IPSecuritas 3.x

Configuration Instructions

for

Juniper Netscreen
Juniper SSG

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.

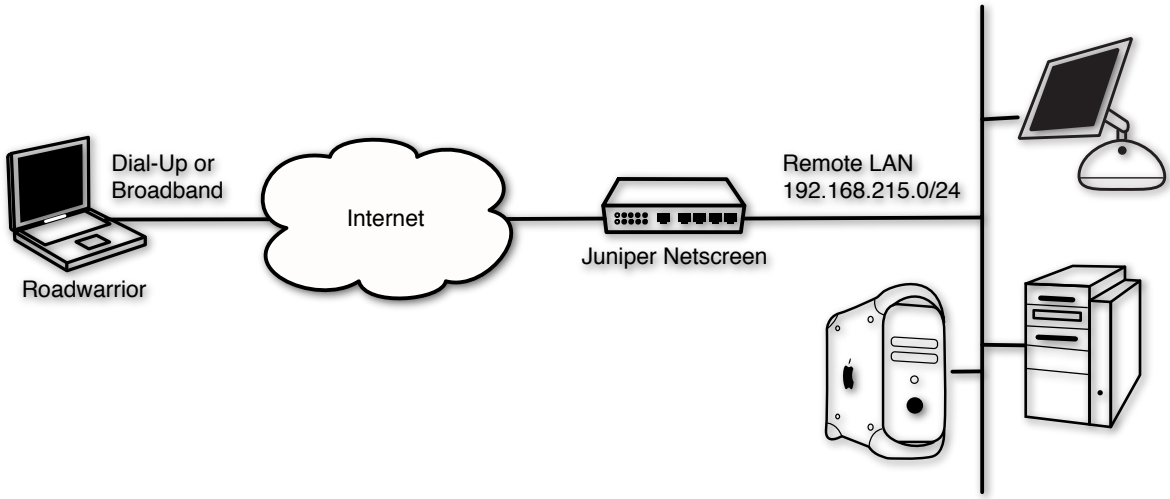
Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic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

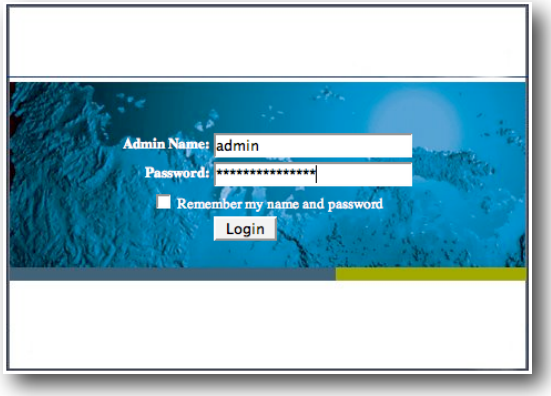
Table of contents

Introduction

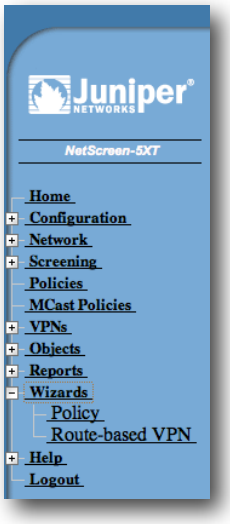
This document describes the steps necessary to establish a protected VPN connection between a Mac client and a Juniper Netscreen firewall. All information in this document is based on the following assumed network.



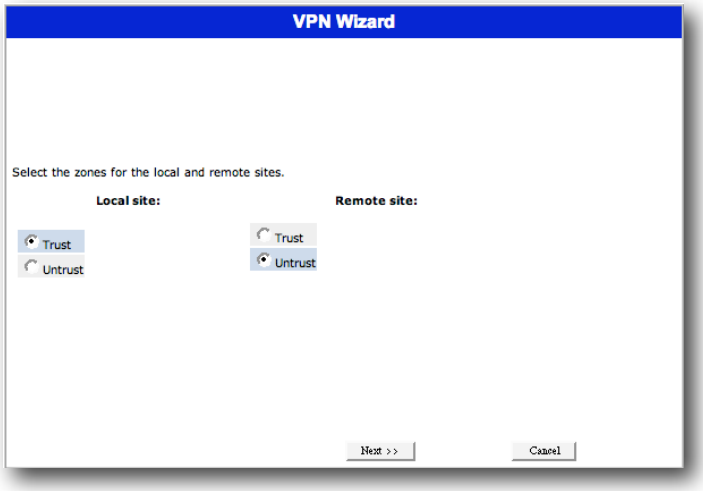
Juniper Netscreen Setup



Open Safari and log into your Netscreen firewall as a user with administrative rights.

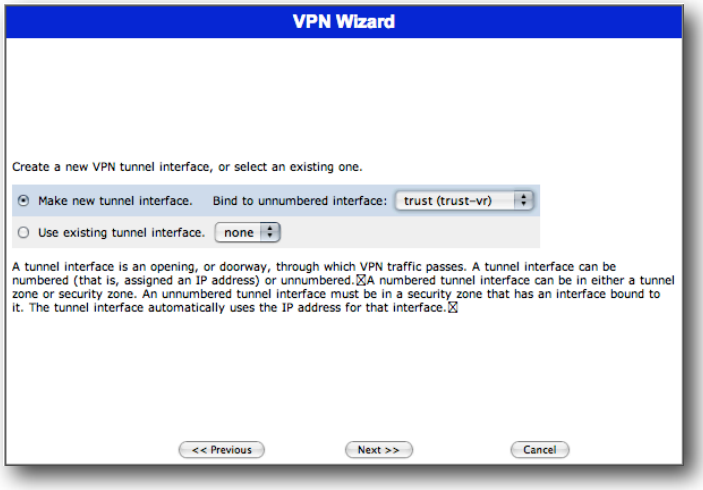


In the main menu, open the **Wizards** group and click on **Route-based VPN**. A new window should open.



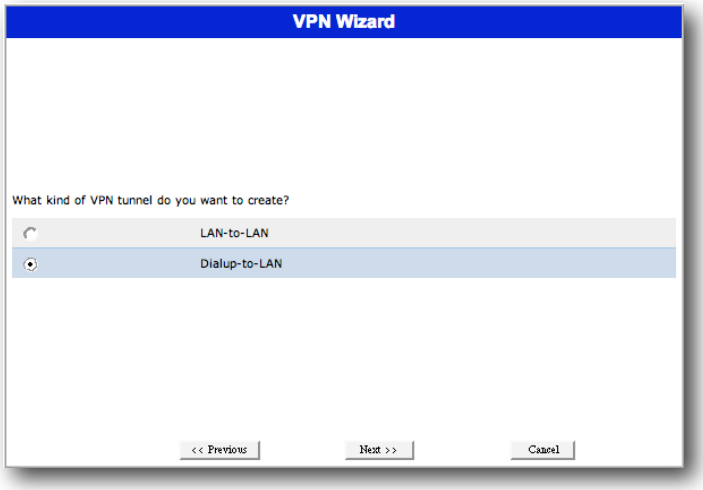
In the new window, select **Trust** for the **local** site and **Untrust** for the **remote** site.

Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



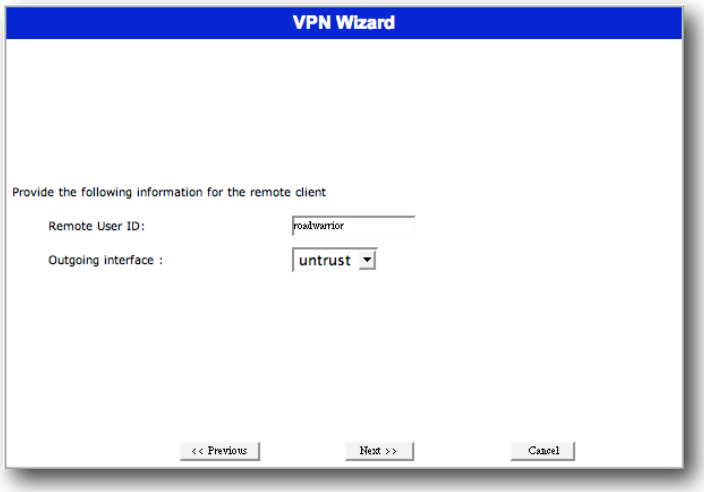
Select **Make new tunnel interface** and bind it to **trust (trust-vr)**.

Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



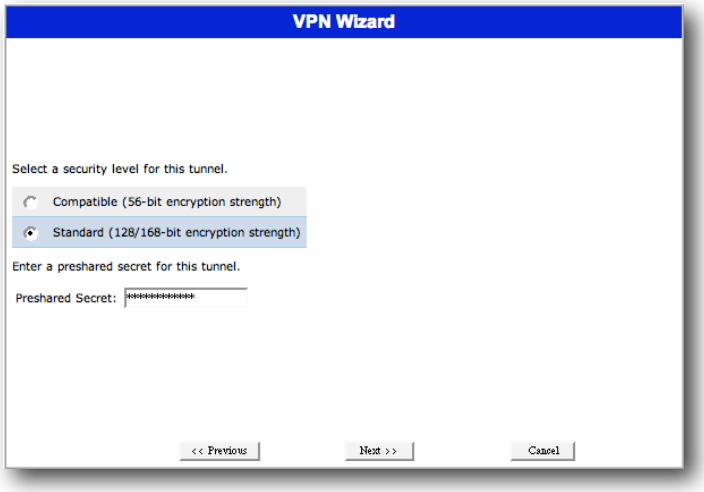
Select Dialup-to-LAN for the type of VPN tunnel you want to create.

Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



Enter a name into the field **Remote User ID** and select **untrust** for the outgoing interface.
Please remember **Remote User ID** as you will need it again when setting up the connection in IPSecuritas.

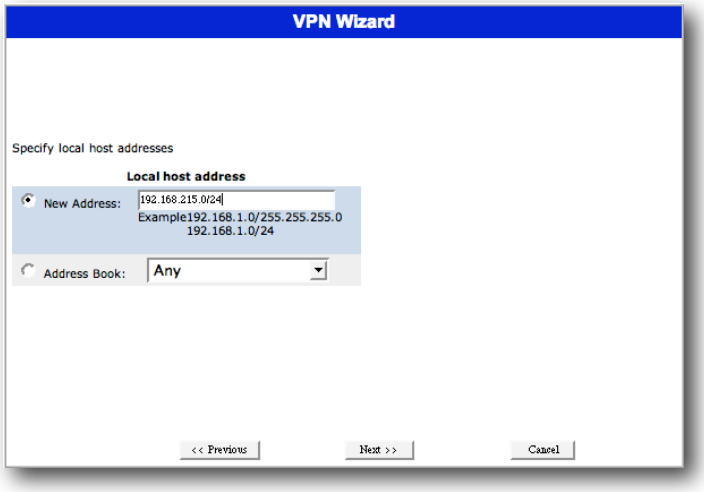
Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



Select **Standard (128/168-bit encryption strength)** for the security level and enter a secure **Preshared Secret** (an arbitrary but not easy to guess word, preferrably with special characters and numbers in it).

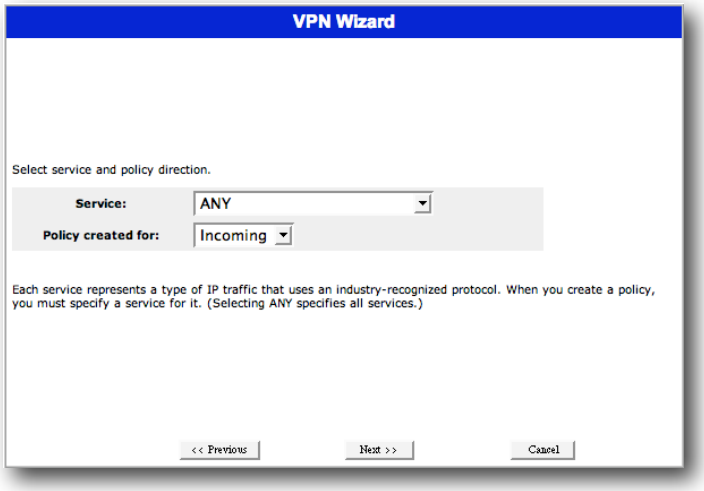
Please remember the preshared secret as you will need it again when setting up the connection in IPSecuritas.

Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



Select **New Address** and enter the local LAN address and its netmask (the trusted interface you want to access). You may limit the netmask to a part of the local LAN.

Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



Select the service you want to make available to the users accessing via VPN. When selecting **ANY**, all traffic passes. Select **Incoming** for the policy direction.

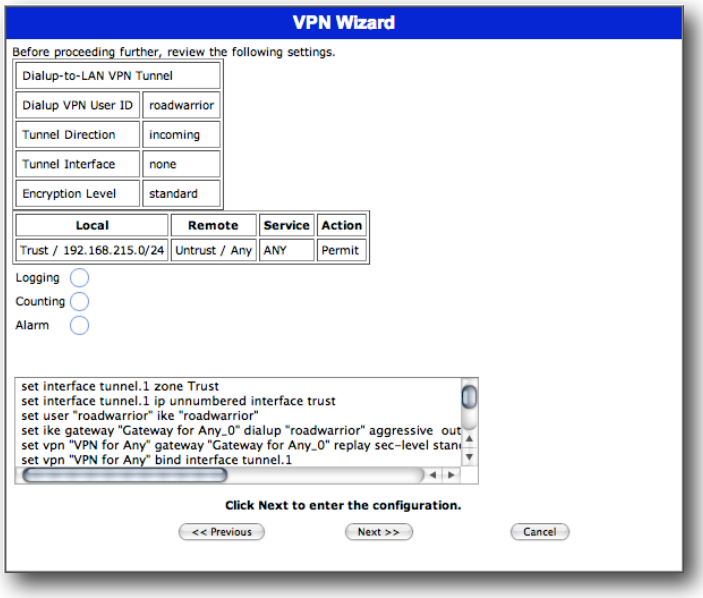
Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.

Set the logging and traffic statistics settings to your needs. If you don't want to monitor VPN traffic and usage, you may disable all options.

Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.

If you want to limit VPN usage to certain times, select an appropriate schedule.

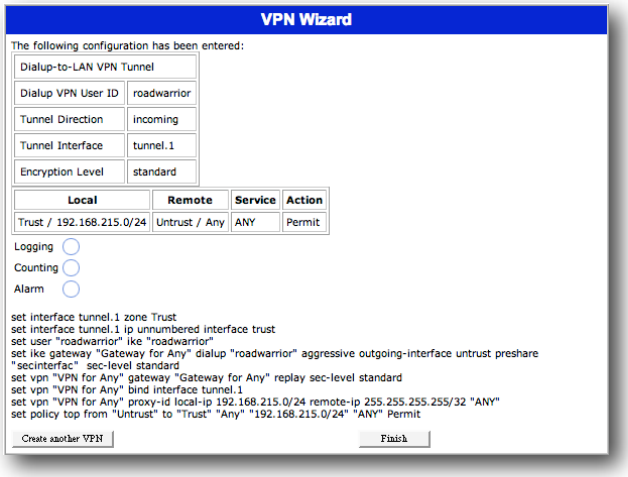
Press **Next**. The window's contents will be replaced with the parameters for the next wizard step.



"192.168.215.0/24" "ANY" Permit

The next window will show you a summary of your settings.
The listing in the text field can be used to configure your Netscreen from the command line.
If you followed all instructions above, you should have the following entries:

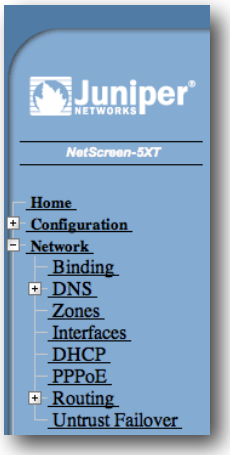
```
set interface tunnel.1 zone Trust
set interface tunnel.1 ip unnumbered interface
trust
set user "roadwarrior" ike "roadwarrior"
set ike gateway "Gateway for Any_0" dialup
"roadwarrior" aggressive  outgoing-interface
untrust preshare "securepassword" sec-level
standard
set vpn "VPN for Any" gateway "Gateway for Any_0"
replay sec-level standard
set vpn "VPN for Any" bind interface tunnel.1
set vpn "VPN for Any" proxy-id local-ip
192.168.215.0/24 remote-ip 255.255.255.255/32
"ANY"
set address Trust "192.168.215.0/24"
192.168.215.0/24
set policy top from "Untrust" to "Trust" "Any"
```



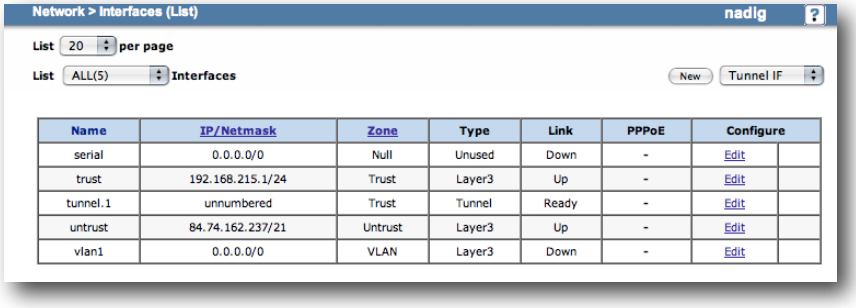
After pressing **Next**, the configuration is saved and incoming VPN traffic allowed.

Press **Finish** to close the VPN wizard.

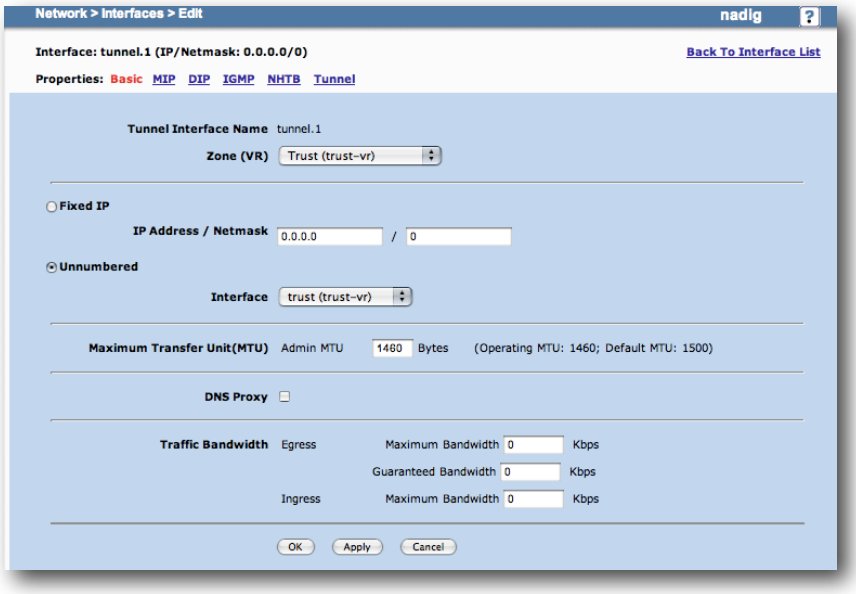
Adapt the MTU



In order for the connection to work properly, you need to adapt the MTU (Maximal Transfer Unit) of the tunnel interface.
In the main interface, click on **Network**, then **Interfaces** in the networks submenu.



Select **Edit** in the table row your tunnel interface appears (most often **tunnel.1**)



Set the **MTU** to **1460** bytes and click **Apply** or **OK** to save the changes.

You may now proceed with the configuration of IPSecuritas, described in the next chapter.

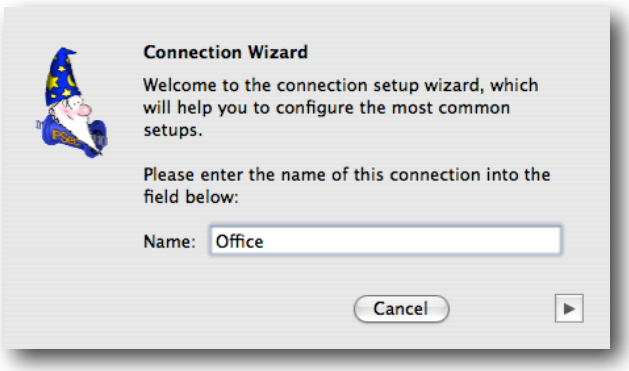
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to Juniper Netscreen firewalls.

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: 

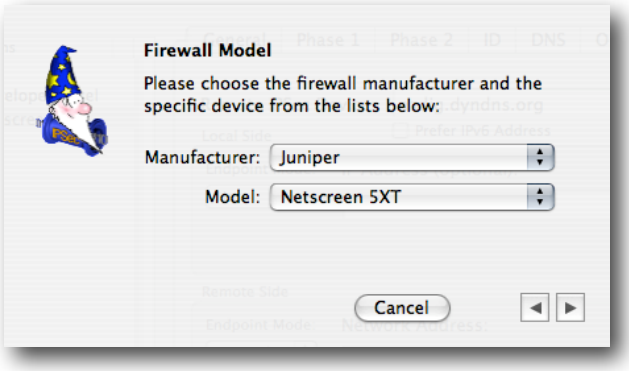
Enter Name of New Connection



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

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

Select Router Model



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

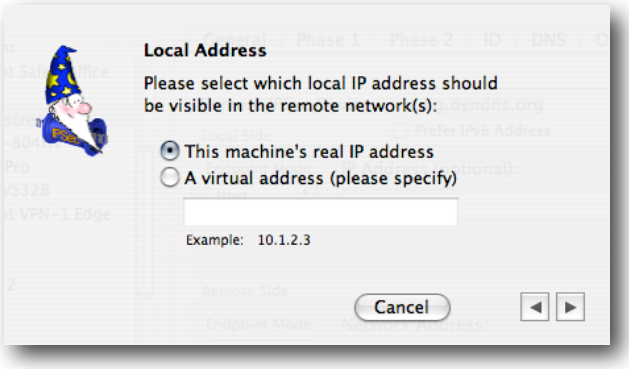
Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

Enter the public IP address or hostname of your Netscreen 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).

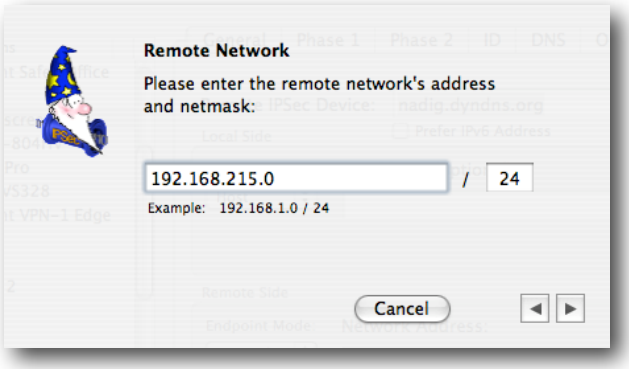
Click on the right arrow to continue with the next step.

Enter 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.

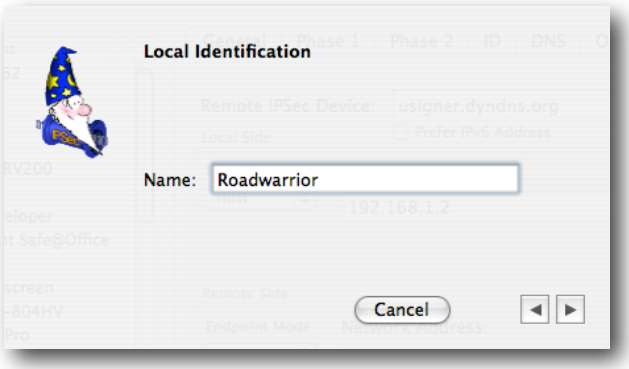
Enter Remote Network



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 Netscreen firewall.

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

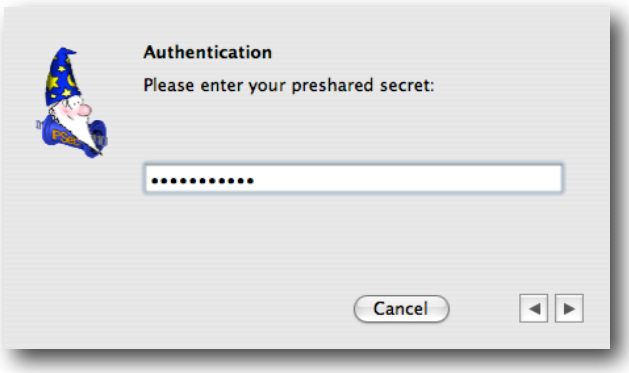
Enter Local Identification



Enter the **Remote User ID** you chose while running the Netscreen VPN wizard into the field for you local identification.

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

Enter Preshared Key



Enter the same **Preshared Key** you chose while running the Netscreen VPN wizard.

Click on the right arrow to finish the connection setup.

Diagnosis

Start IPSec

Press the Start Button in IPSecuritas' main window. A yellow dot appears, which should turn green after a few seconds, indicating a successful connection establishment. The remote LAN should now be accessible.

Reachability Test

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

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

Sample Netscreen

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

Date / Time	Level	Description
2007-01-21 14:51:33	info	IKE<80.218.148.110> Phase 2 msg ID <bfb41773>: Completed negotiations with SPI <f455c868>, tunnel ID <4>, and lifetime <1800> seconds/<0> KB.
2007-01-21 14:51:33	info	IKE<80.218.148.110> Phase 2 msg ID <bfb41773>: Responded to the peer's first message.
2007-01-21 14:51:32	info	IKE<80.218.148.110>: Received initial contact notification and removed Phase 1 SAs.
2007-01-21 14:51:32	info	IKE<80.218.148.110>: Received initial contact notification and removed Phase 2 SAs.
2007-01-21 14:51:32	info	IKE<80.218.148.110>: Received a notification message for DOI <1> <24578> <INITIAL-CONTACT>.
2007-01-21 14:51:32	info	IKE<80.218.148.110> Phase 1: Completed Aggressive mode negotiations with a <28800>-second lifetime.
2007-01-21 14:51:32	info	IKE<80.218.148.110> Phase 1: Completed for user <roadwarrior>.
2007-01-21 14:51:32	info	IKE<80.218.148.110> Phase 1: IKE responder has detected NAT in front of the remote device.
2007-01-21 14:51:32	info	IKE<80.218.148.110> Phase 1: Responder starts AGGRESSIVE mode negotiations.
2007-01-21 14:51:14	notif	All logged events or alarms were cleared by admin admin

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 3.0rc build 1098, Mon Jan 15 21:11:40 CET 2007, nadig
Darwin 8.8.3 Darwin Kernel Version 8.8.3: Wed Oct 18 21:57:10 PDT 2006; root:xnu-792.15.4.obj~4/RELEASE_I386 i386

Jan 21, 19:41:16  Info     APP  IKE daemon started
Jan 21, 19:41:16  Info     APP  IPSec started
Jan 21, 19:41:16  Debug    APP  State change from IDLE to RUNNING after event START
Jan 21, 19:41:16  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Jan 21, 19:41:16  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Jan 21, 19:41:16  Info     IKE  Foreground mode.
Jan 21, 19:41:16  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
Jan 21, 19:41:16  Info     IKE  @(#)This product linked OpenSSL 0.9.7i 14 Oct 2005 (http://www.openssl.org/)
Jan 21, 19:41:16  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
Jan 21, 19:41:16  Info     IKE  Resize address pool from 0 to 255
Jan 21, 19:41:16  Debug    IKE  lifetime = 1800
Jan 21, 19:41:16  Debug    IKE  lifebyte = 0
Jan 21, 19:41:16  Debug    IKE  encklen=0
Jan 21, 19:41:16  Debug    IKE  p:1 t:1
Jan 21, 19:41:16  Debug    IKE  3DES-CBC(5)
Jan 21, 19:41:16  Debug    IKE  SHA(2)
Jan 21, 19:41:16  Debug    IKE  1024-bit MODP group(2)
Jan 21, 19:41:16  Debug    IKE  pre-shared key(1)
Jan 21, 19:41:16  Debug    IKE
Jan 21, 19:41:16  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:16  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
Jan 21, 19:41:16  Debug    IKE  parse successed.
Jan 21, 19:41:16  Info     IKE  10.0.1.2[4500] used as isakmp port (fd=6)
Jan 21, 19:41:16  Info     IKE  10.0.1.2[500] used as isakmp port (fd=7)
Jan 21, 19:41:16  Debug    IKE  get pfkey X_SPDDUMP message
Jan 21, 19:41:16  Debug    IKE
Jan 21, 19:41:16  Debug    IKE  02120000 0f000100 01000000 c1540000 03000500 ff180000 10020000 c0a8d700
Jan 21, 19:41:16  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 0a000102 00000000 00000000
Jan 21, 19:41:16  Debug    IKE  07001200 02000100 b4010000 00000000 28003200 02020000 10020000 54495f72
Jan 21, 19:41:16  Debug    IKE  00000000 00000000 10020000 0a000102 00000000 00000000
Jan 21, 19:41:16  Debug    IKE  get pfkey X_SPDDUMP message
Jan 21, 19:41:16  Debug    IKE
Jan 21, 19:41:16  Debug    IKE  02120000 0f000100 00000000 c1540000 03000500 ff200000 10020000 0a000102
Jan 21, 19:41:16  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 c0a8d700 00000000 00000000
Jan 21, 19:41:16  Debug    IKE  07001200 02000200 b3010000 00000000 28003200 02020000 10020000 0a000102
Jan 21, 19:41:16  Debug    IKE  00000000 00000000 10020000 54495f72 00000000 00000000
Jan 21, 19:41:16  Debug    IKE  sub:0xbffff314: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 21, 19:41:16  Debug    IKE  db :0x308c48: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 21, 19:41:17  Debug    IKE  get pfkey ACQUIRE message
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  02060003 26000000 74020000 00000000 03000500 ff200000 10020000 0a000102
Jan 21, 19:41:17  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 54495f72 00000000 00000000
Jan 21, 19:41:17  Debug    IKE  02001200 02000200 b3010000 00000000 1c000d00 20000000 00030000 00000000
Jan 21, 19:41:17  Debug    IKE  00010008 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Jan 21, 19:41:17  Debug    IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
```

```
Jan 21, 19:41:17  Debug   IKE  00040000 00000000 0001c001 00000000 01000000 01000000 00000000 00000000
Jan 21, 19:41:17  Debug   IKE  00000000 00000000 00000000 00000000 80510100 00000000 80700000 00000000
Jan 21, 19:41:17  Debug   IKE  00000000 00000000 000c0000 00000000 00010001 00000000 01000000 01000000
Jan 21, 19:41:17  Debug   IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Jan 21, 19:41:17  Debug   IKE  80700000 00000000 00000000 00000000
Jan 21, 19:41:17  Debug   IKE  suitable outbound SP found: 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out.
Jan 21, 19:41:17  Debug   IKE  sub:0xbffff300: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 21, 19:41:17  Debug   IKE  db :0x308c48: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in
Jan 21, 19:41:17  Debug   IKE  suitable inbound SP found: 192.168.215.0/24[0] 10.0.1.2/32[0] proto=any dir=in.
Jan 21, 19:41:17  Debug   IKE  new acquire 10.0.1.2/32[0] 192.168.215.0/24[0] proto=any dir=out
Jan 21, 19:41:17  Debug   IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=0:0)
Jan 21, 19:41:17  Debug   IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 21, 19:41:17  Debug   IKE  (trns_id=AES encklen=128 authtype=hmac-sha)
Jan 21, 19:41:17  Debug   IKE  in post_acquire
Jan 21, 19:41:17  Debug   IKE  configuration found for 84.73.95.114.
Jan 21, 19:41:17  Info    IKE  IPsec-SA request for 84.73.95.114 queued due to no phase1 found.
Jan 21, 19:41:17  Debug   IKE  ===
Jan 21, 19:41:17  Info    IKE  initiate new phase 1 negotiation: 10.0.1.2[500]<=>84.73.95.114[500]
Jan 21, 19:41:17  Info    IKE  begin Aggressive mode.
Jan 21, 19:41:17  Debug   IKE  new cookie:
Jan 21, 19:41:17  Debug   IKE  2f2c523a0f56a65a
Jan 21, 19:41:17  Debug   IKE  use ID type of FQDN
Jan 21, 19:41:17  Debug   IKE  compute DH's private.
Jan 21, 19:41:17  Debug   IKE
Jan 21, 19:41:17  Debug   IKE  46528be4 16e892a3 1dbe73f6 f2ba4cfa 755ac446 9cb2e1ac fe4bb246 4ddb656d
Jan 21, 19:41:17  Debug   IKE  7939e3eb e2ac2ed0 dcbf4874 a3afe0fa 6423a37b 24f2c23e 73336767 983bfaa8
Jan 21, 19:41:17  Debug   IKE  667a208a c2f2a9b8 43f42de6 690daa82 742244cc a143438c cbd7a9f6 87a1cfc7
Jan 21, 19:41:17  Debug   IKE  00f0e78c b41336c0 a684f9c0 3019c8f8 d313d4dc 21e40c3d 9937d87e 59713241
Jan 21, 19:41:17  Debug   IKE  compute DH's public.
Jan 21, 19:41:17  Debug   IKE
Jan 21, 19:41:17  Debug   IKE  9cf8cd80 7aa01c3b cbd95842 257810f0 db3bfe71 9122e0b9 bc96c7d1 29368b9d
Jan 21, 19:41:17  Debug   IKE  20bd40f4 ee3ea2e9 e65c8fba 18a81bba d74c1a44 0fa6e53d e517d3c7 662ddfd3
Jan 21, 19:41:17  Debug   IKE  ca0bef1d 6445f56e bd7d60ff c402249d 05ada598 8468d7e5 b9ff90c7 6ef71544
Jan 21, 19:41:17  Debug   IKE  26df046e c6d186c5 394fbd5e 8516723b 4be0af50 2aa71682 dd7d5d21 b330a402
Jan 21, 19:41:17  Debug   IKE  authmethod is pre-shared key
Jan 21, 19:41:17  Debug   IKE  add payload of len 48, next type 4
Jan 21, 19:41:17  Debug   IKE  add payload of len 128, next type 10
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 5
Jan 21, 19:41:17  Debug   IKE  add payload of len 15, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 13
Jan 21, 19:41:17  Debug   IKE  add payload of len 16, next type 0
Jan 21, 19:41:17  Debug   IKE  491 bytes from 10.0.1.2[500] to 84.73.95.114[500]
Jan 21, 19:41:17  Debug   IKE  sockname 10.0.1.2[500]
Jan 21, 19:41:17  Debug   IKE  send packet from 10.0.1.2[500]
Jan 21, 19:41:17  Debug   IKE  send packet to 84.73.95.114[500]
Jan 21, 19:41:17  Debug   IKE  1 times of 491 bytes message will be sent to 84.73.95.114[500]
Jan 21, 19:41:17  Debug   IKE
Jan 21, 19:41:17  Debug   IKE  2f2c523a 0f56a65a 00000000 00000000 01100400 00000000 000001eb 04000034
Jan 21, 19:41:17  Debug   IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c0708
Jan 21, 19:41:17  Debug   IKE  80010005 80030001 80020002 80040002 0a000084 9cf8cd80 7aa01c3b cbd95842
Jan 21, 19:41:17  Debug   IKE  257810f0 db3bfe71 9122e0b9 bc96c7d1 29368b9d 20bd40f4 ee3ea2e9 e65c8fba
Jan 21, 19:41:17  Debug   IKE  18a81bba d74c1a44 0fa6e53d e517d3c7 662ddfd3 ca0bef1d 6445f56e bd7d60ff
Jan 21, 19:41:17  Debug   IKE  c402249d 05ada598 8468d7e5 b9ff90c7 6ef71544 26df046e c6d186c5 394fbd5e
Jan 21, 19:41:17  Debug   IKE  8516723b 4be0af50 2aa71682 dd7d5d21 b330a402 05000014 d982a806 1a68411c
Jan 21, 19:41:17  Debug   IKE  173f6bc1 abe57cf6 0d000013 02000000 726f6164 77617272 696f720d 0000144a
Jan 21, 19:41:17  Debug   IKE  131c8107 0358455c 5728f20e 95452f0d 0000148f 8d83826d 246b6fc7 a8a6a428
Jan 21, 19:41:17  Debug   IKE  c11de80d 00001443 9b59f8ba 676c4c77 37ae22ea b8f5820d 0000144d 1e0e136d
Jan 21, 19:41:17  Debug   IKE  eafa34c4 f3ea9f02 ec72850d 00001480 d0bb3def 54565ee8 4645d4c8 5ce3ee0d
Jan 21, 19:41:17  Debug   IKE  00001499 09b64eed 937c6573 de52ace9 52fa6b0d 0000147d 9419a653 10ca6f2c
Jan 21, 19:41:17  Debug   IKE  179d9215 529d560d 000014cd 60464335 df21f87c fdb2fc68 b6a4480d 00001490
Jan 21, 19:41:17  Debug   IKE  cb80913e bb696e08 6381b5ec 427b1f0d 00001416 f6ca16e4 a4066d83 821a0f0a
Jan 21, 19:41:17  Debug   IKE  eaa8620d 00001444 85152d18 b6bbcd0b e8a84695 79ddcc00 000014af cad71368
Jan 21, 19:41:17  Debug   IKE  a1f1c96b 8696fc77 570100
Jan 21, 19:41:17  Debug   IKE  resend phase1 packet 2f2c523a0f56a65a:0000000000000000
```

```
Jan 21, 19:41:17  Debug    IKE  ===
Jan 21, 19:41:17  Debug    IKE  416 bytes message received from 84.73.95.114[500] to 10.0.1.2[500]
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  2f2c523a 0f56a65a 522a50c4 2af52311 01100400 00000000 000001a0 0d000034
Jan 21, 19:41:17  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 80010005 80020002
Jan 21, 19:41:17  Debug    IKE  80040002 80030001 800b0001 800c0708 0d000020 166f932d 55eb64d8 e4df4fd3
Jan 21, 19:41:17  Debug    IKE  7e2313f0 d0fd8451 00000000 00000000 0d000014 afcad713 68a1f1c9 6b8696fc
Jan 21, 19:41:17  Debug    IKE  77570100 04000018 48656172 74426561 745f4e6f 74696679 386b0100 0a000084
Jan 21, 19:41:17  Debug    IKE  b017ed69 ccd4da4c e38a04f9 710f99ba 8103ed67 6b919760 d6a15b2b cf51b00a
Jan 21, 19:41:17  Debug    IKE  dad4679b 9c3365d6 de503d6c 87ca47b5 91e47911 df7679f2 d338d242 a5e0cff7
Jan 21, 19:41:17  Debug    IKE  93320eaf 5e2c3bf3 84b0046a ce3a04a6 771852d1 68ae4921 9e25c52d 5cd56e0c
Jan 21, 19:41:17  Debug    IKE  42252ca2 1ae90a48 3d5ccdef 06ec3600 938d6cec f10c4b9c 5b31b123 43dd78e6
Jan 21, 19:41:17  Debug    IKE  05000018 d928e2c2 b0ce529f 53d4801e 3e33e534 294bb07d 0800000c 011101f4
Jan 21, 19:41:17  Debug    IKE  54495f72 0d000018 c91aabac 816d46df ea053824 81a0eff3 e83980ce 82000014
Jan 21, 19:41:17  Debug    IKE  90cb8091 3ebb696e 086381b5 ec427b1f 82000018 fd07ab0a 2a0fe473 1450b49d
Jan 21, 19:41:17  Debug    IKE  efed38b7 dd4becea 00000018 14e0c105 95a56d74 bd1c12ba 2d3557eb 3be7c13b
Jan 21, 19:41:17  Debug    IKE  begin.
Jan 21, 19:41:17  Debug    IKE  seen nptype=1(sa)
Jan 21, 19:41:17  Debug    IKE  seen nptype=13(vid)
Jan 21, 19:41:17  Debug    IKE  seen nptype=13(vid)
Jan 21, 19:41:17  Debug    IKE  seen nptype=13(vid)
Jan 21, 19:41:17  Debug    IKE  seen nptype=4(ke)
Jan 21, 19:41:17  Debug    IKE  seen nptype=10(nonce)
Jan 21, 19:41:17  Debug    IKE  seen nptype=5(id)
Jan 21, 19:41:17  Debug    IKE  seen nptype=8(hash)
Jan 21, 19:41:17  Debug    IKE  seen nptype=13(vid)
Jan 21, 19:41:17  Debug    IKE  seen nptype=130(nat-d)
Jan 21, 19:41:17  Debug    IKE  seen nptype=130(nat-d)
Jan 21, 19:41:17  Debug    IKE  succeed.
Jan 21, 19:41:17  Debug    IKE  received unknown Vendor ID
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  166f932d 55eb64d8 e4df4fd3 7e2313f0 d0fd8451 00000000 00000000
Jan 21, 19:41:17  Info     IKE  received Vendor ID: DPD
Jan 21, 19:41:17  Debug    IKE  remote supports DPD
Jan 21, 19:41:17  Debug    IKE  received unknown Vendor ID
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  48656172 74426561 745f4e6f 74696679 386b0100
Jan 21, 19:41:17  Info     IKE  received Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Jan 21, 19:41:17  Info     IKE
Jan 21, 19:41:17  Debug    IKE  total SA len=48
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  00000001 00000001 00000028 01010001 00000020 01010000 80010005 80020002
Jan 21, 19:41:17  Debug    IKE  80040002 80030001 800b0001 800c0708
Jan 21, 19:41:17  Debug    IKE  begin.
Jan 21, 19:41:17  Debug    IKE  seen nptype=2(prop)
Jan 21, 19:41:17  Debug    IKE  succeed.
Jan 21, 19:41:17  Debug    IKE  proposal #1 len=40
Jan 21, 19:41:17  Debug    IKE  begin.
Jan 21, 19:41:17  Debug    IKE  seen nptype=3(trns)
Jan 21, 19:41:17  Debug    IKE  succeed.
Jan 21, 19:41:17  Debug    IKE  transform #1 len=32
Jan 21, 19:41:17  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Jan 21, 19:41:17  Debug    IKE  encryption(3des)
Jan 21, 19:41:17  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Jan 21, 19:41:17  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:17  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Jan 21, 19:41:17  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Jan 21, 19:41:17  Debug    IKE  type=Life Duration, flag=0x8000, lorv=1800
Jan 21, 19:41:17  Debug    IKE  pair 1:
Jan 21, 19:41:17  Debug    IKE  0x309400: next=0x0 tnext=0x0
Jan 21, 19:41:17  Debug    IKE  proposal #1: 1 transform
Jan 21, 19:41:17  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
Jan 21, 19:41:17  Debug    IKE  trns#=1, trns-id=IKE
Jan 21, 19:41:17  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Jan 21, 19:41:17  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Jan 21, 19:41:17  Debug    IKE  type=Group Description, flag=0x8000, lorv=1024-bit MODP group
Jan 21, 19:41:17  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Jan 21, 19:41:17  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Jan 21, 19:41:17  Debug    IKE  type=Life Duration, flag=0x8000, lorv=1800
Jan 21, 19:41:17  Debug    IKE  Compared: DB:Peer
Jan 21, 19:41:17  Debug    IKE  (lifetime = 1800:1800)
Jan 21, 19:41:17  Debug    IKE  (lifebyte = 0:0)
```

```
Jan 21, 19:41:17  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
Jan 21, 19:41:17  Debug    IKE  (encklen = 0:0)
Jan 21, 19:41:17  Debug    IKE  hashtype = SHA:SHA
Jan 21, 19:41:17  Debug    IKE  authmethod = pre-shared key:pre-shared key
Jan 21, 19:41:17  Debug    IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
Jan 21, 19:41:17  Debug    IKE  an acceptable proposal found.
Jan 21, 19:41:17  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:17  Debug    IKE  agreed on pre-shared key auth.
Jan 21, 19:41:17  Info     IKE  Selected NAT-T version: draft-ietf-ipsec-nat-t-ike-02
Jan 21, 19:41:17  Info     IKE
Jan 21, 19:41:17  Info     IKE  Hashing 10.0.1.2[500] with algo #2
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Info     IKE  NAT-D payload #-1 doesn't match
Jan 21, 19:41:17  Info     IKE  Hashing 84.73.95.114[500] with algo #2
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Info     IKE  NAT-D payload #0 verified
Jan 21, 19:41:17  Info     IKE  NAT detected: ME
Jan 21, 19:41:17  Info     IKE  KA list add: 10.0.1.2[4500]->84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE  compute DH's shared.
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  a9714216 692bd9f6 5083ee4c f28e601f 1aad0255 a579e361 73e3c6f0 645475e5
Jan 21, 19:41:17  Debug    IKE  58046aae 5b9f0c79 ec6bd5b7 ffcc321e 692c7b64 819e250b b5532df8 c3f35877
Jan 21, 19:41:17  Debug    IKE  cd7c3ec1 34b3d465 2686f968 99146877 8249bbd3 27a316c8 0337474a 92de3dea
Jan 21, 19:41:17  Debug    IKE  83111041 3a58a5be fcf8f8a6 01bf44ca f7bb0781 74fcc752 6fae9791 0862e51f
Jan 21, 19:41:17  Info     IKE  couldn't find the proper pskey, try to get one by the peer's address.
Jan 21, 19:41:17  Debug    IKE  the psk found.
Jan 21, 19:41:17  Debug    IKE  psk: 2007-01-21 19:41:17: DEBUG2:
Jan 21, 19:41:17  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
Jan 21, 19:41:17  Debug    IKE  nonce 1: 2007-01-21 19:41:17: DEBUG:
Jan 21, 19:41:17  Debug    IKE  d982a806 1a68411c 173f6bc1 abe57cf6
Jan 21, 19:41:17  Debug    IKE  nonce 2: 2007-01-21 19:41:17: DEBUG:
Jan 21, 19:41:17  Debug    IKE  d928e2c2 b0ce529f 53d4801e 3e33e534 294bb07d
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  SKEYID computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  f691fbea 15830885 ed858c94 1b40c74a 56043ffa
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  SKEYID_d computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  b1add714 8491c806 7d785e52 8dbe6b22 bfc32a45
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  SKEYID_a computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  eb97c77a 407a7673 70f1d004 eb4b2a7e 5e6fcdaf
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  SKEYID_e computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  086febe8 ddfb9d68 ef9dd246 e35009ad 460b1096
Jan 21, 19:41:17  Debug    IKE  encryption(3des)
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  compute intermediate encryption key K1
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  00
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  compute intermediate encryption key K2
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  0a1d88b8 ac28d55f 3d9d1ab0 71253b31 85c3dffe
Jan 21, 19:41:17  Debug    IKE  final encryption key computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c 0a1d88b8
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Debug    IKE  encryption(3des)
Jan 21, 19:41:17  Debug    IKE  IV computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  226187ef 0572c7ae
Jan 21, 19:41:17  Debug    IKE  HASH received:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  c91aabac 816d46df ea053824 81a0eff3 e83980ce
```

```
Jan 21, 19:41:17  Debug    IKE  HASH with:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  b017ed69 ccd4da4c e38a04f9 710f99ba 8103ed67 6b919760 d6a15b2b cf51b00a
Jan 21, 19:41:17  Debug    IKE  dad4679b 9c3365d6 de503d6c 87ca47b5 91e47911 df7679f2 d338d242 a5e0cff7
Jan 21, 19:41:17  Debug    IKE  93320eaf 5e2c3bf3 84b0046a ce3a04a6 771852d1 68ae4921 9e25c52d 5cd56e0c
Jan 21, 19:41:17  Debug    IKE  42252ca2 1ae90a48 3d5ccdef 06ec3600 938d6cec f10c4b9c 5b31b123 43dd78e6
Jan 21, 19:41:17  Debug    IKE  9cf8cd80 7aa01c3b cbd95842 257810f0 db3bfe71 9122e0b9 bc96c7d1 29368b9d
Jan 21, 19:41:17  Debug    IKE  20bd40f4 ee3ea2e9 e65c8fba 18a81bba d74c1a44 0fa6e53d e517d3c7 662ddfd3
Jan 21, 19:41:17  Debug    IKE  ca0bef1d 6445f56e bd7d60ff c402249d 05ada598 8468d7e5 b9ff90c7 6ef71544
Jan 21, 19:41:17  Debug    IKE  26df046e c6d186c5 394fbd5e 8516723b 4be0af50 2aa71682 dd7d5d21 b330a402
Jan 21, 19:41:17  Debug    IKE  522a50c4 2af52311 2f2c523a 0f56a65a 00000001 00000001 00000028 01010001
Jan 21, 19:41:17  Debug    IKE  00000020 01010000 800b0001 800c0708 80010005 80030001 80020002 80040002
Jan 21, 19:41:17  Debug    IKE  011101f4 54495f72
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  HASH (init) computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  c91aabac 816d46df ea053824 81a0eff3 e83980ce
Jan 21, 19:41:17  Debug    IKE  HASH for PSK validated.
Jan 21, 19:41:17  Debug    IKE  ===
Jan 21, 19:41:17  Debug    IKE  generate HASH_I
Jan 21, 19:41:17  Debug    IKE  HASH with:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  9cf8cd80 7aa01c3b cbd95842 257810f0 db3bfe71 9122e0b9 bc96c7d1 29368b9d
Jan 21, 19:41:17  Debug    IKE  20bd40f4 ee3ea2e9 e65c8fba 18a81bba d74c1a44 0fa6e53d e517d3c7 662ddfd3
Jan 21, 19:41:17  Debug    IKE  ca0bef1d 6445f56e bd7d60ff c402249d 05ada598 8468d7e5 b9ff90c7 6ef71544
Jan 21, 19:41:17  Debug    IKE  26df046e c6d186c5 394fbd5e 8516723b 4be0af50 2aa71682 dd7d5d21 b330a402
Jan 21, 19:41:17  Debug    IKE  b017ed69 ccd4da4c e38a04f9 710f99ba 8103ed67 6b919760 d6a15b2b cf51b00a
Jan 21, 19:41:17  Debug    IKE  dad4679b 9c3365d6 de503d6c 87ca47b5 91e47911 df7679f2 d338d242 a5e0cff7
Jan 21, 19:41:17  Debug    IKE  93320eaf 5e2c3bf3 84b0046a ce3a04a6 771852d1 68ae4921 9e25c52d 5cd56e0c
Jan 21, 19:41:17  Debug    IKE  42252ca2 1ae90a48 3d5ccdef 06ec3600 938d6cec f10c4b9c 5b31b123 43dd78e6
Jan 21, 19:41:17  Debug    IKE  2f2c523a 0f56a65a 522a50c4 2af52311 00000001 00000001 00000028 01010001
Jan 21, 19:41:17  Debug    IKE  00000020 01010000 800b0001 800c0708 80010005 80030001 80020002 80040002
Jan 21, 19:41:17  Debug    IKE  02000000 726f6164 77617272 696f72
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  HASH (init) computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  3ae16735 64c43a75 26e0ee70 ea19327e 791f02ed
Jan 21, 19:41:17  Info     IKE  Adding remote and local NAT-D payloads.
Jan 21, 19:41:17  Info     IKE  Hashing 84.73.95.114[4500] with algo #2
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Info     IKE  Hashing 10.0.1.2[4500] with algo #2
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Debug    IKE  add payload of len 20, next type 130
Jan 21, 19:41:17  Debug    IKE  add payload of len 20, next type 130
Jan 21, 19:41:17  Debug    IKE  add payload of len 20, next type 0
Jan 21, 19:41:17  Debug    IKE  Adding NON-ESP marker
Jan 21, 19:41:17  Debug    IKE  104 bytes from 10.0.1.2[4500] to 84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE  sockname 10.0.1.2[4500]
Jan 21, 19:41:17  Debug    IKE  send packet from 10.0.1.2[4500]
Jan 21, 19:41:17  Debug    IKE  send packet to 84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE  1 times of 104 bytes message will be sent to 84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  00000000 2f2c523a 0f56a65a 522a50c4 2af52311 08100400 00000000 00000064
Jan 21, 19:41:17  Debug    IKE  82000018 3ae16735 64c43a75 26e0ee70 ea19327e 791f02ed 82000018 2272606d
Jan 21, 19:41:17  Debug    IKE  9bb348d4 883dfea4 87327e3d 473cf75a 00000018 76f61e7f 3b09e3d9 977d7e9a
Jan 21, 19:41:17  Debug    IKE  ec8d3cc4 27b0c82f
Jan 21, 19:41:17  Debug    IKE  compute IV for phase2
Jan 21, 19:41:17  Debug    IKE  phase1 last IV:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  226187ef 0572c7ae 91c6c41a
Jan 21, 19:41:17  Debug    IKE  hash(sha1)
Jan 21, 19:41:17  Debug    IKE  encryption(3des)
Jan 21, 19:41:17  Debug    IKE  phase2 IV computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  23ebc25d bfa1d895
Jan 21, 19:41:17  Debug    IKE  HASH with:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  91c6c41a 0000001c 00000001 01106002 2f2c523a 0f56a65a 522a50c4 2af52311
Jan 21, 19:41:17  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:17  Debug    IKE  HASH computed:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  810c70d1 dc9f8fdf c8bd2b14 1df9dee3 275b6ab6
Jan 21, 19:41:17  Debug    IKE  begin encryption.
Jan 21, 19:41:17  Debug    IKE  encryption(3des)
```

```
Jan 21, 19:41:17  Debug    IKE  pad length = 4
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  0b000018 810c70d1 dc9f8fdf c8bd2b14 1df9dee3 275b6ab6 0000001c 00000001
Jan 21, 19:41:17  Debug    IKE  01106002 2f2c523a 0f56a65a 522a50c4 2af52311 00000004
Jan 21, 19:41:17  Debug    IKE  encryption(3des)
Jan 21, 19:41:17  Debug    IKE  with key:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c 0a1d88b8
Jan 21, 19:41:17  Debug    IKE  encrypted payload by IV:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  23ebc25d bfa1d895
Jan 21, 19:41:17  Debug    IKE  save IV for next:
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  f5429c27 75f5ab1a
Jan 21, 19:41:17  Debug    IKE  encrypted.
Jan 21, 19:41:17  Debug    IKE  Adding NON-ESP marker
Jan 21, 19:41:17  Debug    IKE  88 bytes from 10.0.1.2[4500] to 84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE  sockname 10.0.1.2[4500]
Jan 21, 19:41:17  Debug    IKE  send packet from 10.0.1.2[4500]
Jan 21, 19:41:17  Debug    IKE  send packet to 84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE  1 times of 88 bytes message will be sent to 84.73.95.114[4500]
Jan 21, 19:41:17  Debug    IKE
Jan 21, 19:41:17  Debug    IKE  00000000 2f2c523a 0f56a65a 522a50c4 2af52311 08100501 91c6c41a 00000054
Jan 21, 19:41:17  Debug    IKE  fda0c68e 87105980 5fd38326 0bbbdee7 f96f2132 c391df28 7f534fd8 4d8f3b2e
Jan 21, 19:41:17  Debug    IKE  935d6876 4ae6bfde 1057799e 78f76c3e f5429c27 75f5ab1a
Jan 21, 19:41:17  Debug    IKE  sendto Information notify.
Jan 21, 19:41:17  Debug    IKE  IV freed
Jan 21, 19:41:17  Info     IKE  ISAKMP-SA established 10.0.1.2[4500]-84.73.95.114[4500] spi:2f2c523a0f56a65a:
522a50c42af52311
Jan 21, 19:41:17  Debug    IKE  ===
Jan 21, 19:41:18  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netscreen
Jan 21, 19:41:18  Debug    IKE  ===
Jan 21, 19:41:18  Debug    IKE  begin QUICK mode.
Jan 21, 19:41:18  Info     IKE  initiate new phase 2 negotiation: 10.0.1.2[4500]<=>84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE  compute IV for phase2
Jan 21, 19:41:18  Debug    IKE  phase1 last IV:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  226187ef 0572c7ae c8263db7
Jan 21, 19:41:18  Debug    IKE  hash(sha1)
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  phase2 IV computed:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  d7a494ea 6065d87f
Jan 21, 19:41:18  Debug    IKE  call pfkey_send_getspi
Jan 21, 19:41:18  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 84.73.95.114[0]->10.0.1.2[0]
Jan 21, 19:41:18  Debug    IKE  pfkey getspi sent.
Jan 21, 19:41:18  Debug    IKE  get pfkey GETSPI message
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  02010003 0a000000 74020000 c1540000 02000100 06acbfb4 5e0000fb 90111601
Jan 21, 19:41:18  Debug    IKE  03000500 ff200000 10020000 54495f72 00000000 00000000 03000600 ff200000
Jan 21, 19:41:18  Debug    IKE  10020000 0a000102 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 84.73.95.114[0]->10.0.1.2[0] spi=111984564(0x6acbfb4)
Jan 21, 19:41:18  Info     IKE  NAT detected -> UDP encapsulation (ENC_MODE 1->61443).
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  compute DH's private.
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  7476fe59 ee614cf4 f3fd3cb4 2cacd590 ee924830 3dbad6f7 a7ca1aa0 52a71245
Jan 21, 19:41:18  Debug    IKE  cc7a3a75 c5ba99ae 91acac21 89c1a997 625b7af0 58124eff b5300d7b 269445b6
Jan 21, 19:41:18  Debug    IKE  a9470253 546a7589 7ca435bb 743cbadb d7a075e9 fabef8fb 4c3503aa e6292a89
Jan 21, 19:41:18  Debug    IKE  e08befad bfb134dd ff38b9c7 10370704 a9d8ba24 1e5298af 77d05ecc d921d1dd
Jan 21, 19:41:18  Debug    IKE  compute DH's public.
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  3874ab85 72599946 d9a1e360 cd9bae78 13db9aae c14b32d2 01874a7c 776eafd8
Jan 21, 19:41:18  Debug    IKE  2de7c1b4 d1d3c517 2455eee4 00fd005e f1ddd138 58238a19 414164d9 5b240349
Jan 21, 19:41:18  Debug    IKE  fa4f453f 5f4abe8b d45f6349 5ef78d8f c85b1887 7b7d622d 4b7613c5 65166a48
Jan 21, 19:41:18  Debug    IKE  280d41f1 06926c16 f1e14157 f3597b84 5f85e7e7 e5259ca0 001b950f 374fdfe9
Jan 21, 19:41:18  Debug    IKE  use local ID type IPv4_address
Jan 21, 19:41:18  Debug    IKE  use remote ID type IPv4_subnet
Jan 21, 19:41:18  Debug    IKE  IDci:
Jan 21, 19:41:18  Debug    IKE
```

```
Jan 21, 19:41:18  Debug    IKE  01000000 0a000102
Jan 21, 19:41:18  Debug    IKE  IDcr:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 21, 19:41:18  Debug    IKE  add payload of len 80, next type 10
Jan 21, 19:41:18  Debug    IKE  add payload of len 16, next type 4
Jan 21, 19:41:18  Debug    IKE  add payload of len 128, next type 5
Jan 21, 19:41:18  Debug    IKE  add payload of len 8, next type 5
Jan 21, 19:41:18  Debug    IKE  add payload of len 12, next type 0
Jan 21, 19:41:18  Debug    IKE  HASH with:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  c8263db7 0a000054 00000001 00000001 00000048 01030402 06acbfb4 0300001c
Jan 21, 19:41:18  Debug    IKE  01030000 80010001 80020708 8004f003 80050002 80030002 00000020 020c0000
Jan 21, 19:41:18  Debug    IKE  80010001 80020708 8004f003 80060080 80050002 80030002 04000014 d0f694ff
Jan 21, 19:41:18  Debug    IKE  22d5ad13 31c989af 42ede721 05000084 3874ab85 72599946 d9a1e360 cd9bae78
Jan 21, 19:41:18  Debug    IKE  13db9aae c14b32d2 01874a7c 776eafd8 2de7c1b4 d1d3c517 2455eee4 00fd005e
Jan 21, 19:41:18  Debug    IKE  f1ddd138 58238a19 414164d9 5b240349 fa4f453f 5f4abe8b d45f6349 5ef78d8f
Jan 21, 19:41:18  Debug    IKE  c85b1887 7b7d622d 4b7613c5 65166a48 280d41f1 06926c16 f1e14157 f3597b84
Jan 21, 19:41:18  Debug    IKE  5f85e7e7 e5259ca0 001b950f 374fdfe9 0500000c 01000000 0a000102 00000010
Jan 21, 19:41:18  Debug    IKE  04000000 c0a8d700 ffffff00
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  HASH computed:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  6a8f0ab6 48ce40b3 6899f54e b628d687 27939297
Jan 21, 19:41:18  Debug    IKE  add payload of len 20, next type 1
Jan 21, 19:41:18  Debug    IKE  begin encryption.
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  pad length = 8
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  01000018 6a8f0ab6 48ce40b3 6899f54e b628d687 27939297 0a000054 00000001
Jan 21, 19:41:18  Debug    IKE  00000001 00000048 01030402 06acbfb4 0300001c 01030000 80010001 80020708
Jan 21, 19:41:18  Debug    IKE  8004f003 80050002 80030002 00000020 020c0000 80010001 80020708 8004f003
Jan 21, 19:41:18  Debug    IKE  80060080 80050002 80030002 04000014 d0f694ff 22d5ad13 31c989af 42ede721
Jan 21, 19:41:18  Debug    IKE  05000084 3874ab85 72599946 d9a1e360 cd9bae78 13db9aae c14b32d2 01874a7c
Jan 21, 19:41:18  Debug    IKE  776eafd8 2de7c1b4 d1d3c517 2455eee4 00fd005e f1ddd138 58238a19 414164d9
Jan 21, 19:41:18  Debug    IKE  5b240349 fa4f453f 5f4abe8b d45f6349 5ef78d8f c85b1887 7b7d622d 4b7613c5
Jan 21, 19:41:18  Debug    IKE  65166a48 280d41f1 06926c16 f1e14157 f3597b84 5f85e7e7 e5259ca0 001b950f
Jan 21, 19:41:18  Debug    IKE  374fdfe9 0500000c 01000000 0a000102 00000010 04000000 c0a8d700 ffffff00
Jan 21, 19:41:18  Debug    IKE  00000000 00000008
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  with key:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c 0a1d88b8
Jan 21, 19:41:18  Debug    IKE  encrypted payload by IV:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  d7a494ea 6065d87f
Jan 21, 19:41:18  Debug    IKE  save IV for next:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  2545b600 13799918
Jan 21, 19:41:18  Debug    IKE  encrypted.
Jan 21, 19:41:18  Debug    IKE  Adding NON-ESP marker
Jan 21, 19:41:18  Debug    IKE  328 bytes from 10.0.1.2[4500] to 84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE  sockname 10.0.1.2[4500]
Jan 21, 19:41:18  Debug    IKE  send packet from 10.0.1.2[4500]
Jan 21, 19:41:18  Debug    IKE  send packet to 84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE  1 times of 328 bytes message will be sent to 84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  00000000 2f2c523a 0f56a65a 522a50c4 2af52311 08102001 c8263db7 00000144
Jan 21, 19:41:18  Debug    IKE  b1819372 2083fcbb b3907db4 1626fd57 7c23e867 a5dcb507 f994e905 972d3777
Jan 21, 19:41:18  Debug    IKE  43c439d6 1ac8920c 1bd24e7b 6079cac4 63851136 f141fdbd 9deefabf 0b8dafa9
Jan 21, 19:41:18  Debug    IKE  1187d0b3 b2baf810 f23ac624 57fe1b2e 67affc9e a0dc031d 24bbb8fe a7a1a5b9
Jan 21, 19:41:18  Debug    IKE  1adcdec6 c2bb4b21 e8cc60b0 d6f382a4 026fe934 dbfb4ca6 e6e270bc 607f930a
Jan 21, 19:41:18  Debug    IKE  a4e81c14 0cad07e3 7da712e6 e812e902 1b11b26c d03e623f e09da1d1 8aa74833
Jan 21, 19:41:18  Debug    IKE  7895dd27 503db860 95045c48 498cd4e3 cc633f7e 13261f71 9e023338 d01f1f3b
Jan 21, 19:41:18  Debug    IKE  6d7c88c2 aed66435 8cdad8ee 31a7407d 6dc2a2ec d2ddb8ff be57b287 385f2eea
Jan 21, 19:41:18  Debug    IKE  1a273e43 cb4545e8 ca51b1f3 62e913b0 d6f9a6e6 5142ce04 c93d6e92 7fb063aa
Jan 21, 19:41:18  Debug    IKE  eb29a94b 2391cf1f cf4970f3 cb3e67dc ba3bfc75 32c5516b a06185ee a47285ac
Jan 21, 19:41:18  Debug    IKE  2545b600 13799918
Jan 21, 19:41:18  Debug    IKE  resend phase2 packet 2f2c523a0f56a65a:522a50c42af52311:0000c826
Jan 21, 19:41:18  Debug    IKE  ===
Jan 21, 19:41:18  Debug    IKE  300 bytes message received from 84.73.95.114[4500] to 10.0.1.2[4500]
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  2f2c523a 0f56a65a 522a50c4 2af52311 08102001 c8263db7 0000012c 0d482331
Jan 21, 19:41:18  Debug    IKE  b33a7574 366efbf4 b5b7afc3 11e91518 dc25241f 62004778 fc4fb437 f511dbe7
```

```
Jan 21, 19:41:18  Debug    IKE  6560acc9 451ae20a 9ee80606 cddad89d f02ed41f 4d6d003b 956b1d7e 19599fee
Jan 21, 19:41:18  Debug    IKE  d6456c18 21aabd37 499f8d87 0e4d4a5a 3a69b1e3 30a8fbe6 d4fa0f48 cbe0b506
Jan 21, 19:41:18  Debug    IKE  6d8068fc e4460a14 4dd9c60f 9508bc49 16b8f035 68358c63 61de3af5 d157ada8
Jan 21, 19:41:18  Debug    IKE  8c4475a8 8434b406 7e111fc0 2013f159 72c27dfb 22817c8d 8edf8237 d9331854
Jan 21, 19:41:18  Debug    IKE  1387f17c 7506e9e1 8dc3d144 a4ff149d 932fed4a 83264c81 54f5b4b2 886b78b8
Jan 21, 19:41:18  Debug    IKE  1883d073 b662b9a8 8da2c811 ca64ad66 e7bb7109 a11c60d5 3d9719fb a340f7c5
Jan 21, 19:41:18  Debug    IKE  6ee65d02 3fd95b94 c1cd453f 6f466503 83238323 437a157f d9c97bfd af170c64
Jan 21, 19:41:18  Debug    IKE  eb7e6672 3043a52f 7c3d4355
Jan 21, 19:41:18  Debug    IKE  begin decryption.
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  IV was saved for next processing:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  3043a52f 7c3d4355
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  with key:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c 0a1d88b8
Jan 21, 19:41:18  Debug    IKE  decrypted payload by IV:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  2545b600 13799918
Jan 21, 19:41:18  Debug    IKE  decrypted payload, but not trimed.
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  01000018 56da4211 f26f64de 34cf8658 cc1f76f2 3ebaa8ad 0a000038 00000001
Jan 21, 19:41:18  Debug    IKE  00000001 0000002c 01030401 f455c864 00000020 01030000 80010001 00020004
Jan 21, 19:41:18  Debug    IKE  00000708 8004f003 80050002 80030002 04000018 cc6a62a5 1352c1e9 46ddf982
Jan 21, 19:41:18  Debug    IKE  147b5d21 f4d8779f 05000084 b3aa0f4b 5c5382dc 2b6a91c2 e972a837 33147350
Jan 21, 19:41:18  Debug    IKE  6b6c740f 9e8390c4 8e65d948 5da9f9da 46e257e8 87e98a9b fc53ffe0 13591101
Jan 21, 19:41:18  Debug    IKE  48b8309a b92ea0e1 679939a8 8410a06e 0d2f3f5a 47be4c7f ff79cfee 04d2b092
Jan 21, 19:41:18  Debug    IKE  c594056a 95f1b01f 007d4086 496e9cc7 a1f07d31 86b17766 945ea320 030c21cf
Jan 21, 19:41:18  Debug    IKE  efd77d86 ef473db5 4e9eaafd 0500000c 01000000 0a000102 00000010 04000000
Jan 21, 19:41:18  Debug    IKE  c0a8d700 ffffff00 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  padding len=0
Jan 21, 19:41:18  Debug    IKE  skip to trim padding.
Jan 21, 19:41:18  Debug    IKE  decrypted.
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  2f2c523a 0f56a65a 522a50c4 2af52311 08102001 c8263db7 0000012c 01000018
Jan 21, 19:41:18  Debug    IKE  56da4211 f26f64de 34cf8658 cc1f76f2 3ebaa8ad 0a000038 00000001 00000001
Jan 21, 19:41:18  Debug    IKE  0000002c 01030401 f455c864 00000020 01030000 80010001 00020004 00000708
Jan 21, 19:41:18  Debug    IKE  8004f003 80050002 80030002 04000018 cc6a62a5 1352c1e9 46ddf982 147b5d21
Jan 21, 19:41:18  Debug    IKE  f4d8779f 05000084 b3aa0f4b 5c5382dc 2b6a91c2 e972a837 33147350 6b6c740f
Jan 21, 19:41:18  Debug    IKE  9e8390c4 8e65d948 5da9f9da 46e257e8 87e98a9b fc53ffe0 13591101 48b8309a
Jan 21, 19:41:18  Debug    IKE  b92ea0e1 679939a8 8410a06e 0d2f3f5a 47be4c7f ff79cfee 04d2b092 c594056a
Jan 21, 19:41:18  Debug    IKE  95f1b01f 007d4086 496e9cc7 a1f07d31 86b17766 945ea320 030c21cf efd77d86
Jan 21, 19:41:18  Debug    IKE  ef473db5 4e9eaafd 0500000c 01000000 0a000102 00000010 04000000 c0a8d700
Jan 21, 19:41:18  Debug    IKE  ffffff00 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  begin.
Jan 21, 19:41:18  Debug    IKE  seen nptype=8(hash)
Jan 21, 19:41:18  Debug    IKE  seen nptype=1(sa)
Jan 21, 19:41:18  Debug    IKE  seen nptype=10(nonce)
Jan 21, 19:41:18  Debug    IKE  seen nptype=4(ke)
Jan 21, 19:41:18  Debug    IKE  seen nptype=5(id)
Jan 21, 19:41:18  Debug    IKE  seen nptype=5(id)
Jan 21, 19:41:18  Debug    IKE  succeed.
Jan 21, 19:41:18  Debug    IKE  HASH allocated:hbuf->l=288 actual:tlen=256
Jan 21, 19:41:18  Debug    IKE  HASH(2) received:2007-01-21 19:41:18: DEBUG:
Jan 21, 19:41:18  Debug    IKE  56da4211 f26f64de 34cf8658 cc1f76f2 3ebaa8ad
Jan 21, 19:41:18  Debug    IKE  HASH with:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  c8263db7 d0f694ff 22d5ad13 31c989af 42ede721 0a000038 00000001 00000001
Jan 21, 19:41:18  Debug    IKE  0000002c 01030401 f455c864 00000020 01030000 80010001 00020004 00000708
Jan 21, 19:41:18  Debug    IKE  8004f003 80050002 80030002 04000018 cc6a62a5 1352c1e9 46ddf982 147b5d21
Jan 21, 19:41:18  Debug    IKE  f4d8779f 05000084 b3aa0f4b 5c5382dc 2b6a91c2 e972a837 33147350 6b6c740f
Jan 21, 19:41:18  Debug    IKE  9e8390c4 8e65d948 5da9f9da 46e257e8 87e98a9b fc53ffe0 13591101 48b8309a
Jan 21, 19:41:18  Debug    IKE  b92ea0e1 679939a8 8410a06e 0d2f3f5a 47be4c7f ff79cfee 04d2b092 c594056a
Jan 21, 19:41:18  Debug    IKE  95f1b01f 007d4086 496e9cc7 a1f07d31 86b17766 945ea320 030c21cf efd77d86
Jan 21, 19:41:18  Debug    IKE  ef473db5 4e9eaafd 0500000c 01000000 0a000102 00000010 04000000 c0a8d700
Jan 21, 19:41:18  Debug    IKE  ffffff00
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  HASH computed:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  56da4211 f26f64de 34cf8658 cc1f76f2 3ebaa8ad
Jan 21, 19:41:18  Debug    IKE  total SA len=80
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  00000001 00000001 00000048 01030402 06acbfb4 0300001c 01030000 80010001
```

```
Jan 21, 19:41:18  Debug    IKE  80020708 8004f003 80050002 80030002 00000020 020c0000 80010001 80020708
Jan 21, 19:41:18  Debug    IKE  8004f003 80060080 80050002 80030002
Jan 21, 19:41:18  Debug    IKE  begin.
Jan 21, 19:41:18  Debug    IKE  seen nptype=2(prop)
Jan 21, 19:41:18  Debug    IKE  succeed.
Jan 21, 19:41:18  Debug    IKE  proposal #1 len=72
Jan 21, 19:41:18  Debug    IKE  begin.
Jan 21, 19:41:18  Debug    IKE  seen nptype=3(trns)
Jan 21, 19:41:18  Debug    IKE  seen nptype=3(trns)
Jan 21, 19:41:18  Debug    IKE  succeed.
Jan 21, 19:41:18  Debug    IKE  transform #1 len=28
Jan 21, 19:41:18  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 21, 19:41:18  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=1800
Jan 21, 19:41:18  Debug    IKE  life duration was in TLV.
Jan 21, 19:41:18  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jan 21, 19:41:18  Debug    IKE  UDP encapsulation requested
Jan 21, 19:41:18  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 21, 19:41:18  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  transform #2 len=32
Jan 21, 19:41:18  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 21, 19:41:18  Debug    IKE  type=SA Life Duration, flag=0x8000, lorv=1800
Jan 21, 19:41:18  Debug    IKE  life duration was in TLV.
Jan 21, 19:41:18  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jan 21, 19:41:18  Debug    IKE  UDP encapsulation requested
Jan 21, 19:41:18  Debug    IKE  type=Key Length, flag=0x8000, lorv=128
Jan 21, 19:41:18  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 21, 19:41:18  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  pair 1:
Jan 21, 19:41:18  Debug    IKE  0x309d10: next=0x0 tnext=0x309d20
Jan 21, 19:41:18  Debug    IKE  0x309d20: next=0x0 tnext=0x0
Jan 21, 19:41:18  Debug    IKE  proposal #1: 2 transform
Jan 21, 19:41:18  Debug    IKE  total SA len=52
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  00000001 00000001 0000002c 01030401 f455c864 00000020 01030000 80010001
Jan 21, 19:41:18  Debug    IKE  00020004 00000708 8004f003 80050002 80030002
Jan 21, 19:41:18  Debug    IKE  begin.
Jan 21, 19:41:18  Debug    IKE  seen nptype=2(prop)
Jan 21, 19:41:18  Debug    IKE  succeed.
Jan 21, 19:41:18  Debug    IKE  proposal #1 len=44
Jan 21, 19:41:18  Debug    IKE  begin.
Jan 21, 19:41:18  Debug    IKE  seen nptype=3(trns)
Jan 21, 19:41:18  Debug    IKE  succeed.
Jan 21, 19:41:18  Debug    IKE  transform #1 len=32
Jan 21, 19:41:18  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 21, 19:41:18  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jan 21, 19:41:18  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jan 21, 19:41:18  Debug    IKE  UDP encapsulation requested
Jan 21, 19:41:18  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 21, 19:41:18  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
Jan 21, 19:41:18  Debug    IKE  hmac(modp1024)
Jan 21, 19:41:18  Debug    IKE  pair 1:
Jan 21, 19:41:18  Debug    IKE  0x30a6e0: next=0x0 tnext=0x0
Jan 21, 19:41:18  Debug    IKE  proposal #1: 1 transform
Jan 21, 19:41:18  Warning  IKE  attribute has been modified.
Jan 21, 19:41:18  Debug    IKE  begin compare proposals.
Jan 21, 19:41:18  Debug    IKE  pair[1]: 0x30a6e0
Jan 21, 19:41:18  Debug    IKE  0x30a6e0: next=0x0 tnext=0x0
Jan 21, 19:41:18  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Jan 21, 19:41:18  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jan 21, 19:41:18  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jan 21, 19:41:18  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jan 21, 19:41:18  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jan 21, 19:41:18  Debug    IKE  type=Group Description, flag=0x8000, lorv=2
Jan 21, 19:41:18  Debug    IKE  peer's single bundle:
Jan 21, 19:41:18  Debug    IKE  (proto_id=ESP spisize=4 spi=f455c864 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
Jan 21, 19:41:18  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 21, 19:41:18  Debug    IKE  my single bundle:
Jan 21, 19:41:18  Debug    IKE  (proto_id=ESP spisize=4 spi=06acbfb4 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
Jan 21, 19:41:18  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jan 21, 19:41:18  Debug    IKE  (trns_id=AES encklen=128 authtype=hmac-sha)
Jan 21, 19:41:18  Info     IKE  Adjusting my encmode UDP-Tunnel->Tunnel
Jan 21, 19:41:18  Info     IKE  Adjusting peer's encmode UDP-Tunnel(61443)->Tunnel(1)
```

```
Jan 21, 19:41:18  Debug    IKE  matched
Jan 21, 19:41:18  Debug    IKE  ===
Jan 21, 19:41:18  Debug    IKE  HASH(3) generate
Jan 21, 19:41:18  Debug    IKE  HASH with:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  00c8263d b7d0f694 ff22d5ad 1331c989 af42ede7 21cc6a62 a51352c1 e946ddf9
Jan 21, 19:41:18  Debug    IKE  82147b5d 21f4d877 9f
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  HASH computed:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  36412f18 7101be23 0861c28d a0fe93d7 dc7e85c7
Jan 21, 19:41:18  Debug    IKE  add payload of len 20, next type 0
Jan 21, 19:41:18  Debug    IKE  begin encryption.
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  pad length = 8
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  00000018 36412f18 7101be23 0861c28d a0fe93d7 dc7e85c7 00000000 00000008
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  with key:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  35f1b82f 645dbc25 4e7ff334 566c2857 91bbd61c 0a1d88b8
Jan 21, 19:41:18  Debug    IKE  encrypted payload by IV:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  3043a52f 7c3d4355
Jan 21, 19:41:18  Debug    IKE  save IV for next:
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  1a6da42f 5a15be29
Jan 21, 19:41:18  Debug    IKE  encrypted.
Jan 21, 19:41:18  Debug    IKE  Adding NON-ESP marker
Jan 21, 19:41:18  Debug    IKE  64 bytes from 10.0.1.2[4500] to 84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE  sockname 10.0.1.2[4500]
Jan 21, 19:41:18  Debug    IKE  send packet from 10.0.1.2[4500]
Jan 21, 19:41:18  Debug    IKE  send packet to 84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE  1 times of 64 bytes message will be sent to 84.73.95.114[4500]
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  00000000 2f2c523a 0f56a65a 522a50c4 2af52311 08102001 c8263db7 0000003c
Jan 21, 19:41:18  Debug    IKE  514d8a3f 1c8e4dfa 3b9c04d6 4bfd30dd 5ccabf81 c9d42ffa 1a6da42f 5a15be29
Jan 21, 19:41:18  Debug    IKE  compute DH's shared.
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  85ccf543 447a0baa 8bcaef4b 50026fba 80a32d7a 595ea95f a14c40c1 3da1e801
Jan 21, 19:41:18  Debug    IKE  3425f26f 26b10b15 4a450db5 932cf9e1 311933f6 f6d103a4 e274230c ee4d8d7f
Jan 21, 19:41:18  Debug    IKE  8a4f4a80 f1bf85e0 a871dfb4 652bf169 6effccaf 61560e45 621e204d 450c74c8
Jan 21, 19:41:18  Debug    IKE  888958b9 482e41f7 6eafe7e9 3c0c39c0 46b87cf1 8af8198d eb24f046 a5e235ce
Jan 21, 19:41:18  Debug    IKE  KEYMAT compute with
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  85ccf543 447a0baa 8bcaef4b 50026fba 80a32d7a 595ea95f a14c40c1 3da1e801
Jan 21, 19:41:18  Debug    IKE  3425f26f 26b10b15 4a450db5 932cf9e1 311933f6 f6d103a4 e274230c ee4d8d7f
Jan 21, 19:41:18  Debug    IKE  8a4f4a80 f1bf85e0 a871dfb4 652bf169 6effccaf 61560e45 621e204d 450c74c8
Jan 21, 19:41:18  Debug    IKE  888958b9 482e41f7 6eafe7e9 3c0c39c0 46b87cf1 8af8198d eb24f046 a5e235ce
Jan 21, 19:41:18  Debug    IKE  0306acbf b4d0f694 ff22d5ad 1331c989 af42ede7 21cc6a62 a51352c1 e946ddf9
Jan 21, 19:41:18  Debug    IKE  82147b5d 21f4d877 9f
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  encklen=192 authklen=160
Jan 21, 19:41:18  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jan 21, 19:41:18  Debug    IKE  generating K1...K4 for KEYMAT.
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  4615842f e54c951f 4dad7cba e5f6c1fd b1f06b38 d7132232 a2badc37 aa6a795f
Jan 21, 19:41:18  Debug    IKE  4e075c95 42e2eac5 54dd8305 7b423294 985a9afd 34da5460 8394e837 e95cfd12
Jan 21, 19:41:18  Debug    IKE  778c3478 8a3b640b 5dbbc8d5 5aafa533
Jan 21, 19:41:18  Debug    IKE  KEYMAT compute with
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  85ccf543 447a0baa 8bcaef4b 50026fba 80a32d7a 595ea95f a14c40c1 3da1e801
Jan 21, 19:41:18  Debug    IKE  3425f26f 26b10b15 4a450db5 932cf9e1 311933f6 f6d103a4 e274230c ee4d8d7f
Jan 21, 19:41:18  Debug    IKE  8a4f4a80 f1bf85e0 a871dfb4 652bf169 6effccaf 61560e45 621e204d 450c74c8
Jan 21, 19:41:18  Debug    IKE  888958b9 482e41f7 6eafe7e9 3c0c39c0 46b87cf1 8af8198d eb24f046 a5e235ce
Jan 21, 19:41:18  Debug    IKE  03f455c8 64d0f694 ff22d5ad 1331c989 af42ede7 21cc6a62 a51352c1 e946ddf9
Jan 21, 19:41:18  Debug    IKE  82147b5d 21f4d877 9f
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
```

```
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  encklen=192 authklen=160
Jan 21, 19:41:18  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jan 21, 19:41:18  Debug    IKE  generating K1...K4 for KEYMAT.
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  cc12caa4 63660e32 6f8213b7 ad4d0cb6 795c84b1 774ef69f 54c68e5b d1b573af
Jan 21, 19:41:18  Debug    IKE  bd56743d 414f4587 7b16affe 34921bd3 27eec82c 118608e2 d97a7f8a 9ac6b324
Jan 21, 19:41:18  Debug    IKE  4c22f102 f9c54643 473baa05 084308ae
Jan 21, 19:41:18  Debug    IKE  KEYMAT computed.
Jan 21, 19:41:18  Debug    IKE  call pk_sendupdate
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  call pfkey_send_update_nat
Jan 21, 19:41:18  Debug    APP  Received SADB message type UPDATE, 84.73.95.114 [4500] -> 10.0.1.2 [4500]
Jan 21, 19:41:18  Debug    APP  SA change detected
Jan 21, 19:41:18  Debug    APP  Connection Netscreen is down
Jan 21, 19:41:18  Debug    IKE  pfkey update sent.
Jan 21, 19:41:18  Debug    IKE  encryption(3des)
Jan 21, 19:41:18  Debug    IKE  hmac(hmac_sha1)
Jan 21, 19:41:18  Debug    IKE  call pfkey_send_add_nat
Jan 21, 19:41:18  Debug    APP  Received SADB message type ADD, 10.0.1.2 [4500] -> 84.73.95.114 [4500]
Jan 21, 19:41:18  Debug    APP  SA change detected
Jan 21, 19:41:18  Debug    APP  Connection Netscreen is up
Jan 21, 19:41:18  Debug    IKE  pfkey add sent.
Jan 21, 19:41:18  Debug    IKE  get pfkey UPDATE message
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  02020003 14000000 74020000 c1540000 02000100 06acbfb4 04000202 00000000
Jan 21, 19:41:18  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10021194 54495f72
Jan 21, 19:41:18  Debug    IKE  00000000 00000000 03000600 ff200000 10021194 0a000102 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  04000300 00000000 00000000 00000000 08070000 00000000 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  04000400 00000000 00000000 00000000 a0050000 00000000 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 84.73.95.114[4500]->10.0.1.2[4500]
spi=111984564(0x6acbfb4)
Jan 21, 19:41:18  Info     IKE  IPsec-SA established: ESP/Tunnel 84.73.95.114[4500]->10.0.1.2[4500]
spi=111984564(0x6acbfb4)
Jan 21, 19:41:18  Debug    IKE  ===
Jan 21, 19:41:18  Debug    IKE  get pfkey ADD message
Jan 21, 19:41:18  Debug    IKE
Jan 21, 19:41:18  Debug    IKE  02030003 14000000 74020000 c1540000 02000100 f455c864 04000202 00000000
Jan 21, 19:41:18  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10021194 0a000102
Jan 21, 19:41:18  Debug    IKE  00000000 00000000 03000600 ff200000 10021194 54495f72 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  04000300 00000000 00000000 00000000 08070000 00000000 00000000 00000000
Jan 21, 19:41:18  Debug    IKE  04000400 00000000 00000000 00000000 a0050000 00000000 00000000 00000000
Jan 21, 19:41:18  Info     IKE  IPsec-SA established: ESP/Tunnel 10.0.1.2[4500]->84.73.95.114[4500]
spi=4099262564(0xf455c864)
Jan 21, 19:41:18  Debug    IKE  ===
Jan 21, 19:41:19  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netscreen
Jan 21, 19:41:22  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netscreen
Jan 21, 19:41:25  Debug    APP  Send ping packet to 192.168.215.0/24 of connection Netscreen
```