

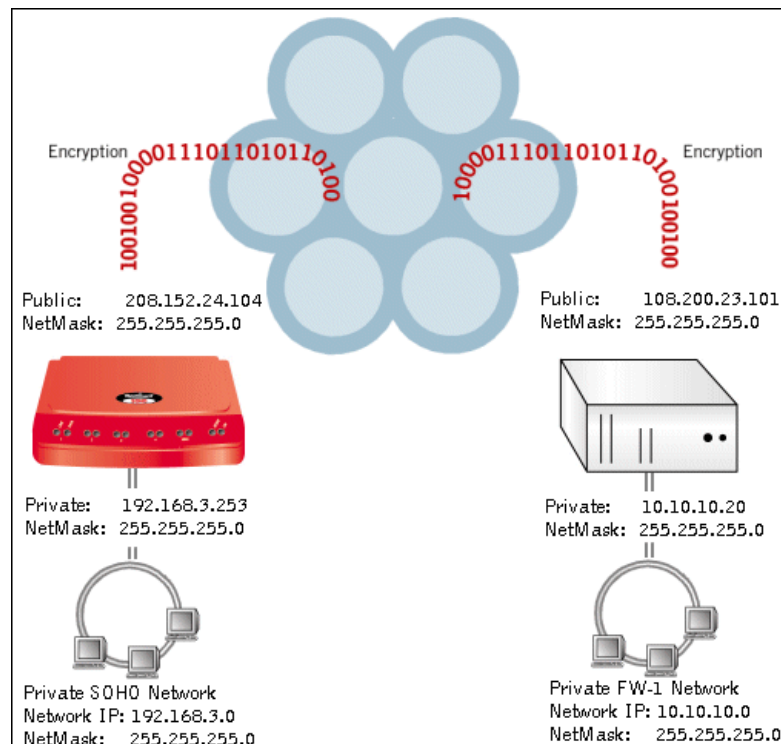
Configuring a Check Point FireWall-1 to SOHO IPsec Tunnel

This document describes the procedures required to configure an IPsec VPN tunnel between a WatchGuard SOHO or SOHO | tc and a Check Point FireWall-1.

The following WatchGuard SOHOs support IPsec tunnels:

- WatchGuard SOHO with VPN Feature Key
- WatchGuard SOHO | tc

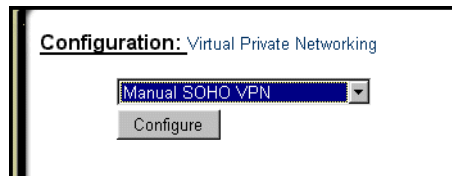
The following diagram illustrates the machines and addresses involved in the connection. The examples used in this document are taken from this set-up.



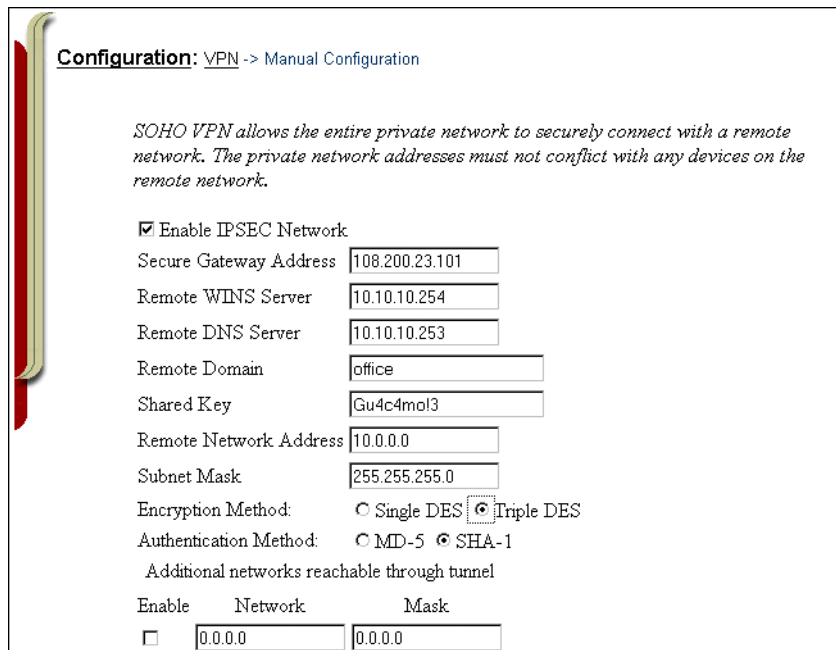
Configuring the WatchGuard SOHO for VPN

This section describes how to configure the WatchGuard SOHO (firmware version 2.3.x) for an IPsec tunnel with a Check Point FireWall-1.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Private IP address of the SOHO.
The default IP address is: 192.168.111.1.
- 2 Click **Virtual Private Networking**.
The Virtual Private Networking page appears.



- 3 Select **Manual SOHO VPN** from the drop list. Click **Configure**.
The Manual Configuration page appears.



Configuration: VPN -> Manual Configuration

SOHO VPN allows the entire private network to securely connect with a remote network. The private network addresses must not conflict with any devices on the remote network.

Enable IPSEC Network

Secure Gateway Address

Remote WINS Server

Remote DNS Server

Remote Domain

Shared Key

Remote Network Address

Subnet Mask

Encryption Method: Single DES Triple DES

Authentication Method: MD-5 SHA-1

Additional networks reachable through tunnel

Enable	Network	Mask
<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

- 4 Check the **Enable IPSEC Network** checkbox.
- 5 Complete the following fields:
 - Secure Gateway Address**
The public, external IP address of the FireWall-1 device. In our example, 108.200.23.101.
 - Remote WINS Server**
The WINS server behind the FireWall-1 device. (This field is optional.)
 - Remote DNS Server**
The DNS server behind the FireWall-1 device. (This field is optional.)

Remote Domain

The remote domain behind the FireWall-1 device. *(This field is optional.)*

Shared Key

Similar to a password, this is used to authenticate both ends of the tunnel to each other; the shared key must be identical on both sites.

Remote Network Address

The address of the network on the trusted side of the FireWall-1 device. In our example, 10.10.10.0.

Subnet Mask

The mask of the network on the trusted side of the FireWall-1 device. In our example, 255.255.255.0.

Encryption Method

The encryption level (single-DES or triple-DES) must match the encryption set in the FireWall-1 configuration. In our example, 3DES.

Authentication Method

The algorithm type (MD-5 or SHA-1) must match the authentication method set for the FireWall-1 device. In our example, SHA-1.

Additional Networks Reachable Through Tunnel

Additional networks on the trusted side of the FireWall-1 device that you wish to connect through this tunnel. These must be configured on the FireWall-1 device as well. *(This field is optional.)*

- 6 Review the configuration information you entered. Click **Submit** at the bottom of the page.
- 7 A page appears prompting you to reboot the SOHO. Confirm your settings, then click **Reboot**.

Configuring FireWall-1 for a SOHO to FireWall-1 IPSec Tunnel

This section describes how to configure the Check Point FireWall-1 version 4.1 SP2 for a tunnel that has a WatchGuard SOHO at the other end.

This document assumes that you have successfully activated the interfaces on the Check Point FireWall-1 and that you have installed the following:

- Version 4.1 SP2 of the FireWall-1 software and have started it
- Version 4.1 of the GUI on the management station

Creating a New Security Policy

- 1 Open the Check Point Policy Editor in the FireWall-1 GUI.
- 2 Select **File** ⇒ **New**.
The New Security Policy dialog box appears.
- 3 Enter the following information:

Policy Name

Enter the name of the configuration you are about to create. In our example, Test.

Policy Type

Select **Security and Address translation**.

Helpers

Select **Empty Policy**.

4 Click **OK**.

Tabs appear for the policy you just created. Following our example, these tabs are labeled Security Policy - Test, Address Translation - Test, and Bandwidth Policy - Standard.

Create Network Objects

To allow IPSec traffic between network addresses you must create icons for the network addresses in question as well as the local and remote firewalls.

Start by creating an icon for the private network behind the SOHO:

1 Select **Manage** ⇒ **Network Objects**.

The Network Objects dialog box appears.

2 Click **New**. Select **Network**.

The Network Properties dialog box appears.

3 Click the **General** tab. Enter the following information:

Name

Enter a name for the network for which this Network Object is being created. In our example, the private network behind the SOHO is named, SOHO-net.

IP Address

Enter the IP address of the network. In our example, 192.168.3.0.

Netmask

Enter the netmask of the network. In our example, 255.255.255.0.

Comment

Add comments or reminders about this configuration. (*This field is optional.*)

Location

Select **External**.

Broadcast

Select **Allowed**.

Color

Select a color for this particular service icon.

4 Leave the NAT tab set to the default settings. Click **OK**.

The Network Objects dialog box appears with the new icon.

Then create an icon for the private network behind the FireWall-1:

1 Click **New**. Select **Network**.

The Network Properties dialog box appears.

2 Click the **General** tab. Enter the following information:

Name

Enter a name for the network for which this Network Object is being created. In our example, the private network behind the FireWall-1, is named, FW1-net.

IP Address

Enter the IP address of the network. In our example, 10.10.10.0.

Netmask

Enter the netmask of the network. In our example, 255.255.255.0.

Comment

Add comments or reminders about this configuration. (*This field is optional.*)

Location

Select **Internal**.

Broadcast

Select **Allowed**.

Color

Select a color for this particular service icon.

- 3 Leave the NAT tab set to the default settings. Click **OK**.
The Network Objects dialog box appears with the new icon.
- 4 The two network icons should now be displayed as, following our examples, FW1-net and SOHO-net.

Configuring Workstations

Perform the following steps to configure the Workstations, that is, the local and remote firewalls.

Start by creating a Workstation for the SOHO. From the Network Objects dialog box:

- 1 Click **New**. Select **Workstation**.
The Workstation Properties dialog box appears.
- 2 Click the **General** tab. Enter the following information:
 - Name**
Enter a name for the firewall for which this Workstation is being created. In our example, SOHO.
 - IP Address**
Enter the external interface IP address of the SOHO. In our example the public, or external IP of the SOHO is 208.152.24.104.
 - Comment**
Add comments about this configuration. (*This field is optional.*)
 - Location**
Select **External**.
 - Type**
Select **Gateway**.
 - Modules Installed**
Since we are defining the SOHO at this point and not the FireWall-1, leave these checkboxes disabled.
 - Color**
Select a color for this particular service icon.
- 3 Click the **Interfaces** tab of the WorkStation Properties dialog box. Click **Add**.
The Interface Properties dialog box appears.
- 4 Click the **General** tab of the Interface Properties dialog box. Click **Add**.
- 5 Enter the following information:
 - Name**
Enter a name for the external interface of the firewall for which this Workstation is being created. In our example, to represent the public, or external interface of the SOHO enter, eth0.
 - Net Address**
Enter the IP address assigned to this particular interface. In our example the public, or external IP of the SOHO is 208.152.24.104.

-
- Net Mask*
Enter the netmask for the IP address assigned to this particular interface. In our example, 255.255.255.0.
- 6 You must also define the private, or internal interface of the SOHO. Again, click **Add**.
- 7 Enter the following information:
- Name*
Enter a name for any other interfaces of the firewall for which this Workstation is being created. In our example, to represent the private, or internal interface of the SOHO enter, eth1.
- Net Address*
Enter the IP address assigned to this particular interface. In our example the private, or internal IP of the SOHO is 192.168.3.253.
- Net Mask*
Enter the netmask for the IP address assigned to this particular interface. In our example, 255.255.255.0.
- 8 Click **OK** to close the Interface Properties dialog box.
The two interfaces should now be displayed on the Interface tab as, following our examples, eth0 and eth1.
- 9 Leave the SNMP and NAT tabs set to the default settings. Click the **VPN** tab.
Enter the following information:
- Domain*
This associates the firewall you are defining with a domain that will use the IPsec tunnel. Following our example, to define a domain behind the SOHO, choose **Other** and select **SOHO-net** from the drop down list.
- Encryption Schemes Defined*
Select **IKE**.
- 10 Click **Edit**.
The IKE Properties window appears. The IKE Properties window allows you to define the Phase 1 negotiation settings for the FireWall-1.

NOTE

The default settings on the SOHO for Phase 1 negotiations are DES, SHA1, and Diffie Helman group 1. These settings cannot be changed. Therefore, it is absolutely critical that the Check Point FireWall-1 is configured to use DES, SHA1, and Diffie Helman group 1 for this Phase of the negotiation.

- 11 Enter the following information:
- Key Negotiation Encryption Method*
Select the encryption method to be used in Phase 1 negotiations. This must be DES, since the SOHO will only use DES in Phase 1.
- Hash Method*
Select the hash method to be used in Phase 1 negotiations. This must be SHA1, since the SOHO will only use SHA1 in Phase 1.
- Authentication Method*
Select **Pre-Shared Secret**.
- Supports Aggressive Mode*
Leave this checkbox disabled.

Supports Subnets

Enable this checkbox.

- 12 Click **Edit Secrets** in the Authentication Method field.
The Shared Secret window appears.
 - 13 Select **FW-1**. Click **Edit**.
The Enter Secret dialog box will appear.
 - 14 Enter the shared secret for this IPSec tunnel.
This value must be the same on both the FireWall-1 and the SOHO.
 - 15 Click **Set**. Click **OK**.
The SOHO Workstation is now configured. The Network Objects dialog box appears.
- Now create a Workstation for the FireWall-1. From the Network Objects dialog box:

- 1 Click **New**. Select **Workstation**.
The Workstation Properties dialog box appears.
- 2 Click the **General** tab. Enter the following information:
 - Name**
Enter a name for the firewall for which this Workstation is being created. In our example, FW1.
 - IP Address**
Enter the external interface IP address of the FireWall-1. In our example the public, or external IP of the FireWall-1 is 108.200.23.101.
 - Comment**
Add comments about this configuration. (*This field is optional.*)
 - Location**
Select **External**.
 - Type**
Select **Gateway**.
 - Modules Installed**
Enable both **VPN-1 & FireWall-1** as well as **Management Station**. Then select **4.1** from the Version drop down list.
 - Color**
Select a color for this particular service icon.
- 3 Click the **Interfaces** tab of the WorkStation Properties dialog box. Click **Add**.
The Interface Properties dialog box appears.
- 4 Click the **General** tab of the Interface Properties dialog box. Click **Add**.
- 5 Enter the following information:
 - Name**
Enter a name for the external interface of the firewall for which this Workstation is being created. In our example, to represent the public, or external interface of the FireWall-1 enter, eth-s5.
 - Net Address**
Enter the IP address assigned to this particular interface. In our example the public, or external IP of the FireWall-1 is 108.200.23.101.
 - Net Mask**
Enter the netmask for the IP address assigned to this particular interface. In our example, 255.255.255.0.
- 6 You must also define the private, or internal interface of the FireWall-1. Again, click **Add**.

-
- 7 Enter the following information:

Name

Enter a name for any other interfaces of the firewall for which this Workstation is being created. In our example, to represent the private, or internal interface of the FireWall-1 enter, eth-s3.

Net Address

Enter the IP address assigned to this particular interface. In our example the private, or internal IP of the FireWall-1 is 10.10.10.20.

Net Mask

Enter the netmask for the IP address assigned to this particular interface. In our example, 255.255.255.0.

- 8 Click **OK** to close the Interface Properties dialog box.

The two interfaces should now be displayed on the Interface tab as, following our examples, eth-s3 and eth-s5.

- 9 Leave the SNMP, NAT, Certificates, and Authentication tabs set to the default settings. Click the **VPN** tab. Enter the following information:

Domain

This associates the firewall you are defining with a domain that will use the IPSec tunnel. Following our example, to define a domain behind the FireWall-1, choose **Other** and select **FW1-net** from the drop down list.

Encryption Schemes Defined

Select **IKE**.

- 10 Click **Edit**.

The IKE Properties window appears. The IKE Properties window allows you to define the Phase 1 negotiation settings for the FireWall-1.

- 11 Enter the following information:

Key Negotiation Encryption Method

Select the encryption method to be used in Phase 1 negotiations. This must be **DES**, since the SOHO will only use **DES** in Phase 1.

Hash Method

Select the hash method to be used in Phase 1 negotiations. This must be **SHA1**, since the SOHO will only use **SHA1** in Phase 1.

Authentication Method

Select **Pre-Shared Secret**.

Supports Aggressive Mode

Leave this checkbox disabled.

Supports Subnets

Enable this checkbox.

- 12 Click **Edit Secrets** in the Authentication Method field.

The Shared Secret window appears.

- 13 Select **SOHO**. Click **Edit**.

The Enter Secret dialog box will appear.

- 14 Enter the shared secret for this IPSec tunnel.

This value must be the same on both the FireWall-1 and the SOHO.

- 15 Click **Set**. Click **OK**.

The FireWall-1 Workstation is now configured. The Network Objects dialog box appears.

- 16 Click **Close** to exit the Network Objects dialog box.

The Check Point Policy Editor window appears.

Creating Rules on the FireWall-1

From the Check Point Policy Editor:

- 1 Select **File** ⇒ **Open**. Select the security policy you created for this tunnel.
- 2 Select **Edit** ⇒ **Add Rule** ⇒ **Top**.
This adds a new rule to the security policy which should be numbered 1. It will have the following columns listed at the top:
No.
Security policy rule number.
Source
Source of the traffic for that rule.
Destination
Destination of the traffic for that rule.
Service
Protocol(s) defined for that rule.
Action
Action taken for traffic passed via that rule.
Track
Type of logging selected for that rule.
Install On
Machines on which you want to install the rule.
Comment
Space to add comments or notes for that rule.
- 3 Right-click the **Source** section. Select **Add**.
The Add Object dialog box appears.
- 4 Select the SOHO network icon you created previously. Following our example, SOHO-net. Click **OK**.
This adds the SOHO network icon to the source list for this rule.
- 5 Right-click the **Source** section. Select **Add**.
The Add Object dialog box appears.
- 6 Select the FireWall-1 network icon you created previously. Following our example, FW1-net. Click **OK**.
This adds the FireWall-1 network icon to the source list for this rule as well.

NOTE

When performing the following steps to configure the **Destination** field, it is critical that the FireWall-1 network is added first before adding the SOHO network.

- 7 Right-click the **Destination** section. Select **Add**.
The Add Object dialog box appears.
- 8 Select the FireWall-1 network icon you created previously. Following our example, FW1-net. Click **OK**.
This adds the FireWall-1 network to the destination list for this rule.
- 9 Right-click the **Destination** section. Select **Add**.
The Add Object dialog box appears.
- 10 Select the SOHO network icon you created previously. Following our example, SOHO-net. Click **OK**.
This adds the SOHO network to the destination list for this rule.

-
- 11 Leave the **Service** section set to **Any**.
This will allow any traffic to flow between the two private networks using this tunnel.
 - 12 In the **Action** section, click the **Drop** icon.
This will reveal a menu of various options.
 - 13 Select **Encrypt** from the menu.

Define Settings for Phase 2 Negotiations

To define the settings that the FireWall-1 will use for phase 2 negotiations, in the Check Point Policy Editor:

- 1 Double-click the **Encrypt** icon from the Action section.
The Encryption Properties dialog box appears.
- 2 Select **IKE** from the Encryption Properties dialog box. Click **Edit**.
The IKE Properties dialog box appears.
- 3 Enter the following:
Transform
Following our example on the SOHO, select **ESP**.
Encryption Algorithm
Following our example on the SOHO, select **3-DES**.
Data Integrity
Following our example on the SOHO, select **SHA1**.
Allowed Peer Gateway
Select **SOHO**.
Perfect Forward Secrecy
Leave this checkbox disabled.
- 4 Click **OK** to close the IKE Properties dialog box. Click **OK** to close the Encryption Properties dialog box.
- 5 Right-click the **Track** section. Set it to **Long**.
This will enable verbose logging for this rule, useful for debugging.
- 6 Right-click the **Gateway** icon. Select **Add**.
- 7 Select **Targets**.
The Select Target window appears.
- 8 Select the **FW-1** icon. Click **OK**.
The FW-1 service icon will be added to the Install section of rule No. 1.
- 9 Right-click the **Gateways** icon under the **Install On** section. Select **Delete**.
This will remove the Gateway icon. You can leave the **Time** and **Comment** sections of this rule at the default settings.

Logging All Dropped Packets

To set up a rule that will allow you to log all dropped packets for trouble shooting purposes do the following:

- 1 Select **Edit** ⇒ **Add Rule** ⇒ **After**.
This adds a new rule to the security policy, No.2.
- 2 Leave the **Source** and **Destination** sections set to **Any**.
- 3 Right-click the **Track** section. Set it to **Long** for verbose logging.
- 4 Right-click the **Gateway** icon. Select **Add**.

- 5 **Select Targets.**
The Select Target window appears.
- 6 **Select the FW-1 icon. Click OK.**
The FW-1 service icon will be added to the Install section of rule No. 2.
- 7 **Right-click the Gateways icon under the Install On section. Select Delete.**
You can leave the **Time** and **Comment** sections of this rule at the default settings.

Saving and Installing the New Configuration

Finally, save the changes made to this configuration and install the new configuration to the FireWall-1.

- 1 **Select Policy ⇒ Properties.**
The Properties Setup dialog box appears.
- 2 **Ensure that the Accept VPN-1 & FireWall-1 Control Connections checkbox is enabled. Click OK.**
- 3 **Select File ⇒ Save** to save the security policy you just created.
- 4 **Install this configuration on the FireWall-1 by selecting Policy ⇒ Install.**

Copyright and Patent Information

Copyright© 1998 - 2001 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, and LiveSecurity are either a trademark or registered trademark of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

DocVer B-2.3.x-SOHO to Check Point FW-1