

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Prepared by SonicWALL, Inc.

6/15/2002

Introduction

This technote will detail all the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL device and a RedCreek Ravlin device. SonicWALL, Inc and RedCreek merged in November 2001, and continue to market the Ravlin product line. This technote assumes that both sides have static IP addresses for the external WAN interfaces, and that the devices have been pre-configured with unique LAN and WAN IP addresses, as well as default IP routes. SonicWALL engineering has tested and validated the settings described in this technote. Please note that all settings and screenshots contained within this technote are taken from a SonicWALL SOHO3 device running firmware 6.3.1.0, and a RedCreek Personal Ravlin II running firmware 3.81.

Before You Begin

SonicWALL strongly recommends using firmware release 6.3.1.0 or newer on the SonicWALL device, and 3.81 or newer on the RedCreek Ravlin device. Customers with new SonicWALL/RedCreek devices, or devices under a current support contract, can download the newest firmware from the <https://www.mysonicwall.com> customer site.

Using a longer SA lifetime may reduce issues with SA's timing out and failing to renegotiate. The downside to doing this is that it's inherently less secure than using standard SA lifetime like 28,800 seconds (8 hours). For reference, the maximum lifetime for a RedCreek Ravlin SA is ----- seconds, and the maximum lifetime for a SonicWALL device SA is 9,999,999 seconds. Since the SA lifetimes must match, this means that the longest SA lifetime for a SonicWALL-to-RedCreek Ravlin VPN tunnel would be ----- seconds (--- hours). One drawback of this method is that if one side crashes or reboots during this SA lifetime, it may be necessary to restart the other side to clear out the invalid SA.

Since the SonicWALL now has a user-selectable keepalive mechanism for SA's as of firmware 6.1.1.0, it will generally be the 'IKE Initiator'. This option has proven useful in many environments where SonicWALLs have a VPN tunnel to a third-party device.

Please take special care to correctly set the Diffie-Hellman (DH) group type on the SonicWALL device and the RedCreek Ravlin device. If the wrong defaults are used on both sides to set up a VPN tunnel, it may result in the ability to initiate a tunnel from the RedCreek Ravlin to the SonicWALL device, yet be unable to initiate a tunnel from the SonicWALL device to the RedCreek Ravlin.

Caveats

There are several known limitations when attempting to establish a VPN tunnel between a SonicWALL device and a RedCreek Ravlin device. Please note the following before you begin:

1. You can only have a single IP subnet on each side of the pairing.
2. You cannot use aggressive mode – only main mode is supported.
3. You must use static IP addresses on the WAN ports of each device – dynamic IP addresses on the WAN port are not supported (PPPoE, DHCP, L2TP).
4. You can only use pre-shared keys as the VPN tunnel setup authentication mechanism.
5. Since SonicWALL devices use its "SA Lifetime" field for both phase one and phase two negotiations, you must take care use the same time for both the ISAKMP and IPSEC fields in the RedCreek Ravlin device.

SonicWALL Setup

1. Log into the SonicWALL's Management GUI using a current web browser, such as Microsoft IE 5.5 or Netscape 6.2.
2. Click on the 'VPN' button on the left side, and then click on the 'Configure' tab along the top.
3. From the 'Security Association' drop-down box, choose "-Add New SA-".
4. From the 'IPSec Keying Mode' drop-down box, choose "IKE using Preshared Secret".
5. In the 'Name' field, enter a unique name for your tunnel to the RedCreek Ravlin.
6. In the 'IPSec Gateway Address' field, enter the static IP address of the 'Public' interface of the RedCreek Ravlin.
7. From the 'Phase 1 DH Group' drop-down box, choose "Group 1".
8. In the 'SA Life time (secs)' field, enter in the security association lifetime in seconds you wish to use for the VPN tunnel to the RedCreek Ravlin.
9. From the 'Phase 1 Encryption/Authentication' drop-down box, choose "3DES & MD5".
10. From the 'Phase 2 Encryption/Authentication' drop-down box, choose "Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)".
11. In the 'Shared Secret' field, enter in the shared secret you wish to use for the VPN tunnel to the RedCreek Ravlin.
12. Choose the 'Specify Destination Networks Below' radio button.
13. Click on the 'Add New Network...' button.
14. In the pop-up screen that appears, enter in the subnet and mask that are behind the 'Private' interface of the RedCreek Ravlin (you may need to use the 'Add New Network..' button multiple times if there are multiple subnets) and then click on the 'Update' button when you are done.
15. Click on the 'Advanced Settings...' button.
16. In the pop-up screen that appears, check the 'Enable Keep Alive' box and then click on the 'OK' button when you are done.
17. Click on the 'Update' button in the lower-right-hand of the screen to save all changes.

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

SonicWALL Device Screenshots

Sample of IPSec Security Association to RedCreek Ravlin (top half):

The screenshot displays the SonicWALL Administration web interface in Microsoft Internet Explorer. The browser's address bar shows the URL `http://192.168.30.1/management.html`. The interface is titled "VPN" and features a navigation menu on the left with options like General, Log, Filter, Tools, Access, Advanced, DHCP, VPN, Anti-Virus, and High Availability. The main content area is titled "Add/Modify IPSec Security Associations" and includes the following configuration fields:

- Security Association: ToPRAVII
- IPSec Keying Mode: IKE using Preshared Secret
- Name: ToPRAVII
- Disable This SA:
- IPSec Gateway Address: 192.168.20.2

Below these fields is the "Security policy" section with the following settings:

- Phase 1 DH Group: Group 1
- SA Life time (secs): 86400
- Phase 1 Encryption/Authentication: 3DES & MD5
- Phase 2 Encryption/Authentication: Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)
- Shared Secret: hellothere

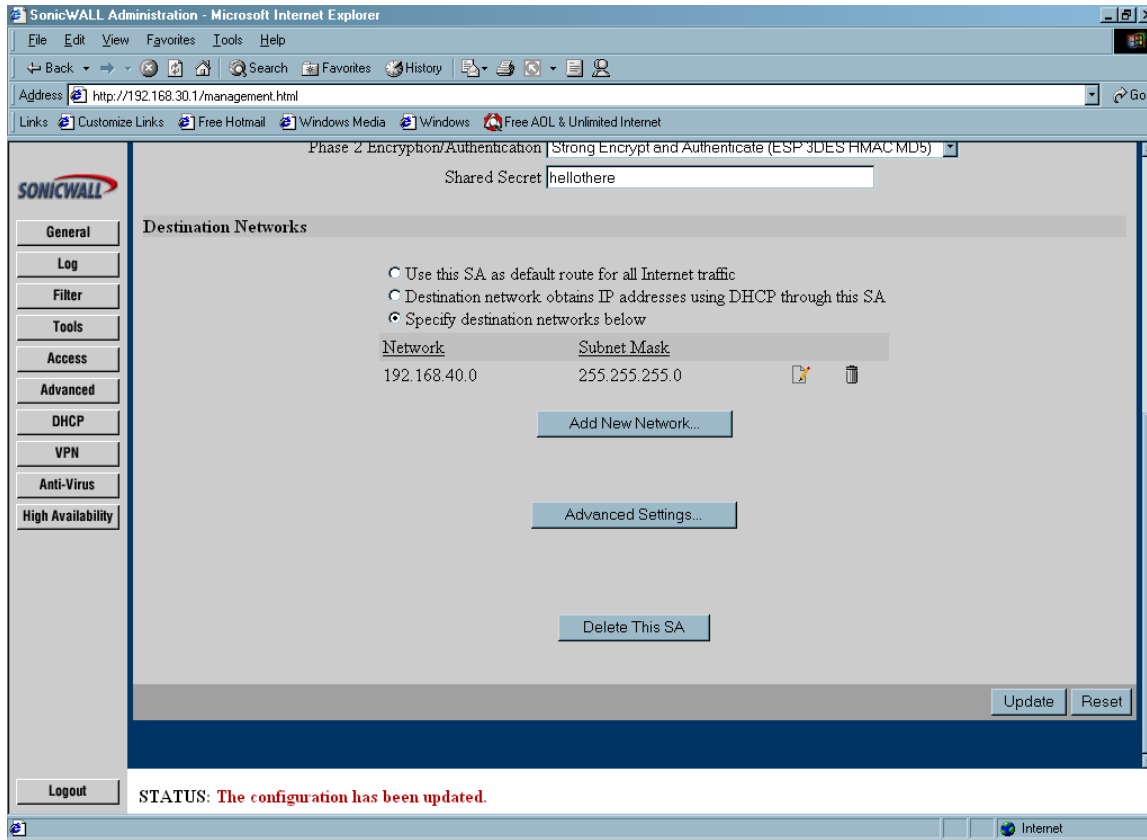
The "Destination Networks" section at the bottom contains two radio button options:

- Use this SA as default route for all Internet traffic
- Destination network obtains IP addresses using DHCP through this SA

A status message at the bottom of the configuration area reads: "STATUS: The configuration has been updated." The browser's status bar at the bottom shows "Done" and "Internet".

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Sample of IPSec Security Association to RedCreek Ravlin (bottom half):



Sample of 'Add New Network':

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

VPN Destination Network - Microsoft Internet Explorer

Edit VPN Destination Network

Network

Subnet mask

Sample of 'Advanced Settings':

VPN Advanced Settings - Microsoft Internet Explorer

Edit Advanced Settings

Use Aggressive Mode

Enable Keep Alive

Require authentication of local users

Require authentication of remote users

- Remote users behind VPN gateway
- Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy

Phase 2 DH Group

Default LAN Gateway

Note that after clicking OK, you must click Update on the main page to save changes made here.

RedCreek Ravlin Setup

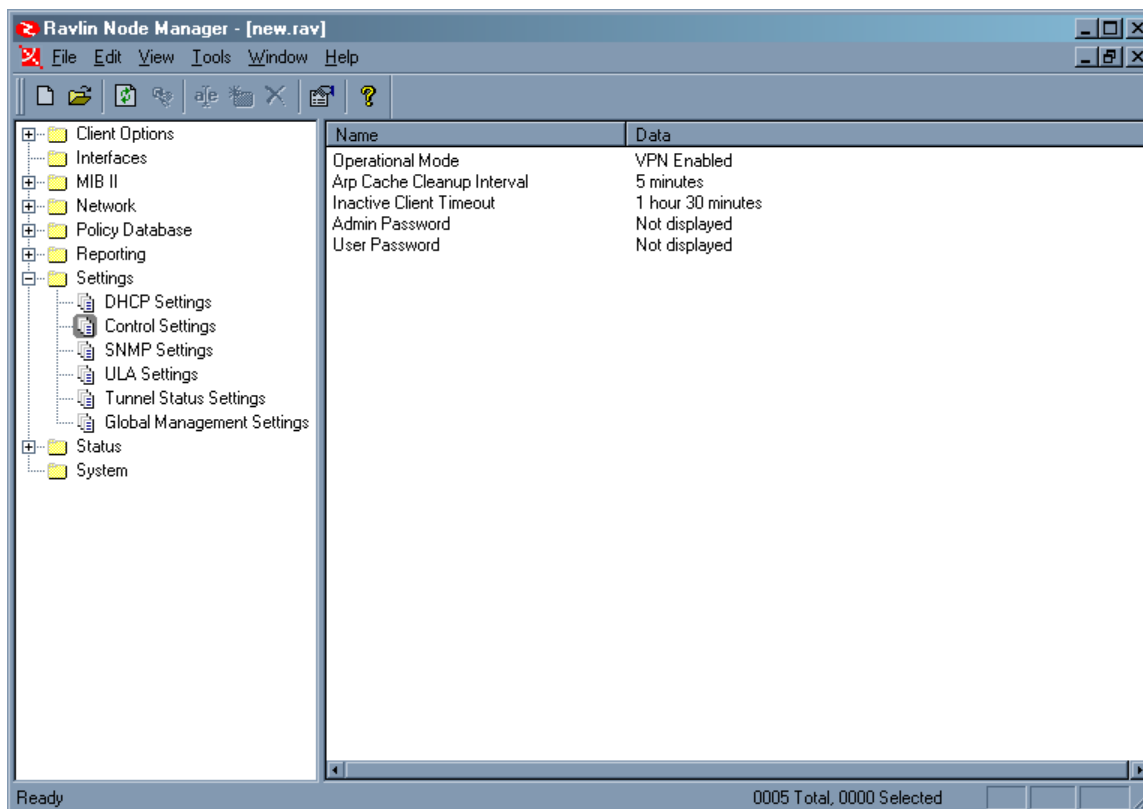
1. Open 'Ravlin Node Manager' and attach to the RedCreek Ravlin device.
2. Double-click on the 'Settings' folder, and then click on 'Control Settings'. Double-Click on 'Operational Mode', select 'Apply Policy to All Traffic' from the drop-down box that appears, and then click on the 'OK' button. This will change the mode of the box to "VPN Enabled".
3. Double-click on the 'Policy Database' folder to expand it, and then double-click on 'Key Management' to expand it. Right- Click on the 'ISAKMP' entry and choose the 'Insert...' option from the menu that pops up. Click on the "table" icon (next to the large X icon). From the table that appears, select the ID '3' entry and then click on the 'OK' button. ID '3' is a predefined entry that uses 3DES Encryption, MD5 Authentication, Diffie-Hellman Group 1, and pre-shared keys. In the 'Pre-Shared Key' field, enter the preshared key you wish to use for both sides of the VPN tunnel, then click on the 'OK' button.
4. Double-click on the 'Policy Database' folder to expand it, and then double-click on 'Protocol Tables' to expand it. Right- Click on the 'IPSEC' entry and choose the 'Insert...' option from the menu that pops up. Click on the "table" icon (next to the large X icon). From the table that appears, select the ID '3' entry and then click on the 'OK' button. ID '3' is a predefined entry that uses 3DES Encryption and MD5 Authentication. From the 'IPSEC Protocol Type' drop-down box, choose 'Encapsulating Security Payload', then click on the 'OK' button.
5. Double-click on the 'Policy Database' folder to expand it, then right-click on 'Protocol Data Entries' and choose the 'Insert...' option from the menu that pops up. A dialog box will ask you if you want to use the 'Policy Entry Wizard' – click on the 'Yes' button.
6. The wizard will ask you to name the policy. Enter 'InternetAccess' and click the 'Next >' button.
7. The wizard will ask you what type of connection it is. Click on the radio button next to 'VPN Gateway (Static IP Address) and click the 'Next >' button.
8. The wizard will ask you to enter in the IP subnet of the RedCreek Ravlin's LAN interface. Click on the "dotted-folder" icon (next to the large X icon). In the fields that appear, enter in the Ravlin's LAN interface IP subnet and mask and click the 'Next >' button.
9. The wizard will ask you to enter in the IP subnet of the "peer networks". Click on the "dotted-folder" icon (next to the large X icon). In the fields that appear, enter in the SonicWALL's LAN interface IP subnet and mask and click the 'Next >' button.
10. The wizard will ask you for remote VPN gateway's IP address. In this field, enter in the IP address of the SonicWALL's WAN interface and click the 'Next >' button.

Creating IKE IPsec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

11. The wizard will ask you to choose the key management type. From the 'Key Management Type' drop-down box, choose 'ISAKMP'. From this list, choose the index entry with a "Proposal ID" of '3' and click the 'Next >' button.
12. The wizard will ask you to set the ISAKMP lifetime. In these fields, set the ISAKMP lifetime you wish to use and click on the 'Next >' button. Make sure this is the same SA lifetime as you have set on the SonicWALL device.
13. The wizard will ask you to choose the IPSEC Protocol entry. From this list, choose the index entry with a "Proposal ID" of '3' and click the 'Next >' button.
14. The wizard will ask you to set the IPSEC lifetime. In these fields, set the IPSEC lifetime you wish to use and click on the 'Next >' button. Make sure this is the same SA lifetime as you have set on the SonicWALL device and had set in step 12 above.
15. The wizard will ask you to set the routing. Click on the radio button next to 'Use Routing Table' and click the 'Next >' button.
16. The wizard will ask you if you wish to use User Level Authentication (ULA). Leave the 'Enable ULA Support' checkbox unchecked and click the 'Next >' button.
17. The wizard will tell you that it's done. Click on the 'Finish' button.

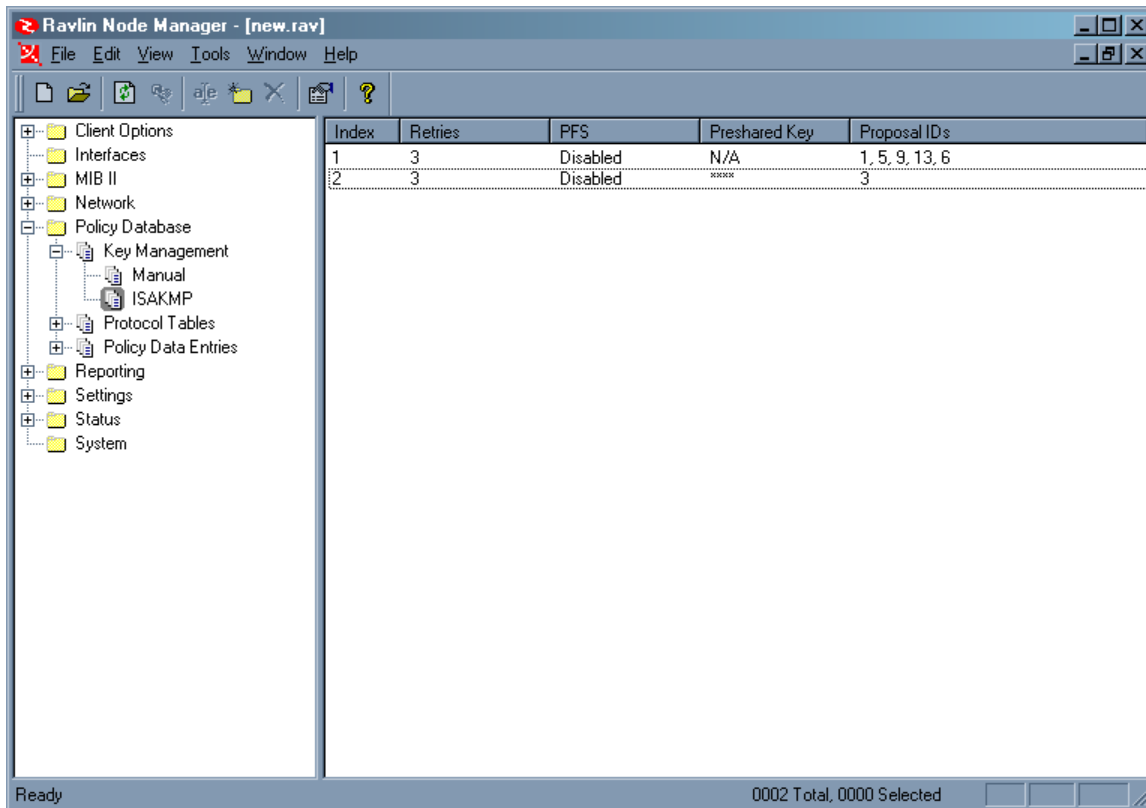
RedCreek Device Screenshots

Activating VPN Tunnels on the RedCreek Ravlin:



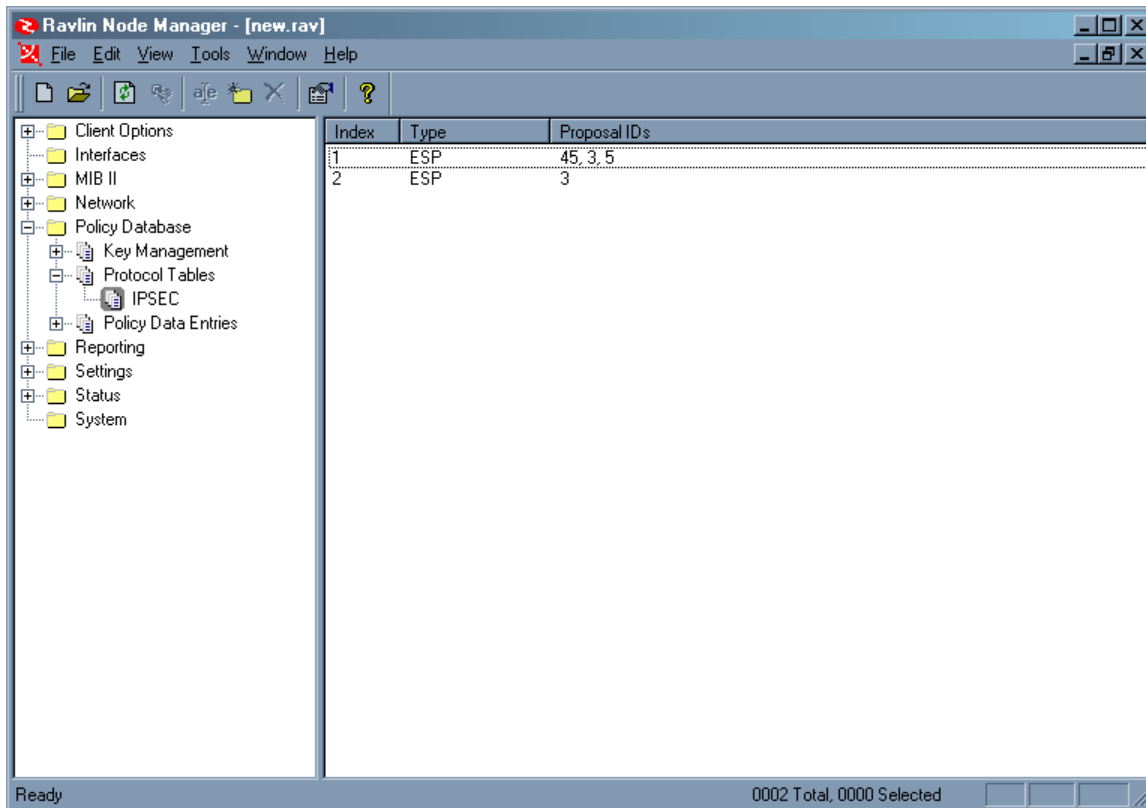
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Creating a ISAKMP policy on the RedCreek Ravlin:



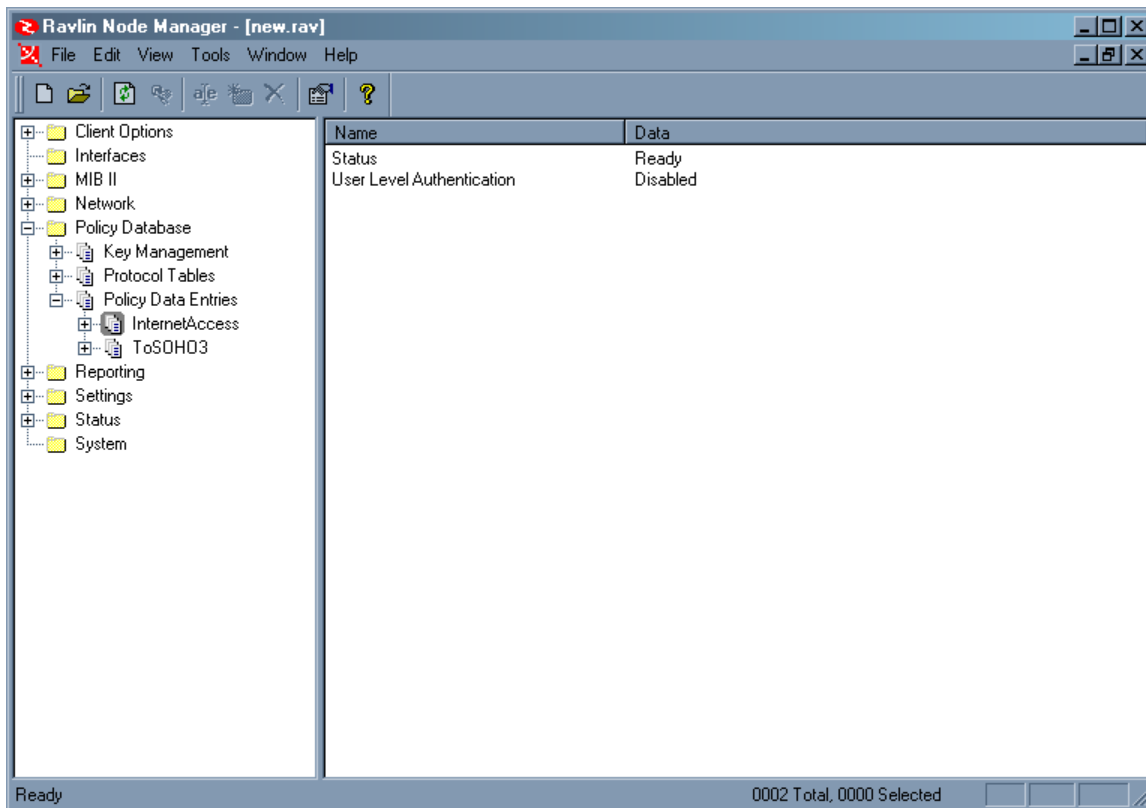
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Creating a IPSEC policy on the RedCreek Ravlin:



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Creating a VPN Tunnel Policy on the RedCreek Ravlin:



OPTIONAL: Configure the RedCreek Ravlin to perform NAT/PAT

The following commands will allow a RedCreek Ravlin to perform NAT/PAT for the “inside/private” IP subnet and also support VPN tunnels to remote destinations. This will allow all users behind the RedCreek Ravlin device to access the public Internet as well as access remote destinations across VPN tunnels.

1. Open ‘Ravlin Node Manager’ and attach to the RedCreek Ravlin device.
2. Double-click on the ‘Network’ folder to expand it, and then select ‘Packet Handling Options’. Double-click on the ‘Firewall and Internet Sharing’ entry until it changes from “Disabled” to “Enabled”.
3. Double-click on the ‘Policy Database’ folder to expand it. Right-Click on the ‘Policy Data Entries’ entry and choose the ‘Insert...’ option from the menu that pops up. A dialog box will ask you if you want to use the ‘Policy Entry Wizard’ – click on the ‘Yes’ button.
4. The wizard will ask you to name the policy. Enter ‘InternetAccess’ and click the ‘Next >’ button.
5. The wizard will ask you what type of connection it is. Click on the radio button next to ‘Non-VPN Bypass Outbound Only’ and click the ‘Next >’ button.
6. The wizard will ask you to enter in the IP subnet of the RedCreek Ravlin’s LAN interface. Click on the “dotted-folder” icon (next to the large X icon). In the fields that appear, enter in the Ravlin’s LAN interface IP subnet and mask and click the ‘Next >’ button.
7. The wizard will ask you to enter in the IP subnet of the “peer networks”. Click on the “dotted-folder” icon (next to the large X icon). In the fields that appear, leave them both set to the default “0.0.0.0” subnet and “0.0.0.0” mask, and click the ‘Next >’ button.
8. The wizard will ask you to set the routing. Click on the radio button next to ‘Use Routing Table’ and click the ‘Next >’ button.
9. The wizard will tell you that it’s done. Click on the ‘Finish’ button.