

SonicWALL VPN with Checkpoint 4.1 using IKE

Prepared by SonicWALL, Inc.

08/16/01

Configuring a VPN using: IKE/3DES/MD5/PFS

Introduction: This white paper 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 has a fundamental understanding of VPN, encryption, authentication, data integrity/hashing and key exchange. This paper was primarily written for use with Checkpoint Firewall-1 v.4.1 SP3 (any platform) and SonicWALL firmware version 6.0.1.1. However this white paper has also been verified to apply to Checkpoint firewalls running SP4.

Service Pack and Firmware Version Interoperability:

When running 6.0.0 series firmware, Manual Key tunnels can be run to all service pack levels except for SP3 (SP3 disabled their manual key features). IKE tunnels can be configured to SP3 and SP4 only.

When running the 5.0.0 series firmware, manual key tunnels can be run to all service pack levels except SP3(SP3 disabled their manual key features). IKE tunnels can be run to SP1 and SP2 only (not SP3 or SP4).

Key Considerations: There are a few key considerations that limit the options when configuring a VPN between a Checkpoint Firewall-1 v.4.1 SP3 firewall and a SonicWALL.

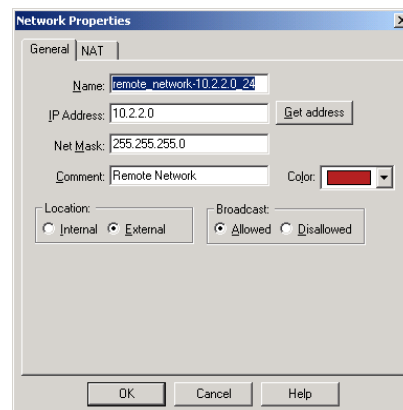
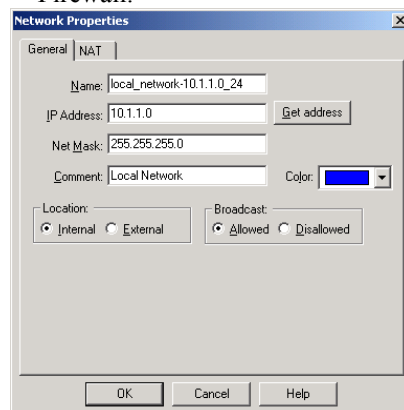
- In Checkpoint's Service Pack 3 release notes, Checkpoint declares they will no longer support manual IPsec key exchange. Therefore IKE is the only functional key exchange option between Checkpoint SP3 and a SonicWALL.
- When a Checkpoint IKE tunnel is configured, it requires the use of a data integrity/hashing method (either MD5 or SHA1).
 - SonicWALLs support both 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 - SonicWALL's encrypt for checkpoint option was originally made to interoperate with Checkpoint fw1 v.3.0b.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. Note- Main mode has been shown to be more secure than aggressive mode.
- The VPN tab of the SonicWALL has a renegotiate button that will can only force a renegotiation when there is a currently agreed upon functional SA agreement. The button is not available to force a re-negotiation after the initial negotiation fails or is broken.

Configuring the Checkpoint Firewall-1 v4.1 SP3 side:

Since Checkpoint Firewall-1 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.

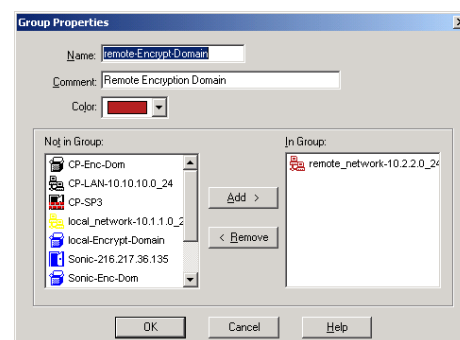
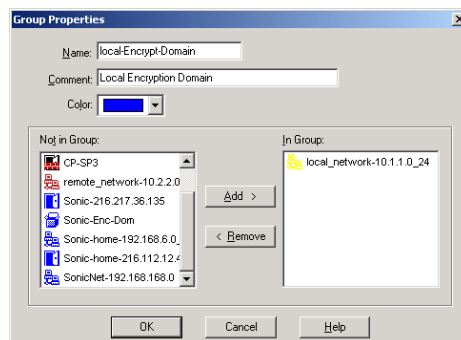
Creating Network Objects

- ✓ Create the network objects (remote and local).
 - Go to Manage/Network Objects
 - Click on New/Network
 - Fill in the requested information for the network as shown below:
 - Note- Internal and external refer to whether they are protected behind the Checkpoint Firewall.



- note- broadcast allowed of disallowed should be based on the networks requirements

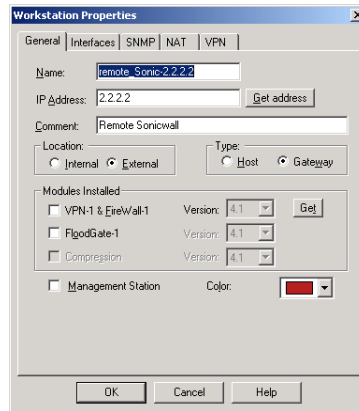
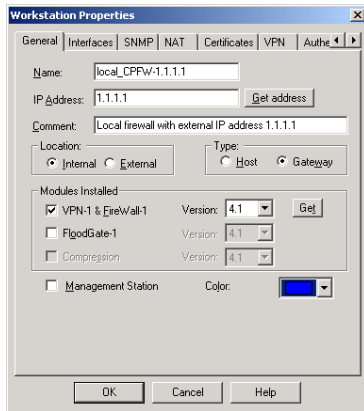
- ✓ Create the local and remote encryption domains as group objects.
 - Go to Manage/Network Objects
 - Click on New/Group
 - Fill in the properties for the group object as shown below:



*note- be sure to include the proper objects into the encryption domain.

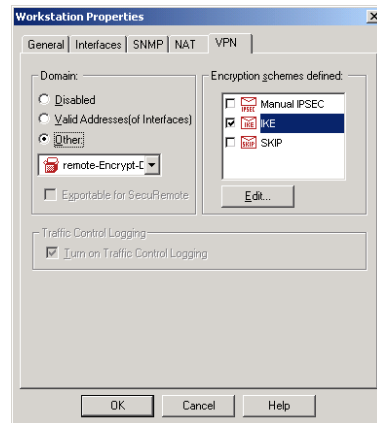
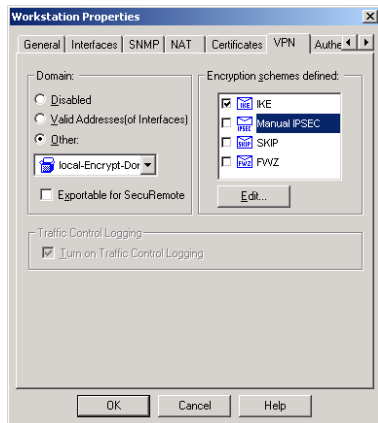
- ✓ Create the local and remote firewall objects as workstation objects.
 - Go to Manage/Network Objects
 - Click on New/Workstation
 - Fill in the property fields for the workstation object as shown below:

SonicWALL VPN with Checkpoint 4.1 using IKE

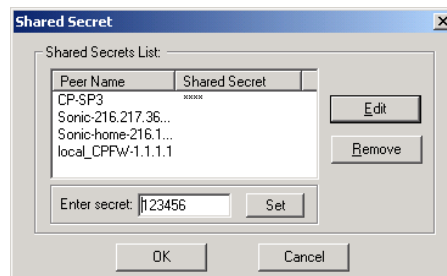
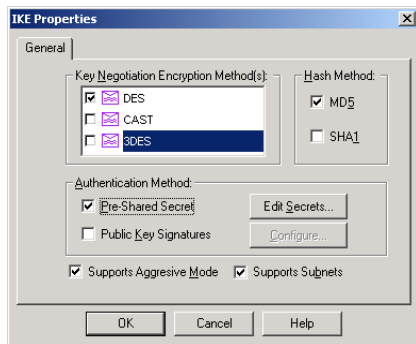


- Note- these workstations must be clicked as Gateway objects and the Checkpoint firewall object must be clicked as VPN-1 Firewall to enable all other needed configuration features.

- Click on the VPN Tab and configure the VPN properties as shown below:



- Note- For Domain, choose 'other' as the type and select the local encryption domain group object in the drop down box for the remote firewall.
- Select IKE as the Encryption Scheme defined. Then click edit to configure the VPN properties and preshared key for the VPN as shown below:

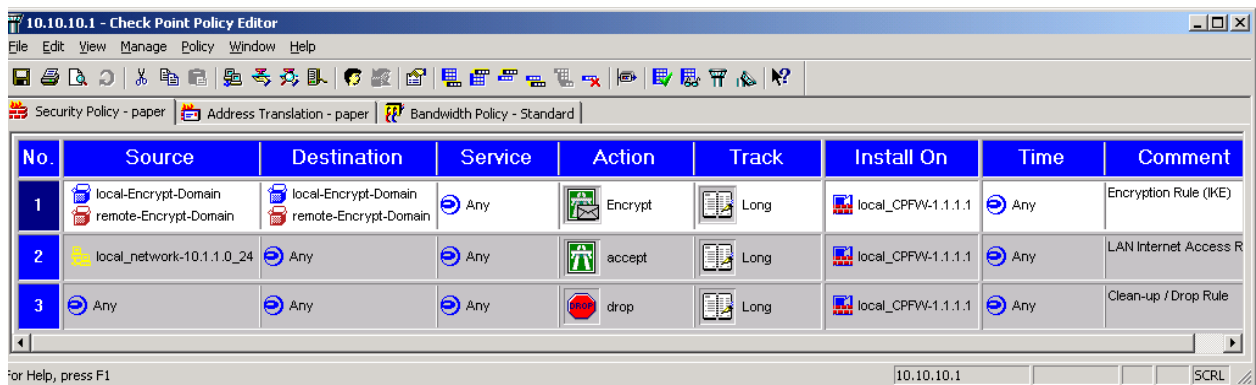


- Select DES or 3DES as the encryption method.
- Select MD5 or SHA-1 as the Hash method.

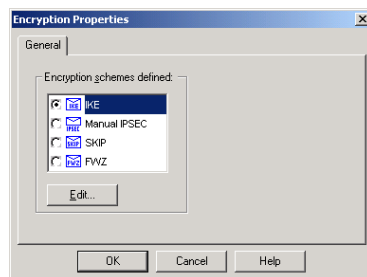
- Select Preshared Key as the Authentication method
 - Click edit secrets and find the opposite firewall of the one being configured and enter a preshared secret (must contain at least 6 characters with at least 4 unique characters).
 - Click OK until all the configuration boxes are gone.

Configuring the Security Policy Objects

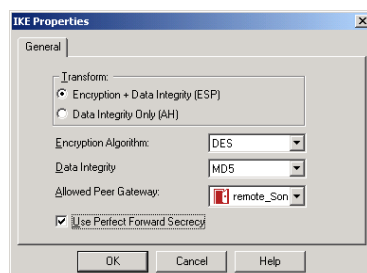
- Create a new rule at or near the top of the policy. (It is important to have all encryption rules at or near the top of the policy (appropriately, of course), such that the traffic is encrypted before it is simply 'accepted' and allowed out.)
- This rule should include both encryption domains as both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



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



- Click on edit and select the appropriate encryption settings:



- Select the encryption algorithm (DES or 3DES) and the data integrity (MD5 or SHA-1).
- Select the remote firewall as the allowed peer gateway
- 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

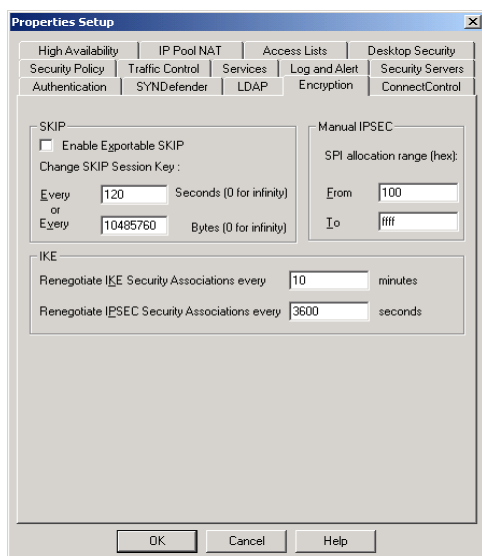
- In most cases, the internal LAN will be accessing the Internet through a Hide-mode NAT (also known as port address translation or many-to-one NAT). The key to remember, is that Checkpoint performs NAT on a received packet before it sends it through the security policy. Therefore it is necessary to create a NAT rule that tells the firewall to not traffic that 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'ing rules so that packets bound for the tunnel aren't NAT'd first.

The screenshot shows the Check Point Policy Editor interface. The 'Address Translation' tab is active, displaying a table of NAT rules. The table has columns for 'No.', 'Original Packet' (Source, Destination, Service), 'Translated Packet' (Source, Destination, Service), 'Install On', and 'Comments'.

No.	Original Packet			Translated Packet			Install On	Comments
	Source	Destination	Service	Source	Destination	Service		
1	local_network-10.1.1.0_24	remote_network-10.2.2.0_24	Any	Original	Original	Original	local_CPFW-1.1.1.1	VPN Traffic (Do Not NAT).
2	local_network-10.1.1.0_24	Any	Any	local_CPFW-1.1.1.1	Original	Original	local_CPFW-1.1.1.1	LAN Hide PAT

Resetting the Key Exchange Times (This is CRITICAL)

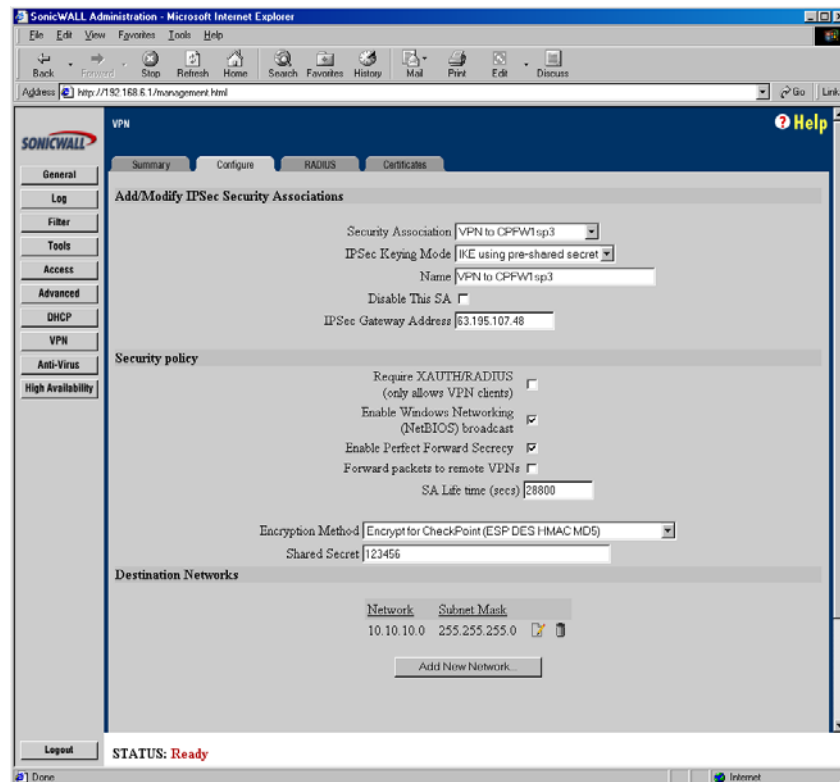
- Due to IKE default incompatibilities, it is also necessary to edit the Policy/Properties tab. Click on Policy/Properties/Encryption tab.
- Change the 'Renegotiate IKE SA every ___ minutes' entry to 10 minutes. Re-install the policy. This change will force the re-keying to occur immediately following any reboot of policy implementation on the Checkpoint side.



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. remote to local SA).
- Leave the SA enabled (not disabled).
- Enter the IPsec Gateway address (The 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 (DES or 3DES) and authentication (MD5 or SHA-1).
- Enter the same shared secret as was entered on the Checkpoint configuration.
- Click 'Add a New Network.' Enter the IP address range of the Checkpoint SA participants.
- 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 is already sync'c up and agreed upon. .
- At present time, it is much easier to troubleshoot using the dynamic log viewer of the Checkpoint firewall.
- 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).
- 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. Note- Main mode has been shown to be more secure than aggressive mode.
- When running 6.0.0 series firmware, Manual Key tunnels can be run to all service pack levels except for SP3 (SP3 disabled their manual key features). IKE tunnels can be configured to SP3 and SP4 only.
- When running the 5.0.0 series firmware, manual key tunnels can be run to all service pack levels except SP3(SP3 disabled their manual key features). IKE tunnels can be run to SP1 and SP2 only (not SP3 or SP4).