Cybersecurity

Good Practices Guide

HA032968 Issue 1

July 2017

Eurotherm®

by Schneider Electric

Legal Information

Table of Contents

Safety Information

Important Information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Introduction[1]

Purpose

This document will help the reader understand what constitutes cybersecurity in the industrial market. Readers will become more familiar with the methods of malicious network penetration, the risks caused by system vulnerabilities, and our recommendations to mitigate those risks. It provides a common, readily understandable reference point for end users, system integrators, OEMs, sales people, business support, and other parties.

This document is not meant to cover cybersecurity in detail. For more detailed information please refer to:

- ISO/IEC 27001:2013 Information Technology - Security techniques - Information security management systems - Requirements.
- IEC 62443 Industrial Communication Networks - Network and System Security.

What is Cybersecurity?

Industrial Control Systems (ICS) security objectives typically follow the priority of availability, integrity, and confidentiality in that order. Complicating matters, the priorities of IT departments can be fundamentally different from those of process control departments. Even though the goals and considerations are the same, their order of priority can be very different.

The IT world typically sees confidentiality, data integrity, and availability as the order of importance. By contrast, the ICS world sees human and plant safety as its paramount responsibility. It follows, then, that system availability, data integrity and confidentiality are the order of importance in ICS systems.

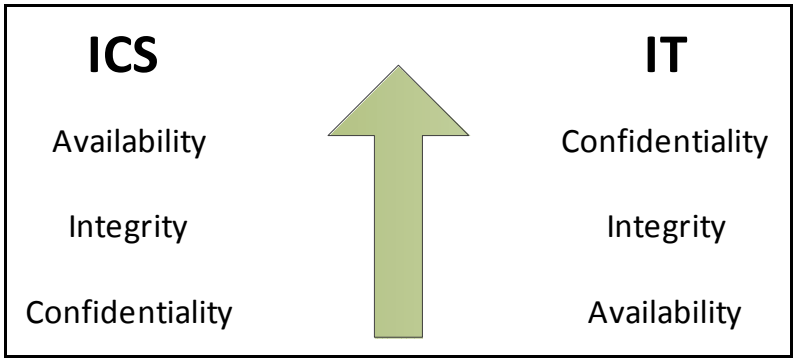


Figure 1 Industrial Control Systems vs Information Technology

Cybersecurity is a part of security as a whole. In general, security consists of three types of actions. They are:

- To help prevent an incident such as unauthorized access or modification to any system or asset
- Detect an incident that has occurred and gather information about the incident.
- React to recover from an incident or stop an incident in progress.

1.Some of the content in this section is based on or clarifies content available on the US-CERT Control Systems: Overview of Cyber Vulnerabilities Web page located at http://www.us-cert.gov/control_systems/csvuls.html. Schneider Electric recommends reviewing all the materials at this Web site to gain a better understanding of control system vulnerabilities and potential threats. This link is provided for informational purposes only and does not represent an endorsement by or affiliation with the US-CERT (DHS).

Cybersecurity is the part of security that focuses on cyber assets. Cybersecurity can be further segmented into the following:

- Information Security: The protection of information against unauthorized disclosure, transfer or modification, whether accidental or intentional.
- End Point Security: The application of hardware, firmware, and software features to a computer system to help protect against unauthorized access to information. Protection of industrial devices such as PACs, HMIs, and SCADA from unauthorized access and disruption of services.
- Network Security: Protection of networks from unauthorized access and disruption of services using devices such as firewalls and using methods such as VLANS for network segmentation.

Cybersecurity is an ongoing process that encompasses procedures, policies, software, and hardware.

Why is Security Important to Industrial Controls Today?

Cybersecurity is no longer a secondary requirement in the industrial controls world. It is as important as safety or high availability.

Industrial control systems based on computer technology and industrial-grade networks have been in use for decades. Earlier control system architectures were developed with proprietary technology and were isolated from the outside world thus making attacks more difficult. In many cases, physical perimeter security was deemed adequate and cybersecurity was not a primary concern.

Today many control systems use open or standardized technologies such as Ethernet TCP/IP to reduce costs and improve performance. Many systems also employ direct communications between control and business systems to improve operational efficiency and manage production assets more cost-effectively.

This technical evolution exposes control systems to vulnerabilities previously thought to affect only office and business computers. Control systems are now vulnerable to cyber attacks from both inside and outside of the industrial control system network.

Security challenges for the control environment include:

- Diverse physical and logical boundaries.
- Multiple sites and large geographic spans.
- Adverse effects of security implementation on process availability.
- Increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open.
- Increased exposure to malicious software from USB devices, vendor and service technician laptops, and from the enterprise network.
- Direct impact of control systems on physical and mechanical systems.

No longer are fences and security guards adequate to protect industrial assets. Companies can be diligent in the steps they take to help secure their systems. A successful cyber attack can result in lost production, damaged company image, environmental disaster, or loss of life. The controls industry and its customers can apply cybersecurity lessons learned from the IT world.

Cyber Threat Profile

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of computer systems and networks. These actions can be initiated from within the physical facility or from an external location. According to control systems security expert Eric Byres of Belden Inc. and Tofino Security, about 50% of the cyber attacks that penetrate the control network system originate from the enterprise system, 17% from the Internet, and 10% from trusted third parties.

A cybersecurity plan needs to account for various potential sources of cyber attacks and accidents, including:

- Internal
  - Inappropriate employee or contractor behavior
  - Disgruntled employees or contractor
- External opportunistic (non-directed):
  - Script kiddies (slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding of how the script works or its potential impact on a system)
  - Recreational hackers
  - Virus writers
- External deliberate (directed):
  - Criminal groups
  - Activists
  - Terrorists
  - Agencies of foreign states
- Accidents

A deliberate cyber attack on a control system may be launched to achieve a number of malicious results, including:

- Disrupt the production process by blocking or delaying the flow of information.
- Damage, disable, or shut down equipment to negatively impact production or the environment.
- Modify or disable safety systems to cause intentional harm.

How Attackers Can Gain Access to the Control Network

A cyber attacker bypasses the perimeter defences to gain access to the control system network. Common points of access include:

- Dial-up access to RTU devices
- Supplier access points (such as technical support access points)
- IT controlled network products
- Corporate virtual private network (VPN)
- Database links
- Poorly configured firewalls

- Peer utilities
- Wireless communication

Dial-up Access to RTU Devices

Many control systems have a modem, similar to the one shown in Figure 2, "RTU Dial-up Modem Backup Connection" (below), for backup use if the main network becomes unavailable. An attacker knows the protocol of the remote terminal unit (RTU) to gain access via dial-up. Most RTUs do not employ strong authentication or other security mechanisms. Many accept and respond to any caller.

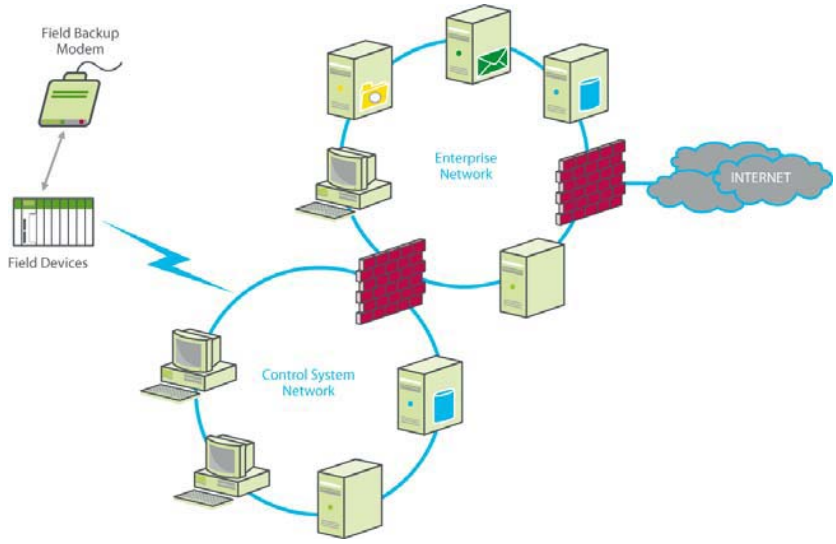


Figure 2 RTU Dial-up Modem Backup Connection

Supplier Access

To reduce down time and costs, organizations often grant access to suppliers for remote diagnostics or maintenance through dial-up, as shown in Figure 3, "Vendor Access Vulnerabilities", or through a VPN. These suppliers sometimes leave ports open on the equipment to simplify their tasks, giving the attacker access to the equipment and links to control system networks.

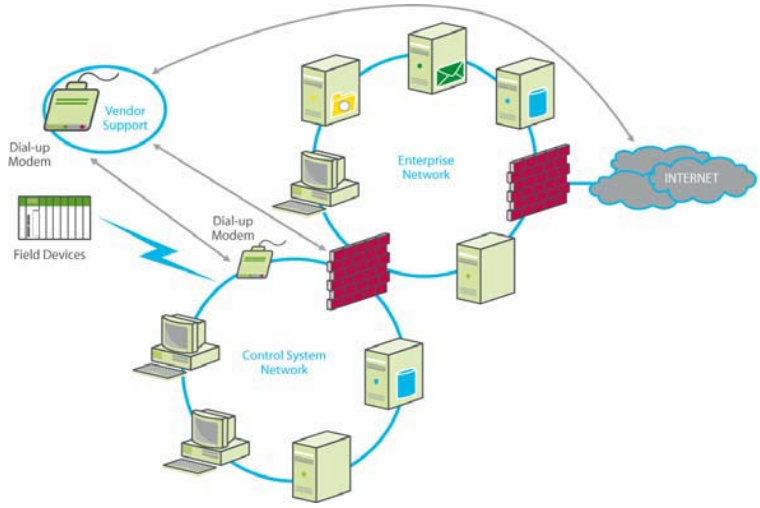


Figure 3 Vendor Access Vulnerabilities

IT-Controlled Communication Equipment

The automation department's network authority is often limited to the control network within the facility. The IT department assumes responsibility for the organization's long-distance communication. As shown in Figure 4, "IT Controlled Equipment", a skilled attacker can access the control network through the communication architecture and reconfigure or compromise communications to the field control devices.

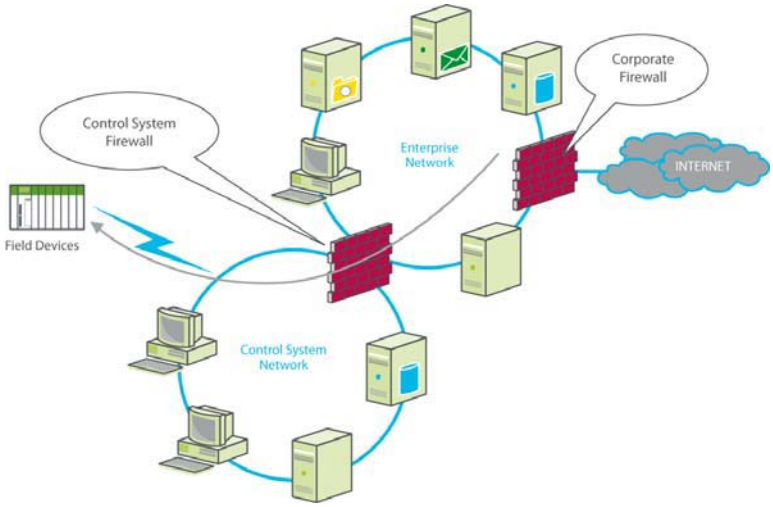


Figure 4 IT Controlled Equipment

Corporate VPNs

Engineers working in the corporate offices often use VPN connections to gain access to the control network, as shown in Figure 5, "Corporate VPN Connections". An attacker can compromise the VPN server, wait for a legitimate user to establish a VPN connection into the control system network, and piggyback on the legitimate connection.

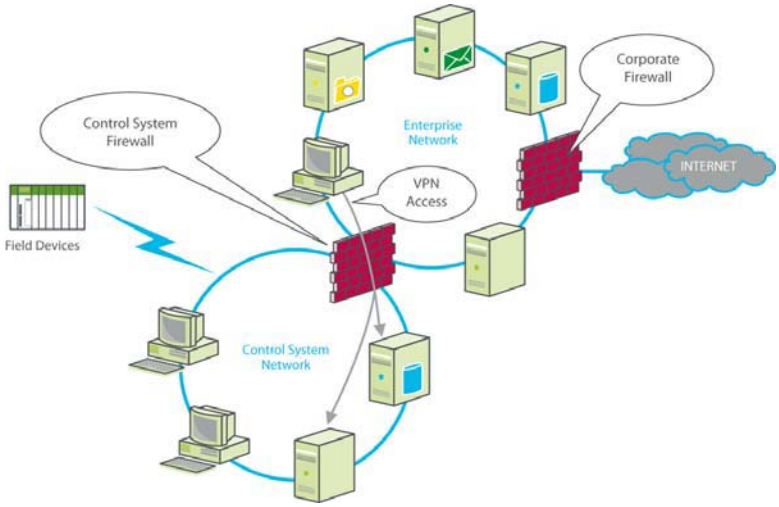


Figure 5 Corporate VPN Connections

Database Links

A majority of control systems use real-time databases, configuration databases, and multiple historian databases. If the firewall or the security on the database is not configured properly, a skilled attacker can gain access to the database from the business network, as shown in Figure 6, "Database Links", and generate SQL commands to take control of the database server on the control system network.

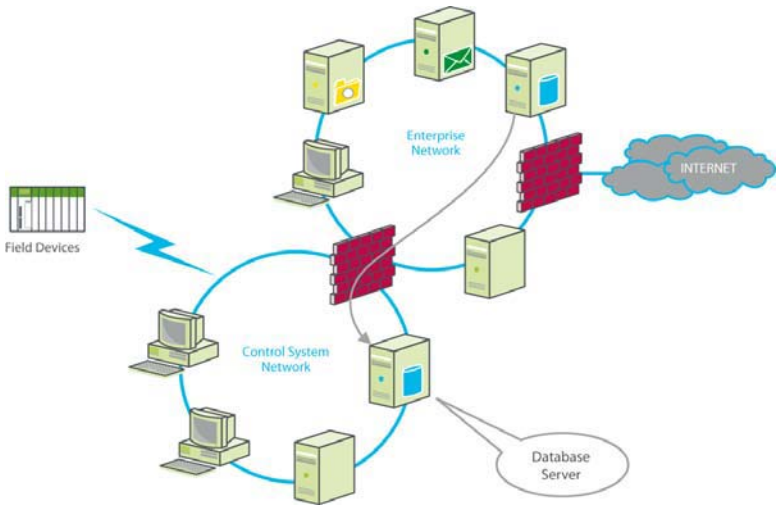


Figure 6 Database Links

Peer Utility Links

Partners and peers are sometimes granted access to information located on either the business or control network, as shown in Figure 7, "Peer Utility Links". With the peer-to-peer link, the security of the system is only as strong as the security of the weakest member.

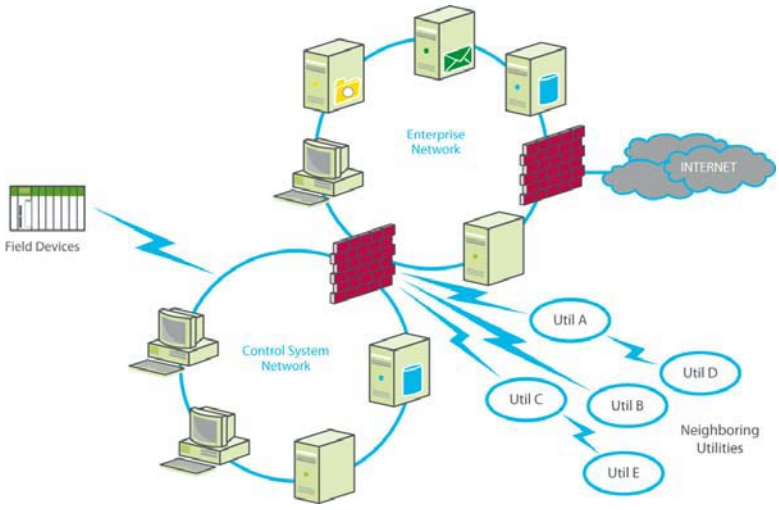


Figure 7 Peer Utility Links

Wireless Communication

With the introduction of wireless communication in industrial architectures, access to the network can be accomplished through any deployed access point. Implement proper configuration and physical security, especially in remote locations that are not monitored and where attackers would have the advantage of time to try to compromise an access point's security. It should be noted that when availability is essential, wireless is not a good choice as it is vulnerable to DOS attack, signal jamming for which there is no countermeasure.

To address this challenge, use the newest available defence mechanisms and proper logging techniques to inform the network administrator about intrusion attempts.

A major component of network security is related to authorization and encryption. The initial security protocol WEP has been declared obsolete since 2004. It was replaced by WPA and later by WPA2. Wireless networks are upgraded to support the newest security protocol, WPA2, which in the enterprise version supports RADIUS server authentication mechanism. This way each client uses a different encryption key and along with the AES encryption protocol is considered extremely difficult to hack.

If the WPA2 Pre-Shared-Key is used instead of the Enterprise version, the length and complexity of the key is the only effective defence against major attacks.

How Attackers Attack

Depending on motives and skills, the attacker may or may not need to know details of the control process to disrupt operations. For example, if the motive is simply to shut down the process, very little knowledge is needed. However, if the attacker wants to attack a specific machine or process, he or she needs to understand how the application program is written.

Highly vulnerable processes include but are not limited to:

- Data acquisition databases. Names of databases vary from supplier to supplier but a majority use a common naming convention with a unique number such as pump1, pump2, breaker1, breaker2, and so on. On the communications protocol level, the devices are simply referred to by number (memory location or register address). For a precise attack, the attacker needs to translate the numbers into meaningful information.
- HMI or SCADA display screens. Gaining access to the HMI screens is one method for understanding the process and the interaction between the operator and the equipment. The information on the screen allows the attacker to translate the reference numbers into something meaningful.

- Infection of equipment. All devices use software to operate. This could be in the form of an operating system like Microsoft Windows that is used in PCs or any firmware or operating system used in network equipment, a SCADA system, Programmable Automation Controllers (PAC)s, cameras, etc. If an attacker manages to modify this software, access to information is easy and very difficult to detect.

  In ICS-CERT Monitor April/May/June 2013 issue it was reported that they received a report from a gas compressor station owner on February 22, 2013 about increased brute force attempts to access their process control network. Of course the Stuxnet virus is one the most well-known, largest and successful industrial attack reported. The Stuxnet virus targeted PLC systems in Iran's nuclear program.

Control of the Process

Once an attacker has enough information about the process, the next step is to manipulate it. One way to gain control of the process is to connect to a data acquisition device, such as a programmable automation controller (PAC) that has access to field devices and send it properly formatted commands. Many PACs, gateways, and data acquisition servers use weak authentication or no authentication and will accept any commands that have been formatted correctly.

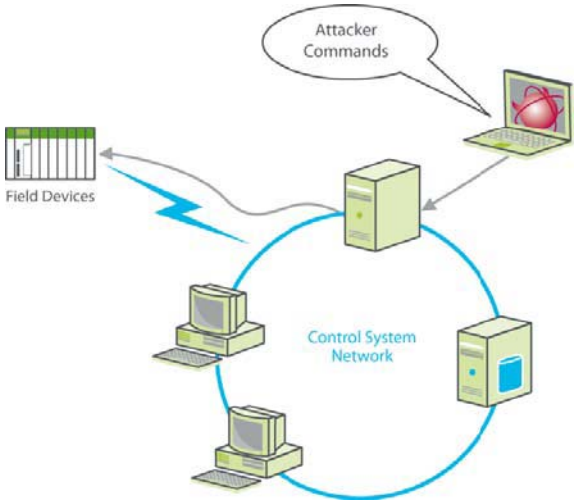


Figure 8 Attacker Commands

Exporting the HMI Screen

Another method of attack is to export the HMI screen to gain control of the operations. If the attacker succeeds, the operator's HMI screen can be viewed and controlled on the attacker's screen. A sophisticated attacker may also modify the operator's screen to display normal operations in order to disguise the attack.

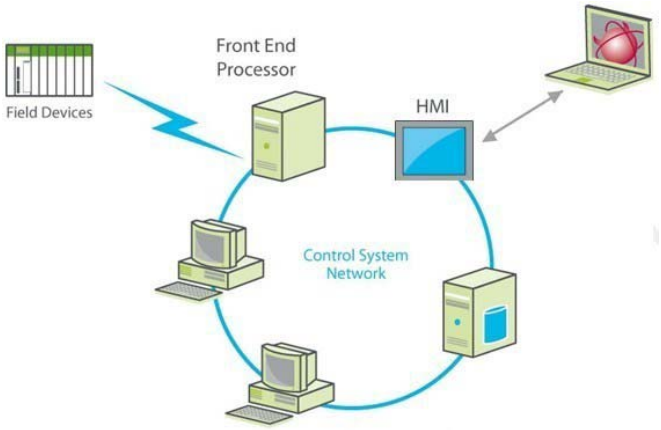


Figure 9 HMI Vulnerabilities

Changing the Database

A successful attacker can access the database and modify the data to disrupt normal operation of the control system or change stored values to affect the system's integrity.

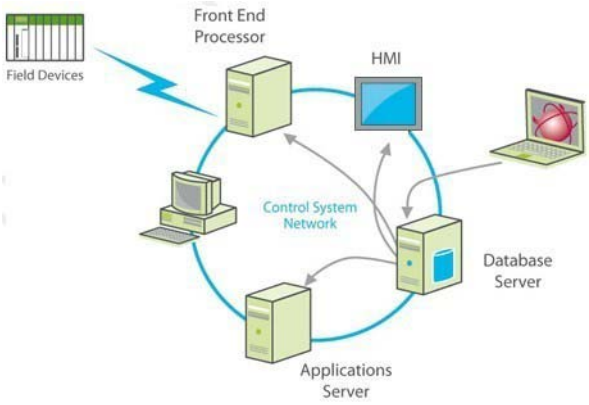


Figure 10 Database Change Attacks

Man-in-the-Middle Attacks

Man-in-the-middle is a type of attack where the attacker intercepts messages from one computer (Host A), manipulates the data, and then forwards it to the intended computer (Host B), as shown in Figure 11, "Man-in-the-Middle Attacks". Both computers appear to be communicating with each other and neither system detects the presence of an intruder in the middle.

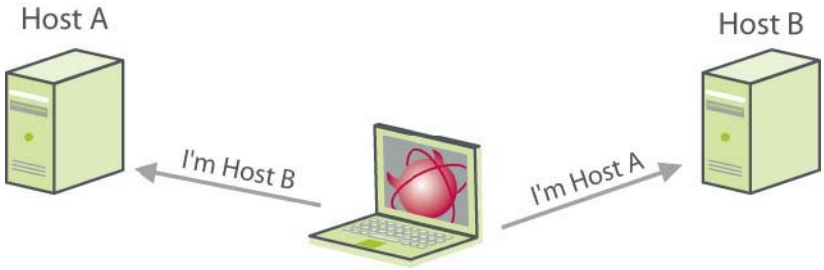


Figure 11 Man-in-the-Middle Attacks

A man-in-the-middle attack can even allow the attacker to spoof the operator HMI screens (that is, display a fake HMI screen) and take control of the control system, as shown in Figure 12, "Attacker Spoofs HMI Operator Screens". For the attack to succeed, the attacker needs to know the protocol of the targeted exchange.

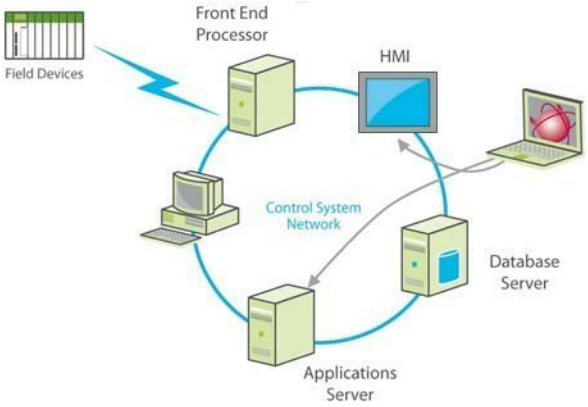


Figure 12 Attacker Spoofs HMI Operator Screens

Denial of Service

Denial of service (DoS) attacks attempt to block legitimate access to network or device services. One common type of DoS attack floods a device with requests so that its response times are slowed to the point where the system is unusable. Another type of DoS attack floods the network with traffic such as TCP SYN, affecting network response times to the point where legitimate use is severely impacted.

Accidental Events

Experts attribute more than 75% of network-related system outages to accidental events. Causes of these accidents can include poor network design, programming errors, improperly functioning network devices, non-compliance with procedures, or human error such as accidentally connecting network cables in wrong ports. Many of the security features and processes discussed in this document can also mitigate accidental events.

In many cases, contractors contribute directly to system design, commissioning, or maintenance. Operational procedures should be refined so that contractors cannot introduce malware or vulnerabilities into the control network. For instance, automatically scan contractor equipment for malware infection before allowing access to any control network equipment. USB keys are another common source of malware infection and should be carefully screened before permitting their use.

Individuals who inadvertently connect a network cable into the wrong port on a multi-port switch can create outages or broadcast storms that could disable the network or severely affect its performance.

In general, the cause might be accidental, but the features, practices, and procedures used for cybersecurity work equally well against accidental system outages.

Whether an incident is an accident or deliberate attack, preparation is key. Incident recovery methods should be developed and tested so that recovery from an outage or other events can be quickly and reliably managed. High availability and redundant architectures play a role in this area when even short system outages cannot be tolerated.

NERC Top Ten Control System Vulnerabilities

The Control System Security Working Group of the North American Electric Reliability Corporation (NERC) publishes a report identifying the top 10 vulnerabilities of control systems. The list is published as follows:

1. Inadequate policies, procedures, and culture that govern control system security:
    - Clash between operational culture with modern IT security methods.
    - IT often does not have an understanding of operational requirements of a control system.
    - Lack of overall awareness and appreciation of the risk associated with enabling the networking of these customized control systems.
    - Absence of control system information security policy.
    - Lack of auditing, enforcing, or adhering to control system information security policy not adhered to, enforced, or audited.
    - Lack of adequate risk assessment.
2. Inadequately designed control system networks that lack sufficient defence-in-depth mechanisms:
    - Network security of control system devices was not adequately considered when originally designed. These systems were designed with availability and reliability in mind.
    - Control systems may not be capable of secure operation in an Internet or intranet working environment without significant investment to reengineer the technology so it is in accordance with appropriate risk assessment criteria.
3. Remote access to the control system without appropriate access control:
    - Inappropriate use of dial-up modems.
    - Use of commonly known passwords or no use of passwords.
    - Implementation of non-secure control system connectivity to the corporate Local Area Network (LAN).
    - Practice of un-auditable and non-secured access by vendors for support.

4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained:
    - Inadequate patch management.
    - Lack of appropriately applied real time virus protection.
    - Inadequate account management.
    - Inadequate change control.
    - Inadequate software inventory.
5. Use of inadequately secured wireless communication for control:
    - Use of commercial off-the-shelf (COTS) consumer-grade wireless devices for control network data.
    - Use of outdated or deprecated security or encryption methods.
6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes:
    - Internet-based Supervisory Control and Data Acquisition (SCADA).
    - Internet or Intranet connectivity initiated from control system networks:
    - File Sharing
    - Instant Messaging
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity:
    - Underused intrusion detection systems.
    - Under-managed network system.
    - Implementation of immature Intrusion Prevention Systems.
8. Unauthorized or inappropriate applications or devices on control system networks:
    - Unauthorized installation of additional software to control system devices.
    - Peripherals with non-control system interfaces, e.g., multi function or multi-network printers.
    - Non-secure Web interfaces for control system devices.
    - Laptops
    - USB memory.
    - Other portable devices e.g., personal digital assistants (PDAs).
9. Control systems command and control data not authenticated:
    - Authentication for LAN-based control commands not implemented.
    - Immature technology for authenticated serial communications to field devices.
    - Lack of security implemented on an object by object basis on the control displays.
10. Inadequately managed, designed, or implemented critical support infrastructure:
    - Inadequate uninterruptible power supply (UPS) or other power systems.
    - Inadequate or malfunctioning HVAC systems.
    - Insufficiently protected telecommunications infrastructure.

- Inadequate or malfunctioning fire suppression systems.
- Lack of recovery plan.
- Insufficient testing or maintenance of redundant infrastructure.

Glossary

A Glossary is available in the "Appendix" on page 81 of this document. Please refer to it whenever necessary.

Schneider Electric Defence-in-Depth

Schneider Electric recommends a defence-in-depth approach to cybersecurity. No single approach is adequate. The defence-in-depth approach layers the network with security features, appliances, and processes.

As shown in Figure 13, "Schneider Electric Defence-in-Depth Components", this defence-in-depth approach integrates a set of related process and systems components to provide higher levels of security in a PlantStruxure network.

Figure 13 Schneider Electric Defence-in-Depth Components

The basic components of Schneider Electric's defence-in-depth approach are:

1. Policies & Procedures. A comprehensive set of policies and procedures which covers all aspects of cyber security including but not limited to:
    - Training and Cybersecurity Awareness programs, these are not limited to employees but also sub-contractors and visitors.
    - Risk Assessment, a systematic security analysis of the entire plant, including physical security, IT and OT network and infrastructure security.
    - Security Plans, built around the results of the Security Risk Assessment, including Business Continuity Plan if a security incident occurs, and plans for deploying IT and OT network and infrastructure security.
2. Network Separation & Segmentation. Physical separation of the control network from other networks using a demilitarised zone (DMZ), and the division of the control network itself into functional zones connected by secure conduits.

3. System Access Controls. Controlling physical access using traditional security measures such as perimeter defences (fences, locked gates and doors, CCTV, etc.) and logical access to the system using firewalls, authentication & authorisation, VPNs, anti-virus software and intrusion detection/prevention systems.
4. Device and System Hardening. This is the process of configuring devices (including PCs, servers, network security devices and control devices) to aid in reducing the attack surface of the system. Device hardening measures include password management, access control, disabling of unused ports, services, applications and functionality.
5. Monitoring & Maintenance. An effective defence-in-depth campaign does not stop when security has been implemented and deployed; security and its constituent components require continual monitoring for unusual or unexpected behaviour, and maintenance (including patch management).

Schneider Electric supports defence-in-depth with a wide selection of devices, including:

- ConneXium Industrial Firewalls to provide a higher level of control network perimeter security and support components such as VPN and DMZ.
- ConneXium Tofino Firewall to help secure communication zones within the control network using basic firewall rules, stateful packet inspection, and deep packet inspection.
- ConneXium infrastructure devices to limit internal access to areas of responsibility and act as a second line of defence in the event of a firewall breach.
- PACs, SCADA, HMI devices, and Ethernet modules hardened with password protection, access control, and the ability to turn off unneeded services.

Details of the Schneider Electric defence-in-depth approach are in the chapters that follow.

Risk Assessment, Security Planning, and Training

This section describes the interrelated process components of Schneider Electric's defence-in-depth. They include risk assessment, security planning, and training.

Risk Assessment

Risk assessment is the process of analysing and documenting the plant and related systems to identify, and prioritize potential threats.

The goals of this phase are to:

- Identify and document all potential threats.
- Prioritize these threats according to severity, business impact, and safety criteria.
- Decide the order in which to address the threats and how to distribute resources to the effort.

The assessment examines possible threats from internal sources such as disgruntled employees and contractors and external sources such as hackers and vandals. It examines potential threats to continuity of operation and assesses the value and vulnerability of assets such as proprietary recipes and other intellectual properties, processes, and financial data.

Use the outcome of this assessment to prioritize cybersecurity resource investments. Address the processes, devices, and networks with the highest risk and highest business and safety implications.

Infrastructure Diagrams

Infrastructure diagrams like the example shown in Figure 14, "Sample Control Systems Diagram" shows the network infrastructure divided into logical segments and zones and the conduits that connect them. They can help identify weaknesses, potential threats, and origins of threats to the devices and processes.

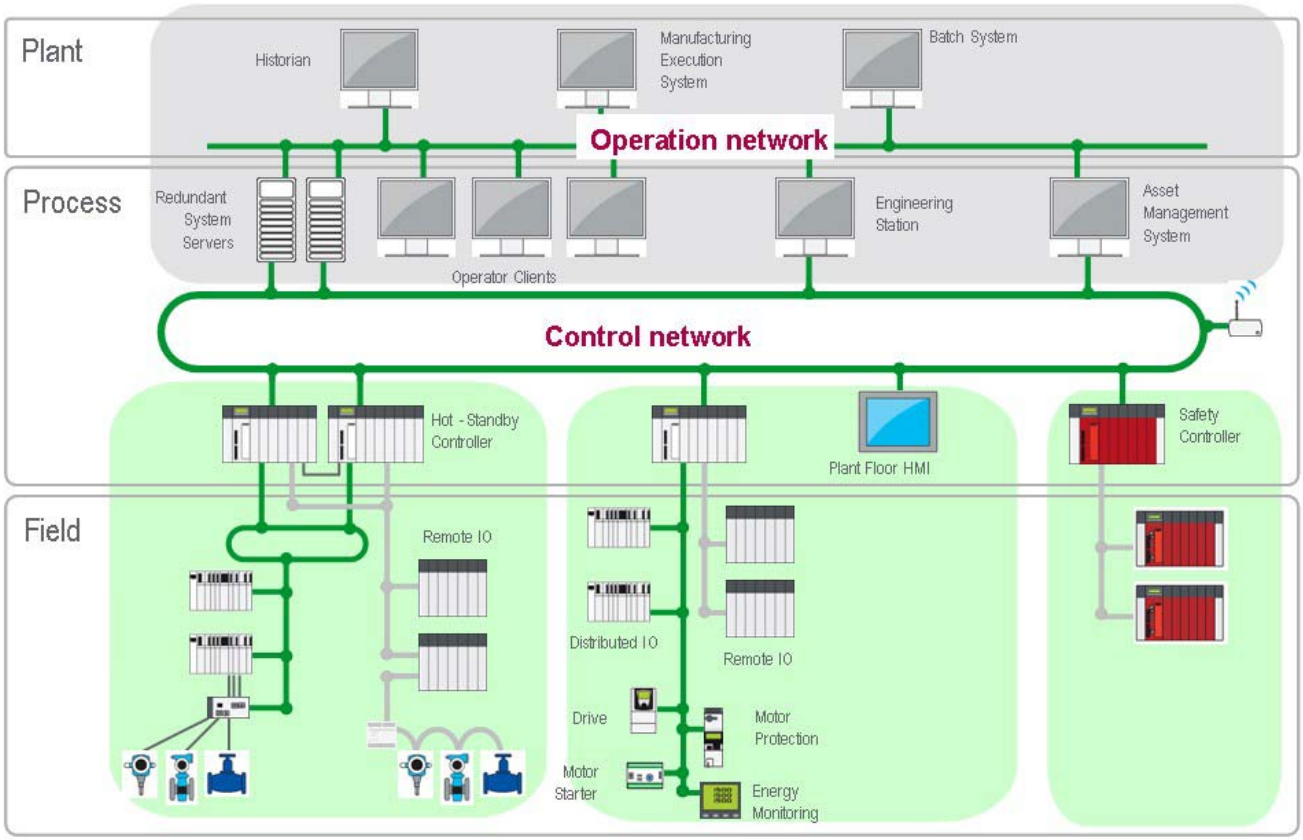


Figure 14 Sample Control Systems Diagram

Security Plan

The security plan defines the policies on which the defence-in-depth implementation is based and the job- and role-specific procedures to execute those policies. The security policies and procedures define:

- Roles and responsibilities of those affected by the policy and procedures.
- Actions, activities, and processes that are allowed and not allowed.
- Consequences of non-compliance.
- Incident response policies and procedures. These define the steps to take if a cyber attack or accident occurs and should include:
  - Incident response plan. Who to notify and what actions to perform to contain the incident.
  - Incident recovery plan. Role-specific procedures for restoring devices and process to known good operating state.

The security plan also details the equipment, software, protocols, procedures, and personnel involved in implementing the components of the defence-in-depth program.

The security plan summarizes the findings of the risk assessment phase and includes detailed network diagrams. It also includes the training plan.

Develop and maintain the security plan with a team representing management, IT staff, control engineering, operation, and security experts.

Review the security plan periodically for changes in threats, environment, and adequate security level.

Training

Awareness plays an important role in the success of a defence-in-depth campaign and the development of a security conscious culture. Schneider Electric recommends the establishment of a two-phase training program for employees and other agents.

The first training phase is a cybersecurity awareness program that educates stakeholders on the organization's security policies, procedures, and standards. This is an ongoing program with update sessions given regularly.

The second training phase includes job- and role-based training classes that detail the relevant security policies, procedures, and standards that pertain to a particular job or function. These classes provide specific steps for applying the security policies and procedures. They also include specific instructions to follow if a cyber attack or accident has occurred.

Also consider providing training classes for vendors, outside repair personnel, and other visitors. These classes provide an overview of company security policies and procedures with a special emphasis on the privileges and restrictions that apply to the visitor.

Network Separation and the DMZ

A firewall Demilitarized Zone (DMZ) separates the industrial control networks from the enterprise and other external communication paths. Bounded by a firewall as shown in Figure 15, "DMZ in Network Architecture", the DMZ provides a security layer to help protect the control room's operations network and the deeper control and device networks.

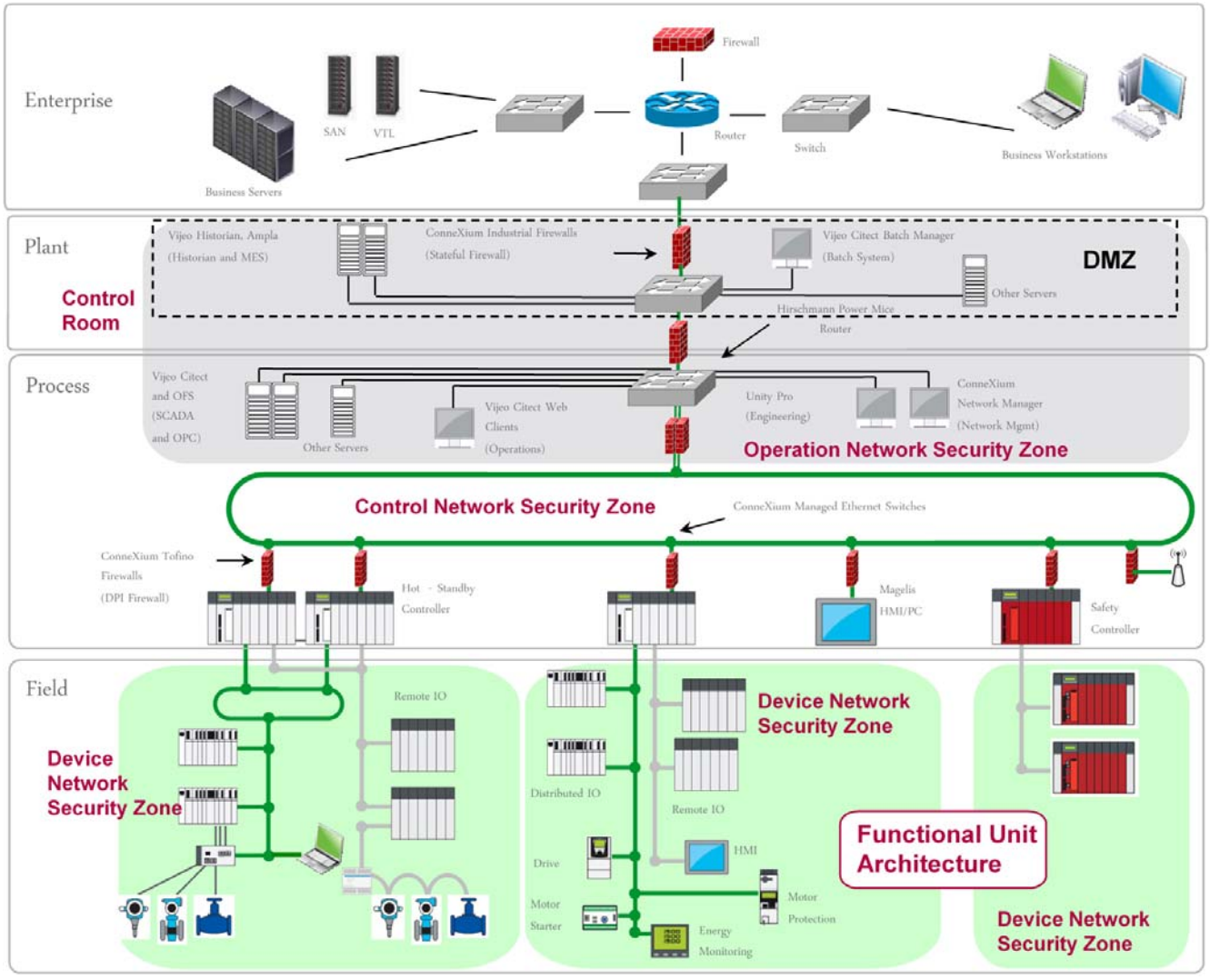


Figure 15 DMZ in Network Architecture

External requests and data terminate at controlled and dedicated servers and services within the DMZ. Requests and data from the control and operations networks terminate at servers and services in the DMZ. Allow no direct path of communication between the industrial control systems and the enterprise networks. For instance, industrial commands cannot travel from the enterprise to the control network, and industrial messages cannot travel from the control to the enterprise network.

Servers and services within the DMZ can include:

- Data servers such as Citect Historian that collect data from the SCADA systems and share it with MES or other reporting systems
- Patch management servers

- Proxy servers for web-connectivity or other protocols
- RADIUS and VPN servers

Some variations of the DMZ approach include a dedicated server or proxy within the DMZ to function as the sole conduit for communications between protected and external networks.

DMZ Guidelines

Take the following measures to provide higher levels of security with DMZs:

- Filter inbound traffic to the control room through a firewall before allowing a connection to a server or service in the DMZ. Likewise, filter outbound traffic from the control room to external network. This traffic should be minimal and tightly controlled on a per protocol, per host and per user basis. Filter traffic destined to the control network from the operations network. Filter traffic from the control network to the operations network. For example, multicast traffic should not enter or leave the control network
- Establish security policies limiting outbound traffic to required communications only. Devices on any industrial control systems network, including the operations, control, or device networks, should not have Internet access.
- Configure the firewalls so that outbound traffic to the corporate network is source- and destination-restricted by service and port.
- Configure firewalls to accept IP packets only if those packets have a correct source IP address for the control network, operations, or enterprise networks. The firewalls should drop any packet that comes in from the enterprise network with a source IP address that matches the address range of any of the control networks. This scenario is indicative of a spoof or errant route.
- Harden servers in the DMZ. See "Hardening Vijeo Citect SCADA Systems" on page 56 for examples of relevant server and client hardening methods.
- Perform security patches and antivirus software updates on a documented, monitored schedule.

Network Segmentation

Divide the control network into logical segments and establish security zones. For instance, in Figure 15, "DMZ in Network Architecture" on page 23, the control network itself is a security zone, and the field network level is divided into three separate device network security zones.

Network segments can be established using devices such as managed Ethernet switches, which provide virtual LAN (VLAN) and access control list management capabilities, firewalls, and routers.

As a first level of defence, ConneXium managed Ethernet switches can be configured to help protect every port from unauthorized access. Port access can be defined for a particular MAC or IP addresses..

Additionally, the rate limiter feature on ConneXium switches can help reduce the likelihood of DoS and other flood attacks. The rate limiter allows the user to specify the maximum amount of traffic allowed in or out of each port.

VLAN functionality can be used to further restrict traffic by segmenting the physical network into multiple logical networks.

Segmentation facilitates the establishment of security zones. A security zone can consist of one or more network segments. Traffic into and out of a zone is subject to a zone-specific set of rules, enforced, monitored, and supported through the use of devices such as ConneXium Industrial Firewalls. The organization of zones can be influenced by many factors including function, location, and security requirements. For instance, a zone may consist of network segments and devices located near each other that serve a related functional task. Another network zone may contain devices that share a common set of security requirements.

Network segmentation and the establishment of security zones can help to:

- Contain malware infections to one network segment.
- Improve security by limiting node visibility.
- Stop intruder scans at the network level before they reach a potential target system.
- Limit the impact of a security breach on a network.
- Restrict broadcasts and multicasts to particular Virtual LANs (VLANs).
- Improve network performance and reduce network congestion.
- Control communication access between segments providing critical devices or systems get a higher level of security.

Virtual LANs (VLANs)

One common method of network segmentation is the use of Virtual LANs (VLANs). VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, simplify network design, and provide another layer of security. For instance, in the architecture shown in Figure 15, "DMZ in Network Architecture" on page 23, a separate VLAN could be established for each of the three device network security zones.

VLAN is an OSI Layer 2 broadcast domain configured on ConneXium managed Ethernet switches and other switches on a port-by-port basis. Traffic on each VLAN segment is isolated from other VLANs. The switch does not filter traffic between two devices on the same VLAN. VLANs can limit the impact of a security breach if a system in one VLAN becomes compromised.

ConneXium managed Ethernet switches provide port-based VLANs per IEC 802.1 Q standard.

VLAN Guidelines

VLAN grouping strategies vary greatly, but common strategies include grouping by:

- Functional or cell/area zone: Each VLAN carries only that traffic which is necessary for the operation of a particular cell/area zone.
- Access requirements: VLANs are grouped according to the access requirements of different types of users such as operators, engineers, and vendors.
- Security: VLANs are grouped to support the control of access to sensitive information, devices, and processes.
- Traffic: VLANs are grouped to balance traffic load in support of the required throughput.

Segmentation guidelines include:

- Use one VLAN per ring topology for all manufacturing traffic per cell/area zone.
- Contain voice over Internet protocol (VoIP) on a dedicated VLAN.
- Assign a restricted VLAN identifier (ID) to packets entering the DMZ from the enterprise network so those packets can access only specific devices in the DMZ.
- Remove all unnecessary traffic from each VLAN.
- Apply quality of service (QoS) access control lists (ACL) to rate-limit the amount of ping traffic allowed.
- Avoid protocols such as telnet and FTP that send passwords in clear text. Use secure shell (SSH) and SFTP sessions if the device supports those protocols. If telnet or FTP is needed, use ACLs or firewall rules to allow connections only between specific hosts.
- Connect untrusted devices to untrusted ports, trusted devices to trusted ports.
- Disable unused ports or put them into an unused or untrusted VLAN that has very restricted access.
- Avoid the use of **VLAN 0 Transparent Mode**. In this mode, the packets are sent without VLAN membership.

Communication Between VLANs

Once the network is segmented into VLANs, users need restricted communications between VLANs. This can be achieved by use of a Layer 3 switch/router that maps traffic from one VLAN to another. Schneider Electric recommends the Hirschmann MICE range of Layer 3 switches or the ConneXium Industrial Firewall configured in routing mode for this purpose.

Firewalls

Firewalls help protect networks by blocking unauthorized access and permitting authorized access. A firewall is a device or set of devices configured to permit, deny, drop, encrypt, decrypt, or proxy traffic between different security zones based upon a set of rules and other criteria. Additionally, firewalls can support event logging to a syslog server or to an internal event log in the firewall. Event logging is used to monitor security events and alarms that occur on an industrial network and can be used to identify network threats. Typical events that can be monitored are:

- Firewall interface up/down
- Attempted log-in to firewall
- Packets matching firewall rule allow or deny
- Denied packets that do not match a rule
- Power failure or power recovery

It is recommended to systematically store and then review these event logs. Entries related to access denial and packet denials should be investigated as they might indicate an attempt to use the industrial protocol to compromise the system. A systematic practice of collecting and reading logs helps administrators identify attacks.

Process control devices require fast data throughput and often cannot tolerate the latency introduced by an aggressive security strategy inside the control network. Firewalls play a role in a security strategy by providing levels of protection at the perimeters or even inside the network. As illustrated by the redundant stateful firewalls that bound the DMZ in Figure 15, "DMZ in Network Architecture" on page 23, a control system relies heavily on perimeter protection and network segmentation to block unwanted and unauthorized traffic.

Common firewall types include the following:

- **Packet Filtering Firewalls**. A packet filtering firewall is a first-generation basic firewall that exerts minimal impact on network performance. Packets are filtered based on basic information in each packet, such as IP address (source and destination) and port number. Rules based on this information are established to determine if a packet will be forwarded or dropped. However, first generation firewalls that provide only packet filtering are not recommended for use in control systems. They lack authentication and do not conceal the protected network's architecture.
- **Application-Proxy Gateway Firewalls**. An application proxy gateway firewall examines packets at the application layer and filters traffic based on rules that regulate access by applications such as browsers or protocols such as FTP. It also acts as a gateway for client requests, determining the final server address. Application proxy gateway firewalls provide a high level of security, but can cause overhead delays that slow down network performance. These firewalls are suitable for systems located in the control room operations network, but not for the performance-sensitive networks of the control system.

- **Host Firewalls**. A host firewall is a software-based firewall that resides on a host device and protects its ports and services. Most laptops, servers, and workstations today feature integrated host firewalls. Host firewalls support the creation of customized rules to help protect particular ports and services. Host firewalls are an important feature of laptops, mobile devices, engineering workstations, and HMIs in industrial networks.
- **Stateful Inspection Firewalls**. Stateful multilayer inspection firewalls, such as the ConneXium Industrial Firewall, combine features of all of the other firewall types. They filter packets at the network layer and validate that the session packets and their contents at the application layer are legitimate. A stateful multilayer inspection firewall also keeps track of the network connections (such as TCP and UDP connections) that traverse the firewall. It allows packets that match known good connections and rejects those that do not match. Stateful inspection checks that inbound packets are the result of an outbound request. Stateful inspection firewalls provide a high level of security, good performance and require less configuration effort.
- **Deep Packet Inspection Firewalls**. Deep packet inspection firewalls, such as the ConneXium Tofino, typically offer the same benefits as stateful firewalls but also offer the ability to interrogate and make forwarding decisions based on the analysis of application packets. For instance, the Tofino can filter based on Modbus and extended Modbus protocols. These firewalls can block certain message types, control application traffic from specific hosts, and help stop application traffic from flooding critical devices. A potential disadvantage of deep packet inspection firewalls is that they can have a greater negative impact on performance than stateful firewalls.

NIST Firewall Guidelines

The National Institute of Standards and Technology (NIST) published the following firewall guidelines in its *Special Publication 800-82: Guide to Industrial Control Systems*:

- By default, "deny all, permit none." (When defining explicit or implicit deny rules, Schneider Electric recommends implementing a drop action rather than a reject action. This prevents system interrogation from external sources.)
- Ports and services between the control system network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
- All "permit" rules should be both IP address and TCP or UDP port specific.
- All rules should restrict traffic to a specific IP address or range of addresses.
- Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in a DMZ.
- Any protocol allowed between the control network and the DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).
- All outbound traffic from the control network to the operations network should be source and destination-restricted by service and port.

- Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.
- Control network devices should not be allowed to access the Internet.
- Control networks should not be directly connected to the Internet, even if protected via a firewall.

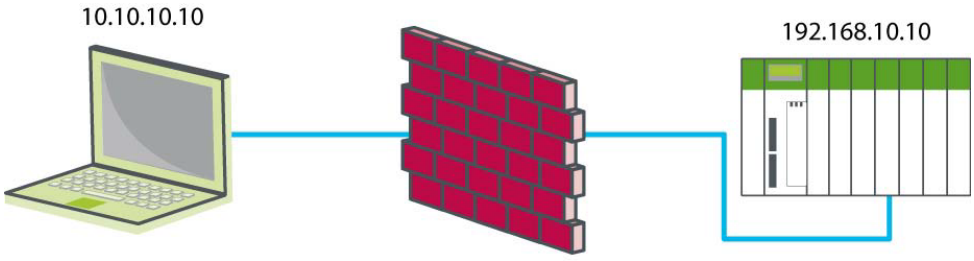
Other Firewall Risk Mitigation Guidelines

Packet Filtering

Packet filtering provides network security based on unique applications and protocols. It filters packets based on IP protocol and the packet source IP address, source port, destination IP address, and destination port. Schneider Electric's ConneXium Industrial Firewall is a stateful firewall.

With packet filtering, access to a device can be restricted to allow only specific protocols (ports).

In Figure 16, "Packet Filtering", the PC communicates with the PLC via port 80, but port 69 messages are blocked by the firewall.



Access List				
System Integrator	Port	NOE Address	Port	Allow
10.10.10.10	Port 80	192.168.10.10	80	OK
10.10.10.10	Port 69	192.168.10.10	69	Block

Figure 16 Packet Filtering

Ports that need extra protection due to inadequate built-in security include:

Table 1: Non-Secure Protocols

Application Protocol	Internet Procotol	Port Number
Telnet	TCP	23
HTTP	TCP/UDP	80
SNMP v1 & v2	TCP/UDP	161
FTP	TCP	20: data 21: command
TFTP	UDP	69

Table 1: Non-Secure Protocols

Application Protocol	Internet Procotol	Port Number
DNS	TCP/UDP	53
POP3	TCP	110
SMTP	TCP/UDP	25
Modbus TCP	TCP	502

Packet filtering should be implemented on incoming connections (untrusted ports) and on outgoing connections (trusted ports).

Some firewalls can inspect the protocol to make intelligent decisions about allowing or restricting specific messages. These firewalls can look into a protocol such as Modbus TCP (port 502) and allow certain function codes to pass while blocking others. An example is the ConneXium Tofino Firewall.

Flood Protection

DoS attacks are a common form of flood attacks. If a DoS attacker penetrates the control network, the impact can be minimized using flood protection provided in the firewall. The sample ConneXium firewall configuration screen in Figure 17, "Sample ConneXium Firewall DoS Protection Configuration Screen" allows the user to set limits on certain traffic types, such as a high number of incoming or outgoing TCP connections per second that could indicate a DoS attack.

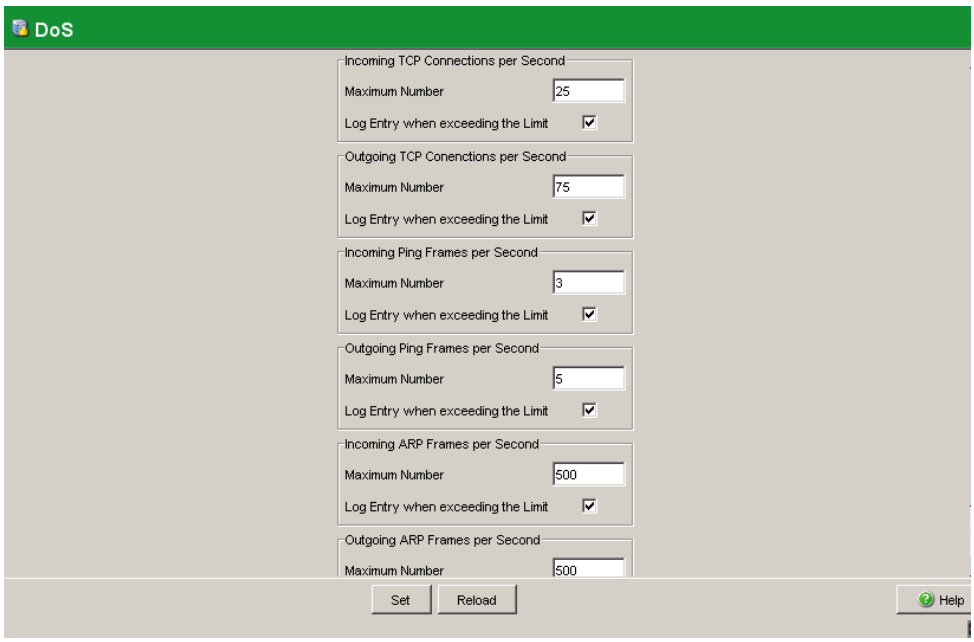


Figure 17 Sample ConneXium Firewall DoS Protection Configuration Screen

Firewalls and Specific Services

This section expands on the network segmentation component of Schneider Electric's defence-in-depth approach. It describes how firewalls process and help manage many of the protocols and services used in industrial control systems, including DNS, HTTP, DHCP, FTP, TFTP, telnet, SMTP, POP , SNMP, and NAT.

Firewalls and Domain Name System (DNS) Server

A Domain Name System (DNS) server is a database used to translate domain names to IP addresses. Many Internet services rely on DNS, but DNS is not commonly used by control systems. According to the NIST, "In most cases there is little reason to allow DNS requests out of the control network to the corporate network and no reason to allow DNS requests into the control network."

DNS Vulnerabilities

DNS servers are vulnerable to many exploits, including DNS cache poisoning and DNS amplification attack.

DNS cache poisoning is initiated by replacing the intended domain IP address with the attacker's domain IP address. Web traffic, e-mail, and other network data can then be redirected to systems under the attacker's control.

DNS amplification attack is a type of DoS attack that generates traffic overload.

DNS Risk Mitigation

Avoid DNS requests from the control network to the corporate network whenever possible. Address exceptions on a case-by-case basis.

Avoid allowing DNS requests into the control network.

If DNS is required, configure the firewall to use specific DNS servers instead of those allocated by an ISP. For instance, on the ConneXium Industrial Firewall **DNS Server** screen, set **DNS Client Configuration** to **User** and enter the IP addresses of up to four DNS servers. Queries will be sent to those servers, and queries will not be sent to any DNS server addresses allocated by an ISP.

Firewalls and Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol is the underlying protocol used by the World Wide Web. It is used in control systems to support embedded Web servers in control products. Schneider Electric Web servers use HTTP communications to display data and send commands via Web pages.

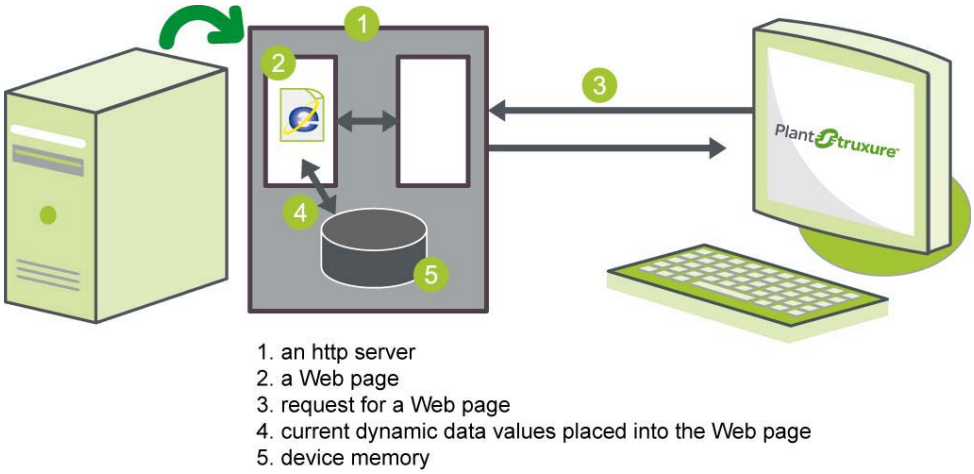


Figure 18 Sample HTTP Exchange

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the HTTP and a cryptographic protocol. By default, HTTP uses port 80 and HTTPS uses port 443.

HTTPS transmits normal HTTP with encryption, commonly using either Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL).

HTTP Vulnerabilities

HTTP has little inherent security and can be used as a transport mechanism for attacks and worms. Common attacks are man-in-the-middle and eavesdropping.

HTTP Risk Mitigation

If the HTTP server is not needed, disable it. Otherwise, use HTTPS instead of HTTP if possible and only allow traffic to specific devices.

Firewalls and DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol based on BootP. It is used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. DHCP is an unauthenticated protocol. The DHCP service works by using the DORA (Discover, Offer, Request, and Acknowledgment) grants.

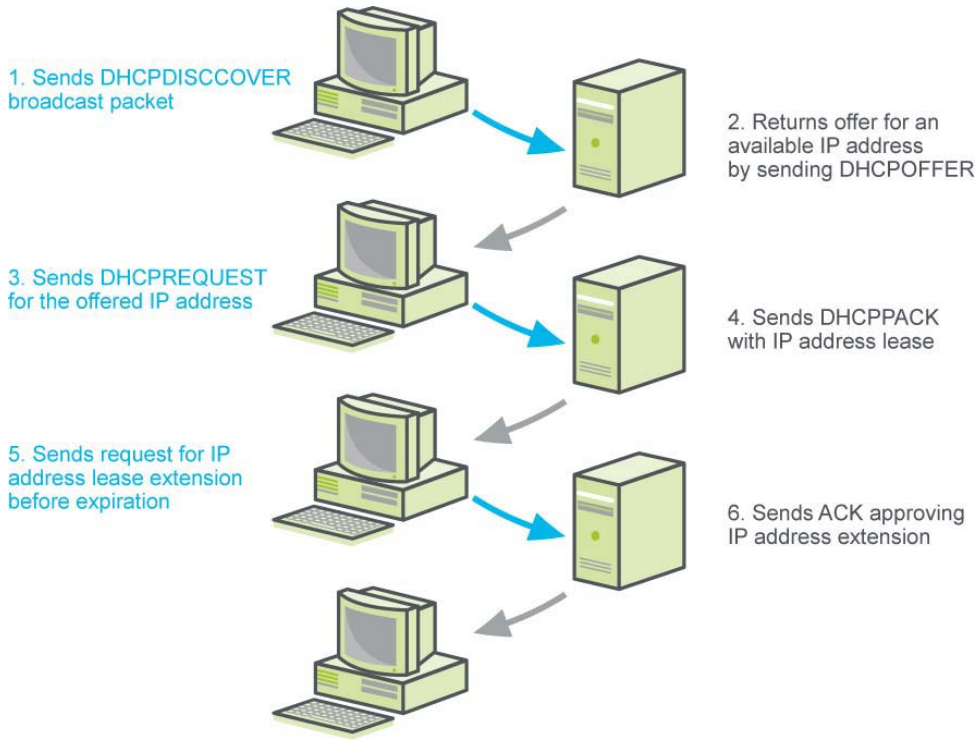


Figure 19 Sample DHCP Exchange

DHCP service uses port 67/UDP in the DHCP server, and 68/UDP in the DHCP clients.

Schneider Electric uses DHCP for Fast Device Replacement (FDR).

DHCP Vulnerabilities

There are two common types of DHCP attacks:

- DHCP starvation attack: The DHCP server is inundated with requests from different MAC addresses. The DHCP server eventually runs out of IP addresses blocking legitimate users from obtaining or renewing their IP addresses.
- DHCP rogue attack: The attacker disguises itself as a DHCP server, responds to a DHCP request with false IP addresses, and then launches a man-in-the-middle attack.

DHCP Risk Mitigation

Allow only authorized persons to have physical or wireless access to the device.

If DHCP is not needed, disable it in the firewall or any device supporting DHCP.

Some Schneider Electric PAC network communication modules have built-in DHCP servers. The DHCP server uses the device's MAC address or device name to serve the IP configuration and the name and location of the configuration file.

Firewalls and FTP or TFTP

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are used for transferring files between devices. TFTP a simplified unidirectional protocol commonly used for special purpose file transfers such as the transmission of boot files between devices.

Schneider Electric Ethernet devices use FTP for various tasks including to firmware loading, display of custom Web pages, and the retrieval of logs and historical data files.

FTP Vulnerabilities

FTP uses a login password that is not encrypted. TFTP requires no authentication. FTP is vulnerable to buffer overflow and FTP Bounce attacks. The FTP bounce attack uses an FTP server in passive mode to transmit information to any device on the network. To begin the bounce attack process, the attacker logs into the FTP server that will be used as the middleman. Once connected to the FTP server, the attacker sends the PORT command to direct all data connections to the illegitimate destination IP address and TCP port.

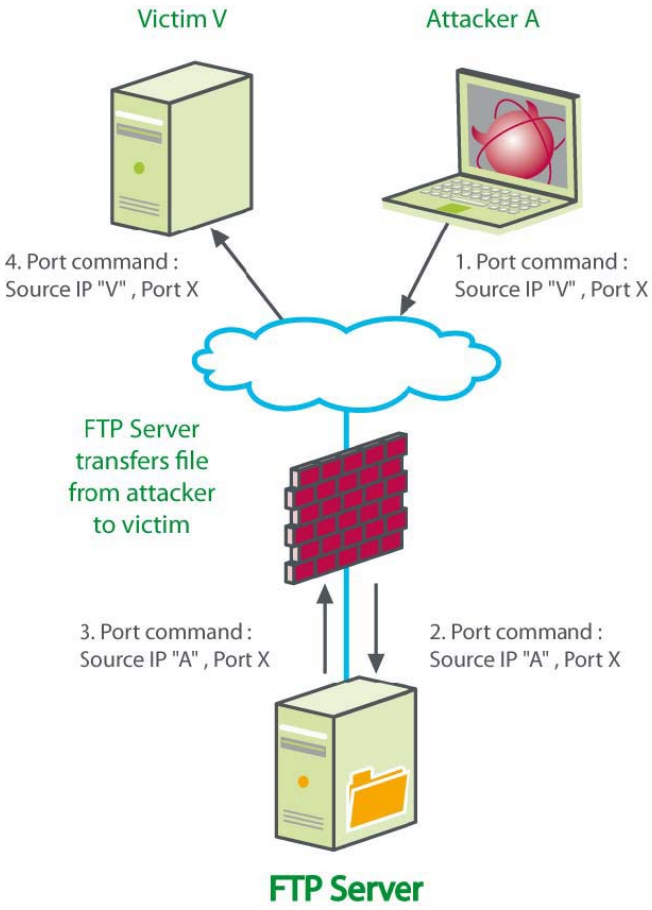


Figure 20 Sample FTP Attack

FTP Risk Mitigation

Allow FTP communications for outbound sessions only unless secured with additional token-based multi-factor authentication and an encrypted tunnel.

If possible, use more secure protocols such as Secure FTP (SFTP), FTP Secure (FTPS) or Secure Copy (SCP).

Configure each server connection individually.

Use packet filtering to allow access only to the FTP server.

Block TFTP communications if they are not required.

Firewalls and Telnet

The telnet protocol provides interactive, text-based communications between a client and a host. Telnet provides access to a command-line interface, typically via port 23. It is mainly used for remote login and simple control services to systems with limited resources or to systems with limited needs for security. Due to security risks, Schneider Electric has limited the use of telnet in its products.

Telnet Vulnerabilities

Telnet is a severe security risk. All telnet traffic, including passwords, is unencrypted. This can allow an attacker considerable control over a device.

Telnet Risk Mitigation

Inbound telnet sessions from the corporate to the control network should be prohibited unless secured with authentication and an encrypted tunnel such as a VPN tunnel.

Outbound telnet sessions should be allowed only over encrypted tunnels to specific devices as described in "Remote Access Control with RAS or VPN" on page 42.

The ConneXium managed switches provide the option to disable the telnet interface. Disable the telnet interface when not using the command line interface to configure the switch.

For the protocol HTTP or FTP if supported use SSH the secure equivalent protocol.

Firewalls and Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3)

Email notification in the automation industry is becoming more prevalent as plants increasingly rely on off-site personnel to troubleshoot and fix detected problems. Schneider Electric Ethernet devices send e-mail but do not receive it. However, there is potential that non-Schneider Electric devices residing on the network can receive e-mail. Use anti-virus software to scan e-mail for viruses. No email client should be enabled on any dedicated control room workstation or server. If receiving email is required, the mail should be received on dedicated business machines connected on the enterprise network.

The Simple Mail Transport Protocol (SMTP) is an Internet standard used by e-mail clients or mail transfer agents (MTA) to send e-mails. An SMTP server performs two functions:

- Verifies that the configuration is valid and grants permission to the computer sending the message.
- Sends the outgoing message to a predefined destination and validates the successful transfer of the message. If the message is not successfully transferred, a message is sent back to the sender.

Post Office Protocol v3 (POP3) or Internet Message Access Protocol (IMAP) is used by local e-mail clients to download e-mail from a remote server. The POP3 server receives the e-mail message and retains the e-mail message until it is retrieved by the local client. POP3 uses port 110.

Figure 21 Sample SMTP & POP3 Exchanges

SMTP and POP3 Vulnerabilities

Directory harvesting is a common form of e-mail attack. The attack relies on invalid e-mail addresses being rejected by the e-mail system either during the SMTP conversation or afterwards via a Delivery Status Notification (DSN). When the attacker receives a rejection from an invalid e-mail address, the e-mail address sent is discarded. When no rejection or DSN is received, the e-mail address is considered valid and is added to a spam database. The attacker typically uses two methods:

- Brute force: an approach that sends messages with all possible alphanumeric characters and waits for a valid response.
- Selective: an approach sending an e-mail using a likely username in hopes of finding a valid one, as shown in Figure 22, "Selective e-Mail Attack".

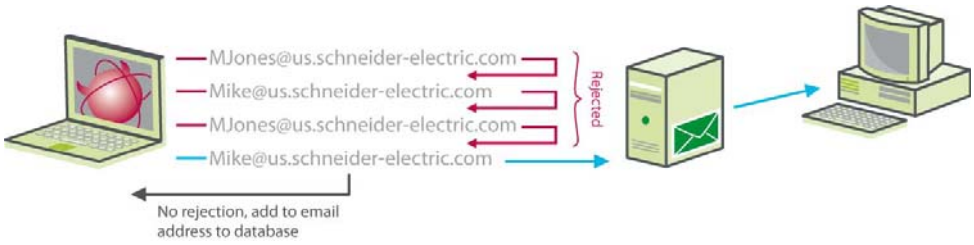


Figure 22 Selective e-Mail Attack

SMTP and POP3 Risk Mitigation

Avoid allowing inbound e-mail to any control network device.

Allow outbound e-mail only when necessary. For instance, a device may send an alert by e-mail.

Firewalls and Simple Network Management Protocol (SNMP)

SNMP provides network management services between a central management console and network devices such as routers, printers, and PACs.

SNMP consists of three parts:

- Manager: an application that manages SNMP agents on a network by issuing requests, getting responses, and listening for and processing agent-issued traps.
- Agent: a network-management software module that resides in a managed device. The agents allow configuration parameters to be changed by managers. Managed devices can be any type of device: routers, access servers, switches, bridges, hubs, PACs, drives.

- Network management system (NMS): the terminal through which administrators can conduct administration tasks.

Schneider Electric Ethernet devices have SNMP service capability for network management. Many Schneider Electric Ethernet devices use SNMP v1, which does not use encryption and is therefore considered insecure.

ConneXium switches are an exception. They use SNMP v3, which uses encryption, authentication, and security features to enhance message integrity. Inherently they also support SNMP v1 and v2.

SNMP Vulnerabilities

SNMP in general is weak in security. Versions 1 and 2 of SNMP use unencrypted community names to both read and configure devices. Community names may not be able to be changed. Version 3 is more secure but is still limited in use.

Often SNMP is automatically installed with **public** as the read string and **private** as the write string. This type of installation provides an attacker the means to perform reconnaissance on a system to create a denial of service.

SNMP also provides information about the system that may allow the attacker to piece together the network system with the interconnection.

SNMP Risk Mitigation

- When possible, deactivate SNMP v1 and v2 and use SNMP v3, which encrypts passwords and messages.
- Change the default passwords of devices that support SNMP.
- Block inbound and outbound SNMP traffic at the boundary of the enterprise network and operations network of the control room.
- Filter SNMP v1 and v2 commands between the control network and operations network to specific hosts or communicate with them over a separate, secured management network.
- Control access by identifying which IP address has privilege to query an SNMP device.
- If SNMP v1 or v2 is needed, use access settings to limit the devices (IP addresses) that can access the switch. Assign different read and read/write passwords to devices.

Firewalls and Network Address Translation (NAT)

Network Address Translation (NAT), also known as IP masquerading, is a service that conceals a device's true IP address from the outside world to keep outside agents from accessing the device directly. As illustrated in Figure 23, "Sample NAT Exchanges", IP addresses used on one side of a network device are mapped to a different set on the other side.

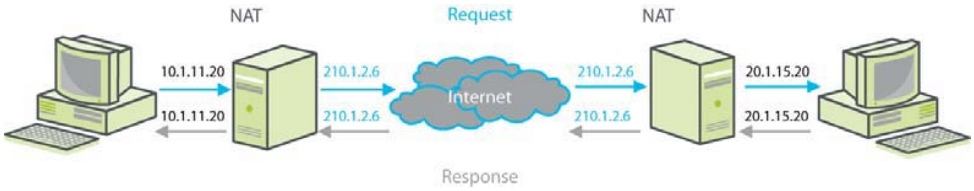


Figure 23 Sample NAT Exchanges

NAT maps the entire network to a single IP address prior to transmitting. NAT relies on the premise that not every internal device is actively communicating with external hosts at any given moment. The firewall tracks the state of each connection and how each private internal IP address and source port was remapped. When the response is received by the firewall, the IP address mapping is reversed and the packets forwarded to the proper internal host.

Although NAT routers are not technically firewalls because they do not filter the packets, NAT does offer devices a level of protection from external networks. NAT does not allow inbound packets that were not sent in response to a request from accessing the device directly.

NAT technology was introduced to slow the advance of IP address space depletion and not as a security mechanism. When incorporating NAT, the use of private IP addresses is possible for devices that need to communicate over the internet. As a side effect, NAT does conceal the true IP address of a device to the outside world. However, it is not in the specification that it will conceal the internal architecture and it should not be used as a security mechanism.

NAT Vulnerabilities

None known.

ConneXium Industrial Firewall NAT Features

NAT features supported by the ConneXium firewall include:

- **1:1 NAT** can be used when setting up identical internal production cells that use the same IP addresses but need to be connected to an external network. The firewall replaces the source IP address of a data packet from the internal network with an IP address of the external network.
- **Inverse 1:1 NAT** allows devices in an internal network to communicate with devices in an external network as if the devices in the external network were in the internal network. With inverse 1:1 NAT, the firewall replaces the destination IP address of a data packet from the internal network with an IP address of the external network

- **Double NAT** allows devices in an internal network to communicate with devices in an external network as if the devices in the external network were in the internal network, and vice versa.

  To devices in the internal network, the firewall allocates a different IP address in the external network (1:1 NAT function). To devices in the external network, the firewall allocates a different IP address in the internal network (inverse 1:1 NAT function).

- **NAT -IP Masquerading** hides the internal network structure (IP addresses) from an external network. The firewall replaces the source IP address of a data packet from the internal network with the external IP address of the firewall.

- **NAT Port-Forwarding** hides the internal network structure from the outside but allows a communication connection to be set up from the outside in. External devices can set up a communication connection to the internal network, and send data packets to a specific port with the external IP address of the firewall.

NAT Configuration Recommendation

Use NAT whenever possible. NAT does not support producer-consumer protocols such as Ethernet/IP or Foundation Fieldbus.

Since NAT is usually used on routers and network gateways, its use requires enabling IP forwarding so that packets can travel between networks.

System Access Control

Regulating access to the control system is an important component of the defence-in-depth approach. This section describes external authentication and authorization with RADIUS, providing secure access with remote access services (RAS) and VPN, and providing security while allowing access for remote control.

External Authentication with RADIUS

Authentication, authorization, and accounting (AAA) protocols authenticate users before granting access to network assets, authorize them for particular assets, and account for use of those assets. AAA is commonly used for access into trusted networks.

Remote Authentication Dial in User Service (RADIUS) is an AAA protocol commonly used in control systems.

RADIUS is a client-server protocol that provides centralized and scalable user management where network devices might number in the hundreds or more. When embedded devices such as switches, PACs, or firewalls have the storage capacity to handle only a few user accounts, RADIUS can substantially increase the number of supportable user accounts. RADIUS also helps to enforce consistency in security policy and user access. It also helps with account management by providing a single location for all accounts.

RADIUS clients are supported by many VPN servers, remote access servers, wireless access points, switches, routers, and other network access devices. Presently, RADIUS authentication is supported in ConneXium Industrial Firewalls and Schneider Electric wireless devices.

A RADIUS server is typically a process running on a Windows or UNIX system. For instance, Windows Server 2008 R2 offers a RADIUS server called Network Policy Server (NPS). In a secure network architecture, locate any dedicated RADIUS servers within the DMZ.

Some network devices also offer RADIUS servers. For instance, ConneXium wireless devices feature built-in RADIUS servers.

Transactions between the RADIUS client and the RADIUS server are authenticated with a shared secret, which is typically a password or pass code. Refer to Figure 24, "Sample RADIUS Authentication Exchange" below.

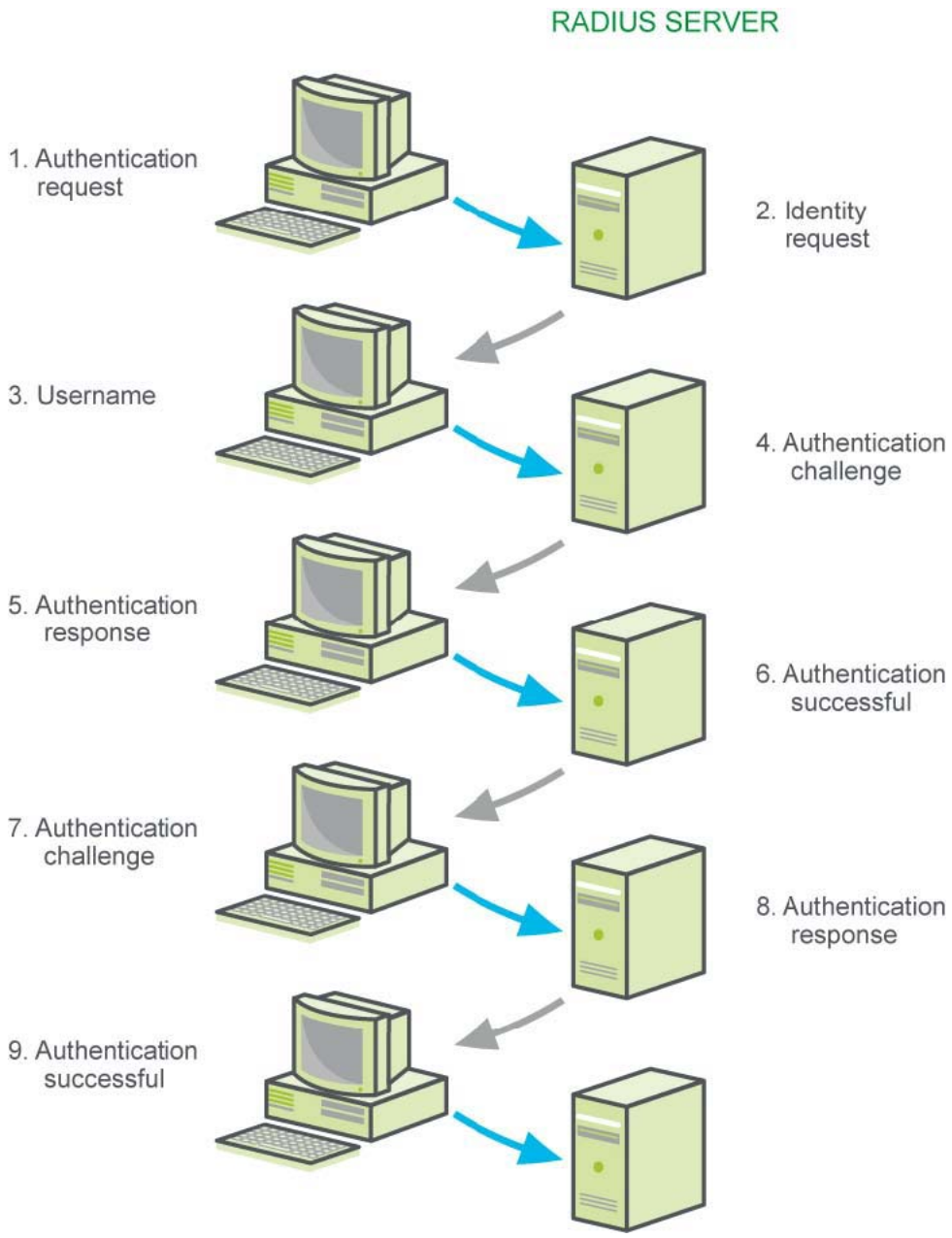


Figure 24 Sample RADIUS Authentication Exchange

Alternatives to RADIUS include Terminal Access Controller Access-Control System (TACACS), TACACS+ and Diameter protocols. These protocols are more commonly found on PC servers and clients than on embedded devices such as switches, PACs, and firewalls. TACACS+ and Diameter are TCP-based and support IPSec and TLS protocols.

RADIUS Authentication Vulnerabilities

The communication of user credentials between the RADIUS client and the RADIUS server is not strongly encrypted. The impact of the weak encryption is mitigated by a strong perimeter if the RADIUS server and client reside on the same internal network and that network is separated by a DMZ.

RADIUS does not encrypt transferred attribute values. This can potentially expose identifiable network elements. If the RADIUS server needs to proxy requests through untrusted networks or if the client and server are separated by untrusted networks, then use IPsec VPNs as described in "Remote Access Control with RAS or VPN" on page 42.

RADIUS Authentication Guidelines

- Use a different shared secret for each RADIUS server-RADIUS client pair. For example, each ConneXium wireless device or ConneXium firewall should have a unique shared secret.
- If possible, configure shared secrets with a minimum length of 16 characters consisting of a random sequence of upper and lower case letters, numbers, and punctuation.
- Implement RADIUS authentication on ConneXium firewalls and ConneXium wireless devices if there are many devices supporting RADIUS.
- For the ConneXium firewall use group authentication:
  - Group authentication allows the assignment of multiple users to groups via a RADIUS server. If the group authentication is active and an unknown person logs in to the user firewall, the firewall checks the user's authenticity via the RADIUS server. If the authentication is successful, and if the firewall has a user firewall account with this group name, the firewall gives the user access. This is particularly important when vendors might perform maintenance on the networks. Using external authentication with groups enabled provides a more secure way of allowing temporary bypass of normal firewall rules. This is also useful for defining user-based rules so software or firmware can be downloaded to critical equipment without the need to open up high-risk ports in the normal firewall table.
  - The credentials of the externally authenticated user should be entered and present in the user firewall accounts.

Remote Access Control with RAS or VPN

Many organizations allow engineers and support personnel to monitor and control the system from remote locations across the public Internet. Remote access to the control network can be susceptible to cyber attacks if not configured correctly.

Methods for providing and managing remote access include remote access servers and VPNs.

Remote Access Server (RAS)

In the RAS model, a remote client uses the telecommunications infrastructure (dial-up) to create a temporary physical circuit to a port on a remote access server. After the physical circuit is made, connection parameters are negotiated.

For additional security, the remote access server can be configured to call back users at a predefined number. This works well for static users but not for mobile users. Remote access servers typically offer asynchronous serial interfaces connected to external analogue modems, ISDN terminal adapters, or direct analogue/ISDN connections. Remote access servers are application-specific computer systems dedicated to the support of 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.

RAS implementations typically provide user credential authorization services. Common industry standard security features include password authentication procedure (PAP), challenge handshake authentication protocol (CHAP), and other feature-enhanced proprietary authentication capabilities.

Many RAS systems support security software protocols such as RADIUS. Other RAS security features include password encryption and data encryption.

VPN

A VPN provides security through encryption and authentication, helping to protect the data as it moves over the public Internet. A VPN client uses the Internet to create a virtual point-to-point connection with a remote VPN server. Figure 25 shows how a VPN can provide access to a secure network architecture.

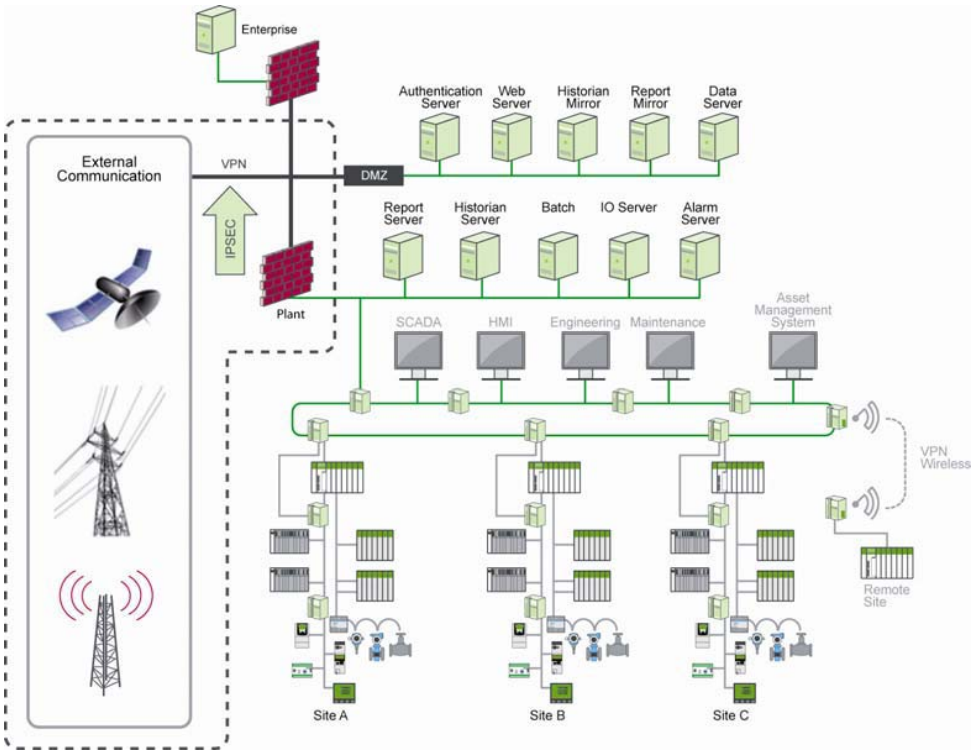


Figure 25 IPSec VPN Access Point in a Secure Network Architecture

Commonly used VPN technologies include secure socket layer (SSL) and the open standard Internet protocol security (IPsec). VPN technology based on SSL can use a web browser or client implementation.

SSL is a common protocol built into most Web browsers. SSL is easier to configure than IPsec and it does not require special client software. SSL works for Web-based (TCP) applications and supports Digital Signature and data encryption.VPN with IPsec provides more of the security features required for remote access to industrial control systems. IPsec is transparent to the application and uses IP network-layer encryption to provide private, secure communications over Internet Protocol (IP) networks. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection.

IPsec supports both digital signature and secret key algorithm.

Figure 26 IPsec

IPsec is a suite of standards for performing encryption, authentication, and secure tunnel setup. IPsec essentially creates private end-to-end tunnels out of the public bandwidth available on the Internet. IPsec uses the following components:

- Internet key exchange (IKE and IKEv2)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

IPsec can be used in transport mode or, as recommended by Schneider Electric, in the tunnel mode.

Transport mode connections are host-to-host. Only the data payload of the IP packet is encrypted and/or authenticated. If NAT is used it requires a special feature NAT-T.

In tunnel mode, connections can be established using gateway-to-gateway, gateway-to-host, or host-to-host architectures. The entire IP packet is encapsulated to help provide a virtual secure hop between two gateways and a secure tunnel across an untrusted Internet.

IPsec VPN tunnel uses algorithms to encrypt and decrypt user information. The three common encryption protocols are:

- AES (Advanced Encryption Standard) - use AES when possible - strong encryption.
- DES (Data Encryption Standard) - provides weak encryption and should not be used.
- Triple-DES (3DES) - effectively doubles encryption strength over DES.

Encrypted communication cannot be analyzed and filtered by firewalls, so if the host at one end of the VPN tunnel is compromised, it will compromise the other end.

A one-way encryption algorithm known as a hash takes an input message of arbitrary length and produces a fixed-length output message. Hash algorithms are used by Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP) to authenticate data. Popular hash algorithms include:

- Message Digest 5 (MD5): 160-bit key. After the inception of MD5, the hash algorithm was compromised and therefore is not recommended for use.
- Secure Hash Algorithm 1 (SHA-1): generates a 160-bit (20-byte) message digest. SHA-1 is slower than MD5 but offers greater protection against brute force attacks. After the inception of the SHA-1 algorithm, SHA-1 was compromised and therefore is not recommended for use.
- Secure Hash Algorithm 2 (256-bit) and 3 (512-bit) are recommended as they offer a much better encryption.

ConneXium Industrial Firewall VPN Features

The ConneXium Industrial Firewall supports the following VPN functions:

- Multipoint VPN: Router Mode
- VPN protocols: IPsec
- Encryption algorithms:
  - DES-56
  - 3DES-168
  - AES-128, AES-192, AES-256
- Authentication:
  - Pre-shared key (PSK)
  - X.509v3 certificates
- Hashing algorithms: MD5, SHA-1, SHA-2
- NAT-T support

Remote Access Vulnerabilities

- Inadequate access restriction.
- Firewall filtering deficiencies.
- Services allowed into the control system network.
- War dial-ups (computer dialing consecutive telephone numbers seeking a modem).
- Connection passwords programmed with vendor's default password.
- Access links not protected with authentication and/or encryption.
- Remote host security policies not present or up to date.
- Wireless has additional challenges because radio waves propagate outside the intended area:
  - Attackers who are within range can hijack or intercept an unprotected connection.
  - Wardriving is a common form of attack where a person in a moving vehicle uses a portable computer or PDA to search for a wireless device.

Remote Access Guidelines

- Approve and install remote access enabling hardware and software in strict accordance with security policies.
- Disable remote access when not needed. Enable it only when the access is required, approved, and authenticated. Consider risk to the process when allowing remote access.
- Change the password immediately after a remote maintenance session has terminated.

- For remote connections via dial-up modem or over the Internet, use an encrypted protocol such as IPsec. Once connected, request a second authentication at the control network firewall using a strong mechanism, such as a token-based multi-factor authentication scheme.
- Automatically lock accounts or access paths after a preset number of consecutive invalid password attempts.
- Change or delete any default passwords or User IDs. Change passwords periodically.
- For remote access modems, change default settings as appropriate:
  - Set dial-out modems to not auto answer.
  - Increase ring count before answer.
  - Use inactivity timeout if available.
  - Use callback whenever possible.
- Weigh the benefits of VPN usage against potential impacts.
- Configure the firewall for a VPN connection using a tunnel network-to-network configuration. Security guidelines apply to both ends of the VPN.

Access for Remote Control

Some applications require remote control, and in some cases, the latency introduced by a firewall can be unacceptably high for the remote control application. Therefore, remote access for remote control is sometimes allowed without going through a firewall. A security risk analysis by the organization is required to balance risk versus functionality.

Remote control with wireless brings additional security challenges. When remote control via wireless is needed, the recommended approach is to use VPN tunnel with IPsec as shown in Figure 27, "VPN Tunnel and IPsec to Help Mitigate Remote Control Risks". Configure firewall rules in ConneXium switches to allow connection via a VPN tunnel. For instance, to allow a VPN dial-in to the switch acting as VPN gateway, configure a firewall rule allowing incoming messages from a client to the network.

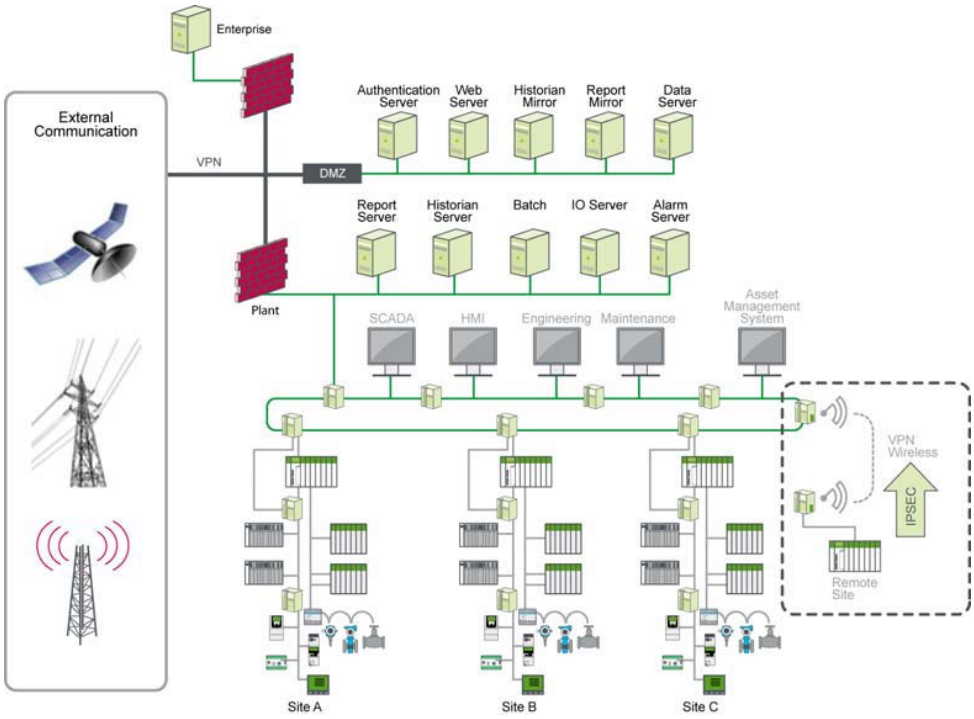


Figure 27 VPN Tunnel and IPsec to Help Mitigate Remote Control Risks

WiFi Remote Control Vulnerabilities

Vulnerabilities associated with IEEE 802.11 wireless include:

- Security settings either not configured or configured for poor security.
- Radio waves that propagate outside the intended area.
- Vulnerability to eavesdropping.
- Physical locations that permit easy access.
- Lack of security polices for setting up a wireless network.
- Attackers who are within range can hijack or intercept an unprotected connection, or 'signal jam' for which there is no countermeasure.
- War driving - a common form of attack where a person is searching for a wireless device in a moving vehicle, using a portable computer or PDA.

NIST Wireless Guidelines

The following wireless LAN guidelines were published by the National Institute of Standards and Technology (NIST) in its Special Publication 800-82: Guide to Industrial Control Systems as they are quoted below:

- Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. Faraday cages and other methods are also available to minimize exposure of the wireless network outside of the designated areas.
- Wireless users' access should use IEEE 802.1x authentication using a secure authentication protocol (e.g., Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]) that authenticates users via a user certificate or a Remote Authentication Dial In User Service (RADIUS) server.
- The wireless access points and data servers for wireless worker devices should be located on an isolated network with documented and minimal (single if possible) connections to the ICS network.
- Wireless access points should be configured to have a unique service set identifier (SSID), disable SSID broadcast, and enable MAC filtering at a minimum.
- Wireless devices, if being used in a Microsoft Windows ICS network, should be configured into a separate organizational unit of the Windows domain.
- Wireless device communications should be encrypted and integrity-protected. The encryption should not degrade the operational performance of the end device. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered.
- For mesh networks, consider the use of broadcast key versus public key management implemented at OSI Layer 2 to maximize performance. Asymmetric cryptography should be used to perform administrative functions, and symmetric encryption should be used to secure each data stream as well as network control traffic. An adaptive routing protocol should be considered if the devices are to be used for wireless mobility. The convergence time of the network should be as fast as possible supporting rapid network recovery in the event of a detected failure or power outage. The use of a mesh network may provide fault tolerance through alternate route selection and pre-emptive fail-over of the network.

ConneXium Wireless Access Point Security Features

Figure 28 shows ConneXium wireless access points used to reduce the risk of cyber attacks.

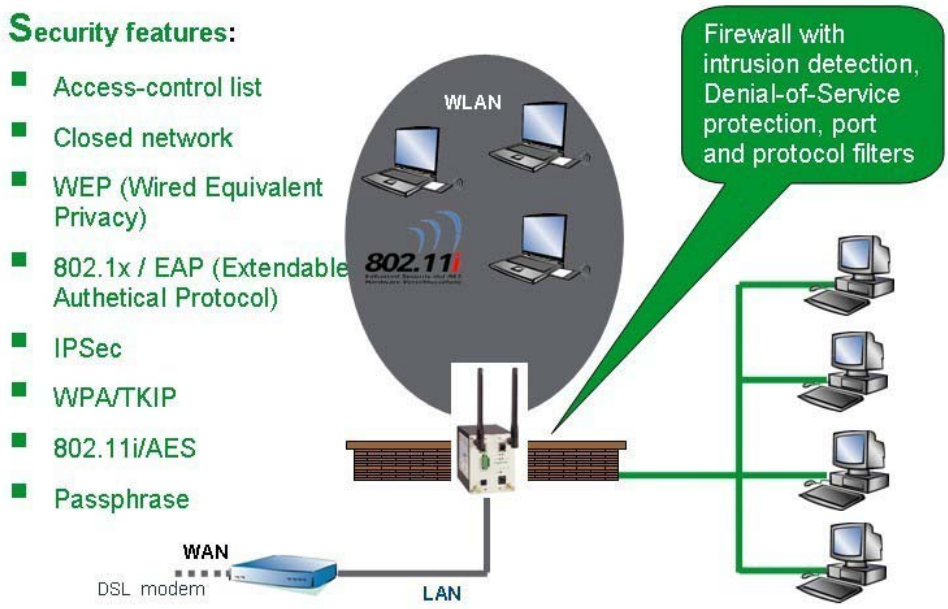


Figure 28 ConneXium Wireless Access Point Security Features

A ConneXium wireless access point can be configured to:

- Require password for device access.
- Lock the device after a programmed number of login attempts to counter brute force attack.
- Limit configurable parameters based on IP address.
- Use MAC and IP address-based black lists and white lists to provide port security.
- Restrict client communication to specific access.
- Provide denial of service protection. Packets from external networks are accepted only if a connection has been initiated from the internal network or if the incoming packets have been accepted by an explicit filter entry.
- Block access from a network to specific stations or domains via URL filter list.

ConneXium wireless access points also feature:

- Integrated RADIUS client and server for authentication.
- Intrusion prevention - firewall blocking of messages not authorized for network.
- Rogue access point detection - A rogue is a device that makes unauthorized attempts to access a WLAN by posing as an authorized access point or client. Background scanning identifies rogue access points and alerts administrators for potential action.
- NAT translation - Internal IP addresses are replaced by the IP address of the access point when communicating externally.

- Terminal access controller access-control system (TACACS) Authentication - Authentication technique for payment card applications.

Wireless Remote Control Risk Mitigation with ETG302x

Schneider Electric's FactoryCast ETG302x provides VPN capabilities for remote control. It is recommended that two ETG302x modules be used to control access to the control network from the RTU station using wireless.

The security recommendations for wireless access with the ETG302x include:

- Use a pre-shared key for authentication.
- Use IPsec tunnel mode.
- Use the preconfigured 3DES (high) encryption and set authentication encryption to SHA-2.
- Enable VPN on both ETG302x modules and configure remote LAN in each.

After enabling VPN mode on both ETG302x modules, configure the General Packet Radio Service (GPRS) DNS name and set the mode to tunnel as shown in the ETG302x configuration screen example in Figure 29, "Sample ETG302x VPN Tunnel Configuration".

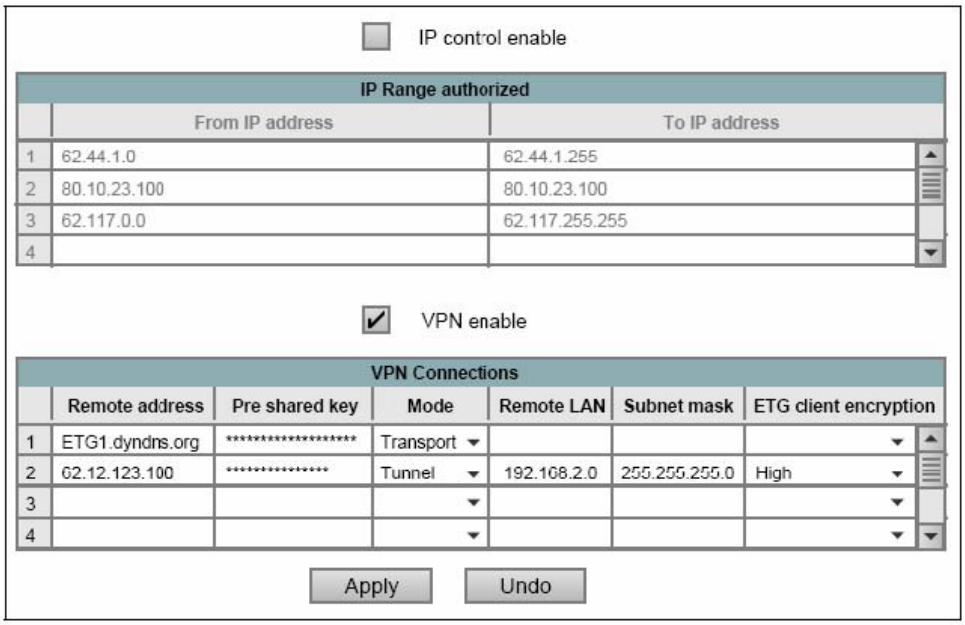


Figure 29 Sample ETG302x VPN Tunnel Configuration

Figure 30, "Sample ETG302x Wireless VPN Configuration" shows a fully configured system providing VPN access across the public Internet to help secure communications.

Legend	Parameter	Settings
1	ETG1 GPRS IP address	etg1.dyndns.org (use dyndns address)
2	ETG2 GPRS IP address	etg2.dyndns.org (use dyndns address)
3	Ethernet address ETG1	192.168.2.10
4	Ethernet address ETG2	173.16.3.1
5	ETG1 & ETG2 VPN authentication	Preshared key
6	ETG1 & 2 VPN mode	Tunnel
7	Remote LAN (ETG1 side)	173.16.*.* or 173.16.0.0 + subnet mask
8	Remote LAN (ETG2 side)	192.168.2.* or 192.168.2.0 + subnet mask

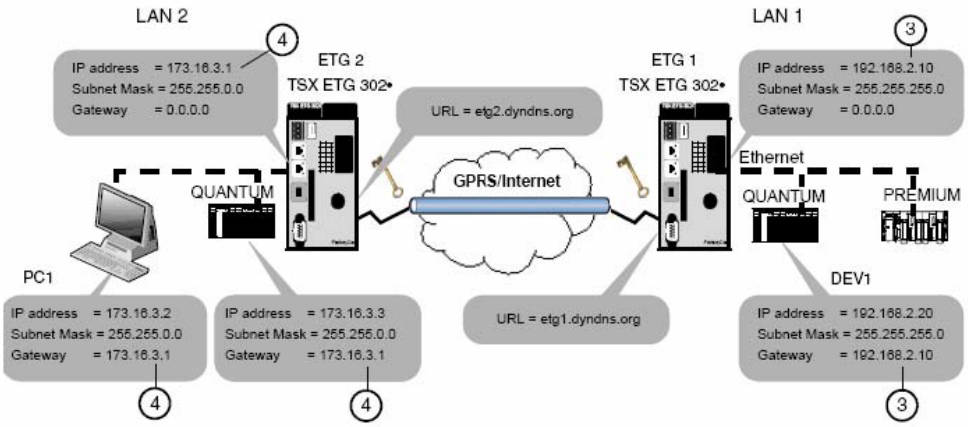


Figure 30 Sample ETG302x Wireless VPN Configuration

Internal Access for Service or Vendor Personnel

Before allowing any computer to communicate in an industrial control network, check that it is properly configured and protected and free of malware.

At a minimum, manually check that all applications, operating systems, and anti-virus software are at the latest patch levels.

Consider the use of Network Access Control (NAC) systems to perform security checks automatically. A NAC can control access to a network by applying a set of rules to a device when it first attempts to access the network. These rules typically regulate anti-virus protection level, applications, operating system patch levels, and configuration. NAC systems may also integrate the automatic remediation process (fixing non-compliant computers before allowing access) into the network systems before communication is allowed.

NAC systems control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

NAC systems are used mainly for endpoint health checks and are often used with role-based access policies. Depending on a person's profile and the result of a posture or health check, access to the network is granted or denied.

A major benefit of using a NAC solution is the ability to block access by devices that lack appropriate anti-virus software, application patch levels or host intrusion prevention software. Such devices would otherwise place other devices on the network at risk of cross-contamination.

NAC support is available in many current operating systems such as Windows 7 and Windows 2008 R2.

Device Hardening

Device hardening is the process of configuring various settings to strengthen security on devices such as those shown in Figure 31, "Device Hardening in Secure Network Architecture".

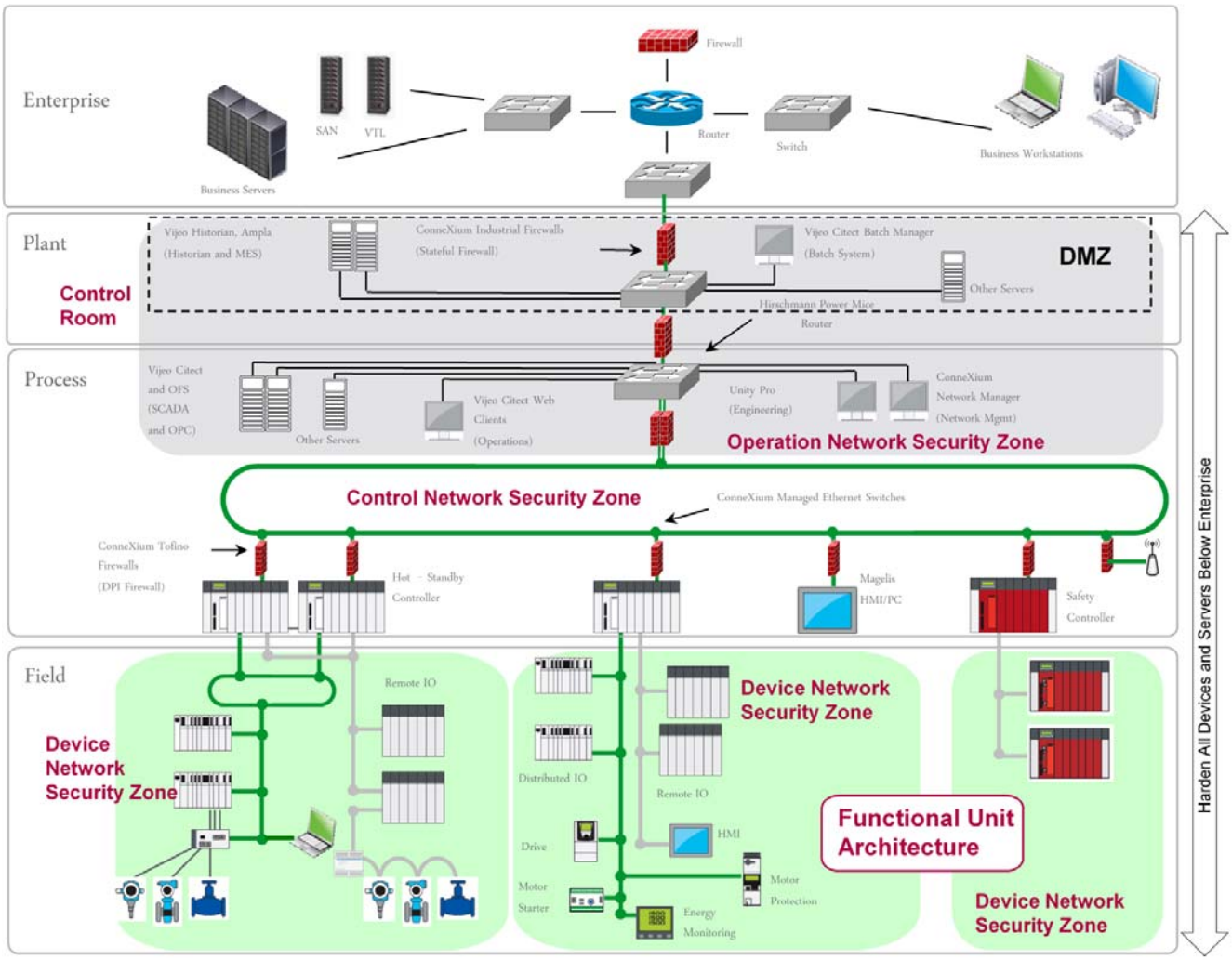


Figure 31 Device Hardening in Secure Network Architecture

Device hardening applies to routers, firewalls, switches and other devices on the network such as SCADA and PACs. Examples of device hardening activities, tools, and methods include:

- Password management including encryption
- Disabling of unused services
- Access Control
- Patches, hotfixes, application updates
- Strong authentication

The following sections describe how some of these activities, tools, and methods are used.

Password Management

Password management is one of the fundamental tools of device hardening. Passwords are often neglected in industrial control systems. Policies and procedures on password management are often inadequate or missing entirely.

Password Management Guidelines

- Enable password authentication on all e-mail and Web servers, PACs, Ethernet interface modules, and embedded Web servers.
- Change all default passwords immediately after installation, including those for:
  - User and application accounts on Windows, SCADA, HMI and other systems
  - Scripts & source code
  - Network control equipment
  - Devices with user accounts
  - FTP Servers
- Grant passwords only to people who need access. Prohibit password sharing.
- Avoid displaying passwords during password entry
  - Require passwords that are difficult to guess. They should contain at least 8 characters and should combine upper and lowercase letters, digits, and special characters when permitted.
- Require users and applications to change passwords on a scheduled interval.
- Remove employee access account when employment has terminated.
- Require use of different passwords for different accounts, systems, and applications.
- Maintain a secure master list of administrator account passwords so that they can quickly be accessed in the event of an emergency.
- Implement password management in a way that does not interfere with the ability of an operator to respond to an event such as an emergency shutdown.
- Do not transmit passwords via e-mail or in any other way over the insecure Internet.

Device Access Control

Another aspect of device hardening is device-level access control. For instance, a Schneider Electric device might maintain an access control table with a list of approved addresses, and the device would only accept access requests that originate from those addresses. This type of access control is useful in controlling access between different areas of the plant.

Access Control Guidelines

Access control should be implemented at all levels: servers, workstations, firewalls, switches, and devices.

Use access control lists such as the one shown in the following Schneider Electric Ethernet module configuration screen to list the addresses from which a TCP connection request will be allowed.

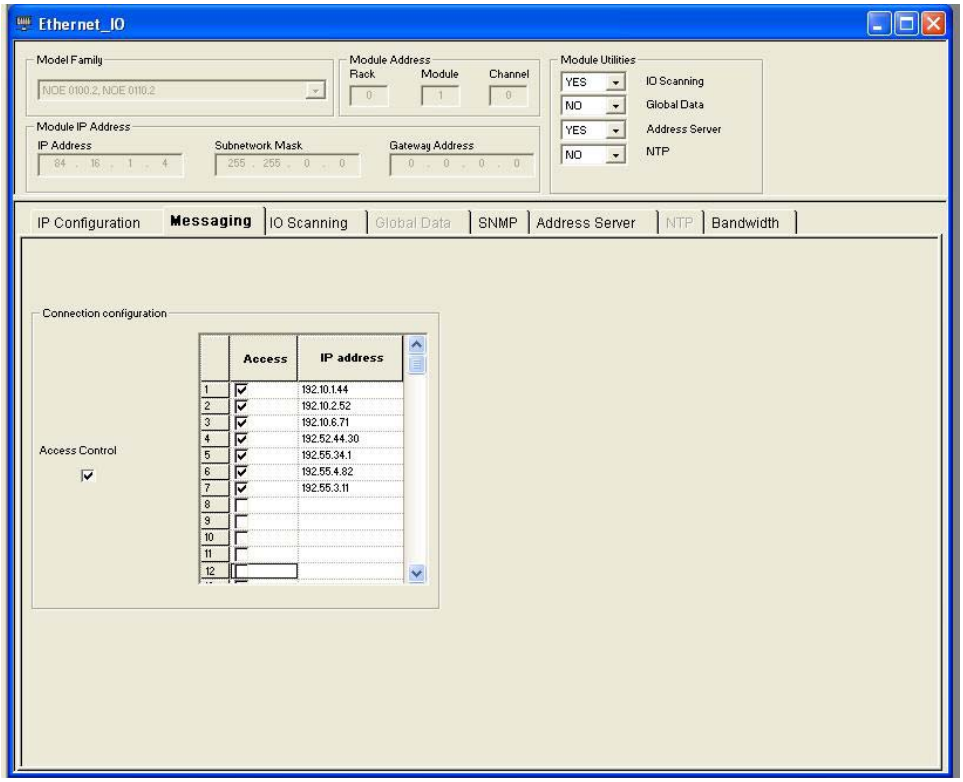


Figure 32 Sample TCP Connection Access Configuration

Hardening ConneXium Ethernet Managed Switches

The following ConneXium managed Ethernet switch features can be configured to harden the switch and provide additional protection against unauthorized users:

- SNMP
- Telnet or Web access
- Ethernet Switch Configurator Software
- Port access control via IP or MAC address
- VLAN, define one for managing the switch and limit access to it.

SNMP

SNMP v1, v2 and v3 are supported by the ConneXium managed Ethernet switches. By default SNMP v1 and v2 are activated with default passwords, public for read access and private for read/write access. For SNMP guidelines, see , "SNMP Risk Mitigation" on page 37.

Telnet and Web Access

The ConneXium managed Ethernet switch telnet server supports device configuration via command line interface over telnet and by access to the switch's embedded Web pages. On delivery, both servers are activated. To harden the switch:

- Change the default read and read/write passwords for the telnet and Web servers

- Deactivate the telnet server if not using the command line interface to configure switch.
- After configuration and operational verification, disable the Web server.

Note: If both the telnet server and the Web server are disabled, the switch's V.24 port will be the only remaining access port.

Ethernet Switch Configurator Software Protection

The Ethernet Switch Configurator Software protocol allows users to assign an IP address, net mask, and default gateway IP to a switch. As part of device hardening, after assigning the IP parameters to the device, disable the Ethernet Switch Configurator Software function or limit the access to read-only.

Ethernet Switch Port Access

A malicious user who has physical access to an unsecured port on a network switch could plug into the network behind the firewall to defeat its incoming filtering protection.

Ethernet switches maintain a table called the Content Address Memory (CAM) that maps individual MAC addresses on the network to the physical ports on the switch. In a MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses filling the CAM table. Once the CAM table is full, the switch becomes an Ethernet hub allowing all incoming packets to be broadcast on all ports. The attacker then could use a packet sniffer (such as Wireshark) running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e-mail and instant messaging conversations), which would not be accessible were the switch operating normally.

The following device hardening methods help to mitigate these vulnerabilities:

- Disable unused ports.
- Lock specific MAC addresses to specific ports on the Ethernet switch.
- Lock specific IP addresses to specific ports on the Ethernet switch.

Hardening Vijeo Citect SCADA Systems

Supervisory Control and Data Acquisition (SCADA) systems are used in industrial control for data collection, human interface, and data analysis. Schneider Electric's Vijeo Citect is an example of this functionality. SCADA systems, due to their typical PC-based architecture, simple access to process control functions, and criticality to the process, are vulnerable devices on the control system network.

Steps required to harden the SCADA system include:

- Grant physical access to the hosting server only to system administrators or similar authorized personnel.
- Keep logical access to the physical server within a dual-firewall DMZ, along with other systems such as workstations, Citect Historian, OFS, and Ampla. Use industrial stateful firewalls, such as the ConneXium Industrial Firewall devices.
- Provide dedicated operator and developer access to the server via Vijeo Citect Web Clients. Do not install developer tools on a running production Vijeo Citect server. These tools should be installed only on dedicated developer workstations.

- Harden the PC server and its operating system via strong and unique user and administrative account passwords. Use enterprise grade operating systems, such as Windows 2008R2 Standard Server, for the data execution prevention (DEP) and user account controls (UAC) capabilities provided by these operating systems. Patch the operating system to current required levels on a documented, monitored schedule.

  Disable or remove unused programs and services. Run Citect with non-administrative privileges only. Do not install Vijeo Citect designer tools on production servers.

  Hardening of servers, particularly user account management and patching should be a continuous process improvement. All file systems should be NTFS.
- Limit information access by configuring roles within Vijeo Citect.
- Do not allow Web and e-mail access on systems directly on or accessing the Vijeo Citect system. Disable or severely restrict Web and e-mail access for any system in the control room.
- Use Web clients instead of Internet display clients.
- Use multiple digital signatures.
- When possible, test any changes such as patching and installation in a dedicated closed test environment prior to production rollout.
- Implement Microsoft Windows authentication. Use Active Directory for central management if possible.
- Routinely track and monitor audit trails to identify suspicious activity and remedy the activity immediately.
- Configure mirrored servers such as the historian in the DMZ for external access. Do not allow direct access on the control system network.
- Validate that there are no IP addresses for non-required devices on the access list.
- When possible use white listing products on all Citect servers and clients instead of anti-virus products. White list products tend to be less resource-intensive than anti-virus tools and they offer stronger protection against zero-day threats.
- If anti-virus products are used, keep the software and virus definitions current. Because anti-virus updates can affect production, consider a risk-benefits assessment to help determine appropriate scheduling.
- Configure Vijeo Citect to authenticate username and password against Windows authentication. Use systematic password maintenance procedures like those used in IT-managed systems.
- Allow no e-mail or Web access on the Citect server or on machines that connect to the server.
- If the Citect server cannot be located in a secure physical location, establish some form of access control process.
- Disable or remove CD-ROM and diskette drives.

- Disable USB ports not used by the keyboard or mice. Dedicate USB drives to the SCADA and only use to import or export data. Scan the USB drive for malware before connection to the SCADA.
- Do not leave remote units open. Establish and enforce procedures to log out of or screen-lock Citect Web Clients.
- As shown in Figure 33, "Sample Vijeo Citect Roles Configuration", assign roles to limit access to plant areas and keep unauthorized personnel out of areas of non-responsibility. If an intruder is able to penetrate, access will be to a specific area and not the entire plant.

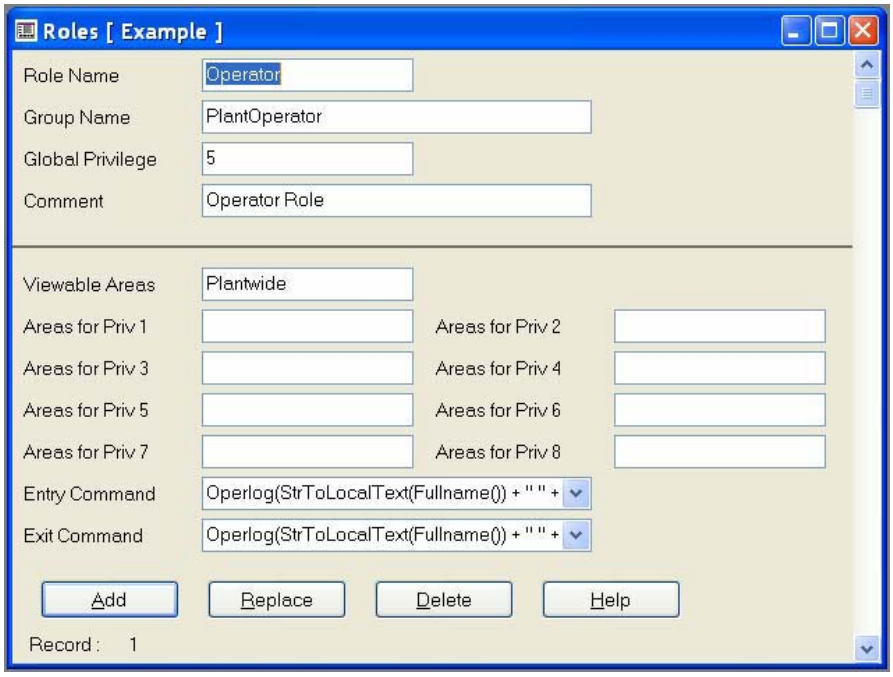


Figure 33 Sample Vijeo Citect Roles Configuration

Hardening Vijeo Historian

Vijeo Historian is a centralized reporting tool for industrial control environments. Because it has many touch points to other industrial systems like the Vijeo Citect SCADA it is vulnerable to cyber attacks. Harden this system as follows:

- Locate client, server, and database components on separate machines if possible.
- Patch MS SQL databases on a documented, monitored schedule to check that MS SQL SA passwords are strong and differ from other passwords.
- Harden all hosting servers and client workstations. See "Hardening Vijeo Citect SCADA Systems" on page 56 for examples of relevant server and client hardening methods.
- Locate the database server and Historian server within the same DMZ as the Vijeo Citect SCADA.
- Use ACLs to control client access to the Historian Web portal in the ConneXium Industrial Firewall that separates the control network from the enterprise network.

Hardening Ampla

Ampla is Schneider Electric's operational management tool for industrial control environments. This system integrates with both enterprise and industrial control servers, and is a potential target vector for other machines in the network.

- Ampla's public interface is based on SOAP, WSDL, and B2MML technologies. Because this SOA (service-orientated architecture) uses HTTP or HTTPS, configure firewall rules to allow access to the Ampla server only to specific hosts on these ports (80 and 443).
- Install all of Ampla's server components and databases on one physical computer server.
- Harden all server and client machines. See Hardening "Hardening Vijeo Citect SCADA Systems" on page 56 for examples of relevant server and client hardening methods.
- Change default passwords for the databases. Use Windows authentication, but also strengthen passwords such as the SA account password.
- Do not run a database with an account holding administrative privileges.

Hardening OPC Factory Server (OFS)

The OFS product provides computer client applications with a group of services (methods) for access to variables of target PAC devices. Because OFS has networked access to control systems, it is a target vector for attacks against industrial assets.

- Patch the hosting server on a documented, monitored schedule.
- Harden the server. See "Hardening Vijeo Citect SCADA Systems" on page 56 for examples of relevant server and client hardening methods.
- Locate the server and client in the same DMZ and, if possible, on the same host. OFS requires DCOM services to operate if the client and the server are remote. DCOM requires many ports to be open if the client and server are separated by a firewall such as the ConneXium Tofino. Locating client and server on same host reduces exposure to DCOM vulnerabilities.
- If Vijeo Citect SCADA is present, install OFS on the same physical server.
- Allow only specific hosts and/or accounts to connect to the Internet Information Services (IIS) server.
- Allow only specific hosts and/or accounts to connect to the FTP server.

Device Hardening for Legacy Devices

In many cases, industrial control systems include older devices that are not equipped with sufficient device hardening features. In this case, an external device can be applied in combination with the installed end device to improve the hardening.

Schneider Electric recommends use of the ConneXium Tofino Firewall to provide these features.

The single combined unit can also take advantage of the firewall's ability to limit network traffic, restrict access to allow only data requests from specific originating devices and even limit access to specific data register areas or use of specific function codes.

Industrial PCs for Enhanced Security

Industrial PCs such as the Magelis Box PCs can host software applications such as Vijeo Citect SCADA servers, Ampla MES Clients, and Unity Pro development environments. These are hardened PCs running either Windows XP or Windows 7 64-bit operating systems designed for the rigors of industrial environments. These systems were designed for low maintenance and can be installed in electrical enclosures for additional physical security. When such systems are enclosed, the keyboard, mouse, and display access can be implemented through the use of an IP based (keyboard, video, mouse) KVM, such as the APC KVM2G.

Industrial PCs can also be used as platforms to host network intrusion detection systems such as Snort. Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. It combines the benefits of signature, protocol, and anomaly-based inspection.

These PCs can also host proxy server applications such as SQUID. Proxy servers can control traffic into and out of the DMZ, thereby providing additional isolation of the control room infrastructure from the enterprise. These systems are also suitable for hosting network management applications such as ConneXium's Configuration Manager.

Hardening Engineering Workstations

Customers may choose from a variety of commercial PC systems for their engineering workstation needs. Harden and manage these PCs using the same methods used to harden industrial PC systems. Key hardening techniques include:

- Strong password management
- User account management
- Methods of least privilege applied to applications and user accounts
- Removal or disabling of unneeded services
- Removal of remote management privileges
- Systematic patch management

Unlike the Schneider Electric industrial PC systems, which might be located in the more trusted control or device networks, these engineering workstations should be located within the operations network.

Patch Management

To reduce vulnerability to attacks, systems should be patched to the latest vendor-recommended software and firmware levels. This is particularly true with computer systems, such as SCADA hosts, that provide an element of control for the deeper layers of the industrial control networks. It is also true of devices on the control and field level networks.

Patch management and deployment approaches include automatic, semi-automatic, and manual. In all cases patch updates should be systematically planned, tested, and executed. Before releasing any patch to a production system, create a system backup with the ability to roll back configurations rapidly. Backups can be accomplished using tools such as NTBackup or Windows Server Backup.

There are numerous ways to keep informed about the availability of new patches. These include subscriptions to free security bulletin services such as http://www.microsoft.com/security/ and http://www.sans.org/newsletters. In addition, vendor Websites for devices, application software, and operating systems can be monitored for updates.

More advanced server patching can be accomplished by hosting a patch management server in the DMZ supporting Windows Server Update Services (Microsoft WSUS server). This is a local repository of Microsoft hotfixes and service packs for operating systems and applications such as MS SQL Server. Local machines within the control room would connect to this server for patch management. Groups of patches would be predefined, tested, and authorized by system administrators prior to deployment.

Firmware patching of other industrial control systems devices such as PACs, network switches, routers, firewalls, and distributed I/O may require system down time and should be performed on a carefully planned schedule. Some patches may address urgent issues and should be installed as soon as possible, regardless of the planned patch management schedule. The patch management plan should have specific guidelines for such exceptions. Even in these exception cases, include testing and backup procedures in the release plan.

Several utilities allow firmware to be deployed from the control room to the field level devices. These include OS Loader, Unity Loader and Web-based access. Use a dedicated machine in the operations network to deploy firmware. Some field devices cannot be remotely patched and will require local access. In these cases, connect only with a security-approved laptop free of malware.

Monitoring and Maintenance

Cybersecurity is a continual process. Monitoring and maintenance are important components of a defence-in-depth approach.

Monitoring

Through proactive monitoring, intrusion attempts can be detected and stopped before they can do any damage. There are several methods of monitoring the network for suspicious activity. They include:

- Routine examination of log files
- SNMP authentication traps
- Network load monitoring
- Use of an Intrusion Detection System (IDS)

Log File Monitoring

- Monitor device event logs for unusual activity.
- Monitor MS Windows Event Viewer (Control Panel/Administrative tools/Event Viewer/Application Log) for unusual activity.
- Monitor log files produced by devices. For example:
  - Quantum PAC log files
  - Alarm log files from PACs and other devices
  - Diagnostic log files such as those produced by ConneXium managed Ethernet switches
  - Syslog files such as those produced by ConneXium Industrial Firewalls

SNMP

- Enable SNMP authentication traps on all devices that support SNMP to monitor for unauthorized login attempts.
- Use network diagnostic tools like ConneXium Network Manager to monitor and immediately investigate unusual traffic load.

Intrusion Detection Systems

An intrusion detection system (IDS) monitors activity on the network for malicious traffic, and logs and reports traffic anomalies. A typical IDS monitors traffic patterns, file access, changes in port status, invalid password entries, and inoperable equipment.

Types of IDS include:

- Network intrusion detection system (NIDS). NIDS monitor traffic to and from all devices on the network by analyzing individual packets for malicious traffic. NIDS are often located at demilitarized zones or network boundaries. Snort is a NIDS.

- Host intrusion detection system (HIDS). A HIDS is an agent that runs on an individual host or device on the network and monitors traffic in and out of the host or device. It analyzes system calls, application logs, file system modifications and other host activities and states to identify intrusions. The agent is usually a software application. Tripwire and OSSEC are HIDS.

Maintenance

Continual maintenance of the control system includes the routine, scheduled updating of anti-virus software with the latest signatures and installing the latest patches for software and firmware used on devices in the network.

A periodic assessment and test of the control system network for security risks should be performed. Check that device configurations are appropriate with security in mind. Use the latest security standards and practices and update as needed.

Network Security Architecture Example

This section builds on the defence-in-depth recommendations provided in the previous sections of this document. It shows how to apply these recommendations to a typical network architecture by providing expanded detail on:

- Security zones
- Location and function of firewalls
- Data flow between security zones
- Device security settings

Note: It should be noted that this example is limited to a single site network with no plant-to-plant communications.

Security Architecture Overview

Figure 34, "Example Architecture" shows a baseline network architecture.Figure 35, "Example Architecture with Defence-in-Depth Recommendation" shows the same architecture with defence-in-depth security recommendations.

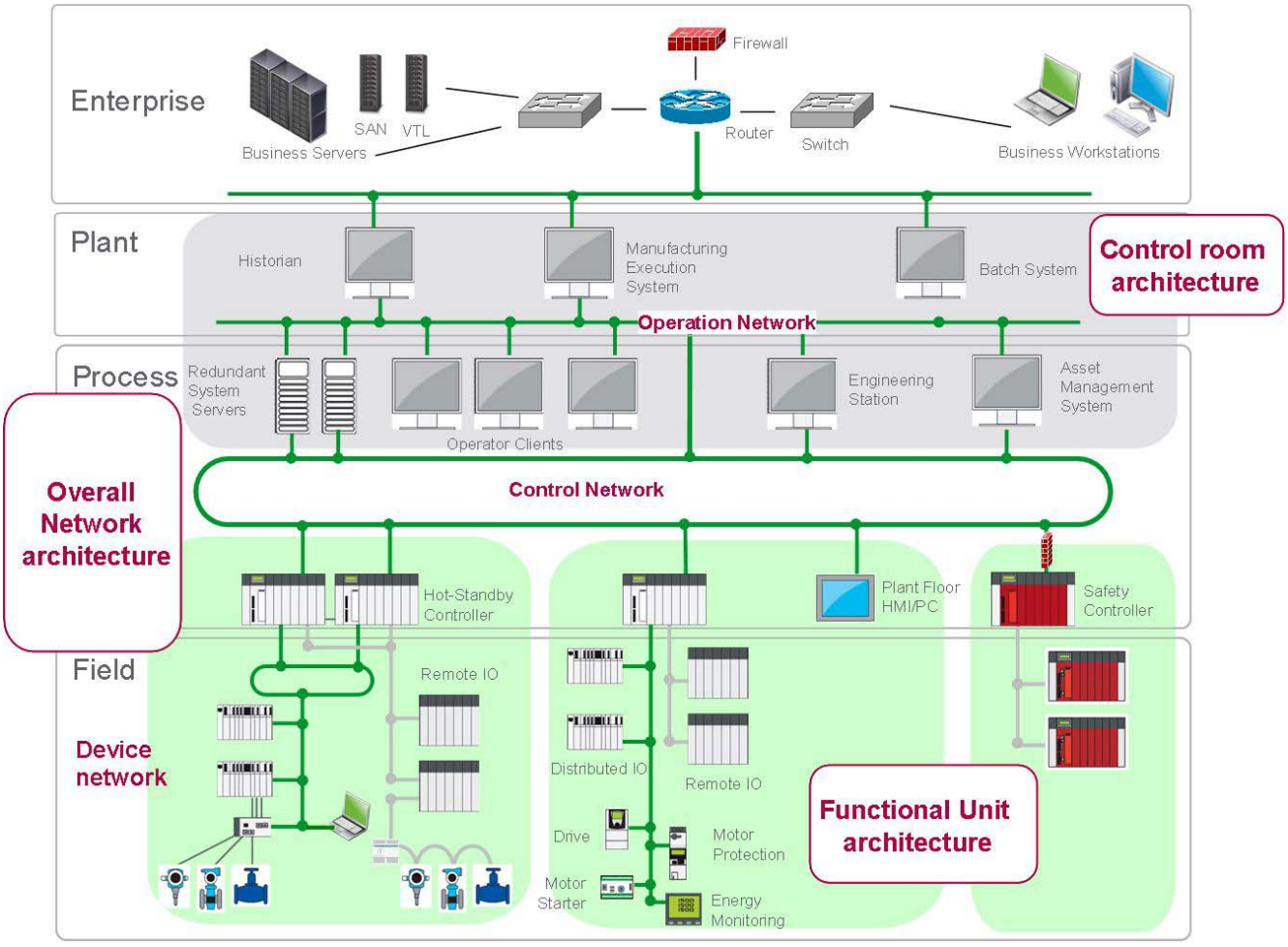


Figure 34 Example Architecture

The example architecture is separated into the following networks: operations network, control network, and all device networks. In the example security architecture (Figure 34), each of these networks is defined as a security zone. Each of the functional units in the device network security zone is a different subnet. The functional unit subnet netmask is sized slightly higher than the actual number of host device in the functional unit. The IP addresses of any Pelco cameras are in the same subnet range as the functional unit in which they are located. To increase the security level, the cameras are placed in a VLAN and subnet separate from the other devices in the functional area.

Security Zones

Security zones are established by locating and configuring the appropriate firewalls at the zone boundaries as shown in Figure 35.

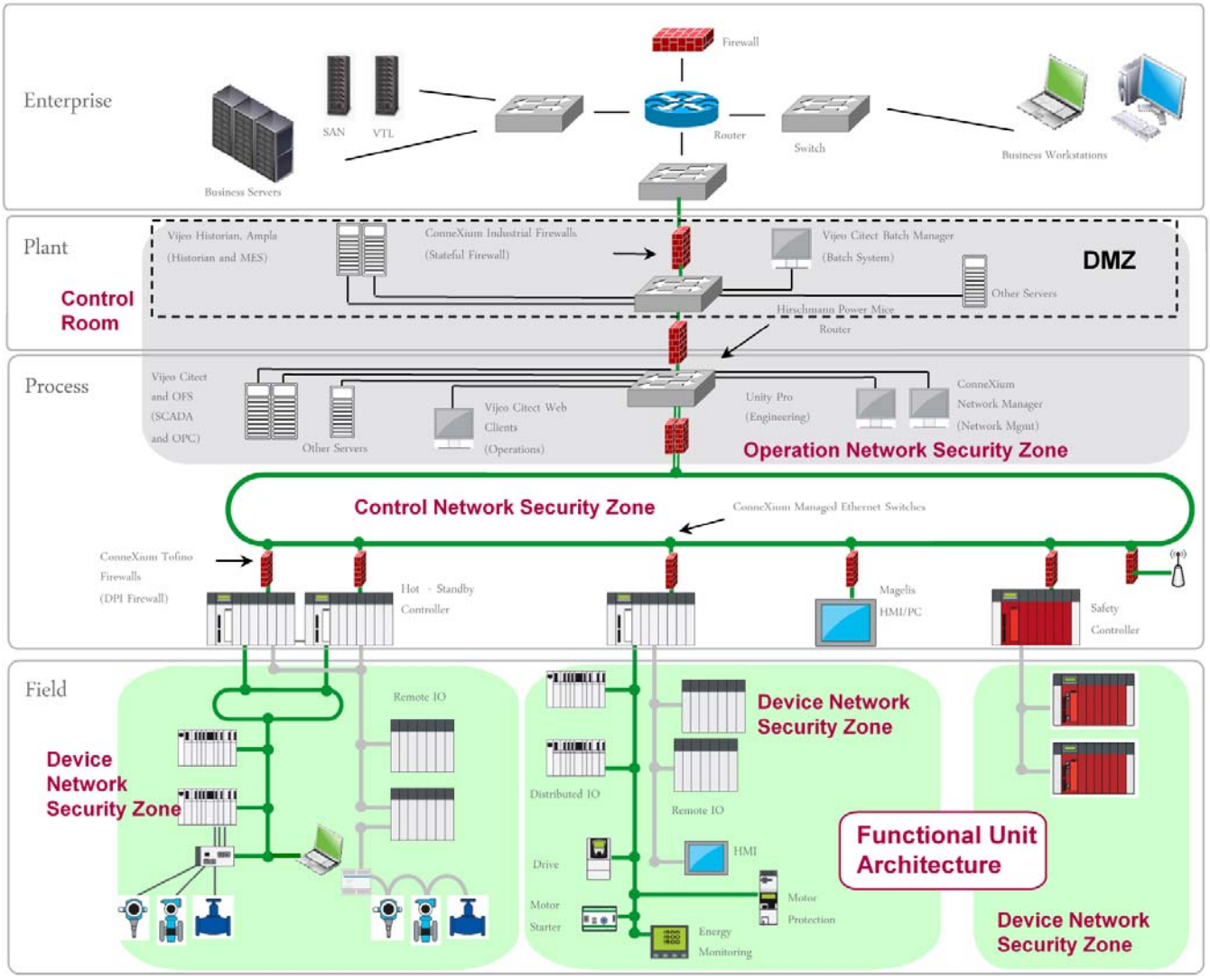


Figure 35 Example Architecture with Defence-in-Depth Recommendation

Communication between the different zones happens through pathways or conduits in which the firewalls reside. The conduits allow control over access to zones, limit propagation of malware, resist denial of service attacks, and maintain the integrity and confidentiality of network traffic.

Place the stateful ConneXium Industrial Firewalls at the demarcations between the enterprise network and the DMZ, between the DMZ and operations network and between the operations network and the control network.

For the boundaries between the control network and the device network, use the ConneXium Tofino Firewall. Tofino provides the additional deep packet inspection of the industrial protocols.

The firewalls are used to restrict the network traffic between the security zones. Figure 36, "Network Data Flow" shows the types of network traffic that are allowed to traverse between the different networks.

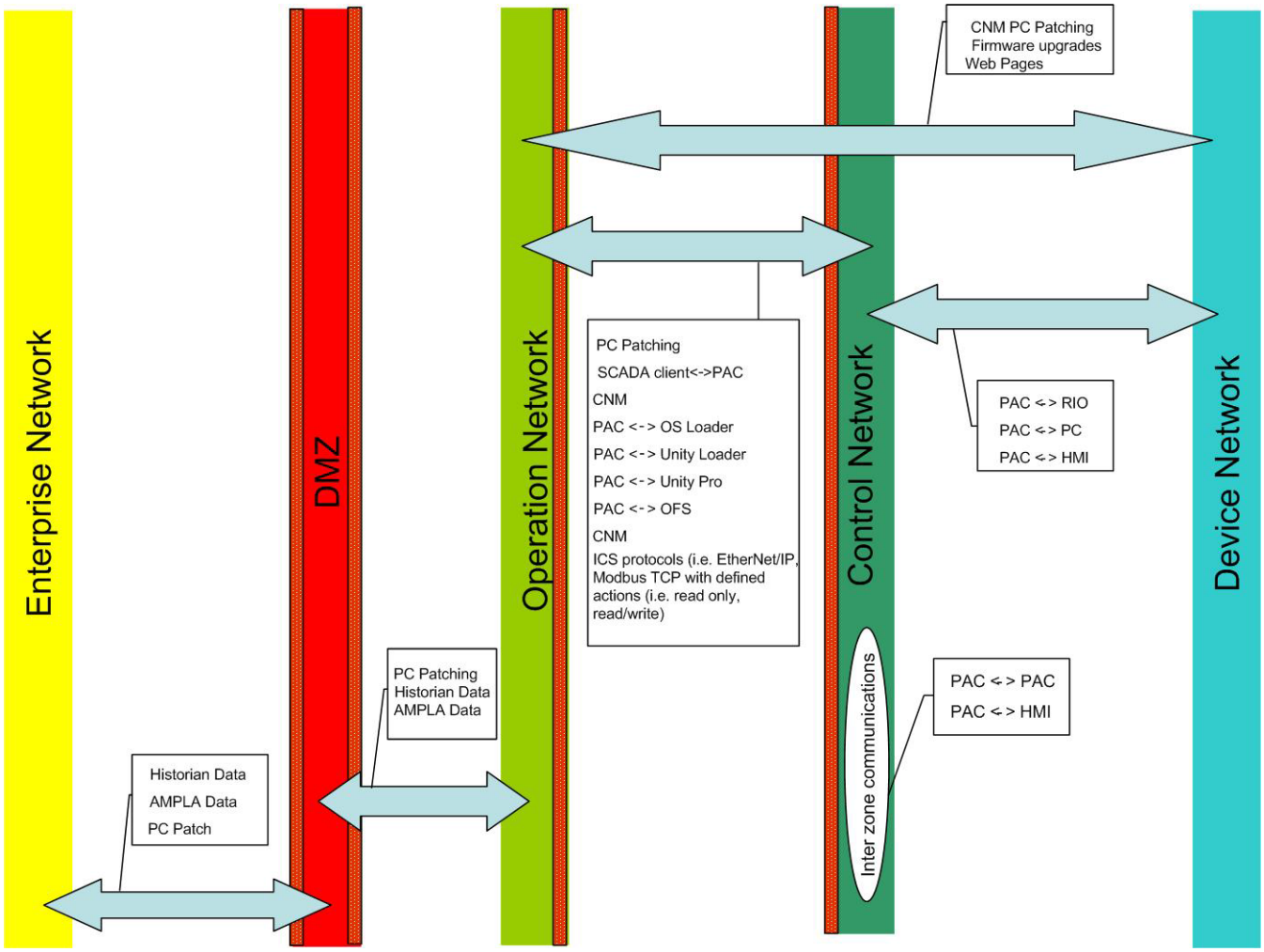


Figure 36 Network Data Flow

ConneXium Industrial Firewalls

ConneXium is a range of Ethernet connectivity devices which includes managed Ethernet switches and industrial firewalls. For more information, see the Schneider Electric website (http://www.schneider-electric.co.uk/en/download/document/DIA6ED2140903EN/).

The ConneXium Industrial Firewalls should be configured to allow only traffic that is mandatory between the immediately adjacent zones. Deny all other traffic.

For the firewalls located at the enterprise network and the DMZ, use the router feature of the firewall to route traffic between the enterprise network and the DMZ.

For the firewalls located at the DMZ and operations network, use the firewall's router feature to route traffic between the DMZ and the operations network.

For the firewalls located at the operations network and control network, use the firewall's transparent mode to relay traffic from the operations network to the control network. Routing of the multiple functional area subnetworks is performed by the Hirschman Power MICE router located in the operations network.

For high availability, the ConneXium Industrial Firewalls and MICE routers should be configured for redundancy.

The following table lists basic ingress and egress recommendations for specific firewall locations.

Table 2: ConneXium Industrial Firewall Ingress and Egress Rules

Firewall Location	Ingress Rules	Egress Rules
Enterprise and DMZ*	• Allow source- destination-, and protocol-specific traffic such as HTTP, SQL, network time protocol (NTP), and DNS, to any DMZ machines • Drop all ICS protocols • Drop any internal ICS source • Drop all defaults	• Allow source- destination-, and protocol-specific traffic from DMZ machines. • Explicitly drop any ICS protocols • Drop all defaults
DMZ and Operations Network*	• Allow only operation hosts with specific protocol to communicate with DMZ network hosts • Drop all defaults	• Allow only DMZ hosts with specific protocol to communicate with operations network hosts • Drop all defaults
Operations Network and Control Network*	• Allow source- destination-, and protocol-specific traffic for ICS protocol • Allow user/vendor time-based ACLs for FTP, TFTP, patching, and other maintenance needs • Reject all multicasts • Drop all defaults	• Allow source- destination-, and protocol-specific traffic for ICS protocol • Allow user/vendor time-based ACLs for FTP, TFTP, patching, and other maintenance needs • Reject all multicasts • Drop all defaults

*Allow only defined hosts within the operations network to configure the firewall

ConneXium Tofino Firewalls

ConneXium is a range of Ethernet connectivity devices which includes managed Ethernet switches and industrial firewalls. For more information, see the Schneider Electric website (http://www.schneider-electric.co.uk/en/download/document/DIA6ED2140903EN/).

Use the deep packet inspection feature of the ConneXium Tofino Firewall to regulate which devices have read access and read/write access.

The following table lists basic ingress and egress recommendations for a Tofino Firewall located between the control and device networks.

Table 3: ConneXium Tofino Firewall Ingress and Egress Rules

Ingress Rules	Egress Rules
• Allow source and destination specific Modbus, extended Modbus, Class 1 or Class 3, EtherNet/IP traffic • Allow source and destination specific traffic for function codes such as 3, 5, 23, 90 • Allow specific hosts to read from specific devices • Allow specific hosts to read from or write to specific devices • Allow multicasts (RTPS, IGMP) • Drop all defaults	• Allow source and destination specific Modbus, extended Modbus, Class 1 or Class 3, EtherNet/IP traffic • Allow source and destination specific traffic for function codes such as 3, 5, 23, 90 • Allow specific hosts to read from specific devices • Allow specific hosts to read from or write to specific devices • Allow multicasts (RTPS, IGMP) • Drop all defaults
Allow only defined hosts within the operations network to configure the firewall.	

ConneXium Managed Ethernet Switches

ConneXium is a range of Ethernet connectivity devices which includes managed Ethernet switches and industrial firewalls. For more information, see the Schneider Electric website (http://www.schneider-electric.co.uk/en/download/document/DIA6ED2140903EN/).

Take the following actions to enhance the security of ConneXium managed Ethernet switches:

- Change default passwords.
- Disable unused ports.
- Disable telnet access (used for configuration via CLI).
- After IP assignment, disable the Ethernet Switch Configurator.
- After configuration, disable the device's Web pages. If both the telnet server and the Web server are disabled, the switch's V.24 port will be the only remaining access port.
- Use IP or MAC access control list to allow access to ports.
- Allow only defined hosts from the operations network to configure the switches.

Device and Application Security Recommendations

Schneider Electric recommends using all available device and applications security features. The following are general recommendations for using security features found in devices and applications.

Login IDs and Passwords

- Use login ID and password authentication on devices and applications that support it.

- Use a unique password for each such device and application.
- Change all default passwords to unique passwords.

SNMP Community Names

- Change all SNMP default community names to unique names.

Access Control Lists (ACL)

- Use access control to manage communication to and from specific IP addresses on all Ethernet modules that support access control (for instance, the 140 NOE 771 x1).

Programming and Configuration Software

- Configure logins, password, and user groups. Create profiles with different access rights such as the ability to open project, create new project, and modify sections. For example, the Unity Pro Security Editor supports these functions.
- Lock sections and derived function blocks (DFBs) to make them read only or no read/write. For example Unity Pro programming software supports these functions

SCADA

- SCADA systems incorporate features that restrict access to runtime systems and areas. Roles can be assigned to particular user accounts. For instance, use CitectSCADA to configure the following:
- Users - user accounts for individual or groups to restrict access to the runtime system. Login user names and passwords need to be set up.
- Areas - different access privileges defined for different geographical or functional boundaries in the system.
- Privileges - level of access applied to system elements within a project. A user assigned a role that possesses the matching privilege can access it.
- Roles - defined set of permissions (privileges and areas) that are assigned to specific users.

SCADA systems such as CitectSCADA may also integrate standard Windows security. Using the integrated Windows security feature, the Windows user can log on to CitectSCADA runtime with runtime privileges configured within the project.

Device Web Pages

Some devices with Web pages provide Web page password, access restriction features and the ability to configure variables, symbols, and direct address data as read-only or write-enabled. Use these security features when they are available.

PACs

Use the following methods to provide increased security:

- On PACs that incorporate a key switch (as it is on the Modicon Quantum Unity Pro 140C PU 65260) set to lock position. This turns on memory protection and disables the use of system menu operations from the device keypad. In this state, all parameters are read only. Remove the key and store it in a secure location.
- Change SNMP default community names for PACs that incorporate built-in Ethernet ports (for instance, the 140 CPU 652 60).
- Use ACLs to manage communication to and from specific IP addresses for PACs with built-in Ethernet ports (for instance, the 140 CPU 65260).
- On PACs that support remote run/stop management, use the feature to help prevent remote commands/requests from accessing the PACs' RUN/STOP modes.

Ethernet Communication Modules

- Change SNMP default community names on all Ethernet modules that support SNMP (for instance, the Modicon Quantum 140 NOE 771 xx).
- Use access control to manage communication to and from specific IP addresses on all Ethernet modules that support access control (for instance, the 140 NOE 771 x1).
- On modules that support it disable unused services such as HTTP, FTP, and TFTP.

Log Files

Enable and configure device and application logging features when available. Schneider Electric recommends systematic monitoring of all log files to help detect changes, unintended behavior, and unauthorized access. See , "Log File Monitoring" on page 62 for more information.

General Recommendations

Use the following methods on devices and or applications that support them:

- Disable unused ports on devices.
- Disable unused USB ports.
- Disable or lock keyboards, touch screens, and PCs when unused or unmanned.
- Remove unused device and application user accounts.

Patch Management

The patching of systems should be a systematic procedure governed by corporate policy. It should be closely aligned with security, scheduled downtimes, backup, change control, verification, and incident management procedures.

There are several ways to deploy patches for PC systems. Schneider Electric recommends the following:

- Prior to patching, create baselines and backups of all production systems.
- Test all patches prior to deployment to production systems.

- Use a dedicated patching server located in the DMZ that can either replicate from a patch repository upstream or serve as its own WSUS (Windows Server Update Service) server directly.
- Configure Windows client PCs to point their MS Windows Server to a dedicated server.
- Have the assigned administrator push patches to PC clients after the patches are tested.

There may be situations in which a patch needs to be manually installed. In these situations, only the assigned administrator should install the patch, using a PC known to be free of malware.

Depending on the device, patching of industrial control systems (firmware upgrades) may be done via network connectivity or may require local connection of a PC to the device. Schneider Electric recommends the following:

- Prior to upgrading any production devices, perform backups and make previous release firmware available.
- If locally connecting to any industrial control device, use a PC that is known to be free of malware.
- When updating industrial devices through the network, verify that the firewall rules and user accounts permit the necessary protocols, such as TFTP and FTP, to pass from source to destination and destination to source.

Conclusions

The defence-in-depth recommendations described in this document can decrease the risk of attacks on typical industrial network architectures. No single component provides adequate defence. It is important to consider all of the defence-in-depth recommendations to mitigate risk.

Methods of Attack

This section describes common methods of cyber attack, including:

- VLAN hopping
- SQL injection on SCADA
- IP Spoofing
- DoS

VLAN Hopping

VLAN hopping is a method of attacking networked resources on a VLAN. The attacker uses switch spoofing or double-encapsulated frames on an unauthorized port to gain access to another VLAN.

Common types of attacks carried out once the intruder has gained access to the desired VLAN:

- MAC flooding attack (confined to the VLAN of origin)
- 802.1Q and ISL tagging attack
- Double-Encapsulated 802.1Q/nested VLAN attack
- ARP attacks
- Private VLAN attack
- Multicast brute force attack
- Spanning-tree attack
- Random frame stress attack

SQL Injection on SCADA

SCADA systems may be vulnerable to SQL Injection attacks. SQL injection is a code injection technique that occurs in the database layer of an application. The attacker executes unauthorized SQL commands by taking advantage of poorly secured code on a system connected to the Internet. Vulnerable points include the login and URL string.

SQL injection attacks are used to steal information from a database and/or to gain access to an organization's host computers through the computer that is hosting the database.

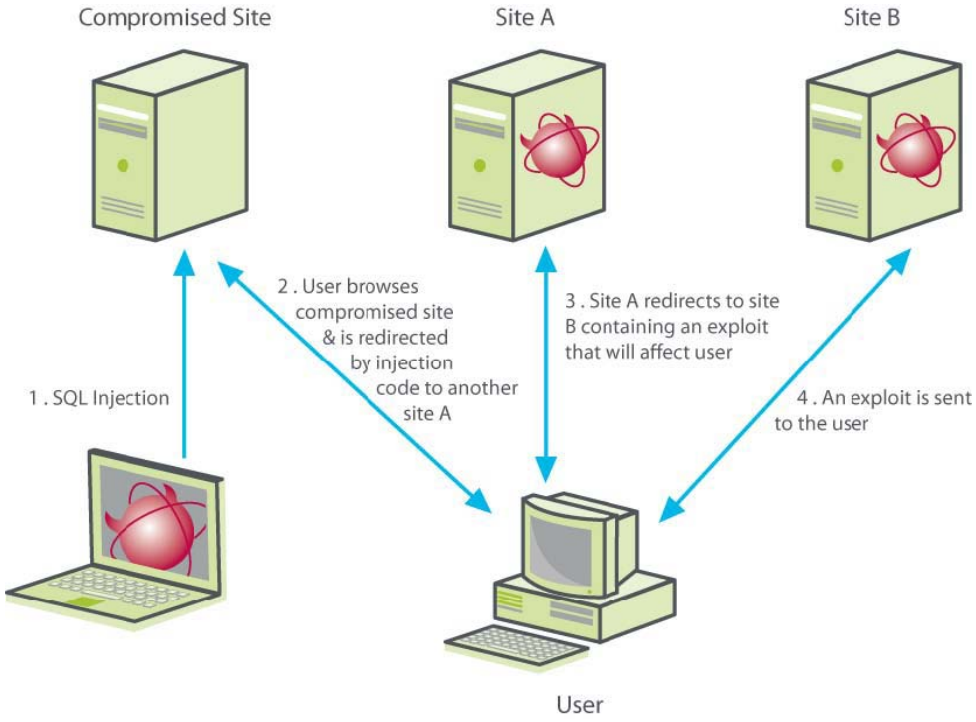


Figure 37 Sample SCADA SQL Injection Risk

IP Spoofing

IP Spoofing is a method used to disguise the identity of an attacker who is attempting to perform malicious attacks such as denial of service and man-in-the-middle. IP spoofing is accomplished by manipulating the IP address.

IP is the main protocol used to communicate data across the Internet. The IP header of the data contains the information necessary to transport data from the source to the destination. The header contains information about the type of IP datagram, how long the datagram remains active on the network, special flags indicating any special purpose the datagram is supposed to serve, such as whether or not the data can be fragmented, the destination and source addresses, and several other fields.

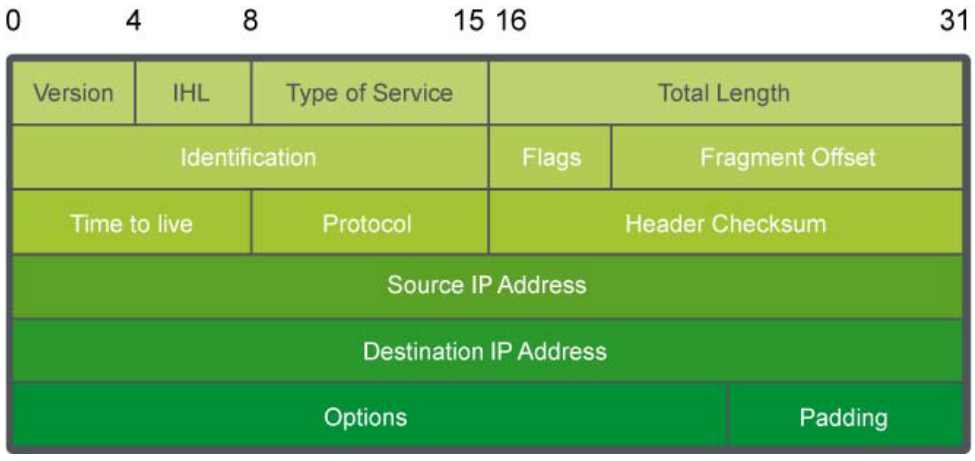


Figure 38 IP Datagram Header

The receiver of the packet is able to identify the sender by the source IP address. IP does not validate the source's IP address. In IP spoofing, the attacker manipulates the datagram. The most common manipulation is creating a false source IP address to hide identity.

The primary motives of the attack are to:

- Gather information about open ports, operating systems, or applications on the host. For example, a port 80 response may indicate that the host is running a Web server. Using telnet, the attacker can see the banner and determine the Web server version and type. Now the attacker can try to exploit any vulnerability associated with that Web server.
- Uncover the sequence-number. TCP requires the use of sequence number for every byte transferred and an acknowledgment from the recipient. An attacker can send several packets to the victim in an attempt to determine the algorithm. Once the algorithm is determined, the attacker tricks the target in believing its legitimacy and launches attacks.
- Hijack an authorized session by monitoring a session between two communicating hosts and injecting traffic that appears to be coming from one host. By doing so, the attacker steals the session from one host and terminates its session. The attacker continues the same session with the same access privileges to the other legitimate host.
- Bypass an ACL security, start a DDOS attack or hide identity of attacker for diverse attacks such as sending illegitimate Modbus write request.

Denial of Service Attacks

DoS is an attempt to deny legitimate users access to a devices' services either temporarily or permanently. One common method involves saturating the victim's computer with external communications requests to either block responses or respond so slowly that the system becomes ineffective. The attacker usually accomplishes this by:

- Crashing the system.
- Denying communication between systems.
- Bringing the network or the system down or have it operate at a reduced speed affecting productivity.
- Hanging the system. This is more disruptive than crashing it because there is no automatic reboot. Productivity can be disrupted indefinitely.

DoS variations include:

- TCP SYN flood attack
- Land attack
- ARP spoofing
- ICMP smurf attack
- Ping of death
- UDP flood attack
- Teardrop attack

TCP SYN Floor Attack

A TCP SYN flood is a form of DoS attack in which an attacker sends a succession of synchronization (SYN) requests to a target's system.

In a TCP SYN attack, the client unknowingly attempts to start a TCP connection to a server that has been breached by the attacker. The client and server exchange information in the following sequence:

1. The client requests a connection by sending a SYN message to the server.
2. The server acknowledges the request by sending SYN-ACK back to the client.
3. The client responds with an ACK and the connection is established.

This sequence, called the TCP three-way handshake, is shown in Figure 39, "Three-Way Handshake".

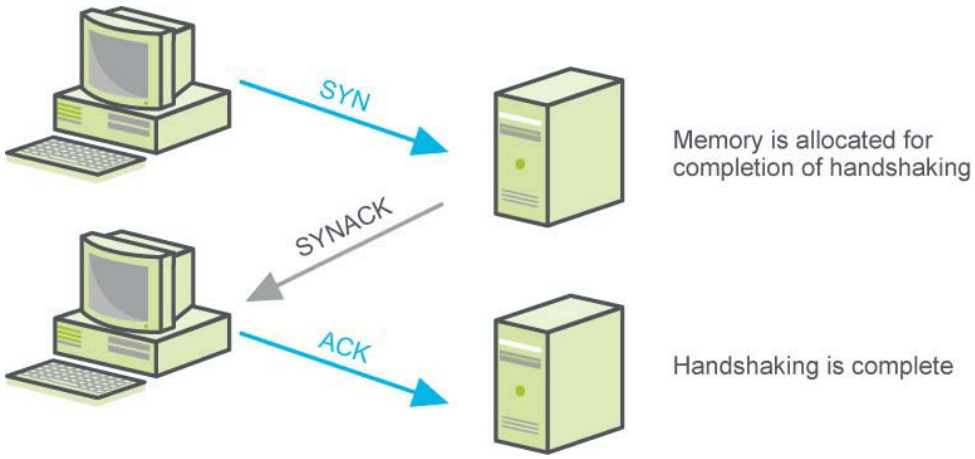


Figure 39 Three-Way Handshake

There is a limit to available resources. Once the limit has been reached, additional requests are dropped as shown in Figure 40, "Requests Dropped when Resource Limits Reached". Older operating systems are more vulnerable than newer operating systems. Newer operating systems manage resources better making it more difficult to overflow tables, but still are vulnerable.

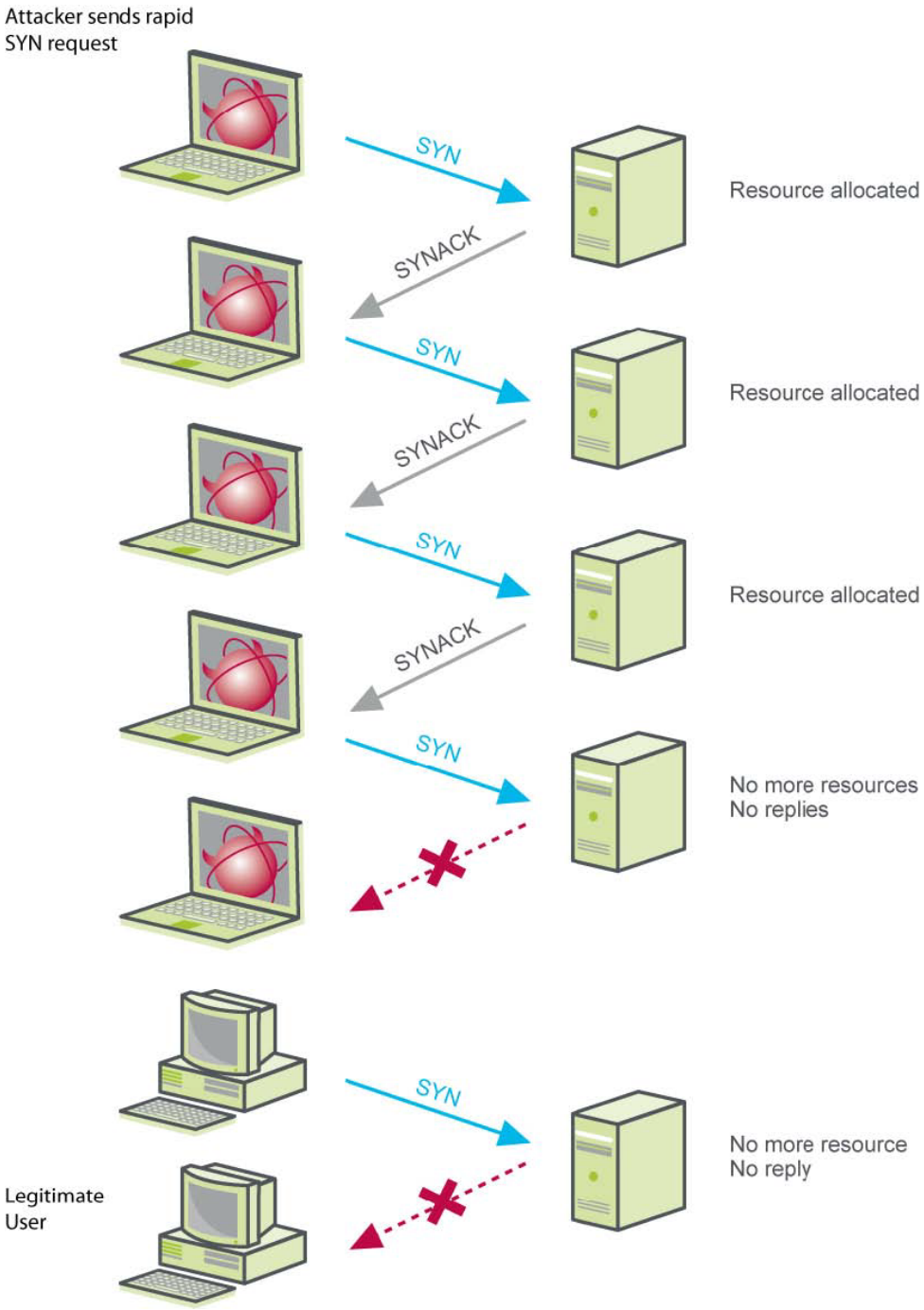


Figure 40 Requests Dropped when Resource Limits Reached

Land Attack

In a land attack a spoofed TCP SYN packet is sent in which the source IP addresses and the source port number are identical to the target IP address and port number. The target machine replies to itself in an endless loop until the idle time-out value is reached.

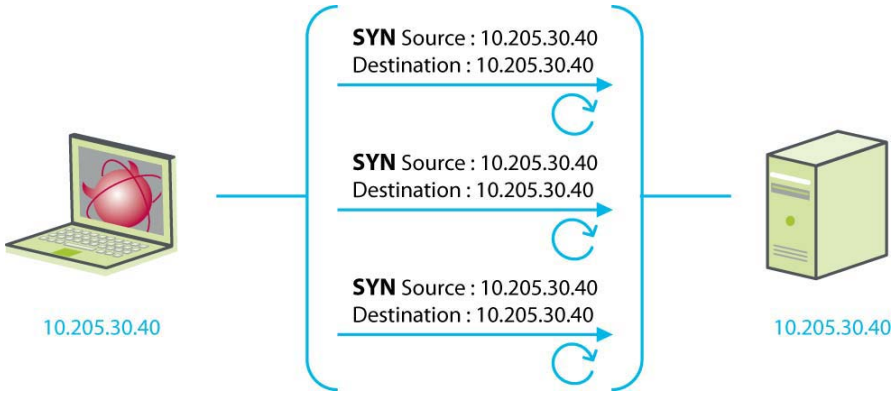


Figure 41 Land Attack

ARP Spoofing

Address Resolution Protocol (ARP) is a Layer 2 protocol that maps an IP address to a MAC address stored in a table (ARP cache) residing in memory.

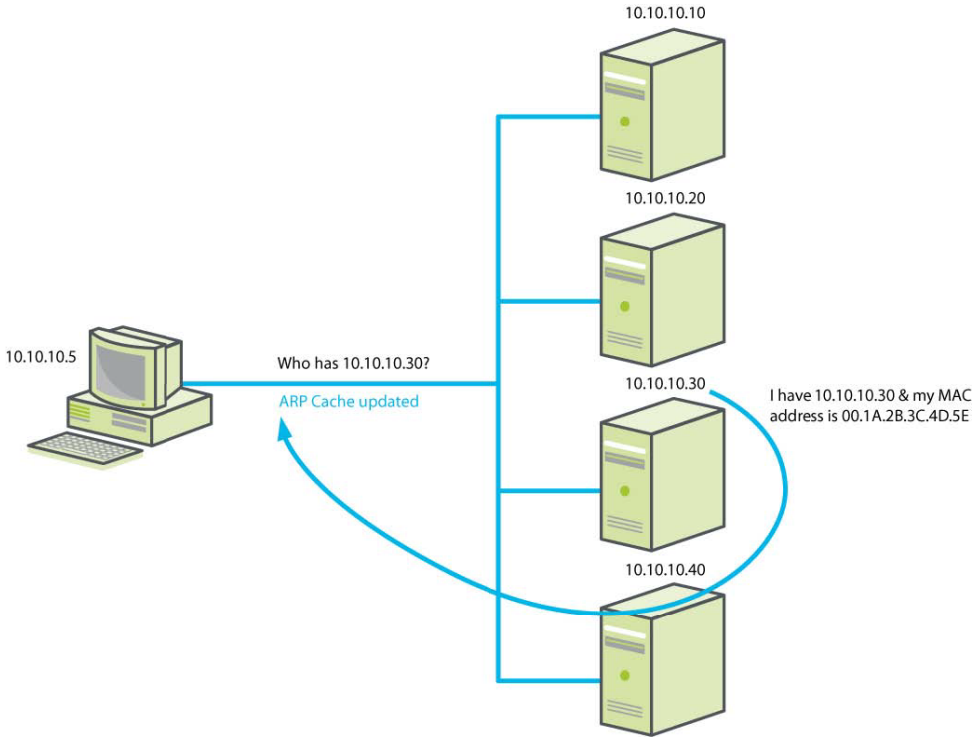


Figure 42 ARP Spoofing

A typical ARP transaction is as follows:

1. ARP checks the local ARP cache for an entry for the destination's IP address. If a match is found, then the hardware address of the destination is added to the frame header and the frame sent.
2. If a match is not found, then an ARP request broadcast is sent to the local network (remember it knows the destination is on the local network by working out the Network ID from the IP address and the subnet mask). The ARP request

contains the sender's IP address and hardware address, the IP address that is being queried and is sent to everyone, but it will not get routed.

3. When the destination host receives the broadcast, it sends an ARP reply with its hardware address and IP address.
4. When the source receives the ARP reply, it will update its ARP cache and then create a frame and send it.

ARP flood spoofing, also known as ARP poisoning or ARP routing, sends fake ARP messages on the network as shown in Figure 43, "ARP Flood Spoofing". The intent is to associate the attacker's MAC address with another node, such as a gateway, by modifying the ARP caches of the system. This allows the attacker to intercept traffic.

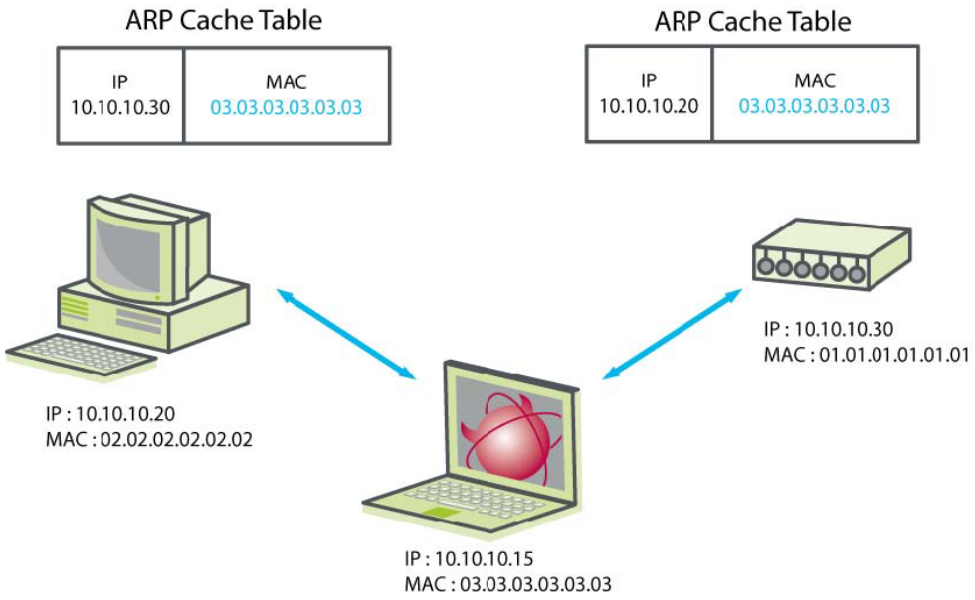


Figure 43 ARP Flood Spoofing

ICMP Smurf

In a smurf attack, the attacker spoofs the target IP address, sending an ICMP echo request (a ping) to the broadcast address on an intermediary network. The target host is flooded with replies. Legitimate users cannot access the server. The ICMP smurf attack is the same as an ICMP flood attack except smurf attacks use other networks to multiply the number of requests.

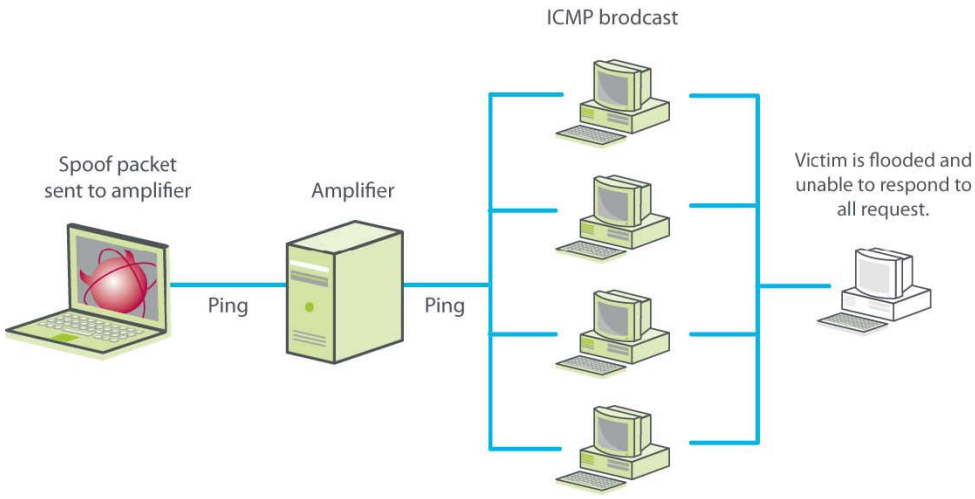


Figure 44 ICMP Smurf Attack

The PING of Death

A feature of TCP/IP is to allow fragmentation by separating a single IP packet into smaller segments. When fragmentation is performed, each IP fragment needs to carry information about which part of the original IP packet it contains. This information is kept in the fragment offset field in the IP header.

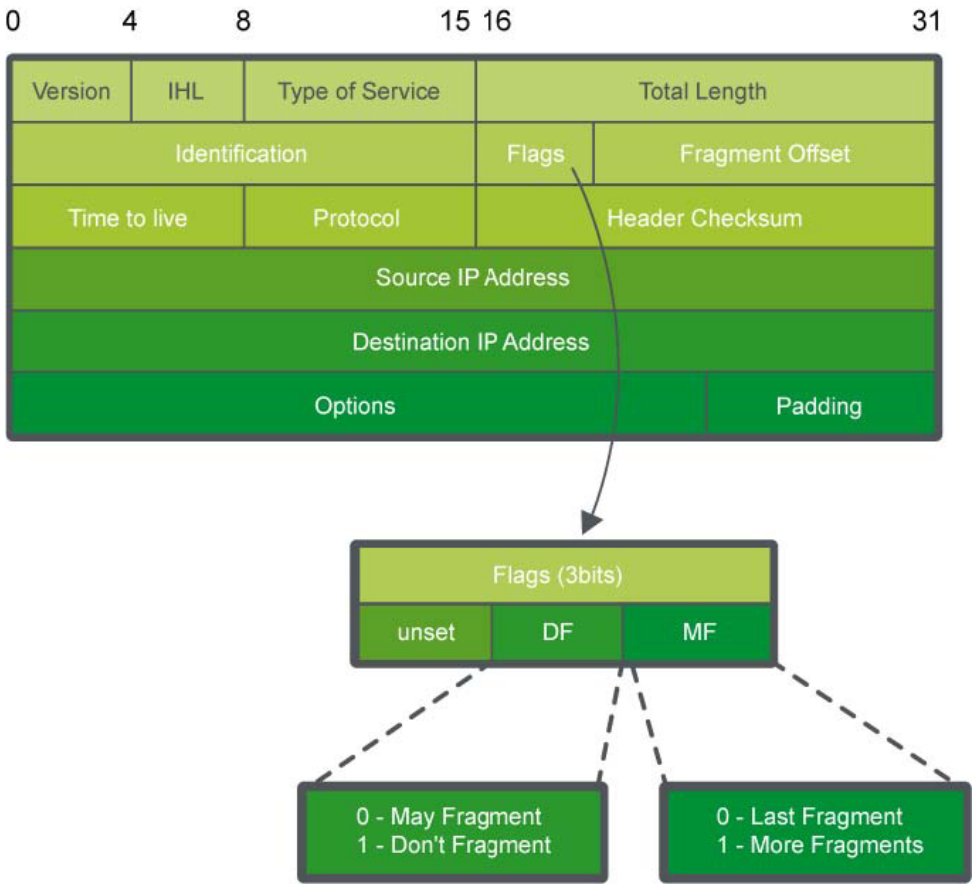


Figure 45 IP Fragmentation

The ping of death attack sends ping request in multiple fragmented packets that are larger than the maximum IP packet size (63, 535 bytes). Because the received ping packet is larger than the allowed IP packet size, the remote system ceases to function while attempting to reassemble the packet.

Figure 46 PING of Death Attack

UDP Flood Attack

A UDP flood attack is similar to the ICMP flooding. The difference is that UDP datagrams of different sizes are used. The attacker sends a UDP packet to a random port on the victim's system. When the victim's system receives a UDP packet, it checks to see if there is an application listening at that port. If not, it replies with an ICMP Destination Unreachable packet to an unreachable spoofed IP address. If enough UDP packets are delivered to enough ports on the victim, the system will cease to function.

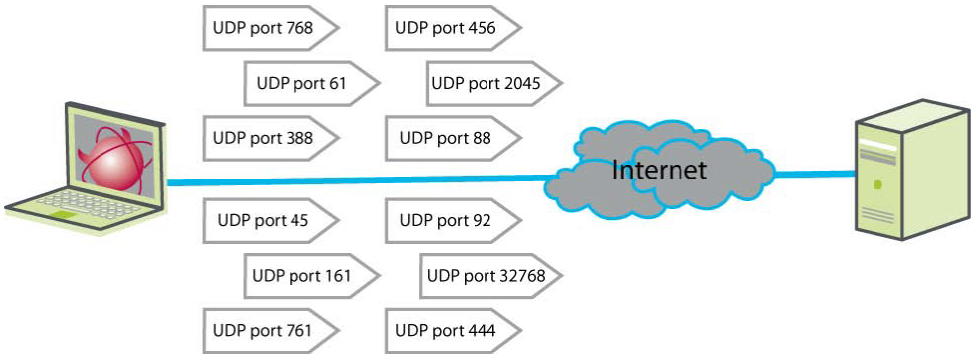


Figure 47 UDP Flood Attack

The primary motivation of the UDP flood attack is not to break into a system but to make the target system inaccessible to legitimate users.

Teardrop Attack

Teardrop attacks involve inserting false offset information into fragmented packets. As a result, during reassembly, empty or overlapping fragments can cause the system to cease functioning.

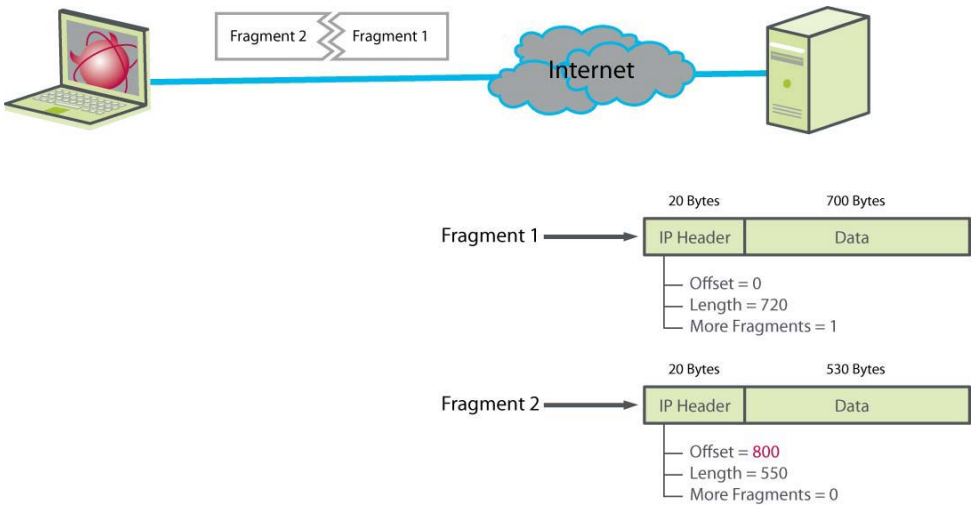


Figure 48 Teardrop Attack

The primary motivation of the teardrop attack is to cause a system to cease functioning.

Appendix

Glossary

Term	Description
BootP	(bootstrap protocol) A TCP/IP network protocol that lets network nodes request configuration information from a BootP server node.
broadcast	A message that is sent out to all devices on the network.
broadcast domain	A collection of devices that receive a broadcast sent on an Ethernet network. The broadcast domain ends at a router positioned in the network. If any device in a broadcast domain broadcasts information, that information is received by all devices in the same domain. It is not received by devices connected through a router.
control network	The portion of the control system network where process data is transferred. It includes SCADA-to-PAC traffic and PAC-to-PAC traffic.
encapsulation	Wrapping a data set in a protocol header. For example, Ethernet data wrapped in a specific Ethernet header before network transit. Also, a method of bridging dissimilar networks where the entire frame from one network is enclosed in the header used by the link-layer protocol of the other network.
FDR	(fast device replacement) service allows a central device (the FDR server) to store configuration parameters for remote devices on the network. If a remote device requires replacement, the server automatically passes the stored configuration parameters on to a replacement device so that it can operate using the same configuration parameters as the replaced device. The replacement is accomplished without manually configuring the parameters. The FDR service should be used for all on the automation network that support it. It reduces the need for service personnel to keep configuration records on hand, and it reduces the chance of human error in entering the new configuration.
forwarding	Process whereby an Ethernet switch or bridge reads the contents of a packet and passes the packet on to the appropriate attached segment.
field network	The portion of the control system network in which field device monitoring and control traffic is primarily transferred. It includes PAC-to-I/O, PAC-to-drive, and primary-to-hot-standby-PAC traffic.
gateway	A combination of hardware and software that interconnects otherwise incompatible networks or networking devices. Gateways include packet assembler/disassembler and protocol converters. Gateways operate at layers 5, 6, and 7-the session, presentation, and application layers, respectively-of the OSI model.
header	The control information added to the beginning of a transmitted message. It contains required information such as the packet or block address, source, destination, message number, length, and routing instructions.

Term	Description
HMI	(human-machine interface) The keypad and screen or other user interface of a device.
host	Generally a node on a network, such as a computer, that can be logged into and used interactively.
ISO layered model	The open systems interconnection (OSI) reference model, which specifies how dissimilar computing devices such as NICs, bridges and routers exchange data over a network. The model is defined by the International Standards Organization. It consists of 7 layers. From lowest to highest, they are physical, data link, network, transport, session, presentation, and application. Each layer performs services for the layer above it (see OSI reference model).
LAN	(local area network) A data communications system consisting of a group of interconnected computers, sharing applications, data, and peripherals. The geographical area is usually a building or a campus.
LAN segmentation	Dividing local area network bandwidth into multiple independent LANs to improve performance and/or security.
latency	The delay incurred by an Ethernet switching or bridging device between receiving the frame and forwarding the frame.
layer	The software protocol levels that comprise a network's architecture, where each layer performs functions for the layer(s) above it (see ISO layered model).
MES	(manufacturing execution system) A computerized system that aids in managing data and communications for production flow.
MICE	(mechanical, ingress, climatic, environmental) An international standardization effort by IEC TC65, TIA TR-42.9, and CENELEC TC215 WG1 to establish environmental standards for industrial Ethernet.
NOE	Quantum140 NOE 771 xx Ethernet communication module
OSI	(open systems interconnect/interconnection) A structure for internetworking heterogeneous devices for distributed application processing according to international standards (see ISO layered model).
OSI reference model	A 7-layer network architecture model of data communication protocols developed by ISO and CCITT. Each layer specifies particular network functions such as addressing, flow control, error control, encapsulation, and reliable message transfer (see ISO layered model).
packet	A series of bits containing data and control information, formatted for transmission from one node to another. It includes a header with a start frame, the source and destination addresses, control data, the message itself, and a trailer with error control data (called the frame check sequence).
PAC	Programmable automation controller
port	A physical or logical connector on a device enabling the connection to be made.
process level network	The portion of the control system network in which process data is transferred. It includes SCADA-to-PAC and PAC-to-PAC traffic.

Term	Description
QoS	(quality of service) A performance specification for measuring and improving the transmission quality and service availability of a communications system.
router	Device capable of filtering and forwarding packets based on the network layer. Whereas a bridge or switch may read only MAC layer addresses to filter, a router can read data such as IP addresses and route accordingly. Unlike bridges, routers operate at level 3 (the network layer) of the OSI model. Also unlike bridges, routers are protocol-specific, acting on routing information carried by the communications protocol in the network layer. Bridges pass layer 2 (data link) packets directly onto the next segment of a LAN, whereas a router can use information about the network topology and so can choose a better route for a layer 3 packet. Because routers operate at level 3, they are independent of the physical layer and so can be used to link a number of different network types. Routers need to exchange information between themselves so that they know the conditions on the network, such as which links are active and which nodes are available.
SNMP	(simple network management protocol) Standard Internet protocol used to manage Ethernet network devices such as switches and routers. A 3-part protocol comprising: structure of management information (SMI), management information base (MIB) and the protocol itself. The SMI and MIB define and store the set of managed entities; SNMP itself conveys information to and from these entities. A TCP/IP host running an SNMP application can query other nodes for network related statistics and detected error conditions. The other hosts, which provide SNMP agents, respond to these queries and allow a single host to gather network statistics from many other network nodes.
VLAN	(virtual local area network) An implementation in some managed Ethernet switches to group ports and nodes based on 802.1Q protocol tags. This allows isolating network traffic and reducing Ethernet collision domains, resulting in better performance and deterministic system behavior.

Reference Documents

Source	Reference
International Electrotechnical Commission	IEC 62443 Industrial Communication Networks - Network and System Security.
US Department of Commerce	National Institute of Standards and Technology Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
US Department of Homeland Security and US Department of Commerce	HTTP://www.us-cert.gov/control_systems/ Catalog of Control Systems Security: Recommendations for Standards Developers - 2008 Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security - National Institute of Standards and Technology (NIST), Keith Stouffer, Joe Falco, Karen Scarfone - 2008 Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program - U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, National SCADA Test Bed (NSTB) - 2008 Control Systems Cyber Security: defence-in-depth Strategies - Idaho National Laboratory - May 2006
The Instrumentation, Systems and Automation Society (ISA)	Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks -2004 Mitigations for Security Vulnerabilities Found in Control System Networks -2006 2008 CSI Computer Crime & Security Survey - Robert Richardson, CSI Director Design Secure Network Segmentation Approach - SANS Institute InfoSec Reading Room - 2005 VLAN Best Practices - White paper FLUKE networks -2004 OPC Security Whitepaper #3 Hardening Guidelines for OPC Hosts.
British Columbia Institute of Technology, Byres Research - 2007	http://www.vicomsoft.com/knowledge/reference/firewalls1.html

Scan for local contents

Eurotherm Ltd
Faraday Close
Durrington
Worthing
West Sussex
BN13 3PL
Phone: +44 (0) 1903 268500
www.eurotherm.co.uk

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

HA032968 Issue 1 CN35592