Legal Disclaimer

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

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

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

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

Acknowledgments
Many thanks to Stephen B (www.suchaproduction.com) and Jason Sjobeck (www.sjobeck.com) for providing setup information, screenshots and support for writing this document.
# Table of contents

Introduction ...........................................................................................................1  
monowall VPN Setup ..................................................................................................1  
  Login to monowall.................................................................1  
  Enable IPSec .................................................................2  
  Configure Mobile Client ........................................................3  
  Add Users .................................................................4  
IPSecuritas Setup .................................................................................................4  
  Start Wizard ..............................................................................4  
  Enter Name of New Connection ....................................................4  
  Select Router Model ..........................................................5  
  Enter Router's Public IP Address ................................................5  
  Enter a Virtual IP Address........................................................5  
  Enter Remote Network ..........................................................6  
  Enter Local Identification .....................................................6  
  Enter Preshared Key ............................................................6  
Diagnosis .............................................................................................................7  
  Reachability Test ........................................................................7  
  Sample monowall Log Output .......................................................7  
  Sample IPSecuritas Log Output ......................................................8
Introduction

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

![Network Diagram]

m0n0wall VPN Setup

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

Login to m0n0wall

First, connect to your monowall in a web browser and enter the administrator password.

Once logged in, click on **IPSec** in the menu **VPN** on the left side of the displayed monowall main page.
Enable IPSec

In the now appearing panel (make sure Tunnels is selected in the tab chooser at the top), switch on the option Enable IPSec and press Save to commit your changes.
Configure Mobile Client

Next, please press on **Mobile clients** in the tab chooser at the top.

Set all properties as shown in the screenshot to the left.

Press **Save** to commit your changes.
Add Users

Now, press on **Pre-shared keys** in the tab chooser at the top. You will be presented with a list of names and accompanying preshared key (which is a secure password string). Press the add icon next to the list to add a new user. Please remember the user name and the pre-shared key you choose, since you need them again when setting up IPSecuritas.

You may use the same name and key for all users or you may create individual name key pairs for each user (recommended).

The setup of monowall is now complete and it will accept incoming IPSec connection requests. You may now proceed with the setup of IPSecuritas, described in the next chapter.

**IPSecuritas Setup**

This section describes the necessary steps to setup IPSecuritas to connect to the monowall 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 **monowall** from the manufacturer list and **monowall** 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 monowall 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](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](http://www.rfc-editor.org/rfc/rfc1918)).

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 m0n0wall.

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

Enter Local Identification

Enter the local identification (which is the identifier you choose when setting up the the pre-shared keys on the monowall).

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

Enter Preshared Key

Enter the same Preshared Key that you set for the identification you entered in the last step.

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 monowall local IP address. If the tunnel works correctly, a similar output is displayed:

```
[Macbook:~] root# ping 192.168.1.1
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=19.290 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=12.823 ms
```

Sample monowall Log Output

While still logged into the monowall web interface, click onto Diagnostics on the left side to unveil its submenu. Click on Logs to display the monowall log entries.

If the connection attempt was successful, you should see a similar log as shown to the left.
Sample IPSecuritas Log Output

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

May 20, 12:15:41 Debug APP State change from IDLE to AUTHENTICATING after event START
May 20, 12:15:41 Info APP IKE daemon started
May 20, 12:15:41 Info APP IPSec started
May 20, 12:15:41 Debug APP State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
May 20, 12:15:41 Debug APP Received SADB message type X_SPDUPDATE - not interesting
May 20, 12:15:41 Debug APP Received SADB message type X_SPDUPDATE - not interesting
May 20, 12:15:41 Info IKE Foreground mode.
May 20, 12:15:41 Info IKE @(#)ipsec-tools CVS (http://ipsec-tools.sourceforge.net)
May 20, 12:15:41 Info IKE @(#)This product linked OpenSSL 0.9.7i 28 Sep 2006 (http://www.openssl.org/)
May 20, 12:15:41 Info IKE Reading configuration from /Library/Application Support/Lobotomo Software/IPSecuritas/racoon.conf
May 20, 12:15:41 Info IKE Resize address pool from 0 to 255
May 20, 12:15:41 Debug IKE lifetime = 28800
May 20, 12:15:41 Debug IKE lifebyte = 0
May 20, 12:15:41 Debug IKE emcklen=0
May 20, 12:15:41 Debug IKE p:1 t:1
May 20, 12:15:41 Debug IKE 3DES-CBC(5)
May 20, 12:15:41 Debug IKE SHA(2)
May 20, 12:15:41 Debug IKE 3DES-CBC(5)
May 20, 12:15:41 Debug IKE hmac(modp1024)
May 20, 12:15:41 Debug IKE pre-shared key(1)
May 20, 12:15:41 Debug IKE compression algorithm can not be checked because sadb message doesn't support it.
May 20, 12:15:41 Debug IKE open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon
May 20, 12:15:41 Debug IKE compression algorithm can not be checked because sadb message doesn't support it.
May 20, 12:15:41 Error IKE inappropriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:41 Error IKE inappopriate sadb acquire message passed.
May 20, 12:15:43  Debug  IKE  seen nptype=18(nonce)
May 20, 12:15:43  Debug  IKE  seen nptype=5(id)
May 20, 12:15:43  Debug  IKE  seen nptype=13(vid)
May 20, 12:15:43  Debug  IKE  seen nptype=28(nat-d)
May 20, 12:15:43  Debug  IKE  succeed.
May 20, 12:15:43  Info   IKE  received Vendor ID: RFC 3947
May 20, 12:15:43  Info   IKE  received Vendor ID: DPD
May 20, 12:15:43  Debug  IKE  remote supports DPD
May 20, 12:15:43  Debug  IKE  total SA len=48
May 20, 12:15:43  Debug  IKE  begin.
May 20, 12:15:43  Debug  IKE  00000001 00000001 00000028 01010001 00000020 01010000 800b0001 800c7080
May 20, 12:15:43  Debug  IKE  80010005 80030001 80020002 80040002
May 20, 12:15:43  Debug  IKE  begin.
May 20, 12:15:43  Debug  IKE  seen nptype=2(prop)
May 20, 12:15:43  Debug  IKE  succeed.
May 20, 12:15:43  Debug  IKE  proposal #1 len=40
May 20, 12:15:43  Debug  IKE  begin.
May 20, 12:15:43  Debug  IKE  seen nptype=3(trns)
May 20, 12:15:43  Debug  IKE  succeed.
May 20, 12:15:43  Debug  IKE  transform #1 len=32
May 20, 12:15:43  Debug  IKE  type=Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug  IKE  type=Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug  IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 20, 12:15:43  Debug  IKE  encryption(3des)
May 20, 12:15:43  Debug  IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 20, 12:15:43  Debug  IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 20, 12:15:43  Debug  IKE  hmac(modp1024)
May 20, 12:15:43  Debug  IKE  pair 1:
May 20, 12:15:43  Debug  IKE  0x3095e0: next=0x0 tnext=0x0
May 20, 12:15:43  Debug  IKE  proposal #1 len=40
May 20, 12:15:43  Debug  IKE  prop#=1, prot-id=ISAKMP, spi-size=0, #trns=1
May 20, 12:15:43  Debug  IKE  trns#=1, trns-id=IKE
May 20, 12:15:43  Debug  IKE  type=Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43  Debug  IKE  type=Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43  Debug  IKE  type=Encryption Algorithm, flag=0x8000, lorv=3DES-CBC
May 20, 12:15:43  Debug  IKE  encryption(3des)
May 20, 12:15:43  Debug  IKE  type=Authentication Method, flag=0x8000, lorv=pre-shared key
May 20, 12:15:43  Debug  IKE  type=Hash Algorithm, flag=0x8000, lorv=SHA
May 20, 12:15:43  Debug  IKE  hmac(modp1024)
May 20, 12:15:43  Debug  IKE  Compared: DB:Peer
May 20, 12:15:43  Debug  IKE  (lifetime = 28800:28800)
May 20, 12:15:43  Debug  IKE  (lifebyte = 0:0)
May 20, 12:15:43  Debug  IKE  enctype = 3DES-CBC:3DES-CBC
May 20, 12:15:43  Debug  IKE  (encklen = 0:0)
May 20, 12:15:43  Debug  IKE  hashtype = SHA:SHA
May 20, 12:15:43  Debug  IKE  authmethod = pre-shared key:pre-shared key
May 20, 12:15:43  Debug  IKE  dh_group = 1024-bit MODP group:1024-bit MODP group
May 20, 12:15:43  Debug  IKE  an acceptable proposal found.
May 20, 12:15:43  Debug  IKE  hmac(modp1024)
May 20, 12:15:43  Debug  IKE  agreed on pre-shared key auth.
May 20, 12:15:43  Info    IKE  Selected NAT-T version: RFC 3947
May 20, 12:15:43  Info    IKE  couldn't find the proper pskey, try to get one by the peer's address.
May 20, 12:15:43  Debug  IKE  the psk found.
May 20, 12:15:43  Info    IKE  the psk found.
May 20, 12:15:43  Info    IKE  the psk found.
May 20, 12:15:43  Info    IKE  the psk found.
May 20, 12:15:43  Info    IKE  the psk found.
May 20, 12:15:43  Info    IKE  the psk found.
May 20, 12:15:43 Debug IKE 1 times of 104 bytes message will be sent to 192.168.215.226[4500]
May 20, 12:15:43 Debug IKE 00000000 489fab77 ca78ff22 0eec5bb9 5976e03b 08100400 00000000 00000004
May 20, 12:15:43 Debug IKE 14000018 1f1462e1 00435e46 39d01763 e2f0f7a2 a5436df4 14000018 58ee9208
May 20, 12:15:43 Debug IKE 72bb8972 667f3791 0f863aea e561cb67 00000000 58ee9208 72bb8972 667f3791
May 20, 12:15:43 Debug IKE 0f863aea e561cb67
May 20, 12:15:43 Debug IKE compute IV for phase2
May 20, 12:15:43 Debug IKE phase1 last IV:
May 20, 12:15:43 Debug IKE 2d44d9e3 27802d21 cbfd5baf
May 20, 12:15:43 Debug IKE hash(sha1)
May 20, 12:15:43 Debug IKE encryption(3des)
May 20, 12:15:43 Debug IKE phase2 IV computed:
May 20, 12:15:43 Debug IKE 4742b91b b0e7d38c
May 20, 12:15:43 Debug IKE HASH with:
May 20, 12:15:43 Debug IKE cbfd5baf 0000001c 00000001 01106002 489fab77 ca78ff22 0eec5bb9 5976e03b
May 20, 12:15:43 Debug IKE hmac(hmac_sha1)
May 20, 12:15:43 Debug IKE HASH computed:
May 20, 12:15:43 Debug IKE 278363b7 1a6ce9db 51e85974 6450f2c0 2541c3fb
May 20, 12:15:43 Debug IKE begin encryption.
May 20, 12:15:43 Debug IKE encryption(3des)
May 20, 12:15:43 Debug IKE pad length = 4
May 20, 12:15:43 Debug IKE 0b000018 278363b7 1a6ce9db 51e85974 6450f2c0 2541c3fb 0000001c 00000001
May 20, 12:15:43 Debug IKE 01106002 489fab77 ca78ff22 0eec5bb9 5976e03b
May 20, 12:15:43 Debug IKE encryption(3des)
May 20, 12:15:43 Debug IKE with key:
May 20, 12:15:43 Debug IKE bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43 Debug IKE encrypted payload by IV:
May 20, 12:15:43 Debug IKE 4742b91b b0e7d38c
May 20, 12:15:43 Debug IKE save IV for next:
May 20, 12:15:43 Debug IKE 1cf987ee 7b770249
May 20, 12:15:43 Debug IKE encrypted.
May 20, 12:15:43 Debug IKE Adding NON-ESP marker
May 20, 12:15:43 Debug IKE sockname 192.168.215.2[4500]
May 20, 12:15:43 Debug IKE 1 times of 88 bytes message will be sent to 192.168.215.226[4500]
May 20, 12:15:43 Debug IKE 00000000 489fab77 ca78ff22 0eec5bb9 5976e03b 08100400 00000004
May 20, 12:15:43 Debug IKE e6fab32c 174d3e92 7162d8c5 e4cc745e 1b79bf13 6337cb27 796ed726 00e69918
May 20, 12:15:43 Debug IKE b0a3ea23 8390c95b 84a75a92 068d389e 1cf987ee 7b770249
May 20, 12:15:43 Debug IKE sendto Information notify.
May 20, 12:15:43 Debug IKE IV freed
May 20, 12:15:43 Debug IKE ===
May 20, 12:15:43 Debug IKE ===
May 20, 12:15:43 Debug IKE begin QUICK mode.
May 20, 12:15:43 Debug IKE compute IV for phase2
May 20, 12:15:43 Debug IKE phase1 last IV:
May 20, 12:15:43 Debug IKE 2d44d9e3 27802d21 a6f8927d
May 20, 12:15:43 Debug IKE hash(sha1)
May 20, 12:15:43 Debug IKE encryption(3des)
May 20, 12:15:43 Debug IKE phase2 IV computed:
May 20, 12:15:43 Debug IKE 527d772b 1f1652d4
May 20, 12:15:43 Debug IKE call pfkey_send_getspi
May 20, 12:15:43 Debug IKE pfkey GETSPI sent: ESP/Tunnel 192.168.215.2[0]-192.168.215.226[0] spi:"126214327(0x785e0b7)"
May 20, 12:15:43 Info IKE NAT detected -> UDP encapsulation (ENC_MODE 1->3).
May 20, 12:15:43 Debug IKE hmac(modp1824)
May 20, 12:15:43 Debug IKE hmac(modp1824)
May 20, 12:15:43  Debug    IKE  ed2a18ef 95373c6f d7d6ac51 1b3fa811 b566ec6c 080a5d39 1e2e61d1 f4ebacbf
May 20, 12:15:43  Debug    IKE  898c6f61 de46657c 87d75cda 2a02a381 f987993c 416090e8 dfafde47 199e7f9f
May 20, 12:15:43  Debug    IKE  c42e3932 446d2556 3dfafaf5 209777b7 90c8e55e f21e51d2 0d7f86d0 66628430
May 20, 12:15:43  Debug    IKE  use local ID type IPv4_address
May 20, 12:15:43  Debug    IKE  use remote ID type IPv4_subnet
May 20, 12:15:43  Debug    IKE  40:00:0000 cba876f2
May 20, 12:15:43  Debug    IKE  IDcr:
May 20, 12:15:43  Debug    IKE  04000000 0a018030 ffffff00
May 20, 12:15:43  Debug    IKE  add payload of len 48, next type 10
May 20, 12:15:43  Debug    IKE  add payload of len 16, next type 4
May 20, 12:15:43  Debug    IKE  add payload of len 128, next type 5
May 20, 12:15:43  Debug    IKE  add payload of len 8, next type 6
May 20, 12:15:43  Debug    IKE  add payload of len 12, next type 0
May 20, 12:15:43  Debug    IKE  HASH with:
May 20, 12:15:43  Debug    IKE  dfafde47 199e7f9f c42e3932 446d2556 3dfafaf5 209777b7 90c8e55e f21e51d2 0d7f86d0
May 20, 12:15:43  Debug    IKE  HASH computed;
May 20, 12:15:43  Debug    IKE  e1bb92d4 4b276a7e b595a518 6f1801ce 01428908
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  01000018 e1bb92d4 4b276a7e b595a518 6f1801ce 01428908 00000034 00000000 00000001
May 20, 12:15:43  Debug    IKE  01000018 e1bb92d4 4b276a7e b595a518 6f1801ce 01428908 00000034 00000000 00000001
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  key: 6f1801ce 01428908 00000034 00000000 00000001
May 20, 12:15:43  Debug    IKE  begin encryption by: 52767720 1f1e6e64
May 20, 12:15:43  Debug    IKE  save payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  save IV for next:
May 20, 12:15:43  Debug    IKE  52767720 1f1e6e64
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  with key: b6788b04 4ac8b8ad 685edf16 01ebab94 3e605a02 0a443b39
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  with key: b6788b04 4ac8b8ad 685edf16 01ebab94 3e605a02 0a443b39
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
May 20, 12:15:43  Debug    IKE  pad length = 8
May 20, 12:15:43  Debug    IKE  add payload of len 20, next type 1
May 20, 12:15:43  Debug    IKE  begin encryption.
May 20, 12:15:43  Debug    IKE  encryption3des
IPSecuritas Configuration Instructions

m0n0wall

---

May 20, 12:15:43 Debug IKE type-Group Description, flag=0x8000, lorv=2
May 20, 12:15:43 Debug IKE hmac(mdp1824)
May 20, 12:15:43 Debug IKE pair 1:
May 20, 12:15:43 Debug IKE 0x309f30: next=0x0 tnext=0x0
May 20, 12:15:43 Debug IKE proposal #1: 1 transform
May 20, 12:15:43 Debug IKE total SA len=48
May 20, 12:15:43 Debug IKE 00000001 00000001 00000028 01030401 04ec30a3 0000001c 01030000 80010001
May 20, 12:15:43 Debug IKE 80027080 80040003 80050002 80030002
May 20, 12:15:43 Debug IKE begin.
May 20, 12:15:43 Debug IKE seen nptype=2(prop)
May 20, 12:15:43 Debug IKE succeed.
May 20, 12:15:43 Debug IKE proposal #1 len=40
May 20, 12:15:43 Debug IKE begin.
May 20, 12:15:43 Debug IKE seen nptype=3(trns)
May 20, 12:15:43 Debug IKE succeed.
May 20, 12:15:43 Debug IKE transform #1 len=28
May 20, 12:15:43 Debug IKE type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43 Debug IKE type=SA Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43 Debug IKE life duration was in TLV.
May 20, 12:15:43 Debug IKE type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
May 20, 12:15:43 Debug IKE UDP encapsulation requested
May 20, 12:15:43 Debug IKE type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 12:15:43 Debug IKE type=Group Description, flag=0x8000, lorv=2
May 20, 12:15:43 Debug IKE hmac(mdp1824)
May 20, 12:15:43 Debug IKE pair 1:
May 20, 12:15:43 Debug IKE 0x309f40: next=0x0 tnext=0x0
May 20, 12:15:43 Debug IKE proposal #1: 1 transform
May 20, 12:15:43 Debug IKE begin compare proposals.
May 20, 12:15:43 Debug IKE pair[1]: 0x309f40
May 20, 12:15:43 Debug IKE prop#=1 prot-id=ESP spi-size=4 #trns=1 trns#=1 trns-id=3DES
May 20, 12:15:43 Debug IKE type=SA Life Type, flag=0x8000, lorv=seconds
May 20, 12:15:43 Debug IKE type=SA Life Duration, flag=0x8000, lorv=28800
May 20, 12:15:43 Debug IKE type=Encryption Mode, flag=0x8000, lorv=UDP-Tunnel
May 20, 12:15:43 Debug IKE type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 20, 12:15:43 Debug IKE type=Group Description, flag=0x8000, lorv=2
May 20, 12:15:43 Debug IKE peer’s single bundle:
May 20, 12:15:43 Debug IKE (proto_id=ESP spisize=4 spi=04ec30a3 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
May 20, 12:15:43 Debug IKE (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 12:15:43 Debug IKE my single bundle:
May 20, 12:15:43 Debug IKE (proto_id=ESP spisize=4 spi=0785e0b7 spi_p=00000000 encmode=UDP-Tunnel reqid=0:0)
May 20, 12:15:43 Debug IKE (trns_id=3DES encklen=0 authtype=hmac-sha)
May 20, 12:15:43 Info IKE Adjusting my encmode UDP-Tunnel->Tunnel
May 20, 12:15:43 Info IKE Adjusting peer’s encmode UDP-Tunnel(3)->Tunnel(1)
May 20, 12:15:43 Debug IKE matched
May 20, 12:15:43 Debug IKE ---
May 20, 12:15:43 Debug IKE HASH(3) generate
May 20, 12:15:43 Debug IKE HASH with:
May 20, 12:15:43 Debug IKE 00a6f892 7dc3d1e7 85f7ad5 50448326 0d7e9d0f fec13547 31e8a86e c934326b
May 20, 12:15:43 Debug IKE b012b442 c3
May 20, 12:15:43 Debug IKE hmac(hmac_sha1)
May 20, 12:15:43 Debug IKE HASH computed:
May 20, 12:15:43 Debug IKE 9446acf6 92a5827 9b65aa22 8d922ef0 5c3c3b30
May 20, 12:15:43 Debug IKE add payload of len 24, next type 0
May 20, 12:15:43 Debug IKE begin encryption.
May 20, 12:15:43 Debug IKE encryption(3des)
May 20, 12:15:43 Debug IKE pad length = 8
May 20, 12:15:43 Debug IKE 00000018 9446acf6 92a5827 9b65aa22 8d922ef0 5c3c3b30 00000000 00000000
May 20, 12:15:43 Debug IKE encryption(3des)
May 20, 12:15:43 Debug IKE with key:
May 20, 12:15:43 Debug IKE bb788043 4cab88a9 685ed1f6 01beab94 36a90502 aa443bb9
May 20, 12:15:43 Debug IKE encrypted payload by IV:
May 20, 12:15:43 Debug IKE eebe7b79 462a7901
May 20, 12:15:43 Debug IKE save IV for next:
May 20, 12:15:43 Debug IKE d87f051d 479cb619
May 20, 12:15:43 Debug IKE encrypted.
May 20, 12:15:43  Debug    IKE  04000400 00000000 00000000 00000000 005a0000 00000000 00000000 00000000
  spi=82587811(0x4ec30a3)
May 20, 12:15:43  Debug    IKE  ---