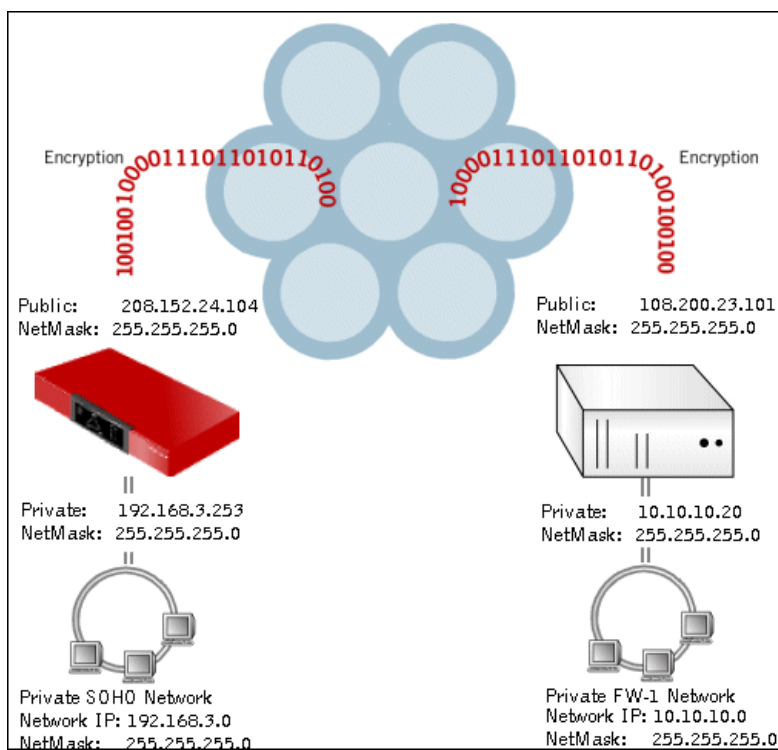


## Configuring an IPSec Tunnel between a Firebox & a Check Point FireWall-1

---

This document describes how to configure an IPSec tunnel with a WatchGuard Firebox II or Firebox III (software version 4.5 or later) at one end and the Check Point FireWall-1 (software version 4.1 SP2) at the other.

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 Firebox II for an IPSec Tunnel to a FireWall-1

---

This procedure describes how to configure a WatchGuard Firebox II, II *Plus* or II *Fast VPN* to create an IPSec Virtual Private Network (VPN) with a Check Point FireWall-1 device at the other end of the tunnel.

---

### NOTE

---

In the following documentation, "Firebox" is used to refer to the Firebox II or Firebox III family of WatchGuard firewalls.

---

To configure the Firebox for an IPSec tunnel, use the WatchGuard Policy Manager to configure the IPSec gateway, tunnel, routing information, and enable the associated policy.

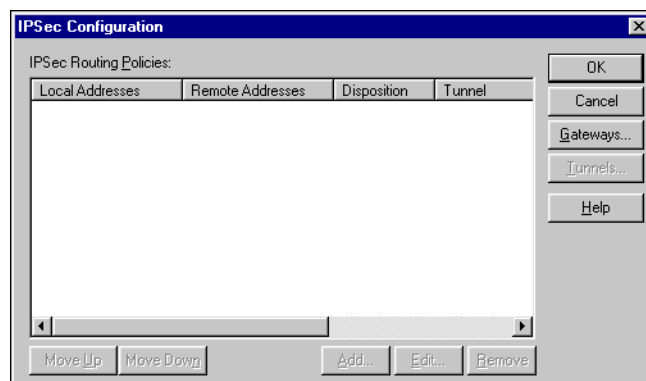
For more information about configuring a Firebox for an IPSec VPN tunnel, consult the *WatchGuard LiveSecurity System User Guide*.

## Setting Up the Gateway

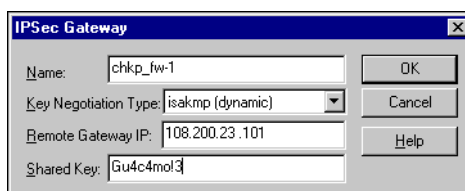
You must first define the remote gateway of the Check Point FireWall-1.

From the WatchGuard Policy Manager:

- 1 Select **Network** ⇒ **Branch Office VPN** ⇒ **IPSec**.  
The IPSEC configuration dialog box appears.



- 2 Select **Gateways**. Click **Add**.  
The IPSec Gateway dialog box appears.



- 3 Enter the gateway information as described below:  
**Name**  
The name used to identify this gateway.

### *Key Negotiation Type*

Select **isakmp (dynamic)**.

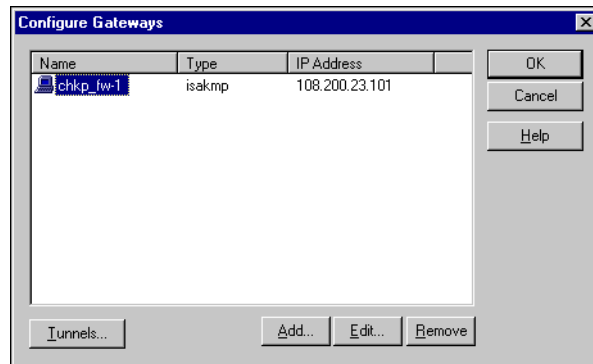
### *Remote Gateway IP*

The external IP address of the remote device that the Firebox will negotiate with when creating the IPSec tunnel. In this case, the FireWall-1.

### *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.

- 4 When you finish adding gateways, click **OK**  
The Configure Gateways dialog box appears displaying the new gateway.



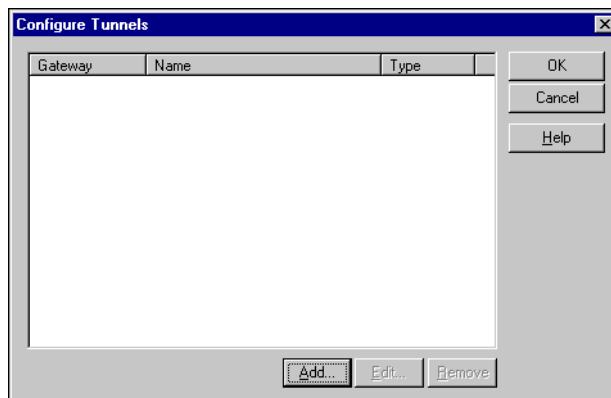
- 5 Click **Tunnels** to continue with Setting up the Tunnel (see below).

## Setting up the Tunnel

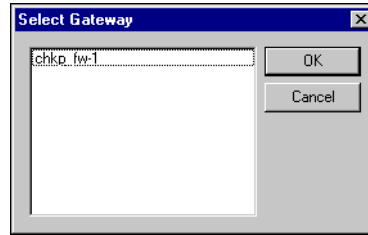
A tunnel encapsulates packets between two gateways. It specifies encryption type, authentication method, or both. A tunnel also specifies endpoints—these are the public, external addresses of the two devices. The following describes how to configure a tunnel using a gateway with the isakmp (dynamic) key negotiation type, which is required for creating a tunnel between a Firebox and a Check Point FireWall-1.

From the IPSec configuration dialog box:

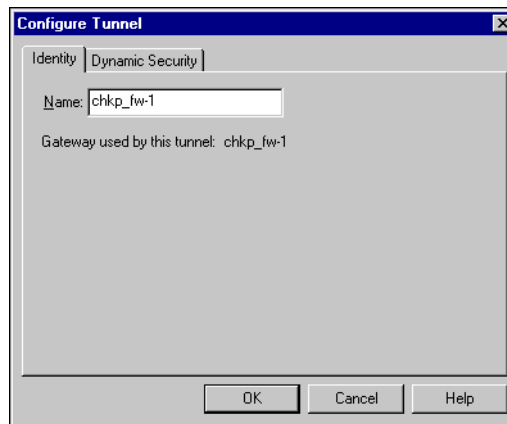
- 1 Click **Tunnels**.  
The Configure Tunnels dialog box appears.



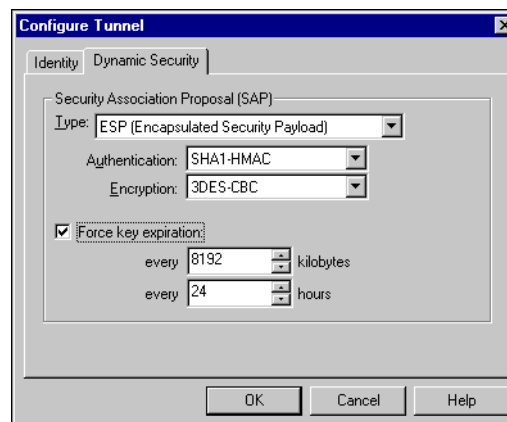
- To add a new tunnel, click **Add**.  
The Select Gateway dialog box appears.



- Click the gateway that you created in "Setting Up the Gateway" on page 2. Click **OK**.  
The Configure Tunnel dialog box appears.
- Enter a tunnel name.  
The Policy Manager uses the tunnel name as an identifier.



- Click the **Dynamic Security** tab.  
The Configure Tunnel dialog box appears.



- Enter the following information:

### Type

Select **ESP (Encapsulated Security Payload)**. This must match the Security Association Proposal type on the FireWall-1 device.

### Authentication

Select **SHA1-HMAC** (a 160-bit algorithm). This must match the authentication type on the FireWall-1 device.

### Encryption

Select **3DES-CBC** (168-bit). This must match the encryption level on the FireWall-1 device.

- 7 To have a new key generated periodically, enable the checkbox labelled **Force Key Expiration**.

With this option, transparent to the user, the ISAKMP controller generates and negotiates a new key for the session. For no key expiration, enter 0 (zero) here. If you enable the Force key expiration box, set the number of kilobytes transferred or hours passed in the session before a new key is generated for continuation of the VPN session.

- 8 Click **OK**.

The Configure Tunnels dialog box appears displaying the newly created tunnel.

- 9 After you add all tunnels for this gateway, click **OK**.

The Configure Gateways dialog box appears.

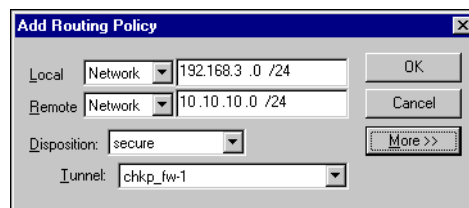
## Creating an IPSec Policy

Policies are sets of rules, much like static routes, for defining how IPSec traffic is routed through the tunnel. Policies are defined by their endpoints. These are not the same as tunnel or gateway endpoints—they are the specific hosts, networks, or both behind the two IPsec devices (for our purposes, the Firebox and the Check Point FireWall-1), which communicate through the tunnel.

From the IPSec Configuration dialog box:

- 1 Click **Add**.

The Edit Routing Policy dialog box appears.



- 2 Enter the following information:

### Local

Host or Network. You can create a policy for a single host or an entire network behind the local device. Following our example, select **Network** and enter the network address of the private, internal network behind the Firebox, 192.168.3.0/24.

### Remote

Host or Network. You can create a policy for a single host or an entire network behind the remote device. Following our example, select **Network** and enter the network address of the private, internal network behind the Pix, 10.10.10.0/24.

### *Disposition*

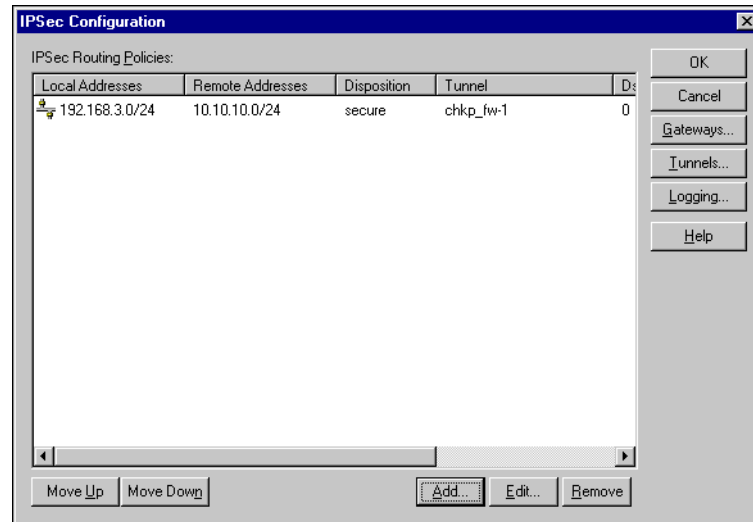
This determines how the Firebox will handle traffic travelling between the tunnel endpoints. Select **secure**.

### *Tunnel*

You can choose the tunnel you want to use between these networks. Following our example, select `cisco_pix`.

### 3 Click **OK**.

The IPSec Configuration dialog box appears listing the newly created policy. Policies are initially listed in the order in which they were created.



### 4 Click **OK** again to close the **IPSec Configuration** dialog box.

## **Creating Services**

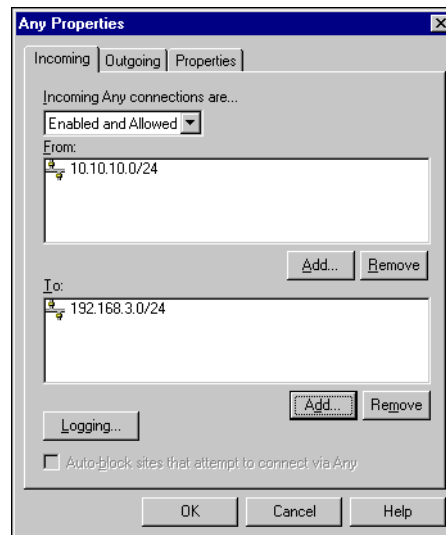
The last step defines what services are going to be allowed through this tunnel. Users behind the Cisco Pix 520 are outside the trusted Firebox network; you must therefore configure the Firebox specifically to allow traffic through the VPN connection. A quick method is to create a host alias that corresponds to the remote VPN hosts, networks, or both. Either use this alias or individually enter the IP addresses when configuring the properties for the service or services you wish to allow. For more information on creating an alias, consult the *WatchGuard LiveSecurity System User Guide*.

You can modify your Firebox security policy to allow the VPN traffic on a service-by-service basis. However, the easiest method is to create an Any service which allows *all* traffic over *any* port.

From the Policy Manager:

- 1 Select **Edit ⇒ Add Service**.
- 2 Expand **Packet Filters**.
- 3 Select the Any service. Click **Add**.  
The Add Service dialog box appears.

- 4 Click **OK**.  
The service's Properties dialog box appears.
- 5 At the **Incoming** tab, select **Enabled and Allowed** from the drop list.
- 6 Under **From**, click **Add**.  
The Add Address dialog box appears.
- 7 Click **Add Other**.  
The Add Member dialog box appears.
- 8 At the **Choose Type** drop list, select **Network IP Address** and enter the IP address of the private, internal network behind the Pix. Following our example, 10.10.10.0/24.
- 9 Click **OK**.  
The Add Address dialog box appears.
- 10 Click **OK**.  
The service's Properties dialog box reappears. It should display the IP Address you entered in the **From** portion of the dialog box.
- 11 Under **To**, click **Add**.  
The Add Address dialog box appears.
- 12 Click **Add Other**.  
The Add Member dialog box appears.
- 13 At the **Choose Type** drop list, select **Network IP Address** and enter the IP address of the private, internal network behind the Firebox. Following our example, 192.168.3.0/24.
- 14 Click **OK**.  
The Add Address dialog box appears.
- 15 Click **OK**.  
The service's Properties dialog box reappears. It should display the IP Address you entered in the **To** portion of the dialog box as well as the IP address of the **From** portion you entered earlier.



- 16 Click the **Outgoing** tab. Select **Enabled and Allowed** from the drop list.
- 17 Under **From**, click **Add**.  
The Add Address dialog box appears.

18 Click **Add Other**.

The Add Member dialog box appears.

19 At the Choose Type drop list, select **Network IP Address** and enter the IP address of the private, internal network behind the Firebox. Following our example, 192.168.3.0/24.

20 Click **OK**.

The Add Address dialog box appears.

21 Click **OK**.

The service's Properties dialog box reappears. It should display the IP Address you entered in the From portion of the dialog box.

22 Under To, click **Add**.

The Add Address dialog box appears.

23 Click **Add Other**.

The Add Member dialog box appears.

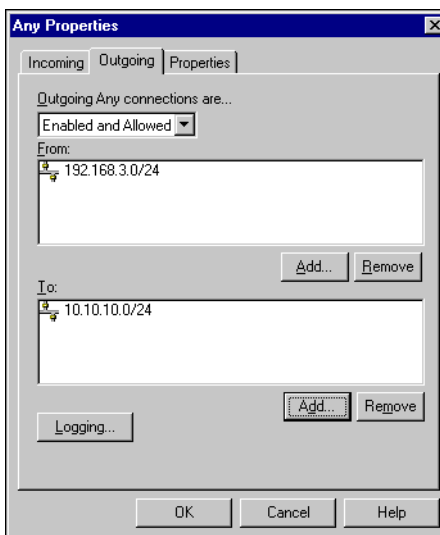
24 At the Choose Type drop list, select **Network IP Address** and enter the IP address of the private, internal network behind the Pix. Following our example, 10.10.10.0/24.

25 Click **OK**.

The Add Address dialog box appears.

26 Click **OK**.

The service's Properties dialog box reappears. It should display the IP Address you entered in the To portion of the dialog box as well as the IP address of the From portion you entered earlier.



27 Click **OK** to close the Any Properties dialog box. Click **Close** to close the Add Service dialog box.

## Saving the Configuration to the Firebox

Finally, save the changes made to the configuration file to the Firebox.

1 Select **File** ⇒ **Save** ⇒ **To Firebox**.

2 Use the Firebox drop list to select the Firebox.

- 3 Enter the configuration (read/write) pass phrase. Click **OK**.  
The configuration file is saved first to the local hard drive and then to the primary area of the Firebox flash disk. You are prompted to reboot the Firebox. The new Firebox configuration will not be enabled until the Firebox is rebooted.

---

## Configuring FireWall-1 for a Firebox to FireWall-1 IPSec Tunnel

---

This section describes how to configure the Check Point FireWall-1 version 4.1 SP2 as the end of a tunnel which has a WatchGuard Firebox II at the other end.

This document assumes that you have successfully activated the interfaces on the Check Point box 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 Firebox:

- 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 Firebox is named, FB-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 FB-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 Firebox. 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, FB.

***IP Address***

Enter the external interface IP address of the Firebox. In our example the public, or external IP of the Firebox 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 Firebox 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 Firebox enter, eth0.

***Net Address***

Enter the IP address assigned to this particular interface. In our example the public, or external IP of the Firebox 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 Firebox. 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 Firebox enter, eth1.

***Net Address***

Enter the IP address assigned to this particular interface. In our example the private, or internal IP of the Firebox 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 Firebox, choose **Other** and select **FB-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 Firebox 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 Firebox 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 Firebox 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 Firebox.

## 15 Click **Set**. Click **OK**.

The Firebox 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 Firebox 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 Firebox 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 **FB**. 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 Firebox.
  - 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 Firebox network icon you created previously. Following our example, FB-net. Click **OK**.  
This adds the Firebox 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 Firebox 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 Firebox network icon you created previously. Following our example, FB-net. Click **OK**.  
This adds the Firebox 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 Firebox, select **ESP**.
  - Encryption Algorithm**  
Following our example on the Firebox, select **3-DES**.
  - Data Integrity**  
Following our example on the Firebox, select **SHA1**.

---

### *Allowed Peer Gateway*

Select **Firebox**.

### *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-4.6 Firebox to Check Point FW-1