248 00000094 01000018
Jan 02, 01:41:21  Debug    IKE  497d6ace 8422b641 5130e179 b0a677ba f27f70e9 0a000034 00000001 00000001
Jan 02, 01:41:21  Debug    IKE  00000028 01030401 c8907f68 0000001c 01030000 80050002 80040001 80010001
Jan 02, 01:41:21  Debug    IKE  00020004 00015180 0500000c eb6c2ece 11b11e70 05000010 04000000 c0a8d700
Jan 02, 01:41:21  Debug    IKE  ffffff00 0000000c 01000000 14010101 00000000
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:21  Debug    IKE  seen nptype=1(sa)
Jan 02, 01:41:21  Debug    IKE  seen nptype=10(nonce)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  received IDci2:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  received IDcr2:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  01000000 14010101
Jan 02, 01:41:21  Debug    IKE  HASH(1) validate:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  497d6ace 8422b641 5130e179 b0a677ba f27f70e9
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  b70df248 0a000034 00000001 00000001 00000028 01030401 c8907f68 0000001c
Jan 02, 01:41:21  Debug    IKE  01030000 80050002 80040001 80010001 00020004 00015180 0500000c eb6c2ece
Jan 02, 01:41:21  Debug    IKE  11b11e70 05000010 04000000 c0a8d700 ffffff00 0000000c 01000000 14010101
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  497d6ace 8422b641 5130e179 b0a677ba f27f70e9
Jan 02, 01:41:21  Error    IKE  failed to get sainfo.
Jan 02, 01:41:21  Error    IKE  failed to get sainfo.
Jan 02, 01:41:21  Error    IKE  failed to pre-process packet.
Jan 02, 01:41:21  Debug    IKE  IV freed
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  begin QUICK mode.
Jan 02, 01:41:21  Info     IKE  initiate new phase 2 negotiation: 10.0.1.2[500]<=>84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  compute IV for phase2
Jan 02, 01:41:21  Debug    IKE  phase1 last IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  31e5576d 297bbda3 c087d4b2
Jan 02, 01:41:21  Debug    IKE  hash(sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  phase2 IV computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  9826c582 20f0f298
Jan 02, 01:41:21  Debug    IKE  call pfkey_send_getspi
Jan 02, 01:41:21  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0]
Jan 02, 01:41:21  Debug    IKE  pfkey getspi sent.
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  148 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 d9973e4b 00000094 c6023f6c
Jan 02, 01:41:21  Debug    IKE  d4bad14f 3a003ee6 670c9f89 bebf4830 d2e045d1 52103096 faa4592b 47b1baf0
Jan 02, 01:41:21  Debug    IKE  0c156b18 7f2746c6 a83dedb1 6840a18b c5bd3f5d f55046d8 c37db129 61fdf371
Jan 02, 01:41:21  Debug    IKE  604f46eb 126afb0c 0b0f30e6 e71061a8 074f0534 ffc91cd8 7a3e48f5 44374aa9
Jan 02, 01:41:21  Debug    IKE  6900c15e 84a3fc54 8aa0d27c 5b86ce77 e9ed0d2a
Jan 02, 01:41:21  Debug    IKE  compute IV for phase2
Jan 02, 01:41:21  Debug    IKE  phase1 last IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  31e5576d 297bbda3 d9973e4b
Jan 02, 01:41:21  Debug    IKE  hash(sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  phase2 IV computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  55e0983c 0139f3ec
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Info     IKE  respond new phase 2 negotiation: 10.0.1.2[500]<=>84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  begin decryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  IV was saved for next processing:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  5b86ce77 e9ed0d2a
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  decrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  55e0983c 0139f3ec
Jan 02, 01:41:21  Debug    IKE  decrypted payload, but not trimed.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000018 b3febcae 009a0761 ae12906d 76f7778e 977bf6a7 0a000034 00000001
Jan 02, 01:41:21  Debug    IKE  00000001 00000028 01030401 d32b9e70 0000001c 01030000 80050002 80040001
Jan 02, 01:41:21  Debug    IKE  80010001 00020004 00015180 0500000c bad3a1aa 9df39f18 05000010 04000000
Jan 02, 01:41:21  Debug    IKE  c0a8d700 ffffff00 0000000c 01000000 0a010101 00000000
Jan 02, 01:41:21  Debug    IKE  padding len=0
Jan 02, 01:41:21  Debug    IKE  skip to trim padding.
Jan 02, 01:41:21  Debug    IKE  decrypted.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 d9973e4b 00000094 01000018
Jan 02, 01:41:21  Debug    IKE  b3febcae 009a0761 ae12906d 76f7778e 977bf6a7 0a000034 00000001 00000001
Jan 02, 01:41:21  Debug    IKE  00000028 01030401 d32b9e70 0000001c 01030000 80050002 80040001 80010001
Jan 02, 01:41:21  Debug    IKE  00020004 00015180 0500000c bad3a1aa 9df39f18 05000010 04000000 c0a8d700
Jan 02, 01:41:21  Debug    IKE  ffffff00 0000000c 01000000 0a010101 00000000
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:21  Debug    IKE  seen nptype=1(sa)
Jan 02, 01:41:21  Debug    IKE  seen nptype=10(nonce)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  received IDci2:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  received IDcr2:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  01000000 0a010101
Jan 02, 01:41:21  Debug    IKE  HASH(1) validate:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  b3febcae 009a0761 ae12906d 76f7778e 977bf6a7
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  d9973e4b 0a000034 00000001 00000001 00000028 01030401 d32b9e70 0000001c
Jan 02, 01:41:21  Debug    IKE  01030000 80050002 80040001 80010001 00020004 00015180 0500000c bad3a1aa
Jan 02, 01:41:21  Debug    IKE  9df39f18 05000010 04000000 c0a8d700 ffffff00 0000000c 01000000 0a010101
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  b3febcae 009a0761 ae12906d 76f7778e 977bf6a7
Jan 02, 01:41:21  Error    IKE  failed to get sainfo.
Jan 02, 01:41:21  Error    IKE  failed to get sainfo.
Jan 02, 01:41:21  Error    IKE  failed to pre-process packet.
Jan 02, 01:41:21  Debug    IKE  IV freed
Jan 02, 01:41:21  Debug    IKE  get pfkey GETSPI message
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  02010003 0a000000 6a000000 7f0e0000 02000100 053920bd 30313030 30303030
Jan 02, 01:41:21  Debug    IKE  03000500 ff200000 10020000 544a5a6e 00000000 00000000 03000600 ff200000
Jan 02, 01:41:21  Debug    IKE  10020000 0a000102 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0] spi=87630013(0x53920bd)
Jan 02, 01:41:21  Debug    IKE  use local ID type IPv4_address
Jan 02, 01:41:21  Debug    IKE  use remote ID type IPv4_subnet
Jan 02, 01:41:21  Debug    IKE  IDci:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000000 0a000102
Jan 02, 01:41:21  Debug    IKE  IDcr:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  add payload of len 68, next type 10
Jan 02, 01:41:21  Debug    IKE  add payload of len 16, next type 5
Jan 02, 01:41:21  Debug    IKE  add payload of len 8, next type 5
Jan 02, 01:41:21  Debug    IKE  add payload of len 12, next type 0
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  c087d4b2 0a000048 00000001 00000001 0000003c 01030402 053920bd 03000018
Jan 02, 01:41:21  Debug    IKE  01020000 80010001 80020e10 80040001 80050002 00000018 02030000 80010001
Jan 02, 01:41:21  Debug    IKE  80020e10 80040001 80050002 05000014 91fffc1f 6fa56dba 028b946c ca582aff
Jan 02, 01:41:21  Debug    IKE  0500000c 01000000 0a000102 00000010 04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2d0a3a80 22d4facf 1651b38c 304c5bda a366edef
Jan 02, 01:41:21  Debug    IKE  add payload of len 20, next type 1
Jan 02, 01:41:21  Debug    IKE  begin encryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  pad length = 8
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000018 2d0a3a80 22d4facf 1651b38c 304c5bda a366edef 0a000048 00000001
Jan 02, 01:41:21  Debug    IKE  00000001 0000003c 01030402 053920bd 03000018 01020000 80010001 80020e10
Jan 02, 01:41:21  Debug    IKE  80040001 80050002 00000018 02030000 80010001 80020e10 80040001 80050002
Jan 02, 01:41:21  Debug    IKE  05000014 91fffc1f 6fa56dba 028b946c ca582aff 0500000c 01000000 0a000102
Jan 02, 01:41:21  Debug    IKE  00000010 04000000 c0a8d700 ffffff00 00000000 00000008
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  encrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  9826c582 20f0f298
Jan 02, 01:41:21  Debug    IKE  save IV for next:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  5e6174f0 af13c4f5
Jan 02, 01:41:21  Debug    IKE  encrypted.
Jan 02, 01:41:21  Debug    IKE  180 bytes from 10.0.1.2[500] to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  sockname 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE  send packet from 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE  send packet to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  1 times of 180 bytes message will be sent to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 c087d4b2 000000b4 a57f62ba
Jan 02, 01:41:21  Debug    IKE  93839c0c bd20a240 594adeb6 04bf2855 99062a01 316c4cb1 3020b15c e3f25088
Jan 02, 01:41:21  Debug    IKE  b046378c c60ed153 6030fc79 3af3b74d 98e17737 3c0367c9 399793dd a73b40aa
Jan 02, 01:41:21  Debug    IKE  52ee22f2 dea3a205 4412ad31 0d46aebb c604d9d1 763fb927 2d959f27 43398291
Jan 02, 01:41:21  Debug    IKE  1e75fd0a f73278a2 f5835d49 db25b400 b3b74d29 bffa8a02 b26b8e9e b00681b4
Jan 02, 01:41:21  Debug    IKE  bdced8f0 fcd865b9 580852c0 5e6174f0 af13c4f5
Jan 02, 01:41:21  Debug    IKE  resend phase2 packet 378e09d248e961b0:aa3a595ca68ccd61:0000c087
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  148 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 92570b37 00000094 a2575560
Jan 02, 01:41:21  Debug    IKE  b8d7c595 7f66f93e 50e73deb e51077e8 37c5ef93 615712bc f46424e0 9717f304
Jan 02, 01:41:21  Debug    IKE  d039e458 23ccfed9 daad5942 7579910d c25eccca 9384db9d c4a188c7 a5c14bba
Jan 02, 01:41:21  Debug    IKE  9268762c fa84c662 01a6647e a387af18 fd6f8766 fa22e55f 46fbb491 0d4f9130
Jan 02, 01:41:21  Debug    IKE  90c583f3 59aefb28 4c8fb0a8 dceac795 999a740c
Jan 02, 01:41:21  Debug    IKE  compute IV for phase2
Jan 02, 01:41:21  Debug    IKE  phase1 last IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  31e5576d 297bbda3 92570b37
Jan 02, 01:41:21  Debug    IKE  hash(sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  phase2 IV computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  6e34671b f31e8c84
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Info     IKE  respond new phase 2 negotiation: 10.0.1.2[500]<=>84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  begin decryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  IV was saved for next processing:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  dceac795 999a740c
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  decrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  6e34671b f31e8c84
Jan 02, 01:41:21  Debug    IKE  decrypted payload, but not trimed.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000018 ba0cd575 01a8aa38 39d06cec f2561927 c76f3d1b 0a000034 00000001
Jan 02, 01:41:21  Debug    IKE  00000001 00000028 01030401 94b834a2 0000001c 01030000 80050002 80040001
Jan 02, 01:41:21  Debug    IKE  80010001 00020004 00015180 0500000c d39f6d9a eeb8990a 05000010 04000000
Jan 02, 01:41:21  Debug    IKE  c0a8d700 ffffff00 0000000c 01000000 0a000102 00000000
Jan 02, 01:41:21  Debug    IKE  padding len=0
Jan 02, 01:41:21  Debug    IKE  skip to trim padding.
Jan 02, 01:41:21  Debug    IKE  decrypted.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 92570b37 00000094 01000018
Jan 02, 01:41:21  Debug    IKE  ba0cd575 01a8aa38 39d06cec f2561927 c76f3d1b 0a000034 00000001 00000001
Jan 02, 01:41:21  Debug    IKE  00000028 01030401 94b834a2 0000001c 01030000 80050002 80040001 80010001
Jan 02, 01:41:21  Debug    IKE  00020004 00015180 0500000c d39f6d9a eeb8990a 05000010 04000000 c0a8d700
Jan 02, 01:41:21  Debug    IKE  ffffff00 0000000c 01000000 0a000102 00000000
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:21  Debug    IKE  seen nptype=1(sa)
Jan 02, 01:41:21  Debug    IKE  seen nptype=10(nonce)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  received IDci2:2007-01-02 01:41:21: DEBUG:
```

```
Jan 02, 01:41:21  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  received IDcr2:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  01000000 0a000102
Jan 02, 01:41:21  Debug    IKE  HASH(1) validate:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  ba0cd575 01a8aa38 39d06cec f2561927 c76f3d1b
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  92570b37 0a000034 00000001 00000001 00000028 01030401 94b834a2 0000001c
Jan 02, 01:41:21  Debug    IKE  01030000 80050002 80040001 80010001 00020004 00015180 0500000c d39f6d9a
Jan 02, 01:41:21  Debug    IKE  eeb8990a 05000010 04000000 c0a8d700 ffffff00 0000000c 01000000 0a000102
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  ba0cd575 01a8aa38 39d06cec f2561927 c76f3d1b
Jan 02, 01:41:21  Debug    IKE  get sa info:
Jan 02, 01:41:21  Debug    IKE  get a src address from ID payload 192.168.215.0[0] prefixlen=24 ul_proto=255
Jan 02, 01:41:21  Debug    IKE  get dst address from ID payload 10.0.1.2[0] prefixlen=32 ul_proto=255
Jan 02, 01:41:21  Debug    IKE  sub:0xbffff354: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 02, 01:41:21  Debug    IKE  db: 0x308c88: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 02, 01:41:21  Debug    IKE  0xbffff354 masked with /24: 192.168.215.0[0]
Jan 02, 01:41:21  Debug    IKE  0x308c88 masked with /24: 192.168.215.0[0]
Jan 02, 01:41:21  Debug    IKE  0xbffff354 masked with /32: 10.0.1.2[0]
Jan 02, 01:41:21  Debug    IKE  0x308c88 masked with /32: 10.0.1.2[0]
Jan 02, 01:41:21  Debug    IKE  sub:0xbffff354: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 02, 01:41:21  Debug    IKE  db: 0x308c88: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 02, 01:41:21  Debug    IKE  sub:0xbffff354: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 02, 01:41:21  Debug    IKE  db: 0x308ec8: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 02, 01:41:21  Debug    IKE  0xbffff354 masked with /32: 10.0.1.2[0]
Jan 02, 01:41:21  Debug    IKE  0x308ec8 masked with /32: 10.0.1.2[0]
Jan 02, 01:41:21  Debug    IKE  0xbffff354 masked with /24: 192.168.215.0[0]
Jan 02, 01:41:21  Debug    IKE  0x308ec8 masked with /24: 192.168.215.0[0]
Jan 02, 01:41:21  Debug    IKE  suitable SP found:10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 02, 01:41:21  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 02, 01:41:21  Debug    IKE  (trns_id=DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Debug    IKE  total SA len=48
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00000001 00000001 00000028 01030401 94b834a2 0000001c 01030000 80050002
Jan 02, 01:41:21  Debug    IKE  80040001 80010001 00020004 00015180
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=2(prop)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  proposal #1 len=40
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=3(trns)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  transform #1 len=28
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jan 02, 01:41:21  Debug    IKE  pair 1:
Jan 02, 01:41:21  Debug    IKE  0x30a270: next=0x0 tnext=0x0
Jan 02, 01:41:21  Debug    IKE  proposal #1: 1 transform
Jan 02, 01:41:21  Debug    IKE  begin compare proposals.
Jan 02, 01:41:21  Debug    IKE  pair[1]: 0x30a270
Jan 02, 01:41:21  Debug    IKE  0x30a270: next=0x0 tnext=0x0
Jan 02, 01:41:21  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jan 02, 01:41:21  Debug    IKE  peer's single bundle:
Jan 02, 01:41:21  Debug    IKE  (proto_id=ESP spisize=4 spi=94b834a2 spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 02, 01:41:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Debug    IKE  my single bundle:
Jan 02, 01:41:21  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 02, 01:41:21  Debug    IKE  (trns_id=DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Warning  IKE  trns_id mismatched: my:DES peer:3DES
Jan 02, 01:41:21  Debug    IKE  matched
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  call pfkey_send_getspi
Jan 02, 01:41:21  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0]
Jan 02, 01:41:21  Debug    IKE  pfkey getspi sent.
Jan 02, 01:41:21  Debug    IKE  get pfkey GETSPI message
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  02010003 0a000000 f7e99872 7f0e0000 02000100 00c3d973 5ce2336a 5e0a3c2e
Jan 02, 01:41:21  Debug    IKE  03000500 ff200000 10020000 544a5a6e 00000000 00000000 03000600 ff200000
Jan 02, 01:41:21  Debug    IKE  10020000 0a000102 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0] spi=12835187(0xc3d973)
Jan 02, 01:41:21  Debug    IKE  total SA len=48
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00000001 00000001 00000028 01030401 00000000 0000001c 01030000 80050002
Jan 02, 01:41:21  Debug    IKE  80040001 80010001 00020004 00015180
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=2(prop)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  proposal #1 len=40
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=3(trns)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  transform #1 len=28
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jan 02, 01:41:21  Debug    IKE  pair 1:
Jan 02, 01:41:21  Debug    IKE  0x309650: next=0x0 tnext=0x0
Jan 02, 01:41:21  Debug    IKE  proposal #1: 1 transform
Jan 02, 01:41:21  Debug    IKE  add payload of len 48, next type 10
Jan 02, 01:41:21  Debug    IKE  add payload of len 16, next type 5
Jan 02, 01:41:21  Debug    IKE  add payload of len 12, next type 5
Jan 02, 01:41:21  Debug    IKE  add payload of len 8, next type 0
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  92570b37 d39f6d9a eeb8990a 0a000034 00000001 00000001 00000028 01030401
Jan 02, 01:41:21  Debug    IKE  00c3d973 0000001c 01030000 80050002 80040001 80010001 00020004 00015180
Jan 02, 01:41:21  Debug    IKE  05000014 bee38e2f 06cb422b 8a76878c 947136a0 05000010 04000000 c0a8d700
Jan 02, 01:41:21  Debug    IKE  ffffff00 0000000c 01000000 0a000102
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  6a611ada 0ea342e8 60f14391 fae3fd86 c62305e6
Jan 02, 01:41:21  Debug    IKE  add payload of len 20, next type 1
Jan 02, 01:41:21  Debug    IKE  begin encryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  pad length = 4
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000018 6a611ada 0ea342e8 60f14391 fae3fd86 c62305e6 0a000034 00000001
Jan 02, 01:41:21  Debug    IKE  00000001 00000028 01030401 00c3d973 0000001c 01030000 80050002 80040001
Jan 02, 01:41:21  Debug    IKE  80010001 00020004 00015180 05000014 bee38e2f 06cb422b 8a76878c 947136a0
Jan 02, 01:41:21  Debug    IKE  05000010 04000000 c0a8d700 ffffff00 0000000c 01000000 0a000102 00000004
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  encrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  dceac795 999a740c
Jan 02, 01:41:21  Debug    IKE  save IV for next:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  d4d369be 2517f50b
Jan 02, 01:41:21  Debug    IKE  encrypted.
Jan 02, 01:41:21  Debug    IKE  156 bytes from 10.0.1.2[500] to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  sockname 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE  send packet from 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE  send packet to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  1 times of 156 bytes message will be sent to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 92570b37 0000009c 4fe29511
Jan 02, 01:41:21  Debug    IKE  2e3de9df 6d15c281 fd4494a6 8a39760a 68198ad2 16cac299 95a98533 17b9ee9c
Jan 02, 01:41:21  Debug    IKE  ddbd2a77 f46e376e 1b43475c c5c20e94 e8dfd73e 21dd6a1a 00c33cd4 13920aa2
Jan 02, 01:41:21  Debug    IKE  4de8662d b7b1c5ab 66d59b07 608c74a2 edeeb5dc 99b609b9 1fcadbb7 9c1eca39
Jan 02, 01:41:21  Debug    IKE  619f141e e86d5137 c1d2602c c187c65d b4e4eed5 d4d369be 2517f50b
Jan 02, 01:41:21  Debug    IKE  resend phase2 packet 378e09d248e961b0:aa3a595ca68ccd61:00009257
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  140 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 c087d4b2 0000008c 5e68128a
Jan 02, 01:41:21  Debug    IKE  8d0a3834 412e5f4f c7670376 38b549fd dc9eaf5f a8299d3d 84b7873c 59303796
Jan 02, 01:41:21  Debug    IKE  eaeeb990 d4cf1b15 cd39d8b0 9f8ef9f5 894a982f fa287d1f 0c0238c7 39c7bf07
Jan 02, 01:41:21  Debug    IKE  22084d11 dd528976 afb9665d 14a819f0 4ecd6561 77fe9110 e213cb4e 46bd36d3
Jan 02, 01:41:21  Debug    IKE  a5cca319 8fc9fd4b f9419681
Jan 02, 01:41:21  Debug    IKE  begin decryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  IV was saved for next processing:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  8fc9fd4b f9419681
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  decrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  5e6174f0 af13c4f5
Jan 02, 01:41:21  Debug    IKE  decrypted payload, but not trimed.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  01000018 6f3cc523 b3178abb 211f3e60 265db03b 45020db3 0a000030 00000001
Jan 02, 01:41:21  Debug    IKE  00000001 00000024 01030401 a78c807a 00000018 02030000 80010001 80020e10
Jan 02, 01:41:21  Debug    IKE  80040001 80050002 0500000c a20a2fbf 8ce60ba3 0500000c 01000000 0a000102
Jan 02, 01:41:21  Debug    IKE  00000010 04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  padding len=0
Jan 02, 01:41:21  Debug    IKE  skip to trim padding.
Jan 02, 01:41:21  Debug    IKE  decrypted.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 c087d4b2 0000008c 01000018
Jan 02, 01:41:21  Debug    IKE  6f3cc523 b3178abb 211f3e60 265db03b 45020db3 0a000030 00000001 00000001
Jan 02, 01:41:21  Debug    IKE  00000024 01030401 a78c807a 00000018 02030000 80010001 80020e10 80040001
Jan 02, 01:41:21  Debug    IKE  80050002 0500000c a20a2fbf 8ce60ba3 0500000c 01000000 0a000102 00000010
Jan 02, 01:41:21  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:21  Debug    IKE  seen nptype=1(sa)
Jan 02, 01:41:21  Debug    IKE  seen nptype=10(nonce)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  seen nptype=5(id)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  HASH allocated:hbuf->l=128 actual:tlen=104
Jan 02, 01:41:21  Debug    IKE  HASH(2) received:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  6f3cc523 b3178abb 211f3e60 265db03b 45020db3
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  c087d4b2 91fffc1f 6fa56dba 028b946c ca582aff 0a000030 00000001 00000001
Jan 02, 01:41:21  Debug    IKE  00000024 01030401 a78c807a 00000018 02030000 80010001 80020e10 80040001
Jan 02, 01:41:21  Debug    IKE  80050002 0500000c a20a2fbf 8ce60ba3 0500000c 01000000 0a000102 00000010
Jan 02, 01:41:21  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  6f3cc523 b3178abb 211f3e60 265db03b 45020db3
Jan 02, 01:41:21  Debug    IKE  total SA len=68
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00000001 00000001 0000003c 01030402 053920bd 03000018 01020000 80010001
Jan 02, 01:41:21  Debug    IKE  80020e10 80040001 80050002 00000018 02030000 80010001 80020e10 80040001
Jan 02, 01:41:21  Debug    IKE  80050002
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=2(prop)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  proposal #1 len=60
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=3(trns)
Jan 02, 01:41:21  Debug    IKE  seen nptype=3(trns)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  transform #1 len=24
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
Jan 02, 01:41:21  Debug    IKE  life duration was in TLV.
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  transform #2 len=24
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
Jan 02, 01:41:21  Debug    IKE  life duration was in TLV.
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  pair 1:
Jan 02, 01:41:21  Debug    IKE  0x309620: next=0x0 tnext=0x309630
Jan 02, 01:41:21  Debug    IKE  0x309630: next=0x0 tnext=0x0
Jan 02, 01:41:21  Debug    IKE  proposal #1: 2 transform
Jan 02, 01:41:21  Debug    IKE  total SA len=44
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00000001 00000001 00000024 01030401 a78c807a 00000018 02030000 80010001
Jan 02, 01:41:21  Debug    IKE  80020e10 80040001 80050002
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=2(prop)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  proposal #1 len=36
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=3(trns)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  transform #2 len=24
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
Jan 02, 01:41:21  Debug    IKE  life duration was in TLV.
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  pair 1:
Jan 02, 01:41:21  Debug    IKE  0x30a040: next=0x0 tnext=0x0
Jan 02, 01:41:21  Debug    IKE  proposal #1: 1 transform
Jan 02, 01:41:21  Debug    IKE  begin compare proposals.
Jan 02, 01:41:21  Debug    IKE  pair[1]: 0x30a040
Jan 02, 01:41:21  Debug    IKE  0x30a040: next=0x0 tnext=0x0
Jan 02, 01:41:21  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=2 trns-id=3DES
Jan 02, 01:41:21  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 02, 01:41:21  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
Jan 02, 01:41:21  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Jan 02, 01:41:21  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 02, 01:41:21  Debug    IKE  peer's single bundle:
Jan 02, 01:41:21  Debug    IKE  (proto_id=ESP spisize=4 spi=a78c807a spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 02, 01:41:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Debug    IKE  my single bundle:
Jan 02, 01:41:21  Debug    IKE  (proto_id=ESP spisize=4 spi=053920bd spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 02, 01:41:21  Debug    IKE  (trns_id=DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 02, 01:41:21  Warning  IKE  trns_id mismatched: my:DES peer:3DES
Jan 02, 01:41:21  Debug    IKE  matched
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  HASH(3) generate
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00c087d4 b291fffc 1f6fa56d ba028b94 6cca582a ffa20a2f bf8ce60b a3
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  da161d5d 595013ba 15336147 d89eb229 fefdcf44
Jan 02, 01:41:21  Debug    IKE  add payload of len 20, next type 0
Jan 02, 01:41:21  Debug    IKE  begin encryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  pad length = 8
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00000018 da161d5d 595013ba 15336147 d89eb229 fefdcf44 00000000 00000008
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  encrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  8fc9fd4b f9419681
Jan 02, 01:41:21  Debug    IKE  save IV for next:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  8be3237c 563fe88c
Jan 02, 01:41:21  Debug    IKE  encrypted.
Jan 02, 01:41:21  Debug    IKE  60 bytes from 10.0.1.2[500] to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  sockname 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE  send packet from 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE  send packet to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE  1 times of 60 bytes message will be sent to 84.74.90.110[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 c087d4b2 0000003c 1af54e98
Jan 02, 01:41:21  Debug    IKE  bc2edd4e ba0ba7d6 5b36d0b0 cff931d1 cacbb3dd 8be3237c 563fe88c
Jan 02, 01:41:21  Debug    IKE  KEYMAT compute with
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  03053920 bd91fffc 1f6fa56d ba028b94 6cca582a ffa20a2f bf8ce60b a3
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encklen=192 authklen=160
Jan 02, 01:41:21  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jan 02, 01:41:21  Debug    IKE  generating K1...K4 for KEYMAT.
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  fd4ba924 18d0f714 285d0497 1dfd7d35 31064b0d 8e7bf859 466ecc36 dd95fae8
Jan 02, 01:41:21  Debug    IKE  89bc3626 4b14d6d2 cca1fc8f 42968d14 10da63c7 5686b8e0 c143f733 4edd33c0
Jan 02, 01:41:21  Debug    IKE  92139574 c728870e 0e315a38 ac587607
Jan 02, 01:41:21  Debug    IKE  KEYMAT compute with
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  03a78c80 7a91fffc 1f6fa56d ba028b94 6cca582a ffa20a2f bf8ce60b a3
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encklen=192 authklen=160
Jan 02, 01:41:21  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jan 02, 01:41:21  Debug    IKE  generating K1...K4 for KEYMAT.
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  0e27b43a 0c4db4ea bf6afa19 1f6b8827 4a9c12d0 e72b0fa2 6ff6b871 558a65d8
Jan 02, 01:41:21  Debug    IKE  40a2c476 afc3ddbe 0fb3f451 a2aa9c2f 73c2ec5e fd662703 41600b0e e00615be
Jan 02, 01:41:21  Debug    IKE  24718bdb e0947287 f730b9a7 c9b37bf2
Jan 02, 01:41:21  Debug    IKE  KEYMAT computed.
Jan 02, 01:41:21  Debug    IKE  call pk_sendupdate
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  call pfkey_send_update_nat
Jan 02, 01:41:21  Debug    IKE  pfkey update sent.
Jan 02, 01:41:21  Debug    APP  Received SADB message type UPDATE, 84.74.90.110 [0] -> 10.0.1.2 [0]
Jan 02, 01:41:21  Debug    APP  SA change detected
Jan 02, 01:41:21  Debug    APP  Connection Netgear FVS328 is down
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  call pfkey_send_add_nat
Jan 02, 01:41:21  Debug    APP  Received SADB message type ADD, 10.0.1.2 [0] -> 84.74.90.110 [0]
Jan 02, 01:41:21  Debug    APP  SA change detected
Jan 02, 01:41:21  Debug    APP  Connection Netgear FVS328 is up
Jan 02, 01:41:21  Debug    IKE  pfkey add sent.
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  52 bytes message received from 84.74.90.110[500] to 10.0.1.2[500]
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 92570b37 00000034 6e6b2562
Jan 02, 01:41:21  Debug    IKE  0c4853f3 3e642a02 58e5a1b4 ea4af8b0 12480200
Jan 02, 01:41:21  Debug    IKE  begin decryption.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  IV was saved for next processing:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  ea4af8b0 12480200
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  with key:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  2ad65215 b7af33f0 4809d824 08cdb28b 4f4b561e 32e36485
Jan 02, 01:41:21  Debug    IKE  decrypted payload by IV:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  d4d369be 2517f50b
Jan 02, 01:41:21  Debug    IKE  decrypted payload, but not trimed.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  00000018 ca3a6695 a9fcf0ee e6aa6199 a0a05a78 de4776d0
Jan 02, 01:41:21  Debug    IKE  padding len=208
Jan 02, 01:41:21  Debug    IKE  skip to trim padding.
Jan 02, 01:41:21  Debug    IKE  decrypted.
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  378e09d2 48e961b0 aa3a595c a68ccd61 08102001 92570b37 00000034 00000018
Jan 02, 01:41:21  Debug    IKE  ca3a6695 a9fcf0ee e6aa6199 a0a05a78 de4776d0
Jan 02, 01:41:21  Debug    IKE  begin.
Jan 02, 01:41:21  Debug    IKE  seen nptype=8(hash)
Jan 02, 01:41:21  Debug    IKE  succeed.
Jan 02, 01:41:21  Debug    IKE  HASH(3) validate:2007-01-02 01:41:21: DEBUG:
Jan 02, 01:41:21  Debug    IKE  ca3a6695 a9fcf0ee e6aa6199 a0a05a78 de4776d0
Jan 02, 01:41:21  Debug    IKE  HASH with:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  0092570b 37d39f6d 9aeeb899 0abee38e 2f06cb42 2b8a7687 8c947136 a0
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  HASH computed:
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  ca3a6695 a9fcf0ee e6aa6199 a0a05a78 de4776d0
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  KEYMAT compute with
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  0300c3d9 73d39f6d 9aeeb899 0abee38e 2f06cb42 2b8a7687 8c947136 a0
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encklen=192 authklen=160
Jan 02, 01:41:21  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jan 02, 01:41:21  Debug    IKE  generating K1...K4 for KEYMAT.
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  1d24dcb4 3b996464 5c894b1d fecc1090 6e036fde 6b57ac2a 67bffa84 11331354
Jan 02, 01:41:21  Debug    IKE  4f7806ba 29d47309 aba668c7 d4008894 8dd21ceb 777b4f90 6884bc9f fb4c12e4
Jan 02, 01:41:21  Debug    IKE  48585c9b 14bb7388 cd1428da cd8d732b
Jan 02, 01:41:21  Debug    IKE  KEYMAT compute with
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  0394b834 a2d39f6d 9aeeb899 0abee38e 2f06cb42 2b8a7687 8c947136 a0
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  encklen=192 authklen=160
Jan 02, 01:41:21  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jan 02, 01:41:21  Debug    IKE  generating K1...K4 for KEYMAT.
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  815159e9 35589e55 a9528f92 65188d0f effe4a5f f8e2af72 0ecb6d45 6a47fd7f
Jan 02, 01:41:21  Debug    IKE  f5ae8c32 88131cd9 2651ad21 fcc9dc87 5c2b9293 99f18e4a 9375b941 d7fb29c7
Jan 02, 01:41:21  Debug    IKE  b2e0878d 8fdf7789 aa0a5220 fdd2ace6
Jan 02, 01:41:21  Debug    IKE  KEYMAT computed.
Jan 02, 01:41:21  Debug    IKE  call pk_sendupdate
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  call pfkey_send_update_nat
Jan 02, 01:41:21  Debug    APP  Received SADB message type UPDATE, 84.74.90.110 [0] -> 10.0.1.2 [0]
Jan 02, 01:41:21  Debug    APP  SA change detected
Jan 02, 01:41:21  Debug    APP  Connection Netgear FVS328 is up
Jan 02, 01:41:21  Debug    IKE  pfkey update sent.
Jan 02, 01:41:21  Debug    IKE  encryption(3des)
Jan 02, 01:41:21  Debug    IKE  hmac(hmac_sha1)
Jan 02, 01:41:21  Debug    IKE  call pfkey_send_add_nat
Jan 02, 01:41:21  Debug    APP  Received SADB message type ADD, 10.0.1.2 [0] -> 84.74.90.110 [0]
Jan 02, 01:41:21  Debug    APP  SA change detected
Jan 02, 01:41:21  Debug    APP  Connection Netgear FVS328 is up
Jan 02, 01:41:21  Debug    IKE  pfkey add sent.
Jan 02, 01:41:21  Debug    IKE  get pfkey UPDATE message
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  02020003 14000000 6a000000 7f0e0000 02000100 053920bd 04000202 00000000
Jan 02, 01:41:21  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 544a5a6e
Jan 02, 01:41:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 0a000102 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000300 00000000 00000000 00000000 100e0000 00000000 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000400 00000000 00000000 00000000 400b0000 00000000 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0] spi=87630013(0x53920bd)
Jan 02, 01:41:21  Info     IKE  IPsec-SA established: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0] spi=87630013(0x53920bd)
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  get pfkey ADD message
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  02030003 14000000 6a000000 7f0e0000 02000100 a78c807a 04000202 00000000
Jan 02, 01:41:21  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 0a000102
Jan 02, 01:41:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 544a5a6e 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000300 00000000 00000000 00000000 100e0000 00000000 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000400 00000000 00000000 00000000 400b0000 00000000 00000000 00000000
Jan 02, 01:41:21  Info     IKE  IPsec-SA established: ESP/Tunnel 10.0.1.2[0]->84.74.90.110[0] spi=2811003002(0xa78c807a)
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  get pfkey UPDATE message
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  02020003 14000000 f7e99872 7f0e0000 02000100 00c3d973 04000202 00000000
Jan 02, 01:41:21  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 544a5a6e
Jan 02, 01:41:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 0a000102 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000300 00000000 00000000 00000000 80510100 00000000 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000400 00000000 00000000 00000000 000e0100 00000000 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0] spi=12835187(0xc3d973)
Jan 02, 01:41:21  Info     IKE  IPsec-SA established: ESP/Tunnel 84.74.90.110[0]->10.0.1.2[0] spi=12835187(0xc3d973)
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:21  Debug    IKE  get pfkey ADD message
Jan 02, 01:41:21  Debug    IKE
Jan 02, 01:41:21  Debug    IKE  02030003 14000000 f7e99872 7f0e0000 02000100 94b834a2 04000202 00000000
Jan 02, 01:41:21  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 0a000102
Jan 02, 01:41:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 544a5a6e 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000300 00000000 00000000 00000000 80510100 00000000 00000000 00000000
Jan 02, 01:41:21  Debug    IKE  04000400 00000000 00000000 00000000 000e0100 00000000 00000000 00000000
Jan 02, 01:41:21  Info     IKE  IPsec-SA established: ESP/Tunnel 10.0.1.2[0]->84.74.90.110[0] spi=2495100066(0x94b834a2)
Jan 02, 01:41:21  Debug    IKE  ===
Jan 02, 01:41:23  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netgear FVS328
Jan 02, 01:41:23  Debug    IKE  get pfkey DELETE message
Jan 02, 01:41:23  Debug    IKE
Jan 02, 01:41:23  Debug    IKE  02040032 0a000000 00000000 00000000 03000500 ff800000 10020000 0a000102
Jan 02, 01:41:23  Debug    IKE  00000000 00000000 03000600 ff800000 10020000 0a000102 00000000 00000000
```