IPSecuritas 3.x

Configuration Instructions

for

Zyxel ZyWALL

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.

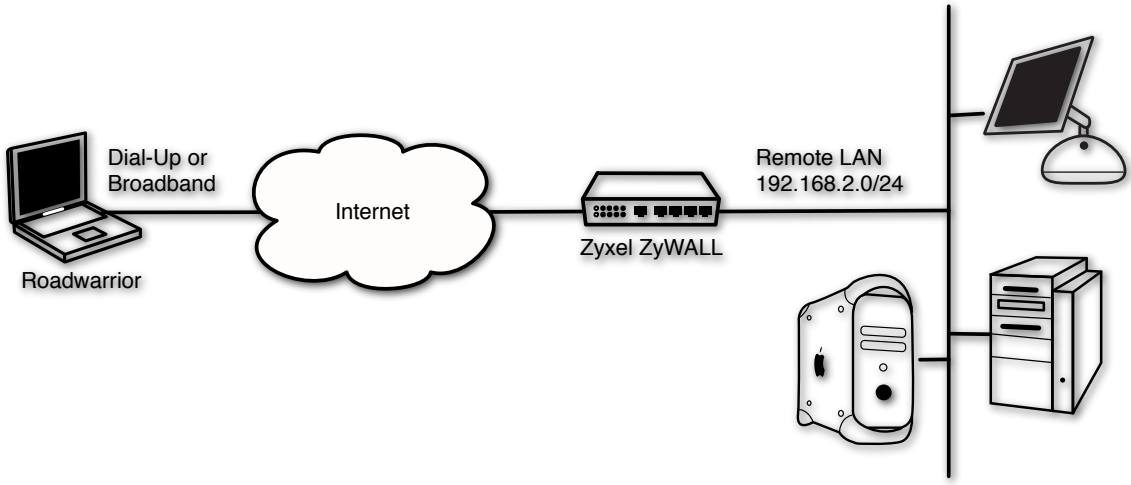
Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic 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

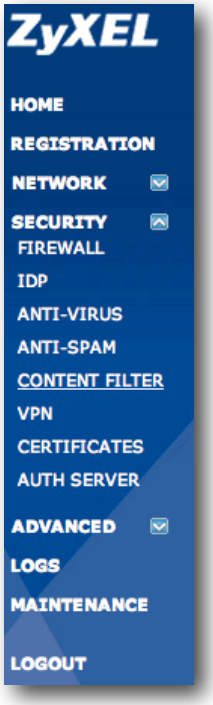
This document describes the steps necessary to establish a protected VPN connection between a Mac client and a Zyxel ZyWALL firewall. All information in this document is based on the following assumed network.



Zyxel ZyWALL Setup

This section describes the necessary steps to setup the Safe@Office firewall to accept incoming connections.

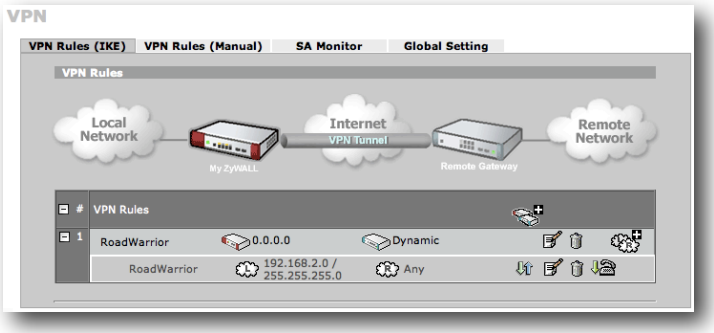
Login



Open a web browser and connect to your Zyxel firewall. Enter the administrator‘s password.

In the main menu on the left side, click on **SECURITY** to disclose the sub-entries and then click on **VPN**.

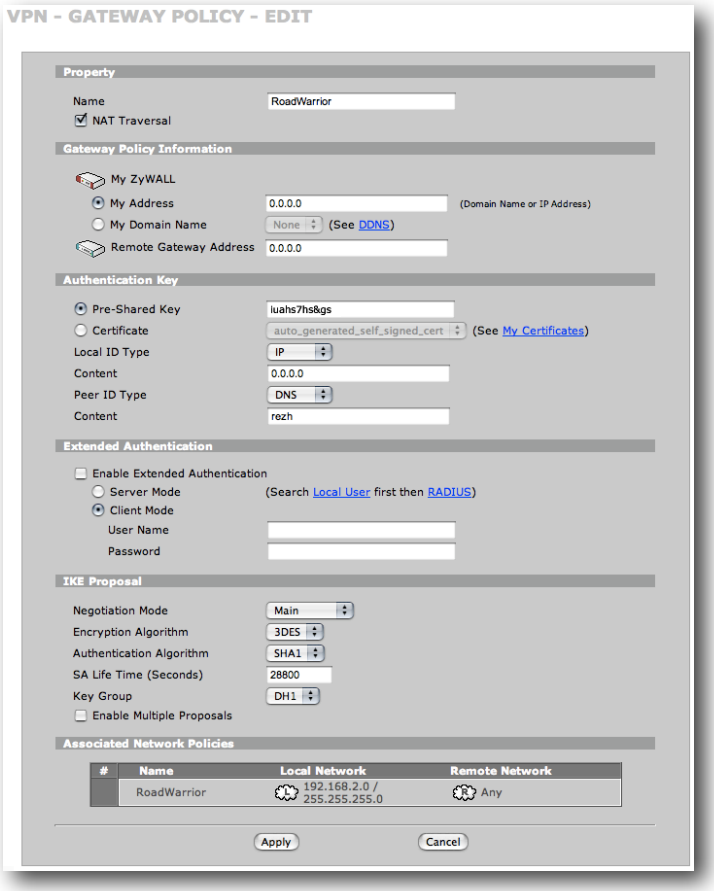
Add VPN Rule



A similar screen as depicted on the left should appear.

Add a new Gateway Policy by clicking on this symbol next to **VPN Rule** on the top line:

Create Gateway Policy



Fill in the Gateway Policy information as follows:

<u>Property</u>
Name: **An arbitrary name**
NAT Traversal: **Enabled**

<u>Gateway Policy Information</u>
My Address: **0.0.0.0**
Remote Gateway Address: **0.0.0.0**

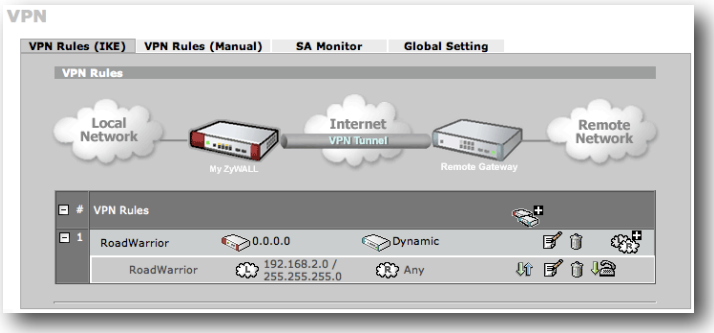
<u>Authentication Key</u>
Pre-Shared Key: **Enabled**
Local ID Type: **IP**
Content: **0.0.0.0**
Peer ID Type: **DNS**
Content: **Any string**

<u>Extended Authentication</u>:
Extended Authentication: **Disabled**

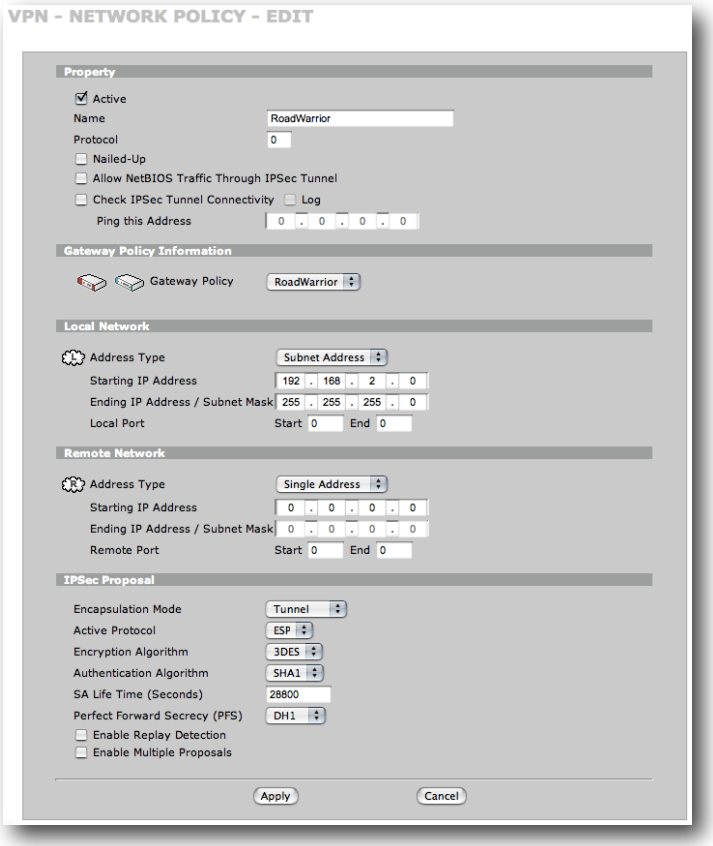
<u>IKE Proposal</u>
Negotiation Mode: **Main**
Encryption Algorithm: **3DES**
Authentication Algorithm: **SHA1**
SA Life Time: **28800**
Key Group: **DH1**
Enabled Multiple Proposals: **Disabled**

Please remember the **preshared key** and the **Peer ID** as you will need it when setting up the connection in IPSecuritas.
Click on apply when you are finished.

Create Network Policy



Back in the VPN overview, click on the disclose icon of the newly created Gateway Policy, then click on the this symbol to add a network policy:



Fill in the Network Policy information as follows:

<u>Property</u>
Active: **Enabled**
Name: **An arbitrary name**
Protocol: **0**
Nailed-Up: **Disabled**
Allow NetBIOS Traffic: **Disabled**
Check IPSec Tunnel: **Disabled**

<u>Gateway Policy Information</u>
Gateway Policy: **The newly created policy**

<u>Local Network</u>
Address Type: **Subnet Address**
Starting Address: **192.168.2.0**
Subnet Mask: **255.255.255.0**
Local Port: **0 - 0**

<u>Remote Network</u>
Address Type: Single **Address**
Starting IP Address: **0.0.0.0**

<u>IPSec Proposal</u>
Encapsulation Mode: **Tunnel**
Active Protocol: **ESP**
Encryption Algorithm: **3DES**
Authentication Algorithm: **SHA1**
SA Life Time: **28800**
Perfect Forward Secrecy: **DH1**
Enabled Replay Detection: **Disabled**
Enabled Multiple Proposals: **Disable**

Click on **Apply** to save the settings and finish the ZyWALL configuration. You may now proceed with the configuration of the connection in IPSecuritas now.

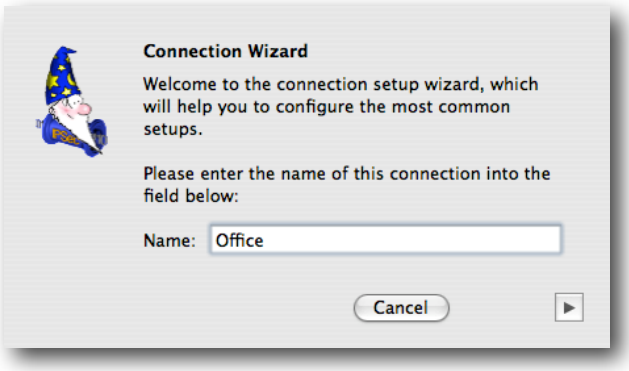
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the ZyWALL firewall.

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



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

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

Select Router Model

Select **Zyxel** from the manufacturer list and your **ZyWALL** model from the model list.

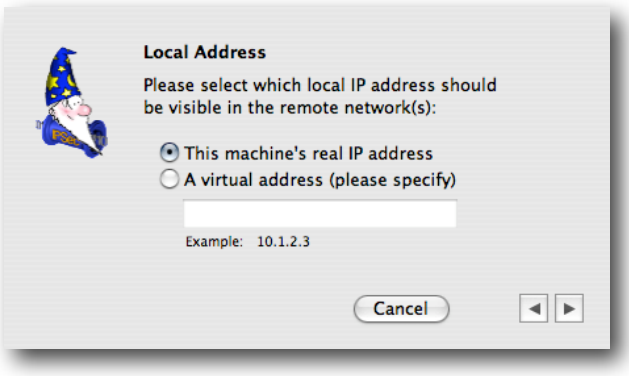
Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

Enter the public IP address or hostname of your Safe@Office firewall. 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.

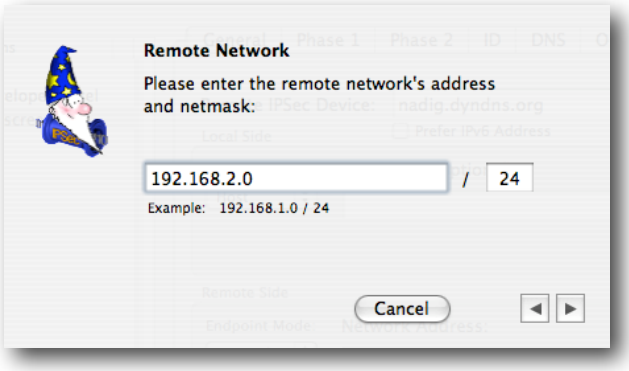
Enter a Virtual IP Address



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.

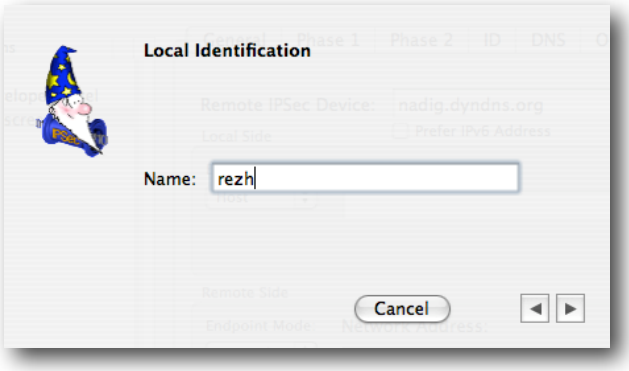
Enter Remote Network



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 ZyWALL.

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

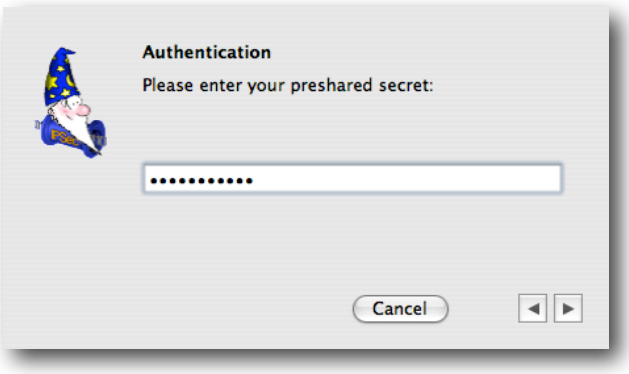
Enter Local Identication



Enter the ZyWALL's **local identification** (which you had to enter in the **Gateway Policy** setup of the ZyWALL).

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

Enter Preshared Key



Enter the same **Preshared Key** of the ZyWALL (which you had to enter in the **Gateway Policy** setup of the ZyWALL).

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 ZyWALL **local IP address**. If the tunnel works correctly, a similar output is displayed:

```
[MacBook:~] root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=19.290 ms
```

Sample Safe@Office Log Output

The following is a sample log from the ZyWALL after a successful connection establishment:

#	Time	Message	Source	Destination	Note
1	01/18/2000 11:30:35	Rule [Roadwarrior] Tunnel built successfully	192.168.215.2	192.168.215.225	IKE
2	01/18/2000 11:30:35	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
3	01/18/2000 11:30:34	Adjust TCP MSS to 1398	192.168.215.225	192.168.215.2	IKE
4	01/18/2000 11:30:34	Recv:[HASH]	192.168.215.2	192.168.215.225	IKE
5	01/18/2000 11:30:34	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
6	01/18/2000 11:30:34	Send:[HASH][SA][NONCE][KE][ID][ID]	192.168.215.225	192.168.215.2	IKE
7	01/18/2000 11:30:34	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.225	192.168.215.2	IKE
8	01/18/2000 11:30:33	Swap rule to rule [Roadwarrior]	192.168.215.2	192.168.215.225	IKE
9	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
10	01/18/2000 11:30:33	Swap rule to rule [Roadwarrior]	192.168.215.2	192.168.215.225	IKE
11	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
12	01/18/2000 11:30:33	Start Phase 2: Quick Mode	192.168.215.2	192.168.215.225	IKE
13	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
14	01/18/2000 11:30:33	Recv:[HASH][SA][NONCE][KE][ID][ID]	192.168.215.2	192.168.215.225	IKE
15	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
16	01/18/2000 11:30:33	Adjust TCP MSS to 1460	192.168.215.225	192.168.215.2	IKE
17	01/18/2000 11:30:33	Recv:[HASH][NOTFY:INIT_CONTACT]	192.168.215.2	192.168.215.225	IKE
18	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
19	01/18/2000 11:30:33	Phase 1 IKE SA process done	192.168.215.225	192.168.215.2	IKE
20	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.225	192.168.215.2	IKE
21	01/18/2000 11:30:33	Send:[ID][HASH]	192.168.215.225	192.168.215.2	IKE
22	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.225	192.168.215.2	IKE
23	01/18/2000 11:30:33	Recv:[ID][HASH]	192.168.215.2	192.168.215.225	IKE
24	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
25	01/18/2000 11:30:33	Send:[KE][NONCE][NATD][NATD]	192.168.215.225	192.168.215.2	IKE
26	01/18/2000 11:30:33	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.225	192.168.215.2	IKE
27	01/18/2000 11:30:32	Recv:[KE][NONCE][NATD][NATD]	192.168.215.2	192.168.215.225	IKE
28	01/18/2000 11:30:32	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
29	01/18/2000 11:30:32	Send:[SA][VID][VID][VID]	192.168.215.225	192.168.215.2	IKE
30	01/18/2000 11:30:32	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.225	192.168.215.2	IKE
31	01/18/2000 11:30:32	Recv:[SA][VID][VID][VID][VID][VID][3F9F3466	192.168.215.2	192.168.215.225	IKE
32	01/18/2000 11:30:32	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE

33	01/18/2000 11:30:32	Recv Main Mode request from [192.168.215.2]	192.168.215.2	192.168.215.225	IKE
34	01/18/2000 11:30:32	Rule [Road Warrier] Receiving IKE request	192.168.215.2	192.168.215.225	IKE
35	01/18/2000 11:30:32	The cookie pair is : 0x113CF0DDD0FD274E / 0x8F1739363F9F3466	192.168.215.2	192.168.215.225	IKE
36	01/18/2000 11:30:28	Send:[HASH][DEL]	192.168.215.225	192.168.215.2	IKE
37	01/18/2000 11:30:28	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.225	192.168.215.2	IKE
38	01/18/2000 11:30:28	Recv:[HASH][DEL]	192.168.215.2	192.168.215.225	IKE
39	01/18/2000 11:30:28	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
40	01/18/2000 11:30:24	Rule [Roadwarrior] Tunnel built successfully	192.168.215.2	192.168.215.225	IKE
41	01/18/2000 11:30:24	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
42	01/18/2000 11:30:24	Adjust TCP MSS to 1398	192.168.215.225	192.168.215.2	IKE
43	01/18/2000 11:30:23	Recv:[HASH]	192.168.215.2	192.168.215.225	IKE
44	01/18/2000 11:30:23	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
45	01/18/2000 11:30:23	Send:[HASH][SA][NONCE][KE][ID][ID]	192.168.215.225	192.168.215.2	IKE
46	01/18/2000 11:30:23	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.225	192.168.215.2	IKE
47	01/18/2000 11:30:23	Swap rule to rule [Roadwarrior]	192.168.215.2	192.168.215.225	IKE
48	01/18/2000 11:30:23	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
49	01/18/2000 11:30:23	Swap rule to rule [Roadwarrior]	192.168.215.2	192.168.215.225	IKE
50	01/18/2000 11:30:23	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
51	01/18/2000 11:30:23	Start Phase 2: Quick Mode	192.168.215.2	192.168.215.225	IKE
52	01/18/2000 11:30:23	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
53	01/18/2000 11:30:23	Recv:[HASH][SA][NONCE][KE][ID][ID]	192.168.215.2	192.168.215.225	IKE
54	01/18/2000 11:30:23	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
55	01/18/2000 11:30:22	Recv:[HASH][NOTFY:INIT_CONTACT]	192.168.215.2	192.168.215.225	IKE
56	01/18/2000 11:30:22	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
57	01/18/2000 11:30:22	Phase 1 IKE SA process done	192.168.215.225	192.168.215.2	IKE
58	01/18/2000 11:30:22	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.225	192.168.215.2	IKE
59	01/18/2000 11:30:22	Send:[ID][HASH][NOTFY:INIT_CONTACT]257E89EF	192.168.215.225	192.168.215.2	IKE
60	01/18/2000 11:30:22	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.225	192.168.215.2	IKE
61	01/18/2000 11:30:22	Recv:[ID][HASH]	192.168.215.2	192.168.215.225	IKE
62	01/18/2000 11:30:22	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
63	01/18/2000 11:30:22	Send:[KE][NONCE][NATD][NATD]	192.168.215.225	192.168.215.2	IKE
64	01/18/2000 11:30:22	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.225	192.168.215.2	IKE
65	01/18/2000 11:30:22	Recv:[KE][NONCE][NATD][NATD]	192.168.215.2	192.168.215.225	IKE
66	01/18/2000 11:30:22	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
67	01/18/2000 11:30:21	Send:[SA][VID][VID][VID]	192.168.215.225	192.168.215.2	IKE
68	01/18/2000 11:30:21	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.225	192.168.215.2	IKE
69	01/18/2000 11:30:21	Recv:[SA][VID][VID][VID][VID][VID][257E89EF	192.168.215.2	192.168.215.225	IKE
70	01/18/2000 11:30:21	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE
71	01/18/2000 11:30:21	Recv Main Mode request from [192.168.215.2]	192.168.215.2	192.168.215.225	IKE
72	01/18/2000 11:30:21	Rule [Road Warrier] Receiving IKE request	192.168.215.2	192.168.215.225	IKE
73	01/18/2000 11:30:21	The cookie pair is : 0x4FC636F2B4F809F7 / 0x3826ACF5257E89EF	192.168.215.2	192.168.215.225	IKE

Sample IPSecuritas Log Output

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

```
IPSecuritas 3.0rc3 build 1669, Thu May 17 08:30:27 CEST 2007, nadig
Darwin 8.9.1 Darwin Kernel Version 8.9.1: Thu Feb 22 20:55:00 PST 2007; root:xnu-792.18.15~1/RELEASE_I386 i386

May 18, 22:50:20  Debug    APP  State change from IDLE to AUTHENTICATING after event START
May 18, 22:50:20  Info     APP  IKE daemon started
May 18, 22:50:20  Info     APP  IPSec started
May 18, 22:50:20  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
May 18, 22:50:20  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 18, 22:50:20  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 18, 22:50:20  Info     IKE  Foreground mode.
May 18, 22:50:20  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
May 18, 22:50:20  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
May 18, 22:50:20  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
May 18, 22:50:20  Info     IKE  Resize address pool from 0 to 255
May 18, 22:50:20  Debug    IKE  lifetime = 480
May 18, 22:50:20  Debug    IKE  lifebyte = 0
May 18, 22:50:20  Debug    IKE  encklen=0
May 18, 22:50:20  Debug    IKE  p:1 t:1
May 18, 22:50:20  Debug    IKE  DES-CBC(1)
May 18, 22:50:20  Debug    IKE  MD5(1)
May 18, 22:50:20  Debug    IKE  768-bit MODP group(1)
May 18, 22:50:20  Debug    IKE  pre-shared key(1)
May 18, 22:50:20  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
May 18, 22:50:20  Debug    IKE  parse successed.
May 18, 22:50:20  Debug    IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
May 18, 22:50:20  Info     IKE  192.168.215.2[4500] used as isakmp port (fd=7)
May 18, 22:50:20  Info     IKE  192.168.215.2[500] used as isakmp port (fd=8)
May 18, 22:50:20  Debug    IKE  get pfkey X_SPDDUMP message
May 18, 22:50:20  Debug    IKE  02120000 0f000100 01000000 ee180000 03000500 ff180000 10020000 0a010200
May 18, 22:50:20  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 0a010202 00000000 00000000
May 18, 22:50:20  Debug    IKE  07001200 02000100 38a70900 00000000 28003200 02020000 10020000 c0a8d7e1
May 18, 22:50:20  Debug    IKE  00000000 00000000 10020000 c0a8d702 00000000 00000000
May 18, 22:50:20  Debug    IKE  get pfkey X_SPDDUMP message
May 18, 22:50:20  Debug    IKE  02120000 0f000100 00000000 ee180000 03000500 ff200000 10020000 0a010202
May 18, 22:50:20  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 0a010200 00000000 00000000
May 18, 22:50:20  Debug    IKE  07001200 02000200 37a70900 00000000 28003200 02020000 10020000 c0a8d702
May 18, 22:50:20  Debug    IKE  00000000 00000000 10020000 c0a8d7e1 00000000 00000000
May 18, 22:50:20  Debug    IKE  sub:0xbffff340: 10.1.2.2/32[0] 10.1.2.0/24[0] proto=any dir=out
May 18, 22:50:20  Debug    IKE  db :0x308bb8: 10.1.2.0/24[0] 10.1.2.2/32[0] proto=any dir=in
May 18, 22:50:21  Info     APP  Initiated connection Zyxel P1
May 18, 22:50:21  Debug    IKE  get pfkey ACQUIRE message
May 18, 22:50:21  Debug    IKE  02060003 14000000 d5010000 b90b0000 03000500 ff200000 10020000 c0a8d702
May 18, 22:50:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e1 00000000 00000000
May 18, 22:50:21  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
May 18, 22:50:21  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
May 18, 22:50:21  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 37a70900 00000000
May 18, 22:50:21  Debug    IKE  suitable outbound SP found: 10.1.2.2/32[0] 10.1.2.0/24[0] proto=any dir=out.
May 18, 22:50:21  Debug    IKE  sub:0xbffff31c: 10.1.2.0/24[0] 10.1.2.2/32[0] proto=any dir=in
May 18, 22:50:21  Debug    IKE  db :0x308bb8: 10.1.2.0/24[0] 10.1.2.2/32[0] proto=any dir=in
May 18, 22:50:21  Debug    IKE  suitable inbound SP found: 10.1.2.0/24[0] 10.1.2.2/32[0] proto=any dir=in.
May 18, 22:50:21  Debug    IKE  new acquire 10.1.2.2/32[0] 10.1.2.0/24[0] proto=any dir=out
May 18, 22:50:21  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:50:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:50:21  Debug    IKE  in post_acquire
May 18, 22:50:21  Debug    IKE  configuration found for 192.168.215.225.
May 18, 22:50:21  Info     IKE  IPsec-SA request for 192.168.215.225 queued due to no phase1 found.
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Info     IKE  initiate new phase 1 negotiation: 192.168.215.2[500]<=>192.168.215.225[500]
May 18, 22:50:21  Info     IKE  begin Identity Protection mode.
May 18, 22:50:21  Debug    IKE  new cookie:
May 18, 22:50:21  Debug    IKE  8f1739363f9f3466
May 18, 22:50:21  Debug    IKE  add payload of len 48, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
```

```
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 13
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 0
May 18, 22:50:21  Debug    IKE  320 bytes from 192.168.215.2[500] to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  1 times of 320 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 00000000 00000000 01100200 00000000 00000140 0d000034
May 18, 22:50:21  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c01e0
May 18, 22:50:21  Debug    IKE  80010001 80030001 80020001 80040001 0d000014 4a131c81 07035845 5c5728f2
May 18, 22:50:21  Debug    IKE  0e95452f 0d000014 8f8d8382 6d246b6f c7a8a6a4 28c11de8 0d000014 439b59f8
May 18, 22:50:21  Debug    IKE  ba676c4c 7737ae22 eab8f582 0d000014 4d1e0e13 6deafa34 c4f3ea9f 02ec7285
May 18, 22:50:21  Debug    IKE  0d000014 80d0bb3d ef54565e e84645d4 c85ce3ee 0d000014 9909b64e ed937c65
May 18, 22:50:21  Debug    IKE  73de52ac e952fa6b 0d000014 7d9419a6 5310ca6f 2c179d92 15529d56 0d000014
May 18, 22:50:21  Debug    IKE  cd604643 35df21f8 7cfdb2fc 68b6a448 0d000014 90cb8091 3ebb696e 086381b5
May 18, 22:50:21  Debug    IKE  ec427b1f 0d000014 16f6ca16 e4a4066d 83821a0f 0aeaa862 0d000014 4485152d
May 18, 22:50:21  Debug    IKE  18b6bbcd 0be8a846 9579ddcc 00000014 afcad713 68a1f1c9 6b8696fc 77570100
May 18, 22:50:21  Debug    IKE  resend phase1 packet 8f1739363f9f3466:0000000000000000
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Debug    IKE  148 bytes message received from 192.168.215.225[500] to 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 01100200 00000000 00000094 0d000038
May 18, 22:50:21  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 80010001 80020001
May 18, 22:50:21  Debug    IKE  80030001 80040001 800b0001 000c0004 000001e0 0d000014 4485152d 18b6bbcd
May 18, 22:50:21  Debug    IKE  0be8a846 9579ddcc 0d000012 afcad713 68a1f1c9 6b8696fc 77570000 00186250
May 18, 22:50:21  Debug    IKE  27749d5a b97f5616 c1602765 cf480a3b 7d0b0000
May 18, 22:50:21  Debug    IKE  begin.
May 18, 22:50:21  Debug    IKE  seen nptype=1(sa)
May 18, 22:50:21  Debug    IKE  seen nptype=13(vid)
May 18, 22:50:21  Debug    IKE  seen nptype=13(vid)
May 18, 22:50:21  Debug    IKE  seen nptype=13(vid)
May 18, 22:50:21  Debug    IKE  succeed.
May 18, 22:50:21  Info     IKE  received Vendor ID: draft-ietf-ipsec-nat-t-ike-00
May 18, 22:50:21  Debug    IKE  received unknown Vendor ID
May 18, 22:50:21  Debug    IKE  afcad713 68a1f1c9 6b8696fc 7757
May 18, 22:50:21  Debug    IKE  received unknown Vendor ID
May 18, 22:50:21  Debug    IKE  62502774 9d5ab97f 5616c160 2765cf48 0a3b7d0b
May 18, 22:50:21  Info     IKE  Selected NAT-T version: draft-ietf-ipsec-nat-t-ike-00
May 18, 22:50:21  Debug    IKE  total SA len=52
May 18, 22:50:21  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 80010001 80020001
May 18, 22:50:21  Debug    IKE  80030001 80040001 800b0001 000c0004 000001e0
May 18, 22:50:21  Debug    IKE  begin.
May 18, 22:50:21  Debug    IKE  seen nptype=2(prop)
May 18, 22:50:21  Debug    IKE  succeed.
May 18, 22:50:21  Debug    IKE  proposal #1 len=44
May 18, 22:50:21  Debug    IKE  begin.
May 18, 22:50:21  Debug    IKE  seen nptype=3(trns)
May 18, 22:50:21  Debug    IKE  succeed.
May 18, 22:50:21  Debug    IKE  transform #1 len=36
May 18, 22:50:21  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=DES-CBC
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=MD5
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 18, 22:50:21  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
May 18, 22:50:21  Debug    IKE  hmac(modp768)
May 18, 22:50:21  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:21  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
May 18, 22:50:21  Debug    IKE  pair 1:
May 18, 22:50:21  Debug    IKE  0x3096c0: next=0x0 tnext=0x0
May 18, 22:50:21  Debug    IKE  proposal #1: 1 transform
May 18, 22:50:21  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
May 18, 22:50:21  Debug    IKE  trns#=1, trns-id=IKE
May 18, 22:50:21  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=DES-CBC
May 18, 22:50:21  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=MD5
May 18, 22:50:21  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 18, 22:50:21  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
May 18, 22:50:21  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:21  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
```

```
May 18, 22:50:21  Debug    IKE  Compared: DB:Peer
May 18, 22:50:21  Debug    IKE  (lifetime = 480:480)
May 18, 22:50:21  Debug    IKE  (lifebyte = 0:0)
May 18, 22:50:21  Debug    IKE  enctype = DES-CBC:DES-CBC
May 18, 22:50:21  Debug    IKE  (encklen = 0:0)
May 18, 22:50:21  Debug    IKE  hashtype = MD5:MD5
May 18, 22:50:21  Debug    IKE  authmethod = pre-shared key:pre-shared key
May 18, 22:50:21  Debug    IKE  dh_group = 768-bit MODP group:768-bit MODP group
May 18, 22:50:21  Debug    IKE  an acceptable proposal found.
May 18, 22:50:21  Debug    IKE  hmac(modp768)
May 18, 22:50:21  Debug    IKE  agreed on pre-shared key auth.
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Debug    IKE  compute DH's private.
May 18, 22:50:21  Debug    IKE  5a29bd56 686af3d6 9e385b0c 160cabd0 24d706ad fe04ee82 b04a5911 28461953
May 18, 22:50:21  Debug    IKE  3df4b21d f0146640 7ba64523 d277ac84 fcee6287 3f3f2067 1fbfe0eb 82950b96
May 18, 22:50:21  Debug    IKE  e8bb1b9b 635428f7 2db0f07a bd97ec5a 9c224bf3 5642961f 3a2d5732 e0402895
May 18, 22:50:21  Debug    IKE  compute DH's public.
May 18, 22:50:21  Debug    IKE  ac576921 acb91cb5 81aacee0 51d6b014 b222d404 062451f3 6ac6bbb7 92b0989e
May 18, 22:50:21  Debug    IKE  4b43f46f 1bda23e9 f16b3e0e 2cb6e44c dccfdb12 504b3e48 5a8802d7 8d4323ec
May 18, 22:50:21  Debug    IKE  e413afad bcb85d8b 5be55817 ee442325 1495d12c 9c6188cb 9d39ecc4 40a5327f
May 18, 22:50:21  Info     IKE  Hashing 192.168.215.225[500] with algo #1
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Info     IKE  Hashing 192.168.215.2[500] with algo #1
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Info     IKE  Adding remote and local NAT-D payloads.
May 18, 22:50:21  Debug    IKE  add payload of len 96, next type 10
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 130
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 130
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 0
May 18, 22:50:21  Debug    IKE  188 bytes from 192.168.215.2[500] to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  1 times of 188 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 04100200 00000000 000000bc 0a000064
May 18, 22:50:21  Debug    IKE  ac576921 acb91cb5 81aacee0 51d6b014 b222d404 062451f3 6ac6bbb7 92b0989e
May 18, 22:50:21  Debug    IKE  4b43f46f 1bda23e9 f16b3e0e 2cb6e44c dccfdb12 504b3e48 5a8802d7 8d4323ec
May 18, 22:50:21  Debug    IKE  e413afad bcb85d8b 5be55817 ee442325 1495d12c 9c6188cb 9d39ecc4 40a5327f
May 18, 22:50:21  Debug    IKE  82000014 f4487fb4 358d79ac c772bf12 7c3e47ad 82000014 41e178ad ae526bb1
May 18, 22:50:21  Debug    IKE  9ccf0274 2ced0155 00000014 ce120d3d 6659dab7 604dbf4f afffa394
May 18, 22:50:21  Debug    IKE  resend phase1 packet 8f1739363f9f3466:113cf0ddd0fd274e
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Debug    IKE  192 bytes message received from 192.168.215.225[500] to 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 04100200 00000000 000000c0 0a000064
May 18, 22:50:21  Debug    IKE  88a30f55 e2f485bc 404b0e65 ded18562 64a124da cd1d7dd1 139096ef 6ae0a1f0
May 18, 22:50:21  Debug    IKE  e83ecfa6 4306f058 f55ce9c7 2e534dfe 945c5135 70003104 b3992bd7 e037a893
May 18, 22:50:21  Debug    IKE  2cf4031b 2ab89de5 47dd2733 3fd4b82d ff78d822 41e68bb8 103ff033 691ea95d
May 18, 22:50:21  Debug    IKE  82000018 8beafdea 8fd58e38 ff13cd61 558b0ce7 3c50abdf 82000014 ce120d3d
May 18, 22:50:21  Debug    IKE  6659dab7 604dbf4f afffa394 00000014 41e178ad ae526bb1 9ccf0274 2ced0155
May 18, 22:50:21  Debug    IKE  begin.
May 18, 22:50:21  Debug    IKE  seen nptype=4(ke)
May 18, 22:50:21  Debug    IKE  seen nptype=10(nonce)
May 18, 22:50:21  Debug    IKE  seen nptype=130(nat-d)
May 18, 22:50:21  Debug    IKE  seen nptype=130(nat-d)
May 18, 22:50:21  Debug    IKE  succeed.
May 18, 22:50:21  Info     IKE  Hashing 192.168.215.2[500] with algo #1
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Info     IKE  NAT-D payload #0 verified
May 18, 22:50:21  Info     IKE  Hashing 192.168.215.225[500] with algo #1
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Info     IKE  NAT-D payload #1 verified
May 18, 22:50:21  Info     IKE  NAT not detected
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Debug    IKE  compute DH's shared.
May 18, 22:50:21  Debug    IKE  bea3f93a ded3e0b3 e5020f2e 9eaa885e 777fbe65 06eb58d6 df967ce2 8c53f266
May 18, 22:50:21  Debug    IKE  e23f278f 06a15fe9 0db7dfc4 775ba7f1 7478c77d 7292f5fb 1050106c 18ee75f0
May 18, 22:50:21  Debug    IKE  4427e5eb 844cf6fb 86054ccf 97ee625f 245580e8 1efdb951 db18b5b8 754561d0
May 18, 22:50:21  Debug    IKE  the psk found.
May 18, 22:50:21  Debug    IKE  psk: 2007-05-18 22:50:21: DEBUG2:
May 18, 22:50:21  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
May 18, 22:50:21  Debug    IKE  nonce 1: 2007-05-18 22:50:21: DEBUG:
May 18, 22:50:21  Debug    IKE  f4487fb4 358d79ac c772bf12 7c3e47ad
May 18, 22:50:21  Debug    IKE  nonce 2: 2007-05-18 22:50:21: DEBUG:
May 18, 22:50:21  Debug    IKE  8beafdea 8fd58e38 ff13cd61 558b0ce7 3c50abdf
```

```
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  SKEYID computed:
May 18, 22:50:21  Debug    IKE  342fd03e fb4771e8 7673ec27 224046f2
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  SKEYID_d computed:
May 18, 22:50:21  Debug    IKE  619d16df 54dae618 53f771f4 6b14a046
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  SKEYID_a computed:
May 18, 22:50:21  Debug    IKE  1a5a346a af5b2412 ded3e66f 9de12e1e
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  SKEYID_e computed:
May 18, 22:50:21  Debug    IKE  a6b9d6c5 6ccc0fc9 fd7df9f8 0fb935c6
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Debug    IKE  final encryption key computed:
May 18, 22:50:21  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  IV computed:
May 18, 22:50:21  Debug    IKE  9acd877f f38cab04
May 18, 22:50:21  Debug    IKE  use ID type of FQDN
May 18, 22:50:21  Debug    IKE  HASH with:
May 18, 22:50:21  Debug    IKE  ac576921 acb91cb5 81aacee0 51d6b014 b222d404 062451f3 6ac6bbb7 92b0989e
May 18, 22:50:21  Debug    IKE  4b43f46f 1bda23e9 f16b3e0e 2cb6e44c dccfdb12 504b3e48 5a8802d7 8d4323ec
May 18, 22:50:21  Debug    IKE  e413afad bcb85d8b 5be55817 ee442325 1495d12c 9c6188cb 9d39ecc4 40a5327f
May 18, 22:50:21  Debug    IKE  88a30f55 e2f485bc 404b0e65 ded18562 64a124da cd1d7dd1 139096ef 6ae0a1f0
May 18, 22:50:21  Debug    IKE  e83ecfa6 4306f058 f55ce9c7 2e534dfe 945c5135 70003104 b3992bd7 e037a893
May 18, 22:50:21  Debug    IKE  2cf4031b 2ab89de5 47dd2733 3fd4b82d ff78d822 41e68bb8 103ff033 691ea95d
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 00000001 00000001 00000028 01010001
May 18, 22:50:21  Debug    IKE  00000020 01010000 800b0001 800c01e0 80010001 80030001 80020001 80040001
May 18, 22:50:21  Debug    IKE  02000000 6e616469 67
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  HASH (init) computed:
May 18, 22:50:21  Debug    IKE  0396714d ab91cc8d eac0692a 0a10654c
May 18, 22:50:21  Debug    IKE  add payload of len 9, next type 8
May 18, 22:50:21  Debug    IKE  add payload of len 16, next type 0
May 18, 22:50:21  Debug    IKE  begin encryption.
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  pad length = 7
May 18, 22:50:21  Debug    IKE  0800000d 02000000 6e616469 67000000 14039671 4dab91cc 8deac069 2a0a1065
May 18, 22:50:21  Debug    IKE  4c000000 00000007
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  with key:
May 18, 22:50:21  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:21  Debug    IKE  encrypted payload by IV:
May 18, 22:50:21  Debug    IKE  9acd877f f38cab04
May 18, 22:50:21  Debug    IKE  save IV for next:
May 18, 22:50:21  Debug    IKE  e832ca1f 5923e12a
May 18, 22:50:21  Debug    IKE  encrypted.
May 18, 22:50:21  Debug    IKE  68 bytes from 192.168.215.2[500] to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  1 times of 68 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 05100201 00000000 00000044 95ceb5f7
May 18, 22:50:21  Debug    IKE  786e052a 4ed622c3 b9358ba8 81ee52d6 187a18c0 4ddef0e1 d3f08601 e832ca1f
May 18, 22:50:21  Debug    IKE  5923e12a
May 18, 22:50:21  Debug    IKE  resend phase1 packet 8f1739363f9f3466:113cf0ddd0fd274e
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Debug    IKE  60 bytes message received from 192.168.215.225[500] to 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 05100201 00000000 0000003c 66a35520
May 18, 22:50:21  Debug    IKE  225a18df 834cecfa 8c74806a 5336b921 b5d8e7cb 1ed2b4ca e30bae22
May 18, 22:50:21  Debug    IKE  begin decryption.
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  IV was saved for next processing:
May 18, 22:50:21  Debug    IKE  1ed2b4ca e30bae22
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  with key:
May 18, 22:50:21  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:21  Debug    IKE  decrypted payload by IV:
May 18, 22:50:21  Debug    IKE  e832ca1f 5923e12a
May 18, 22:50:21  Debug    IKE  decrypted payload, but not trimed.
May 18, 22:50:21  Debug    IKE  0800000c 01000000 c0a8d7e1 00000014 14c867e9 69ed8aa7 63e84fb7 ca85ffa9
May 18, 22:50:21  Debug    IKE  padding len=169
```

```
May 18, 22:50:21  Debug    IKE  skip to trim padding.
May 18, 22:50:21  Debug    IKE  decrypted.
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 05100201 00000000 0000003c 0800000c
May 18, 22:50:21  Debug    IKE  01000000 c0a8d7e1 00000014 14c867e9 69ed8aa7 63e84fb7 ca85ffa9
May 18, 22:50:21  Debug    IKE  begin.
May 18, 22:50:21  Debug    IKE  seen nptype=5(id)
May 18, 22:50:21  Debug    IKE  seen nptype=8(hash)
May 18, 22:50:21  Debug    IKE  succeed.
May 18, 22:50:21  Debug    IKE  HASH received:
May 18, 22:50:21  Debug    IKE  14c867e9 69ed8aa7 63e84fb7 ca85ffa9
May 18, 22:50:21  Debug    IKE  HASH with:
May 18, 22:50:21  Debug    IKE  88a30f55 e2f485bc 404b0e65 ded18562 64a124da cd1d7dd1 139096ef 6ae0a1f0
May 18, 22:50:21  Debug    IKE  e83ecfa6 4306f058 f55ce9c7 2e534dfe 945c5135 70003104 b3992bd7 e037a893
May 18, 22:50:21  Debug    IKE  2cf4031b 2ab89de5 47dd2733 3fd4b82d ff78d822 41e68bb8 103ff033 691ea95d
May 18, 22:50:21  Debug    IKE  ac576921 acb91cb5 81aacee0 51d6b014 b222d404 062451f3 6ac6bbb7 92b0989e
May 18, 22:50:21  Debug    IKE  4b43f46f 1bda23e9 f16b3e0e 2cb6e44c dccfdb12 504b3e48 5a8802d7 8d4323ec
May 18, 22:50:21  Debug    IKE  e413afad bcb85d8b 5be55817 ee442325 1495d12c 9c6188cb 9d39ecc4 40a5327f
May 18, 22:50:21  Debug    IKE  113cf0dd d0fd274e 8f173936 3f9f3466 00000001 00000001 00000028 01010001
May 18, 22:50:21  Debug    IKE  00000020 01010000 800b0001 800c01e0 80010001 80030001 80020001 80040001
May 18, 22:50:21  Debug    IKE  01000000 c0a8d7e1
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  HASH (init) computed:
May 18, 22:50:21  Debug    IKE  14c867e9 69ed8aa7 63e84fb7 ca85ffa9
May 18, 22:50:21  Debug    IKE  HASH for PSK validated.
May 18, 22:50:21  Debug    IKE  peer's ID:2007-05-18 22:50:21: DEBUG:
May 18, 22:50:21  Debug    IKE  01000000 c0a8d7e1
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:21  Debug    IKE  compute IV for phase2
May 18, 22:50:21  Debug    IKE  phase1 last IV:
May 18, 22:50:21  Debug    IKE  1ed2b4ca e30bae22 8e6d91e0
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  phase2 IV computed:
May 18, 22:50:21  Debug    IKE  ce208a53 892a50fc
May 18, 22:50:21  Debug    IKE  HASH with:
May 18, 22:50:21  Debug    IKE  8e6d91e0 0000001c 00000001 01106002 8f173936 3f9f3466 113cf0dd d0fd274e
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  HASH computed:
May 18, 22:50:21  Debug    IKE  05d7de00 425ef47e 9496ebb2 65434865
May 18, 22:50:21  Debug    IKE  begin encryption.
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  pad length = 8
May 18, 22:50:21  Debug    IKE  0b000014 05d7de00 425ef47e 9496ebb2 65434865 0000001c 00000001 01106002
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 00000000 00000008
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  with key:
May 18, 22:50:21  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:21  Debug    IKE  encrypted payload by IV:
May 18, 22:50:21  Debug    IKE  ce208a53 892a50fc
May 18, 22:50:21  Debug    IKE  save IV for next:
May 18, 22:50:21  Debug    IKE  7bc939e7 2964cfa6
May 18, 22:50:21  Debug    IKE  encrypted.
May 18, 22:50:21  Debug    IKE  84 bytes from 192.168.215.2[500] to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 08100501 8e6d91e0 00000054 7a356613
May 18, 22:50:21  Debug    IKE  0272a550 1a8d2797 abbc7bbe aa9e2d17 13650285 98a02680 d9249c0c acac9c0f
May 18, 22:50:21  Debug    IKE  d141a0f5 69b50528 874879cd 7bc939e7 2964cfa6
May 18, 22:50:21  Debug    IKE  sendto Information notify.
May 18, 22:50:21  Debug    IKE  IV freed
May 18, 22:50:21  Info     IKE  ISAKMP-SA established 192.168.215.2[500]-192.168.215.225[500] spi:
8f1739363f9f3466:113cf0ddd0fd274e
May 18, 22:50:21  Debug    IKE  ===
May 18, 22:50:22  Debug    IKE  msg 16 not interesting
May 18, 22:50:22  Debug    IKE  ===
May 18, 22:50:22  Debug    IKE  begin QUICK mode.
May 18, 22:50:22  Info     IKE  initiate new phase 2 negotiation: 192.168.215.2[500]<=>192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  compute IV for phase2
May 18, 22:50:22  Debug    IKE  phase1 last IV:
May 18, 22:50:22  Debug    IKE  1ed2b4ca e30bae22 daec08f0
May 18, 22:50:22  Debug    IKE  hash(md5)
May 18, 22:50:22  Debug    IKE  encryption(des)
```

```
May 18, 22:50:22  Debug    IKE  phase2 IV computed:
May 18, 22:50:22  Debug    IKE  36338123 a4bdf618
May 18, 22:50:22  Debug    IKE  call pfkey_send_getspi
May 18, 22:50:22  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.225[0]->192.168.215.2[0]
May 18, 22:50:22  Debug    IKE  pfkey getspi sent.
May 18, 22:50:22  Debug    IKE  get pfkey GETSPI message
May 18, 22:50:22  Debug    IKE  02010003 0a000000 d5010000 ee180000 02000100 079d6fea 0e580000 746f7068
May 18, 22:50:22  Debug    IKE  03000500 ff200000 10020000 c0a8d7e1 00000000 00000000 03000600 ff200000
May 18, 22:50:22  Debug    IKE  10020000 c0a8d702 00000000 00000000
May 18, 22:50:22  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.225[0]->192.168.215.2[0]
spi=127758314(0x79d6fea)
May 18, 22:50:22  Debug    IKE  hmac(modp768)
May 18, 22:50:22  Debug    IKE  hmac(modp768)
May 18, 22:50:22  Debug    IKE  hmac(modp768)
May 18, 22:50:22  Debug    IKE  compute DH's private.
May 18, 22:50:22  Debug    IKE  419440be c16f93ab c1b4a503 1320c4c1 3d9c8b31 0daf2a14 ed1e47fd c7c0b3a3
May 18, 22:50:22  Debug    IKE  8715628b 14b76f70 bfe17191 6e74e5cc ef9f396f 5e8a4fc5 d332b148 8619f982
May 18, 22:50:22  Debug    IKE  dbaff398 1b4cbc96 155a6b7a e1fdf6cb 676fc892 a80f55f2 39766f28 bf2cb21e
May 18, 22:50:22  Debug    IKE  compute DH's public.
May 18, 22:50:22  Debug    IKE  b9685992 243f8657 adac1d90 95a25ac5 d8e177b1 99a5e1da 8219cff0 bb34af6c
May 18, 22:50:22  Debug    IKE  255d9c6b f64fb794 652cf3f5 d52b9046 c8f205c6 bf3b967a 60e50073 59096b0d
May 18, 22:50:22  Debug    IKE  6748c4c6 cc3c37f7 587671e5 96ba530e 325eb7a4 0998f46a 389bf876 0b200b04
May 18, 22:50:22  Debug    IKE  use local ID type IPv4_address
May 18, 22:50:22  Debug    IKE  use remote ID type IPv4_subnet
May 18, 22:50:22  Debug    IKE  IDci:
May 18, 22:50:22  Debug    IKE  01000000 0a010202
May 18, 22:50:22  Debug    IKE  IDcr:
May 18, 22:50:22  Debug    IKE  04000000 0a010200 ffffff00
May 18, 22:50:22  Debug    IKE  add payload of len 48, next type 10
May 18, 22:50:22  Debug    IKE  add payload of len 16, next type 4
May 18, 22:50:22  Debug    IKE  add payload of len 96, next type 5
May 18, 22:50:22  Debug    IKE  add payload of len 8, next type 5
May 18, 22:50:22  Debug    IKE  add payload of len 12, next type 0
May 18, 22:50:22  Debug    IKE  HASH with:
May 18, 22:50:22  Debug    IKE  daec08f0 0a000034 00000001 00000001 00000028 01030401 079d6fea 0000001c
May 18, 22:50:22  Debug    IKE  01030000 80010001 800201e0 80040001 80050002 80030001 04000014 f3b8c86f
May 18, 22:50:22  Debug    IKE  aaf09bcc 4234f534 6dfe42d8 05000064 b9685992 243f8657 adac1d90 95a25ac5
May 18, 22:50:22  Debug    IKE  d8e177b1 99a5e1da 8219cff0 bb34af6c 255d9c6b f64fb794 652cf3f5 d52b9046
May 18, 22:50:22  Debug    IKE  c8f205c6 bf3b967a 60e50073 59096b0d 6748c4c6 cc3c37f7 587671e5 96ba530e
May 18, 22:50:22  Debug    IKE  325eb7a4 0998f46a 389bf876 0b200b04 0500000c 01000000 0a010202 00000010
May 18, 22:50:22  Debug    IKE  04000000 0a010200 ffffff00
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  HASH computed:
May 18, 22:50:22  Debug    IKE  18738b63 32308174 769b1b3f 0a45bf1e
May 18, 22:50:22  Debug    IKE  add payload of len 16, next type 1
May 18, 22:50:22  Debug    IKE  begin encryption.
May 18, 22:50:22  Debug    IKE  encryption(des)
May 18, 22:50:22  Debug    IKE  pad length = 4
May 18, 22:50:22  Debug    IKE  01000014 18738b63 32308174 769b1b3f 0a45bf1e 0a000034 00000001 00000001
May 18, 22:50:22  Debug    IKE  00000028 01030401 079d6fea 0000001c 01030000 80010001 800201e0 80040001
May 18, 22:50:22  Debug    IKE  80050002 80030001 04000014 f3b8c86f aaf09bcc 4234f534 6dfe42d8 05000064
May 18, 22:50:22  Debug    IKE  b9685992 243f8657 adac1d90 95a25ac5 d8e177b1 99a5e1da 8219cff0 bb34af6c
May 18, 22:50:22  Debug    IKE  255d9c6b f64fb794 652cf3f5 d52b9046 c8f205c6 bf3b967a 60e50073 59096b0d
May 18, 22:50:22  Debug    IKE  6748c4c6 cc3c37f7 587671e5 96ba530e 325eb7a4 0998f46a 389bf876 0b200b04
May 18, 22:50:22  Debug    IKE  0500000c 01000000 0a010202 00000010 04000000 0a010200 ffffff00 00000004
May 18, 22:50:22  Debug    IKE  encryption(des)
May 18, 22:50:22  Debug    IKE  with key:
May 18, 22:50:22  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:22  Debug    IKE  encrypted payload by IV:
May 18, 22:50:22  Debug    IKE  36338123 a4bdf618
May 18, 22:50:22  Debug    IKE  save IV for next:
May 18, 22:50:22  Debug    IKE  34d0e168 6f29d6b8
May 18, 22:50:22  Debug    IKE  encrypted.
May 18, 22:50:22  Debug    IKE  252 bytes from 192.168.215.2[500] to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  1 times of 252 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 08102001 daec08f0 000000fc a3f1472d
May 18, 22:50:22  Debug    IKE  a3f12b43 5a53c013 3c4a27fb b76f03c5 ae3d89f1 963eff3f 845ff010 74aac3ca
May 18, 22:50:22  Debug    IKE  ec65bad0 700e5391 f85612ce 571b5a4e e6ac8058 414b85a6 0b62f0ee b22fd7c3
May 18, 22:50:22  Debug    IKE  8c101651 74c62162 1cf8c632 477edd26 bec318bc d2ae157c 521078e3 72e29666
May 18, 22:50:22  Debug    IKE  20d09245 0491b01a 25f31c2f 20ace6b0 4470ab7b e3491c72 0d527671 38ca7c39
May 18, 22:50:22  Debug    IKE  21087ccf 5e54aaa5 c06e1876 baa7fd5a 5eac97cd e36c1c9f 29d9086a fedc2012
```

```
May 18, 22:50:22  Debug    IKE  13f0dfc1 cba49e4f 90fa45f7 26249093 475637fa b9b05229 cc948c2b dcd0d687
May 18, 22:50:22  Debug    IKE  0be51d1b c65d04e2 287666a0 94d9e74c f6c64d9d 34d0e168 6f29d6b8
May 18, 22:50:22  Debug    IKE  resend phase2 packet 8f1739363f9f3466:113cf0ddd0fd274e:0000daec
May 18, 22:50:22  Debug    IKE  msg 16 not interesting
May 18, 22:50:22  Debug    IKE  msg 16 not interesting
May 18, 22:50:22  Debug    IKE  msg 15 not interesting
May 18, 22:50:22  Debug    IKE  msg 15 not interesting
May 18, 22:50:22  Debug    IKE  msg 15 not interesting
May 18, 22:50:22  Debug    IKE  ===
May 18, 22:50:22  Debug    IKE  260 bytes message received from 192.168.215.225[500] to 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 08102001 daec08f0 00000104 21ad8865
May 18, 22:50:22  Debug    IKE  0c050fa7 2fff08af 93b3ba1c 49cb71bb 4d5a3d56 5e5d2da3 73a97423 12b6e289
May 18, 22:50:22  Debug    IKE  c9689072 f2523e51 16d491cd c7bc35a4 90172041 1df63515 c6aed4a5 0ec42eb5
May 18, 22:50:22  Debug    IKE  924a317b 2c4c9df6 b2d7298e d0e40ead 6a7b18e2 8c4d3b0d 9cecd46c a3be4249
May 18, 22:50:22  Debug    IKE  d531c627 1ad8c084 f6500294 4fcea940 050b7dea 0b5d49b6 b8c88d68 61fe4040
May 18, 22:50:22  Debug    IKE  3e8d2268 49c9c954 f8b7ba8b 6c8d7e79 e2b0859b e342d468 084669e1 31d1f280
May 18, 22:50:22  Debug    IKE  e43ec5ad ab8a9bdf 89d85bcd e3ddb3e6 78439f0c b58e1a84 9ee97128 a8eca85b
May 18, 22:50:22  Debug    IKE  884b58d7 43173e36 262cd791 02413d01 0d60be31 ac8f39d2 0b74abae 055187c6
May 18, 22:50:22  Debug    IKE  24e2b80b
May 18, 22:50:22  Debug    IKE  begin decryption.
May 18, 22:50:22  Debug    IKE  encryption(des)
May 18, 22:50:22  Debug    IKE  IV was saved for next processing:
May 18, 22:50:22  Debug    IKE  055187c6 24e2b80b
May 18, 22:50:22  Debug    IKE  encryption(des)
May 18, 22:50:22  Debug    IKE  with key:
May 18, 22:50:22  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:22  Debug    IKE  decrypted payload by IV:
May 18, 22:50:22  Debug    IKE  34d0e168 6f29d6b8
May 18, 22:50:22  Debug    IKE  decrypted payload, but not trimed.
May 18, 22:50:22  Debug    IKE  01000014 14dcd277 ea3ed36a 0e202f63 5f753b1a 0a000038 00000001 00000001
May 18, 22:50:22  Debug    IKE  0000002c 01030401 5d652259 00000020 01030000 80030001 80010001 00020004
May 18, 22:50:22  Debug    IKE  000001e0 80040001 80050002 04000018 d230023f a99a2a25 6863b762 b6fcf4cc
May 18, 22:50:22  Debug    IKE  56352171 05000064 c9201d70 ede7ae36 18a4e4e1 d537c617 63478798 4bbe2b8f
May 18, 22:50:22  Debug    IKE  ca2b32f6 4b35a378 a244de37 4d7ee1b5 9c8c5078 4aef12ad 05816fff 54a4e322
May 18, 22:50:22  Debug    IKE  53248c41 6e7ea6bb ed010e05 ce9c8471 31bebe61 962ab27b c4b50326 b5426848
May 18, 22:50:22  Debug    IKE  defad7ef 9d9f8ff9 0500000c 01000000 0a010202 00000010 04000000 0a010200
May 18, 22:50:22  Debug    IKE  ffffff00 00000000
May 18, 22:50:22  Debug    IKE  padding len=0
May 18, 22:50:22  Debug    IKE  skip to trim padding.
May 18, 22:50:22  Debug    IKE  decrypted.
May 18, 22:50:22  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 08102001 daec08f0 00000104 01000014
May 18, 22:50:22  Debug    IKE  14dcd277 ea3ed36a 0e202f63 5f753b1a 0a000038 00000001 00000001 0000002c
May 18, 22:50:22  Debug    IKE  01030401 5d652259 00000020 01030000 80030001 80010001 00020004 000001e0
May 18, 22:50:22  Debug    IKE  80040001 80050002 04000018 d230023f a99a2a25 6863b762 b6fcf4cc 56352171
May 18, 22:50:22  Debug    IKE  05000064 c9201d70 ede7ae36 18a4e4e1 d537c617 63478798 4bbe2b8f ca2b32f6
May 18, 22:50:22  Debug    IKE  4b35a378 a244de37 4d7ee1b5 9c8c5078 4aef12ad 05816fff 54a4e322 53248c41
May 18, 22:50:22  Debug    IKE  6e7ea6bb ed010e05 ce9c8471 31bebe61 962ab27b c4b50326 b5426848 defad7ef
May 18, 22:50:22  Debug    IKE  9d9f8ff9 0500000c 01000000 0a010202 00000010 04000000 0a010200 ffffff00
May 18, 22:50:22  Debug    IKE  00000000
May 18, 22:50:22  Debug    IKE  begin.
May 18, 22:50:22  Debug    IKE  seen nptype=8(hash)
May 18, 22:50:22  Debug    IKE  seen nptype=1(sa)
May 18, 22:50:22  Debug    IKE  seen nptype=10(nonce)
May 18, 22:50:22  Debug    IKE  seen nptype=4(ke)
May 18, 22:50:22  Debug    IKE  seen nptype=5(id)
May 18, 22:50:22  Debug    IKE  seen nptype=5(id)
May 18, 22:50:22  Debug    IKE  succeed.
May 18, 22:50:22  Debug    IKE  HASH allocated:hbuf->l=248 actual:tlen=224
May 18, 22:50:22  Debug    IKE  HASH(2) received:2007-05-18 22:50:22: DEBUG:
May 18, 22:50:22  Debug    IKE  14dcd277 ea3ed36a 0e202f63 5f753b1a
May 18, 22:50:22  Debug    IKE  HASH with:
May 18, 22:50:22  Debug    IKE  daec08f0 f3b8c86f aaf09bcc 4234f534 6dfe42d8 0a000038 00000001 00000001
May 18, 22:50:22  Debug    IKE  0000002c 01030401 5d652259 00000020 01030000 80030001 80010001 00020004
May 18, 22:50:22  Debug    IKE  000001e0 80040001 80050002 04000018 d230023f a99a2a25 6863b762 b6fcf4cc
May 18, 22:50:22  Debug    IKE  56352171 05000064 c9201d70 ede7ae36 18a4e4e1 d537c617 63478798 4bbe2b8f
May 18, 22:50:22  Debug    IKE  ca2b32f6 4b35a378 a244de37 4d7ee1b5 9c8c5078 4aef12ad 05816fff 54a4e322
May 18, 22:50:22  Debug    IKE  53248c41 6e7ea6bb ed010e05 ce9c8471 31bebe61 962ab27b c4b50326 b5426848
May 18, 22:50:22  Debug    IKE  defad7ef 9d9f8ff9 0500000c 01000000 0a010202 00000010 04000000 0a010200
May 18, 22:50:22  Debug    IKE  ffffff00
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  HASH computed:
May 18, 22:50:22  Debug    IKE  14dcd277 ea3ed36a 0e202f63 5f753b1a
May 18, 22:50:22  Debug    IKE  total SA len=48
May 18, 22:50:22  Debug    IKE  00000001 00000001 00000028 01030401 079d6fea 0000001c 01030000 80010001
```

```
May 18, 22:50:22  Debug    IKE  800201e0 80040001 80050002 80030001
May 18, 22:50:22  Debug    IKE  begin.
May 18, 22:50:22  Debug    IKE  seen nptype=2(prop)
May 18, 22:50:22  Debug    IKE  succeed.
May 18, 22:50:22  Debug    IKE  proposal #1 len=40
May 18, 22:50:22  Debug    IKE  begin.
May 18, 22:50:22  Debug    IKE  seen nptype=3(trns)
May 18, 22:50:22  Debug    IKE  succeed.
May 18, 22:50:22  Debug    IKE  transform #1 len=28
May 18, 22:50:22  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:22  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=480
May 18, 22:50:22  Debug    IKE  life duration was in TLV.
May 18, 22:50:22  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:50:22  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 18, 22:50:22  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
May 18, 22:50:22  Debug    IKE  hmac(modp768)
May 18, 22:50:22  Debug    IKE  pair 1:
May 18, 22:50:22  Debug    IKE  0x30a5c0: next=0x0 tnext=0x0
May 18, 22:50:22  Debug    IKE  proposal #1: 1 transform
May 18, 22:50:22  Debug    IKE  total SA len=52
May 18, 22:50:22  Debug    IKE  00000001 00000001 0000002c 01030401 5d652259 00000020 01030000 80030001
May 18, 22:50:22  Debug    IKE  80010001 00020004 000001e0 80040001 80050002
May 18, 22:50:22  Debug    IKE  begin.
May 18, 22:50:22  Debug    IKE  seen nptype=2(prop)
May 18, 22:50:22  Debug    IKE  succeed.
May 18, 22:50:22  Debug    IKE  proposal #1 len=44
May 18, 22:50:22  Debug    IKE  begin.
May 18, 22:50:22  Debug    IKE  seen nptype=3(trns)
May 18, 22:50:22  Debug    IKE  succeed.
May 18, 22:50:22  Debug    IKE  transform #1 len=32
May 18, 22:50:22  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
May 18, 22:50:22  Debug    IKE  hmac(modp768)
May 18, 22:50:22  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:22  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
May 18, 22:50:22  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:50:22  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 18, 22:50:22  Debug    IKE  pair 1:
May 18, 22:50:22  Debug    IKE  0x30a590: next=0x0 tnext=0x0
May 18, 22:50:22  Debug    IKE  proposal #1: 1 transform
May 18, 22:50:22  Warning  IKE  attribute has been modified.
May 18, 22:50:22  Debug    IKE  begin compare proposals.
May 18, 22:50:22  Debug    IKE  pair[1]: 0x30a590
May 18, 22:50:22  Debug    IKE  0x30a590: next=0x0 tnext=0x0
May 18, 22:50:22  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
May 18, 22:50:22  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
May 18, 22:50:22  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:22  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
May 18, 22:50:22  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:50:22  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 18, 22:50:22  Debug    IKE  peer's single bundle:
May 18, 22:50:22  Debug    IKE  (proto_id=ESP spisize=4 spi=5d652259 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:50:22  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:50:22  Debug    IKE  my single bundle:
May 18, 22:50:22  Debug    IKE  (proto_id=ESP spisize=4 spi=079d6fea spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:50:22  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:50:22  Debug    IKE  matched
May 18, 22:50:22  Debug    IKE  ===
May 18, 22:50:22  Debug    IKE  HASH(3) generate
May 18, 22:50:22  Debug    IKE  HASH with:
May 18, 22:50:22  Debug    IKE  00daec08 f0f3b8c8 6faaf09b cc4234f5 346dfe42 d8d23002 3fa99a2a 256863b7
May 18, 22:50:22  Debug    IKE  62b6fcf4 cc563521 71
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  HASH computed:
May 18, 22:50:22  Debug    IKE  90ab69fa 7faf489a 63290568 9e0194b4
May 18, 22:50:22  Debug    IKE  add payload of len 16, next type 0
May 18, 22:50:22  Debug    IKE  begin encryption.
May 18, 22:50:22  Debug    IKE  encryption(des)
May 18, 22:50:22  Debug    IKE  pad length = 4
May 18, 22:50:22  Debug    IKE  00000014 90ab69fa 7faf489a 63290568 9e0194b4 00000004
May 18, 22:50:22  Debug    IKE  encryption(des)
May 18, 22:50:22  Debug    IKE  with key:
May 18, 22:50:22  Debug    IKE  a6b9d6c5 6ccc0fc9
May 18, 22:50:22  Debug    IKE  encrypted payload by IV:
May 18, 22:50:22  Debug    IKE  055187c6 24e2b80b
```

```
May 18, 22:50:22  Debug    IKE  save IV for next:
May 18, 22:50:22  Debug    IKE  c1020bd8 2dae21dd
May 18, 22:50:22  Debug    IKE  encrypted.
May 18, 22:50:22  Debug    IKE  52 bytes from 192.168.215.2[500] to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  1 times of 52 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  8f173936 3f9f3466 113cf0dd d0fd274e 08102001 daec08f0 00000034 98c48fbf
May 18, 22:50:22  Debug    IKE  92ac07c0 7672d388 039d1e8d c1020bd8 2dae21dd
May 18, 22:50:22  Debug    IKE  compute DH's shared.
May 18, 22:50:22  Debug    IKE  18017732 d4093f47 866dac68 c58ac9f2 6bb9dfa2 fd47dd57 19c652f9 b8b21b26
May 18, 22:50:22  Debug    IKE  c219c775 ac2079f3 d0e8eb10 45814171 418e9e03 de05f6d1 6cf859bd 5ca88702
May 18, 22:50:22  Debug    IKE  89c212ed 0e267f4a 34b5435a 9ba3d3fa 2ac6370e a3e981ff 4a2cd314 9381c592
May 18, 22:50:22  Debug    IKE  KEYMAT compute with
May 18, 22:50:22  Debug    IKE  18017732 d4093f47 866dac68 c58ac9f2 6bb9dfa2 fd47dd57 19c652f9 b8b21b26
May 18, 22:50:22  Debug    IKE  c219c775 ac2079f3 d0e8eb10 45814171 418e9e03 de05f6d1 6cf859bd 5ca88702
May 18, 22:50:22  Debug    IKE  89c212ed 0e267f4a 34b5435a 9ba3d3fa 2ac6370e a3e981ff 4a2cd314 9381c592
May 18, 22:50:22  Debug    IKE  03079d6f eaf3b8c8 6faaf09b cc4234f5 346dfe42 d8d23002 3fa99a2a 256863b7
May 18, 22:50:22  Debug    IKE  62b6fcf4 cc563521 71
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  encryption(3des)
May 18, 22:50:22  Debug    IKE  hmac(hmac_sha1)
May 18, 22:50:22  Debug    IKE  encklen=192 authklen=160
May 18, 22:50:22  Debug    IKE  generating 512 bits of key (dupkeymat=4)
May 18, 22:50:22  Debug    IKE  generating K1...K4 for KEYMAT.
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  6636e434 ea23d162 ccdeb8ea deacd347 48f17954 28203a54 03fa7dd2 20e5bc84
May 18, 22:50:22  Debug    IKE  7687338a b377dfc1 142860ee 708f8576 11467e66 610c4dd6 57721630 4cb939b8
May 18, 22:50:22  Debug    IKE  KEYMAT compute with
May 18, 22:50:22  Debug    IKE  18017732 d4093f47 866dac68 c58ac9f2 6bb9dfa2 fd47dd57 19c652f9 b8b21b26
May 18, 22:50:22  Debug    IKE  c219c775 ac2079f3 d0e8eb10 45814171 418e9e03 de05f6d1 6cf859bd 5ca88702
May 18, 22:50:22  Debug    IKE  89c212ed 0e267f4a 34b5435a 9ba3d3fa 2ac6370e a3e981ff 4a2cd314 9381c592
May 18, 22:50:22  Debug    IKE  035d6522 59f3b8c8 6faaf09b cc4234f5 346dfe42 d8d23002 3fa99a2a 256863b7
May 18, 22:50:22  Debug    IKE  62b6fcf4 cc563521 71
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  encryption(3des)
May 18, 22:50:22  Debug    IKE  hmac(hmac_sha1)
May 18, 22:50:22  Debug    IKE  encklen=192 authklen=160
May 18, 22:50:22  Debug    IKE  generating 512 bits of key (dupkeymat=4)
May 18, 22:50:22  Debug    IKE  generating K1...K4 for KEYMAT.
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:22  Debug    IKE  6a723ebd 86ba4878 df7bf22d 8680e991 4a945337 7dafe7be 15cc66f0 0903f36b
May 18, 22:50:22  Debug    IKE  60f97cbd a20e7978 4ff3b5d5 052c2ec1 139c9028 904aaa37 d4a00da0 dd69d8e9
May 18, 22:50:22  Debug    IKE  KEYMAT computed.
May 18, 22:50:22  Debug    IKE  call pk_sendupdate
May 18, 22:50:22  Debug    IKE  encryption(3des)
May 18, 22:50:22  Debug    IKE  hmac(hmac_sha1)
May 18, 22:50:22  Debug    IKE  call pfkey_send_update_nat
May 18, 22:50:22  Debug    APP  Received SADB message type UPDATE, 192.168.215.225 [0] -> 192.168.215.2 [0]
May 18, 22:50:22  Debug    APP  SA change detected
May 18, 22:50:22  Debug    IKE  pfkey update sent.
May 18, 22:50:22  Debug    IKE  encryption(3des)
May 18, 22:50:22  Debug    IKE  hmac(hmac_sha1)
May 18, 22:50:22  Debug    IKE  call pfkey_send_add_nat
May 18, 22:50:22  Debug    APP  Received SADB message type ADD, 192.168.215.2 [0] -> 192.168.215.225 [0]
May 18, 22:50:22  Debug    APP  SA change detected
May 18, 22:50:22  Debug    APP  Connection Zyxel P1 is up
May 18, 22:50:22  Debug    IKE  pfkey add sent.
May 18, 22:50:22  Debug    IKE  get pfkey UPDATE message
May 18, 22:50:22  Debug    IKE  02020003 14000000 d5010000 ee180000 02000100 079d6fea 04000202 00000000
May 18, 22:50:22  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d7e1
May 18, 22:50:22  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d702 00000000 00000000
May 18, 22:50:22  Debug    IKE  04000300 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
May 18, 22:50:22  Debug    IKE  04000400 00000000 00000000 00000000 80010000 00000000 00000000 00000000
May 18, 22:50:22  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.225[0]->192.168.215.2[0]
spi=127758314(0x79d6fea)
May 18, 22:50:22  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.225[0]->192.168.215.2[0]
spi=127758314(0x79d6fea)
May 18, 22:50:22  Debug    IKE  ===
```

```
May 18, 22:50:22  Debug    IKE  get pfkey ADD message
May 18, 22:50:22  Debug    IKE  02030003 14000000 d5010000 ee180000 02000100 5d652259 04000202 00000000
May 18, 22:50:22  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d702
May 18, 22:50:22  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e1 00000000 00000000
May 18, 22:50:22  Debug    IKE  04000300 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
May 18, 22:50:22  Debug    IKE  04000400 00000000 00000000 00000000 80010000 00000000 00000000 00000000
May 18, 22:50:22  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.2[0]->192.168.215.225[0]
spi=1566909017(0x5d652259)
May 18, 22:50:22  Debug    IKE  ===
```