

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and NetScreen Devices

Prepared by SonicWALL, Inc.

8/14/2002

Introduction

This technote will detail all the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL device and a NetScreen device. 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 TELE3 device running firmware 6.3.1.0, and a NetScreen 5XP device running firmware 3.0.3r2.0.

Before You Begin

SonicWALL strongly recommends using firmware release 6.3.1.0 or newer on the SonicWALL device, and 3.01 or newer on the NetScreen device. Customers with new SonicWALL 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 NetScreen SA is 2,147,483,648 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-NetScreen VPN tunnel would be 9,999,999 seconds (166,666 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 NetScreen 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 NetScreen device to the SonicWALL device, yet be unable to initiate a tunnel from the SonicWALL device to the NetScreen device.

Caveats

There are four caveats when attempting to establish a VPN tunnel between a SonicWALL device and a NetScreen device. Please note the following before you begin:

1. You can only use pre-shared keys as the VPN tunnel setup authentication mechanism.
2. 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 NetScreen device.
3. Do not use the "group" feature to combine multiple LAN IP subnet address book entries on the NetScreen device when creating a VPN Policy. You will need to create a separate Policy for each LAN IP subnet of the NetScreen.
4. The SonicWALL device will periodically log the following message: "IPSec packet from an illegal host". This message is related to the proprietary dead-peer detection routine the NetScreen device runs, and can be safely ignored.

Example SonicWALL Setup

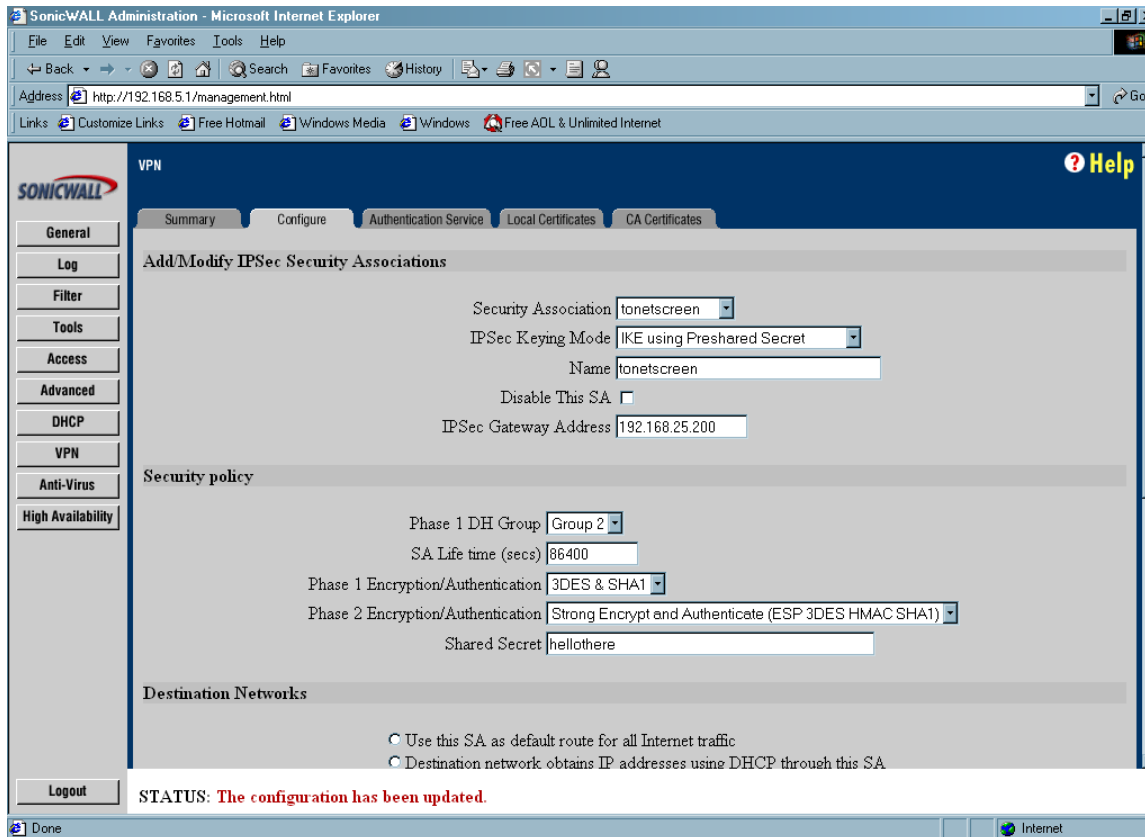
1. Log into the SonicWALL's Management GUI using a current web browser, such as Microsoft IE 5.5 or Netscape 6.2.
2. Click on the 'VPN' button on the left side, and then click on the 'Configure' tab along the top.
3. From the 'Security Association' drop-down box, choose "-Add New SA-".
4. From the 'IPSec Keying Mode' drop-down box, choose "IKE using Preshared Secret".
5. In the 'Name' field, enter a unique name for your tunnel to the NetScreen device.
6. In the 'IPSec Gateway Address' field, enter the static IP address of the 'Public' interface of the NetScreen device.
7. From the 'Phase 1 DH Group' drop-down box, choose "Group 2".
8. In the 'SA Life time (secs)' field, enter "86400".
9. From the 'Phase 1 Encryption/Authentication' drop-down box, choose "3DES & SHA1".
10. From the 'Phase 2 Encryption/Authentication' drop-down box, choose "Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)".
11. In the 'Shared Secret' field, enter in the shared secret you wish to use for the VPN tunnel to the NetScreen device.
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 NetScreen device (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.

NOTE: Values can and will be different depending upon your networking environment. The above steps use example data – you will need to substitute your network values where necessary.

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

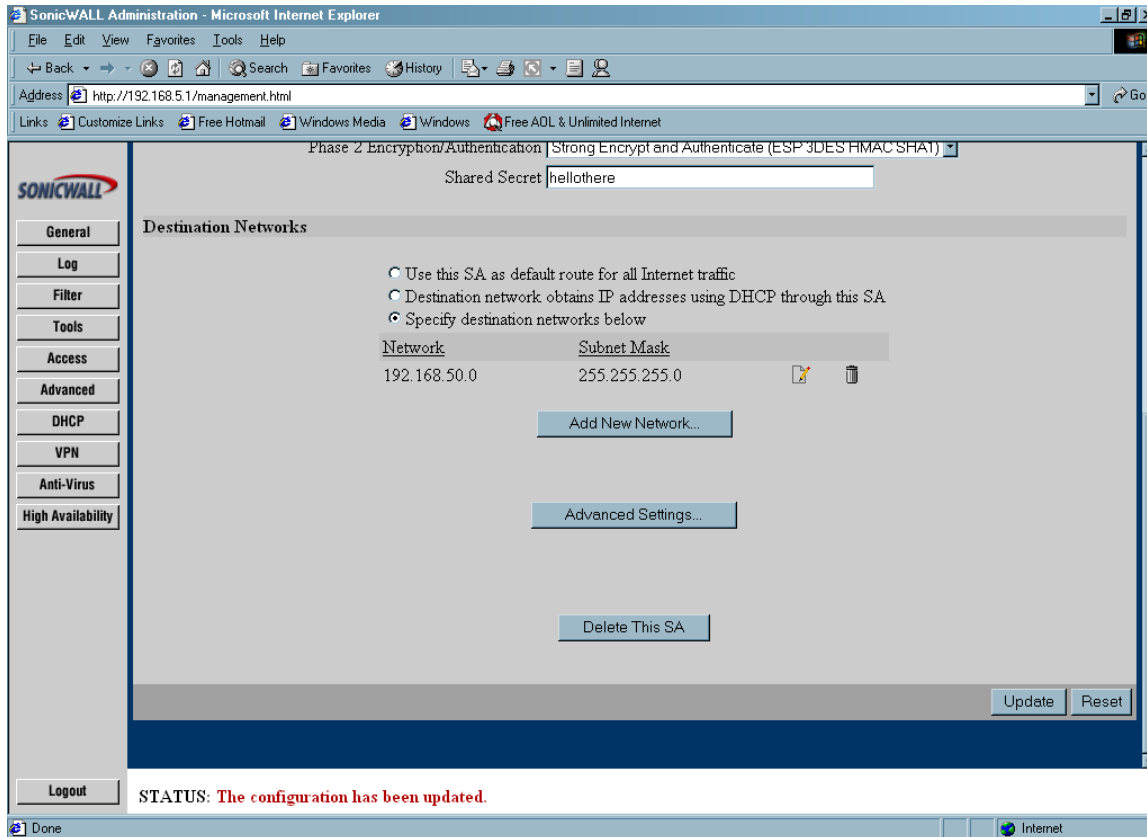
SonicWALL Device Screenshots

Example of IPSec Security Association to NetScreen device (top half):

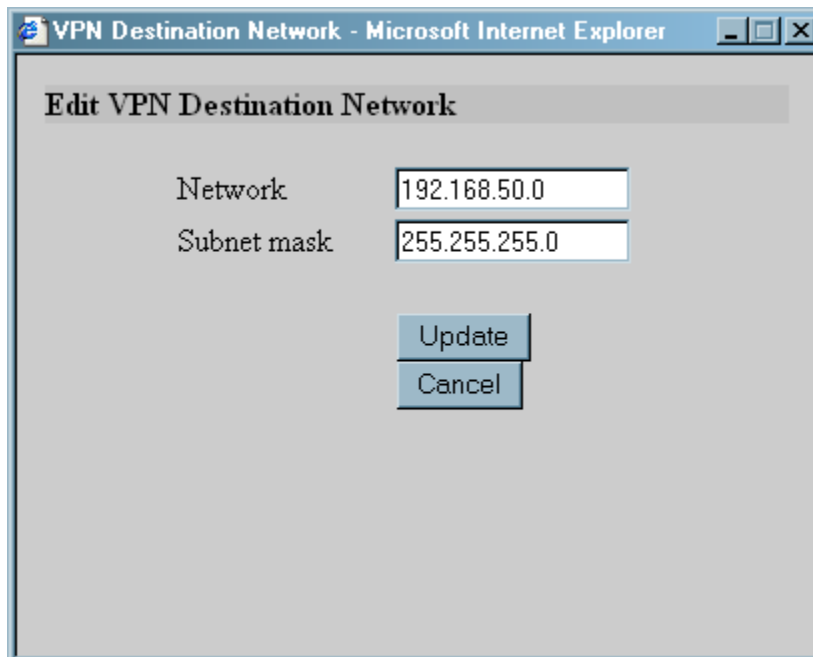


Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of IPSec Security Association to NetScreen device (bottom half):



Example of 'Add New Network':



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example 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

OK Cancel

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

NetScreen Device Setup

NetScreen's VPN setup is considerably more complex than the one-screen setup that SonicWALL devices use. To get a working, bi-directional VPN tunnel established on a NetScreen device, you must do the following tasks in precise order:

- Create local LAN IP subnet object in the 'Address Book – Trusted' section (may exist already)
- Create remote LAN IP subnet object in the 'Address Book – Untrusted' section
- Create a custom Phase One policy in the 'VPN' section
- Create a custom Phase Two policy in the 'VPN' section
- Create a Gateway object in the 'VPN' section
- Create an AutoKey IKE object in the 'VPN' section
- Create an Outgoing access rule in the 'Policy' section
- Create an Incoming access rule in the 'Policy' section

Sequence

1. Log into the NetScreen device's Management GUI using a current web browser, such as Microsoft IE 5.5 or Netscape 6.2.
2. Click on the 'Address' button and then the 'Trusted' tab. There should be an object labeled 'Internal' containing the LAN IP subnet. If not, click on the 'New Address' link at the bottom. In the 'Address Name' field, enter in "Internal". In the 'IP Address/Domain Name' field, enter in the NetScreen device's LAN IP subnet. In the 'Netmask' field, enter in the subnet mask for the NetScreen device's LAN IP subnet. Next to 'Location', select the 'Trust' radio button. Then, click on the 'OK' button to save.
3. Click on the 'Address' button and then the 'Untrusted' tab. Click on the 'New Address' link at the bottom. In the 'Address Name' field, enter in "sonicwall". In the "IP Address/Domain Name" field, enter in the SonicWALL device's LAN IP subnet. In the "Netmask" field, enter in the subnet mask for the SonicWALL device's LAN IP subnet. Next to 'Location', select the 'Untrust' radio button. Then, click on the 'OK' button to save.
4. Click on the 'VPN' button and then the 'P1 Proposal' tab. Click on the 'New Phase 1 Proposal' link at the bottom. In the 'Name' field, enter in "sonicwall". From the 'Authentication Method' drop-down box, select "Preshare". From the 'DH Group' drop-down box, select "Group 2". From the 'Encryption Algorithm:' drop-down box, select "3DES-CBC". In the 'Lifetime' field, enter in "86400" and then select the "Sec" radio button directly under the field. Then, click on the 'OK' button to save.
5. Click on the 'VPN' button and then the 'P2 Proposal' tab. Click on the 'New Phase 2 Proposal' link at the bottom. In the 'Name' field, enter in "sonicwall". From the 'Perfect Forward Secrecy' drop-down box, select "NO-PFS". Under 'Encapsulation', select the 'Encryption (ESP)' radio button. From the 'Encryption Algorithm' drop-down box, select "3DES-CBC". From the 'Authentication Algorithm' drop-down box directly under that, select "SHA-1". In the 'Lifetime – In Time' field, enter in "86400" and then select the "Sec" radio button directly under the dialog box. Then, click on the 'OK' button to save.
6. Click on the 'VPN' button and then the 'Gateway (P1)' tab. Click on the 'New Remote Tunnel Gateway' link at the bottom. In the 'Gateway Name' field, enter in "tosonicwall". Under 'Remote Gateway' choose the 'Static IP Address' radio button. In the 'Static IP Address – IP Address' field, enter in the WAN IP of the remote SonicWALL device. Next to 'Mode (Initiator)', select the "Main (ID Protection)" radio button. From the first 'Phase 1 Proposal' drop-down box, select "sonicwall". In the 'Preshared Key' field, enter in the shared secret you wish to use for the VPN tunnel to the SonicWALL device. Then, click on the 'OK' button to save.

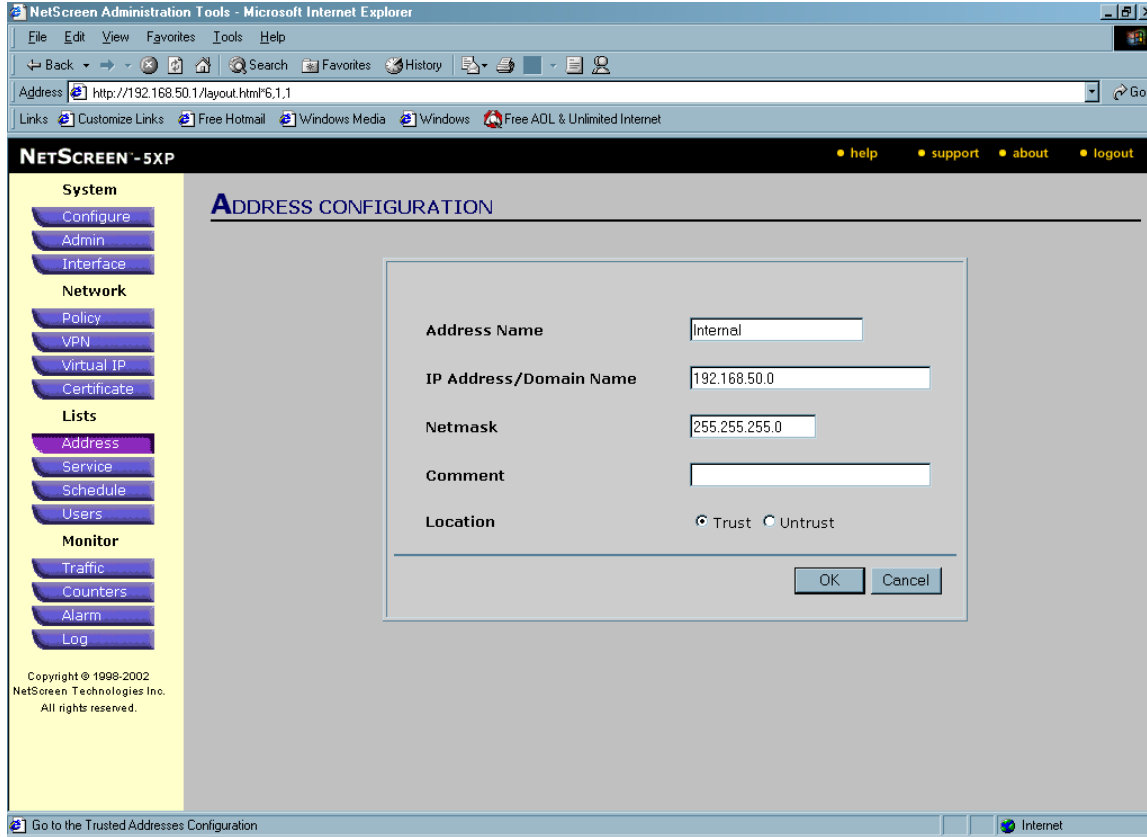
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

7. Click on the 'VPN' button and then the 'AutoKey (P2)' tab. Click on the 'New AutoKey IKE Entry' link at the bottom. In the 'Name' field, enter in "tosonicwall". Next to 'Enable Replay Detection', check the box labeled 'Enable'. From the 'Remote Gateway Tunnel' drop-down box, select "tosonicwall". From the first 'Phase 2 Proposal' drop-down box, select "sonicwall". Next to 'VPN Monitor', check the box labeled 'Enable'. Then, click on the 'OK' button to save.
8. Click on the 'Policy' button and then the 'Outgoing' tab. Click on the 'New Policy' link at the bottom. In the 'Name (optional)' field, enter in "tosonicwall". From the 'Source Address' drop-down box, select "Internal". From the 'Destination Address' drop-down box, select "sonicwall". From the 'Service' drop-down box, select "ANY". Next to 'NAT', select the "Off" radio button. From the 'Action' drop-down box, select "Tunnel". From the 'VPN Tunnel' drop-down box, select "tosonicwall". Check the box next to 'Modify matching incoming VPN policy'. Check the box next to 'Logging'. Check the box next to 'Counting'. Next to 'Traffic Shaping', select the "Off" radio button. Then, click on the 'OK' button to save.
9. Click on the 'Policy' button and then the 'Outgoing' tab. You will need to move this new policy so that it runs before the default rule. In the rule with 'Source – Internal' and 'Destination – sonicwall', click on the opposing-arrows symbol to the right and move it before the Policy ID of the default rule. You may need to do the same for the 'Incoming' tab.

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

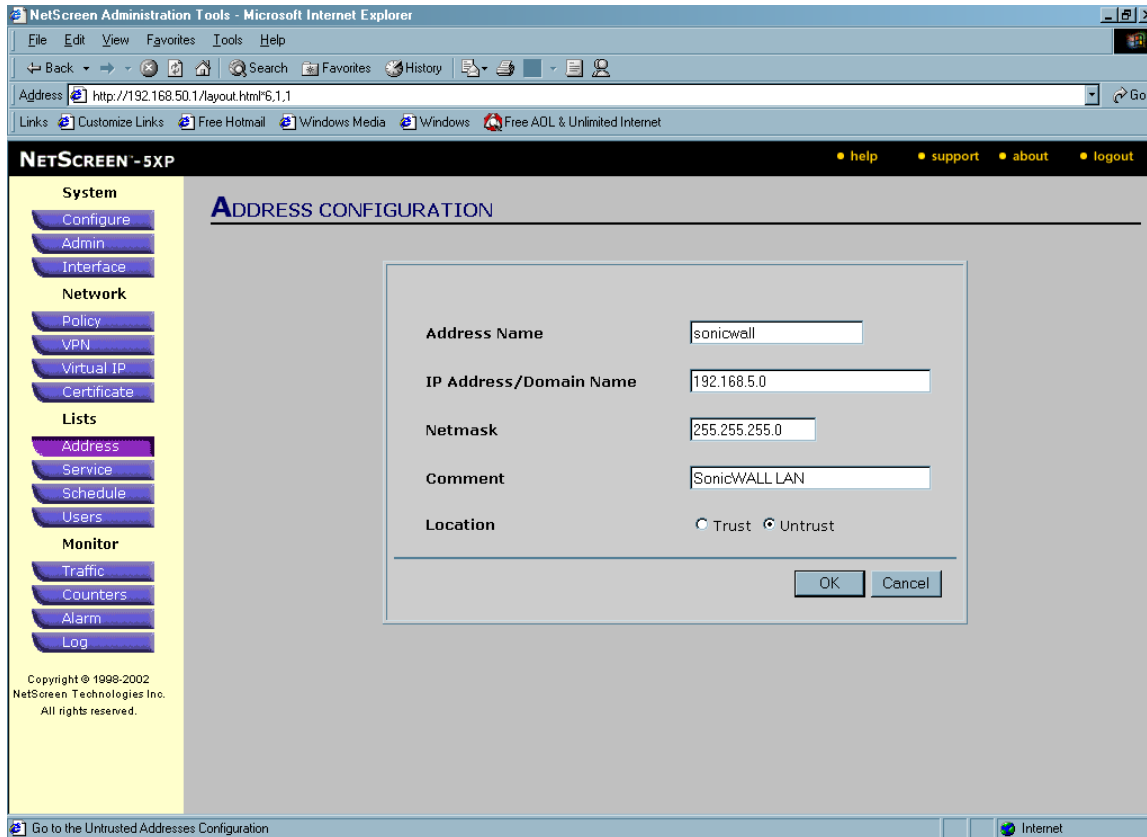
NetScreen device Screenshots

Example of 'Address Book – Trusted':



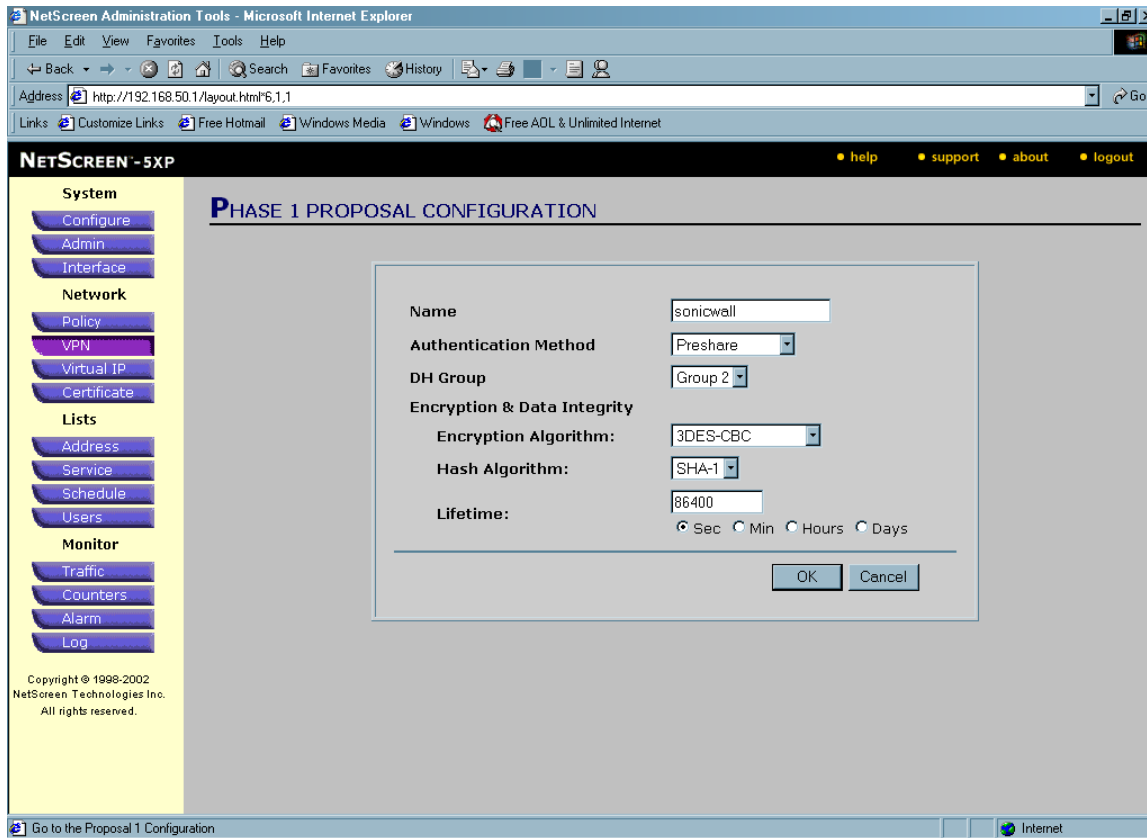
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of 'Address Book – Untrusted':



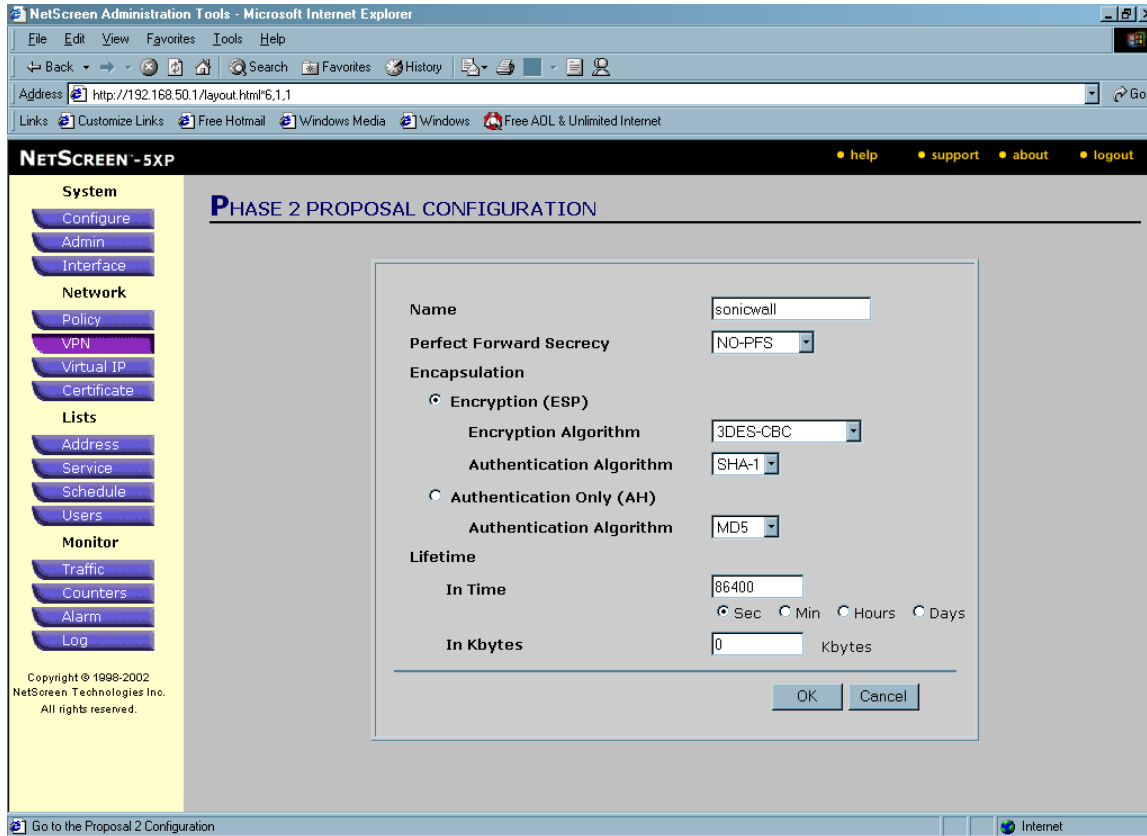
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of 'P1 Proposal':



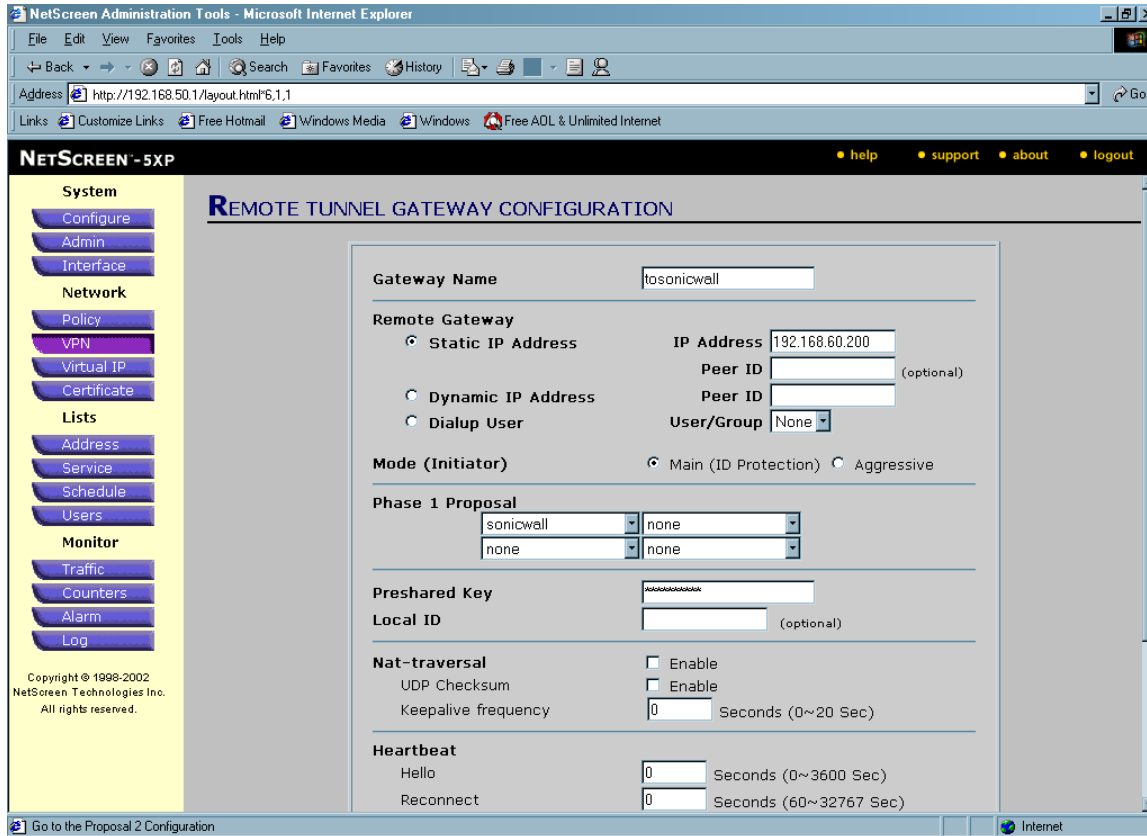
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of 'P2 Proposal':



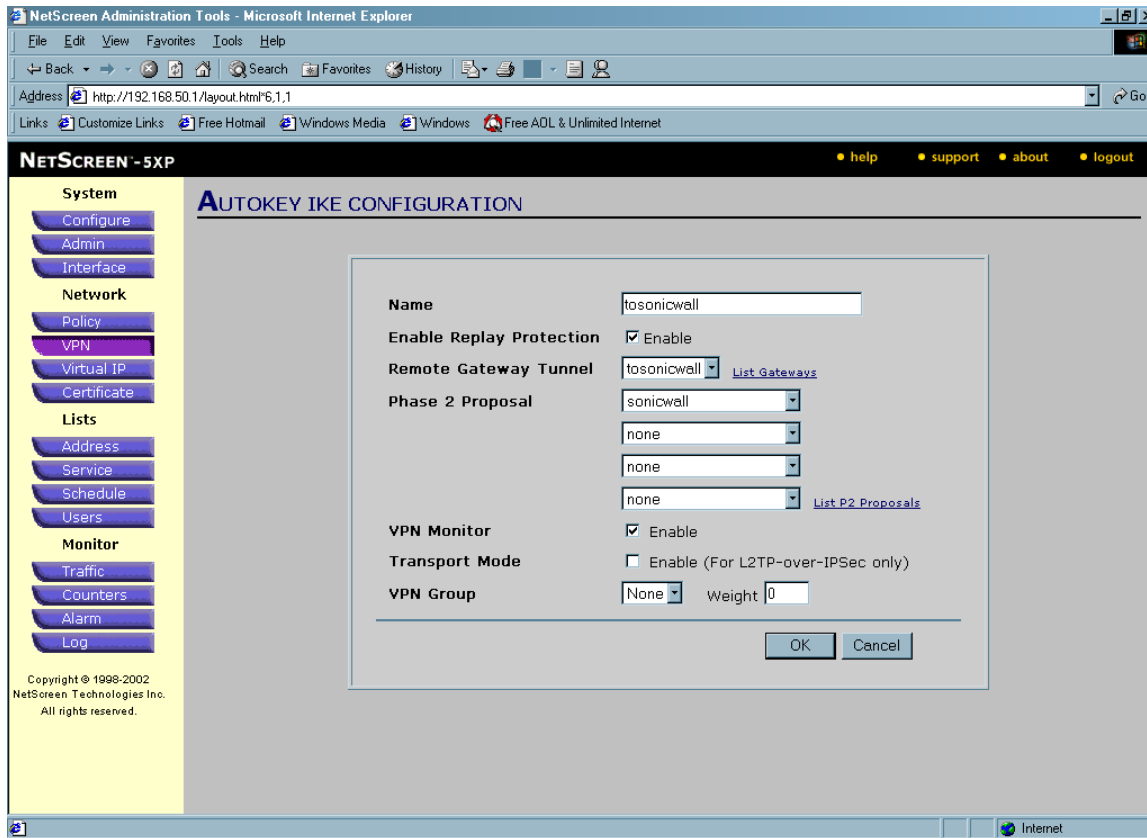
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of 'Gateway':



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of 'AutoKey IKE Entry':



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and RedCreek Ravlins

Example of 'Policy':

