IPSecuritas 3.x

Configuration Instructions

for

SonicWALL Pro

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.

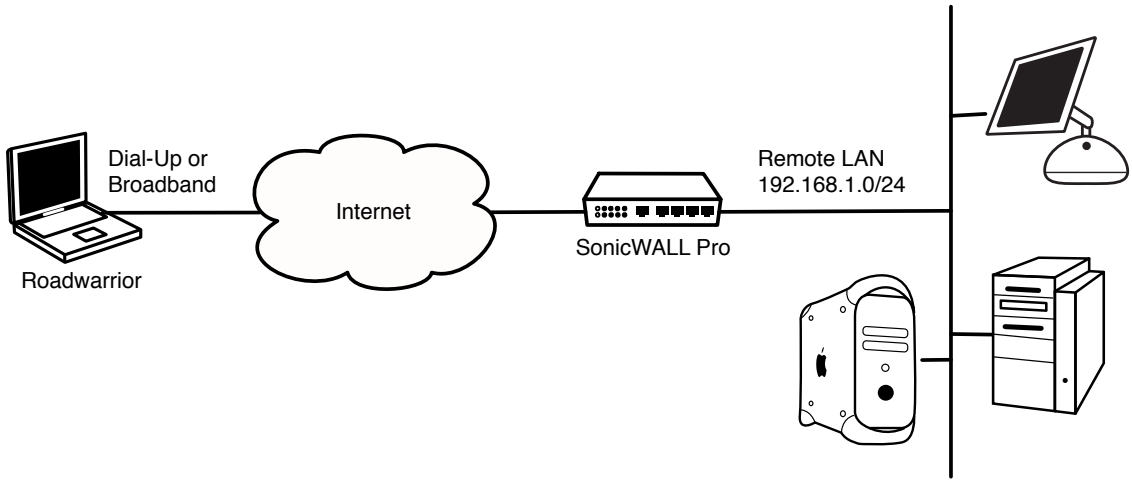
Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic 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 SonicWALL Pro router/firewall. All information in this document is based on the following assumed network.

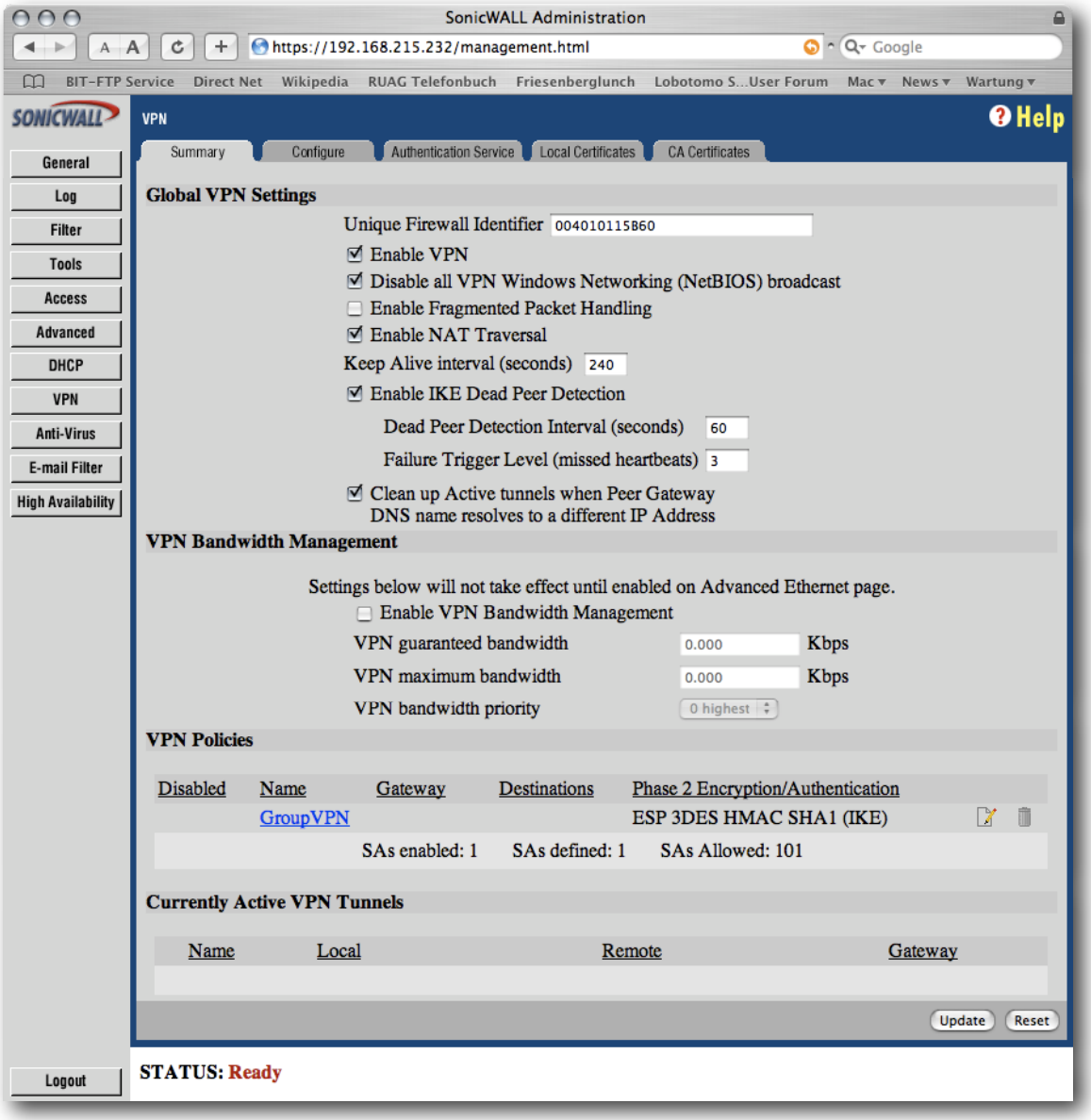


SonicWALL Pro VPN Setup

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

Configure Basic IPSec Parameters

Open a web browser and connect to your SonicWALL router. Enter the administrator's user name and

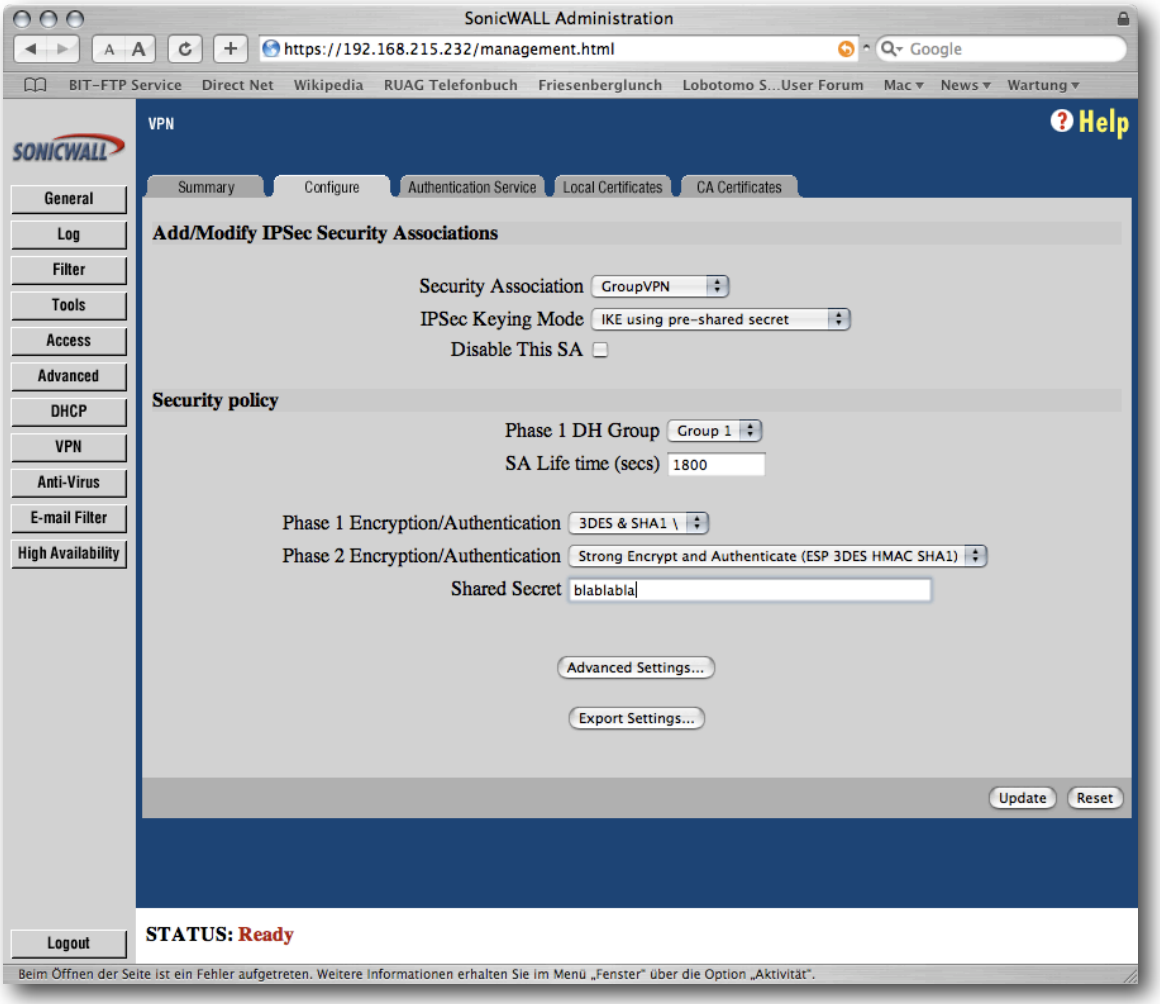


password if asked for. On the left side, click on **VPN** to display the VPN Summary. Please enable the options **Enable VPN**, **Enable NAT Traversal** and **Enable IKE Dead Peer Detection** in order to allow incoming IPSec connections. The other parameters can be adjusted to your liking, although the defaults work fine.

Press **Update** to save your changes.

Add GroupVPN rule

Next, click on the **Configure** tab at the top of the VPN page. Add a **GroupVPN** rule with the same settings as shown in the image below except for the **Shared Secret**. Please choose a secure password



only known to you and enter it into the text field. The advanced settings may be left at the default values.

Press **Update** to save your changes. You may now proceed with the setup of IPSecuritas described in the next chapter.

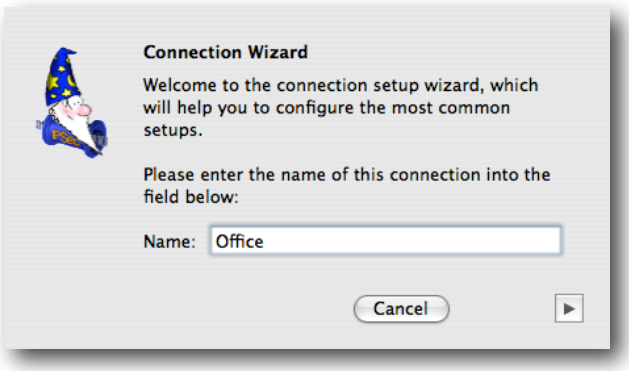
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the SonicWALL Pro 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: 

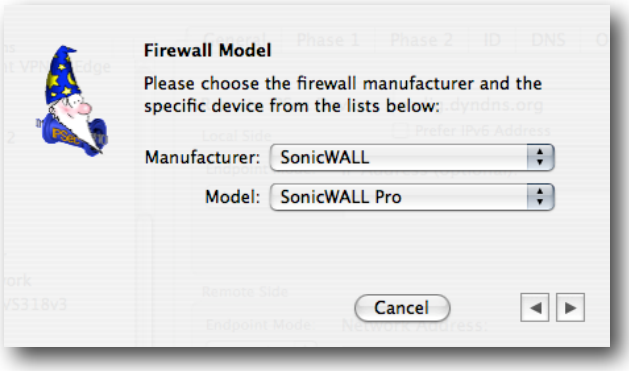
Enter Name of New Connection



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

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

Select Router Model



Select **SonicWALL** from the manufacturer list and **SonicWALL Pro** from the model list.

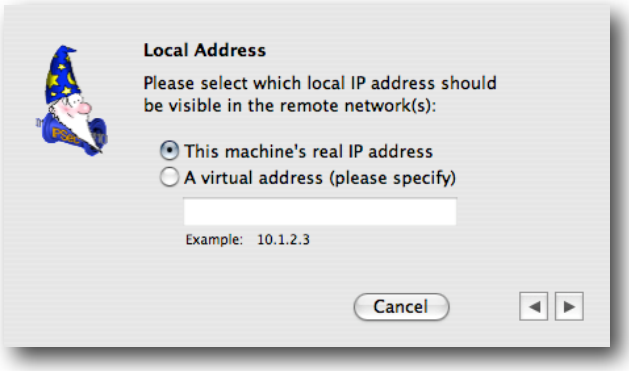
Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

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

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

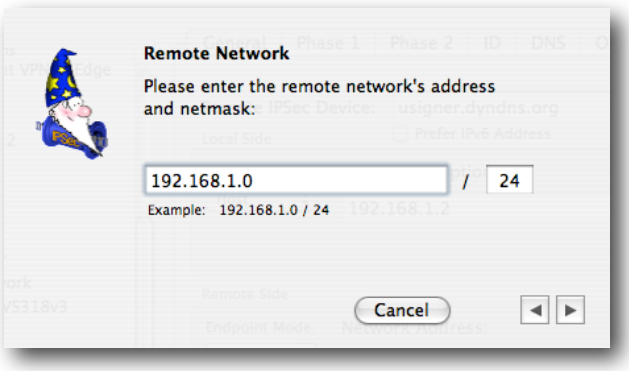
Enter a Virtual IP Address



Enter a virtual local IP address. This address appears as the source address of any packet going through the tunnel. If no address is specified, the real local IP address is used instead.
In order to prevent address collisions between the local network and the remote network, it is recommended to use an address from one the ranges reserved for private network (see **RFC 1918**).

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

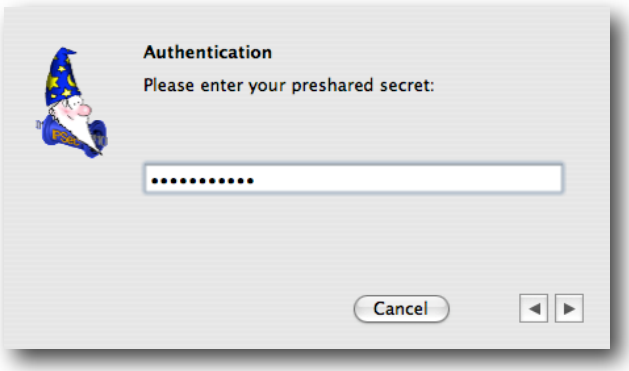
Enter Remote Network



Enter the remote network address and netmask (please note that the netmask needs to be entered in **CIDR** format). This has to match with the settings of the SonicWALL Pro.

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

Enter Preshared Key



Enter the same **Preshared Key** that you used for the SonicWALL Pro.

Click on the right arrow to finish the connection setup.

Diagnosis

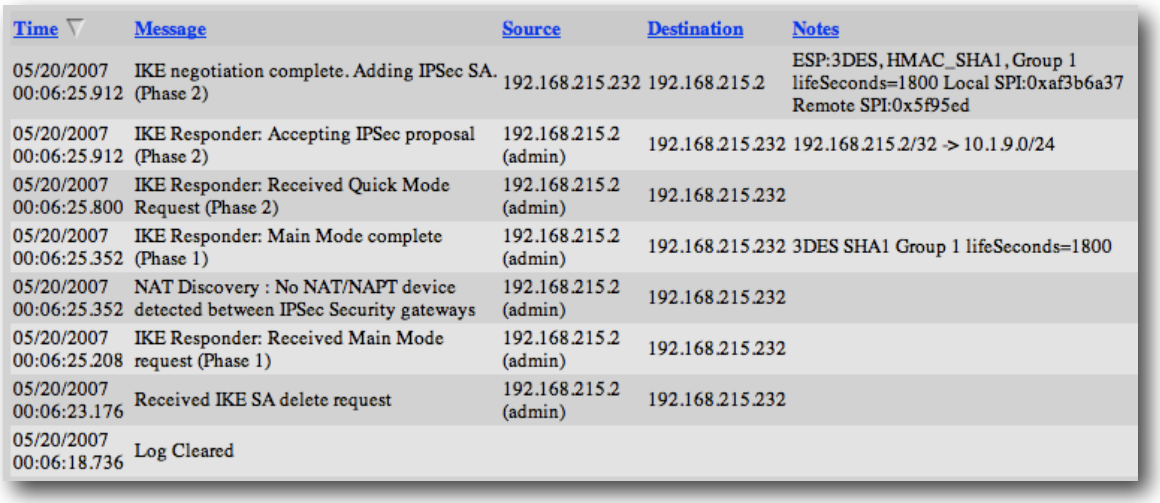
Reachability Test

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

```
[MacBook:~] root# ping 192.168.1.1
PING 192.168.215.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=19.290 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=12.823 ms
```

SonicWALL Connection State

While still logged into the SonicWALL Pro web interface, open the Log page by clicking onto the Log button on the left side. A similar screen as depicted in the image below should appear after a successful connection establishement.



Time	Message	Source	Destination	Notes
05/20/2007 00:06:25.912	IKE negotiation complete. Adding IPSec SA. (Phase 2)	192.168.215.232	192.168.215.2	ESP:3DES, HMAC_SHA1, Group 1 lifeSeconds=1800 Local SPI:0xaf3b6a37 Remote SPI:0x5f95ed
05/20/2007 00:06:25.912	IKE Responder: Accepting IPSec proposal (Phase 2)	192.168.215.2 (admin)	192.168.215.232	192.168.215.2/32 -> 10.1.9.0/24
05/20/2007 00:06:25.800	IKE Responder: Received Quick Mode Request (Phase 2)	192.168.215.2 (admin)	192.168.215.232	
05/20/2007 00:06:25.352	IKE Responder: Main Mode complete (Phase 1)	192.168.215.2 (admin)	192.168.215.232	3DES SHA1 Group 1 lifeSeconds=1800
05/20/2007 00:06:25.352	NAT Discovery : No NAT/NAPT device detected between IPSec Security gateways	192.168.215.2 (admin)	192.168.215.232	
05/20/2007 00:06:25.208	IKE Responder: Received Main Mode request (Phase 1)	192.168.215.2 (admin)	192.168.215.232	
05/20/2007 00:06:23.176	Received IKE SA delete request	192.168.215.2 (admin)	192.168.215.232	
05/20/2007 00:06:18.736	Log Cleared			

Sample IPSecuritas Log Output

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

```
IPSecuritas 3.0rc3 build 1669, Thu May 17 08:30:27 CEST 2007, nadig
Darwin 8.9.1 Darwin Kernel Version 8.9.1: Thu Feb 22 20:55:00 PST 2007; root:xnu-792.18.15~1/RELEASE_I386 i386

May 20, 00:03:52  Debug    APP  State change from IDLE to AUTHENTICATING after event START
May 20, 00:03:52  Info     APP  IKE daemon started
May 20, 00:03:52  Info     APP  IPSec started
May 20, 00:03:52  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
May 20, 00:03:52  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 20, 00:03:52  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
May 20, 00:03:52  Info     IKE  Foreground mode.
May 20, 00:03:52  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
May 20, 00:03:52  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
May 20, 00:03:52  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
May 20, 00:03:52  Info     IKE  Resize address pool from 0 to 255
May 20, 00:03:52  Debug    IKE  lifetime = 1800
May 20, 00:03:52  Debug    IKE  lifebyte = 0
May 20, 00:03:52  Debug    IKE  encklen=0
May 20, 00:03:52  Debug    IKE  p:1 t:1
May 20, 00:03:52  Debug    IKE  3DES-CBC(5)
May 20, 00:03:52  Debug    IKE  SHA(2)
```

```
May 20, 00:03:52  Debug    IKE  768-bit MODP group(1)
May 20, 00:03:52  Debug    IKE  pre-shared key(1)
May 20, 00:03:52  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
May 20, 00:03:52  Debug    IKE  parse successed.
May 20, 00:03:52  Debug    IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
May 20, 00:03:52  Info     IKE  192.168.215.2[4500] used as isakmp port (fd=7)
May 20, 00:03:52  Info     IKE  192.168.215.2[500] used as isakmp port (fd=8)
May 20, 00:03:52  Debug    IKE  get pfkey X_SPDDUMP message
May 20, 00:03:52  Debug    IKE  02120000 0f000100 01000000 091b0000 03000500 ff180000 10020000 0a010900
May 20, 00:03:52  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d702 00000000 00000000
May 20, 00:03:52  Debug    IKE  07001200 02000100 86a70900 00000000 28003200 02020000 10020000 c0a8d7e8
May 20, 00:03:52  Debug    IKE  00000000 00000000 10020000 c0a8d702 00000000 00000000
May 20, 00:03:52  Debug    IKE  get pfkey X_SPDDUMP message
May 20, 00:03:52  Debug    IKE  02120000 0f000100 00000000 091b0000 03000500 ff200000 10020000 c0a8d702
May 20, 00:03:52  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 0a010900 00000000 00000000
May 20, 00:03:52  Debug    IKE  07001200 02000200 85a70900 00000000 28003200 02020000 10020000 c0a8d702
May 20, 00:03:52  Debug    IKE  00000000 00000000 10020000 c0a8d7e8 00000000 00000000
May 20, 00:03:52  Debug    IKE  sub:0xbffff340: 192.168.215.2/32[0] 10.1.9.0/24[0] proto=any dir=out
May 20, 00:03:52  Debug    IKE  db :0x308b78: 10.1.9.0/24[0] 192.168.215.2/32[0] proto=any dir=in
May 20, 00:03:52  Debug    IKE  msg 5 not interesting
May 20, 00:03:53  Info     APP  Initiated connection SonicWall Pro
May 20, 00:03:53  Debug    IKE  get pfkey ACQUIRE message
May 20, 00:03:53  Debug    IKE  02060003 14000000 02020000 b90b0000 03000500 ff200000 10020000 c0a8d702
May 20, 00:03:53  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e8 00000000 00000000
May 20, 00:03:53  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
May 20, 00:03:53  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
May 20, 00:03:53  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 85a70900 00000000
May 20, 00:03:53  Debug    IKE  suitable outbound SP found: 192.168.215.2/32[0] 10.1.9.0/24[0] proto=any dir=out.
May 20, 00:03:53  Debug    IKE  sub:0xbffff31c: 10.1.9.0/24[0] 192.168.215.2/32[0] proto=any dir=in
May 20, 00:03:53  Debug    IKE  db :0x308b78: 10.1.9.0/24[0] 192.168.215.2/32[0] proto=any dir=in
May 20, 00:03:53  Debug    IKE  suitable inbound SP found: 10.1.9.0/24[0] 192.168.215.2/32[0] proto=any dir=in.
May 20, 00:03:53  Debug    IKE  new acquire 192.168.215.2/32[0] 10.1.9.0/24[0] proto=any dir=out
May 20, 00:03:53  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 20, 00:03:53  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 00:03:53  Debug    IKE  in post_acquire
May 20, 00:03:53  Debug    IKE  configuration found for 192.168.215.232.
May 20, 00:03:53  Info     IKE  IPsec-SA request for 192.168.215.232 queued due to no phase1 found.
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Info     IKE  initiate new phase 1 negotiation: 192.168.215.2[500]<=>192.168.215.232[500]
May 20, 00:03:53  Info     IKE  begin Identity Protection mode.
May 20, 00:03:53  Debug    IKE  new cookie:
May 20, 00:03:53  Debug    IKE  0fa3eec76544653c
May 20, 00:03:53  Debug    IKE  add payload of len 48, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 13
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 0
May 20, 00:03:53  Debug    IKE  320 bytes from 192.168.215.2[500] to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  sockname 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  1 times of 320 bytes message will be sent to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 00000000 00000000 01100200 00000000 00000140 0d000034
May 20, 00:03:53  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0708
May 20, 00:03:53  Debug    IKE  80010005 80030001 80020002 80040001 0d000014 4a131c81 07035845 5c5728f2
May 20, 00:03:53  Debug    IKE  0e95452f 0d000014 8f8d8382 6d246b6f c7a8a6a4 28c11de8 0d000014 439b59f8
May 20, 00:03:53  Debug    IKE  ba676c4c 7737ae22 eab8f582 0d000014 4d1e0e13 6deafa34 c4f3ea9f 02ec7285
May 20, 00:03:53  Debug    IKE  0d000014 80d0bb3d ef54565e e84645d4 c85ce3ee 0d000014 9909b64e ed937c65
May 20, 00:03:53  Debug    IKE  73de52ac e952fa6b 0d000014 7d9419a6 5310ca6f 2c179d92 15529d56 0d000014
May 20, 00:03:53  Debug    IKE  cd604643 35df21f8 7cfdb2fc 68b6a448 0d000014 90cb8091 3ebb696e 086381b5
May 20, 00:03:53  Debug    IKE  ec427b1f 0d000014 16f6ca16 e4a4066d 83821a0f 0aeaa862 0d000014 4485152d
May 20, 00:03:53  Debug    IKE  18b6bbcd 0be8a846 9579ddcc 00000014 afcad713 68a1f1c9 6b8696fc 77570100
May 20, 00:03:53  Debug    IKE  resend phase1 packet 0fa3eec76544653c:0000000000000000
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Debug    IKE  100 bytes message received from 192.168.215.232[500] to 192.168.215.2[500]
```

```
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 01100200 00000000 00000064 0d000034
May 20, 00:03:53  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 80010005 80020002
May 20, 00:03:53  Debug    IKE  80040001 80030001 800b0001 800c0708 00000014 4485152d 18b6bbcd 0be8a846
May 20, 00:03:53  Debug    IKE  9579ddcc
May 20, 00:03:53  Debug    IKE  begin.
May 20, 00:03:53  Debug    IKE  seen nptype=1(sa)
May 20, 00:03:53  Debug    IKE  seen nptype=13(vid)
May 20, 00:03:53  Debug    IKE  succeed.
May 20, 00:03:53  Info     IKE  received Vendor ID: draft-ietf-ipsec-nat-t-ike-00
May 20, 00:03:53  Info     IKE  Selected NAT-T version: draft-ietf-ipsec-nat-t-ike-00
May 20, 00:03:53  Debug    IKE  total SA len=48
May 20, 00:03:53  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 80010005 80020002
May 20, 00:03:53  Debug    IKE  80040001 80030001 800b0001 800c0708
May 20, 00:03:53  Debug    IKE  begin.
May 20, 00:03:53  Debug    IKE  seen nptype=2(prop)
May 20, 00:03:53  Debug    IKE  succeed.
May 20, 00:03:53  Debug    IKE  proposal #1 len=40
May 20, 00:03:53  Debug    IKE  begin.
May 20, 00:03:53  Debug    IKE  seen nptype=3(trns)
May 20, 00:03:53  Debug    IKE  succeed.
May 20, 00:03:53  Debug    IKE  transform #1 len=32
May 20, 00:03:53  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
May 20, 00:03:53  Debug    IKE  hmac(modp768)
May 20, 00:03:53  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 20, 00:03:53  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 20, 00:03:53  Debug    IKE  type=Life Duration, flag=0x8000, lorv=1800
May 20, 00:03:53  Debug    IKE  pair 1:
May 20, 00:03:53  Debug    IKE  0x3095c0: next=0x0 tnext=0x0
May 20, 00:03:53  Debug    IKE  proposal #1: 1 transform
May 20, 00:03:53  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
May 20, 00:03:53  Debug    IKE  trns#=1, trns-id=IKE
May 20, 00:03:53  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 20, 00:03:53  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 20, 00:03:53  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
May 20, 00:03:53  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 20, 00:03:53  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
May 20, 00:03:53  Debug    IKE  type=Life Duration, flag=0x8000, lorv=1800
May 20, 00:03:53  Debug    IKE  Compared: DB:Peer
May 20, 00:03:53  Debug    IKE  (lifetime = 1800:1800)
May 20, 00:03:53  Debug    IKE  (lifebyte = 0:0)
May 20, 00:03:53  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
May 20, 00:03:53  Debug    IKE  (encklen = 0:0)
May 20, 00:03:53  Debug    IKE  hashtype = SHA:SHA
May 20, 00:03:53  Debug    IKE  authmethod = pre-shared key:pre-shared key
May 20, 00:03:53  Debug    IKE  dh_group = 768-bit MODP group:768-bit MODP group
May 20, 00:03:53  Debug    IKE  an acceptable proposal found.
May 20, 00:03:53  Debug    IKE  hmac(modp768)
May 20, 00:03:53  Debug    IKE  agreed on pre-shared key auth.
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Debug    IKE  compute DH's private.
May 20, 00:03:53  Debug    IKE  4d23a003 8a77f47b d877dc14 d274ae48 72f97471 132117a7 f8cd944b 16c2dc79
May 20, 00:03:53  Debug    IKE  8e475d34 05a747ec 4b4034e2 61a81646 216dda0b 43f6f54d e91fbdfc 78e5c321
May 20, 00:03:53  Debug    IKE  00daa089 d91330da 363db0d4 fde92b91 16147768 09c0c83b 4009155c 3234a3ce
May 20, 00:03:53  Debug    IKE  compute DH's public.
May 20, 00:03:53  Debug    IKE  fcb29ef4 c023bfd4 f4b1b4a5 db38cead b3a62761 685f4f7e d0a49f38 13080d6e
May 20, 00:03:53  Debug    IKE  8eb7244e d5fa33ab 82069fa1 addefad2 b54670da 0ce9f137 e09dcf6f 4e610e2f
May 20, 00:03:53  Debug    IKE  844501a1 3adf7f64 ce83cd69 6f8f6024 6b606c22 e524b57e 0fac0ddb 134a7081
May 20, 00:03:53  Info     IKE  Hashing 192.168.215.232[500] with algo #2
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Info     IKE  Hashing 192.168.215.2[500] with algo #2
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Info     IKE  Adding remote and local NAT-D payloads.
May 20, 00:03:53  Debug    IKE  add payload of len 96, next type 10
May 20, 00:03:53  Debug    IKE  add payload of len 16, next type 130
May 20, 00:03:53  Debug    IKE  add payload of len 20, next type 130
May 20, 00:03:53  Debug    IKE  add payload of len 20, next type 0
May 20, 00:03:53  Debug    IKE  196 bytes from 192.168.215.2[500] to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  sockname 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet to 192.168.215.232[500]
```

```
May 20, 00:03:53  Debug    IKE  1 times of 196 bytes message will be sent to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 04100200 00000000 000000c4 0a000064
May 20, 00:03:53  Debug    IKE  fcb29ef4 c023bfd4 f4b1b4a5 db38cead b3a62761 685f4f7e d0a49f38 13080d6e
May 20, 00:03:53  Debug    IKE  8eb7244e d5fa33ab 82069fa1 addefad2 b54670da 0ce9f137 e09dcf6f 4e610e2f
May 20, 00:03:53  Debug    IKE  844501a1 3adf7f64 ce83cd69 6f8f6024 6b606c22 e524b57e 0fac0ddb 134a7081
May 20, 00:03:53  Debug    IKE  82000014 80711313 95269779 c26fc46c 077d9a10 82000018 66c062c4 f6316755
May 20, 00:03:53  Debug    IKE  9ade54c3 af63137c 70b9e55d 00000018 d7aa5498 1395c949 be0fb813 f38ab038
May 20, 00:03:53  Debug    IKE  2588e02c
May 20, 00:03:53  Debug    IKE  resend phase1 packet 0fa3eec76544653c:9736a3d5862bc018
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Debug    IKE  236 bytes message received from 192.168.215.232[500] to 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 04100200 00000000 000000ec 82000064
May 20, 00:03:53  Debug    IKE  9b124a00 5e3697dd b2421f81 2d0ba7ca 8f42bb84 1802a4e3 f5bb2a38 ed5052d5
May 20, 00:03:53  Debug    IKE  a62fb675 23f7a8ea 9c45e885 66536d1e 638c4e42 de73af06 23702296 e09ed40b
May 20, 00:03:53  Debug    IKE  155ee7b5 ab68d850 c5ab6081 cfdccc50 2daf99bc 4d1af257 d582543e a9a6ff67
May 20, 00:03:53  Debug    IKE  82000018 d7aa5498 1395c949 be0fb813 f38ab038 2588e02c 0a000018 66c062c4
May 20, 00:03:53  Debug    IKE  f6316755 9ade54c3 af63137c 70b9e55d 0d000018 12e41251 ec4f2133 43125445
May 20, 00:03:53  Debug    IKE  5e9121f2 abde2c53 0d00000c da8e9378 80010000 0d00000c 404bf439 522ca3f6
May 20, 00:03:53  Debug    IKE  0000000c 09002689 dfd6b712
May 20, 00:03:53  Debug    IKE  begin.
May 20, 00:03:53  Debug    IKE  seen nptype=4(ke)
May 20, 00:03:53  Debug    IKE  seen nptype=130(nat-d)
May 20, 00:03:53  Debug    IKE  seen nptype=130(nat-d)
May 20, 00:03:53  Debug    IKE  seen nptype=10(nonce)
May 20, 00:03:53  Debug    IKE  seen nptype=13(vid)
May 20, 00:03:53  Debug    IKE  seen nptype=13(vid)
May 20, 00:03:53  Debug    IKE  seen nptype=13(vid)
May 20, 00:03:53  Debug    IKE  succeed.
May 20, 00:03:53  Info     IKE  Hashing 192.168.215.2[500] with algo #2
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Info     IKE  NAT-D payload #0 verified
May 20, 00:03:53  Info     IKE  Hashing 192.168.215.232[500] with algo #2
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Info     IKE  NAT-D payload #1 verified
May 20, 00:03:53  Debug    IKE  received unknown Vendor ID
May 20, 00:03:53  Debug    IKE  da8e9378 80010000
May 20, 00:03:53  Debug    IKE  received unknown Vendor ID
May 20, 00:03:53  Debug    IKE  404bf439 522ca3f6
May 20, 00:03:53  Info     IKE  received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt
May 20, 00:03:53  Info     IKE  NAT not detected
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Debug    IKE  compute DH's shared.
May 20, 00:03:53  Debug    IKE  0ca8a425 bfbd73fc c03ede58 fde4b366 680f4f97 169eab10 ff969c3a 12f4ae8e
May 20, 00:03:53  Debug    IKE  f4c119cc f7e4215b 710bed43 b29a9fdd 49021e18 ebc16ddd c69a97e2 b2ce0a53
May 20, 00:03:53  Debug    IKE  1410feda 753d0c36 aeb25549 f6ad870e 8f056452 26e4ec3f 296a69ed 84be5015
May 20, 00:03:53  Debug    IKE  the psk found.
May 20, 00:03:53  Debug    IKE  psk: 2007-05-20 00:03:53: DEBUG2:
May 20, 00:03:53  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
May 20, 00:03:53  Debug    IKE  nonce 1: 2007-05-20 00:03:53: DEBUG:
May 20, 00:03:53  Debug    IKE  80711313 95269779 c26fc46c 077d9a10
May 20, 00:03:53  Debug    IKE  nonce 2: 2007-05-20 00:03:53: DEBUG:
May 20, 00:03:53  Debug    IKE  12e41251 ec4f2133 43125445 5e9121f2 abde2c53
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  SKEYID computed:
May 20, 00:03:53  Debug    IKE  12803670 9c9cffe9 c474f1f8 37024854 7ca13837
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  SKEYID_d computed:
May 20, 00:03:53  Debug    IKE  0ea4e3b1 a0923a7b 1a282610 901780fc 7ad90cd8
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  SKEYID_a computed:
May 20, 00:03:53  Debug    IKE  ebea0a2c 0c48ebaf 8bd4a2e3 b6f5d4b1 95a55fba
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  SKEYID_e computed:
May 20, 00:03:53  Debug    IKE  07201f76 ddc3c7c7 91b9b908 5bf97c67 9221a712
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  compute intermediate encryption key K1
May 20, 00:03:53  Debug    IKE  00
May 20, 00:03:53  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  compute intermediate encryption key K2
May 20, 00:03:53  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41
```

```
May 20, 00:03:53  Debug    IKE  3ad25040 89d68abf ea577fb8 0008d456 58821d5d
May 20, 00:03:53  Debug    IKE  final encryption key computed:
May 20, 00:03:53  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  IV computed:
May 20, 00:03:53  Debug    IKE  a88086be 1c6f03a8
May 20, 00:03:53  Debug    IKE  use ID type of IPv4_address
May 20, 00:03:53  Debug    IKE  HASH with:
May 20, 00:03:53  Debug    IKE  fcb29ef4 c023bfd4 f4b1b4a5 db38cead b3a62761 685f4f7e d0a49f38 13080d6e
May 20, 00:03:53  Debug    IKE  8eb7244e d5fa33ab 82069fa1 addefad2 b54670da 0ce9f137 e09dcf6f 4e610e2f
May 20, 00:03:53  Debug    IKE  844501a1 3adf7f64 ce83cd69 6f8f6024 6b606c22 e524b57e 0fac0ddb 134a7081
May 20, 00:03:53  Debug    IKE  9b124a00 5e3697dd b2421f81 2d0ba7ca 8f42bb84 1802a4e3 f5bb2a38 ed5052d5
May 20, 00:03:53  Debug    IKE  a62fb675 23f7a8ea 9c45e885 66536d1e 638c4e42 de73af06 23702296 e09ed40b
May 20, 00:03:53  Debug    IKE  155ee7b5 ab68d850 c5ab6081 cfdccc50 2daf99bc 4d1af257 d582543e a9a6ff67
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 00000001 00000001 00000028 01010001
May 20, 00:03:53  Debug    IKE  00000020 01010000 800b0001 800c0708 80010005 80030001 80020002 80040001
May 20, 00:03:53  Debug    IKE  011101f4 c0a8d702
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  HASH (init) computed:
May 20, 00:03:53  Debug    IKE  08ff942f ae6970e7 27d207ab a5d61d76 b89c323b
May 20, 00:03:53  Debug    IKE  add payload of len 8, next type 8
May 20, 00:03:53  Debug    IKE  add payload of len 20, next type 0
May 20, 00:03:53  Debug    IKE  begin encryption.
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  pad length = 4
May 20, 00:03:53  Debug    IKE  0800000c 011101f4 c0a8d702 00000018 08ff942f ae6970e7 27d207ab a5d61d76
May 20, 00:03:53  Debug    IKE  b89c323b 00000004
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  with key:
May 20, 00:03:53  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:53  Debug    IKE  encrypted payload by IV:
May 20, 00:03:53  Debug    IKE  a88086be 1c6f03a8
May 20, 00:03:53  Debug    IKE  save IV for next:
May 20, 00:03:53  Debug    IKE  ee603ec9 2961335e
May 20, 00:03:53  Debug    IKE  encrypted.
May 20, 00:03:53  Debug    IKE  68 bytes from 192.168.215.2[500] to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  sockname 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  1 times of 68 bytes message will be sent to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 05100201 00000000 00000044 0a316bf6
May 20, 00:03:53  Debug    IKE  bda4051f 9cc2a7e3 187a129f b727db7b 20f3e76a 8a8d514d 83110d25 ee603ec9
May 20, 00:03:53  Debug    IKE  2961335e
May 20, 00:03:53  Debug    IKE  resend phase1 packet 0fa3eec76544653c:9736a3d5862bc018
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Debug    IKE  68 bytes message received from 192.168.215.232[500] to 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 05100201 00000000 00000044 37541dc6
May 20, 00:03:53  Debug    IKE  a37e007f 6584993e 89ed2891 92edfdff 45b530e0 923211dd 0825d4d7 6db0b2c8
May 20, 00:03:53  Debug    IKE  4f814da9
May 20, 00:03:53  Debug    IKE  begin decryption.
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  IV was saved for next processing:
May 20, 00:03:53  Debug    IKE  6db0b2c8 4f814da9
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  with key:
May 20, 00:03:53  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:53  Debug    IKE  decrypted payload by IV:
May 20, 00:03:53  Debug    IKE  ee603ec9 2961335e
May 20, 00:03:53  Debug    IKE  decrypted payload, but not trimed.
May 20, 00:03:53  Debug    IKE  0800000c 01000000 c0a8d7e8 00000018 d158c4e6 a97a38b8 ada0cb36 cbb07cc8
May 20, 00:03:53  Debug    IKE  d3ec16c6 00000003
May 20, 00:03:53  Debug    IKE  padding len=3
May 20, 00:03:53  Debug    IKE  skip to trim padding.
May 20, 00:03:53  Debug    IKE  decrypted.
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 05100201 00000000 00000044 0800000c
May 20, 00:03:53  Debug    IKE  01000000 c0a8d7e8 00000018 d158c4e6 a97a38b8 ada0cb36 cbb07cc8 d3ec16c6
May 20, 00:03:53  Debug    IKE  00000003
May 20, 00:03:53  Debug    IKE  begin.
May 20, 00:03:53  Debug    IKE  seen nptype=5(id)
May 20, 00:03:53  Debug    IKE  seen nptype=8(hash)
May 20, 00:03:53  Debug    IKE  succeed.
May 20, 00:03:53  Debug    IKE  HASH received:
May 20, 00:03:53  Debug    IKE  d158c4e6 a97a38b8 ada0cb36 cbb07cc8 d3ec16c6
```

```
May 20, 00:03:53  Debug    IKE  HASH with:
May 20, 00:03:53  Debug    IKE  9b124a00 5e3697dd b2421f81 2d0ba7ca 8f42bb84 1802a4e3 f5bb2a38 ed5052d5
May 20, 00:03:53  Debug    IKE  a62fb675 23f7a8ea 9c45e885 66536d1e 638c4e42 de73af06 23702296 e09ed40b
May 20, 00:03:53  Debug    IKE  155ee7b5 ab68d850 c5ab6081 cfdccc50 2daf99bc 4d1af257 d582543e a9a6ff67
May 20, 00:03:53  Debug    IKE  fcb29ef4 c023bfd4 f4b1b4a5 db38cead b3a62761 685f4f7e d0a49f38 13080d6e
May 20, 00:03:53  Debug    IKE  8eb7244e d5fa33ab 82069fa1 addefad2 b54670da 0ce9f137 e09dcf6f 4e610e2f
May 20, 00:03:53  Debug    IKE  844501a1 3adf7f64 ce83cd69 6f8f6024 6b606c22 e524b57e 0fac0ddb 134a7081
May 20, 00:03:53  Debug    IKE  9736a3d5 862bc018 0fa3eec7 6544653c 00000001 00000001 00000028 01010001
May 20, 00:03:53  Debug    IKE  00000020 01010000 800b0001 800c0708 80010005 80030001 80020002 80040001
May 20, 00:03:53  Debug    IKE  01000000 c0a8d7e8
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  HASH (init) computed:
May 20, 00:03:53  Debug    IKE  d158c4e6 a97a38b8 ada0cb36 cbb07cc8 d3ec16c6
May 20, 00:03:53  Debug    IKE  HASH for PSK validated.
May 20, 00:03:53  Debug    IKE  peer's ID:2007-05-20 00:03:53: DEBUG:
May 20, 00:03:53  Debug    IKE  01000000 c0a8d7e8
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:53  Debug    IKE  compute IV for phase2
May 20, 00:03:53  Debug    IKE  phase1 last IV:
May 20, 00:03:53  Debug    IKE  6db0b2c8 4f814da9 efa069af
May 20, 00:03:53  Debug    IKE  hash(sha1)
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  phase2 IV computed:
May 20, 00:03:53  Debug    IKE  b7f816e3 e35af04b
May 20, 00:03:53  Debug    IKE  HASH with:
May 20, 00:03:53  Debug    IKE  efa069af 0000001c 00000001 01106002 0fa3eec7 6544653c 9736a3d5 862bc018
May 20, 00:03:53  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:53  Debug    IKE  HASH computed:
May 20, 00:03:53  Debug    IKE  e709f066 8eb6a409 9ccd0206 a4b7878a 25efc7f2
May 20, 00:03:53  Debug    IKE  begin encryption.
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  pad length = 4
May 20, 00:03:53  Debug    IKE  0b000018 e709f066 8eb6a409 9ccd0206 a4b7878a 25efc7f2 0000001c 00000001
May 20, 00:03:53  Debug    IKE  01106002 0fa3eec7 6544653c 9736a3d5 862bc018 00000004
May 20, 00:03:53  Debug    IKE  encryption(3des)
May 20, 00:03:53  Debug    IKE  with key:
May 20, 00:03:53  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:53  Debug    IKE  encrypted payload by IV:
May 20, 00:03:53  Debug    IKE  b7f816e3 e35af04b
May 20, 00:03:53  Debug    IKE  save IV for next:
May 20, 00:03:53  Debug    IKE  0add426a a1ee36dc
May 20, 00:03:53  Debug    IKE  encrypted.
May 20, 00:03:53  Debug    IKE  84 bytes from 192.168.215.2[500] to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  sockname 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 00:03:53  Debug    IKE  send packet to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.232[500]
May 20, 00:03:53  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 08100501 efa069af 00000054 3cba40b4
May 20, 00:03:53  Debug    IKE  da2bc2c8 3726ba4a 868043cb 6518e1d5 befcfc9d 108329bf a50cd9b7 a5a41d24
May 20, 00:03:53  Debug    IKE  0c366a39 a8d60b62 3aa40014 0add426a a1ee36dc
May 20, 00:03:53  Debug    IKE  sendto Information notify.
May 20, 00:03:53  Debug    IKE  IV freed
May 20, 00:03:53  Info     IKE  ISAKMP-SA established 192.168.215.2[500]-192.168.215.232[500] spi:0fa3eec76544653c:
9736a3d5862bc018
May 20, 00:03:53  Debug    IKE  ===
May 20, 00:03:54  Debug    IKE  ===
May 20, 00:03:54  Debug    IKE  begin QUICK mode.
May 20, 00:03:54  Info     IKE  initiate new phase 2 negotiation: 192.168.215.2[500]<=>192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  compute IV for phase2
May 20, 00:03:54  Debug    IKE  phase1 last IV:
May 20, 00:03:54  Debug    IKE  6db0b2c8 4f814da9 ce89b841
May 20, 00:03:54  Debug    IKE  hash(sha1)
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  phase2 IV computed:
May 20, 00:03:54  Debug    IKE  b2f49e7b 99453bf4
May 20, 00:03:54  Debug    IKE  call pfkey_send_getspi
May 20, 00:03:54  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.232[0]->192.168.215.2[0]
May 20, 00:03:54  Debug    IKE  pfkey getspi sent.
May 20, 00:03:54  Debug    IKE  get pfkey GETSPI message
May 20, 00:03:54  Debug    IKE  02010003 0a000000 02020000 091b0000 02000100 0097964f 32302030 303a3033
May 20, 00:03:54  Debug    IKE  03000500 ff200000 10020000 c0a8d7e8 00000000 00000000 03000600 ff200000
May 20, 00:03:54  Debug    IKE  10020000 c0a8d702 00000000 00000000
May 20, 00:03:54  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.232[0]->192.168.215.2[0]
spi=9934415(0x97964f)
```

```
May 20, 00:03:54  Debug    IKE  hmac(modp768)
May 20, 00:03:54  Debug    IKE  hmac(modp768)
May 20, 00:03:54  Debug    IKE  hmac(modp768)
May 20, 00:03:54  Debug    IKE  compute DH's private.
May 20, 00:03:54  Debug    IKE  6ccee236 64c3a731 05255238 0f2e506a e2f8ac5d 34adb3f0 2c7a3e6e 445236c7
May 20, 00:03:54  Debug    IKE  69adadb1 dd0b61e7 02432519 ee8b4cc7 f48577e9 92527152 db2a00b9 9e7012b8
May 20, 00:03:54  Debug    IKE  34c5bd07 a377acaa 13f2e076 409c2d71 54fddc9b 46130683 6869cb99 4764e125
May 20, 00:03:54  Debug    IKE  compute DH's public.
May 20, 00:03:54  Debug    IKE  619482fa eba40cca 8c286fc5 9939a70e e52ca6a6 3be5f479 20a99a46 a480bb3b
May 20, 00:03:54  Debug    IKE  9a9da945 5261cd5f 7c6bd7ce 2cadc4b6 200b475e 1dea6394 776676ec beed0788
May 20, 00:03:54  Debug    IKE  b9fa4b33 7815d012 9cd67d43 a9cdb5ae ba0f2a05 671eecfe 5d143802 0dabf96d
May 20, 00:03:54  Debug    IKE  use local ID type IPv4_address
May 20, 00:03:54  Debug    IKE  use remote ID type IPv4_subnet
May 20, 00:03:54  Debug    IKE  IDci:
May 20, 00:03:54  Debug    IKE  01000000 c0a8d702
May 20, 00:03:54  Debug    IKE  IDcr:
May 20, 00:03:54  Debug    IKE  04000000 0a010900 ffffff00
May 20, 00:03:54  Debug    IKE  add payload of len 48, next type 10
May 20, 00:03:54  Debug    IKE  add payload of len 16, next type 4
May 20, 00:03:54  Debug    IKE  add payload of len 96, next type 5
May 20, 00:03:54  Debug    IKE  add payload of len 8, next type 5
May 20, 00:03:54  Debug    IKE  add payload of len 12, next type 0
May 20, 00:03:54  Debug    IKE  HASH with:
May 20, 00:03:54  Debug    IKE  ce89b841 0a000034 00000001 00000001 00000028 01030401 0097964f 0000001c
May 20, 00:03:54  Debug    IKE  01030000 80010001 80020708 80040001 80050002 80030001 04000014 bfe956b2
May 20, 00:03:54  Debug    IKE  e9f317a5 2f184240 eb8306b1 05000064 619482fa eba40cca 8c286fc5 9939a70e
May 20, 00:03:54  Debug    IKE  e52ca6a6 3be5f479 20a99a46 a480bb3b 9a9da945 5261cd5f 7c6bd7ce 2cadc4b6
May 20, 00:03:54  Debug    IKE  200b475e 1dea6394 776676ec beed0788 b9fa4b33 7815d012 9cd67d43 a9cdb5ae
May 20, 00:03:54  Debug    IKE  ba0f2a05 671eecfe 5d143802 0dabf96d 0500000c 01000000 c0a8d702 00000010
May 20, 00:03:54  Debug    IKE  04000000 0a010900 ffffff00
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  HASH computed:
May 20, 00:03:54  Debug    IKE  156c2e98 8ca01d22 2a38ee00 365457fd 2b63cf20
May 20, 00:03:54  Debug    IKE  add payload of len 20, next type 1
May 20, 00:03:54  Debug    IKE  begin encryption.
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  pad length = 8
May 20, 00:03:54  Debug    IKE  01000018 156c2e98 8ca01d22 2a38ee00 365457fd 2b63cf20 0a000034 00000001
May 20, 00:03:54  Debug    IKE  00000001 00000028 01030401 0097964f 0000001c 01030000 80010001 80020708
May 20, 00:03:54  Debug    IKE  80040001 80050002 80030001 04000014 bfe956b2 e9f317a5 2f184240 eb8306b1
May 20, 00:03:54  Debug    IKE  05000064 619482fa eba40cca 8c286fc5 9939a70e e52ca6a6 3be5f479 20a99a46
May 20, 00:03:54  Debug    IKE  a480bb3b 9a9da945 5261cd5f 7c6bd7ce 2cadc4b6 200b475e 1dea6394 776676ec
May 20, 00:03:54  Debug    IKE  beed0788 b9fa4b33 7815d012 9cd67d43 a9cdb5ae ba0f2a05 671eecfe 5d143802
May 20, 00:03:54  Debug    IKE  0dabf96d 0500000c 01000000 c0a8d702 00000010 04000000 0a010900 ffffff00
May 20, 00:03:54  Debug    IKE  00000000 00000008
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  with key:
May 20, 00:03:54  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:54  Debug    IKE  encrypted payload by IV:
May 20, 00:03:54  Debug    IKE  b2f49e7b 99453bf4
May 20, 00:03:54  Debug    IKE  save IV for next:
May 20, 00:03:54  Debug    IKE  37375e0e da0e534e
May 20, 00:03:54  Debug    IKE  encrypted.
May 20, 00:03:54  Debug    IKE  260 bytes from 192.168.215.2[500] to 192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  sockname 192.168.215.2[500]
May 20, 00:03:54  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 00:03:54  Debug    IKE  send packet to 192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  1 times of 260 bytes message will be sent to 192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 08102001 ce89b841 00000104 0b1a502d
May 20, 00:03:54  Debug    IKE  1db3b85b 5f26582a 084f2281 fa4e4536 dfcacfed b160ec81 423a3f98 0200e9cb
May 20, 00:03:54  Debug    IKE  232d2463 bb18f99e 6ee129e1 fae30d31 cf6bea98 76a60644 62238445 5d996e8b
May 20, 00:03:54  Debug    IKE  12110f7c 3f1431ae 635e8538 d795add8 594a20ad 8e00249d c41c4e01 93b485d8
May 20, 00:03:54  Debug    IKE  9ebacc72 d0c6bf20 0ea46375 e2edbd7a ea84f80b b052a2c7 f0edeb46 750c59ff
May 20, 00:03:54  Debug    IKE  9a96b3ea aacb544c bd65cab5 4c9bca02 422341df dbd06923 c5882aab 8b9695e9
May 20, 00:03:54  Debug    IKE  e1e1e31b 524a03fc d0670549 f3c3f19c ee937f58 2b74c015 eb8c2b2e f7d94f5b
May 20, 00:03:54  Debug    IKE  017e2c66 744b870b acff01f5 fe6543a1 2f4a6a41 0897f85d 2465066a 37375e0e
May 20, 00:03:54  Debug    IKE  da0e534e
May 20, 00:03:54  Debug    IKE  resend phase2 packet 0fa3eec76544653c:9736a3d5862bc018:0000ce89
May 20, 00:03:54  Debug    IKE  ===
May 20, 00:03:54  Debug    IKE  260 bytes message received from 192.168.215.232[500] to 192.168.215.2[500]
May 20, 00:03:54  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 08102001 ce89b841 00000104 b04ea581
May 20, 00:03:54  Debug    IKE  7670b47e cf0c2c28 be2fbc0f 88f2a31b 753f5060 b7b9c1ab 1fda7581 4eccf1c7
May 20, 00:03:54  Debug    IKE  90120827 d2c770b9 10c65ab9 dbb20bf6 f66e9139 b370d30e 88d487dd b13cfab4
May 20, 00:03:54  Debug    IKE  2a3d3daa 914b7c6c e87a8bf5 e99f1cde 807a9494 eff6b9e9 1626f5c6 0494a3e3
```

```
May 20, 00:03:54  Debug    IKE  8034e67a c7b5ce4f d8ba3304 1c597c71 159726a2 3be9cc57 114cb7d2 f7887427
May 20, 00:03:54  Debug    IKE  12012d67 83efd700 88825582 525df8e0 c93f49f0 91f2375e 29bb49ab 95f3075a
May 20, 00:03:54  Debug    IKE  da0ee240 b66f5038 f71c8d65 5682f6ca 440703f8 bc68c3f7 211bc089 917e953f
May 20, 00:03:54  Debug    IKE  b0020d2f 93dbc5ad 75ce2d41 eb042f0f 695082f2 17353dc8 e71aeb9b b122e6a8
May 20, 00:03:54  Debug    IKE  82afba9f
May 20, 00:03:54  Debug    IKE  begin decryption.
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  IV was saved for next processing:
May 20, 00:03:54  Debug    IKE  b122e6a8 82afba9f
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  with key:
May 20, 00:03:54  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:54  Debug    IKE  decrypted payload by IV:
May 20, 00:03:54  Debug    IKE  37375e0e da0e534e
May 20, 00:03:54  Debug    IKE  decrypted payload, but not trimed.
May 20, 00:03:54  Debug    IKE  01000018 bd7ac0ac 1344d6c7 9140b43d 9e14cd94 4aad54d7 0a000034 00000001
May 20, 00:03:54  Debug    IKE  00000001 00000028 01030401 e75e7f54 0000001c 01030000 80010001 80020708
May 20, 00:03:54  Debug    IKE  80030001 80040001 80050002 04000018 ddab6c11 5c386d3b 0883e4a5 09caf37b
May 20, 00:03:54  Debug    IKE  83384356 05000064 30bd4c27 38009c4c a6579aa2 ae50465c 69a1c450 50640bf3
May 20, 00:03:54  Debug    IKE  b7e07734 5dc320c0 e7c474fa 343c2a90 fda161fd 025a3594 312e47ab e4bc1473
May 20, 00:03:54  Debug    IKE  bcac6a38 bffc4a02 fb0fcb73 9f944f80 4d2395d3 b7491a9f a8e755f4 6404eb46
May 20, 00:03:54  Debug    IKE  f39178cd 21a9bc1d 0500000c 01000000 c0a8d702 00000010 04000000 0a010900
May 20, 00:03:54  Debug    IKE  ffffff00 00000003
May 20, 00:03:54  Debug    IKE  padding len=3
May 20, 00:03:54  Debug    IKE  skip to trim padding.
May 20, 00:03:54  Debug    IKE  decrypted.
May 20, 00:03:54  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 08102001 ce89b841 00000104 01000018
May 20, 00:03:54  Debug    IKE  bd7ac0ac 1344d6c7 9140b43d 9e14cd94 4aad54d7 0a000034 00000001 00000001
May 20, 00:03:54  Debug    IKE  00000028 01030401 e75e7f54 0000001c 01030000 80010001 80020708 80030001
May 20, 00:03:54  Debug    IKE  80040001 80050002 04000018 ddab6c11 5c386d3b 0883e4a5 09caf37b 83384356
May 20, 00:03:54  Debug    IKE  05000064 30bd4c27 38009c4c a6579aa2 ae50465c 69a1c450 50640bf3 b7e07734
May 20, 00:03:54  Debug    IKE  5dc320c0 e7c474fa 343c2a90 fda161fd 025a3594 312e47ab e4bc1473 bcac6a38
May 20, 00:03:54  Debug    IKE  bffc4a02 fb0fcb73 9f944f80 4d2395d3 b7491a9f a8e755f4 6404eb46 f39178cd
May 20, 00:03:54  Debug    IKE  21a9bc1d 0500000c 01000000 c0a8d702 00000010 04000000 0a010900 ffffff00
May 20, 00:03:54  Debug    IKE  00000003
May 20, 00:03:54  Debug    IKE  begin.
May 20, 00:03:54  Debug    IKE  seen nptype=8(hash)
May 20, 00:03:54  Debug    IKE  seen nptype=1(sa)
May 20, 00:03:54  Debug    IKE  seen nptype=10(nonce)
May 20, 00:03:54  Debug    IKE  seen nptype=4(ke)
May 20, 00:03:54  Debug    IKE  seen nptype=5(id)
May 20, 00:03:54  Debug    IKE  seen nptype=5(id)
May 20, 00:03:54  Debug    IKE  succeed.
May 20, 00:03:54  Debug    IKE  HASH allocated:hbuf->l=248 actual:tlen=220
May 20, 00:03:54  Debug    IKE  HASH(2) received:2007-05-20 00:03:54: DEBUG:
May 20, 00:03:54  Debug    IKE  bd7ac0ac 1344d6c7 9140b43d 9e14cd94 4aad54d7
May 20, 00:03:54  Debug    IKE  HASH with:
May 20, 00:03:54  Debug    IKE  ce89b841 bfe956b2 e9f317a5 2f184240 eb8306b1 0a000034 00000001 00000001
May 20, 00:03:54  Debug    IKE  00000028 01030401 e75e7f54 0000001c 01030000 80010001 80020708 80030001
May 20, 00:03:54  Debug    IKE  80040001 80050002 04000018 ddab6c11 5c386d3b 0883e4a5 09caf37b 83384356
May 20, 00:03:54  Debug    IKE  05000064 30bd4c27 38009c4c a6579aa2 ae50465c 69a1c450 50640bf3 b7e07734
May 20, 00:03:54  Debug    IKE  5dc320c0 e7c474fa 343c2a90 fda161fd 025a3594 312e47ab e4bc1473 bcac6a38
May 20, 00:03:54  Debug    IKE  bffc4a02 fb0fcb73 9f944f80 4d2395d3 b7491a9f a8e755f4 6404eb46 f39178cd
May 20, 00:03:54  Debug    IKE  21a9bc1d 0500000c 01000000 c0a8d702 00000010 04000000 0a010900 ffffff00
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  HASH computed:
May 20, 00:03:54  Debug    IKE  bd7ac0ac 1344d6c7 9140b43d 9e14cd94 4aad54d7
May 20, 00:03:54  Debug    IKE  total SA len=48
May 20, 00:03:54  Debug    IKE  00000001 00000001 00000028 01030401 0097964f 0000001c 01030000 80010001
May 20, 00:03:54  Debug    IKE  80020708 80040001 80050002 80030001
May 20, 00:03:54  Debug    IKE  begin.
May 20, 00:03:54  Debug    IKE  seen nptype=2(prop)
May 20, 00:03:54  Debug    IKE  succeed.
May 20, 00:03:54  Debug    IKE  proposal #1 len=40
May 20, 00:03:54  Debug    IKE  begin.
May 20, 00:03:54  Debug    IKE  seen nptype=3(trns)
May 20, 00:03:54  Debug    IKE  succeed.
May 20, 00:03:54  Debug    IKE  transform #1 len=28
May 20, 00:03:54  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 00:03:54  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=1800
May 20, 00:03:54  Debug    IKE  life duration was in TLV.
May 20, 00:03:54  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 20, 00:03:54  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 00:03:54  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
```

```
May 20, 00:03:54  Debug    IKE  hmac(modp768)
May 20, 00:03:54  Debug    IKE  pair 1:
May 20, 00:03:54  Debug    IKE  0x309ee0: next=0x0 tnext=0x0
May 20, 00:03:54  Debug    IKE  proposal #1: 1 transform
May 20, 00:03:54  Debug    IKE  total SA len=48
May 20, 00:03:54  Debug    IKE  00000001 00000001 00000028 01030401 e75e7f54 0000001c 01030000 80010001
May 20, 00:03:54  Debug    IKE  80020708 80030001 80040001 80050002
May 20, 00:03:54  Debug    IKE  begin.
May 20, 00:03:54  Debug    IKE  seen nptype=2(prop)
May 20, 00:03:54  Debug    IKE  succeed.
May 20, 00:03:54  Debug    IKE  proposal #1 len=40
May 20, 00:03:54  Debug    IKE  begin.
May 20, 00:03:54  Debug    IKE  seen nptype=3(trns)
May 20, 00:03:54  Debug    IKE  succeed.
May 20, 00:03:54  Debug    IKE  transform #1 len=28
May 20, 00:03:54  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 00:03:54  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=1800
May 20, 00:03:54  Debug    IKE  life duration was in TLV.
May 20, 00:03:54  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
May 20, 00:03:54  Debug    IKE  hmac(modp768)
May 20, 00:03:54  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 20, 00:03:54  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 00:03:54  Debug    IKE  pair 1:
May 20, 00:03:54  Debug    IKE  0x309e10: next=0x0 tnext=0x0
May 20, 00:03:54  Debug    IKE  proposal #1: 1 transform
May 20, 00:03:54  Warning  IKE  attribute has been modified.
May 20, 00:03:54  Debug    IKE  begin compare proposals.
May 20, 00:03:54  Debug    IKE  pair[1]: 0x309e10
May 20, 00:03:54  Debug    IKE  0x309e10: next=0x0 tnext=0x0
May 20, 00:03:54  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
May 20, 00:03:54  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 00:03:54  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=1800
May 20, 00:03:54  Debug    IKE  type=Group Description, flag=0x8000, lorv=1
May 20, 00:03:54  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 20, 00:03:54  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 00:03:54  Debug    IKE  peer's single bundle:
May 20, 00:03:54  Debug    IKE  (proto_id=ESP spisize=4 spi=e75e7f54 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 20, 00:03:54  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 00:03:54  Debug    IKE  my single bundle:
May 20, 00:03:54  Debug    IKE  (proto_id=ESP spisize=4 spi=0097964f spi_p=00000000 encmode=Tunnel reqid=0:0)
May 20, 00:03:54  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 00:03:54  Debug    IKE  matched
May 20, 00:03:54  Debug    IKE  ===
May 20, 00:03:54  Debug    IKE  HASH(3) generate
May 20, 00:03:54  Debug    IKE  HASH with:
May 20, 00:03:54  Debug    IKE  00ce89b8 41bfe956 b2e9f317 a52f1842 40eb8306 b1ddab6c 115c386d 3b0883e4
May 20, 00:03:54  Debug    IKE  a509caf3 7b833843 56
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  HASH computed:
May 20, 00:03:54  Debug    IKE  c8a372f8 e62c04de 5c2893ad 827e8f1d 849c5919
May 20, 00:03:54  Debug    IKE  add payload of len 20, next type 0
May 20, 00:03:54  Debug    IKE  begin encryption.
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  pad length = 8
May 20, 00:03:54  Debug    IKE  00000018 c8a372f8 e62c04de 5c2893ad 827e8f1d 849c5919 00000000 00000008
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  with key:
May 20, 00:03:54  Debug    IKE  ee0323ea ddf82661 65a3341a c0df0935 22200d41 3ad25040
May 20, 00:03:54  Debug    IKE  encrypted payload by IV:
May 20, 00:03:54  Debug    IKE  b122e6a8 82afba9f
May 20, 00:03:54  Debug    IKE  save IV for next:
May 20, 00:03:54  Debug    IKE  d84efc42 5ea6a2cd
May 20, 00:03:54  Debug    IKE  encrypted.
May 20, 00:03:54  Debug    IKE  60 bytes from 192.168.215.2[500] to 192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  sockname 192.168.215.2[500]
May 20, 00:03:54  Debug    IKE  send packet from 192.168.215.2[500]
May 20, 00:03:54  Debug    IKE  send packet to 192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  1 times of 60 bytes message will be sent to 192.168.215.232[500]
May 20, 00:03:54  Debug    IKE  0fa3eec7 6544653c 9736a3d5 862bc018 08102001 ce89b841 0000003c 84c24de6
May 20, 00:03:54  Debug    IKE  08c70f89 de9bad9a 80854830 c92e0f5d f6b34645 d84efc42 5ea6a2cd
May 20, 00:03:54  Debug    IKE  compute DH's shared.
May 20, 00:03:54  Debug    IKE  8d724ba6 ba2ec93a a4ffd855 7eeb1611 44b8bab2 9c9faa88 23ccbea0 27b2df55
May 20, 00:03:54  Debug    IKE  f3babb59 715505eb 6021730d 724b3ded 1b58ac21 23753638 956387d7 acc5e917
May 20, 00:03:54  Debug    IKE  9a7ab119 5030e07d 88745ecb 40b04fcf 98ec8831 0f96be8b 7a620a13 b35b75e6
```

```
May 20, 00:03:54  Debug    IKE  KEYMAT compute with
May 20, 00:03:54  Debug    IKE  8d724ba6 ba2ec93a a4ffd855 7eeb1611 44b8bab2 9c9faa88 23ccbea0 27b2df55
May 20, 00:03:54  Debug    IKE  f3babb59 715505eb 6021730d 724b3ded 1b58ac21 23753638 956387d7 acc5e917
May 20, 00:03:54  Debug    IKE  9a7ab119 5030e07d 88745ecb 40b04fcf 98ec8831 0f96be8b 7a620a13 b35b75e6
May 20, 00:03:54  Debug    IKE  03009796 4fbfe956 b2e9f317 a52f1842 40eb8306 b1ddab6c 115c386d 3b0883e4
May 20, 00:03:54  Debug    IKE  a509caf3 7b833843 56
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  encklen=192 authklen=160
May 20, 00:03:54  Debug    IKE  generating 640 bits of key (dupkeymat=4)
May 20, 00:03:54  Debug    IKE  generating K1...K4 for KEYMAT.
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  8e9836b5 32f7b84e 2e3d4f0c 157c9288 0ecac2df 498b99c5 2aa2cd65 79afc720
May 20, 00:03:54  Debug    IKE  b513aa3c edab23e9 5807aa42 9383dc99 b84ed32c e82a6964 60628b50 e6967353
May 20, 00:03:54  Debug    IKE  7e73b182 41f8ce73 d652068a 714312ba
May 20, 00:03:54  Debug    IKE  KEYMAT compute with
May 20, 00:03:54  Debug    IKE  8d724ba6 ba2ec93a a4ffd855 7eeb1611 44b8bab2 9c9faa88 23ccbea0 27b2df55
May 20, 00:03:54  Debug    IKE  f3babb59 715505eb 6021730d 724b3ded 1b58ac21 23753638 956387d7 acc5e917
May 20, 00:03:54  Debug    IKE  9a7ab119 5030e07d 88745ecb 40b04fcf 98ec8831 0f96be8b 7a620a13 b35b75e6
May 20, 00:03:54  Debug    IKE  03e75e7f 54bfe956 b2e9f317 a52f1842 40eb8306 b1ddab6c 115c386d 3b0883e4
May 20, 00:03:54  Debug    IKE  a509caf3 7b833843 56
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  encklen=192 authklen=160
May 20, 00:03:54  Debug    IKE  generating 640 bits of key (dupkeymat=4)
May 20, 00:03:54  Debug    IKE  generating K1...K4 for KEYMAT.
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  12baa47e 256f3c8e 84b6fd7d f6770cc5 20e7d97f 7f79bdba 0bfcdd84 7cffce9e
May 20, 00:03:54  Debug    IKE  b9c666d6 fa602102 85112b1c 4fe8f88b 44910ac8 103f8b8d ec6b6389 f72b6507
May 20, 00:03:54  Debug    IKE  1b61992c c3b7ca91 e57aa9d9 aa58aa81
May 20, 00:03:54  Debug    IKE  KEYMAT computed.
May 20, 00:03:54  Debug    IKE  call pk_sendupdate
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  call pfkey_send_update_nat
May 20, 00:03:54  Debug    IKE  pfkey update sent.
May 20, 00:03:54  Debug    APP  Received SADB message type UPDATE, 192.168.215.232 [0] -> 192.168.215.2 [0]
May 20, 00:03:54  Debug    APP  SA change detected
May 20, 00:03:54  Debug    IKE  encryption(3des)
May 20, 00:03:54  Debug    IKE  hmac(hmac_sha1)
May 20, 00:03:54  Debug    IKE  call pfkey_send_add_nat
May 20, 00:03:54  Debug    APP  Received SADB message type ADD, 192.168.215.2 [0] -> 192.168.215.232 [0]
May 20, 00:03:54  Debug    APP  SA change detected
May 20, 00:03:54  Debug    APP  Connection SonicWall Pro is up
May 20, 00:03:54  Debug    IKE  pfkey add sent.
May 20, 00:03:54  Debug    IKE  get pfkey UPDATE message
May 20, 00:03:54  Debug    IKE  02020003 14000000 02020000 091b0000 02000100 0097964f 04000202 00000000
May 20, 00:03:54  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d7e8
May 20, 00:03:54  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d702 00000000 00000000
May 20, 00:03:54  Debug    IKE  04000300 00000000 00000000 00000000 08070000 00000000 00000000 00000000
May 20, 00:03:54  Debug    IKE  04000400 00000000 00000000 00000000 a0050000 00000000 00000000 00000000
May 20, 00:03:54  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.232[0]->192.168.215.2[0]
spi=9934415(0x97964f)
May 20, 00:03:54  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.232[0]->192.168.215.2[0]
spi=9934415(0x97964f)
May 20, 00:03:54  Debug    IKE  ===
May 20, 00:03:54  Debug    IKE  get pfkey ADD message
May 20, 00:03:54  Debug    IKE  02030003 14000000 02020000 091b0000 02000100 e75e7f54 04000202 00000000
May 20, 00:03:54  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d702
May 20, 00:03:54  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e8 00000000 00000000
May 20, 00:03:54  Debug    IKE  04000300 00000000 00000000 00000000 08070000 00000000 00000000 00000000
May 20, 00:03:54  Debug    IKE  04000400 00000000 00000000 00000000 a0050000 00000000 00000000 00000000
May 20, 00:03:54  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.2[0]->192.168.215.232[0]
spi=3881729876(0xe75e7f54)
May 20, 00:03:54  Debug    IKE  ===
```