

SonicWALL VPN with Watchguard using IKE

Prepared by SonicWALL, Inc.

8/10/01

Configuring a VPN using: IKE/3DES/MD5

Introduction: This white paper was written under the assumption that the reader already has a basic knowledge of Watchguard and SonicWALL firewall technologies and basic configuration. It will require that the user has a fundamental understanding of VPN, encryption, authentication, data integrity/hashing and key exchange. This paper was primarily written for use with a Watchguard Firebox II (LiveSecurity Version 4.61) and SonicWALL firmware version 6.1.0.

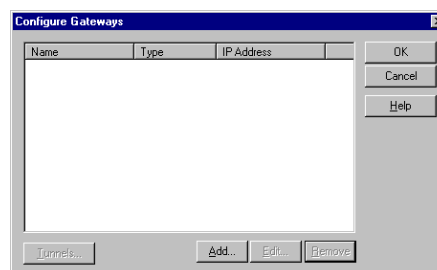
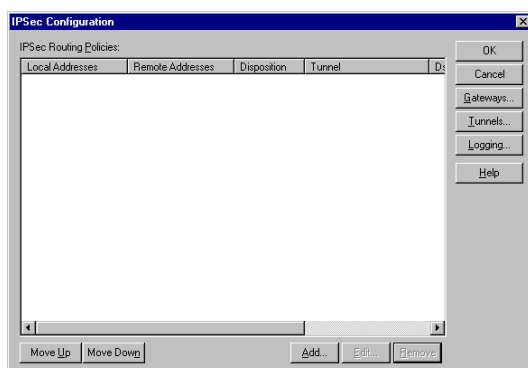
Key Considerations: This white paper details a configuration that allows for a VPN to be configured between a SonicWALL access security product and a Watchguard Firebox II. This paper details the IKE or dynamic key exchange setup using 3DES encryption and MD5 authentication. Tunnels can also be setup using DES encryption and SHA1 authentication with relatively intuitive adjustments. This configuration works for the 6.1.0 SonicWALL firmware going to the 4.61 version of the LiveSecurity/WatchGuard Control Center.

Configuring the Watchguard Firebox II side:

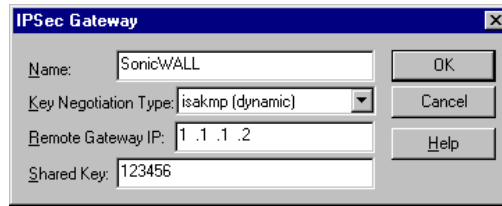
The Watchguard VPN configuration is the trickier part of the configuration. Watchguard calls it's VPN configuration section 'Branch Office VPN.' It breaks up this section into 3 parts: IPSec, Basic DVCP and Watchguard VPN. Basic DVCP is the client VPN configuration which we will not get into here. Watchguard has it's own proprietary VPN configuration between 2 Watchguard boxes found in the Watchguard VPN section. The IPSec option is the choice we are interested in. This is the IPSec compliant option used for 3rd party interoperability. It involves 3 principle configurations: Gateway, Tunnel and Routing Policies.

Configuring the Gateway:

- From the Policy Manager, click on Network>Branch Office VPN>IPSec
- In the IPSec Configuration box, click on Gateway.



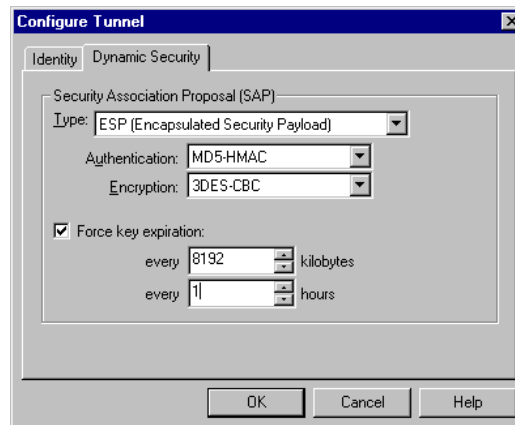
- Click on Add to bring up the IPSec Gateway box.



- Create a name for the gateway that identifies the gateway (no spaces or symbols).
- Select 'isakmp (dynamic)' as the Key Negotiation Type.
- Enter the SonicWALL's WAN IP address.
- Enter the agreed on shared secret.
- Click OK.

Configuring the tunnel:

- From the IPsec Configuration box, Click on Tunnels to bring up the 'Configure Tunnels' box. Click 'Add.'
- Select the Gateway you just created and click OK.
- Enter a name for the Tunnel (i.e. SonicTunnel).
- Click on the Dynamic Security Tab.

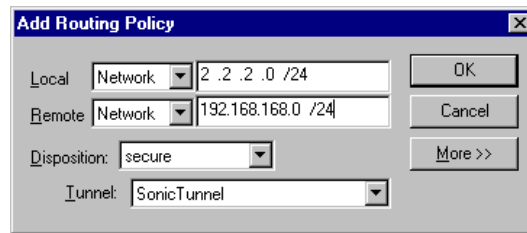


- Select **ESP (Encapsulated Security Protocol)** as the type.
- Select **MD5 HMAC** as the authentication.
- Select **3DES-CBC** as the encryption.
- Check the Force Key negotiation checkbox.
- Change the every ____ hours box to **1 (one)** hour. * (This is critical!).
- Click OK.

*If this is not changed, the tunnel will not come back up if the SonicWALL is rebooted. The Firebox II will not allow the SA to be renegotiated (within a reasonable amount of time), unless this change is made.

Configuring the Routing Policy

- From the IPsec Configuration box, click Add. This will bring up the Add Routing Policy Box.

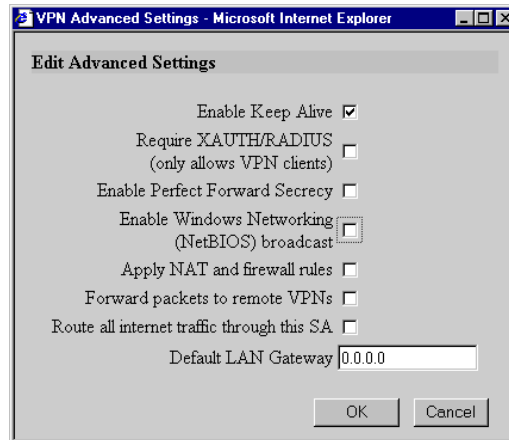


- Here you must describe the encryption domains or the source and destination networks that will traverse the tunnel
 - In the **Local** boxes, enter information to describe the host or network behind the Firebox II.
 - If it is a host, select 'host' if it is a network, select network.
 - Enter the IP address in 'slash' format (A.B.C.D/XY).
 - In the Remote boxes, enter information to describe the host or network behind the SonicWALL.
 - If it is a host, select 'host' if it is a network, select network.
 - Enter the IP address in 'slash' format (A.B.C.D/XY).
 - Select **Secure** as the disposition.
 - Select the tunnel you created above as the tunnel.
 - Click OK.
- Click OK to close out the IPsec Configuration box.
- Click File>Save to Firebox.

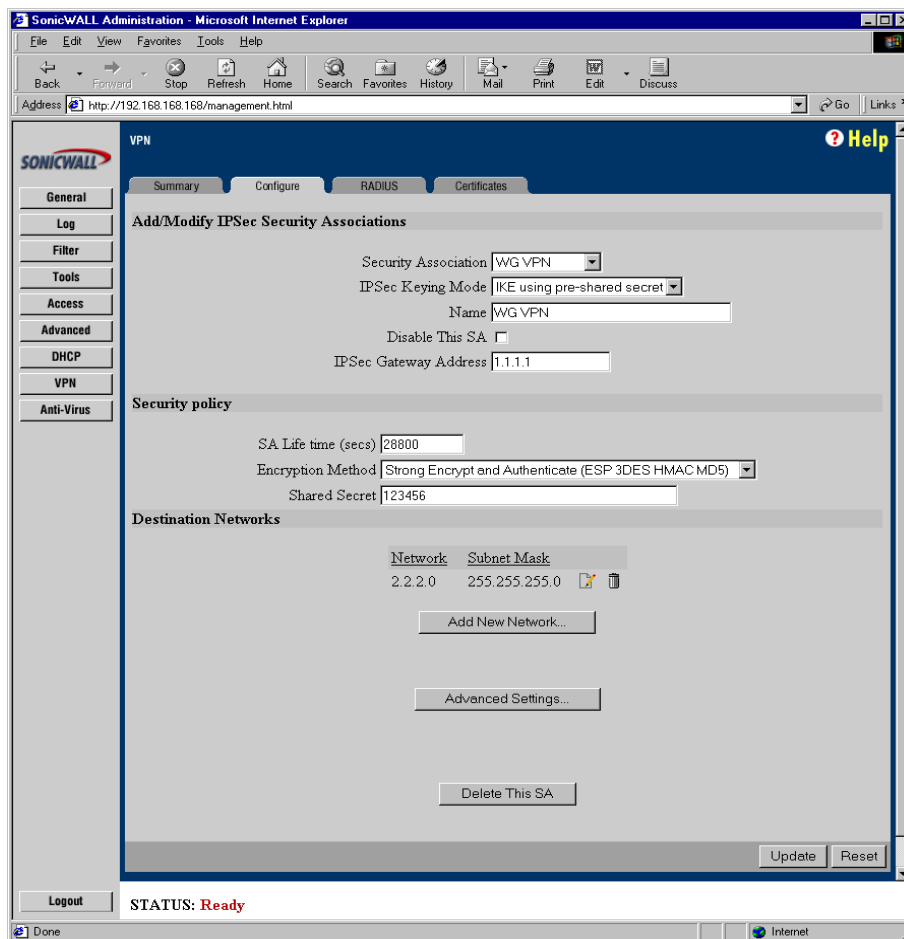
Configuring the SonicWALL Side

The SonicWALL side is relatively simple to configure. Some considerations to take into account is the amount of traffic passing through the box (if it's a tele/soho/XPRS/PRO) and how many SA's are bogging the box down.

- Begin configuring by logging in to the SonicWALL, and clicking on the VPN tab. (We will assume the box is registered/upgraded and has a basic config).
- Click on Add New SA in the first drop down menu.
- Select 'IKE using preshared secret as the IPsec Keying Mode.
- Name the SA appropriately (I.E. Watchguard to SonicWALL SA).
- Leave the SA enabled (not disabled).
- Enter the IPsec Gateway address (The address of the Watchguard Firebox II).
- Check the security policy boxes as needed to allow appropriate access, but make sure Perfect Forwarding Secrecy (PFS) is turned off (this is critical).
- Leave the SA Life time (secs) 28800 (the default setting).
- Select 'Encrypt and Authenticate (ESP 3DES HMAC MD5)'.
- Enter the same shared-secret as was entered on the Watchguard configuration.
- Click 'Add a New Network.' Enter the IP address range of the Watchguard SA LAN participants.
- Click OK; the box should close.
- Click on **Advanced Settings**. Check the **Enable keep alive** box



- Click update to update the firewall policy.



Troubleshooting and Miscellaneous Tips

- The re-negotiate SA button that appears on the VPN Summary page is only available when the SA is already sync'c up and agreed upon. This allows you to renegotiate the SA only when the SA is already established. It will NOT force a renegotiation unless the SA is currently agreed on and in sync.
- Use the SonicWALL log in conjunction with the Watchguard log viewer to troubleshoot your VPN connection on a packet layer level.
- It is absolutely critical that PFS is turned off. The tunnel will not function if it is on.
- If the **force key expiration** setting is not reset from 24 hours to 1 hour, the SA will not be renegotiated if the SonicWALL is rebooted. The Firebox will not accept the renegotiation request from the SonicWALL.
- There are issues with the IKE renegotiation for all SonicWALL firmware versions before the 6.1.0 code. If you are having issues, verify that you are using the 6.1.0 code or newer.
- The Firebox II generally is more rigid on allowing an SA to be reset. When in doubt, try rebooting the Firebox II, if an SA will not negotiate or renegotiate.