



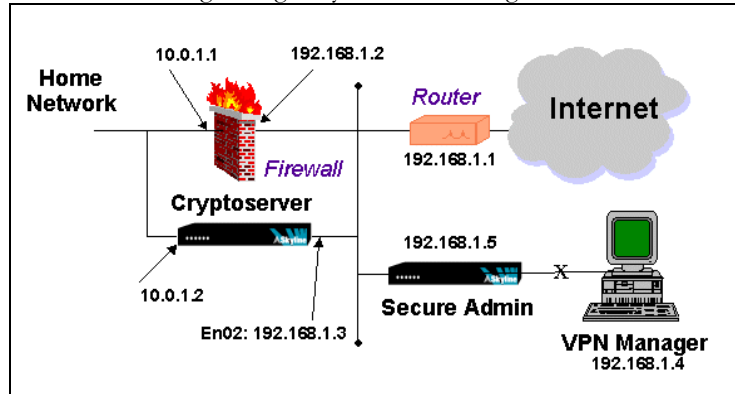
VPN Manager Quick Start Manual

Overview

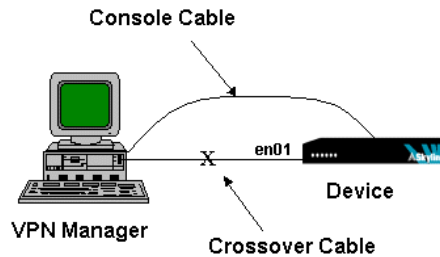
This manual provides two VPN Manager Quick Start Guides. The first focuses on Remote Access deployments. The second focuses on Site-to-Site VPN deployments.

VPN Manager Quick Start Guide for Remote Access:

1. Create a Network Map. Note that the VPN Manager usually connects to en01 of the Secure Admin device via a crossover cable. The outside port of the Secure Admin device (en02), must have IP Connectivity to the outside port (en02) of each Cryptoserver that is being managed by the VPN Manager:



2. Configure VPN Manager Platform (either a Win2000 or WinNT server):
 - a. Configure the FTP Server (Internet Information Services on Win2000 or Microsoft Internet Server on WinNT):
 - i. Allow at least 10 connections
 - ii. Uncheck "Allow only anonymous connections"
 - iii. Allow both Read and Write access to the Home Directory.
 - b. Add user ID and password. This user ID will be used by the Cryptoservers to download files from the VPN Manager. The defaults are "skyline.remote" for the username and "Skyline" for the password. These defaults can be overridden (refer to Chapter 4 of the VPN Manager Users Guide).
 - c. Install the VPN Manager from the CD.
3. Prepare Cryptoserver Devices:
 - a. Connect the Cryptoserver to VPN Manager. Connect an Ethernet crossover cable to en01 of the device. Connect a console cable from the VPN Manager COM port to the device console port:



- b. Configure HyperTerminal COM interface to communicate with the Cryptoserver. Use defaults except for:
 - i. Bits per second: 19200
 - ii. Flow Control: None
 - c. Console into the device and enter the following command:

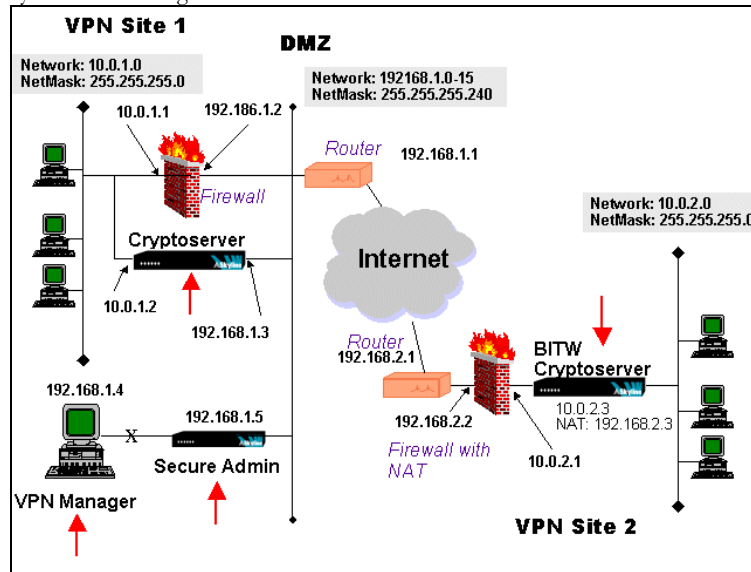

```
dpf gen keys both
```
 - d. If using a BorderGuard 4000 in a 100baseT environment with Cisco Switches enter the following commands:


```
set if en01 full
set if en01 speed 100
set if en02 full
set if en02 speed 100
reset
```
4. Initialize the Secure Administrator device:
 - a. Start the Initializer by clicking on the Initializer icon on the desktop.
 - b. Click on the Cryptoserver icon in the upper left hand corner to show the Initializer menu:

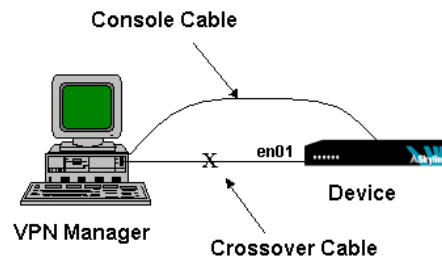
- i. Select “SA FW”.
 - ii. Select LAN and enter an unused IP address on the VPN Manager’s local segment. This IP address is a temporary address used to initialize the device. For the map above, address 192.168.1.100 is valid.
 - iii. In the Initializer dialog, fill in the appropriate IP address information. For the map shown, the inside IP address would be 192.168.1.5. The inside gateway address would be 192.168.1.1. The outside gateway should be left blank.
 - iv. Verify that the VPN Manager IP is correct.
 - v. Click on Apply.
5. Setup the VPN Manager:
 - a. Enter Default Settings: Select the Enterprise folder in the tree view and click on Properties Button. At a minimum, the following should be set:
 - i. Device Defaults: Enter a new default password.
 - ii. Client and VPN Sleeve Defaults: Enter appropriate default sleeve parameters. Be sure to select Long keys if applicable.
 - iii. Contact Information: This page is very important if using the VPN Manager to subscribe remote access clients as this information will appear on the Client GUI.
 - b. Enter Secure Admin information: Select the Secure Admin Device in the Devices folder and click on the Properties button. At a minimum, the following should be set:
 - i. Cryptoserver Definition: Enter the Connect IP.
 - ii. Cryptoserver Options: Enter the correct password.
 - iii. VPN Sleeve Options: Be sure to choose the key length that you plan to use for the management sleeves. This key length must match the Secure Admin key length when initializing all devices (refer to step 6.b.iii).
6. Initialize the Remote Access devices:
 - a. Prepare the device as outlined in Step 3 above.
 - b. From the Initializer menu, click on the Cryptoserver icon in the upper left hand corner to show the Initializer menu:
 - i. Select “VPN None”.
 - ii. Deselect “Outside Network” if the device is a one-port Remote Access device.
 - iii. Select the “Secure Admin” menu option: Verify that the Secure Admin IP is correct. Also it is very important to make sure that the key length is the same as the one set in Step 5.b.iii above.
 - iv. Select LAN and verify that it still contains a valid IP address.
 - v. On the Initializer dialog, fill in the appropriate IP address information. For the example shown, the inside IP would be 10.0.1.2. The inside gateway address would be 10.0.1.1. The outside IP would be 192.168.1.3 and the outside gateway address would be 192.168.1.1.
 - vi. Click on Apply.
7. Deploy the Initialized device.
8. Add a Remote Access Device to the VPN Manager:
 - a. Add a Home Network/Access Group to the VPN Manager by clicking on the New Home Network button:
 - i. Enter the Network Segment: This is the segment that your Remote Clients will have a virtual presence on.
 - ii. Enter a Name that will be meaningful to the remote user as this name will also be the name of the Access Group which appears on the Client GUI.
 - b. Add the Remote Access device to the Access Group:
 - i. Select the Access Group in the tree view and click on the New Cryptoserver button.
 - ii. Enter the Connect IP Address.
 - c. Upload the Secure Admin Device: From the Secure Admin device’s popup menu select Upload->Site-to-site. After a few minutes the Remote Access Cryptoserver should connect to the VPN Manager.
 - d. Subscribe Clients:
 - i. Create a Client Group by clicking on the New Client Group tool bar button.
 - ii. Create a Client by clicking on the New Client tool bar button.
 - iii. Drag and Drop the Client to the Access Group created in Step a.
 - iv. From the Client’s popup menu select Generate Subscription Diskette.
 - v. Upload the Cryptoserver: From the Cryptoserver’s popup menu select Upload->Remote Access.

VPN Manager Quick Start Guide for Site-to-Site VPNs:

1. Create a Network Map. Note that the VPN Manager usually connects to en01 of the Secure Admin device via a crossover cable. The outside port of the Secure Admin device (en02), must have IP Connectivity to the outside port (en02) of each Cryptoserver that is being managed by the VPN Manager:



2. Configure VPN Manager Platform (either a Win2000 or WinNT server):
 - a. Configure the FTP Server (Internet Information Services on Win2000 or Microsoft Internet Server on WinNT):
 - i. Allow at least 10 connections
 - ii. Uncheck "Allow only anonymous connections"
 - iii. Allow both Read and Write access to the Home Directory.
 - b. Add user ID and password. This user ID will be used by the Cryptoservers to download files from the VPN Manager. The defaults are "skyline.remote" for the username and "Skyline" for the password. These defaults can be overridden (refer to Chapter 4 of the VPN Manager Users Guide).
 - c. Install the VPN Manager from the CD.
3. Prepare Cryptoserver Devices:
 - a. Connect the Cryptoserver to VPN Manager. Connect an Ethernet crossover cable to en01 of the device. Connect a console cable from the VPN Manager COM port to the device console port:



- b. Configure HyperTerminal COM interface to communicate with the Cryptoserver. Use defaults except for:
 - vi. Bits per second: 19200
 - vii. Flow Control: None
 - c. Console into the device and enter the following command:


```
dpf gen keys both
```
 - d. If using a BorderGuard 4000 in a 100baseT environment with Cisco Switches enter the following commands:


```
set if en01 full
set if en01 speed 100
set if en02 full
set if en02 speed 100
reset
```
4. Initialize the Secure Administrator device:
 - a. Start the Initializer by clicking on the Initializer icon on the desktop.

- b. Click on the Cryptoserver icon in the upper left hand corner to show the Initializer menu:
 - i. Select "SA FW".
 - ii. Select LAN and enter an unused IP address on the VPN Manager's local segment. This IP address is a temporary address used to initialize the device. For the map above, address 192.168.1.100 is valid.
 - iii. In the Initializer dialog, fill in the appropriate IP address information. For the map shown, the inside IP address would be 192.168.1.5. The inside gateway address would be 192.168.1.1. The outside gateway should be left blank.
 - iv. Verify that the VPN Manager IP is correct.
 - v. Click on Apply.
5. Setup the VPN Manager:
 - a. Enter Default Settings: Select the Enterprise folder in the tree view and click on Properties Button. At a minimum, the following should be set:
 - i. Device Defaults: Enter a new default password.
 - ii. Client and VPN Sleeve Defaults: Enter appropriate default sleeve parameters. Be sure to select Long keys if applicable.
 - iii. Contact Information: This page is very important if using the VPN Manager to subscribe remote access clients as this information will appear on the Client GUI.
 - b. Enter Secure Admin information: Select the Secure Admin Device in the Devices folder and click on the Properties button. At a minimum, the following should be set:
 - i. Cryptoserver Definition: Enter the Connect IP.
 - ii. Cryptoserver Options: Enter the correct password.
 - iii. VPN Sleeve Options: Be sure to choose the key length that you plan to use for the management sleeves. This key length must match the Secure Admin key length when initializing all devices (refer to step 6.b.iii).
6. Initialize the Site 1 VPN device:
 - a. Prepare the device as outlined in Step 3 above.
 - b. From the Initializer menu, click on the Cryptoserver icon in the upper left hand corner to show the Initializer menu:
 - i. Select "VPN Routed",
 - ii. Select the "Secure Admin" menu option: Verify that the Secure Admin IP is correct. Also it is very important to make sure that the key length is the same as the one set in Step 5.b.iii above.
 - iii. Select LAN and verify that it still contains a valid IP address.
 - iv. On the Initializer dialog, fill in the appropriate IP address information. For the example shown, the inside IP would be 10.0.1.2. The inside gateway address would be 10.0.1.1. The outside IP would be 192.168.1.3 and the outside gateway address would be 192.168.1.1.
 - v. Click on Apply.
7. Initialize the Site 2 VPN device:
 - a. Prepare the device as outlined in Step 3 above.
 - b. From the Initializer menu, click on the Cryptoserver icon in the upper left hand corner to show the Initializer menu:
 - i. Select "VPN BITW",
 - ii. Select the "Secure Admin" menu option: Verify that the Secure Admin IP is correct. Also it is very important to make sure that the key length is the same as the one set in Step 5.b.iii above.
 - iii. Select LAN and verify that it still contains a valid IP address.
 - iv. Select NAT and check the "Enable NAT" box. Enter 192.168.2.3 as the NAT address.
 - v. On the Initializer dialog, fill in the appropriate IP address information. For the example shown, the inside IP would be 10.0.2.3. The inside gateway address would be 10.0.2.1. There is no outside IP address or outside gateway address.
 - vi. Click on Apply.
8. Deploy the Initialized devices.
9. Add Site-to-Site VPN Devices to the VPN Manager:
 - a. Add a VPN to the VPN Manager by clicking on the New VPN toolbar button.
 - b. Set up the default VPN properties.
 - c. Add the Site 1 device to the VPN:
 - i. Select the VPN in tree view and click on the New Cryptoserver button.
 - ii. Enter the Connect IP Address (192.168.1.3).
 - d. Add the Site 2 device to the VPN:
 - i. Select the VPN or the Central Office VPN device and click on the New Cryptoserver button.
 - ii. Enter the Connect IP Address (192.168.2.3).
 - e. Upload the Secure Admin device.
 - f. Enter the VPN Policy by editing the VPN Properties for each device.
 - g. Upload the Site-to-Site configuration by selecting the VPN object in the tree view and select Upload->Site-to-Site.