

VR2004C/VR2004AC VPN Security Routers Frequently Asked Questions

GLOSSARY OF TERMS	3
Q1. WHAT IS VIRTUAL PRIVATE NETWORKING?	3
Q2. WHAT IS VPN END POINT?	3
Q3. WHAT IS ENCRYPTION?	3
Q4. WHAT IS DES AND 3DES?	3
Q5. WHAT IS IKE?	3
Q6. WHAT IS SECURITY ASSOCIATION (SA)?	4
Q7. WHAT IS PPTP?	4
Q8. WHAT IS IPSEC?	4
Q9. WHAT IS NAT?	4
Q10. ISN'T NAT THE SAME AS "FIREWALL"?	4
GENERAL QUESTIONS	5
Q1. WHAT IS THE VR2004C/VR2004AC VPN SECURITY ROUTER?	5
Q2. WHAT IS THE DEFAULT IP ADDRESS OF VR2004C/VR2004AC?	5
Q3. CAN I USE MY OWN LAN IP ADDRESSES OR AM I REQUIRED TO CHANGE TO IP ADDRESSES PROVIDED BY VR2004C/VR2004AC?	5
Q4. HOW CAN I GET THE LATEST VR2004C/VR2004AC FIRMWARE?	5
Q5. WHAT IS THE DEFAULT ADMINISTRATOR'S USERNAME AND PASSWORD FOR THE VR2004C/VR2004AC?	5
Q6. WHAT PLATFORMS ARE COMPATIBLE WITH THE VR2004C/VR2004AC?	5
ADVANCED QUESTIONS	6
Q1. I AM NOT ABLE TO SEE THE WEB CONFIGURATION SCREEN OF THE VR2004C/VR2004AC. WHAT CAN I DO?	6
Q2. WHY WON'T THE VR2004C/VR2004AC OBTAIN AN IP ADDRESS FROM MY ISP?	6
Q3. HOW CAN I MAKE SURE MY PC'S TCP/IP SETTING IS CORRECT? AND HOW DO I KNOW THE MAC ADDRESS OF MY PC?	6
Q4. WHAT CAN I DO IF I HAVE FORGOTTEN THE PASSWORD OF VR2004C/VR2004AC?	7
Q5. WHAT IF MY ISP CHECKS MY COMPUTER 'HOST NAME'?	7
Q6. WHAT IF MY ISP CHECKS MY MAC ADDRESS?	7
Q7. HOW DO I KNOW WHETHER MY ISP USES STATIC (MANUALLY ASSIGNED) OR DYNAMIC (ASSIGNED BY A DHCP SERVER) IP ADDRESS?	7
Q8. HOW EASY IS IT TO CONNECT TO THE INTERNET USING THE VR2004C/VR2004AC?	8
Q9. I CAN'T CONNECT TO THE INTERNET?	8
Q10. I DON'T KNOW HOW TO USE THE SYSTEM LOG FUNCTION?	8
Q11. DOES THE VR2004C/VR2004AC SUPPORT PPPoE?	8
Q12. DOES THE VR2004C/VR2004AC SUPPORT PPTP?	8
Q13. WHAT IS THE MAXIMUM NUMBER OF USERS SUPPORTED BY THE VR2004C/VR2004AC?	9

VPN CONFIGURATION (GENERAL QUESTION)	9
Q1. DOES THE VR2004C/VR2004AC SUPPORT VPN?	9
Q2. WHAT'S THE DIFFERENCE BETWEEN IKE AND MANUAL MODE?	9
Q3. WHEN I SETUP THE VPN CONNECTION, WHICH FIELDS MUST BE FILLED IN?.....	9
Q4. WHAT DO I NEED TO ESTABLISH A VPN TUNNEL?	10
Q5. HOW MANY VPN TUNNELS CAN THE VR2004C/VR2004AC SUPPORT AT ONE TIME?	10
VPN CONFIGURATION (VPN SETTINGS DESCRIBE)	11
Q1. CAN YOU DESCRIBE EACH FIELD IN THE VPN SETTINGS PAGE?	11
REFERENCE SECTION	13
Q1. WHAT IS SSH?	13
Q2. WHAT IS SAFENET?	13

Glossary of Terms

Q1. What is Virtual Private Networking?

Typically, a Virtual Private Network (VPN) is defined as: a group of two or more computer systems connected to a private network with limited public-network access that communicates securely over a public network, such as the internet. Security experts agree that VPN should include encryption, authentication of remote users or hosts, and mechanisms for hiding or masking information about private network topology from potential attackers on the public network (Internet).

Q2. What is VPN end point?

VPN end point capability within a router provides the ability to initiate a VPN tunnel to some other location that supports either a VPN client or has VPN end point capability.

Q3. What is encryption?

Encryption is a mathematical operation that transforms data from standard text to ciphered text. Usually the mathematical operation requires that an alphanumeric key be supplied along with the standard text. The key plus standard text are processed by the encryption operation, which then produces secure scrambled text. Decryption is the opposite of encryption; it is the mathematical operation that transforms ciphered text to standard text.

Q4. What is DES and 3DES?

Digital Encryption Standard (DES) is encryption used for data communication where both the sender and receiver must know the same secret key that is used to encrypt and decrypt the data, or to generate and verify a message authentication code. DES encryption uses a 56-bit key. 3DES is a variation on DES that uses a 168-bit key, providing a higher level of security, and is considered by security experts to be unbreakable.

Q5. What is IKE?

Internet Key Exchange is a negotiation and key exchange protocol specified by the Internet Engineering Task Force (IETF). An IKE security association (SA) automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass IP traffic.

Q6. What is Security Association (SA)?

Security Association is a group of security settings related to a specific VPN tunnel. A Security Association groups together all the necessary settings needed to create a VPN tunnel. Different SAs may be created to connect branch offices, allow secure remote management, and pass unsupported traffic. All SAs require a specified encryption method, IPSec gateway address and destination network address.

Q7. What is PPTP?

Point-to-Point Tunneling Protocol builds on the functionality of the Point-to-Point protocol (PPP) to provide remote access that can be tunneled through the internet to a destination site or computer. PPTP encapsulates PPP packets using generic routing encapsulation protocol.

Q8. What is IPSec?

Internet Protocol Security is a robust VPN standard that covers authentication and encryption of data traffic over the Internet. VPN technology employing IPSec will encrypt all outgoing data and decrypt all incoming data so that a public network (like the Internet) can be used as the transportation media. IPSec can support two encryption modes: transport and tunnel. Transport mode encrypts the data portion of each packet but leaves the header unencrypted. The more secure tunnel mode encrypts both the header and the data. At the receiving end, an IPSec compliant device decrypts each packet. For IPSec to work, both the sending and receiving devices must share a key. IKE protocol is a key management standard which is commonly used in conjunction with the IPSec standard. Unlike PPTP, IPSec is specific only to the Internet Protocol (IP) and does not provide security for other protocols.

Q9. What is NAT?

Network Address Translation is used in a router to prevent hacking into the local area network (LAN). NAT substitutes a "private" IP address of devices located on the LAN side of the router with a new "public" IP address that is visible on the internet side of the router. By virtue of this simple implementation, any of up to 253 devices located on the LAN will be hidden from Internet hackers. Only the router's IP address is visible on the Internet.

Q10. Isn't NAT the same as "firewall"?

No. Though the term "firewall" has been used when describing a router's ability to hide the LAN IP addresses, a true firewall employs a technology called Stateful Packet Inspection (SPI). Firewalls provide a greater level of security and are generally more expensive than a NAT router. Firewalls give the administrator the ability to set up specific IP addresses or domain names that are allowed to be accessed, while refusing any other attempt to access the LAN. This is often referred to as filtering. Firewalls can also allow remote access to the private network through the use of secure login procedures and authentication certificates (VPN). Firewalls are used to prevent Denial of Service (DoS) attacks and can use software to provide content filtering to deny access to unwanted web sites.

General Questions

Q1. What is the VR2004C/VR2004AC VPN Security Router?

VR2004C/VR2004AC is a network security device used to connect multiple PCs (Local Area network, or LAN) in the small office to the Internet (Wide Area Network, or WAN) security via a broadband modem connection, such as DSL or cable modem.

Q2. What is the default IP address of VR2004C/VR2004AC?

The default IP address of VR2004C/VR2004AC is 192.168.123.254

Q3. Can I use my own LAN IP addresses or am I required to change to IP addresses provided by VR2004C/VR2004AC?

Yes, the VR2004C/VR2004AC VPN Security Routers allow users to configure the devices' IP address, and thus allows the LAN users to keep their original LAN IP settings.

Q4. How can I get the latest VR2004C/VR2004AC firmware?

The latest VR2004C/VR2004AC firmware versions are posted at <http://www.asante.com/>, where they can be downloaded for free.

Q5. What is the default administrator's username and password for the VR2004C/VR2004AC?

By default, VR2004C/VR2004AC's user name is "admin". There is no default password.

Q6. What platforms are compatible with the VR2004C/VR2004AC?

The VR2004C/VR2004AC can be used on all platforms (such as Macintosh, Linux, UNIX, Windows, etc.) that employ the TCP/IP protocol and can use a browser (such as Netscape and Internet Explorer). The VR2004C/VR2004AC VPN Security Router has a built-in HTTP web server for management access using a browser.

Advanced Questions

Q1. I am not able to see the web configuration screen of the VR2004C/VR2004AC. What can I do?

First, you must verify that your computer's TCP/IP is properly setup (Please refer to Q3). Then, verify that your computer is in the same network as the VR2004C/VR2004AC. Next, you must remove the proxy settings and dial-up settings in your browser's setup (InternetExplorer/Netscape), then check the web configuration screen again.

Q2. Why won't the VR2004C/VR2004AC obtain an IP address from my ISP?

Check that your Cable/xDSL modem is powered on and properly connected to the WAN port of the VR2004C/VR2004AC. Check that your ISP is DHCP capable and supports dynamic IP addressing. You may need to give the MAC address of the VR2004C/VR2004AC to your ISP.

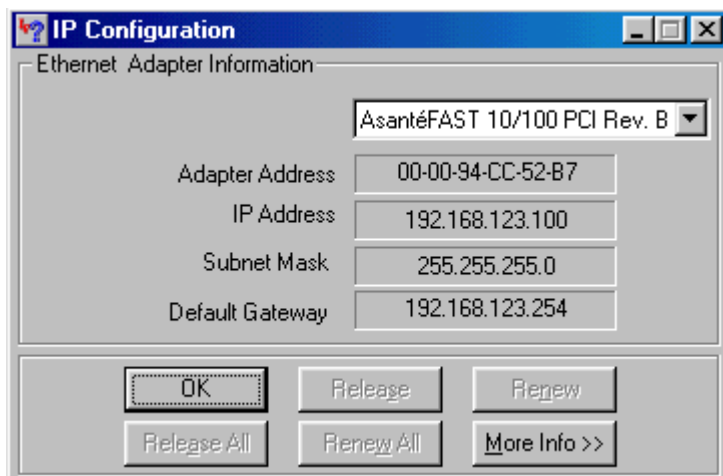
Q3. How can I make sure my PC's TCP/IP setting is correct? And how do I know the MAC address of my PC?

Two utilities which are useful for discovering a computer's IP configuration are:

WINIPCFG (for windows 95/98/ME)

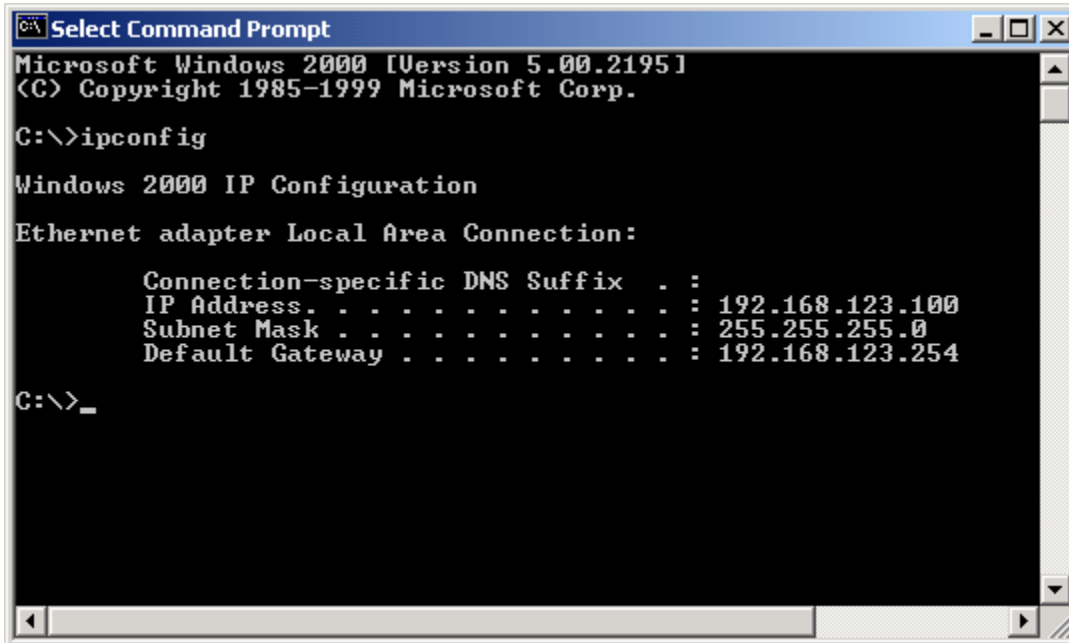
Inside the windows 95/98/ME Start button, select Run and type *wipcfg*. In the example below this computer has an IP address of 192.168.123.100 and the default gateway is 192.168.123.254. The default gateway should be the network device's (VR2004C/VR2004AC) IP address. The MAC address in windows 95/98/ME is called the Adapter Address.

You can also type **wipcfg** in the DOS command.



IPCONFIG (for windows 2000/NT)

In the DOS command type *IPCONFIG* and press Enter. Your PC's IP information will be displayed as shown below:



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.123.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.123.254

C:\>_
```

Q4. What can I do if I have forgotten the password of VR2004C/VR2004AC?

The password is used to protect the VR2004C/VR2004AC from unauthorized access. If you forgot the password of the VR2004C/VR2004AC, you must reset it to factory default and then reconfigure it again. To reset it to the factory default, you have to push the reset button on the back of VR2004C/VR2004AC for 5 seconds.

Q5.What if my ISP checks my computer 'host name'?

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. In this case, you must input the computer's 'Host Name' of the in the 'Networking' settings into the Host Name field of the VR2004C/VR2004AC.

Q6.What if my ISP checks my MAC address?

Some ISPs only provide an IP address to the user with an authorized MAC address. Normally, this MAC address is the computer's MAC address. In this case, you must either copy this computer's MAC address to theVR2004C/VR2004AC's WAN Ethernet MAC address setting, or report the MAC address of the VR2004C/VR2004AC to your ISP.

Q7. How do I know whether my ISP uses static (manually assigned) or dynamic (assigned by a DHCP server) IP address?

Most ISPs use dynamic IP address. You should consult your ISP to confirm this information.

Q8. How easy is it to connect to the Internet using the VR2004C/VR2004AC?

You can setup the VR2004C/VR2004AC using your existing Web browser (i.e.: Netscape or Internet Explorer). Simply connect your Cable/DSL modem to the WAN port on the back of the VR2004C/VR2004AC, connect your computer(s) to the LAN ports, and then configure the VR2004C/VR2004AC by typing "192.168.123.254" at the URL address line in your web browser. Please refer to the VR2004C/VR2004AC manual for complete information.

Q9. I can't connect to the Internet?

Check to see if the power of your Cable/DSL is on!

Check to see if your Cable/DSL link light is on to verify a good physical connection.

Check to see if the WAN Ethernet link of the VR2004C/VR2004AC is on to verify that your Cable/DSL modem is connected properly.

Check to see if the computer is successfully connected to the network.

Check to see if the network adapter has been properly installed.

Check to see if the TCP/IP stack is successfully installed.

Check to see if the computer is physically connected to the network (Ethernet).

Check to see if the computer's IP settings are correct.

Try to "ping" from the computer to 192.168.123.254.

Connect from your browser to the VR2004C/VR2004AC (192.168.123.254) and click on the Router Status menu to see the connection status.

Q10. I don't know how to use the System Log function?

The System Log function allows the administrator to assign the IP address of a server, on which a log server is running. If a particular event happens, the router sends a notification to the log server; the log server can then present the log to the users. A free log server (ex: kiwis Syslog Daemon) can be downloaded from the internet at:

<http://www.kiwisyslog.com/>.

Q11. Does the VR2004C/VR2004AC support PPPoE?

Yes, the VR2004C/VR2004AC supports PPPoE client function.

Q12. Does the VR2004C/VR2004AC support PPTP?

Yes, the VR2004C/VR2004AC supports PPTP client function.

Q13. What is the maximum number of users supported by the VR2004C/VR2004AC?

The VR2004C/VR2004AC can support up to 253 users. Please note that the performance of the router will deteriorate as the number of users increases due to network traffic.

VPN Configuration (General Question)

Q1. Does the VR2004C/VR2004AC support VPN?

Yes, the VR2004C/VR2004AC router supports VPN (Virtual Private Networking).

Q2. What's the difference between IKE and Manual mode?

IKE mode:

IKE is an automated method for establishing a shared security policy and authenticated keys. A pre-shared key is used for mutual identification.

Manual mode:

Manual mode allows you to pre-define the keys. The settings at the remote route or host must both match these settings exactly.

Q3. When I setup the VPN connection, which fields must be filled in?

- If you are running Secure Association (SA) and have selected **IKE** and **Enable UID** (Unique Identifier String) as the authentication method, these fields as follow must be filled in:

Connection Name
Local IPsec Identifier
Remote IPsec Identifier
Remote IP Network
Remote IP Netmask
Remote Gateway IP
Pre-shared Key

If you are running Secure Association (SA) and have selected **IKE** and **Disable UID**, as authentication method, then you do not need to enter **Local IPsec Identifier** and **Local IPsec Identifier**.

- If you are running Secure Association (SA) and have selected **Manual** and **Enable UID** (Unique Identifier String) as authentication method, these fields below must be filled in:

Connection Name
Local IPSec Identifier
Remote IPSec Identifier
Remote IP Network
Remote IP Netmask
Remote Gateway IP
Incoming SPI
Outgoing SPI
Preshared Key
Authentication Key

If you are running Secure Association (SA) and have selected **Manual** and **Disable UID** as authentication method, then you do not need to enter **Local IPSec Identifier** and **Local IPSec Identifier**.

Q4. What do I need to establish a VPN tunnel?

1. VR2004C/VR2004AC to VR2004C/VR2004AC: Using two VPN devices like the VR2004C/VR2004AC between the corporate and remote office can establish a VPN tunnel.
2. VR2004C/VR2004AC to other VPN product: You may use another VPN product such as Cisco, Check point, or Nortel at the corporate office and use the VR2004C/VR2004AC to establish the VPN tunnel from home or remote office.
3. VR2004C/VR2004AC to Mobile User: Use the VR2004C/VR2004AC to establish a VPN tunnel at the main office. It's easy and safe for the mobile user to login to the main office's server running the client software such as SSH, SafeNet, Win2000, or Windows XP Professional.

Q5. How many VPN tunnels can the VR2004C/VR2004AC support at one time?

As a standard feature, the VR2004C/VR2004AC has the ability to support up to 8 VPN tunnels at one time.

VPN Configuration (VPN Settings Describe)

Q1.Can you describe each field in the VPN settings page?

- If you are running Secure Association (SA) and have selected **IKE** and **Enable UID** (Unique Identifier String) as authentication method:
 1. **Connection Name:** This is for identification purposes only
 2. **Local IPSec Identifier:** Enter router's wan port IP or entry string.
 3. **Remote IPSec Identifier:** Enter remote router's wan port IP or entry string. This IP or string must exactly match the identifiers used in the configuration of the remote router.
 4. **Remote IP Network:** Define the remote network.
 5. **Remote IP Netmask:** Define the remote netmask.
 6. **Remote Gateway IP:** The Gateway IP will be the public IP address of the remote router.
 7. **Network Interface:** Select the Network Interface
 8. **Perfect Forward Secure:** Click either the Enabled or Disabled radio button. This feature provides better security; it ensures that the encryption keys generated are not relevant to each other.
 9. **Encryption Protocol:** The type must match the information provided by the remote device.
 - **Null** - Fastest, but no security.
 - **DES** - Faster but less secure than 3DES.
 - **3DES** - (Triple DES) Most secure.
 10. **Preshared Key:** Enter the Preshared Key name (you can enter the alphanumeric name). The value must match the information provided by the remote device.
 11. **Key Life:** Enter the amount of time that tells the router to renegotiate the key. The default of 3600 seconds = 1 hour
 12. **IKE Life Time:** Enter the amount of time that tells the router to renegotiate the IKE security association. The default of 28800 seconds = 8 hours.

- If you are running Secure Association (SA) and have selected **Manual** and **Enable UID** (Unique Identifier String) as authentication method:
 1. **Connection Name:** This is for identification purposes only
 2. **Local IPSec Identifier:** Enter router's wan port IP or entry string.
 3. **Remote IPSec Identifier:** Enter the remote router's wan port IP or entry string. This IP or string must exactly match the identifiers used in the configuration of the remote router.
 4. **Remote IP Network:** Define the remote network.
 5. **Remote IP Netmask:** Define the remote netmask.
 6. **Remote Gateway IP:** The Gateway IP will be the public IP address of the remote router.
 7. **Network Interface:** Select the network interface

- 8. Incoming SPI:** Enter the security parameter index that the remote host will send to identify the security association (SA). The incoming SPI value must match the outgoing SPI at the other end of the tunnel.
- 9. Outgoing SPI:** Enter the security parameter index that this router will send to identify the security association (SA). The outgoing SPI value must match the incoming SPI at the other end of the tunnel.
- 10. Encryption Protocol:** The type must match the information provided by the remote device.
 - **Null** - Fastest, but no security.
 - **DES** - Faster but less secure than 3DES.
 - **3DES** - (Triple DES) Most secure.
- 11. Encryption Key:** The string is used as a key to encrypt and decrypt the data transmitted. The value must match the information provided by the remote device.
- 12. Authentication Protocol:** VR2004C/VR2004AC supports two authentication algorithms (MD5 or SHA-1); user can select an appropriate authentication algorithm. The type must match the information provided by the remote device.
- 13. Authentication Key:** This string is used as key authentication. The value must match the information provided by the remote device.

Reference Section

Q1. What is SSH?

SSH Sentinel is a software product for securing Internet Protocol (IP) based traffic using the IPsec protocol as specified by Internet Engineering Task Force (IETF) standards. SSH Sentinel is an easy-to-use product designed for end users. It allows you to encrypt and authenticate important network connections, like remote access to corporate networks remote administration, file transfer, sending and receiving email (SMTP, POP) and IP telephony.

SSH Sentinel software currently supports the following Microsoft Windows operating systems: Windows 95, Windows 98, Windows ME, Windows NT4, and Windows 2000. Next, the software will be available on the Linux platform. SSH Sentinel is designed to be a client type of IPsec application. The features are designed for a single user workstation using a single network adapter and the Internet Protocol (IP). SSH Sentinel supports all network connection types, including dial-up. The product is designed to be secure and robust, easy to use, and quick to adapt to the environment at hand. Key characteristics include intuitive installation and configuration, as well as an easy way to use certificates for authentication.

SSH Sentinel was implemented due to numerous customer and end-user requests to bring out a real IPsec solution for commercial platforms and to enable full-scale network encryption with strong authentication.

Q2. What is SafeNet?

SafeNet/Soft-PK is a Windows-compatible software product that secures data communications sent from a desktop or laptop computer across a public or private TCP/IP network. When SafeNet/Soft-PK operates on an unprotected public network, such as the Internet, it creates a virtual private network (VPN) between end users.

Network Applications

SafeNet/Soft-PK supports secure client-to-gateway or client-to-client communications. Traveling Road warriors, for example, can telecommute from their home or virtual offices to the main office through the Internet or other dial-in remote access devices for secure client-to-gateway communications. For example, organizations that require a low-cost solution for secure communications among their employees or members across a private LAN, WAN, or individual dial-up connections can use SafeNet/Soft-PK for secure client-to-client communications.

Interoperability

SafeNet/Soft-PK is interoperable with IPsec devices from major equipment manufacturers. It has been awarded IPsec certification from the International Computer Security Association (ICSA). SafeNet/Soft-PK interoperates with IPsec-compliant gateways such as firewalls, VPN routers, and gateway encryptors. An up-to-date list of ICSA-certified products can be found at www.icsa.net .