Lobotomo Software

IPSecuritas 3.x

Configuration Instructions

for

Cisco PIX 500 Series

(501, 506, 506E, 515, 515E, 520, 525, 535)

© Lobotomo Software
June 17, 2009

Legal Disclaimer

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

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

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

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

Table of contents

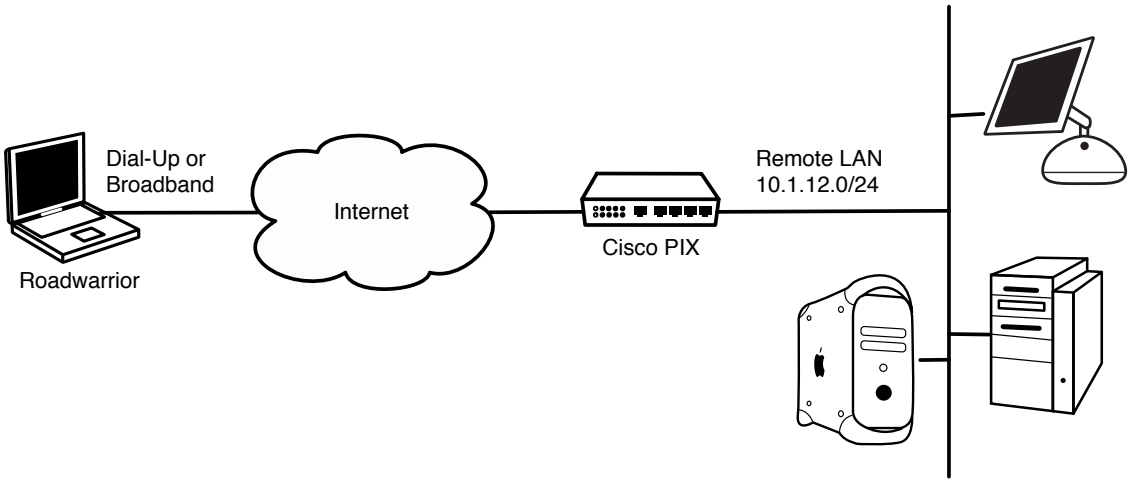
Introduction 1
Cisco PIX VPN Setup (Device Manager 3.0) 1
- Login 1
- Edit IPSec Policies 2
- Add new IPSec Rule 3
- Add new Tunnel Policy 4
- Save new IPSec Rule 5
- Add IKE Policy 6
- Edit IKE Policy 7
- Add Preshared Key 8
- Enter Pre-Shared Key 9
- Enable Firewall Bypass for IPSec Traffic 10
- Enable Management Access through IPSec 11

Cisco PIX VPN Setup (Terminal CLI) 12
IPSecuritas Setup 13
- Start Wizard 13
- Enter Name of New Connection 14
- Select Router Model 14
- Enter Router's Public IP Address 14
- Enter a Virtual IP Address 15
- Enter Remote Network 15
- Enter Preshared Key 15

Diagnosis 16
- Reachability Test 16
- Sample Cisco PIX Log Output 16
- Sample IPSecuritas Log Output 18

Introduction

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

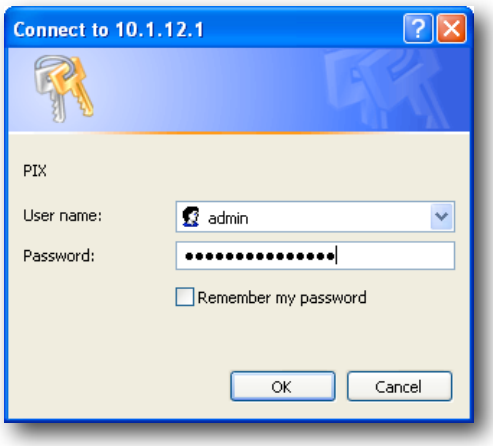


This setup guide has been written for and tested with a Cisco PIX 501 with firmware version 6.3, but it should also work with the other Series 500 models.
Please send comments and corrections to lobotomo@lobotomo.com.

Cisco PIX VPN Setup (Device Manager 3.0)

This section describes the necessary steps to setup the Cisco PIX with the PIX Device Manager to accept incoming connections.
If you prefer to setup the Cisco PIX from the command line, go to the chapter Cisco PIX VPN Setup (Terminal CLI) further below.

Login



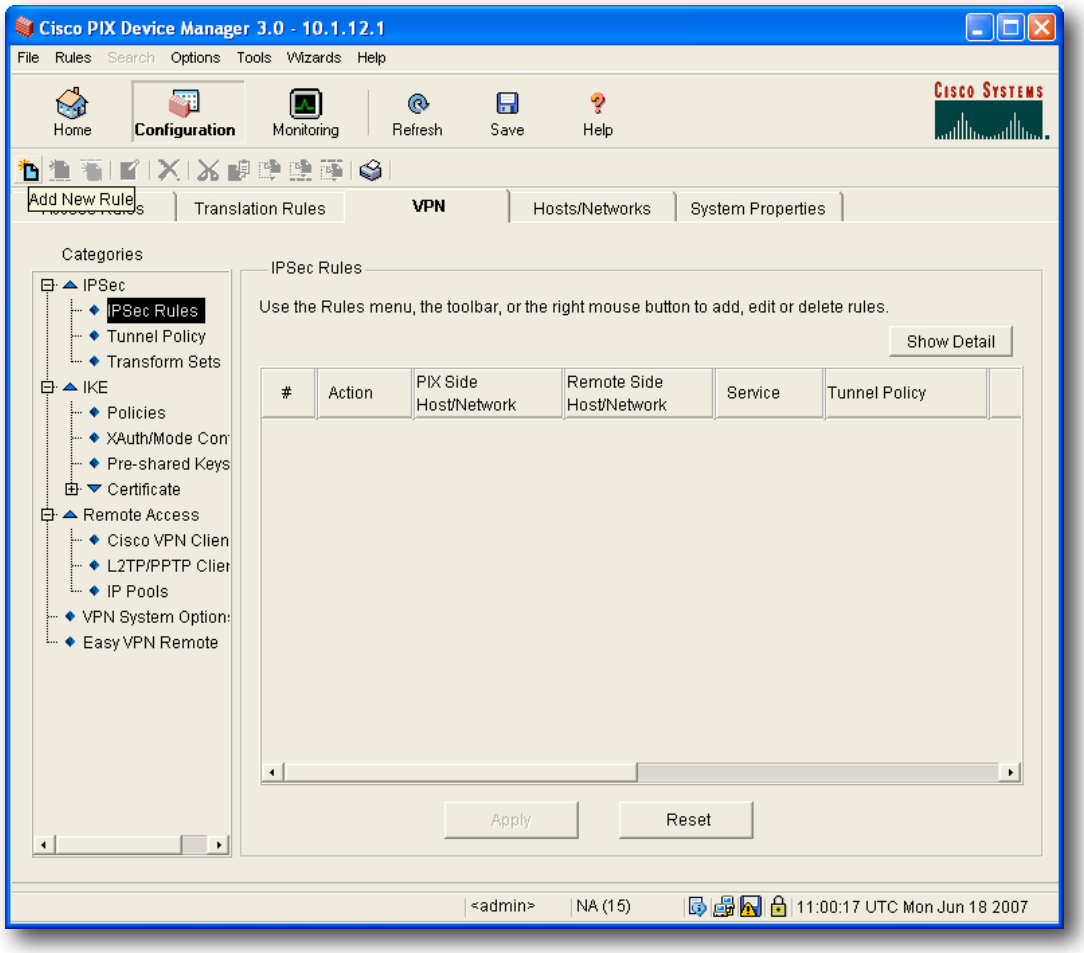
Please connect to your Cisco router with a web browser and enter an user name and password with administrative permissions.

In the main window appearing after login, press the **Configuration** button in the toolbar.

Edit IPSec Policies

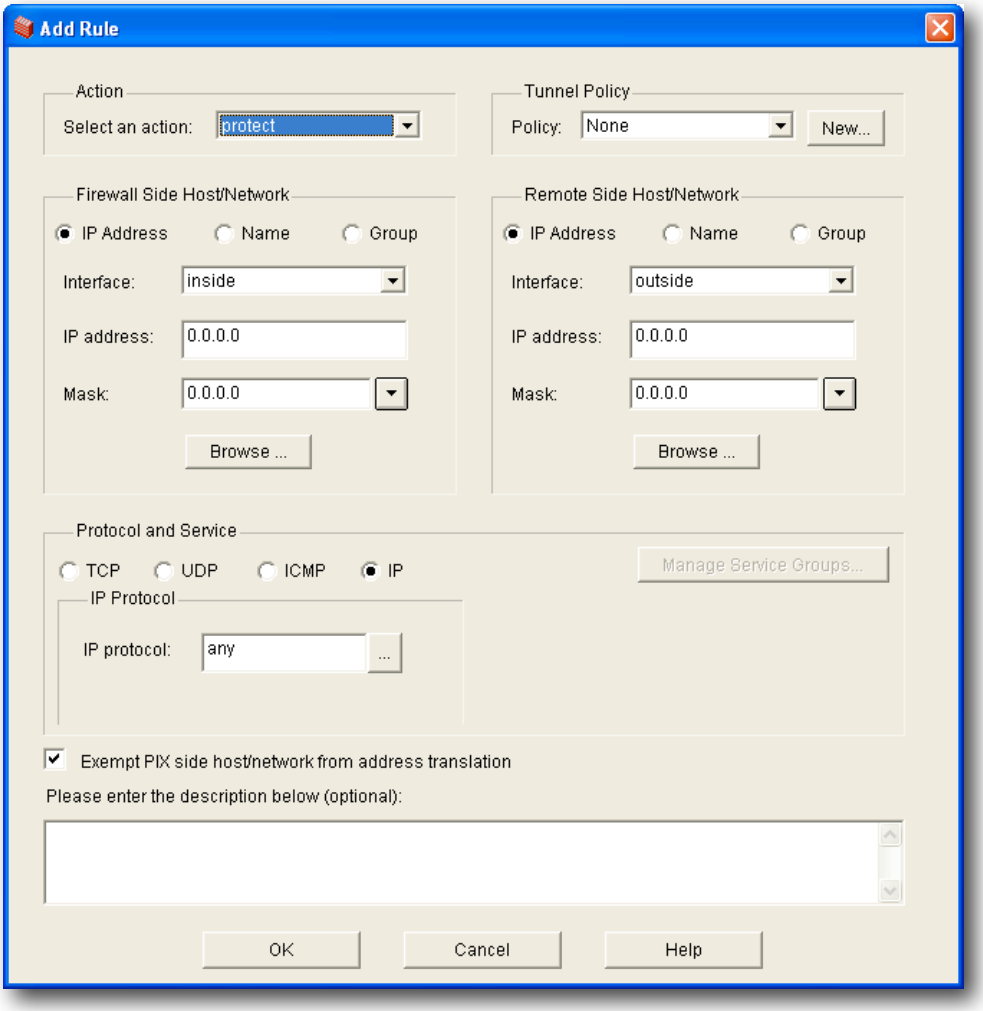
First change to the VPN configuration page by clicking on the **VPN** tab. Under **Categories** on the left side, click on **IPSec** to reveal its subitems, then click on **IPSec Rules** to display the IPSec rule list.

Click on the **Add New Rule** button on the top left side to add a new IPSec rule. A new window should appear (see next page).



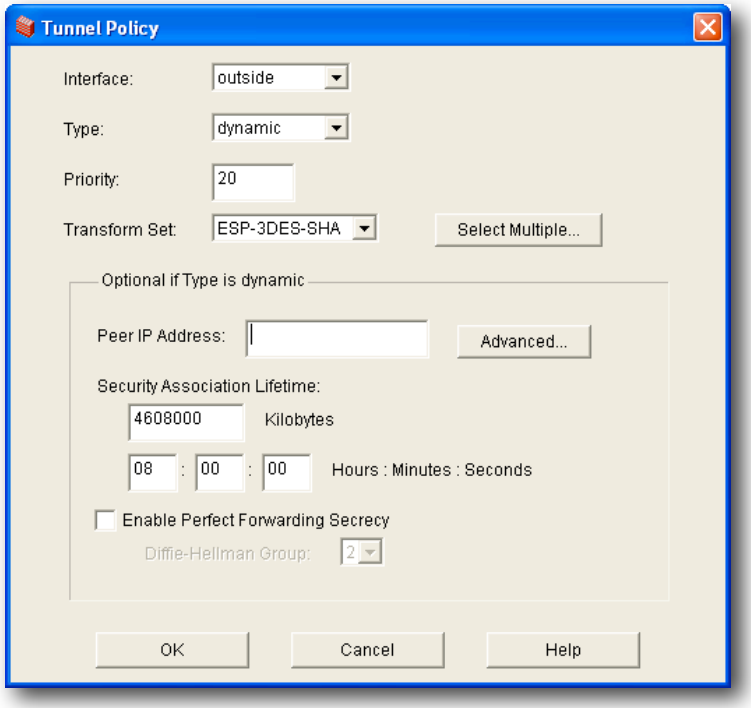
Add new IPSec Rule

You may leave all settings on their default values (see image below). Alternatively, you may limit the access to and from certain address ranges.
Next, click on the **New** button to add a new tunnel policy. A new window should appear (see next page).



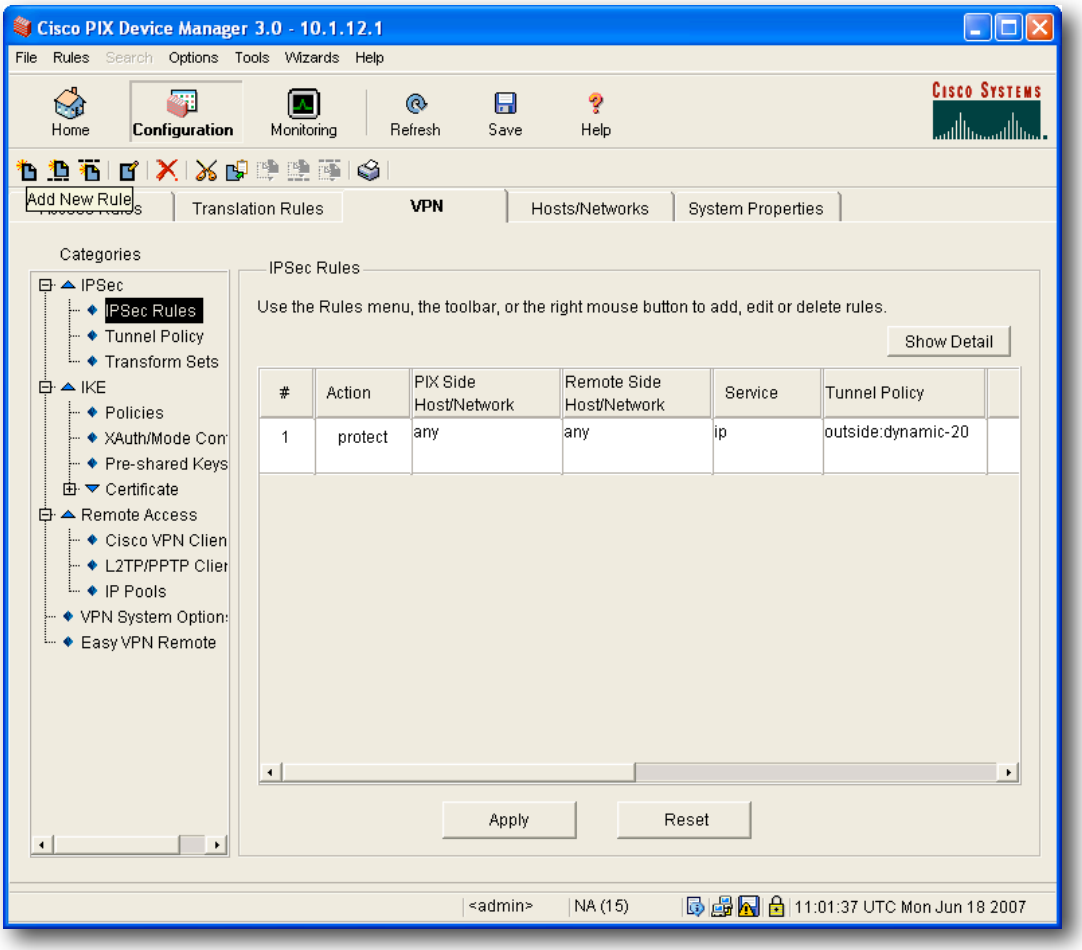
Add new Tunnel Policy

You again may leave the settings at their default values (**CAUTION:** if you decide to change some of these settings, the connection created with the IPSecuritas wizard will most probably not work before you adjust its settings accordingly). Click **OK** to save the settings.



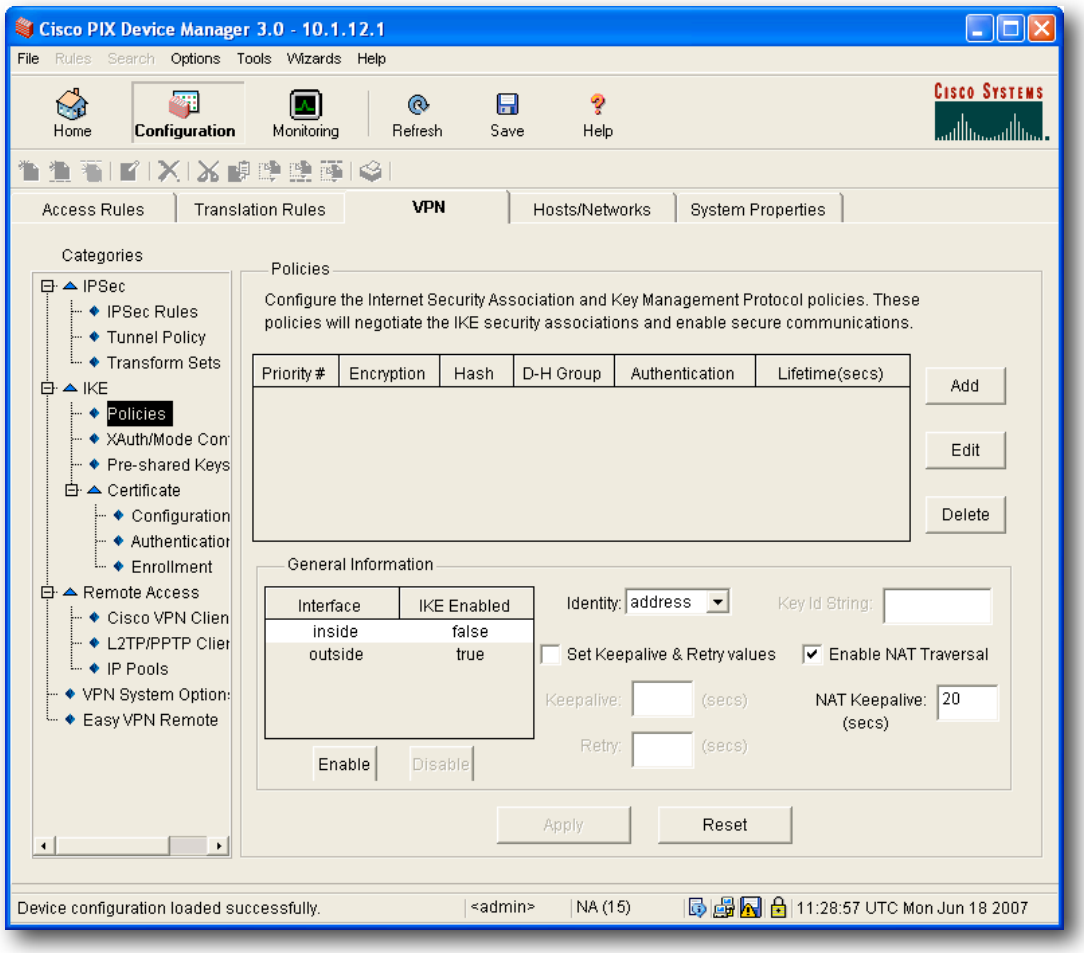
Save new IPSec Rule

The created IPSec rule should now appear in the list of rules. Click **Apply** to save your changes.



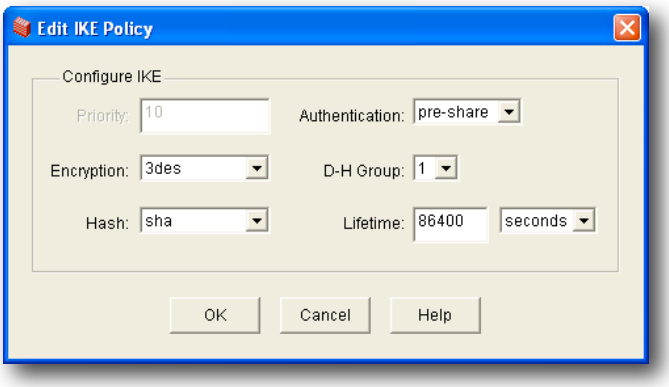
Add IKE Policy

Next, click on **IKE** under **Categories** on the left side to unveil its subitems and click on **Policies**. Click on **Add** to create a new policy. A new window should appear (see next page).



Edit IKE Policy

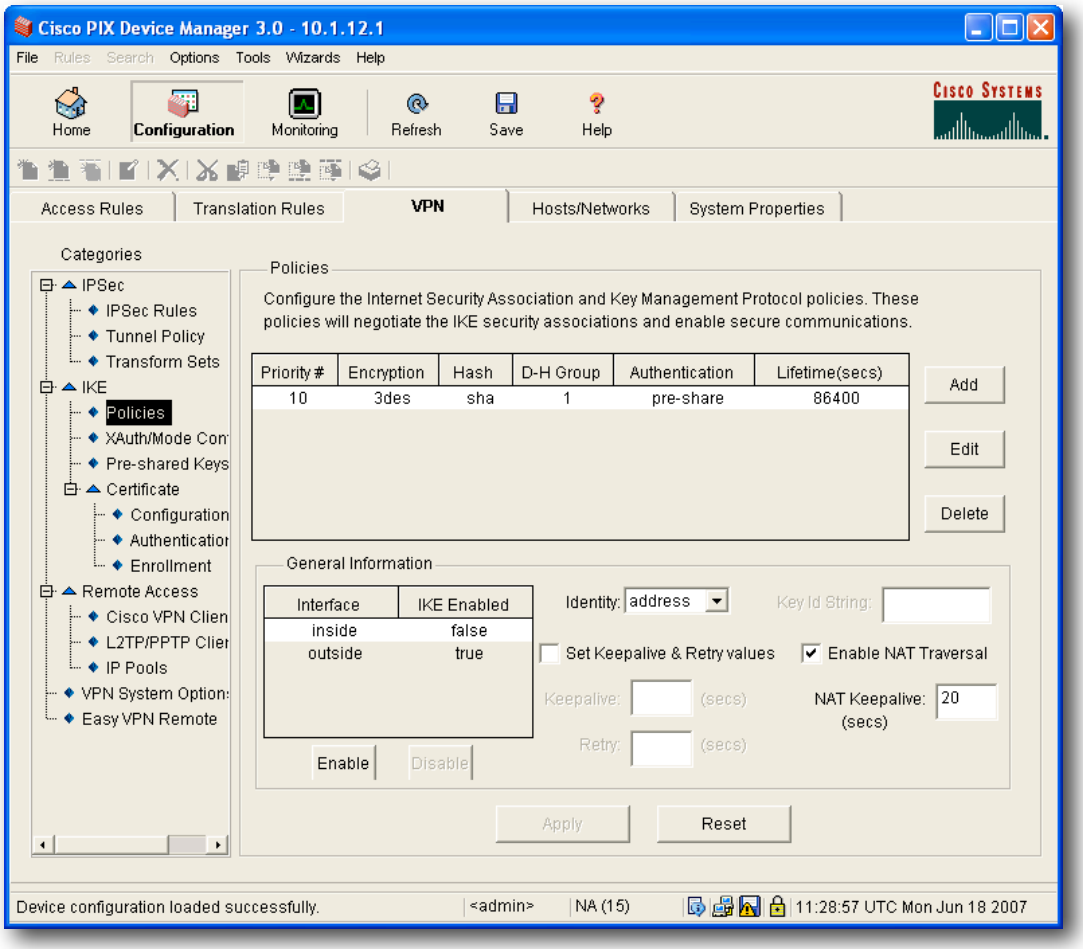
You may leave the IKE settings at their default values (**CAUTION:** if you decide to change some of these settings, the connection created with the IPSecuritas wizard will most probably not work before you adjust its settings accordingly). Press **OK** to save the policy.



The new policy should now appear in the policy list. Please make the following changes to the IKE settings:

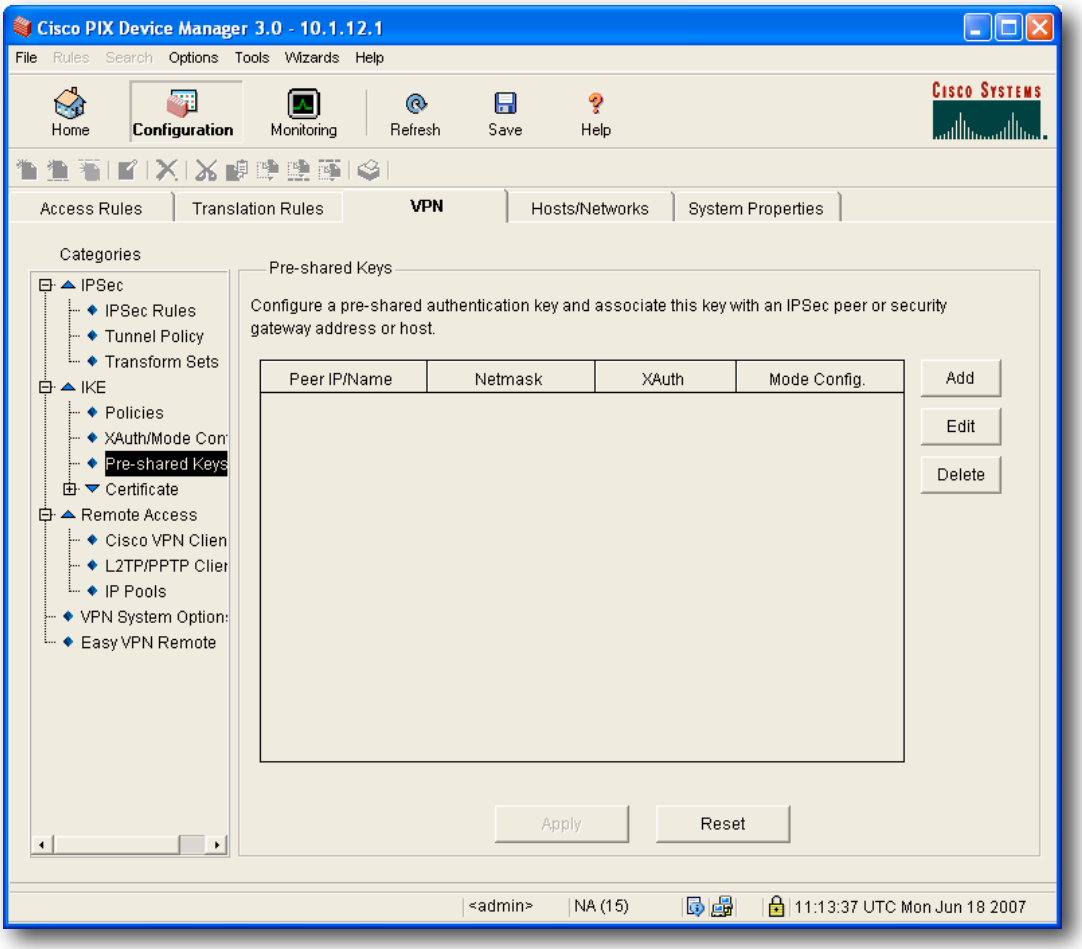
1. Enable IKE on the appropriate interface (usually **outside** or **wan**)
2. Set **Identity** to **address**
3. Enable **NAT Traversal**

Press **Apply** to save the changes you made.



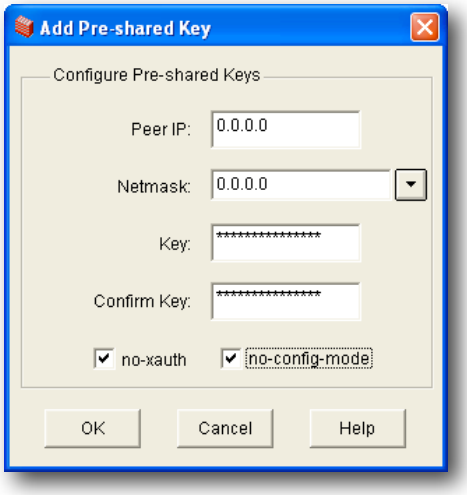
Add Preshared Key

Now add a preshared key for all incoming connections. Please note that this key is the same for all mobile IPSec users connecting with a dynamic IP address.
To do so, click on **Pre-shared Keys** in the **IKE** section in the **Categories** list and press the Add button to the right. A new window should be opened (see next page).

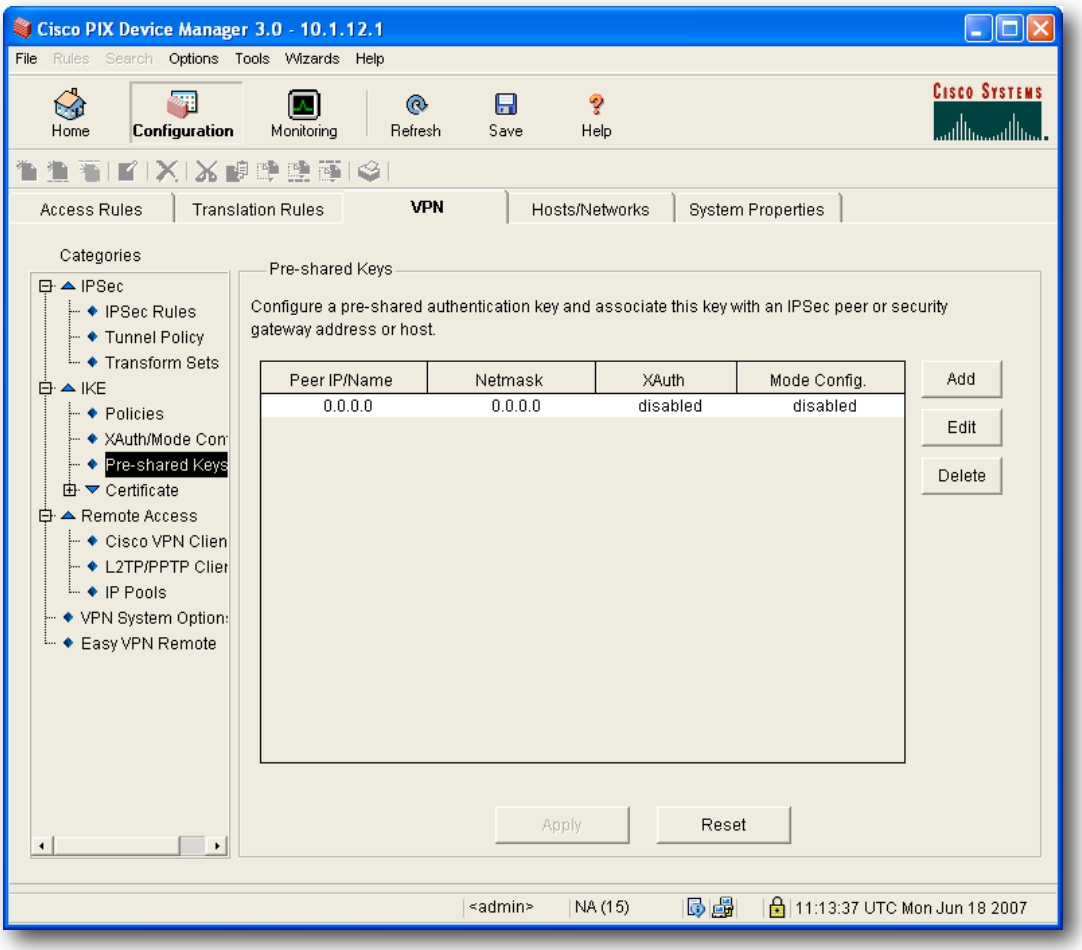


Enter Pre-Shared Key

In the new window, enter **0.0.0.0** into the **Peer IP** field and the **Netmask** field. Enter the pre-shared key (a safe password only known to you and the IPSec users) twice into the next two fields. Please remember the key you use as you will need it again when setting up the connection in IPSecuritas. Enable both options **no-xauth** and **no-config-mode**. Press **OK** to save you changes.



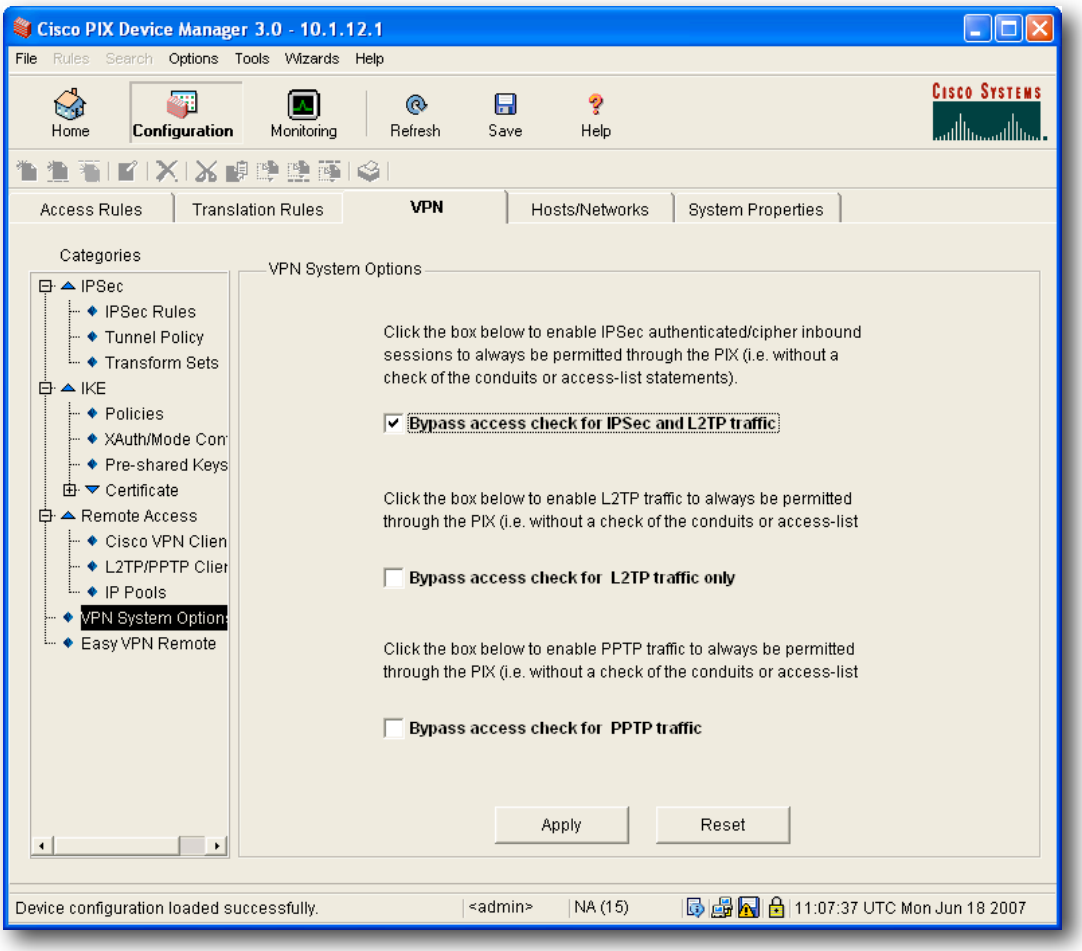
The new pre-shared key will now appear in the list of pre-shared keys. Press **Apply** to save your changes.



Enable Firewall Bypass for IPSec Traffic

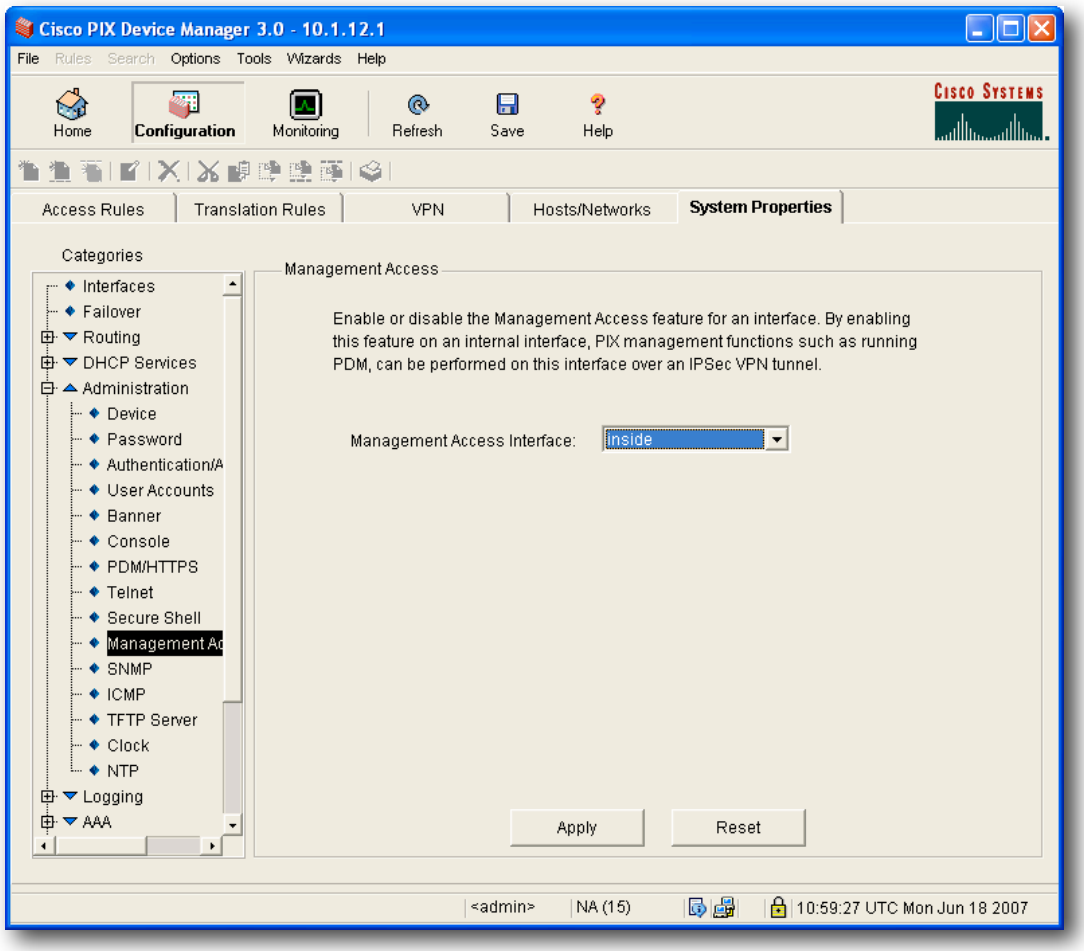
Click on **VPN System Options** to display the VPN options, then enable the option **Bypass access check for IPSec and L2TP traffic**. Press **Apply** to save you changes.

NOTE: This will bypass any firewall check on traffic from or to an IPSec user and may not be want you want, depending on your sense of security. Please bear in mind to add appropriate firewall rules if you decide to not enable this option!



Enable Management Access through IPSec

This step is optional and only required if you want to access the Cisco router management functionality like Telnet or PDM access or like to ping the router's inside address through an IPSec tunnel remotely. Click on the **System Properties** tab to display the general settings, then click on **Administration** in the Categories list to unveil its subitems and select **Management Access**. Allow Management Access in the **inside** (or **lan**) interface.
Press **Apply** to save your changes.



Cisco PIX VPN Setup (Terminal CLI)

This section describes the necessary steps to setup the Cisco PIX with the CLI to accept incoming connections.
The following steps assume that the inbound interface is bound to the network 10.1.12.0/24. Replace all occurrences of this address with your own network address in the following steps.

Login to the Cisco PIX via Telnet or SSH:

```
[Lobotomo-MacBook:~] nadig% telnet 10.1.12.1
Trying 10.1.12.1...
Connected to 10.1.12.1.
Escape character is '^]'.


User Access Verification

Password:
```

Please enter your telnet password at the prompt. Next, enable the administrative commands on the PIX:

```
pixfirewall> enable
Password: ***************
```

Now enable IPSec with the following two commands:

```
sysopt connection permit-ipsec
isakmp enable outside
```

Setup the IPSec policy (Phase 2):

```
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 20 match address outside_cryptomap_dyn_20
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
```

Setup the IKE Policy (Phase 1):

```
isakmp enable outside
isakmp key PASSWORD address 0.0.0.0 netmask 0.0.0.0 no-xauth no-config-mode
isakmp identity address
isakmp nat-traversal 20
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
```

Please replace **PASSWORD** with a safe preshared key (a secret password) and remember it for the setup of IPSecuritas.
Now setup the access list entry for VPN traffic destined for your local network:

```
access-list inside_nat0_outbound permit ip 10.1.12.0 255.255.255.0 any
access-list outside_cryptomap_dyn_20 permit ip 10.1.12.0 255.255.255.0 any
```

Omit the first line if you are not using NAT in your setup.

Enable management through IPSec tunnels. This step is optional but will allow you to ping the inside interface and run the Device Manager GUI through a VPN tunnel from remote places:

```
management-access inside
icmp permit any inside
```

Write these changes back to Flash memory:

```
write mem
```

You may now proceed with the sezup of a connection in IPSecuritas.

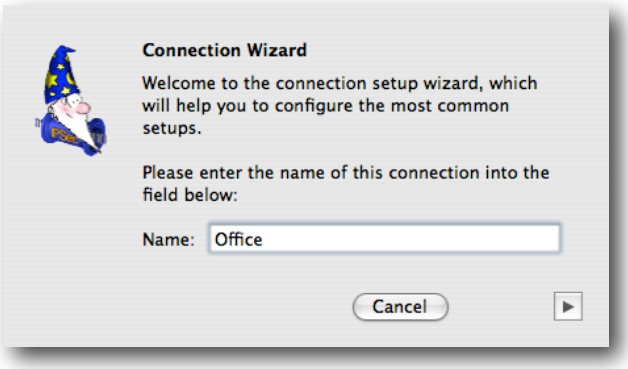
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the Cisco PIX 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:

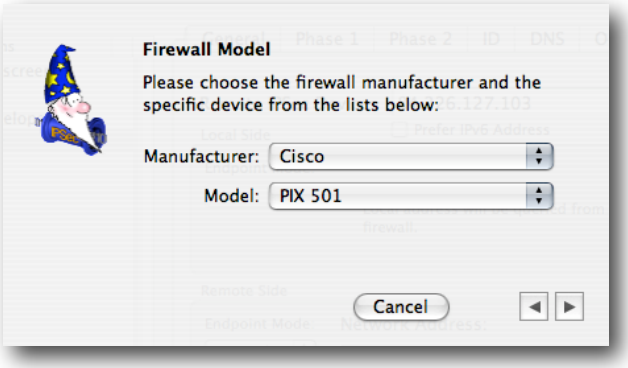
Enter Name of New Connection



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

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

Select Router Model



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

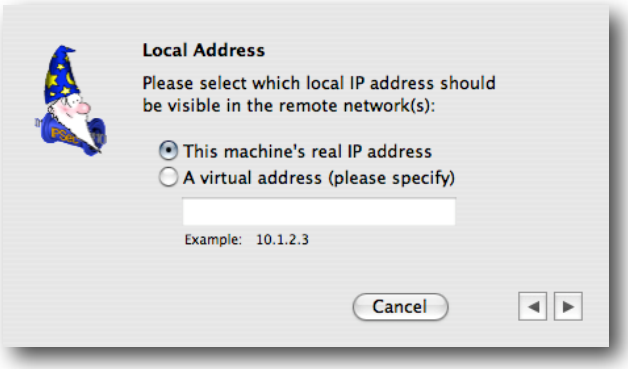
Click on the right arrow to continue with the next step.

Enter Router's Public IP Address

Enter the public IP address or hostname of your Cisco PIX 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.

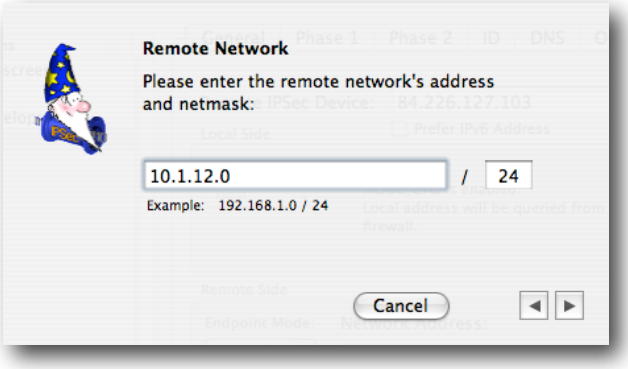
Enter a Virtual IP Address



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**). Please use different addresses for different users.

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

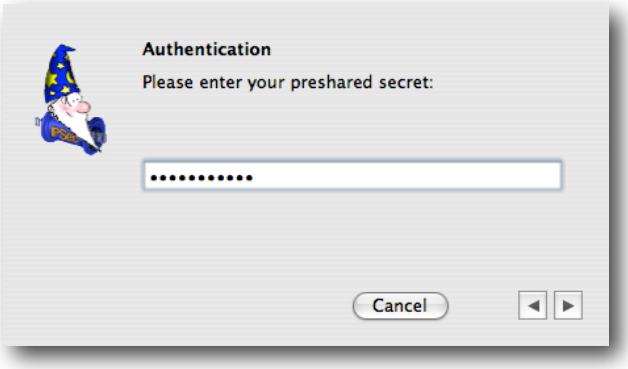
Enter Remote Network



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 Cisco PIX.

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

Enter Preshared Key



Enter the same **Preshared Key** that you used for the Cisco PIX.

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 Cisco PIX **local IP address**. If the tunnel works correctly, a similar output is displayed (NOTE: the Cisco PIX will only respond to ping packets if management access is enabled on the inside (or lan) interface):

```
[MacBook:~] root# ping 10.1.12.1
PING 10.1.12.1 (10.1.12.1): 56 data bytes
64 bytes from 10.1.12.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 10.1.12.1: icmp_seq=1 ttl=64 time=19.290 ms
64 bytes from 10.1.12.1: icmp_seq=2 ttl=64 time=12.823 ms
```

Sample Cisco PIX Log Output

Login to the Cisco PIX via Telnet or SSH:

```
[Lobotomo-MacBook:~] nadig% telnet 10.1.12.1
Trying 10.1.12.1...
Connected to 10.1.12.1.
Escape character is '^]'.


User Access Verification

Password:
```

Please enter your telnet password at the prompt. Next, enable the administrative commands on the PIX:

```
pixfirewall> enable
Password: ***************
```

Enter the following command to enable log output for IKE and IPSec:

```
debug crypto ipsec
debug crypto isakmp
```

Now start IPSec in IPSecuritas. You should see a similar output after a successful connection attempt:

```
crypto_isakmp_process_block:src:192.168.215.1, dest:192.168.215.235 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:      encryption 3DES-CBC
ISAKMP:      auth pre-share
ISAKMP:      hash SHA
ISAKMP:      default group 1
```

```
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (0:0): sending NAT-T vendor ID - rev 2 & 3
ISAKMP (0:0): Detected port floating
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:192.168.215.1, dest:192.168.215.235 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0:0): Detected NAT-D payload
ISAKMP (0:0): NAT does not match MINE hash
hash received: 2b 9b 8c ff bc f2 c2 c9 f1 d4 1c d0 f3 ad e0 3 31 51 5c cd
my nat hash  : 77 9e d4 a0 d0 ae 53 d6 0 68 77 94 62 14 ac a1 bf c2 14 7b
ISAKMP (0:0): Detected NAT-D payload
ISAKMP (0:0): NAT does not match HIS hash
hash received: 2b 9b 8c ff bc f2 c2 c9 f1 d4 1c d0 f3 ad e0 3 31 51 5c cd
his nat hash : 4b cc 45 fd 6c 3e 42 6 27 9c 5e 74 1 c6 57 9d 91 e 43 8c
ISAKMP (0:0): constructed HIS NAT-D
ISAKMP (0:0): constructed MINE NAT-D
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:192.168.215.1, dest:192.168.215.235 spt:4500 dpt:4500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP: Locking UDP_ENC struct 0xabc2f4 from crypto_ikmp_udp_enc_ike_init, count 1
ISAKMP (0): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 0
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:192.168.215.1/4500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:192.168.215.1/4500 Ref cnt incremented to:1 Total VPN Peers:1
crypto_isakmp_process_block:src:192.168.215.1, dest:192.168.215.235 spt:4500 dpt:4500
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 3178223285
ISAKMP (0): processing notify INITIAL_CONTACT
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:192.168.215.1, dest:192.168.215.235 spt:4500 dpt:4500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3285749123

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:      encaps is 61443
ISAKMP:      authenticator is HMAC-SHA
```

```
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.168.215.235, src= 192.168.215.1,
    dest_proxy= 10.1.12.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.5.2/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400

ISAKMP (0): processing NONCE payload. message ID = 3285749123

ISAKMP (0): processing ID payload. message ID = 3285749123
ISAKMP (0): ID_IPV4_ADDR src 192.168.5.2 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 3285749123
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.12.0/255.255.255.0 prot 0 port 0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xad4da6b5(2907547317) for SA
        from   192.168.215.1 to 192.168.215.235 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:192.168.215.1, dest:192.168.215.235 spt:4500 dpt:4500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from   192.168.215.1 to 192.168.215.235 (proxy     192.168.5.2 to       10.1.12.0)
        has spi 2907547317 and conn_id 1 and flags 400
        lifetime of 86400 seconds
        outbound SA from 192.168.215.235 to   192.168.215.1 (proxy       10.1.12.0 to     192.168.5.2)
        has spi 117097157 and conn_id 2 and flags 400
        lifetime of 86400 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 192.168.215.235, src= 192.168.215.1,
    dest_proxy= 10.1.12.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.5.2/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 86400s and 0kb,
    spi= 0xad4da6b5(2907547317), conn_id= 1, keysize= 0, flags= 0x400
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 192.168.215.235, dest= 192.168.215.1,
    src_proxy= 10.1.12.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 192.168.5.2/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 86400s and 0kb,
    spi= 0x6fac2c5(117097157), conn_id= 2, keysize= 0, flags= 0x400

VPN Peer: IPSEC: Peer ip:192.168.215.1/4500 Ref cnt incremented to:2 Total VPN Peers:1
ISAKMP: Locking UDP_ENC struct 0xabc2f4 from crypto_ikmp_udp_enc_handle_kei_mess, count 2
VPN Peer: IPSEC: Peer ip:192.168.215.1/4500 Ref cnt incremented to:3 Total VPN Peers:1
ISAKMP: Locking UDP_ENC struct 0xabc2f4 from crypto_ikmp_udp_enc_handle_kei_mess, count 3
return status is IKMP_NO_ERROR
```

Sample IPSecuritas Log Output

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

```
IPSecuritas 3.0.1p1 build 1704, Fri Jun 22 21:23:57 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

Jun 24, 18:30:21  Debug    APP  State change from IDLE to AUTHENTICATING after event START
Jun 24, 18:30:21  Info     APP  IKE daemon started
Jun 24, 18:30:21  Info     APP  IPSec started
Jun 24, 18:30:21  Debug    APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
Jun 24, 18:30:21  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Jun 24, 18:30:21  Debug    APP  Received SADB message type X_SPDUPDATE - not interesting
Jun 24, 18:30:21  Info     IKE  Foreground mode.
Jun 24, 18:30:21  Info     IKE  @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
Jun 24, 18:30:21  Info     IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
Jun 24, 18:30:21  Info     IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/
racoon.conf"
Jun 24, 18:30:21  Info     IKE  Resize address pool from 0 to 255
Jun 24, 18:30:21  Debug    IKE  lifetime = 86400
Jun 24, 18:30:21  Debug    IKE  lifebyte = 0
Jun 24, 18:30:21  Debug    IKE  encklen=0
```

```
Jun 24, 18:30:21  Debug    IKE  p:1 t:1
Jun 24, 18:30:21  Debug    IKE  3DES-CBC(5)
Jun 24, 18:30:21  Debug    IKE  SHA(2)
Jun 24, 18:30:21  Debug    IKE  768-bit MODP group(1)
Jun 24, 18:30:21  Debug    IKE  pre-shared key(1)
Jun 24, 18:30:21  Debug    IKE  compression algorithm can not be checked because sadb message doesn't support it.
Jun 24, 18:30:21  Debug    IKE  parse successed.
Jun 24, 18:30:21  Debug    IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
management.
Jun 24, 18:30:21  Info     IKE  192.168.215.1[4500] used as isakmp port (fd=7)
Jun 24, 18:30:21  Info     IKE  192.168.215.1[500] used as isakmp port (fd=8)
Jun 24, 18:30:21  Debug    IKE  get pfkey X_SPDDUMP message
Jun 24, 18:30:21  Debug    IKE  02120000 0f000100 01000000 a2100000 03000500 ff180000 10020000 0a010c00
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a80502 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  07001200 02000100 a8030000 00000000 28003200 02036202 10020000 c0a8d7eb
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 10020000 c0a8d701 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  get pfkey X_SPDDUMP message
Jun 24, 18:30:21  Debug    IKE  02120000 0f000100 00000000 a2100000 03000500 ff200000 10020000 c0a80502
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 03000600 ff180000 10020000 0a010c00 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  07001200 02000200 a7030000 00000000 28003200 02036102 10020000 c0a8d701
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 10020000 c0a8d7eb 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  sub:0xbffff330: 192.168.5.2/32[0] 10.1.12.0/24[0] proto=any dir=out
Jun 24, 18:30:21  Debug    IKE  db :0x308b78: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in
Jun 24, 18:30:21  Debug    IKE  get pfkey ACQUIRE message
Jun 24, 18:30:21  Debug    IKE  02060003 26000000 0d020000 00000000 03000500 ff200000 10020000 c0a8d701
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7eb 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  02001200 02000200 a7030000 00000000 1c000d00 20000000 00030000 00000000
Jun 24, 18:30:21  Debug    IKE  00010008 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  00040000 00000000 0001c001 00000000 01000000 01000000 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 00000000 00000000 80510100 00000000 80700000 00000000
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 000c0000 00000000 00010001 00000000 01000000 01000000
Jun 24, 18:30:21  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Jun 24, 18:30:21  Debug    IKE  80700000 00000000 00000000 00000000
Jun 24, 18:30:21  Debug    IKE  suitable outbound SP found: 192.168.5.2/32[0] 10.1.12.0/24[0] proto=any dir=out.
Jun 24, 18:30:21  Debug    IKE  sub:0xbffff30c: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in
Jun 24, 18:30:21  Debug    IKE  db :0x308b78: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in
Jun 24, 18:30:21  Debug    IKE  suitable inbound SP found: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in.
Jun 24, 18:30:21  Debug    IKE  new acquire 192.168.5.2/32[0] 10.1.12.0/24[0] proto=any dir=out
Jun 24, 18:30:21  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=610:609)
Jun 24, 18:30:21  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jun 24, 18:30:21  Debug    IKE  in post_acquire
Jun 24, 18:30:21  Debug    IKE  configuration found for 192.168.215.235.
Jun 24, 18:30:21  Info     IKE  IPsec-SA request for 192.168.215.235 queued due to no phase1 found.
Jun 24, 18:30:21  Debug    IKE  ===
Jun 24, 18:30:21  Info     IKE  initiate new phase 1 negotiation: 192.168.215.1[500]<=>192.168.215.235[500]
Jun 24, 18:30:21  Info     IKE  begin Identity Protection mode.
Jun 24, 18:30:21  Debug    IKE  new cookie:
Jun 24, 18:30:21  Debug    IKE  895769d61b7501f9
Jun 24, 18:30:21  Debug    IKE  add payload of len 52, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 20, next type 13
Jun 24, 18:30:21  Debug    IKE  add payload of len 16, next type 0
Jun 24, 18:30:21  Debug    IKE  348 bytes from 192.168.215.1[500] to 192.168.215.235[500]
Jun 24, 18:30:21  Debug    IKE  sockname 192.168.215.1[500]
Jun 24, 18:30:21  Debug    IKE  send packet from 192.168.215.1[500]
Jun 24, 18:30:21  Debug    IKE  send packet to 192.168.215.235[500]
Jun 24, 18:30:21  Debug    IKE  1 times of 348 bytes message will be sent to 192.168.215.235[500]
Jun 24, 18:30:21  Debug    IKE  895769d6 1b7501f9 00000000 00000000 01100200 00000000 0000015c 0d000038
Jun 24, 18:30:21  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 800b0001 000c0004
Jun 24, 18:30:21  Debug    IKE  00015180 80010005 80030001 80020002 80040001 0d000014 4a131c81 07035845
Jun 24, 18:30:21  Debug    IKE  5c5728f2 0e95452f 0d000014 8f8d8382 6d246b6f c7a8a6a4 28c11de8 0d000014
Jun 24, 18:30:21  Debug    IKE  439b59f8 ba676c4c 7737ae22 eab8f582 0d000014 4d1e0e13 6deafa34 c4f3ea9f
Jun 24, 18:30:21  Debug    IKE  02ec7285 0d000014 80d0bb3d ef54565e e84645d4 c85ce3ee 0d000014 9909b64e
```

```
Jun 24, 18:30:21  Debug    IKE  ed937c65 73de52ac e952fa6b 0d000014 7d9419a6 5310ca6f 2c179d92 15529d56
Jun 24, 18:30:21  Debug    IKE  0d000014 cd604643 35df21f8 7cfdb2fc 68b6a448 0d000014 90cb8091 3ebb696e
Jun 24, 18:30:21  Debug    IKE  086381b5 ec427b1f 0d000014 16f6ca16 e4a4066d 83821a0f 0aeaa862 0d000014
Jun 24, 18:30:21  Debug    IKE  4485152d 18b6bbcd 0be8a846 9579ddcc 0d000018 4048b7d5 6ebce885 25e7de7f
Jun 24, 18:30:21  Debug    IKE  00d6c2d3 80000000 00000014 afcad713 68a1f1c9 6b8696fc 77570100
Jun 24, 18:30:21  Debug    IKE  resend phase1 packet 895769d61b7501f9:0000000000000000
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  124 bytes message received from 192.168.215.235[500] to 192.168.215.1[500]
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 01100200 00000000 0000007c 0d000038
Jun 24, 18:30:22  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 80010005 80020002
Jun 24, 18:30:22  Debug    IKE  80040001 80030001 800b0001 000c0004 00015180 0d000014 7d9419a6 5310ca6f
Jun 24, 18:30:22  Debug    IKE  2c179d92 15529d56 00000014 90cb8091 3ebb696e 086381b5 ec427b1f
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=1(sa)
Jun 24, 18:30:22  Debug    IKE  seen nptype=13(vid)
Jun 24, 18:30:22  Debug    IKE  seen nptype=13(vid)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Info     IKE  received Vendor ID: draft-ietf-ipsec-nat-t-ike-03
Jun 24, 18:30:22  Info     IKE  received Vendor ID: draft-ietf-ipsec-nat-t-ike-02
Jun 24, 18:30:22  Info     IKE
Jun 24, 18:30:22  Info     IKE  Selected NAT-T version: draft-ietf-ipsec-nat-t-ike-03
Jun 24, 18:30:22  Debug    IKE  total SA len=52
Jun 24, 18:30:22  Debug    IKE  00000001 00000001 0000002c 01010001 00000024 01010000 80010005 80020002
Jun 24, 18:30:22  Debug    IKE  80040001 80030001 800b0001 000c0004 00015180
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=2(prop)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  proposal #1 len=44
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=3(trns)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  transform #1 len=36
Jun 24, 18:30:22  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
Jun 24, 18:30:22  Debug    IKE  hmac(modp768)
Jun 24, 18:30:22  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Jun 24, 18:30:22  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Jun 24, 18:30:22  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Jun 24, 18:30:22  Debug    IKE  pair 1:
Jun 24, 18:30:22  Debug    IKE  0x309110: next=0x0 tnext=0x0
Jun 24, 18:30:22  Debug    IKE  proposal #1: 1 transform
Jun 24, 18:30:22  Debug    IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
Jun 24, 18:30:22  Debug    IKE  trns#=1, trns-id=IKE
Jun 24, 18:30:22  Debug    IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
Jun 24, 18:30:22  Debug    IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
Jun 24, 18:30:22  Debug    IKE  type=Group Description, flag=0x8000, lorv=768-bit MODP group
Jun 24, 18:30:22  Debug    IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
Jun 24, 18:30:22  Debug    IKE  type=Life Type, flag=0x8000, lorv=seconds
Jun 24, 18:30:22  Debug    IKE  type=Life Duration, flag=0x0000, lorv=4
Jun 24, 18:30:22  Debug    IKE  Compared: DB:Peer
Jun 24, 18:30:22  Debug    IKE  (lifetime = 86400:86400)
Jun 24, 18:30:22  Debug    IKE  (lifebyte = 0:0)
Jun 24, 18:30:22  Debug    IKE  enctype = 3DES-CBC:3DES-CBC
Jun 24, 18:30:22  Debug    IKE  (encklen = 0:0)
Jun 24, 18:30:22  Debug    IKE  hashtype = SHA:SHA
Jun 24, 18:30:22  Debug    IKE  authmethod = pre-shared key:pre-shared key
Jun 24, 18:30:22  Debug    IKE  dh_group = 768-bit MODP group:768-bit MODP group
Jun 24, 18:30:22  Debug    IKE  an acceptable proposal found.
Jun 24, 18:30:22  Debug    IKE  hmac(modp768)
Jun 24, 18:30:22  Debug    IKE  agreed on pre-shared key auth.
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  compute DH's private.
Jun 24, 18:30:22  Debug    IKE  6ec068af 311f9a21 9a4cecb1 0df8ed3a f7e575e5 ad050164 aae96fb2 bd2d3a3c
Jun 24, 18:30:22  Debug    IKE  bfbf3577 772430c4 48bb0eff 73341e9a 9a6f5eda d3395071 a5c8ca77 90c5b960
Jun 24, 18:30:22  Debug    IKE  9155fb14 c173262a dfdcbad9 63808d1c 0189e739 445971d8 c07f4984 16a58fef
Jun 24, 18:30:22  Debug    IKE  compute DH's public.
Jun 24, 18:30:22  Debug    IKE  138672cf 20222f08 e4b17796 8d711915 6847741a 7bf04334 f83f36d6 fa7fa222
Jun 24, 18:30:22  Debug    IKE  9dcf6b16 98667d43 d73b8ef8 b9141ae7 710c2dc9 666092a1 72d6bbe5 86d3681d
Jun 24, 18:30:22  Debug    IKE  db5b9841 693981cb 5bb96fcf fca14ecd 7a6457e6 c22c8ff5 e2d68956 df2190eb
Jun 24, 18:30:22  Info     IKE  Hashing 192.168.215.235[500] with algo #2 (NAT-T forced)
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
```

```
Jun 24, 18:30:22  Info     IKE  Hashing 192.168.215.1[500] with algo #2 (NAT-T forced)
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Info     IKE  Adding remote and local NAT-D payloads.
Jun 24, 18:30:22  Debug    IKE  add payload of len 96, next type 10
Jun 24, 18:30:22  Debug    IKE  add payload of len 16, next type 130
Jun 24, 18:30:22  Debug    IKE  add payload of len 20, next type 130
Jun 24, 18:30:22  Debug    IKE  add payload of len 20, next type 0
Jun 24, 18:30:22  Debug    IKE  196 bytes from 192.168.215.1[500] to 192.168.215.235[500]
Jun 24, 18:30:22  Debug    IKE  sockname 192.168.215.1[500]
Jun 24, 18:30:22  Debug    IKE  send packet from 192.168.215.1[500]
Jun 24, 18:30:22  Debug    IKE  send packet to 192.168.215.235[500]
Jun 24, 18:30:22  Debug    IKE  1 times of 196 bytes message will be sent to 192.168.215.235[500]
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 04100200 00000000 000000c4 0a000064
Jun 24, 18:30:22  Debug    IKE  138672cf 20222f08 e4b17796 8d711915 6847741a 7bf04334 f83f36d6 fa7fa222
Jun 24, 18:30:22  Debug    IKE  9dcf6b16 98667d43 d73b8ef8 b9141ae7 710c2dc9 666092a1 72d6bbe5 86d3681d
Jun 24, 18:30:22  Debug    IKE  db5b9841 693981cb 5bb96fcf fca14ecd 7a6457e6 c22c8ff5 e2d68956 df2190eb
Jun 24, 18:30:22  Debug    IKE  82000014 e3aad014 aa16c3ae b232c92f 82e529c9 82000018 2b9b8cff bcf2c2c9
Jun 24, 18:30:22  Debug    IKE  f1d41cd0 f3ade003 31515ccd 00000018 2b9b8cff bcf2c2c9 f1d41cd0 f3ade003
Jun 24, 18:30:22  Debug    IKE  31515ccd
Jun 24, 18:30:22  Debug    IKE  resend phase1 packet 895769d61b7501f9:e459750f8040831f
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  272 bytes message received from 192.168.215.235[500] to 192.168.215.1[500]
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 04100200 00000000 00000110 0a000064
Jun 24, 18:30:22  Debug    IKE  b2bdfa4f a763238f 84e35bee e0e68c50 01647231 e24acc00 09faddc0 2cfb4514
Jun 24, 18:30:22  Debug    IKE  689a055c ffdbe0a8 0dad53de 80438599 ea963c18 14459478 b4f88da5 3c4a80ba
Jun 24, 18:30:22  Debug    IKE  0f0a9dfe 99c2083b dd523892 f89841d7 fd38e335 1ed3e330 a8a86eac 8141424b
Jun 24, 18:30:22  Debug    IKE  0d000018 1a09c88f d2eb9761 2be692ea 615f949b 5e741db2 0d00000c 09002689
Jun 24, 18:30:22  Debug    IKE  dfd6b712 0d000014 afcad713 68a1f1c9 6b8696fc 77570100 0d000014 12f5f28c
Jun 24, 18:30:22  Debug    IKE  457168a9 702d9fe2 74cc0100 82000014 119ed212 8041831f 5cda46fa 1854e2a7
Jun 24, 18:30:22  Debug    IKE  82000018 4bcc45fd 6c3e4206 279c5e74 01c6579d 910e438c 00000018 779ed4a0
Jun 24, 18:30:22  Debug    IKE  d0ae53d6 00687794 6214aca1 bfc2147b
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=4(ke)
Jun 24, 18:30:22  Debug    IKE  seen nptype=10(nonce)
Jun 24, 18:30:22  Debug    IKE  seen nptype=13(vid)
Jun 24, 18:30:22  Debug    IKE  seen nptype=13(vid)
Jun 24, 18:30:22  Debug    IKE  seen nptype=13(vid)
Jun 24, 18:30:22  Debug    IKE  seen nptype=13(vid)
Jun 24, 18:30:22  Debug    IKE  seen nptype=130(nat-d)
Jun 24, 18:30:22  Debug    IKE  seen nptype=130(nat-d)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Info     IKE  received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt
Jun 24, 18:30:22  Info     IKE  received Vendor ID: DPD
Jun 24, 18:30:22  Info     IKE  received Vendor ID: CISCO-UNITY
Jun 24, 18:30:22  Debug    IKE  received unknown Vendor ID
Jun 24, 18:30:22  Debug    IKE  119ed212 8041831f 5cda46fa 1854e2a7
Jun 24, 18:30:22  Info     IKE  NAT-D payload #0 doesn't match
Jun 24, 18:30:22  Info     IKE  NAT-D payload #1 doesn't match
Jun 24, 18:30:22  Info     IKE  NAT detected: ME PEER
Jun 24, 18:30:22  Info     IKE  KA list add: 192.168.215.1[4500]->192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  compute DH's shared.
Jun 24, 18:30:22  Debug    IKE  c39ea4e7 58cd0c2c b70aeb4f 065b1649 276f71d4 cddad354 e38632e2 7f1b8441
Jun 24, 18:30:22  Debug    IKE  9f030e59 e0620864 6410eeca 6c33effd fd47d575 8d32cd12 9af458ae d55dbbb7
Jun 24, 18:30:22  Debug    IKE  06ec1ca3 0221da19 e831773c 5340789e d97e8fc3 bbbdd6f0 119af10a ecda8db2
Jun 24, 18:30:22  Debug    IKE  the psk found.
Jun 24, 18:30:22  Debug    IKE  psk: 2007-06-24 18:30:22: DEBUG2:
Jun 24, 18:30:22  Debug    IKE  63656c6c 732e696e 2e667261 6d6573
Jun 24, 18:30:22  Debug    IKE  nonce 1: 2007-06-24 18:30:22: DEBUG:
Jun 24, 18:30:22  Debug    IKE  e3aad014 aa16c3ae b232c92f 82e529c9
Jun 24, 18:30:22  Debug    IKE  nonce 2: 2007-06-24 18:30:22: DEBUG:
Jun 24, 18:30:22  Debug    IKE  1a09c88f d2eb9761 2be692ea 615f949b 5e741db2
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  SKEYID computed:
Jun 24, 18:30:22  Debug    IKE  73117d0e b9bcc385 1e4d8fb3 f08d7771 c02ad5e6
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  SKEYID_d computed:
Jun 24, 18:30:22  Debug    IKE  7fae617c 6de5face 6c7ee717 ac7aebce eba7b4e5
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  SKEYID_a computed:
Jun 24, 18:30:22  Debug    IKE  04dcf5e5 17b8dd0c 3b86e3e3 670aa640 6d52e2a4
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  SKEYID_e computed:
Jun 24, 18:30:22  Debug    IKE  06422930 f325a2e7 0ba20bf6 37563890 68ef71b3
```

```
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Debug    IKE  len(SKEYID_e) < len(Ka) (20 < 24), generating long key (Ka = K1 | K2 | ...)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  compute intermediate encryption key K1
Jun 24, 18:30:22  Debug    IKE  00
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  compute intermediate encryption key K2
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718
Jun 24, 18:30:22  Debug    IKE  dc516947 e1c354cb edebea39 e87bbb40 c61f28e6
Jun 24, 18:30:22  Debug    IKE  final encryption key computed:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  IV computed:
Jun 24, 18:30:22  Debug    IKE  2bb9c289 ba8edf7a
Jun 24, 18:30:22  Debug    IKE  use ID type of IPv4_address
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  138672cf 20222f08 e4b17796 8d711915 6847741a 7bf04334 f83f36d6 fa7fa222
Jun 24, 18:30:22  Debug    IKE  9dcf6b16 98667d43 d73b8ef8 b9141ae7 710c2dc9 666092a1 72d6bbe5 86d3681d
Jun 24, 18:30:22  Debug    IKE  db5b9841 693981cb 5bb96fcf fca14ecd 7a6457e6 c22c8ff5 e2d68956 df2190eb
Jun 24, 18:30:22  Debug    IKE  b2bdfa4f a763238f 84e35bee e0e68c50 01647231 e24acc00 09faddc0 2cfb4514
Jun 24, 18:30:22  Debug    IKE  689a055c ffdbe0a8 0dad53de 80438599 ea963c18 14459478 b4f88da5 3c4a80ba
Jun 24, 18:30:22  Debug    IKE  0f0a9dfe 99c2083b dd523892 f89841d7 fd38e335 1ed3e330 a8a86eac 8141424b
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 00000001 00000001 0000002c 01010001
Jun 24, 18:30:22  Debug    IKE  00000024 01010000 800b0001 000c0004 00015180 80010005 80030001 80020002
Jun 24, 18:30:22  Debug    IKE  80040001 011101f4 c0a8d701
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH (init) computed:
Jun 24, 18:30:22  Debug    IKE  66cfb9fd d1fac876 97b47c08 f7e90762 bb987ab4
Jun 24, 18:30:22  Debug    IKE  add payload of len 8, next type 8
Jun 24, 18:30:22  Debug    IKE  add payload of len 20, next type 0
Jun 24, 18:30:22  Debug    IKE  begin encryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  pad length = 4
Jun 24, 18:30:22  Debug    IKE  0800000c 011101f4 c0a8d701 00000018 66cfb9fd d1fac876 97b47c08 f7e90762
Jun 24, 18:30:22  Debug    IKE  bb987ab4 ffca9803
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  encrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  2bb9c289 ba8edf7a
Jun 24, 18:30:22  Debug    IKE  save IV for next:
Jun 24, 18:30:22  Debug    IKE  76577f6d 2410a158
Jun 24, 18:30:22  Debug    IKE  encrypted.
Jun 24, 18:30:22  Debug    IKE  Adding NON-ESP marker
Jun 24, 18:30:22  Debug    IKE  72 bytes from 192.168.215.1[4500] to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  sockname 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet from 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  1 times of 72 bytes message will be sent to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  00000000 895769d6 1b7501f9 e459750f 8040831f 05100201 00000000 00000044
Jun 24, 18:30:22  Debug    IKE  72b27365 f489b595 895dce4b 7e111ca1 5c3e1dbd 38f6d330 b700384d af9a4f3d
Jun 24, 18:30:22  Debug    IKE  76577f6d 2410a158
Jun 24, 18:30:22  Debug    IKE  resend phase1 packet 895769d61b7501f9:e459750f8040831f
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  68 bytes message received from 192.168.215.235[4500] to 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 05100201 00000000 00000044 e8761860
Jun 24, 18:30:22  Debug    IKE  d4d60ae1 0e9dd4a1 2fb9bc6c 52c0c7e2 28489847 4c6bbf30 9064824e b79b64c1
Jun 24, 18:30:22  Debug    IKE  cc00e593
Jun 24, 18:30:22  Debug    IKE  begin decryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  IV was saved for next processing:
Jun 24, 18:30:22  Debug    IKE  b79b64c1 cc00e593
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  decrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  76577f6d 2410a158
Jun 24, 18:30:22  Debug    IKE  decrypted payload, but not trimed.
Jun 24, 18:30:22  Debug    IKE  0800000c 01110000 c0a8d7eb 00000018 2ab5ddfc e0a5d55c bc82546d 3cf4bc02
Jun 24, 18:30:22  Debug    IKE  730997ef 00000000
Jun 24, 18:30:22  Debug    IKE  padding len=1
```

```
Jun 24, 18:30:22  Debug    IKE  skip to trim padding.
Jun 24, 18:30:22  Debug    IKE  decrypted.
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 05100201 00000000 00000044 0800000c
Jun 24, 18:30:22  Debug    IKE  01110000 c0a8d7eb 00000018 2ab5ddfc e0a5d55c bc82546d 3cf4bc02 730997ef
Jun 24, 18:30:22  Debug    IKE  00000000
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=5(id)
Jun 24, 18:30:22  Debug    IKE  seen nptype=8(hash)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  HASH received:
Jun 24, 18:30:22  Debug    IKE  2ab5ddfc e0a5d55c bc82546d 3cf4bc02 730997ef
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  b2bdfa4f a763238f 84e35bee e0e68c50 01647231 e24acc00 09faddc0 2cfb4514
Jun 24, 18:30:22  Debug    IKE  689a055c ffdbe0a8 0dad53de 80438599 ea963c18 14459478 b4f88da5 3c4a80ba
Jun 24, 18:30:22  Debug    IKE  0f0a9dfe 99c2083b dd523892 f89841d7 fd38e335 1ed3e330 a8a86eac 8141424b
Jun 24, 18:30:22  Debug    IKE  138672cf 20222f08 e4b17796 8d711915 6847741a 7bf04334 f83f36d6 fa7fa222
Jun 24, 18:30:22  Debug    IKE  9dcf6b16 98667d43 d73b8ef8 b9141ae7 710c2dc9 666092a1 72d6bbe5 86d3681d
Jun 24, 18:30:22  Debug    IKE  db5b9841 693981cb 5bb96fcf fca14ecd 7a6457e6 c22c8ff5 e2d68956 df2190eb
Jun 24, 18:30:22  Debug    IKE  e459750f 8040831f 895769d6 1b7501f9 00000001 00000001 0000002c 01010001
Jun 24, 18:30:22  Debug    IKE  00000024 01010000 800b0001 000c0004 00015180 80010005 80030001 80020002
Jun 24, 18:30:22  Debug    IKE  80040001 01110000 c0a8d7eb
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH (init) computed:
Jun 24, 18:30:22  Debug    IKE  2ab5ddfc e0a5d55c bc82546d 3cf4bc02 730997ef
Jun 24, 18:30:22  Debug    IKE  HASH for PSK validated.
Jun 24, 18:30:22  Debug    IKE  peer's ID:2007-06-24 18:30:22: DEBUG:
Jun 24, 18:30:22  Debug    IKE  01110000 c0a8d7eb
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  compute IV for phase2
Jun 24, 18:30:22  Debug    IKE  phase1 last IV:
Jun 24, 18:30:22  Debug    IKE  b79b64c1 cc00e593 bd6fd6b5
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  phase2 IV computed:
Jun 24, 18:30:22  Debug    IKE  8b9ab957 8319c497
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  bd6fd6b5 0000001c 00000001 01106002 895769d6 1b7501f9 e459750f 8040831f
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH computed:
Jun 24, 18:30:22  Debug    IKE  9073a5cb 2f3ad15e 9f924886 45309e9c 405be6f1
Jun 24, 18:30:22  Debug    IKE  begin encryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  pad length = 4
Jun 24, 18:30:22  Debug    IKE  0b000018 9073a5cb 2f3ad15e 9f924886 45309e9c 405be6f1 0000001c 00000001
Jun 24, 18:30:22  Debug    IKE  01106002 895769d6 1b7501f9 e459750f 8040831f ec998a03
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  encrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  8b9ab957 8319c497
Jun 24, 18:30:22  Debug    IKE  save IV for next:
Jun 24, 18:30:22  Debug    IKE  9f599b25 dc5d0669
Jun 24, 18:30:22  Debug    IKE  encrypted.
Jun 24, 18:30:22  Debug    IKE  Adding NON-ESP marker
Jun 24, 18:30:22  Debug    IKE  88 bytes from 192.168.215.1[4500] to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  sockname 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet from 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  1 times of 88 bytes message will be sent to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  00000000 895769d6 1b7501f9 e459750f 8040831f 08100501 bd6fd6b5 00000054
Jun 24, 18:30:22  Debug    IKE  065df84b 3b82fa8b 4321d25a 9771e9fd 4c379752 3dbbd045 6119d340 7b7a6233
Jun 24, 18:30:22  Debug    IKE  b3742703 f88c86f3 f75fc77b 7314a9b1 9f599b25 dc5d0669
Jun 24, 18:30:22  Debug    IKE  sendto Information notify.
Jun 24, 18:30:22  Debug    IKE  IV freed
Jun 24, 18:30:22  Info     IKE  ISAKMP-SA established 192.168.215.1[4500]-192.168.215.235[4500] spi:
895769d61b7501f9:e459750f8040831f
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  84 bytes message received from 192.168.215.235[4500] to 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 08100501 76eeba03 00000054 1421b136
Jun 24, 18:30:22  Debug    IKE  754a0437 37791dc1 c1f9471b 04aaab06 51374d92 0b90cda5 425c96fb edcdd37c
Jun 24, 18:30:22  Debug    IKE  5307a3ea 502b69b3 30b723e3 c7935cef 3deeed7f
Jun 24, 18:30:22  Debug    IKE  receive Information.
Jun 24, 18:30:22  Debug    IKE  compute IV for phase2
```

```
Jun 24, 18:30:22  Debug    IKE  phase1 last IV:
Jun 24, 18:30:22  Debug    IKE  b79b64c1 cc00e593 76eeba03
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  phase2 IV computed:
Jun 24, 18:30:22  Debug    IKE  14b2d52a e9748aef
Jun 24, 18:30:22  Debug    IKE  begin decryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  IV was saved for next processing:
Jun 24, 18:30:22  Debug    IKE  c7935cef 3deeed7f
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  decrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  14b2d52a e9748aef
Jun 24, 18:30:22  Debug    IKE  decrypted payload, but not trimed.
Jun 24, 18:30:22  Debug    IKE  0b000018 b52701a9 4e19a2c8 01e69ed9 99841f52 b4a6d6bd 0000001c 00000001
Jun 24, 18:30:22  Debug    IKE  01106002 895769d6 1b7501f9 e459750f 8040831f 00000000
Jun 24, 18:30:22  Debug    IKE  padding len=1
Jun 24, 18:30:22  Debug    IKE  skip to trim padding.
Jun 24, 18:30:22  Debug    IKE  decrypted.
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 08100501 76eeba03 00000054 0b000018
Jun 24, 18:30:22  Debug    IKE  b52701a9 4e19a2c8 01e69ed9 99841f52 b4a6d6bd 0000001c 00000001 01106002
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 00000000
Jun 24, 18:30:22  Debug    IKE  IV freed
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  76eeba03 0000001c 00000001 01106002 895769d6 1b7501f9 e459750f 8040831f
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH computed:
Jun 24, 18:30:22  Debug    IKE  b52701a9 4e19a2c8 01e69ed9 99841f52 b4a6d6bd
Jun 24, 18:30:22  Debug    IKE  hash validated.
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=8(hash)
Jun 24, 18:30:22  Debug    IKE  seen nptype=11(notify)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  call pfkey_send_dump
Jun 24, 18:30:22  Info     APP  Initiated connection Cisco PIX 501
Jun 24, 18:30:22  Debug    IKE  get pfkey ACQUIRE message
Jun 24, 18:30:22  Debug    IKE  02060003 24000000 0e020000 00000000 03000500 ff200000 10020000 c0a8d701
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7eb 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  1c000d00 20000000 00030000 00000000 00010008 00000000 01000000 01000000
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Jun 24, 18:30:22  Debug    IKE  80700000 00000000 00000000 00000000 00040000 00000000 0001c001 00000000
Jun 24, 18:30:22  Debug    IKE  01000000 01000000 00000000 00000000 00000000 00000000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  80510100 00000000 80700000 00000000 00000000 00000000 000c0000 00000000
Jun 24, 18:30:22  Debug    IKE  00010001 00000000 01000000 01000000 00000000 00000000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 80510100 00000000 80700000 00000000 00000000 00000000
Jun 24, 18:30:22  Error    IKE  inappropriate sadb acquire message passed.
Jun 24, 18:30:22  Debug    IKE  get pfkey ACQUIRE message
Jun 24, 18:30:22  Debug    IKE  02060003 14000000 9d000000 f40b0000 03000500 ff200000 10020000 c0a8d701
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7eb 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  0a000d00 20000000 000c0000 00000000 00010001 00000000 01000000 01000000
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 00000000 00000000 00000000 00000000 80510100 00000000
Jun 24, 18:30:22  Debug    IKE  80700000 00000000 00000000 00000000 02001200 02000200 a7030000 00000000
Jun 24, 18:30:22  Debug    IKE  suitable outbound SP found: 192.168.5.2/32[0] 10.1.12.0/24[0] proto=any dir=out.
Jun 24, 18:30:22  Debug    IKE  sub:0xbffff30c: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in
Jun 24, 18:30:22  Debug    IKE  db :0x308b78: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in
Jun 24, 18:30:22  Debug    IKE  suitable inbound SP found: 10.1.12.0/24[0] 192.168.5.2/32[0] proto=any dir=in.
Jun 24, 18:30:22  Debug    IKE  new acquire 192.168.5.2/32[0] 10.1.12.0/24[0] proto=any dir=out
Jun 24, 18:30:22  Debug    IKE  (proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=610:609)
Jun 24, 18:30:22  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jun 24, 18:30:22  Debug    IKE  in post_acquire
Jun 24, 18:30:22  Debug    IKE  configuration found for 192.168.215.235.
Jun 24, 18:30:22  Debug    IKE  begin QUICK mode.
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  begin QUICK mode.
Jun 24, 18:30:22  Info     IKE  initiate new phase 2 negotiation: 192.168.215.1[4500]<=>192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  compute IV for phase2
Jun 24, 18:30:22  Debug    IKE  phase1 last IV:
Jun 24, 18:30:22  Debug    IKE  b79b64c1 cc00e593 c3d88d83
Jun 24, 18:30:22  Debug    IKE  hash(sha1)
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  phase2 IV computed:
Jun 24, 18:30:22  Debug    IKE  05e2f150 a8a3bdfc
```

```
Jun 24, 18:30:22  Debug    IKE  call pfkey_send_getspi
Jun 24, 18:30:22  Debug    IKE  pfkey GETSPI sent: ESP/Tunnel 192.168.215.235[0]->192.168.215.1[0]
Jun 24, 18:30:22  Debug    IKE  pfkey getspi sent.
Jun 24, 18:30:22  Debug    IKE  get pfkey GETSPI message
Jun 24, 18:30:22  Debug    IKE  02010003 0a000000 9d000000 a2100000 02000100 06fac2c5 30303030 20303130
Jun 24, 18:30:22  Debug    IKE  03000500 ff200000 10020000 c0a8d7eb 00000000 00000000 03000600 ff200000
Jun 24, 18:30:22  Debug    IKE  10020000 c0a8d701 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  pfkey GETSPI succeeded: ESP/Tunnel 192.168.215.235[0]->192.168.215.1[0]
spi=117097157(0x6fac2c5)
Jun 24, 18:30:22  Info     IKE  NAT detected -> UDP encapsulation (ENC_MODE 1->61443).
Jun 24, 18:30:22  Debug    IKE  use local ID type IPv4_address
Jun 24, 18:30:22  Debug    IKE  use remote ID type IPv4_subnet
Jun 24, 18:30:22  Debug    IKE  IDci:
Jun 24, 18:30:22  Debug    IKE  01000000 c0a80502
Jun 24, 18:30:22  Debug    IKE  IDcr:
Jun 24, 18:30:22  Debug    IKE  04000000 0a010c00 ffffff00
Jun 24, 18:30:22  Debug    IKE  add payload of len 48, next type 10
Jun 24, 18:30:22  Debug    IKE  add payload of len 16, next type 5
Jun 24, 18:30:22  Debug    IKE  add payload of len 8, next type 5
Jun 24, 18:30:22  Debug    IKE  add payload of len 12, next type 0
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  c3d88d83 0a000034 00000001 00000001 00000028 01030401 06fac2c5 0000001c
Jun 24, 18:30:22  Debug    IKE  01030000 80010001 00020004 00015180 8004f003 80050002 05000014 c363e586
Jun 24, 18:30:22  Debug    IKE  5ee352d7 e44a07e3 9fe14a43 0500000c 01000000 c0a80502 00000010 04000000
Jun 24, 18:30:22  Debug    IKE  0a010c00 ffffff00
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH computed:
Jun 24, 18:30:22  Debug    IKE  c37dad00 ff1dead8 7f20bd41 b82615b5 7377b2db
Jun 24, 18:30:22  Debug    IKE  add payload of len 20, next type 1
Jun 24, 18:30:22  Debug    IKE  begin encryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  pad length = 4
Jun 24, 18:30:22  Debug    IKE  01000018 c37dad00 ff1dead8 7f20bd41 b82615b5 7377b2db 0a000034 00000001
Jun 24, 18:30:22  Debug    IKE  00000001 00000028 01030401 06fac2c5 0000001c 01030000 80010001 00020004
Jun 24, 18:30:22  Debug    IKE  00015180 8004f003 80050002 05000014 c363e586 5ee352d7 e44a07e3 9fe14a43
Jun 24, 18:30:22  Debug    IKE  0500000c 01000000 c0a80502 00000010 04000000 0a010c00 ffffff00 bec39c03
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  encrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  05e2f150 a8a3bdfc
Jun 24, 18:30:22  Debug    IKE  save IV for next:
Jun 24, 18:30:22  Debug    IKE  b3e239ab be3fe574
Jun 24, 18:30:22  Debug    IKE  encrypted.
Jun 24, 18:30:22  Debug    IKE  Adding NON-ESP marker
Jun 24, 18:30:22  Debug    IKE  160 bytes from 192.168.215.1[4500] to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  sockname 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet from 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  1 times of 160 bytes message will be sent to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  00000000 895769d6 1b7501f9 e459750f 8040831f 08102001 c3d88d83 0000009c
Jun 24, 18:30:22  Debug    IKE  7e316eba bbfc4deb 458efb9b 126bfb63 e4d786b2 23b8a9fe 3a3915a9 303b2da5
Jun 24, 18:30:22  Debug    IKE  1e476745 620484bc 6ec12c56 e6e77717 e98c8526 f876053e 55756070 fad014c9
Jun 24, 18:30:22  Debug    IKE  1d388355 aa838d9f ebe02b56 e3cc9ec1 2c1b9833 70cd9874 da8e0354 e50c3772
Jun 24, 18:30:22  Debug    IKE  a02e55cf 8b8503a5 a9358ab5 7157aafd 9392d964 b636a0cf b3e239ab be3fe574
Jun 24, 18:30:22  Debug    IKE  resend phase2 packet 895769d61b7501f9:e459750f8040831f:0000c3d8
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  204 bytes message received from 192.168.215.235[4500] to 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 08102001 c3d88d83 000000cc 3475ff0d
Jun 24, 18:30:22  Debug    IKE  bf8da900 b374b012 9700476f 47b4635d d0306d62 7f2ce5d4 b59ccfdd 23f2fed4
Jun 24, 18:30:22  Debug    IKE  59112f7e 08befbee 1c2e1abc a755a942 ad076abc 65349f1f 52a0bf7c e94e1127
Jun 24, 18:30:22  Debug    IKE  9b8c8c75 b2f5b6a6 a21c3606 0e00fb96 8d8149d8 5b07427f dbe5bc60 e77b89f8
Jun 24, 18:30:22  Debug    IKE  c4699c88 566d4304 bc2e415c 42eb1716 30de7b71 e320015c 7d990fce c0fb3cb4
Jun 24, 18:30:22  Debug    IKE  e3acfa30 4de708b1 ed814077 3c369828 e386be7e e3ef94e6 1bc4f741 7df9a568
Jun 24, 18:30:22  Debug    IKE  6160afb7 c86eeda5 50715e64
Jun 24, 18:30:22  Debug    IKE  begin decryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  IV was saved for next processing:
Jun 24, 18:30:22  Debug    IKE  c86eeda5 50715e64
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  decrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  b3e239ab be3fe574
```

```
Jun 24, 18:30:22  Debug    IKE  decrypted payload, but not trimed.
Jun 24, 18:30:22  Debug    IKE  01000018 f3bd0241 9673e747 e712c98f a3d479d4 dd7add0c 0a000034 00000001
Jun 24, 18:30:22  Debug    IKE  00000001 00000028 01030401 ad4da6b5 0000001c 01030000 8004f003 80010001
Jun 24, 18:30:22  Debug    IKE  00020004 00015180 80050002 05000018 4ac01c9d 78ab3f11 0be5f709 bc33cd51
Jun 24, 18:30:22  Debug    IKE  73d78a0f 0500000c 01000000 c0a80502 0b000010 04000000 0a010c00 ffffff00
Jun 24, 18:30:22  Debug    IKE  00000028 00000001 03046000 ad4da6b5 80010001 00020004 00007080 80010002
Jun 24, 18:30:22  Debug    IKE  00020004 00465000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  padding len=1
Jun 24, 18:30:22  Debug    IKE  skip to trim padding.
Jun 24, 18:30:22  Debug    IKE  decrypted.
Jun 24, 18:30:22  Debug    IKE  895769d6 1b7501f9 e459750f 8040831f 08102001 c3d88d83 000000cc 01000018
Jun 24, 18:30:22  Debug    IKE  f3bd0241 9673e747 e712c98f a3d479d4 dd7add0c 0a000034 00000001 00000001
Jun 24, 18:30:22  Debug    IKE  00000028 01030401 ad4da6b5 0000001c 01030000 8004f003 80010001 00020004
Jun 24, 18:30:22  Debug    IKE  00015180 80050002 05000018 4ac01c9d 78ab3f11 0be5f709 bc33cd51 73d78a0f
Jun 24, 18:30:22  Debug    IKE  0500000c 01000000 c0a80502 0b000010 04000000 0a010c00 ffffff00 00000028
Jun 24, 18:30:22  Debug    IKE  00000001 03046000 ad4da6b5 80010001 00020004 00007080 80010002 00020004
Jun 24, 18:30:22  Debug    IKE  00465000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=8(hash)
Jun 24, 18:30:22  Debug    IKE  seen nptype=1(sa)
Jun 24, 18:30:22  Debug    IKE  seen nptype=10(nonce)
Jun 24, 18:30:22  Debug    IKE  seen nptype=5(id)
Jun 24, 18:30:22  Debug    IKE  seen nptype=5(id)
Jun 24, 18:30:22  Debug    IKE  seen nptype=11(notify)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  Notify Message received
Jun 24, 18:30:22  Warning  IKE  ignore RESPONDER-LIFETIME notification.
Jun 24, 18:30:22  Debug    IKE  HASH allocated:hbuf->l=192 actual:tlen=160
Jun 24, 18:30:22  Debug    IKE  HASH(2) received:2007-06-24 18:30:22: DEBUG:
Jun 24, 18:30:22  Debug    IKE  f3bd0241 9673e747 e712c98f a3d479d4 dd7add0c
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  c3d88d83 c363e586 5ee352d7 e44a07e3 9fe14a43 0a000034 00000001 00000001
Jun 24, 18:30:22  Debug    IKE  00000028 01030401 ad4da6b5 0000001c 01030000 8004f003 80010001 00020004
Jun 24, 18:30:22  Debug    IKE  00015180 80050002 05000018 4ac01c9d 78ab3f11 0be5f709 bc33cd51 73d78a0f
Jun 24, 18:30:22  Debug    IKE  0500000c 01000000 c0a80502 0b000010 04000000 0a010c00 ffffff00 00000028
Jun 24, 18:30:22  Debug    IKE  00000001 03046000 ad4da6b5 80010001 00020004 00007080 80010002 00020004
Jun 24, 18:30:22  Debug    IKE  00465000
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH computed:
Jun 24, 18:30:22  Debug    IKE  f3bd0241 9673e747 e712c98f a3d479d4 dd7add0c
Jun 24, 18:30:22  Debug    IKE  total SA len=48
Jun 24, 18:30:22  Debug    IKE  00000001 00000001 00000028 01030401 06fac2c5 0000001c 01030000 80010001
Jun 24, 18:30:22  Debug    IKE  00020004 00015180 8004f003 80050002
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=2(prop)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  proposal #1 len=40
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=3(trns)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  transform #1 len=28
Jun 24, 18:30:22  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jun 24, 18:30:22  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jun 24, 18:30:22  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jun 24, 18:30:22  Debug    IKE  UDP encapsulation requested
Jun 24, 18:30:22  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jun 24, 18:30:22  Debug    IKE  pair 1:
Jun 24, 18:30:22  Debug    IKE  0x30a0d0: next=0x0 tnext=0x0
Jun 24, 18:30:22  Debug    IKE  proposal #1: 1 transform
Jun 24, 18:30:22  Debug    IKE  total SA len=48
Jun 24, 18:30:22  Debug    IKE  00000001 00000001 00000028 01030401 ad4da6b5 0000001c 01030000 8004f003
Jun 24, 18:30:22  Debug    IKE  80010001 00020004 00015180 80050002
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=2(prop)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  proposal #1 len=40
Jun 24, 18:30:22  Debug    IKE  begin.
Jun 24, 18:30:22  Debug    IKE  seen nptype=3(trns)
Jun 24, 18:30:22  Debug    IKE  succeed.
Jun 24, 18:30:22  Debug    IKE  transform #1 len=28
Jun 24, 18:30:22  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jun 24, 18:30:22  Debug    IKE  UDP encapsulation requested
Jun 24, 18:30:22  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jun 24, 18:30:22  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
```

```
Jun 24, 18:30:22  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jun 24, 18:30:22  Debug    IKE  pair 1:
Jun 24, 18:30:22  Debug    IKE  0x30a0e0: next=0x0 tnext=0x0
Jun 24, 18:30:22  Debug    IKE  proposal #1: 1 transform
Jun 24, 18:30:22  Warning  IKE  attribute has been modified.
Jun 24, 18:30:22  Debug    IKE  begin compare proposals.
Jun 24, 18:30:22  Debug    IKE  pair[1]: 0x30a0e0
Jun 24, 18:30:22  Debug    IKE  0x30a0e0: next=0x0 tnext=0x0
Jun 24, 18:30:22  Debug    IKE  prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
Jun 24, 18:30:22  Debug    IKE  type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
Jun 24, 18:30:22  Debug    IKE  type=SA Life Type, flag=0x8000, lorv=seconds
Jun 24, 18:30:22  Debug    IKE  type=SA Life Duration, flag=0x0000, lorv=4
Jun 24, 18:30:22  Debug    IKE  type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
Jun 24, 18:30:22  Debug    IKE  peer's single bundle:
Jun 24, 18:30:22  Debug    IKE  (proto_id=ESP spisize=4 spi=ad4da6b5 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
Jun 24, 18:30:22  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jun 24, 18:30:22  Debug    IKE  my single bundle:
Jun 24, 18:30:22  Debug    IKE  (proto_id=ESP spisize=4 spi=06fac2c5 spi_p=00000000 encmode=UDP-Tunnel reqid=610:609)
Jun 24, 18:30:22  Debug    IKE  (trns_id=3DES encklen=0 authtype=hmac-sha)
Jun 24, 18:30:22  Info     IKE  Adjusting my encmode UDP-Tunnel->Tunnel
Jun 24, 18:30:22  Info     IKE  Adjusting peer's encmode UDP-Tunnel(61443)->Tunnel(1)
Jun 24, 18:30:22  Debug    IKE  matched
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  HASH(3) generate
Jun 24, 18:30:22  Debug    IKE  HASH with:
Jun 24, 18:30:22  Debug    IKE  00c3d88d 83c363e5 865ee352 d7e44a07 e39fe14a 434ac01c 9d78ab3f 110be5f7
Jun 24, 18:30:22  Debug    IKE  09bc33cd 5173d78a 0f
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  HASH computed:
Jun 24, 18:30:22  Debug    IKE  edcdd5d7 2eac7fae 24ddf2a3 dfc143b5 0ff0b9d0
Jun 24, 18:30:22  Debug    IKE  add payload of len 20, next type 0
Jun 24, 18:30:22  Debug    IKE  begin encryption.
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  pad length = 8
Jun 24, 18:30:22  Debug    IKE  00000018 edcdd5d7 2eac7fae 24ddf2a3 dfc143b5 0ff0b9d0 8ef1afdb 84f8e007
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  with key:
Jun 24, 18:30:22  Debug    IKE  cfb1ed84 4d213b48 600d05a8 db17a815 40256718 dc516947
Jun 24, 18:30:22  Debug    IKE  encrypted payload by IV:
Jun 24, 18:30:22  Debug    IKE  c86eeda5 50715e64
Jun 24, 18:30:22  Debug    IKE  save IV for next:
Jun 24, 18:30:22  Debug    IKE  08f8ec1a 289cab3f
Jun 24, 18:30:22  Debug    IKE  encrypted.
Jun 24, 18:30:22  Debug    IKE  Adding NON-ESP marker
Jun 24, 18:30:22  Debug    IKE  64 bytes from 192.168.215.1[4500] to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  sockname 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet from 192.168.215.1[4500]
Jun 24, 18:30:22  Debug    IKE  send packet to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  1 times of 64 bytes message will be sent to 192.168.215.235[4500]
Jun 24, 18:30:22  Debug    IKE  00000000 895769d6 1b7501f9 e459750f 8040831f 08102001 c3d88d83 0000003c
Jun 24, 18:30:22  Debug    IKE  828c8ecd 12183b3e b9fd339b 763d4c26 8fcaf280 62f6752b 08f8ec1a 289cab3f
Jun 24, 18:30:22  Debug    IKE  KEYMAT compute with
Jun 24, 18:30:22  Debug    IKE  0306fac2 c5c363e5 865ee352 d7e44a07 e39fe14a 434ac01c 9d78ab3f 110be5f7
Jun 24, 18:30:22  Debug    IKE  09bc33cd 5173d78a 0f
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  encklen=192 authklen=160
Jun 24, 18:30:22  Debug    IKE  generating 640 bits of key (dupkeymat=4)
Jun 24, 18:30:22  Debug    IKE  generating K1...K4 for KEYMAT.
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  ff70919f 1a50b7bd 9ba30a6d 29535480 4380f04c befe051d 4c98d2fc 9eb1ae41
Jun 24, 18:30:22  Debug    IKE  660fbb71 86665ced d202cb23 f37335b9 11b98d82 389ba99d 01141a79 66350219
Jun 24, 18:30:22  Debug    IKE  2b4465c7 f752f4c4 81dd0970 b1c7c226
Jun 24, 18:30:22  Debug    IKE  KEYMAT compute with
Jun 24, 18:30:22  Debug    IKE  03ad4da6 b5c363e5 865ee352 d7e44a07 e39fe14a 434ac01c 9d78ab3f 110be5f7
Jun 24, 18:30:22  Debug    IKE  09bc33cd 5173d78a 0f
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  encklen=192 authklen=160
Jun 24, 18:30:22  Debug    IKE  generating 640 bits of key (dupkeymat=4)
```

```
Jun 24, 18:30:22  Debug    IKE  generating K1...K4 for KEYMAT.
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  5be11f2f bc5c91af 70e6d853 53b332b3 4e912651 a15c16ab 8f6f3919 3348746d
Jun 24, 18:30:22  Debug    IKE  71ab0cd7 0f9e89b0 6b78c6eb 8f015643 5060d524 1e88eb41 a91504cb 9863b17f
Jun 24, 18:30:22  Debug    IKE  074c8511 44c15913 2fbf3865 1198a747
Jun 24, 18:30:22  Debug    IKE  KEYMAT computed.
Jun 24, 18:30:22  Debug    IKE  call pk_sendupdate
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  call pfkey_send_update_nat
Jun 24, 18:30:22  Debug    IKE  pfkey update sent.
Jun 24, 18:30:22  Debug    APP  Received SADB message type UPDATE, 192.168.215.235 [4500] -> 192.168.215.1 [4500]
Jun 24, 18:30:22  Debug    APP  SA change detected
Jun 24, 18:30:22  Debug    IKE  encryption(3des)
Jun 24, 18:30:22  Debug    IKE  hmac(hmac_sha1)
Jun 24, 18:30:22  Debug    IKE  call pfkey_send_add_nat
Jun 24, 18:30:22  Debug    APP  Received SADB message type ADD, 192.168.215.1 [4500] -> 192.168.215.235 [4500]
Jun 24, 18:30:22  Debug    APP  SA change detected
Jun 24, 18:30:22  Debug    APP  Connection Cisco PIX 501 is up
Jun 24, 18:30:22  Debug    IKE  pfkey add sent.
Jun 24, 18:30:22  Debug    IKE  get pfkey UPDATE message
Jun 24, 18:30:22  Debug    IKE  02020003 14000000 9d000000 a2100000 02000100 06fac2c5 04000202 00000000
Jun 24, 18:30:22  Debug    IKE  02001300 02000000 00000000 62020000 03000500 ff200000 10021194 c0a8d7eb
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 03000600 ff200000 10021194 c0a8d701 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  04000300 00000000 00000000 00000000 80510100 00000000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  04000400 00000000 00000000 00000000 000e0100 00000000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  pfkey UPDATE succeeded: ESP/Tunnel 192.168.215.235[4500]->192.168.215.1[4500]
spi=117097157(0x6fac2c5)
Jun 24, 18:30:22  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.235[4500]->192.168.215.1[4500]
spi=117097157(0x6fac2c5)
Jun 24, 18:30:22  Debug    IKE  ===
Jun 24, 18:30:22  Debug    IKE  get pfkey ADD message
Jun 24, 18:30:22  Debug    IKE  02030003 14000000 9d000000 a2100000 02000100 ad4da6b5 04000202 00000000
Jun 24, 18:30:22  Debug    IKE  02001300 02000000 00000000 61020000 03000500 ff200000 10021194 c0a8d701
Jun 24, 18:30:22  Debug    IKE  00000000 00000000 03000600 ff200000 10021194 c0a8d7eb 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  04000300 00000000 00000000 00000000 80510100 00000000 00000000 00000000
Jun 24, 18:30:22  Debug    IKE  04000400 00000000 00000000 00000000 000e0100 00000000 00000000 00000000
Jun 24, 18:30:22  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.1[4500]->192.168.215.235[4500]
spi=2907547317(0xad4da6b5)
```