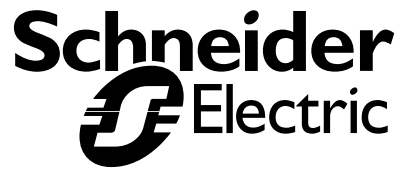


# Securing Your Automation Network

Network Services  
*Whitepaper*



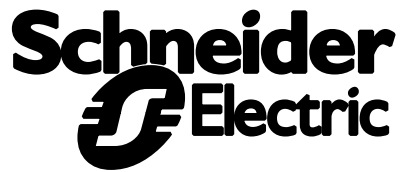


July 06, 2001

Automation Business  
Network Services

## Securing Your Automation Network

Overview	2
Security Goals	2
Logical & Physical Security	2
Transparent Factory Security	3
Routing & Switching Security	3
Virtual LAN's	5
Firewall Technologies	6
Authentication Technologies	6
VPN's & Secure Remote Access	9
IP Security (IPSec)	11
Remote Access Services	12
VPN / RAS Cost Comparison	13
Summary	14



## **Overview**

This paper covers the importance of securing automation devices for access internally on an Intranet, or externally over the Internet. Choosing an Ethernet Fieldbus offers the competitive advantage of speed, flexibility and accessibility though steps should be taken to secure automation devices and any associated programming workstations and servers. This paper seeks to educate the Controls Engineer on security strategies, technologies and options available.

## **Security Goals**

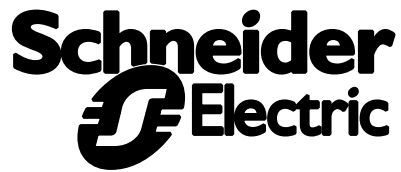
Once Automation devices and the computers used to program them share a topology model and communications protocol similar to PC's, (TCP/IP), concerns arise over accessibility from unauthorized parties. Methods of security can range from technologies based within the infrastructure itself such as physical connection paths and virtual LAN's to hardware/software based devices such as firewalls and security management servers. A comprehensive Security Plan exists for both internal and external protection. Preserving the integrity of the network by preventing unwanted traffic from unauthorized sources, securing the programming logic and preventing intrusion are essential elements of such a plan. With a secure network, engineers can then reap the benefits of access to devices for programming, service or information.

## **Logical & Physical Security**

Having no physical connections to the corporate network or the Internet is clearly the most secure option, however it isolates the devices from the very value-added resources that an ethernet fieldbus offers. For that reason, this paper will address the integration aspect of the ethernet fieldbus.

An often-overlooked security measure is physically securing switches and wiring closets. Measures such as enclosing devices in a lockable cabinet or closet where possible and limiting access to authorized persons is a simple method to prevent tampering or accidental de-coupling of a device link. Note as well that physical access to a device may allow an unauthorized person to destroy configurations, returning some switches to factory defaults, by cycling power while depressing certain switch buttons. It makes sense to secure a backup copy of these configurations via TFTP, (Trivial File Transfer Protocol; a feature found in many switches), each time a change is made. This is not only a security measure, but a recovery measure should the device fail and require replacement.

Another method of easily securing infrastructure devices such as switches is password protection. Out of the box, most switches may be accessed via a serial DB9 console connection. This management interface is used for example, to assign an IP address for remote TCP/IP based Telnet management.



Default passwords for OEM switches may be standardized across the entire product line and are published both in the documentation and on the web. Many users, including IT organizations fail to change the default passwords and permissions. Should an unauthorized user reach an unsecured switch via serial console, or via Telnet, they may be in complete command of the switch with the ability to destroy configurations, disable ports etc.

It is evident therefore, that even without an ethernet connection to the corporate LAN or Internet, that physical security and password protection should be part of everyone's security plan.

## **Transparent Factory Security**

Web enabled devices such as ConneXium<sup>®</sup> switches and FactoryCast<sup>®</sup> modules etc. have extended functionality with graphical interfaces, web hosting, and Java/ActiveX controls. Once installed on your network, it is advisable to change the default password on the ConneXium via v.24 serial or ethernet. For a FactoryCast module, follow the instructions in Chapter 3 of the NOE manual. Instructions are available on how to change the default FTP password and create additional user ID's as necessary to restrict web services to Authorized users only.

Programming tools such as Concept and SCADA programs such as Monitor Pro can also be configured to have varying levels of access to user logic and other components.

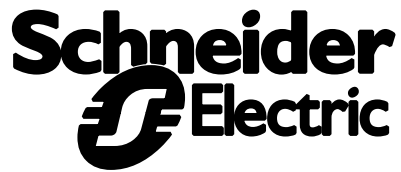
Devices such as some Schneider Automation CPU's are equipped with keys to allow the CPU to be started/stopped, and to protect the internal memory. These keys should be removed and distributed to authorized personnel.

Particularly in large environments, documenting code changes, device changes, and infrastructure changes, and cabling identification is key to maintaining devices and programs which may be infrequently visited for service.

## **Routing & Switching Security**

As the sophistication of the Automation Ethernet network grows, features once found only in enterprise class devices are finding their way into daily use at the workgroup level. Access Control features can be configured in some switches and routers to allow only specific workstations to access a device or pass through to a target. These features include Virtual LAN implementation, port security, password implementation, and Access Control List filtering on supported switches and routers.

*Note that some of these technologies may or may not exist to some degree depending on the OEM and switch model chosen. Many may also require specialized skills and knowledge to configure and administer.*



### Physical Security

Physical security is crucial to a secure operating environment. Switches and routers must be held in place in a secure and sturdy fashion (preferably installed in a rack or enclosure in a secure area). Network equipment is usually equipped to be restored to factory defaults should a password be forgotten. This could be problematic should an unauthorized person gain physical access to the network equipment. This is the reason that all ports including console and auxiliary ports should be secured by a lock and or enclosure. The location must also be secured by some sort of locking mechanism so that no unauthorized party may gain physical access.

### Port Based Security

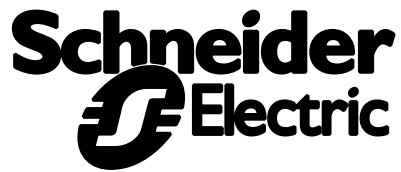
Port security on a switch can prevent unauthorized users from plugging in devices, such as workstations or printers. Such devices could disrupt the Automation network by introducing excessive amounts of traffic and possibly errors. Administratively disabling unused ports will not allow any traffic to pass should such a device be plugged in.

Additionally, port based hardware address (MAC Address) management may be used on a switch in order to deny access to a non-authorized device (the port will not provide service if a non-configured MAC Address is sensed). This can also be used as a precaution to make sure that none of your users has connected a hub to allow more than the allotted number of workstations and or devices per port. Note that if a device is replaced with one having a different MAC address, the port assignment must be appropriately re-assigned by the administrator.

Access Lists can be utilized on supported switches and routers to permit or deny users from gaining access to specific network devices or specific resources on network devices. This is commonly known as packet and service filtering, and is placed on certain interfaces. It should be noted that using access lists ties up processor resources and also needs to be locally administered on each interface within each routing device. This makes access lists not always the most optimal way to secure resources. Proper setup by professionals is crucial when using these filtering devices. Improper setup could render the network inoperable.

### Access Control Lists

An example of Access Control List implementation would be that if user John Doe has to program a device. John is a programmer and thus we need to be able to let him have access to program the device, but we do want to restrict John from accessing the device via web browser. To accomplish this we would create an Access Control List stating that if the source IP address equals that of John Doe's workstation, and the destination IP address equals that of the device, and the destination port equals 80, then deny access to the device. Port 80 is the port a web browser would use to connect to any http host. However, if John Doe were to attempt the same connection on port 502, the Modbus TCP port, he would be allowed to do so.



## Virtual LANs

Virtual LAN's, (a grouping of ethernet ports on an IEEE 802.1Q compliant switch, or a grouping of switches), may be used to help isolate packet and broadcast traffic on the Automation network from the IT network. Such measures are generally reserved for isolating extraneous traffic such as broadcasts which may interfere with control communications, but can be implemented as a sort of security tool. Switches can be divided into VLANs that could render devices on separate VLANs unreachable. The downside to switch port based VLANs as a security strategy is management, a port can belong to multiple VLANs extending across multiple switches. Multi-layered VLANs can be challenging to administer as a single port may belong to many VLANs. For multiple VLANs to span multiple switches, the Spanning Tree Protocol, STP, may have to be disabled as well. For example, if there exists on each of two switches, two VLAN's, VLAN1 and VLAN2. And each VLAN needs a connection to the corresponding VLAN on the other switch, there would have to be two links between each switch, one for each VLAN. STP will disallow multiple links between devices to prevent loops.

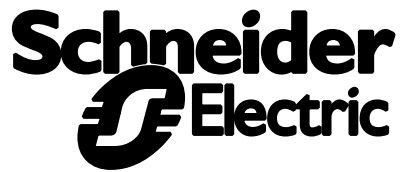
VLANs can be used to segment broadcast domains within a network. VLANs are logically segmented local area networks; thus physical areas do not restrict them. Utilizing VLANs reclaims network bandwidth by breaking down broadcast domains, and segments one network of devices from another within the same switch. VLAN segmentation is accomplished by assigning the ports of a device into separate VLAN memberships. For example, ports 1 & 2 may be assigned to VLAN1. Ports 3 & 4 may be assigned to VLAN2. Ports 1 & 2 will not see broadcasts or traffic from ports 3 & 4, and vice versa. This separation is accomplished at OSI Layer 2. If a third VLAN were created using ports 1,2,3,4 & 5, a device on port 5 would see all broadcast traffic from ports 1,2,3 & 4.

An implementation example would be if an administrator wanted to separate traffic from office PC's from PLC or SCADA devices. As these devices may not normally communicate with each other, separating them via VLAN would allow the two networks to co-exist on the same switch.

Other configurations can be implemented in order to conserve bandwidth for Automation devices. Such settings include whether or not to pass or block multicasts, and rate limit broadcasts. Other technologies such as Quality of Service (QoS), IEEE 802.3p can prioritize packets on 7 levels by setting 3 bits in the packet header. This allows traffic types or port assignments to have a higher priority should a bottleneck occur and can be very useful to prioritize Automation traffic over that of office PC traffic. Though not specifically a security measure, it does preserve the integrity of the Automation network.

## Firewall Technologies

A firewall is a device that is implemented on a network in order to provide security from potential intruders.



A firewall can have more granular control over what can and cannot be accessed from outside the secure network than an access list can provide. A firewall can be a network appliance or a piece of software on a stand-alone server or router equipped with multiple network adapters or interfaces. A firewall provides this granular control by using its own protocol stack, and depending on the firewall, it checks each level of the stack for erroneous information.

Network appliance firewalls are a bundled, ready-to-run single purpose computer that provides an operating system and firewall application. The device is tuned for service as a firewall and is managed from a secure workstation "inside" the firewall. These may be helpful to enterprises as a self-contained solution.

Other firewall OEM's that provide software that installs onto an existing PC or UNIX workstation with multiple network adapters dedicated to this task. In both cases, some providers offer add-on software and hardware modules for Remote Authentication and encryption/decryption accelerators for improved performance. These configurations may be helpful to enterprises that require scalability, more interfaces, etc.

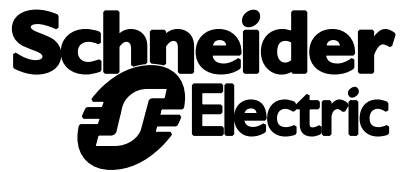
A firewall works by examining each packet that passes between the two adapters and comparing Access Rules at several different levels before allowing that packet to pass. Once a packet has been validated by all of the requirements to pass through, the firewall applies Network Address Translation (NAT). Network Address Translation is used to hide the internal network IP addresses by substituting the actual source address with the outside address of the firewall. This acts to hide the original internal address of the sender that is inside the firewall.

Firewalls allow filtering on MAC Addresses, IP Addresses, Port Numbers, or even certain commands and Services. Each firewall offers a different level of security depending on vendor, cost, etc. Selecting and implementing a firewall into any infrastructure requires research, planning and feature/cost comparison. Each vendor offers different features including VPN authentication support, logging, more memory, and performance classes. (The more security checks performed the slower transactions will take place).

Additionally, some Firewall Management suites allow rules to be downloaded and applied to other network devices in the organization such as routers that may be internal or external.

## **Authentication Technologies**

Password management for devices can also become an issue. Therefore server platforms are available to centrally administer passwords. These services include RADIUS, (Remote Authentication Dial-In User Service), and TACACS/TACACS+ (Terminal Access Controller / Access Controller System). These services allow the secure centralized maintenance of logins and passwords. Access to a device, network or resource such as a server can be centrally administered on such a server. When users request access to a device, the users' credentials are checked against a database on that server for permission. Rules in



place will allow or deny the user access.

Authentication is the process where a network user establishes an identity. Verifying the identity of a user requires at least one of three authentication factors: a password, a smart card, hardware or software token, or a biometric. A password or Personal Identification Number (PIN) is something a user knows and does not require any hardware. However, a smart card (or another token such as USB token), SecurID FOB, or a biometric (or fingerprint), is something the user has. This requires the deployment of a device, whether it is a peripheral or integrated into the workstation. Smart card and USB tokens, which are things you possess require readers. Biometrics require a scanning device, whether it is a camera, microphone or specialized device such as a fingerprint reader. While authentication techniques vary, they are similar in that the passwords are generated by authentication devices and cannot be reused by an attacker who has monitored a connection.

#### Password Authentication

Passwords are the most commonly used method of using confidential knowledge to authenticate users. Easy to administer and convenient for most users, passwords are also the least expensive method of user authentication. The following are characteristics of strong passwords:

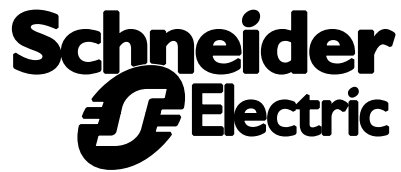
- 6 to 8 characters in length
- Not formed from personal information
- Not a word found in a dictionary or list of names
- Mix of letters and numerals
- Mix of upper and lower-case letters

Unfortunately, passwords have some drawbacks. Often, users select passwords that are obvious, short and simple, which make them easy to guess. This problem is usually solved by implementing the above password rules that may require a certain password length or include capital letters or numbers, and may force users to change passwords on a regular basis. These rules though may make passwords even harder to remember, which leads some users to write them down and compromise the original goal of security.

Even with password rules in place, passwords can still be shared between users who want more convenience, which can make the system more vulnerable. In addition, passwords can be stolen by monitoring keyboard keystrokes or network traffic, by tricking individuals into revealing their password, by guessing at them, or with brute force methods such as dictionary attack utilities.

#### Smart Cards and Token Authentication

A stronger way to authenticate users is to provide them with tokens that contain a digital code that acts like a key. A smart card or token authentication, for example, generates a response that the host system can use in place of a traditional password. Since tokens or smart cards work in conjunction with software or hardware on the host, the generated response is unique for every login. The result is



a one-time password that, even if monitored, cannot be re-used by an intruder to gain access to an account.

Smart cards are one way to provide strong authentication of users. Smart cards and intelligent tokens are similar in size to a standard credit card embedded with an integrated circuit chip. The card itself is the item that the user must possess. Smart cards are inserted into a card reader as part of the authentication process. They often contain a digital certificate and they are usually presented in combination with a password or PIN. They are used in different applications that require strong security protection and authentication. All of these applications require sensitive data to be stored in the card, such as biometrics information of the cardholder, personal history, and cryptographic keys for authentication, etc. For example, when a user presents a smart card to a reading device such as a computer, the computer reads the PIN and writes it to the smart card. Only if the PIN matches will the smart card allow the other information it contains to be accessed by the computer.

Smart cards can work with PKI (Public Key Infrastructure) systems by writing the private key of the person on the card. The smart card not only acts as storage for the key, which can be read into any computing device used by the person, but also connects the person with his private key. For an instance, your credit/debit bank card. Physical possession of the card plus knowledge of the PIN allow access to the private keys, assuring that this key really does belong to the cardholder. The private key can then be used to form digital signature to messages sent by user working with this computer.

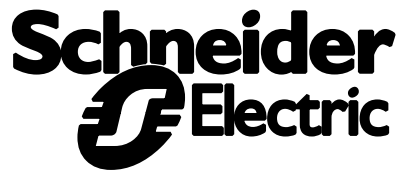
Tokens are a very cost-effective and popular method of delivering authentication when combined with knowledge factor to achieve dual-factor security. Tokens represent a stronger method of user authentication than knowledge factors alone because they can be combined with factors of user authentication: possession (the token) and knowledge (the password or PIN). Tokens that are used to access computer networks include RSA SecurID tokens, USB tokens, and proximity tokens.

RSA SecurID tokens are available as both hardware and software tokens. These tokens generate a different 6-digit code every sixty seconds. The code is know only to the token and the access control unit. As an added level of security, these tokens are combined with a PIN. Because the code changes every minute, it is impossible for a hacker to record the code and re-use it later to login to the system.

USB tokens are small hardware devices that can be plugged into a USB port on a computer. They are also used in conjunction with a password or PIN.

Proximity tokens use radio signals to deliver unique codes to access control units. These tokens do not need to be placed into a reader or plugged into a port. Remote keys for unlocking and locking vehicle doors are a type of proximity token.

Smart cards and tokens can both be lost or stolen, and users must remember to have them in their possession, which means smart cards and tokens, are somewhat inconvenient. They can be difficult to manage because they must be issued and tracked. As result, they are more expensive than simple passwords to implement and manage.



### Biometric Authentication

Biometrics is the strongest single approach to achieving user authentication. This involves the analysis of a unique physical attribute of a person. Biometrics that are used in strong user authentication can be more convenient than a password. Passwords are easily forgotten and have a tendency to proliferate; whereas fingerprint data is proprietary, cannot be guessed, and does not need to be memorized. Moreover, a user can present and process their fingerprint in about the same amount of times it takes to type in a password. Biometrics authentication factors include fingerprint scans, retinal scan or iris scans, voice recognition, and facial recognition. There are many other types of biometric authentication factors including hand geometry systems, DNA systems, and signature/typing patterns.

Biometric factors represent the strongest form of user authentication because they can not be lost or stolen, shared or forgotten. However, biometric factors are prone to three types of error:

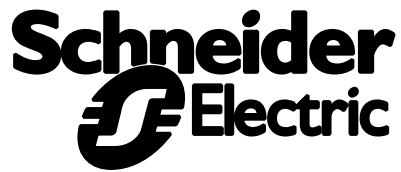
- False rejection of a person's physical attribute. In another word, the system does not recognize the biometric even though it is valid.
- False acceptance of a person's physical attribute. In this situation, the system accepts the wrong person.
- Failure to enroll a person's physical attribute. Obviously, a person without hands cannot make use of the fingerprint system, but these types of problems may be even more subtle. For example, a beard might prevent a user from using a facial recognition system, exceptionally dry skin can confuse a fingerprint system and a speech impediment can render a voice recognition system useless.

Although a higher level of security is achieved with stronger user authentication, users may face more inconvenience as a consequence of enhanced security. They may be required to keep cards or tokens in their possession, or they may have to present their identification more than once, which may frustrate some users.

Biometric information has been used for example at the Super Bowl to scan the facial features of attendees to locate persons with outstanding warrants. It is also under consideration at some law enforcement organizations to scan facial features of Driver's License holders from DMV records.

## **Virtual Private Networks and Secure Remote Access**

As more and more corporate workers find themselves on assignment outside of the office, the need for remote access continues to increase. Remote access servers (RAS) and virtual private network (VPN) are two technologies that offer remote access service. Remote access is vital to organizations for Sales, Support, Branch Offices, and off-site partners. With RAS, a remote access client uses the telecommunications infrastructure, (dial-up) to create a temporary physical circuit with a port on a remote



access server. Once the physical or virtual circuit is created, the rest of the connection parameters can be negotiated. With VPN, a VPN client uses the Internet to create a virtual point-to-point connection with a remote VPN server. Once the virtual point-to-point connection is authenticated and created, the rest of the connection parameters can also be negotiated. Although RAS has proven popular, many businesses are looking at low-cost VPN to perform the same functions and therefore reducing telecommunications costs. For additional security, the RAS server can be configured to call back users at a predefined number. This works well for static users but not for mobile users.

#### Virtual Private Networks (VPN)

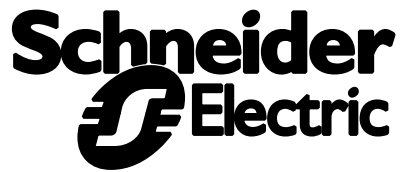
A VPN can be defined as a means for using the public network infrastructure, such as the Internet, to provide private, secure access to applications and corporate network resources for remote employees, business partners, and customers. With a VPN deployed across the Internet, virtual private connections can be established from almost anywhere in the world. VPN technology enables company offices or individuals in different locations to securely access a central network without having to dial directly into the company network. Additionally, telecommunications costs are reduced as the corporate network and the remote user need only to connect to their local Internet access points or POPs (Point-of-Presence), rather than dial long distances, and perhaps for long periods of time to a central RAS server.

A VPN uses a secure tunneled connection, allowing only authenticated users access to the corporate Intranet. With tunneling, each message packet is encapsulated or "wrapped" within an IP packet for transmission across the public network via an encrypted "tunnel". Encapsulation is presented at the security server or firewall. Upon authentication, the packet is then decoded and unwrapped for forwarding to the destination host.

Currently, there are a handful of VPN protocols rising to the surface in the industry – namely L2TP, IPSec, and SOCKS 5. These protocols provide tunneling functions and they are the building blocks used to create VPN links. Some of the protocols overlap in functionality, and offer similar but complementary functionality.

Layer-2 Tunneling Protocol (L2TP) is the combination of Cisco Systems' Layer-2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP supports any routed protocols, including IP, IPX, and AppleTalk. It also supports relevant WAN backbone technology, including Frame Relay, ATM, X.25, and SONET.

One key to L2TP is its use of PPTP. PPTP is a method for sending network packets over an existing TCP/IP connection (called a tunnel). A VPN requires that the client and server each have an active Internet connection. The server typically has a Permanent Virtual Circuit, (PVC), and connection to the Internet. The client connects to the Internet via Dial-up, PVC, SVC, (Switched Virtual Circuit), to an Internet Service Provider (ISP) and initiates a PPTP connection to the PPTP server over the Internet. The connection request includes access credentials (such as username, password, and domain), and an authentication protocol such as Microsoft Challenge Handshake Authentication Protocol, (MS-



CHAP). A VPN connection exists between the server and client only after the PPTP server authenticates the client. The PPTP session acts as a tunnel through which network packets flow from server to client or vice versa.

The L2F portion of L2TP lets remote clients connect and authenticate to networks over ISP and NSP links. Beside the basic VPN capability, L2TP can create multiple tunnels from a single client. For instance, the remote client can connect to the corporation database application and to the company's Intranet simultaneously.

## **IPSec**

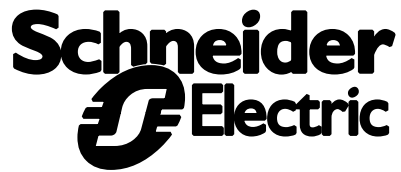
IPSec is a popular and widely supported standard set of protocols and encryption methods for creating a secure session between IPSec gateways. IPSec uses an Authentication Header, (AH), and Encapsulating Security Payload, (ESP) service. These services provide integrity of the frame and authentication of the origin. They also prevent re-playing the frames should an intruder intercept them. Encryption keys may be distributed manually by the administrator or automatically by services such as Internet Key Exchange, (IKE).

With IPSec, only the sender and recipient know the security key. If the authentication data is validated, the recipient knows that the communication came from the sender, and that it was not changed in transit. However, IPSec does not specify a proprietary way to perform authentication and encryption. For instance, IPSec can perform the encryption negotiation and authentication, while an L2TP VPN receives the internal data packet, initiates the tunnel, and passes the encapsulated packet to the other VPN end point.

Another approach to VPNs is SOCKS 5 that is a bit different from L2TP and IPSec. SOCKS 5 follow a proxy server model and works at the TCP socket level. To use SOCKS 5, client system must have SOCKS 5 client software and the server must have SOCKS 5 server software.

Here is how the SOCKS 5 model works. First, the SOCKS 5 client intercepts a client request for services. The request is sent to the SOCKS 5 server, which checks the request against a security database. If the request is granted, the SOCKS 5 server establishes an authenticated session with the client and acts as a proxy for the client, performing the requested operations. Because it works at the TCP level, SOCKS 5 lets you specify which applications can traverse the firewall into the Internet, and which are restricted.

Virtual Private Networking (VPN) solutions may be a combination of many different technologies such as encryption, user and data authentication and access control techniques working together to deliver a VPN solution that protects data privacy and ensures appropriate access control. The key technologies that comprise the security component of a VPN are authentication, data encryption, user access control, and event logging.



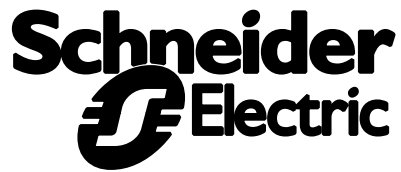
- Authentication – Authentication is needed to verify the user's identity as well as the integrity of the data. User authentication requires a remote user to authenticate himself to a server and the server to authenticate itself to the remote user. Data authentication provides assurance that a message has not been changed while in transit between the sender and the receiver.
- Data Encryption – Encryption is to protect the privacy of data. While the encryption process must be strong enough to ensure that private information sent over the Internet remains private, it must also be implemented in a way that does not significantly affect network performance. A standard developed for Government use, DES, (Data Encryption Standard), utilizes a 56 bit key. TripleDES uses 3 – 56 bit keys for 168-bit encryption.
- User Access Control – Access control is a way to guarantee the security of network connections. It also provides a remote user access to private LAN resources and does not imply the user should have access to the entire network. Different users have different needs; so their access privileges should be set accordingly.
- Event Logging – This log records important events such as adding or deleting a user and session start and end data. One of the most important events to track is a unsuccessful user login attempt. The log can also help to track an unauthorized user.

## Remote Access Services

A remote access server (RAS) is a stand-alone device that allows remote users, at home or on the road, to dial into and access services on the local network as if they were in the office. Remote access servers typically offer async serial interfaces connected to external analog modems, ISDN terminal adapters, or direct analog/ISDN connections. Remote Access Servers are application-specific computer systems that specifically support LAN to WAN connections.

Proprietary remote access servers are designed to handle a mix of protocols and remote node capabilities, and some offer remote control capabilities. Clients dial in using Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) encapsulation while the RAS handles the user's attachment, control and protocol assignment.

Remote access services typically offer security, providing the authentication of a user by ensuring that they have an account on the network and the proper password. Industry standard security features such as PAP (Password Authentication Procedure), CHAP (Challenge Handshake Authentication Protocol) and other feature-enhanced proprietary authentication capabilities are common. Manufacturers now support many industry-leading security software products such as RADIUS (Remote Authentication Dial-In User Service), further expanding their security options. RAS security features include password encryption using different forms of authentication protocols, data encryption to maintain security in case of unauthorized interception of remote access



transmission, and callback security to predetermine a client's number before allowing access to the network.

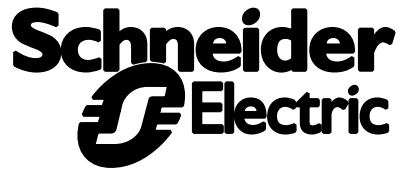
The following steps show what happens during a call from a client to RAS server:

- Through Dial-Up Networking, a client dials a Remote Access Server.
- The server sends a challenge (requesting a username and password) to the client.
- The client sends an encrypted response to the server.
- The server checks the response against the user database.
- If the account is valid, the server checks for Remote Access permission.
- If Remote Access permission has been granted, the server connects the client.

## **VPN and RAS Implementation Cost Comparison**

VPN and RAS both serve the purpose, providing organizations LAN access to remote communities of interest. The most important differences between VPN and RAS are the client/server software and the communications access. RAS client/server software may not include authentication, encryption, and access control options in older systems. This means that information is not secure during transmission. However, there are important differences between these two technologies in performing this function, including:

- **Communication costs** – Using a VPN, remote users place a local call to their ISP (Internet Service Provider), then connect to the company gateway or firewall for authentication. Once validated, they will have a secure tunnel to the corporate LAN via the Internet. An ISP account cost about \$20 per month for unlimited access while daytime long-distance calls can cost 25 cents or more per minute. Using RAS, remote users place a long-distance or toll call to the company's modem bank or host server in order to connect to the LAN. The cost difference is substantial, and its significance grows over time or as the number of remote users increase. A toll free access number may be offered by the organization, though at substantial cost.
- **Equipment Costs** – A VPN server can be nothing more than a typical, Pentium III network server capable of handling about 50 concurrent sessions and cost about \$3,900. It can also be an add-on module for a firewall. A 12-modem RAS server costs about \$9,600 and a 48-modem RAS costs about \$15,600. As the price of sophisticated firewalls and security software has declined, they compete favorably against hardware and telecommunications intensive modem pool devices or "chatterboxes".
- **Personnel Costs** – VPN administration can be handled by mid-level IT personnel. While RAS equipment requires additional expertise handling modem banks and solving telecommunication issues, and therefore needs a more specialized administrator, as well as support from your Telecommunications provider.
- **Authentication and Encryption** – VPN user authentication, data authentication, and encryption capabilities in client and server software are inherent. RAS products often do not include these



capabilities. Adding encryption capabilities may require integrating a third party's authentication and encryption products into RAS solutions.

- Access control – VPNs may use an access control system which enables the system administrator to specify what each remote user has access to once connected to the organization's LAN. Remote users with similar needs can be placed into groups with pre-defined access privileges thus simplifying system management. RAS does not have as robust an access control system.

For example, this cost comparison is a hypothetical organization with 100 remote users over a year period. As mentioned previously, the greater the number of remote users and the longer the time period, the more impact communications access charges have. The following table shows the costs incurred by using a VPN and the potential costs it would have incurred using RAS.

	VPN	RAS
Client/Server software	\$12,895	Include with hardware
Authentication Technology	Include with VPN	\$6,000
Server Hardware	\$5,100	\$15,600
Internet Connectivity (T1)	\$2,400	NA
RAS Connectivity	NA	\$6,624
Network Administration	\$20,000	\$40,000
Communications Access	\$24,000	\$158,400
<b>Total Costs</b>	<b>\$63,395</b>	<b>\$226,624</b>

The above example does not include other, less-objective operational costs incurred with either VPN or RAS systems, for instance, the cost of deployment. VPNs allow the client software and authentication tokens to be deployed over the Internet at a minimal cost. RAS client software can be deployed electronically; however, it does not have built-in authentication. A third-party physical authentication system for RAS needs to be setup and prepared for deployment, and the tokens must be delivered, either in person or via mail, to end users. This incurs deployment costs for RAS are several times that of a VPN. Also the on-going support for RAS has a much higher cost than has the support for a VPN.

## Summary

Protecting operations and intellectual property is critical in today's inter-connected and mobile, marketplace. The gains in productivity and flexibility are substantial though they require careful planning and a deep understanding of the technologies.

Schneider Automation Eclipse Network Services are experienced professionals whom can create a network security plan for Automation, evaluate your current plan, implement and service Firewall and VPN initiatives for Automation.