P2000

Security Management System

VPN/DSL Security Option

Installation Manual

P2000

Security Management System

VPN/DSL Security Option

Installation Manual

Johnson
Controls

Security Solutions
(805) 522-5555
www.johnsoncontrols.com

Acknowledgment

Cardkey P2000, BadgeMaster, and Metasys are trademarks of Johnson Controls, Inc.

All other company and product names are trademarks or registered trademarks of their respective owners.

$C\,E$

Declaration of Conformity

This product complies with the requirements of the European Council Electromagnetic Compatibility Directive 2004/108/EEC and the Low Voltage Directive 2006/95/EEC.

This equipment must not be modified for any reason and it must be installed as stated in the Manufacturer's instruction.

If this shipment (or any part thereof) is supplied as second-hand equipment, equipment for sale outside the European Economic Area or as spare parts for either a single unit or system, it is not covered by the Directives.

This product is listed under Underwriters Laboratories UL 1076 for Proprietary Burglar Alarm Units and Systems. When installed at the site the following requirements must be met to comply with this standard.

1. Transient protection devices that are installed must not be removed or defeated.

2. The computers audible alarm indicator must not be disabled.

3. All system components must be connected to a UL Listed Uninterruptible Power Supply that provides a minimum of 24 hours of AC emergency power.

4. The maximum number of Panels that may be connected to the P2000 or P2K system is 1000.

5. The P2000 or P2K shall give priority to signals in the order given below and shall annunciate subsequent signals at a rate no less than one every 10 seconds

Priority 0	Highest Priority	Hold-up or Panic Alarm
Priority 1	Second Highest	Burglar Alarm
Priority 2	Third Highest	Burglar Alarm Supervision
Priority 3	Fourth Highest	Other Supervisory Alarms
Priority 4	Fifth Highest	Guard Tour

6. The "Pop-up" feature for input points must be enabled.

7. At the host computer (Central Station), alarms must not be filtered away from the host using the feature "Message Filtering".

8. Alarms must not be forwarded away from the host computer (Central Station) using the feature "Message Forwarding".

9. The "Panel Poll Interval" must not exceed 90 seconds.

10. The "Host Poll Delay" must not exceed 200 seconds.

11. P2000 or P2K server must use transient suppression devices on the LAN interfaces at the computers. The table below specifies the devices that must be used for the various types of LAN interfaces.

LAN Interface	Manufacturer of Device	Device Part Number
10Base-2	Black Box	SP350A-R2 (In-line connector)
10Base-2	Black Box	SP501A ("T" connector)
10Base-5 (AUI)	Black Box	SP362
10/100Base-T	Black Box	SP512A-R3

12. Systems requiring the use of a network hub, router, and/or serial port server shall have that equipment installed in a temperature controlled environment. The temperature controlled environment must be maintained between 13 - 35°C (55 - 95°F) by the HVAC system. Twenty-four hour standby power shall be provided for the HVAC system.

13. The installer shall incorporate a supply line transient suppression device complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum rating of 330 V. Supply line transient suppression device is to be used with the power supply to the network hub, router, serial port server, serial-to-ethernet converter and RS232-to-RS485 converter.

14. The Hewlett Packard ML370 or ML350 serving as the P2000 or P2K host computer shall be installed in a temperature controlled environment. The temperature controlled environment must be maintained between 13 - 35°C (55 - 95°F) by the HVAC system. Twenty four hour standby power shall be provided for the HVAC system.

15. The 240 Vac configurations have not been tested by Underwriters Laboratories except for the ML370 G3 and the ML350 G5.

16. The workstation defined as "Server" must have the alarm monitor parameter set to "always active".

17. For P2000 or P2K software version 2.5 or later, when configuring "Service Startup" parameters the following services shall not be disabled.

> P2000 RTL Route Service
> P2000 CK720 Download Service
> P2000 CK720 Priority Service v1.0
> P2000 CK720 Priority Service v2.1
> P2000 CK720 Upload Service
> P2000 Periodic Service
> P2000 S321 SIO Handler Service
> P2000 S321-IP Interface Service
> P2000 SIO Handler Service
> P2000 Smart Download Service

18. For Line Security over the Internet, between the P2000 or P2K server and the controllers CK705, CK720, CK721, CK721-A, and S321-IP the following equipment shall be used.

> NetScreen, Model NS-5XT-X0X (where X is any number 0 to 9), 4-Port VPN router

The P2000 or P2K server and router shall be configured to use an encryption method including an Authentication Header (AH) and an algorithm capable of Triple-DES (3DES) or better that is NIST certified.

19. For Line Security over the Internet, between the P2000 or P2K server and the controllers D620, D6AP, and S320, the following equipment shall be used.

> NetScreen, Model NS-5XT-X0X (where X is any number 0 to 9), 4-Port VPN router and
> Digi International, Model EtherLite2 serial port server

The P2000 or P2K server and router shall be configured to use an encryption method including an Authentication Header (AH) and an algorithm capable of Triple-DES (3DES) or better that is NIST certified.

20. For Line Security over the Internet, between the P2000 or P2K server and the controller S321-DIN, the following equipment shall be used.

> NetScreen, Model NS-5XT-X0X (where X is any number 0 to 9), 4-Port VPN router and
> Digi International, Model Digi One SP serial-to-ethernet converter or
> B&B Electronics Mfg Co., Model 485OT9L RS232-to-RS485 converter

The P2000 or P2K server and router shall be configured to use an encryption method including an Authentication Header (AH) and an algorithm capable of Triple-DES (3DES) or better that is NIST certified.

21. The router and serial port server shall be installed within the same room as the controllers S320, D620 and/or D6AP and within 20 feet of the controller when employed for encrypted line security.

22. P2000 or P2K systems use the Digi International Model Digi One SP converter or B&B Electronics Model 485OT9L converter to communicate to S321-DIN controllers.

23. The B&B Electronics Model 485OT9L converter shall be installed within the same room as the P2000 or P2K server and within 20 feet of the server under all conditions of use.

24. The Digi International Model Digi One SP may be mounted at the central supervising station or the protected premise. When used at the central supervising station, a Cylix Model TSP-4B-E transient suppression device shall be used on the RS485 communication line. When used at the protected premise, a Blackbox Model RS512A-R3 transient suppression device shall be used on the LAN communication line.

25. A spare router, serial port server, serial-to-ethernet converter and RS232-to-RS485 converter shall be available and put in to service within 6 minutes when they are employed for encrypted line security with the controllers CK705, CK720, CK721, CK721-A, S320, S321-DIN, S321-IP, D620 and/or D6AP.

26. P2000 workstations, network hubs, routers, serial port servers, serial-to-ethernet converters, and RS232-to-RS485 converters must use signal line transient suppression devices complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50V.

27. Alarm signals received at a remote P2000 or P2K server via the Remote Message Services from a different P2000 or P2K server are supplementary.

28. Alarm signals received at a P2000 workstation are supplementary.

29. Alarm signals received at a personal computer or personal digital assistant through the Web Access feature are supplementary.

30. P2000 or P2K systems use the PC232-S4-1 Protocol Converter to communicate to D620, D6AP and/or S320 controllers; a controller must be connected to the port defined as Loop 1 at the P2000 or P2K for Protocol Converter's tamper switch to report as an alarm.

31. The communication medium between the protected property and communications service provider shall be for the exclusive use of the protected property and is not to be shared with other communications service provider subscriber.

32. The following features have not been investigated by Underwriters Laboratories:

    BACNet interface
    Dial-Up
    Fire server
    Intrusion server
    Isonas interface

33. The following products have not been investigated by Underwriters Laboratories and shall not be used in a listed system:

    P900 product line
    OSI product line
    Aritech® intrusion panel
    Notifier fire alarm panel

34. The P2000 or P2K and HID Edge access control unit may be used for access control monitoring purposes only.

35. A Panel Down alarm message received at the central station may be an indication of a compromise attempt.

36. For the S321-IP, the "Heartbeat Transmit Interval" must not exceed 90 seconds and the "Host Reception Timeout" must not exceed 200 seconds.

TABLE OF CONTENTS

INTRODUCTION

This document describes how to provide end-to-end security between the P2000 server and CK721-A, CK721, CK720, S321, or S320 controllers or P2000 workstations using a Virtual Private Network (VPN).

A VPN provides a means of securing communications between a P2000 server and one or more remote CK721-A/CK721/CK720/S321/S320 controllers and/or P2000 workstations across an untrusted public Wide Area Network (WAN).

A VPN connection can link two Local Area Networks (LANs). The traffic that flows between these points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN. To secure communication while passing through the WAN, the two participants create an IP Security (IPSec) tunnel.

CHAPTER SUMMARIES

- *Chapter 1: Introduction* describes the purpose of this document and the manual conventions.
- *Chapter 2: Configuration* contains information on IP addresses and VPN configuration.
- *Appendix A: Glossary* explains some of the terms used in this manual.

MANUAL CONVENTIONS

The following items are used throughout this manual to indicate special circumstances, exceptions, important points regarding the equipment or personal safety, or to emphasize a particular point.

> **NOTE**
> *Notes indicate important points or exceptions to the information provided in the main text.*

Cautions remind you that certain actions, if not performed exactly as stated, can cause damage to equipment, security problems, or cause the system to operate incorrectly due to errors in system setup or programming.

CAUTION

Warnings indicate that the possibility of personal injury exists if an action or actions are not performed exactly as stated.

WARNING

CONFIGURATION

IPSEC PARAMETERS

An IPSec tunnel consists of a pair of unidirectional Security Associations (SAs)—one at each end of the tunnel—that specify the security parameter index (SPI), destination IP address, and security protocol (Authentication Header or Encapsulating Security Payload) employed.

Table 2-1: IPSEC Parameters

Mode	Tunnel
Protocol	Encapsulating Security Payload (ESP), Authentication Protocol (AH)
Authentication	SH1 Secure Hash Algorithm-1 (SHA-1)
ESP Encryption	Triple DES (3DES) 168-bit Key
Key Management	AutoKey IKE with a preshared key
Diffie-Hellman Exchange	Group 2 1024-bit modulus
Perfect Forward Secrecy (PFS)	Enabled
Phase 1	3DES Main Mode (six message exchange) Group 2: Preshared Key
Phase 2	Quick Mode ESP PFS

P2000 Server IP Address

IP Address: 200.0.0.1 (static IP address)

Subnet Mask: 255.255.255.0

VPN Router WAN IP Address

IP Address: 201.0.0.2 (static IP address)

Subnet Mask: 255.255.255.0

VPN Router LAN IP Address

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

HARDWARE INSTALLATION AND CONFIGURATION

The hardware listed below is *not* provided in the P2000 hardware package. In order to implement the VPN/DSL Security Option, you must purchase the necessary equipment from your local computer supplier or by contacting the manufacturer directly.

The VPN/DSL Security Option can be configured with the Linksys® and/or NetScreen® routers listed below. Linksys routers are less expensive, but are not National Institute of Standards and Technology (NIST) certified or Underwriters Laboratories (UL®) compliant. Select the routers according to your site requirements.

Table 2-2: Required Hardware

Make/Model	Description
Combination of two of the following (see router combination information below): NetScreen-5XT (NIST Certified) Linksys BEFVP41 Linksys BEFSX41	VPN Routers with 4-Port 10/100 Switch

You must have one of the following router combinations:

- Two (2) NetScreen-5XT routers

- One (1) Linksys BEFSX41 (front end) router and one (1) Linksys BEFVP41 (back end) router

- One (1) NetScreen-5XT (front end) router and one (1) Linksys BEFVP41 (back end) router

Contact Information: NetScreen www.juniper.net
Linksys www.linksys.com

Figure 2-1: Router Hardware Configuration

P2000 Server to Back End Router Connection

To connect the P2000 Server to the back end router, connect a network cable from one of the Router's Trusted (or available LAN) ports to the P2000 Server.
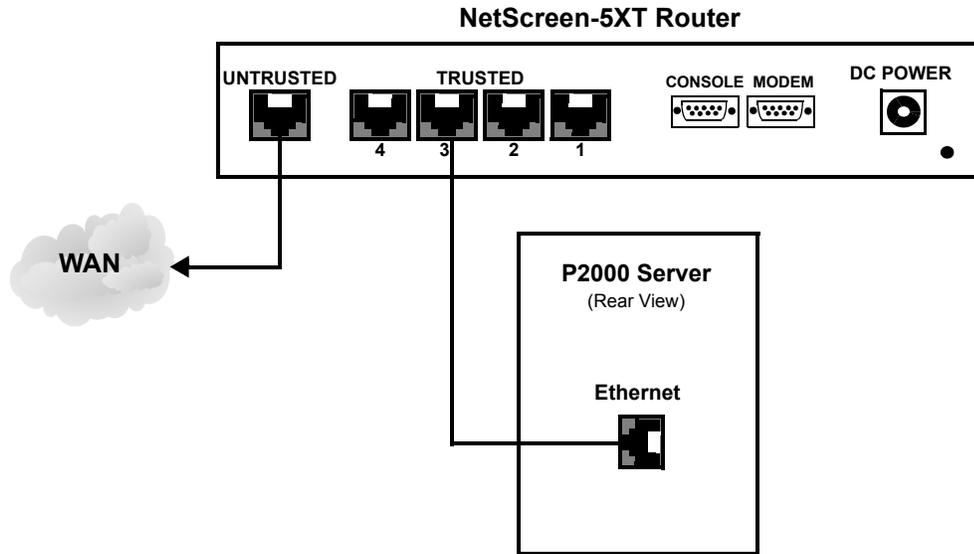

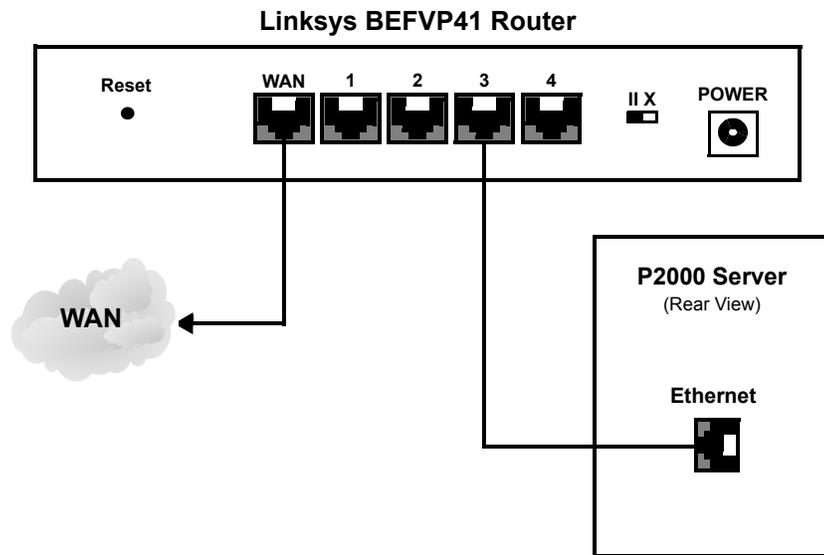*Figure 2-2: P2000 Server to NetScreen-5XT Router Connection*

Figure 2-3: P2000 Server to Linksys BEFVP41 Router Connection

NetScreen-5XT Router Installation and Configuration

This section describes how to install and configure the NetScreen-5XT router.

NetScreen-5XT Installation

The NetScreen-5XT router may be used as the front end router, back end router, or both.

➤ **To install the NetScreen-5XT router:**

1. Connect the power adapter to the rear panel of the NetScreen-5XT.

   The NetScreen-5XT device runs a 100-240 VAC +/- 10% and 12 watts. When properly connected to an AC power source, the power LED on the faceplate illuminates solid green. When power fails, the power LED turns off.

2. Connect a network cable from a laptop or PC to one of the NetScreen-5XT's available **Trusted** ports.

   This connection will be used to configure the NetScreen's settings.

3. **Back End Installation:** Connect a network cable from the P2000 Server to a **Trusted** port of the NetScreen-5XT router. See Figure 2-4.
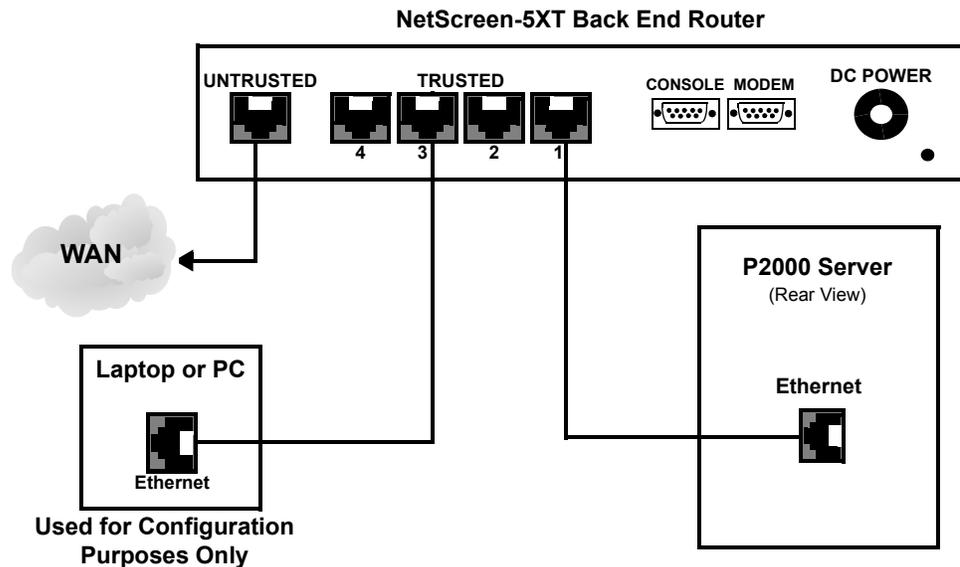

Figure 2-4: NetScreen-5XT Back End Installation

4. **Front End Installation:** Connect a network cable from the NetScreen-5XT's **Untrusted** port to the WAN. See Figure 2-5.

Connect a network cable from an available **Trusted** port on the NetScreen-5XT to the Controller or Workstation.
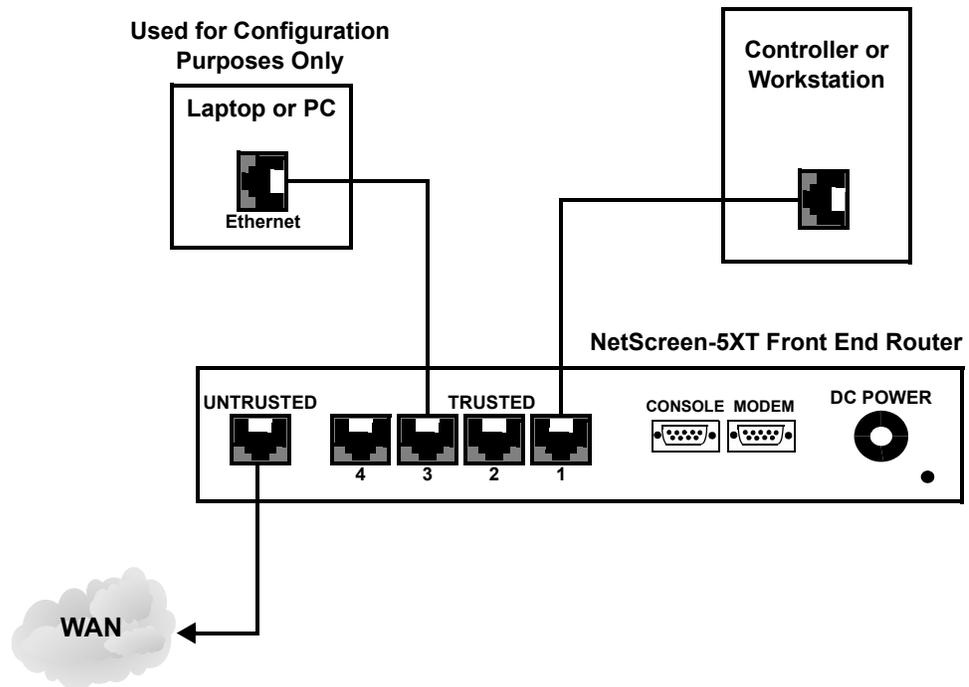

Figure 2-5: NetScreen-5XT Front End Installation

NetScreen-5XT Configuration

This section provides instructions for configuring the NetScreen-5XT's parameters using the WebUI.

➤ **To access the NetScreen using the WebUI:**

Follow these steps to access the NetScreen-5XT device with the WebUI management application.

1. Connect a local PC or laptop to one of the **Trusted** interfaces on the router.

2. Change the IP address of the PC to `192.168.1.xxx` (where xxx can be between 2 and 254) and change the subnet mask to `255.255.255.0`.
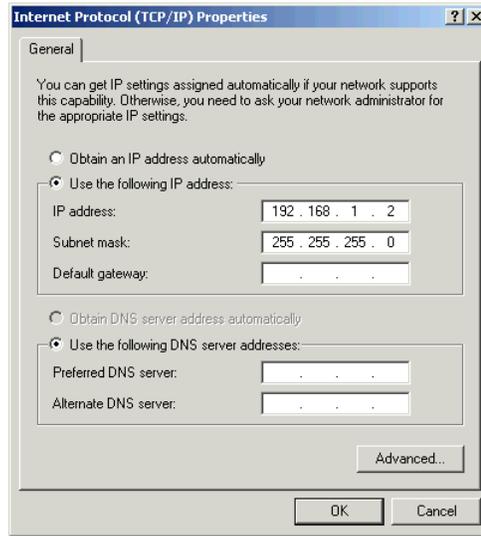
3. Open your browser and enter the NetScreen's default LAN IP address of `192.168.1.1` in the **Address** bar.

   Example: `http://192.168.1.1`

   The Enter Network Password dialog box appears.

4. Enter `netscreen` in the **User Name** and **Password** fields. Use lowercase letters only. The User Name and Password fields are both case sensitive.

5. Click **OK**.

   The Initial Configuration Wizard appears.

➤ **To configure the NetScreen with the Initial Configuration Wizard:**

1. Select **NAT Mode** and click **Next**.

2. Enter `master` into the **Password** and **Confirm Password** fields; click **Next**.

3. Select **Static IP**, enter the following, and click **Next**:

    Untrusted Zone Interface IP: `200.0.0.2`
    Netmask: `255.255.255.0`
    Gateway: `200.0.0.1`

4. Enter the following and click **Next**.

    <u>Front End Router</u>:

    Trust Zone Interface IP: `192.168.1.1`
    Netmask: `255.255.255.0`

Back End Router:

Trust Zone Interface IP: 200.0.0.3
Netmask: 255.255.255.0

5. Click **Next**.

6. Click **Next**.

7. Select **No** to DHCP and click **Next**.

8. Review and confirm the settings (Trust Interface in NAT mode):

Admin Login Name: netscreen
Password: ********
Trust Interface IP: 192.168.1.1 (Front End Router) or
                           200.0.0.3 (Back End Router)
Trust Interface Netmask: 255.255.255.0
Untrust Interface: 200.0.0.2
Management Service: Telnet enabled
Management Service: Web enabled
Management Service: Ping enabled

9. Close your browser instance, open a new instance, enter `http://192.168.1.1` and press **<Enter>** on your keyboard. The Enter Network Password dialog box appears.

10. Enter `netscreen` in the **User Name** field and `master` in the **Password** field. Click **OK**. The NetScreen Administration Tools window appears.

11. Continue with the following configuration instructions.

➤ **To configure the date and time:**

1. On the NetScreen Administration Tools window, select **Configuration>Date/Time** in the left-hand frame.

2. Configure the date and time accordingly. Refer to the NetScreen documentation for details.

3. Click **Apply**.
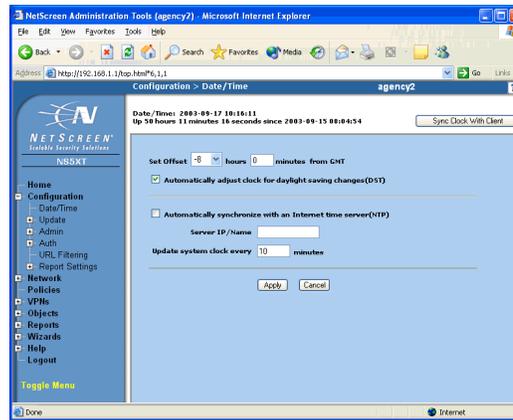
➤ **To verify the network interface settings:**

1. Select **Network>Interfaces** in the left-hand frame.

2. Verify the displayed settings.

3. If the settings require changes, click **Edit** in the Configure column and edit the settings as necessary.
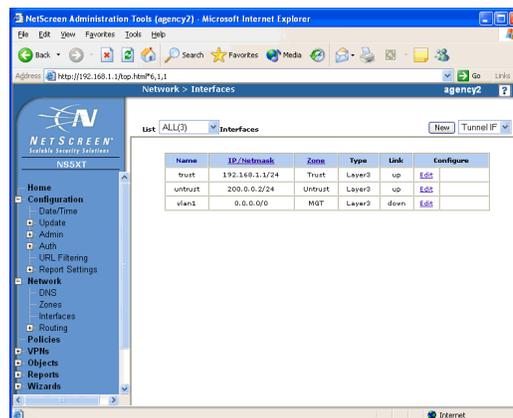
➤ **To verify the routing table settings:**

1. Select **Network>Routing>Routing Table** in the left-hand frame.

2. Verify the displayed settings.
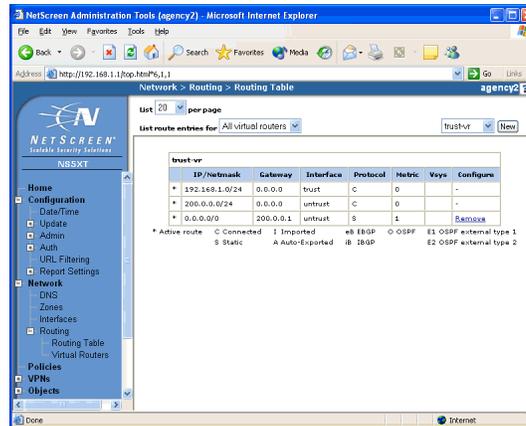
➤ **To configure the VPN settings with the VPN Wizard:**

1. Select **Wizards>VPN** in the left-hand frame to launch the VPN Wizard.

2. Select **LAN-to-LAN** and click **Next**.

3. Ensure **Local Static IP <-> Remote Static IP** is selected and click **Next**.

4. Enter `200.0.0.xxx` (where xxx can be between 2 and 254) in the **Remote Gateway IP Address** field and click **Next**.

5. Select **Standard (128/168-bit encryption strength)**, enter `master` in the **Preshared Secret** field, and click **Next**.

6. Enter the following *remote* IP address into the **IP** field according to the router you are configuring.

    Front End Router: `200.0.0.0`

    Back End Router: `192.168.1.0`

7. Change the **Netmask** to `255.255.255.0` and click **Next**.

8. Enter the following *local* IP address into the **IP** field according to the router you are configuring.

    Front End Router: `192.168.1.0`

    Back End Router: `200.0.0.0`

9. Change the **Netmask** to `255.255.255.0` and click **Next**.

10. Review the VPN tunnel settings and click **Next** to continue.

11. Click **Finish** to complete the configuration.

Resetting the NetScreen-5XT Router

If necessary, the NetScreen-5XT router can be reset to its default settings in one of two ways:

- Using Command Line Interface (CLI) Commands

- Pressing the Asset Recovery Button

For detailed information on resetting the NetScreen-5XT router to its default settings, refer to the manufacturer's documentation.

Linksys BEFVP41 Router Installation and Configuration

This section describes how to install and configure the Linksys BEFVP41 router.

Linksys BEFVP41 Installation

The Linksys BEFVP41 router may only be used as the back end router. All connections to the Linksys BEFVP41 router are made to the device's rear panel.

➤ **To install the BEFVP41 router:**

1. Connect the power adapter to the rear panel of the Linksys BEFVP41.

2. Connect a network cable from a laptop or PC to one of the Linksys BEFVP41's available Ports 1-4. This connection will be used to configure the router's settings.

3. Connect a network cable from the P2000 Server to one of the available Ports 1-4 of the router. See Figure 2-6.

Linksys BEFVP41 Back End Router
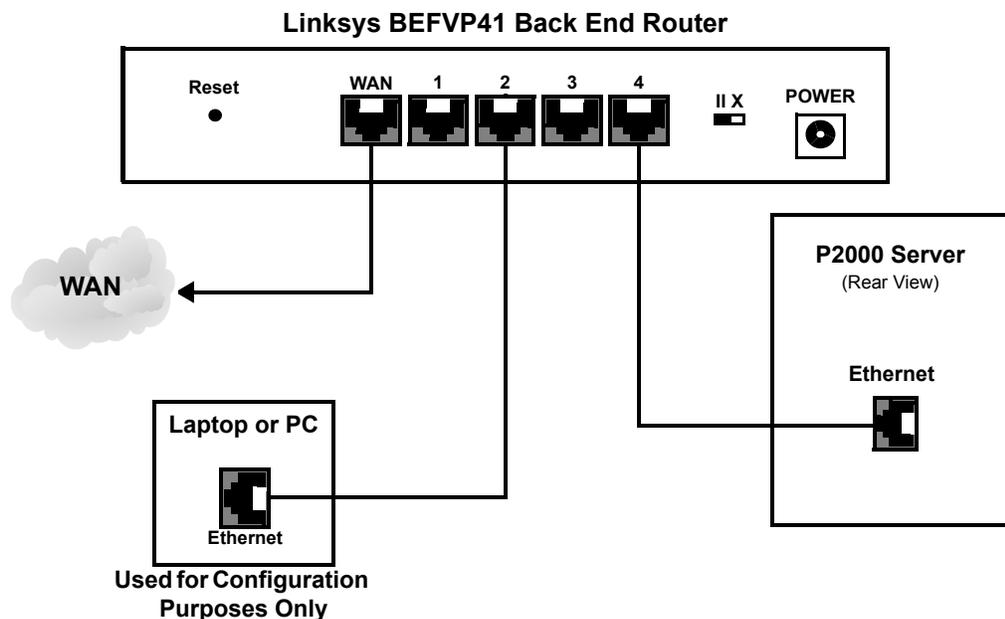
Figure 2-6: Linksys BEFVP41 Back End Router Installation

Linksys BEFVP41 Configuration

This section describes how to configure the Linksys BEFVP41 router.

➤ **To access the Linksys device:**

1. Change the IP address of your PC or laptop to `192.168.1.xxx` (where xxx can be between 2 and 254) and the subnet mask to `255.255.255.0`.

2. Open your web browser and enter `192.168.1.1` in the **Address** bar; press **<Enter>**.

   Example: `http://192.168.1.1`

   The Enter Network Password dialog box appears.

3. Enter `admin` in the **Password** field and leave the **User Name** field blank. Click **OK**.

4. On the Linksys Setup window, click the **VPN** tab.

➤ **On the VPN tab:**

1. Select the **Enable** radio button next to This Tunnel.

2. Enter a **Tunnel Name**. This name should be unique for this particular tunnel.

3. Verify that **Subnet** is the option selected from the **Local Secure Group** field.

4. Enter `200.0.0.0 as` the **IP Address**.

5. Select **Subnet** from the **Remote Secure Group** field.

6. Enter as the **IP ADDress Subnet ID** in the IP field. This is the IP Address of the remote endpoint on the other side of the tunnel (for example, `192.168.1.0`).

7. Select **IP Address** from the **Remote Security Gateway** field and enter `201.0.0.2` as the IP address.

8. Select **3DES** for Encryption and **SHA** for Authentication.

9. Select the **PFS (Perfect Forward Secrecy)** check box and verify that `master` is entered in the **Pre-shared Key** field.

10. Click the **Connect** button to establish a connection.

11. Verify that the **Status** indicates that the Router is **Connected**.

Linksys BEFSX41 Router Installation and Configuration

This section describes how to install and configure the Linksys BEFSX41 router. This router may only be used as the front end router.

Linksys BEFSX41 Installation

All connections to the Linksys BEFSX41 router are made to the device's rear panel.

➤ **To install the BEFSX41 router:**

1. Connect the power adapter to the rear panel of the Linksys BEFSX41.

2. Connect a network cable from a laptop or PC to one of the Linksys BEFSX41's available Ports 1-4. This connection will be used to configure the router's settings.

3. Connect a network cable from one of the Linksys BEFSX41's available Ports 1-4 to the Controller or Workstation.

4. Connect a network cable from the Linksys BEFSX41's **WAN** port to the WAN. See Figure 2-7.
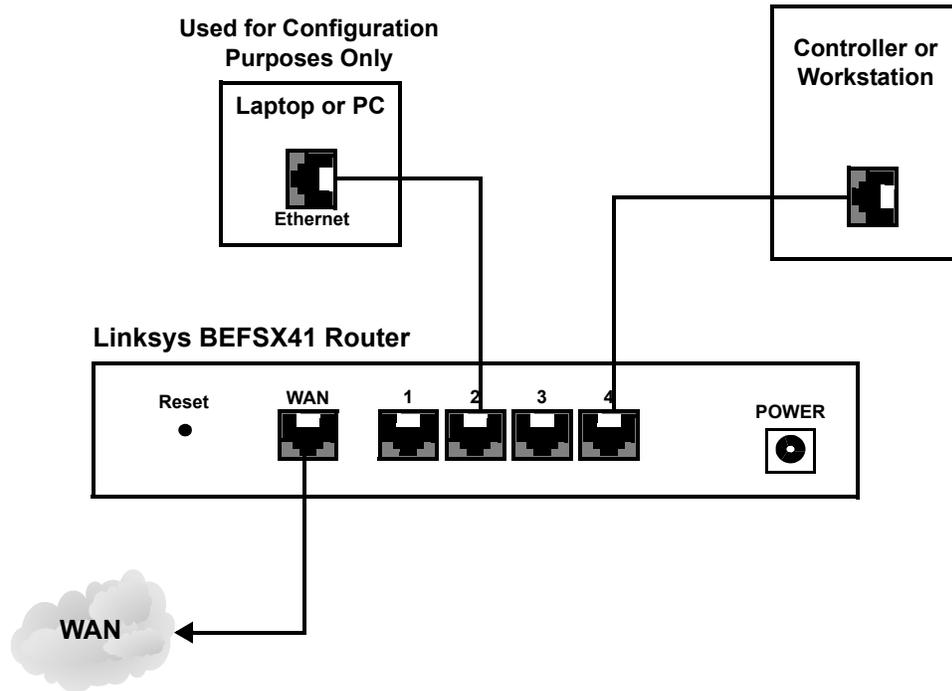
Figure 2-7: Linksys BEFSX41 Front End Router Installation

Linksys BEFSX41 Configuration

This section describes how to configure the Linksys BEFSX41 router.
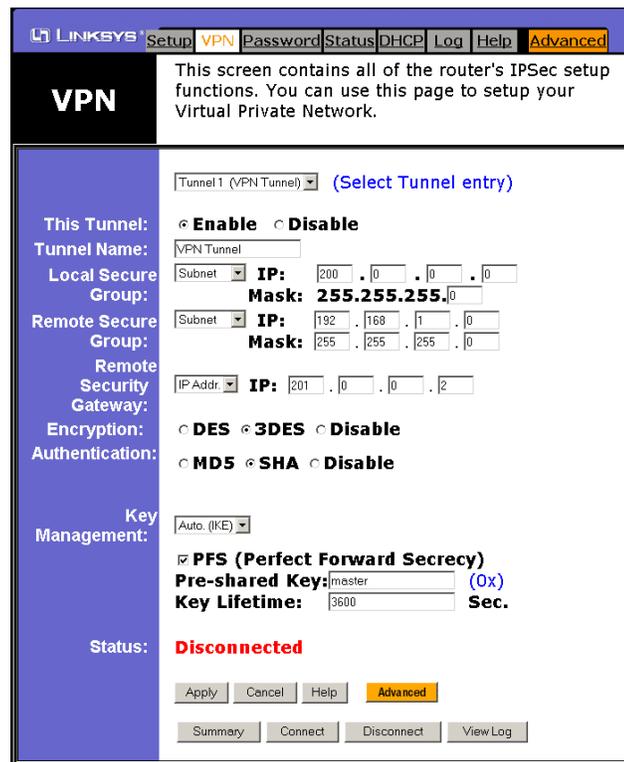
➤ **To access the Linksys device:**

1. Change the IP address of your PC or laptop to `192.168.1.xxx` (where xxx can be between 2 and 254) and the subnet mask to `255.255.255.0`.

2. Open your web browser and enter `192.168.1.1` in the **Address** bar; press **<Enter>**.

   Example: `http://192.168.1.1`

   The Enter Network Password dialog box appears.

3. Enter `admin` in the **Password** field and leave the **User Name** field blank. Click **OK**.

4. On the Linksys Setup window, click the **VPN** tab.

➤ **On the VPN tab:**

1. Select the **Enable** radio button next to This Tunnel.

2. Enter a **Tunnel Name**. This name should be unique for this particular tunnel.

3. Verify that **Subnet** is the option selected from the **Local Secure Group** field. Verify also that the **IP Address** is `192.168.1.0`

4. Select **Subnet** from the **Remote Secure Group** field.

5. Enter the **IP Address Subnet ID** in the IP field. This would be the IP Address of the remote endpoint on the other side of the tunnel (for example, `200.0.0.0`).

6. Select **IP Address** from the **Remote Security Gateway** field and enter `201.0.0.1` as the IP address.

7. Select **3DES** for Encryption and **SHA** for Authentication.

8. Select the **PFS (Perfect Forward Secrecy)** check box and verify that `master` is entered in the **Pre-shared Key** field.

9. Click the **Connect** button to establish a connection.

10. Verify that the **Status** indicates that the Router is **Connected**.

Resetting the Linksys Router

The Reset button on the Linksys router enables you to restore the router's factory defaults and clear all of its settings, including any IP addresses you entered.

The Reset button can be used in one of two ways:

- If the Linksys router is having connection problems, press the Reset button for a moment with a bent paper clip or a pencil tip. This clears up any jammed connections and is similar to pressing the Reset button to reboot your PC.

- If you are experiencing extreme problems with the Linksys router and have tried all other troubleshooting measures, press the Reset button and hold it down until the red Diag LED on the front panel turns on and off completely.

Installing the Digi EtherLite Device (S320 Connection Only)

Installation of the Digi EtherLite is required only if connecting to an S320 controller. The Digi EtherLite is a shared serial device that enables serial ports to share a single IP address. The basic requirements to share the serial device are:

- The Digi EtherLite device must be physically connected to the Ethernet and accessible by both nodes.

- The same serial port number must be configured on both nodes.

➤ **To install the Digi EtherLite device:**

1. Connect the Digi EtherLite to the network using 10Base-T cable to one of the available, Trusted LAN Ports on the front end VPN router.

2. Apply power to the Digi Etherlite device.
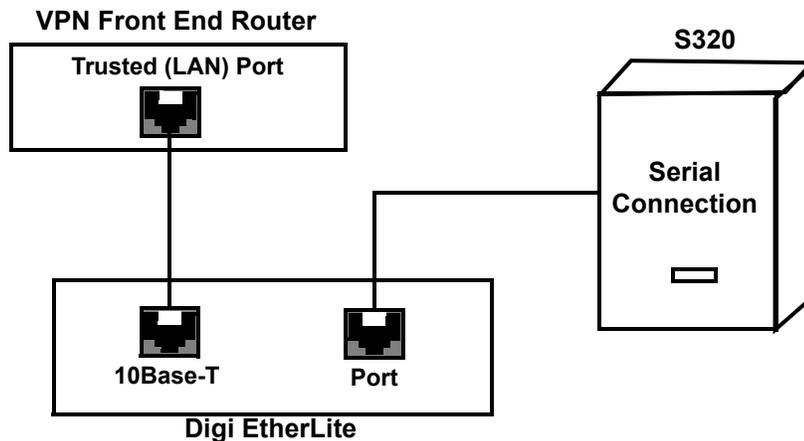
Figure 2-8: Digi EtherLite Device Connections

NOTE

To configure the Digi Etherlite and install the driver, refer to the manufacturer's instructions.

Installing the Digi One® SP (S321 Connection Only)

Installation of the Digi One SP is required only if connecting to an S321 controller. The Digi One SP device enables an S321 controller to connect to the router via the controller's serial port.

➤ **To install the Digi One SP converter:**

1. Change the DIP switch settings on the bottom of the Digi One SP converter according to Figure 2-9 and Table 2-3.

Digi One SP Converter
(Back View)
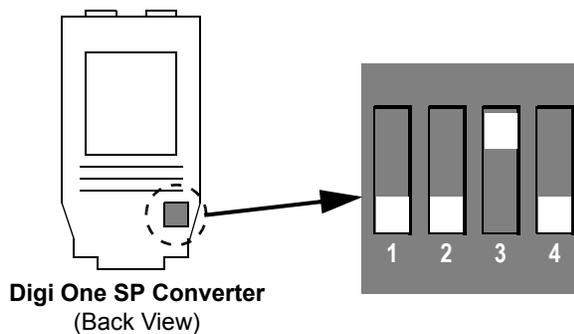
Figure 2-9: Digi One SP Converter DIP Switch Settings

Table 2-3: Digi One SP Converter DIP Switch Positions

DIP Switch	Position
1	Down/OFF
2	Down/OFF
3	Up/ON
4	Down/OFF

2. Using Belden® 9773 (18 AWG, shielded, 3 twisted pair) or equivalent, wire the pins from the S321 serial port to a DB-9F connector according and Figure 2-10 and Table 2-4.
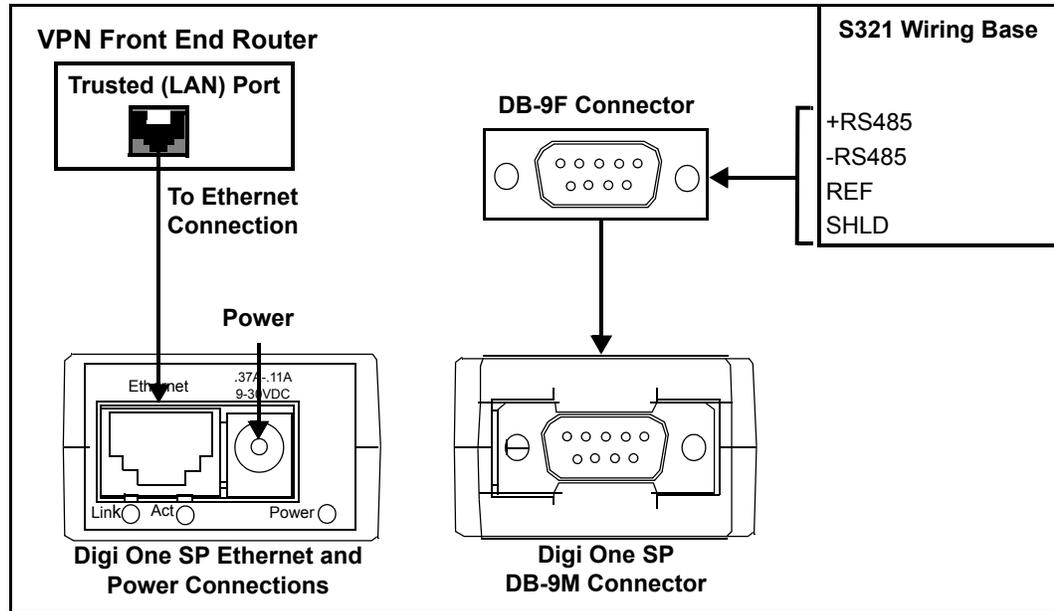
Figure 2-10: Digi One SP Connections

Table 2-4: Digi One SP DB-9F Connections

S321 Wiring Base	DB-9F Connector
+RS485	PIN 2
	PIN 3
-RS485	PIN 6
	PIN 9
REF	PIN 5

3. Connect the DB-9F connector to the Digi One SP's DB-9M connector.

4. Run an Ethernet cable from the Digi One SP to one of the available, Trusted LAN Ports on the front end VPN router.

5. Connect the power cable to the Digi One SP and run to an appropriate 110/240 VAC power source.

NOTE

To install the driver for the Digi One SP and configure the device, download the driver and configure the software according to the screen captures located at:

ftp://cardkey:cardkey2000@ftp2.johnsoncontrols.com/cardkey-out/S321/ DigiOneSP%20(Working%20Driver)/

*Do **not** install the driver provided with the Digi One SP or on their web site. Use only the driver provided on the Johnson Controls File Transfer Protocol (FTP) site.*

GLOSSARY

Authentication – Ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as DES or 3DES, or on public-key systems using digital signatures.

Cryptography – The processes, art, and science of keeping messages and data secure. Cryptography is used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation.

Data Encryption Standard (DES) – A 40- and 56-bit encryption algorithm that was developed by the National Institute of Standards and Technology (NIST). DES is a block encryption method originally developed by IBM. It has since been certified by the U.S. government for transmission of any data that is not classified top secret. DES uses an algorithm for private-key encryption. The key consists of 64 bits of data, which are transformed and combined with the first 64 bits of the message to be sent. To apply the encryption, the message is broken up into 64-bit blocks so that each can be combined with the key using a complex 16-step process. Although DES is fairly weak, with only one iteration, repeating it using slightly different keys can provide excellent security.

Diffie-Hellman – An exchange that allows the participants to produce a shared secret value. The strength of the technique is that it allows the participants to create the secret value over an unsecured medium without passing the secret value through the wire. There are five Diffie-Hellman (DH) groups.

The size of the prime modulus used in each group's calculation differs as follows:

- DH Group 1: 768-bit modulus3
- DH Group 2: 1024-bit modulus
- DH Group 5: 1536-bit modulus

The larger the modulus, the more secure the generated key is considered to be; however, the larger the modulus, the longer the key-generation process takes. Because the modulus for each DH group is a different size, the participants must agree to use the same group.

Encryption – The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when the data is stored on a transportable magnetic medium. A key is required to decode the information. To decipher the message, the receiver of the encrypted data must have the proper decryption key.

In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. DES (Data Encryption Standard) and 3DES (Triple DES) are two of the most popular public-key encryption schemes.

ESP/AH – The IP level security protocols, AH and ESP, were originally proposed by the Network Working Group focused on IP security mechanisms, IPSec. The term IPSec is used loosely here to refer to packets, keys, and routes that are associated with these protocols. The IP Authentication Header (AH) protocol provides authentication.

The Encapsulating Security Protocol (ESP) provides both authentication and encryption.

ESP – The Encapsulating Security Payload (ESP) protocol provides a means to ensure privacy (encryption), and source authentication and content integrity (authentication). ESP in tunnel mode encapsulates the entire IP packet (header and payload), and then appends a new IP header to the now encrypted packet. This new IP header contains the destination address needed to route the protected data through the network.

With ESP, you can encrypt and authenticate, encrypt only, or authenticate only. For encryption, you can choose either of the following encryption algorithms:

Data Encryption Standard (DES) – A cryptographic block algorithm with a 56-bit key.

Triple DES (3DES) – A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides a significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

Advanced Encryption Standard (AES) – An emerging encryption standard which, when adopted by Internet infrastructures worldwide, will offer greater interoperability with other network security devices. This version of AES uses a 128-bit key.

For authentication, you can use either MD5 or SHA-1 algorithms.

Filter List – A list of IP addresses permitted to send packets to the current routing domain.

Firewall – A security system, usually a combination of hardware and software, intended to protect a network against external threats coming from another network, including the Internet. Firewalls prevent an organization's networked computers from communicating directly with computers that are external to the network, and vice versa. Instead, all incoming and outgoing communication is routed through a proxy server outside the organization's network. Firewalls also audit network activity, recording the volume of traffic and information about unauthorized attempts to gain access.

Gateway – The router that resides at the point of entry to the current routing domain, often called the default gateway.

Internet Key Exchange (IKE) – The method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

IP Security (IPSec) – Security standard produced by the Internet Engineering Task Force (IETF). It is a protocol suite that provides everything you need for secure communications— authentication, integrity, and confidentiality— and makes key exchange practical even in larger networks. See also *DES-CBC,* and *ESP/AH*.

ISAKMP – The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols to provide a complete solution to Internet key management.

Kerberos V5 – An Internet standard security protocol for handling authentication of user or system identity. With Kerberos V5, passwords that are sent across network lines are encrypted, not sent as plaintext. Kerberos V5 also includes other security features.

Key Management – The only reasonable way to protect the integrity and privacy of information is to rely upon the use of secret information in the form of private keys for signing and/or encryption. The management and handling of these pieces of secret information is generally referred to as "key management." This includes the activities of selection, exchange, storage, certification, expiration, revocation, changing, and transmission of keys. Most of the work in managing information security systems lies in the key management.

MD5 – Message Digest (version) 5, an algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used, like a "fingerprint" of the input, to verify authenticity.

Netmask – A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refers to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refers to a single host.

Network Address Translation (NAT) – A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don't have to get a registered IP address for every machine in your network. packet A unit of information transmitted as a whole from one device to another on a network. In packet-switching networks, a packet is defined more specifically as a transmission unit of fixed maximum size that consists of binary digits representing data; a header containing an identification number, source, and destination addresses; and sometimes error-control data.

Packet Internet Groper (ping) – A simple utility that tests if a network connection is complete, from the server to the workstation, by sending a message to the remote computer. If the remote computer receives the message, it responds with a reply message. The reply consists of the remote workstation's IP address, the number of bytes in the message, how long it took to reply—given in milliseconds (ms)—and the length of Time to Live (TTL) in seconds. Ping works at the IP level and will often respond even when higher-level TCP-based services cannot.

Perfect Forward Secrecy (PFS) – A method for deriving Phase 2 keys independent from and unrelated to the preceding keys. Alternatively, the Phase 1 proposal creates the key (the SKEYID_d key) from which all Phase 2 keys are derived. The SKEYID_d key can generate Phase 2 keys with a minimum of CPU processing. Unfortunately, if an unauthorized party gains access to the SKEYID_d key, all your encryption keys are compromised. PFS addresses this security risk by forcing a new Diffie-Hellman key exchange to occur for each Phase 2 tunnel. Using PFS is thus more secure, although the re-keying procedure in Phase 2 might take slightly longer with PFS enabled.

Point-to-Point Tunneling Protocol (PPTP) – PPTP is an extension of the Point-to-Point Protocol that is used for communication on the Internet. It was developed by Microsoft to support virtual private networks (VPNs), which allow individuals and organizations to use the Internet as a secure means of communication. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection.

Replay Protection – A replay attack occurs when somebody intercepts a series of packets and uses them later either to flood the system, causing a denial-of-service (DoS), or to gain entry to the trusted network. The replay protection feature enables devices to check every IPSec packet to see if it has been received before.

Security Association – An SA is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. For bidirectional communication, there must be at least two SAs, one for each direction. The VPN participants negotiate and agree to Phase 1 and Phase 2 SAs during an AutoKey IKE negotiation. See also *Security Parameters Index*.

Security Parameters Index – (SPI) is a hexadecimal value which uniquely identifies each tunnel. It also tells the NetScreen device which key to use to decrypt packets.

SHA-1 – Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)

Tunneling – A method of data encapsulation. With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.

Virtual Private Network (VPN) – A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling, screening, encryption, and IPSec.