
# IPSecuritas 3.x

## Configuration Instructions

for

## Netgear FVS318v3


June 17, 2009

## Legal Disclaimer

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

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

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

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

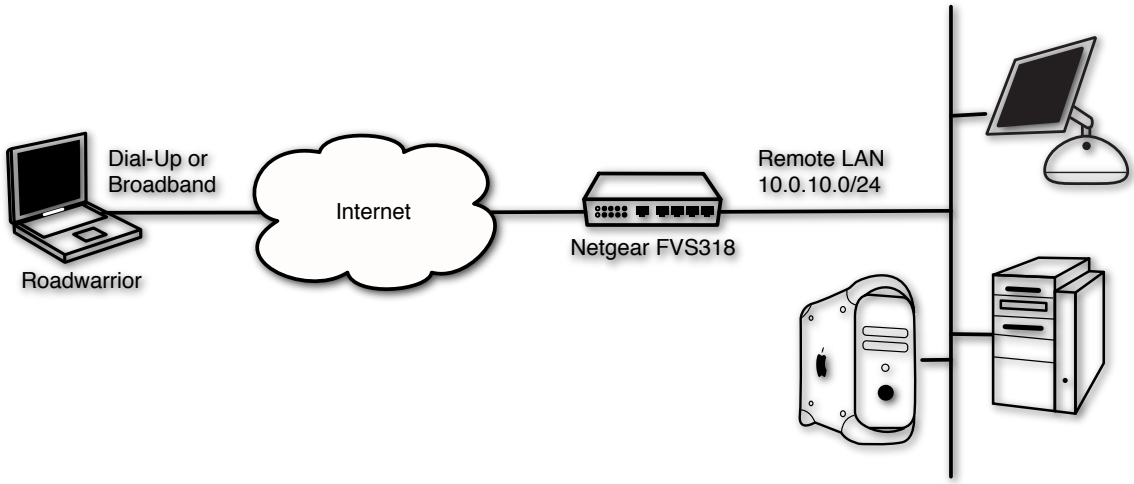
## Acknowledgments

Many thanks to Stefan Wowereit for providing setup information, screenshots and support for writing this document.

# Table of contents

# Introduction

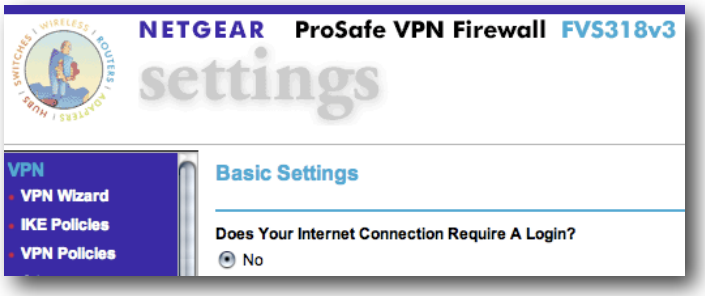
This document describes the steps necessary to establish a protected VPN connection between a Mac client and a Netgear FVS318 router/firewall. All information in this document is based on the following assumed network.




# Netgear FVS318 Wizard Setup

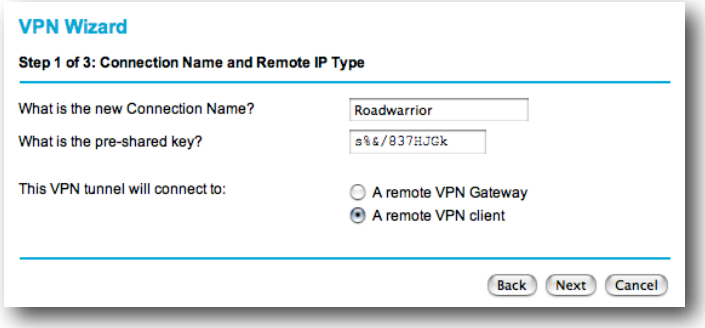
This section describes the necessary steps to setup the FVS318 to accept incoming connections.

## Start VPN Wizard




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

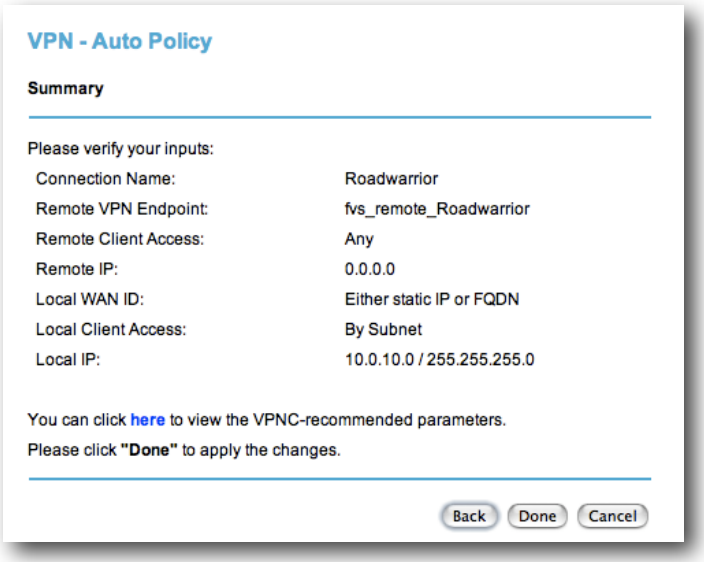
## Enter Name and Preshared Key




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

Click on **Next**.

### Finish the Wizard



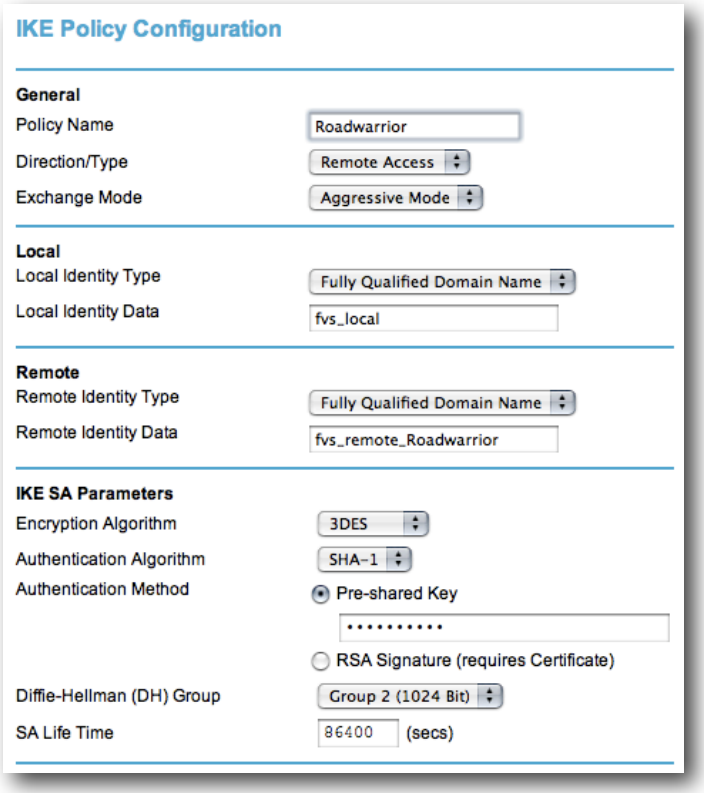

Check if all of your information is correct. The Local IP should correspond to your local LAN address.

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

## Netgear FVS318 Manual Setup

This section describes the manual setup of the FVS318 in case you don't want to use the VPN wizard. Please keep in mind that the seetings in IPSecuritas also need to be adjusted in case your manual settings differ from the one described here.

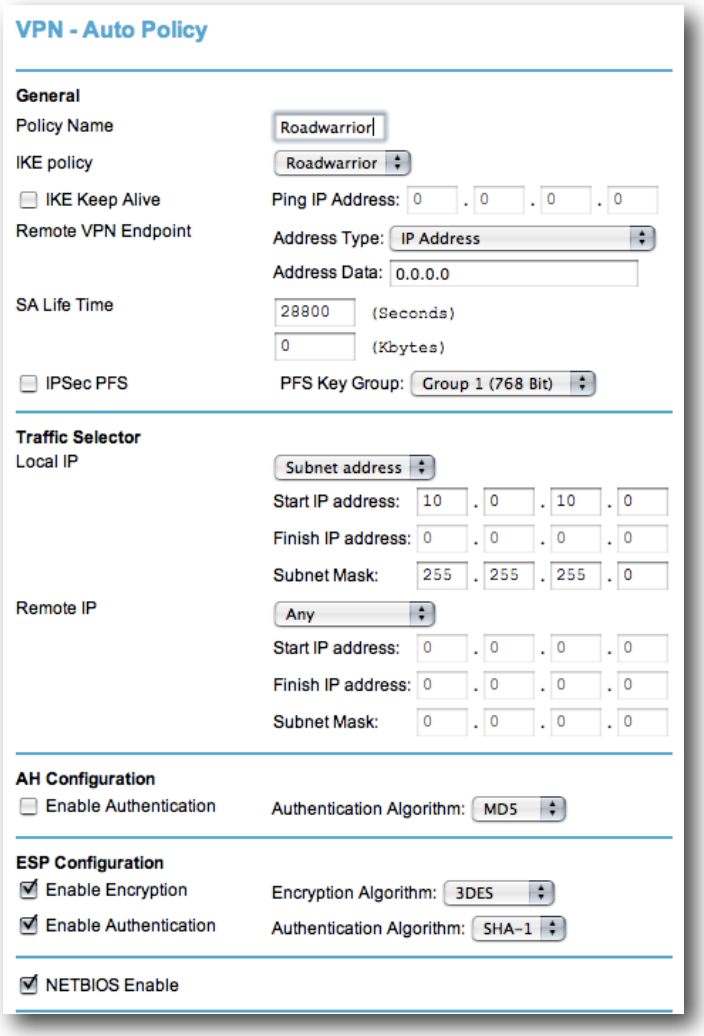
### IKE Policy




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

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

### VPN Policy




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

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

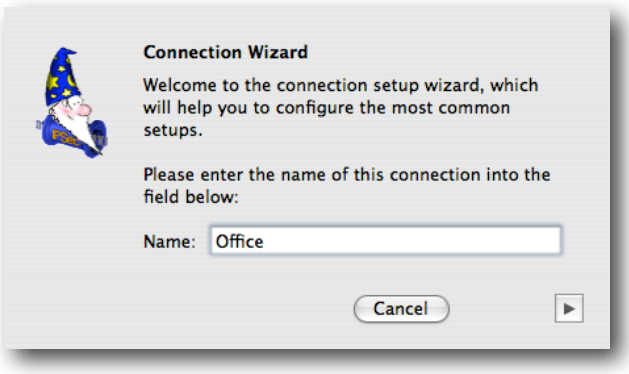
## IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the FVS318 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: 

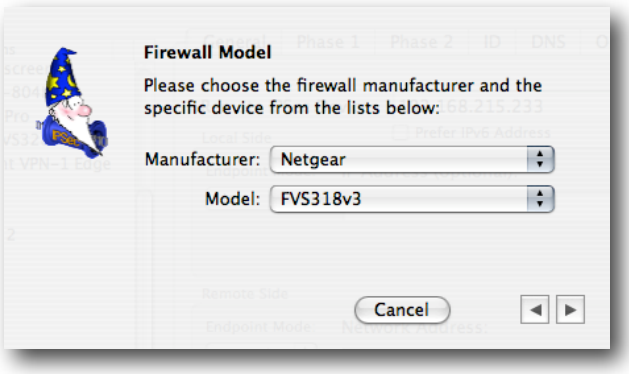
## Enter Name of New Connection




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

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

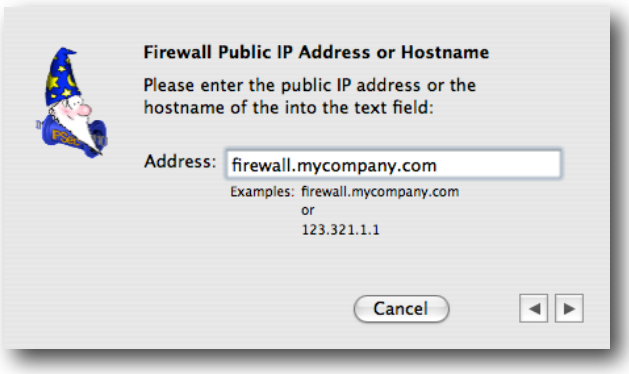
## Select Router Model




Select **Netgear** from the manufacturer list and **FVS318** from the model list.

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

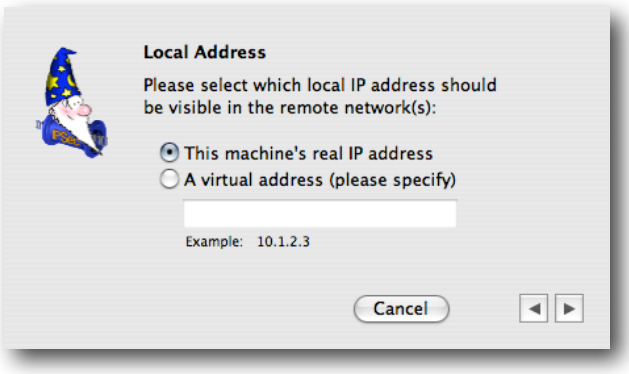
## Enter Router's Public IP Address




Enter the public IP address or hostname of your Netgear FVS318 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.

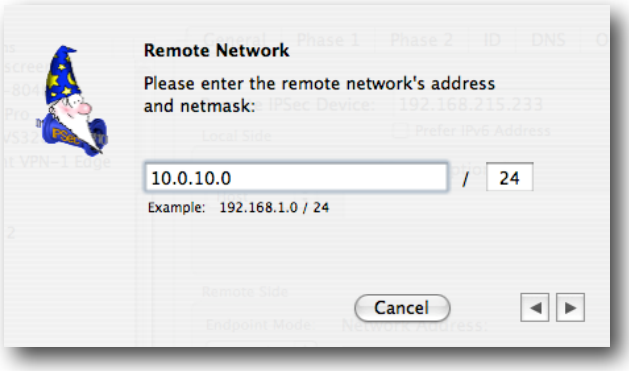
## Enter a Virtual IP Address




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.

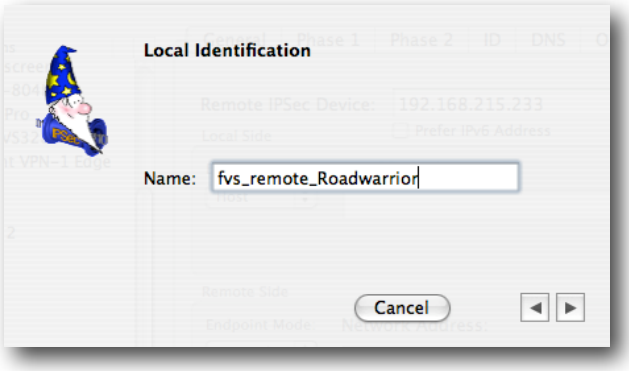
## Enter Remote Network




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 FVS318.

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

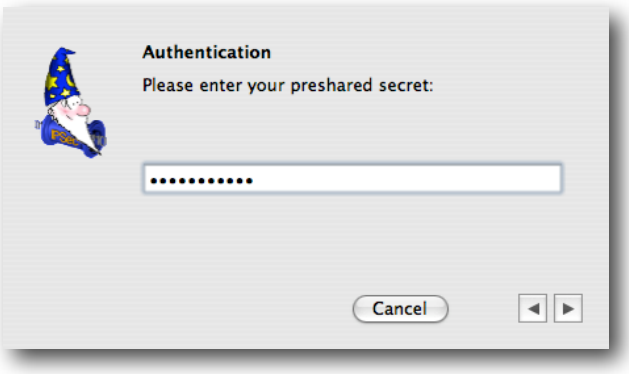
## Enter Remote Identification




Enter the FVS318's remote identification (which is **fvs_remote_Roadwarrior** by default if you used the FVS318 VPN wizard with the connection name **Roadwarrior** as described above).

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

### Enter Preshared Key




Enter the same **Preshared Key** that you used for the FVS318.

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 FVS318 **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 FVS318 Log Output

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

```
[2000-01-01 00:28:14]<POLICY: Roadwarrior> PAYLOADS: HASH,DEL
[2000-01-01 00:28:14]<POLICY: Roadwarrior> PAYLOADS: HASH,DEL
[2000-01-01 00:28:14]**** SENT OUT INFORMATIONAL EXCHANGE MESSAGE ****
[2000-01-01 00:28:14]<POLICY: Roadwarrior> PAYLOADS: HASH,DEL
[2000-01-01 00:28:14]**** RECEIVED  THIRD MESSAGE OF QUICK MODE ****
[2000-01-01 00:28:14]<POLICY: Roadwarrior> PAYLOADS: HASH
[2000-01-01 00:28:14]**** QUICK MODE COMPLETED ****
[2000-01-01 00:28:14][==== IKE PHASE 2 ESTABLISHED====]
[2000-01-01 00:28:14]**** RECEIVED  THIRD MESSAGE OF QUICK MODE ****
[2000-01-01 00:28:14]<POLICY: Roadwarrior> PAYLOADS: HASH
[2000-01-01 00:28:14]**** QUICK MODE COMPLETED ****
[2000-01-01 00:28:14][==== IKE PHASE 2 ESTABLISHED====]
```

### Sample IPSecuritas Log Output

The following is a sample log file from the FVS318 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 29, 22:07:53  Debug    APP  State change from IDLE to AUTHENTICATING after event START
Apr 29, 22:07:54  Info     APP  IKE daemon started
Apr 29, 22:07:54  Info     APP  IPSec started
Apr 29, 22:07:54  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
Apr 29, 22:07:54  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Apr 29, 22:07:54  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Apr 29, 22:07:54  Info     IKE  Foreground mode.
Apr 29, 22:07:54  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
```

```
Apr 29, 22:07:54  Info    IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
Apr 29, 22:07:54  Info    IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
Apr 29, 22:07:54  Info    IKE  Resize address pool from 0 to 255
Apr 29, 22:07:54  Debug   IKE  lifetime = 86400
Apr 29, 22:07:54  Debug   IKE  lifebyte = 0
Apr 29, 22:07:54  Debug   IKE  encklen=0
Apr 29, 22:07:54  Debug   IKE  p:1 t:1
Apr 29, 22:07:54  Debug   IKE  3DES-CBC(5)
Apr 29, 22:07:54  Debug   IKE  SHA(2)
Apr 29, 22:07:54  Debug   IKE  1024-bit MODP group(2)
Apr 29, 22:07:54  Debug   IKE  pre-shared key(1)
Apr 29, 22:07:54  Debug   IKE  hmac(modp1024)
Apr 29, 22:07:54  Debug   IKE  compression algorithm can not be checked because sadb message doesn't support it.
Apr 29, 22:07:54  Debug   IKE  parse successed.
Apr 29, 22:07:54  Debug   IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
Apr 29, 22:07:54  Info    IKE  192.168.215.3[4500] used as isakmp port (fd=7)
Apr 29, 22:07:54  Info    IKE  192.168.215.3[500] used as isakmp port (fd=8)
Apr 29, 22:07:54  Debug   IKE  get pfkey X_SPDDUMP message
Apr 29, 22:07:54  Debug   IKE  02120000 0f000100 01000000 c0090000 03000500 ff180000 10020000 0a000a00
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d703 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  07001200 02000100 2a010000 00000000 28003200 0203a400 10020000 c0a8d7e9
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 10020000 c0a8d703 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  get pfkey X_SPDDUMP message
Apr 29, 22:07:54  Debug   IKE  02120000 0f000100 00000000 c0090000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 03000600 ff180000 10020000 0a000a00 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  07001200 02000200 29010000 00000000 28003200 0203a300 10020000 c0a8d703
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 10020000 c0a8d7e9 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  sub:0xbffff340: 192.168.215.3/32[0] 10.0.10.0/24[0] proto=any dir=out
Apr 29, 22:07:54  Debug   IKE  db :0x308c88: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 29, 22:07:54  Info    APP  Initiated connection Netgear FVS318v3
Apr 29, 22:07:54  Debug   IKE  get pfkey ACQUIRE message
Apr 29, 22:07:54  Debug   IKE  02060003 24000000 19010000 00000000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e9 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  1c000d00 20000000 00030000 00000000 00010008 00000000 01000000 01000000
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:07:54  Debug   IKE  80700000 00000000 00000000 00000000 00040000 00000000 0001c001 00000000
Apr 29, 22:07:54  Debug   IKE  01000000 01000000 00000000 00000000 00000000 00000000 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  80510100 00000000 80700000 00000000 00000000 00000000 000c0000 00000000
Apr 29, 22:07:54  Debug   IKE  00010001 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
Apr 29, 22:07:54  Error   IKE  inappropriate sadb acquire message passed.
Apr 29, 22:07:54  Debug   IKE  get pfkey ACQUIRE message
Apr 29, 22:07:54  Debug   IKE  02060003 14000000 fd040000 2c020000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e9 00000000 00000000
Apr 29, 22:07:54  Debug   IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 29, 22:07:54  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:07:54  Debug   IKE  80700000 00000000 00000000 00000000 02001200 02000200 29010000 00000000
Apr 29, 22:07:54  Debug   IKE  suitable outbound SP found: 192.168.215.3/32[0] 10.0.10.0/24[0] proto=any dir=out.
Apr 29, 22:07:54  Debug   IKE  sub:0xbffff31c: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 29, 22:07:54  Debug   IKE  db :0x308c88: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 29, 22:07:54  Debug   IKE  suitable inbound SP found: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in.
Apr 29, 22:07:54  Debug   IKE  new acquire 192.168.215.3/32[0] 10.0.10.0/24[0] proto=any dir=out
Apr 29, 22:07:54  Debug   IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=164:163)
Apr 29, 22:07:54  Debug   IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:07:54  Debug   IKE  in post_acquire
Apr 29, 22:07:54  Debug   IKE  configuration found for 192.168.215.233.
Apr 29, 22:07:54  Info    IKE  IPsec-SA request for 192.168.215.233 queued due to no phase1 found.
Apr 29, 22:07:54  Debug   IKE  ===
Apr 29, 22:07:54  Info    IKE  initiate new phase 1 negotiation: 192.168.215.3[500]<=>192.168.215.233[500]
Apr 29, 22:07:54  Info    IKE  begin Aggressive mode.
Apr 29, 22:07:54  Debug   IKE  new cookie:
Apr 29, 22:07:54  Debug   IKE  c98582761037a59c
Apr 29, 22:07:54  Debug   IKE  use ID type of FQDN
Apr 29, 22:07:54  Debug   IKE  compute DH's private.
Apr 29, 22:07:54  Debug   IKE  68d31852 4e26277c 15a5433c 5c01ee5d 9dbe6796 74e10ab2 275a812e 48576c94
Apr 29, 22:07:54  Debug   IKE  96bb566a b66abdbe bb63d12b eb93398a 4df8ce85 c6b3e1fc 3b66a5a3 7358803d
Apr 29, 22:07:54  Debug   IKE  5ca746fb b7ad4877 76d38a93 71564e43 77b7765e dd72e74c 340b2ee6 617dbf9e
Apr 29, 22:07:54  Debug   IKE  cfd9e040 74492152 a76a2187 801a1acb d25ff013 1f34ea7c f95e0f3b 4727fadc
Apr 29, 22:07:54  Debug   IKE  compute DH's public.
Apr 29, 22:07:54  Debug   IKE  a8929629 07406d20 89dabc0b 45132280 a4fa01af 0fea2aeb 1091c42c 15621a3e
Apr 29, 22:07:54  Debug   IKE  723d9bf1 84a676cb e1ddddd4 6a2780ba efaedae2 b2d71860 63f22c36 adfbee4a
Apr 29, 22:07:54  Debug   IKE  a2d2c0fc 6042fbe8 c88585d7 92db08b4 51bb6aa0 ad86157f e97743d6 a9ba0a93
```

```
Apr 29, 22:07:54  Debug    IKE  83a06051 374de993 46c58100 5f42e336 1f06d2e4 ee2fedd3 6ed5b834 cd54568d
Apr 29, 22:07:54  Debug    IKE  authmethod is pre-shared key
Apr 29, 22:07:54  Debug    IKE  add payload of len 52, next type 4
Apr 29, 22:07:54  Debug    IKE  add payload of len 128, next type 10
Apr 29, 22:07:54  Debug    IKE  add payload of len 16, next type 5
Apr 29, 22:07:54  Debug    IKE  add payload of len 26, next type 13
Apr 29, 22:07:54  Debug    IKE  add payload of len 20, next type 13
Apr 29, 22:07:54  Debug    IKE  add payload of len 16, next type 0
Apr 29, 22:07:54  Debug    IKE  310 bytes from 192.168.215.3[500] to 192.168.215.233[500]
Apr 29, 22:07:54  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:54  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:54  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:54  Debug    IKE  1 times of 310 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:54  Debug    IKE  c9858276 1037a59c 00000000 00000000 01100400 00000000 00000136 04000038
Apr 29, 22:07:54  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Apr 29, 22:07:54  Debug    IKE  00015180 80010005 80030001 80020002 80040002 0a000084 a8929629 07406d20
Apr 29, 22:07:54  Debug    IKE  89dabc0b 45132280 a4fa01af 0fea2aeb 1091c42c 15621a3e 723d9bf1 84a676cb
Apr 29, 22:07:54  Debug    IKE  e1ddddd4 6a2780ba efaedae2 b2d71860 63f22c36 adfbee4a a2d2c0fc 6042fbe8
Apr 29, 22:07:54  Debug    IKE  c88585d7 92db08b4 51bb6aa0 ad86157f e97743d6 a9ba0a93 83a06051 374de993
Apr 29, 22:07:54  Debug    IKE  46c58100 5f42e336 1f06d2e4 ee2fedd3 6ed5b834 cd54568d 05000014 d2239efe
Apr 29, 22:07:54  Debug    IKE  c58178ce f4d41b86 965c4310 0d00001e 02000000 6676735f 72656d6f 74655f52
Apr 29, 22:07:54  Debug    IKE  6f616477 61727269 6f720d00 00184048 b7d56ebc e88525e7 de7f00d6 c2d38000
Apr 29, 22:07:54  Debug    IKE  00000000 0014afca d71368a1 f1c96b86 96fc7757 0100
Apr 29, 22:07:54  Debug    IKE  resend phase1 packet c98582761037a59c:0000000000000000
Apr 29, 22:07:55  Info     APP  Initiated connection Netgear FVS318v3
Apr 29, 22:07:55  Debug    IKE  get pfkey ACQUIRE message
Apr 29, 22:07:55  Debug    IKE  02060003 14000000 fe040000 2c020000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:07:55  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e9 00000000 00000000
Apr 29, 22:07:55  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 29, 22:07:55  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:07:55  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 29010000 00000000
Apr 29, 22:07:55  Debug    IKE  ignore the acquire because ph2 found
Apr 29, 22:07:56  Info     APP  Initiated connection Netgear FVS318v3
Apr 29, 22:07:56  Debug    IKE  get pfkey ACQUIRE message
Apr 29, 22:07:56  Debug    IKE  02060003 14000000 ff040000 2c020000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:07:56  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e9 00000000 00000000
Apr 29, 22:07:56  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 29, 22:07:56  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:07:56  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 29010000 00000000
Apr 29, 22:07:56  Debug    IKE  suitable outbound SP found: 192.168.215.3/32[0] 10.0.10.0/24[0] proto=any dir=out.
Apr 29, 22:07:56  Debug    IKE  sub:0xbffff31c: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 29, 22:07:56  Debug    IKE  db :0x308c88: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in
Apr 29, 22:07:56  Debug    IKE  suitable inbound SP found: 10.0.10.0/24[0] 192.168.215.3/32[0] proto=any dir=in.
Apr 29, 22:07:56  Debug    IKE  new acquire 192.168.215.3/32[0] 10.0.10.0/24[0] proto=any dir=out
Apr 29, 22:07:56  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=164:163)
Apr 29, 22:07:56  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:07:56  Debug    IKE  in post_acquire
Apr 29, 22:07:56  Debug    IKE  configuration found for 192.168.215.233.
Apr 29, 22:07:56  Info     IKE  request for establishing IPsec-SA was queued due to no phase1 found.
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  269 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 01100400 00000000 0000010d 04000038
Apr 29, 22:07:57  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Apr 29, 22:07:57  Debug    IKE  00015180 80010005 80030001 80020002 80040002 0a000084 9e648451 f86dec2f
Apr 29, 22:07:57  Debug    IKE  7dfd3271 a76cf978 e7aeba4e 76d06781 8b6da95d cef9fb37 f2f2c49f ea920789
Apr 29, 22:07:57  Debug    IKE  30c963d1 b50272b8 c6fdccc1 66ae7dd6 ce688296 a8c6d323 b664651b fa152ae8
Apr 29, 22:07:57  Debug    IKE  a6e5f746 30cb7a13 3dd4319f b92f6abc b590558d d477a9fd 8dc55445 89fcc232
Apr 29, 22:07:57  Debug    IKE  66e393b5 93e2d944 ab596ee3 fe7008b3 007ffcc8 e1bb0842 0500000c 8ba3c67d
Apr 29, 22:07:57  Debug    IKE  b30acccd 08000011 02000000 6676735f 6c6f6361 6c000000 1839c55e 93e6040c
Apr 29, 22:07:57  Debug    IKE  c1bebe43 1734ac06 3d398086 da
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=1(sa)
Apr 29, 22:07:57  Debug    IKE  seen nptype=4(ke)
Apr 29, 22:07:57  Debug    IKE  seen nptype=10(nonce)
Apr 29, 22:07:57  Debug    IKE  seen nptype=5(id)
Apr 29, 22:07:57  Debug    IKE  seen nptype=8(hash)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Warning  IKE  No ID match.
Apr 29, 22:07:57  Debug    IKE  total SA len=52
Apr 29, 22:07:57  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Apr 29, 22:07:57  Debug    IKE  00015180 80010005 80030001 80020002 80040002
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:07:57  Debug    IKE  succeed.
```

```
Apr 29, 22:07:57  Debug    IKE  proposal #1 len=44
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  transform #1 len=36
Apr 29, 22:07:57  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Apr 29, 22:07:57  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Apr 29, 22:07:57  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Apr 29, 22:07:57  Info     APP  Initiated connection Netgear FVS318v3
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Apr 29, 22:07:57  Debug    IKE  hmac(modp1024)
Apr 29, 22:07:57  Debug    IKE  pair 1:
Apr 29, 22:07:57  Debug    IKE  0x309190: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:07:57  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
Apr 29, 22:07:57  Debug    IKE  trns#=1, trns-id=IKE
Apr 29, 22:07:57  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Apr 29, 22:07:57  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Apr 29, 22:07:57  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Apr 29, 22:07:57  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Apr 29, 22:07:57  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Apr 29, 22:07:57  Debug    IKE  Compared: DB:Peer
Apr 29, 22:07:57  Debug    IKE  (lifetime = 86400:86400)
Apr 29, 22:07:57  Debug    IKE  (lifebyte = 0:0)
Apr 29, 22:07:57  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
Apr 29, 22:07:57  Debug    IKE  (encklen = 0:0)
Apr 29, 22:07:57  Debug    IKE  hashtype = SHA:SHA
Apr 29, 22:07:57  Debug    IKE  authmethod = pre-shared key:pre-shared key
Apr 29, 22:07:57  Debug    IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
Apr 29, 22:07:57  Debug    IKE  an acceptable proposal found.
Apr 29, 22:07:57  Debug    IKE  hmac(modp1024)
Apr 29, 22:07:57  Debug    IKE  agreed on pre-shared key auth.
Apr 29, 22:07:57  Debug    IKE  compute DH's shared.
Apr 29, 22:07:57  Debug    IKE  9ae0a73d c0a1a120 fc9f0a2b d26ea525 ee0ea9e2 eedc6839 e095ff3a ddf7fb37
Apr 29, 22:07:57  Debug    IKE  b2a5beb0 c477a92b fa3fa1b6 b7d25548 94e680a4 2bdaf45c 604f8079 a5185041
Apr 29, 22:07:57  Debug    IKE  7ce926a7 a2614946 5e191baf c8766aa9 b292532e fe7c463f 0efede9f 916cc541
Apr 29, 22:07:57  Debug    IKE  0a5b7a50 b2fc1bdf e2422401 da00fa74 a834e2bd 9ce2ad85 162ff507 1555f6d2
Apr 29, 22:07:57  Info     IKE  couldn't find the proper pskey, try to get one by the peer's address.
Apr 29, 22:07:57  Debug    IKE  the psk found.
Apr 29, 22:07:57  Debug    IKE  psk: 2007-04-29 22:07:57: DEBUG2:
Apr 29, 22:07:57  Debug    IKE  77747336 6a733825 6773
Apr 29, 22:07:57  Debug    IKE  nonce 1: 2007-04-29 22:07:57: DEBUG:
Apr 29, 22:07:57  Debug    IKE  d2239efe c58178ce f4d41b86 965c4310
Apr 29, 22:07:57  Debug    IKE  nonce 2: 2007-04-29 22:07:57: DEBUG:
Apr 29, 22:07:57  Debug    IKE  8ba3c67d b30acccd
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  SKEYID computed:
Apr 29, 22:07:57  Debug    IKE  10e568e2 1b51ba8f 86ac3f39 237e1f50 aebc16b8
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  SKEYID_d computed:
Apr 29, 22:07:57  Debug    IKE  3f5b104e daeca87e 6bd2403d dad098d5 9064725e
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  SKEYID_a computed:
Apr 29, 22:07:57  Debug    IKE  8093bcf5 0910b098 4405521d 0c0e1871 d8ed99db
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  SKEYID_e computed:
Apr 29, 22:07:57  Debug    IKE  fd6663f4 c36a3ebc a8c9ac2a 2eed1589 1a3df9a8
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  compute intermediate encryption key K1
Apr 29, 22:07:57  Debug    IKE  00
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  compute intermediate encryption key K2
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5
Apr 29, 22:07:57  Debug    IKE  6acc75c2 46fe17c8 eca8b065 e0d68396 bb859aa3
Apr 29, 22:07:57  Debug    IKE  final encryption key computed:
```

```
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  IV computed:
Apr 29, 22:07:57  Debug    IKE  2af65c6b 968efc3f
Apr 29, 22:07:57  Debug    IKE  HASH received:
Apr 29, 22:07:57  Debug    IKE  39c55e93 e6040cc1 bebe4317 34ac063d 398086da
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  9e648451 f86dec2f 7dfd3271 a76cf978 e7aeba4e 76d06781 8b6da95d cef9fb37
Apr 29, 22:07:57  Debug    IKE  f2f2c49f ea920789 30c963d1 b50272b8 c6fdccc1 66ae7dd6 ce688296 a8c6d323
Apr 29, 22:07:57  Debug    IKE  b664651b fa152ae8 a6e5f746 30cb7a13 3dd4319f b92f6abc b590558d d477a9fd
Apr 29, 22:07:57  Debug    IKE  8dc55445 89fcc232 66e393b5 93e2d944 ab596ee3 fe7008b3 007ffcc8 e1bb0842
Apr 29, 22:07:57  Debug    IKE  a8929629 07406d20 89dabc0b 45132280 a4fa01af 0fea2aeb 1091c42c 15621a3e
Apr 29, 22:07:57  Debug    IKE  723d9bf1 84a676cb e1ddddd4 6a2780ba efaedae2 b2d71860 63f22c36 adfbee4a
Apr 29, 22:07:57  Debug    IKE  a2d2c0fc 6042fbe8 c88585d7 92db08b4 51bb6aa0 ad86157f e97743d6 a9ba0a93
Apr 29, 22:07:57  Debug    IKE  83a06051 374de993 46c58100 5f42e336 1f06d2e4 ee2fedd3 6ed5b834 cd54568d
Apr 29, 22:07:57  Debug    IKE  36e077fd d9e25151 c9858276 1037a59c 00000001 00000001 0000002c 01010001
Apr 29, 22:07:57  Debug    IKE  00000024 01010000 800b0001 000c0004 00015180 80010005 80030001 80020002
Apr 29, 22:07:57  Debug    IKE  80040002 02000000 6676735f 6c6f6361 6c
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH (init) computed:
Apr 29, 22:07:57  Debug    IKE  39c55e93 e6040cc1 bebe4317 34ac063d 398086da
Apr 29, 22:07:57  Debug    IKE  HASH for PSK validated.
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  generate HASH_I
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  a8929629 07406d20 89dabc0b 45132280 a4fa01af 0fea2aeb 1091c42c 15621a3e
Apr 29, 22:07:57  Debug    IKE  723d9bf1 84a676cb e1ddddd4 6a2780ba efaedae2 b2d71860 63f22c36 adfbee4a
Apr 29, 22:07:57  Debug    IKE  a2d2c0fc 6042fbe8 c88585d7 92db08b4 51bb6aa0 ad86157f e97743d6 a9ba0a93
Apr 29, 22:07:57  Debug    IKE  83a06051 374de993 46c58100 5f42e336 1f06d2e4 ee2fedd3 6ed5b834 cd54568d
Apr 29, 22:07:57  Debug    IKE  9e648451 f86dec2f 7dfd3271 a76cf978 e7aeba4e 76d06781 8b6da95d cef9fb37
Apr 29, 22:07:57  Debug    IKE  f2f2c49f ea920789 30c963d1 b50272b8 c6fdccc1 66ae7dd6 ce688296 a8c6d323
Apr 29, 22:07:57  Debug    IKE  b664651b fa152ae8 a6e5f746 30cb7a13 3dd4319f b92f6abc b590558d d477a9fd
Apr 29, 22:07:57  Debug    IKE  8dc55445 89fcc232 66e393b5 93e2d944 ab596ee3 fe7008b3 007ffcc8 e1bb0842
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 00000001 00000001 0000002c 01010001
Apr 29, 22:07:57  Debug    IKE  00000024 01010000 800b0001 000c0004 00015180 80010005 80030001 80020002
Apr 29, 22:07:57  Debug    IKE  80040002 02000000 6676735f 72656d6f 74655f52 6f616477 61727269 6f72
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH (init) computed:
Apr 29, 22:07:57  Debug    IKE  00b9ae66 0ca60dfa d7575936 f53a1d22 fcd75fc3
Apr 29, 22:07:57  Debug    IKE  add payload of len 20, next type 0
Apr 29, 22:07:57  Debug    IKE  52 bytes from 192.168.215.3[500] to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  1 times of 52 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08100400 00000000 00000034 00000018
Apr 29, 22:07:57  Debug    IKE  00b9ae66 0ca60dfa d7575936 f53a1d22 fcd75fc3
Apr 29, 22:07:57  Debug    IKE  compute IV for phase2
Apr 29, 22:07:57  Debug    IKE  phase1 last IV:
Apr 29, 22:07:57  Debug    IKE  2af65c6b 968efc3f afd64e51
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  phase2 IV computed:
Apr 29, 22:07:57  Debug    IKE  55a6ad91 f706c647
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  afd64e51 0000001c 00000001 01106002 c9858276 1037a59c 36e077fd d9e25151
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  366ade3d 136cf48a 4f8448cf 652b9978 b1b27ed8
Apr 29, 22:07:57  Debug    IKE  begin encryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  pad length = 4
Apr 29, 22:07:57  Debug    IKE  0b000018 366ade3d 136cf48a 4f8448cf 652b9978 b1b27ed8 0000001c 00000001
Apr 29, 22:07:57  Debug    IKE  01106002 c9858276 1037a59c 36e077fd d9e25151 00000004
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  encrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  55a6ad91 f706c647
Apr 29, 22:07:57  Debug    IKE  save IV for next:
Apr 29, 22:07:57  Debug    IKE  7a8d5918 0993ba09
Apr 29, 22:07:57  Debug    IKE  encrypted.
Apr 29, 22:07:57  Debug    IKE  84 bytes from 192.168.215.3[500] to 192.168.215.233[500]
```

```
Apr 29, 22:07:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08100501 afd64e51 00000054 c3a6cab2
Apr 29, 22:07:57  Debug    IKE  cb4a4b28 b0baa63c b42b56d9 197e53bd 11643566 36476b33 cbb85da8 94f0c4d9
Apr 29, 22:07:57  Debug    IKE  1800f025 258a9153 96e8ba2c 7a8d5918 0993ba09
Apr 29, 22:07:57  Debug    IKE  sendto Information notify.
Apr 29, 22:07:57  Debug    IKE  IV freed
Apr 29, 22:07:57  Info     IKE  ISAKMP-SA established 192.168.215.3[500]-192.168.215.233[500] spi:c98582761037a59c:
36e077fdd9e25151
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  begin QUICK mode.
Apr 29, 22:07:57  Info     IKE  initiate new phase 2 negotiation: 192.168.215.3[500]<=>192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  compute IV for phase2
Apr 29, 22:07:57  Debug    IKE  phase1 last IV:
Apr 29, 22:07:57  Debug    IKE  2af65c6b 968efc3f fb200e51
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  phase2 IV computed:
Apr 29, 22:07:57  Debug    IKE  6d36543a 7ef81008
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_getspi
Apr 29, 22:07:57  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.233[0]->192.168.215.3[0]
Apr 29, 22:07:57  Debug    IKE  pfkey getspi sent.
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  begin QUICK mode.
Apr 29, 22:07:57  Info     IKE  initiate new phase 2 negotiation: 192.168.215.3[500]<=>192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  compute IV for phase2
Apr 29, 22:07:57  Debug    IKE  phase1 last IV:
Apr 29, 22:07:57  Debug    IKE  2af65c6b 968efc3f c2ab803e
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  phase2 IV computed:
Apr 29, 22:07:57  Debug    IKE  9fd9c245 9fcec0a0
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_getspi
Apr 29, 22:07:57  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.233[0]->192.168.215.3[0]
Apr 29, 22:07:57  Debug    IKE  pfkey getspi sent.
Apr 29, 22:07:57  Debug    IKE  get pfkey ACQUIRE message
Apr 29, 22:07:57  Debug    IKE  02060003 14000000 00050000 2c020000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:07:57  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e9 00000000 00000000
Apr 29, 22:07:57  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 29, 22:07:57  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:07:57  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 29010000 00000000
Apr 29, 22:07:57  Debug    IKE  ignore the acquire because ph2 found
Apr 29, 22:07:57  Debug    IKE  get pfkey GETSPI message
Apr 29, 22:07:57  Debug    IKE  02010003 0a000000 ff040000 c0090000 02000100 05c299b4 32392032 323a3037
Apr 29, 22:07:57  Debug    IKE  03000500 ff200000 10020000 c0a8d7e9 00000000 00000000 03000600 ff200000
Apr 29, 22:07:57  Debug    IKE  10020000 c0a8d703 00000000 00000000
Apr 29, 22:07:57  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.233[0]->192.168.215.3[0]
spi=96639412(0x5c299b4)
Apr 29, 22:07:57  Debug    IKE  use local ID type IPv4_address
Apr 29, 22:07:57  Debug    IKE  use remote ID type IPv4_subnet
Apr 29, 22:07:57  Debug    IKE  IDci:
Apr 29, 22:07:57  Debug    IKE  01000000 c0a8d703
Apr 29, 22:07:57  Debug    IKE  IDcr:
Apr 29, 22:07:57  Debug    IKE  04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  add payload of len 44, next type 10
Apr 29, 22:07:57  Debug    IKE  add payload of len 16, next type 5
Apr 29, 22:07:57  Debug    IKE  add payload of len 8, next type 5
Apr 29, 22:07:57  Debug    IKE  add payload of len 12, next type 0
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  fb200e51 0a000030 00000001 00000001 00000024 01030401 05c299b4 00000018
Apr 29, 22:07:57  Debug    IKE  01030000 80010001 80027080 80040001 80050002 05000014 9a674412 a9d4bc2a
Apr 29, 22:07:57  Debug    IKE  6a8df285 c0986d83 0500000c 01000000 c0a8d703 00000010 04000000 0a000a00
Apr 29, 22:07:57  Debug    IKE  ffffff00
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  1b4f55a9 83f6f353 e3e46064 b57a9f4b 31b2096a
Apr 29, 22:07:57  Debug    IKE  add payload of len 20, next type 1
Apr 29, 22:07:57  Debug    IKE  begin encryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  pad length = 8
Apr 29, 22:07:57  Debug    IKE  01000018 1b4f55a9 83f6f353 e3e46064 b57a9f4b 31b2096a 0a000030 00000001
```

```
Apr 29, 22:07:57  Debug    IKE  00000001 00000024 01030401 05c299b4 00000018 01030000 80010001 80027080
Apr 29, 22:07:57  Debug    IKE  80040001 80050002 05000014 9a674412 a9d4bc2a 6a8df285 c0986d83 0500000c
Apr 29, 22:07:57  Debug    IKE  01000000 c0a8d703 00000010 04000000 0a000a00 ffffff00 00000000 00000008
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  encrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  6d36543a 7ef81008
Apr 29, 22:07:57  Debug    IKE  save IV for next:
Apr 29, 22:07:57  Debug    IKE  200fb6f5 0049393c
Apr 29, 22:07:57  Debug    IKE  encrypted.
Apr 29, 22:07:57  Debug    IKE  156 bytes from 192.168.215.3[500] to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  1 times of 156 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000009c f1e4e175
Apr 29, 22:07:57  Debug    IKE  69f0a1c0 ef4db980 1f6c5396 393fbf3b 2edf81aa e72f89f3 d1ec0807 6a1feefb
Apr 29, 22:07:57  Debug    IKE  41c43d69 780893c2 0ff7a74e be663eb5 bd9ad568 1b5ae78f 401c4709 7c561ef8
Apr 29, 22:07:57  Debug    IKE  2e155108 134e880e e53b3d4f 2bb9148f ae2b3db2 a1bc4fdb c747d7e7 aa918b16
Apr 29, 22:07:57  Debug    IKE  e662881e 8e8a84f1 d9c02e6d c2b784b9 7c556b4f 200fb6f5 0049393c
Apr 29, 22:07:57  Debug    IKE  resend phase2 packet c98582761037a59c:36e077fdd9e25151:0000fb20
Apr 29, 22:07:57  Debug    IKE  get pfkey GETSPI message
Apr 29, 22:07:57  Debug    IKE  02010003 0a000000 fd040000 c0090000 02000100 03ae91d5 27010000 00000000
Apr 29, 22:07:57  Debug    IKE  03000500 ff200000 10020000 c0a8d7e9 00000000 00000000 03000600 ff200000
Apr 29, 22:07:57  Debug    IKE  10020000 c0a8d703 00000000 00000000
Apr 29, 22:07:57  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.233[0]->192.168.215.3[0]
spi=61772245(0x3ae91d5)
Apr 29, 22:07:57  Debug    IKE  use local ID type IPv4_address
Apr 29, 22:07:57  Debug    IKE  use remote ID type IPv4_subnet
Apr 29, 22:07:57  Debug    IKE  IDci:
Apr 29, 22:07:57  Debug    IKE  01000000 c0a8d703
Apr 29, 22:07:57  Debug    IKE  IDcr:
Apr 29, 22:07:57  Debug    IKE  04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  add payload of len 44, next type 10
Apr 29, 22:07:57  Debug    IKE  add payload of len 16, next type 5
Apr 29, 22:07:57  Debug    IKE  add payload of len 8, next type 5
Apr 29, 22:07:57  Debug    IKE  add payload of len 12, next type 0
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  c2ab803e 0a000030 00000001 00000001 00000024 01030401 03ae91d5 00000018
Apr 29, 22:07:57  Debug    IKE  01030000 80010001 80027080 80040001 80050002 05000014 9b9dcb8c f7164b63
Apr 29, 22:07:57  Debug    IKE  cd3c4d1b e64b66a5 0500000c 01000000 c0a8d703 00000010 04000000 0a000a00
Apr 29, 22:07:57  Debug    IKE  ffffff00
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  490fd66f 8398cbe7 cd8f9676 2bfd410f decbf9a0
Apr 29, 22:07:57  Debug    IKE  add payload of len 20, next type 1
Apr 29, 22:07:57  Debug    IKE  begin encryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  pad length = 8
Apr 29, 22:07:57  Debug    IKE  01000018 490fd66f 8398cbe7 cd8f9676 2bfd410f decbf9a0 0a000030 00000001
Apr 29, 22:07:57  Debug    IKE  00000001 00000024 01030401 03ae91d5 00000018 01030000 80010001 80027080
Apr 29, 22:07:57  Debug    IKE  80040001 80050002 05000014 9b9dcb8c f7164b63 cd3c4d1b e64b66a5 0500000c
Apr 29, 22:07:57  Debug    IKE  01000000 c0a8d703 00000010 04000000 0a000a00 ffffff00 00000000 00000008
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  encrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  9fd9c245 9fcec0a0
Apr 29, 22:07:57  Debug    IKE  save IV for next:
Apr 29, 22:07:57  Debug    IKE  6536af2a 68134586
Apr 29, 22:07:57  Debug    IKE  encrypted.
Apr 29, 22:07:57  Debug    IKE  156 bytes from 192.168.215.3[500] to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  1 times of 156 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000009c be154cf4
Apr 29, 22:07:57  Debug    IKE  9bbbdd11 87fe1efb b33b8a19 c21fc6c2 99504a6c 61b9632a 98a6ea18 b710cc8d
Apr 29, 22:07:57  Debug    IKE  8bf32a67 bc5194da 3b873857 3e5747c2 f393e4c8 b7555238 104273e5 9ae92f41
Apr 29, 22:07:57  Debug    IKE  ee6adebf 707c5b59 3ecd7507 271863d8 0e47c2b1 dcb9501a 88c9a85e 47a38cf8
Apr 29, 22:07:57  Debug    IKE  7fe1d8c0 d8a562e1 6563a184 86e9e041 59bfe4ff 6536af2a 68134586
Apr 29, 22:07:57  Debug    IKE  resend phase2 packet c98582761037a59c:36e077fdd9e25151:0000c2ab
Apr 29, 22:07:57  Debug    IKE  ===
```

```
Apr 29, 22:07:57  Debug    IKE  140 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000008c 98f29cf1
Apr 29, 22:07:57  Debug    IKE  655c7078 ce3cdd2a b8d60813 b6fa46bf f7007966 cc1bb4ed da3e1651 c88d6143
Apr 29, 22:07:57  Debug    IKE  c2585e92 6cd1e701 b986bcd7 885a4ad8 dbf2b69c 601e5976 1ff5cc1a 7c399fdb
Apr 29, 22:07:57  Debug    IKE  2ffbedef e98e14e7 c1347a30 5cf35a7d ab977b24 58e9e635 7a62f843 1381baea
Apr 29, 22:07:57  Debug    IKE  2682a4c5 4ad63659 fbdfd676
Apr 29, 22:07:57  Debug    IKE  begin decryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  IV was saved for next processing:
Apr 29, 22:07:57  Debug    IKE  4ad63659 fbdfd676
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  decrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  200fb6f5 0049393c
Apr 29, 22:07:57  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:07:57  Debug    IKE  01000018 46580473 ebb09ade 842e0457 b5bb753a 48f840e6 0a000030 00000001
Apr 29, 22:07:57  Debug    IKE  00000001 00000024 01030401 89dc3936 00000018 01030000 80010001 80027080
Apr 29, 22:07:57  Debug    IKE  80040001 80050002 0500000c a135cb6c d9a0c880 0500000c 01000000 c0a8d703
Apr 29, 22:07:57  Debug    IKE  00000010 04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  padding len=0
Apr 29, 22:07:57  Debug    IKE  skip to trim padding.
Apr 29, 22:07:57  Debug    IKE  decrypted.
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000008c 01000018
Apr 29, 22:07:57  Debug    IKE  46580473 ebb09ade 842e0457 b5bb753a 48f840e6 0a000030 00000001 00000001
Apr 29, 22:07:57  Debug    IKE  00000024 01030401 89dc3936 00000018 01030000 80010001 80027080 80040001
Apr 29, 22:07:57  Debug    IKE  80050002 0500000c a135cb6c d9a0c880 0500000c 01000000 c0a8d703 00000010
Apr 29, 22:07:57  Debug    IKE  04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=8(hash)
Apr 29, 22:07:57  Debug    IKE  seen nptype=1(sa)
Apr 29, 22:07:57  Debug    IKE  seen nptype=10(nonce)
Apr 29, 22:07:57  Debug    IKE  seen nptype=5(id)
Apr 29, 22:07:57  Debug    IKE  seen nptype=5(id)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  HASH allocated:hbuf->l=128 actual:tlen=104
Apr 29, 22:07:57  Debug    IKE  HASH(2) received:2007-04-29 22:07:57: DEBUG:
Apr 29, 22:07:57  Debug    IKE  46580473 ebb09ade 842e0457 b5bb753a 48f840e6
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  fb200e51 9a674412 a9d4bc2a 6a8df285 c0986d83 0a000030 00000001 00000001
Apr 29, 22:07:57  Debug    IKE  00000024 01030401 89dc3936 00000018 01030000 80010001 80027080 80040001
Apr 29, 22:07:57  Debug    IKE  80050002 0500000c a135cb6c d9a0c880 0500000c 01000000 c0a8d703 00000010
Apr 29, 22:07:57  Debug    IKE  04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  46580473 ebb09ade 842e0457 b5bb753a 48f840e6
Apr 29, 22:07:57  Debug    IKE  total SA len=44
Apr 29, 22:07:57  Debug    IKE  00000001 00000001 00000024 01030401 05c299b4 00000018 01030000 80010001
Apr 29, 22:07:57  Debug    IKE  80027080 80040001 80050002
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  proposal #1 len=36
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  transform #1 len=24
Apr 29, 22:07:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
Apr 29, 22:07:57  Debug    IKE  life duration was in TLV.
Apr 29, 22:07:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:07:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:07:57  Debug    IKE  pair 1:
Apr 29, 22:07:57  Debug    IKE  0x309590: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:07:57  Debug    IKE  total SA len=44
Apr 29, 22:07:57  Debug    IKE  00000001 00000001 00000024 01030401 89dc3936 00000018 01030000 80010001
Apr 29, 22:07:57  Debug    IKE  80027080 80040001 80050002
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  proposal #1 len=36
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=3(trns)
```

```
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  transform #1 len=24
Apr 29, 22:07:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
Apr 29, 22:07:57  Debug    IKE  life duration was in TLV.
Apr 29, 22:07:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:07:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:07:57  Debug    IKE  pair 1:
Apr 29, 22:07:57  Debug    IKE  0x309580: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:07:57  Debug    IKE  begin compare proposals.
Apr 29, 22:07:57  Debug    IKE  pair[1]: 0x309580
Apr 29, 22:07:57  Debug    IKE  0x309580: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Apr 29, 22:07:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
Apr 29, 22:07:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:07:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:07:57  Debug    IKE  peer's single bundle:
Apr 29, 22:07:57  Debug    IKE  (proto_id=ESP spisize=4 spi=89dc3936 spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 29, 22:07:57  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:07:57  Debug    IKE  my single bundle:
Apr 29, 22:07:57  Debug    IKE  (proto_id=ESP spisize=4 spi=05c299b4 spi_p=00000000 encmode=Tunnel reqid=164:163)
Apr 29, 22:07:57  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:07:57  Debug    IKE  matched
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  HASH(3) generate
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  00fb200e 519a6744 12a9d4bc 2a6a8df2 85c0986d 83a135cb 6cd9a0c8 80
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  58952023 1e4e3dbe 910abcbf ca868651 df580779
Apr 29, 22:07:57  Debug    IKE  add payload of len 20, next type 0
Apr 29, 22:07:57  Debug    IKE  begin encryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  pad length = 8
Apr 29, 22:07:57  Debug    IKE  00000018 58952023 1e4e3dbe 910abcbf ca868651 df580779 00000000 00000008
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  encrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  4ad63659 fbdfd676
Apr 29, 22:07:57  Debug    IKE  save IV for next:
Apr 29, 22:07:57  Debug    IKE  a01651c9 f7dbfa84
Apr 29, 22:07:57  Debug    IKE  encrypted.
Apr 29, 22:07:57  Debug    IKE  60 bytes from 192.168.215.3[500] to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000003c 67f8e2e9
Apr 29, 22:07:57  Debug    IKE  191d2508 eaa5eba5 e495ab4b 7311a4fc 479d3be1 a01651c9 f7dbfa84
Apr 29, 22:07:57  Debug    IKE  KEYMAT compute with
Apr 29, 22:07:57  Debug    IKE  0305c299 b49a6744 12a9d4bc 2a6a8df2 85c0986d 83a135cb 6cd9a0c8 80
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encklen=192 authklen=160
Apr 29, 22:07:57  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 29, 22:07:57  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  f7acca85 0d82cd36 088364f4 fd40e470 410d460e 889bc7a1 2332804f b119dd02
Apr 29, 22:07:57  Debug    IKE  a32827fb 96ec8c39 2828a84d 8a0247ff 78e718c6 71061189 5b5cbeaa 52343d24
Apr 29, 22:07:57  Debug    IKE  6a965fea ef238e2f 16bcf096 a755bfc7
Apr 29, 22:07:57  Debug    IKE  KEYMAT compute with
Apr 29, 22:07:57  Debug    IKE  0389dc39 369a6744 12a9d4bc 2a6a8df2 85c0986d 83a135cb 6cd9a0c8 80
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encklen=192 authklen=160
Apr 29, 22:07:57  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 29, 22:07:57  Debug    IKE  generating K1...K4 for KEYMAT.
```

```
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  c138833a 06c63071 c167be98 7819fffb 59a787c6 f445005e d922a971 3a9f60e4
Apr 29, 22:07:57  Debug    IKE  3b154179 b862a401 bd78b5a1 2852780e f59cdf42 2f21536d f7fec970 c2bc192f
Apr 29, 22:07:57  Debug    IKE  afe59061 7e25fa84 a3cb99b4 342dac65
Apr 29, 22:07:57  Debug    IKE  KEYMAT computed.
Apr 29, 22:07:57  Debug    IKE  call pk_sendupdate
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_update_nat
Apr 29, 22:07:57  Debug    APP  Received SADB message type UPDATE, 192.168.215.233 [0] -> 192.168.215.3 [0]
Apr 29, 22:07:57  Debug    APP  SA change detected
Apr 29, 22:07:57  Debug    IKE  pfkey update sent.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_add_nat
Apr 29, 22:07:57  Debug    APP  Received SADB message type ADD, 192.168.215.3 [0] -> 192.168.215.233 [0]
Apr 29, 22:07:57  Debug    APP  SA change detected
Apr 29, 22:07:57  Debug    APP  Connection Netgear FVS318v3 is up
Apr 29, 22:07:57  Debug    IKE  pfkey add sent.
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  140 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000008c 71e585cf
Apr 29, 22:07:57  Debug    IKE  e71c0321 cd5249ff ac6d80f0 7cb5acb0 aba1da6e 09e05b4d 9cfa163d d4f5287d
Apr 29, 22:07:57  Debug    IKE  5998baab 4a409d6a d0cee19e 726ad237 6c60a7cc 5d05a261 af703a5e fe7befa5
Apr 29, 22:07:57  Debug    IKE  7c685bde fe996ea7 5f55f537 9e74ef11 245b791e 101e054a 53427a42 12d4b4bc
Apr 29, 22:07:57  Debug    IKE  2260e15f c7223b1e 90ecc8e3
Apr 29, 22:07:57  Debug    IKE  begin decryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  IV was saved for next processing:
Apr 29, 22:07:57  Debug    IKE  c7223b1e 90ecc8e3
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  decrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  6536af2a 68134586
Apr 29, 22:07:57  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:07:57  Debug    IKE  01000018 f1439e61 91e92b55 a30b821b 601cea08 e99d6344 0a000030 00000001
Apr 29, 22:07:57  Debug    IKE  00000001 00000024 01030401 82858ecd 00000018 01030000 80010001 80027080
Apr 29, 22:07:57  Debug    IKE  80040001 80050002 0500000c ab6e6275 89be7ad8 0500000c 01000000 c0a8d703
Apr 29, 22:07:57  Debug    IKE  00000010 04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  padding len=0
Apr 29, 22:07:57  Debug    IKE  skip to trim padding.
Apr 29, 22:07:57  Debug    IKE  decrypted.
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000008c 01000018
Apr 29, 22:07:57  Debug    IKE  f1439e61 91e92b55 a30b821b 601cea08 e99d6344 0a000030 00000001 00000001
Apr 29, 22:07:57  Debug    IKE  00000024 01030401 82858ecd 00000018 01030000 80010001 80027080 80040001
Apr 29, 22:07:57  Debug    IKE  80050002 0500000c ab6e6275 89be7ad8 0500000c 01000000 c0a8d703 00000010
Apr 29, 22:07:57  Debug    IKE  04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=8(hash)
Apr 29, 22:07:57  Debug    IKE  seen nptype=1(sa)
Apr 29, 22:07:57  Debug    IKE  seen nptype=10(nonce)
Apr 29, 22:07:57  Debug    IKE  seen nptype=5(id)
Apr 29, 22:07:57  Debug    IKE  seen nptype=5(id)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  HASH allocated:hbuf->l=128 actual:tlen=104
Apr 29, 22:07:57  Debug    IKE  HASH(2) received:2007-04-29 22:07:57: DEBUG:
Apr 29, 22:07:57  Debug    IKE  f1439e61 91e92b55 a30b821b 601cea08 e99d6344
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  c2ab803e 9b9dcb8c f7164b63 cd3c4d1b e64b66a5 0a000030 00000001 00000001
Apr 29, 22:07:57  Debug    IKE  00000024 01030401 82858ecd 00000018 01030000 80010001 80027080 80040001
Apr 29, 22:07:57  Debug    IKE  80050002 0500000c ab6e6275 89be7ad8 0500000c 01000000 c0a8d703 00000010
Apr 29, 22:07:57  Debug    IKE  04000000 0a000a00 ffffff00
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  f1439e61 91e92b55 a30b821b 601cea08 e99d6344
Apr 29, 22:07:57  Debug    IKE  total SA len=44
Apr 29, 22:07:57  Debug    IKE  00000001 00000001 00000024 01030401 03ae91d5 00000018 01030000 80010001
Apr 29, 22:07:57  Debug    IKE  80027080 80040001 80050002
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:07:57  Debug    IKE  succeed.
```

```
Apr 29, 22:07:57  Debug    IKE  proposal #1 len=36
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  transform #1 len=24
Apr 29, 22:07:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
Apr 29, 22:07:57  Debug    IKE  life duration was in TLV.
Apr 29, 22:07:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:07:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:07:57  Debug    IKE  pair 1:
Apr 29, 22:07:57  Debug    IKE  0x30a5d0: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:07:57  Debug    IKE  total SA len=44
Apr 29, 22:07:57  Debug    IKE  00000001 00000001 00000024 01030401 82858ecd 00000018 01030000 80010001
Apr 29, 22:07:57  Debug    IKE  80027080 80040001 80050002
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  proposal #1 len=36
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  transform #1 len=24
Apr 29, 22:07:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
Apr 29, 22:07:57  Debug    IKE  life duration was in TLV.
Apr 29, 22:07:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:07:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:07:57  Debug    IKE  pair 1:
Apr 29, 22:07:57  Debug    IKE  0x30a230: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:07:57  Debug    IKE  begin compare proposals.
Apr 29, 22:07:57  Debug    IKE  pair[1]: 0x30a230
Apr 29, 22:07:57  Debug    IKE  0x30a230: next=0x0 tnext=0x0
Apr 29, 22:07:57  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Apr 29, 22:07:57  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:07:57  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=28800
Apr 29, 22:07:57  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:07:57  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:07:57  Debug    IKE  peer's single bundle:
Apr 29, 22:07:57  Debug    IKE  (proto_id=ESP spisize=4 spi=82858ecd spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 29, 22:07:57  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:07:57  Debug    IKE  my single bundle:
Apr 29, 22:07:57  Debug    IKE  (proto_id=ESP spisize=4 spi=03ae91d5 spi_p=00000000 encmode=Tunnel reqid=164:163)
Apr 29, 22:07:57  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:07:57  Debug    IKE  matched
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  HASH(3) generate
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  00c2ab80 3e9b9dcb 8cf7164b 63cd3c4d 1be64b66 a5ab6e62 7589be7a d8
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  7d11e6d2 784e3158 8d1407b9 67d61f6b d7b23b95
Apr 29, 22:07:57  Debug    IKE  add payload of len 20, next type 0
Apr 29, 22:07:57  Debug    IKE  begin encryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  pad length = 8
Apr 29, 22:07:57  Debug    IKE  00000018 7d11e6d2 784e3158 8d1407b9 67d61f6b d7b23b95 00000000 00000008
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  encrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  c7223b1e 90ecc8e3
Apr 29, 22:07:57  Debug    IKE  save IV for next:
Apr 29, 22:07:57  Debug    IKE  3c702240 b394ac2b
Apr 29, 22:07:57  Debug    IKE  encrypted.
Apr 29, 22:07:57  Debug    IKE  60 bytes from 192.168.215.3[500] to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000003c 02dc470b
Apr 29, 22:07:57  Debug    IKE  b3980b8a d960a967 ff969c41 7a0cb81f 463660ed 3c702240 b394ac2b
```

```
Apr 29, 22:07:57  Debug    IKE  KEYMAT compute with
Apr 29, 22:07:57  Debug    IKE  0303ae91 d59b9dcb 8cf7164b 63cd3c4d 1be64b66 a5ab6e62 7589be7a d8
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encklen=192 authklen=160
Apr 29, 22:07:57  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 29, 22:07:57  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  d6e9616e e2bc1ffe d2bf9319 74d1c2ca c5d0bc75 e1f9eaba dac2a4e8 c2e0d94d
Apr 29, 22:07:57  Debug    IKE  1a212a6d 7f1ed4e3 0680bb27 d4666805 9bf4e6e2 cc52e925 b4ca0352 1591d12d
Apr 29, 22:07:57  Debug    IKE  73e3e7d6 15ebd0f8 d654d939 eeebf3d6
Apr 29, 22:07:57  Debug    IKE  KEYMAT compute with
Apr 29, 22:07:57  Debug    IKE  0382858e cd9b9dcb 8cf7164b 63cd3c4d 1be64b66 a5ab6e62 7589be7a d8
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  encklen=192 authklen=160
Apr 29, 22:07:57  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 29, 22:07:57  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  4c6d64dc 848802b4 e5c35cfa 22356db1 9b54c962 cbd5eb15 78362a2c 577428dc
Apr 29, 22:07:57  Debug    IKE  92a704d5 60155f54 afa8580e ee55c27a d5515e7f e2d945fd 8ccff101 932a734d
Apr 29, 22:07:57  Debug    IKE  7262296f 7e51eeb7 7f1d4c12 d2b6d923
Apr 29, 22:07:57  Debug    IKE  KEYMAT computed.
Apr 29, 22:07:57  Debug    IKE  call pk_sendupdate
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_update_nat
Apr 29, 22:07:57  Debug    APP  Received SADB message type UPDATE, 192.168.215.233 [0] -> 192.168.215.3 [0]
Apr 29, 22:07:57  Debug    APP  SA change detected
Apr 29, 22:07:57  Debug    IKE  pfkey update sent.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_add_nat
Apr 29, 22:07:57  Debug    APP  Received SADB message type ADD, 192.168.215.3 [0] -> 192.168.215.233 [0]
Apr 29, 22:07:57  Debug    APP  SA change detected
Apr 29, 22:07:57  Debug    IKE  pfkey add sent.
Apr 29, 22:07:57  Debug    IKE  get pfkey UPDATE message
Apr 29, 22:07:57  Debug    IKE  02020003 14000000 ff040000 c0090000 02000100 05c299b4 04000202 00000000
Apr 29, 22:07:57  Debug    IKE  02001300 02000000 00000000 a4000000 03000500 ff200000 10020000 c0a8d7e9
Apr 29, 22:07:57  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d703 00000000 00000000
Apr 29, 22:07:57  Debug    IKE  04000300 00000000 00000000 00000000 80700000 00000000 00000000 00000000
Apr 29, 22:07:57  Debug    IKE  04000400 00000000 00000000 00000000 005a0000 00000000 00000000 00000000
Apr 29, 22:07:57  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.233[0]->192.168.215.3[0]
spi=96639412(0x5c299b4)
Apr 29, 22:07:57  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.233[0]->192.168.215.3[0]
spi=96639412(0x5c299b4)
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  68 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08100501 ea082305 00000044 e9ad5410
Apr 29, 22:07:57  Debug    IKE  4002d4aa c9f35bee 9c83b6df 111ace24 62b9abd5 a0d91055 363bc749 d0fe2e30
Apr 29, 22:07:57  Debug    IKE  f36eb635
Apr 29, 22:07:57  Debug    IKE  receive Information.
Apr 29, 22:07:57  Debug    IKE  compute IV for phase2
Apr 29, 22:07:57  Debug    IKE  phase1 last IV:
Apr 29, 22:07:57  Debug    IKE  2af65c6b 968efc3f ea082305
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  phase2 IV computed:
Apr 29, 22:07:57  Debug    IKE  ed3d4abe 277d8309
Apr 29, 22:07:57  Debug    IKE  begin decryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  IV was saved for next processing:
Apr 29, 22:07:57  Debug    IKE  d0fe2e30 f36eb635
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  decrypted payload by IV:
```

```
Apr 29, 22:07:57  Debug    IKE  ed3d4abe 277d8309
Apr 29, 22:07:57  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:07:57  Debug    IKE  0c000018 e0bc50bf 4506eb9b ede25a95 dfa6f4b3 26af5e44 00000010 00000001
Apr 29, 22:07:57  Debug    IKE  03040001 baa54ab1
Apr 29, 22:07:57  Debug    IKE  padding len=177
Apr 29, 22:07:57  Debug    IKE  skip to trim padding.
Apr 29, 22:07:57  Debug    IKE  decrypted.
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08100501 ea082305 00000044 0c000018
Apr 29, 22:07:57  Debug    IKE  e0bc50bf 4506eb9b ede25a95 dfa6f4b3 26af5e44 00000010 00000001 03040001
Apr 29, 22:07:57  Debug    IKE  baa54ab1
Apr 29, 22:07:57  Debug    IKE  IV freed
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  ea082305 00000010 00000001 03040001 baa54ab1
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  e0bc50bf 4506eb9b ede25a95 dfa6f4b3 26af5e44
Apr 29, 22:07:57  Debug    IKE  hash validated.
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=8(hash)
Apr 29, 22:07:57  Debug    IKE  seen nptype=12(delete)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  delete payload for protocol ESP
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_dump
Apr 29, 22:07:57  Debug    IKE  purged SAs.
Apr 29, 22:07:57  Error    IKE  failed to recv from pfkey (Resource temporarily unavailable)
Apr 29, 22:07:57  Debug    IKE  ===
Apr 29, 22:07:57  Debug    IKE  68 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08100501 ba437fb6 00000044 79af0d60
Apr 29, 22:07:57  Debug    IKE  70bbdb68 59845961 82768d65 6c112b23 88da15f1 ae0ee82a d467ff17 a649b507
Apr 29, 22:07:57  Debug    IKE  62d327d1
Apr 29, 22:07:57  Debug    IKE  receive Information.
Apr 29, 22:07:57  Debug    IKE  compute IV for phase2
Apr 29, 22:07:57  Debug    IKE  phase1 last IV:
Apr 29, 22:07:57  Debug    IKE  2af65c6b 968efc3f ba437fb6
Apr 29, 22:07:57  Debug    IKE  hash(sha1)
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  phase2 IV computed:
Apr 29, 22:07:57  Debug    IKE  a0c18ae0 0f53c614
Apr 29, 22:07:57  Debug    IKE  begin decryption.
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  IV was saved for next processing:
Apr 29, 22:07:57  Debug    IKE  a649b507 62d327d1
Apr 29, 22:07:57  Debug    IKE  encryption(3des)
Apr 29, 22:07:57  Debug    IKE  with key:
Apr 29, 22:07:57  Debug    IKE  3b67932a 42457112 96291630 9a5ebc24 65eca8a5 6acc75c2
Apr 29, 22:07:57  Debug    IKE  decrypted payload by IV:
Apr 29, 22:07:57  Debug    IKE  a0c18ae0 0f53c614
Apr 29, 22:07:57  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:07:57  Debug    IKE  0c000018 254094bc 7f162895 32e1da86 b60d2e0c a7d5439b 00000010 00000001
Apr 29, 22:07:57  Debug    IKE  03040001 99328e18
Apr 29, 22:07:57  Debug    IKE  padding len=24
Apr 29, 22:07:57  Debug    IKE  skip to trim padding.
Apr 29, 22:07:57  Debug    IKE  decrypted.
Apr 29, 22:07:57  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08100501 ba437fb6 00000044 0c000018
Apr 29, 22:07:57  Debug    IKE  254094bc 7f162895 32e1da86 b60d2e0c a7d5439b 00000010 00000001 03040001
Apr 29, 22:07:57  Debug    IKE  99328e18
Apr 29, 22:07:57  Debug    IKE  IV freed
Apr 29, 22:07:57  Debug    IKE  HASH with:
Apr 29, 22:07:57  Debug    IKE  ba437fb6 00000010 00000001 03040001 99328e18
Apr 29, 22:07:57  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:07:57  Debug    IKE  HASH computed:
Apr 29, 22:07:57  Debug    IKE  254094bc 7f162895 32e1da86 b60d2e0c a7d5439b
Apr 29, 22:07:57  Debug    IKE  hash validated.
Apr 29, 22:07:57  Debug    IKE  begin.
Apr 29, 22:07:57  Debug    IKE  seen nptype=8(hash)
Apr 29, 22:07:57  Debug    IKE  seen nptype=12(delete)
Apr 29, 22:07:57  Debug    IKE  succeed.
Apr 29, 22:07:57  Debug    IKE  delete payload for protocol ESP
Apr 29, 22:07:57  Debug    IKE  call pfkey_send_dump
Apr 29, 22:07:57  Debug    IKE  purged SAs.
Apr 29, 22:08:02  Debug    IKE  ===
Apr 29, 22:08:02  Debug    IKE  140 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:08:02  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000008c 71e585cf
Apr 29, 22:08:02  Debug    IKE  e71c0321 cd5249ff ac6d80f0 7cb5acb0 aba1da6e 09e05b4d 9cfa163d d4f5287d
```

```
Apr 29, 22:08:02  Debug    IKE  5998baab 4a409d6a d0cee19e 726ad237 6c60a7cc 5d05a261 af703a5e fe7befa5
Apr 29, 22:08:02  Debug    IKE  7c685bde fe996ea7 5f55f537 9e74ef11 245b791e 101e054a 53427a42 12d4b4bc
Apr 29, 22:08:02  Debug    IKE  2260e15f c7223b1e 90ecc8e3
Apr 29, 22:08:02  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:08:02  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:08:02  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:08:02  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:08:02  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000003c 02dc470b
Apr 29, 22:08:02  Debug    IKE  b3980b8a d960a967 ff969c41 7a0cb81f 463660ed 3c702240 b394ac2b
Apr 29, 22:08:02  Info     IKE  the packet is retransmitted by 192.168.215.233[500].
Apr 29, 22:08:02  Debug    IKE  ===
Apr 29, 22:08:02  Debug    IKE  140 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:08:02  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000008c 98f29cf1
Apr 29, 22:08:02  Debug    IKE  655c7078 ce3cdd2a b8d60813 b6fa46bf f7007966 cc1bb4ed da3e1651 c88d6143
Apr 29, 22:08:02  Debug    IKE  c2585e92 6cd1e701 b986bcd7 885a4ad8 dbf2b69c 601e5976 1ff5cc1a 7c399fdb
Apr 29, 22:08:02  Debug    IKE  2ffbedef e98e14e7 c1347a30 5cf35a7d ab977b24 58e9e635 7a62f843 1381baea
Apr 29, 22:08:02  Debug    IKE  2682a4c5 4ad63659 fbdfd676
Apr 29, 22:08:02  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:08:02  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:08:02  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:08:02  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:08:02  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000003c 67f8e2e9
Apr 29, 22:08:02  Debug    IKE  191d2508 eaa5eba5 e495ab4b 7311a4fc 479d3be1 a01651c9 f7dbfa84
Apr 29, 22:08:02  Info     IKE  the packet is retransmitted by 192.168.215.233[500].
Apr 29, 22:08:07  Error    IKE  192.168.215.233 give up to get IPsec-SA due to time up to wait.
Apr 29, 22:08:07  Debug    IKE  IV freed
Apr 29, 22:08:07  Debug    IKE  ===
Apr 29, 22:08:07  Debug    IKE  140 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:08:07  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000008c 98f29cf1
Apr 29, 22:08:07  Debug    IKE  655c7078 ce3cdd2a b8d60813 b6fa46bf f7007966 cc1bb4ed da3e1651 c88d6143
Apr 29, 22:08:07  Debug    IKE  c2585e92 6cd1e701 b986bcd7 885a4ad8 dbf2b69c 601e5976 1ff5cc1a 7c399fdb
Apr 29, 22:08:07  Debug    IKE  2ffbedef e98e14e7 c1347a30 5cf35a7d ab977b24 58e9e635 7a62f843 1381baea
Apr 29, 22:08:07  Debug    IKE  2682a4c5 4ad63659 fbdfd676
Apr 29, 22:08:07  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:08:07  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:08:07  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:08:07  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:08:07  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 fb200e51 0000003c 67f8e2e9
Apr 29, 22:08:07  Debug    IKE  191d2508 eaa5eba5 e495ab4b 7311a4fc 479d3be1 a01651c9 f7dbfa84
Apr 29, 22:08:07  Info     IKE  the packet is retransmitted by 192.168.215.233[500].
Apr 29, 22:08:07  Debug    IKE  ===
Apr 29, 22:08:07  Debug    IKE  140 bytes message received from 192.168.215.233[500] to 192.168.215.3[500]
Apr 29, 22:08:07  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000008c 71e585cf
Apr 29, 22:08:07  Debug    IKE  e71c0321 cd5249ff ac6d80f0 7cb5acb0 aba1da6e 09e05b4d 9cfa163d d4f5287d
Apr 29, 22:08:07  Debug    IKE  5998baab 4a409d6a d0cee19e 726ad237 6c60a7cc 5d05a261 af703a5e fe7befa5
Apr 29, 22:08:07  Debug    IKE  7c685bde fe996ea7 5f55f537 9e74ef11 245b791e 101e054a 53427a42 12d4b4bc
Apr 29, 22:08:07  Debug    IKE  2260e15f c7223b1e 90ecc8e3
Apr 29, 22:08:07  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:08:07  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:08:07  Debug    IKE  send packet to 192.168.215.233[500]
Apr 29, 22:08:07  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.233[500]
Apr 29, 22:08:07  Debug    IKE  c9858276 1037a59c 36e077fd d9e25151 08102001 c2ab803e 0000003c 02dc470b
Apr 29, 22:08:07  Debug    IKE  b3980b8a d960a967 ff969c41 7a0cb81f 463660ed 3c702240 b394ac2b
Apr 29, 22:08:07  Info     IKE  the packet is retransmitted by 192.168.215.233[500].
```