IPSecuritas 3.x

Configuration Instructions

for

Checkpoint Safe@Office

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.

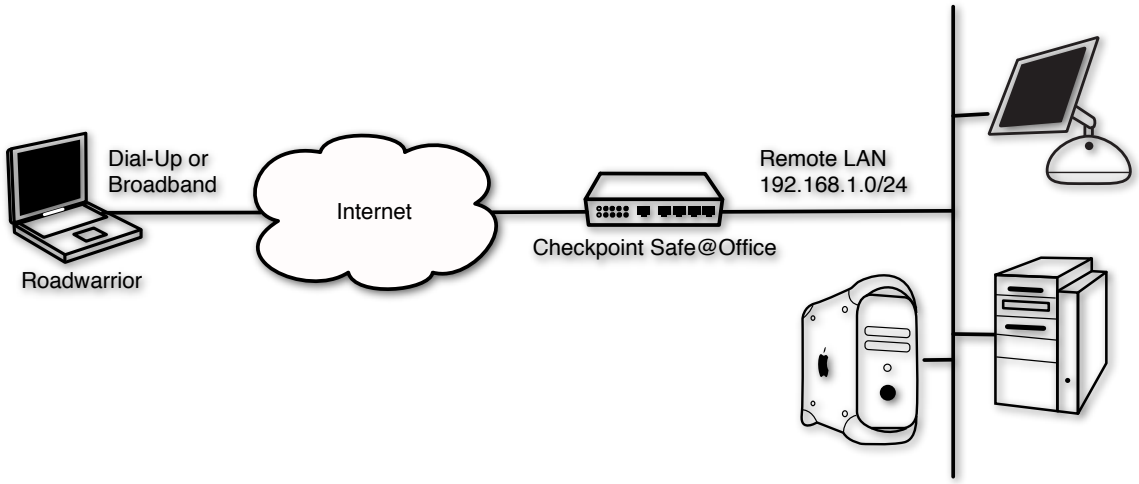
Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic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

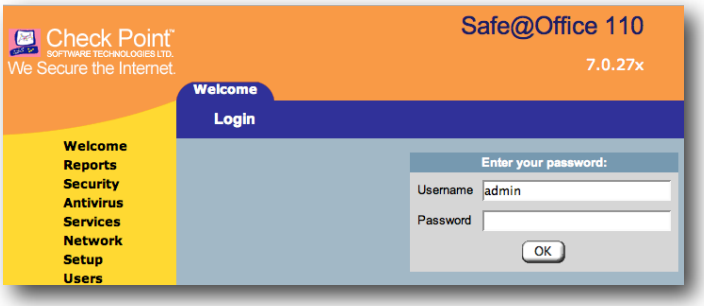
This document describes the steps necessary to establish a protected VPN connection between a Mac client and a Checkpoint Safe@Office firewall. All information in this document is based on the following assumed network.



Checkpoint Safe@Office Setup

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

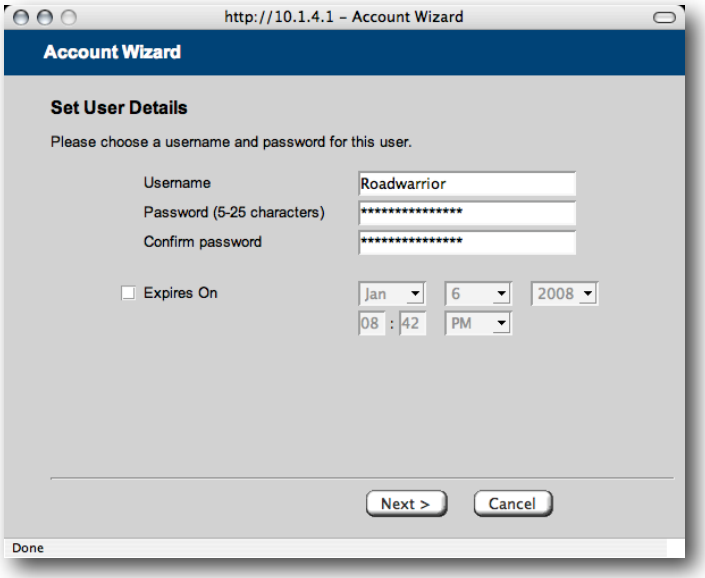
Login



Open a web browser and connect to your Checkpoint router. Enter the administrator user name (usually admin) and password.

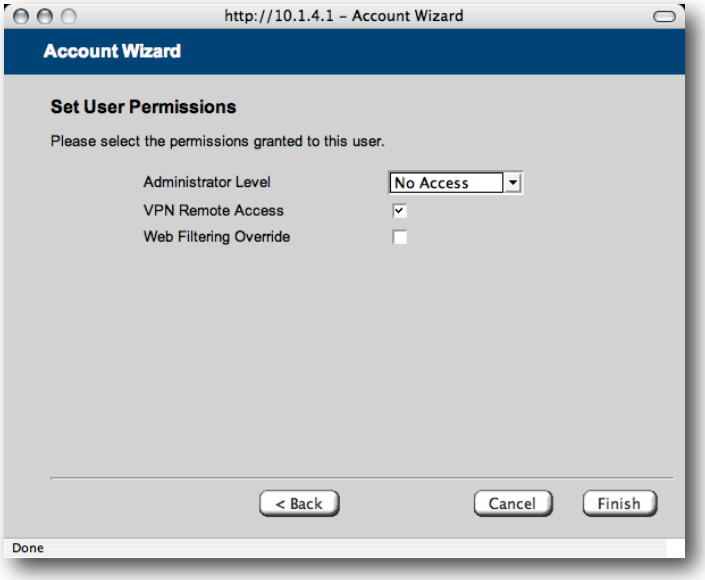
Note: If you have trouble connecting with Safari, try Firefox instead

Add VPN Users



Click on **Users** on the left side, then select **New User** to add a new VPN user.
Enter a username without spaces or special characters and a password (both case sensitive).
This information will be needed during the Wizard setup of IPSecuritas.
You might want to enter a expiry date for additional security.

Proceed to the next step by clicking on **Next**.



Set the **Administrator Level** to **No Access** unless you want to give the VPN user access to the firewall's configuration.
Enable **VPN Remote Access**.

Click on **Finish** to create the user.

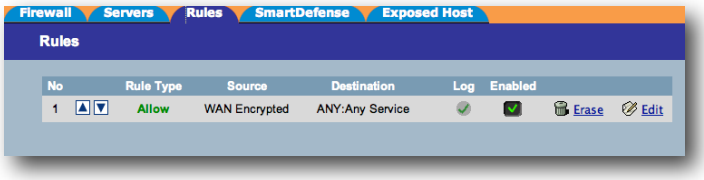
Repeat this procedure for more users if needed.

Enable VPN Server

Click on **VPN** on the left side to open the VPN server settings. **Enable** VPN access from the Internet, enable **NAT** and **firewall** bypasses.
If you want to restrict the access to the local networks by VPN users, **disable** the firewall bypass and add appropriate firewall rules (see below)

Click on **Apply**.

Configure the Firewall (Optional)



This step is only needed if firewall bypass is disabled in the VPN server settings.
Add rules for VPN by setting the source to **WAN Encrypted**.

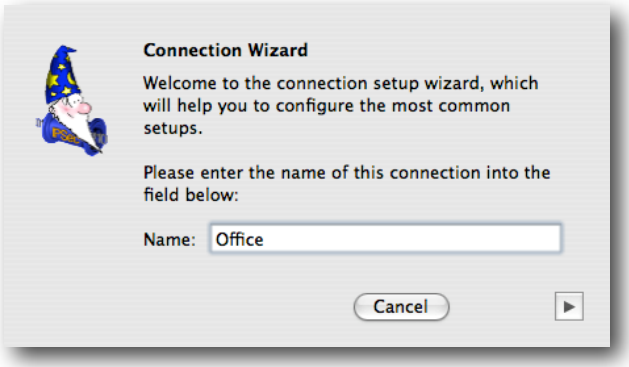
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the Safe@Office 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: 

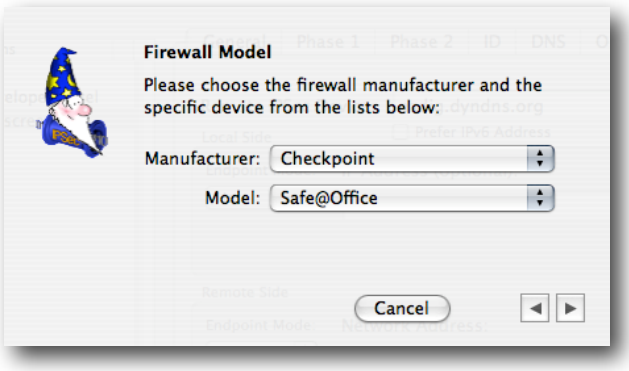
Enter Name of New Connection



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

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

Select Router Model



Select **Checkpoint** from the manufacturer list and **Safe@Office** from the model list.

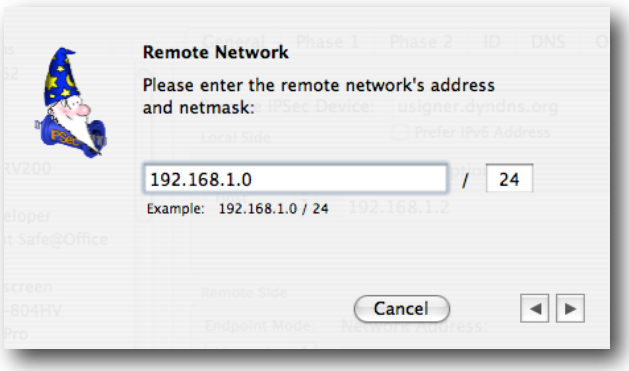
Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

Enter the public IP address or hostname of your Safe@Office firewall. In case your ISP assigned you a dynamic IP address, you should register with a dynamic IP DNS service (like http://www.dyndns.org).

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

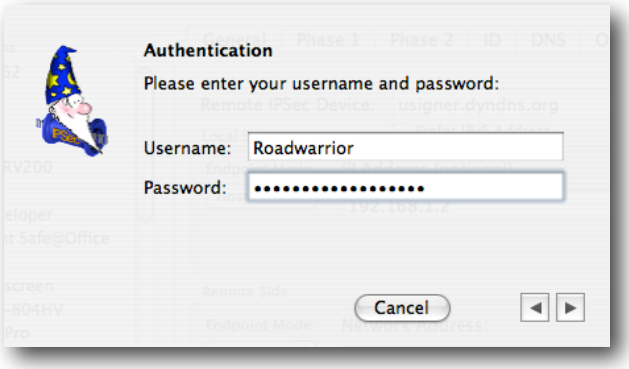
Enter Remote Network



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 Safe@Office.

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

Enter User and Password Information



Enter the VPN user name and her password. These settings have to match the settings of the Safe@Office.

Click on the right arrow to finish the connection setup.

Diagnosis

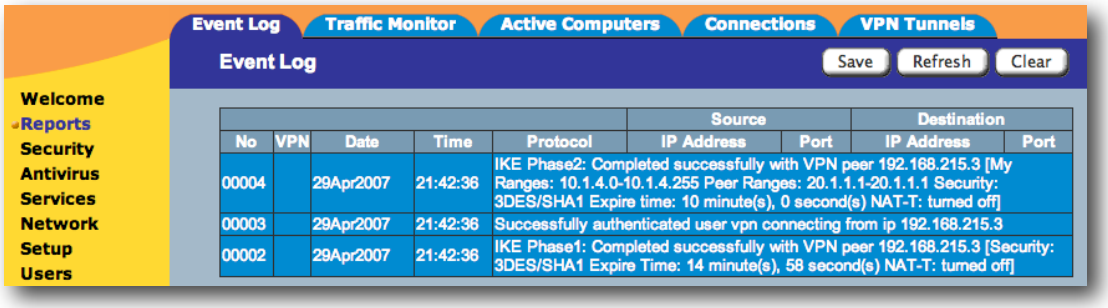
Reachability Test

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

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

Sample Safe@Office Log Output

The following is a sample log from the Safe@Office after a successful connection establishment:



Sample IPSecuritas Log Output

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

```
IPSecuritas 3.0prc3 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, 22:24:39  Debug    APP  State change from IDLE to AUTHENTICATING after event START
Apr 29, 22:24:39  Info     APP  IKE daemon started
Apr 29, 22:24:39  Info     APP  IPSec started
Apr 29, 22:24:39  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
Apr 29, 22:24:39  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Apr 29, 22:24:39  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Apr 29, 22:24:39  Info     IKE  Foreground mode.
Apr 29, 22:24:39  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
Apr 29, 22:24:39  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
Apr 29, 22:24:39  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
```

```
Apr 29, 22:24:39  Info    IKE  Resize address pool from 0 to 255
Apr 29, 22:24:39  Debug   IKE  lifetime = 900
Apr 29, 22:24:39  Debug   IKE  lifebyte = 0
Apr 29, 22:24:39  Debug   IKE  encklen=0
Apr 29, 22:24:39  Debug   IKE  p:1 t:1
Apr 29, 22:24:39  Debug   IKE  3DES-CBC(5)
Apr 29, 22:24:39  Debug   IKE  SHA(2)
Apr 29, 22:24:39  Debug   IKE  1024-bit MODP group(2)
Apr 29, 22:24:39  Debug   IKE  Hybrid RSA client(64221)
Apr 29, 22:24:39  Debug   IKE  compression algorithm can not be checked because sadb message doesn't support it.
Apr 29, 22:24:39  Debug   IKE  parse successed.
Apr 29, 22:24:39  Debug   IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
Apr 29, 22:24:39  Info    IKE  192.168.215.3[4500] used as isakmp port (fd=7)
Apr 29, 22:24:39  Info    IKE  192.168.215.3[500] used as isakmp port (fd=8)
Apr 29, 22:24:39  Debug   IKE  get pfkey X_SPDDUMP message
Apr 29, 22:24:39  Debug   IKE  02120000 0f000100 01000000 e7090000 03000500 ff180000 10020000 0a010400
Apr 29, 22:24:39  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 14010101 00000000 00000000
Apr 29, 22:24:39  Debug   IKE  07001200 02000100 30010000 00000000 28003200 02020000 10020000 c0a8d7e3
Apr 29, 22:24:39  Debug   IKE  00000000 00000000 10020000 c0a8d703 00000000 00000000
Apr 29, 22:24:39  Debug   IKE  get pfkey X_SPDDUMP message
Apr 29, 22:24:39  Debug   IKE  02120000 0f000100 00000000 e7090000 03000500 ff200000 10020000 14010101
Apr 29, 22:24:39  Debug   IKE  00000000 00000000 03000600 ff180000 10020000 0a010400 00000000 00000000
Apr 29, 22:24:39  Debug   IKE  07001200 02000200 2f010000 00000000 28003200 02020000 10020000 c0a8d703
Apr 29, 22:24:39  Debug   IKE  00000000 00000000 10020000 c0a8d7e3 00000000 00000000
Apr 29, 22:24:39  Debug   IKE  sub:0xbffff340: 20.1.1.1/32[0] 10.1.4.0/24[0] proto=any dir=out
Apr 29, 22:24:39  Debug   IKE  db :0x308bf8: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in
Apr 29, 22:24:40  Info    APP  Initiated connection Checkpoint Safe@Office
Apr 29, 22:24:40  Debug   IKE  get pfkey ACQUIRE message
Apr 29, 22:24:40  Debug   IKE  02060003 24000000 1c010000 00000000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:24:40  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e3 00000000 00000000
Apr 29, 22:24:40  Debug   IKE  1c000d00 20000000 00030000 00000000 00010008 00000000 01000000 01000000
Apr 29, 22:24:40  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:24:40  Debug   IKE  80700000 00000000 00000000 00000000 00040000 00000000 0001c001 00000000
Apr 29, 22:24:40  Debug   IKE  01000000 01000000 00000000 00000000 00000000 00000000 00000000 00000000
Apr 29, 22:24:40  Debug   IKE  80510100 00000000 80700000 00000000 00000000 00000000 000c0000 00000000
Apr 29, 22:24:40  Debug   IKE  00010001 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Apr 29, 22:24:40  Debug   IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
Apr 29, 22:24:40  Error   IKE  inappropriate sadb acquire message passed.
Apr 29, 22:24:40  Debug   IKE  get pfkey ACQUIRE message
Apr 29, 22:24:40  Debug   IKE  02060003 14000000 06050000 2c020000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:24:40  Debug   IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e3 00000000 00000000
Apr 29, 22:24:40  Debug   IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 29, 22:24:40  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:24:40  Debug   IKE  80700000 00000000 00000000 00000000 02001200 02000200 2f010000 00000000
Apr 29, 22:24:40  Debug   IKE  suitable outbound SP found: 20.1.1.1/32[0] 10.1.4.0/24[0] proto=any dir=out.
Apr 29, 22:24:40  Debug   IKE  sub:0xbffff31c: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in
Apr 29, 22:24:40  Debug   IKE  db :0x308bf8: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in
Apr 29, 22:24:40  Debug   IKE  suitable inbound SP found: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in.
Apr 29, 22:24:40  Debug   IKE  new acquire 20.1.1.1/32[0] 10.1.4.0/24[0] proto=any dir=out
Apr 29, 22:24:40  Debug   IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 29, 22:24:40  Debug   IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:24:40  Debug   IKE  (trns_id=AES encklen=256 authtype=hmac-sha)
Apr 29, 22:24:40  Debug   IKE  (trns_id=AES encklen=192 authtype=hmac-sha)
Apr 29, 22:24:40  Debug   IKE  (trns_id=AES encklen=128 authtype=hmac-sha)
Apr 29, 22:24:40  Debug   IKE  in post_acquire
Apr 29, 22:24:40  Debug   IKE  configuration found for 192.168.215.227.
Apr 29, 22:24:40  Info    IKE  IPsec-SA request for 192.168.215.227 queued due to no phase1 found.
Apr 29, 22:24:40  Debug   IKE  ===
Apr 29, 22:24:40  Info    IKE  initiate new phase 1 negotiation: 192.168.215.3[500]<=>192.168.215.227[500]
Apr 29, 22:24:40  Info    IKE  begin Identity Protection mode.
Apr 29, 22:24:40  Debug   IKE  new cookie:
Apr 29, 22:24:40  Debug   IKE  341d80089acf997d
Apr 29, 22:24:40  Debug   IKE  add payload of len 48, next type 13
Apr 29, 22:24:40  Debug   IKE  add payload of len 8, next type 13
Apr 29, 22:24:40  Debug   IKE  add payload of len 16, next type 13
Apr 29, 22:24:40  Debug   IKE  add payload of len 16, next type 0
Apr 29, 22:24:40  Debug   IKE  132 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:40  Debug   IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:40  Debug   IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:40  Debug   IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:40  Debug   IKE  1 times of 132 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:40  Debug   IKE  341d8008 9acf997d 00000000 00000000 01100200 00000000 00000084 0d000034
Apr 29, 22:24:40  Debug   IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0384
```

```
Apr 29, 22:24:40  Debug    IKE  80010005 8003fadd 80020002 80040002 0d00000c 09002689 dfd6b712 0d000014
Apr 29, 22:24:40  Debug    IKE  12f5f28c 457168a9 702d9fe2 74cc0100 00000014 afcad713 68a1f1c9 6b8696fc
Apr 29, 22:24:40  Debug    IKE  77570100
Apr 29, 22:24:40  Debug    IKE  resend phase1 packet 341d80089acf997d:0000000000000000
Apr 29, 22:24:40  Debug    IKE  ===
Apr 29, 22:24:40  Debug    IKE  80 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:40  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 01100200 00000000 00000050 00000034
Apr 29, 22:24:40  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0384
Apr 29, 22:24:40  Debug    IKE  80010005 8003fadd 80020002 80040002
Apr 29, 22:24:40  Debug    IKE  begin.
Apr 29, 22:24:40  Debug    IKE  seen nptype=1(sa)
Apr 29, 22:24:40  Debug    IKE  succeed.
Apr 29, 22:24:40  Debug    IKE  total SA len=48
Apr 29, 22:24:40  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0384
Apr 29, 22:24:40  Debug    IKE  80010005 8003fadd 80020002 80040002
Apr 29, 22:24:40  Debug    IKE  begin.
Apr 29, 22:24:40  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:24:40  Debug    IKE  succeed.
Apr 29, 22:24:40  Debug    IKE  proposal #1 len=40
Apr 29, 22:24:40  Debug    IKE  begin.
Apr 29, 22:24:40  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:24:40  Debug    IKE  succeed.
Apr 29, 22:24:40  Debug    IKE  transform #1 len=32
Apr 29, 22:24:40  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:40  Debug    IKE  type=Life Duration, flag=0x8000, lorv=900
Apr 29, 22:24:40  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Apr 29, 22:24:40  Debug    IKE  encryption(3des)
Apr 29, 22:24:40  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=Hybrid RSA client
Apr 29, 22:24:40  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Apr 29, 22:24:40  Debug    IKE  hash(sha1)
Apr 29, 22:24:40  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Apr 29, 22:24:40  Debug    IKE  hmac(modp1024)
Apr 29, 22:24:40  Debug    IKE  pair 1:
Apr 29, 22:24:40  Debug    IKE  0x3090e0: next=0x0 tnext=0x0
Apr 29, 22:24:40  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:24:40  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
Apr 29, 22:24:40  Debug    IKE  trns#=1, trns-id=IKE
Apr 29, 22:24:40  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:40  Debug    IKE  type=Life Duration, flag=0x8000, lorv=900
Apr 29, 22:24:40  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Apr 29, 22:24:40  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=Hybrid RSA client
Apr 29, 22:24:40  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Apr 29, 22:24:40  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Apr 29, 22:24:40  Debug    IKE  Compared: DB:Peer
Apr 29, 22:24:40  Debug    IKE  (lifetime = 900:900)
Apr 29, 22:24:40  Debug    IKE  (lifebyte = 0:0)
Apr 29, 22:24:40  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
Apr 29, 22:24:40  Debug    IKE  (encklen = 0:0)
Apr 29, 22:24:40  Debug    IKE  hashtype = SHA:SHA
Apr 29, 22:24:40  Debug    IKE  authmethod = Hybrid RSA client:Hybrid RSA client
Apr 29, 22:24:40  Debug    IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
Apr 29, 22:24:40  Debug    IKE  an acceptable proposal found.
Apr 29, 22:24:40  Debug    IKE  hmac(modp1024)
Apr 29, 22:24:40  Debug    IKE  agreed on Hybrid RSA client auth.
Apr 29, 22:24:40  Debug    IKE  ===
Apr 29, 22:24:40  Debug    IKE  compute DH's private.
Apr 29, 22:24:40  Debug    IKE  66073d43 a4c37f97 3bdb3b9f 3ae364ed e2069647 df9d999f ebee8583 79c59414
Apr 29, 22:24:40  Debug    IKE  cbf2dc1d 0d98d596 1aaa4fc4 10645236 bcaea455 92bf6bcb 724f66b0 4c9033d3
Apr 29, 22:24:40  Debug    IKE  8dde8fdb f922429c ca9bb727 0f20dd97 9c29bb6d e596f3e0 62ced30c ab2c1896
Apr 29, 22:24:40  Debug    IKE  99b230da ee16d06b fe9466e8 35a835fe fe5bc7e8 e52f91a2 48a77103 9b257edf
Apr 29, 22:24:40  Debug    IKE  compute DH's public.
Apr 29, 22:24:40  Debug    IKE  6a96db52 8aa39d7e 26c35c97 8f6815c7 7020255b 4650332c d4f64bf3 1d4b4a2c
Apr 29, 22:24:40  Debug    IKE  fa63ddcf c9cf8f99 3d1b7422 f62ee5c8 5be1d8a2 7502582e 76389d19 6a052d4c
Apr 29, 22:24:40  Debug    IKE  58280349 b98032b3 fd9e784c d2253873 4107e33c c94cd90a 51e8caf9 d2764a32
Apr 29, 22:24:40  Debug    IKE  58c1fabe c79e7c74 0c61b49f 89b4bbd8 62d836cd d2f9a839 5f1305dc acdf8b8a
Apr 29, 22:24:40  Debug    IKE  add payload of len 128, next type 10
Apr 29, 22:24:40  Debug    IKE  add payload of len 16, next type 0
Apr 29, 22:24:40  Debug    IKE  180 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:40  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:40  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:40  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:40  Debug    IKE  1 times of 180 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:40  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 04100200 00000000 000000b4 0a000084
Apr 29, 22:24:40  Debug    IKE  6a96db52 8aa39d7e 26c35c97 8f6815c7 7020255b 4650332c d4f64bf3 1d4b4a2c
```

```
Apr 29, 22:24:40  Debug    IKE  fa63ddcf c9cf8f99 3d1b7422 f62ee5c8 5be1d8a2 7502582e 76389d19 6a052d4c
Apr 29, 22:24:40  Debug    IKE  58280349 b98032b3 fd9e784c d2253873 4107e33c c94cd90a 51e8caf9 d2764a32
Apr 29, 22:24:40  Debug    IKE  58c1fabe c79e7c74 0c61b49f 89b4bbd8 62d836cd d2f9a839 5f1305dc acdf8b8a
Apr 29, 22:24:40  Debug    IKE  00000014 98b1bd20 5f020dd5 d469f1e0 c5f2dd93
Apr 29, 22:24:40  Debug    IKE  resend phase1 packet 341d80089acf997d:83f17532d8e4e1d8
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  184 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 04100200 00000000 000000b8 0a000084
Apr 29, 22:24:41  Debug    IKE  b96894cc 37b2b2de 1b3577ac a237942d dd7aa820 39c3a1ff a7b7523d a32f9e3e
Apr 29, 22:24:41  Debug    IKE  96596ad8 3ca1baa9 16424e6a e5173ddd efb90d95 b29ffecb 115764aa d07ccec8
Apr 29, 22:24:41  Debug    IKE  37d17202 2ddba5bd c265c09f 0aeaeb3c 56ce30ad e23cf433 a2706d1a c3d6e214
Apr 29, 22:24:41  Debug    IKE  d06e12ed cb19f80f 0f4ae2c2 e8a36a1b dacf2c56 3df5318b 159bb067 04b8a859
Apr 29, 22:24:41  Debug    IKE  00000018 2fac2991 7fe20a09 8256cf73 27a30c22 3f0d8dc6
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=4(ke)
Apr 29, 22:24:41  Debug    IKE  seen nptype=10(nonce)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  compute DH's shared.
Apr 29, 22:24:41  Debug    IKE  22719f95 e8c7b58b 6f2dc822 b014b89e cce52573 0389b9fc 4eece938 2a849001
Apr 29, 22:24:41  Debug    IKE  291ddcbe f52046ae 15a770ed cfb12e1d b1265958 a76bc729 da3a5d09 8f6835ba
Apr 29, 22:24:41  Debug    IKE  749fbfdb 2316d939 052defed 3d8db3d5 8bdb3cd8 072c8229 8acfedd8 e43b5294
Apr 29, 22:24:41  Debug    IKE  41c68024 e518ed69 f51a9389 558be0ef 017f84a5 95c95632 e87c765d dd1c21e7
Apr 29, 22:24:41  Debug    IKE  nonce1: 2007-04-29 22:24:41: DEBUG:
Apr 29, 22:24:41  Debug    IKE  98b1bd20 5f020dd5 d469f1e0 c5f2dd93
Apr 29, 22:24:41  Debug    IKE  nonce2: 2007-04-29 22:24:41: DEBUG:
Apr 29, 22:24:41  Debug    IKE  2fac2991 7fe20a09 8256cf73 27a30c22 3f0d8dc6
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  SKEYID computed:
Apr 29, 22:24:41  Debug    IKE  0e5ebd9d 0907cdf4 1a384dac 093b0add d8b7cb49
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  SKEYID_d computed:
Apr 29, 22:24:41  Debug    IKE  55a956e5 2544e3c2 fb259628 d7441872 eaeb1cf5
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  SKEYID_a computed:
Apr 29, 22:24:41  Debug    IKE  34f5186d c504c1a6 0d96c296 f860b9ac 61e9ec18
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  SKEYID_e computed:
Apr 29, 22:24:41  Debug    IKE  c501e492 710fea21 f85ed368 80a79212 27426799
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  hash(sha1)
Apr 29, 22:24:41  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  compute intermediate encryption key K1
Apr 29, 22:24:41  Debug    IKE  00
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  compute intermediate encryption key K2
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77
Apr 29, 22:24:41  Debug    IKE  b922f72e e531a722 d16bd4a5 f0b662bc 32af89b5
Apr 29, 22:24:41  Debug    IKE  final encryption key computed:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  hash(sha1)
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV computed:
Apr 29, 22:24:41  Debug    IKE  ec1c2c32 6717d0dc
Apr 29, 22:24:41  Debug    IKE  use ID type of IPv4_address
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  6a96db52 8aa39d7e 26c35c97 8f6815c7 7020255b 4650332c d4f64bf3 1d4b4a2c
Apr 29, 22:24:41  Debug    IKE  fa63ddcf c9cf8f99 3d1b7422 f62ee5c8 5be1d8a2 7502582e 76389d19 6a052d4c
Apr 29, 22:24:41  Debug    IKE  58280349 b98032b3 fd9e784c d2253873 4107e33c c94cd90a 51e8caf9 d2764a32
Apr 29, 22:24:41  Debug    IKE  58c1fabe c79e7c74 0c61b49f 89b4bbd8 62d836cd d2f9a839 5f1305dc acdf8b8a
Apr 29, 22:24:41  Debug    IKE  b96894cc 37b2b2de 1b3577ac a237942d dd7aa820 39c3a1ff a7b7523d a32f9e3e
Apr 29, 22:24:41  Debug    IKE  96596ad8 3ca1baa9 16424e6a e5173ddd efb90d95 b29ffecb 115764aa d07ccec8
Apr 29, 22:24:41  Debug    IKE  37d17202 2ddba5bd c265c09f 0aeaeb3c 56ce30ad e23cf433 a2706d1a c3d6e214
Apr 29, 22:24:41  Debug    IKE  d06e12ed cb19f80f 0f4ae2c2 e8a36a1b dacf2c56 3df5318b 159bb067 04b8a859
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 00000001 00000001 00000028 01010001
Apr 29, 22:24:41  Debug    IKE  00000020 01010000 800b0001 800c0384 80010005 8003fadd 80020002 80040002
Apr 29, 22:24:41  Debug    IKE  011101f4 c0a8d703
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH (init) computed:
Apr 29, 22:24:41  Debug    IKE  6d904cb2 fc5ee392 52d2ccb6 6fcb8d35 4a924e94
Apr 29, 22:24:41  Debug    IKE  add payload of len 8, next type 8
Apr 29, 22:24:41  Debug    IKE  add payload of len 20, next type 0
```

```
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 4
Apr 29, 22:24:41  Debug    IKE  0800000c 011101f4 c0a8d703 00000018 6d904cb2 fc5ee392 52d2ccb6 6fcb8d35
Apr 29, 22:24:41  Debug    IKE  4a924e94 00000004
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  ec1c2c32 6717d0dc
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  32bfe81c cdd4a9a0
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  68 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 68 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 05100201 00000000 00000044 42656fdf
Apr 29, 22:24:41  Debug    IKE  a9f91c8f 61ae1e99 61d2206f 095ee8d6 2fd5affc 75525896 9c98d22f 32bfe81c
Apr 29, 22:24:41  Debug    IKE  cdd4a9a0
Apr 29, 22:24:41  Debug    IKE  resend phase1 packet 341d80089acf997d:83f17532d8e4e1d8
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  1220 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 05100201 00000000 000004c4 27c4dbba
Apr 29, 22:24:41  Debug    IKE  37fcc9c3 7cccae41 d1e1ca43 d049adcb 679798b7 4828e5cb ed8a5921 3ee6e972
Apr 29, 22:24:41  Debug    IKE  01a8bb45 97d67a96 0b02563d 89c8cc36 a0ec0fdb 77f2e213 2a993e08 5da5b7b5
Apr 29, 22:24:41  Debug    IKE  cac8e62d e49213e9 5263f87f cb085fcb 28014d07 baef3d05 262ff138 7827911a
Apr 29, 22:24:41  Debug    IKE  a8745b46 7ebbdbd0 b17aa7be ddb94327 4914c2f2 0d464413 6f880504 16fd7e15
Apr 29, 22:24:41  Debug    IKE  10d79d4f b9f03b4e c3a28760 c2bb4f07 9d3de6b7 1c8e35ad c7014a74 0fd1f85b
Apr 29, 22:24:41  Debug    IKE  44e015fe c9c2a30a ec6c26ae 5f60492c 1d9f548b 222c9eba d6a80c41 bfe22d9e
Apr 29, 22:24:41  Debug    IKE  d49a738d be8d558f 5bfc99bf 1115c898 d6a4cf4d 7b01e7ed 74a1dc2a 24604daf
Apr 29, 22:24:41  Debug    IKE  5a45fd83 37c9d9e8 766e4281 403c469e 9e4eb452 97754791 e5f02c39 46e03f74
Apr 29, 22:24:41  Debug    IKE  e8710375 4a84cc24 f2fb6763 a4f4916d a4359bdb a41403ec e4c8a424 62309fee
Apr 29, 22:24:41  Debug    IKE  952ede48 a4a6bee7 5ce33404 c5e0583e 41cc9fe5 22272d18 3c5e6a9a 0d4df3c4
Apr 29, 22:24:41  Debug    IKE  e6c2f8fb 126c50e2 be2056f6 2d6d710d c21e5d22 185e1f4f 9ba707b4 dd755b4b
Apr 29, 22:24:41  Debug    IKE  118b513c 264ffaea 904acdfb d98959bb e6a4db6c c06c1588 e48d69ec 167a2be2
Apr 29, 22:24:41  Debug    IKE  c794f838 bae458fd 7acdcb96 f25622ab 2f064fb2 46076e6e 5b131e60 d29f4a8b
Apr 29, 22:24:41  Debug    IKE  1b2261c3 5f3e2a03 26837da8 4379efb8 e4db9c84 bb0d6ca1 4401f228 946d9b72
Apr 29, 22:24:41  Debug    IKE  012e788e 2b997d55 c760aa6d 2c8c083b 5d63b228 761373d9 ee310271 212fba8e
Apr 29, 22:24:41  Debug    IKE  0b074058 6a1bba6f 89f04ebc 420e875d 2117a45e d303634b f3d9fd07 42e7a321
Apr 29, 22:24:41  Debug    IKE  1887d4d5 c975f3ad 6688d0c7 dd5d5800 401a060b c770e72d 6de30002 f5f2fdef
Apr 29, 22:24:41  Debug    IKE  7a23e231 99846e6d 08bf51f2 9c93cf22 3ac98c93 7259ec38 bef4db83 b9565c7c
Apr 29, 22:24:41  Debug    IKE  b8fa073b a5faca03 3346d5fd 8b0369ba 9298ef59 7003d575 9febd04a 27005a0f
Apr 29, 22:24:41  Debug    IKE  5fa9b2ac 33b5429d d829981b bfedb31d d95b0276 0d430b96 374f7f6c 07edb453
Apr 29, 22:24:41  Debug    IKE  8be9ac86 26d5da95 1b1e53e7 cba1c442 90f65aca 8e3acb35 0773b8d1 98ecf67e
Apr 29, 22:24:41  Debug    IKE  6b8135e7 f65941a4 b693621e eb36aa4f febc0436 60a09884 5d9c7470 3edc4bc0
Apr 29, 22:24:41  Debug    IKE  7ff69c31 b45c0113 c7f1e262 2eb71391 c2ad7768 0904c3e8 a84256b4 d41b7c87
Apr 29, 22:24:41  Debug    IKE  98bb4798 f68ba785 7115d4f7 4598b765 f515aab3 4707f946 1e2c7e97 e7e4c7dd
Apr 29, 22:24:41  Debug    IKE  fed20997 ca7ecdd1 abe96616 b6b54bdf 726b7779 4859a5fb 3744967c 8982eda3
Apr 29, 22:24:41  Debug    IKE  c19cadbf 7bbda37f 4f0ccf88 c36d1e8c 5f0022ae 4e0aa479 98807414 9ebd813e
Apr 29, 22:24:41  Debug    IKE  a07e3365 433351db 271b0c14 b8551eab 535501b4 625e1e54 461a48a1 11fdd1e0
Apr 29, 22:24:41  Debug    IKE  fac8b249 f322d4ac 0eab6984 4734148f 80f2a781 c9c5f744 4c9d849a 51a0a66a
Apr 29, 22:24:41  Debug    IKE  5e2dede6 d8b72322 84fab440 0a291d10 55b295c1 f09245d4 228c0fdb 04475955
Apr 29, 22:24:41  Debug    IKE  68043095 0e7b4aa0 bc65749d 05dfe844 693b1ab0 64f1415c a9720bb5 be82f0f0
Apr 29, 22:24:41  Debug    IKE  47611fa1 18215a47 278c327e 6c17299b b3829349 fc0f3411 c2ea3ec4 aaa7d246
Apr 29, 22:24:41  Debug    IKE  3246e495 7a50a335 cc6a2e0c 35fad931 1b94f42e cce88563 34e6e6cc f05ea63f
Apr 29, 22:24:41  Debug    IKE  d91e377e 8c389a12 f945c018 82bc99cc c3cb7d30 1853dab4 dc046b5a 8c1355bd
Apr 29, 22:24:41  Debug    IKE  f542e0df 5db3e746 b11cd910 da0ba5d0 31a5de72 75379afe 0f9e6f16 3bc988c4
Apr 29, 22:24:41  Debug    IKE  e3683c34 2b524337 262d3768 ca86b177 41542450 9ca9db29 19dc28cd 56a9273c
Apr 29, 22:24:41  Debug    IKE  1da899fd f6c13675 40c6f928 3bbad321 f1a5e7ba b614f1c5 fb4b16c6 b3fdc109
Apr 29, 22:24:41  Debug    IKE  0a4c0abd da472f4a 7668ecf3 5177303e 8ed444d8 486f415a 9ab8b94b 8822330c
Apr 29, 22:24:41  Debug    IKE  fbd77f55
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  8822330c fbd77f55
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  32bfe81c cdd4a9a0
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:41  Debug    IKE  0600000c 01000000 c0a8d7e3 06000207 04308201 fe308201 67a00302 01000201
```

```
Apr 29, 22:24:41  Debug    IKE  01300d06 092a8648 86f70d01 01040500 30463113 30110603 55040a13 0a456d62
Apr 29, 22:24:41  Debug    IKE  65646465 644e4731 10300e06 0355040b 13074c6f 63616c43 41311d30 1b060355
Apr 29, 22:24:41  Debug    IKE  04031314 43412d30 303a3038 3a64613a 35323a31 653a6532 301e170d 30373031
Apr 29, 22:24:41  Debug    IKE  30353137 33383138 5a170d32 37303130 31313733 3831385a 30443113 30110603
Apr 29, 22:24:41  Debug    IKE  55040a13 0a456d62 65646465 644e4731 11300f06 0355040b 13084761 74657761
Apr 29, 22:24:41  Debug    IKE  7973311a 30180603 55040313 1130303a 30383a64 613a3532 3a31653a 65323081
Apr 29, 22:24:41  Debug    IKE  9f300d06 092a8648 86f70d01 01010500 03818d00 30818902 818100a2 daa41df7
Apr 29, 22:24:41  Debug    IKE  9056c925 ce98ce00 b9e75b09 9662f936 c7d110a7 bef80788 8d69ac8a 9da9b9a4
Apr 29, 22:24:41  Debug    IKE  12e8b723 aba464b0 95d9ecb1 63e034e7 9e030893 2073d911 08aaa20d 34acedca
Apr 29, 22:24:41  Debug    IKE  96fd7164 a9cb9a4b 64d71748 2a9babb6 48ce4292 4a2b0477 0eaa6eca f8d094c6
Apr 29, 22:24:41  Debug    IKE  351d038f e8f1be89 f80ec724 ad07da00 a3b1b2dd 9deee1e2 37721702 03010001
Apr 29, 22:24:41  Debug    IKE  300d0609 2a864886 f70d0101 04050003 81810025 182d5a3c f4149148 74730145
Apr 29, 22:24:41  Debug    IKE  f7d34d48 0e6ccdd7 35970ae0 57d38c6e d6e9be83 7cb9ccec bbfd2147 6ec25996
Apr 29, 22:24:41  Debug    IKE  b8e73b48 693f9061 d79ea1b1 0ceb9780 6921cb7f a72f5dc4 7a8f25bf a696f1b8
Apr 29, 22:24:41  Debug    IKE  658aa113 3f2a5334 5f0fcf14 32608c84 869ac925 74ccb879 6b7ec042 45598edc
Apr 29, 22:24:41  Debug    IKE  0224b098 487fbca0 c7fc31b0 cdac3b4e 27f5b009 00020904 30820200 30820169
Apr 29, 22:24:41  Debug    IKE  a0030201 00020101 300d0609 2a864886 f70d0101 04050030 46311330 11060355
Apr 29, 22:24:41  Debug    IKE  040a130a 456d6265 64646564 4e473110 300e0603 55040b13 074c6f63 616c4341
Apr 29, 22:24:41  Debug    IKE  311d301b 06035504 03131443 412d3030 3a30383a 64613a35 323a3165 3a653230
Apr 29, 22:24:41  Debug    IKE  1e170d30 37303130 35313733 3831315a 170d3237 30313031 31373338 31315a30
Apr 29, 22:24:41  Debug    IKE  46311330 11060355 040a130a 456d6265 64646564 4e473110 300e0603 55040b13
Apr 29, 22:24:41  Debug    IKE  074c6f63 616c4341 311d301b 06035504 03131443 412d3030 3a30383a 64613a35
Apr 29, 22:24:41  Debug    IKE  323a3165 3a653230 819f300d 06092a86 4886f70d 01010105 0003818d 00308189
Apr 29, 22:24:41  Debug    IKE  02818100 ca5ce97c 521b0121 06ed390d 27cf47c4 bb853814 960394ba 7d0272c8
Apr 29, 22:24:41  Debug    IKE  9d374b10 81d1a995 33052230 b33cafd1 8c9e1df5 593c7ba4 c4ab3633 4a1aa746
Apr 29, 22:24:41  Debug    IKE  6a9ec899 ccbb2de1 47b1a944 7ece0da4 92b54596 a403fbf0 2a448a6c b5cca96c
Apr 29, 22:24:41  Debug    IKE  1d5bc942 7add33a6 e4704fd1 6ba399e4 64cd73bc 0bd73d52 b989fad3 fa17b6d3
Apr 29, 22:24:41  Debug    IKE  9e160043 02030100 01300d06 092a8648 86f70d01 01040500 03818100 b5531db5
Apr 29, 22:24:41  Debug    IKE  dde78683 96f23861 6a2e1af2 276029bd 64fca0f7 311dc44c fca38c80 98727e01
Apr 29, 22:24:41  Debug    IKE  f99cbbf4 ca365eed 4f0bb02a 33773315 838a3175 21991ef5 85ffd601 9ca0cfef
Apr 29, 22:24:41  Debug    IKE  7136859d bae0dd71 f77485a9 e2b978fa fcda8292 39ace195 a691ef08 fe9e8c95
Apr 29, 22:24:41  Debug    IKE  94b7e042 811e4c94 82bf52f0 eee412e1 aeff9e43 54df16d4 72a022b4 00000084
Apr 29, 22:24:41  Debug    IKE  5b8ff1d4 457882c6 ef4bb230 f1419ddd 9e5af68f fcbc2566 e76239f5 ff32caee
Apr 29, 22:24:41  Debug    IKE  d28ee170 75db59d6 cf0a8ad6 f729356a f26e9454 7a79ceda 38fb7ff1 53e7ba4b
Apr 29, 22:24:41  Debug    IKE  bacfdd44 29e07f97 63cc6c6b ad99c371 bb617da4 a6765bd0 f7c6eced 6c3cfdc8
Apr 29, 22:24:41  Debug    IKE  6f4ccfa7 d95574cb d2f7bb05 77431e8f ea979bcb 89983214 fc9dc44e 0be88f22
Apr 29, 22:24:41  Debug    IKE  00000000 00000007
Apr 29, 22:24:41  Debug    IKE  padding len=7
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 05100201 00000000 000004c4 0600000c
Apr 29, 22:24:41  Debug    IKE  01000000 c0a8d7e3 06000207 04308201 fe308201 67a00302 01000201 01300d06
Apr 29, 22:24:41  Debug    IKE  092a8648 86f70d01 01040500 30463113 30110603 55040a13 0a456d62 65646465
Apr 29, 22:24:41  Debug    IKE  644e4731 10300e06 0355040b 13074c6f 63616c43 41311d30 1b060355 04031314
Apr 29, 22:24:41  Debug    IKE  43412d30 303a3038 3a64613a 35323a31 653a6532 301e170d 30373031 30353137
Apr 29, 22:24:41  Debug    IKE  33383138 5a170d32 37303130 31313733 3831385a 30443113 30110603 55040a13
Apr 29, 22:24:41  Debug    IKE  0a456d62 65646465 644e4731 11300f06 0355040b 13084761 74657761 7973311a
Apr 29, 22:24:41  Debug    IKE  30180603 55040313 1130303a 30383a64 613a3532 3a31653a 65323081 9f300d06
Apr 29, 22:24:41  Debug    IKE  092a8648 86f70d01 01010500 03818d00 30818902 818100a2 daa41df7 9056c925
Apr 29, 22:24:41  Debug    IKE  ce98ce00 b9e75b09 9662f936 c7d110a7 bef80788 8d69ac8a 9da9b9a4 12e8b723
Apr 29, 22:24:41  Debug    IKE  aba464b0 95d9ecb1 63e034e7 9e030893 2073d911 08aaa20d 34acedca 96fd7164
Apr 29, 22:24:41  Debug    IKE  a9cb9a4b 64d71748 2a9babb6 48ce4292 4a2b0477 0eaa6eca f8d094c6 351d038f
Apr 29, 22:24:41  Debug    IKE  e8f1be89 f80ec724 ad07da00 a3b1b2dd 9deee1e2 37721702 03010001 300d0609
Apr 29, 22:24:41  Debug    IKE  2a864886 f70d0101 04050003 81810025 182d5a3c f4149148 74730145 f7d34d48
Apr 29, 22:24:41  Debug    IKE  0e6ccdd7 35970ae0 57d38c6e d6e9be83 7cb9ccec bbfd2147 6ec25996 b8e73b48
Apr 29, 22:24:41  Debug    IKE  693f9061 d79ea1b1 0ceb9780 6921cb7f a72f5dc4 7a8f25bf a696f1b8 658aa113
Apr 29, 22:24:41  Debug    IKE  3f2a5334 5f0fcf14 32608c84 869ac925 74ccb879 6b7ec042 45598edc 0224b098
Apr 29, 22:24:41  Debug    IKE  487fbca0 c7fc31b0 cdac3b4e 27f5b009 00020904 30820200 30820169 a0030201
Apr 29, 22:24:41  Debug    IKE  00020101 300d0609 2a864886 f70d0101 04050030 46311330 11060355 040a130a
Apr 29, 22:24:41  Debug    IKE  456d6265 64646564 4e473110 300e0603 55040b13 074c6f63 616c4341 311d301b
Apr 29, 22:24:41  Debug    IKE  06035504 03131443 412d3030 3a30383a 64613a35 323a3165 3a653230 1e170d30
Apr 29, 22:24:41  Debug    IKE  37303130 35313733 3831315a 170d3237 30313031 31373338 31315a30 46311330
Apr 29, 22:24:41  Debug    IKE  11060355 040a130a 456d6265 64646564 4e473110 300e0603 55040b13 074c6f63
Apr 29, 22:24:41  Debug    IKE  616c4341 311d301b 06035504 03131443 412d3030 3a30383a 64613a35 323a3165
Apr 29, 22:24:41  Debug    IKE  3a653230 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100
Apr 29, 22:24:41  Debug    IKE  ca5ce97c 521b0121 06ed390d 27cf47c4 bb853814 960394ba 7d0272c8 9d374b10
Apr 29, 22:24:41  Debug    IKE  81d1a995 33052230 b33cafd1 8c9e1df5 593c7ba4 c4ab3633 4a1aa746 6a9ec899
Apr 29, 22:24:41  Debug    IKE  ccbb2de1 47b1a944 7ece0da4 92b54596 a403fbf0 2a448a6c b5cca96c 1d5bc942
Apr 29, 22:24:41  Debug    IKE  7add33a6 e4704fd1 6ba399e4 64cd73bc 0bd73d52 b989fad3 fa17b6d3 9e160043
Apr 29, 22:24:41  Debug    IKE  02030100 01300d06 092a8648 86f70d01 01040500 03818100 b5531db5 dde78683
Apr 29, 22:24:41  Debug    IKE  96f23861 6a2e1af2 276029bd 64fca0f7 311dc44c fca38c80 98727e01 f99cbbf4
Apr 29, 22:24:41  Debug    IKE  ca365eed 4f0bb02a 33773315 838a3175 21991ef5 85ffd601 9ca0cfef 7136859d
Apr 29, 22:24:41  Debug    IKE  bae0dd71 f77485a9 e2b978fa fcda8292 39ace195 a691ef08 fe9e8c95 94b7e042
Apr 29, 22:24:41  Debug    IKE  811e4c94 82bf52f0 eee412e1 aeff9e43 54df16d4 72a022b4 00000084 5b8ff1d4
```

```
Apr 29, 22:24:41  Debug    IKE  457882c6 ef4bb230 f1419ddd 9e5af68f fcbc2566 e76239f5 ff32caee d28ee170
Apr 29, 22:24:41  Debug    IKE  75db59d6 cf0a8ad6 f729356a f26e9454 7a79ceda 38fb7ff1 53e7ba4b bacfdd44
Apr 29, 22:24:41  Debug    IKE  29e07f97 63cc6c6b ad99c371 bb617da4 a6765bd0 f7c6eced 6c3cfdc8 6f4ccfa7
Apr 29, 22:24:41  Debug    IKE  d95574cb d2f7bb05 77431e8f ea979bcb 89983214 fc9dc44e 0be88f22 00000000
Apr 29, 22:24:41  Debug    IKE  00000007
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=5(id)
Apr 29, 22:24:41  Debug    IKE  seen nptype=6(cert)
Apr 29, 22:24:41  Debug    IKE  seen nptype=6(cert)
Apr 29, 22:24:41  Debug    IKE  seen nptype=9(sig)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  CERT saved:
Apr 29, 22:24:41  Debug    IKE  308201fe 30820167 a0030201 00020101 300d0609 2a864886 f70d0101 04050030
Apr 29, 22:24:41  Debug    IKE  46311330 11060355 040a130a 456d6265 64646564 4e473110 300e0603 55040b13
Apr 29, 22:24:41  Debug    IKE  074c6f63 616c4341 311d301b 06035504 03131443 412d3030 3a30383a 64613a35
Apr 29, 22:24:41  Debug    IKE  323a3165 3a653230 1e170d30 37303130 35313733 3831385a 170d3237 30313031
Apr 29, 22:24:41  Debug    IKE  31373338 31385a30 44311330 11060355 040a130a 456d6265 64646564 4e473111
Apr 29, 22:24:41  Debug    IKE  300f0603 55040b13 08476174 65776179 73311a30 18060355 04031311 30303a30
Apr 29, 22:24:41  Debug    IKE  383a6461 3a35323a 31653a65 3230819f 300d0609 2a864886 f70d0101 01050003
Apr 29, 22:24:41  Debug    IKE  818d0030 81890281 8100a2da a41df790 56c925ce 98ce00b9 e75b0996 62f936c7
Apr 29, 22:24:41  Debug    IKE  d110a7be f807888d 69ac8a9d a9b9a412 e8b723ab a464b095 d9ecb163 e034e79e
Apr 29, 22:24:41  Debug    IKE  03089320 73d91108 aaa20d34 acedca96 fd7164a9 cb9a4b64 d717482a 9babb648
Apr 29, 22:24:41  Debug    IKE  ce42924a 2b04770e aa6ecaf8 d094c635 1d038fe8 f1be89f8 0ec724ad 07da00a3
Apr 29, 22:24:41  Debug    IKE  b1b2dd9d eee1e237 72170203 01000130 0d06092a 864886f7 0d010104 05000381
Apr 29, 22:24:41  Debug    IKE  81002518 2d5a3cf4 14914874 730145f7 d34d480e 6ccdd735 970ae057 d38c6ed6
Apr 29, 22:24:41  Debug    IKE  e9be837c b9ccecbb fd21476e c25996b8 e73b4869 3f9061d7 9ea1b10c eb978069
Apr 29, 22:24:41  Debug    IKE  21cb7fa7 2f5dc47a 8f25bfa6 96f1b865 8aa1133f 2a53345f 0fcf1432 608c8486
Apr 29, 22:24:41  Debug    IKE  9ac92574 ccb8796b 7ec04245 598edc02 24b09848 7fbca0c7 fc31b0cd ac3b4e27
Apr 29, 22:24:41  Debug    IKE  f5b0
Apr 29, 22:24:41  Debug    IKE  Certificate:
Apr 29, 22:24:41  Debug    IKE      Data:
Apr 29, 22:24:41  Debug    IKE          Version: 1 (0x0)
Apr 29, 22:24:41  Debug    IKE          Serial Number: 1 (0x1)
Apr 29, 22:24:41  Debug    IKE          Signature Algorithm: md5WithRSAEncryption
Apr 29, 22:24:41  Debug    IKE          Issuer: O=EmbeddedNG, OU=LocalCA, CN=CA-00:08:da:52:1e:e2
Apr 29, 22:24:41  Debug    IKE          Validity
Apr 29, 22:24:41  Debug    IKE              Not Before: Jan  5 17:38:18 2007 GMT
Apr 29, 22:24:41  Debug    IKE              Not After : Jan  1 17:38:18 2027 GMT
Apr 29, 22:24:41  Debug    IKE          Subject: O=EmbeddedNG, OU=Gateways, CN=00:08:da:52:1e:e2
Apr 29, 22:24:41  Debug    IKE          Subject Public Key Info:
Apr 29, 22:24:41  Debug    IKE              Public Key Algorithm: rsaEncryption
Apr 29, 22:24:41  Debug    IKE              RSA Public Key: (1024 bit)
Apr 29, 22:24:41  Debug    IKE                  Modulus (1024 bit):
Apr 29, 22:24:41  Debug    IKE                      00:a2:da:a4:1d:f7:90:56:c9:25:ce:98:ce:00:b9:
Apr 29, 22:24:41  Debug    IKE                      e7:5b:09:96:62:f9:36:c7:d1:10:a7:be:f8:07:88:
Apr 29, 22:24:41  Debug    IKE                      8d:69:ac:8a:9d:a9:b9:a4:12:e8:b7:23:ab:a4:64:
Apr 29, 22:24:41  Debug    IKE                      b0:95:d9:ec:b1:63:e0:34:e7:9e:03:08:93:20:73:
Apr 29, 22:24:41  Debug    IKE                      d9:11:08:aa:a2:0d:34:ac:ed:ca:96:fd:71:64:a9:
Apr 29, 22:24:41  Debug    IKE                      cb:9a:4b:64:d7:17:48:2a:9b:ab:b6:48:ce:42:92:
Apr 29, 22:24:41  Debug    IKE                      4a:2b:04:77:0e:aa:6e:ca:f8:d0:94:c6:35:1d:03:
Apr 29, 22:24:41  Debug    IKE                      8f:e8:f1:be:89:f8:0e:c7:24:ad:07:da:00:a3:b1:
Apr 29, 22:24:41  Debug    IKE                      b2:dd:9d:ee:e1:e2:37:72:17
Apr 29, 22:24:41  Debug    IKE                  Exponent: 65537 (0x10001)
Apr 29, 22:24:41  Debug    IKE      Signature Algorithm: md5WithRSAEncryption
Apr 29, 22:24:41  Debug    IKE          25:18:2d:5a:3c:f4:14:91:48:74:73:01:45:f7:d3:4d:48:0e:
Apr 29, 22:24:41  Debug    IKE          6c:cd:d7:35:97:0a:e0:57:d3:8c:6e:d6:e9:be:83:7c:b9:cc:
Apr 29, 22:24:41  Debug    IKE          ec:bb:fd:21:47:6e:c2:59:96:b8:e7:3b:48:69:3f:90:61:d7:
Apr 29, 22:24:41  Debug    IKE          9e:a1:b1:0c:eb:97:80:69:21:cb:7f:a7:2f:5d:c4:7a:8f:25:
Apr 29, 22:24:41  Debug    IKE          bf:a6:96:f1:b8:65:8a:a1:13:3f:2a:53:34:5f:0f:cf:14:32:
Apr 29, 22:24:41  Debug    IKE          60:8c:84:86:9a:c9:25:74:cc:b8:79:6b:7e:c0:42:45:59:8e:
Apr 29, 22:24:41  Debug    IKE          dc:02:24:b0:98:48:7f:bc:a0:c7:fc:31:b0:cd:ac:3b:4e:27:
Apr 29, 22:24:41  Debug    IKE          f5:b0
Apr 29, 22:24:41  Warning  IKE  ignore 2nd CERT payload.
Apr 29, 22:24:41  Debug    IKE  SIGN passed:
Apr 29, 22:24:41  Debug    IKE  5b8ff1d4 457882c6 ef4bb230 f1419ddd 9e5af68f fcbc2566 e76239f5 ff32caee
Apr 29, 22:24:41  Debug    IKE  d28ee170 75db59d6 cf0a8ad6 f729356a f26e9454 7a79ceda 38fb7ff1 53e7ba4b
Apr 29, 22:24:41  Debug    IKE  bacfdd44 29e07f97 63cc6c6b ad99c371 bb617da4 a6765bd0 f7c6eced 6c3cfdc8
Apr 29, 22:24:41  Debug    IKE  6f4ccfa7 d95574cb d2f7bb05 77431e8f ea979bcb 89983214 fc9dc44e 0be88f22
Apr 29, 22:24:41  Debug    IKE  CERT validated
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  b96894cc 37b2b2de 1b3577ac a237942d dd7aa820 39c3a1ff a7b7523d a32f9e3e
Apr 29, 22:24:41  Debug    IKE  96596ad8 3ca1baa9 16424e6a e5173ddd efb90d95 b29ffecb 115764aa d07ccec8
Apr 29, 22:24:41  Debug    IKE  37d17202 2ddba5bd c265c09f 0aeaeb3c 56ce30ad e23cf433 a2706d1a c3d6e214
Apr 29, 22:24:41  Debug    IKE  d06e12ed cb19f80f 0f4ae2c2 e8a36a1b dacf2c56 3df5318b 159bb067 04b8a859
```

```
Apr 29, 22:24:41  Debug    IKE  6a96db52 8aa39d7e 26c35c97 8f6815c7 7020255b 4650332c d4f64bf3 1d4b4a2c
Apr 29, 22:24:41  Debug    IKE  fa63ddcf c9cf8f99 3d1b7422 f62ee5c8 5be1d8a2 7502582e 76389d19 6a052d4c
Apr 29, 22:24:41  Debug    IKE  58280349 b98032b3 fd9e784c d2253873 4107e33c c94cd90a 51e8caf9 d2764a32
Apr 29, 22:24:41  Debug    IKE  58c1fabe c79e7c74 0c61b49f 89b4bbd8 62d836cd d2f9a839 5f1305dc acdf8b8a
Apr 29, 22:24:41  Debug    IKE  83f17532 d8e4e1d8 341d8008 9acf997d 00000001 00000001 00000028 01010001
Apr 29, 22:24:41  Debug    IKE  00000020 01010000 800b0001 800c0384 80010005 8003fadd 80020002 80040002
Apr 29, 22:24:41  Debug    IKE  01000000 c0a8d7e3
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH (init) computed:
Apr 29, 22:24:41  Debug    IKE  9516df4e dceb7572 bdb5853c 7d0d11c5 db742faf
Apr 29, 22:24:41  Debug    IKE  SIG authenticated
Apr 29, 22:24:41  Debug    IKE  peer's ID:2007-04-29 22:24:41: DEBUG:
Apr 29, 22:24:41  Debug    IKE  01000000 c0a8d7e3
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  compute IV for phase2
Apr 29, 22:24:41  Debug    IKE  phase1 last IV:
Apr 29, 22:24:41  Debug    IKE  8822330c fbd77f55 c6deea76
Apr 29, 22:24:41  Debug    IKE  hash(sha1)
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  phase2 IV computed:
Apr 29, 22:24:41  Debug    IKE  4fbe8d03 8e189c82
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  c6deea76 0000001c 00000001 01106002 341d8008 9acf997d 83f17532 d8e4e1d8
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  61059f2e be838ca5 858d3112 aa3859ed 52fd60ca
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 4
Apr 29, 22:24:41  Debug    IKE  0b000018 61059f2e be838ca5 858d3112 aa3859ed 52fd60ca 0000001c 00000001
Apr 29, 22:24:41  Debug    IKE  01106002 341d8008 9acf997d 83f17532 d8e4e1d8 00000004
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  4fbe8d03 8e189c82
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  303b443a 9eb65c18
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  84 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100501 c6deea76 00000054 2f8b5434
Apr 29, 22:24:41  Debug    IKE  8858dd57 2bf9090f eeda6c1c ab938510 7e4a8935 b9f6ee6c 20969b61 763eba14
Apr 29, 22:24:41  Debug    IKE  439c8620 fd4b0ed9 b0cb233c 303b443a 9eb65c18
Apr 29, 22:24:41  Debug    IKE  sendto Information notify.
Apr 29, 22:24:41  Debug    IKE  IV freed
Apr 29, 22:24:41  Info     IKE  ISAKMP-SA established 192.168.215.3[500]-192.168.215.227[500] spi:341d80089acf997d:
83f17532d8e4e1d8
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  76 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000004c c32e3412
Apr 29, 22:24:41  Debug    IKE  336b19a8 82158078 5d6966a4 ef104e8e 95577c34 459b996b 628d1d3e da9db06f
Apr 29, 22:24:41  Debug    IKE  2662bd6a dc08829f 59c15c45
Apr 29, 22:24:41  Debug    IKE  compute IV for phase2
Apr 29, 22:24:41  Debug    IKE  phase1 last IV:
Apr 29, 22:24:41  Debug    IKE  8822330c fbd77f55 70fa1e90
Apr 29, 22:24:41  Debug    IKE  hash(sha1)
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  phase2 IV computed:
Apr 29, 22:24:41  Debug    IKE  7f86169b 821c377e
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  dc08829f 59c15c45
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  7f86169b 821c377e
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
```

```
Apr 29, 22:24:41  Debug    IKE  0e000018 4ed7e6bc 0388044e 3a6616a5 dbfbc9fc 7d20cdc0 00000010 0100c2f9
Apr 29, 22:24:41  Debug    IKE  800d0000 000e0000 00000000 00000007
Apr 29, 22:24:41  Debug    IKE  padding len=7
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000004c 0e000018
Apr 29, 22:24:41  Debug    IKE  4ed7e6bc 0388044e 3a6616a5 dbfbc9fc 7d20cdc0 00000010 0100c2f9 800d0000
Apr 29, 22:24:41  Debug    IKE  000e0000 00000000 00000007
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000004c 0e000018
Apr 29, 22:24:41  Debug    IKE  4ed7e6bc 0388044e 3a6616a5 dbfbc9fc 7d20cdc0 00000010 0100c2f9 800d0000
Apr 29, 22:24:41  Debug    IKE  000e0000 00000000 00000007
Apr 29, 22:24:41  Debug    IKE  Seen payload 8
Apr 29, 22:24:41  Debug    IKE  0e000018 4ed7e6bc 0388044e 3a6616a5 dbfbc9fc 7d20cdc0
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  70fa1e90 00000010 0100c2f9 800d0000 000e0000
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  4ed7e6bc 0388044e 3a6616a5 dbfbc9fc 7d20cdc0
Apr 29, 22:24:41  Debug    IKE  Seen payload 14
Apr 29, 22:24:41  Debug    IKE  00000010 0100c2f9 800d0000 000e0000
Apr 29, 22:24:41  Debug    IKE  Configuration exchange type mode config REQUEST
Apr 29, 22:24:41  Debug    IKE  Short attribute XAUTH_TYPE = 0
Apr 29, 22:24:41  Debug    IKE  Attribute XAUTH_USER_NAME, len 0
Apr 29, 22:24:41  Debug    IKE  Sending MODE_CFG REPLY
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  70fa1e90 00000013 0200c2f9 800d0000 000e0003 76706e
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  b8d07255 4032977c a0c5fab7 d62bb546 994639ff
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet to send
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000047 0e000018
Apr 29, 22:24:41  Debug    IKE  b8d07255 4032977c a0c5fab7 d62bb546 994639ff 00000013 0200c2f9 800d0000
Apr 29, 22:24:41  Debug    IKE  000e0003 76706e
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 5
Apr 29, 22:24:41  Debug    IKE  0e000018 b8d07255 4032977c a0c5fab7 d62bb546 994639ff 00000013 0200c2f9
Apr 29, 22:24:41  Debug    IKE  800d0000 000e0003 76706e00 00000005
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  dc08829f 59c15c45
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  133ff102 8e9509d4
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  76 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 76 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000004c b007a8d6
Apr 29, 22:24:41  Debug    IKE  789277bc e4debc6f 990029fa baf60cd4 7af5c94e 7113fe32 a2db084f c215cc71
Apr 29, 22:24:41  Debug    IKE  e5bc66f3 133ff102 8e9509d4
Apr 29, 22:24:41  Debug    IKE  sendto mode config attr.
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  100 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000064 d7a59455
Apr 29, 22:24:41  Debug    IKE  22125ba8 ef11efb8 77185c46 f9a64fd9 632c7621 d4def83b 95e869b7 9d37ba30
Apr 29, 22:24:41  Debug    IKE  b4e7284f dd89a197 a8532b3f 135aed33 996175e2 81480209 47099a03 7e037a55
Apr 29, 22:24:41  Debug    IKE  2d511548
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  7e037a55 2d511548
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  133ff102 8e9509d4
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:41  Debug    IKE  0e000018 cc4eaacc dabc2079 616d414e 7123354c 279de682 0000002e 0100e316
Apr 29, 22:24:41  Debug    IKE  800d0000 0012001a 56504e20 53657276 65723a20 456e7465 72205061 7373776f
```

```
Apr 29, 22:24:41  Debug    IKE  7264000f 00000001
Apr 29, 22:24:41  Debug    IKE  padding len=1
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000064 0e000018
Apr 29, 22:24:41  Debug    IKE  cc4eaacc dabc2079 616d414e 7123354c 279de682 0000002e 0100e316 800d0000
Apr 29, 22:24:41  Debug    IKE  0012001a 56504e20 53657276 65723a20 456e7465 72205061 7373776f 7264000f
Apr 29, 22:24:41  Debug    IKE  00000001
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000064 0e000018
Apr 29, 22:24:41  Debug    IKE  cc4eaacc dabc2079 616d414e 7123354c 279de682 0000002e 0100e316 800d0000
Apr 29, 22:24:41  Debug    IKE  0012001a 56504e20 53657276 65723a20 456e7465 72205061 7373776f 7264000f
Apr 29, 22:24:41  Debug    IKE  00000001
Apr 29, 22:24:41  Debug    IKE  Seen payload 8
Apr 29, 22:24:41  Debug    IKE  0e000018 cc4eaacc dabc2079 616d414e 7123354c 279de682
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  70fa1e90 0000002e 0100e316 800d0000 0012001a 56504e20 53657276 65723a20
Apr 29, 22:24:41  Debug    IKE  456e7465 72205061 7373776f 7264000f 0000
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  cc4eaacc dabc2079 616d414e 7123354c 279de682
Apr 29, 22:24:41  Debug    IKE  Seen payload 14
Apr 29, 22:24:41  Debug    IKE  0000002e 0100e316 800d0000 0012001a 56504e20 53657276 65723a20 456e7465
Apr 29, 22:24:41  Debug    IKE  72205061 7373776f 7264000f 0000
Apr 29, 22:24:41  Debug    IKE  Configuration exchange type mode config REQUEST
Apr 29, 22:24:41  Debug    IKE  Short attribute XAUTH_TYPE = 0
Apr 29, 22:24:41  Debug    IKE  Attribute XAUTH_CHALLENGE, len 26
Apr 29, 22:24:41  Warning  IKE  Ignored attribute XAUTH_CHALLENGE
Apr 29, 22:24:41  Debug    IKE  Attribute XAUTH_USER_PASSWORD, len 0
Apr 29, 22:24:41  Debug    IKE  Sending MODE_CFG REPLY
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  70fa1e90 0000001f 0200e316 800d0000 000f000f 63656c6c 732e696e 2e667261
Apr 29, 22:24:41  Debug    IKE  6d6573
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  943d6b10 0d845c4b e010ae3c fd486348 9621c65d
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet to send
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000053 0e000018
Apr 29, 22:24:41  Debug    IKE  943d6b10 0d845c4b e010ae3c fd486348 9621c65d 0000001f 0200e316 800d0000
Apr 29, 22:24:41  Debug    IKE  000f000f 63656c6c 732e696e 2e667261 6d6573
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 1
Apr 29, 22:24:41  Debug    IKE  0e000018 943d6b10 0d845c4b e010ae3c fd486348 9621c65d 0000001f 0200e316
Apr 29, 22:24:41  Debug    IKE  800d0000 000f000f 63656c6c 732e696e 2e667261 6d657301
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  7e037a55 2d511548
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  237f05a4 1a8bc9d0
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  84 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000054 b259750b
Apr 29, 22:24:41  Debug    IKE  318ab117 fa9db6ad 9485e3fa 902f1ef1 d1216461 2ebf4593 61cf1888 a4b2797e
Apr 29, 22:24:41  Debug    IKE  76f3f910 6fa84bfc 90428867 237f05a4 1a8bc9d0
Apr 29, 22:24:41  Debug    IKE  sendto mode config attr.
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  100 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000064 d7a59455
Apr 29, 22:24:41  Debug    IKE  22125ba8 ef11efb8 77185c46 f9a64fd9 632c7621 d4def83b 95e869b7 9d37ba30
Apr 29, 22:24:41  Debug    IKE  b4e7284f dd89a197 a8532b3f 135aed33 996175e2 81480209 47099a03 7e037a55
Apr 29, 22:24:41  Debug    IKE  2d511548
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  7e037a55 2d511548
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
```

```
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  237f05a4 1a8bc9d0
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:41  Debug    IKE  3e40f4be 58506ac8 dabc2079 616d414e 7123354c 279de682 0000002e 0100e316
Apr 29, 22:24:41  Debug    IKE  800d0000 0012001a 56504e20 53657276 65723a20 456e7465 72205061 7373776f
Apr 29, 22:24:41  Debug    IKE  7264000f 00000001
Apr 29, 22:24:41  Debug    IKE  padding len=1
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000064 3e40f4be
Apr 29, 22:24:41  Debug    IKE  58506ac8 dabc2079 616d414e 7123354c 279de682 0000002e 0100e316 800d0000
Apr 29, 22:24:41  Debug    IKE  0012001a 56504e20 53657276 65723a20 456e7465 72205061 7373776f 7264000f
Apr 29, 22:24:41  Debug    IKE  00000001
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000064 3e40f4be
Apr 29, 22:24:41  Debug    IKE  58506ac8 dabc2079 616d414e 7123354c 279de682 0000002e 0100e316 800d0000
Apr 29, 22:24:41  Debug    IKE  0012001a 56504e20 53657276 65723a20 456e7465 72205061 7373776f 7264000f
Apr 29, 22:24:41  Debug    IKE  00000001
Apr 29, 22:24:41  Warning  IKE  Short payload
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  108 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000006c 4e23f0e4
Apr 29, 22:24:41  Debug    IKE  95bbe340 3b5910ff f7e51191 fbb0a5ce 3f24d6cb b9d4a0c5 23aae9cb 7967cf1a
Apr 29, 22:24:41  Debug    IKE  dfc3fb64 1f950576 ad3072f6 c0dde5d2 33c44927 eb82bb8c 49736e7f 9bc8980f
Apr 29, 22:24:41  Debug    IKE  13bbab40 4d5ae451 9471e45f
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  4d5ae451 9471e45f
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  237f05a4 1a8bc9d0
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:41  Debug    IKE  0e000018 8c9c1bbe c1232de3 b6637931 46fe89d1 8a3a44d0 00000035 0300185d
Apr 29, 22:24:41  Debug    IKE  80140001 00110025 56504e20 53657276 65723a20 53756363 65737366 756c7920
Apr 29, 22:24:41  Debug    IKE  41757468 656e7469 63617465 64000002
Apr 29, 22:24:41  Debug    IKE  padding len=2
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000006c 0e000018
Apr 29, 22:24:41  Debug    IKE  8c9c1bbe c1232de3 b6637931 46fe89d1 8a3a44d0 00000035 0300185d 80140001
Apr 29, 22:24:41  Debug    IKE  00110025 56504e20 53657276 65723a20 53756363 65737366 756c7920 41757468
Apr 29, 22:24:41  Debug    IKE  656e7469 63617465 64000002
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 0000006c 0e000018
Apr 29, 22:24:41  Debug    IKE  8c9c1bbe c1232de3 b6637931 46fe89d1 8a3a44d0 00000035 0300185d 80140001
Apr 29, 22:24:41  Debug    IKE  00110025 56504e20 53657276 65723a20 53756363 65737366 756c7920 41757468
Apr 29, 22:24:41  Debug    IKE  656e7469 63617465 64000002
Apr 29, 22:24:41  Debug    IKE  Seen payload 8
Apr 29, 22:24:41  Debug    IKE  0e000018 8c9c1bbe c1232de3 b6637931 46fe89d1 8a3a44d0
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  70fa1e90 00000035 0300185d 80140001 00110025 56504e20 53657276 65723a20
Apr 29, 22:24:41  Debug    IKE  53756363 65737366 756c7920 41757468 656e7469 63617465 64
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  8c9c1bbe c1232de3 b6637931 46fe89d1 8a3a44d0
Apr 29, 22:24:41  Debug    IKE  Seen payload 14
Apr 29, 22:24:41  Debug    IKE  00000035 0300185d 80140001 00110025 56504e20 53657276 65723a20 53756363
Apr 29, 22:24:41  Debug    IKE  65737366 756c7920 41757468 656e7469 63617465 64
Apr 29, 22:24:41  Debug    IKE  Configuration exchange type mode config SET
Apr 29, 22:24:41  Debug    IKE  Attribute XAUTH_STATUS
Apr 29, 22:24:41  Debug    IKE  Attribute XAUTH_MESSAGE
Apr 29, 22:24:41  Debug    IKE  Unexpected SET attribute XAUTH_MESSAGE
Apr 29, 22:24:41  Debug    IKE  Sending MODE_CFG ACK
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  70fa1e90 0000000c 0400185d 80140001
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  96d0a25b 7154f148 4576ceb6 42e65b2d 0192e29c
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet to send
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000040 0e000018
```

```
Apr 29, 22:24:41  Debug    IKE  96d0a25b 7154f148 4576ceb6 42e65b2d 0192e29c 0000000c 0400185d 80140001
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 4
Apr 29, 22:24:41  Debug    IKE  0e000018 96d0a25b 7154f148 4576ceb6 42e65b2d 0192e29c 0000000c 0400185d
Apr 29, 22:24:41  Debug    IKE  80140001 00000004
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  4d5ae451 9471e45f
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  f63d1891 9dd086fa
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  68 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 68 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 70fa1e90 00000044 f3ccbb29
Apr 29, 22:24:41  Debug    IKE  80d75eaf c1eda415 342cf212 4c71bcf6 49ee3a5c 6a4d96a8 39609fdb f63d1891
Apr 29, 22:24:41  Debug    IKE  9dd086fa
Apr 29, 22:24:41  Debug    IKE  sendto mode config attr.
Apr 29, 22:24:41  Debug    IKE  Sending MODE_CFG REQUEST
Apr 29, 22:24:41  Debug    IKE  IV freed
Apr 29, 22:24:41  Debug    IKE  compute IV for phase2
Apr 29, 22:24:41  Debug    IKE  phase1 last IV:
Apr 29, 22:24:41  Debug    IKE  8822330c fbd77f55 bcf8f3db
Apr 29, 22:24:41  Debug    IKE  hash(sha1)
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  phase2 IV computed:
Apr 29, 22:24:41  Debug    IKE  be3ca1b1 4023ecbc
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  bcf8f3db 00000058 0100f291 00010004 00000000 00020004 00000000 00030004
Apr 29, 22:24:41  Debug    IKE  00000000 00040004 00000000 70000004 00000000 70020004 00000000 70030004
Apr 29, 22:24:41  Debug    IKE  00000000 70040004 00000000 70060004 00000000 00070004 00000000
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  a4aac0a3 8bdb1e57 8523fc4a 9b5db280 290e2a88
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet to send
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000008c 0e000018
Apr 29, 22:24:41  Debug    IKE  a4aac0a3 8bdb1e57 8523fc4a 9b5db280 290e2a88 00000058 0100f291 00010004
Apr 29, 22:24:41  Debug    IKE  00000000 00020004 00000000 00030004 00000000 00040004 00000000 70000004
Apr 29, 22:24:41  Debug    IKE  00000000 70020004 00000000 70030004 00000000 70040004 00000000 70060004
Apr 29, 22:24:41  Debug    IKE  00000000 00070004 00000000
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 8
Apr 29, 22:24:41  Debug    IKE  0e000018 a4aac0a3 8bdb1e57 8523fc4a 9b5db280 290e2a88 00000058 0100f291
Apr 29, 22:24:41  Debug    IKE  00010004 00000000 00020004 00000000 00030004 00000000 00040004 00000000
Apr 29, 22:24:41  Debug    IKE  70000004 00000000 70020004 00000000 70030004 00000000 70040004 00000000
Apr 29, 22:24:41  Debug    IKE  70060004 00000000 00070004 00000000 00000000 00000008
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  be3ca1b1 4023ecbc
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  1b5020f4 fc9d5277
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  148 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 148 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 00000094 2125c4bb
Apr 29, 22:24:41  Debug    IKE  863e0e15 75cedbdb 6fed6d0c 4ba078e5 e17d272e 5f17a397 4fc1aaef 82c22cbf
Apr 29, 22:24:41  Debug    IKE  9e2f9995 fc766212 6d513bce d9566f08 15c6cbf6 bd3c8116 b2ef458b da11d744
Apr 29, 22:24:41  Debug    IKE  38d760f8 7301a9cd 419cca77 398d0990 56246bfc f2816b42 abcb3811 a59cb671
Apr 29, 22:24:41  Debug    IKE  48cf459b 792b6c60 39659eeb 1b5020f4 fc9d5277
Apr 29, 22:24:41  Debug    IKE  sendto mode config attr.
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  108 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c d712f6bf
```

```
Apr 29, 22:24:41  Debug    IKE  01477120 e4cb0706 8ce35c70 1a0b18ec 36962603 932b74d1 5524b8ec 8b344001
Apr 29, 22:24:41  Debug    IKE  be7e8d57 557f5356 c7f15f65 54b5f28d 0420e9a4 74f30f02 769bbd20 4cd7d6ea
Apr 29, 22:24:41  Debug    IKE  558ba56a 5199ac28 33cf4e26
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  5199ac28 33cf4e26
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  1b5020f4 fc9d5277
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:41  Debug    IKE  0e000018 3a21a1f2 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291
Apr 29, 22:24:41  Debug    IKE  00010004 c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480
Apr 29, 22:24:41  Debug    IKE  40050004 00000000 00000000 00000007
Apr 29, 22:24:41  Debug    IKE  padding len=7
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c 0e000018
Apr 29, 22:24:41  Debug    IKE  3a21a1f2 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291 00010004
Apr 29, 22:24:41  Debug    IKE  c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480 40050004
Apr 29, 22:24:41  Debug    IKE  00000000 00000000 00000007
Apr 29, 22:24:41  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c 0e000018
Apr 29, 22:24:41  Debug    IKE  3a21a1f2 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291 00010004
Apr 29, 22:24:41  Debug    IKE  c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480 40050004
Apr 29, 22:24:41  Debug    IKE  00000000 00000000 00000007
Apr 29, 22:24:41  Debug    IKE  Seen payload 8
Apr 29, 22:24:41  Debug    IKE  0e000018 3a21a1f2 b685e1ce a58593dc f80fca55 ecc6fcd8
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  bcf8f3db 00000030 0200f291 00010004 c0a8fe7d 00020004 ffffff00 00030004
Apr 29, 22:24:41  Debug    IKE  c0a8fe01 00050004 0003f480 40050004 00000000
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  3a21a1f2 b685e1ce a58593dc f80fca55 ecc6fcd8
Apr 29, 22:24:41  Debug    IKE  Seen payload 14
Apr 29, 22:24:41  Debug    IKE  00000030 0200f291 00010004 c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01
Apr 29, 22:24:41  Debug    IKE  00050004 0003f480 40050004 00000000
Apr 29, 22:24:41  Debug    IKE  Configuration exchange type mode config REPLY
Apr 29, 22:24:41  Debug    IKE  Attribute INTERNAL_IP4_ADDRESS, len 4
Apr 29, 22:24:41  Debug    IKE  Attribute INTERNAL_IP4_NETMASK, len 4
Apr 29, 22:24:41  Debug    IKE  Attribute INTERNAL_IP4_DNS, len 4
Apr 29, 22:24:41  Debug    IKE  Attribute INTERNAL_ADDRESS_EXPIRY, len 4
Apr 29, 22:24:41  Warning  IKE  Ignored attribute INTERNAL_ADDRESS_EXPIRY
Apr 29, 22:24:41  Debug    IKE  Attribute 16389, len 4
Apr 29, 22:24:41  Warning  IKE  Ignored attribute 16389
Apr 29, 22:24:41  Info     APP  Initiated connection Checkpoint Safe@Office
Apr 29, 22:24:41  Debug    IKE  get pfkey ACQUIRE message
Apr 29, 22:24:41  Debug    IKE  02060003 14000000 07050000 2c020000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:24:41  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e3 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Apr 29, 22:24:41  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Apr 29, 22:24:41  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 2f010000 00000000
Apr 29, 22:24:41  Debug    IKE  suitable outbound SP found: 20.1.1.1/32[0] 10.1.4.0/24[0] proto=any dir=out.
Apr 29, 22:24:41  Debug    IKE  sub:0xbffff31c: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in
Apr 29, 22:24:41  Debug    IKE  db :0x308bf8: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in
Apr 29, 22:24:41  Debug    IKE  suitable inbound SP found: 10.1.4.0/24[0] 20.1.1.1/32[0] proto=any dir=in.
Apr 29, 22:24:41  Debug    IKE  new acquire 20.1.1.1/32[0] 10.1.4.0/24[0] proto=any dir=out
Apr 29, 22:24:41  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 29, 22:24:41  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  (trns_id=AES encklen=256 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  (trns_id=AES encklen=192 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  (trns_id=AES encklen=128 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  in post_acquire
Apr 29, 22:24:41  Debug    IKE  configuration found for 192.168.215.227.
Apr 29, 22:24:41  Debug    IKE  begin QUICK mode.
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  begin QUICK mode.
Apr 29, 22:24:41  Info     IKE  initiate new phase 2 negotiation: 192.168.215.3[500]<=>192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  compute IV for phase2
Apr 29, 22:24:41  Debug    IKE  phase1 last IV:
Apr 29, 22:24:41  Debug    IKE  8822330c fbd77f55 d9144325
Apr 29, 22:24:41  Debug    IKE  hash(sha1)
```

```
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  phase2 IV computed:
Apr 29, 22:24:41  Debug    IKE  92679c3c adbbbf45
Apr 29, 22:24:41  Debug    IKE  call pfkey_send_getspi
Apr 29, 22:24:41  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.227[0]->192.168.215.3[0]
Apr 29, 22:24:41  Debug    IKE  pfkey getspi sent.
Apr 29, 22:24:41  Debug    IKE  get pfkey GETSPI message
Apr 29, 22:24:41  Debug    IKE  02010003 0a000000 07050000 e7090000 02000100 0ce999eb 32392032 323a3234
Apr 29, 22:24:41  Debug    IKE  03000500 ff200000 10020000 c0a8d7e3 00000000 00000000 03000600 ff200000
Apr 29, 22:24:41  Debug    IKE  10020000 c0a8d703 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.227[0]->192.168.215.3[0]
spi=216635883(0xce999eb)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  compute DH's private.
Apr 29, 22:24:41  Debug    IKE  4be820b5 e1782c4c 13f2908d 2cf0eb08 7b3890d9 a3dab2c2 0aca8666 ef2a5df8
Apr 29, 22:24:41  Debug    IKE  da72abca 45a9787e d7da6fc8 b64f9ea7 ca866b86 20f48114 93b1439f c4a281a2
Apr 29, 22:24:41  Debug    IKE  01d6686d 0cf37d1d 5b6df94a 970add9f 009790a4 2d2ea3c4 6bc34bfc aab6c8ba
Apr 29, 22:24:41  Debug    IKE  compute DH's public.
Apr 29, 22:24:41  Debug    IKE  1ed85e16 26055d97 22082867 84edd0cb 28912b85 35a81909 1330db18 45877221
Apr 29, 22:24:41  Debug    IKE  62bb764d df6ba09e 821e0c63 9f795fd9 38a34f42 c400d888 d4b7ee8d e92da706
Apr 29, 22:24:41  Debug    IKE  9509c6e5 381fd131 73506ef9 fd7adbaa 8f2c9373 86e3efae 963c10ba dfd43161
Apr 29, 22:24:41  Debug    IKE  use local ID type IPv4_address
Apr 29, 22:24:41  Debug    IKE  use remote ID type IPv4_subnet
Apr 29, 22:24:41  Debug    IKE  IDci:
Apr 29, 22:24:41  Debug    IKE  01000000 14010101
Apr 29, 22:24:41  Debug    IKE  IDcr:
Apr 29, 22:24:41  Debug    IKE  04000000 0a010400 ffffff00
Apr 29, 22:24:41  Debug    IKE  add payload of len 144, next type 10
Apr 29, 22:24:41  Debug    IKE  add payload of len 16, next type 4
Apr 29, 22:24:41  Debug    IKE  add payload of len 96, next type 5
Apr 29, 22:24:41  Debug    IKE  add payload of len 8, next type 5
Apr 29, 22:24:41  Debug    IKE  add payload of len 12, next type 0
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  d9144325 0a000094 00000001 00000001 00000088 01030404 0ce999eb 0300001c
Apr 29, 22:24:41  Debug    IKE  01030000 80010001 80020258 80040001 80050002 80030001 03000020 020c0000
Apr 29, 22:24:41  Debug    IKE  80010001 80020258 80040001 80060100 80050002 80030001 03000020 030c0000
Apr 29, 22:24:41  Debug    IKE  80010001 80020258 80040001 800600c0 80050002 80030001 00000020 040c0000
Apr 29, 22:24:41  Debug    IKE  80010001 80020258 80040001 80060080 80050002 80030001 04000014 f7b105a9
Apr 29, 22:24:41  Debug    IKE  6dd12da1 f2ca8a4a 64c013a5 05000064 1ed85e16 26055d97 22082867 84edd0cb
Apr 29, 22:24:41  Debug    IKE  28912b85 35a81909 1330db18 45877221 62bb764d df6ba09e 821e0c63 9f795fd9
Apr 29, 22:24:41  Debug    IKE  38a34f42 c400d888 d4b7ee8d e92da706 9509c6e5 381fd131 73506ef9 fd7adbaa
Apr 29, 22:24:41  Debug    IKE  8f2c9373 86e3efae 963c10ba dfd43161 0500000c 01000000 14010101 00000010
Apr 29, 22:24:41  Debug    IKE  04000000 0a010400 ffffff00
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  78aff3ed 043de5c3 c469fc81 50f502d6 545ba034
Apr 29, 22:24:41  Debug    IKE  add payload of len 20, next type 1
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 8
Apr 29, 22:24:41  Debug    IKE  01000018 78aff3ed 043de5c3 c469fc81 50f502d6 545ba034 0a000094 00000001
Apr 29, 22:24:41  Debug    IKE  00000001 00000088 01030404 0ce999eb 0300001c 01030000 80010001 80020258
Apr 29, 22:24:41  Debug    IKE  80040001 80050002 80030001 03000020 020c0000 80010001 80020258 80040001
Apr 29, 22:24:41  Debug    IKE  80060100 80050002 80030001 03000020 030c0000 80010001 80020258 80040001
Apr 29, 22:24:41  Debug    IKE  800600c0 80050002 80030001 00000020 040c0000 80010001 80020258 80040001
Apr 29, 22:24:41  Debug    IKE  80060080 80050002 80030001 04000014 f7b105a9 6dd12da1 f2ca8a4a 64c013a5
Apr 29, 22:24:41  Debug    IKE  05000064 1ed85e16 26055d97 22082867 84edd0cb 28912b85 35a81909 1330db18
Apr 29, 22:24:41  Debug    IKE  45877221 62bb764d df6ba09e 821e0c63 9f795fd9 38a34f42 c400d888 d4b7ee8d
Apr 29, 22:24:41  Debug    IKE  e92da706 9509c6e5 381fd131 73506ef9 fd7adbaa 8f2c9373 86e3efae 963c10ba
Apr 29, 22:24:41  Debug    IKE  dfd43161 0500000c 01000000 14010101 00000010 04000000 0a010400 ffffff00
Apr 29, 22:24:41  Debug    IKE  00000000 00000008
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  92679c3c adbbbf45
```

```
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  565933d8 fde8729d
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  356 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 356 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08102001 d9144325 00000164 2c6d92d1
Apr 29, 22:24:41  Debug    IKE  e55b6f6d bb112e10 6cc8e7d0 7492692d 12c13133 4c1cfa80 c55e36a4 21a24a3c
Apr 29, 22:24:41  Debug    IKE  66957211 65f026b4 27c37537 1e42f747 03bcd24b 1750fbc7 c7a6e824 ddbf0fd6
Apr 29, 22:24:41  Debug    IKE  2021aabf da2eb845 bb4cc610 62c4797c 7a4a6364 71edf42c 43befcea 822b2cb7
Apr 29, 22:24:41  Debug    IKE  fb91dbce 5ef0bd00 2dd77afe f4608fbd 3f0024f6 5301d893 fb56ffb4 75e1be45
Apr 29, 22:24:41  Debug    IKE  d06606f3 ef05636c 16cc89cf 8d02c8fe 9dbf7c09 2c183f68 2cd6e7d0 1b0e5a68
Apr 29, 22:24:41  Debug    IKE  0ce4c009 f2350622 65884646 bd1e4334 3059f968 8c51e1e8 cce9545e c2a45858
Apr 29, 22:24:41  Debug    IKE  7d847bb5 c92ce1d6 98879607 36e98c5e 6953b1cc ba23a385 c754841a b3c00aef
Apr 29, 22:24:41  Debug    IKE  1bc02744 9b3027ad 2c6a08c7 6fae123c ff19862e fd2208d2 8c9b8e9d b3de3120
Apr 29, 22:24:41  Debug    IKE  724ce49c 8054baf2 09387494 f48d2782 b3e011ab a1347b4a 0049a688 26db3b79
Apr 29, 22:24:41  Debug    IKE  91123425 8de6bfac 5f12037e a5048abe f192d962 9956b52a 81ab0662 565933d8
Apr 29, 22:24:41  Debug    IKE  fde8729d
Apr 29, 22:24:41  Debug    IKE  resend phase2 packet 341d80089acf997d:83f17532d8e4e1d8:0000d914
Apr 29, 22:24:41  Debug    IKE  msg 16 not interesting
Apr 29, 22:24:41  Debug    IKE  msg 16 not interesting
Apr 29, 22:24:41  Debug    IKE  msg 16 not interesting
Apr 29, 22:24:41  Debug    IKE  msg 15 not interesting
Apr 29, 22:24:41  Debug    IKE  msg 15 not interesting
Apr 29, 22:24:41  Debug    IKE  msg 15 not interesting
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  260 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08102001 d9144325 00000104 d1b89d1f
Apr 29, 22:24:41  Debug    IKE  e0c19e2e 14c0877b 8d1e65fa 2c6f140b 2926ad90 d02717b6 532fcd0f 3511d747
Apr 29, 22:24:41  Debug    IKE  3826125a 51419c71 1729cc28 fb06952f 445d6a14 9cdef2ef 4d319f35 5de97423
Apr 29, 22:24:41  Debug    IKE  92bfe373 e2e33e35 2bd15005 beb80e5e 6129d04a b85490d0 16b06a6b 5a3a552e
Apr 29, 22:24:41  Debug    IKE  79b12231 22272e16 7603413e 2e5a7bf5 b24c7ad1 02c8ceb1 1934ef6f 6d29d1f3
Apr 29, 22:24:41  Debug    IKE  3a708351 06ef6178 b6c4645e 583b1438 71cccbfb 5c007537 fd837557 3828f28a
Apr 29, 22:24:41  Debug    IKE  54b5b2ec 76b348cd 2cccc80d 569c9c27 d3fee2aa 9046cf08 4a46ebba 64f1bda8
Apr 29, 22:24:41  Debug    IKE  ab10c68f 437a0ce0 58cb558f 89b363ef 55004a26 c971d42b ad4f983e 4f70f554
Apr 29, 22:24:41  Debug    IKE  2b742df9
Apr 29, 22:24:41  Debug    IKE  IV freed
Apr 29, 22:24:41  Debug    IKE  begin decryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:41  Debug    IKE  4f70f554 2b742df9
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  565933d8 fde8729d
Apr 29, 22:24:41  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:41  Debug    IKE  01000018 7e686c2d d4a8f7c4 69b210a6 9712d822 5a52280b 0a000034 00000001
Apr 29, 22:24:41  Debug    IKE  00000001 00000028 01030401 738263c8 0000001c 01030000 80010001 80020258
Apr 29, 22:24:41  Debug    IKE  80040001 80050002 80030001 04000018 6eafbbac de67d570 e7b87af0 3ad1c0ad
Apr 29, 22:24:41  Debug    IKE  f863b91b 05000064 6694b2cc 11cb8fb5 e0ba3ea3 6c42baeb c731b9c9 945d7495
Apr 29, 22:24:41  Debug    IKE  9a0734a8 1fd93041 7639956b 9bf6c705 fb7dcb43 c17708a5 2b7ddb5a df74111a
Apr 29, 22:24:41  Debug    IKE  e53e5f87 7a4a4883 1abaa155 76bef803 c28d2e08 2490de86 14d5b1c6 08a3afb7
Apr 29, 22:24:41  Debug    IKE  715d5f48 592b3bef 0500000c 01000000 14010101 00000010 04000000 0a010400
Apr 29, 22:24:41  Debug    IKE  ffffff00 00000003
Apr 29, 22:24:41  Debug    IKE  padding len=3
Apr 29, 22:24:41  Debug    IKE  skip to trim padding.
Apr 29, 22:24:41  Debug    IKE  decrypted.
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08102001 d9144325 00000104 01000018
Apr 29, 22:24:41  Debug    IKE  7e686c2d d4a8f7c4 69b210a6 9712d822 5a52280b 0a000034 00000001 00000001
Apr 29, 22:24:41  Debug    IKE  00000028 01030401 738263c8 0000001c 01030000 80010001 80020258 80040001
Apr 29, 22:24:41  Debug    IKE  80050002 80030001 04000018 6eafbbac de67d570 e7b87af0 3ad1c0ad f863b91b
Apr 29, 22:24:41  Debug    IKE  05000064 6694b2cc 11cb8fb5 e0ba3ea3 6c42baeb c731b9c9 945d7495 9a0734a8
Apr 29, 22:24:41  Debug    IKE  1fd93041 7639956b 9bf6c705 fb7dcb43 c17708a5 2b7ddb5a df74111a e53e5f87
Apr 29, 22:24:41  Debug    IKE  7a4a4883 1abaa155 76bef803 c28d2e08 2490de86 14d5b1c6 08a3afb7 715d5f48
Apr 29, 22:24:41  Debug    IKE  592b3bef 0500000c 01000000 14010101 00000010 04000000 0a010400 ffffff00
Apr 29, 22:24:41  Debug    IKE  00000003
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=8(hash)
Apr 29, 22:24:41  Debug    IKE  seen nptype=1(sa)
Apr 29, 22:24:41  Debug    IKE  seen nptype=10(nonce)
Apr 29, 22:24:41  Debug    IKE  seen nptype=4(ke)
```

```
Apr 29, 22:24:41  Debug    IKE  seen nptype=5(id)
Apr 29, 22:24:41  Debug    IKE  seen nptype=5(id)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  HASH allocated:hbuf->l=248 actual:tlen=220
Apr 29, 22:24:41  Debug    IKE  HASH(2) received:2007-04-29 22:24:41: DEBUG:
Apr 29, 22:24:41  Debug    IKE  7e686c2d d4a8f7c4 69b210a6 9712d822 5a52280b
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  d9144325 f7b105a9 6dd12da1 f2ca8a4a 64c013a5 0a000034 00000001 00000001
Apr 29, 22:24:41  Debug    IKE  00000028 01030401 738263c8 0000001c 01030000 80010001 80020258 80040001
Apr 29, 22:24:41  Debug    IKE  80050002 80030001 04000018 6eafbbac de67d570 e7b87af0 3ad1c0ad f863b91b
Apr 29, 22:24:41  Debug    IKE  05000064 6694b2cc 11cb8fb5 e0ba3ea3 6c42baeb c731b9c9 945d7495 9a0734a8
Apr 29, 22:24:41  Debug    IKE  1fd93041 7639956b 9bf6c705 fb7dcb43 c17708a5 2b7ddb5a df74111a e53e5f87
Apr 29, 22:24:41  Debug    IKE  7a4a4883 1abaa155 76bef803 c28d2e08 2490de86 14d5b1c6 08a3afb7 715d5f48
Apr 29, 22:24:41  Debug    IKE  592b3bef 0500000c 01000000 14010101 00000010 04000000 0a010400 ffffff00
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  7e686c2d d4a8f7c4 69b210a6 9712d822 5a52280b
Apr 29, 22:24:41  Debug    IKE  total SA len=144
Apr 29, 22:24:41  Debug    IKE  00000001 00000001 00000088 01030404 0ce999eb 0300001c 01030000 80010001
Apr 29, 22:24:41  Debug    IKE  80020258 80040001 80050002 80030001 03000020 020c0000 80010001 80020258
Apr 29, 22:24:41  Debug    IKE  80040001 80060100 80050002 80030001 03000020 030c0000 80010001 80020258
Apr 29, 22:24:41  Debug    IKE  80040001 800600c0 80050002 80030001 00000020 040c0000 80010001 80020258
Apr 29, 22:24:41  Debug    IKE  80040001 80060080 80050002 80030001
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  proposal #1 len=136
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:24:41  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:24:41  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:24:41  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  transform #1 len=28
Apr 29, 22:24:41  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:41  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 29, 22:24:41  Debug    IKE  life duration was in TLV.
Apr 29, 22:24:41  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:24:41  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:24:41  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  transform #2 len=32
Apr 29, 22:24:41  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:41  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 29, 22:24:41  Debug    IKE  life duration was in TLV.
Apr 29, 22:24:41  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:24:41  Debug    IKE  type=Key Length, flag=0x8000, lorv=256
Apr 29, 22:24:41  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:24:41  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  transform #3 len=32
Apr 29, 22:24:41  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:41  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 29, 22:24:41  Debug    IKE  life duration was in TLV.
Apr 29, 22:24:41  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:24:41  Debug    IKE  type=Key Length, flag=0x8000, lorv=192
Apr 29, 22:24:41  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:24:41  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  transform #4 len=32
Apr 29, 22:24:41  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:41  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 29, 22:24:41  Debug    IKE  life duration was in TLV.
Apr 29, 22:24:41  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:24:41  Debug    IKE  type=Key Length, flag=0x8000, lorv=128
Apr 29, 22:24:41  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:24:41  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  pair 1:
Apr 29, 22:24:41  Debug    IKE  0x30ac00: next=0x0 tnext=0x30b4f0
Apr 29, 22:24:41  Debug    IKE  0x30b4f0: next=0x0 tnext=0x30b500
Apr 29, 22:24:41  Debug    IKE  0x30b500: next=0x0 tnext=0x30ba50
Apr 29, 22:24:41  Debug    IKE  0x30ba50: next=0x0 tnext=0x0
Apr 29, 22:24:41  Debug    IKE  proposal #1: 4 transform
```

```
Apr 29, 22:24:41  Debug    IKE  total SA len=48
Apr 29, 22:24:41  Debug    IKE  00000001 00000001 00000028 01030401 738263c8 0000001c 01030000 80010001
Apr 29, 22:24:41  Debug    IKE  80020258 80040001 80050002 80030001
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=2(prop)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  proposal #1 len=40
Apr 29, 22:24:41  Debug    IKE  begin.
Apr 29, 22:24:41  Debug    IKE  seen nptype=3(trns)
Apr 29, 22:24:41  Debug    IKE  succeed.
Apr 29, 22:24:41  Debug    IKE  transform #1 len=28
Apr 29, 22:24:41  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:41  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 29, 22:24:41  Debug    IKE  life duration was in TLV.
Apr 29, 22:24:41  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:24:41  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:24:41  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 29, 22:24:41  Debug    IKE  hmac(modp768)
Apr 29, 22:24:41  Debug    IKE  pair 1:
Apr 29, 22:24:41  Debug    IKE  0x30abd0: next=0x0 tnext=0x0
Apr 29, 22:24:41  Debug    IKE  proposal #1: 1 transform
Apr 29, 22:24:41  Debug    IKE  begin compare proposals.
Apr 29, 22:24:41  Debug    IKE  pair[1]: 0x30abd0
Apr 29, 22:24:41  Debug    IKE  0x30abd0: next=0x0 tnext=0x0
Apr 29, 22:24:41  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Apr 29, 22:24:41  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Apr 29, 22:24:41  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=600
Apr 29, 22:24:41  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
Apr 29, 22:24:41  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Apr 29, 22:24:41  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
Apr 29, 22:24:41  Debug    IKE  peer's single bundle:
Apr 29, 22:24:41  Debug    IKE  (proto_id=ESP spisize=4 spi=738263c8 spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 29, 22:24:41  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  my single bundle:
Apr 29, 22:24:41  Debug    IKE  (proto_id=ESP spisize=4 spi=0ce999eb spi_p=00000000 encmode=Tunnel reqid=0:0)
Apr 29, 22:24:41  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  (trns_id=AES encklen=256 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  (trns_id=AES encklen=192 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  (trns_id=AES encklen=128 authtype=hmac-sha)
Apr 29, 22:24:41  Debug    IKE  matched
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  HASH(3) generate
Apr 29, 22:24:41  Debug    IKE  HASH with:
Apr 29, 22:24:41  Debug    IKE  00d91443 25f7b105 a96dd12d a1f2ca8a 4a64c013 a56eafbb acde67d5 70e7b87a
Apr 29, 22:24:41  Debug    IKE  f03ad1c0 adf863b9 1b
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  HASH computed:
Apr 29, 22:24:41  Debug    IKE  4f707b62 a41c57c1 4089fb65 62a49d6e ca4acbd8
Apr 29, 22:24:41  Debug    IKE  add payload of len 20, next type 0
Apr 29, 22:24:41  Debug    IKE  begin encryption.
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  pad length = 8
Apr 29, 22:24:41  Debug    IKE  00000018 4f707b62 a41c57c1 4089fb65 62a49d6e ca4acbd8 00000000 00000008
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  with key:
Apr 29, 22:24:41  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:41  Debug    IKE  encrypted payload by IV:
Apr 29, 22:24:41  Debug    IKE  4f70f554 2b742df9
Apr 29, 22:24:41  Debug    IKE  save IV for next:
Apr 29, 22:24:41  Debug    IKE  fbf97c65 b27cc3ce
Apr 29, 22:24:41  Debug    IKE  encrypted.
Apr 29, 22:24:41  Debug    IKE  60 bytes from 192.168.215.3[500] to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  sockname 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet from 192.168.215.3[500]
Apr 29, 22:24:41  Debug    IKE  send packet to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.227[500]
Apr 29, 22:24:41  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08102001 d9144325 0000003c ad54861a
Apr 29, 22:24:41  Debug    IKE  2a134cf4 326a5ea4 2ce345f9 5d70fc13 b4705ec0 fbf97c65 b27cc3ce
Apr 29, 22:24:41  Debug    IKE  compute DH's shared.
Apr 29, 22:24:41  Debug    IKE  46626513 f0811778 19afc3f3 081a0d19 05d5d15b c02bc7a1 2ff22516 0663e8d2
Apr 29, 22:24:41  Debug    IKE  59ee59c2 bc8fe780 7877d70e 9d08f72a f5b68c88 f926ae9c 9d35ff66 af7a66b6
Apr 29, 22:24:41  Debug    IKE  c4c4ddf7 19551c7e 814042bc 2b5c896b aef671c9 7652f3a1 01813c31 99e0082b
Apr 29, 22:24:41  Debug    IKE  KEYMAT compute with
Apr 29, 22:24:41  Debug    IKE  46626513 f0811778 19afc3f3 081a0d19 05d5d15b c02bc7a1 2ff22516 0663e8d2
```

```
Apr 29, 22:24:41  Debug    IKE  59ee59c2 bc8fe780 7877d70e 9d08f72a f5b68c88 f926ae9c 9d35ff66 af7a66b6
Apr 29, 22:24:41  Debug    IKE  c4c4ddf7 19551c7e 814042bc 2b5c896b aef671c9 7652f3a1 01813c31 99e0082b
Apr 29, 22:24:41  Debug    IKE  030ce999 ebf7b105 a96dd12d a1f2ca8a 4a64c013 a56eafbb acde67d5 70e7b87a
Apr 29, 22:24:41  Debug    IKE  f03ad1c0 adf863b9 1b
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  encklen=192 authklen=160
Apr 29, 22:24:41  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 29, 22:24:41  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  274d7033 0d9f01f5 d68d8d98 d1b24ae1 14c57efe 21c62101 1c7dc83d c9baffd3
Apr 29, 22:24:41  Debug    IKE  9009b7b1 41455e1d 1ae6acc1 671963cb 9f9f1a3c 45927d5c a32351c7 4038221f
Apr 29, 22:24:41  Debug    IKE  255b0b67 4935d224 309fe38d 504c9067
Apr 29, 22:24:41  Debug    IKE  KEYMAT compute with
Apr 29, 22:24:41  Debug    IKE  46626513 f0811778 19afc3f3 081a0d19 05d5d15b c02bc7a1 2ff22516 0663e8d2
Apr 29, 22:24:41  Debug    IKE  59ee59c2 bc8fe780 7877d70e 9d08f72a f5b68c88 f926ae9c 9d35ff66 af7a66b6
Apr 29, 22:24:41  Debug    IKE  c4c4ddf7 19551c7e 814042bc 2b5c896b aef671c9 7652f3a1 01813c31 99e0082b
Apr 29, 22:24:41  Debug    IKE  03738263 c8f7b105 a96dd12d a1f2ca8a 4a64c013 a56eafbb acde67d5 70e7b87a
Apr 29, 22:24:41  Debug    IKE  f03ad1c0 adf863b9 1b
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  encklen=192 authklen=160
Apr 29, 22:24:41  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Apr 29, 22:24:41  Debug    IKE  generating K1...K4 for KEYMAT.
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  9c7abae1 983f0593 0a77fa95 ad6047cf 5436ba0d cfdf1bba 850f738b 319f6b71
Apr 29, 22:24:41  Debug    IKE  bf9dd5f7 e231df33 5ba38443 fe95610b ffc850ef b23718be 6d13034a 745bad0f
Apr 29, 22:24:41  Debug    IKE  75bf802c ab5679e7 7921f283 d4857b03
Apr 29, 22:24:41  Debug    IKE  KEYMAT computed.
Apr 29, 22:24:41  Debug    IKE  call pk_sendupdate
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  call pfkey_send_update_nat
Apr 29, 22:24:41  Debug    IKE  pfkey update sent.
Apr 29, 22:24:41  Debug    APP  Received SADB message type UPDATE, 192.168.215.227 [0] -> 192.168.215.3 [0]
Apr 29, 22:24:41  Debug    APP  SA change detected
Apr 29, 22:24:41  Debug    IKE  encryption(3des)
Apr 29, 22:24:41  Debug    IKE  hmac(hmac_sha1)
Apr 29, 22:24:41  Debug    IKE  call pfkey_send_add_nat
Apr 29, 22:24:41  Debug    APP  Received SADB message type ADD, 192.168.215.3 [0] -> 192.168.215.227 [0]
Apr 29, 22:24:41  Debug    APP  SA change detected
Apr 29, 22:24:41  Debug    APP  Connection Checkpoint Safe@Office is up
Apr 29, 22:24:41  Debug    IKE  pfkey add sent.
Apr 29, 22:24:41  Debug    IKE  get pfkey UPDATE message
Apr 29, 22:24:41  Debug    IKE  02020003 14000000 07050000 e7090000 02000100 0ce999eb 04000202 00000000
Apr 29, 22:24:41  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d7e3
Apr 29, 22:24:41  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d703 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  04000300 00000000 00000000 00000000 58020000 00000000 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  04000400 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.227[0]->192.168.215.3[0]
spi=216635883(0xce999eb)
Apr 29, 22:24:41  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.227[0]->192.168.215.3[0]
spi=216635883(0xce999eb)
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:41  Debug    IKE  get pfkey ADD message
Apr 29, 22:24:41  Debug    IKE  02030003 14000000 07050000 e7090000 02000100 738263c8 04000202 00000000
Apr 29, 22:24:41  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d703
Apr 29, 22:24:41  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e3 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  04000300 00000000 00000000 00000000 58020000 00000000 00000000 00000000
Apr 29, 22:24:41  Debug    IKE  04000400 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
Apr 29, 22:24:41  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.3[0]->192.168.215.227[0]
spi=1937925064(0x738263c8)
Apr 29, 22:24:41  Debug    IKE  ===
Apr 29, 22:24:42  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:42  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:43  Debug    IKE  ===
Apr 29, 22:24:43  Debug    IKE  108 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:43  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c d712f6bf
```

```
Apr 29, 22:24:43  Debug    IKE  01477120 e4cb0706 8ce35c70 1a0b18ec 36962603 932b74d1 5524b8ec 8b344001
Apr 29, 22:24:43  Debug    IKE  be7e8d57 557f5356 c7f15f65 54b5f28d 0420e9a4 74f30f02 769bbd20 4cd7d6ea
Apr 29, 22:24:43  Debug    IKE  558ba56a 5199ac28 33cf4e26
Apr 29, 22:24:43  Debug    IKE  compute IV for phase2
Apr 29, 22:24:43  Debug    IKE  phase1 last IV:
Apr 29, 22:24:43  Debug    IKE  8822330c fbd77f55 bcf8f3db
Apr 29, 22:24:43  Debug    IKE  hash(sha1)
Apr 29, 22:24:43  Debug    IKE  encryption(3des)
Apr 29, 22:24:43  Debug    IKE  phase2 IV computed:
Apr 29, 22:24:43  Debug    IKE  be3ca1b1 4023ecbc
Apr 29, 22:24:43  Debug    IKE  begin decryption.
Apr 29, 22:24:43  Debug    IKE  encryption(3des)
Apr 29, 22:24:43  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:43  Debug    IKE  5199ac28 33cf4e26
Apr 29, 22:24:43  Debug    IKE  encryption(3des)
Apr 29, 22:24:43  Debug    IKE  with key:
Apr 29, 22:24:43  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:43  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:43  Debug    IKE  be3ca1b1 4023ecbc
Apr 29, 22:24:43  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:43  Debug    IKE  ab6c815d 869f1f39 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291
Apr 29, 22:24:43  Debug    IKE  00010004 c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480
Apr 29, 22:24:43  Debug    IKE  40050004 00000000 00000000 00000007
Apr 29, 22:24:43  Debug    IKE  padding len=7
Apr 29, 22:24:43  Debug    IKE  skip to trim padding.
Apr 29, 22:24:43  Debug    IKE  decrypted.
Apr 29, 22:24:43  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c ab6c815d
Apr 29, 22:24:43  Debug    IKE  869f1f39 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291 00010004
Apr 29, 22:24:43  Debug    IKE  c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480 40050004
Apr 29, 22:24:43  Debug    IKE  00000000 00000000 00000007
Apr 29, 22:24:43  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:43  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c ab6c815d
Apr 29, 22:24:43  Debug    IKE  869f1f39 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291 00010004
Apr 29, 22:24:43  Debug    IKE  c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480 40050004
Apr 29, 22:24:43  Debug    IKE  00000000 00000000 00000007
Apr 29, 22:24:43  Warning  IKE  Short payload
Apr 29, 22:24:43  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:43  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:44  Debug    IKE  ===
Apr 29, 22:24:44  Debug    IKE  108 bytes message received from 192.168.215.227[500] to 192.168.215.3[500]
Apr 29, 22:24:44  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c d712f6bf
Apr 29, 22:24:44  Debug    IKE  01477120 e4cb0706 8ce35c70 1a0b18ec 36962603 932b74d1 5524b8ec 8b344001
Apr 29, 22:24:44  Debug    IKE  be7e8d57 557f5356 c7f15f65 54b5f28d 0420e9a4 74f30f02 769bbd20 4cd7d6ea
Apr 29, 22:24:44  Debug    IKE  558ba56a 5199ac28 33cf4e26
Apr 29, 22:24:44  Debug    IKE  begin decryption.
Apr 29, 22:24:44  Debug    IKE  encryption(3des)
Apr 29, 22:24:44  Debug    IKE  IV was saved for next processing:
Apr 29, 22:24:44  Debug    IKE  5199ac28 33cf4e26
Apr 29, 22:24:44  Debug    IKE  encryption(3des)
Apr 29, 22:24:44  Debug    IKE  with key:
Apr 29, 22:24:44  Debug    IKE  53a90eea 9a355cc5 5f402261 60100ae3 ee8bba77 b922f72e
Apr 29, 22:24:44  Debug    IKE  decrypted payload by IV:
Apr 29, 22:24:44  Debug    IKE  be3ca1b1 4023ecbc
Apr 29, 22:24:44  Debug    IKE  decrypted payload, but not trimed.
Apr 29, 22:24:44  Debug    IKE  ab6c815d 869f1f39 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291
Apr 29, 22:24:44  Debug    IKE  00010004 c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480
Apr 29, 22:24:44  Debug    IKE  40050004 00000000 00000000 00000007
Apr 29, 22:24:44  Debug    IKE  padding len=7
Apr 29, 22:24:44  Debug    IKE  skip to trim padding.
Apr 29, 22:24:44  Debug    IKE  decrypted.
Apr 29, 22:24:44  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c ab6c815d
Apr 29, 22:24:44  Debug    IKE  869f1f39 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291 00010004
Apr 29, 22:24:44  Debug    IKE  c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480 40050004
Apr 29, 22:24:44  Debug    IKE  00000000 00000000 00000007
Apr 29, 22:24:44  Debug    IKE  MODE_CFG packet
Apr 29, 22:24:44  Debug    IKE  341d8008 9acf997d 83f17532 d8e4e1d8 08100601 bcf8f3db 0000006c ab6c815d
Apr 29, 22:24:44  Debug    IKE  869f1f39 b685e1ce a58593dc f80fca55 ecc6fcd8 00000030 0200f291 00010004
Apr 29, 22:24:44  Debug    IKE  c0a8fe7d 00020004 ffffff00 00030004 c0a8fe01 00050004 0003f480 40050004
Apr 29, 22:24:44  Debug    IKE  00000000 00000000 00000007
Apr 29, 22:24:44  Warning  IKE  Short payload
Apr 29, 22:24:44  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:44  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:45  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:45  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
```

```
Apr 29, 22:24:46  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:46  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:47  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:47  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:48  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:48  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:49  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:49  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
Apr 29, 22:24:50  Debug    APP  Send ping packet to 10.1.4.1 of connection Checkpoint Safe@Office
Apr 29, 22:24:50  Debug    APP  Received ping answer 10.1.4.1 for connection Checkpoint Safe@Office
```