IPSecuritas 3.x

Configuration Instructions

for

Zyxel ZyWALL

© 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
Zyxel ZyWALL Setup ......................................................................................................1
  Login ...........................................................................................................................1
  Add VPN Rule .............................................................................................................2
  Create Gateway Policy ...............................................................................................2
  Create Network Policy ..............................................................................................3
IPSecuritas Setup ........................................................................................................4
  Start Wizard ................................................................................................................4
    Enter Name of New Connection ..............................................................................4
    Select Router Model .................................................................................................4
    Enter Router’s Public IP Address .............................................................................4
    Enter a Virtual IP Address .......................................................................................5
    Enter Remote Network ..............................................................................................5
    Enter Local Identification .........................................................................................5
    Enter Preshared Key .................................................................................................6
Diagnosis .......................................................................................................................6
  Reachability Test .........................................................................................................6
  Sample Safe@Office Log Output .................................................................................7
  Sample IPSecuritas Log Output ...................................................................................9
Introduction

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

Zyxel ZyWALL Setup

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

Login

Open a web browser and connect to your Zyxel firewall. Enter the administrator's password.

In the main menu on the left side, click on SECURITY to disclose the sub-entries and then click on VPN.
Add VPN Rule

A similar screen as depicted on the left should appear.

Add a new Gateway Policy by clicking on this symbol next to VPN Rule on the top line:

Create Gateway Policy

Fill in the Gateway Policy information as follows:

- **Property**: Name: *An arbitrary name*
- **NAT Traversal**: Enabled

**Gateway Policy Information**
- **My Address**: 0.0.0.0
- **Remote Gateway Address**: 0.0.0.0

- **Authentication Key**
  - **Pre-Shared Key**: Enabled
  - **Local ID Type**: IP
  - **Content**: 0.0.0.0
  - **Peer ID Type**: DNS
  - **Content**: Any string

- **Extended Authentication**
  - **IKE Proposal**
    - **Negotiation Mode**: Main
    - **Encryption Algorithm**: 3DES
    - **Authentication Algorithm**: SHA1
    - **SA Life Time**: 28800
    - **Key Group**: DH1
    - **Enabled Multiple Proposals**: Disabled

Please remember the **preshared key** and the **Peer ID** as you will need it when setting up the connection in IPSecuritas.

Click on apply when you are finished.
Create Network Policy

Back in the VPN overview, click on the disclose icon of the newly created Gateway Policy, then click on the this symbol to add a network policy:

![Network Policy Symbol]

Fill in the Network Policy information as follows:

- **Property**
  - Active: **Enabled**
  - Name: **An arbitrary name**
  - Protocol: **0 Nailed-Up**
  - Allow NetBIOS Traffic Through IPSec Tunnel: **Disabled**
  - Check IPSec Tunnel Connectivity: **Log**

**Gateway Policy Information**

- **Gateway Policy:** The newly created policy
- **Local Network**
  - Address Type: **Subnet Address**
  - Starting Address: **192.168.2.0**
  - Subnet Mask: **255.255.255.0**
  - Local Port: **0 - 0**

- **Remote Network**
  - Address Type: **Single Address**
  - Starting IP Address: **0.0.0.0**
  - Remote Port: **0 - 0**

**IPSec Proposal**

- **Encapsulation Mode:** Tunnel
- **Active Protocol:** ESP
- **Encryption Algorithm:** 3DES
- **Authentication Algorithm:** SHA1
- **SA Life Time:** 28800
- **Perfect Forward Secrecy:** DH1
- **Enabled Replay Detection:** Disabled
- **Enabled Multiple Proposals:** Disable

Click on **Apply** to save the settings and finish the ZyWALL configuration. You may now proceed with the configuration of the connection in IPSecuritas now.
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the ZyWALL firewall.

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 **Zyxel** from the manufacturer list and your **ZyWALL** model from the model list.

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

Enter Router’s Public IP Address

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

Click on the right arrow to continue with the next step.
Enter a Virtual IP Address

Enter a virtual local IP address. This address appears as the source address of any packet going through the tunnel. If no address is specified, the real local IP address is used instead.

In order to prevent address collisions between the local network and the remote network, it is recommended to use an address from one the ranges reserved for private network (see RFC 1918).

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

Enter Remote Network

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

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

Enter Local Identification

Enter the ZyWALL's local identification (which you had to enter in the Gateway Policy setup of the ZyWALL).

Click on the right arrow to continue with the next step.
Enter Preshared Key

Enter the same **Preshared Key** of the ZyWALL (which you had to enter in the **Gateway Policy** setup of the ZyWALL).

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

```
[MacBook:]$ root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=19.290 ms
```
The following is a sample log from the ZyWALL after a successful connection establishment:

<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Message</th>
<th>Source</th>
<th>Destination</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>01/18/2000 11:30:35</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>3</td>
<td>01/18/2000 11:30:34</td>
<td>Adjust TCP MSS to 1396</td>
<td>192.168.215.2</td>
<td>192.168.215.2</td>
<td>IKE</td>
</tr>
<tr>
<td>5</td>
<td>01/18/2000 11:30:34</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>7</td>
<td>01/18/2000 11:30:34</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.2</td>
<td>IKE</td>
</tr>
<tr>
<td>9</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>11</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>13</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>15</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>16</td>
<td>01/18/2000 11:30:33</td>
<td>Adjust TCP MSS to 1460</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>18</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>19</td>
<td>01/18/2000 11:30:33</td>
<td>Phase 1 IKE SA process done</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>20</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>22</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>24</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>26</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>28</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>30</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>31</td>
<td>01/18/2000 11:30:33</td>
<td>Recv [SA][VID][VID][VID][VID][VID][VID][VID][VID][VID][VID][VID]</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>32</td>
<td>01/18/2000 11:30:33</td>
<td>The cookie pair is: 0x113CF00DD0FD274E/0xF17383030F9F3456</td>
<td>192.168.215.2</td>
<td>192.168.215.225</td>
<td>IKE</td>
</tr>
<tr>
<td>Time</td>
<td>Event and Details</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>Rule [Road Warrior] Receiving IKE request</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:32</td>
<td>The cookie pair is: 0x13CFD0D5DFD374E/0x8F1739353F9F1466 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:38</td>
<td>Send:[HASH][DEL]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:38</td>
<td>Recv:[HASH][DEL]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Rule [Roadwarrior] Tunnel built successfully</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Adjust TCP MSS to 1398</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Recv:[HASH]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Send:[HASH][NOCE][KE][ID]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:38</td>
<td>Swap rule to rule [Roadwarrior]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Swap rule to rule [Roadwarrior]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Start Phase 2: Quick Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Recv:[HASH][NOCE][KE][ID][ID]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Recv:[HASH][NOCEFy][INIT. CONTACT]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:38</td>
<td>Phase 1 IKE SA process done</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>Send:[ID][NOCTY][INIT. CONTACT][257E96EF]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>Recv:[ID][HASH]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:32</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>Send:[KE][NOCE][NATD][NATD]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>Recv:[KE][NOCE][NATD][NATD]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/18/2000 11:30:32</td>
<td>Send:[SA][VID][VID][VID]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:32</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:32</td>
<td>Recv:[SA][VID][VID][VID][VID][VID][257E96EF]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:32</td>
<td>The cookie pair is: 0x4f6CF65F2B4F800F7/0x3826ACFS5257E96EF 192.168.215.225 IKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/19/2000 11:30:32</td>
<td>Rule [Road Warrior] Receiving IKE request</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample IPSecuritas Log Output

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

```
IPSecuritas 3.0rc3 build 1609, Thu May 17 08:30:27 CEST 2007, nadig
Darwin 8.9.1 Darwin Kernel Version 8.9.1: Thu Feb 22 20:55:00 PST 2007; root:xnu-792.18.15-1/RELEASE_I386 i386
IPSecuritas Configuration Instructions
Zyxel ZyWALL

May 18, 22:50:20  Debug  APP  State change from IDLE to AUTHENTICATING after event START
May 18, 22:50:20  Info   APP  daemon started
May 18, 22:50:20  Info   APP  IPSec started
May 18, 22:50:20  Debug  APP  State change from AUTHENTICATING to RUNNING after event AUTHENTICATED
May 18, 22:50:20  Debug  APP  Received SADB message type X_SPDUPDATE - not interesting
May 18, 22:50:20  Debug  APP  Received SADB message type X_SPDUPDATE - not interesting
May 18, 22:50:20  Info   IKE  Foreground mode.
May 18, 22:50:20  Info   IKE  @(#)This product linked OpenSSL 0.9.7l 28 Sep 2006 (http://www.openssl.org/)
May 18, 22:50:20  Info   IKE  Reading configuration from "/Library/Application Support/Lobotomo Software/IPSecuritas/racoon.conf"
May 18, 22:50:20  Info   IKE  Resize address pool from 0 to 255
May 18, 22:50:20  Info   IKE  lifetime = 480
May 18, 22:50:20  Info   IKE  lifebyte = 0
May 18, 22:50:20  Info   IKE  encklen=0
May 18, 22:50:20  Info   IKE  p:1 t:1
May 18, 22:50:20  Info   IKE  DES-(BC)(1)
May 18, 22:50:20  Info   IKE  MD5(1)
May 18, 22:50:20  Info   IKE  768-bit MODP group(1)
May 18, 22:50:20  Info   IKE  pre-shared key(1)
May 18, 22:50:20  Info   IKE  compression algorithm can not be checked because sadb message doesn't support it.
May 18, 22:50:20  Info   IKE  parse succeeded.
May 18, 22:50:20  Info   IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon management.
May 18, 22:50:20  Info   IKE  192.168.215.2[14500] used as isakmp port (fd=7)
May 18, 22:50:20  Info   IKE  192.168.215.2[500] used as isakmp port (fd=8)
May 18, 22:50:20  Info   IKE  get pfkey X_SPDMPDU message
May 18, 22:50:20  Info   IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon management.
May 18, 22:50:20  Info   IKE  192.168.215.2[14500] used as isakmp port (fd=7)
May 18, 22:50:20  Info   IKE  get pfkey X_SPDMPDU message
May 18, 22:50:20  Info   IKE  open /Library/Application Support/Lobotomo Software/IPSecuritas/admin.sock as racoon management.
May 18, 22:50:20  Info   IKE  get pfkey X_SPDMPDU message
May 18, 22:50:20  Info   IKE  get pfkey X_SPDMPDU message
```

9
May 18, 22:50:21  Debug  IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug  IKE  SKEYID computed:
May 18, 22:50:21  Debug  IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug  IKE  SKEYID_d computed:
May 18, 22:50:21  Debug  IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug  IKE  SKEYID_a computed:
May 18, 22:50:21  Debug  IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug  IKE  SKEYID_e computed:
May 18, 22:50:21  Debug  IKE  encryption(des)
May 18, 22:50:21  Debug  IKE  hash(md5)
May 18, 22:50:21  Debug  IKE  final encryption key computed:
May 18, 22:50:21  Debug  IKE  hash(md5)
May 18, 22:50:21  Debug  IKE  IV computed:
May 18, 22:50:21  Debug  IKE  use ID type of FQDN
May 18, 22:50:21  Debug  IKE  HASH with:
May 18, 22:50:21  Debug  IKE  HASH (init) computed:
May 18, 22:50:21  Debug  IKE  add payload of len 9, next type 8
May 18, 22:50:21  Debug  IKE  add payload of len 16, next type 0
May 18, 22:50:21  Debug  IKE  begin encryption.
May 18, 22:50:21  Debug  IKE  encryption(des)
May 18, 22:50:21  Debug  IKE  pad length = 7
May 18, 22:50:21  Debug  IKE  encrypted payload by IV:
May 18, 22:50:21  Debug  IKE  encrypted payload, but not trimed.
May 18, 22:50:21  Debug  IKE  send phase1 packet 8f1739363f9f346:113cfbdadfd274e
May 18, 22:50:21  Debug  IKE  resend phase1 packet 8f1739363f9f346:113cfbdadfd274e
May 18, 22:50:21  Debug  IKE  sockname 192.168.215.2[500]
May 18, 22:50:21  Debug  IKE  send packet from 192.168.215.2[500]
May 18, 22:50:21  Debug  IKE  send packet to 192.168.215.225[500]
May 18, 22:50:21  Debug  IKE  1 times of 68 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:21  Debug  IKE  encrypted payload by IV:
May 18, 22:50:21  Debug  IKE  decrypted payload by IV:
May 18, 22:50:21  Debug  IKE  decrypted payload, but not trimmed.
May 18, 22:50:21  Debug  IKE  padding len=169

IPSecuritas Configuration Instructions
Zyxel ZyWALL
IPSecuritas Configuration Instructions
Zyxel ZyWALL

May 18, 22:50:21  Debug    IKE  skip to trim padding.
May 18, 22:50:21  Debug    IKE  decrypted.
May 18, 22:50:21  Debug    IKE  8f173936 3f9f3466 113cf0dd dbf2d7ae 05100201 00000000 0000003c 0800000c
May 18, 22:50:21  Debug    IKE  begin.
May 18, 22:50:21  Debug    IKE  seen nptype=5(id)
May 18, 22:50:21  Debug    IKE  seen nptype=8(hash)
May 18, 22:50:21  Debug    IKE  succeed.
May 18, 22:50:21  Debug    IKE  HASH received:
May 18, 22:50:21  Debug    IKE  HASH with:
May 18, 22:50:21  Debug    IKE  hmac(hmac_md5)
May 18, 22:50:21  Debug    IKE  HASH (init) computed:
May 18, 22:50:21  Debug    IKE  HASH for PSK validated.
May 18, 22:50:21  Debug    IKE  ===> 
May 18, 22:50:21  Debug    IKE  compute IV for phase2
May 18, 22:50:21  Debug    IKE  phase1 last IV:
May 18, 22:50:21  Debug    IKE  hash(md5)
May 18, 22:50:21  Debug    IKE  encryption(des)
May 18, 22:50:21  Debug    IKE  phase2 IV computed:
May 18, 22:50:21  Debug    IKE  encrypt payload by IV:
May 18, 22:50:21  Debug    IKE  save IV for next:
May 18, 22:50:21  Debug    IKE  encrypted.
May 18, 22:50:21  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:21  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:21  Debug    IKE  7bc939e7 2964cfa6
May 18, 22:50:21  Debug    IKE  7bc939e7 2964cfa6
May 18, 22:50:21  Debug    IKE  7bc939e7 2964cfa6
May 18, 22:50:21  Debug    IKE  ===> 
May 18, 22:50:22  Debug    IKE  begin QUICK mode.
May 18, 22:50:22  Debug    IKE  send packet from 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  send packet to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  1 times of 84 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:22  Debug    IKE  sockname 192.168.215.2[500]
May 18, 22:50:22  Debug    IKE  msg 16 not interesting
May 18, 22:50:22 Debug IKE 800201e0 80040001 80050002 80030001
May 18, 22:50:22 Debug IKE begin.
May 18, 22:50:22 Debug IKE seen nptype=2(prop)
May 18, 22:50:22 Debug IKE succeed.
May 18, 22:50:22 Debug IKE proposal #1 len=40
May 18, 22:50:22 Debug IKE begin.
May 18, 22:50:22 Debug IKE seen nptype=3(trns)
May 18, 22:50:22 Debug IKE succeed.
May 18, 22:50:22 Debug IKE transform #1 len=28
May 18, 22:50:22 Debug IKE type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:22 Debug IKE type=SA Life Duration, flag=0x8000, lorv=480
May 18, 22:50:22 Debug IKE life duration was in TLV.
May 18, 22:50:22 Debug IKE type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:50:22 Debug IKE type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 18, 22:50:22 Debug IKE hmac(modp768)
May 18, 22:50:22 Debug IKE pair 1:
May 18, 22:50:22 Debug IKE 0x30a5c0: next=0x0 tnext=0x0
May 18, 22:50:22 Debug IKE proposal #1: 1 transform
May 18, 22:50:22 Debug IKE total SA len=52
May 18, 22:50:22 Debug IKE 00000001 00000001 0000002c 01030401 5d652259 00000020 01030000 80030001
May 18, 22:50:22 Debug IKE 80010001 00020004 000001e0 80040001 80050002
May 18, 22:50:22 Debug IKE begin.
May 18, 22:50:22 Debug IKE seen nptype=2(prop)
May 18, 22:50:22 Debug IKE succeed.
May 18, 22:50:22 Debug IKE proposal #1 len=44
May 18, 22:50:22 Debug IKE begin.
May 18, 22:50:22 Debug IKE seen nptype=3(trns)
May 18, 22:50:22 Debug IKE succeed.
May 18, 22:50:22 Debug IKE transform #1 len=32
May 18, 22:50:22 Debug IKE type=Group Description, flag=0x8000, lorv=1
May 18, 22:50:22 Debug IKE hmac(modp768)
May 18, 22:50:22 Debug IKE type=SA Life Type, flag=0x8000, lorv=seconds
May 18, 22:50:22 Debug IKE type=SA Life Duration, flag=0x8000, lorv=4
May 18, 22:50:22 Debug IKE type=Encryption Mode, flag=0x8000, lorv=Tunnel
May 18, 22:50:22 Debug IKE type=Authentication Algorithm, flag=0x8000, lorv=hmac-sha
May 18, 22:50:22 Debug IKE peer's single bundle:
May 18, 22:50:22 Debug IKE (proto_id=ESP spisize=4 spi=5d652259 spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:50:22 Debug IKE (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:50:22 Debug IKE my single bundle:
May 18, 22:50:22 Debug IKE (proto_id=ESP spisize=4 spi=079d6fea spi_p=00000000 encmode=Tunnel reqid=0:0)
May 18, 22:50:22 Debug IKE (trns_id=3DES encklen=0 authtype=hmac-sha)
May 18, 22:50:22 Debug IKE matched
May 18, 22:50:22 Debug IKE begin compare proposals.
May 18, 22:50:22 Debug IKE pair[1]: 0x30e590
May 18, 22:50:22 Debug IKE 0x30e590: next=4x0 tnext=4x0
May 18, 22:50:22 Debug IKE proposal #1: 1 transform
May 18, 22:50:22 Debug IKE Warning IKE attribute has been modified.
May 18, 22:50:22 Debug IKE begin compare proposals.
May 18, 22:50:22 Debug IKE pair[1]: 0x30e590
May 18, 22:50:22 Debug IKE 0x30e590: next=4x0 tnext=4x0
May 18, 22:50:22 Debug IKE proposal #1: 1 transform
IPSecuritas Configuration Instructions

Zyxel ZyWALL

---

May 18, 22:50:22 Debug IKE save IV for next:
May 18, 22:50:22 Debug IKE c1020bd8 2dae21dd
May 18, 22:50:22 Debug IKE encrypted.
May 18, 22:50:22 Debug IKE send packet from 192.168.215.2[500]
May 18, 22:50:22 Debug IKE send packet to 192.168.215.225[500]
May 18, 22:50:22 Debug IKE 1 times of 52 bytes message will be sent to 192.168.215.225[500]
May 18, 22:50:22 Debug IKE 8f173936 3f9f3466 113cf0dd d0fd274e 08102001 daec08f0 00000034 98c48fbf
May 18, 22:50:22 Debug IKE c219c775 ac2079f3 d0e8eb10 45814171 418e9e03 de05f6d1 6cf859bd 5ca88702
May 18, 22:50:22 Debug IKE compute DH's shared.
May 18, 22:50:22 Debug IKE 18017732 d4093f47 866dac68 c58ac9f2 6bb9dfa2 fd47dd57 19c652f9 b8b21b26
May 18, 22:50:22 Debug IKE c219c775 ac2079f3 d0e8eb10 45814171 418e9e03 6cf859bd 5ca88702
May 18, 22:50:22 Debug IKE KEYMAT compute with
May 18, 22:50:22 Debug IKE 03079d6f eaf3b8c8 6faaf09b cc4234f5 346dfe42 d8d23002 3fa99a2a 256863b7
May 18, 22:50:22 Debug IKE hmac(hmac_md5)
May 18, 22:50:22 Debug IKE encryption(3des)
May 18, 22:50:22 Debug IKE hmac(hmac_sha1)
May 18, 22:50:22 Debug IKE generating K1...K4 for KEYMAT.
May 18, 22:50:22 Debug IKE hmac(hmac_md5)
May 18, 22:50:22 Debug IKE hmac(hmac_md5)
May 18, 22:50:22 Debug IKE 6a723ebd 86ba4878 df7bf22d 8680e991 4a945337 7dafe7be 15cc66f0 0903f36b
May 18, 22:50:22 Debug IKE 60f97cbd a20e7978 4ff3b5d5 052c2ec1 139c9028 904aaa37 d4a00da0 dd69d8e9
May 18, 22:50:22 Debug IKE KEYMAT computed.
May 18, 22:50:22 Debug IKE call pk_sendupdate
May 18, 22:50:22 Debug IKE hmac(hmac_md5)
May 18, 22:50:22 Debug IKE call pfkey_send_update_nat
May 18, 22:50:22 Debug IKE Received SADB message type UPDATE, 192.168.215.225 [0] -> 192.168.215.2 [0]
May 18, 22:50:22 Debug IKE SA change detected
May 18, 22:50:22 Debug IKE pfkey add sent.
May 18, 22:50:22 Debug IKE get pfkey UPDATE message
May 18, 22:50:22 Debug IKE 02020003 14000000 d5010000 ee180000 02000100 079d6fe0 04000202 00000000
May 18, 22:50:22 Debug IKE 02001300 02000000 00000000 00000000 03000500 f2000000 10000000 c0ab0ed7e1
May 18, 22:50:22 Debug IKE 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
May 18, 22:50:22 Debug IKE 04000040 00000000 00000000 00000000 00000000 00000000 00000000 00000000

---


---


---

May 18, 22:50:22 Info IKE ----
May 18, 22:50:22  Debug    IKE  get pfkey ADD message
May 18, 22:50:22  Debug    IKE  02030003 14000000 ee180000 02000100 5d652259 04000202 00000000
May 18, 22:50:22  Debug    IKE  02001300 02000000 00000000 00000000 03000500 ff200000 10020000 c0a8d7e1 00000000 00000000
May 18, 22:50:22  Debug    IKE  00000000 00000000 03000600 ff200000 10020000 c0a8d7e1 00000000 00000000
May 18, 22:50:22  Debug    IKE  04000300 00000000 00000000 00000000 e0010000 00000000 00000000 00000000
May 18, 22:50:22  Debug    IKE  04000400 00000000 00000000 00000000 80010000 00000000 00000000 00000000
May 18, 22:50:22  Info     IKE  IPsec-SA established: ESP/Tunnel 192.168.215.2[0]->192.168.215.225[0]
                      spi=1566909017(0x5d652259)
May 18, 22:50:22  Debug    IKE  ---