SEL Application Guide Volume VII AG2002-05

Securing SEL Ethernet Products With VPN Technology

Allen Risley, Chad Marlow, Paul Oman, and Dave Dolezilek

INTRODUCTION

The industry trend to increase the level of power system automation and remote accessibility, coupled with a dramatic increase in the number and sophistication of TCP/IP and telephone-based cyber attacks, is exposing the electric power industry to a growing risk of electronic intrusion. Furthermore, our electric power infrastructure is a potentially high-value target for individuals, organizations, and nations with anti-U.S. sentiments or political agendas. As a result, there is a very real and rapidly increasing probability that malicious individuals will attempt to gain remote access to your power control equipment in order to destabilize the power grid and/or destroy parts of your power system. At the heart of this vulnerability is the capability for remote access to control and protection equipment used by generation facilities and Transmission and Distribution (T&D) utilities. Remote access to protective equipment historically has been limited to proprietary systems and dedicated network connections. Now, however, there is an increased use of public telephone services, protocols, and network facilities, concurrent with a growing, more sophisticated, worldwide population of computer users and computer hackers. These persons, regardless of location or nationality, represent a growing threat to the safety and reliability of electric power systems, and there is increasing evidence suggesting that organized information warfare groups have targeted United States infrastructures. The North American electric power industry has been identified as one of America's critical infrastructures. Electronic intruders randomly or maliciously operating circuit breakers, reclosers, and switchgear could have disastrous consequences on the safety and reliability of our electric power systems. It is important to note that, even though we do not typically connect critical SCADA equipment to the Internet (the Internet is by far the most hostile of all public network infrastructures), we do expose this equipment to malicious attack every time we use the public infrastructure to build our SCADA network and engineering access connections. Examples of such public media include leased and dialup lines over the telecommunications infrastructure, as well as the air between and around wireless transmitters (data sent via wireless link will radiate a considerable distance).

SEL recommends communications strategies that provide both security and dependability. Security ensures that corrupted data or commands from an illegitimate source are ignored whereas dependability ensures that valid commands and requests are not ignored by mistake.

Threats of security breaches of the communications infrastructure not only jeopardize the safety, reliability, and economy of the power system, but also expose confidential commercial information. This commercial information reveals strategic business practices and, perhaps more importantly, reveals customer profiles. This customer data is often targeted as an easy source of identity theft. Care must be given to the appropriate separation of operational and business networks.

SCHWEITZER ENGINEERING LABORATORIES
2350 NE Hopkins Court • Pullman, WA • 99163-5603 • USA
Phone: (509) 332-1890 • Fax: (509) 332-7990
E-mail: info@selinc.com • Internet: www.selinc.com

SEL recommends that the following information security measures be taken to defend against possible electronic security threats:

- Ensure privacy of sensitive data and information
- Confirm integrity of data, requests, and commands received
- Prevent manipulation of valid requests and commands to jeopardize system functionality and performance
- Confirm authentication of the source of received data, requests, and commands

MALICIOUS INTRUSION THREATS

More often than not, an attacker's goal is to gain control over some or all of your networked assets. The most direct method for gaining access to a networked device is to acquire the login information for that system. There are a number of ways to gain such information, including social engineering, physical theft, password guessing, password cracking, and network interception. Social engineering involves gathering sensitive but publicly available information and/or manipulating insiders. To thwart social-engineering-based attacks your company needs to create and implement well-defined practices for safeguarding confidential information.

Password guessing attacks can be manual or automated. An attacker can simply start entering possible login strings at a system prompt. Any knowledge of the system hardware or legitimate users can be applied to narrow the search and increase the likelihood that a valid password will be entered. One common hacker technique is to look at the welcome banner issued by the computer or IED, which often identifies the make and model of the equipment, thus enabling the hacker to try the vendor's default password(s). For this reason, it is important to always replace vendor passwords with your own. For more complicated attacks, scripts can easily be written to continuously attempt logins using a list of words stored in a file, typically called a dictionary. Attack dictionaries can potentially contain thousands of commonly used passwords, including street slang, foreign words, and entertainment names and buzzwords like C3PO, Wookie, Gandalf, and Coolio. Hence, it is important to choose passwords that are not words, names, or pronounceable acronyms. If the attacker can obtain the weakly encrypted passwords from intercepted packets or operating system password files, he or she can employ password-cracking techniques to get the login information. If the encryption technique is known, the attacker can encrypt all entries in an attack dictionary and compare the resulting cyphertext against that which was stolen. If a match is found, then the attacker has successfully cracked the login information for the system. There are many scripts and programs, both commercial and free, that do this automatically. L0phtCrack, a commercial product available for around $250 (earlier versions can be found for free), is capable of cracking Windows NT and Windows 2000 passwords because these operating systems use weak encrytion protocols to transmit and store the passwords. It can directly obtain the encrypted password file from a networked host or server or it can intercept the challenge/response authentication traffic that is exchanged between networked machines. Other cracking programs are available that are capable of cracking Unix/Linux password files as well as many other weak encryption formats. Most password cracking programs come with an extensive dictionary file and also support brute force password attacks that try all combinations of letters, numbers, and characters.

One popular method for password theft is to intercept the login information from normal network traffic transmitted between systems negotiating a remote connection. Figure 1 shows the output from a packet interception tool (also known as a network sniffer) freely available over the

Internet. The bottom portion of the sniffer display shows the actual text or control information contained in the packet selected in the top portion of the display. Many protocols, such as ftp or Telnet, exchange login information in plain text that can be easily read from the intercepted packet. Even applications that display asterisks at the user password prompt transfer the password characters across the network. Thus, if sniffed, the actual password would be exposed. Other protocols, such as SSH (Secure Shell), use encryption techniques to hide login exchanges. Some encryption protocols are stronger than others, so it is very important to understand the relative strengths and weaknesses of all protocols that are being used on your network to exchange login information. If you are using a plain text protocol to implement remote access over public networks, it is essential that you use strong encryption techniques, like Virtual Private Networking (VPN), to hide the transmitted information. Many sniffing tools are available for free download. Some are passive sniffers incapable of rerouting network traffic, but others are actually capable of rerouting network traffic to make it visible to the attacker. This capability allows the attacker to intercept traffic that would not otherwise have traveled over his or her network. The attacker can copy all packets of interest to a file and then forward the traffic to the intended destination so as not to interrupt normal communication.

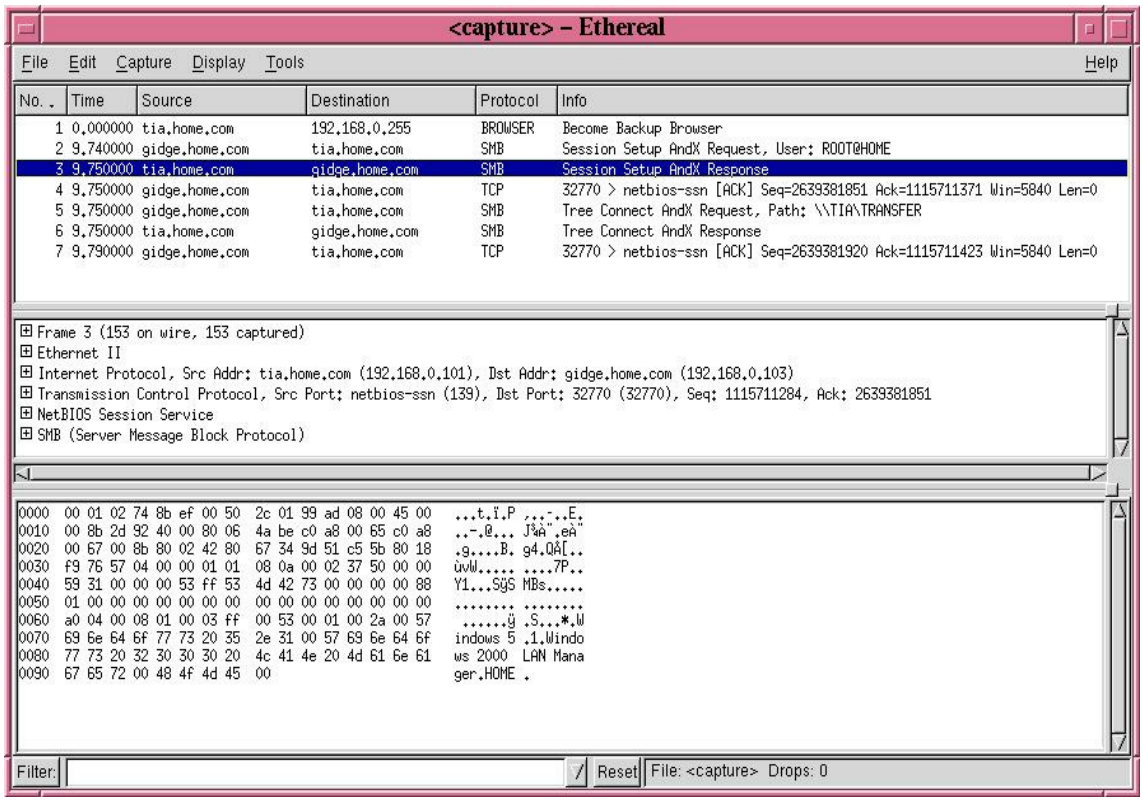

Figure 1: Network Sniffer

There are also methods for gaining access to remote systems that bypass the login information altogether. One such method, known as session hijacking or a man-in-the-middle attack, involves taking over a legitimate remote session, such as ftp or Telnet, between an authorized user and a remote host (the target system). In order to achieve this, the attacker must be able to directly view the session traffic with his or her local computer. This requirement is automatic if the attacker is on a network segment between the legitimate user and the remote host; however, if this is not the case, the attacker can reroute the traffic using active packet sniffers. If the packet is not encrypted, or is weakly encrypted, and the session is visible to the attacker, then it is susceptible to session hijacking. By setting (spoofing) the source address to that of the legitimate user, and

matching the TCP sequence numbers, the attacker can successfully pose as the legitimate user and take over the session at any time. Some tools, such as Hunt and Ettercap, allow pushbutton session hijacking on TCP/IP networks. These tools will identify exploitable sessions on the network, list them, and, at the push of a button, hijack the session of choice. All the authorized user will notice is that communication to the remote host has been lost, which will probably be blamed on network congestion and simply ignored. With a hijacked session, the attacker has all the rights and privileges on the remote machine that the original user had. In fact, from the remote host's point of view, the attacker *is* the original user.

DEFENDING YOUR ASSETS WITH VIRTUAL PRIVATE NETWORKING

In light of these vulnerabilities, it is increasingly evident that effective procedures and techniques must be employed to reduce the chances of cyber-intrusion[1]. One very effective technique involves the use of a Virtual Private Network (VPN). VPN devices allow two networks, physically separated by a possibly great distance and connected through an insecure network infrastructure, to communicate in a very secure manner. They effectively combine much of the traffic filtering capability of a firewall with the security of strong encryption and authentication.

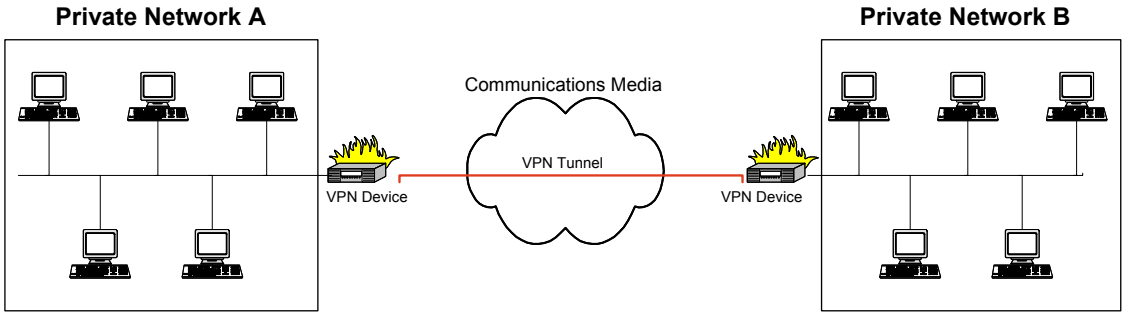

Figure 2: Generic VPN Network

Figure 2 shows two such networks connected by some form of insecure, intervening communications network. The two VPN devices are used to securely bridge private, secure networks, A and B, respectively. Most VPN devices support many simultaneous tunnels, which allows secure, bidirectional communication between many users with a single VPN device at each remote site. The security offered by these tunnels comes in the form of strong authentication and encryption. Each tunnel between two points has a shared key associated with it, which is programmed into the two VPN devices at the endpoints of the tunnel. This key is used to encrypt the startup dialogue between the two VPNs. Communication begins with an exchange of new keys, which will be used to encrypt all traffic between the devices for a pre-configured length of time. At the end of this time frame, the devices will exchange a new, randomly chosen encryption key. This programmable key lifetime and automated key exchange adds to the security of the connection because, if the lifetime is set short enough, the encryption keys will change often enough to prohibit the attacker from cracking the encryption method and compromising the network. The identity of the device sending the packet is authenticated using a strong hash algorithm that, in essence, forces the device on the other end of the tunnel to "prove" its identity prior to accepting communications traffic from it. The term "tunnel" is a reference to the act of tunneling one communications protocol within the data field of another protocol. In the

[1] It is important to note that no functional network is ever 100 percent safe from cyber attack. However, it is possible to secure the network sufficiently so as to make the probability of cyber intrusion quite low. The most important factor in this process is ensuring that the fewest possible number of potential attackers have access to your network. This is why we do not recommend connecting critical equipment to the Internet.

case of a VPN, the tunneled protocols are both on the same network layer and are, in fact, identical protocols. A VPN device will encrypt an entire IP packet and embed it within the data field of an unencrypted IP packet. Referring to Figure 3: User 1 on private network A sends a packet to User 2 on private network B. The bridging VPN devices are configured such that any traffic from private network A, addressed to an IP address on private network B, will first be strongly encrypted and then sent to the IP address of the VPN device on network B instead of directly to the intended destination. When the VPN device on network B receives the traffic from the VPN device on network A, it removes the embedded, encrypted IP packet, decrypts it, and sends it off to be routed on private network B (i.e. to the intended destination, User 2). It is important to note that the encryption process hides not only the original data, but also the TCP/UDP and IP headers of the original packet. This has the effect of hiding the details of the addresses, communications protocols, and topology of the connected private networks from prying eyes. Due to the encryption of the entire data payload, an intercepted packet will look like jumbled, random bits to a malicious attacker. This greatly reduces the threat of login information interception. Furthermore, the strong authentication provided by the VPN devices reduces the chances of a malicious attacker gaining access to the private network because, if properly configured, the VPN devices will block all traffic that does not properly pass authentication.

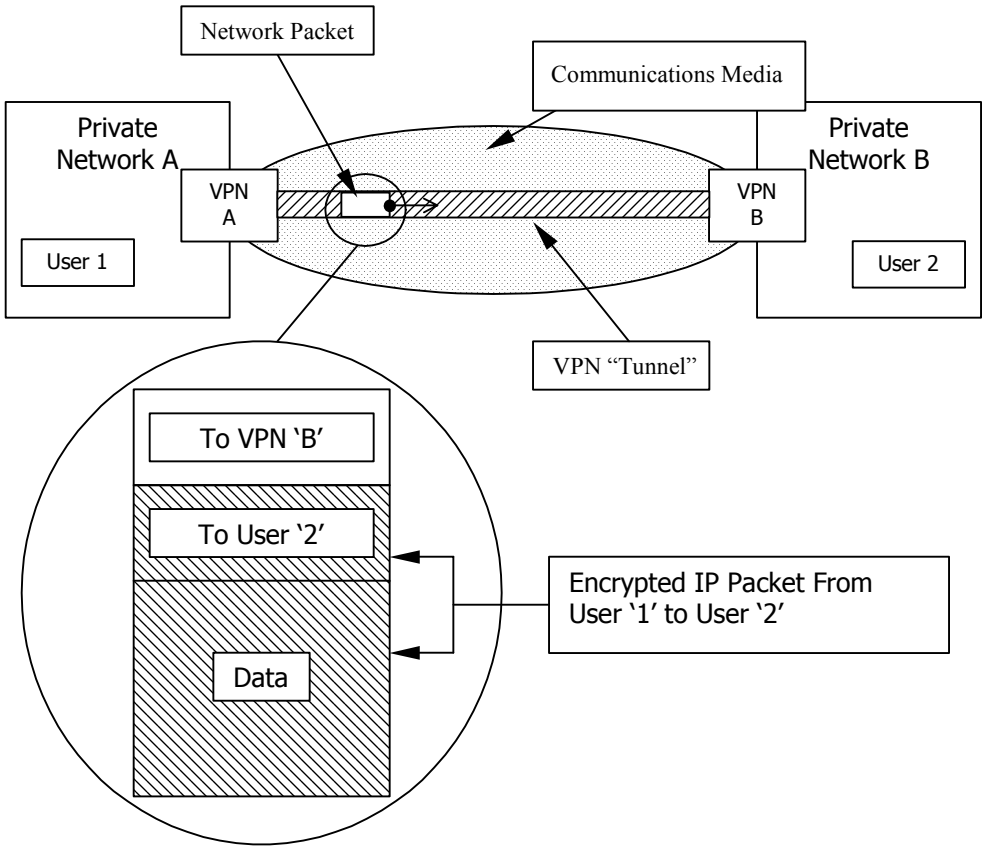

Figure 3: VPN Tunneling

USING VPN TECHNOLOGY WITH SEL NETWORKING PRODUCTS

In the following example, we show that the SEL 2701 Ethernet Processor and the SEL 2890 Ethernet Transceiver can be effectively secured with VPN technology. For this example, we chose to implement the VPN functionality on both sides of the secure tunnel with the Linksys BEFVP41 Etherfast Cable/DSL VPN Router. This solution can be purchased for about $150.00

each (we use two such devices in this example). We chose the Linksys product for this description because of its relatively low price and rich features. The BEFVP41 supports 3-DES (Triple Data Encryption Standard) encryption, which is still thought to have no inherent weaknesses, as well as SHA (Secure Hash Algorithm) hash authentication. Furthermore, the BEFVP41 supports up to 70 simultaneous VPN tunnels. The Linksys product is a combination VPN and router, so there are two IP addresses associated with the device: one for the wide area network (WAN) side of the device, which makes up the VPN functionality, and one for the local area network (LAN) side of the device, which makes up the router functionality. In essence, the WAN address constitutes the VPN presence, or identity, on the network associated with the insecure communications media, while the LAN address constitutes the VPN presence, or identity, on the private network. Despite its rich feature set, it is very important to remember that the BEFVP41 is not an environmentally hardened device. It is not rated to operate in the same temperature extremes as utility substation hardened equipment, typically –40 to +85 C, nor does it have the same demonstrated product longevity in this environment. Care must be taken when using nonsubstation-hardened equipment within mission critical communications designs.

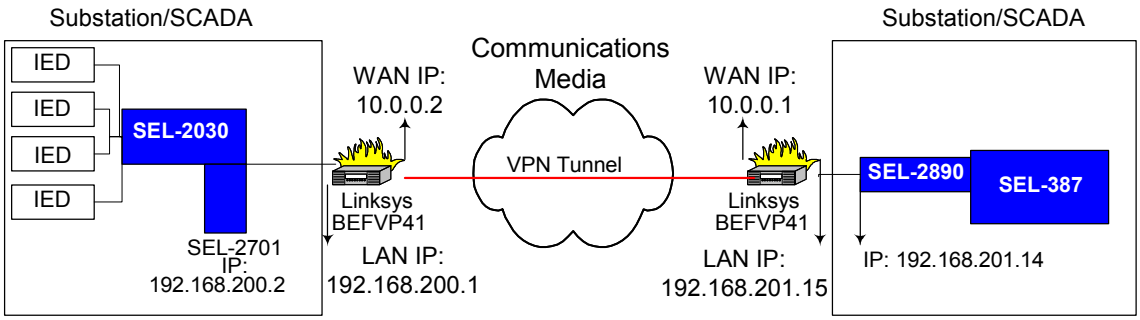

Figure 4: Secure Connection of an SEL-2030 and an SEL-387

As shown in Figure 4, this configuration securely connects an SEL-2030 Communications Processor and an SEL-387 Current Differential and Overcurrent Relay through an SEL-2701 Ethernet Processor and an SEL-2890 Ethernet Transceiver, respectively. The SEL-2701 and the LAN side of one VPN device were placed on the same private network, and thus were able to directly communicate with one another. The WAN side of each VPN was placed on another network in order to simulate the insecure "communications media" of Figure 2. Finally, the LAN side of the second VPN was placed on the same network as the SEL-2890 in order to create yet another simulated network.

To compare the above configuration with the VPN network diagram of Figure 2, the SEL-2030 and the LAN side of the first VPN will constitute Private Network A, while the SEL-2890 and the LAN side of the second VPN will constitute Private Network B. The VPN tunnel will then be built between the two WAN sides of the VPN devices, thus constituting the insecure communications media. With the tunnel built, secure, transparent communication is possible between Private Network A and Private Network B over the insecure intervening network. The details of the settings used to accomplish this follow.

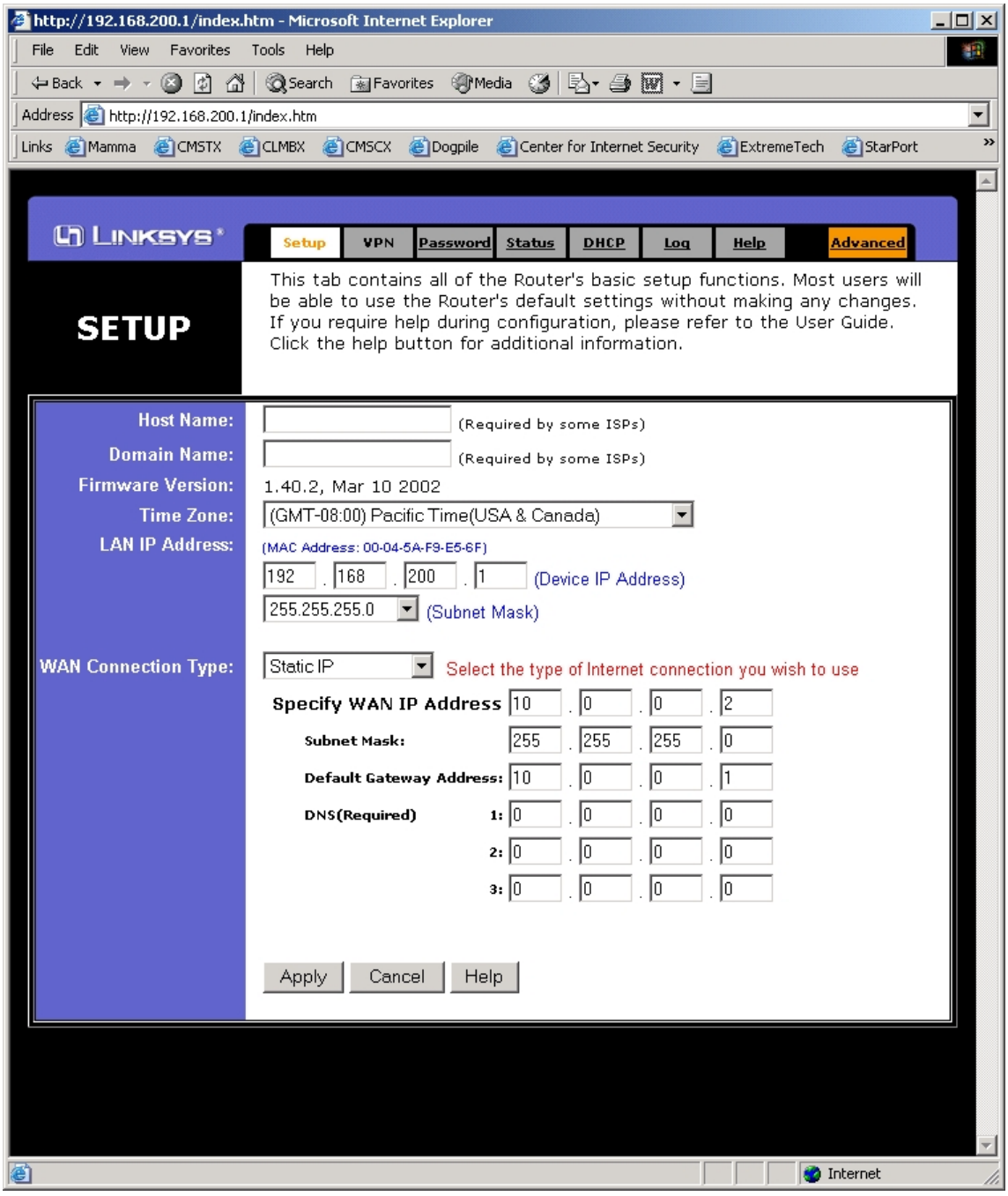

Figure 5: IP Address Setup Screen for VPN on Network A (the network with the SEL-2030)

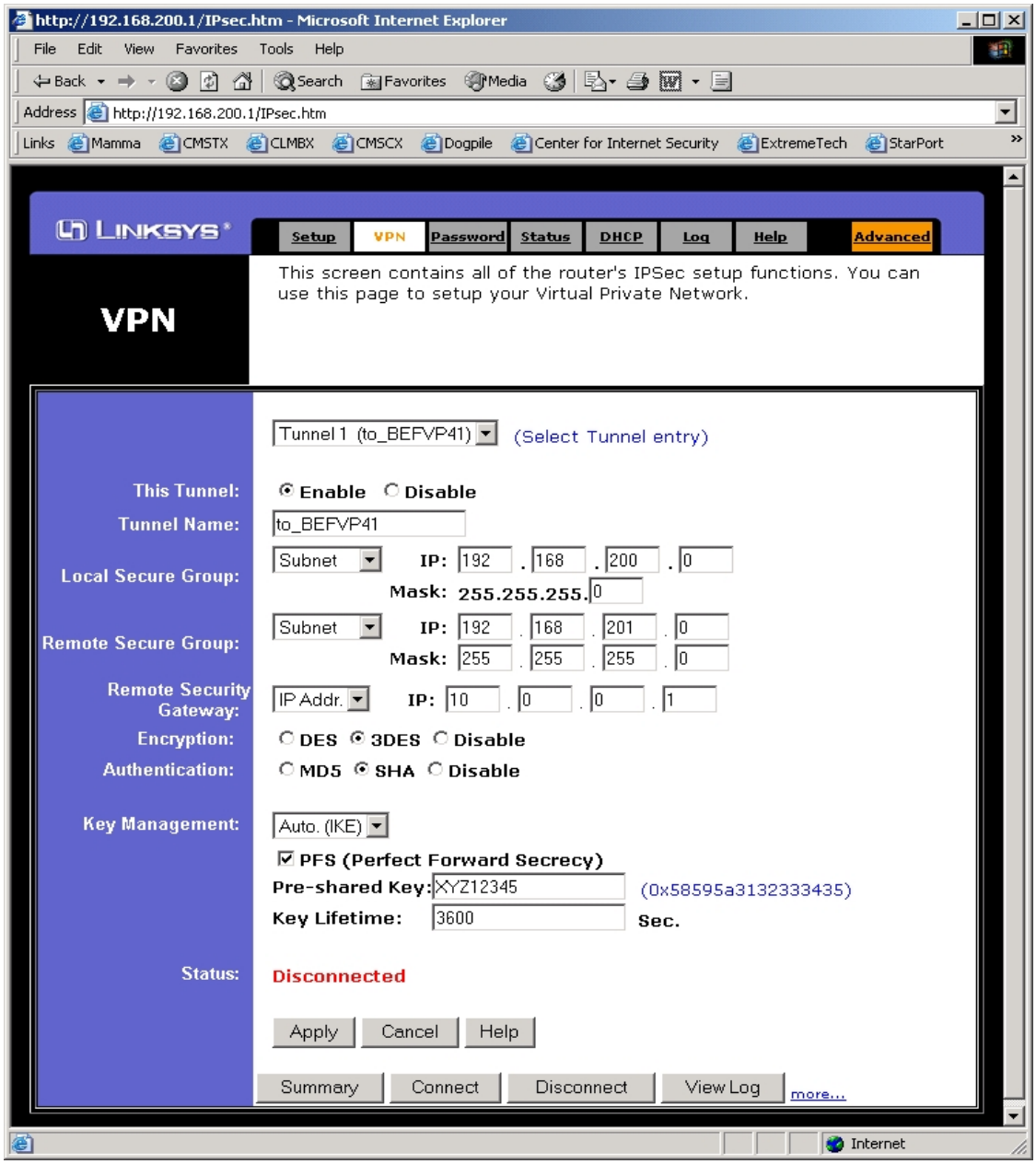

Figure 6: VPN Tunnel Setup Screen for VPN on Network A

The BEFVP41 VPN/Router is configured through a web browser (HTML) interface. You can access this interface from any computer connected to the LAN side of the device by opening a web browser and typing the LAN side IP address in the browser address field. It is important to note that if the VPN settings are configured to allow remote access, the VPN settings can be reconfigured from the WAN side of the device as well (see discussion describing Figure 11). This capability, if allowed, can be a significant security risk.

Assuming that the device is to be configured from the LAN side of the device, the default (out of the box) LAN IP address of the BEFVP41 is 192.168.1.1, which will give you initial access to the settings screens until the LAN IP address is changed, after which you can just enter the new address in the browser address field to gain access. The configuration interface is password protected, so you will be asked to enter a username and password when a connection is attempted.

The username field is ignored (just leave it blank), but the proper password is required to gain access to the device configuration utilities. The BEFVP41 ships with a default password of "admin", which will grant initial access to the device until the password configuration is changed (see the description of Figure 9). Figure 5 and Figure 6 show two of the thirteen configuration screens for the BEFVP41 VPN device connected to the network with the SEL-2030 and SEL-2701 (Private Network A in Figure 2).

Similarly, Figure 7 and Figure 8 show the same two configuration screens for the VPN device connected to the network with the SEL-387 and SEL-2890 (Private Network B in Figure 2). The Setup screen, shown in Figure 5 and Figure 7 for the two VPN routers, is used to configure the network identity of the VPN router. The chosen LAN IP address and subnet mask must be compatible with the local, private network on which the VPN is being placed. The WAN IP address, subnet mask, and gateway IP address must be compatible with the addressing scheme of the intervening network media. Your company IT manager or network technician should have these addresses.

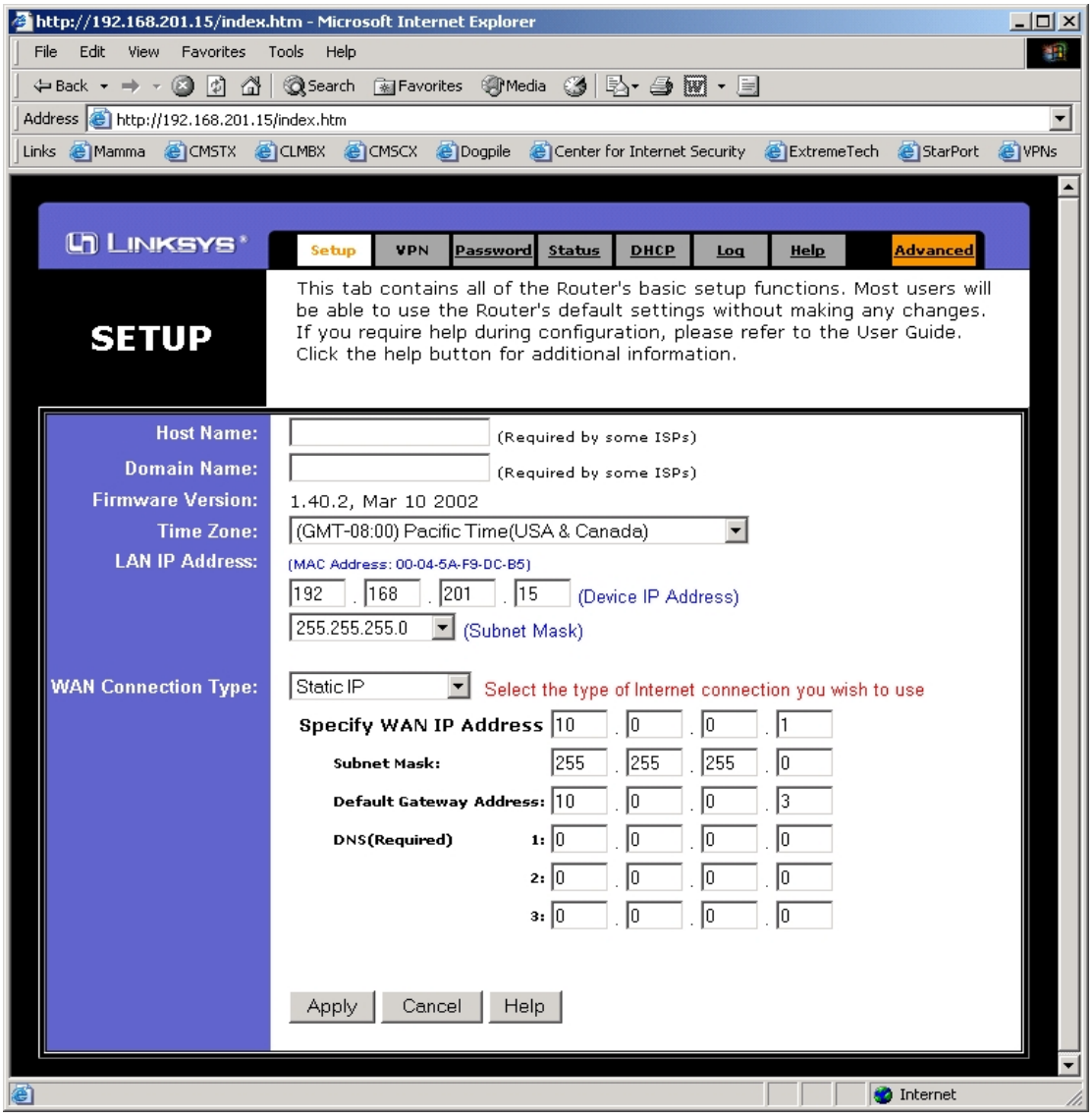

Figure 7: IP Address Setup Screen for VPN on Network B (the network with the SEL-387)

For our example, the first Linksys BEFVP41 was configured with a LAN IP of 192.168.200.1 while the SEL-2701 was configured with an IP of 192.168.200.2 so that the SEL-2701 and the LAN side of the first VPN device would be on the same network (Private Network A in Figure 2). Similarly, the second VPN device was configured with a LAN IP of 192.168.201.15 and the SEL-2890 was configured with an IP of 192.168.201.14, thus forming another network (Private Network B in Figure 2). The WAN port on the first VPN device was configured with 10.0.0.2 and the WAN port on the second was configured with 10.0.0.1. This allows both VPN devices to communicate over the intervening media via their respective WAN ports.

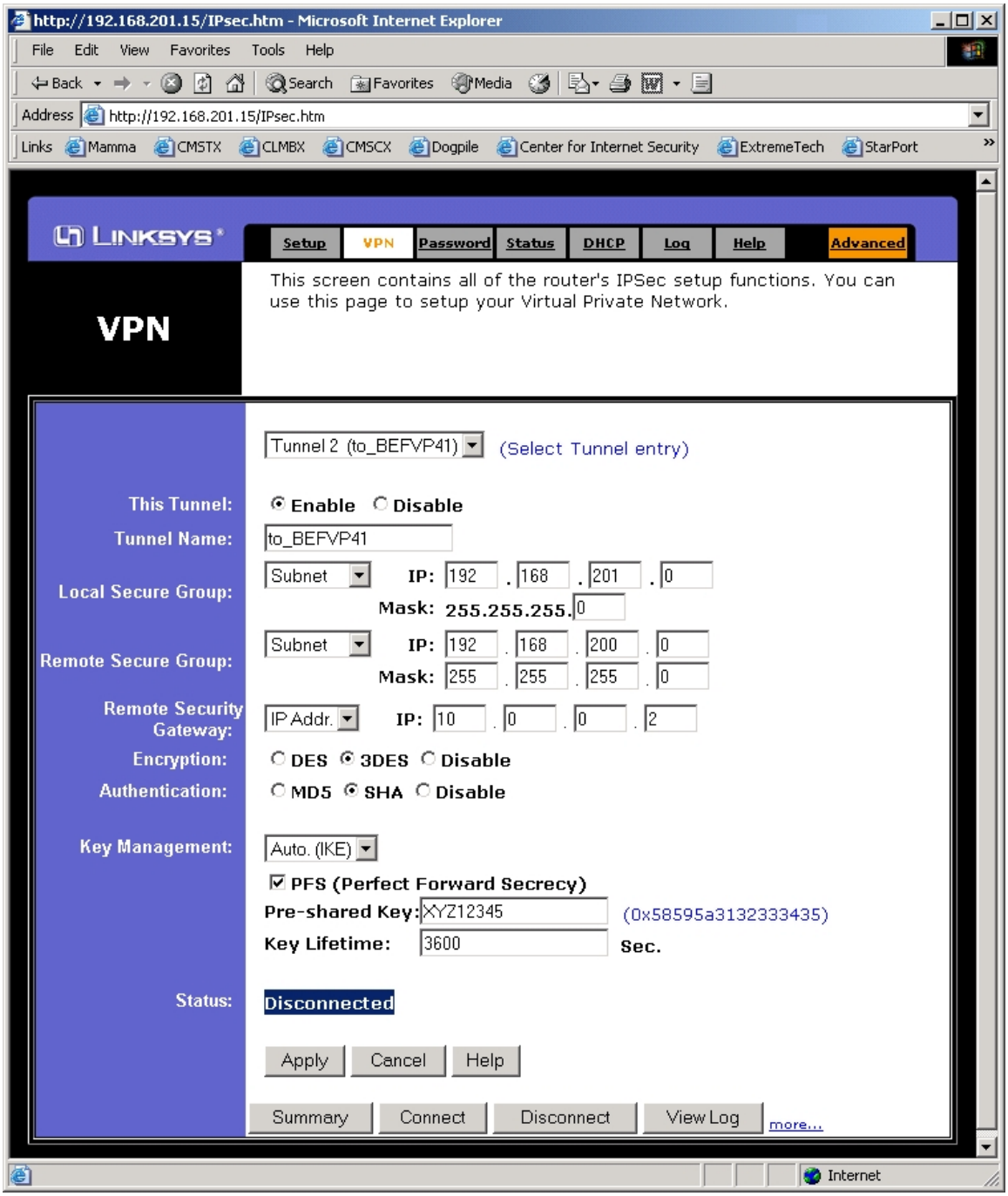

Figure 8: VPN Tunnel Setup Screen for VPN on Network B

The VPN screen, shown in Figure 6 and Figure 8 for our two VPN routers, is used to configure the encryption and tunneling settings on the VPN router. The top drop-down menu on the screen allows you to choose which tunnel you want to define and activate. As stated earlier, the BEFVP41 allows up to 70 simultaneous tunnels, each of which must be configured separately with independent settings and keys. For our example, we configure and activate only one tunnel that connects our two test networks together. Make sure that the enabled box is checked on the This Tunnel setting in order to activate the tunnel that you are about to create. The Local Secure Group setting is used to define who on the local network can send data through the constructed secure tunnel. The Remote Secure Group, on the other hand, is used to define who on the remote network can send data through the tunnel and into the local network. These settings can be an entire network, a list of IP addresses, or an entire class C network. For our example, we are securely linking the entire class C network, defined by the addresses 192.168.200.0 – 192.168.200.255, to the class C network defined by the addresses 192.168.201.0 – 192.168.201.255. The Remote Security Gateway setting is simply the WAN side IP address of the VPN device on the other side of the tunnel.

The Encryption and Authentication settings are used to choose the encryption and authentication protocols that secure the tunnel. Of the two-encryption protocols supported by the BEFVP41, 3-DES is by far the most secure (DES uses a 56-bit key, while 3-DES uses a 168-bit key). It is very important to choose the most secure settings for the VPN devices being used to protect critical equipment. For this example, we chose 3-DES encryption with SHA authentication. Finally, you should choose the Auto (IKE) (Internet Key Exchange) option in the Key Management dropdown box. This option tells the VPN to use the IKE protocol to exchange new encryption keys on a regular basis. This option is much more secure than choosing manual, or static-encryption keys. In order to use the IKE protocol with the BEFVP41 VPN, you have to specify a pre-shared key as well as a key lifetime in the settings provided. It is very important to remember that the two VPN devices on the ends of the tunnel must use the same encryption and authentication protocols, and they must have the same pre-shared key and key exchange settings.

The previous discussion covered the steps required to build a functioning secure tunnel with the BEFVP41 VPN/Router. There are many features of the VPN device that, if improperly configured, could leave your network wide open to electronic intrusion. Figures 9-13, below, show five of the BEFVP41 setup screens that should be carefully reviewed for possible security vulnerabilities prior to putting the VPN device in service. Each of these screens will be carefully described in the following sections. These figures show the settings for the VPN device on network B. Because the settings for network A are identical, the corresponding screens for network A are not shown below.

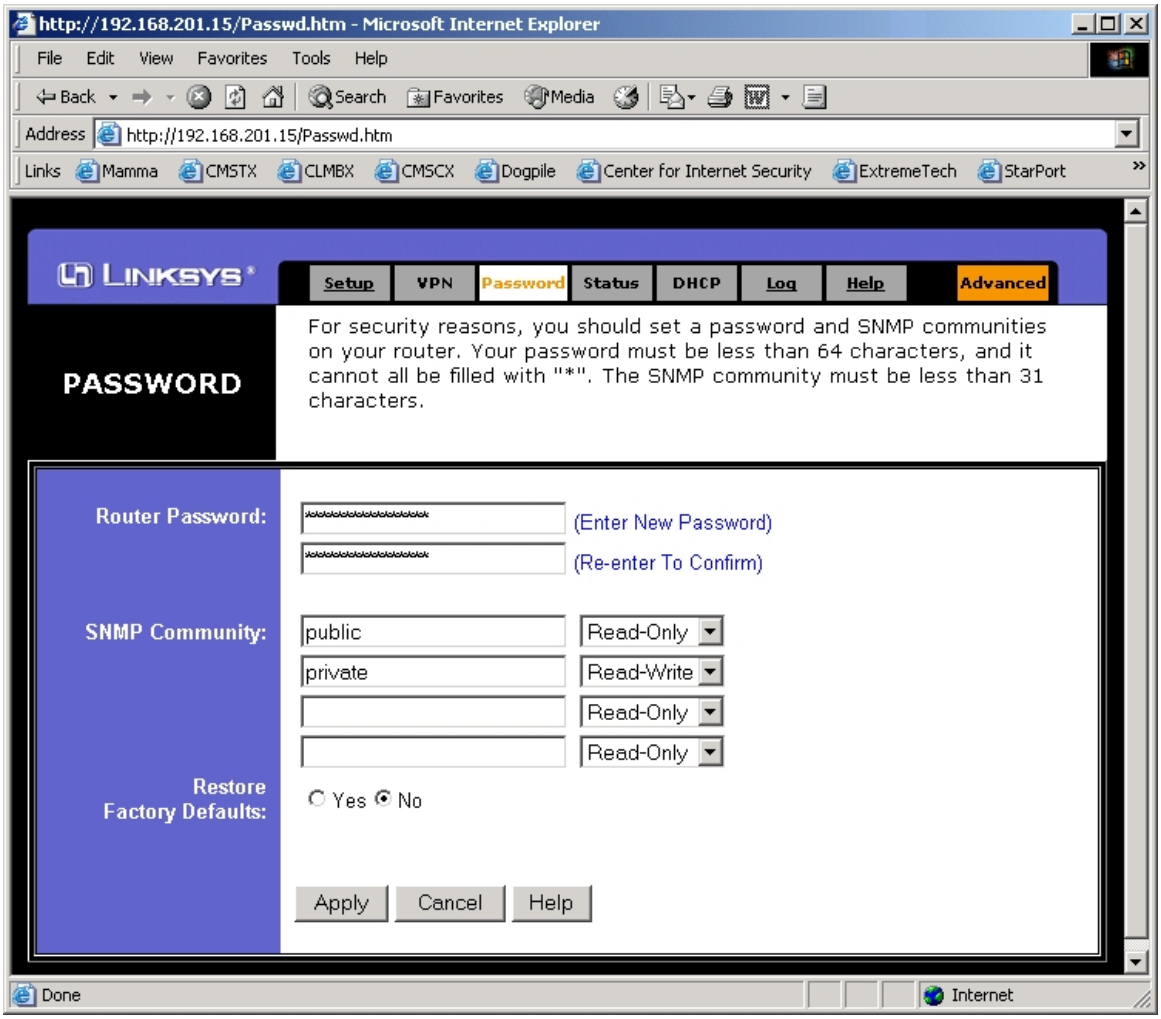

Figure 9: Password Setup Screen for VPN on Network B

The BEFVP41 VPN/Router is configured through a password-protected web browser interface. Figure 9 shows the password setup screen of the BEFVP41. The BEFVP41 ships with a very insecure password ("admin"), which should be changed prior to commissioning. To change the password, just enter the new password in the Router Password fields. Remember to use strong password practices by choosing a password that is not a pronounceable word or recognizable term [7]. Once the password is changed, you will need the new password to access the configuration utilities via the web browser. Also, make sure that the Restore Factory Defaults field is set to No. This will keep the device from restoring the factory default settings and wiping out all of the configuration changes that have been applied to date.

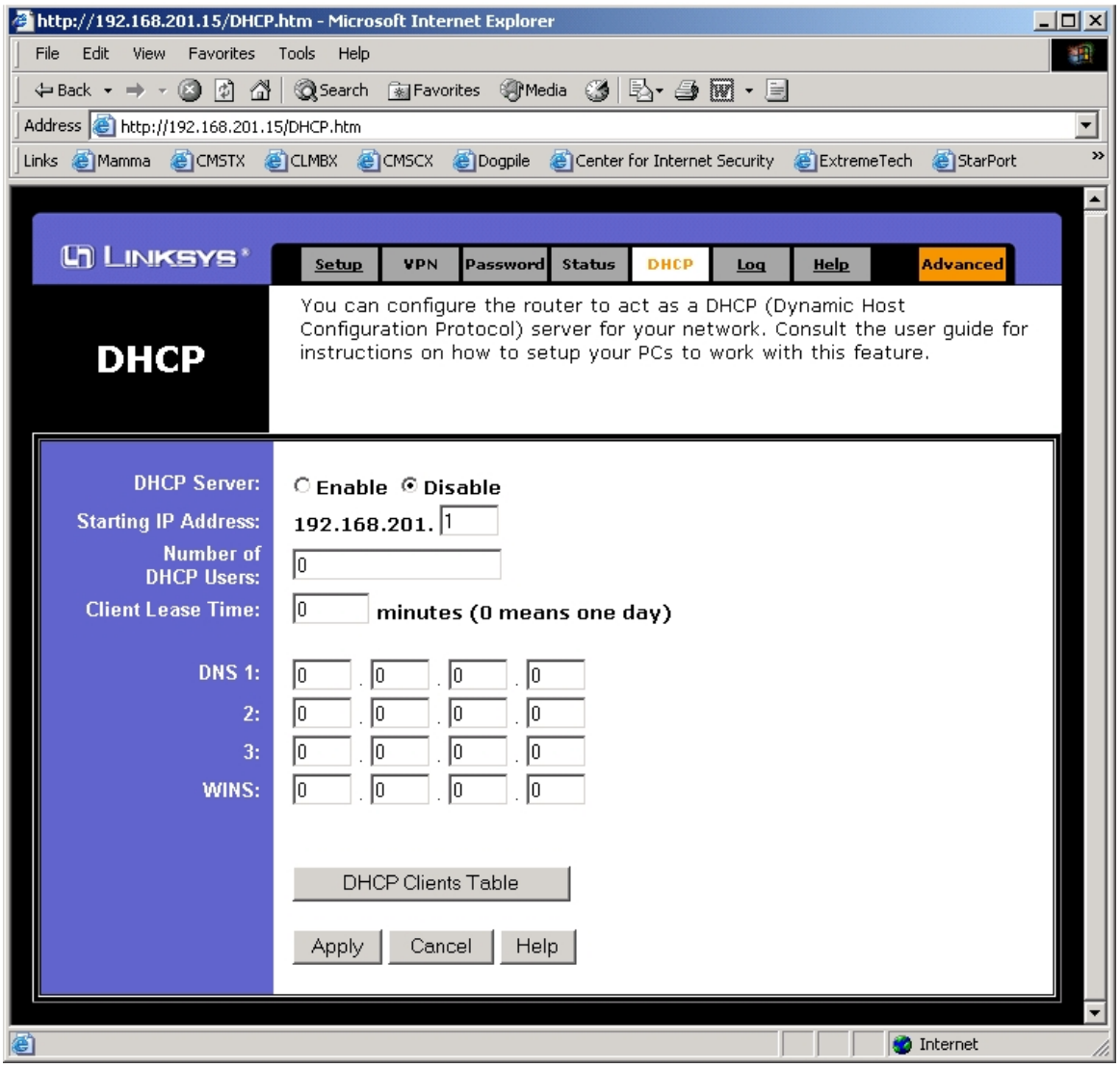

Figure 10: DHCP Setup Screen for VPN on Network B

Figure 10 shows the DHCP setup screen for the BEFVP41. For most utility applications, the private network will be configured with static (fixed) IP addresses. If this is the case, turn off the DHCP Server in the device by choosing Disable in the DHCP Server setting. This will keep the router from handing out dynamic IP addresses to new devices connecting to the network. Also note that if your private network is **currently** configured, and working, with dynamic IP addresses, then a DHCP server must already exist on the network and the server in the BEFVP41 will still not be needed. It is always a good idea, from a security standpoint, to disable all services that are not required on the network. This is especially true for perimeter devices like a VPN.

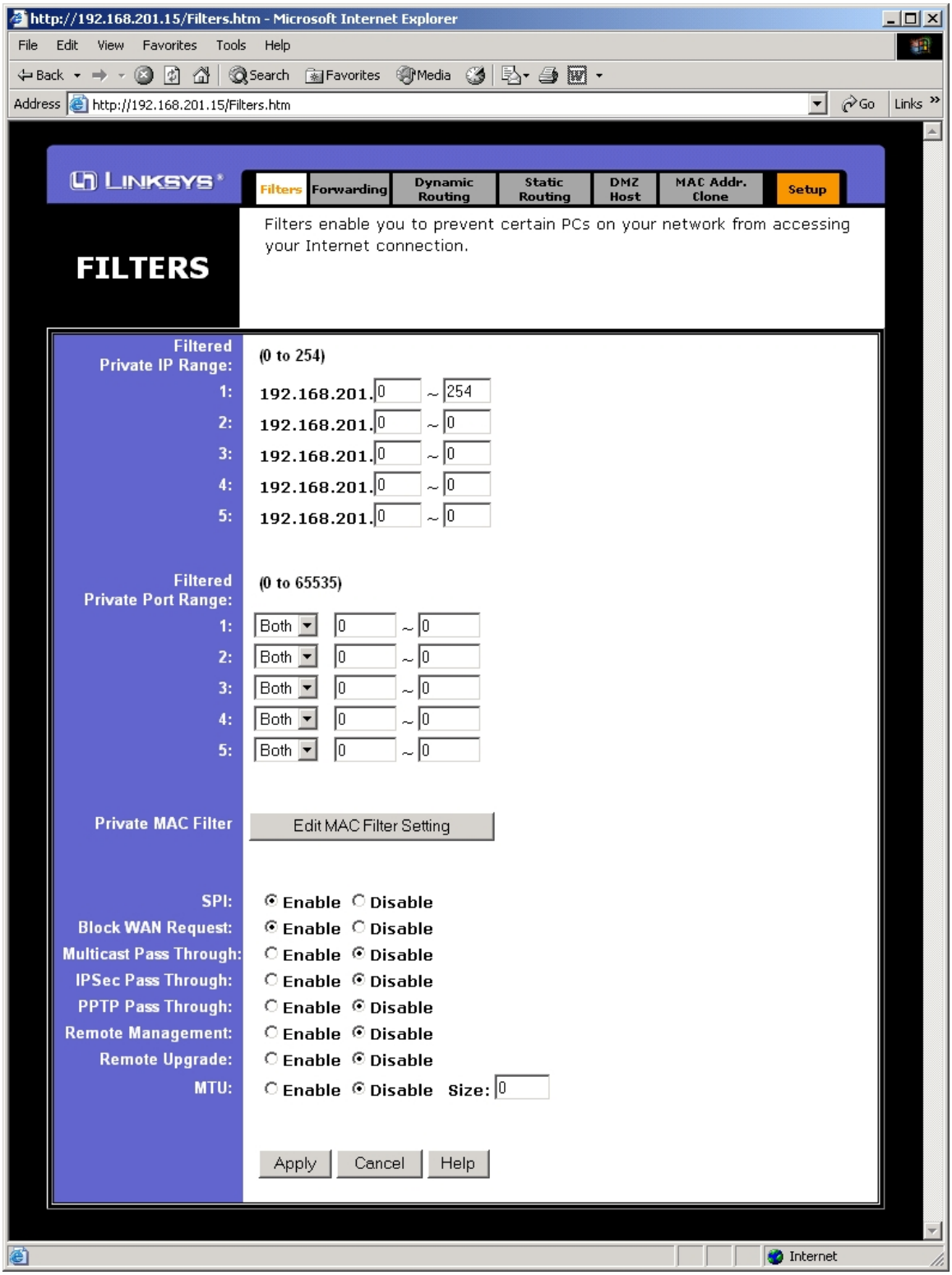

Figure 11: Ingress and Egress Packet Filtering Setup Screen for VPN on Network B

The BEFVP41 has the ability to filter traffic that **enters** the private network through the WAN connection (ingress filtering), and **exits** the private network through the WAN connection (egress filtering). Figure 11 shows the packet filter settings page of the BEFVP41 VPN/Router. The Filtered Private IP Range, Filtered Private Port Range, and Private MAC Filter fields are used to configure the egress filtering (out of the private network). It is very important to make the distinction between traffic that travels through the secure tunnel and other traffic out of the private network. The egress settings shown in Figure 11 are used to filter all traffic out of the private network that is **not** destined to addresses on the other end of one of the active tunnels. In order to maximize security in a critical utility application, all traffic out of the private network should be directed to locations for which a dedicated tunnel has been built. In other words, all traffic out of the private network should be confined to known, secure destinations. This can be done by filtering all private IP addresses by entering the range 0-254 (this represents the entire address range of the private network) in the Filtered Private IP Range field. This has the effect of blocking all traffic out of the private network that is not destined to the other side of one of the active tunnels. You can leave the Filtered Private Port and Private MAC Filter fields deactivated (default settings) because we have already confined all outbound traffic to within the secure tunnels by filtering on the IP addresses.

The buttons at the bottom of the packet filtering setup screen can be used to enable some fairly powerful security options. The SPI button should be set to Enable. This turns on the stateful packet inspection firewall, which, when enabled, will constantly monitor all traffic through the VPN device to block all suspicious traffic. The Block WAN Request button should be set to Enable. This prevents the VPN/Router from responding to connection requests from outside the secure tunnels. This will keep the VPN from responding to echo requests (Pings) and port scanning traffic that originates from sources not associated with one of the active tunnels. The Multicast Pass Through, IPSec Pass Through, and PPTP Pass Through buttons should all be set to Disable. When these aredisabled the VPN will not allow multicast and third-party encryption traffic to pass through the device. Multicast traffic is often associated with denial-of-service (DOS) electronic attacks and, as such, should be filtered from leaving the private network. The IPSec and PPTP pass-through options allow encryption traffic that originates from within the private network to travel through the VPN device. It is assumed that the BEFVP41 will provide all network encryption and that these pass-through options will not be required. The Remote Management button should be set to Disable. It is very important to make sure that remote management is never allowed for critical applications! If enabled, the remote utility screens, pictured in Figures 5-13 will be accessible to anybody on the **outside** of the private network that has the administration password. Once the VPN is configured properly, there is typically very little reason to change its settings. Because of this, it is usually better to confine the ability to configure the VPN settings to users **inside** the private network. Similarly, the Remote Upgrade button should be set to Disable because, if it is enabled, the ability to flash the firmware of the VPN/Router will be extended to those outside of the private network. This level of access is a potential security risk. Finally, the MTU fields allow configuration of the maximum packet size allowed on the network. We recommend leaving these fields at their default settings.

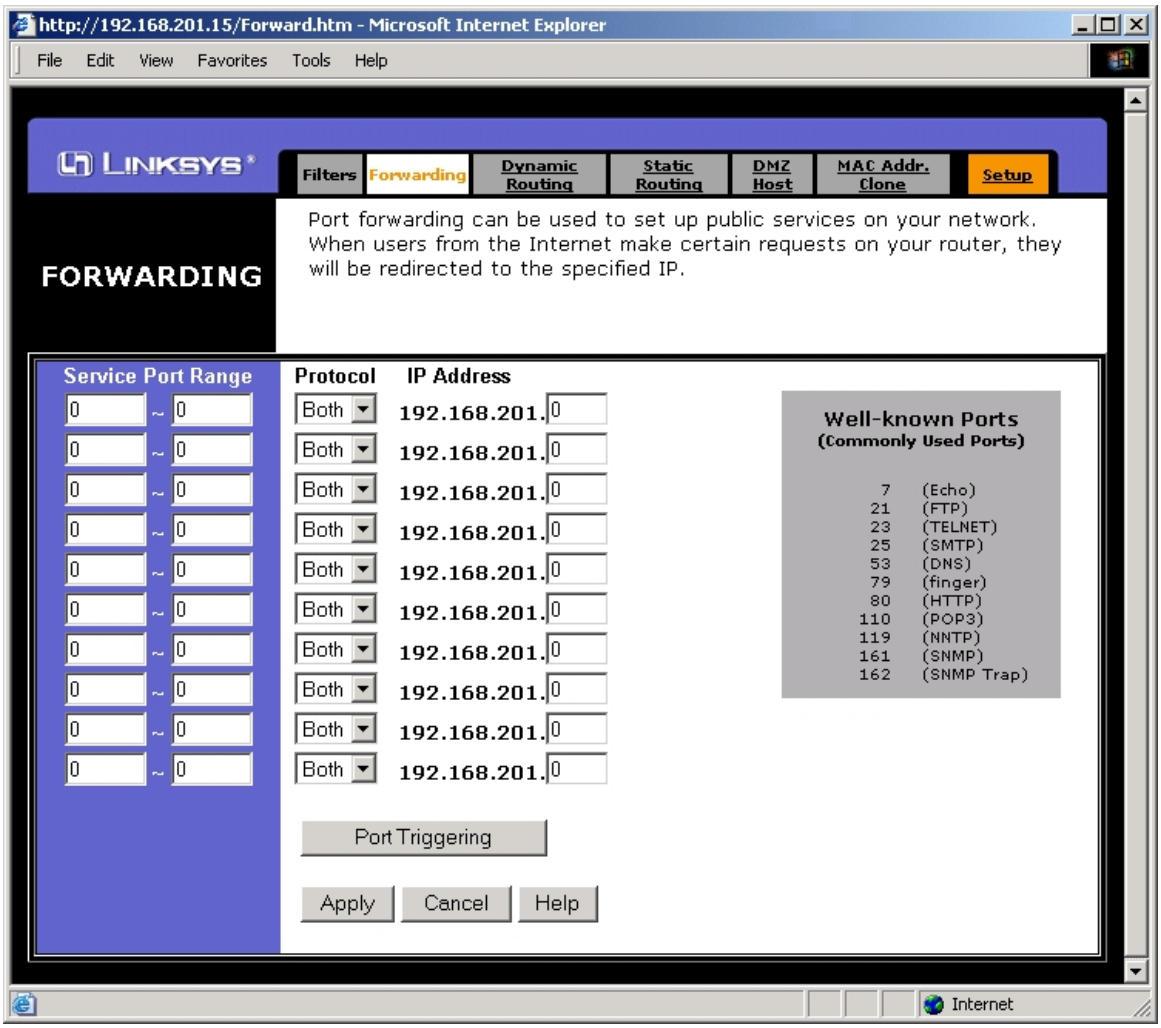

Figure 12: Port Forwarding Setup Screen for VPN on Network B

The port forwarding setup screen, shown in Figure 12, can create an insecure hole right to the heart of your private network if it is configured incorrectly. If any service ports are forwarded to a destination address within your private network, all traffic from **outside** your network (including general traffic that is not associated with one of the secure tunnels) will be forwarded to the specified destination. This is best explained with an example. If the WAN IP address of the VPN is 10.0.0.2, and the port forwarding is set to forward all ftp traffic (port 21) to the 192.168.201.5 IP address on your private network, then the device with IP address 192.168.201.5 will be directly exposed to all traffic that is directed to 10.0.0.2 on port 21 (even if it is not a legitimate ftp session). This essentially punches a hole right through the VPN device and exposes equipment within the private network to direct outside access. Because we would like to confine all traffic into or out of the private network to within the secure tunnels, this forwarding capability is both unnecessary and ill-advised. It can be disabled by entering zeros in all fields, as shown in Figure 12.

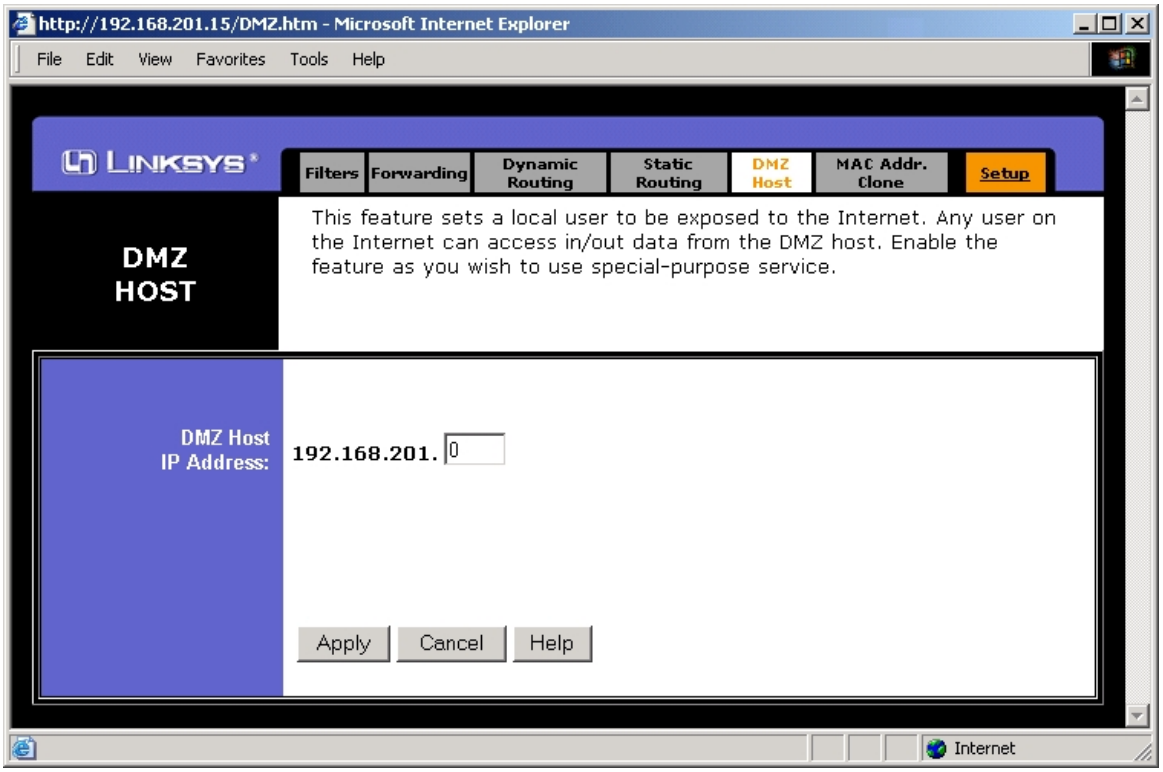

Figure 13: DMZ Host Setup Screen for VPN on Network B

The BEFVP41 VPN/Router DMZ host setup screen is shown in Figure 13. Entering a valid IP address of one of the devices on the private network will expose that device to **all** traffic that comes into the VPN. This is very similar to the port forwarding feature explained above, but the DMZ feature will forward all traffic, on all ports, to the DMZ host. This is clearly a potential security risk and therefore should not be enabled. In order to disable this feature, simply enter a zero in the DMZ Host IP Address field.

CONCLUSION

In this example, SEL has demonstrated that transparent, encrypted, and authenticated communication between SEL Ethernet networking products is possible through the use of Virtual Private Networking technology. It is important to note that there are a wide variety of VPN vendors as well as a wide variety of VPN platforms. For instance, VPN client (not gateway) software is included with the Windows 2000 and Windows XP operating systems. This software will allow a PC to communicate through an existing VPN gateway like the Linksys product used here. Furthermore, most commonly used encryption and authentication methods are standardized, so there is a very good chance that one VPN platform or vendor will successfully link to a completely different product provided the security settings are the same in the two products. For example, in our work, we were able to show that the software-implemented VPN client included in the Windows 2000 operating system was completely compatible with the hardware-implemented Linksys BEFVP41 VPN Router. In this case, both the platform (software vs. hardware) and the vendor (Microsoft vs. Linksys) were different, yet they were able to connect successfully. You will probably find that many of the settings and concepts shown in this application guide will prove useful and applicable to configuring a VPN tunnel with products other than the Linksys BEFVP41.

REFERENCES

[1] IEEE Power Engineering Society, *IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, New York, NY, April 4, 2000.

[2] National Security Telecommunications Advisory Committee Information Assurance Task Force, *Electric Power Risk Assessment*, March 1997. (see http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html)

[3] The White House Office of the Press Secretary, *White House Communications on Critical Infrastructure Protection*, October 22, 1997. (see http://www.julieryan.com/Infrastructure/IPdoc.html)

[4] U.S. Federal Bureau of Investigation, National Infrastructure Protection Center, 2000. (see http://www.nipc.gov)

[5] P. Oman, E. Schweitzer, and D. Frincke, "Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems," *27th Annual Western Protective Relay Conference*, Paper #4, (October 23–26, Spokane, WA), 2000. (see http://www.selinc.com)

[6] P. Oman, E. Schweitzer, and J. Roberts, "Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions," *Proceedings of the 2001 Western Power Delivery Automation Conference*, Paper No. 1, (April 9–12, Spokane, WA), 2001. (see http://www.selinc.com)

[7] "Attack & Defend Tools For Remotely Accessible Control and Protection Equipment in Electric Power Systems," Paul Oman, Allen Risley, Jeff Roberts, Edmond O. Schweitzer, *Texas A&M University Conference for Protective Relay Engineers*, (Apr. 8–11, College Station, TX), and the *Georgia Tech Protective Relaying Conference*, (May 1–3, Atlanta, GA), 2002.

FACTORY ASSISTANCE

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA USA 99163-5603
Telephone: (509) 332-1890
Fax: (509) 332-7990
Internet: www.selinc.com