IPSecuritas 3.0

Configuration Instructions

for

Draytek Vigor

May 23, 2007

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.

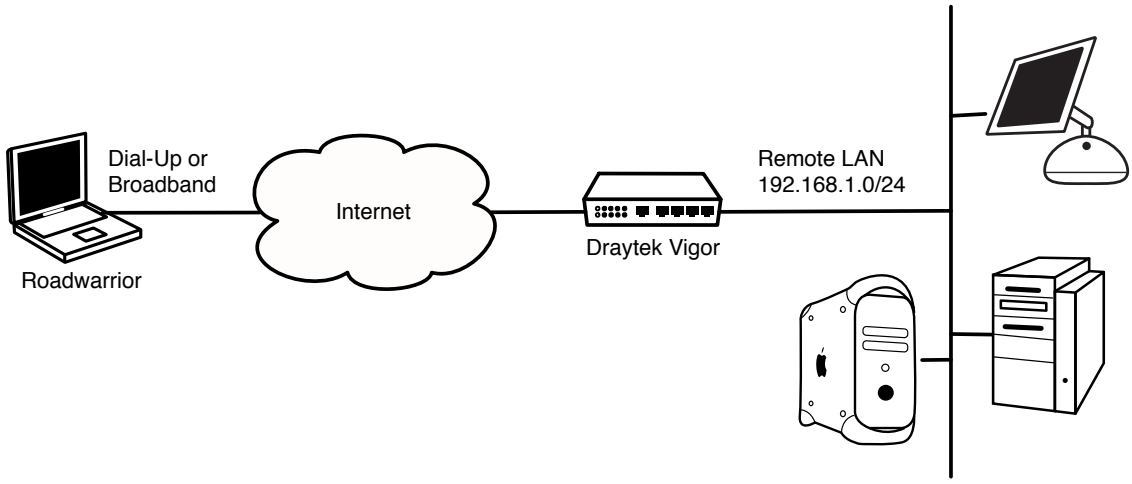
Acknowledgments

Many thanks to Stefan Wowereit 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 Draytek Vigor router/firewall. All information in this document is based on the following assumed network.

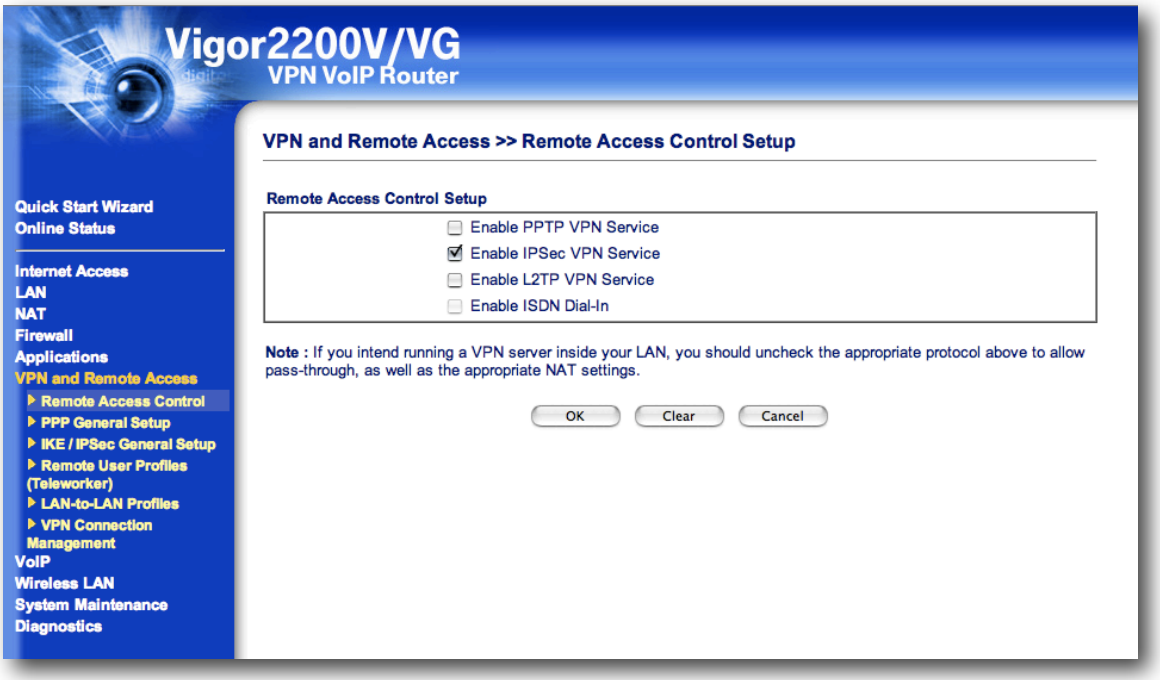


Draytek Vigor VPN Setup

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

Enable IPSec

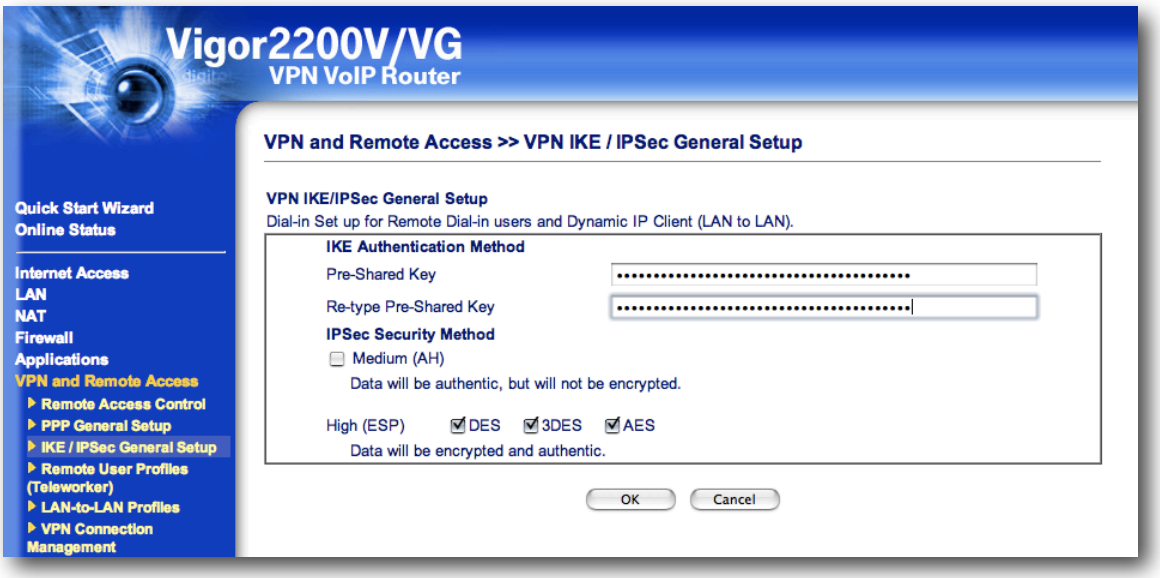
Open a web browser and connect to your Draytek router. Enter the administrator's user name and password if asked for. On the left side, click on **VPN and Remote Access** to open the submenu, then



click on **Remote Access Control**. Make sure the option **Enable IPSec VPN Service** is enabled (the other options may be switched off if you don't need them).
Press **OK** to save your changes.

Configure IKE and IPSec

On the left side, click on **IKE/IPSec General Setup**. Then, on the right side, enter a preshared key (a secure password) into the two text fields. Please remember the preshared key as you will need it again when setting up IPSecuritas. Disable the option **Medium (AH)** and make sure the options **DES**,



3DES and **AES** are enabled.
Press **OK** to save your changes. You may now proceed with the setup of IPSecuritas described in the next chapter.

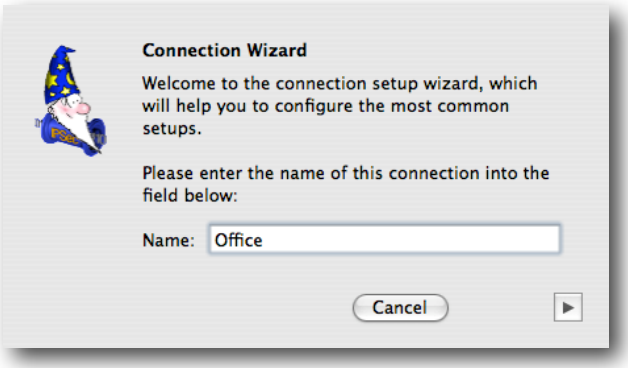
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the Draytek Vigor 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: 

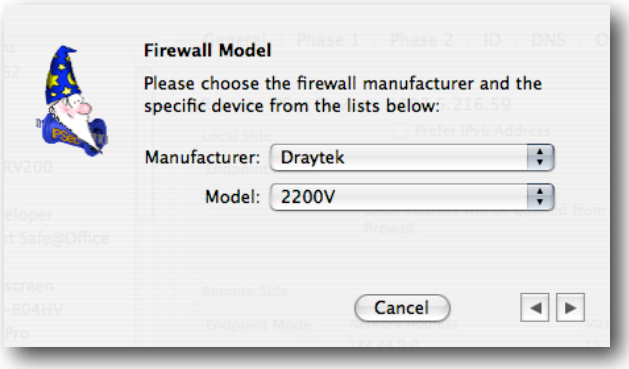
Enter Name of New Connection



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

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

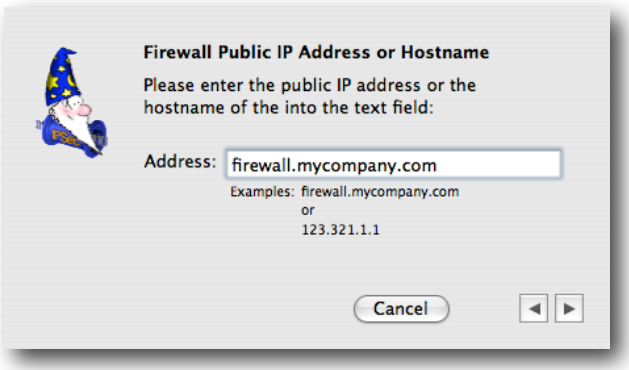
Select Router Model



Select **Draytek** from the manufacturer list and your model of firewall from the model list.

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

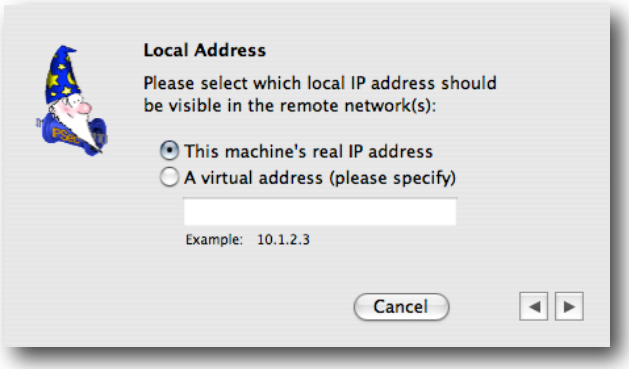
Enter Router's Public IP Address



Enter the public IP address or hostname of your Draytek Vigor 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.

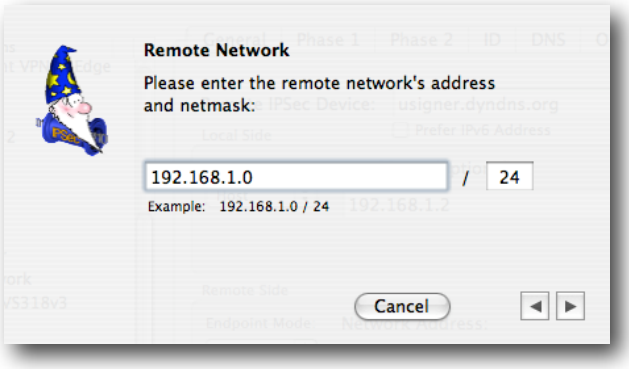
Enter a Virtual IP Address



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.

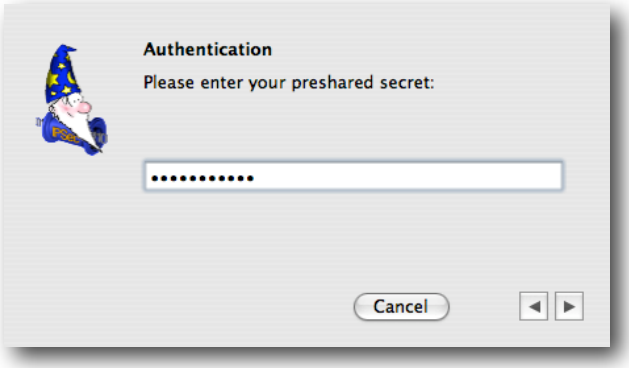
Enter Remote Network



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 Draytek Vigor.

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

Enter Preshared Key



Enter the same **Preshared Key** that you used for the Draytek Vigor.

Click on the right arrow to finish the connection setup.

Diagnosis

Reachability Test

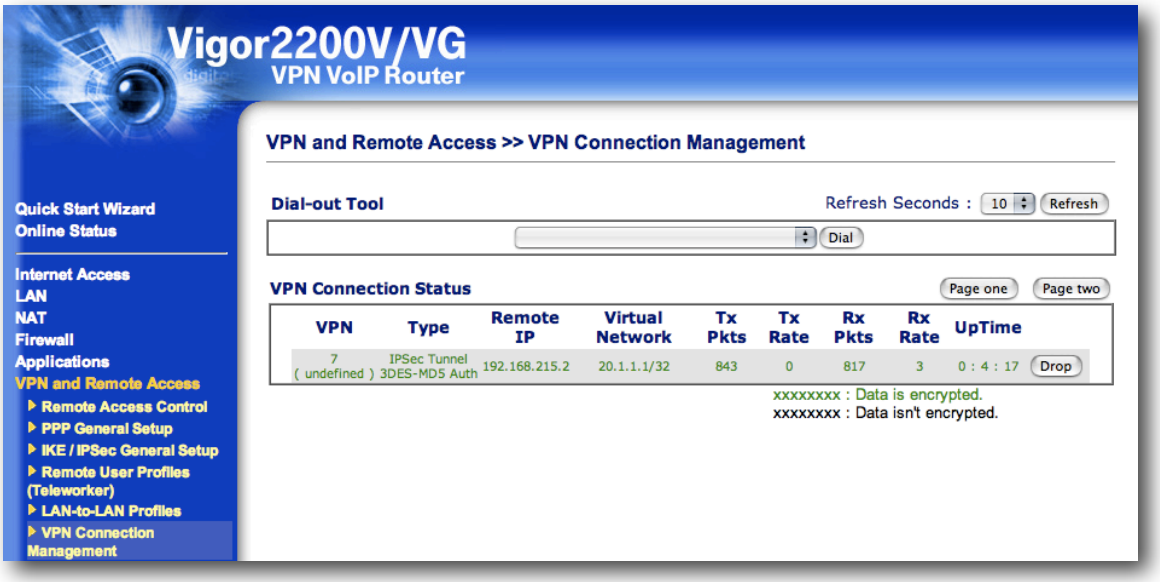
To test reachability of the remote host, open an **Terminal Window** (Utilities -> Terminal) and enter the command **ping**, followed by the Draytek Vigor **local IP address**. If the tunnel works correctly, a similar output is displayed:

```
[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
```

Vigor Connection State

While still logged into the Draytek Vigor web interface, open the VPN submenu by clicking on **VPN and Remote Access** on the left side. Then click on **VPN Connection Management** in the

submenu to display the conection status. A similar screen as depicted in the image below should appear,



listing all active VPN tunnels in the second table.

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 18, 22:45:47  Debug    APP  State change from IDLE to AUTHENTICATING after event START
May 18, 22:45:47  Info     APP  IKE daemon started
May 18, 22:45:47  Info     APP  IPSec started
May 18, 22:45:47  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
May 18, 22:45:47  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 18, 22:45:47  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 18, 22:45:47  Info     IKE  Foreground mode.
May 18, 22:45:47  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
May 18, 22:45:47  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
May 18, 22:45:47  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
May 18, 22:45:47  Info     IKE  Resize address pool from 0 to 255
May 18, 22:45:47  Debug    IKE  lifetime = 3600
May 18, 22:45:47  Debug    IKE  lifebyte = 0
May 18, 22:45:47  Debug    IKE  encklen=0
May 18, 22:45:47  Debug    IKE  p:1 t:1
May 18, 22:45:47  Debug    IKE  3DES-CBC(5)
May 18, 22:45:47  Debug    IKE  SHA(2)
May 18, 22:45:47  Debug    IKE  1024-bit MODP group(2)
May 18, 22:45:47  Debug    IKE  pre-shared key(1)
May 18, 22:45:47  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
May 18, 22:45:47  Debug    IKE  parse successed.
May 18, 22:45:47  Debug    IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
May 18, 22:45:47  Info     IKE  192.168.215.2[4500] used as isakmp port (fd=7)
May 18, 22:45:47  Info     IKE  192.168.215.2[500] used as isakmp port (fd=8)
May 18, 22:45:47  Debug    IKE  get pfkey X_SPDDUMP message
May 18, 22:45:47  Debug    IKE  02120000 0f000100 01000000 d5180000 03000500 ff180000 10020000 0a000b00
May 18, 22:45:47  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 14010101 00000000 00000000
May 18, 22:45:47  Debug    IKE  07001200 02000100 34a70900 00000000 28003200 02020000 10020000 c0a8d7ea
May 18, 22:45:47  Debug    IKE  00000000 00000000 10020000 c0a8d702 00000000 00000000
May 18, 22:45:47  Debug    IKE  get pfkey X_SPDDUMP message
May 18, 22:45:47  Debug    IKE  02120000 0f000100 00000000 d5180000 03000500 ff200000 10020000 14010101
May 18, 22:45:47  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 0a000b00 00000000 00000000
May 18, 22:45:47  Debug    IKE  07001200 02000200 33a70900 00000000 28003200 02020000 10020000 c0a8d702
May 18, 22:45:47  Debug    IKE  00000000 00000000 10020000 c0a8d7ea 00000000 00000000
```

```
May 18, 22:45:47  Debug   IKE  sub:0xbffff340: 20.1.1.1/32[0] 10.0.11.0/24[0] proto=any dir=out
May 18, 22:45:47  Debug   IKE  db :0x308b88: 10.0.11.0/24[0] 20.1.1.1/32[0] proto=any dir=in
May 18, 22:45:48  Info    APP  Initiated connection Vigor
May 18, 22:45:48  Debug   IKE  get pfkey ACQUIRE message
May 18, 22:45:48  Debug   IKE  02060003 24000000 10040000 00000000 03000500 ff200000 10020000 c0a8d702
May 18, 22:45:48  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7ea 00000000 00000000
May 18, 22:45:48  Debug   IKE  1c000d00 20000000 00030000 00000000 00010008 00000000 01000000 01000000
May 18, 22:45:48  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
May 18, 22:45:48  Debug   IKE  80700000 00000000 00000000 00000000 00040000 00000000 0001c001 00000000
May 18, 22:45:48  Debug   IKE  01000000 01000000 00000000 00000000 00000000 00000000 00000000 00000000
May 18, 22:45:48  Debug   IKE  80510100 00000000 80700000 00000000 00000000 00000000 000c0000 00000000
May 18, 22:45:48  Debug   IKE  00010001 00000000 01000000 01000000 00000000 00000000 00000000 00000000
May 18, 22:45:48  Debug   IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
May 18, 22:45:48  Error   IKE  inappropriate sadb acquire message passed.
May 18, 22:45:48  Debug   IKE  get pfkey ACQUIRE message
May 18, 22:45:48  Debug   IKE  02060003 14000000 d3010000 b90b0000 03000500 ff200000 10020000 c0a8d702
May 18, 22:45:48  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7ea 00000000 00000000
May 18, 22:45:48  Debug   IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
May 18, 22:45:48  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
May 18, 22:45:48  Debug   IKE  80700000 00000000 00000000 00000000 02001200 02000200 33a70900 00000000
May 18, 22:45:48  Debug   IKE  suitable outbound SP found: 20.1.1.1/32[0] 10.0.11.0/24[0] proto=any dir=out.
May 18, 22:45:48  Debug   IKE  sub:0xbffff31c: 10.0.11.0/24[0] 20.1.1.1/32[0] proto=any dir=in
May 18, 22:45:48  Debug   IKE  db :0x308b88: 10.0.11.0/24[0] 20.1.1.1/32[0] proto=any dir=in
May 18, 22:45:48  Debug   IKE  suitable inbound SP found: 10.0.11.0/24[0] 20.1.1.1/32[0] proto=any dir=in.
May 18, 22:45:48  Debug   IKE  new acquire 20.1.1.1/32[0] 10.0.11.0/24[0] proto=any dir=out
May 18, 22:45:48  Debug   IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:45:48  Debug   IKE  (trns_id=3DES encklen=0 authtype=hmac-md5)
May 18, 22:45:48  Debug   IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:45:48  Debug   IKE  in post_acquire
May 18, 22:45:48  Debug   IKE  configuration found for 192.168.215.234.
May 18, 22:45:48  Info    IKE  IPsec-SA request for 192.168.215.234 queued due to no phase1 found.
May 18, 22:45:48  Debug   IKE  ===
May 18, 22:45:48  Info    IKE  initiate new phase 1 negotiation: 192.168.215.2[500]<=>192.168.215.234[500]
May 18, 22:45:48  Info    IKE  begin Identity Protection mode.
May 18, 22:45:48  Debug   IKE  new cookie:
May 18, 22:45:48  Debug   IKE  99a821b45212f14b
May 18, 22:45:48  Debug   IKE  add payload of len 48, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 13
May 18, 22:45:48  Debug   IKE  add payload of len 16, next type 0
May 18, 22:45:48  Debug   IKE  320 bytes from 192.168.215.2[500] to 192.168.215.234[500]
May 18, 22:45:48  Debug   IKE  sockname 192.168.215.2[500]
May 18, 22:45:48  Debug   IKE  send packet from 192.168.215.2[500]
May 18, 22:45:48  Debug   IKE  send packet to 192.168.215.234[500]
May 18, 22:45:48  Debug   IKE  1 times of 320 bytes message will be sent to 192.168.215.234[500]
May 18, 22:45:48  Debug   IKE  99a821b4 5212f14b 00000000 00000000 01100200 00000000 00000140 0d000034
May 18, 22:45:48  Debug   IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0e10
May 18, 22:45:48  Debug   IKE  80010005 80030001 80020002 80040002 0d000014 4a131c81 07035845 5c5728f2
May 18, 22:45:48  Debug   IKE  0e95452f 0d000014 8f8d8382 6d246b6f c7a8a6a4 28c11de8 0d000014 439b59f8
May 18, 22:45:48  Debug   IKE  ba676c4c 7737ae22 eab8f582 0d000014 4d1e0e13 6deafa34 c4f3ea9f 02ec7285
May 18, 22:45:48  Debug   IKE  0d000014 80d0bb3d ef54565e e84645d4 c85ce3ee 0d000014 9909b64e ed937c65
May 18, 22:45:48  Debug   IKE  73de52ac e952fa6b 0d000014 7d9419a6 5310ca6f 2c179d92 15529d56 0d000014
May 18, 22:45:48  Debug   IKE  cd604643 35df21f8 7cfdb2fc 68b6a448 0d000014 90cb8091 3ebb696e 086381b5
May 18, 22:45:48  Debug   IKE  ec427b1f 0d000014 16f6ca16 e4a4066d 83821a0f 0aeaa862 0d000014 4485152d
May 18, 22:45:48  Debug   IKE  18b6bbcd 0be8a846 9579ddcc 00000014 afcad713 68a1f1c9 6b8696fc 77570100
May 18, 22:45:48  Debug   IKE  resend phase1 packet 99a821b45212f14b:0000000000000000
May 18, 22:45:48  Debug   IKE  ===
May 18, 22:45:48  Debug   IKE  80 bytes message received from 192.168.215.234[500] to 192.168.215.2[500]
May 18, 22:45:48  Debug   IKE  99a821b4 5212f14b b858253f 5665bc74 01100200 00000000 00000050 00000034
May 18, 22:45:48  Debug   IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0e10
May 18, 22:45:48  Debug   IKE  80010005 80030001 80020002 80040002
May 18, 22:45:48  Debug   IKE  begin.
May 18, 22:45:48  Debug   IKE  seen nptype=1(sa)
May 18, 22:45:48  Debug   IKE  succeed.
May 18, 22:45:48  Debug   IKE  total SA len=48
```

```
May 18, 22:45:48  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0e10
May 18, 22:45:48  Debug    IKE  80010005 80030001 80020002 80040002
May 18, 22:45:48  Debug    IKE  begin.
May 18, 22:45:48  Debug    IKE  seen nptype=2(prop)
May 18, 22:45:48  Debug    IKE  succeed.
May 18, 22:45:48  Debug    IKE  proposal #1 len=40
May 18, 22:45:48  Debug    IKE  begin.
May 18, 22:45:48  Debug    IKE  seen nptype=3(trns)
May 18, 22:45:48  Debug    IKE  succeed.
May 18, 22:45:48  Debug    IKE  transform #1 len=32
May 18, 22:45:48  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 18, 22:45:48  Debug    IKE  type=Life Duration, flag=0x8000, lorv=3600
May 18, 22:45:48  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 18, 22:45:48  Debug    IKE  encryption(3des)
May 18, 22:45:48  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 18, 22:45:48  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 18, 22:45:48  Debug    IKE  hash(sha1)
May 18, 22:45:48  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
May 18, 22:45:48  Debug    IKE  hmac(modp1024)
May 18, 22:45:48  Debug    IKE  pair 1:
May 18, 22:45:48  Debug    IKE  0x3093a0: next=0x0 tnext=0x0
May 18, 22:45:48  Debug    IKE  proposal #1: 1 transform
May 18, 22:45:48  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
May 18, 22:45:48  Debug    IKE  trns#=1, trns-id=IKE
May 18, 22:45:48  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 18, 22:45:48  Debug    IKE  type=Life Duration, flag=0x8000, lorv=3600
May 18, 22:45:48  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 18, 22:45:48  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 18, 22:45:48  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 18, 22:45:48  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
May 18, 22:45:48  Debug    IKE  Compared: DB:Peer
May 18, 22:45:48  Debug    IKE  (lifetime = 3600:3600)
May 18, 22:45:48  Debug    IKE  (lifebyte = 0:0)
May 18, 22:45:48  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
May 18, 22:45:48  Debug    IKE  (encklen = 0:0)
May 18, 22:45:48  Debug    IKE  hashtype = SHA:SHA
May 18, 22:45:48  Debug    IKE  authmethod = pre-shared key:pre-shared key
May 18, 22:45:48  Debug    IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
May 18, 22:45:48  Debug    IKE  an acceptable proposal found.
May 18, 22:45:48  Debug    IKE  hmac(modp1024)
May 18, 22:45:48  Debug    IKE  agreed on pre-shared key auth.
May 18, 22:45:48  Debug    IKE  ===
May 18, 22:45:48  Debug    IKE  compute DH's private.
May 18, 22:45:48  Debug    IKE  75bfe564 f69ef5d6 f60624ae d1cfa0d4 5ed281c4 1b070eb2 330d27f1 3d410093
May 18, 22:45:48  Debug    IKE  76ea9438 264db82d af728fee 52703639 541b8a48 aad37b45 fdc5e1a6 28194c38
May 18, 22:45:48  Debug    IKE  295be993 f375f6d5 e21031d0 95bf1652 753b17f1 4506a425 07845733 8fe3c65c
May 18, 22:45:48  Debug    IKE  593dd3bc ee473763 19727fce b96c64f1 69d87987 89a6c17a 1d5dab6e 58364484
May 18, 22:45:48  Debug    IKE  compute DH's public.
May 18, 22:45:48  Debug    IKE  0759d828 9ba129a3 5af46160 882d70c8 9ae9b19d 574392b0 f49db999 cfa8c0d5
May 18, 22:45:48  Debug    IKE  83a34273 d55958c7 1218d9fb 8c216483 8a9afbd4 b6c0f918 619130af e487b49a
May 18, 22:45:48  Debug    IKE  91f63409 4b3ecc74 36caf5cb 55d61961 39020b9b c60d6a79 ea6c13fa 6cbf6273
May 18, 22:45:48  Debug    IKE  9d354a21 2521b01c be3583a3 204ea8fa bddeba6f c231508b 3dd11f20 0f2714e2
May 18, 22:45:48  Debug    IKE  add payload of len 128, next type 10
May 18, 22:45:48  Debug    IKE  add payload of len 16, next type 0
May 18, 22:45:48  Debug    IKE  180 bytes from 192.168.215.2[500] to 192.168.215.234[500]
May 18, 22:45:48  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:45:48  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:45:48  Debug    IKE  send packet to 192.168.215.234[500]
May 18, 22:45:48  Debug    IKE  1 times of 180 bytes message will be sent to 192.168.215.234[500]
May 18, 22:45:48  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 04100200 00000000 000000b4 0a000084
May 18, 22:45:48  Debug    IKE  0759d828 9ba129a3 5af46160 882d70c8 9ae9b19d 574392b0 f49db999 cfa8c0d5
May 18, 22:45:48  Debug    IKE  83a34273 d55958c7 1218d9fb 8c216483 8a9afbd4 b6c0f918 619130af e487b49a
May 18, 22:45:48  Debug    IKE  91f63409 4b3ecc74 36caf5cb 55d61961 39020b9b c60d6a79 ea6c13fa 6cbf6273
May 18, 22:45:48  Debug    IKE  9d354a21 2521b01c be3583a3 204ea8fa bddeba6f c231508b 3dd11f20 0f2714e2
May 18, 22:45:48  Debug    IKE  00000014 a0384a8f 94c4e716 e2dbba57 aa1639e3
May 18, 22:45:48  Debug    IKE  resend phase1 packet 99a821b45212f14b:b858253f5665bc74
May 18, 22:45:49  Debug    IKE  ===
May 18, 22:45:49  Debug    IKE  180 bytes message received from 192.168.215.234[500] to 192.168.215.2[500]
May 18, 22:45:49  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 04100200 00000000 000000b4 0a000084
May 18, 22:45:49  Debug    IKE  d0f509a6 2d62fe18 fc145ffa 4e3e7f6f 5c7cddc5 e76f6690 f4f1ae31 b421465b
May 18, 22:45:49  Debug    IKE  40fd5a86 b9604036 95930cf5 a6da77af e64c92aa b8394744 c1bda345 c1879bec
May 18, 22:45:49  Debug    IKE  79a52ed7 32f49627 4ca08f88 bdefad6a 52819d42 a670fff7 01dd5a4d 85068ccf
May 18, 22:45:49  Debug    IKE  a0d5a98f 72283041 27348e06 0f04bc29 9581640d 634d9fc0 aeb8106d 4260cb4e
May 18, 22:45:49  Debug    IKE  00000014 bb5dae57 abd56ab5 5aad562b 954a2512
```

```
May 18, 22:45:49  Debug    IKE  begin.
May 18, 22:45:49  Debug    IKE  seen nptype=4(ke)
May 18, 22:45:49  Debug    IKE  seen nptype=10(nonce)
May 18, 22:45:49  Debug    IKE  succeed.
May 18, 22:45:49  Debug    IKE  ===
May 18, 22:45:49  Debug    IKE  compute DH's shared.
May 18, 22:45:49  Debug    IKE  692427d9 74af73a3 cd2e1b71 2982c768 886b05b4 1eb11fd8 faaf0e57 f36e3e80
May 18, 22:45:49  Debug    IKE  4237a7ac 134e46d1 b1396ca1 f7af4268 fef55abf 2511cfe2 7572c07a 18e8f08f
May 18, 22:45:49  Debug    IKE  f536b277 8074b129 f99f181e 5e1b8b9f 94f308a3 f359503a 064f7601 bf893f0c
May 18, 22:45:49  Debug    IKE  3bef33c6 00daca36 d6cf021f d6af2fc4 263a5f44 bd28b874 efe8433c 29bfd22d
May 18, 22:45:49  Debug    IKE  the psk found.
May 18, 22:45:49  Debug    IKE  psk: 2007-05-18 22:45:49: DEBUG2:
May 18, 22:45:49  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
May 18, 22:45:49  Debug    IKE  nonce 1: 2007-05-18 22:45:49: DEBUG:
May 18, 22:45:49  Debug    IKE  a0384a8f 94c4e716 e2dbba57 aa1639e3
May 18, 22:45:49  Debug    IKE  nonce 2: 2007-05-18 22:45:49: DEBUG:
May 18, 22:45:49  Debug    IKE  bb5dae57 abd56ab5 5aad562b 954a2512
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  SKEYID computed:
May 18, 22:45:49  Debug    IKE  22274329 26dc04b5 e5269031 3d98e585 5fa26e7d
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  SKEYID_d computed:
May 18, 22:45:49  Debug    IKE  5b301722 8df05107 7ee83052 4f89cc3e 889fe1fd
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  SKEYID_a computed:
May 18, 22:45:49  Debug    IKE  c53aff44 e80c5974 20b39554 187d0a2a 40f2bc81
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  SKEYID_e computed:
May 18, 22:45:49  Debug    IKE  8d54e47e 5ba76b88 ff277cd3 f87d4b32 9d83fc70
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  hash(sha1)
May 18, 22:45:49  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  compute intermediate encryption key K1
May 18, 22:45:49  Debug    IKE  00
May 18, 22:45:49  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  compute intermediate encryption key K2
May 18, 22:45:49  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59
May 18, 22:45:49  Debug    IKE  90b6af3b 08bb4acf 888623ba 10be7972 fe62df66
May 18, 22:45:49  Debug    IKE  final encryption key computed:
May 18, 22:45:49  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:49  Debug    IKE  hash(sha1)
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  IV computed:
May 18, 22:45:49  Debug    IKE  7e75778f 0e973d55
May 18, 22:45:49  Debug    IKE  use ID type of IPv4_address
May 18, 22:45:49  Debug    IKE  HASH with:
May 18, 22:45:49  Debug    IKE  0759d828 9ba129a3 5af46160 882d70c8 9ae9b19d 574392b0 f49db999 cfa8c0d5
May 18, 22:45:49  Debug    IKE  83a34273 d55958c7 1218d9fb 8c216483 8a9afbd4 b6c0f918 619130af e487b49a
May 18, 22:45:49  Debug    IKE  91f63409 4b3ecc74 36caf5cb 55d61961 39020b9b c60d6a79 ea6c13fa 6cbf6273
May 18, 22:45:49  Debug    IKE  9d354a21 2521b01c be3583a3 204ea8fa bddeba6f c231508b 3dd11f20 0f2714e2
May 18, 22:45:49  Debug    IKE  d0f509a6 2d62fe18 fc145ffa 4e3e7f6f 5c7cddc5 e76f6690 f4f1ae31 b421465b
May 18, 22:45:49  Debug    IKE  40fd5a86 b9604036 95930cf5 a6da77af e64c92aa b8394744 c1bda345 c1879bec
May 18, 22:45:49  Debug    IKE  79a52ed7 32f49627 4ca08f88 bdefad6a 52819d42 a670fff7 01dd5a4d 85068ccf
May 18, 22:45:49  Debug    IKE  a0d5a98f 72283041 27348e06 0f04bc29 9581640d 634d9fc0 aeb8106d 4260cb4e
May 18, 22:45:49  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 00000001 00000001 00000028 01010001
May 18, 22:45:49  Debug    IKE  00000020 01010000 800b0001 800c0e10 80010005 80030001 80020002 80040002
May 18, 22:45:49  Debug    IKE  011101f4 c0a8d702
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  HASH (init) computed:
May 18, 22:45:49  Debug    IKE  878080de 5e7268e2 c1fafd35 c736b8d5 6c2c920c
May 18, 22:45:49  Debug    IKE  add payload of len 8, next type 8
May 18, 22:45:49  Debug    IKE  add payload of len 20, next type 0
May 18, 22:45:49  Debug    IKE  begin encryption.
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  pad length = 4
May 18, 22:45:49  Debug    IKE  0800000c 011101f4 c0a8d702 00000018 878080de 5e7268e2 c1fafd35 c736b8d5
May 18, 22:45:49  Debug    IKE  6c2c920c 00000004
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  with key:
May 18, 22:45:49  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:49  Debug    IKE  encrypted payload by IV:
May 18, 22:45:49  Debug    IKE  7e75778f 0e973d55
```

```
May 18, 22:45:49  Debug    IKE  save IV for next:
May 18, 22:45:49  Debug    IKE  10c6d60d 429d2a56
May 18, 22:45:49  Debug    IKE  encrypted.
May 18, 22:45:49  Debug    IKE  68 bytes from 192.168.215.2[500] to 192.168.215.234[500]
May 18, 22:45:49  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:45:49  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:45:49  Debug    IKE  send packet to 192.168.215.234[500]
May 18, 22:45:49  Debug    IKE  1 times of 68 bytes message will be sent to 192.168.215.234[500]
May 18, 22:45:49  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 05100201 00000000 00000044 d761b37b
May 18, 22:45:49  Debug    IKE  3d18592a aea56851 a33a9423 03d98fe9 45d634cd 61072bcb 98db7fbb 10c6d60d
May 18, 22:45:49  Debug    IKE  429d2a56
May 18, 22:45:49  Debug    IKE  resend phase1 packet 99a821b45212f14b:b858253f5665bc74
May 18, 22:45:49  Debug    IKE  ===
May 18, 22:45:49  Debug    IKE  68 bytes message received from 192.168.215.234[500] to 192.168.215.2[500]
May 18, 22:45:49  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 05100201 00000000 00000044 c0185d0d
May 18, 22:45:49  Debug    IKE  e9710948 577bd3bd a496652c 93a3a7b1 a2251b35 3d247ca0 b3dc1a5b 77a5586a
May 18, 22:45:49  Debug    IKE  3843ba91
May 18, 22:45:49  Debug    IKE  begin decryption.
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  IV was saved for next processing:
May 18, 22:45:49  Debug    IKE  77a5586a 3843ba91
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  with key:
May 18, 22:45:49  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:49  Debug    IKE  decrypted payload by IV:
May 18, 22:45:49  Debug    IKE  10c6d60d 429d2a56
May 18, 22:45:49  Debug    IKE  decrypted payload, but not trimed.
May 18, 22:45:49  Debug    IKE  0800000c 01000000 c0a8d7ea 00000018 2dd945ba 2b1af931 030e2103 27a5c2fc
May 18, 22:45:49  Debug    IKE  431dc16c 00000000
May 18, 22:45:49  Debug    IKE  padding len=0
May 18, 22:45:49  Debug    IKE  skip to trim padding.
May 18, 22:45:49  Debug    IKE  decrypted.
May 18, 22:45:49  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 05100201 00000000 00000044 0800000c
May 18, 22:45:49  Debug    IKE  01000000 c0a8d7ea 00000018 2dd945ba 2b1af931 030e2103 27a5c2fc 431dc16c
May 18, 22:45:49  Debug    IKE  00000000
May 18, 22:45:49  Debug    IKE  begin.
May 18, 22:45:49  Debug    IKE  seen nptype=5(id)
May 18, 22:45:49  Debug    IKE  seen nptype=8(hash)
May 18, 22:45:49  Debug    IKE  succeed.
May 18, 22:45:49  Debug    IKE  HASH received:
May 18, 22:45:49  Debug    IKE  2dd945ba 2b1af931 030e2103 27a5c2fc 431dc16c
May 18, 22:45:49  Debug    IKE  HASH with:
May 18, 22:45:49  Debug    IKE  d0f509a6 2d62fe18 fc145ffa 4e3e7f6f 5c7cddc5 e76f6690 f4f1ae31 b421465b
May 18, 22:45:49  Debug    IKE  40fd5a86 b9604036 95930cf5 a6da77af e64c92aa b8394744 c1bda345 c1879bec
May 18, 22:45:49  Debug    IKE  79a52ed7 32f49627 4ca08f88 bdefad6a 52819d42 a670fff7 01dd5a4d 85068ccf
May 18, 22:45:49  Debug    IKE  a0d5a98f 72283041 27348e06 0f04bc29 9581640d 634d9fc0 aeb8106d 4260cb4e
May 18, 22:45:49  Debug    IKE  0759d828 9ba129a3 5af46160 882d70c8 9ae9b19d 574392b0 f49db999 cfa8c0d5
May 18, 22:45:49  Debug    IKE  83a34273 d55958c7 1218d9fb 8c216483 8a9afbd4 b6c0f918 619130af e487b49a
May 18, 22:45:49  Debug    IKE  91f63409 4b3ecc74 36caf5cb 55d61961 39020b9b c60d6a79 ea6c13fa 6cbf6273
May 18, 22:45:49  Debug    IKE  9d354a21 2521b01c be3583a3 204ea8fa bddeba6f c231508b 3dd11f20 0f2714e2
May 18, 22:45:49  Debug    IKE  b858253f 5665bc74 99a821b4 5212f14b 00000001 00000001 00000028 01010001
May 18, 22:45:49  Debug    IKE  00000020 01010000 800b0001 800c0e10 80010005 80030001 80020002 80040002
May 18, 22:45:49  Debug    IKE  01000000 c0a8d7ea
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  HASH (init) computed:
May 18, 22:45:49  Debug    IKE  2dd945ba 2b1af931 030e2103 27a5c2fc 431dc16c
May 18, 22:45:49  Debug    IKE  HASH for PSK validated.
May 18, 22:45:49  Debug    IKE  peer's ID:2007-05-18 22:45:49: DEBUG:
May 18, 22:45:49  Debug    IKE  01000000 c0a8d7ea
May 18, 22:45:49  Debug    IKE  ===
May 18, 22:45:49  Debug    IKE  compute IV for phase2
May 18, 22:45:49  Debug    IKE  phase1 last IV:
May 18, 22:45:49  Debug    IKE  77a5586a 3843ba91 9dc894b8
May 18, 22:45:49  Debug    IKE  hash(sha1)
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  phase2 IV computed:
May 18, 22:45:49  Debug    IKE  2289f398 bec3e48f
May 18, 22:45:49  Debug    IKE  HASH with:
May 18, 22:45:49  Debug    IKE  9dc894b8 0000001c 00000001 01106002 99a821b4 5212f14b b858253f 5665bc74
May 18, 22:45:49  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:49  Debug    IKE  HASH computed:
May 18, 22:45:49  Debug    IKE  6ba1c342 7fbc6082 160f7c16 f59c324b dc083709
May 18, 22:45:49  Debug    IKE  begin encryption.
May 18, 22:45:49  Debug    IKE  encryption(3des)
```

```
May 18, 22:45:49  Debug    IKE  pad length = 4
May 18, 22:45:49  Debug    IKE  0b000018 6ba1c342 7fbc6082 160f7c16 f59c324b dc083709 0000001c 00000001
May 18, 22:45:49  Debug    IKE  01106002 99a821b4 5212f14b b858253f 5665bc74 00000004
May 18, 22:45:49  Debug    IKE  encryption(3des)
May 18, 22:45:49  Debug    IKE  with key:
May 18, 22:45:49  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:49  Debug    IKE  encrypted payload by IV:
May 18, 22:45:49  Debug    IKE  2289f398 bec3e48f
May 18, 22:45:49  Debug    IKE  save IV for next:
May 18, 22:45:49  Debug    IKE  614e2930 e4a1f4b6
May 18, 22:45:49  Debug    IKE  encrypted.
May 18, 22:45:49  Debug    IKE  84 bytes from 192.168.215.2[500] to 192.168.215.234[500]
May 18, 22:45:49  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:45:49  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:45:49  Debug    IKE  send packet to 192.168.215.234[500]
May 18, 22:45:49  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.234[500]
May 18, 22:45:49  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 08100501 9dc894b8 00000054 8ce4122e
May 18, 22:45:49  Debug    IKE  57e888f8 5a5a925a 4f1354c7 fbc7852f f1cbfc97 40857b63 15fe1344 dc7117b5
May 18, 22:45:49  Debug    IKE  bd0ed916 40299e17 ea1233e1 614e2930 e4a1f4b6
May 18, 22:45:49  Debug    IKE  sendto Information notify.
May 18, 22:45:49  Debug    IKE  IV freed
May 18, 22:45:49  Info     IKE  ISAKMP-SA established 192.168.215.2[500]-192.168.215.234[500] spi:
99a821b45212f14b:b858253f5665bc74
May 18, 22:45:49  Debug    IKE  ===
May 18, 22:45:49  Debug    IKE  msg 16 not interesting
May 18, 22:45:49  Debug    IKE  msg 16 not interesting
May 18, 22:45:49  Debug    IKE  msg 16 not interesting
May 18, 22:45:49  Debug    IKE  msg 15 not interesting
May 18, 22:45:49  Debug    IKE  msg 15 not interesting
May 18, 22:45:49  Debug    IKE  msg 15 not interesting
May 18, 22:45:50  Debug    IKE  ===
May 18, 22:45:50  Debug    IKE  begin QUICK mode.
May 18, 22:45:50  Info     IKE  initiate new phase 2 negotiation: 192.168.215.2[500]<=>192.168.215.234[500]
May 18, 22:45:50  Debug    IKE  compute IV for phase2
May 18, 22:45:50  Debug    IKE  phase1 last IV:
May 18, 22:45:50  Debug    IKE  77a5586a 3843ba91 ac905169
May 18, 22:45:50  Debug    IKE  hash(sha1)
May 18, 22:45:50  Debug    IKE  encryption(3des)
May 18, 22:45:50  Debug    IKE  phase2 IV computed:
May 18, 22:45:50  Debug    IKE  1418718e 88cdf130
May 18, 22:45:50  Debug    IKE  call pfkey_send_getspi
May 18, 22:45:50  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.234[0]->192.168.215.2[0]
May 18, 22:45:50  Debug    IKE  pfkey getspi sent.
May 18, 22:45:50  Debug    IKE  get pfkey GETSPI message
May 18, 22:45:50  Debug    IKE  02010003 0a000000 d3010000 d5180000 02000100 0ffcaffc 7f31ed44 205b0525
May 18, 22:45:50  Debug    IKE  03000500 ff200000 10020000 c0a8d7ea 00000000 00000000 03000600 ff200000
May 18, 22:45:50  Debug    IKE  10020000 c0a8d702 00000000 00000000
May 18, 22:45:50  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.234[0]->192.168.215.2[0]
spi=268218364(0xffcaffc)
May 18, 22:45:50  Debug    IKE  hmac(modp1024)
May 18, 22:45:50  Debug    IKE  hmac(modp1024)
May 18, 22:45:50  Debug    IKE  hmac(modp1024)
May 18, 22:45:50  Debug    IKE  hmac(modp1024)
May 18, 22:45:50  Debug    IKE  hmac(modp1024)
May 18, 22:45:50  Debug    IKE  compute DH's private.
May 18, 22:45:50  Debug    IKE  4a634f16 4f07ac0d eed0b34e 473fe1e9 74b8c126 da5ae355 f93bce76 2ca743a7
May 18, 22:45:50  Debug    IKE  be7b9476 5eaaf8fe edb418b7 ae386dab e170a170 86478947 b7843a98 261dda53
May 18, 22:45:50  Debug    IKE  8884556d 03e5363f 463d8bd6 f9ae0bf1 381e867e da6156d5 a3988bfe 51e8bfde
May 18, 22:45:50  Debug    IKE  14090702 ce280736 8fc8f945 ea503f1f 76b3c979 06bd4ff0 0883391d b29ec65a
May 18, 22:45:50  Debug    IKE  compute DH's public.
May 18, 22:45:50  Debug    IKE  bac9f5c3 be90855c ae0d78f1 e3dee7e0 b9a004bd c8136180 1e38432c 427e67d5
May 18, 22:45:50  Debug    IKE  6a9640bd 3f609701 b58bef01 7a71c074 01072c6c a73764ba b8583ac5 950be377
May 18, 22:45:50  Debug    IKE  8675eb04 172fcf67 54a100e5 457ffba6 6acb344c 58958ef6 d7cf30ca c0819973
May 18, 22:45:50  Debug    IKE  16532791 62b942d2 9f7ce31d 9c4bcb0b fd69578b 45cfc310 064ceebd 79ceba2b
May 18, 22:45:50  Debug    IKE  use local ID type IPv4_address
May 18, 22:45:50  Debug    IKE  use remote ID type IPv4_subnet
May 18, 22:45:50  Debug    IKE  IDci:
May 18, 22:45:50  Debug    IKE  01000000 14010101
May 18, 22:45:50  Debug    IKE  IDcr:
May 18, 22:45:50  Debug    IKE  04000000 0a000b00 ffffff00
May 18, 22:45:50  Debug    IKE  add payload of len 76, next type 10
May 18, 22:45:50  Debug    IKE  add payload of len 16, next type 4
May 18, 22:45:50  Debug    IKE  add payload of len 128, next type 5
May 18, 22:45:50  Debug    IKE  add payload of len 8, next type 5
```

```
May 18, 22:45:50  Debug    IKE  add payload of len 12, next type 0
May 18, 22:45:50  Debug    IKE  HASH with:
May 18, 22:45:50  Debug    IKE  ac905169 0a000050 00000001 00000001 00000044 01030402 0ffcaffc 0300001c
May 18, 22:45:50  Debug    IKE  01030000 80010001 80020e10 80040001 80050001 80030002 0000001c 02030000
May 18, 22:45:50  Debug    IKE  80010001 80020e10 80040001 80050002 80030002 04000014 85a23695 590d33fb
May 18, 22:45:50  Debug    IKE  4344db30 cc116b7a 05000084 bac9f5c3 be90855c ae0d78f1 e3dee7e0 b9a004bd
May 18, 22:45:50  Debug    IKE  c8136180 1e38432c 427e67d5 6a9640bd 3f609701 b58bef01 7a71c074 01072c6c
May 18, 22:45:50  Debug    IKE  a73764ba b8583ac5 950be377 8675eb04 172fcf67 54a100e5 457ffba6 6acb344c
May 18, 22:45:50  Debug    IKE  58958ef6 d7cf30ca c0819973 16532791 62b942d2 9f7ce31d 9c4bcb0b fd69578b
May 18, 22:45:50  Debug    IKE  45cfc310 064ceebd 79ceba2b 0500000c 01000000 14010101 00000010 04000000
May 18, 22:45:50  Debug    IKE  0a000b00 ffffff00
May 18, 22:45:50  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:50  Debug    IKE  HASH computed:
May 18, 22:45:50  Debug    IKE  2f3bb51b b33e62d2 5586cc2f 4c99adee 9a9a8711
May 18, 22:45:50  Debug    IKE  add payload of len 20, next type 1
May 18, 22:45:50  Debug    IKE  begin encryption.
May 18, 22:45:50  Debug    IKE  encryption(3des)
May 18, 22:45:50  Debug    IKE  pad length = 4
May 18, 22:45:50  Debug    IKE  01000018 2f3bb51b b33e62d2 5586cc2f 4c99adee 9a9a8711 0a000050 00000001
May 18, 22:45:50  Debug    IKE  00000001 00000044 01030402 0ffcaffc 0300001c 01030000 80010001 80020e10
May 18, 22:45:50  Debug    IKE  80040001 80050001 80030002 0000001c 02030000 80010001 80020e10 80040001
May 18, 22:45:50  Debug    IKE  80050002 80030002 04000014 85a23695 590d33fb 4344db30 cc116b7a 05000084
May 18, 22:45:50  Debug    IKE  bac9f5c3 be90855c ae0d78f1 e3dee7e0 b9a004bd c8136180 1e38432c 427e67d5
May 18, 22:45:50  Debug    IKE  6a9640bd 3f609701 b58bef01 7a71c074 01072c6c a73764ba b8583ac5 950be377
May 18, 22:45:50  Debug    IKE  8675eb04 172fcf67 54a100e5 457ffba6 6acb344c 58958ef6 d7cf30ca c0819973
May 18, 22:45:50  Debug    IKE  16532791 62b942d2 9f7ce31d 9c4bcb0b fd69578b 45cfc310 064ceebd 79ceba2b
May 18, 22:45:50  Debug    IKE  0500000c 01000000 14010101 00000010 04000000 0a000b00 ffffff00 00000004
May 18, 22:45:50  Debug    IKE  encryption(3des)
May 18, 22:45:50  Debug    IKE  with key:
May 18, 22:45:50  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:50  Debug    IKE  encrypted payload by IV:
May 18, 22:45:50  Debug    IKE  1418718e 88cdf130
May 18, 22:45:50  Debug    IKE  save IV for next:
May 18, 22:45:50  Debug    IKE  08f1e1dd 9f72fde9
May 18, 22:45:50  Debug    IKE  encrypted.
May 18, 22:45:50  Debug    IKE  316 bytes from 192.168.215.2[500] to 192.168.215.234[500]
May 18, 22:45:50  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:45:50  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:45:50  Debug    IKE  send packet to 192.168.215.234[500]
May 18, 22:45:50  Debug    IKE  1 times of 316 bytes message will be sent to 192.168.215.234[500]
May 18, 22:45:50  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 08102001 ac905169 0000013c 30e7998b
May 18, 22:45:50  Debug    IKE  a7dc9579 eb875e02 36f55008 3f1948f5 61467eb3 a11fd9da 241ae149 c8993161
May 18, 22:45:50  Debug    IKE  56c2cbf3 2f5b6cbf e160efec 2d56ecb6 9e54e102 6fbfa651 6c3844a4 70d843fa
May 18, 22:45:50  Debug    IKE  2fdbe9b2 025a669e 1dbd06f6 ec73ee2f 6a10da3a 6dbcced0 56839f6d 611dc173
May 18, 22:45:50  Debug    IKE  13a3a167 dba411a1 1f7f8bce e3f447ac 7825d6a8 d2f5c0e7 44cbb596 cc5d9263
May 18, 22:45:50  Debug    IKE  73b1f210 017e2389 ce54cc41 88207ac3 b786d816 535c0e35 3b8893bc 22741e3c
May 18, 22:45:50  Debug    IKE  7a8ddd69 ab21ab5b 907df68a 3266d6ec 6a9b1c48 cbc35a56 025c4186 d56306d8
May 18, 22:45:50  Debug    IKE  a4ff53d7 c3c04952 78b08376 0bae74ba a94bf13c f0801e0f 0595b724 2c7a9995
May 18, 22:45:50  Debug    IKE  b3424d7c 9048bfe0 0484c7b7 4abcf37d f8bdc425 deac6c1e c8116024 bd017e4e
May 18, 22:45:50  Debug    IKE  de7c7669 40b0a997 88089b50 df8f7290 c560dd22 08f1e1dd 9f72fde9
May 18, 22:45:50  Debug    IKE  resend phase2 packet 99a821b45212f14b:b858253f5665bc74:0000ac90
May 18, 22:45:51  Debug    IKE  ===
May 18, 22:45:51  Debug    IKE  284 bytes message received from 192.168.215.234[500] to 192.168.215.2[500]
May 18, 22:45:51  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 08102001 ac905169 0000011c 56628f20
May 18, 22:45:51  Debug    IKE  3a3e6b26 2d7dc017 9a96b936 988a3dea a5078742 8a2d8703 bb683c1b e242378d
May 18, 22:45:51  Debug    IKE  c33c302f 95e25bbf 0c0e2ed7 3c44af78 880dcbe9 be89c929 c6912504 2698caf1
May 18, 22:45:51  Debug    IKE  9c6ea23d 57bece01 f5c076fe 88c473c9 9c722ee2 68cdbace a0c437b7 521dc1e9
May 18, 22:45:51  Debug    IKE  f0a51a78 7e3cb222 c238f5bc be0003af c88a80ce d31f1c06 d92d9033 05cb2518
May 18, 22:45:51  Debug    IKE  1ebd2926 6cada62b 997766f1 8bedfedb ce65af44 a597bd12 80c44059 d774990e
May 18, 22:45:51  Debug    IKE  cf2d6727 9cd85395 16cbc037 23d6ebbd 22f81f1b 5a309bad 85b5e762 1785ec25
May 18, 22:45:51  Debug    IKE  96940d9e 3994aa48 198acc39 9d13695c 8cf93777 27895e62 0a14e077 4de30b09
May 18, 22:45:51  Debug    IKE  93cbc953 d246b5f9 5ebb227a 5dd627f2 82f3b8e9 38cb24a5 3ab1da8a
May 18, 22:45:51  Debug    IKE  begin decryption.
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  IV was saved for next processing:
May 18, 22:45:51  Debug    IKE  38cb24a5 3ab1da8a
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  with key:
May 18, 22:45:51  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:51  Debug    IKE  decrypted payload by IV:
May 18, 22:45:51  Debug    IKE  08f1e1dd 9f72fde9
May 18, 22:45:51  Debug    IKE  decrypted payload, but not trimed.
May 18, 22:45:51  Debug    IKE  01000018 78e8c3d9 e0fc4a47 c0877984 d57b32aa a1ed326d 0a000034 00000001
May 18, 22:45:51  Debug    IKE  00000001 00000028 01030401 478e1d83 0000001c 01030000 80010001 80020e10
```

```
May 18, 22:45:51  Debug    IKE  80040001 80050001 80030002 04000014 22118844 2291c8e4 f2f97cbe dfef77bb
May 18, 22:45:51  Debug    IKE  05000084 97686bd3 aed65287 d5b2a908 6a02fd92 791a4de3 9b377844 25df3850
May 18, 22:45:51  Debug    IKE  b5cbf0d2 a82cc644 11601286 f9980c42 4e71843b 3c944948 625fefe4 9785ab69
May 18, 22:45:51  Debug    IKE  75cbc753 83cdca62 415dfca0 9d39fc7f 2baf1047 c05e3f93 59f2a343 119a2423
May 18, 22:45:51  Debug    IKE  6d884f0f d703afd4 29fcfa36 48d6f908 52c6e21d 76850063 124965bc 46800f94
May 18, 22:45:51  Debug    IKE  f5364267 0500000c 01000000 14010101 00000010 04000000 0a000b00 ffffff00
May 18, 22:45:51  Debug    IKE  padding len=0
May 18, 22:45:51  Debug    IKE  skip to trim padding.
May 18, 22:45:51  Debug    IKE  decrypted.
May 18, 22:45:51  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 08102001 ac905169 0000011c 01000018
May 18, 22:45:51  Debug    IKE  78e8c3d9 e0fc4a47 c0877984 d57b32aa a1ed326d 0a000034 00000001 00000001
May 18, 22:45:51  Debug    IKE  00000028 01030401 478e1d83 0000001c 01030000 80010001 80020e10 80040001
May 18, 22:45:51  Debug    IKE  80050001 80030002 04000014 22118844 2291c8e4 f2f97cbe dfef77bb 05000084
May 18, 22:45:51  Debug    IKE  97686bd3 aed65287 d5b2a908 6a02fd92 791a4de3 9b377844 25df3850 b5cbf0d2
May 18, 22:45:51  Debug    IKE  a82cc644 11601286 f9980c42 4e71843b 3c944948 625fefe4 9785ab69 75cbc753
May 18, 22:45:51  Debug    IKE  83cdca62 415dfca0 9d39fc7f 2baf1047 c05e3f93 59f2a343 119a2423 6d884f0f
May 18, 22:45:51  Debug    IKE  d703afd4 29fcfa36 48d6f908 52c6e21d 76850063 124965bc 46800f94 f5364267
May 18, 22:45:51  Debug    IKE  0500000c 01000000 14010101 00000010 04000000 0a000b00 ffffff00
May 18, 22:45:51  Debug    IKE  begin.
May 18, 22:45:51  Debug    IKE  seen nptype=8(hash)
May 18, 22:45:51  Debug    IKE  seen nptype=1(sa)
May 18, 22:45:51  Debug    IKE  seen nptype=10(nonce)
May 18, 22:45:51  Debug    IKE  seen nptype=4(ke)
May 18, 22:45:51  Debug    IKE  seen nptype=5(id)
May 18, 22:45:51  Debug    IKE  seen nptype=5(id)
May 18, 22:45:51  Debug    IKE  succeed.
May 18, 22:45:51  Debug    IKE  HASH allocated:hbuf->l=272 actual:tlen=248
May 18, 22:45:51  Debug    IKE  HASH(2) received:2007-05-18 22:45:51: DEBUG:
May 18, 22:45:51  Debug    IKE  78e8c3d9 e0fc4a47 c0877984 d57b32aa a1ed326d
May 18, 22:45:51  Debug    IKE  HASH with:
May 18, 22:45:51  Debug    IKE  ac905169 85a23695 590d33fb 4344db30 cc116b7a 0a000034 00000001 00000001
May 18, 22:45:51  Debug    IKE  00000028 01030401 478e1d83 0000001c 01030000 80010001 80020e10 80040001
May 18, 22:45:51  Debug    IKE  80050001 80030002 04000014 22118844 2291c8e4 f2f97cbe dfef77bb 05000084
May 18, 22:45:51  Debug    IKE  97686bd3 aed65287 d5b2a908 6a02fd92 791a4de3 9b377844 25df3850 b5cbf0d2
May 18, 22:45:51  Debug    IKE  a82cc644 11601286 f9980c42 4e71843b 3c944948 625fefe4 9785ab69 75cbc753
May 18, 22:45:51  Debug    IKE  83cdca62 415dfca0 9d39fc7f 2baf1047 c05e3f93 59f2a343 119a2423 6d884f0f
May 18, 22:45:51  Debug    IKE  d703afd4 29fcfa36 48d6f908 52c6e21d 76850063 124965bc 46800f94 f5364267
May 18, 22:45:51  Debug    IKE  0500000c 01000000 14010101 00000010 04000000 0a000b00 ffffff00
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  HASH computed:
May 18, 22:45:51  Debug    IKE  78e8c3d9 e0fc4a47 c0877984 d57b32aa a1ed326d
May 18, 22:45:51  Debug    IKE  total SA len=76
May 18, 22:45:51  Debug    IKE  00000001 00000001 00000044 01030402 0ffcaffc 0300001c 01030000 80010001
May 18, 22:45:51  Debug    IKE  80020e10 80040001 80050001 80030002 0000001c 02030000 80010001 80020e10
May 18, 22:45:51  Debug    IKE  80040001 80050002 80030002
May 18, 22:45:51  Debug    IKE  begin.
May 18, 22:45:51  Debug    IKE  seen nptype=2(prop)
May 18, 22:45:51  Debug    IKE  succeed.
May 18, 22:45:51  Debug    IKE  proposal #1 len=68
May 18, 22:45:51  Debug    IKE  begin.
May 18, 22:45:51  Debug    IKE  seen nptype=3(trns)
May 18, 22:45:51  Debug    IKE  seen nptype=3(trns)
May 18, 22:45:51  Debug    IKE  succeed.
May 18, 22:45:51  Debug    IKE  transform #1 len=28
May 18, 22:45:51  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:45:51  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
May 18, 22:45:51  Debug    IKE  life duration was in TLV.
May 18, 22:45:51  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:45:51  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-md5
May 18, 22:45:51  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 18, 22:45:51  Debug    IKE  hmac(modp1024)
May 18, 22:45:51  Debug    IKE  transform #2 len=28
May 18, 22:45:51  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:45:51  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
May 18, 22:45:51  Debug    IKE  life duration was in TLV.
May 18, 22:45:51  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:45:51  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 18, 22:45:51  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 18, 22:45:51  Debug    IKE  hmac(modp1024)
May 18, 22:45:51  Debug    IKE  pair 1:
May 18, 22:45:51  Debug    IKE  0x309fb0: next=0x0 tnext=0x309770
May 18, 22:45:51  Debug    IKE  0x309770: next=0x0 tnext=0x0
May 18, 22:45:51  Debug    IKE  proposal #1: 2 transform
May 18, 22:45:51  Debug    IKE  total SA len=48
```

```
May 18, 22:45:51  Debug    IKE  00000001 00000001 00000028 01030401 478e1d83 0000001c 01030000 80010001
May 18, 22:45:51  Debug    IKE  80020e10 80040001 80050001 80030002
May 18, 22:45:51  Debug    IKE  begin.
May 18, 22:45:51  Debug    IKE  seen nptype=2(prop)
May 18, 22:45:51  Debug    IKE  succeed.
May 18, 22:45:51  Debug    IKE  proposal #1 len=40
May 18, 22:45:51  Debug    IKE  begin.
May 18, 22:45:51  Debug    IKE  seen nptype=3(trns)
May 18, 22:45:51  Debug    IKE  succeed.
May 18, 22:45:51  Debug    IKE  transform #1 len=28
May 18, 22:45:51  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:45:51  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
May 18, 22:45:51  Debug    IKE  life duration was in TLV.
May 18, 22:45:51  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:45:51  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-md5
May 18, 22:45:51  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 18, 22:45:51  Debug    IKE  hmac(modp1024)
May 18, 22:45:51  Debug    IKE  pair 1:
May 18, 22:45:51  Debug    IKE  0x30a410: next=0x0 tnext=0x0
May 18, 22:45:51  Debug    IKE  proposal #1: 1 transform
May 18, 22:45:51  Debug    IKE  begin compare proposals.
May 18, 22:45:51  Debug    IKE  pair[1]: 0x30a410
May 18, 22:45:51  Debug    IKE  0x30a410: next=0x0 tnext=0x0
May 18, 22:45:51  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
May 18, 22:45:51  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:45:51  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=3600
May 18, 22:45:51  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:45:51  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-md5
May 18, 22:45:51  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
May 18, 22:45:51  Debug    IKE  peer's single bundle:
May 18, 22:45:51  Debug    IKE  (proto_id=ESP spisize=4 spi=478e1d83 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:45:51  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-md5)
May 18, 22:45:51  Debug    IKE  my single bundle:
May 18, 22:45:51  Debug    IKE  (proto_id=ESP spisize=4 spi=0ffcaffc spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:45:51  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-md5)
May 18, 22:45:51  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:45:51  Debug    IKE  matched
May 18, 22:45:51  Debug    IKE  ===
May 18, 22:45:51  Debug    IKE  HASH(3) generate
May 18, 22:45:51  Debug    IKE  HASH with:
May 18, 22:45:51  Debug    IKE  00ac9051 6985a236 95590d33 fb4344db 30cc116b 7a221188 442291c8 e4f2f97c
May 18, 22:45:51  Debug    IKE  bedfef77 bb
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  HASH computed:
May 18, 22:45:51  Debug    IKE  0fe16387 a147d3fb 0a84d33a 5c4f67cd 903fa603
May 18, 22:45:51  Debug    IKE  add payload of len 20, next type 0
May 18, 22:45:51  Debug    IKE  begin encryption.
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  pad length = 8
May 18, 22:45:51  Debug    IKE  00000018 0fe16387 a147d3fb 0a84d33a 5c4f67cd 903fa603 00000000 00000008
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  with key:
May 18, 22:45:51  Debug    IKE  0b204d11 3a3ff2af 598583e9 c8ba97af aa998d59 90b6af3b
May 18, 22:45:51  Debug    IKE  encrypted payload by IV:
May 18, 22:45:51  Debug    IKE  38cb24a5 3ab1da8a
May 18, 22:45:51  Debug    IKE  save IV for next:
May 18, 22:45:51  Debug    IKE  57d5ef60 c7f9cf14
May 18, 22:45:51  Debug    IKE  encrypted.
May 18, 22:45:51  Debug    IKE  60 bytes from 192.168.215.2[500] to 192.168.215.234[500]
May 18, 22:45:51  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:45:51  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:45:51  Debug    IKE  send packet to 192.168.215.234[500]
May 18, 22:45:51  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.234[500]
May 18, 22:45:51  Debug    IKE  99a821b4 5212f14b b858253f 5665bc74 08102001 ac905169 0000003c ce4a3cc9
May 18, 22:45:51  Debug    IKE  fce8026a 2af61cc8 d068f2b1 ad706e3c 14b3f5ab 57d5ef60 c7f9cf14
May 18, 22:45:51  Debug    IKE  compute DH's shared.
May 18, 22:45:51  Debug    IKE  c209058d 917ca075 4de2d595 2a6e2546 8bd01b77 5cbc0149 3451cf84 1de982ef
May 18, 22:45:51  Debug    IKE  5d351c7f 3b3e3d3d e964b74f a84c9647 fda1454a 5e8d249f 2918993a 1e5d67e8
May 18, 22:45:51  Debug    IKE  3088e9b2 89d68a9e 63194e9f 9e4baa4c 9fa4d09d 3a9c996d 09648b26 695bb27f
May 18, 22:45:51  Debug    IKE  710cebc1 ade9979e be80146a 2f3ae97a 5798e593 205737b1 9be4fee7 293d6310
May 18, 22:45:51  Debug    IKE  KEYMAT compute with
May 18, 22:45:51  Debug    IKE  c209058d 917ca075 4de2d595 2a6e2546 8bd01b77 5cbc0149 3451cf84 1de982ef
May 18, 22:45:51  Debug    IKE  5d351c7f 3b3e3d3d e964b74f a84c9647 fda1454a 5e8d249f 2918993a 1e5d67e8
May 18, 22:45:51  Debug    IKE  3088e9b2 89d68a9e 63194e9f 9e4baa4c 9fa4d09d 3a9c996d 09648b26 695bb27f
```

```
May 18, 22:45:51  Debug    IKE  710cebc1 ade9979e be80146a 2f3ae97a 5798e593 205737b1 9be4fee7 293d6310
May 18, 22:45:51  Debug    IKE  030ffcaf fc85a236 95590d33 fb4344db 30cc116b 7a221188 442291c8 e4f2f97c
May 18, 22:45:51  Debug    IKE  bedfef77 bb
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  hmac(hmac_md5)
May 18, 22:45:51  Debug    IKE  encklen=192 authklen=128
May 18, 22:45:51  Debug    IKE  generating 640 bits of key (dupkeymat=4)
May 18, 22:45:51  Debug    IKE  generating K1...K4 for KEYMAT.
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  621d07cb 96cfea2f b9711fa9 d6f3c583 fef0a923 13b60f55 75dfa90c a8c38641
May 18, 22:45:51  Debug    IKE  fbad69af ed88ecf8 1ed18b50 b11e292c f375668a 94e9cf00 36c719bc dfd8de43
May 18, 22:45:51  Debug    IKE  c93c187d 52294fa4 3a69b7f4 2ab629c1
May 18, 22:45:51  Debug    IKE  KEYMAT compute with
May 18, 22:45:51  Debug    IKE  c209058d 917ca075 4de2d595 2a6e2546 8bd01b77 5cbc0149 3451cf84 1de982ef
May 18, 22:45:51  Debug    IKE  5d351c7f 3b3e3d3d e964b74f a84c9647 fda1454a 5e8d249f 2918993a 1e5d67e8
May 18, 22:45:51  Debug    IKE  3088e9b2 89d68a9e 63194e9f 9e4baa4c 9fa4d09d 3a9c996d 09648b26 695bb27f
May 18, 22:45:51  Debug    IKE  710cebc1 ade9979e be80146a 2f3ae97a 5798e593 205737b1 9be4fee7 293d6310
May 18, 22:45:51  Debug    IKE  03478e1d 8385a236 95590d33 fb4344db 30cc116b 7a221188 442291c8 e4f2f97c
May 18, 22:45:51  Debug    IKE  bedfef77 bb
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  hmac(hmac_md5)
May 18, 22:45:51  Debug    IKE  encklen=192 authklen=128
May 18, 22:45:51  Debug    IKE  generating 640 bits of key (dupkeymat=4)
May 18, 22:45:51  Debug    IKE  generating K1...K4 for KEYMAT.
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  hmac(hmac_sha1)
May 18, 22:45:51  Debug    IKE  4d5c6288 6070443a feacef51 e38d0f30 d9ccea2f 01d05db5 56d16cac 3ce83081
May 18, 22:45:51  Debug    IKE  c26e8858 658ddfee df5b24b1 9f26fcb4 45b04d72 e88b1fa9 a601884d 2e0d74c2
May 18, 22:45:51  Debug    IKE  93a2fc1c 3b901df8 8befe963 17f30f33
May 18, 22:45:51  Debug    IKE  KEYMAT computed.
May 18, 22:45:51  Debug    IKE  call pk_sendupdate
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  hmac(hmac_md5)
May 18, 22:45:51  Debug    IKE  call pfkey_send_update_nat
May 18, 22:45:51  Debug    APP  Received SADB message type UPDATE, 192.168.215.234 [0] -> 192.168.215.2 [0]
May 18, 22:45:51  Debug    APP  SA change detected
May 18, 22:45:51  Debug    IKE  pfkey update sent.
May 18, 22:45:51  Debug    IKE  encryption(3des)
May 18, 22:45:51  Debug    IKE  hmac(hmac_md5)
May 18, 22:45:51  Debug    IKE  call pfkey_send_add_nat
May 18, 22:45:51  Debug    APP  Received SADB message type ADD, 192.168.215.2 [0] -> 192.168.215.234 [0]
May 18, 22:45:51  Debug    APP  SA change detected
May 18, 22:45:51  Debug    APP  Connection Vigor is up
May 18, 22:45:51  Debug    IKE  pfkey add sent.
May 18, 22:45:51  Debug    IKE  get pfkey UPDATE message
May 18, 22:45:51  Debug    IKE  02020003 14000000 d3010000 d5180000 02000100 0ffcaffc 04000102 00000000
May 18, 22:45:51  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d7ea
May 18, 22:45:51  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d702 00000000 00000000
May 18, 22:45:51  Debug    IKE  04000300 00000000 00000000 00000000 100e0000 00000000 00000000 00000000
May 18, 22:45:51  Debug    IKE  04000400 00000000 00000000 00000000 400b0000 00000000 00000000 00000000
May 18, 22:45:51  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.234[0]->192.168.215.2[0]
spi=268218364(0xffcaffc)
May 18, 22:45:51  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.234[0]->192.168.215.2[0]
spi=268218364(0xffcaffc)
May 18, 22:45:51  Debug    IKE  ===
May 18, 22:45:51  Debug    IKE  get pfkey ADD message
May 18, 22:45:51  Debug    IKE  02030003 14000000 d3010000 d5180000 02000100 478e1d83 04000102 00000000
May 18, 22:45:51  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d702
May 18, 22:45:51  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7ea 00000000 00000000
May 18, 22:45:51  Debug    IKE  04000300 00000000 00000000 00000000 100e0000 00000000 00000000 00000000
May 18, 22:45:51  Debug    IKE  04000400 00000000 00000000 00000000 400b0000 00000000 00000000 00000000
May 18, 22:45:51  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.2[0]->192.168.215.234[0]
spi=1200496003(0x478e1d83)
May 18, 22:45:51  Debug    IKE  ===
```