IPSecuritas 3.x

Configuration Instructions

for

m0n0wall

© Lobotomo Software
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.

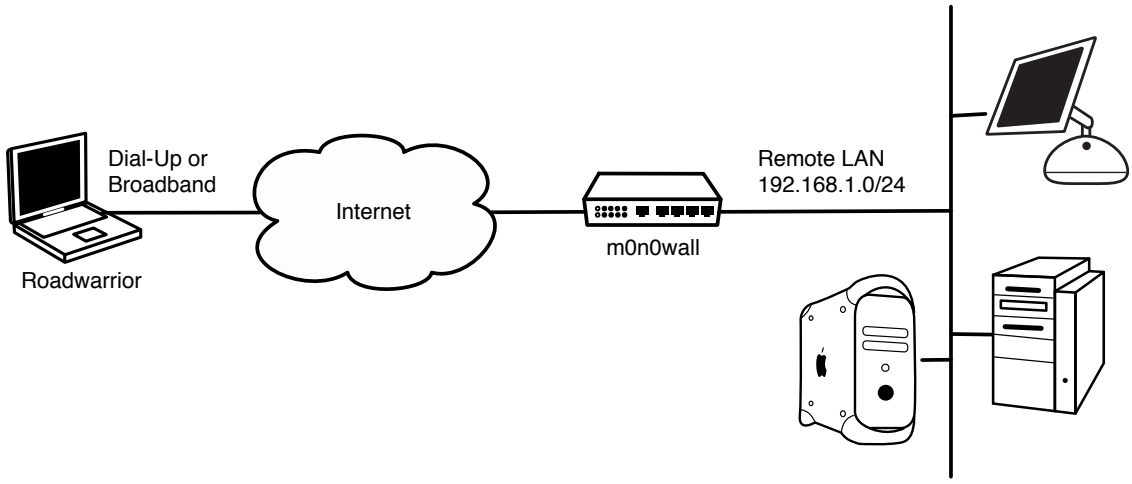
Acknowledgments

Many thanks to Stephen B (www.suchaproduction.com) and Jason Sjobeck (www.sjobeck.com) for providing setup information, screenshots and support for writing this document.

Table of contents

Introduction

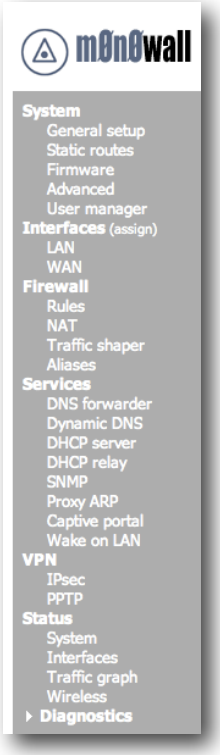
This document describes the steps necessary to establish a protected VPN connection between a Mac client and a monowall router/firewall. All information in this document is based on the following assumed network.



m0n0wall VPN Setup

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

Login to m0n0wall

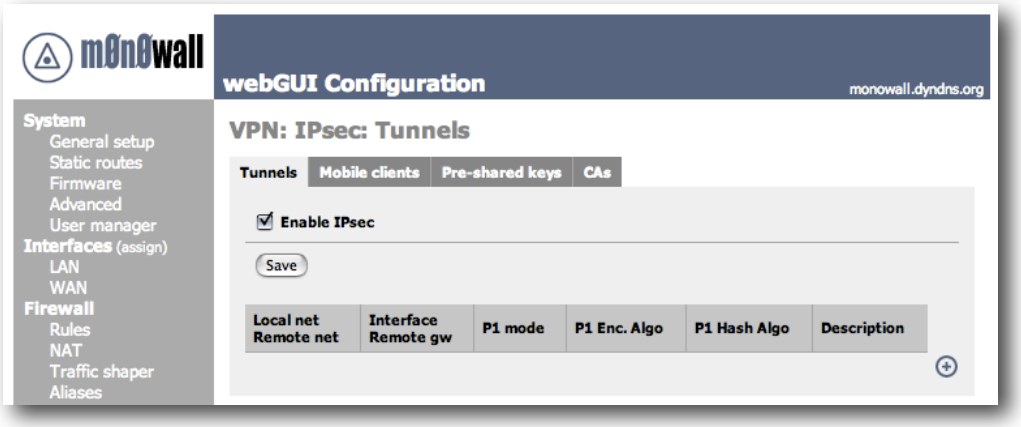


First, connect to your monowall in a web browser and enter the administrator password.

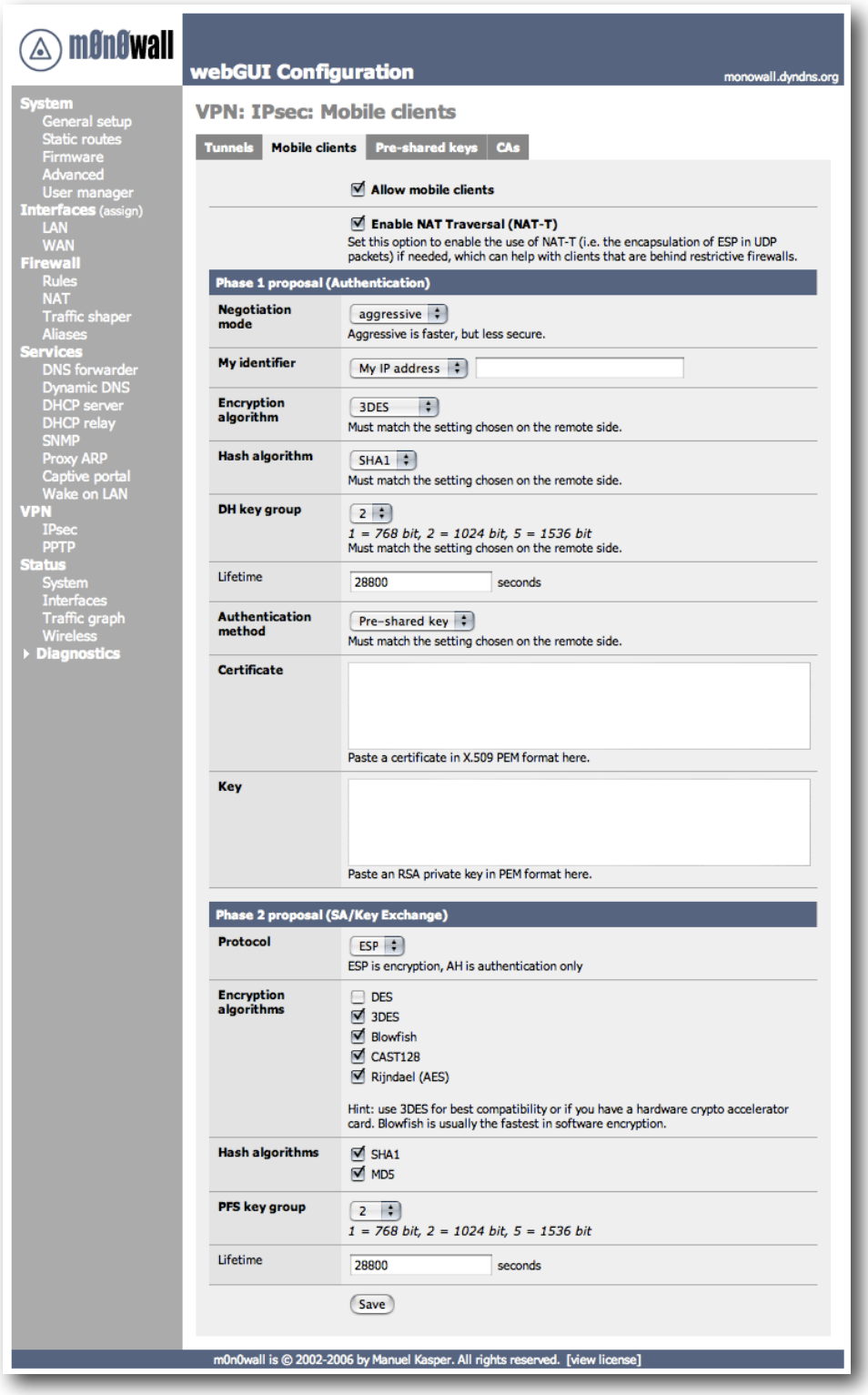
Once logged in, click on **IPSec** in the menu **VPN** on the left side of the displayed monowall main page.

Enable IPSec

In the now appearing panel (make sure **Tunnels** is selected in the tab chooser at the top), switch on the option **Enable IPSec** and press **Save** to commit your changes.



Configure Mobile Client



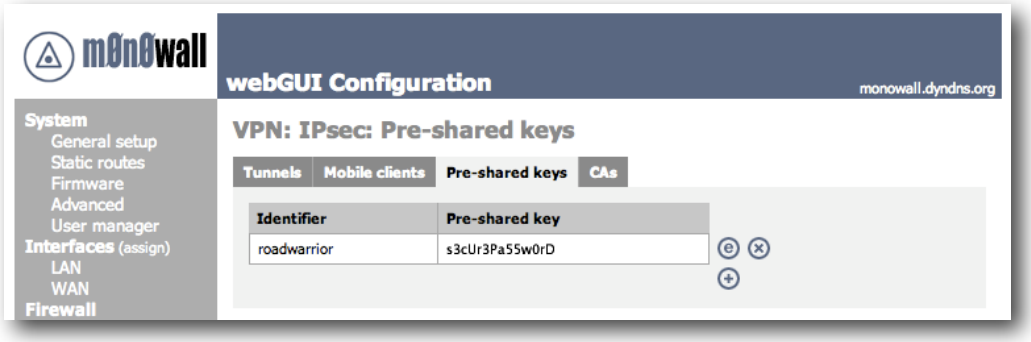
Next, please press on **Mobile clients** in the tab chooser at the top.

Set all properties as shown in the screenshot to the left.

Press **Save** to commit your changes.

Add Users

Now, press on **Pre-shared keys** in the tab chooser at the top. You will be presented with a list of names and accompanying preshared key (which is a secure password string). Press the add icon next to the list ⊕ to add a new user. Please remember the user name and the pre-shared key you choose, since



you need them again when setting up IPSecuritas.
You may use the same name and key for all users or you may create individual name key pairs for each user (recommended).

The setup of monowall is now complete and it will accept incoming IPSec connection requests. You may now proceed with the setup of IPSecuritas, described in the next chapter.

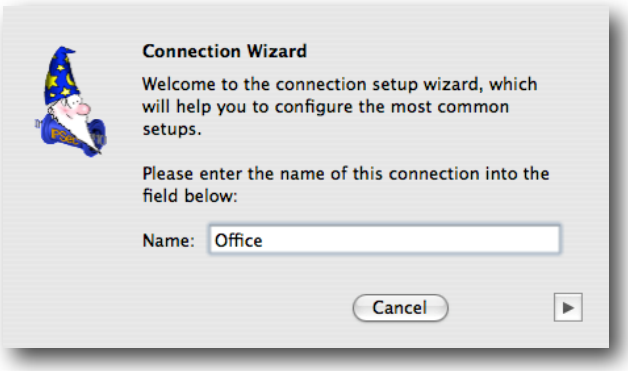
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the monowall 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:

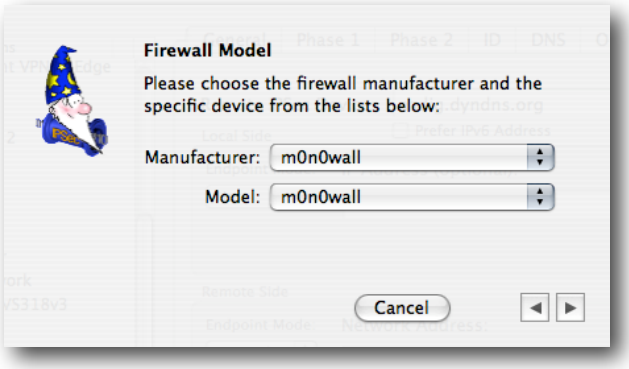
Enter Name of New Connection



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

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

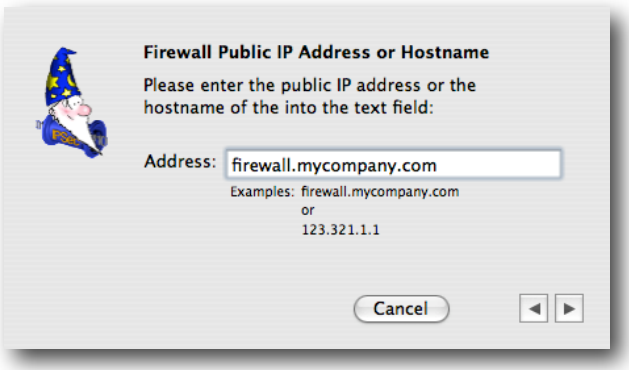
Select Router Model



Select **monowall** from the manufacturer list and **monowall** from the model list.

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

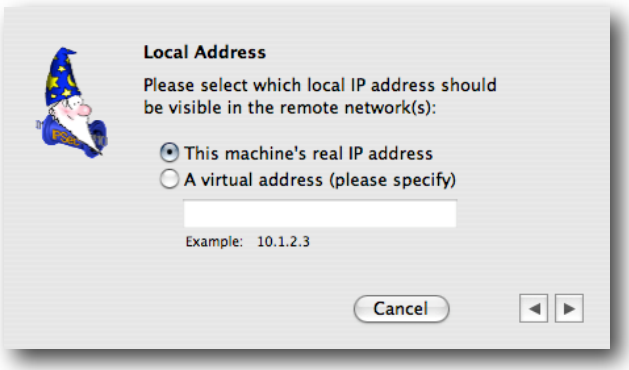
Enter Router's Public IP Address



Enter the public IP address or hostname of your monowall 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).

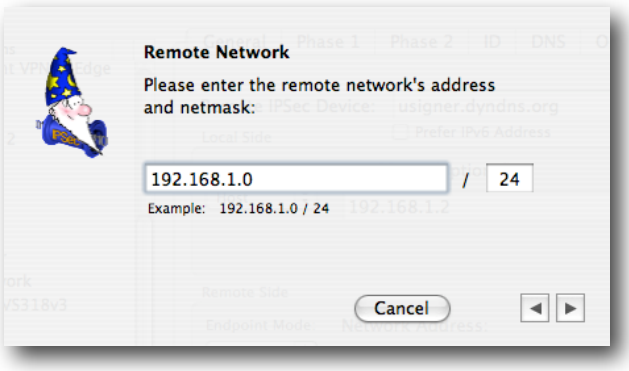
Click on the right arrow to continue with the next step.

Enter a Virtual IP Address



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.

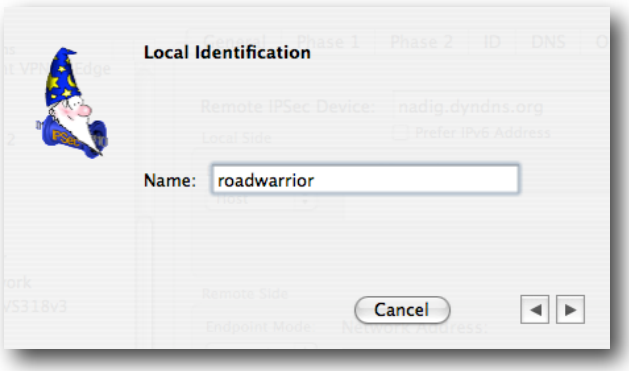
Enter Remote Network



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 monowall.

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

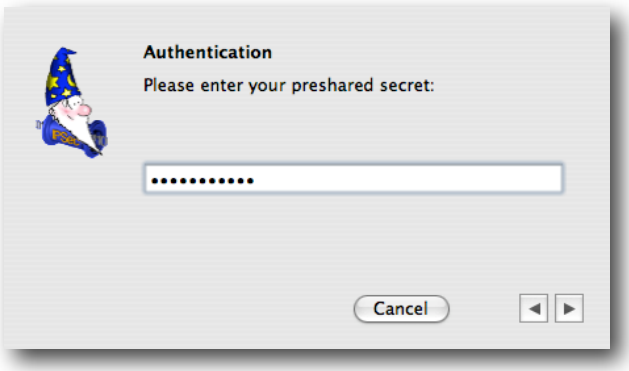
Enter Local Identification



Enter the local identification (which is the identifier you choose when setting up the the pre-shared keys on the monowall).

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

Enter Preshared Key



Enter the same **Preshared Key** that you set for the identification you entered in the last step.

Click on the right arrow to finish the connection setup.

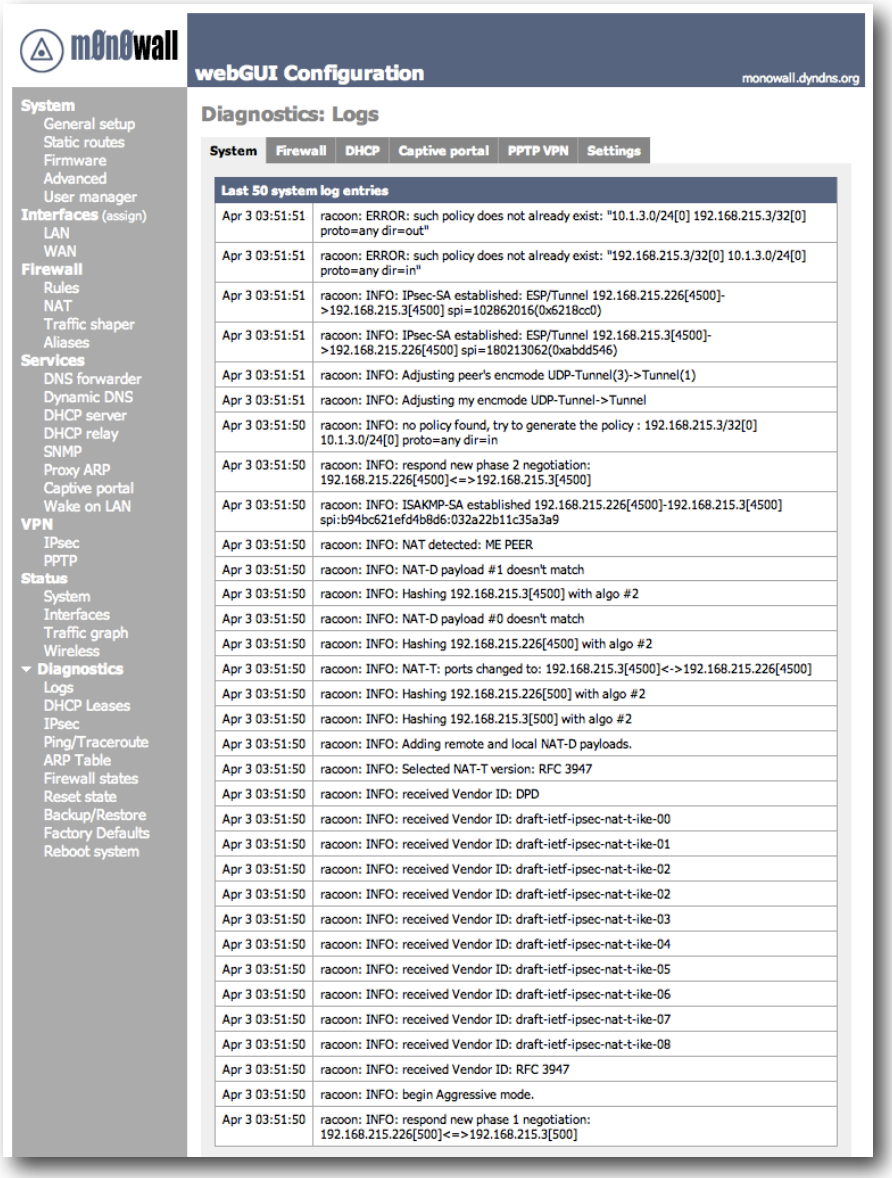
Diagnosis

Reachability Test

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

```
[MacBook:~] root# ping 192.168.1.1
PING 192.168.215.1 (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
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=12.823 ms
```

Sample m0n0wall Log Output



While still logged into the monowall web interface, click onto **Diagnostics** on the left side to unveil its submenu.
Click on **Logs** to display the monowall log entries.

If the connection attempt was successful, you should see a similar log as shown to the left.

Sample IPSecuritas Log Output

The following is a sample log file 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 20, 12:15:41  Debug    APP  State change from IDLE to AUTHENTICATING after event START
May 20, 12:15:41  Info     APP  IKE daemon started
May 20, 12:15:41  Info     APP  IPSec started
May 20, 12:15:41  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
May 20, 12:15:41  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 20, 12:15:41  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 20, 12:15:41  Info     IKE  Foreground mode.
May 20, 12:15:41  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
May 20, 12:15:41  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
May 20, 12:15:41  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
May 20, 12:15:41  Info     IKE  Resize address pool from 0 to 255
May 20, 12:15:41  Debug    IKE  lifetime = 28800
May 20, 12:15:41  Debug    IKE  lifebyte = 0
May 20, 12:15:41  Debug    IKE  encklen=0
May 20, 12:15:41  Debug    IKE  p:1 t:1
May 20, 12:15:41  Debug    IKE  3DES-CBC(5)
May 20, 12:15:41  Debug    IKE  SHA(2)
May 20, 12:15:41  Debug    IKE  1024-bit MODP group(2)
May 20, 12:15:41  Debug    IKE  pre-shared key(1)
May 20, 12:15:41  Debug    IKE  hmac(modp1024)
May 20, 12:15:41  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
May 20, 12:15:41  Debug    IKE  parse successed.
May 20, 12:15:41  Debug    IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
May 20, 12:15:41  Info     IKE  192.168.215.2[4500] used as isakmp port (fd=7)
May 20, 12:15:41  Info     IKE  192.168.215.2[500] used as isakmp port (fd=8)
May 20, 12:15:41  Debug    IKE  get pfkey X_SPDDUMP message
May 20, 12:15:41  Debug    IKE  02120000 0f000100 01000000 88250000 03000500 ff180000 10020000 0a010300
May 20, 12:15:41  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d702 00000000 00000000
May 20, 12:15:41  Debug    IKE  07001200 02000100 96a70900 00000000 28003200 02020000 10020000 c0a8d7e2
May 20, 12:15:41  Debug    IKE  00000000 00000000 10020000 c0a8d702 00000000 00000000
May 20, 12:15:41  Debug    IKE  get pfkey X_SPDDUMP message
May 20, 12:15:41  Debug    IKE  02120000 0f000100 00000000 88250000 03000500 ff200000 10020000 c0a8d702
May 20, 12:15:41  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 0a010300 00000000 00000000
May 20, 12:15:41  Debug    IKE  07001200 02000200 95a70900 00000000 28003200 02020000 10020000 c0a8d702
May 20, 12:15:41  Debug    IKE  00000000 00000000 10020000 c0a8d7e2 00000000 00000000
May 20, 12:15:41  Debug    IKE  sub:0xbffff340: 192.168.215.2/32[0] 10.1.3.0/24[0] proto=any dir=out
May 20, 12:15:41  Debug    IKE  db :0x308c68: 10.1.3.0/24[0] 192.168.215.2/32[0] proto=any dir=in
May 20, 12:15:42  Info     APP  Initiated connection m0n0Wall
May 20, 12:15:42  Debug    IKE  get pfkey ACQUIRE message
May 20, 12:15:42  Debug    IKE  02060003 24000000 48040000 00000000 03000500 ff200000 10020000 c0a8d702
May 20, 12:15:42  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e2 00000000 00000000
May 20, 12:15:42  Debug    IKE  1c000d00 20000000 00030000 00000000 00010008 00000000 01000000 01000000
May 20, 12:15:42  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
May 20, 12:15:42  Debug    IKE  80700000 00000000 00000000 00000000 00040000 00000000 0001c001 00000000
May 20, 12:15:42  Debug    IKE  01000000 01000000 00000000 00000000 00000000 00000000 00000000 00000000
May 20, 12:15:42  Debug    IKE  80510100 00000000 80700000 00000000 00000000 00000000 000c0000 00000000
May 20, 12:15:42  Debug    IKE  00010001 00000000 01000000 01000000 00000000 00000000 00000000 00000000
May 20, 12:15:42  Debug    IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
May 20, 12:15:42  Error    IKE  inappropriate sadb acquire message passed.
May 20, 12:15:42  Debug    IKE  get pfkey ACQUIRE message
May 20, 12:15:42  Debug    IKE  02060003 14000000 06020000 b90b0000 03000500 ff200000 10020000 c0a8d702
May 20, 12:15:42  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e2 00000000 00000000
May 20, 12:15:42  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
May 20, 12:15:42  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
May 20, 12:15:42  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 95a70900 00000000
May 20, 12:15:42  Debug    IKE  suitable outbound SP found: 192.168.215.2/32[0] 10.1.3.0/24[0] proto=any dir=out.
May 20, 12:15:42  Debug    IKE  sub:0xbffff31c: 10.1.3.0/24[0] 192.168.215.2/32[0] proto=any dir=in
May 20, 12:15:42  Debug    IKE  db :0x308c68: 10.1.3.0/24[0] 192.168.215.2/32[0] proto=any dir=in
May 20, 12:15:42  Debug    IKE  suitable inbound SP found: 10.1.3.0/24[0] 192.168.215.2/32[0] proto=any dir=in.
May 20, 12:15:42  Debug    IKE  new acquire 192.168.215.2/32[0] 10.1.3.0/24[0] proto=any dir=out
May 20, 12:15:42  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 20, 12:15:42  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 12:15:42  Debug    IKE  in post_acquire
```

```
May 20, 12:15:42  Debug    IKE  configuration found for 192.168.215.226.
May 20, 12:15:42  Info     IKE  IPsec-SA request for 192.168.215.226 queued due to no phase1 found.
May 20, 12:15:42  Debug    IKE  ===
May 20, 12:15:42  Info     IKE  initiate new phase 1 negotiation: 192.168.215.2[500]<=>192.168.215.226[500]
May 20, 12:15:42  Info     IKE  begin Aggressive mode.
May 20, 12:15:42  Debug    IKE  new cookie:
May 20, 12:15:42  Debug    IKE  489fab77ca78ff22
May 20, 12:15:42  Debug    IKE  use ID type of FQDN
May 20, 12:15:42  Debug    IKE  compute DH's private.
May 20, 12:15:42  Debug    IKE  6905f53a 6861b6b3 f681dce4 ccc2dcc1 3969c4f5 32058a69 e53d3625 de9e1ac7
May 20, 12:15:42  Debug    IKE  3d68bfbd b618a08b b640e76a dc06de4c b0a53009 12ba21bf 2ea1e475 ecdbade4
May 20, 12:15:42  Debug    IKE  a3055013 13072673 f3e45c62 c4f9176a 52cf8050 4bd9be17 cd2a118f c74576bb
May 20, 12:15:42  Debug    IKE  2b8d170a 51508d4b 8d825a0c ec1f0cd7 3820ab60 576f7954 3df8c8f4 727a0f41
May 20, 12:15:42  Debug    IKE  compute DH's public.
May 20, 12:15:42  Debug    IKE  3658591a 2da7b45a ab105969 dbca0dce 786771b1 d88a9e29 19ffc8f5 3cdd567a
May 20, 12:15:42  Debug    IKE  45561cb4 f2a94dba bbe63d49 6884e905 0ad1fa73 16a4199f 9609a1ad e54907d9
May 20, 12:15:42  Debug    IKE  c7c7b2ec 79bcb3ce eba3dda0 c4960837 208b3a9f 6de92e44 e92d8a69 e56a068d
May 20, 12:15:42  Debug    IKE  c18ae7fc bc223f08 144436d6 213e3505 b66e275e 242ace4a 4a261d4d 85b8e750
May 20, 12:15:42  Debug    IKE  authmethod is pre-shared key
May 20, 12:15:42  Debug    IKE  add payload of len 48, next type 4
May 20, 12:15:42  Debug    IKE  add payload of len 128, next type 10
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 5
May 20, 12:15:42  Debug    IKE  add payload of len 15, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 13
May 20, 12:15:42  Debug    IKE  add payload of len 16, next type 0
May 20, 12:15:42  Debug    IKE  491 bytes from 192.168.215.2[500] to 192.168.215.226[500]
May 20, 12:15:42  Debug    IKE  sockname 192.168.215.2[500]
May 20, 12:15:42  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 12:15:42  Debug    IKE  send packet to 192.168.215.226[500]
May 20, 12:15:42  Debug    IKE  1 times of 491 bytes message will be sent to 192.168.215.226[500]
May 20, 12:15:42  Debug    IKE  489fab77 ca78ff22 00000000 00000000 01100400 00000000 000001eb 04000034
May 20, 12:15:42  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c7080
May 20, 12:15:42  Debug    IKE  80010005 80030001 80020002 80040002 0a000084 3658591a 2da7b45a ab105969
May 20, 12:15:42  Debug    IKE  dbca0dce 786771b1 d88a9e29 19ffc8f5 3cdd567a 45561cb4 f2a94dba bbe63d49
May 20, 12:15:42  Debug    IKE  6884e905 0ad1fa73 16a4199f 9609a1ad e54907d9 c7c7b2ec 79bcb3ce eba3dda0
May 20, 12:15:42  Debug    IKE  c4960837 208b3a9f 6de92e44 e92d8a69 e56a068d c18ae7fc bc223f08 144436d6
May 20, 12:15:42  Debug    IKE  213e3505 b66e275e 242ace4a 4a261d4d 85b8e750 05000014 acb79f3a 1166a626
May 20, 12:15:42  Debug    IKE  4f6d1fd9 36035f57 0d000013 02000000 726f6164 77617272 696f720d 0000144a
May 20, 12:15:42  Debug    IKE  131c8107 0358455c 5728f20e 95452f0d 0000148f 8d83826d 246b6fc7 a8a6a428
May 20, 12:15:42  Debug    IKE  c11de80d 00001443 9b59f8ba 676c4c77 37ae22ea b8f5820d 0000144d 1e0e136d
May 20, 12:15:42  Debug    IKE  eafa34c4 f3ea9f02 ec72850d 00001480 d0bb3def 54565ee8 4645d4c8 5ce3ee0d
May 20, 12:15:42  Debug    IKE  00001499 09b64eed 937c6573 de52ace9 52fa6b0d 0000147d 9419a653 10ca6f2c
May 20, 12:15:42  Debug    IKE  179d9215 529d560d 000014cd 60464335 df21f87c fdb2fc68 b6a4480d 00001490
May 20, 12:15:42  Debug    IKE  cb80913e bb696e08 6381b5ec 427b1f0d 00001416 f6ca16e4 a4066d83 821a0f0a
May 20, 12:15:42  Debug    IKE  eaa8620d 00001444 85152d18 b6bbcd0b e8a84695 79ddcc00 000014af cad71368
May 20, 12:15:42  Debug    IKE  a1f1c96b 8696fc77 570100
May 20, 12:15:42  Debug    IKE  resend phase1 packet 489fab77ca78ff22:0000000000000000
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  356 bytes message received from 192.168.215.226[500] to 192.168.215.2[500]
May 20, 12:15:43  Debug    IKE  489fab77 ca78ff22 0eec5bb9 5976e03b 01100400 00000000 00000164 04000034
May 20, 12:15:43  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c7080
May 20, 12:15:43  Debug    IKE  80010005 80030001 80020002 80040002 0a000084 6abcdfca fd6edf9d f1c73b33
May 20, 12:15:43  Debug    IKE  12877671 87224c29 f2a07e4a d6d4f6ab f457531a 14c9dfd7 557ace32 664823d7
May 20, 12:15:43  Debug    IKE  7071a0a8 9b192ba9 af8ae0a4 9dca146e ecf0787c c776e444 fe5549fc 19462523
May 20, 12:15:43  Debug    IKE  c55e5428 3b5430d4 1e22299f 1159037b bfc1e01c 5bd21912 2d7d2062 d6cc9885
May 20, 12:15:43  Debug    IKE  a2d238ee 5151e47d 63c3feb3 490df121 1999bbeb 05000014 df2b3d6d b81b625d
May 20, 12:15:43  Debug    IKE  53233f41 fdf8058e 0800000c 011101f4 c0a8d7e2 0d000018 6ecb0022 9d00b8d5
May 20, 12:15:43  Debug    IKE  1d8a2657 f9835f90 3989a857 14000014 4a131c81 07035845 5c5728f2 0e95452f
May 20, 12:15:43  Debug    IKE  14000018 cebd5d96 5ab8ef5b fc8d317b d296d5fd 0fdd84f8 0d000018 54984c17
May 20, 12:15:43  Debug    IKE  3086c59d 60e09cb4 22ff2de8 9e6fe7d1 00000014 afcad713 68a1f1c9 6b8696fc
May 20, 12:15:43  Debug    IKE  77570100
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=1(sa)
May 20, 12:15:43  Debug    IKE  seen nptype=4(ke)
```

```
May 20, 12:15:43  Debug    IKE  seen nptype=10(nonce)
May 20, 12:15:43  Debug    IKE  seen nptype=5(id)
May 20, 12:15:43  Debug    IKE  seen nptype=8(hash)
May 20, 12:15:43  Debug    IKE  seen nptype=13(vid)
May 20, 12:15:43  Debug    IKE  seen nptype=20(nat-d)
May 20, 12:15:43  Debug    IKE  seen nptype=20(nat-d)
May 20, 12:15:43  Debug    IKE  seen nptype=13(vid)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Info     IKE  received Vendor ID: RFC 3947
May 20, 12:15:43  Info     IKE  received Vendor ID: DPD
May 20, 12:15:43  Debug    IKE  remote supports DPD
May 20, 12:15:43  Debug    IKE  total SA len=48
May 20, 12:15:43  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c7080
May 20, 12:15:43  Debug    IKE  80010005 80030001 80020002 80040002
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=2(prop)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  proposal #1 len=40
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=3(trns)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  transform #1 len=32
May 20, 12:15:43  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug    IKE  type=Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 20, 12:15:43  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  pair 1:
May 20, 12:15:43  Debug    IKE  0x3095e0: next=0x0 tnext=0x0
May 20, 12:15:43  Debug    IKE  proposal #1: 1 transform
May 20, 12:15:43  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
May 20, 12:15:43  Debug    IKE  trns#=1, trns-id=IKE
May 20, 12:15:43  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug    IKE  type=Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 20, 12:15:43  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 20, 12:15:43  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 20, 12:15:43  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
May 20, 12:15:43  Debug    IKE  Compared: DB:Peer
May 20, 12:15:43  Debug    IKE  (lifetime = 28800:28800)
May 20, 12:15:43  Debug    IKE  (lifebyte = 0:0)
May 20, 12:15:43  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
May 20, 12:15:43  Debug    IKE  (encklen = 0:0)
May 20, 12:15:43  Debug    IKE  hashtype = SHA:SHA
May 20, 12:15:43  Debug    IKE  authmethod = pre-shared key:pre-shared key
May 20, 12:15:43  Debug    IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
May 20, 12:15:43  Debug    IKE  an acceptable proposal found.
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  agreed on pre-shared key auth.
May 20, 12:15:43  Info     IKE  Selected NAT-T version: RFC 3947
May 20, 12:15:43  Info     IKE  NAT-D payload #-1 doesn't match
May 20, 12:15:43  Info     IKE  NAT-D payload #0 doesn't match
May 20, 12:15:43  Info     IKE  NAT detected: ME PEER
May 20, 12:15:43  Info     IKE  KA list add: 192.168.215.2[4500]->192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  compute DH's shared.
May 20, 12:15:43  Debug    IKE  189f8161 87a7fb66 28c1daef 067663e7 97be7389 2a492c21 b1e9a0d4 e6729090
May 20, 12:15:43  Debug    IKE  ee9658ab 448b358d bbac8a2b 00c9afc6 5d2056ec 16a6f2fc 15c072b8 6daa1854
May 20, 12:15:43  Debug    IKE  6436983f 5b017f1e b1754da6 5dcf6180 7ff935d2 c7eabee1 2d231881 b58b97b5
May 20, 12:15:43  Debug    IKE  461d2e45 475b6518 256241ab 9eaa5609 686ff9bc 5f855841 a3df8bc0 fe0caa0b
May 20, 12:15:43  Info     IKE  couldn't find the proper pskey, try to get one by the peer's address.
May 20, 12:15:43  Debug    IKE  the psk found.
May 20, 12:15:43  Debug    IKE  psk: 2007-05-20 12:15:43: DEBUG2:
May 20, 12:15:43  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
May 20, 12:15:43  Debug    IKE  nonce 1: 2007-05-20 12:15:43: DEBUG:
May 20, 12:15:43  Debug    IKE  acb79f3a 1166a626 4f6d1fd9 36035f57
May 20, 12:15:43  Debug    IKE  nonce 2: 2007-05-20 12:15:43: DEBUG:
May 20, 12:15:43  Debug    IKE  df2b3d6d b81b625d 53233f41 fdf8058e
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  SKEYID computed:
May 20, 12:15:43  Debug    IKE  b7b0630e aeaae765 8b2bccd0 090aade9 d62145b3
```

```
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  SKEYID_d computed:
May 20, 12:15:43  Debug    IKE  1717a9cf 5642d771 016d6c40 089bc384 98b86c2b
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  SKEYID_a computed:
May 20, 12:15:43  Debug    IKE  84a2ae44 be71bf6d a40cd9e7 838d42ff 46cdf35d
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  SKEYID_e computed:
May 20, 12:15:43  Debug    IKE  ecdec30a 53ed983a 93dd9daa 4df47eb5 0503b18d
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  compute intermediate encryption key K1
May 20, 12:15:43  Debug    IKE  00
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  compute intermediate encryption key K2
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502
May 20, 12:15:43  Debug    IKE  aa443bb9 3a75bc81 b1605434 42930304 c4f39c74
May 20, 12:15:43  Debug    IKE  final encryption key computed:
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  IV computed:
May 20, 12:15:43  Debug    IKE  2d44d9e3 27802d21
May 20, 12:15:43  Debug    IKE  HASH received:
May 20, 12:15:43  Debug    IKE  6ecb0022 9d00b8d5 1d8a2657 f9835f90 3989a857
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  6abcdfca fd6edf9d f1c73b33 12877671 87224c29 f2a07e4a d6d4f6ab f457531a
May 20, 12:15:43  Debug    IKE  14c9dfd7 557ace32 664823d7 7071a0a8 9b192ba9 af8ae0a4 9dca146e ecf0787c
May 20, 12:15:43  Debug    IKE  c776e444 fe5549fc 19462523 c55e5428 3b5430d4 1e22299f 1159037b bfc1e01c
May 20, 12:15:43  Debug    IKE  5bd21912 2d7d2062 d6cc9885 a2d238ee 5151e47d 63c3feb3 490df121 1999bbeb
May 20, 12:15:43  Debug    IKE  3658591a 2da7b45a ab105969 dbca0dce 786771b1 d88a9e29 19ffc8f5 3cdd567a
May 20, 12:15:43  Debug    IKE  45561cb4 f2a94dba bbe63d49 6884e905 0ad1fa73 16a4199f 9609a1ad e54907d9
May 20, 12:15:43  Debug    IKE  c7c7b2ec 79bcb3ce eba3dda0 c4960837 208b3a9f 6de92e44 e92d8a69 e56a068d
May 20, 12:15:43  Debug    IKE  c18ae7fc bc223f08 144436d6 213e3505 b66e275e 242ace4a 4a261d4d 85b8e750
May 20, 12:15:43  Debug    IKE  0eec5bb9 5976e03b 489fab77 ca78ff22 00000001 00000001 00000028 01010001
May 20, 12:15:43  Debug    IKE  00000020 01010000 800b0001 800c7080 80010005 80030001 80020002 80040002
May 20, 12:15:43  Debug    IKE  011101f4 c0a8d7e2
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  HASH (init) computed:
May 20, 12:15:43  Debug    IKE  6ecb0022 9d00b8d5 1d8a2657 f9835f90 3989a857
May 20, 12:15:43  Debug    IKE  HASH for PSK validated.
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  generate HASH_I
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  3658591a 2da7b45a ab105969 dbca0dce 786771b1 d88a9e29 19ffc8f5 3cdd567a
May 20, 12:15:43  Debug    IKE  45561cb4 f2a94dba bbe63d49 6884e905 0ad1fa73 16a4199f 9609a1ad e54907d9
May 20, 12:15:43  Debug    IKE  c7c7b2ec 79bcb3ce eba3dda0 c4960837 208b3a9f 6de92e44 e92d8a69 e56a068d
May 20, 12:15:43  Debug    IKE  c18ae7fc bc223f08 144436d6 213e3505 b66e275e 242ace4a 4a261d4d 85b8e750
May 20, 12:15:43  Debug    IKE  6abcdfca fd6edf9d f1c73b33 12877671 87224c29 f2a07e4a d6d4f6ab f457531a
May 20, 12:15:43  Debug    IKE  14c9dfd7 557ace32 664823d7 7071a0a8 9b192ba9 af8ae0a4 9dca146e ecf0787c
May 20, 12:15:43  Debug    IKE  c776e444 fe5549fc 19462523 c55e5428 3b5430d4 1e22299f 1159037b bfc1e01c
May 20, 12:15:43  Debug    IKE  5bd21912 2d7d2062 d6cc9885 a2d238ee 5151e47d 63c3feb3 490df121 1999bbeb
May 20, 12:15:43  Debug    IKE  489fab77 ca78ff22 0eec5bb9 5976e03b 00000001 00000001 00000028 01010001
May 20, 12:15:43  Debug    IKE  00000020 01010000 800b0001 800c7080 80010005 80030001 80020002 80040002
May 20, 12:15:43  Debug    IKE  02000000 726f6164 77617272 696f72
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  HASH (init) computed:
May 20, 12:15:43  Debug    IKE  1f1462e1 00435e46 39d01763 e2f0f7a2 a5436df4
May 20, 12:15:43  Info     IKE  Adding remote and local NAT-D payloads.
May 20, 12:15:43  Info     IKE  Hashing 192.168.215.226[4500] with algo #2 (NAT-T forced)
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Info     IKE  Hashing 192.168.215.2[4500] with algo #2 (NAT-T forced)
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 20
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 20
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 0
May 20, 12:15:43  Debug    IKE  Adding NON-ESP marker
May 20, 12:15:43  Debug    IKE  104 bytes from 192.168.215.2[4500] to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  sockname 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet from 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet to 192.168.215.226[4500]
```

```
May 20, 12:15:43  Debug    IKE  1 times of 104 bytes message will be sent to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  00000000 489fab77 ca78ff22 0eec5bb9 5976e03b 08100400 00000000 00000064
May 20, 12:15:43  Debug    IKE  14000018 1f1462e1 00435e46 39d01763 e2f0f7a2 a5436df4 14000018 58ee9208
May 20, 12:15:43  Debug    IKE  72bb8972 667f3791 0f863aea e561cb67 00000018 58ee9208 72bb8972 667f3791
May 20, 12:15:43  Debug    IKE  0f863aea e561cb67
May 20, 12:15:43  Debug    IKE  compute IV for phase2
May 20, 12:15:43  Debug    IKE  phase1 last IV:
May 20, 12:15:43  Debug    IKE  2d44d9e3 27802d21 cbfd5baf
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  phase2 IV computed:
May 20, 12:15:43  Debug    IKE  4742b91b b0e7d38c
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  cbfd5baf 0000001c 00000001 01106002 489fab77 ca78ff22 0eec5bb9 5976e03b
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  HASH computed:
May 20, 12:15:43  Debug    IKE  278363b7 1a6ce9db 51e85974 6450f2c0 2541c3fb
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  pad length = 4
May 20, 12:15:43  Debug    IKE  0b000018 278363b7 1a6ce9db 51e85974 6450f2c0 2541c3fb 0000001c 00000001
May 20, 12:15:43  Debug    IKE  01106002 489fab77 ca78ff22 0eec5bb9 5976e03b 00000004
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  with key:
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43  Debug    IKE  encrypted payload by IV:
May 20, 12:15:43  Debug    IKE  4742b91b b0e7d38c
May 20, 12:15:43  Debug    IKE  save IV for next:
May 20, 12:15:43  Debug    IKE  1cf987ee 7b770249
May 20, 12:15:43  Debug    IKE  encrypted.
May 20, 12:15:43  Debug    IKE  Adding NON-ESP marker
May 20, 12:15:43  Debug    IKE  88 bytes from 192.168.215.2[4500] to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  sockname 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet from 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  1 times of 88 bytes message will be sent to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  00000000 489fab77 ca78ff22 0eec5bb9 5976e03b 08100501 cbfd5baf 00000054
May 20, 12:15:43  Debug    IKE  e6fab32c 174d3e92 7162d8c5 e4cc745e 1b79bf13 6337cb27 796ed726 00e69918
May 20, 12:15:43  Debug    IKE  b0a3ea23 8390c95b 84a75a92 068d389e 1cf987ee 7b770249
May 20, 12:15:43  Debug    IKE  sendto Information notify.
May 20, 12:15:43  Debug    IKE  IV freed
May 20, 12:15:43  Info     IKE  ISAKMP-SA established 192.168.215.2[4500]-192.168.215.226[4500] spi:
489fab77ca78ff22:0eec5bb95976e03b
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  begin QUICK mode.
May 20, 12:15:43  Info     IKE  initiate new phase 2 negotiation: 192.168.215.2[4500]<=>192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  compute IV for phase2
May 20, 12:15:43  Debug    IKE  phase1 last IV:
May 20, 12:15:43  Debug    IKE  2d44d9e3 27802d21 a6f8927d
May 20, 12:15:43  Debug    IKE  hash(sha1)
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  phase2 IV computed:
May 20, 12:15:43  Debug    IKE  527d772b 1f1652d4
May 20, 12:15:43  Debug    IKE  call pfkey_send_getspi
May 20, 12:15:43  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.226[0]->192.168.215.2[0]
May 20, 12:15:43  Debug    IKE  pfkey getspi sent.
May 20, 12:15:43  Debug    IKE  get pfkey GETSPI message
May 20, 12:15:43  Debug    IKE  02010003 0a000000 06020000 88250000 02000100 0785e0b7 80700000 00000000
May 20, 12:15:43  Debug    IKE  03000500 ff200000 10020000 c0a8d7e2 00000000 00000000 03000600 ff200000
May 20, 12:15:43  Debug    IKE  10020000 c0a8d702 00000000 00000000
May 20, 12:15:43  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.226[0]->192.168.215.2[0]
spi=126214327(0x785e0b7)
May 20, 12:15:43  Info     IKE  NAT detected -> UDP encapsulation (ENC_MODE 1->3).
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  compute DH's private.
May 20, 12:15:43  Debug    IKE  7c55b11e 10faa628 fff676d8 02b1b9a1 0b47959f ebc909d3 ef84b119 ec33a13b
May 20, 12:15:43  Debug    IKE  13772a3f 1d48b0e0 2d0080f2 de2d8a5f 261e4c2f e9af858a 6bf39dcc ff012078
May 20, 12:15:43  Debug    IKE  9805409c ea7b5ca9 f6ef9f11 771744af f8b07657 13c2c608 a16efbb7 480482f0
May 20, 12:15:43  Debug    IKE  ea592311 ccb45451 22e78b0c f726eac5 e0e90254 95384e36 84bdf3d0 cd8b97ed
May 20, 12:15:43  Debug    IKE  compute DH's public.
May 20, 12:15:43  Debug    IKE  0207a581 cea0d81f 45c1a73a 51dc46a4 463412c9 a086ccbe 7252ba2a 584bd718
```

```
May 20, 12:15:43  Debug    IKE  ed2a18ef 9537ec6f d7d64ac5 1b3fb113 b566e6c6 0b06ad39 1e26e1d1 f4ebac6f
May 20, 12:15:43  Debug    IKE  898cf641 de646757 8d775cda 2a02a301 f987993c 416090e8 ddfd4de7 199e7f89
May 20, 12:15:43  Debug    IKE  c42e9392 446d2556 3dfdaff5 20977b74 9abcb55e f21e152d 0d7f8da6 66620430
May 20, 12:15:43  Debug    IKE  use local ID type IPv4_address
May 20, 12:15:43  Debug    IKE  use remote ID type IPv4_subnet
May 20, 12:15:43  Debug    IKE  IDci:
May 20, 12:15:43  Debug    IKE  01000000 c0a8d702
May 20, 12:15:43  Debug    IKE  IDcr:
May 20, 12:15:43  Debug    IKE  04000000 0a010300 ffffff00
May 20, 12:15:43  Debug    IKE  add payload of len 48, next type 10
May 20, 12:15:43  Debug    IKE  add payload of len 16, next type 4
May 20, 12:15:43  Debug    IKE  add payload of len 128, next type 5
May 20, 12:15:43  Debug    IKE  add payload of len 8, next type 5
May 20, 12:15:43  Debug    IKE  add payload of len 12, next type 0
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  a6f8927d 0a000034 00000001 00000001 00000028 01030401 0785e0b7 0000001c
May 20, 12:15:43  Debug    IKE  01030000 80010001 80027080 80040003 80050002 80030002 04000014 c3d1e785
May 20, 12:15:43  Debug    IKE  f7adc550 4403260d 7e9d0ffe 05000084 0207a581 cea0d81f 45c1a73a 51dc46a4
May 20, 12:15:43  Debug    IKE  463412c9 a086ccbe 7252ba2a 584bd718 ed2a18ef 9537ec6f d7d64ac5 1b3fb113
May 20, 12:15:43  Debug    IKE  b566e6c6 0b06ad39 1e26e1d1 f4ebac6f 898cf641 de646757 8d775cda 2a02a301
May 20, 12:15:43  Debug    IKE  f987993c 416090e8 ddfd4de7 199e7f89 c42e9392 446d2556 3dfdaff5 20977b74
May 20, 12:15:43  Debug    IKE  9abcb55e f21e152d 0d7f8da6 66620430 0500000c 01000000 c0a8d702 00000010
May 20, 12:15:43  Debug    IKE  04000000 0a010300 ffffff00
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  HASH computed:
May 20, 12:15:43  Debug    IKE  e1bb92d0 4b276a7e b595a518 6ef101ce 01428908
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  01000018 e1bb92d0 4b276a7e b595a518 6ef101ce 01428908 0a000034 00000001
May 20, 12:15:43  Debug    IKE  00000001 00000028 01030401 0785e0b7 0000001c 01030000 80010001 80027080
May 20, 12:15:43  Debug    IKE  80040003 80050002 80030002 04000014 c3d1e785 f7adc550 4403260d 7e9d0ffe
May 20, 12:15:43  Debug    IKE  05000084 0207a581 cea0d81f 45c1a73a 51dc46a4 463412c9 a086ccbe 7252ba2a
May 20, 12:15:43  Debug    IKE  584bd718 ed2a18ef 9537ec6f d7d64ac5 1b3fb113 b566e6c6 0b06ad39 1e26e1d1
May 20, 12:15:43  Debug    IKE  f4ebac6f 898cf641 de646757 8d775cda 2a02a301 f987993c 416090e8 ddfd4de7
May 20, 12:15:43  Debug    IKE  199e7f89 c42e9392 446d2556 3dfdaff5 20977b74 9abcb55e f21e152d 0d7f8da6
May 20, 12:15:43  Debug    IKE  66620430 0500000c 01000000 c0a8d702 00000010 04000000 0a010300 ffffff00
May 20, 12:15:43  Debug    IKE  00000000 00000008
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  with key:
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43  Debug    IKE  encrypted payload by IV:
May 20, 12:15:43  Debug    IKE  527d772b 1f1652d4
May 20, 12:15:43  Debug    IKE  save IV for next:
May 20, 12:15:43  Debug    IKE  df3bc39f 1f94bd76
May 20, 12:15:43  Debug    IKE  encrypted.
May 20, 12:15:43  Debug    IKE  Adding NON-ESP marker
May 20, 12:15:43  Debug    IKE  296 bytes from 192.168.215.2[4500] to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  sockname 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet from 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  1 times of 296 bytes message will be sent to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  00000000 489fab77 ca78ff22 0eec5bb9 5976e03b 08102001 a6f8927d 00000124
May 20, 12:15:43  Debug    IKE  752ad4ec 1fdc2f7b 22e25f1d f7a063d9 2f667fc1 42c16c73 28826fbf 5706d34f
May 20, 12:15:43  Debug    IKE  bdbb6b5a ec9c70df 58f09d54 b03bd5a7 2af4dca5 9ada3821 bf3b26bb a0b7cfb0
May 20, 12:15:43  Debug    IKE  109026c2 b6183cdf a03df18d d4782174 de3b3c75 737eafb1 1b26ddb7 fccb200e
May 20, 12:15:43  Debug    IKE  bbe6e8ed 7787d71b 0fcfa759 0ab2fa1b d75c46ab af1b36c5 3bef4dd5 1568ad24
May 20, 12:15:43  Debug    IKE  a2ff3a16 6d9f1e53 befe7206 c0c28615 4202bd00 a30ed2d0 700bffc3 d8e28c5e
May 20, 12:15:43  Debug    IKE  917e27dc 6aa55f80 88f80747 7acd0f09 de49fd4a b3cbf134 34243ecf 95902256
May 20, 12:15:43  Debug    IKE  bccdc6bf 874b175b 4d91bae5 7fb240d4 c4a325f1 38dfdfe7 974da6cf bb0c2e94
May 20, 12:15:43  Debug    IKE  5d91f943 a7239f59 c8cc8f15 fd558bd9 b24ad92a 3bce43bb 5336bfd5 739e46fa
May 20, 12:15:43  Debug    IKE  df3bc39f 1f94bd76
May 20, 12:15:43  Debug    IKE  resend phase2 packet 489fab77ca78ff22:0eec5bb95976e03b:0000a6f8
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  292 bytes message received from 192.168.215.226[4500] to 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  489fab77 ca78ff22 0eec5bb9 5976e03b 08102001 a6f8927d 00000124 4efe15f0
May 20, 12:15:43  Debug    IKE  c2c47b72 ad9e6e86 638eb5cb d024668d e06261f3 cb7ae1fa fa94d7a8 eaacc688
May 20, 12:15:43  Debug    IKE  6d8396ce b35f39bf 9f856647 c3db40cb dfbaccf2 71eba180 a85d7885 40daee3e
May 20, 12:15:43  Debug    IKE  2004e90c 7360d7fa 469be4e0 772ae165 8cf89820 99bc195c 7537e786 cba0d9a6
May 20, 12:15:43  Debug    IKE  1f2c8d5b 1397ff44 19f67eaa f5756eae 5c82408e f2ac4fd8 03ad29a7 b3d916b2
May 20, 12:15:43  Debug    IKE  7c8e7c66 f7b2d174 5e6b0a3f f5ef4bc3 bebba4ac 20bef7ba 8bbe14dd f5048f4f
May 20, 12:15:43  Debug    IKE  a22ebe13 3da076e6 2c2cb469 156637be ec0e5b44 dc6a945f 881c3cc1 b9ad781e
May 20, 12:15:43  Debug    IKE  b32256d6 f9e6acb9 eb65eb10 8d4de3fb 40450361 de80d3d8 c7187835 8445fa6b
```

```
May 20, 12:15:43  Debug    IKE  4af8116a c82b41e4 886f9f16 d2a819d6 e1886d76 d4e46f54 fb66db23 eebe7b79
May 20, 12:15:43  Debug    IKE  462a7901
May 20, 12:15:43  Debug    IKE  begin decryption.
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  IV was saved for next processing:
May 20, 12:15:43  Debug    IKE  eebe7b79 462a7901
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  with key:
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43  Debug    IKE  decrypted payload by IV:
May 20, 12:15:43  Debug    IKE  df3bc39f 1f94bd76
May 20, 12:15:43  Debug    IKE  decrypted payload, but not trimed.
May 20, 12:15:43  Debug    IKE  01000018 55bebbd6 abd23bf8 41610b90 198d2c26 c3dca8a5 0a000034 00000001
May 20, 12:15:43  Debug    IKE  00000001 00000028 01030401 04ec30a3 0000001c 01030000 80010001 80027080
May 20, 12:15:43  Debug    IKE  80040003 80050002 80030002 04000014 c1354731 e8a86ec9 34326bb0 12b442c3
May 20, 12:15:43  Debug    IKE  05000084 2b99b73a 645dd432 27377540 4e63ce32 51eb6b28 75725c31 18457933
May 20, 12:15:43  Debug    IKE  9b52bb38 66057163 167a5f54 f86165a6 d8319ce2 0123c6cd 79529888 7afe77e4
May 20, 12:15:43  Debug    IKE  2865e85c e7dc7fb0 ef80a9ec f42d7c94 b9c5cadb 2a3eca6f 18f9e9bc e6a38f1b
May 20, 12:15:43  Debug    IKE  65d41ed7 2614d2bd 3d5685eb 43bf32f1 3153fa31 c51622bf 588655d2 855b1184
May 20, 12:15:43  Debug    IKE  772d3008 0500000c 01000000 c0a8d702 00000010 04000000 0a010300 ffffff00
May 20, 12:15:43  Debug    IKE  abede894 a599bd07
May 20, 12:15:43  Debug    IKE  padding len=7
May 20, 12:15:43  Debug    IKE  skip to trim padding.
May 20, 12:15:43  Debug    IKE  decrypted.
May 20, 12:15:43  Debug    IKE  489fab77 ca78ff22 0eec5bb9 5976e03b 08102001 a6f8927d 00000124 01000018
May 20, 12:15:43  Debug    IKE  55bebbd6 abd23bf8 41610b90 198d2c26 c3dca8a5 0a000034 00000001 00000001
May 20, 12:15:43  Debug    IKE  00000028 01030401 04ec30a3 0000001c 01030000 80010001 80027080 80040003
May 20, 12:15:43  Debug    IKE  80050002 80030002 04000014 c1354731 e8a86ec9 34326bb0 12b442c3 05000084
May 20, 12:15:43  Debug    IKE  2b99b73a 645dd432 27377540 4e63ce32 51eb6b28 75725c31 18457933 9b52bb38
May 20, 12:15:43  Debug    IKE  66057163 167a5f54 f86165a6 d8319ce2 0123c6cd 79529888 7afe77e4 2865e85c
May 20, 12:15:43  Debug    IKE  e7dc7fb0 ef80a9ec f42d7c94 b9c5cadb 2a3eca6f 18f9e9bc e6a38f1b 65d41ed7
May 20, 12:15:43  Debug    IKE  2614d2bd 3d5685eb 43bf32f1 3153fa31 c51622bf 588655d2 855b1184 772d3008
May 20, 12:15:43  Debug    IKE  0500000c 01000000 c0a8d702 00000010 04000000 0a010300 ffffff00 abede894
May 20, 12:15:43  Debug    IKE  a599bd07
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=8(hash)
May 20, 12:15:43  Debug    IKE  seen nptype=1(sa)
May 20, 12:15:43  Debug    IKE  seen nptype=10(nonce)
May 20, 12:15:43  Debug    IKE  seen nptype=4(ke)
May 20, 12:15:43  Debug    IKE  seen nptype=5(id)
May 20, 12:15:43  Debug    IKE  seen nptype=5(id)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  HASH allocated:hbuf->l=280 actual:tlen=248
May 20, 12:15:43  Debug    IKE  HASH(2) received:2007-05-20 12:15:43: DEBUG:
May 20, 12:15:43  Debug    IKE  55bebbd6 abd23bf8 41610b90 198d2c26 c3dca8a5
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  a6f8927d c3d1e785 f7adc550 4403260d 7e9d0ffe 0a000034 00000001 00000001
May 20, 12:15:43  Debug    IKE  00000028 01030401 04ec30a3 0000001c 01030000 80010001 80027080 80040003
May 20, 12:15:43  Debug    IKE  80050002 80030002 04000014 c1354731 e8a86ec9 34326bb0 12b442c3 05000084
May 20, 12:15:43  Debug    IKE  2b99b73a 645dd432 27377540 4e63ce32 51eb6b28 75725c31 18457933 9b52bb38
May 20, 12:15:43  Debug    IKE  66057163 167a5f54 f86165a6 d8319ce2 0123c6cd 79529888 7afe77e4 2865e85c
May 20, 12:15:43  Debug    IKE  e7dc7fb0 ef80a9ec f42d7c94 b9c5cadb 2a3eca6f 18f9e9bc e6a38f1b 65d41ed7
May 20, 12:15:43  Debug    IKE  2614d2bd 3d5685eb 43bf32f1 3153fa31 c51622bf 588655d2 855b1184 772d3008
May 20, 12:15:43  Debug    IKE  0500000c 01000000 c0a8d702 00000010 04000000 0a010300 ffffff00
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  HASH computed:
May 20, 12:15:43  Debug    IKE  55bebbd6 abd23bf8 41610b90 198d2c26 c3dca8a5
May 20, 12:15:43  Debug    IKE  total SA len=48
May 20, 12:15:43  Debug    IKE  00000001 00000001 00000028 01030401 0785e0b7 0000001c 01030000 80010001
May 20, 12:15:43  Debug    IKE  80027080 80040003 80050002 80030002
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=2(prop)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  proposal #1 len=40
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=3(trns)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  transform #1 len=28
May 20, 12:15:43  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug    IKE  life duration was in TLV.
May 20, 12:15:43  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
May 20, 12:15:43  Debug    IKE  UDP encapsulation requested
May 20, 12:15:43  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
```

```
May 20, 12:15:43  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  pair 1:
May 20, 12:15:43  Debug    IKE  0x309f30: next=0x0 tnext=0x0
May 20, 12:15:43  Debug    IKE  proposal #1: 1 transform
May 20, 12:15:43  Debug    IKE  total SA len=48
May 20, 12:15:43  Debug    IKE  00000001 00000001 00000028 01030401 04ec30a3 0000001c 01030000 80010001
May 20, 12:15:43  Debug    IKE  80027080 80040003 80050002 80030002
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=2(prop)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  proposal #1 len=40
May 20, 12:15:43  Debug    IKE  begin.
May 20, 12:15:43  Debug    IKE  seen nptype=3(trns)
May 20, 12:15:43  Debug    IKE  succeed.
May 20, 12:15:43  Debug    IKE  transform #1 len=28
May 20, 12:15:43  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug    IKE  life duration was in TLV.
May 20, 12:15:43  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
May 20, 12:15:43  Debug    IKE  UDP encapsulation requested
May 20, 12:15:43  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 12:15:43  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 20, 12:15:43  Debug    IKE  hmac(modp1024)
May 20, 12:15:43  Debug    IKE  pair 1:
May 20, 12:15:43  Debug    IKE  0x309f40: next=0x0 tnext=0x0
May 20, 12:15:43  Debug    IKE  proposal #1: 1 transform
May 20, 12:15:43  Debug    IKE  begin compare proposals.
May 20, 12:15:43  Debug    IKE  pair[1]: 0x309f40
May 20, 12:15:43  Debug    IKE  0x309f40: next=0x0 tnext=0x0
May 20, 12:15:43  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
May 20, 12:15:43  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
May 20, 12:15:43  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 12:15:43  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 20, 12:15:43  Debug    IKE  peer's single bundle:
May 20, 12:15:43  Debug    IKE  (proto_id=ESP spisize=4 spi=04ec30a3 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
May 20, 12:15:43  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 12:15:43  Debug    IKE  my single bundle:
May 20, 12:15:43  Debug    IKE  (proto_id=ESP spisize=4 spi=0785e0b7 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
May 20, 12:15:43  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 12:15:43  Info     IKE  Adjusting my encmode UDP-Tunnel->Tunnel
May 20, 12:15:43  Info     IKE  Adjusting peer's encmode UDP-Tunnel(3)->Tunnel(1)
May 20, 12:15:43  Debug    IKE  matched
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  HASH(3) generate
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  00a6f892 7dc3d1e7 85f7adc5 50440326 0d7e9d0f fec13547 31e8a86e c934326b
May 20, 12:15:43  Debug    IKE  b012b442 c3
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  HASH computed:
May 20, 12:15:43  Debug    IKE  9446acf6 92ae5827 9ba5aa22 8d922ef0 5c3c3b30
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 0
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  00000018 9446acf6 92ae5827 9ba5aa22 8d922ef0 5c3c3b30 00000000 00000008
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  with key:
May 20, 12:15:43  Debug    IKE  bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43  Debug    IKE  encrypted payload by IV:
May 20, 12:15:43  Debug    IKE  eebe7b79 462a7901
May 20, 12:15:43  Debug    IKE  save IV for next:
May 20, 12:15:43  Debug    IKE  d87f051d 479cb619
May 20, 12:15:43  Debug    IKE  encrypted.
May 20, 12:15:43  Debug    IKE  Adding NON-ESP marker
May 20, 12:15:43  Debug    IKE  64 bytes from 192.168.215.2[4500] to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  sockname 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet from 192.168.215.2[4500]
May 20, 12:15:43  Debug    IKE  send packet to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  1 times of 64 bytes message will be sent to 192.168.215.226[4500]
May 20, 12:15:43  Debug    IKE  00000000 489fab77 ca78ff22 0eec5bb9 5976e03b 08102001 a6f8927d 0000003c
May 20, 12:15:43  Debug    IKE  fd8d7127 4cf9c07a 95158a1c b58407d1 f5b7bc6e 0f4227b1 d87f051d 479cb619
```

```
May 20, 12:15:43  Debug    IKE  compute DH's shared.
May 20, 12:15:43  Debug    IKE  ba444ced 08183b45 f06a5c36 932e0f12 bb7c91ef e341d87c 5c39bfef fdfc7e50
May 20, 12:15:43  Debug    IKE  ac002457 c7d665f1 1841ba1e a3578ab3 3596f6e1 adb67a49 c736001a c8cbea91
May 20, 12:15:43  Debug    IKE  f7c96b33 aac88186 5a985182 25ccdc89 0cdafcfc a59c3141 b5537606 6194bc27
May 20, 12:15:43  Debug    IKE  8ad02730 16de9365 488bc308 c84a3003 74815377 7c3d4d07 67b99dc5 ae883816
May 20, 12:15:43  Debug    IKE  KEYMAT compute with
May 20, 12:15:43  Debug    IKE  ba444ced 08183b45 f06a5c36 932e0f12 bb7c91ef e341d87c 5c39bfef fdfc7e50
May 20, 12:15:43  Debug    IKE  ac002457 c7d665f1 1841ba1e a3578ab3 3596f6e1 adb67a49 c736001a c8cbea91
May 20, 12:15:43  Debug    IKE  f7c96b33 aac88186 5a985182 25ccdc89 0cdafcfc a59c3141 b5537606 6194bc27
May 20, 12:15:43  Debug    IKE  8ad02730 16de9365 488bc308 c84a3003 74815377 7c3d4d07 67b99dc5 ae883816
May 20, 12:15:43  Debug    IKE  030785e0 b7c3d1e7 85f7adc5 50440326 0d7e9d0f fec13547 31e8a86e c934326b
May 20, 12:15:43  Debug    IKE  b012b442 c3
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  encklen=192 authklen=160
May 20, 12:15:43  Debug    IKE  generating 640 bits of key (dupkeymat=4)
May 20, 12:15:43  Debug    IKE  generating K1...K4 for KEYMAT.
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  e20d98d8 0c940238 ba5e604e c38a8b3b 29260ca7 ae551f5a 7dbf8400 3b77bec5
May 20, 12:15:43  Debug    IKE  98fcbe62 0d44426d 72bcb1a5 6005cef9 5a2f1122 ffca8a37 54a32a41 128fe20e
May 20, 12:15:43  Debug    IKE  7b634d5f f0b6678d 6579b2a1 ce46d375
May 20, 12:15:43  Debug    IKE  KEYMAT compute with
May 20, 12:15:43  Debug    IKE  ba444ced 08183b45 f06a5c36 932e0f12 bb7c91ef e341d87c 5c39bfef fdfc7e50
May 20, 12:15:43  Debug    IKE  ac002457 c7d665f1 1841ba1e a3578ab3 3596f6e1 adb67a49 c736001a c8cbea91
May 20, 12:15:43  Debug    IKE  f7c96b33 aac88186 5a985182 25ccdc89 0cdafcfc a59c3141 b5537606 6194bc27
May 20, 12:15:43  Debug    IKE  8ad02730 16de9365 488bc308 c84a3003 74815377 7c3d4d07 67b99dc5 ae883816
May 20, 12:15:43  Debug    IKE  0304ec30 a3c3d1e7 85f7adc5 50440326 0d7e9d0f fec13547 31e8a86e c934326b
May 20, 12:15:43  Debug    IKE  b012b442 c3
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  encklen=192 authklen=160
May 20, 12:15:43  Debug    IKE  generating 640 bits of key (dupkeymat=4)
May 20, 12:15:43  Debug    IKE  generating K1...K4 for KEYMAT.
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  eb18b6aa ecb53198 6c779238 cec7634b 1e36882b b1fc2fd4 edc027d4 28bd2676
May 20, 12:15:43  Debug    IKE  7480bb48 6606c01b d45f7db7 12ae18c4 330c7b59 91111b16 41c2c92b 95193cbf
May 20, 12:15:43  Debug    IKE  19141b79 17c61fe4 f8b78be3 249c545c
May 20, 12:15:43  Debug    IKE  KEYMAT computed.
May 20, 12:15:43  Debug    IKE  call pk_sendupdate
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  call pfkey_send_update_nat
May 20, 12:15:43  Debug    APP  Received SADB message type UPDATE, 192.168.215.226 [4500] -> 192.168.215.2 [4500]
May 20, 12:15:43  Debug    APP  SA change detected
May 20, 12:15:43  Debug    IKE  pfkey update sent.
May 20, 12:15:43  Debug    IKE  encryption(3des)
May 20, 12:15:43  Debug    IKE  hmac(hmac_sha1)
May 20, 12:15:43  Debug    IKE  call pfkey_send_add_nat
May 20, 12:15:43  Debug    APP  Received SADB message type ADD, 192.168.215.2 [4500] -> 192.168.215.226 [4500]
May 20, 12:15:43  Debug    APP  SA change detected
May 20, 12:15:43  Debug    APP  Connection m0n0Wall is up
May 20, 12:15:43  Debug    IKE  pfkey add sent.
May 20, 12:15:43  Debug    IKE  get pfkey UPDATE message
May 20, 12:15:43  Debug    IKE  02020003 14000000 06020000 88250000 02000100 0785e0b7 04000202 00000000
May 20, 12:15:43  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10021194 c0a8d7e2
May 20, 12:15:43  Debug    IKE  00000000 00000000 03000600 ff200000 10021194 c0a8d702 00000000 00000000
May 20, 12:15:43  Debug    IKE  04000300 00000000 00000000 00000000 80700000 00000000 00000000 00000000
May 20, 12:15:43  Debug    IKE  04000400 00000000 00000000 00000000 005a0000 00000000 00000000 00000000
May 20, 12:15:43  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.226[4500]->192.168.215.2[4500]
spi=126214327(0x785e0b7)
May 20, 12:15:43  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.226[4500]->192.168.215.2[4500]
spi=126214327(0x785e0b7)
May 20, 12:15:43  Debug    IKE  ===
May 20, 12:15:43  Debug    IKE  get pfkey ADD message
May 20, 12:15:43  Debug    IKE  02030003 14000000 06020000 88250000 02000100 04ec30a3 04000202 00000000
May 20, 12:15:43  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10021194 c0a8d702
May 20, 12:15:43  Debug    IKE  00000000 00000000 03000600 ff200000 10021194 c0a8d7e2 00000000 00000000
May 20, 12:15:43  Debug    IKE  04000300 00000000 00000000 00000000 80700000 00000000 00000000 00000000
```

```
May 20, 12:15:43  Debug    IKE  04000400 00000000 00000000 00000000 005a0000 00000000 00000000 00000000
May 20, 12:15:43  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.2[4500]->192.168.215.226[4500]
spi=82587811(0x4ec30a3)
May 20, 12:15:43  Debug    IKE  ===
```