

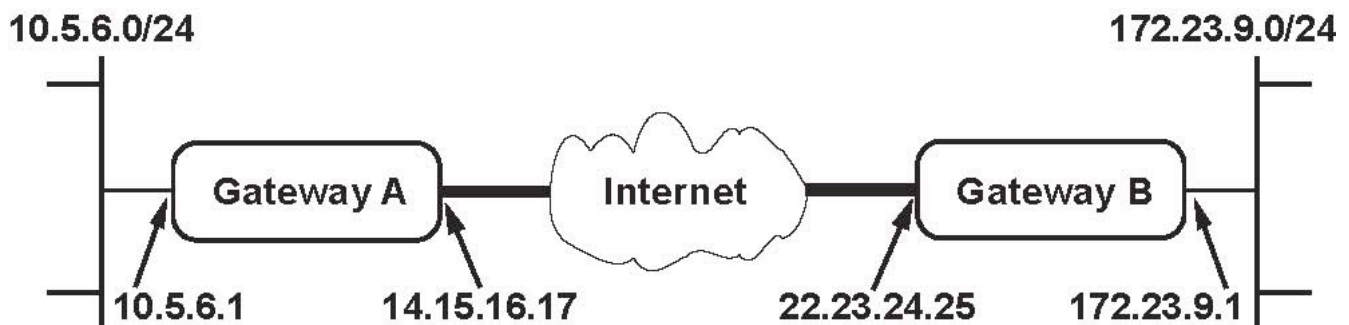
SnapGear Documentation

Examples for IPsec Interoperability

This document contains two examples for **Scenario 1** of the VPN Consortium's Documentation Profiles for IPsec Interoperability, **Basic Interop** and **AES Interop**.

Basic Interop Scenario 1: Gateway-to-gateway with preshared secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication. The tunnel requires TripleDES for encryption, SHA-1 for hash, 1024-bit key exchange, and a preshared secret for authentication.



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To setup the SnapGear as Gateway A in this scenario, use the following steps . The easiest method of accessing the Console is browsing to the SnapGear device from a Javascript enabled web browser running on a PC located on the SnapGear's LAN. (See **Step 1. below**)

To setup the other Vendor's product as Gateway B in this scenario, refer to their Documentation Profile at <http://www.vpnc.org/InteropProfiles/>.

SUMMARY OF STEPS

Step 1. Booting the SnapGear Device and Activating the Interfaces.

Step 2. Configure the IPSec General Settings.

Step 3. Add a New IPSec Tunnel.

Step 4. Configure the Local Endpoint Settings.

Step 5. Configure the Remote Endpoint Settings.

Step 6. Configure the IKE Phase 1 parameters.

Step 7. Configure the IKE Phase 2 parameters.

Step 8. Confirm VPN Operations, Troubleshooting and Log Monitoring.

The following subsections explain each of these steps in detail. These steps are based on all Secure Computing SnapGear Models with **Version 3.1.5u3 firmware**.

Step 1. Booting the SnapGear Device and Activating the Interfaces.

1.1. . Power Up the unit without any other cabling in place. Plug the 5V DC Mini-Plug in first. Always plug the AC plug (three prong plug) of the power adapter in last.

1.2. About 25—30 seconds after power is applied, confirm that the unit is in Factory Default mode with all the front LED's blinking green (most models).

Note: If the unit is not at Factory Default, reset the unit by gently pressing the 'ERASE' switch next to the 5V DC Mini-Jack with a ball-point pen tip or a paper clip two times within 20 seconds. The unit will reboot into the Factory Default mode.

1.3. Connect the supplied cable to Ethernet Port A1. Connect the other end to a PC or workstation Ethernet Jack. The workstation should have a Java-enabled Internet Browser application installed, such as Microsoft Internet Explorer or Mozilla Firefox. Configure the PC for any PC IP Address in the range of 192.168.0.2 to 192.168.0.254. The PC's 'Default gateway:' IP Address is the Factory Default address of the SnapGear unit, 192.168.0.1. DNS settings are not required at this time.

1.4. Use the following web address in a Web Browser to log into the unit, <http://192.168.0.1>. The Default username is 'root' and the Default password is 'default'. It is good practice to change this password. The latest SnapGear firmware automates access to this recommended step during initial configuration. Enter the new Password in the 'New Password' and 'Confirm Password' windows. If this password is forgotten the SnapGear will have to be erased back to the Factory Default mode to regain access, see the Note in Step 1.2.

- 1.5. It is good practice to cable the Ethernet Port B for Internet access prior to running the Quick Setup Wizard. The Wizard can automatically configure some circuit types if the port is cabled prior to the completing the Internet steps. Connect the other end of the cable to the Cable Modem, DSL Router, or other device supplied by the ISP. Cable and power that device as instructed by the ISP.
- 1.6. After setting the new root password, the Quick Setup Wizard starts on the LAN Page. All of the settings established by the Wizard can be changed later using the regular Menu system. Type a unique hostname in the **Hostname** field that will identify this unit, e.g. Gateway-A. Leave the LAN 'Direct Connection Settings' on the default selection of 'Manual configuration'. Click on the **Next** Button to proceed.
- 1.7. Type the SnapGear LAN address into the **IP Address** field, 10.5.6.1. This is the address that all other hosts on the LAN will use as their Default Gateway. Type the network mask into the **Subnet Mask** field using '24' or the Dotted-Quad notation of '255.255.255.0'. Click on the **Next** Button to proceed.
- 1.8. Select an **Internet Port Configuration** of **Direct Connection** for Ethernet Port B. Click on the **Next** Button to proceed.
- 1.9. Select an **ISP Connection** of Manual Configuration. Click on the **Next** Button to proceed.
- 1.10. Type the SnapGear Internet (WAN) address into the **IP Address** field, 14.15.16.17. Type the network mask into the **Subnet Mask** field using '24' or the Dotted-Quad notation of '255.255.255.0'. Scenario 1 does not list Internet Gateway addresses, but be sure to enter an appropriate IP address in the **Gateway Address** field. Do the same for the **DNS Server(s)** field. Click on the **Next** Button to proceed.
- 1.11. The **Switch Configuration** selection should be left at the default setting of '4 LAN Ports' for now. Using 4 LAN Ports lets you plug up to four devices directly into the SnapGear as part of the 10.5.6.0/24 network. Click on the **Next** Button to proceed.
- 1.12. The last step in Quick Setup Wizard is the review page. It is especially important to confirm the new LAN settings. Since the LAN IP Address has been moved from the default 192.168.0.0/24 Network, communication with the PC will cease after the 'Finish' control is Clicked. In this example, all you have to do is adjust the web address in Web Browser to http://10.5.6.1. Remember to plan for any required changes to your PC's Ethernet configuration for the 10.5.6.0/24 network prior to Clicking the 'Finish' control.
- 1.13. The Quick Setup Wizard completes with a page containing links to the **Save/Restore page** and the Secure Computing SnapGear registration site.
- 1.14. Clicking the **Save/Restore page** hyperlink opens the Remote Backup/Restore page. Enter and Confirm a Backup password, then Click the **Save** control. Click the **Save** button in the **File Download** dialog and **Browse** the workstation file system to save the backup file. Use the **System** navigation menu, **Backup/Restore** Link to backup successful VPN configurations or to restore known-good configurations.

Note: Right-Click the round (?) Icon in any configuration screen and select 'Open in new window' or 'Open in new tab' to read more detail on the task being performed or any options that may be available.

Step 2. Configure IPsec General Settings

- 2.1. From the **VPN** navigation menu on the left hand side of the **SnapGear Management Console** select the **IPSec** hyperlink.
- 2.2. Check the box next to **Enable IPSec**. Leave the **IPSec MTU** field blank unless you know that Gateway B or the Internet circuit between the Gateways requires an IPSec Maximum Transmission Unit below 1500 bytes.
- 2.3. Click the **Submit** Button. The configuration window should return a prompt of
Action Successful
The configuration has been updated

Step 3. Add a New IPSec Tunnel

- 3.1. Scroll down to the controls beneath the **Tunnel List**. The **Quick Setup** Button is generally recommended for SnapGear-to-SnapGear VPN configurations. Click the **Advanced** Button.
- 3.2. The configuration window should return a new working pane called **Tunnel Settings**. Fill out the form fields so they appear as follows:
Tunnel Name: GatewayA_to_GatewayB
Enable this tunnel: Checked
Local Interface: default gateway interface
Keying: Main mode (IKE)
Local address: static IP address
Remote address: static IP address
Authentication: Preshared Secret
- 3.3. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Local Endpoint Settings**.

Step 4. Configure the Local Endpoint Settings

- 4.1. Fill out the **Local Endpoint Settings** form so it appears as follows:
Initiate Tunnel Negotiation: Checked
Optional Endpoint ID: Leave this blank to use the default gateway interface IP as the Endpoint ID.
IP Payload Compression: Unchecked
Dead Peer Detection: Unchecked (The Delay and Timeout Fields will disappear.)
IPSec Offload device: Leave the Dropdown List set to **None** unless you are chaining SnapGear devices to accommodate a higher than normal VPN capacity for the devices in your inventory.
Initiate Phase 1 & 2 rekeying: Checked
- 4.2. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Remote Endpoint Settings**.

Step 5. Configure the Remote Endpoint Settings.

- 5.1. Fill out the **Remote Endpoint Settings** form so it appears as follows:

The remote party's IP address: 22.23.24.25

Optional Endpoint ID: Leave this blank to use the remote party's IP address as the Endpoint ID.

- 5.2. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Phase 1 Settings**.

Step 6. Configure the IKE Phase 1 Parameters.

- 6.1. Fill out the **Phase 1 Settings** form so it appears as follows:

Key lifetime (sec): 28800

Rekey margin (sec): 600

Rekey fuzz%: 100

Preshared secret: hr5xb84l6aa9r6

Phase 1 Proposal: 3DES-SHA-Diffie Hellman Group 2 (1024 bit)

- 6.2. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Phase 2 Settings**.

Step 7. Configure the IKE Phase 2 Parameters.

- 7.1. Fill out the top of the **Phase 2 Settings** form so it appears as follows:

Local Network: 10.5.6.0/24

Remote Network: 172.23.9.0/24

- 7.2. Click the **Add** Button. The entries just completed should appear in the summary table at the top of the form.

Note: Scenario 1 uses just one Local LAN for Gateway A and one Peer LAN for Gateway B. Additional Peer Networks for custom scenarios can be configured by repeating Step 7.1 and Step 7.2.

- 7.3. Fill out the bottom of the **Phase 2 Settings** form so it appears as follows:

Key Lifetime(sec): 3600

Phase 2 Proposal: 3DES-SHA

Perfect Forward Secrecy: Checked

Diffie Hellman Group: Diffie Hellman Group 2 (1024bit)

Note: Perfect Forward Secrecy (PFS) requires an exact match for the Diffie Hellman Group (DH Group) in the Phase Two Proposals. Be sure that the Gateway B vendor instructions for PFS are well understood before determining whether to use PFS.

- 7.4. Click on the **Finish** Button to proceed. The configuration window should return to the **IPSec General Settings** pane and there should be a **Connection** entry in the **Tunnel List** labeled 'GatewayA_to_GatewayB'. The **Remote Party** table entry should be '22.23.24.25'. The table **Status** entry will be '**Down**' or '**Negotiating Phase 1**' unless the configuration for Gateway B has also been completed. (See Step 8. below)

- 7.5. Clicking the 'Pad & Pencil' Icon will re-open the configuration panes for Steps 2 – 7 so that corrections may be entered. Clicking the 'Trashcan' Icon will DELETE, not disable the VPN configuration.

- 7.6. To disable one of the VPN Connections in the Tunnel List, click on the small green tick icon to the left of its name in the table. To enable a disabled tunnel, click the empty grey box to the left of its name. It can also be enabled/disabled via the edit/modify menu (pad&pencil icon on the right) – but the tick is quicker and does the same thing.
- 7.7. To disable ALL IPSec VPN Connections, Uncheck the **Enable IPSec** box at the top of the **IPSec General Settings** pane and then Click the **Submit** button. The **Tunnel List** Connection configurations will remain but they will not function until **IPSec** is re-enabled.

Step 8. Confirm VPN Operations, Troubleshooting, and Log Monitoring.

- 8.1. From the **System** navigation menu on the left hand side of the **SnapGear Management Console** and select the **Diagnostics** hyperlink. Select the **Network Tests** Tab and enter the Internet IP for the Gateway B device in the **IP Address of Remote Machine** field, 22.23.24.25. Click the **Ping** Button. After approximately 15 seconds the page will refresh with the results of the ping test and the banner

Action Successful

The following results were returned:

```
PING 22.23.24.25 (22.23.24.25) 56(84) bytes of data.  
64 bytes from 22.23.24.25: icmp_seq=1 ttl=64 time=1.18 ms  
64 bytes from 22.23.24.25: icmp_seq=2 ttl=64 time=1.11 ms  
64 bytes from 22.23.24.25: icmp_seq=3 ttl=64 time=1.33 ms  
64 bytes from 22.23.24.25: icmp_seq=4 ttl=64 time=1.31 ms  
  
--- 22.23.24.25 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3028ms  
rtt min/avg/max/mdev = 1.114/1.238/1.337/0.092 ms
```

If the test results indicate 'Destination Host Unreachable' there may be a problem with the cabling, the Internet or test circuit, or the upstream routes. This test assumes that Gateway B has been configured to reply to 'icmp/echo_request' messages, at least from Gateway A.

- 8.2. Internet access or the test circuit is confirmed if Gateway B's Internet address responds to the Ping test in Step 8.1. If not, go to the **System** navigation menu on the left hand side of the **SnapGear Management Console** and select the **Diagnostics** hyperlink. Look under the **System Tab, Connections Table** for Port B. If the 'State' entry is 'checking', the connection has not been completely negotiated. Confirm all of the Internet cabling, power, and Internet Service Provider (ISP) instructions. Remember to check the cabling for the ISP circuit; which can be a Coaxial Cable, a DSL phone line and filter adapter, or some other cable type. Try power cycling the ISP device and monitoring the indicator lights on the device. Some Cable Modem providers recommend leaving their devices off for five minutes or more in order to insure new circuit negotiation.
- 8.3. If the ping test of Gateway B's Internet address is successful and the **Tunnel List** labeled 'GatewayA_to_GatewayB' has a **Status** entry of '**Running**', this indicates that the VPN Tunnel is established. Using a Client in the Gateway A LAN (10.5.6.0/24), Ping Gateway B's LAN interface address at 172.23.9.1 or an address on the Peer Network of 172.23.9.0/24. This test assumes that the Gateway B has been configured to allow 'icmp/echo_request' messages, at least from the Gateway A LAN. The SnapGear default policy is to allow all IP protocols through the VPN.
- 8.4. The **Tunnel List** labeled 'GatewayA_to_GatewayB' may have **Status** entries as follows:

Down – this indicates that the tunnel is not being negotiated. This may be due to the following reasons; IPsec is disabled, the tunnel is disabled, or the tunnel could not be loaded due to misconfiguration.

Negotiating Phase 1 indicates that IPsec is negotiating Phase 1 to establish the tunnel. Main mode packets are transmitted during this stage of the negotiation process.

Negotiating Phase 2 indicates that IPsec is negotiating Phase 2 to establish the tunnel. Quick mode packets are transmitted during this stage of the negotiation process.

Running, Renegotiating Phase 1 indicates that the tunnel has been established and the tunnel is renegotiating its Phase 1 keys.

Running, Renegotiating Phase 2 indicates that the tunnel has been established and the tunnel is renegotiating its Phase 2 keys.

Each of these status entries is also a hyperlink to details on; the VPN interface and crypto package loads, a **Connection Details** summary of the VPN Proposals for Phase 1 and Phase 2, and the **Negotiation State**. Right-Click the link and choose ‘Open in a new window’ or ‘Open in a new tab’ to view these details. These log entries can be copied and pasted for examination by Secure Computing Technical Support.

- 8.5. It is good practice to have Gateway A and Gateway B synchronized to reliable time references so that reliable logs can be gathered from both devices for the same VPN connection attempts.
- 8.6. Additional log material can be found in the **System** navigation menu, **Diagnostics** hyperlink, **System Log** Tab. Scrolling down to the bottom of the syslog report reveals a filter tool field labeled **Match this string**. Enter an identifying string for IPsec messages on the SnapGear, e.g. ‘Pluto’ and Click the **Update** Button to reduce the report to particular items of interest. Again, These log entries can be copied and pasted for examination by Secure Computing Technical Support. Use the **Remote Syslog** Tab or the **Email Delivery** Tab to configure the Syslog stream for transport off of the SnapGear device for storage or analysis.
- 8.7. Use the **System** navigation menu, **Help and Support** hyperlink, **Technical Support Report** Tab to access the **Download the Technical Support Report** hyperlink and download a complete configuration file (TSR) for examination by Secure Computing Technical Support.
- 8.8. Use the **System** navigation menu, **Diagnostics** hyperlink, **Packet Capture** Tab to access GUI controls for the ‘tcpdump’ tool.

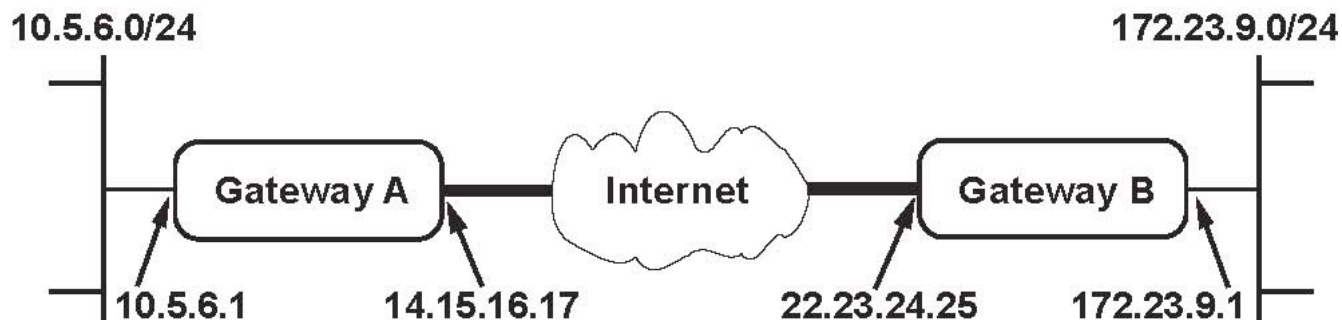
Select the capture interface from the **Interface** Dropdown List and enter filter requirements in the **Options** field. Click the **Add** Button to store one or more Packet Capture Filters in the Index Table at the top of the page.

Activate a Capture Filter by Clicking the Checkbox in the left-hand column of the Index Table. Click the hyperlink entries in the **Download** column to open a File Download dialog. The **.pcap** files are compatible with Ethereal, Wireshark, and other Sniffer utilities. Click the Trashcan Icon to delete a Capture Filter and the associated data.

Use the Packet Display area to select a Capture Filter Index, enter any display filters in the **Options** field, and open a limited report with the **Display** Button.

AES Interop Scenario 1: Gateway-to-gateway with preshared secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication. The tunnel requires 128-bit AES for encryption, SHA-1 for hash, 1024-bit key exchange, and a preshared secret for authentication.



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- AES (128bit)
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- AES (128bit)
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To setup the SnapGear as Gateway A in this scenario, use the following steps . The easiest method of accessing the Console is browsing to the SnapGear device from a Javascript enabled web browser running on a PC located on the SnapGear's LAN. (See **Step 1. below**)

To setup the other Vendor's product as Gateway B in this scenario, refer to their Documentation Profile at <http://www.vpnc.org/InteropProfiles/>.

SUMMARY OF STEPS

Step 1. Booting the SnapGear Device and Activating the Interfaces.

Step 2. Configure the IPSec General Settings.

Step 3. Add a New IPSec Tunnel.

Step 4. Configure the Local Endpoint Settings.

Step 5. Configure the Remote Endpoint Settings.

Step 6. Configure the IKE Phase 1 parameters.

Step 7. Configure the IKE Phase 2 parameters.

Step 8. Confirm VPN Operations, Troubleshooting and Log Monitoring.

The following subsections explain each of these steps in detail. These steps are based on all Secure Computing SnapGear Models with **Version 3.1.5u3 firmware**.

Step 1. Booting the SnapGear Device and Activating the Interfaces.

1.1. . Power Up the unit without any other cabling in place. Plug the 5V DC Mini-Plug in first. Always plug the AC plug (three prong plug) of the power adapter in last.

1.2. About 25—30 seconds after power is applied, confirm that the unit is in Factory Default mode with all the front LED's blinking green (most models).

Note: If the unit is not at Factory Default, reset the unit by gently pressing the 'ERASE' switch next to the 5V DC Mini-Jack with a ball-point pen tip or a paper clip two times within 20 seconds. The unit will reboot into the Factory Default mode.

1.3. Connect the supplied cable to Ethernet Port A1. Connect the other end to a PC or workstation Ethernet Jack. The workstation should have a Java-enabled Internet Browser application installed, such as Microsoft Internet Explorer or Mozilla Firefox. Configure the PC for any PC IP Address in the range of 192.168.0.2 to 192.168.0.254. The PC's 'Default gateway:' IP Address is the Factory Default address of the SnapGear unit, 192.168.0.1. DNS settings are not required at this time.

1.4. Use the following web address in a Web Browser to log into the unit, <http://192.168.0.1>. The Default username is 'root' and the Default password is 'default'. It is good practice to change this password. The latest SnapGear firmware automates access to this recommended step during initial configuration. Enter the new Password in the 'New Password' and 'Confirm Password' windows. If this password is forgotten the SnapGear will have to be erased back to the Factory Default mode to regain access, see the Note in Step 1.2.

- 1.5. It is good practice to cable the Ethernet Port B for Internet access prior to running the Quick Setup Wizard. The Wizard can automatically configure some circuit types if the port is cabled prior to the completing the Internet steps. Connect the other end of the cable to the Cable Modem, DSL Router, or other device supplied by the ISP. Cable and power that device as instructed by the ISP.
- 1.6. After setting the new root password, the Quick Setup Wizard starts on the LAN Page. All of the settings established by the Wizard can be changed later using the regular Menu system. Type a unique hostname in the **Hostname** field that will identify this unit, e.g. Gateway-A. Leave the LAN 'Direct Connection Settings' on the default selection of 'Manual configuration'. Click on the **Next** Button to proceed.
- 1.7. Type the SnapGear LAN address into the **IP Address** field, 10.5.6.1. This is the address that all other hosts on the LAN will use as their Default Gateway. Type the network mask into the **Subnet Mask** field using '24' or the Dotted-Quad notation of '255.255.255.0'. Click on the **Next** Button to proceed.
- 1.8. Select an **Internet Port Configuration** of **Direct Connection** for Ethernet Port B. Click on the **Next** Button to proceed.
- 1.9. Select an **ISP Connection** of Manual Configuration. Click on the **Next** Button to proceed.
- 1.10. Type the SnapGear Internet (WAN) address into the **IP Address** field, 14.15.16.17. Type the network mask into the **Subnet Mask** field using '24' or the Dotted-Quad notation of '255.255.255.0'. Scenario 1 does not list Internet Gateway addresses, but be sure to enter an appropriate IP address in the **Gateway Address** field. Do the same for the **DNS Server(s)** field. Click on the **Next** Button to proceed.
- 1.11. The **Switch Configuration** selection should be left at the default setting of '4 LAN Ports' for now. Using 4 LAN Ports lets you plug up to four devices directly into the SnapGear as part of the 10.5.6.0/24 network. Click on the **Next** Button to proceed.
- 1.12. The last step in Quick Setup Wizard is the review page. It is especially important to confirm the new LAN settings. Since the LAN IP Address has been moved from the default 192.168.0.0/24 Network, communication with the PC will cease after the 'Finish' control is Clicked. In this example, all you have to do is adjust the web address in Web Browser to http://10.5.6.1. Remember to plan for any required changes to your PC's Ethernet configuration for the 10.5.6.0/24 network prior to Clicking the 'Finish' control.
- 1.13. The Quick Setup Wizard completes with a page containing links to the **Save/Restore page** and the Secure Computing SnapGear registration site.
- 1.14. Clicking the **Save/Restore page** hyperlink opens the Remote Backup/Restore page. Enter and Confirm a Backup password, then Click the **Save** control. Click the **Save** button in the **File Download** dialog and **Browse** the workstation file system to save the backup file. Use the **System** navigation menu, **Backup/Restore** Link to backup successful VPN configurations or to restore known-good configurations.

Note: Right-Click the round (?) Icon in any configuration screen and select 'Open in new window' or 'Open in new tab' to read more detail on the task being performed or any options that may be available.

Step 2. Configure IPsec General Settings

- 2.1. From the **VPN** navigation menu on the left hand side of the **SnapGear Management Console** select the **IPSec** hyperlink.
- 2.2. Check the box next to **Enable IPSec**. Leave the **IPSec MTU** field blank unless you know that Gateway B or the Internet circuit between the Gateways requires an IPSec Maximum Transmission Unit below 1500 bytes.
- 2.3. Click the **Submit** Button. The configuration window should return a prompt of
Action Successful
The configuration has been updated

Step 3. Add a New IPSec Tunnel

- 3.1. Scroll down to the controls beneath the **Tunnel List**. The **Quick Setup** Button is generally recommended for SnapGear-to-SnapGear VPN configurations. Click the **Advanced** Button.
- 3.2. The configuration window should return a new working pane called **Tunnel Settings**. Fill out the form fields so they appear as follows:
Tunnel Name: GatewayA_to_GatewayB_AES
Enable this tunnel: Checked
Local Interface: default gateway interface
Keying: Main mode (IKE)
Local address: static IP address
Remote address: static IP address
Authentication: Preshared Secret
- 3.3. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Local Endpoint Settings**.

Step 4. Configure the Local Endpoint Settings

- 4.1. Fill out the **Local Endpoint Settings** form so it appears as follows:
Initiate Tunnel Negotiation: Checked
Optional Endpoint ID: Leave this blank to use the default gateway interface IP as the Endpoint ID.
IP Payload Compression: Unchecked
Dead Peer Detection: Unchecked (The Delay and Timeout Fields will disappear.)
IPSec Offload device: Leave the Dropdown List set to **None** unless you are chaining SnapGear devices to accommodate a higher than normal VPN capacity for the devices in your inventory.
Initiate Phase 1 & 2 rekeying: Checked
- 4.2. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Remote Endpoint Settings**.

Step 5. Configure the Remote Endpoint Settings.

- 5.1. Fill out the **Remote Endpoint Settings** form so it appears as follows:

The remote party's IP address: 22.23.24.25

Optional Endpoint ID: Leave this blank to use the remote party's IP address as the Endpoint ID.

- 5.2. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Phase 1 Settings**.

Step 6. Configure the IKE Phase 1 Parameters.

- 6.1. Fill out the **Phase 1 Settings** form so it appears as follows:

Key lifetime (sec): 28800

Rekey margin (sec): 600

Rekey fuzz%: 100

Preshared secret: hr5xb84l6aa9r6

Phase 1 Proposal: AES(128bit)-SHA-Diffie Hellman Group 2 (1024 bit)

- 6.2. Click on the **Next** Button to proceed. The configuration window should return a new working pane called **Phase 2 Settings**.

Step 7. Configure the IKE Phase 2 Parameters.

- 7.1. Fill out the top of the **Phase 2 Settings** form so it appears as follows:

Local Network: 10.5.6.0/24

Remote Network: 172.23.9.0/24

- 7.2. Click the **Add** Button. The entries just completed should appear in the summary table at the top of the form.

Note: Scenario 1 uses just one Local LAN for Gateway A and one Peer LAN for Gateway B. Additional Peer Networks for custom scenarios can be configured by repeating Step 7.1 and Step 7.2.

- 7.3. Fill out the bottom of the **Phase 2 Settings** form so it appears as follows:

Key Lifetime(sec): 3600

Phase 2 Proposal: AES(128bit)-SHA

Perfect Forward Secrecy: Checked

Diffie Hellman Group: Diffie Hellman Group 2 (1024bit)

Note: Perfect Forward Secrecy (PFS) requires an exact match for the Diffie Hellman Group (DH Group) in the Phase Two Proposals. Be sure that the Gateway B vendor instructions for PFS are well understood before determining whether to use PFS.

- 7.4. Click on the **Finish** Button to proceed. The configuration window should return to the **IPSec General Settings** pane and there should be a **Connection** entry in the **Tunnel List** labeled 'GatewayA_to_GatewayB_AES'. The **Remote Party** table entry should be '22.23.24.25'. The table **Status** entry will be '**Down**' or '**Negotiating Phase 1**' unless the configuration for Gateway B has also been completed. (See Step 8. below)

- 7.5. Clicking the 'Pad & Pencil' Icon will re-open the configuration panes for Steps 2 – 7 so that corrections may be entered. Clicking the 'Trashcan' Icon will DELETE, not disable the VPN configuration.

- 7.6. To disable one of the VPN Connections in the Tunnel List, Click the corresponding 'Pad & Pencil' Icon and then Uncheck the **Enable this tunnel** box in the **Tunnel Settings** pane. Click through all of the **Next** Buttons on each pane, ending with the **Finish** Button on the last pane. The entry for that Connection should reappear without the green checkmark in the left-hand column.
- 7.7. To disable ALL IPSec VPN Connections, Uncheck the **Enable IPSec** box at the top of the **IPSec General Settings** pane and then Click the **Submit** button. The **Tunnel List** Connection configurations will remain but they will not function until **IPSec** is re-enabled.

Step 9. Confirm VPN Operations, Troubleshooting, and Log Monitoring.

- 9.1. From the **System** navigation menu on the left hand side of the **SnapGear Management Console** and select the **Diagnostics** hyperlink. Select the **Network Tests** Tab and enter the Internet IP for the Gateway B device in the **IP Address of Remote Machine** field, 22.23.24.25. Click the **Ping** Button. After approximately 15 seconds the page will refresh with the results of the ping test and the banner

Action Successful

The following results were returned:

```
PING 22.23.24.25 (22.23.24.25) 56(84) bytes of data.  
64 bytes from 22.23.24.25: icmp_seq=1 ttl=64 time=1.18 ms  
64 bytes from 22.23.24.25: icmp_seq=2 ttl=64 time=1.11 ms  
64 bytes from 22.23.24.25: icmp_seq=3 ttl=64 time=1.33 ms  
64 bytes from 22.23.24.25: icmp_seq=4 ttl=64 time=1.31 ms  
  
--- 22.23.24.25 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3028ms  
rtt min/avg/max/mdev = 1.114/1.238/1.337/0.092 ms
```

If the test results indicate 'Destination Host Unreachable' there may be a problem with the cabling, the Internet or test circuit, or the upstream routes. This test assumes that Gateway B has been configured to reply to 'icmp/echo_request' messages, at least from Gateway A.

- 9.2. Internet access or the test circuit is confirmed if Gateway B's Internet address responds to the Ping test in Step 8.1. If not, go to the **System** navigation menu on the left hand side of the **SnapGear Management Console** and select the **Diagnostics** hyperlink. Look under the **System Tab, Connections Table** for Port B. If the 'State' entry is 'checking', the connection has not been completely negotiated. Confirm all of the Internet cabling, power, and Internet Service Provider (ISP) instructions. Remember to check the cabling for the ISP circuit; which can be a Coaxial Cable, a DSL phone line and filter adapter, or some other cable type. Try power cycling the ISP device and monitoring the indicator lights on the device. Some Cable Modem providers recommend leaving their devices off for five minutes or more in order to insure new circuit negotiation.
- 9.3. If the ping test of Gateway B's Internet address is successful and the **Tunnel List** labeled 'GatewayA_to_GatewayB' has a **Status** entry of '**Running**', this indicates that the VPN Tunnel is established. Using a Client in the Gateway A LAN (10.5.6.0/24), Ping Gateway B's LAN interface address at 172.23.9.1 or an address on the Peer Network of 172.23.9.0/24. This test assumes that the Gateway B has been configured to allow 'icmp/echo_request' messages, at least from the Gateway A LAN. The SnapGear default policy is to allow all IP protocols through the VPN.
- 9.4. The **Tunnel List** labeled 'GatewayA_to_GatewayB' may have **Status** entries as follows:

Down – this indicates that the tunnel is not being negotiated. This may be due to the following reasons; IPsec is disabled, the tunnel is disabled, or the tunnel could not be loaded due to misconfiguration.

Negotiating Phase 1 indicates that IPsec is negotiating Phase 1 to establish the tunnel. Main mode packets are transmitted during this stage of the negotiation process.

Negotiating Phase 2 indicates that IPsec is negotiating Phase 2 to establish the tunnel. Quick mode packets are transmitted during this stage of the negotiation process.

Running, Renegotiating Phase 1 indicates that the tunnel has been established and the tunnel is renegotiating its Phase 1 keys.

Running, Renegotiating Phase 2 indicates that the tunnel has been established and the tunnel is renegotiating its Phase 2 keys.

Each of these status entries is also a hyperlink to details on; the VPN interface and crypto package loads, a **Connection Details** summary of the VPN Proposals for Phase 1 and Phase 2, and the **Negotiation State**. Right-Click the link and choose ‘Open in a new window’ or ‘Open in a new tab’ to view these details. These log entries can be copied and pasted for examination by Secure Computing Technical Support.

- 9.5. It is good practice to have Gateway A and Gateway B synchronized to reliable time references so that reliable logs can be gathered from both devices for the same VPN connection attempts.
- 9.6. Additional log material can be found in the **System** navigation menu, **Diagnostics** hyperlink, **System Log** Tab. Scrolling down to the bottom of the syslog report reveals a filter tool field labeled **Match this string**. Enter an identifying string for IPsec messages on the SnapGear, e.g. ‘Pluto’ and Click the **Update** Button to reduce the report to particular items of interest. Again, These log entries can be copied and pasted for examination by Secure Computing Technical Support. Use the **Remote Syslog** Tab or the **Email Delivery** Tab to configure the Syslog stream for transport off of the SnapGear device for storage or analysis.
- 9.7. Use the **System** navigation menu, **Help and Support** hyperlink, **Technical Support Report** Tab to access the **Download the Technical Support Report** hyperlink and download a complete configuration file (TSR) for examination by Secure Computing Technical Support.
- 9.8. Use the **System** navigation menu, **Diagnostics** hyperlink, **Packet Capture** Tab to access GUI controls for the ‘tcpdump’ tool.

Select the capture interface from the **Interface** Dropdown List and enter filter requirements in the **Options** field. Click the **Add** Button to store one or more Packet Capture Filters in the Index Table at the top of the page.

Activate a Capture Filter by Clicking the Checkbox in the left-hand column of the Index Table. Click the hyperlink entries in the **Download** column to open a File Download dialog. The **.pcap** files are compatible with Ethereal, Wireshark, and other Sniffer utilities. Click the Trashcan Icon to delete a Capture Filter and the associated data.

Use the Packet Display area to select a Capture Filter Index, enter any display filters in the **Options** field, and open a limited report with the **Display** Button.