

SonicWALL – Axent Raptor Firewall

VPN Interoperability

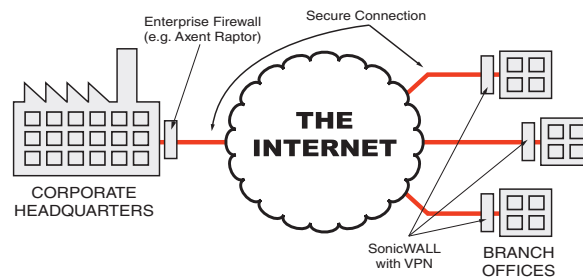
A Tech Note prepared by SonicWALL, Inc.

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 Axent Technologies' Raptor Firewall, 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.

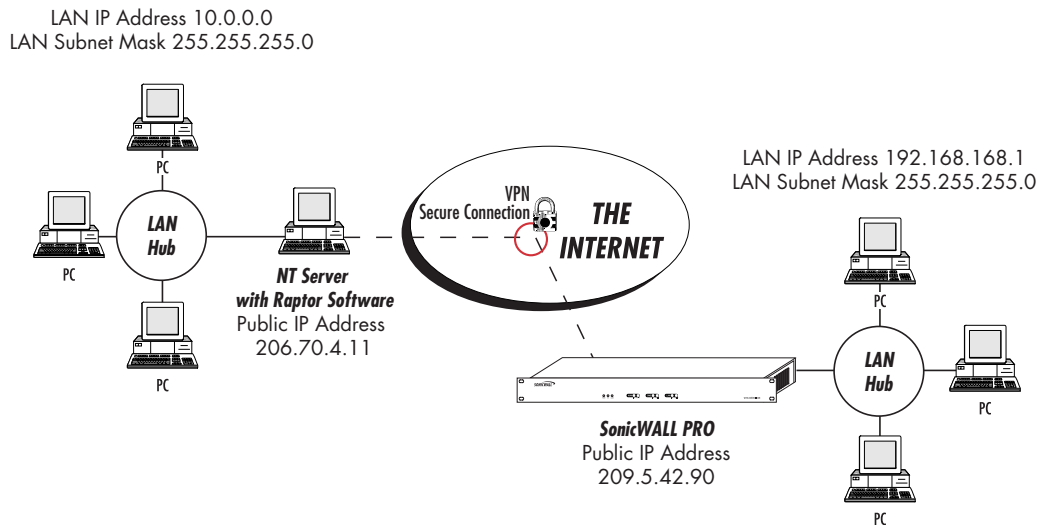
The technology used to protect alternative portals into an enterprise network and remote networks from external attack, and to isolate internal segments of a large network from internal threats, are the same as those which protect the main entrance: firewalls at portals, and Virtual Private Networks (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 Axent's Raptor Firewall. This tech note details the steps to configure Raptor to support SonicWALL VPN.

Configuration Instructions

Note: This paper assumes a familiarity with the Raptor Management Console (RMC). This white paper describes a hypothetical Raptor-SonicWALL VPN tunnel; substitute your own network's IP addresses, Key Profile names and



Secure Subnet Entity names.

To create the Raptor-SonicWALL VPN tunnel, first launch and log into the Raptor Security Policy application. You will need to make the following changes to the Axent Raptor:

1. Create a local Key Profile called Raptor with a gateway address "206.70.4.11."
2. Create a local Secure Subnet Entity with an address "10.0.0.0."
3. Create a remote Key Profile called SonicWALL and a gateway address "209.5.42.90."
4. Create a remote Secure Subnet Entity with an address "192.168.168.1."
5. Define an IPsec Secure Tunnel using the same values designated on the SonicWALL PRO.

Configure the Local Key Profile: Raptor

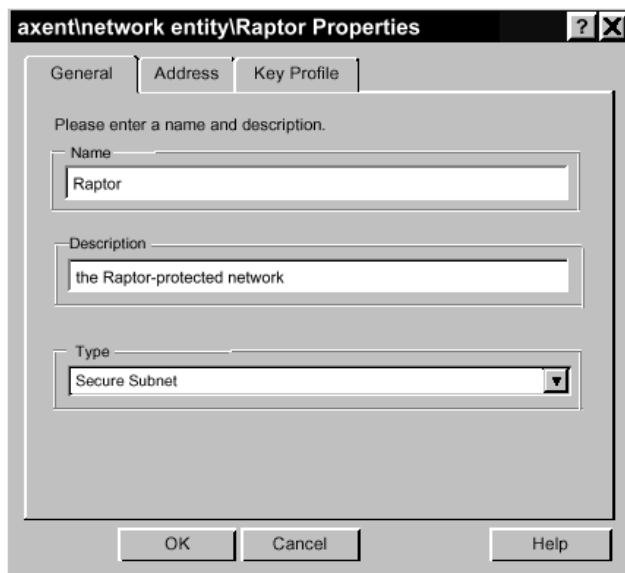
1. Click the **Key Profiles** icon in RMC, then right mouse click and choose **New>Key Profile**. The **Key Profile Properties** window should appear.



2. Enter the **Name** “Raptor.”
3. Select “Static” from the **Type** pulldown menu.
4. Enter the Raptor’s public IP address, “206.70.4.11,” in the **Gateway IP Address** field.
5. Check the **Internal Network** checkbox. Click **OK**.

Configure Local Secure Subnet: Raptor

1. Click the **Network Entities** icon in RMC.
2. Select the **Secure Subnet** icon from the available Entity icons. Right mouse click and select *New>Secure Subnet* from the Action menu. The following *Network Entity Properties* page should appear.



3. In the **General** tab, assign the local Secure Subnet the **Name** “Raptor.”
4. Enter the **Description** “the Raptor-protected network.”
5. Select the **Address** tab. Enter the Raptor’s **Network Address** “10.0.0.0” and **Network Mask** “255.255.255.0.”
6. In the **Secure Subnet Properties Key Profile** tab, select the **Raptor** profile. Click **OK** to save your Secure Subnet Entity.

Configure Remote Key Profile: SonicWALL

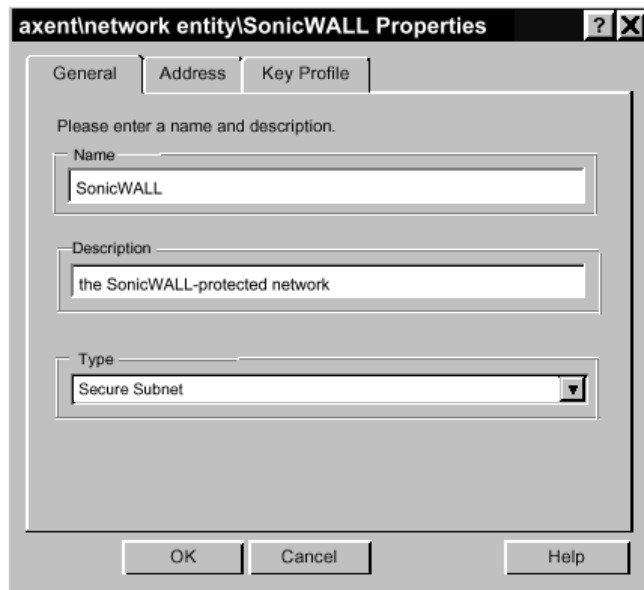
1. Select the **Key Profile** icon, then right mouse click and choose **New>Key Profile**. The **Key Profile Properties** window should appear.

The screenshot shows a dialog box titled "axentkey profile\SonicWALL Properties". It has a "General" tab selected. The text inside says "Please identify the Key Profile and select its type, address and whether it is internal." There are three input fields: "Name" with "SonicWALL", "Type" with a dropdown menu showing "STATIC", and "Gateway IP Address" with "209.5.42.90". Below these is a checkbox labeled "Internal Network" which is checked. At the bottom are three buttons: "OK", "Cancel", and "Help".

2. Enter the *Name* “SonicWALL.”
3. Select “STATIC” from the **Type** pulldown menu.
4. Enter SonicWALL’s public IP address, “209.5.42.90,” in the **Gateway IP Address** field.
5. Click **OK**.

Configure Remote Secure Subnet: SonicWALL

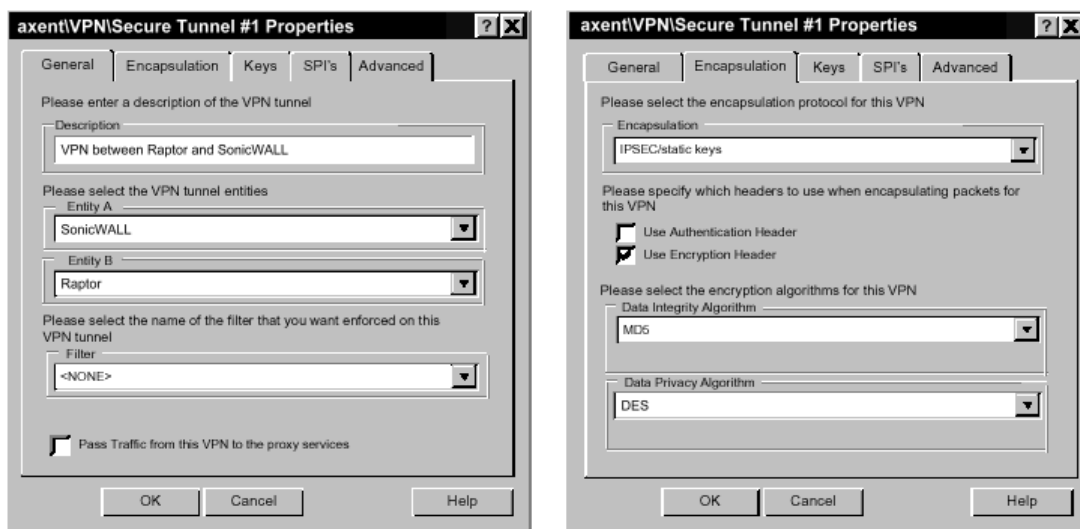
6. Click the **Network Entities** icon in RMC.
7. Select the **Secure Subnet** icon from the available Entity icons. Right mouse click and select **New>Secure Subnet** from the Action menu. The following **Network Entity Properties** page should appear.



8. In the **General** tab, assign the remote Secure Subnet the **Name** "SonicWALL."
9. Enter the **Description** "the SonicWALL-protected network."
10. Select the **Address** tab. Enter the SonicWALL's **Network Address** "192.168.168.1" and *Network Mask* "255.255.255.0."
11. In the **Secure Subnet Properties Key Profile** tab, select the **SonicWALL** profile. Click **OK** to save your Secure Subnet Entity.

Configure an IPsec Secure Tunnel

1. Select the **Secure Tunnels** icon in RMC. Right mouse click and select **New>Secure Tunnel** from the Action menu.



2. In the **General** tab, enter the *Description* “VPN between Raptor and SonicWALL.”
3. Choose “SonicWALL” from the **Entity A** pulldown menu.
4. Select “Raptor” from the **Entity B** pulldown menu.
5. Select the **Filter** “<none>.”
6. Leave the **Pass Traffic from this VPN to the proxy services** checkbox unchecked.
7. Select the **Encapsulation** tab and choose the **Encapsulation** “IPSEC/static keys.”
8. Check the **Use Encryption Header** box. Do NOT check the **Use Authentication Header** boxes.
9. Choose the **Data Integrity Algorithm** “MD5.”
10. Specify “DES” in the **Data Privacy Algorithm** pulldown menu.
11. Select the **Keys** tab and generate a set of IPsec keys by clicking the **Generate Keys** button. The Entity A and Entity B **Integrity Algorithm Keys** will need to be the same and will also need to match SonicWALL’s **Authentication Key** (see Note). The Entity A and Entity B **Privacy Algorithm Keys** will need to be the same and will need to match SonicWALL’s **Encryption Key**.
12. Click the **SPIs** tab. You must assign a Security Parameter Index (SPI) to each endpoint by entering a number between 1 and 65535 in each Entity field in the SPI’s tab. You can also click the **Generate SPIs** button to let RMC choose unique encapsulation SPIs for you. The Raptor SPIs must match the corresponding SPIs.

Note: SonicWALL's SPIs are hexadecimal. Raptor uses decimal SPIs. Therefore, if the Raptor has generated the SPIs, you will need to convert the SPIs from decimal to hexadecimal. Alternatively, if SonicWALL has generated the SPIs, you will need to convert the SPIs from hexadecimal to decimal.

13. Click *OK* to save your IPsec Secure Tunnel configuration.

Configure the SonicWALL Internet Security Appliance

1. Please refer to the SonicWALL manual for instructions on configuring SonicWALL VPN settings.
2. Once you have created a SonicWALL Security Association named "Raptor," select the **Encryption Method** "Encrypt with Authenticate (ESP DES HMAC-MD5)."
3. Make sure the **Encryption Key**, **Authentication Key** and the **SPIs** match the values specified in the Axent Raptor.
4. If you have upgraded SonicWALL firmware to 4.0 or greater, be sure to select **IPSec Keying Mode** "Manual Key."
5. Other SonicWALL-to-Raptor VPN configurations may be possible, but only the encryption method listed has been thoroughly tested.