

# Central Policy Manager Reference Guide

---

Central Policy Manager 4.1



---

## Notice to Users

---

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

## Copyright, Trademark, and Patent Information

---

Copyright© 1998 - 2002 WatchGuard Technologies, Inc. All rights reserved.

Firebox, Firebox 1000, Firebox 2500, Firebox 4500, Firebox II, Firebox II Plus, Firebox II FastVPN, Firebox III, Firebox SOHO, Firebox SOHO|tc, Firebox V100, Firebox V80, Firebox V60, Firebox V10, LiveSecurity, RapidStream, RapidCore, WatchGuard, WatchGuard Technologies, Inc., AppLock, AppLock/Web, Designing peace of mind, DVCP technology, Enforcer/MUVPN, FireChip, HackAdmin, HostWatch, LockSolid, RapidCare, SchoolMate, ServerLock, ServiceWatch, Smart Security, Simply Done., SpamScreen, Vcontroller are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"  
THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.  
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"  
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

The mod\_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod\_ssl project (<http://www.modssl.org/>)."

4. The names "mod\_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod\_ssl" nor may "mod\_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod\_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

---

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Part No: Online Only

---

# Contents

---

<b>CHAPTER 1 Creating an IPSec Manual Key Policy</b>	<b>1</b>
Creating a New IPSec Manual Key Policy	1
<i>Entering the traffic specifications</i>	1
<i>Selecting the action</i>	2
<i>Making this policy bidirectional</i>	2
Creating a Custom IPSec Action	2
<i>Configuring ESP protocols</i>	4
<i>Configuring AH protocol</i>	5
<i>Completing this action</i>	5
<b>CHAPTER 2 Editing IKE Proposals and Pairs</b>	<b>7</b>
Selecting an Existing IKE Pair Setting	8
Creating a New IKE Proposal	9
<i>Entering a single transform</i>	11
<i>Entering more than one transform</i>	12
Changing the Authentication Process	14
<i>Using symmetric certificate matching rules</i>	15
<i>Using asymmetric certificate matching rules</i>	16
<i>Defining a custom preshared key</i>	17

---

<b>CHAPTER 3</b>	<b>Creating Policies for Multi-Tenant Virtual User Domains</b>	19
	Creating policies for VLAN tenants	20
	<i>The advantages of a VLAN</i>	21
	<i>Inserting VLAN tenant security policies</i>	21
	<i>Routing VLAN traffic through a WatchGuard appliance</i>	23
	<i>Important: Using a Firebox Vclass appliance in a VLAN setting</i>	25
	Creating policies for user-domain tenants	25
	<i>Inserting user domain tenant security policies</i>	25
	<i>Additional information</i>	26
	<i>An example of a user-domain policy in use</i>	26
	An overview of user-domain tenant authentication	27
	<i>Inserting user domain tenant security policies</i>	28
	How a user domain tenant makes a connection	28
	Activating the Firebox Vclass “authenticate with certificates” feature	28
	<i>Importing a VPN certificate into a user’s Web browser</i>	29
<b>CHAPTER 4</b>	<b>Defining Alarms</b>	31
	About Built-in Alarms	31
	About Probe Counters	31
	About Overriding Alarms	32
	Creating a New Alarm	33
	<i>Adding system probe counters</i>	35
	<i>Adding VPN peer probe counters</i>	37
	<i>Completing the alarm definition</i>	38
<b>CHAPTER 5</b>	<b>Setting up and Managing Log Files</b>	39
	Types of Logs	39
	Log Size and Rollover	40
	Viewing the CPM Log	41
	Viewing the Logs for Specific Appliances	41

---

Revising Log Settings for an Appliance .....	42
Managing a Large Number of Log Entries .....	43
<i>Changing the number of log entries per page</i> .....	43
<i>Filtering the contents of a log</i> .....	44
<i>Creating a cumulative set of filters</i> .....	45
Archiving Log Files .....	45
<b>CHAPTER 6 Maintaining Appliances</b> .....	<b>49</b>
About the Shortcut Menu .....	49
Remotely Restarting an Appliance .....	50
Remotely Shutting Down an Appliance .....	51
Restoring an Appliance to the Factory Default State ...	51
Archiving an Appliance's Profile as an XML File .....	52
Synchronizing an Appliance's Clock with CPM Server ..	52
<b>CHAPTER 7 Special Topics</b> .....	<b>53</b>
<i>Installing CPM Server on a Solaris host</i> .....	53
Backing up the CPM Database .....	54
Restoring an Archived CPM Server Database .....	55
<b>CHAPTER 8 Case Studies</b> .....	<b>59</b>
Case Study: Dynamic NAT Firewall Policy .....	59
<i>Policy ("dnat_access")</i> .....	59
Case Study: QoS Actions .....	60
<i>Example 1:</i> .....	60
<i>Example 2:</i> .....	61
Case Study: VLAN in WatchGuard appliances .....	62
Case Study: Tunnel Switching Between Remote Sites ..	63
<i>Adding a new site</i> .....	65
<b>APPENDIX 9 About the CPM Configuration Files</b> .....	<b>67</b>
CPM Server Config file .....	67
CPM Client Config file .....	70

---

Appendix 10 **A Catalog of Real-time Monitor Probe**  
**Counters** ..... 73

System Counters	..... 73
Aggregate counters for all VPN end-point pairs	..... 79
IPSec counters per VPN end-point pair	..... 80
Policy counters for all policies	..... 81
Policy counters per policy	..... 82

# Creating an IPSec Manual Key Policy

---

This chapter describes the process of creating a VPN policy that uses a manual key. Initially, you must create a set of manual key IPSec actions for use in your policies. Critical parts of these actions include the required security protocols, the preferred algorithms for each, the manual key text for use with each protocol, and the local and peer SPI values for the two appliances.

Note that manual key VPN policies cannot be applied to more than two appliances.

## Creating a New IPSec Manual Key Policy

---

To create a policy that establishes a bi-directional ,manual-key VPN connection between two appliances, follow these steps. You do not need to create a separate policy for each direction of data traffic. You can apply bidirectionality to a single unidirectional policy to activate traffic in both directions.

### Entering the traffic specifications

- 1 Create a new policy row.

- 2 Drag-and-drop an address entry that represents the private network of one of the two appliances into the **Source** cell.  
If you are creating a bidirectional VPN policy, you can drag either address entry into the Source or Destination cells.
- 3 Drag-and-drop the address entry representing the private network of the second appliance into the **Destination** cell.
- 4 If you don't want to use "ANY", drag-and-drop the relevant services from the **Services** tab into the policy row **Service** cell.

## Selecting the action

- 1 Open the **IPSec Action** tab and drag-and-drop the appropriate manual key action into the **Action** cell.  
CPM does not include any default manual-key IPSec actions. You must create these actions before creating manual key policies. For more information, see "Creating a Custom IPSec Action," below.
- 2 If necessary, open the **Schedule** tab and drag a schedule entry into the **Schedule** cell.  
If the Schedule cell does not appear in the policy row, select View => Show Columns => Schedule.

## Making this policy bidirectional

- 1 Reopen the **Policies** tab, if it is not visible.
- 2 In the newly created policy, right-click the newly added IPSec action, or the **Action** cell.
- 3 Select **Bi-Directional** to apply bidirectionality to this IPSec action and the policy.

## Creating a Custom IPSec Action

---

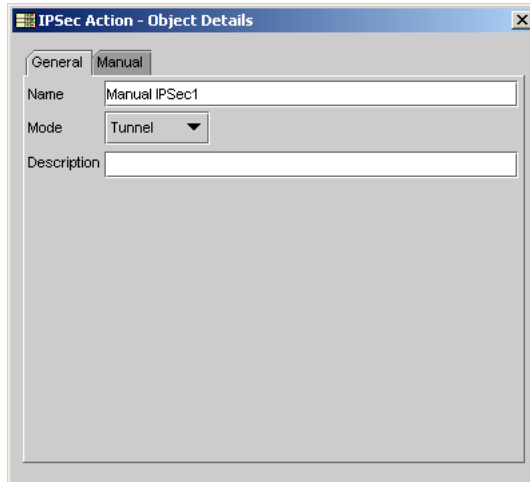
If you find the default IPSec actions insufficient for your particular network requirements, you can create and customize your own IPSec action. These actions are usable in as many policies as you want to apply them to:

- 1 Click the Configuration Editor window's **IPSec Action** tab.

- Click the Create a New Object icon (shown at right) and select **New Manual IPsec** from the menu.



The IPsec Action dialog box appears, with its features distributed into two tabs: General and Manual.

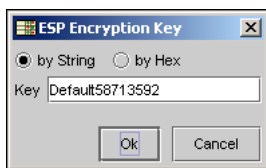


- In the **General** tab (open by default) in the **Name** field, type a name for this new action.  
The name can consist of numbers, letters, hyphens (-), and underscore (\_) characters.
- From the **Mode** menu, select either **Tunnel** or **Transport**.  
If you select **Tunnel**, this policy prompts the Firebox Vclass appliance to hide any information about the original sender of data. This option is preferred for site-to-site connections, in which the traffic goes through the Firebox Vclass appliance.  
If you select **Transport**, no additional identity masking is applied. This option is recommended for use in secured communication directed to either Firebox Vclass appliance, such as SNMP traffic.
- Click the **Manual** tab.
- In both **Local SPI** and **Peer SPI** fields, type a different unique number (between 256 and 65535) in each field.  
The Local SPI entry is used to identify the key stored in the source security appliance, while the Peer SPI entry identifies the key used by the destination appliance. If you are activating bidirectionality, you can enter the numbers arbitrarily, in either field.

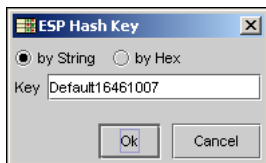
- 7 If you want to type the key text in hexadecimal notation, select the checkbox marked **use Hex**.

## Configuring ESP protocols

- 1 From the **ESP Encrypt Alg** menu, select the option you want.
- 2 Click **Enter Key**.  
The ESP Encryption Key dialog box appears, listing a default key composed of a randomly generated series of numbers.



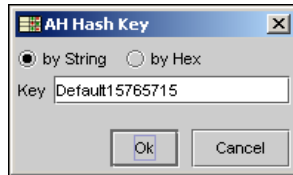
- 3 If you want to type the key text in hexadecimal notation, click **by Hex**.
- 4 In the **Key** field, enter the key.  
You can accept the default, CPM-generated key text by clicking OK.
- 5 Click **OK** to save the new key entry and close the **ESP Encryption Key** dialog box.
- 6 When the **Select IPSec** dialog box's Manual tab reappears, open the **ESP Hash Alg** menu and select the option you want.
- 7 Click **Enter Key** (to the right of the ESP Hash Alg menu.)  
The ESP Hash Key dialog box appears, listing a default key that incorporates a randomly generated series of numbers.



- 8 If you want to type the key text in hexadecimal notation, click **by Hex**.
- 9 In the **Key** field, enter the key.  
You can accept the default, CPM-generated key text by clicking OK.
- 10 Click **OK** to save the key entry and close this dialog box.

## Configuring AH protocol

- 1 Click the **Authentication Protocol** checkbox.
- 2 Open the **Hash Alg** menu and select the option you want.
- 3 Click **Enter Key** (to the right of the AH Hash Alg menu.)  
The AH Hash Key dialog box appears, listing a default key that incorporates a randomly generated series of numbers.



- 4 If you want to type the key text in hexadecimal notation, click **by Hex**.
- 5 In the **Key** field, enter the text of the key.  
You can accept the default, CPM-generated key text by clicking OK.
- 6 Click **OK** to save the key entry.  
The IPSec Action dialog box reappears.

## Completing this action

You can now save your new action entries and then select this action for use in the policy.

- 1 To save your manual IPSec action entries, click **OK**.
- 2 You can now add this action to any new or existing policies.



# Editing IKE Proposals and Pairs

---

Every time an automatic key IPsec action is applied to a policy, CPM automatically generates an IKE proposal that is used by the security appliances affected by that policy. The default IKE proposals will meet the majority of your needs. However, you can use CPM to customize an existing proposal or create a new proposal. This is especially useful if you are establishing VPN tunnels between a Firebox Vclass appliance and a “foreign” appliance that has its own internal proposal structure.

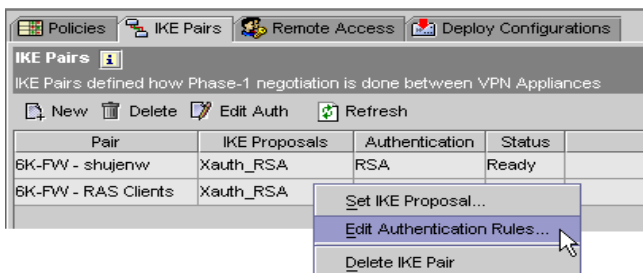
You can also review and modify the settings for both existing IKE pairs that are used in automatic key IKE exchanges.

Before you can select or revise the IKE proposals for a specific pair of peers, the following conditions must be in effect:

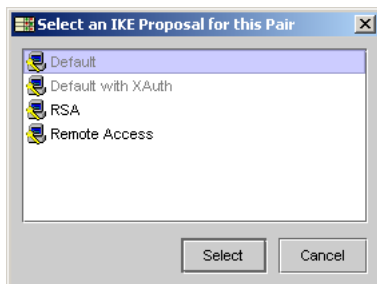
- Each peer security appliance must be listed in the Configuration Editor window and currently visible to CPM by a live connection.
- All relevant pairings of security appliances (“peers”) must be recorded in CPM as peer pairs in the Configuration Editor window IKE Pairs tab.
- If third-party authentication is to be used, the certificates must have already been imported to the security appliances.

## Selecting an Existing IKE Pair Setting

- 1 From the Configuration Editor window, click the **IKE Pairs** tab.  
The IKE Pairs tab appears, listing all of the existing VPN/IKE pairs of security appliances.



- 2 Select the pair that you want to review and edit. Right-click the row containing the pair you want to edit to open the action menu.
- 3 Select **Set IKE Proposal**.  
The Select IKE Proposal dialog box appears.



When selecting an existing IKE pair setting, you can choose from one of four basic IKE proposals:

### *Default*

This proposal uses the main mode, with a preshared key and the following settings: 3DES-MD5, DH group 1, SA lifetime of 10 hours.

***Default with XAuth***

This proposal uses the main mode with extended authentication, RSA signature, 3DES-MD5, DH group 1, and an SA lifetime of 10 hours.

***RSA***

This proposal uses the main mode, an RSA signature, 3DES-MD5, DH group 2, and an SA lifetime of 8 hours.

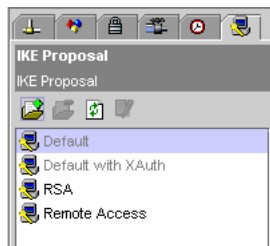
***Remote Access***

This proposal (for remote access use) uses the main mode with extended authentication, RSA signature, 3DES-MD5, DH group 2, and an SA lifetime of 8 hours.

- 4 Select an existing proposal and click **Select** to link it to the pair.

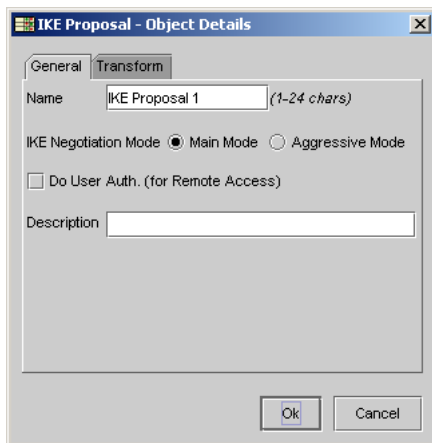
## Creating a New IKE Proposal

- 1 Click the **IKE Proposal** tab.



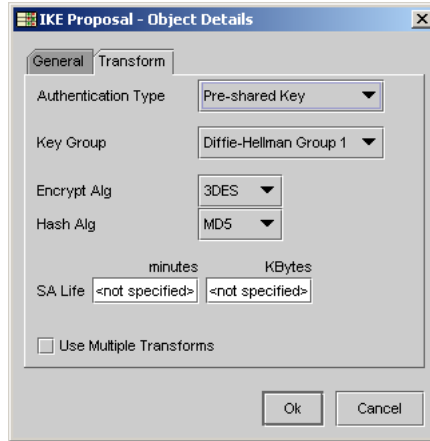
- 2 In the tab header, click the Create a New Object button (shown at right).

The IKE Proposal dialog box appears



- 3 In the **Name** field, type a name for the proposal.
- 4 Click **Main Mode** or **Aggressive Mode**.  
If you choose "Aggressive", this action can include only one IKE proposal and related transform. "Main" is recommended as it provides more flexibility and security.
- 5 If this proposal is for use in RAS VPN connections, click to select the **Do User Auth** checkbox. (You can only use Main mode if this option is selected.)
- 6 (Optional) In the **Description** box, type a description of this proposal.

- Click the **Transform** tab.



## Entering a single transform

You can create a single transform for the new IKE proposal you created. You can also create and add any number of transforms if you chose the Main mode in the General tab. If you chose the Aggressive mode, your proposal is restricted to a single transform.

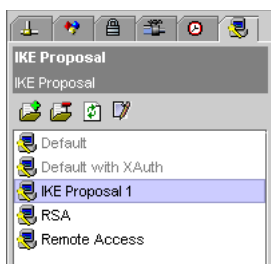
Use the following procedure to create a single transform:

- From the **Authentication Type** menu, select the appropriate option:
  - RSA Signature***  
If you have an RSA certificate, select this option.
  - DSS Signature***  
If you have a DSS certificate, select this option.
  - Pre-shared Key***  
If you want to use a pre-shared secret key, select this option.
- From the **Key Group** menu, select the appropriate DH group option. DH (Diffie-Hellman) groups consist of key agreements that enable two peer systems who have no prior knowledge of one another to publicly exchange and agree on a shared secret key.
- From the **Encrypt Alg** menu, select the appropriate encryption algorithm.
- From the **Hash Alg** menu, select the appropriate hashing algorithm.

- 5 Make any required changes to the **SA Life** values. The **Seconds** field represents the amount of time you want a given transform to be active. This establishes the duration of protection for phase two negotiations.

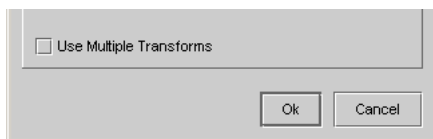
To set the maximum size in kilobytes of all key negotiation packets transmitted during phase two negotiations, click the **Kbytes** field and type the value you want.

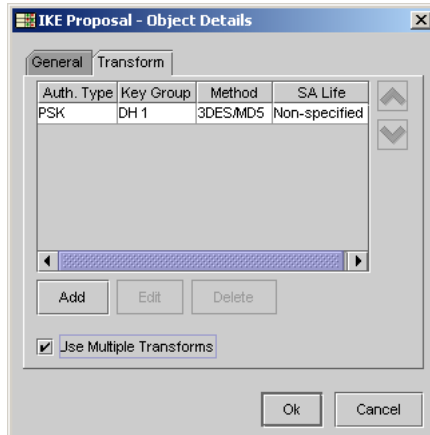
- 6 Click **OK** to save this transform and apply it to this proposal.
- 7 Select your newly saved proposal name in the list and click **Select**.  
The New IKE Proposals window closes and the newly recorded IKE proposal name appears in the tab, as shown here.



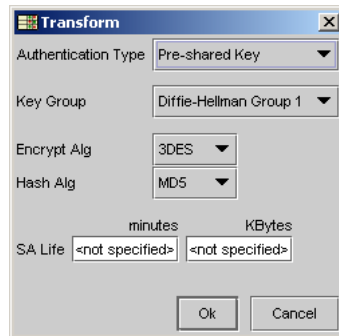
## Entering more than one transform

- 1 Click the **Use Multiple Transforms** checkbox in the Transforms tab.



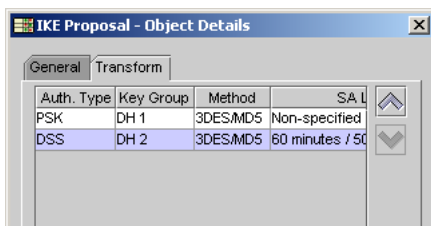


- To add another transform to this list, click **Add**. The Transform dialog box appears.



- From the **Authentication Type** menu, select the appropriate option:
  - RSA Signature***  
If you have an RSA certificate, select this option.
  - DSS Signature***  
If you have a DSS certificate, select this option.
  - Pre-shared Key***  
If you want to use a pre-shared secret key, select this option.

- 4 From the **Key Group** menu, select either DH group option.  
DH (Diffie-Hellman) groups consist of key agreements that enable two peer systems who have no prior knowledge of one another to publicly exchange and agree on a shared secret key.
- 5 From the **Encrypt Alg** and **Hash Alg** menus, select the appropriate options.
- 6 Make any required changes to the **SA Life** values. The **Seconds** field represents the amount of time you want a given transform to be active. This establishes the duration of protection for phase two negotiations.  
The **KBytes** field establishes the maximum size in kilobytes of all key negotiation packets transmitted during phase two negotiations.
- 7 Click **OK** to save this transform and apply it to this proposal.  
The Transform dialog box closes, and the new transform appears at the top of the Transform tab list.



- 8 To add another transform, repeat steps 2–7.
- 9 If you want to change the preference order, click a transform entry and click the arrow buttons to the right to move it to the proper location in this list.

## Changing the Authentication Process

---

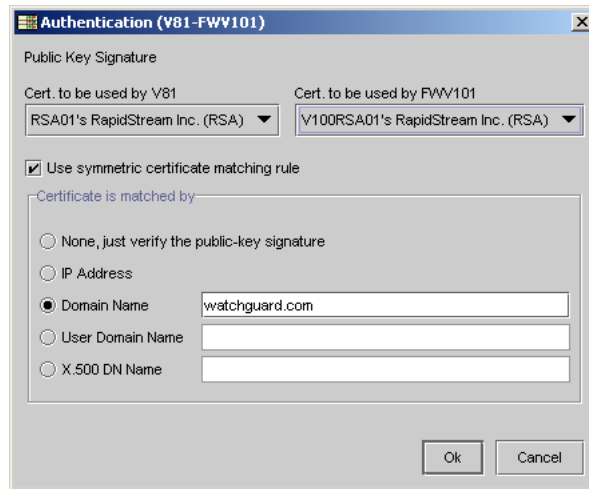
If you create a new proposal that uses either RSA or DSS signatures for authentication, you must replace the default authentication settings with the certificates used by each appliance:

- 1 Open the IKE Pairs window, and right-click the row of the peer pair.
- 2 When the action menu appears, select **Edit Authentication Rules**.  
The Authentication dialog box appears.

**NOTE**

If you have not yet established a connection to the specific peer appliances, CPM displays a dialog box informing you that it cannot connect to the device (to obtain certificate information). You must pause your work at this point and use CPM to connect to that appliance, after which you can continue with this process.

- 3 Use this dialog box to choose the following:



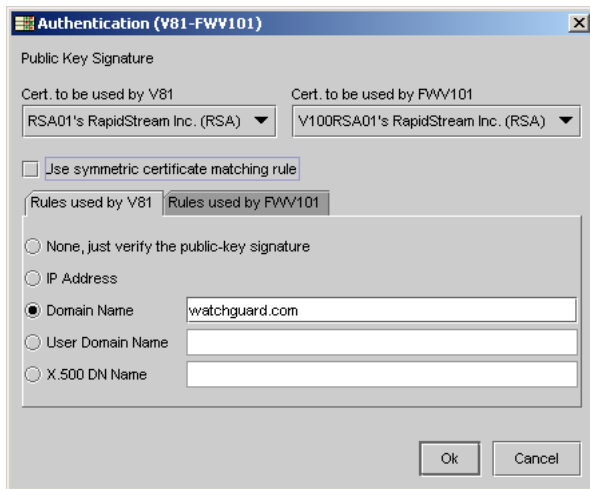
- Which certificate is to be used (if more than one is associated with a security appliance)
  - Which ID type and specific ID values the appliances will need to exchange to establish authentication.
- 4 Use both **Cert to use** menus to select appropriate certificates for each appliance.

### Using symmetric certificate matching rules

- 1 Click the buttons by each of the **Certificate is matched by** options to activate them.
- 2 Type the relevant identification text by all the options that require them.

## Using asymmetric certificate matching rules

- 1 Click to clear the **Use symmetric certificate matching rule** if you want to establish unique ID types and values for each appliance.  
A new set of Rules used by features appear, divided into appliance-specific tabbed workspaces.

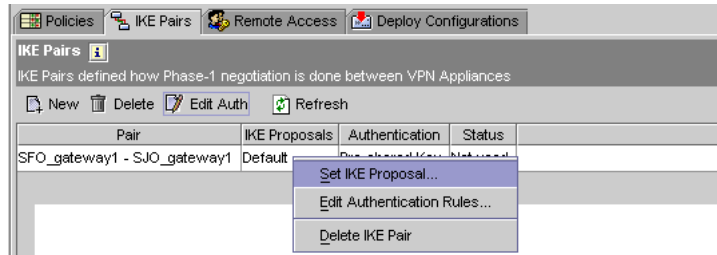


- 2 Click on each appliance tab and make the appropriate ID type choices and value entries.

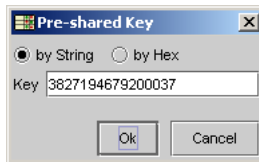
## Defining a custom preshared key

Every new IKE pair entry is automatically assigned a randomly generated preshared key for use in authentication. You can replace the randomly assigned secret key text with your own text:

- 1 Select any IKE peer pair using “PSK” and click **Edit Proposals**. Or, right-click the peer pair row and select **Edit Authentication Rules**. The Authentication/PSK dialog box appears.



- 2 Click **Edit Key**. The Pre-shared Key dialog box appears.



- 3 Click the button by the text entry method of your preference: **by String** or **By Hex**.
- 4 In the **Key** text field, type the pre-shared key.
- 5 Click **OK** to save your key entry.
- 6 When the **Authentication** dialog box reappears, click **OK** to save this PSK proposal.



# Creating Policies for Multi-Tenant Virtual User Domains

---

CPM can be used to manage traffic in a multiple-tenant network environment. The tenants are represented on CPM as a virtual appliance, which are created in the Configuration Editor. These virtual appliances (and the attending network addresses) allow you to create security policies, to manage domains that are either based on an actual VLAN (with hardware) or a user domain.

**About VLANs:** If, for example, you are an ISP, you'll want to segregate your customer (tenant) assets into separate VLANs. This provides a secured environment for your tenants in your network as all network traffic between different VLAN's are managed by VLAN switches.

All Firebox Vclass security appliances support IEEE 802.1q VLAN packets, thus allowing network administrator to create separate policies for each tenant utilizing a single shared security appliance. This effectively reduces the cost of providing firewall and VPN services to all tenants.

---

## NOTE

If you have RapidStream security appliances, they can be used to manage multiple-tenant domains, provided you have upgraded them to the RapidStream operating system version 3.2. Contact WatchGuard Support and ask for "Vclass 3.2 SP1". Any RapidStream appliances

running older operating system software cannot be used to manage such traffic.

---

**About User Domains:** In addition to VLAN-type tenants, all Vclass security appliances allow administrators to apply security policies to VLAN-like tenants in a non-VLAN environment. This type of tenancy is called a *User Domain*. By logging on and presenting user ID, password, and domain name to a Vclass security appliance, an end user can access the Internet or utilize VPN policies defined for their specified domain. Creating user-domain tenant policies is an easy way to achieve multi-tenant application without the need for VLAN hardware. This is especially useful when tenants cannot be distinguished by different IP subnets.

This chapter discusses the two types of tenants and how they can be defined and used in creating multi-tenant policies.

- 1: Creating policies for VLAN tenants” on page 20
- 2: Creating policies for User Domain tenants” on page 25

## Creating policies for VLAN tenants

---

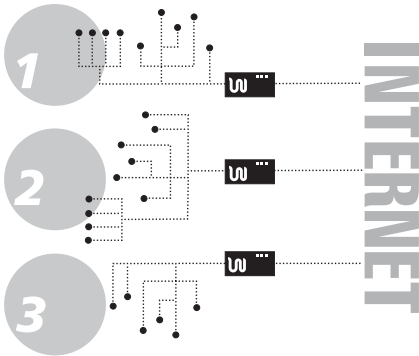
Virtual LAN (referred to as *VLAN*) has become increasingly popular for both corporate networks and service providers, as a way of partitioning their network into discreet regions or a way of segregating a range of separate users who need to remain discreet from one another.

- For the corporate network administrator, a VLAN allows the quick and efficient partitioning of an ever-growing local area network.
- For service providers, a VLAN can be used to segregate traffic from different customers.

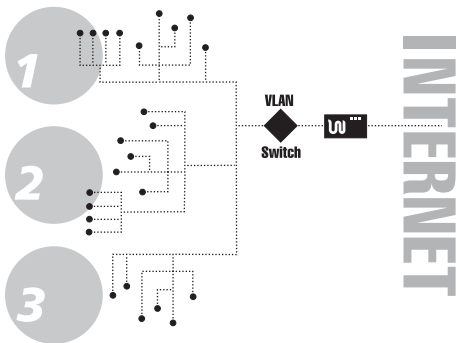
Both RapidStream appliances (running v3.2 software) and Firebox Vclass security appliances permit you to use VLAN tags or IDs as part of the traffic specification in a policy, so that your appliance can route traffic to and from a VLAN segment by means of a VLAN switch. This permits bi-directional traffic from the VLAN segment to other segments, network regions or to the Internet.

## The advantages of a VLAN

To show an example of an effective VLAN implementation, an IT administrator creates three discreet network regions, each with its own firewall gateway appliance, as shown here



By using a single security appliance and a VLAN switch, the administrator could partition the network in the same way, but with much less cost (and effort), as shown here.



## Inserting VLAN tenant security policies

To assist network administrators in creating security policies for use in a VLAN-enabled environment, CPM allows definitions of virtual appliances and any related network addresses, which can be used as part of the traffic specification in security policies. Each virtual appliance is assigned

the VLAN ID of a tenant, and the corresponding address entry allows you to direct traffic for that tenant to the designated network assets.

To add a virtual appliance:

- 1 Determine which gateway appliance the specific tenant virtual appliance should be associated with.



- 2 Create the needed virtual appliance for each "VLAN" tenant, as noted in \*\*"Creating a new "virtual" appliance record" on page 133. You need specify the VLAN ID. You should also assign an IP address so a virtual interface will be created so the appliance will appear to be attached to the corresponding vlan.



- 3 Right-click the virtual appliance and choose "New Address" from the shortcut menu.
- 4 Use the resulting dialog box to enter the IP address of the tenant-specific network asset.



- 5 It could be a single address, a range of IP addresses, or a subnet.
- 6 Repeat this address-entry process as needed to insert other distinct network asset addresses.

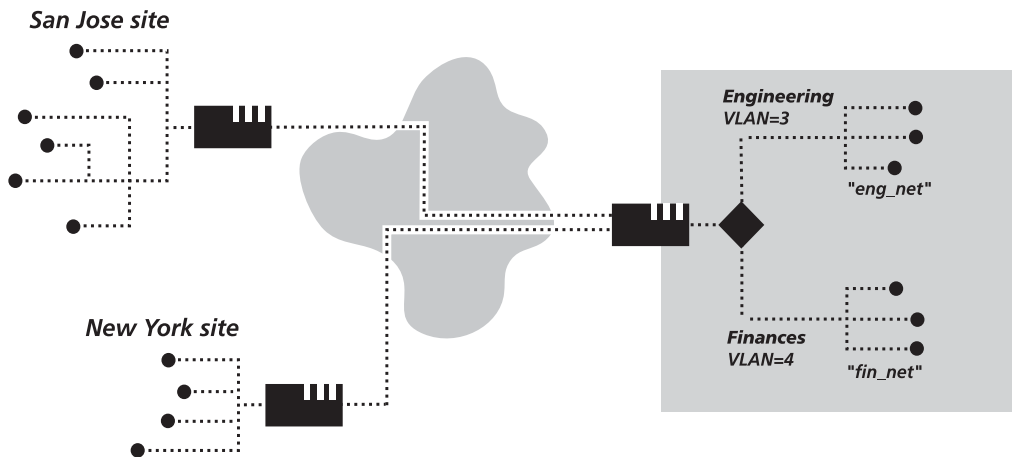
- When the virtual appliance and addresses are ready, you can now drag-and-drop these address entries as Source or Destination, when creating or editing security policies.

## Routing VLAN traffic through a WatchGuard appliance

The following is an example of how to route VLAN traffic through a WatchGuard appliance.

### Example

Assume that there are two VLAN's in one site's private network; one is for the Engineering department (with VLAN id = 3), and the other is for the Finance department (with VLAN id = 4).

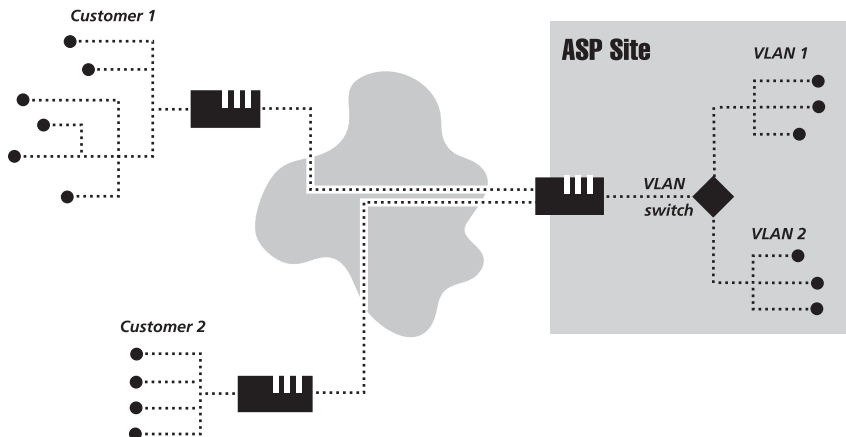


A network administrator can create two VLAN virtual appliances in CPM, one for each department, then create security policies similar to the following:

Source	Destination	Service	Action
Eng_net@MainGateway	SanJose_net@SanJose	ANY	<->ipsec
Fin_net@MainGateway	NewYork_net@NewYork	ANY	<->ipsec

In the above example, the first policy is a bidirectional VPN policy between the San Jose site and the engineering department network, the second policy is a bidirectional VPN policy between the New York site and the finance department network.

Another application of a Firebox Vclass appliance's VLAN capability is to assist an ASP or ISP to set up a multi-tenant secured VLAN, as shown in the following illustration. This example shows how a single appliance and switch can be combined at the ASP site.



Each of the separate customers (also using a Firebox Vclass appliance) can connect to the ASP site via VPN tunnels established between Firebox Vclass appliances. Directed by the policy defined on the ASP's Firebox Vclass appliance, each customer's traffic will be tagged with the correct VLAN ID, then sent to the correct VLAN.

---

**NOTE**

**IMPORTANT:** Firebox Vclass appliances will not attach a VLAN tag to data sent through a VPN tunnel to another appliance. Therefore, that site's network does not have to be VLAN-enabled.

---

---

**NOTE**

The current line of Firebox Vclass appliances recognize VLAN/802.1Q headers in data streams. for routing purposes.

---

## Important: Using a Firebox Vclass appliance in a VLAN setting

If your SNMP management stations, DNS servers, OSPF routers, RADIUS servers, and mail servers are located in a VLAN-enabled network, you need to explicitly define separate policies that allow Firebox Vclass appliances to send traffic to those devices. Otherwise, some Firebox Vclass features will not work; for example, SNMP trap notification, DNS lookup, etc. Here is an example of a policy that would allow SNMP traps sent from a Firebox Vclass security appliance to a SNMP management station in VLAN 20.

```

└ABC (appliance)
├ABC_VA (virtual appliance, VLAN id=20, private)
├SNMP_STATION (address, ip <ip of the SNMP station>)
└Private-ABC (address, interface-0, private)

```

Source	Destination	Service	Actions
!Private-ABC@ABC	SNMP_STATION@ABC	SNMP trap	Pass

## Creating policies for user-domain tenants

In addition to VLAN tenant-specific policies, CPM also permits you to set up *user domain*-specific policies, which enables a security appliance to perform traffic management for multi-tenant domains without the attendant VLAN hardware.

### Inserting user domain tenant security policies

- 1 Create the needed virtual appliance for each "User Domain" tenant, as noted in "Creating a new "virtual" appliance record" on page 133. REMEMBER: each virtual appliance must be created in relation to a gateway appliance, and not as a standalone appliance.
- 2 Right-click the virtual appliance and choose "New Address" from the shortcut menu.
- 3 Use the resulting dialog box to enter the IP address of the tenant-specific network asset.
- 4 Repeat this address-entry process as needed.

- 5 When the virtual appliance and addresses are ready, you can now drag-and-drop these address entries as Source or Destination, when creating or editing security policies.

## Additional information

The concept behind the definition of a user domain tenant involves identifying the tenant and establishing the means of authenticating that tenant. For example, the administrator first defines a new user domain-specific virtual appliance. At this time, the administrator must link this entry to the relevant RADIUS system, to provide authentication services. At this time, the administrator can create the needed policies for this user domain (and the tenants).

When a user domain tenant wants to initiate an Internet or other external network connection through the Firebox Vclass appliance, they would first log into the appliance by means of the user name, password, and domain name previously defined in the tenant record. After this is verified by the RADIUS system, the Firebox appliance associates the user (IP address) to the relevant domain. Any traffic from the user will then be covered by policies that incorporate that domain.

## An example of a user-domain policy in use

As noted previously, the key element in user-domain tenant policies is *user authentication*. This is how traffic pertaining to a specific tenant is identified. For example:

- The administrator creates a user-domain tenant record for “Engineering” domain users, that uses a RADIUS server for user authentication.
- Policies are created to manage traffic for an external network, originating from “Engineering”.
- When one of the tenant users wants to make an external connection, they open their Web browser and log into the Firebox appliance. Their PC’s IP address (e.g., 192.168.12.36) is also noted by the appliance.
- After the user provides a user name, password and domain name (specified in the Tenant entry as referenced by the policy), the user name and password are validated by the RADIUS system.

- Once this is achieved, the user is granted access to the external network.
- The appliance now classifies packets from 192.168.12.36 (the user's computer) as traffic from the "Engineering" domain tenant.
- Finally, after a set idle time expires, the connection is broken, and that user will have to log in and re-authenticate themselves before being granted access to the external network again.

One of the advantages of creating and applying user-domain tenants to policies is that there is no strict relationship between a tenant and the originating computer's IP address. The PC used by a tenant user is noted dynamically by the appliance during the authentication process; the user name, password and domain are the key, and the IP address simply becomes a temporary location for the duration of the connection.

## **An overview of user-domain tenant authentication**

---

There are two types of tenant authentication that can be applied in a user-domain multi-tenant policy:

### *Manual authentication*

The client user supplies three required entries by means of a Web browser form: (1) a unique user name, (2) a related password and (3) a domain name.

### *Certificate-based authentication*

A pre-installed VPN certificate automatically supplies the client user name and domain name. The password must be manually entered by the user. This certificate must be imported by an IT administrator into the client system's Web browser (which is required for all secure access).

Once the three entries are supplied to the Firebox Vclass appliance, the appliance will initiate a RADIUS system authentication request to check the user name and password. **ALERT:** Firebox Vclass appliances cannot perform tenant authentication, as there is no internal-use database for this purpose.

## Inserting user domain tenant security policies

You can create any number of user-domain virtual appliances (and all associated addresses) for use in policies, as detailed previously in “Creating a new “virtual” appliance record” on page 133. This allows you to both create and revise new and existing user-domain tenant entries.

You can then utilize these entries as Source or Address when creating or editing security policies.

## How a user domain tenant makes a connection

---

After a user domain tenancy is established for relevant users, and the RADIUS system is loaded with authentication data for the potential users, the actual network connections are managed in this manner:

- 1 The user opens their browser and attempts to connect to the Firebox Vclass appliance.  
(A URL such as “https://192.168.13.5/logon/” would be entered in the Location field of the browser.)
- 2 When the connection is made, a Login form appears in the browser.
- 3 The user clicks in each of the three text entry fields (User Name and Password) and types the required information.
- 4 When they click **OK**, the browser will display either a Confirmation message, indicating that their connection is complete and ready for use, or will display an Invalid Entry alert, and permit them to try reentering their login information.
- 5 They can now perform any network tasks with this connection.

## Activating the Firebox Vclass “authenticate with certificates” feature

---

Following the importing of both certificates, you can activate the *user-domain* “Authentication with certificates” features in this Firebox Vclass appliance. This task can only be done by means of the WatchGuard CLI.

To complete this task, follow these steps:

- 1 Use a telnet/SSH application (or a console connection) to log into the security appliance.
- 2 Enter these command lines:  
 RS(config) cert <ENTER>  
 RS(config-cert) # ssl verify\_client on <ENTER>
- 1 If you need to deactivate this authentication feature, enter these command lines:  
 RS(config) cert <ENTER>  
 RS(config-cert) # ssl verify\_client off <ENTER>

---

**NOTE**

---

REMINDER: You should have activated this feature only **after** importing the root and client certificates for this appliance. If you do not do so, you will not be able to use CPM to administer this appliance as the certificate-less appliance will block all such administrative login attempts.

---

## Importing a VPN certificate into a user’s Web browser

If a client user must perform the x.509 client certificate importation at their site, they can do so through their Web browser, as detailed here. (You may want to create a ReadMe file representing this procedure for inclusion with the certificate file/text.)

- 1 Obtain the client x.509 certificate.
- 2 Send/deliver the resulting file to the client user.
- 3 Forward them a copy of these instructions for installing the certificate in their primary Web browser.
  - Copy the certificate file to a handy folder.
  - Start your Web browser (probably, Internet Explorer).
  - Open the **Tools** menu and choose **Internet Options**.
  - When the Internet Options dialog box appears, click the **Content** tab.
  - When the tab contents appear, click **Certificates**.
  - When the Certificates dialog box appears, click **Import**.

- When the Import Certificates wizard appears, work through it to locate, select and import the certificate file.
- After the wizard process is complete, the new certificate name should appear in the Certificate dialog box.
- Close this and all other Internet Options dialog boxes.
- Quit and restart Internet Explorer. The certificate is now ready for use in establishing VPN connections to the company network.

The client user should be ready to initiate “user-domain” connections to the company network.

# Defining Alarms

---

You can define two types of alarms: *Individual alarms* apply to just one appliance and *global alarms* apply to all appliances in a network. This chapter describes how to create both types of alarms.

## About Built-in Alarms

---

When first installed, CPM has several built-in global alarms that are automatically deployed to every Firebox Vclass appliance. Although these built-in global alarms cannot be modified or deleted, you can copy them and use their settings as a basis to create new alarms.

For more information on the default alarms, see Appendix A, “A Catalog of Alarm Probes and Counters.”

## About Probe Counters

---

Alarm definitions can use either of two types of probe counters:

*System probe counters* report on system statistics such as total number of packets, percentage of memory in use, or log file size. When you define system probe

counters, you specify the type of counter, the operation performed, and the threshold that leads to the triggering condition. For example, suppose you wanted to trigger an alarm when memory utilization exceeds 85%. You would specify:

- **Memory Util** as the counter
- **Becomes greater than (“>”)** as the operation
- **85%** as the threshold

*VPN peer probe counters* report VPN-related statistics on a specific pair of peer appliances. You define VPN peer probe counters using a process similar to the one for defining system probe counters. However, unlike a system probe, a VPN peer probe can include either Vclass appliances only or a combination of Vclass and non-Vclass appliances. Because of these VPN-specific possibilities, VPN peer probe counters have certain qualifications that do not affect system probe counters.

A VPN peer probe can monitor single VPN peer appliances. Or, you can apply the alarm to all VPN peers. For example, suppose you want to monitor the tunnels from X to Y. You have two options: set up an alarm to monitor the inbound tunnel at Y and use X as the instance; or monitor the outbound tunnel at X, and use Y as the instance.

For the first option, you create an individual alarm for Appliance Y containing an inbound tunnel probe with X as the instance. For the second option, you create an individual alarm for appliance X containing an outbound tunnel probe with Y as the instance.

## About Overriding Alarms

---

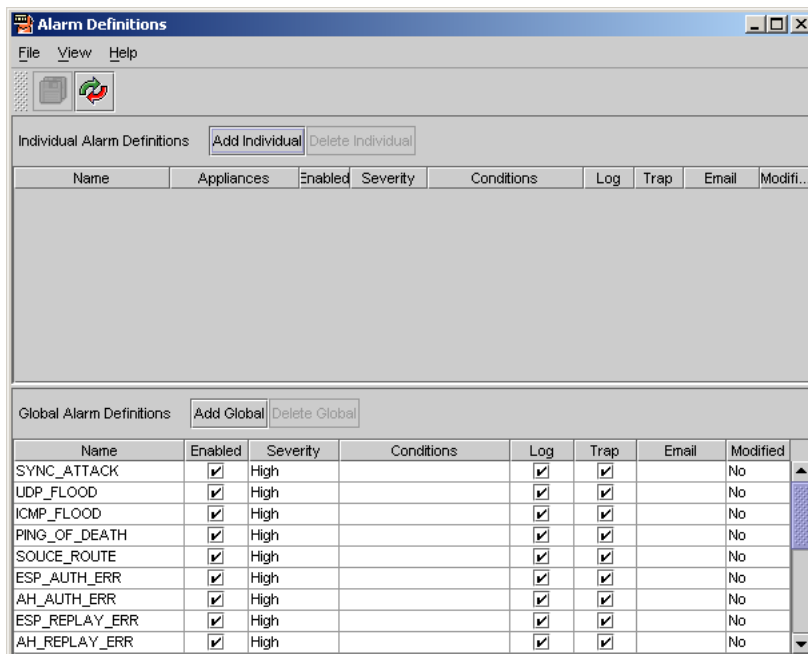
You can refine the conditions that trigger global alarms as applied to specific appliances. These types of alarms are called *overriding alarms*. For example, if you want to turn off the alarm of “SOURCE\_ROUTE” on some appliances, but still keep it on for other appliances, you can create an overriding alarm with the name “SOURCE\_ROUTE”, disable this overriding alarm, and select the appliances whose “SOURCE\_ROUTE” alarm should be disabled.

## Creating a New Alarm

Use the following procedure to define either an individual or a global alarm:

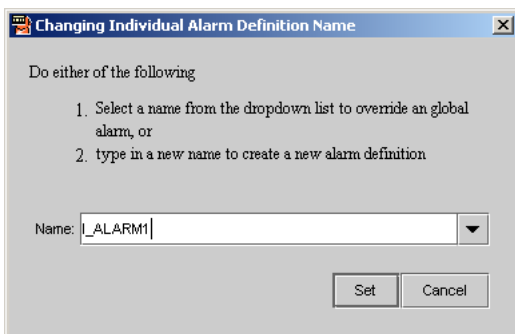
- 1 From the Appliance Manager window, select **Window** ⇒ **Alarm Console**.
- 2 Select **File** ⇒ **Definitions**.

The Alarm Definitions dialog box appears with a new row in the Alarm table.

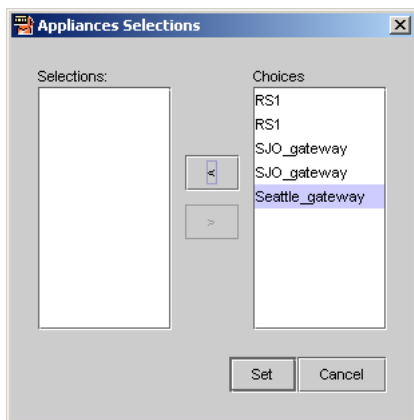


- 3 If you are defining an individual alarm, click **Add Individual**. If you are defining a global alarm, click **Add Global**.

- 4 Double-click the **Name** field in this new row.  
Depending on which type of alarm you are defining, either the Change Individual Alarm Name dialog box or the Change Global Alarm Name dialog box appears.



- 5 Type a new name.  
Alarm names can consist of up to 24 alphanumeric characters. The name cannot include blank spaces.
- 6 Click **Set** to save and apply the name.  
The Alarm Definition dialog box now displays the new name in the Name column.
- 7 (For individual alarms only) Double-click the **Appliances** field. Select an appliance name in the **Choices** list. Click the left arrow (<) button to transfer that appliance to the **Selections** list.  
You can include more than one appliance in an individual alarm definition, especially if the alarm is triggered by the action of two appliances such as VPN peer appliances.



- 8 Click **Set** to save your definition.

---

**NOTE**

---

The **Enable** checkbox is automatically selected in all new definitions. You can deactivate the alarm temporarily at any future time by reopening the **Alarm Definitions** dialog box and double-clicking the checkbox.

---

- 9 The **Severity** field is automatically set to **Medium**. To change this setting, double-click this field and select one of the settings.

## Adding system probe counters

To add system probe counters to an individual or global alarm definition:

- 1 In the **Alarm Definitions** dialog box, double-click the empty **Conditions** field in the new alarm row.  
The Alarm Conditions dialog box appears.

The screenshot shows the 'Alarm Conditions' dialog box. It features a 'Description:' text field at the top. Below this are three buttons: 'Add System Probe', 'Add VPN Peer Probe', and 'Delete'. A table with four columns is visible, with headers 'Instance', 'Probe', 'Op', and 'Threshold'. At the bottom of the dialog, there are two radio buttons: 'And' (unselected) and 'Or' (selected). The 'Set' and 'Cancel' buttons are located in the bottom right corner.

- 2 In the **Description** text field, type a description of this condition's function or purpose. This description will appear in the **Alarm Definitions** dialog box entry.  
The description can consist of up to 128 alphanumeric characters. You can use blank spaces, but they count against the total number of characters.

3 Click **Add System Probe**.

Conditions:			
<input type="button" value="Add System Probe"/> <input type="button" value="Add VPN Peer Probe"/> <input type="button" value="Delete"/>			
Instance	Probe	Op	Threshold
< SYSTEM >	CPU Util. (%)	becomes >	0

An empty row appears in the Conditions table, as shown above.

- 4 From the **Instance** menu, select the appropriate option.
- 5 From the **Probe** menu, select any of the system probes listed. (For a complete listing of all probe counters available, see Appendix A, “A Catalog of Alarm Probes and Counters.”)
- 6 Click **Op** and select the operator required.

The Op menu choices include the following:

becomes >	Condition will be true if the counter value becomes greater than the threshold value
becomes <	Condition will be true if the counter value becomes less than the threshold value
becomes =	Condition will be true if the counter value becomes equal to the threshold value
>=	Indicates “greater than or equal to”
>	Indicates “greater than”
=	Indicates “equal to”
!=	Indicates “not equal”
<=	Indicates “less than or equal to”
<	Indicates “less than”

- 7 Double-click the **Threshold** field. When a text entry field appears, type the value (a whole number or a percentage) applicable to this counter.  
If you are entering a number that represents a percentage, you can enter the whole number and omit the “%” symbol.
- 8 If you are adding more than one condition to this definition, select a logic choice (**And** or **Or**) by clicking the appropriate radio button. Be sure to do this before adding other conditions.
- 9 If required, repeat this process to add more conditions to the alarm definition.
- 10 To save your conditions when you are finished, click **Set**.

## Adding VPN peer probe counters

To add VPN peer probe counters to an alarm definition:

- 1 In the new alarm definition row, double-click the **Conditions** field.  
The Alarm Conditions dialog box appears.
- 2 Click **Add VPN Peer Probe**.  
An empty row appears in the Conditions table below the buttons.
- 3 If you want to monitor a single appliance, from the **Instance** menu, select one of the security appliances in this VPN connection.
- 4 If you apply this alarm definition to individual appliances in a VPN connection, you must insert additional probes for each participating appliance.
- 5 Click the **Probe** field to open the **Probe** menu and select any of the system probes listed. (For a complete listing of all probe counters available, see Appendix A, “A Catalog of Alarm Probes and Counters.”)  
When you make a selection, it appears in the Probe field.
- 6 Click **Op** (operations) and select the operator required.  
The Op menu choices include the following:

becomes >	Condition will be true if the counter value becomes greater than the threshold value
becomes <	Condition will be true if the counter value becomes less than the threshold value
becomes =	Condition will be true if the counter value becomes equal to the threshold value
> =	Indicates “greater than or equal to”
>	Indicates “greater than”
=	Indicates “equal to”
!=	Indicates “not equal”
< =	Indicates “less than or equal to”
<	Indicates “less than”

- 7 Double-click the **Threshold** field. When a text entry field appears, type the value (a whole number or a percentage) applicable to this counter.  
The type of number entered depends on the specific probe counter. If typing a percentage, type only the whole number; do not include the “%” symbol.
- 8 If you are adding more than one condition to this definition, select a logic choice (**And**, **Or**) by clicking the appropriate radio button. Be sure to do this before adding other conditions.
- 9 If required, repeat this procedure to add more system probe conditions to this alarm definition.

- 10 To save your conditions when you are finished, click **Set**.

## Completing the alarm definition

When the **Alarm Definition** dialog box reappears after you save your condition entries, you need to complete the Log, Trap, and Email entries.

- 1 The **Log** checkbox is selected by default, which means any time this alarm is triggered, it will be included in the Alarm log file. If you do not want to have this alarm logged, click to clear the checkbox.
- 2 The **Trap** checkbox is also selected by default, which means any time this alarm is triggered, an SNMP trap will be sent to the SNMP workstation monitoring all affected appliances. To deactivate this trap, click to clear the checkbox.
- 3 Double-click the **Email** field to activate the text entry features. Type an email address or an email/paging address for the contact administrator.
- 4 When you are finished with this alarm definition, click **Save** (in the dialog box toolbar).  
This saves the definition to the CPM Server database and closes the Alarm Definition dialog box.
- 5 When the Alarm window appears, click **Save** (the "disk" button in the Alarm toolbar.)

If you have created any individual alarm definitions, they will be deployed to the respective appliances the next time you deploy an updated profile to those appliances.

# Setting up and Managing Log Files

---

In addition to system monitoring and alarm capabilities, CPM provides an extensive list of log options. After configuring the log files you want kept and the degree of detail recorded, you can save them onto the Server host or onto a remote syslog server if one is available. After the recording begins, you can open and view all available logs, and then archive the logs as text files for future reference.

## Types of Logs

---

You can view two kinds of logs: those originated by the CPM server, (recording all the administrator activities) and those logs originated by each of the security appliances, including event logs, alarm logs, traffic logs, and so on. The following list describes each of the separate logs:

### *CPM Server*

Records information from CPM, including which CPM administrator logged in at what date and time, and what he or she did. This log is fairly limited in scope and does not track any actual system activity.

***Event***

Records all the events such as key negotiation activities, denial-of-service attacks, device failures, and administrative activities in a specified appliance.

***Traffic***

Records all the traffic going through a given appliance and whether or not these streams are passed or blocked according to the current set of policies in the appliance.

***Alarm***

Records a history of all the alarms that have been triggered by various events or occurrences for a specific appliance.

***RAS User***

Records a history of every RAS client connection made through a specific appliance, including user name, origin of the connection, when the user logged in (and out), and a summary of connection statistics.

***Phase One/Two SA***

These two logs record the creation/expiration histories for each phase of security associations pertaining to VPN tunnels established in the selected security appliance.

---

## **Log Size and Rollover**

---

CPM allows you to open and view all of the log files downloaded from any number of WatchGuard appliances. However, the appliances are all allotted a fixed file-storage capacity in which each log file is limited to the following predetermined sizes:

Event log: 200 KB

Alarm log: 20 KB

Traffic log: 1 MB

RAS User log: 200 KB

Phase One SA log: 200 KB

Phase Two SA log: 200 KB

When a particular log file exceeds the preset limit, the oldest entries are automatically deleted to make room for the most recent entries. To help you manage your log files so that you don't lose any entries, a predefined alarm, "Log\_file\_full", alerts you when a specific log file is getting too big. When you receive this alarm, you can archive the nearly full log as a text file for future reference.

## Viewing the CPM Log

---

CPM itself records a limited range of CPM administrator activities for future reference. The CPM log records all the most recent admin-user sessions (including the date and time), administrative login name, the level of access used in this session and a summary of the tasks performed by that administrator.

The CPM log records up to 1,000 entries and then automatically purges itself of the earliest records to make room new entries. To view this log, follow these steps:

- 1 If the CPM Console is not visible, make it active.
- 2 Click **CPM Server**.  
The CPM Server Information dialog box appears, displaying the General Info tab.
- 3 Click the **Server Log** tab.  
The Server Log appears.
- 4 To get the very latest records of CPM admin activity, click **Refresh**.
- 5 When you are finished reviewing the log entries, click **Close**.

## Viewing the Logs for Specific Appliances

---

If you want to review the activities of a specific appliance, you can open the Log Manager (on an individual appliance basis) and use a wide range of system-monitoring features.

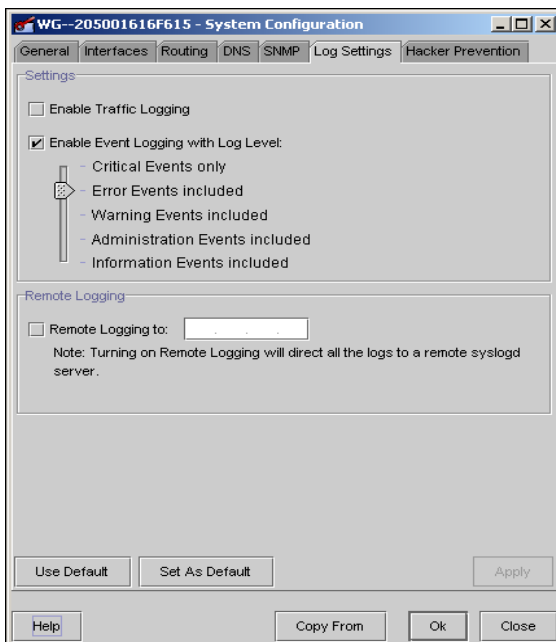
- 1 To download and view the log contents for a specific appliance, make the Appliance Manager window active.

- 2 Right-click a specific appliance row and select **Show Log** from the menu.  
The Log Manager window appears, displaying the Alarm Log tab.  
When this window appears, CPM has already contacted the selected security appliance, extracted the latest logs, and loaded them into this tab. Any delay you may experience is due to the amount of data being transmitted from the appliance to CPM.
- 3 You can review this log at this time, and then click on any of the other log tabs.

## Revising Log Settings for an Appliance

---

- 1 With the Log Manager window open, click **Settings**.  
The System Configuration dialog box appears, displaying the Log Settings tab.



You can set the following options:

- 2 Click the **Enable Traffic Log** checkbox to activate (or deactivate) the Traffic Log for this appliance.
- 3 Click the **Enable Event Logging with Log Level** checkbox to activate (or deactivate) the Event Log for this appliance.
- 4 Click the slider below the **Enable Event Logging** checkbox and move it until it is level with the logging level you want.  
The slider allows you to include fewer events or more events in your event log file—depending upon which selection you make. The “Critical Events only” selection creates a log file with only those major events, while the remaining selections below add increasing amounts of information and detail to the log file. Because the system purges the contents of the log files when a certain size is reached, the more events you include the more often the logs are purged.
- 5 Click the **Apply** button in the lower-right corner of the dialog box.  
Any changes to these settings are applied to the selected WatchGuard appliance the next time you deploy new information to that appliance.

## Managing a Large Number of Log Entries

---

When faced with a large number of log records to sift through, you can use two features of the Log Manager to filter out certain contents of an opened log.

- Increasing (or decreasing) the number of log entries viewed at a time
- Filtering the contents of a specific log, to screen out unwanted records

### Changing the number of log entries per page

- 1 Open the Log Manager window for any appliance.
- 2 Review the status message at the bottom of the screen to determine the actual number of logs displayed and the total number of records available.
- 3 If a log has more than 500 entries, you can view additional records by clicking **Next**.  
This prompts CPM to download the next group of records.
- 4 To review earlier groups of records, click the **Previous** button.

- 5 To increase the number of records shown in a page, click **No. of entries**.  
A Counter pop-up appears next to the slider bar.  
The default setting (500) restricts the download of log records to 500 entries at one time.
- 6 To increase the number of entries displayed from 500 to any of the higher values, move the slider to the number you want. Click anywhere in the Log Manager window to close this menu and apply your change.
- 7 To decrease the number where possible, move the slider to the number you want. Click anywhere in the Log Manager window to close this menu and apply your change.
- 8 Click each log tab (Alarm, Event, Traffic, RAS Users, Phase One SA, or Phase Two SA) to view the entries.
- 9 Click **Refresh** to update the current list with the very latest log activities.
- 10 Click **Close** to close the Log Manager window when you are finished viewing the logs.

## Filtering the contents of a log

When a particular log appears in the Log Manager window, a large number of other entries might appear. You can filter the entries such that the window displays only the activities or reports you want to see.

- 1 Open the Log Manager window for a selected appliance, if you have not already done so.
- 2 Right-click a specific column header to open the **Filter** dialog box.
- 3 You can isolate specific records by doing one of the following:
  - Click the preferred choice in the **Filter** dialog box
  - Hold down the Shift key and click several choices
  - Click and type a text string in the **Search** field
- 4 When you have made your selection or selections, click the **Filter** button.  
CPM filters out all unwanted records, and displays the records you want.

## Creating a cumulative set of filters

- 1 After applying a filter to one column, you can right-click other column headings and repeat this process to further filter all the contents of this tab until you have the exact records you want.  
To undo any filtering, right-click a column header.
- 2 When the **Filter** pop-up reappears, click **Disable Filter** to remove the filter from the column.  
The asterisk (\*) disappears from the column header and CPM restores previously-hidden log entries.
- 3 Repeat this process with all other filtered columns.

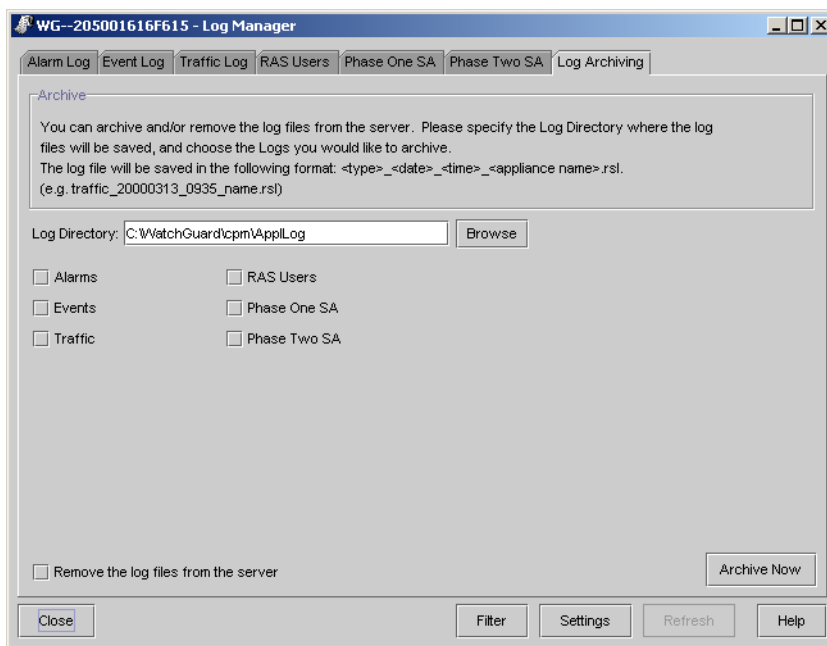
Any filtering applied to Log Manager tabs is disabled automatically when you exit the CPM Client .

## Archiving Log Files

---

- 1 Open the Appliance Manager window.
- 2 Right-click an appliance record in the Appliances table, and select **Show Log** from the shortcut menu.  
This opens the Log Manager window for that particular appliance.

- 3 Click the **Log Archiving** tab.  
The Log Archiving features appear, as shown below.



- 4 Click any one (or combination) of the log-specific checkboxes (Alarms, Events, Traffic, RAS Users, Phase One SA, and Phase Two SA).
- 5 If you want CPM to purge all current log files from the appliance after this archiving is complete, click the checkbox marked **Remove the log files**.
- 6 Click **Browse** (to the right of the Log Directory features).
- 7 When the **Select Directory** dialog box appears, use the dialog box navigation features to locate and select the destination drive and directory.
- 8 In the **File name** field of this dialog box, type a name for this log archive.
- 9 Click **Select**.  
The file name and pathway appear in the Log directory field.

10 Click **Archive Now**.

A status dialog box appears during the archival process.

11 When the backup is complete, a dialog box appears. Click **OK**.

---

**NOTE**

---

You cannot set up the CPM Server or the Firebox Vclass appliance to perform automatic backups of configuration archives.

---



# Maintaining Appliances

---

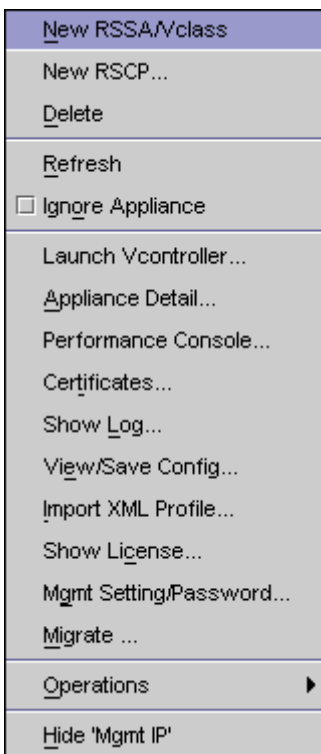
In addition to monitoring your appliances with CPM (the Appliance Manager and Appliance Details windows), you can perform a number of maintenance tasks with CPM, including the following:

- Remotely restarting an appliance
- Remotely shutting down an appliance
- Upgrading/updating an appliance's operating system software
- Restoring an active appliance to the factory-default state
- Archiving a profile as an XML format file
- Synchronizing an appliance's clock with the CPM Server system clock

## About the Shortcut Menu

---

The Appliance Manager window combines many appliance-management features into a handy shortcut menu. You can open this menu by right-clicking an appliance listing in the "Security Appliances" table.



## Remotely Restarting an Appliance

---

- 1 After logging into CPM, open the Appliance Manager window.
- 2 Locate the appliance record in the Group folders and select it.
- 3 When the appliance record row appears in the WatchGuard Appliances table, right-click it to open the shortcut menu.
- 4 Select **Operations** ⇒ **Reboot**.
- 5 If a confirmation dialog box appears, click **OK**.  
Wait for about five minutes. The Appliance Manager notes this appliance as 'Out of contact' for the duration of the shutdown/restart. After the appliance is active and online, CPM detects its state and notes the status as "In contact".

## Remotely Shutting Down an Appliance

---

- 1 After logging into CPM, open the Appliance Manager window.
- 2 Locate and click the appliance icon in the Groups list.
- 3 When the appliance record appears in the WatchGuard Appliances table to the right, right-click it to open the shortcut menu.
- 4 Select **Operations** ⇒ **Reboot**.
- 5 If a confirmation dialog box appears, click **OK**.  
Wait for about a minute. The Appliance Manager notes this appliance as 'Out of contact' at the conclusion of the shutdown.

## Restoring an Appliance to the Factory Default State

---

You can, if necessary, use CPM to restore an active appliance (local or remote) to the factory-default state if you need to reinstall the software or start over. If the appliance is in a remote location, it must be in contact with CPM. After you have restored it to the factory-default state, you must use Vcontroller from a local workstation to reinstall and configure it, or transfer the appliance to your current location so that you can use CPM to reinstall and configure it.

- 1 After logging into CPM, open the Appliance Manager window.
- 2 Locate the appliance record in the Group folders and select it.
- 3 When the appliance record row appears in the Appliances table, right-click it to open the shortcut menu.
- 4 Select **Operations** ⇒ **Reboot**.
- 5 If a confirmation dialog box appears, click **OK**.  
Wait for about a minute. The Appliance Manager notes this appliance as "Out of contact" at the conclusion of the shutdown.
- 6 You now have two options:
  - Have an administrator who is "local" to that appliance use Vcontroller to restore the appliance to a usable condition.
  - Transport the appliance to your current location, and use CPM to restore the appliance.

## Archiving an Appliance's Profile as an XML File

---

In anticipation of system problems or losses, you should regularly back up each appliance's profile as an XML file. This file can be used to quickly restore a problematic or crashed system.

Note that importing a profile can only be done with an appliance that has been configured and had a minimalist profile deployed to it previously. You cannot just discover an appliance and then apply an XML-format profile to that device; it must be loaded with extended-feature licenses and x.509 certificates, and then deployed with a working profile that at least sets the IP addressing of the data interfaces.

## Synchronizing an Appliance's Clock with CPM Server

---

If you are not sure whether an appliance is using the correct clock settings (date, time), you can synchronize it with CPM Server.

- 1 After logging into CPM, open the Appliance Manager window.
- 2 Locate the appliance record in the Group folders and select it.
- 3 When the appliance record row appears in the Appliances table, right-click it to open the shortcut menu.
- 4 Choose **Operations** ⇒ **Sync Time** from the shortcut menu.
- 5 If a confirmation dialog box appears, click **OK** to proceed.  
The CPM Server will reset the appliance clock (date and time), but will not reboot the appliance.

---

## Installing CPM Server on a Solaris host

The following section details the process of installing the CPM Server on a Solaris host computer. Note that you must use Solaris v2.8.

CPM for Solaris requires that you install JRE version 1.4.1\_01 before you install CPM.

To install the CPM Server, follow these steps:

- 1 Insert the WatchGuard CD into the CD-ROM. (Under Solaris, the CD should automatically mount at `/cdrom`).
- 2 Run this command:  
`cd /cdrom/`
- 3 Run this command:  
`/setup.sh`
- 4 During the resulting software installation process, the installer will ask you if you have already installed the latest versions of the Java Run-time Environment and JDK. If you have done so, you must type “Y” and then type the pathway to the JRE/JDK directory.

The installer will locate and assess this JDK collection.

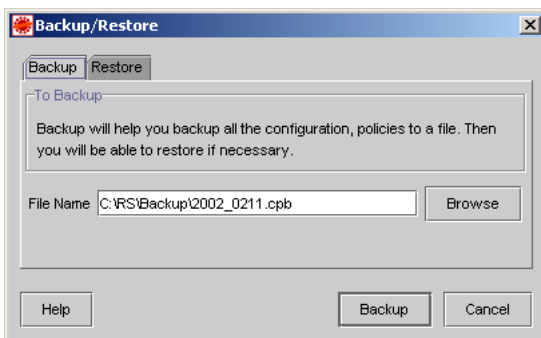
If this is an older version of JDK, the installer will alert you and ask if you prefer to use it instead of a more recent version. WatchGuard recommends that you obtain and install the most recent version

- 5 If you haven't installed JRE/JDK, type "N". The installer will quit, and it will provide information on where on the Sun Web site to obtain the proper version of JRE/JDK software.
- 6 When the JDK software has been installed (and any required Solaris updates are completed), run this command:  
**cd/cdrom/watchguard**  
Then run this command:  
**./setup.sh**  
This restarts the installation process.
- 7 When asked by the installation script to indicate where the JDK is, type the pathway to that directory.  
The installation can now proceed to completion.

## Backing up the CPM Database

---

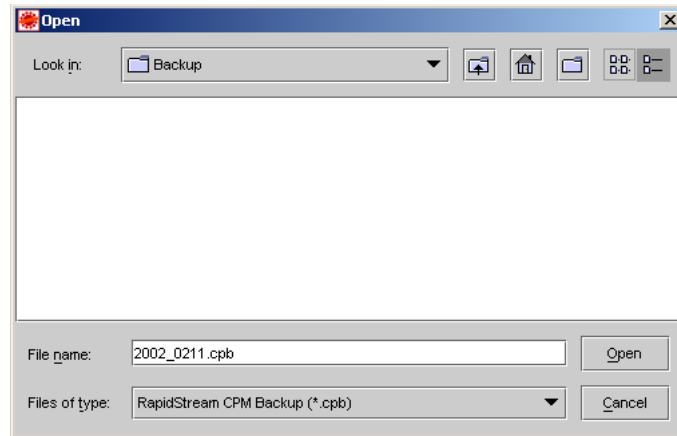
- 1 Log in to the CPM Client.
- 2 When the CPM Console appears, click **Backup/Restore**.  
The Backup/Restore dialog box appears, displaying the Backup tab.



- 3 A default file name and directory pathway are noted in the File Name field. This directory is located on your client workstation, and can be used for all CPM Server archiving provided your workstation has enough disk capacity.

If you want to specify another directory (on another networked drive), click **Browse**.

The CPM Open dialog box appears.

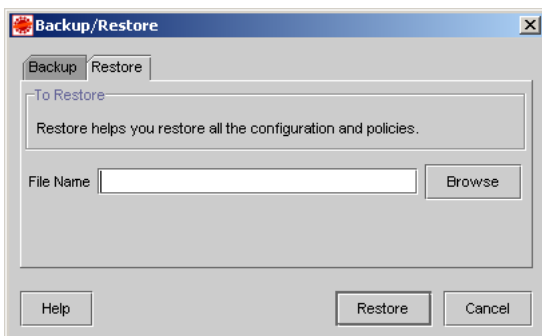


- 4 If you want to change the default file name, delete the existing text and type a name of your choosing.  
You must use .cpb as the file extension.
- 5 Click **Open**.
- 6 Click **Start BackUp** to initiate the backup process.  
When the backup ends, a confirmation dialog box appears, indicating the backup was successful.
- 7 Click **OK**.

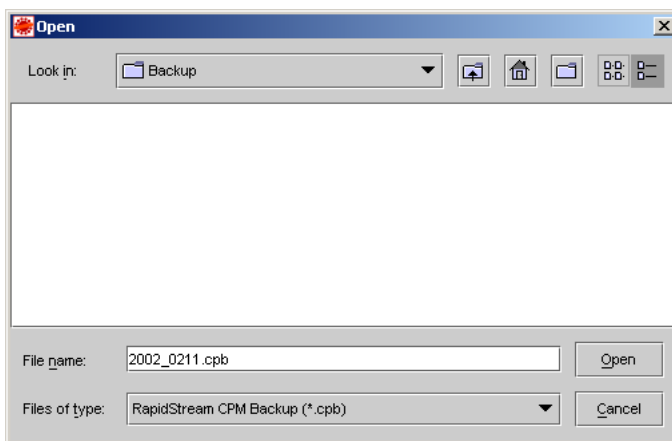
## Restoring an Archived CPM Server Database

- 1 Log into the CPM Server.
- 2 When the CPM Console appears, click **Backup/Restore**.  
The Backup/Restore dialog box appears, displaying the Backup tab.

- 3 Click the **Restore** tab.



- 4 To locate the archive file, click **Browse**.  
The CPM Open dialog box appears.



- 5 Use the dialog box directory navigation features to locate and select the archive file.  
The file extension must have been entered as ".CPB" or CPM will not be able to find and restore the backup file.
- 6 Click **Open**.  
The Restore tab reappears, displaying the file name and pathway in the File Name field.
- 7 Click **Start Restore** to initiate the software restoration process.  
This will overwrite all information currently stored in the appliance.  
A Restart Confirmation dialog box appears.

- 8 Click **Yes** to proceed (or click **No** to cancel the entire restoration process).  
When the restoration is complete, a dialog box appears indicating the restoration was successful.
- 9 Click **OK** to close this dialog box.



---

This chapter provides case studies for the following CPM features:

- Dynamic NAT
- QoS
- VLANs
- Tunnel switching

## Case Study: Dynamic NAT Firewall Policy

---

To set up a dynamic NAT firewall policy that permits all internal users in all extended network locations to have Internet access, do the following:

### Policy ("dnat\_access")

#### *Addresses*

Open this window and create an address group that includes all private networks behind your Firebox Vclass appliances, named (for example) "All\_Private".

You may want to create individual address entries for each appliance, specifically referencing the IP type "Any" and the Port

“Private”. These addresses represent all potential users in the network behind the Private interface of each appliance.

*Services*

Open this window and create a new combined-services group incorporating the protocols you want to permit. Examples: HTTP and FTP.

*Policies*

Open this window and create a new policy with these parameters:

- Source:** Choose “All\_Private”.
- Destination:** Choose the “Internet” address.
- Services:** Choose the newly created services (singly or in a group.)
- Actions:** Choose Firewall/Pass  
Choose Do Dynamic NAT

---

## Case Study: QoS Actions

---

When using QoS actions within your policies to prioritize certain network traffic, remember that any traffic streams not included in explicit QoS actions will be affected by a “default” built-in QoS action with a WFQ weight of 5. The following example explains how this works in conjunction with other QoS policies.

### Example 1:

- Default: (No QoS action) WFQ weight=5
- Policy 1: QoS action A with WFQ weight=5
- Policy 2: No QoS
- Policy 3: No QoS
- Policy 4: QoS action B with WFQ weight = 10
- Policy 5: No QoS

In this case, the ratios between all three QoS actions are 5 (default), 5 (QoS A), 10 (QoS B), which is a 1:1:2 ratio. When the network capacity is fully

utilized, policy 1 traffic uses 25% of the bandwidth, policy 4 uses 50%, and all other traffic (apportioned to three policies) shares the remaining 25%.

### **Example 2:**

Default: (No QoS action) WFQ weight=5

Policy 1: QoS action A with WFQ weight=15

Policy 2: No QoS

Policy 3: No QoS

Policy 4: QoS action B with WFQ weight = 5

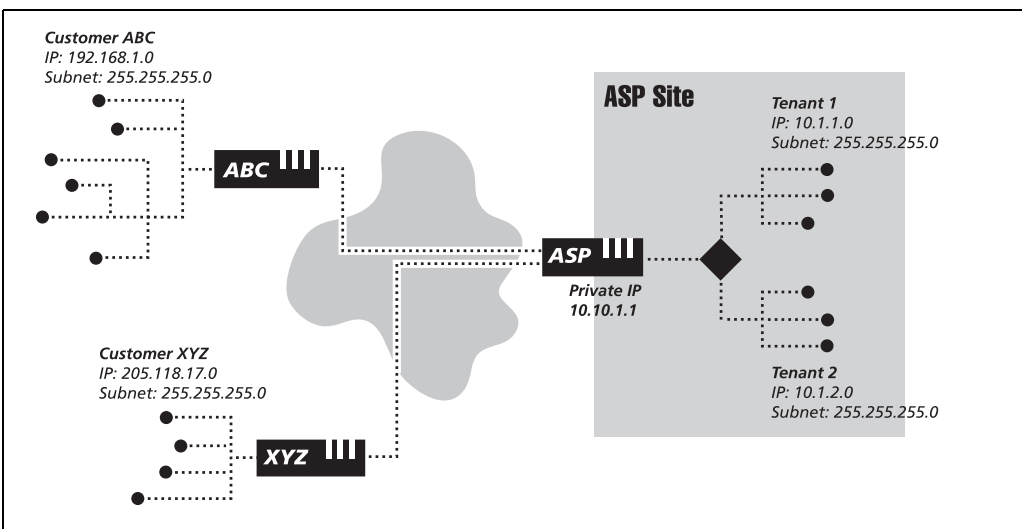
Policy 5: No QoS

Policy 6: QoS action B with WFQ weight = 5

In this case, the ratios between the four QoS actions are 5 (default), 15 (QoS A), and 5 (QoS B) which is a 1:3:1 ratio. Therefore, when the network capacity is fully utilized, policy 1 traffic uses 60% of the total bandwidth ( $3/5$ ), policy 4 and policy 6 traffic share 20% ( $1/5$ ) of the bandwidth, and all other traffic shares the remaining 20% ( $1/5$ ) of bandwidth.

## Case Study: VLAN in WatchGuard appliances

As illustrated below, here is a working scenario showing how the WatchGuard security appliance can manage traffic to and from a typical VLAN.



In this example, we start with an ASP site that hosts two customers' assets.

- Customer ABC's servers are in network 10.1.1.0/255.255.255.0, which has been assigned VLAN ID 3.
- Customer XYZ's servers are in network 10.1.2.0/255.255.255.0, which has been assigned VLAN ID 25.

To make this work, the needed VPN policies will be applied in the ASP's security appliance to allow Company ABC and XYZ to access their assets in the ASP through secure VPN tunnels. Since the ASP should not be

allowed to access Company ABC and XYZ's private networks, we will create uni-directional VPN policies on the WatchGuard appliances.

```

-ABC (appliance)
  L ABC_NET (address, subnet 192.168.1.0/24, private)
-ASP (appliance)
  L ABC_VA (virtual appliance, VLAN id=3, private)
  L ABC_VLAN (address, subnet 10.1.1.0/24)
  L XYZ_VA (virtual appliance, VLAN id=25, private)
  L XYZ_VLAN (address, subnet 10.1.2.0/24)
-XYZ (appliance)
  L XYZ_NET (address, subnet 205.118.17.0/24, private)

```

We then create the following policies

Source	Destination	Service	Action
ABC_NET@ABC	ABC_VLAN@ASP	ANY	->IPSEC
XYZ_NET@XYZ	XYZ_VLAN@ASP	ANY	->IPSEC

## Case Study: Tunnel Switching Between Remote Sites

To establish tunnel switching through the central site (site C) for traffic from remote sites A and B, follow these steps:

- 1 Open the Appliance window and add new appliance entries for each of the remote appliances.
- 2 Open the Policies window, and then open the **Addresses** dialog box.
- 3 Select the centralized site location in the Addresses list and create a new address entry for this appliance for tunnel switching use. The address entries should include the following:

**Name** Type "central\_ANY"

**IP Type** Select "ANY"

**Location** Select the security appliance at the central site

**Port** Select the Private interface

- 4 Reopen the Address window and (switching to Location mode) create address entries for the network at each remote site. (such as net\_A, net\_B) These address entries should reflect the following:

**IP Type** Select IP subnet or IP Range and make the appropriate entries.

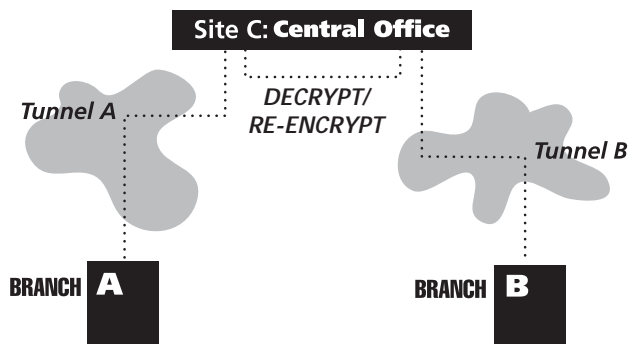
**Location** Select that site's security appliance

**Port** Private

- 5 Open the Policies window and create a single new policy that includes all the tunneling appliances with the following parameters:
 

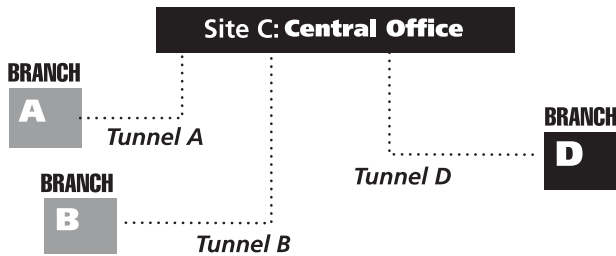
<b>Source</b>	Select each of the remote site networks (such as net_A, net_B)
<b>Destination</b>	Select the central site (“central_ANY”)
<b>Service</b>	Select ANY
<b>Action</b>	Choose IPSec, and when the Select IPSec dialog box appears, choose “Maximum Security” and click Select.
- 6 Save this policy.
- 7 If the remote sites will be using dynamic NAT for all internal-to-Web connections, you can insert a policy that permits those sites to use tunnel switching for such access. The parameters would include the following:
 

<b>Source</b>	“central_ANY”
<b>Destination</b>	Internet
<b>Service</b>	Select ANY or HTTP
<b>Action</b>	Dynamic NAT
- 8 Move this last policy in a lower sort order (lower in the Policy table), as it is covering all traffic from private networks to the external network.
- 9 Finally, deploy all this to the relevant appliances. As a result, your network connections should work as shown here:



## Adding a new site

If you need to add a third security appliance to this tunnel-switching setup (as illustrated below with “branch D”) you can do so by making these changes.



To add another appliance to the tunnel switching scheme, follow these steps:

- 1 Create a new *appliance* entry for network\_D
- 2 Create a new *address* entry for net\_D
- 3 Add this “net—D” entry to the **Source** cell of the existing tunnel-switching policy.
- 4 After you deploy the new policy, the expanded tunneling network will be in place.



# About the CPM Configuration Files

---

Two key files contain all the configuration information concerning the WatchGuard CPM Client and Server. You can open and edit these files as needed:

- The *cpm\_server.conf* file for the CPM Server
- The *cpm\_client.conf* file for the CPM Client

## CPM Server Config file

---

The *cpm\_server.conf* file is used to set up certain run-time parameters for the CPM Server. It can be found in the CPM Server installation directory. The following parameters can be customized:

<b>Parameter name</b>	<b>Values</b>	<b>Purpose</b>
POLICY_FILE		This file specifies the Java Runtime Environment security policy for running the CPM server. Do not edit.
REGISTRY_PORT	A valid TCP port number, default = 7850	Used for the Server to bind to the port and receive RMI over SSL requests from clients. Must be the same as the matching CPM Client entry.
SOCKET_PORT	A valid UDP port number, default = 7850	For appliances to send unsolicited notifications to the server, including heartbeats, and alarm and status notifications. Do not edit.
NO_WORKER	3	Number of worker threads to handle appliances. If the CPM Server host is powerful enough, you can increase this number.
SSL	true or false (Default=false)	Tells the CPM Server whether SSL should be used to communicate with the client. Must be the same as the matching CPM Client entry.
SQL port	Default=7851	The port number listened to by the CPM Server database engine.
RMI_Base_Port	Default=0	The port number used by the CPM Client for server communication. If the value is 0 (zero), a dynamic port number will be assigned. This is useful when the CPM Client connects from an external network, outside the firewall.

CPM_SERVER_IP		Used to record the primary IP address of the CPM Server if there is more than one network interface in the host computer. Can be left blank if there is only one interface on the CPM Server host.
NOTIF_QUEUE_SIZE	A numeric value	Represents the size (integer) of the queues used for receiving messages from appliances. Not necessary to edit this.
SIMULATED	TRUE or FALSE	Allows CPM to support "virtual" (simulated) appliances.
FILE_TRANSFER_BLOCK_SIZE	A numeric value	The block size used when sending files or RMI. Not necessary to edit this.
CPM_BACKUP_SERVER_IP		Not supported. Do not edit.
TRACE	SCREEN, LOG or OFF	Determines how to handle a log file.
SNMP_RETRIES	A numeric value	Sets the number of retries to use for SNMP requests.
PROX_PORT	A list of port numbers	Used for proxying the Vcontroller through the CPM Server. Not necessary to edit this.
SNMP_TIMEOUT	A numeric value	Sets the timeout for SNMP requests.
SNMP_RECEIVE_TRAPS	TRUE or FALSE	If TRUE, the CPM Server enables SNMP trap reception.
SNMP_TRAP_IP	IP address	The address on the CPM Server to listen on for SNMP traps.

SNMP_TRAP_PORT	Port number	"162" is the default SNMP trap port.
SNMP_TRAP_EOID	A comma-separated list	All of the enterprise object IDs of the traps the CPM Server accepts. The RSCP EOID is 1.3.6.1.4.1.4355.7.3 The RSSA EOID is 1.3.6.1.4.1.4355.2.3
POLICY_FILE		For internal CPM use. Do not edit.

---

## CPM Client Config file

---

The `cpm_client.conf` file is used to record certain run-time parameters for the CPM Client. It can be found in these locations in the client workstation:

- User's home directory/`cpm_client.conf`
- `cpm_client.conf.default` in the CPM client directory

Parameter name	Values	Purpose
REGISTRY_PORT	A valid TCP port number.	The client sends RMI over SSL requests to the specified port of the server. Must be the same as the matching CPM Server entry.
SSL	true or false	Tells the client whether SSL should be used to communicate with the server. Must be the same as the matching CPM Server entry.
CPM_DIR		For internal CPM use, and should not be changed.
DOMAIN		For internal CPM use, and should not be changed.

---

---

<b>Parameter name</b>	<b>Values</b>	<b>Purpose</b>
SERVER_HOST		For internal CPM use, and should not be changed.
MRU_DOMAINS		For internal CPM use, and should not be changed.
USERNAME		For internal CPM use, and should not be changed.

---



# A Catalog of Real-time Monitor Probe Counters

---

## System Counters

---

Counter Name	Function
<b>CPU Util. (%)</b>	System CPU utilization
<b>Memory Util. (%)</b>	System memory utilization
<b>Interface 1(Public)Status (1=up)</b>	Interface 1 status (1-up; 0-down)
<b>Interface 0(Private)Status (1=up)</b>	Interface 0 status (1-up; 0-down)
<b>Interface 2(DMZ)Status (1=up)</b>	Interface 2 status (1-up; 0-down)
<b>System Throughput bytes/sec</b>	Number of bytes processed per second
<b>Packets Recv/sec</b>	Packets received rate (packets/second)
<b>Packets Sent/sec</b>	Packets sent rate (packets/second)
<b>IPSec Throughput bytes/sec</b>	IPSec traffic throughput (bytes/sec)
<b>IPSec Packets/sec</b>	IPSec traffic throughput (packets/sec)
<b>Total IPSec Tunnels</b>	Total number of active IPSec tunnels

<b>Counter Name</b>	<b>Function</b>
<b>Interface 1(Public)Recv. (Bytes)</b>	Number of bytes received from Interface 1 (bytes)
<b>Interface 1(Public)Sent (Bytes)</b>	Number of bytes sent from Interface 1 (bytes)
<b>Interface 1(Public)Recv. (Packets)</b>	Number of packets received from Interface 1 (packets)
<b>Interface 1(Public)Sent (Packets)</b>	Number of packets sent from Interface 1 (packets)
<b>Interface 1(Public)Recv Throughput, (Bytes/sec)</b>	Rate of bytes received from Interface 1 (bytes/sec)
<b>Interface 1(Public)Sent Throughput, (Bytes/sec)</b>	Rate of bytes sent from Interface 1 (bytes/sec)
<b>Interface 1(Public)Recv Throughput, (Packets/sec)</b>	Rate of packets received from Interface 1 (packets/sec)
<b>Interface 1(Public)Sent Throughput, (Packets/sec)</b>	Rate of packets sent from Interface 1 (packets/sec)
<b>Interface 0(Private) Received (Bytes)</b>	Number of bytes received from Interface 0 (bytes)
<b>Interface 0(Private) Sent (Bytes)</b>	Number of bytes sent from Interface 0 (bytes)
<b>Interface 0(Private) Recv. (Packets)</b>	Number of packets received from Interface 0 (packets)
<b>Interface 0(Private) Sent (Packets)</b>	Number of packets sent from Interface 0 (packets)
<b>Interface 0(Private) Recv. Throughput, (Bytes/sec)</b>	Rate of bytes received from Interface 0 (bytes/sec)
<b>Interface 0(Private) Sen Throughput, (Bytes/sec)</b>	Rate of bytes sent from Interface 0 (bytes/sec)

<b>Counter Name</b>	<b>Function</b>
<b>Interface 0(Private) Recv. Throughput, (Packets/sec)</b>	Rate of packets received from Interface 0 (packets/sec)
<b>Interface 0(Private) Sent Throughput, (Packets/sec)</b>	Rate of packets sent from Interface 0 (packets/sec)
<b>Interface 2(DMZ)Recv. (Bytes)</b>	Number of bytes received from Interface 2 (bytes)
<b>Interface 2(DMZ)Sent (Bytes)</b>	Number of bytes sent from Interface 2 (bytes)
<b>Interface 2(DMZ)Recv. (Packets)</b>	Number of packets received from Interface 2 (packets)
<b>Interface 2(DMZ)Sent (Packets)</b>	Number of packets sent from Interface 2 (packets)
<b>Interface 2(DMZ)Recv. Throughput, (Bytes/sec)</b>	Rate of bytes received from Interface 2 (bytes/sec)
<b>Interface 2(DMZ)Sent Throughput, (Bytes/sec)</b>	Rate of bytes sent from Interface 2 (bytes/sec)
<b>Interface 2(DMZ)Recv. Throughput, (Packets/sec)</b>	Rate of packets received from Interface 2 (packets/sec)
<b>Interface 2(DMZ)Sent Throughput, (Packets/sec)</b>	Rate of packets sent from Interface 2 (packets/sec)
<b>Log Disk Total (KB)</b>	Total disk space for log files in Kbytes
<b>Log Disk Used (KB)</b>	Total disk space used for log files in Kbytes
<b>Log Disk Free (KB)</b>	Total disk space available for log files in Kbytes
<b>Log Disk Used (%)</b>	Percentage of disk space used for log files
<b>Log Disk Free (%)</b>	Percentage of disk space available for log files

<b>Counter Name</b>	<b>Function</b>
<b>Log Directory Size(KB)</b>	Total size of the directory containing log files in Kbytes
<b>Event Log Size (KB)</b>	Event log file size in Kbytes
<b>Traffic Log Size (KB)</b>	Traffic log file size in Kbytes
<b>Alarm Log Size (KB)</b>	Alarm log file size in Kbytes
<b>Event Log Increment (KB)</b>	Event log file size increment per interval
<b>Traffic Log Increment (KB)</b>	Traffic log file size increment per interval
<b>Alarm Log Increment (KB)</b>	Alarm log file size increment per interval
<b>Event Log Growth Rate (KB/sec)</b>	Event log file size increment rate (Kbytes/second)
<b>Traffic Log Growth Rate (KB/sec)</b>	Traffic log file size increment rate (Kbytes/second)
<b>Alarm Log Growth Rate (KB/sec)</b>	Alarm log file size increment rate (Kbytes/second)
<b>Phase One SA Log Size (KB)</b>	Phase one SA log file size in Kbytes
<b>Phase Two SA Log Size (KB)</b>	Phase two SA log file size in Kbytes
<b>Remote User Log Size (KB)</b>	Remote user log file size in Kbytes
<b>Incoming Stream Requests</b>	Number of incoming stream requests
<b>Interface 1(Public) Stream Requests</b>	Number of incoming stream requests from Interface 1
<b>Interface 0(Private) Stream Requests</b>	Number of incoming stream requests from Interface 0

<b>Counter Name</b>	<b>Function</b>
<b>Interface 2(DMZ) Stream Requests</b>	Number of incoming stream requests from Interface 2
<b>Incoming Stream Req./sec</b>	Rate of incoming stream requests
<b>Interface 1(Public) Stream Req./sec</b>	Rate of incoming stream requests from Interface 1
<b>Interface 0(Private) Stream Req./sec</b>	Rate of incoming stream requests from Interface 0
<b>Interface 2(DMZ) Stream Req./sec</b>	Rate of incoming stream requests from Interface 2
<b>Incoming Stream Requests Denied</b>	Number of denied stream requests
<b>Interface 1(Public) Stream Requests Denied</b>	Number of denied stream requests from Interface 1
<b>Interface 0(Private) Stream Requests Denied</b>	Number of denied stream requests from Interface 0
<b>Interface 2(DMZ) Stream Requests Denied</b>	Number of denied stream requests from Interface 2
<b>Incoming Stream Req. Denied/sec</b>	Rate of denied stream requests
<b>Interface 1(Public) Stream Requests Denied/sec</b>	Rate of denied stream requests from Interface 1
<b>Interface 0(Private) Stream Requests Denied/sec</b>	Rate of denied stream requests from Interface 0
<b>Interface 2(DMZ) Stream Requests Denied/sec</b>	Rate of denied stream requests from Interface 2
<b>Total Bytes Recv.</b>	Number of bytes received
<b>Total Bytes Sent</b>	Number of bytes sent

<b>Counter Name</b>	<b>Function</b>
<b>Total Packets Recv.</b>	Number of packets received
<b>Total Packets Sent.</b>	Number of packets sent
<b>Total IPSEC Traffic (bytes)</b>	IPSEC traffic in bytes
<b>Total IPSEC Packets</b>	IPSEC packets
<b>Total Tunnel Mode SA</b>	Number of tunnel mode SA in the system currently
<b>Total Transport Mode SA</b>	Number of transport mode SA in the system currently
<b>Total ESP SA</b>	Number of ESP protocol SA in the system currently
<b>Total AH SA</b>	Number of AH protocol SA in the system currently
<b>Total Manual Key SA</b>	Number of SA using manual key in the system currently
<b>Total Auto Key SA</b>	Number of SA using auto (IKE) key in the system currently
<b>Total Expired SA</b>	Total number of expired SA since start of system
<b>HA1 Port Status (1=up)</b>	HA1 interface status (1=up; 0=down)
<b>HA2 Port Status (1=up)</b>	HA2 interface status (1=up; 0=down)
<b>Active User Sessions</b>	Number of remote users' sessions
<b>Remote Users Logon</b>	Number of remote user logons since last poll

<b>Counter Name</b>	<b>Function</b>
<b>Remote Users Logoff</b>	Number of remote user logoffs since last poll
<b>Remote Users Authentication Failed</b>	Number of remote user logons failed since last poll

## Aggregate counters for all VPN end-point pairs

<b>Counter Name</b>	<b>Description of Counter's Function</b>
<b>Total Inbound SA</b>	Total number of inbound SA
<b>Total Outbound SA</b>	Total number of outbound SA
<b>Total SA</b>	Total number of SA
<b>Total Inbound Bytes/sec</b>	Traffic rate through inbound SA
<b>Total Outbound Bytes/sec</b>	Traffic rate through outbound SA
<b>Total Inbound Pkts/sec</b>	Packet rate through inbound SA
<b>Total Outbound Pkts/sec</b>	Packet rate through outbound SA
<b>Total Decryption Error Rate (%)</b>	Total Decryption Error Packet Rate
<b>Total Authentication Error Rate (%)</b>	Total Authentication Error Packet Rate
<b>Total Inbound SA</b>	Total number of inbound SA

## IPSec counters per VPN end-point pair

Counter Name	Description of Counter's Function
<b>Inbound SA</b>	Number of inbound SA of a VPN end-point pair
<b>Outbound SA</b>	Number of outbound SA of a VPN end-point pair
<b>Inbound Bytes/sec</b>	Traffic rate through inbound SA of a VPN end-point pair
<b>Outbound Bytes/sec</b>	Traffic rate through outbound SA of a VPN end-point pair
<b>Inbound Pkts/sec</b>	Traffic rate through inbound SA of a VPN end-point pair
<b>Outbound Pkts/sec</b>	Traffic rate through outbound SA of a VPN end-point pair
<b>Decryption Error Rate (%)</b>	Decryption error packet rate of a VPN end-point pair
<b>ESP Authentication Error Rate (%)</b>	ESP authentication error packet rate of a VPN end-point pair
<b>AH Authentication Error Rate (%)</b>	AH authentication error packet rate of a VPN end-point pair
<b>Replay Error Rate (%)</b>	Replay error packet rate of a VPN end-point pair
<b>Inbound Bytes</b>	Number of inbound bytes of a VPN end-point pair
<b>Outbound Bytes</b>	Number of outbound bytes of a VPN end-point pair
<b>Inbound Packets</b>	Number of inbound packets of a VPN end-point pair
<b>Outbound Packets</b>	Number of outbound packets of a VPN end-point pair

## Policy counters for all policies

<b>Counter Name</b>	<b>Description of Counter's Function</b>
<b>Number of Policies</b>	Total number of policies
<b>Packets Disc. by Firewall</b>	Total number of packets discarded by Firewall policies
<b>Packets Disc. at Interface 1(Public)(%)</b>	Percentage of packets discarded at Interface 1
<b>Packets Disc. at Interface 0(Private)(%)</b>	Percentage of packets discarded at Interface 0
<b>Packets Disc. at Interface 2(DMZ)(%)</b>	Percentage of packets discarded at Interface 2
<b>Packets Disc. by IPSec Error (%)</b>	Percentage of packets discarded by IPSec errors (decryption error, authentication error, replay error).
<b>Packets Disc. by Decryption Error (%)</b>	Percentage of packets discarded by Decryption errors
<b>Packets Disc. by Authentication Error (%)</b>	Percentage of packets discarded by Authentication errors
<b>Packets Disc. by Replay Error (%)</b>	Percentage of packets discarded by Replay errors

## Policy counters per policy

<b>Counter Name</b>	<b>Description of Counter's Function</b>
<b>Traffic (Bytes)</b>	Number of bytes handled by a policy
<b>Traffic (Packets)</b>	Number of packets handled by a policy
<b>Throughput (Bytes/sec)</b>	Throughput in bytes/sec of a policy
<b>Throughput (Pkts/sec)</b>	Throughput packets/sec of a policy
<b>Number of SA</b>	Number of SA belongs to a policy
<b>Packet Disc. (%)</b>	Packet discarded rate of a policy
<b>Decryption Error Packets</b>	Number of packets handled by a policy with decryption error
<b>Authentication Error Packets</b>	Number of packets handled by a policy with authentication error
<b>Replay Error Packets</b>	Number of error packets handled by a policy with replay error.
<b>Decryption Error Rate (%)</b>	Decryption error rate of a policy
<b>Authentication Error Rate (%)</b>	Authentication error rate of a policy
<b>Replay Error Rate (%)</b>	Replay error rate of a policy

---

# Index

## A

- AH Hash Key dialog box 5
- Alarm Conditions dialog box 35, 37
- Alarm Definition dialog box 34
- Alarm Definitions dialog box 33
- Alarm logs 40
- alarms
  - adding System Probe counters 35
  - adding VPN peer probes 37
  - built-in 31
  - defining 31–38
  - overriding 32
  - types of 31
- appliances
  - archiving profile as an XML file 52
  - remotely restarting 50
  - remotely shutting down 51
  - restoring to factory-default state 51
  - synchronizing clock with CPM Server 52
  - viewing logs for 41
- Authentication dialog box 14
- authentication, changing process for 14

## B

- Backup/Restore dialog box 55

## C

- case studies
  - Dynamic NAT 59
  - QoS actions 60
  - tunnel switching 63
- Certificate-based authentication (VLAN) 27
- Change Global Alarm Name dialog box 34
- Change Individual Alarm Name dialog box 34
- clocks, synchronizing with CPM Server 52
- CPM

- backing up database 54
- configuration files 67
- CPM Client Config file 70
- CPM database, backing up 54
- CPM Open dialog box 55
- CPM Server
  - installing on Solaris host 53
  - restoring archived database 55
  - viewing the CPM Server log 41
- CPM Server Config file 67
- CPM Server Information dialog box 41
- custom IPsec actions, creating 2

## D

- dialog boxes
  - AH Hash Key 5
  - Alarm Conditions 35, 37
  - Alarm Definition 34
  - Alarm Definitions 33
  - Authentication 14
  - Backup Confirmation 55
  - Backup/Restore 55
  - Backup/Restore (Backup tab) 54
  - Change Global Alarm Name 34
  - Change Individual Alarm Name 34
  - CPM Open 55
  - CPM Server Info (Server Log tab) 41
  - CPM Server Information 41
  - ESP Encryption Key 4
  - ESP Hash Key 4
  - Filter 44
  - IKE Proposal 10
  - IPsec Action 3
  - pre-shared key 17
  - Select Directory 46
  - Select IKE Proposal 8
  - System Configuration 42
- Dynamic NAT case study 59

## E

- entering VLAN IDs

---

user domain tenants ??–20, 21–??, 25–26, 28

ESP Encryption Key dialog box 4

ESP Hash Key dialog box 4

ESP protocols, configuring 4

Event logs 40

## F

Filter dialog box 44

## I

IKE pairs, selecting existing settings for 8

IKE Proposal dialog box 10

IKE proposals, creating new 9

IPSec Action dialog box 3

IPSec actions, creating custom 2

IPSec manual key policies  
creating 1–5

## L

Log Manager window 42

logs

archiving log files 45

filtering the contents of 44

managing large number of entries 43

revising settings for 42

setting up and managing 39–47

size and rollover 40

types of 39

viewing for specific appliances 41

## M

Manual Authentication (VLAN) 27

manual key policies

creating 1–5

## O

overriding alarms 32

## P

Phase One/Two SA logs 40

Pre-shared Key dialog box 17

preshared key, defining custom 17

probe counters 31

probes

real-time monitor 73–82

profiles, archiving as XML file 52

## Q

QoS actions, case study 60

## R

RAS User logs 40

real-time monitor probe counters 73–82

## S

Select Directory dialog box 46

Select IKE Proposal dialog box 8

Solaris, installing CPM Server on 53

Storing Virtual LAN tenant ID's ??–25

System Configuration dialog box 42

system probe counters 31

## T

Traffic logs 40

Transport mode 3

Tunnel mode 3

tunnel switching, case study 63

---

# V

## VLAN

- activating "authenticate with certificates" 28
- advantages 21
- Case studies 62
- certificate-based authentication 27
- creating policies ??–30
- entering user domain tenant IDs ??–20, 21–??, 25–26, 28
- importing a VPN certificate into a user's browser 29
- manual authentication 27
- multiple-tenant domain management ??–30
- obtaining and using VPN certificates ??–30
- policies overview 20
- storing tenant IDs ??–25
- user domain authentication overview 27
- User domain policies 25

## Vmanager

- how to create multi-tenant domain policies 20
- User domain policies 25

## VPN peer probes 32