

Configuring Checkpoint VPN-1 for use with the PGP VPN Client

PGP Version 6.5.1

Checkpoint VPN-1 Version 4

COPYRIGHT

Copyright © 1999 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

** ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, Compass 7, CNX, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee Associates, McAfee, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetRoom, NetScan, Net Shield, NetShield, Net Tools, NetOctopus, NetStalker, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, T-POD, TeleSniffer, TIS, TMach, TMeg, Trusted Mach, Trusted Mail, Total Network Visibility, Total Virus Defense, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall, and ZAC 2000* are registered trademarks of Network Associates and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

LICENSE AGREEMENT

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Table of Contents

Chapter 1. Introduction	5
Organization of this Document	5
Basic Requirements	5
Software Requirements	5
Hardware Requirements	6
Chapter 2. Installation and Configuration	7
Installing PGP	7
Installing Checkpoint	7
Setting up a basic network	8
Create Checkpoint's Network Objects	9
Configuring the Network Objects' IPSec settings	9
Integrated Firewall—Peterson	10
Internal Workstation—Versa	11
External Workstation—Chico	12
Checkpoint rules—the very basics	15
PGPnet Configuration on Chico	17

The **PGP VPN Client** is a full-featured desktop encryption and authentication solution incorporating integrated email, file, disk and network security. The virtual private network component of this product is known as “PGPnet.”

This guide describes how to configure PGP VPN Client version 6.5.1 or later to work with Checkpoint VPN-1 software. **This document does not attempt to describe how to configure Checkpoint in general.**

This document describes the process of establishing connections via shared secrets (passwords). Later versions of this document will discuss the use of certificates in establishing secure connections.

Organization of this Document

[Chapter 1, “Introduction”](#) (this chapter) describes product requirements and provides an overview of the configuration process.

[Chapter 2, “Installation and Configuration”](#) describes how to configure Checkpoint VPN-1 for use with PGPnet.

Basic Requirements

Before you begin, we recommend that you become familiar with installing and using the PGP VPN Client.

Software Requirements

You must have the following software:

- PGP VPN Client, Version 6.5.1
- The strong-crypto version of Checkpoint's VPN-1 software (TripleDES) (Your installer CD's label should state “Strong DES Edition.”)
- The appropriate license code to use when installing (“vpnstrong”)
- Checkpoint's Service Pack 2. Ensure the one you use is the “Strong DES” or “TripleDES” version.

Hardware Requirements

NOTE: This document assumes the use of a Windows NT machine running the Checkpoint firewall software. Be aware that the Checkpoint software is available on other platforms; the settings discussed in this document are Windows NT-specific.

You must have the following hardware:

- A Windows NT 4.0 machine containing two network cards. Each card must have a static IP address.
- At least one Ethernet hub.
- At least one machine to put in the protected area behind the firewall.
- At least one machine to host PGPnet on the external side of the firewall. This machine must meet the requirements for PGPnet operation.

Installing PGP

The instructions for installing the PGP VPN Client are available in the documentation that accompanies the PGP product.

Do not install PGP on the same machine on which you plan to install Checkpoint.

Installing Checkpoint

Before you install, make sure you have your Checkpoint license codes available. The license information provided by Checkpoint consists of both the features that you have purchased (such as “vpnstrong”) and an alphanumeric license code.

The license code is based on the features you have purchased and the external static IP address of the firewall, so bear in mind that you will need to obtain a new code from Checkpoint if your IP address changes or if you need to add more features to the firewall.

NOTE: If you do receive a new license code, it does not have to replace the old one, but can be added to it.

1. On the CD, go to the **Windows** directory and run **Setup.exe** to install Checkpoint.
2. Reboot.
3. Run Checkpoint’s **Service Pack 2**.
4. Set up an Administrator account for yourself in the **FireWall-1 Configuration** utility.

At this point you are ready to log in to Checkpoint and set up your firewall. See the documentation that accompanies the Checkpoint VPN-1 firewall for instructions on how to log in and set up the firewall itself.

Setting up a basic network

NOTE: The following examples and screen captures are based on a test-lab setting. The examples show one of the most basic of IPSec configurations: one firewall, one external client, and one protected machine behind the firewall.

The machines described in the examples have the following names: the firewall is named **Peterson**, the external client is named **Chico**, and the protected machine is named **Versa**.

You must supply two network cards for the machine that is housing the firewall, and each card must have a static IP address. One of the network cards is the interface to the external, or untrusted, network and the other card is the interface to the internal, or trusted, network.

The test network described in this document is described below. Check with your network administrator to obtain IP addresses for your own use; the ones supplied below are examples:

Name	Role	Interface/Location	IP Address
Peterson	Checkpoint Firewall	External (Untrusted)	123.45.67.89
Peterson	Checkpoint Firewall	Internal (Trusted)	192.168.100.100
Chico	Workstation	Untrusted Network	123.45.67.88
Versa	Workstation	Trusted Network	192.168.100.101

Table 2-1. The Network Objects

Create Checkpoint's Network Objects

Before you set up any FireWall-1 rules, you should set up the Network Objects (machines identified to the firewall) that will be participating in the IPSec communications.

1. Launch the **Security Policy** program, which should be located in **Start→Program Files→FireWall-1**
2. Log in using the Administrator account you created previously.
3. Choose **Network Objects** from the **Manage** menu.
4. Click **New** to create a new Integrated Firewall, and then repeat the process to add two new Workstation entries. In this case, we created the objects described in [Table 2-1](#).

Once you have created these objects, the Network Objects list will appear as shown in [Figure 2-1](#).

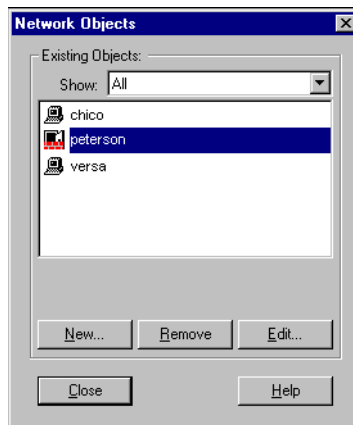


Figure 2-1. The Network Objects dialog box

Configuring the Network Objects' IPSec settings

The following sections describe in detail how to configure the IPSec features of the Network Objects you created.

The Network Objects consist of:

- The [Integrated Firewall—Peterson](#)
- The [Internal Workstation—Versa](#)
- The [External Workstation—Chico](#)

Integrated Firewall—Peterson

For this example, we created a new Integrated Firewall and named it **Peterson**.

In the **Network Objects** dialog box, select **Peterson** and click **Edit**.

General settings

Figure 2-2 displays the items that must be set on the **General** tab of the **Workstation Properties** dialog:

- **IP address.** The IP address shown is the address of the network card for the external, or untrusted, network.
- **Location.** In the example, **Location** is set to **Internal**, meaning that the firewall is gateway between the internal and external networks.
- **Type.** Here, **Type** must be set to **Gateway**.
- **FireWall-1 installed** is checked with **Version** set to **4.0**.

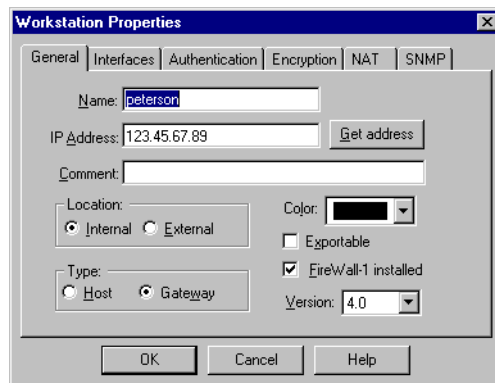


Figure 2-2. General settings for Peterson

Encryption Settings

Once you have made settings on the **General** tab for **Peterson**, navigate to the **Encryption** tab as shown in Figure 2-3.

- **Encryption Method.** Enable either **CAST**, **3DES**, or both.

NOTE: Do not enable **DES**. PGPnet does not support 56-bit **DES**. Its key size is too small and it does not meet PGP's nor the IETF's standard for strong cryptography.

- **Hash Method.** Enable either **MD5**, **SHA1**, or both.
- **Authentication Method.** **Pre-shared secret** is set in [Figure 2-3](#), but note that you can't actually set this until the other Network Objects are created. This process is covered later in the document, in the section “[Encryption Settings](#)” on page 13.

NOTE: Do not enable **Supports Aggressive Mode**, as this is not compatible with PGPnet.

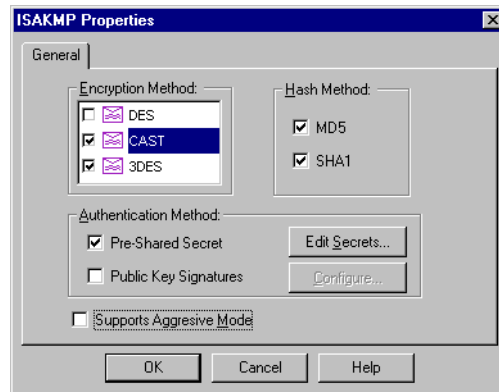


Figure 2-3. Encryption settings for Peterson

Internal Workstation—Versa

In the example, **Versa** is the workstation used in the trusted area of the network; that is, the machine that is protected behind the firewall.

NOTE: In the example, the IPSec connection is a tunnel to the firewall and not beyond it; so **Versa** does not require any encryption options.

- The **IP address** should be set to one that is in the same network as the internal interface of the firewall.
- **Location** is set to **Internal**.
- **Type** is set to **Host**.

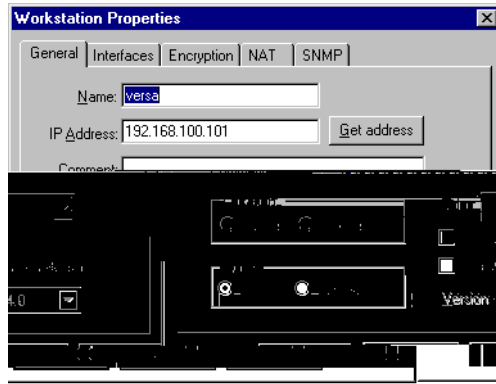


Figure 2-4. General Settings for Versa

External Workstation—Chico

Chico is a workstation that sits outside the firewall in the untrusted area. In most cases, the untrusted area is located on the Internet, outside your trusted network.

Chico is the machine running PGPnet.

NOTE: “Shared secret” authentication requires that you specify the IP address and identity of the external workstation, as shown in [Figure 2-5](#).

General Settings

- **IP address.** Enter Chico’s IP address.

In this example, **Chico** is on the same network as the external interface of the firewall, but it need not be that way. The only requirement is that the two machines be able to successfully route IP traffic back and forth.

- Set **Location** to **External**.
- Set **Type** to **Host**.

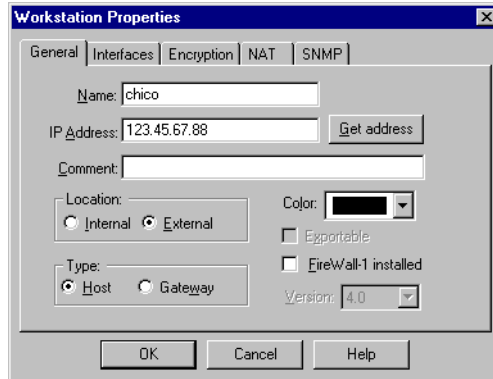


Figure 2-5. General settings for Chico

Encryption Settings

Because **Chico** is the machine running PGPnet, you must set encryption options on **Chico** itself. Checkpoint, however, still needs to know what sort of IPSec traffic will be coming from that workstation. (See [Figure 2-6](#).)

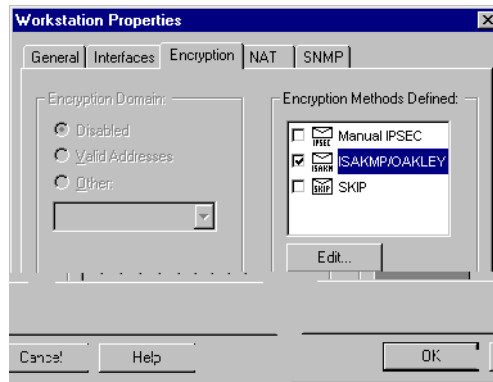


Figure 2-6. Encryption settings for Chico

- Enable **ISAKMP/OAKLEY**.

NOTE: Do not enable either **Manual IPsec** or **SKIP**.

- Click **Edit**.

The **ISAKMP Properties** window appears, as shown in [Figure 2-7](#).

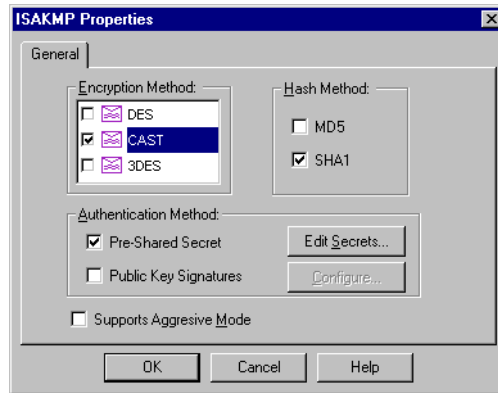


Figure 2-7. ISAKMP Properties for Chico

- Enable either **CAST**, **3DES**, or both.

NOTE: Do not enable **DES**.

- Enable either **MD5**, **SHA1**, or both.

NOTE: Do not enable **Supports Aggressive Mode**, as this is not compatible with PGPnet.

- Enable **Pre-Shared Secret** and click **Edit Secrets**. This causes the **Shared Secret** dialog to appear, as shown in [Figure 2-8](#). (Recall that we could not set this before with **Peterson** because you must have configured at least two Network Objects to set a shared secret.)

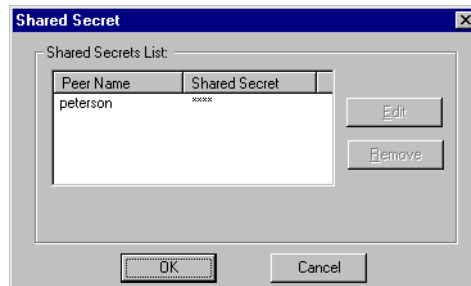


Figure 2-8. Shared Secret setup

- Select the object/machine with which you wish to communicate.

- Click **Edit** and set a **Shared Secret**—a password or passphrase.
- This same **Shared Secret** must be set in the **PGPnet** settings on **Chico** itself.

This tells Checkpoint that **Chico** is going to attempt an IPSec connection with **Peterson** using the Shared Secret that you specify.

Checkpoint rules—the very basics

In a real-world environment, a Checkpoint FireWall-1 is usually configured with a large set of rules. These rules are used to implement the organization's security policy. Here we are concerned only with the mechanics of establishing IPSec communication.

- Create a new rule: select **Edit**→**Add Rule**→**Top**. The FireWall-1 Security Policy dialog appears.
- In the new rule, right-click on **Any** in the **Source** column and choose **Add**. Then pick your external workstation from the **Network Objects** dialog (in this case, **Chico**).
- Do the same for **Destination**, but instead pick your internal or trusted workstation (in this case, **Versa**).
- Now set your **Action** to **Encrypt**. To do this, right-click on **Drop** in the **Action** column and choose **Encrypt**.

NOTE: Do not select **Client Encrypt** (this is a feature you would use to Encrypt to SecuryRemote)

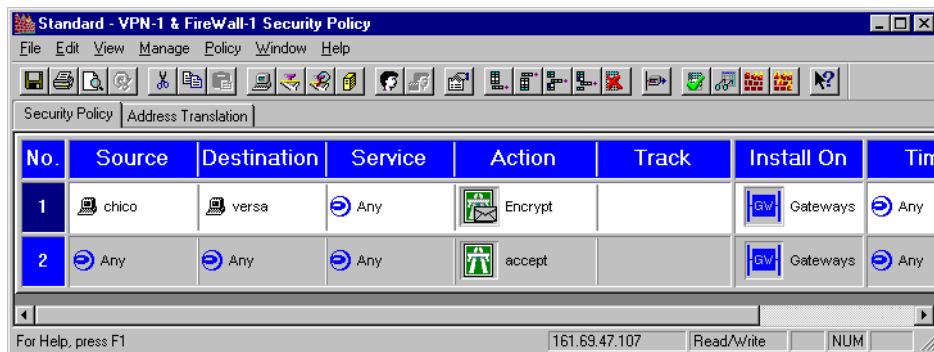


Figure 2-9. Settings for the Checkpoint Security Policy

Action—Encrypt

The preceding steps establish an **Encrypt** rule, but you still have to specify the **Encryption Properties** for that rule.

- To get the **Encryption Properties** dialog, right-click on the **Encrypt** entry in the **Action** column of the rule you just created.
- Select **ISAKMP/OAKLEY** as shown in [Figure 2-10](#), and then click **Edit**.

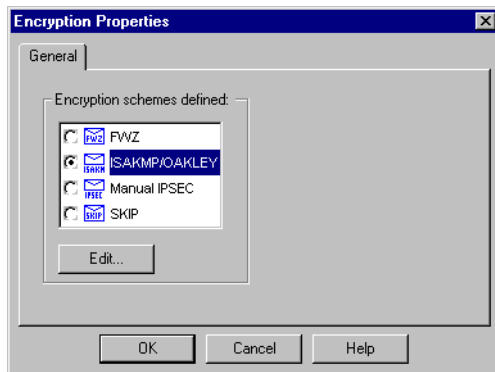


Figure 2-10. Encryption Properties

- The **ISAKMP Properties** dialog will appear as shown in [Figure 2-11](#).

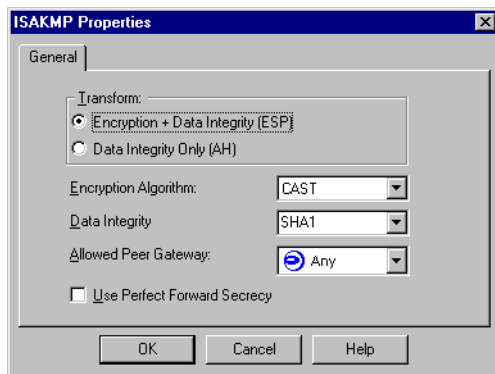


Figure 2-11. ISAKMP Properties

- Select either **Transform** choice.
 - **ESP** will perform both encryption and authentication.
 - **AH** performs only authentication. If you choose **AH**, make sure that your advanced PGPnet settings have an IPsec proposal that matches this dialog.

- For **Encryption Algorithm** select **CAST** or **3DES**.

NOTE: Do not select **DES**, **DES-40CP**, or **CAST-40**.

- For **Data Integrity** select either **MD5** or **SHA1**.
- You may enable **Use Perfect Forward Secrecy** or simply leave it unchecked.
- Install your new Security Policy. (See the Checkpoint documentation for instructions.)

You have now completed all of the steps required for Checkpoint.

PGPnet Configuration on Chico

The machine in the external network—the one running PGPnet—needs no custom IPsec configuration settings.

NOTE: If you decide to change PGPnet's default settings, do not set the following PGPnet Advanced options, as they are incompatible with Checkpoint:

- 1536-bit Perfect Forward Secrecy (use 1024).
- Any IPPCP settings (neither LZS nor Deflate are supported in Checkpoint).

You must create **Host** entries in PGPnet as shown in [Figure 2-12](#). For more details on configuring PGPnet and working with the **Hosts** panel, see the PGP documentation.

- Create a **Gateway** entry in the **Host** list. It should have the **IP address** of the external interface of the Checkpoint firewall (in this case, **Peterson**).

IMPORTANT: The **Gateway** entry must have the same shared secret as that entered in the Checkpoint setup.

- Create a sub-entry (for **Versa**, in this case) underneath the **Gateway**.
- Select the Gateway entry (**Peterson**) and click **Connect**.
- The green ball should appear, indicating a successful connection.

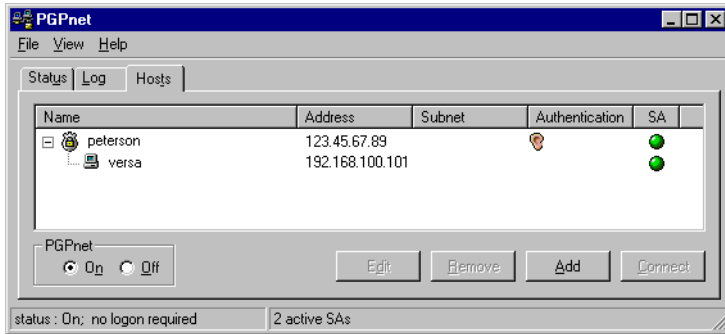


Figure 2-12. The PGPnet Hosts list