IPSecuritas 3.x

Configuration Instructions

for

D-Link DI-804HV

© 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.

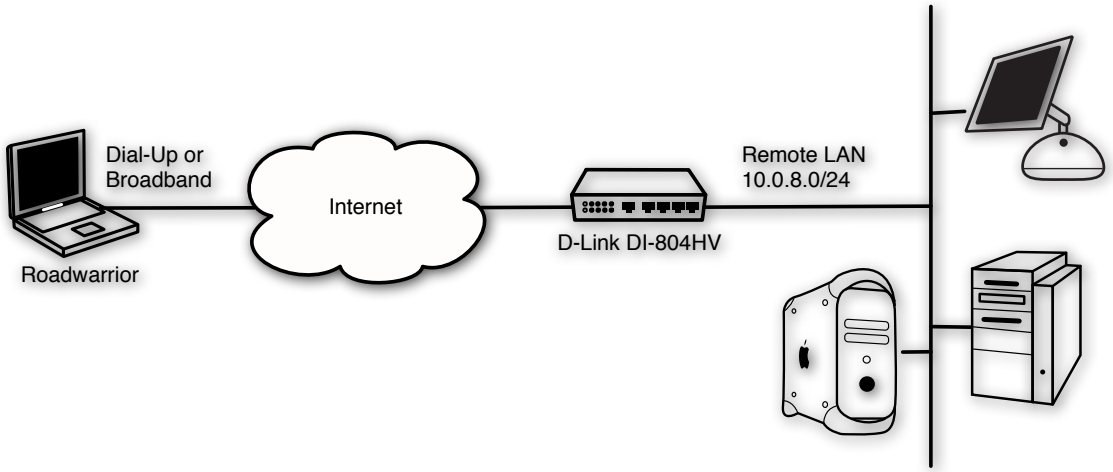
Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic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

Table of contents

Introduction

This document describes the steps necessary to establish a protected VPN connection between a Mac client and a D-Link DI-804HV router. All information in this document is based on the following assumed network.

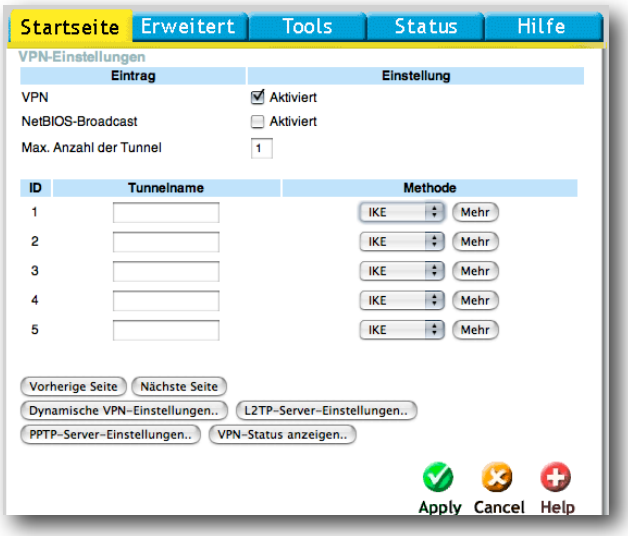


D-Link DI-804HV Setup

Login

Open a web browser and connect to your D-Link router. Enter the administrators user name and password. On the left side, click on **VPN.**

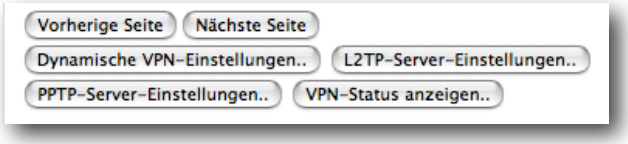
Enable VPN



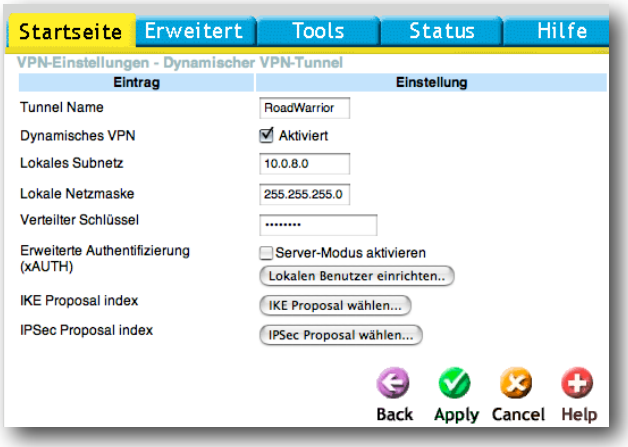
Enable VPN by ticking the checkbox **VPN**. Click on Apply. The router will restart and bring you back to the same page after a few seconds.
Increase the maximum number of tunnel if necessary (if there are more than one users accessing the local network through VPN).

IMPORTANT: it is crucial to apply the changed settings in each of the following steps before you continue, otherwise the settings will not be stored properly.

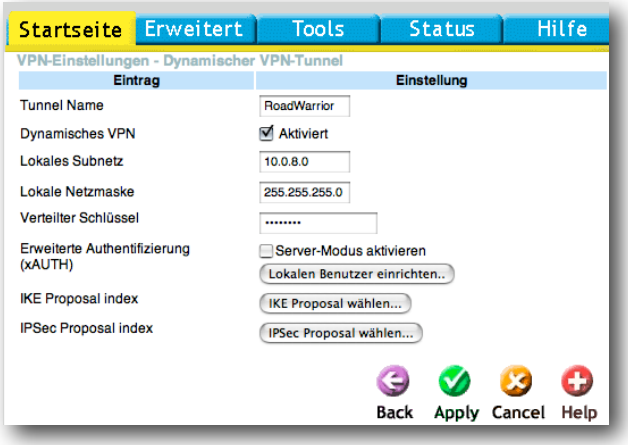
Enable Dynamic VPN



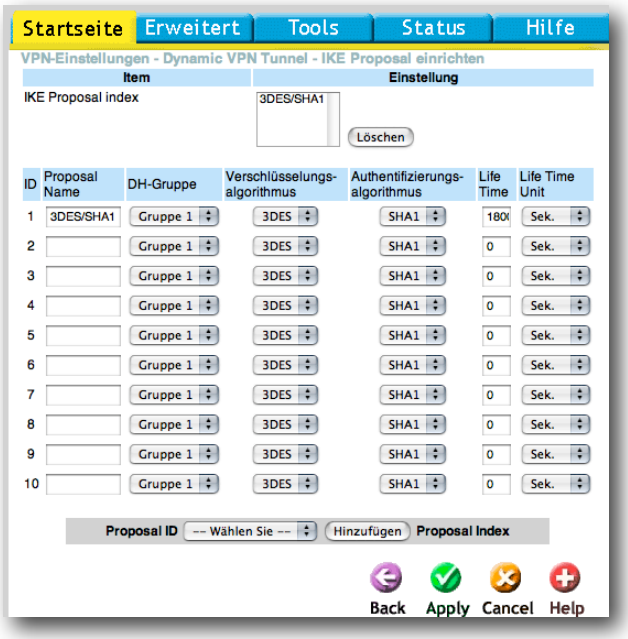
Click on **Dynamic VPN Settings** (the left buttom in the second row of buttons).



Enter an arbitrary name for the tunnel, activate dynamic VPN by ticking the checkbox .
Then enter the local subnet (and netmask) you like to access through the tunnel (this is usually identical to the local network range, although you might want to limit access to a smaller range for security reasons).
Then enter a secure preshared key. Please remember the key you enter since you'll need it again when setting up the tunnel in IPSecuritas.
Click on **Apply**.



Next, click on **Choose IKE Proposal**.

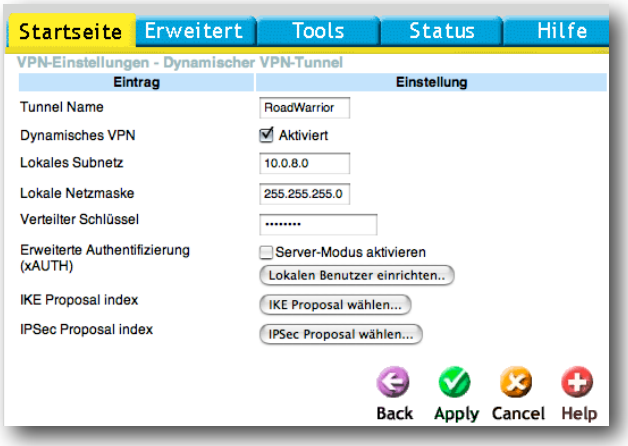


Set a name for the first unused proposal and set the parameters to the following:

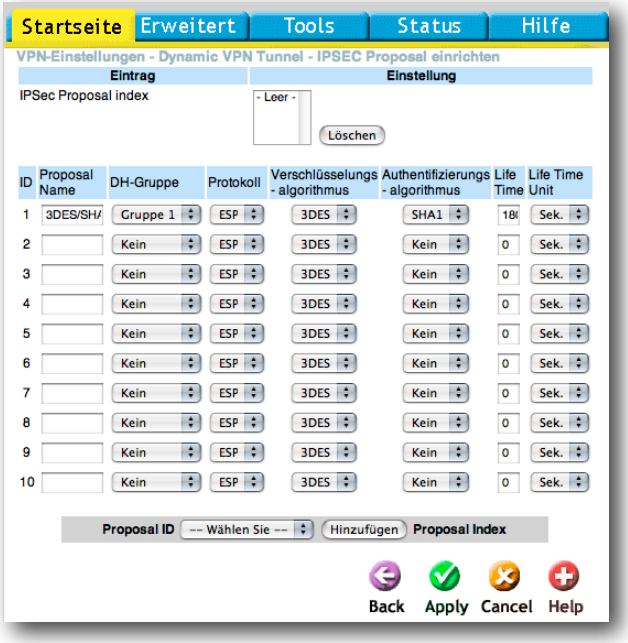
DH-Group: Group 1
Encryption Algorithm: 3DES
Authentication Algorithm: SHA1
Life Time: 1800 Seconds

Select the proposal ID that you just edited with the popup menu at the bottom and press the button labeled **Add**.

The click on **Apply**.



Next, click on **Choose IPSec Proposal**.



Set a name for the first unused proposal and set the parameters to the following:

DH-Group: Group 1
Encryption Algorithm: 3DES
Authentication Algorithm: SHA1
Life Time: 1800 Seconds

Select the proposal ID that you just edited with the popup menu at the bottom and press the button labeled **Add**.

Then click on **Apply**.

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

Click on **Next**.

Finish the Wizard

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

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

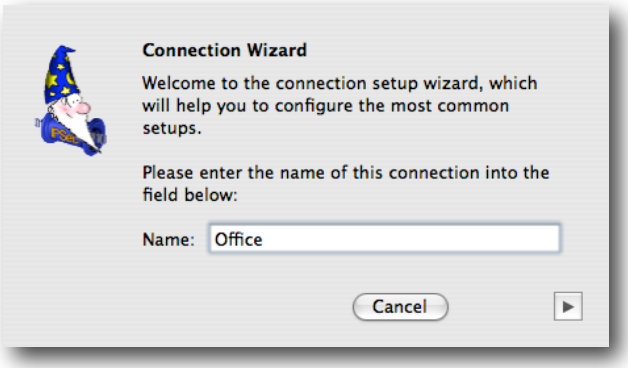
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the DI-804HV router.

Start Wizard

Start IPSecuritas unless already running. Go to the menu **Connections** 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 **D-Link** from the manufacturer list and DI-804HV from the model list.

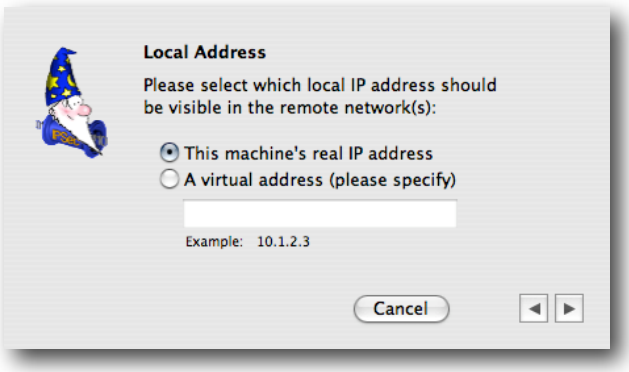
Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

Enter the public IP address or hostname of your D-Link 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.

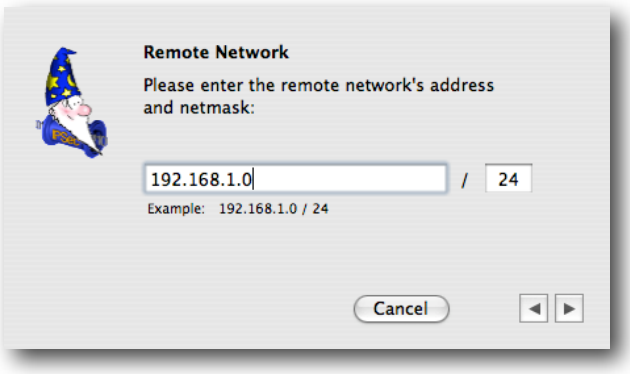
Enter a Virtual IP Address



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.

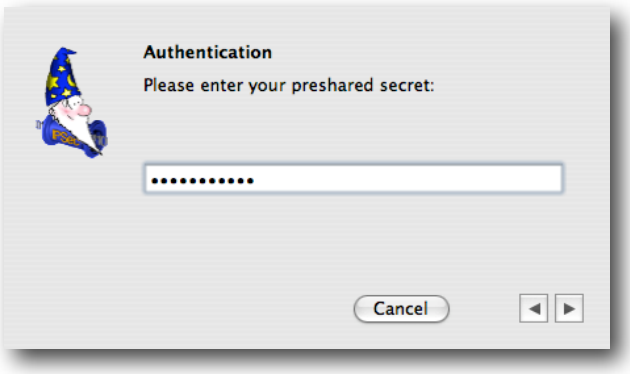
Enter Remote Network



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 D-Link router.

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

Enter Preshared Key



Enter the same **Preshared Key** that you used for the D-Link DI-804HV.

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 DI-804HV **local IP address**. If the tunnel works correctly, a similar output is displayed:

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

Sample DI-804HV Log Output

The following is a sample log file from the DI-804HV after a successful connection establishment:

```
Montag August 29, 2005 03:27:11 Receive IKE INFO : 192.168.215.3 --> 192.168.215.231
Montag August 29, 2005 03:27:11 Receive IKE (INFO) : delete 192.168.215.3 -> 192.168.215.231 phase 1
Montag August 29, 2005 03:27:11 Send IKE (INFO) : delete [10.1.8.0| 192.168.215.231]-->[192.168.215.3|192.168.215.3]
phase 2
Montag August 29, 2005 03:27:11 IKE phase2 (IPSec SA) remove : 10.1.8.0 <-> 192.168.215.3
Montag August 29, 2005 03:27:11 inbound SPI = 0x9c0e0010, outbound SPI = 0xf74b0b6
Montag August 29, 2005 03:27:11 Send IKE (INFO) : delete 192.168.215.231 -> 192.168.215.3 phase 1
Montag August 29, 2005 03:27:11 IKE phase1 (ISAKMP SA) remove : 192.168.215.231 <-> 192.168.215.3
Montag August 29, 2005 03:27:11 Receive IKE M1(INIT) : 192.168.215.3 --> 192.168.215.231
Montag August 29, 2005 03:27:11 Try to match with ENC:3DES AUTH:PSK HASH:SHA1 Group:Group1
```

```
Montag August 29, 2005 03:27:12 Send IKE M2(RESP) : 192.168.215.231 --> 192.168.215.3
Montag August 29, 2005 03:27:12 Receive IKE M3(KEYINIT) : 192.168.215.3 --> 192.168.215.231
Montag August 29, 2005 03:27:12 Send IKE M4(KEYRESP) : 192.168.215.231 --> 192.168.215.3
Montag August 29, 2005 03:27:12 Receive IKE M5(IDINIT) : 192.168.215.3 --> 192.168.215.231
Montag August 29, 2005 03:27:12 Send IKE M6(IDRESP) : 192.168.215.231 --> 192.168.215.3
Montag August 29, 2005 03:27:12 IKE Phase1 (ISAKMP SA) established : 192.168.215.231 <-> 192.168.215.3
Montag August 29, 2005 03:27:12 Receive IKE INFO : 192.168.215.3 --> 192.168.215.231
Montag August 29, 2005 03:27:12 Receive IKE Q1(QINIT) : [192.168.215.3]-->[192.168.215.231]
Montag August 29, 2005 03:27:12 SPD : add dynamic user [10.1.8.0]<->[192.168.215.3] OK
Montag August 29, 2005 03:27:12 Requested routing is [192.168.215.3|192.168.215.3]<->[192.168.215.231|10.1.8.0]
Montag August 29, 2005 03:27:12 Try to match ESP with MODE:Tunnel PROTOCAL:ESP-3DES AUTH:SHA1 HASH:Others
PFS(Group):Group1
Montag August 29, 2005 03:27:12 Try to match ESP with MODE:Tunnel PROTOCAL:ESP-3DES AUTH:SHA1 HASH:Others
PFS(Group):Group1
Montag August 29, 2005 03:27:13 Send IKE Q2(QRESP) : 10.1.8.0 --> 192.168.215.3
Montag August 29, 2005 03:27:13 Receive IKE Q3(QHASH) : [192.168.215.3| 192.168.215.3]-->[192.168.215.231|10.1.8.0]
Montag August 29, 2005 03:27:13 IKE Phase2 (IPSEC SA) established : [192.168.215.3|192.168.215.3]<->[192.168.215.231|
10.1.8.0]
Montag August 29, 2005 03:27:13 inbound SPI = 0xa10e0010, outbound SPI = 0x4fc0e5
```

Sample IPSecuritas Log Output

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

```
IPSecuritas 3.0prc3 build 1521, Tue Apr 24 21:14:06 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

Apr 25, 21:09:56  Debug    APP  State change from IDLE to AUTHENTICATING after event START
Apr 25, 21:09:56  Info     APP  IKE daemon started
Apr 25, 21:09:56  Info     APP  IPSec started
Apr 25, 21:09:56  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
Apr 25, 21:09:56  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Apr 25, 21:09:56  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Apr 25, 21:09:56  Info     IKE  Foreground mode.
Apr 25, 21:09:56  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
Apr 25, 21:09:56  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
Apr 25, 21:09:56  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
Apr 25, 21:09:56  Info     IKE  Resize address pool from 0 to 255
Apr 25, 21:09:56  Debug    IKE  lifetime = 600
Apr 25, 21:09:56  Debug    IKE  lifebyte = 0
Apr 25, 21:09:56  Debug    IKE  encklen=0
Apr 25, 21:09:56  Debug    IKE  p:1 t:1
Apr 25, 21:09:56  Debug    IKE  3DES-CBC(5)
Apr 25, 21:09:56  Debug    IKE  SHA(2)
Apr 25, 21:09:56  Debug    IKE  768-bit MODP group(1)
Apr 25, 21:09:56  Debug    IKE  pre-shared key(1)
Apr 25, 21:09:56  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
Apr 25, 21:09:56  Debug    IKE  parse successed.
Apr 25, 21:09:56  Debug    IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
Apr 25, 21:09:56  Info     IKE  192.168.215.3[4500] used as isakmp port (fd=7)
Apr 25, 21:09:56  Info     IKE  192.168.215.3[500] used as isakmp port (fd=8)
Apr 25, 21:09:56  Debug    IKE  get pfkey X_SPDDUMP message
Apr 25, 21:09:56  Debug    IKE  02120000 0f000100 01000000 f1150000 03000500 ff180000 10020000 0a010800
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d703 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  07001200 02000100 ba020000 00000000 28003200 02020000 10020000 c0a8d7e7
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 10020000 c0a8d703 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  get pfkey X_SPDDUMP message
Apr 25, 21:09:56  Debug    IKE  02120000 0f000100 00000000 f1150000 03000500 ff200000 10020000 c0a8d703
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 0a010800 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  07001200 02000200 b9020000 00000000 28003200 02020000 10020000 c0a8d703
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 10020000 c0a8d7e7 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  sub:0xbffff560: 192.168.215.3/32[0] 10.1.8.0/24[0] proto=any dir=out
Apr 25, 21:09:56  Debug    IKE  db :0x308b78: 10.1.8.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 25, 21:09:56  Info     APP  Initiated connection D-Link DI-804HV
Apr 25, 21:09:56  Debug    IKE  get pfkey ACQUIRE message
Apr 25, 21:09:56  Debug    IKE  02060003 24000000 20070000 00000000 03000500 ff200000 10020000 c0a8d703
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e7 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  1c000d00 20000000 00030000 00000000 00010008 00000000 01000000 01000000
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 25, 21:09:56  Debug    IKE  80700000 00000000 00000000 00000000 00040000 00000000 0001c001 00000000
```

```
Apr 25, 21:09:56  Debug    IKE  01000000 01000000 00000000 00000000 00000000 00000000 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  80510100 00000000 80700000 00000000 00000000 00000000 000c0000 00000000
Apr 25, 21:09:56  Debug    IKE  00010001 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
Apr 25, 21:09:56  Error    IKE  inappropriate sadb acquire message passed.
Apr 25, 21:09:56  Debug    IKE  get pfkey ACQUIRE message
Apr 25, 21:09:56  Debug    IKE  02060003 14000000 f7000000 1d150000 03000500 ff200000 10020000 c0a8d703
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e7 00000000 00000000
Apr 25, 21:09:56  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 25, 21:09:56  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 25, 21:09:56  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 b9020000 00000000
Apr 25, 21:09:56  Debug    IKE  suitable outbound SP found: 192.168.215.3/32[0] 10.1.8.0/24[0] proto=any dir=out.
Apr 25, 21:09:56  Debug    IKE  sub:0xbffff53c: 10.1.8.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 25, 21:09:56  Debug    IKE  db :0x308b78: 10.1.8.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 25, 21:09:56  Debug    IKE  suitable inbound SP found: 10.1.8.0/24[0] 192.168.215.3/32[0] proto=any dir=in.
Apr 25, 21:09:56  Debug    IKE  new acquire 192.168.215.3/32[0] 10.1.8.0/24[0] proto=any dir=out
Apr 25, 21:09:56  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 25, 21:09:56  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 25, 21:09:56  Debug    IKE  in post_acquire
Apr 25, 21:09:56  Debug    IKE  configuration found for 192.168.215.231.
Apr 25, 21:09:56  Info     IKE  IPsec-SA request for 192.168.215.231 queued due to no phase1 found.
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Info     IKE  initiate new phase 1 negotiation: 192.168.215.3[500]<=>192.168.215.231[500]
Apr 25, 21:09:56  Info     IKE  begin Identity Protection mode.
Apr 25, 21:09:56  Debug    IKE  new cookie:
Apr 25, 21:09:56  Debug    IKE  3b7e773457ed7f02
Apr 25, 21:09:56  Debug    IKE  add payload of len 48, next type 13
Apr 25, 21:09:56  Debug    IKE  add payload of len 16, next type 0
Apr 25, 21:09:56  Debug    IKE  100 bytes from 192.168.215.3[500] to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  sockname 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet from 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  1 times of 100 bytes message will be sent to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 00000000 00000000 01100200 00000000 00000064 0d000034
Apr 25, 21:09:56  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0258
Apr 25, 21:09:56  Debug    IKE  80010005 80030001 80020002 80040001 00000014 afcad713 68a1f1c9 6b8696fc
Apr 25, 21:09:56  Debug    IKE  77570100
Apr 25, 21:09:56  Debug    IKE  resend phase1 packet 3b7e773457ed7f02:0000000000000000
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Debug    IKE  84 bytes message received from 192.168.215.231[500] to 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 01100200 00000000 00000054 00000038
Apr 25, 21:09:56  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 80010005 80020002
Apr 25, 21:09:56  Debug    IKE  80030001 80040001 800b0001 000c0004 00000258
Apr 25, 21:09:56  Debug    IKE  begin.
Apr 25, 21:09:56  Debug    IKE  seen nptype=1(sa)
Apr 25, 21:09:56  Debug    IKE  succeed.
Apr 25, 21:09:56  Debug    IKE  total SA len=52
Apr 25, 21:09:56  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 80010005 80020002
Apr 25, 21:09:56  Debug    IKE  80030001 80040001 800b0001 000c0004 00000258
Apr 25, 21:09:56  Debug    IKE  begin.
Apr 25, 21:09:56  Debug    IKE  seen nptype=2(prop)
Apr 25, 21:09:56  Debug    IKE  succeed.
Apr 25, 21:09:56  Debug    IKE  proposal #1 len=44
Apr 25, 21:09:56  Debug    IKE  begin.
Apr 25, 21:09:56  Debug    IKE  seen nptype=3(trns)
Apr 25, 21:09:56  Debug    IKE  succeed.
Apr 25, 21:09:56  Debug    IKE  transform #1 len=36
Apr 25, 21:09:56  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Apr 25, 21:09:56  Debug    IKE  hash(sha1)
Apr 25, 21:09:56  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Apr 25, 21:09:56  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
Apr 25, 21:09:56  Debug    IKE  hmac(modp768)
Apr 25, 21:09:56  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Apr 25, 21:09:56  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Apr 25, 21:09:56  Debug    IKE  pair 1:
Apr 25, 21:09:56  Debug    IKE  0x3094d0: next=0x0 tnext=0x0
Apr 25, 21:09:56  Debug    IKE  proposal #1: 1 transform
Apr 25, 21:09:56  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
Apr 25, 21:09:56  Debug    IKE  trns#=1, trns-id=IKE
Apr 25, 21:09:56  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Apr 25, 21:09:56  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Apr 25, 21:09:56  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
```

```
Apr 25, 21:09:56  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
Apr 25, 21:09:56  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Apr 25, 21:09:56  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Apr 25, 21:09:56  Debug    IKE  Compared: DB:Peer
Apr 25, 21:09:56  Debug    IKE  (lifetime = 600:600)
Apr 25, 21:09:56  Debug    IKE  (lifebyte = 0:0)
Apr 25, 21:09:56  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
Apr 25, 21:09:56  Debug    IKE  (encklen = 0:0)
Apr 25, 21:09:56  Debug    IKE  hashtype = SHA:SHA
Apr 25, 21:09:56  Debug    IKE  authmethod = pre-shared key:pre-shared key
Apr 25, 21:09:56  Debug    IKE  dh_group = 768-bit MODP group:768-bit MODP group
Apr 25, 21:09:56  Debug    IKE  an acceptable proposal found.
Apr 25, 21:09:56  Debug    IKE  hmac(modp768)
Apr 25, 21:09:56  Debug    IKE  agreed on pre-shared key auth.
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Debug    IKE  compute DH's private.
Apr 25, 21:09:56  Debug    IKE  744dc277 1336ef8a db56ba1b c7d86c0e efd07e07 3c498b3d ade551eb 58a78ac5
Apr 25, 21:09:56  Debug    IKE  24bd5777 e1c28e25 82870d0f fa4ce696 314d0086 f7847808 07ad900a 7d3339c8
Apr 25, 21:09:56  Debug    IKE  506ac3ba 709f5d11 a65e8163 f5ed194e 5c0bd4f6 c1b73f58 20c48e87 49dc2ef6
Apr 25, 21:09:56  Debug    IKE  compute DH's public.
Apr 25, 21:09:56  Debug    IKE  8ca035a2 78c5ff51 9e66485d d7cf31c9 bb7cf040 2f9e704d 97d985c6 6ba0eb9a
Apr 25, 21:09:56  Debug    IKE  67bc9167 72d5b28f 7dbe490f 4e2f9078 5b6a38fe c2608d5b e1e9d9e0 ebf290f9
Apr 25, 21:09:56  Debug    IKE  1ae0edae 86cd7e3d 92cd4286 75809729 1f0574ee af257e61 cb963aa0 7669777d
Apr 25, 21:09:56  Debug    IKE  add payload of len 96, next type 10
Apr 25, 21:09:56  Debug    IKE  add payload of len 16, next type 0
Apr 25, 21:09:56  Debug    IKE  148 bytes from 192.168.215.3[500] to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  sockname 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet from 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  1 times of 148 bytes message will be sent to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 04100200 00000000 00000094 0a000064
Apr 25, 21:09:56  Debug    IKE  8ca035a2 78c5ff51 9e66485d d7cf31c9 bb7cf040 2f9e704d 97d985c6 6ba0eb9a
Apr 25, 21:09:56  Debug    IKE  67bc9167 72d5b28f 7dbe490f 4e2f9078 5b6a38fe c2608d5b e1e9d9e0 ebf290f9
Apr 25, 21:09:56  Debug    IKE  1ae0edae 86cd7e3d 92cd4286 75809729 1f0574ee af257e61 cb963aa0 7669777d
Apr 25, 21:09:56  Debug    IKE  00000014 d338a17f 9d1b8125 f7448853 4a9eff5b
Apr 25, 21:09:56  Debug    IKE  resend phase1 packet 3b7e773457ed7f02:5aeaba933d28bcb5
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Debug    IKE  152 bytes message received from 192.168.215.231[500] to 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 04100200 00000000 00000098 0a000064
Apr 25, 21:09:56  Debug    IKE  5f83ce9a e463347b 14364c57 4cd183cd 766028ba 774ce0e8 32614725 3791be91
Apr 25, 21:09:56  Debug    IKE  ecc13c12 7f978dd0 3ab64f9c 58b5b1ce 3b55f56b f279f662 a4450ff7 a0940bc4
Apr 25, 21:09:56  Debug    IKE  86d8cfcd 42c8b0ab 63ccbb6f 7c664d97 728fe5f8 77f68ed5 c120a628 a00c28e6
Apr 25, 21:09:56  Debug    IKE  00000018 fe44f3cb 1734404c 584d19fc 1f99c27d 4944f3e2
Apr 25, 21:09:56  Debug    IKE  begin.
Apr 25, 21:09:56  Debug    IKE  seen nptype=4(ke)
Apr 25, 21:09:56  Debug    IKE  seen nptype=10(nonce)
Apr 25, 21:09:56  Debug    IKE  succeed.
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Debug    IKE  compute DH's shared.
Apr 25, 21:09:56  Debug    IKE  5d56800c a888889a 2725aa76 6eb8ad1b 6494cbce 717c78d0 0663dd33 feed51e6
Apr 25, 21:09:56  Debug    IKE  06c58aa0 04b29b37 0f6d9f54 7c0dd28d af3059f3 2e5df437 933327eb 186ad535
Apr 25, 21:09:56  Debug    IKE  8e0dd932 20daa714 b2f7c019 0a403b6c 3f411e62 e4571107 db1e17eb 3973442f
Apr 25, 21:09:56  Debug    IKE  the psk found.
Apr 25, 21:09:56  Debug    IKE  psk: 2007-04-25 21:09:56: DEBUG2:
Apr 25, 21:09:56  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
Apr 25, 21:09:56  Debug    IKE  nonce 1: 2007-04-25 21:09:56: DEBUG:
Apr 25, 21:09:56  Debug    IKE  d338a17f 9d1b8125 f7448853 4a9eff5b
Apr 25, 21:09:56  Debug    IKE  nonce 2: 2007-04-25 21:09:56: DEBUG:
Apr 25, 21:09:56  Debug    IKE  fe44f3cb 1734404c 584d19fc 1f99c27d 4944f3e2
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  SKEYID computed:
Apr 25, 21:09:56  Debug    IKE  e4d7d6ac 022a3672 da35af5f 8c29215f d3464c53
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  SKEYID_d computed:
Apr 25, 21:09:56  Debug    IKE  adbaf0b7 696dc48b cc049885 121da788 db89b9de
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  SKEYID_a computed:
Apr 25, 21:09:56  Debug    IKE  e0991613 ac16adba 1e33ed8b 9b98f430 7b5c2687
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  SKEYID_e computed:
Apr 25, 21:09:56  Debug    IKE  f270bc9a d39ad044 b0b706be 13d57265 7e6a8465
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  hash(sha1)
Apr 25, 21:09:56  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
```

```
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  compute intermediate encryption key K1
Apr 25, 21:09:56  Debug    IKE  00
Apr 25, 21:09:56  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  compute intermediate encryption key K2
Apr 25, 21:09:56  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca
Apr 25, 21:09:56  Debug    IKE  fbce41ae ae452550 3a1f4266 05a0697e 799bb29e
Apr 25, 21:09:56  Debug    IKE  final encryption key computed:
Apr 25, 21:09:56  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:56  Debug    IKE  hash(sha1)
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  IV computed:
Apr 25, 21:09:56  Debug    IKE  aa4345b9 04bac003
Apr 25, 21:09:56  Debug    IKE  use ID type of IPv4_address
Apr 25, 21:09:56  Debug    IKE  HASH with:
Apr 25, 21:09:56  Debug    IKE  8ca035a2 78c5ff51 9e66485d d7cf31c9 bb7cf040 2f9e704d 97d985c6 6ba0eb9a
Apr 25, 21:09:56  Debug    IKE  67bc9167 72d5b28f 7dbe490f 4e2f9078 5b6a38fe c2608d5b e1e9d9e0 ebf290f9
Apr 25, 21:09:56  Debug    IKE  1ae0edae 86cd7e3d 92cd4286 75809729 1f0574ee af257e61 cb963aa0 7669777d
Apr 25, 21:09:56  Debug    IKE  5f83ce9a e463347b 14364c57 4cd183cd 766028ba 774ce0e8 32614725 3791be91
Apr 25, 21:09:56  Debug    IKE  ecc13c12 7f978dd0 3ab64f9c 58b5b1ce 3b55f56b f279f662 a4450ff7 a0940bc4
Apr 25, 21:09:56  Debug    IKE  86d8cfcd 42c8b0ab 63ccbb6f 7c664d97 728fe5f8 77f68ed5 c120a628 a00c28e6
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 00000001 00000001 00000028 01010001
Apr 25, 21:09:56  Debug    IKE  00000020 01010000 800b0001 800c0258 80010005 80030001 80020002 80040001
Apr 25, 21:09:56  Debug    IKE  011101f4 c0a8d703
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  HASH (init) computed:
Apr 25, 21:09:56  Debug    IKE  f3444d97 5afe4416 4d69683c 034afe85 ef3562d3
Apr 25, 21:09:56  Debug    IKE  add payload of len 8, next type 8
Apr 25, 21:09:56  Debug    IKE  add payload of len 20, next type 0
Apr 25, 21:09:56  Debug    IKE  begin encryption.
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  pad length = 4
Apr 25, 21:09:56  Debug    IKE  0800000c 011101f4 c0a8d703 00000018 f3444d97 5afe4416 4d69683c 034afe85
Apr 25, 21:09:56  Debug    IKE  ef3562d3 00000004
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  with key:
Apr 25, 21:09:56  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:56  Debug    IKE  encrypted payload by IV:
Apr 25, 21:09:56  Debug    IKE  aa4345b9 04bac003
Apr 25, 21:09:56  Debug    IKE  save IV for next:
Apr 25, 21:09:56  Debug    IKE  8e844998 0b47a9f5
Apr 25, 21:09:56  Debug    IKE  encrypted.
Apr 25, 21:09:56  Debug    IKE  68 bytes from 192.168.215.3[500] to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  sockname 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet from 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  1 times of 68 bytes message will be sent to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 05100201 00000000 00000044 9788aaea
Apr 25, 21:09:56  Debug    IKE  302dd659 254e95f6 848ea10c b852d1bf 1bb84e36 5358ee2c bbf11af6 8e844998
Apr 25, 21:09:56  Debug    IKE  0b47a9f5
Apr 25, 21:09:56  Debug    IKE  resend phase1 packet 3b7e773457ed7f02:5aeaba933d28bcb5
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Debug    IKE  92 bytes message received from 192.168.215.231[500] to 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 05100201 00000000 0000005c c11b9eeb
Apr 25, 21:09:56  Debug    IKE  d619b543 bf1644ed b4910468 19f87335 ef0b19df 81e86690 04884f0b df06d2c5
Apr 25, 21:09:56  Debug    IKE  84d6a024 34e20636 5a366e21 3e08f391 decae9ab c4804bc6 a6d99199
Apr 25, 21:09:56  Debug    IKE  begin decryption.
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  IV was saved for next processing:
Apr 25, 21:09:56  Debug    IKE  c4804bc6 a6d99199
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  with key:
Apr 25, 21:09:56  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:56  Debug    IKE  decrypted payload by IV:
Apr 25, 21:09:56  Debug    IKE  8e844998 0b47a9f5
Apr 25, 21:09:56  Debug    IKE  decrypted payload, but not trimed.
Apr 25, 21:09:56  Debug    IKE  0800000c 01000000 c0a8d7e7 00000018 514571a6 0308ea48 2d8aeb0f fa1d500d
Apr 25, 21:09:56  Debug    IKE  c816dcf2 ecc13c12 7f978dd0 3ab64f9c 58b5b1ce 3b55f56b f279f662 a4450ff7
Apr 25, 21:09:56  Debug    IKE  padding len=247
Apr 25, 21:09:56  Debug    IKE  skip to trim padding.
Apr 25, 21:09:56  Debug    IKE  decrypted.
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 05100201 00000000 0000005c 0800000c
Apr 25, 21:09:56  Debug    IKE  01000000 c0a8d7e7 00000018 514571a6 0308ea48 2d8aeb0f fa1d500d c816dcf2
```

```
Apr 25, 21:09:56  Debug    IKE  ecc13c12 7f978dd0 3ab64f9c 58b5b1ce 3b55f56b f279f662 a4450ff7
Apr 25, 21:09:56  Debug    IKE  begin.
Apr 25, 21:09:56  Debug    IKE  seen nptype=5(id)
Apr 25, 21:09:56  Debug    IKE  seen nptype=8(hash)
Apr 25, 21:09:56  Debug    IKE  succeed.
Apr 25, 21:09:56  Debug    IKE  HASH received:
Apr 25, 21:09:56  Debug    IKE  514571a6 0308ea48 2d8aeb0f fa1d500d c816dcf2
Apr 25, 21:09:56  Debug    IKE  HASH with:
Apr 25, 21:09:56  Debug    IKE  5f83ce9a e463347b 14364c57 4cd183cd 766028ba 774ce0e8 32614725 3791be91
Apr 25, 21:09:56  Debug    IKE  ecc13c12 7f978dd0 3ab64f9c 58b5b1ce 3b55f56b f279f662 a4450ff7 a0940bc4
Apr 25, 21:09:56  Debug    IKE  86d8cfcd 42c8b0ab 63ccbb6f 7c664d97 728fe5f8 77f68ed5 c120a628 a00c28e6
Apr 25, 21:09:56  Debug    IKE  8ca035a2 78c5ff51 9e66485d d7cf31c9 bb7cf040 2f9e704d 97d985c6 6ba0eb9a
Apr 25, 21:09:56  Debug    IKE  67bc9167 72d5b28f 7dbe490f 4e2f9078 5b6a38fe c2608d5b e1e9d9e0 ebf290f9
Apr 25, 21:09:56  Debug    IKE  1ae0edae 86cd7e3d 92cd4286 75809729 1f0574ee af257e61 cb963aa0 7669777d
Apr 25, 21:09:56  Debug    IKE  5aeaba93 3d28bcb5 3b7e7734 57ed7f02 00000001 00000001 00000028 01010001
Apr 25, 21:09:56  Debug    IKE  00000020 01010000 800b0001 800c0258 80010005 80030001 80020002 80040001
Apr 25, 21:09:56  Debug    IKE  01000000 c0a8d7e7
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  HASH (init) computed:
Apr 25, 21:09:56  Debug    IKE  514571a6 0308ea48 2d8aeb0f fa1d500d c816dcf2
Apr 25, 21:09:56  Debug    IKE  HASH for PSK validated.
Apr 25, 21:09:56  Debug    IKE  peer's ID:2007-04-25 21:09:56: DEBUG:
Apr 25, 21:09:56  Debug    IKE  01000000 c0a8d7e7
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:56  Debug    IKE  compute IV for phase2
Apr 25, 21:09:56  Debug    IKE  phase1 last IV:
Apr 25, 21:09:56  Debug    IKE  c4804bc6 a6d99199 e75ef8b0
Apr 25, 21:09:56  Debug    IKE  hash(sha1)
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  phase2 IV computed:
Apr 25, 21:09:56  Debug    IKE  d6a4bd6a 56eb9905
Apr 25, 21:09:56  Debug    IKE  HASH with:
Apr 25, 21:09:56  Debug    IKE  e75ef8b0 0000001c 00000001 01106002 3b7e7734 57ed7f02 5aeaba93 3d28bcb5
Apr 25, 21:09:56  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:56  Debug    IKE  HASH computed:
Apr 25, 21:09:56  Debug    IKE  33b18456 8281c610 88d84610 7ee6237f 18c2a858
Apr 25, 21:09:56  Debug    IKE  begin encryption.
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  pad length = 4
Apr 25, 21:09:56  Debug    IKE  0b000018 33b18456 8281c610 88d84610 7ee6237f 18c2a858 0000001c 00000001
Apr 25, 21:09:56  Debug    IKE  01106002 3b7e7734 57ed7f02 5aeaba93 3d28bcb5 00000004
Apr 25, 21:09:56  Debug    IKE  encryption(3des)
Apr 25, 21:09:56  Debug    IKE  with key:
Apr 25, 21:09:56  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:56  Debug    IKE  encrypted payload by IV:
Apr 25, 21:09:56  Debug    IKE  d6a4bd6a 56eb9905
Apr 25, 21:09:56  Debug    IKE  save IV for next:
Apr 25, 21:09:56  Debug    IKE  c985a67b 25d11fce
Apr 25, 21:09:56  Debug    IKE  encrypted.
Apr 25, 21:09:56  Debug    IKE  84 bytes from 192.168.215.3[500] to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  sockname 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet from 192.168.215.3[500]
Apr 25, 21:09:56  Debug    IKE  send packet to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.231[500]
Apr 25, 21:09:56  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 08100501 e75ef8b0 00000054 4a57d6dd
Apr 25, 21:09:56  Debug    IKE  cef42565 c36ea9c7 7467691a b4fc7b2e 9a64ccbd a243f746 30929d9c 8c29074d
Apr 25, 21:09:56  Debug    IKE  35a28321 7caebef1 08628cb6 c985a67b 25d11fce
Apr 25, 21:09:56  Debug    IKE  sendto Information notify.
Apr 25, 21:09:56  Debug    IKE  IV freed
Apr 25, 21:09:56  Info     IKE  ISAKMP-SA established 192.168.215.3[500]-192.168.215.231[500] spi:
3b7e773457ed7f02:5aeaba933d28bcb5
Apr 25, 21:09:56  Debug    IKE  ===
Apr 25, 21:09:57  Info     APP  Initiated connection D-Link DI-804HV
Apr 25, 21:09:57  Debug    IKE  get pfkey ACQUIRE message
Apr 25, 21:09:57  Debug    IKE  02060003 14000000 f8000000 1d150000 03000500 ff200000 10020000 c0a8d703
Apr 25, 21:09:57  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e7 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 25, 21:09:57  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 25, 21:09:57  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 b9020000 00000000
Apr 25, 21:09:57  Debug    IKE  ignore the acquire because ph2 found
Apr 25, 21:09:57  Debug    IKE  ===
Apr 25, 21:09:57  Debug    IKE  begin QUICK mode.
Apr 25, 21:09:57  Info     IKE  initiate new phase 2 negotiation: 192.168.215.3[500]<=>192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  compute IV for phase2
```

```
Apr 25, 21:09:57  Debug    IKE  phase1 last IV:
Apr 25, 21:09:57  Debug    IKE  c4804bc6 a6d99199 a34d6ddc
Apr 25, 21:09:57  Debug    IKE  hash(sha1)
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  phase2 IV computed:
Apr 25, 21:09:57  Debug    IKE  2c66cf4d 6a69e52a
Apr 25, 21:09:57  Debug    IKE  call pfkey_send_getspi
Apr 25, 21:09:57  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.231[0]->192.168.215.3[0]
Apr 25, 21:09:57  Debug    IKE  pfkey getspi sent.
Apr 25, 21:09:57  Debug    IKE  get pfkey GETSPI message
Apr 25, 21:09:57  Debug    IKE  02010003 0a000000 f7000000 f1150000 02000100 002598dc 00000000 0000000b
Apr 25, 21:09:57  Debug    IKE  03000500 ff200000 10020000 c0a8d7e7 00000000 00000000 03000600 ff200000
Apr 25, 21:09:57  Debug    IKE  10020000 c0a8d703 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.231[0]->192.168.215.3[0]
spi=2463964(0x2598dc)
Apr 25, 21:09:57  Debug    IKE  hmac(modp768)
Apr 25, 21:09:57  Debug    IKE  hmac(modp768)
Apr 25, 21:09:57  Debug    IKE  hmac(modp768)
Apr 25, 21:09:57  Debug    IKE  compute DH's private.
Apr 25, 21:09:57  Debug    IKE  58cd66d9 dc36e14d f324b5fd b8fbf1dc b09e2639 c0d95fc9 21063623 5261b73f
Apr 25, 21:09:57  Debug    IKE  1de5405d e2ffbfac be45cad2 bbc10d3c 0d5c2817 5ac6c720 ed5a65f7 081b162a
Apr 25, 21:09:57  Debug    IKE  0233262e 764ffd00 c97b0cb8 8f71d525 7381e845 a7e03b6c b28e6538 89c638df
Apr 25, 21:09:57  Debug    IKE  compute DH's public.
Apr 25, 21:09:57  Debug    IKE  d7bac09a f8413261 0d8c7d05 8881807f 51c31830 db4d4ad5 68f8d1a2 80508f85
Apr 25, 21:09:57  Debug    IKE  77e97b50 c7d595f6 7df2531f ee40337b 492f64de 762322b7 8fb92ebb 28ea3006
Apr 25, 21:09:57  Debug    IKE  6f1e9786 2f368036 a5659d75 3d9b1c8f d322ed45 4c920ff8 8678ba47 142f728e
Apr 25, 21:09:57  Debug    IKE  use local ID type IPv4_address
Apr 25, 21:09:57  Debug    IKE  use remote ID type IPv4_subnet
Apr 25, 21:09:57  Debug    IKE  IDci:
Apr 25, 21:09:57  Debug    IKE  01000000 c0a8d703
Apr 25, 21:09:57  Debug    IKE  IDcr:
Apr 25, 21:09:57  Debug    IKE  04000000 0a010800 ffffff00
Apr 25, 21:09:57  Debug    IKE  add payload of len 48, next type 10
Apr 25, 21:09:57  Debug    IKE  add payload of len 16, next type 4
Apr 25, 21:09:57  Debug    IKE  add payload of len 96, next type 5
Apr 25, 21:09:57  Debug    IKE  add payload of len 8, next type 5
Apr 25, 21:09:57  Debug    IKE  add payload of len 12, next type 0
Apr 25, 21:09:57  Debug    IKE  HASH with:
Apr 25, 21:09:57  Debug    IKE  a34d6ddc 0a000034 00000001 00000001 00000028 01030401 002598dc 0000001c
Apr 25, 21:09:57  Debug    IKE  01030000 80010001 80020258 80040001 80050002 80030001 04000014 bc6ce34c
Apr 25, 21:09:57  Debug    IKE  176ecb56 d499cb70 260dcd04 05000064 d7bac09a f8413261 0d8c7d05 8881807f
Apr 25, 21:09:57  Debug    IKE  51c31830 db4d4ad5 68f8d1a2 80508f85 77e97b50 c7d595f6 7df2531f ee40337b
Apr 25, 21:09:57  Debug    IKE  492f64de 762322b7 8fb92ebb 28ea3006 6f1e9786 2f368036 a5659d75 3d9b1c8f
Apr 25, 21:09:57  Debug    IKE  d322ed45 4c920ff8 8678ba47 142f728e 0500000c 01000000 c0a8d703 00000010
Apr 25, 21:09:57  Debug    IKE  04000000 0a010800 ffffff00
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  HASH computed:
Apr 25, 21:09:57  Debug    IKE  864e15ef 0f093af3 31bf557d 49f760ed 269007e1
Apr 25, 21:09:57  Debug    IKE  add payload of len 20, next type 1
Apr 25, 21:09:57  Debug    IKE  begin encryption.
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  pad length = 8
Apr 25, 21:09:57  Debug    IKE  01000018 864e15ef 0f093af3 31bf557d 49f760ed 269007e1 0a000034 00000001
Apr 25, 21:09:57  Debug    IKE  00000001 00000028 01030401 002598dc 0000001c 01030000 80010001 80020258
Apr 25, 21:09:57  Debug    IKE  80040001 80050002 80030001 04000014 bc6ce34c 176ecb56 d499cb70 260dcd04
Apr 25, 21:09:57  Debug    IKE  05000064 d7bac09a f8413261 0d8c7d05 8881807f 51c31830 db4d4ad5 68f8d1a2
Apr 25, 21:09:57  Debug    IKE  80508f85 77e97b50 c7d595f6 7df2531f ee40337b 492f64de 762322b7 8fb92ebb
Apr 25, 21:09:57  Debug    IKE  28ea3006 6f1e9786 2f368036 a5659d75 3d9b1c8f d322ed45 4c920ff8 8678ba47
Apr 25, 21:09:57  Debug    IKE  142f728e 0500000c 01000000 c0a8d703 00000010 04000000 0a010800 ffffff00
Apr 25, 21:09:57  Debug    IKE  00000000 00000008
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  with key:
Apr 25, 21:09:57  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:57  Debug    IKE  encrypted payload by IV:
Apr 25, 21:09:57  Debug    IKE  2c66cf4d 6a69e52a
Apr 25, 21:09:57  Debug    IKE  save IV for next:
Apr 25, 21:09:57  Debug    IKE  97d6d14d a4929060
Apr 25, 21:09:57  Debug    IKE  encrypted.
Apr 25, 21:09:57  Debug    IKE  260 bytes from 192.168.215.3[500] to 192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 25, 21:09:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 25, 21:09:57  Debug    IKE  send packet to 192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  1 times of 260 bytes message will be sent to 192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 08102001 a34d6ddc 00000104 e9e1197e
```

```
Apr 25, 21:09:57  Debug    IKE  704fe933 9bcb7d32 28580f73 2e0e259b 4dfa1389 35d8e72c 23eca5f4 a4a42e66
Apr 25, 21:09:57  Debug    IKE  87fb7cde 053193e7 7ee6f0ad 2053617f 05da87e3 dce3496f 0d841fb2 abbfd719
Apr 25, 21:09:57  Debug    IKE  0340246c 2feca740 389c6fb7 e331f32e 635e9e9a d57491bc c775f7ca 73936d4d
Apr 25, 21:09:57  Debug    IKE  a4efe557 a5ef793e aa4c18c7 8f83297f d0680cbf cbbbee52 e3c7b1aa 5e71a1d1
Apr 25, 21:09:57  Debug    IKE  03e1f017 f173ab1a 119c2c18 c687c24e 662fe2d4 bf66861e e3199be5 cec6ead8
Apr 25, 21:09:57  Debug    IKE  5a586116 2caddbbf 80999d8e 19adf412 6975e479 5fea44c7 fc470899 b001b8b8
Apr 25, 21:09:57  Debug    IKE  3b7cc6f3 2c35ff0b f1c84a77 3921e8a7 2af1351a 8f6b9d46 0241b721 97d6d14d
Apr 25, 21:09:57  Debug    IKE  a4929060
Apr 25, 21:09:57  Debug    IKE  resend phase2 packet 3b7e773457ed7f02:5aeaba933d28bcb5:0000a34d
Apr 25, 21:09:57  Debug    IKE  ===
Apr 25, 21:09:57  Debug    IKE  260 bytes message received from 192.168.215.231[500] to 192.168.215.3[500]
Apr 25, 21:09:57  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 08102001 a34d6ddc 00000104 eb482394
Apr 25, 21:09:57  Debug    IKE  78e4915c d60ff36b a12dff69 1a0d7676 122e9917 88ef4935 b8210726 b1f71305
Apr 25, 21:09:57  Debug    IKE  75e95eb9 a6482116 92bb9fc8 7845e7f6 c23fbbf8 d4e8e10d 1af92b58 2eae9467
Apr 25, 21:09:57  Debug    IKE  201ce3a5 ca5d5b0c e7ef8041 b3937ccc 98e14a2d b66876c8 81ffbe57 fb3cc6b9
Apr 25, 21:09:57  Debug    IKE  503ba61f 3165f6b6 6ecf9eb3 572695a0 b6d82480 946ad07e 78b125a2 759888f0
Apr 25, 21:09:57  Debug    IKE  9fe9cf05 161f7634 b0aed13a cbada802 97c5b3e2 85754ba9 c881fd4e 9de23159
Apr 25, 21:09:57  Debug    IKE  838bb4b0 0b13529c 7abec629 c2175e3c fc747140 d0441195 afdfd405 2f9b4d3a
Apr 25, 21:09:57  Debug    IKE  ff6b0baf 09bd0ac4 2615e146 637e6c4c c18f8254 cbf823f5 ef4941b9 d00a3768
Apr 25, 21:09:57  Debug    IKE  c66ab7c2
Apr 25, 21:09:57  Debug    IKE  begin decryption.
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  IV was saved for next processing:
Apr 25, 21:09:57  Debug    IKE  d00a3768 c66ab7c2
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  with key:
Apr 25, 21:09:57  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:57  Debug    IKE  decrypted payload by IV:
Apr 25, 21:09:57  Debug    IKE  97d6d14d a4929060
Apr 25, 21:09:57  Debug    IKE  decrypted payload, but not trimed.
Apr 25, 21:09:57  Debug    IKE  01000018 b7c5ddc3 e4a226e4 39aeb7f1 2004ae61 4e6de27a 0a000038 00000001
Apr 25, 21:09:57  Debug    IKE  00000001 0000002c 01030401 a60e0010 00000020 01030000 80050002 80040001
Apr 25, 21:09:57  Debug    IKE  80030001 80010001 00020004 00000258 04000018 47d1b35e 54951f8d 3ce9182f
Apr 25, 21:09:57  Debug    IKE  55a589ca b21e7da3 05000064 2dcb1a01 995a1b44 e580e807 e7769018 de5879f4
Apr 25, 21:09:57  Debug    IKE  0449dde4 93bb5c84 213f249d 89842106 9d298f0f 3b4ce19e 30d7a829 30369077
Apr 25, 21:09:57  Debug    IKE  778512a6 422ddfa5 e0a96d66 0606fda3 8151478b b7feaf43 d5d3e3f7 4d519793
Apr 25, 21:09:57  Debug    IKE  d923331f f29866af b115d14e 0500000c 01000000 c0a8d703 00000010 04000000
Apr 25, 21:09:57  Debug    IKE  0a010800 ffffff00
Apr 25, 21:09:57  Debug    IKE  padding len=0
Apr 25, 21:09:57  Debug    IKE  skip to trim padding.
Apr 25, 21:09:57  Debug    IKE  decrypted.
Apr 25, 21:09:57  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 08102001 a34d6ddc 00000104 01000018
Apr 25, 21:09:57  Debug    IKE  b7c5ddc3 e4a226e4 39aeb7f1 2004ae61 4e6de27a 0a000038 00000001 00000001
Apr 25, 21:09:57  Debug    IKE  0000002c 01030401 a60e0010 00000020 01030000 80050002 80040001 80030001
Apr 25, 21:09:57  Debug    IKE  80010001 00020004 00000258 04000018 47d1b35e 54951f8d 3ce9182f 55a589ca
Apr 25, 21:09:57  Debug    IKE  b21e7da3 05000064 2dcb1a01 995a1b44 e580e807 e7769018 de5879f4 0449dde4
Apr 25, 21:09:57  Debug    IKE  93bb5c84 213f249d 89842106 9d298f0f 3b4ce19e 30d7a829 30369077 778512a6
Apr 25, 21:09:57  Debug    IKE  422ddfa5 e0a96d66 0606fda3 8151478b b7feaf43 d5d3e3f7 4d519793 d923331f
Apr 25, 21:09:57  Debug    IKE  f29866af b115d14e 0500000c 01000000 c0a8d703 00000010 04000000 0a010800
Apr 25, 21:09:57  Debug    IKE  ffffff00
Apr 25, 21:09:57  Debug    IKE  begin.
Apr 25, 21:09:57  Debug    IKE  seen nptype=8(hash)
Apr 25, 21:09:57  Debug    IKE  seen nptype=1(sa)
Apr 25, 21:09:57  Debug    IKE  seen nptype=10(nonce)
Apr 25, 21:09:57  Debug    IKE  seen nptype=4(ke)
Apr 25, 21:09:57  Debug    IKE  seen nptype=5(id)
Apr 25, 21:09:57  Debug    IKE  seen nptype=5(id)
Apr 25, 21:09:57  Debug    IKE  succeed.
Apr 25, 21:09:57  Debug    IKE  HASH allocated:hbuf->l=248 actual:tlen=224
Apr 25, 21:09:57  Debug    IKE  HASH(2) received:2007-04-25 21:09:57: DEBUG:
Apr 25, 21:09:57  Debug    IKE  b7c5ddc3 e4a226e4 39aeb7f1 2004ae61 4e6de27a
Apr 25, 21:09:57  Debug    IKE  HASH with:
Apr 25, 21:09:57  Debug    IKE  a34d6ddc bc6ce34c 176ecb56 d499cb70 260dcd04 0a000038 00000001 00000001
Apr 25, 21:09:57  Debug    IKE  0000002c 01030401 a60e0010 00000020 01030000 80050002 80040001 80030001
Apr 25, 21:09:57  Debug    IKE  80010001 00020004 00000258 04000018 47d1b35e 54951f8d 3ce9182f 55a589ca
Apr 25, 21:09:57  Debug    IKE  b21e7da3 05000064 2dcb1a01 995a1b44 e580e807 e7769018 de5879f4 0449dde4
Apr 25, 21:09:57  Debug    IKE  93bb5c84 213f249d 89842106 9d298f0f 3b4ce19e 30d7a829 30369077 778512a6
Apr 25, 21:09:57  Debug    IKE  422ddfa5 e0a96d66 0606fda3 8151478b b7feaf43 d5d3e3f7 4d519793 d923331f
Apr 25, 21:09:57  Debug    IKE  f29866af b115d14e 0500000c 01000000 c0a8d703 00000010 04000000 0a010800
Apr 25, 21:09:57  Debug    IKE  ffffff00
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  HASH computed:
Apr 25, 21:09:57  Debug    IKE  b7c5ddc3 e4a226e4 39aeb7f1 2004ae61 4e6de27a
Apr 25, 21:09:57  Debug    IKE  total SA len=48
```

```
Apr 25, 21:09:57  Debug    IKE  00000001 00000001 00000028 01030401 002598dc 0000001c 01030000 80010001
Apr 25, 21:09:57  Debug    IKE  80020258 80040001 80050002 80030001
Apr 25, 21:09:57  Debug    IKE  begin.
Apr 25, 21:09:57  Debug    IKE  seen nptype=2(prop)
Apr 25, 21:09:57  Debug    IKE  succeed.
Apr 25, 21:09:57  Debug    IKE  proposal #1 len=40
Apr 25, 21:09:57  Debug    IKE  begin.
Apr 25, 21:09:57  Debug    IKE  seen nptype=3(trns)
Apr 25, 21:09:57  Debug    IKE  succeed.
Apr 25, 21:09:57  Debug    IKE  transform #1 len=28
Apr 25, 21:09:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 25, 21:09:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 25, 21:09:57  Debug    IKE  life duration was in TLV.
Apr 25, 21:09:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 25, 21:09:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 25, 21:09:57  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 25, 21:09:57  Debug    IKE  hmac(modp768)
Apr 25, 21:09:57  Debug    IKE  pair 1:
Apr 25, 21:09:57  Debug    IKE  0x309e90: next=0x0 tnext=0x0
Apr 25, 21:09:57  Debug    IKE  proposal #1: 1 transform
Apr 25, 21:09:57  Debug    IKE  total SA len=52
Apr 25, 21:09:57  Debug    IKE  00000001 00000001 0000002c 01030401 a60e0010 00000020 01030000 80050002
Apr 25, 21:09:57  Debug    IKE  80040001 80030001 80010001 00020004 00000258
Apr 25, 21:09:57  Debug    IKE  begin.
Apr 25, 21:09:57  Debug    IKE  seen nptype=2(prop)
Apr 25, 21:09:57  Debug    IKE  succeed.
Apr 25, 21:09:57  Debug    IKE  proposal #1 len=44
Apr 25, 21:09:57  Debug    IKE  begin.
Apr 25, 21:09:57  Debug    IKE  seen nptype=3(trns)
Apr 25, 21:09:57  Debug    IKE  succeed.
Apr 25, 21:09:57  Debug    IKE  transform #1 len=32
Apr 25, 21:09:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 25, 21:09:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 25, 21:09:57  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 25, 21:09:57  Debug    IKE  hmac(modp768)
Apr 25, 21:09:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 25, 21:09:57  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Apr 25, 21:09:57  Debug    IKE  pair 1:
Apr 25, 21:09:57  Debug    IKE  0x30a5f0: next=0x0 tnext=0x0
Apr 25, 21:09:57  Debug    IKE  proposal #1: 1 transform
Apr 25, 21:09:57  Warning  IKE  attribute has been modified.
Apr 25, 21:09:57  Debug    IKE  begin compare proposals.
Apr 25, 21:09:57  Debug    IKE  pair[1]: 0x30a5f0
Apr 25, 21:09:57  Debug    IKE  0x30a5f0: next=0x0 tnext=0x0
Apr 25, 21:09:57  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Apr 25, 21:09:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 25, 21:09:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 25, 21:09:57  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 25, 21:09:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 25, 21:09:57  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Apr 25, 21:09:57  Debug    IKE  peer's single bundle:
Apr 25, 21:09:57  Debug    IKE  (proto_id=ESP spisize=4 spi=a60e0010 spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 25, 21:09:57  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 25, 21:09:57  Debug    IKE  my single bundle:
Apr 25, 21:09:57  Debug    IKE  (proto_id=ESP spisize=4 spi=002598dc spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 25, 21:09:57  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 25, 21:09:57  Debug    IKE  matched
Apr 25, 21:09:57  Debug    IKE  ===
Apr 25, 21:09:57  Debug    IKE  HASH(3) generate
Apr 25, 21:09:57  Debug    IKE  HASH with:
Apr 25, 21:09:57  Debug    IKE  00a34d6d dcbc6ce3 4c176ecb 56d499cb 70260dcd 0447d1b3 5e54951f 8d3ce918
Apr 25, 21:09:57  Debug    IKE  2f55a589 cab21e7d a3
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  HASH computed:
Apr 25, 21:09:57  Debug    IKE  f2d76b2e 3a5921be cb82466c b8fa9ccc 915dd742
Apr 25, 21:09:57  Debug    IKE  add payload of len 20, next type 0
Apr 25, 21:09:57  Debug    IKE  begin encryption.
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  pad length = 8
Apr 25, 21:09:57  Debug    IKE  00000018 f2d76b2e 3a5921be cb82466c b8fa9ccc 915dd742 00000000 00000008
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  with key:
Apr 25, 21:09:57  Debug    IKE  384be987 4bf1713e 076ecb2a bb746839 7b3c4aca fbce41ae
Apr 25, 21:09:57  Debug    IKE  encrypted payload by IV:
```

```
Apr 25, 21:09:57  Debug    IKE  d00a3768 c66ab7c2
Apr 25, 21:09:57  Debug    IKE  save IV for next:
Apr 25, 21:09:57  Debug    IKE  7ad170f9 17e6683a
Apr 25, 21:09:57  Debug    IKE  encrypted.
Apr 25, 21:09:57  Debug    IKE  60 bytes from 192.168.215.3[500] to 192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 25, 21:09:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 25, 21:09:57  Debug    IKE  send packet to 192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.231[500]
Apr 25, 21:09:57  Debug    IKE  3b7e7734 57ed7f02 5aeaba93 3d28bcb5 08102001 a34d6ddc 0000003c 3dc69ffd
Apr 25, 21:09:57  Debug    IKE  f24b23ef fdecc4d8 2bf6f2d2 190f51f8 2859b76d 7ad170f9 17e6683a
Apr 25, 21:09:57  Debug    IKE  compute DH's shared.
Apr 25, 21:09:57  Debug    IKE  71adbf7d acd83309 ea3759a1 f51f264f 2c6818f6 f45af36d 12ff532a 9defcbec
Apr 25, 21:09:57  Debug    IKE  4fa8f50d 275e0087 8290df42 46973f2d ed55b771 9ea98985 2bfb18b0 411cf29b
Apr 25, 21:09:57  Debug    IKE  79823f4e f33e0dbb fe044ece 13bbf2a4 f4a16bff 7482b3c4 15d0c2a8 c410c4cb
Apr 25, 21:09:57  Debug    IKE  KEYMAT compute with
Apr 25, 21:09:57  Debug    IKE  71adbf7d acd83309 ea3759a1 f51f264f 2c6818f6 f45af36d 12ff532a 9defcbec
Apr 25, 21:09:57  Debug    IKE  4fa8f50d 275e0087 8290df42 46973f2d ed55b771 9ea98985 2bfb18b0 411cf29b
Apr 25, 21:09:57  Debug    IKE  79823f4e f33e0dbb fe044ece 13bbf2a4 f4a16bff 7482b3c4 15d0c2a8 c410c4cb
Apr 25, 21:09:57  Debug    IKE  03002598 dcbc6ce3 4c176ecb 56d499cb 70260dcd 0447d1b3 5e54951f 8d3ce918
Apr 25, 21:09:57  Debug    IKE  2f55a589 cab21e7d a3
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  encklen=192 authklen=160
Apr 25, 21:09:57  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 25, 21:09:57  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  0d47047b 0c298773 2f37a62e aca3f7ce 12c9867e 0a1ef708 1f344a57 c5d38efe
Apr 25, 21:09:57  Debug    IKE  9a3f08ee 65bcc778 ec9cb4f7 86448e2d 71bc4e4c 36ec96f5 0a8aa394 15e7b472
Apr 25, 21:09:57  Debug    IKE  d0d231d9 42b918ba 44cf4a54 63e61d5a
Apr 25, 21:09:57  Debug    IKE  KEYMAT compute with
Apr 25, 21:09:57  Debug    IKE  71adbf7d acd83309 ea3759a1 f51f264f 2c6818f6 f45af36d 12ff532a 9defcbec
Apr 25, 21:09:57  Debug    IKE  4fa8f50d 275e0087 8290df42 46973f2d ed55b771 9ea98985 2bfb18b0 411cf29b
Apr 25, 21:09:57  Debug    IKE  79823f4e f33e0dbb fe044ece 13bbf2a4 f4a16bff 7482b3c4 15d0c2a8 c410c4cb
Apr 25, 21:09:57  Debug    IKE  03a60e00 10bc6ce3 4c176ecb 56d499cb 70260dcd 0447d1b3 5e54951f 8d3ce918
Apr 25, 21:09:57  Debug    IKE  2f55a589 cab21e7d a3
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  encklen=192 authklen=160
Apr 25, 21:09:57  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 25, 21:09:57  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  f29525d1 d9918b5e 0adeaae1 c25705d0 f71623f9 243cab8f 93ddccec 4101084b
Apr 25, 21:09:57  Debug    IKE  dab411ec 92f9986d 83a3cfcc 64852808 c521650d 67fefaff c47d3dfc 6a40eda2
Apr 25, 21:09:57  Debug    IKE  f1f1b145 608d273e d69e7ec1 8eddb773
Apr 25, 21:09:57  Debug    IKE  KEYMAT computed.
Apr 25, 21:09:57  Debug    IKE  call pk_sendupdate
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  call pfkey_send_update_nat
Apr 25, 21:09:57  Debug    IKE  pfkey update sent.
Apr 25, 21:09:57  Debug    APP  Received SADB message type UPDATE, 192.168.215.231 [0] -> 192.168.215.3 [0]
Apr 25, 21:09:57  Debug    APP  SA change detected
Apr 25, 21:09:57  Debug    IKE  encryption(3des)
Apr 25, 21:09:57  Debug    IKE  hmac(hmac_sha1)
Apr 25, 21:09:57  Debug    IKE  call pfkey_send_add_nat
Apr 25, 21:09:57  Debug    APP  Received SADB message type ADD, 192.168.215.3 [0] -> 192.168.215.231 [0]
Apr 25, 21:09:57  Debug    APP  SA change detected
Apr 25, 21:09:57  Debug    APP  Connection D-Link DI-804HV is up
Apr 25, 21:09:57  Debug    IKE  pfkey add sent.
Apr 25, 21:09:57  Debug    IKE  get pfkey UPDATE message
Apr 25, 21:09:57  Debug    IKE  02020003 14000000 f7000000 f1150000 02000100 002598dc 04000202 00000000
Apr 25, 21:09:57  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d7e7
Apr 25, 21:09:57  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d703 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  04000300 00000000 00000000 00000000 58020000 00000000 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  04000400 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.231[0]->192.168.215.3[0]
spi=2463964(0x2598dc)
```

```
Apr 25, 21:09:57  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.231[0]->192.168.215.3[0]
spi=2463964(0x2598dc)
Apr 25, 21:09:57  Debug    IKE  ===
Apr 25, 21:09:57  Debug    IKE  get pfkey ADD message
Apr 25, 21:09:57  Debug    IKE  02030003 14000000 f7000000 f1150000 02000100 a60e0010 04000202 00000000
Apr 25, 21:09:57  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d703
Apr 25, 21:09:57  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e7 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  04000300 00000000 00000000 00000000 58020000 00000000 00000000 00000000
Apr 25, 21:09:57  Debug    IKE  04000400 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
Apr 25, 21:09:57  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.3[0]->192.168.215.231[0]
spi=2785935376(0xa60e0010)
Apr 25, 21:09:57  Debug    IKE  ===
```