

# **SonicWALL – Check Point Firewall-1**

## **VPN Interoperability**

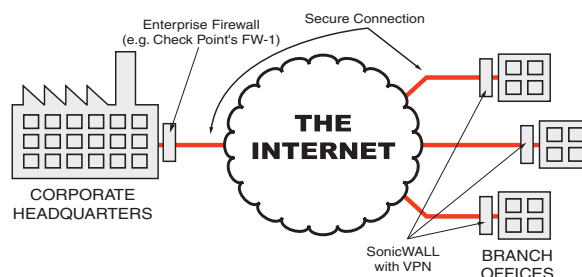
A Tech Note prepared by SonicWALL, Inc.

SonicWALL, Inc.  
1160 Bordeaux Drive  
Sunnyvale, CA 94089-1209  
1-888-557-6642  
<http://www.sonicwall.com>

## Introduction

The most common prescription against unwanted Internet access has been fortification of the enterprise network's main entrance against hackers. High-end solutions, such as Check Point Software's Firewall-1, are now firmly and properly established at the main entrances to the enterprise network. But that is not enough. Although the front door may be fortified and monitored, other entrances that may not be as well protected against attacks. Remote offices may not be protected at all, placing their own data and application availability at risk, and perhaps also providing an unguarded "back door" into the fortified headquarters network.

The technology used to protect alternative portals into an enterprise network and remote networks from external attack, and to isolate internal segments of a large network from internal threats, are the same as those which protect the main entrance: firewalls at portals, and Virtual Private Networks (VPNs) between the enterprise network and remote offices or telecommuters. A VPN provides a secure, encrypted path over the Internet, and the use of VPN should be required for accessing any non-public information over the Internet.



As VPN standards are still evolving, different vendors' implementations are not always fully interoperable. Yet a good remote office firewall should be adaptable to support all of the leading enterprise VPN products. One of SonicWALL VPN's strengths is its ability to interoperate with VPN solutions offered by different vendors. One of these products is Check Point Firewall-1. This tech note details the steps to configure Firewall-1 to support SonicWALL VPN.

## Configuring Check Point Firewall-1

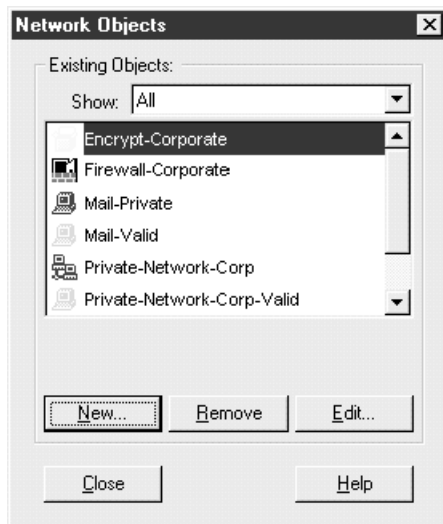
*Note: This paper assumes a familiarity with the Check Point Firewall-1 Management tools. The following steps also assume that the Firewall-1 is installed and properly configured.*

Launch and log into the **Firewall-1 Security Policy** application.

1) Check the existing **Firewall** object to make sure the **Encryption Domain** includes all objects for any encryption methods in use. Click the **Encryption** tab and make sure the **Manual IPSEC** encryption algorithm is selected. If SecuRemote is used, **FWZ** must also be selected.

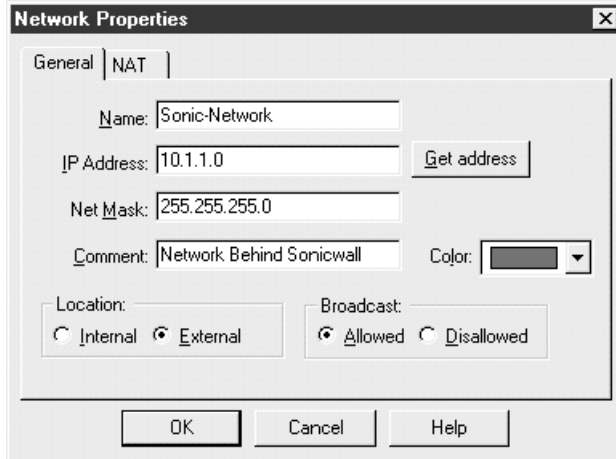
2) Create the Remote Object(s) - These are the resources, behind the remote SonicWALL such as **Workstation**, **Network**, or **Group** objects. We will use a **Network** in the following example:

- From the **Manage** menu select **Network Objects**.
- Click the **New** button and select **Network**.



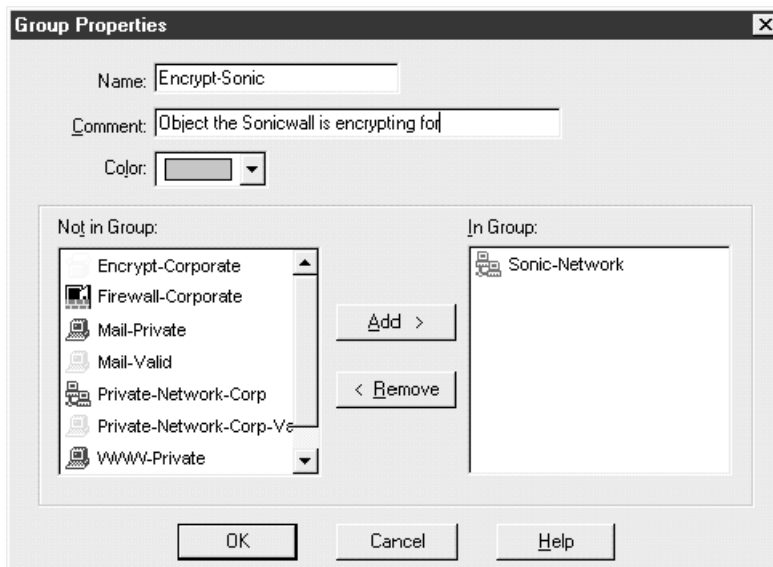
- Give the **Network Object** a unique name, such as "SonicWALL-Network".
- Give the **Network Object** an **IP Address Range** ("10.1.1.0").
- Give the **Network Object** a **Subnet Mask** ("255.255.255.0").
- Give the **Network Object** a **Comment** (optional).

- Select **External** for the **Location** option.
- Click the **OK** button when finished.



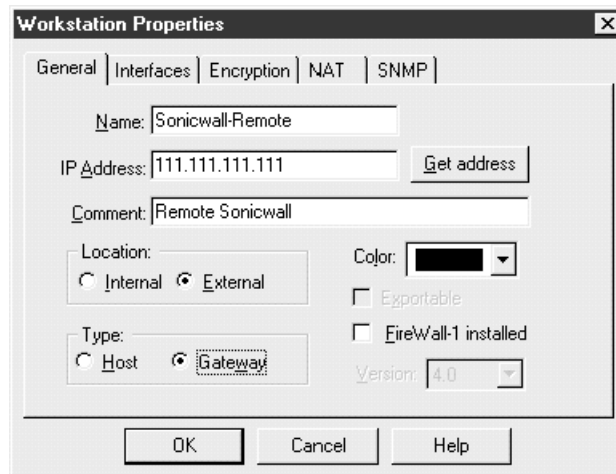
3) For easier management, create a Group and place all objects that are protected by the remote SonicWALL in that group.

- Press the **New** button and select the **Group** option.
- Give the **Group** object a unique name, such as "Encrypt-SonicWALL".
- Give the **Group** object a **Comment** (optional).
- Select the objects that are behind the remote SonicWALL and **Add** them to the group.
- Click the **OK** button when finished.

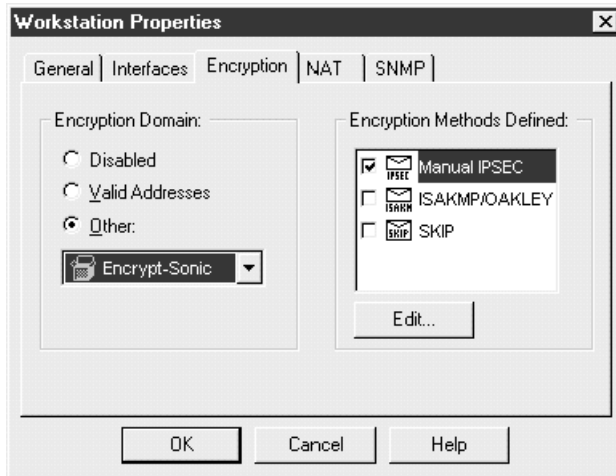


4) Now create the remote SonicWALL firewall object.

- Press the **New** button and select the **Workstation** option.
- Give the workstation object a unique name, such as "SonicWALL-Remote".
- Give the **Workstation** object the external IP address of the remote SonicWALL ("111.111.111.111").
- Give the **Workstation** object a comment (optional).
- Select **External** for the **Location**.
- Select **Gateway** for the **Type**.
- Leave the **Firewall-1 Installed** box unchecked.
- Click the **Encryption** tab.



- Select the **Other** radio button and select the **Group** or **Network** for which the SonicWALL will be encrypting traffic.
- Select the encryption method **Manual IPSEC**.
- Click the **OK** button when finished.

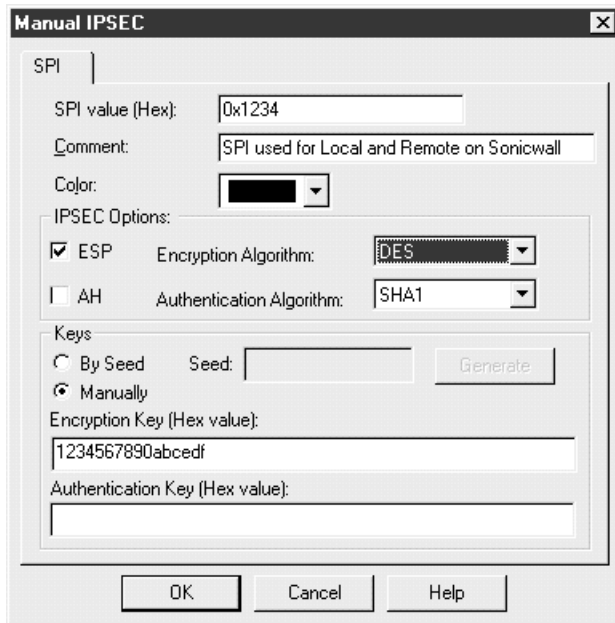


5) Next, create the SPI key(s) needed to synchronize encryption algorithms.

- From the **Manage** menu select the **Keys** option.
- Click the **New** button and select **SPI**.



- Give the **SPI Value** a unique hexadecimal value.
- Give the **SPI Key** a comment (optional).
- Check the **ESP** box and select **DES** as **Encryption Algorithm**.
- Make sure that the **AH** box is unchecked (ignore any warning).
- **Authentication Algorithm** field should be greyed out.
- Enter an **Encryption Key** (*Note: must be 16 hexadecimal characters*).
- **Authentication Key** field should be greyed out.



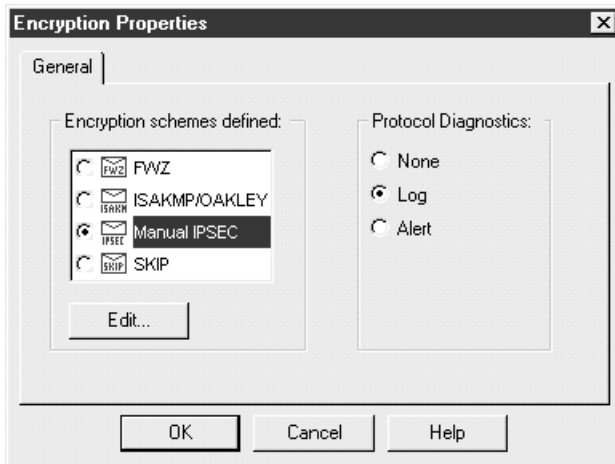
- The **Encryption Key** and **SPI Key** number must match the settings on the remote SonicWALL for the VPN to work.
- 6) Next, create a rule to allow the Check Point Firewall to exchange IPSEC packets with the remote SonicWALL.
- From the **Edit** menu, select **Add Rule**. This rule should be added below any Client VPN rules (for SecuRemote to work properly) and above the normal resource access rules. The rule should contain both firewall objects (Check Point Firewall-1 and SonicWALL), the **Service** group should be **IPSEC**, and it should be **Accepted**. Logging is optional and should be used to debug any problems.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	SecuRemoteUsers@Any	Encrypt-Corporate	Any	Client Encrypt		Firewall-Corporate	Any	Client VPN Rule
2	Firewall-Corporate Sonicwall-Remote	Sonicwall-Remote Firewall-Corporate	IPSEC	accept		Firewall-Corporate	Any	
3	Any	Any	Any	drop	Short	Firewall-Corporate	Any	Implicit Drop

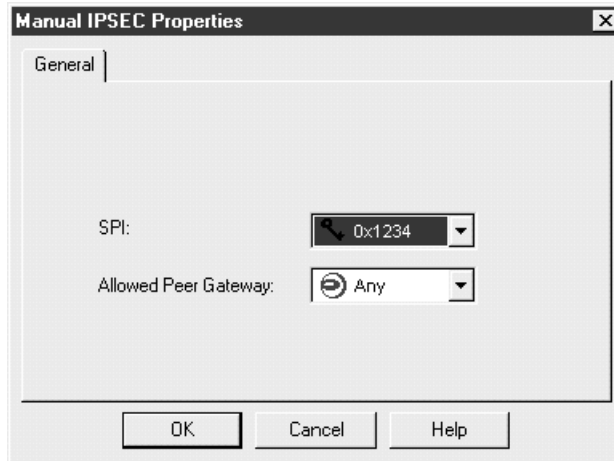
- 7) Add a rule to allow the two networks/groups to send encrypted data to each other. This rule should follow immediately after the firewall IPSEC packet exchange rule. The rule should contain both the local network/group with the remote network/group. If desired, services that are allowed to traverse the VPN tunnel may be restricted. The action for this rule should be **Encrypt**.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	SecuRemoteUsers@Any	Encrypt-Corporate	Any	Client Encrypt		Firewall-Corporate	Any	Client VPN Rule
2	Firewall-Corporate Sonicwall-Remote	Sonicwall-Remote Firewall-Corporate	IPSEC	accept		Firewall-Corporate	Any	
3	Encrypt-Corporate Encrypt-Sonic	Encrypt-Sonic Encrypt-Corporate	Any	Encrypt		Firewall-Corporate	Any	
4	Any	Any	Any	drop	Short	Firewall-Corporate	Any	Implicit Drop

- Right click the **Encrypt** action and select **Edit Properties**.
- Select the **Manual IPSEC** and the **Logging** radio buttons.



- Click the **Edit** button.
- Select the **SPI Key** for this VPN tunnel.
- Click the **OK** button when finished with the IPSEC properties and click the **OK** button when finished with the **Encryption Properties**.



- 8) From the **Policy** menu, select **Install** to activate the security policy. The VPN tunnel will function once the remote SonicWALL has been configured with a corresponding **Security Association**.

## Configuring the SonicWALL Internet Security Appliance

- 1) Please refer to the SonicWALL manual for instructions on configuring SonicWALL VPN settings.
- 2) Go to the **VPN>Configure** screen in the SonicWALL management interface. Create a **SonicWALL Security Association**, using manual key encryption, and name it "Check Point" (any name will work).
- 3) Do not use the 'allow remote clients' checkbox. Enter a valid **destination address range** (referring to the LAN behind Check Point). Specify the Check Point's external address as the **IPSec Gateway address**.
- 4) Select the **Encryption Method** "Encrypt for Checkpoint (ESP DES rfc1829)".
- 5) Make sure the **Encryption Key** and the **SPIs** match the values specified in the Check Point screens (The SonicWALL doesn't need the '0x' prefixes to denote hexadecimal fields like the Check Point does). There is no need for an authentication key.
- 6) **Update** the screen and **restart** SonicWALL to activate the VPN configuration.

## Acknowledgment

SonicWALL would like to thank Ignyte Technologies, Inc. for their help in the creation of this tech note. Ignyte is a network systems integration company committed to helping clients identify, plan, and implement business solutions based on information systems. Please visit Ignyte's Web site at <<http://www.ignyte.com>>.