

SonicWALL VPN with CheckPoint NG using IKE

Prepared by SonicWALL, Inc.

09/03/01

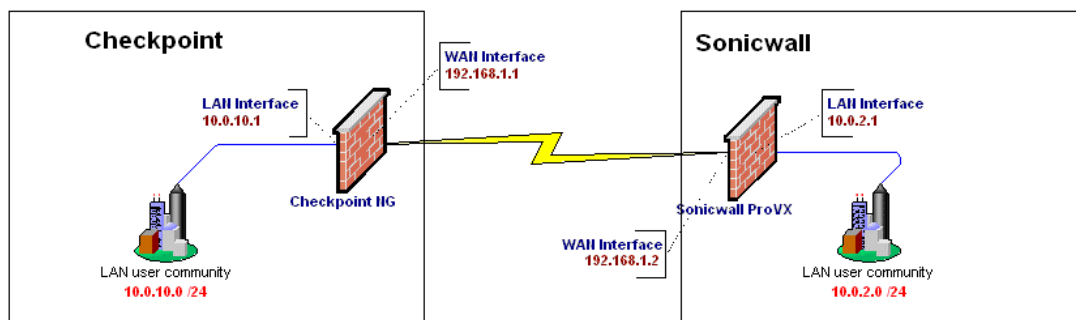
Configuring a VPN using: IKE/3DES/MD5

Introduction: This Tech Note was written under the assumption that the reader already has a basic knowledge of Checkpoint and SonicWALL firewall technologies and basic configuration. It will require that the user have a fundamental understanding of VPN, encryption, authentication, data integrity/hashing and key exchange. This paper was written for the configuration of Checkpoint NG and SonicWALL firmware version 6.1.1.0.

Key Considerations: There are a few key considerations that limit the options when configuring a VPN between a Checkpoint NG firewall and a SonicWALL firewall.

- Though supported by SonicWALL, Checkpoint NG no longer supports the use of manual keys in the creation of VPN tunnels, thus no mention will be found in this document. IKE is the only functional key exchange option between Checkpoint NG and a SonicWALL.
- When a Checkpoint IKE tunnel is configured, it requires the use of a data integrity/hashing method (either MD5 or SHA1).
 - SonicWALLs support MD5 and SHA-1 as well as DES or 3DES.
 - SonicWALL's encrypt for checkpoint option was originally made to interoperate with Checkpoint fw1 v.3.0b. Since then, all encryption methods that match up with corresponding Checkpoint configurations should work (including DES/3DES and MD5/SHA1).
 - There have been issues seen with Checkpoint boxes running on Solaris platform in which aggressive mode must be turned off on the Checkpoint side for the configuration to work. Security administrators should note that Main mode is more secure than Aggressive mode.
- The VPN tab of the SonicWALL has a renegotiate button that can only force a renegotiation when there is a currently agreed upon SA agreement. The button is not available to force a re-negotiation after the initial negotiation fails or is broken.

Here is a diagram of the example configuration:

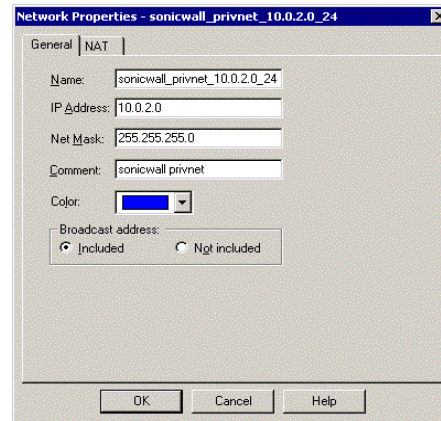
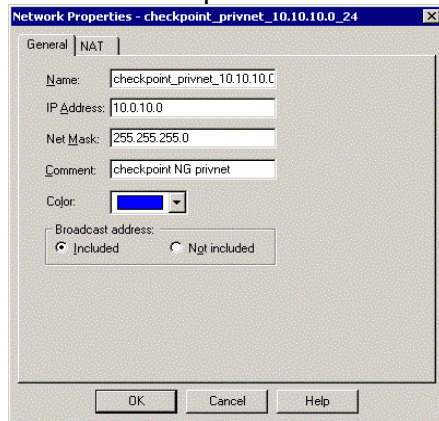


Configuring the Checkpoint NG side:

Since Checkpoint has an object-oriented configuration GUI, it is necessary to create the objects in the security policy rules before creating the actual rules. We will assume that a basic policy has been installed and all access, NAT and routing setups have already been completed.

Creating Network Objects

- ✓ Create the network objects (for both sides of the tunnel).
 - Go to Manage/Network Objects
 - Click on New/Network
 - Fill in the requested information for the network as shown below:



- ✓ Create the local and remote firewall objects as workstation objects.
 - Go to Manage/Network Objects
 - Click on New/Workstation
 - Fill in the property fields for the workstation object as shown below:

Workstation Properties - checkpoint

General

Name:

IP Address:

Comment:

Color:

Type: Host Gateway

Check Point Products

Check Point products installed: Version

VPN-1 & FireWall-1
 FloodGate-1
 Policy Server
 Primary Management Station

Object Management

Managed by this Management Server (Internal)
 Managed by another Management Server (External)

Secure Internal Communication

Communication... DN:

Interoperable VPN Device

Workstation Properties - sonicwall

General

Name:

IP Address:

Comment:

Color:

Type: Host Gateway

Check Point Products

Check Point products installed: Version

VPN-1 & FireWall-1
 FloodGate-1
 Policy Server
 Management Station

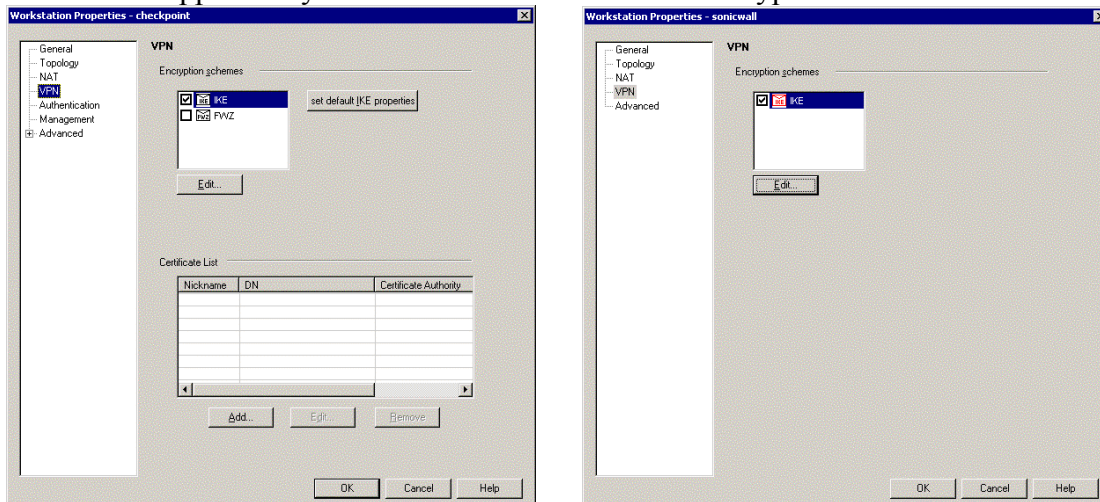
Object Management

Managed by this Management Server (Internal)
 Managed by another Management Server (External)

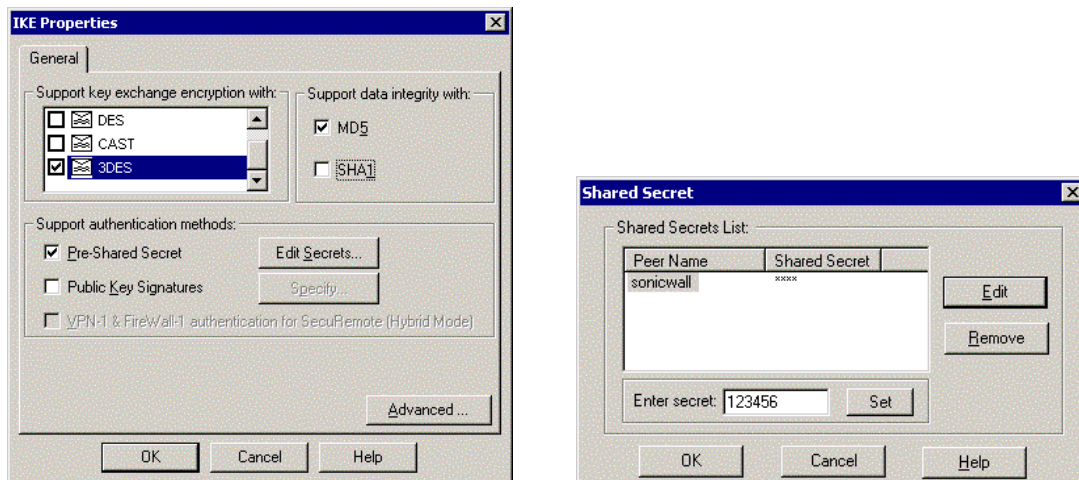
Interoperable VPN Device

- *Note- both workstations must be specified as Gateway objects, and have the 'Interoperable VPN Device' box checked. The version of Checkpoint firewall must also be specified to enable all other needed configuration features as well.*

- Click on the VPN Tab, and you should see the following screens for the corresponding gateways. Notice that Checkpoint has an option for using the FWZ encryption scheme. This is a Checkpoint proprietary encryption method, and is not supported by SonicWALL. Select the IKE encryption method.



- Select IKE as the Encryption Scheme defined. Then click edit to configure the VPN properties and Preshared secret for the VPN as shown below:



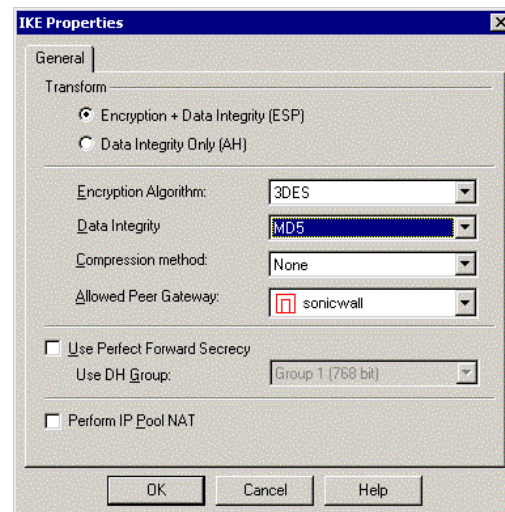
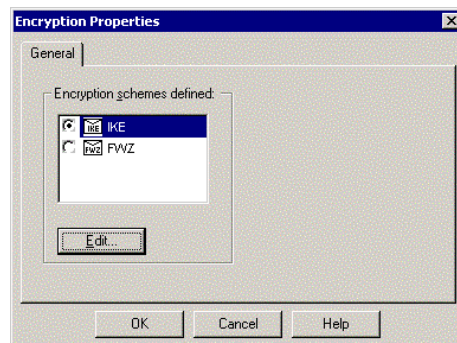
- Select DES or 3DES as the encryption method.
- Select MD5 or SHA-1 as the Hash method.
- Select Preshared Key as the Authentication method
 - Click edit secrets and find the opposite firewall of the one being configured and enter a Preshared secret (must contain at least 6 characters with at least 4 unique characters).
 - Click OK until all the configuration boxes are gone.

Configuring the Security Policy Objects

- Create a new rule at or near the top of the policy. (It is important to have all encryption rules at or near the top of the policy (appropriately, of course), such that the traffic is encrypted before it is simply 'accepted' and allowed out.)
- This rule should include both the Checkpoint and SonicWALL's networks as both source and destination and the action should be 'encrypt' as shown below.

NO	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	checkpoint_privnet_10.0.10.0_24 sonicwall_privnet_10.0.2.0_24	sonicwall_privnet_10.0.2.0_24 checkpoint_privnet_10.0.10.0_24	* Any	Encrypt	Log	checkpoint	* Any	VPN Rule-Checkpoint and Sonicwall Private Networks
2	checkpoint_privnet_10.0.10.0_24	* Any	* Any	accept	Log	checkpoint	* Any	Allow LAN to Internet
3	* Any	* Any	* Any	drop	Log	checkpoint	* Any	Cleanup Rule

- Double click on the 'encrypt' action to edit the encryption properties.
- Select IKE as the form of encryption.
- Click on edit and select the appropriate encryption settings as shown below:



- Select the encryption algorithm 3DES and the data integrity MD5.
- Select the SonicWALL as the allowed peer gateway from the drop-down menu.
- Perfect Forwarding Secrecy can be used, but must be configured the same on both sides. Click OK until all configuration boxes are closed.

Configuring the NAT Tab

- In most cases, the internal LAN will be accessing the Internet through a Hide-mode NAT (also known as port address translation or many-to-one NAT). The key to remember is that Checkpoint performs NAT on a received packet before it sends it

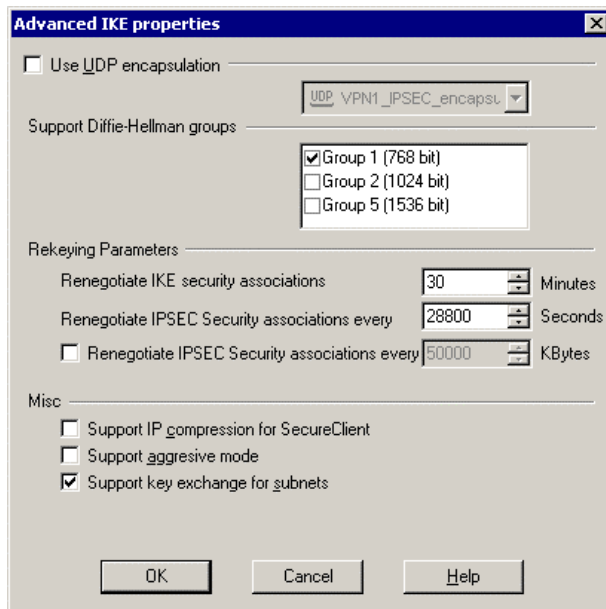
through the security policy. Therefore it is necessary to create a NAT rule that tells the firewall what traffic is to be encrypted.

- This is shown below, as packets to be encrypted are kept as ‘original/original.’ This should be placed above other NAT rules so that packets bound for the tunnel aren’t NAT’d first.

NO	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	checkpoint_privnet_10.0.10.0_24	sonicwall_privnet_10.0.2.0_24	* Any	= Original	= Original	= Original	checkpoint	VPN Traffic-Do Not NAT
2	checkpoint_privnet_10.0.10.0_24	* Any	* Any	checkpoint	= Original	= Original	checkpoint	General NATP

Resetting the Key Exchange Times (This is CRITICAL)

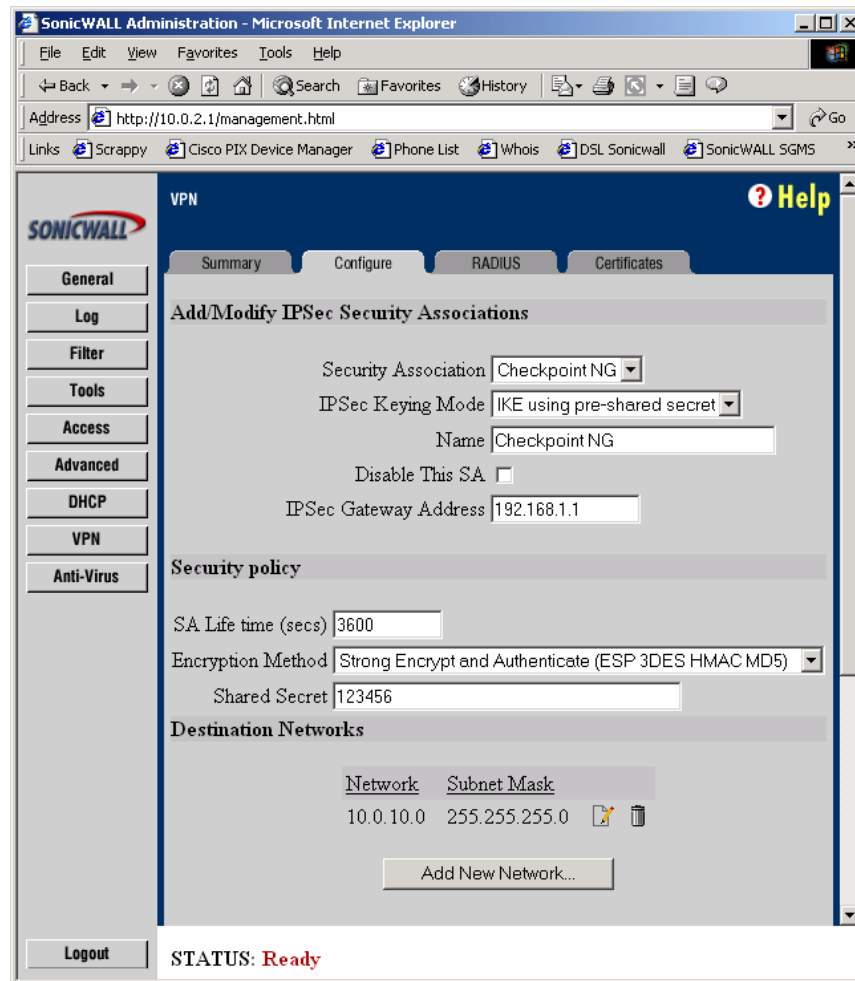
- Due to IKE default incompatibilities, it is also necessary to edit the Policy/Properties tab. Click on Policy/Properties/Encryption tab.
- Change the ‘Renegotiate IKE SA every ___ minutes’ entry to 30 minutes. Re-install the policy. This will force the re-keying to occur every 30 minutes, and is a good balance of security and overhead. This used to have to be set very low, however, both the Checkpoint and SonicWALL will immediately bring the tunnel back up even if the other side is rebooted.



Configuring the SonicWALL Side

The SonicWALL side is relatively simple to configure. Some considerations to take into account are the amount of traffic passing through the box (Tele2/Soho2/XPRS2/PROVX) and how many SA's are going through the box.

- Log into the SonicWALL, and click on the VPN tab. (We will assume the box is registered, has VPN enabled, and has a basic configuration)
- 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. SonicWALL to Checkpoint NG).
- Leave the SA enabled (not disabled).
- Enter the IPSec Gateway address (The external address of the Checkpoint Firewall).
- Check the security policy boxes as needed to allow appropriate access.
- Leave the SA Life time (secs) 28800
- Select your encryption type to match up with the Checkpoint configuration encryption (3DES) and authentication (MD5).
- Enter the same shared secret as was entered on the Checkpoint configuration (ex: 123456)
- Click 'Add a New Network.' Enter the IP address range of the Checkpoint private network (LAN side).
- Click OK, The SA and the firewall should be updated already. (See below).



Troubleshooting and Miscellaneous Tips

- The re-negotiate SA button that appears on the VPN Summary page is only available when the SA has already been created.
- Make sure the **SA lifetime** on the SonicWALL matches the value entered for the **renegotiate IPsec security association every XXX seconds** field on the Checkpoint.
- Troubleshooting can be done using either the SonicWALL's log viewer or the Checkpoint log viewer.
- Changing the SA re-key times will affect overhead and load on the firewall, please be certain the firewall can handle the extra load based on what model it is and how much NAT'd or encrypted traffic is passing through it.
- SonicWALL's 'encrypt for checkpoint' options were originally made to interoperate with Checkpoint fw1 v.3.0b. Since then, all encryption methods that match up with corresponding Checkpoint configurations should work (including DES/3DES and MD5/SHA1).

Troubleshooting and Miscellaneous Tips continued...

- There have been issues seen with Checkpoint boxes running on Solaris platform in which aggressive mode must be turned off on the Checkpoint side for the configuration to work. Security administrators should note that Main mode is more secure than Aggressive mode.