Rockwell Automation

Scalable secure remote access solutions for OEMs

Introduction

Secure remote access to production assets, data, and applications, along with the latest collaboration tools, provides plant and sites with the ability to apply the right skills and resources at the right time, independent of their physical location. OEMs are looking to reduce costs, add more value to their Industrial Automation and Control Systems (IACS) customers and differentiate themselves from their competitors. This paper outlines the means to enable secure remote access to plant or site-based applications & data and can be used as guidance for OEMs to collaborate with their customers when designing a secure remote access solution.

Technical challenges

OEMs have traditionally relied on deploying on-site personnel to provide support for IACS or used methods such as standalone dial-up access without using a firewall. This method of Remote Access often circumvents perimeter security, creates the threat of a “back door” into the IACS and can represent a significant security risk. As OEMs want to provide secure support remotely, and respond to issues in real time, this method is no longer sufficient.

Technologies for remote access to traditional enterprise networks have been around for quite some time, such as Virtual Private Networks (VPNs). However, successfully applying technologies to provide effective remote access to IACS has been a challenge.

This is due to several reasons:

- IACS is often managed by Operational Technology (OT) organizations, while enterprise-level remote access solutions such as VPNs are the responsibility of the Information Technology (IT) organization. Successful implementation of remote access to IACS requires collaboration between IT and OT organizations.
- Remote access can expose critical IACS components to various cybersecurity threats that may be present on a remote or partner computer, potentially impacting production.
- It is challenging to confirm that the end device (computer) being used for remote access is secure and has the appropriate versions of the applications needed for remote access and control.
- Limiting the capabilities of the remote user to those functions that are appropriate and do not require local presence due to line-of-sight or other similar requirements can be difficult.
- OT organizations are often unable to limit a partner or remote employee’s access to only specific machines, applications, or parts of the network for which they are responsible and have authorization. Solutions like the Stratix® 4300 coupled with FactoryTalk® Remote Access™ provide operation permission control with default roles (administrator, network security, device installer and device access) for user group management and asset management by folders. Furthermore, the solution provides an integrated firewall to restrict access to specific machines or devices via VPN.
- One size does not fit all. An IACS remote access solution that works for one customer may not be sufficient for another. An IACS remote access solution that is required by one customer may be too burdensome or even impractical for another. As noted below, a viable remote access solution is dependent upon industry requirements, customer requirements (security policies and procedures), customer size and their support infrastructure.

As a result, remote access solutions, while widely deployed in the enterprise network, have not been as widely adopted to support the IACS network. When VPN technology has been used, it has often been subject to the previously mentioned challenges, and therefore limited to employees only (not partners), and can still result in some security risks, including cybersecurity threats and unauthorized access, if not properly implemented. To truly achieve collaborative OT engineering, access needs to be scalable, regardless of location or company. Access needs to be secure to effectively communicate, diagnose problems and implement corrective actions. Access needs to be limited to those individuals that are authorized to access systems and their authorized actions need to be aligned with IT and OT policies and procedures.

When collaborating with your customer to implement remote access to your IACS solutions (for example, machine), the following questions will help identify the organization's level of readiness:

- Do they have an IT security policy?
- Do they have an IACS security policy?
- Do they have a remote access policy for employees and the infrastructure to support?
- What VPN technology/products do they use?
- Do they have a "partner" remote access policy - the ability and process to add partners (OEM, SI, automation vendor or contractor)?
- For partners, is your solution ready to be integrated into your customer's IACS network infrastructure? Does your solution support remote access? Is your solution aligned with established IACS security standards such as ISA99 and NIST 800-82?

Some other key considerations include:

- Monitoring and auditing activities of remote users to identify misuse
- Determine if there are any "line of site" (visual requirements) or other restrictions that need to be identified before allowing certain remote access capabilities
- Define what software tools are allowed for remote access

Principals of secure remote access

Defense in depth

When designing a secure remote access solution, a defense in depth approach should be implemented. This approach creates multiple security layers that address the different potential threats that could occur in a remote access solution. Although there is no single technology or methodology that fully secures IACS networks, combining multiple security technologies forms a strong deterrent to most known types of threats and security breaches, while limiting the impact of any compromise. To deliver a comprehensive defense in depth security program, companies need to rely on multiple types of controls. These controls can be categorized as:

Administrative

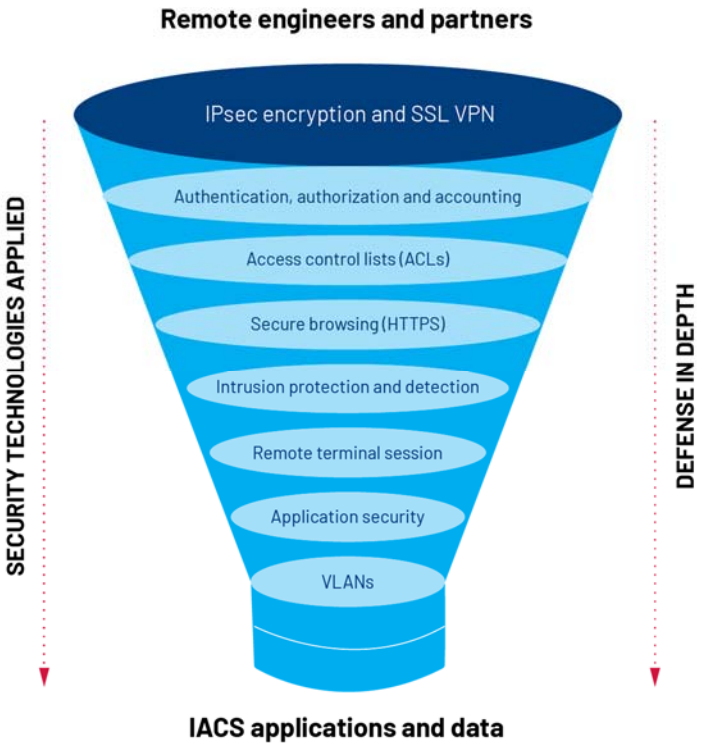
- Mostly security policies and procedures
- Examples include password policies, security awareness training, and so on

Technical

- Also called “logical” controls and consist of hardware, software, and electronics to monitor and control access to information systems
- Examples include firewalls, IPS/IDS, smartcards, and so on

Physical

- Mostly mechanical controls to monitor and control physical access
- Examples include locks, security guards, security cameras, and so on



It's important to remember that it's not just about the technical controls and that a complete security program includes administrative, technical and physical controls. The diagram above is an example of technical controls that can be implemented to create a defense in depth strategy.

Approach

There are several approaches to providing Secure Remote Access to an IACS, two of which are direct and indirect access. The choice of these approaches is dependent upon the criteria previously noted such as customer security policies and procedures. Each approach has several design considerations that could impact the proper operation of the IACS and should be accounted for in the design and implementation of an IACS remote access solution.

Direct access

Direct access allows the remote user to establish a secure connection "directly" to the IACS.

After creating a secure VPN tunnel, the software on the remote user's computer, initiates communication directly with the IACS.

- Design considerations – how will these be enforced?
    - Network and application authentication and authorization
    - Change management, version control, regulatory compliance and software license management
    - Health management of the remote client (computer)
    - Alignment with established IACS security standards

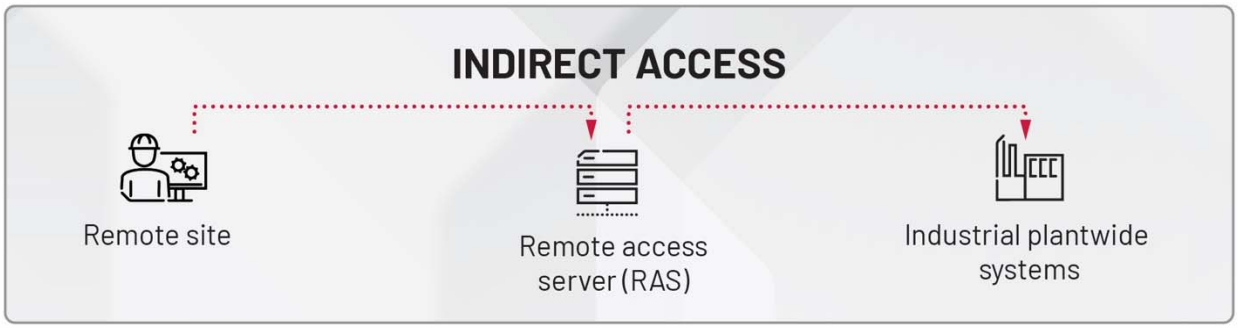
NOTE: Though little to no IT support is required when following this approach, best security practices should be in alignment with established IACS security standards.

Indirect access

Indirect access allows the remote user to establish a secure connection to the IACS through an intermediary server usually residing in the DMZ (Demilitarized Zone) providing remote gateway access to a remote access server (RAS) in the IACS. The remote client uses either a thin client software application or a web browser to establish a connection to the RAS once the VPN session has been established.

- Design considerations
    - Multiple layers of network authentication and authorization
    - Simplified asset management – change management, version control, regulatory compliance and software license management
    - Simplified health management of the remote client
    - Greater alignment with established IACS security standards

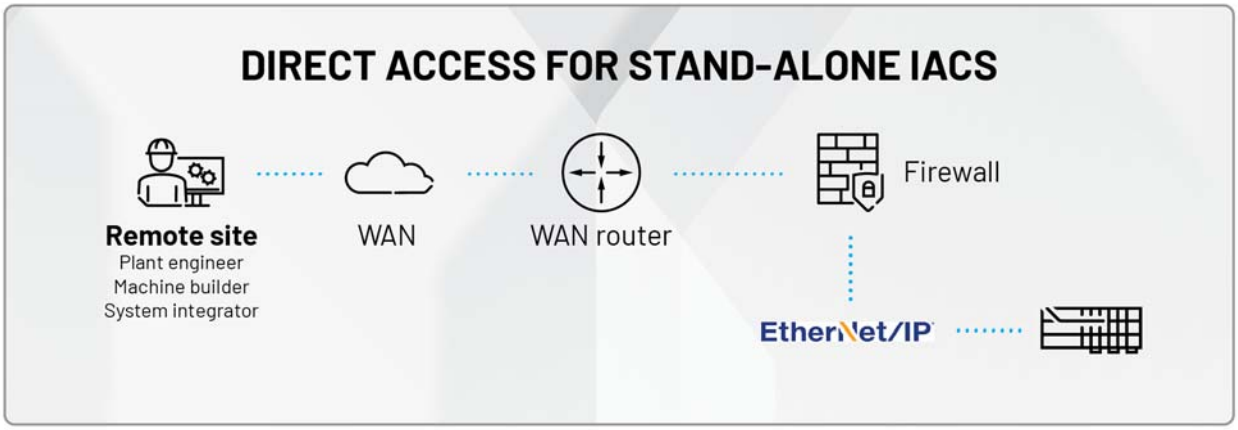
NOTE: Indirect access is often considered a more secure approach due to greater alignment with IACS security standards. This is due in part to having a dedicated asset, such as a computer, within the IACS used for remote access.



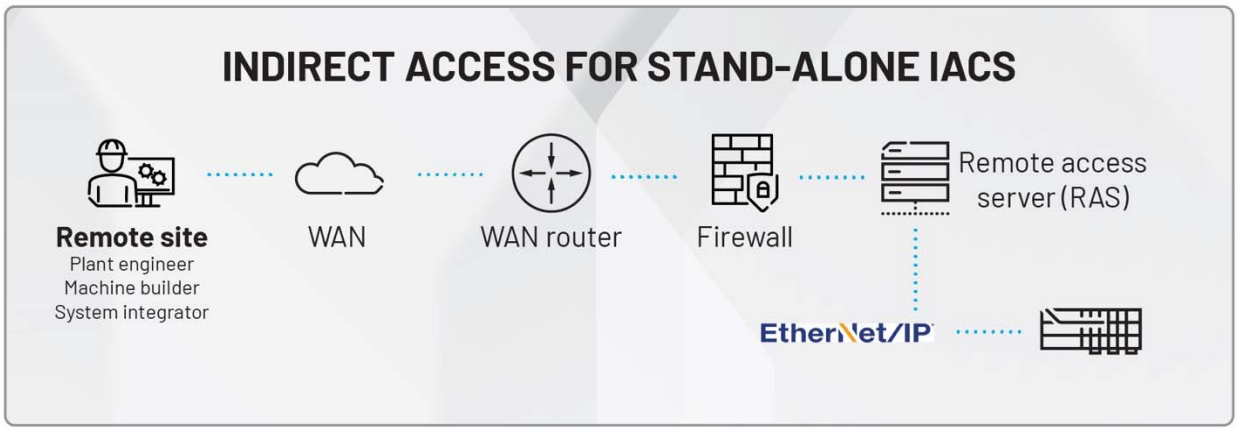
When analyzing secure remote access solutions, you must determine whether the type of system that needs to be accessed, are standalone isolated IACS or an enterprise integrated IACS.

- Standalone isolated IACS representative example
    - Small plant or site, could be small single-operator shops, remote location (not enterprise-integrated) with few automated machines
    - Little to no IT support with minimal to no security policies
    - Little to no alignment with established IACS security standards
    - Standalone or integrated OEM machines and equipment
- Enterprise-Integrated IACS Representative Example
    - Larger plant or site
    - Industrial network interfaces with the enterprise network
    - Strong IT presence with defense in depth security policies
    - Alignment with established IACS security standards

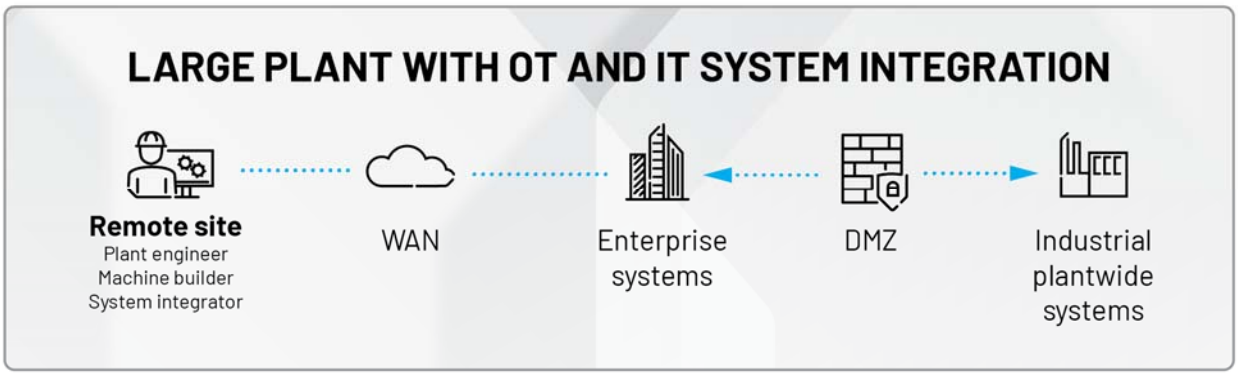
Example: Direct access for standalone IACS



Example: Indirect access for standalone IACS



Example: Indirect access for enterprise-integrated IACS
(Large plant or site with OT and IT system integration)



Remote access solutions

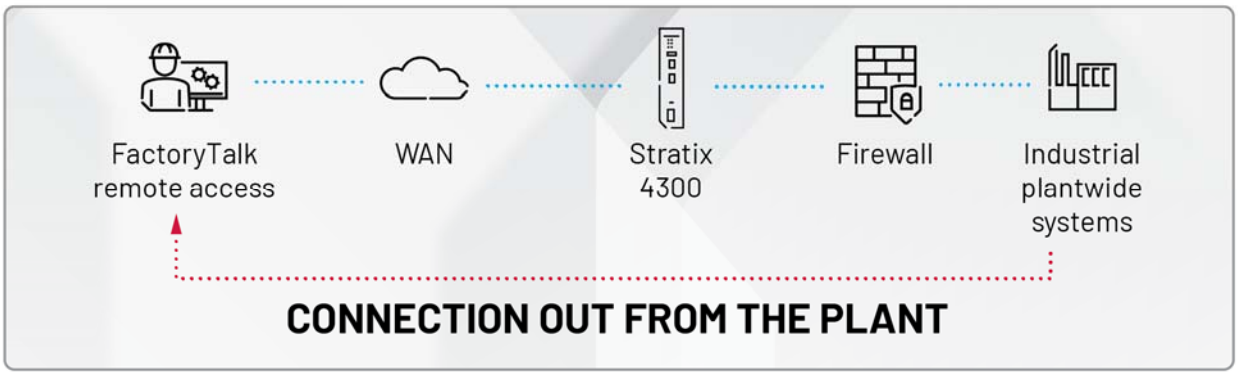
Remote Access for Industrial Equipment

Remote Access for Industrial Equipment is a hardware and software solution to enable remote connectivity. This solution requires both FactoryTalk Remote Access software and the Stratix 4300 Remote Access Router to support customers in applying the appropriate technical resources while independent of physical location. These products enable remote connectivity to remote systems and applications when travel is not feasible to provide in-person support for installation, programming updates, and on-demand troubleshooting and maintenance.

FactoryTalk Remote Access is the web-based client used to configure and manage remote connections to the Stratix 4300 Remote Access Router. FactoryTalk Remote Access software allows users to configure operation permission policies, user group management and asset management. The Stratix 4300 router is offered in two and five 10/100/1000 Mbps Gigabit Ethernet copper port variants to allow access to remote systems and its subnetworks. A customer can use these products to meet their connectivity needs.

Connection out from the plant (Stratix 4300)

End-user initiated connections can also provide secure remote access capabilities provided the control system has personnel on-site and that there is already secure internet connectivity established using multi-layer security controls.

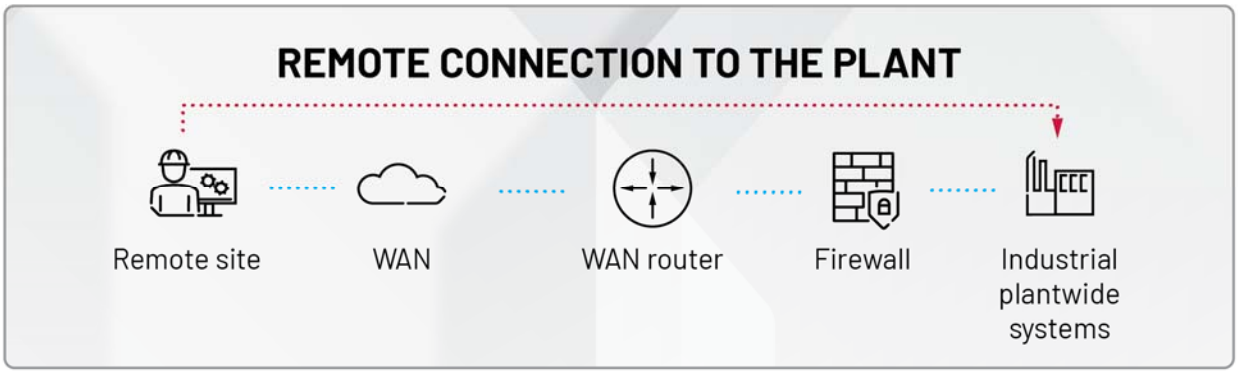


The risk of opening outbound connections to the internet (http/https) to use such services should not be overlooked and should be restricted to certain sites and IP addresses to help prevent browsing the web from the control systems. The use of web browsers can pose significant risk and have been known to be a source of attacks.

Another solution is a gateway VPN remote access router, such as the Stratix 4300, which resides in the control system and establishes remote access through a hosted VPN service. Care should be taken with this solution to analyze the hosted service provider, their location and whether they are adhering to best security practices. It is also important that the gateway VPN is aligned with established IACS security standards, such as ISA99 and NIST 800-82, and meets the security requirements of the manufacturer's security policy.

Remote connection into the plant (WAN routers/modems: DSL, cellular, satellite, cable, T1's, and so on)

When traditional modems are not an option due to the infeasibility of installing phone lines, cellular access to establish a WAN connection provides an excellent alternative. This is becoming a popular option due to the increasing, speed, affordable cost, and convenience.



However, as stated above regarding dial-in modems, cellular WAN connections using cellular modems and routers should be used with other security technologies to provide defense in depth or at a minimum have these features built into the device (firewall bundle). Other WAN connectivity options include DSL, Cable, T1's, Satellite, and so on. The type of connectivity that will be used to establish WAN connectivity to the standalone system will be dependent upon the plant or site location, budget constraints, and access policy. One thing to note is that when implementing a VPN, typically a static IP address would need to be assigned by the WAN provider.

- The following are some security features to look for when designing a solution:
- Does it have VPN capabilities, SSL or IPsec?
- Does it provide a firewall?
    - Does it filter industrial protocols like CIP™, Modbus and so on?
- NAT (Network Access Translation)?
- Is it built for industrial use?
- Can it provide auditing?
- Does it have an intrusion detection and/or prevention system?

Enterprise-Integrated IACS

- Rockwell Automation & Cisco: Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide
    - https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

Direct Access Solutions

- Rockwell Automation provides a secure remote access solution used for outbound connections from the plant or site. This solution includes the Stratix 4300 remote access router
    - rok.auto/stratix4300

Customized Solutions

- For customized solutions, The Rockwell Automation Industrial Maintenance & Support Service can design a secure solution that meets your needs
    - https://www.rockwellautomation.com/en-us/capabilities/industrial-maintenance-support.html

Summary

The evolution of secure remote access capabilities allows OEMs to improve productivity, reduce cost and respond more quickly to events that impact their customer. By using these secure remote access solutions, the OEMs can provide real-time remote support. These capabilities are increasingly important as manufacturing operations become more complex and globally distributed while the availability of skilled workers to support systems on-site on a 24-hour basis is decreasing. The remote access capabilities for standalone systems give OEMs the ability to apply the right skills and resources at the right time, independent of their physical location. This allows for higher efficiency, less downtime and lower cost.

Given the critical nature of IACS applications, however, it's important that any remote access solution provides the appropriate levels of security to meet the needs of the manufacturer and align with established IACS security standards. Applying the principles of defense in depth confirms that there is never direct unsecure remote access to an IACS application.

Glossary of Terms

CIP - Common Industrial Protocol

The Common Industrial Protocol (CIP) encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications – control, safety, synchronization, motion, configuration and information. CIP is owned and maintained by ODVA. ODVA is an international

association comprising members from the world's leading automation companies.

DMZ - Demilitarized Zone

Refers to a buffer or network segment between two network zones. A DMZ is commonly found between a corporate network and the internet where data and services can be shared/accessed from users in either the internet or corporate networks. A DMZ is typically established with network firewalls to manage and secure the traffic from either zone.

IACS - Industrial Automation and Control Systems

Refers to the set of devices and applications used to automate and control the relevant manufacturing process. Rather than use various terms with a similar meaning (for example, production systems and plant floor systems, we standardized on this term for use in this paper). That is not to suggest any specific focus or limitations. We intend that the ideas and concepts outline herein are applicable in various types of manufacturing including but not limited to batch, continuous, discrete, hybrid and process. Other documents and industry references may refer to Industrial Control Systems (ICS). For this document, those terms are interchangeable. This document uses IACS, as reflected in the ISA99 standards, and is aligned with the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE)

IP Protocol Suite

A set of networking standards on which the internet and most enterprise networking is based. It includes the Layer 3 Internet Protocol (IP), the Layer-4 Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

IPS - Intrusion Prevention Systems

A network security device that monitors network activity for malicious or unwanted behavior.

IPSec - IP Security

A framework of open standards that provides data confidentiality, data integrity and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE (see above) to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can help protect one or more data flows between a pair of hosts, between a pair of security gateways or between a security gateway and a host.

Manufacturing Zone (Plant or Site)

A network zone in the Plant Logical Framework as shown in Chapter 2 of the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. The zone contains the complete set of applications, systems, infrastructure, and devices that are critical to the continued operations of the plant. In other documentation (for example, ISA99), this zone may also be referred to as the Control zone. The terms are interchangeable in this regard.

NAT - Network Address Translation

Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the internet by translating those addresses into globally routable address space.

Remote Terminal Session

Remote desktop refers to a set of protocols and software that enable one computer or user to remotely access and control another computer through graphical Terminal Emulation. Software that makes it, appears to a remote host as a directly attached terminal, including the Microsoft® RDP, Remote Desktop Protocol and VNC Virtual Network Computing.

SSL - Secure Socket Layer

Encryption technology for the Web used to provide secure transactions, such as the transmission of credit

card numbers for ecommerce.

Subnet or Subnetwork

In IP networks, a subnet is a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by a network administrator to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks.

VPN - Virtual Private Network

A network that uses primarily public telecommunication infrastructure, such as the internet, to provide remote offices or traveling users an access to a central organizational network. VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to help prevent disclosure of private information to unauthorized parties. VPNs may serve any network functionality that is found on any network, such as sharing of data and access to network resources, printers, databases, websites and so on. A VPN user typically experiences the central network in a manner that is identical to being connected directly to the central network. VPN technology via the public internet has replaced the need to requisition and maintain expensive dedicated leased-line telecommunication circuits once typical in wide-area network installations.

WAN - Wide Area Network

A wide area network (WAN) is a telecommunication network that covers a broad area (that is, any network that links across metropolitan, regional or national boundaries). Business and government entities utilize WANs to relay data among employees, clients, buyers and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively conduct its daily function regardless of location.

Publication ENET-WP025B-EN-P — January 2022 | Supersedes Publication ENET-WP025A-EN-P — March 2015