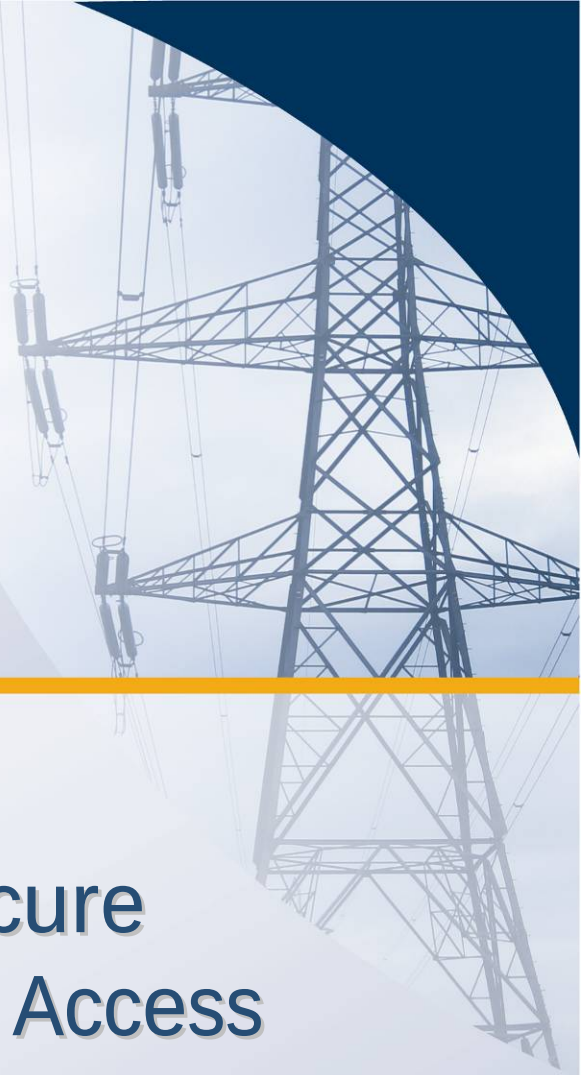
NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Guidance for Secure Interactive Remote Access

July 2011

to ensure the reliability of the bulk power system

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Table of Contents

Figures:

Disclaimer

This guidance document is intended to explain or facilitate implementation of secure interactive remote access; it does **not** contain mandatory requirements subject to compliance review.

Executive Summary

Registered Entities use interactive remote access technologies to access Cyber Assets to support and maintain control systems networks. However, these interactive remote access technologies have raised security concerns within the control systems community. Various organizations, such as the North American Electric Reliability Corporation, the Federal Bureau of Investigation, the Department of Energy, and the Department of Homeland Security have released notices and intelligence documents indicating potential security problems when secure interactive remote access is not properly authorized, designed, or configured.

Registered Entities must establish and enforce sound security measures within their organizations. Training, security policies, and documented processes will help ensure that security is not compromised inadvertently through the introduction of unsecured computers or unsecured access. Properly configuring software on those computers used to access the Cyber Assets, and implementing securely designed network architectures are crucial to the continued security of the Cyber Assets themselves. Also essential are secure methods to authenticate users.

This guidance document provides an overview of interactive remote access concepts, and includes example technology and policy solutions that Registered Entities may consider to strengthen security for interactive remote access to control system networks. Included in this document are case studies describing the steps that six companies have taken to implement secure interactive remote access. These case studies represent a range of entity size, perceived cost, and level of sophistication. Each case study is accompanied by a description of the secure interactive remote access implementation, and a network architecture diagram to aid Registered Entities in designing their own secure interactive remote access architecture.

Finally, this guidance document concludes with a brief list of recommended references that the technical reader may use to further explore the topic of secure interactive remote access and secure authentication.

Background

This guidance document, which supplements a North American Electric Reliability Corporation (NERC) Recommendation to Industry regarding secure interactive remote access, was initially developed as part of NERC Standard Project 2010-15.

Scope

This guidance document is intended to assist a Registered Entity in applying secure approaches for interactive remote access to Bulk Power System (BPS) Cyber Assets within a control system network, specifically including interactive remote access to support or maintain control system networks. A control system network is any network of Cyber Assets which is used to monitor or control a portion of the Bulk Power System.

While this guidance document primarily addresses securing interactive remote access to control system networks for the purpose of support or maintenance, the concepts and suggestions also apply to other remote access uses.

Audience

The intended audience includes those individuals responsible for developing the technical solutions for interactive remote access to control system networks. Other individuals who may benefit from this information include specific management personnel involved in identifying different solution options and determining corporate direction based on criteria such as risk, budget, security, etc.

Intent

This document describes security concerns regarding interactive remote access; provides specific recommendations that Registered Entities may implement to ensure secure interactive remote access to Cyber Assets; and includes case studies demonstrating secure methods of interactive remote access to Cyber Assets.

Other Materials

Other NERC products have addressed security with respect to interactive remote access, including an awareness bulletin and a Compliance Application Notice (CAN). The following descriptions provide detail on the specific issues the bulletin and the CAN address, and how they relate to this guidance document.

Critical Infrastructure Protection (CIP) Awareness Bulletin
On March 31, 2010, NERC issued a restricted distribution (marked *For Official Use Only*) bulletin, *CIP Awareness Bulletin on the subject of "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)."* The Awareness Bulletin addressed all aspects of remote access and VPN use in the electricity sector. The Awareness Bulletin contains several supporting arguments for the type of remote access

addressed in this guideline. While the Awareness Bulletin referenced generic VPN-based remote access without specific reference to its application, the principles in the bulletin apply to the interactive remote access methods covered in this guidance document.

CAN-0005

CAN-0005 also addresses the topic of remote access to Critical Cyber Assets, specifically, system operator laptops with the capability and purpose of controlling Critical Assets remotely. The CAN's purpose is in determining whether the Cyber Assets used to initiate the remote access should be considered Critical Cyber Assets. This guidance document described how remote access can be implemented in a secure manner. This guidance document therefore compliments CAN-0005.

Protecting Cyber Assets: Secure Interactive Remote Access Concepts

Secure interactive remote access allows users to access Cyber Assets to repair operating systems, troubleshoot hardware and application software issues, and repair data and modeling problems that cause application errors. Secure interactive remote access also provides a mechanism to monitor power system operations and status, allowing users to access the power system status beyond the boundaries of normally-authorized users and access requiring escort.

Before providing users with interactive remote access to Cyber Assets, Registered Entities must ensure strong security measures are in place to properly protect Cyber Assets. This section addresses integrating people, processes, and technology—three key elements necessary to successfully protect Cyber Assets—into developing security solutions.

People, Processes, and Technology: Protecting Computers Used for Secure Interactive Remote Access

People

While all three elements are important, ensuring that the appropriate people understand, develop, and execute the processes and technologies is seminal. Organizations must gain Senior Management support and approval for these processes and technologies. To sustain proper security practices, organizations must also invest in continuous training to ensure employees' skills are cultivated and maintained. Finally, the organization must have the tools and technologies that support the activities of employees to enable them to be successful.

Processes

Prior to investing in and implementing technologies, organization should first build their processes and then select the technologies that best meets their needs. Organizations should build continuous auditing and monitoring into their processes to maintain regular insight into the status of controls, enhancing risk and control oversight capability through monitoring and detection Once an organization establishes a process, the organization should also establish continuous training opportunities to ensure employees understand the process, their roles and responsibilities, and any changes to the process.

Technology

Most organizations have standards and policies to protect their computers against malware and other compromises. The NERC CIP standards require that the organization adopt basic security practices, such as protecting Critical Cyber Assets and other Cyber Assets within an Electronic Security Perimeter with firewalls and anti-malware software, and ensuring that security patches are updated. However, accessing a Critical Cyber Asset from outside networks using VPN technology raises different security concerns.

Security practices and proposed solutions for addressing these concerns are outlined in the next section.

Security Practices and Proposed Solutions for Secure Interactive Remote Access

General Security Practices for VPN Remote Access

An organization can apply the following practices help prevent remote computers using a Virtual Private Network (VPN) from threatening the organization's control system networks or Electronic Security Perimeters:

- Encourage or require the use of company-owned computers, which are subject to the organization's policies, maintained (i.e., contain anti-malware protection signatures, patches, etc.) by the IT department, and monitored by the company's configuration management system (if available), for VPN access.

- Restrict unauthorized installation of software by the user, allowing only company-approved applications.

- Educate interactive remote access users on the importance of using anti-malware software, keeping patches current, and maintaining a personal firewall to protect the computers and the information on them, as well as the company's assets. Implement a policy, or include in the corporate computer use policy, a requirement that anti-malware software, current patches, and a client firewall are installed on machines used for interactive remote access. This is especially important in cases where the use of company-owned computers for interactive remote access is not required.

- Include language in maintenance contracts obligating vendors to maintain anti-malware software and up-to-date patches, and protect with firewalls the computers they use for interactive remote access.

- Configure the VPN system to check for the presence of anti-malware software on connecting machines. Institute network access control[1] policies, which allow connections from machines with approved versions only.

- Configure the VPN to prevent split tunneling.[2]

- Force VPN traffic through a firewall or an intrusion prevention system (IPS)—or both—after it is unencrypted, so that the firewall or IPS can detect and mitigate any malicious content or behavior.

[1] See Wikipedia article on Network Access Control available at http://en.wikipedia.org/wiki/Network_Access_Control.
[2] See Wikipedia article on split tunneling available at http://en.wikipedia.org/wiki/Split_tunneling.

- Limit allowable protocols from computers and networks that are not company-owned.

- Disable all ports and services not required for the operation of application software.

- Restrict the use of the remote computer to "work only" functions (i.e., the remote computer should not be used for personal use, or shared with family members). The policy should restrict personal use and connectivity to public networks.

- Provide interactive remote access users with a bootable compact disc (CD) that includes the VPN client and the tools necessary to access internal resources remotely (e.g., secure shell, Remote Desktop protocol client, etc.). All of the considerations listed above should be implemented on the bootable CD system. Every time users connect, they boot into a hardened (i.e., all unnecessary services removed) operating system from read-only media. The operating system is configured with no disk drivers, so a malicious actor would not have the ability to read or write data to the local hard disk. The Air Force research Laboratory developed such a solution for the Department of Defense (DoD).[3] The linux.com website also published detailed instructions for implementing a boot CD solution.[4] Users can also implement a boot CD solution using Microsoft Windows, if Windows is required for interactive remote access.

Controlling Interactive Remote Access to Generation Facilities

Generation facilities may require interactive remote access to cyber assets for a variety of reasons, such as allowing company maintenance personnel to support and troubleshoot cyber assets during emergencies and outside regular operating hours as well as allowing vendors to remotely troubleshoot and test the generator units and control systems.

Entities may use multiple procedural and technical controls to restrict and secure interactive remote access to Cyber Assets located within generation facilities, such as:

- Requiring externally initiated connections to authenticate through an intermediate server, and connect using a desktop sharing protocol such as Remote Desktop Protocol (RDP) to the corporate network. The external user then follows the steps for the internal connection method, as described below.
- Restricting network connections to only be initiated from authorized corporate systems within the corporate network.
- Limiting continuous connections to a specified time limit (such as 16-hours) to ensure that the remote connection is re-established at least once per work-day. If

[3] See http://spi.dod.mil/docs/LPS_family.pdf.
[4] Waddell, Jeffery Douglas, "Secure Boot CDs for VPN HOWTO", June 15, 2007, http://www.linux.com/learn/docs/ldp/732-Secure-BootCD-VPN-HOWTO.

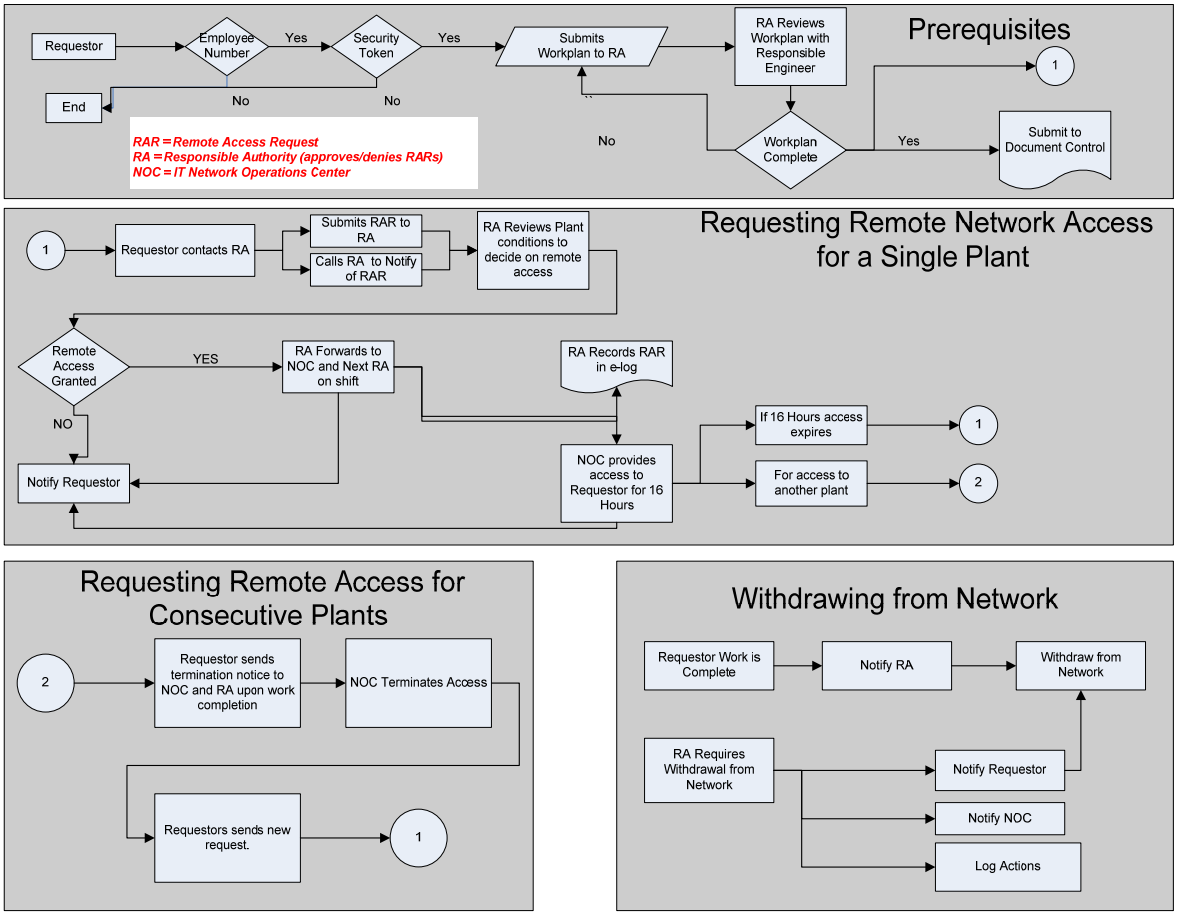
the remote user requires additional time, the remote user must receive special approval.

- Developing a detailed plan describing the work to be performed remotely, the need for interactive remote access, and the expected duration of the interactive remote access connection. This plan should be approved by appropriate plant personnel prior to granting interactive remote access.
- Restricting each user to one connection to an individual plant at one time.
- Requiring all users—internal or external—to (1) have unique, assigned user identifications (ID) and security tokens prior to being granted interactive remote access; (2) participate in cybersecurity training; and (3) undergo Personnel Risk Assessments prior to obtaining a user ID and token.
- Establishing a multi-step/multi-group approval process that may include:
    - Developing an interactive remote access form to be approved by appropriate plant personnel prior to interactive remote access being granted;
    - Assigning information technology (IT) Network Operations Center (NOC) personnel responsibility to grant and remove interactive remote access. NOC personnel should also ensure that interactive remote access is removed when the work is completed or if the specified time limit is reached, whichever comes first.
    - Developing daily reports from the NOC for verification and review of current interactive remote access.

NOTE: *Connections should only be allowed to plant ancillary systems like Plant Information, soot blowing, etc.; however, some plant systems themselves are tied to the plant Distributed Control System.*

The sample flowchart below outlines the steps necessary to grant and remove generating facility interactive remote access.

Figure 1: Sample Process Flow Drawing for Granting Access to Generating Facilities

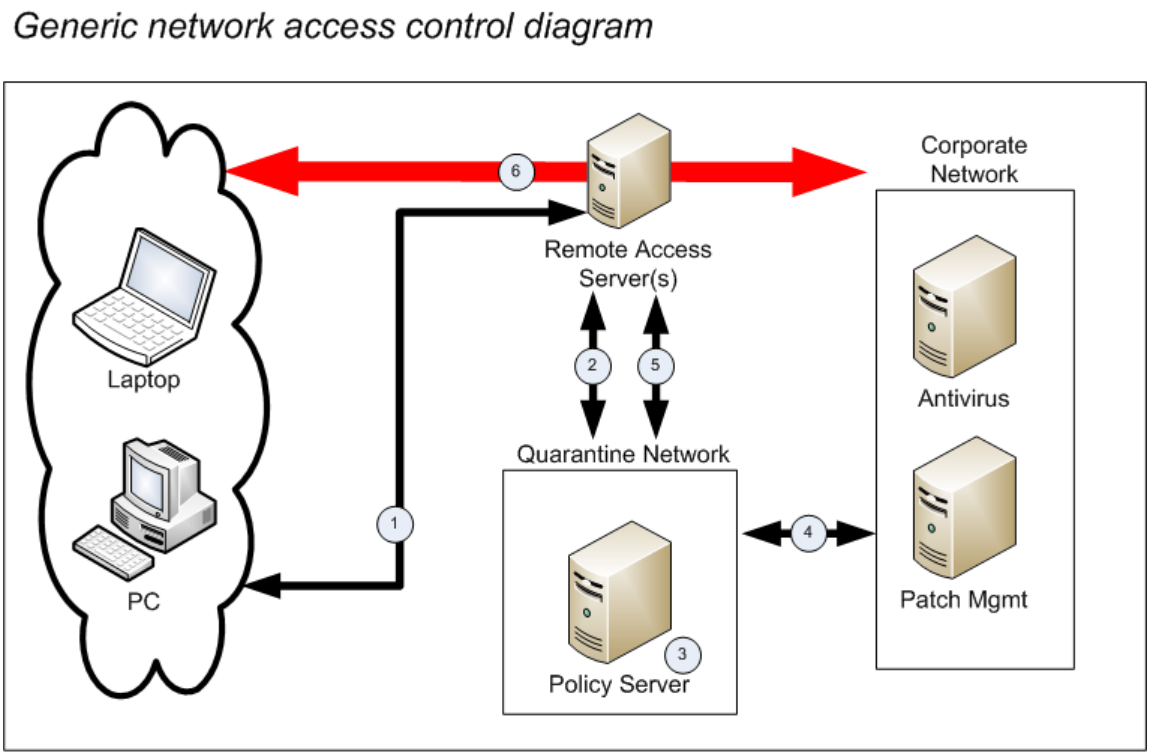


Network Access Quarantine

Registered Entities should perform checks on the interactive remote access computer to determine if the computer should be permitted interactive remote access connectivity. These checks—sometimes called *health*, *suitability*, *screening*, or *assessment* checks—require software on the user's system to verify compliance with certain requirements from the organization's secure configuration baseline. For example, the user's anti-malware software must be up-to-date, the operating system must be fully patched, and the remote computer must be owned and controlled by the organization. These checks should be performed before granting the interactive remote access computer any access to the corporate network.

Based on the results of these checks, the organization can determine whether the remote computer should be permitted to use interactive remote access. If the user has acceptable authorization credentials but the remote computer does not pass the health check, the user and remote computer should be denied network access or limited access to a quarantine network so that authorized personnel can fix the security deficiencies.

Figure 2: Generic Network Access Control Diagram



1. A remote user makes a request to access the corporate network. This interactive remote access request is made through a Remote Access Server.
2. The Remote Access Server queries the remote user's computer for configuration information, including patch levels and anti-malware update levels. The Remote Access Server sends the remote user's configuration information to the Policy Server.
3. The Policy Server validates the remote user's computer configuration settings against its policy settings, and determines if the remote user's computer meets the policy. If the remote user's computer configuration meets the policy, the user is granted access to the corporate network (step 6).
4. If the remote user's computer does not meet the policy settings, the remote user's computer is placed on a Quarantine Network. The Policy Server or Remote Access Server then attempts to update the user's computer to meet the policy settings by accessing patch management and anti-malware update services. The update servers may be logically located on the Quarantine Network, or may be located within the corporate network. If the update servers are located on the corporate network, the Remote Access Server ensures that the remote computer can *only* access the update servers, not any other resources on the corporate network.[5]

[5] Denying the user's computer access to the corporate network and the control system network until it is current with corporate policy is a strong security solution. However, this solution may require additional overhead, such as using multiple update servers (on the corporate network or Quarantine Network) to keep systems current and updated.

5. Following the update of the remote user's computer, the configuration is again checked against the policy settings by the Policy Server (as in step 3). If the remote user's computer meets policy, it is granted access to the corporate network (step 6). If the remote user's computer still does not meet the policy requirements, it either remains in the Quarantine Network to allow the remote user to manually update the computer to meet the policy settings, or it is disconnected from interactive remote access.
6. Once the remote user's computer has successfully met the policy settings, it is granted access to the corporate network. Interactive remote access to Cyber Assets within an Electronic Security Perimeter may still require additional access control and intermediate servers.

Multi-Factor Authentication

Multi-factor authentication technologies use authentication factors from at least two of three generally accepted categories: something known (e.g., a password or personal identification number or PIN), something possessed (e.g., a one-time password token or a smart-card), and something unique about the user (e.g., fingerprint or iris pattern).[6] Systems that use two or more factors are described as using multi-factor authentication; systems that use *only* two factors are described as using two-factor authentication. User IDs are *not* considered factors in a multi-factor authentication system.[7]

Examples
The following are examples of factors used in multi-factor authentication. More detailed descriptions are provided for some of the newer or lesser-known methods below.

Something Known	Something Possessed	Something Unique About The User
• Password • PIN • Passphrase	• One-time password tokens • Soft tokens • Magnetic cards • Smart cards • USB tokens • Hybrid USB/One-time password tokens • Grid Card or Scratch Card* • Dynamic Grid Card* • Out-of-band One-time* password • Challenge-response systems*	• Fingerprint • Facial features • Iris (has replaced retina)

[6] Additional categories, such as location are occasionally used, but not very often.
[7] A source of information about multi-factor authentication is contained in the Appendix (page 7) of the Federal Financial Institutions Examination Council's document *Authentication in an Internet Banking Environment (*http://www.ffiec.gov/pdf/authentication_guidance.pdf). Also of note is the discussion in the appendix delineating the difference between "identification" and "authentication."

	• Digital Certificates	

** Description below*

Grid Card or Scratch Card: Inexpensive alternatives to one-time password tokens. The user receives a credit card size card with a grid of codes in labeled rows and columns. The codes in the grid are unique to the user. When logging in, the user receives a random row and column number and is prompted to provide the code associated with the designated cell in the grid. A variation of the password token is to receive a single number in each cell in the grid. The user then receives the starting cell on the grid and follows a predetermined, user-chosen path through the grid to determine the rest of the code (e.g., one cell to the right, one up, two to the right, one down, etc.). This path provides another layer of security because only the user knows the correct path through the grid.

Dynamic Grid Card: A variation where the grid or other pattern of numbers and characters is displayed on the screen when logging in. A scheme is used by which the user selects numbers or characters based on something they know, such as the path method described previously. Some advantages to using a dynamic grid card are: (1) the grid changes each time the user logs in; and (2) the user does not have to maintain a physical card.

Out-of-band One-time passwords: Passwords that are delivered real-time through text messaging. They provide an additional layer of security because a separate communication channel is used to deliver the password to the user. An adversary would have to subvert this communication channel as well as the computer network channel to gain access to the system. Also, since the password is for a one-time use only, the window of opportunity for an adversary is much smaller than for a traditional computer password system, where passwords typically live for three-to-six months.

Challenge-response systems: Used to provide some level of assurance that the system being accessed is the desired system, in addition to authenticating the user. In a challenge-response system, after the user connects to the system, the user is presented with a unique “question” (the challenge), and must respond with the correct “answer” (the response). A dynamic grid card is an example of a challenge-response system. However, a more common example sends a cryptographically-generated number associated with a specific user, which the user enters into a calculator token to generate a corresponding number. The number is then sent back to the accessed computer. If the user is presented with an invalid challenge, the token detects the error, and no response is generated, indicating that the user is not accessing the desired computer. If the response is not correct, then the user is not authorized.

Benefits of Multi-factor Authentication
One benefit of multi-factor authentication is the added layer of security it provides. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Another benefit of multi-factor authentication is that it can provide an extra layer of security at a low cost. For example, an inexpensive two-factor authentication solution is to use the server as a software appliance or a hypervisor system appliance.[8]

Drawbacks of Multi-Factor Authentication
While inexpensive multi-factor authentication solutions exist, some of the more common solutions can be expensive. For example, hardware tokens are popular, but the logistics of managing and maintaining the tokens add to the expense. Specifically, an administrator must establish policies and procedures to manage all tokens, and then associate a token with a user. Grid cards and out-of-band one-time passwords are less expensive alternatives to tokens.

Another drawback of multi-factor authentication is that not all solutions are secure. Software tokens are less-secure than hardware tokens because the software can be cloned and the computer clock moved forward to predict future passwords or to analyze the password generation algorithm.

Assessing the Implementation of Interactive Remote Access Controls

The Registered Entity should assess the implementation of the technical controls for interactive remote access, create an action plan to remediate or mitigate any findings, and document the execution status of that action plan. This assessment should include:

- A review of the technology solutions used to provide interactive remote access, which should be current.
- A check of the version and patch-level of all software (including all software used for interactive remote access) to verify that the software is supported, patches are updated, and no unauthorized software has been added to the cyber asset.
- A configuration review of the Cyber Assets used to provide interactive remote access to ensure they are deployed as designed.
- A comparison of the record of all individuals authorized for interactive remote access with the interactive remote access system(s) user accounts and access rights to validate that access is granted only to authorized users.
- A hardware verification check to ensure that no new hardware has been added, or unapproved version updates have occurred.

[8] See http://en.wikipedia.org/wiki/Hypervisor.

Network Architecture Decisions

This guidance does not specify a specific network architecture, rather, it provides for a great deal of flexibility in designing and using network communications within an organization. Registered Entities must balance the security of the communications against the practical considerations for monitoring and controlling network traffic.

Communications network can be established, configured and managed as one of two security designations: "internal networks" and "public networks." Internal networks have a restricted membership, and implicitly include a level or trust among the participants. Public networks have unrestricted membership, and there is no trust (implied or otherwise) among members. In fact, public networks could be considered hostile environments. Note that while all public networks are also considered "shared networks," some instances of internal networks are also "shared networks." Registered Entities must consider their acceptable level of risk associated with the level of trust with other members of a shared network when making network architecture decisions.

The term "internal network" is intended to capture instances such as any of the following:

- An internal corporate network managed by a Registered Entity;
- A corporate network run by a shared services organization, which may serve multiple separate and distinct Registered Entities, and not owned by any one Registered Entity;
- A network that is owned and maintained for use by a consortium of different Registered Entities that have no other formal corporate relationship (e.g., an association of municipalities in a state); or
- A network established for use by all entities, regardless of individual entity organization, within a defined geography (e.g., a network run by a regional entity, an ISO or an RTO).

The term "public network" is intended to capture instances such as any of the following:

- The Internet
- A network managed by a third party with no restriction on membership, such as a metro-area fiber network

One key area in determining network architecture is encryption, and whether encryption is essential or merely a best practice. Whenever the communication crosses a public network or across a dial-up network, encrypting the traffic is essential because the traffic is vulnerable to interception and modification.

Registered Entities may also consider encrypting traffic over internal networks. Although many either do feel the need to, or for monitoring purposes do not want to, encrypt traffic

when it is on an internal network, some understand that even internal networks may be subject to security vulnerabilities, eavesdropping or other malicious use.

Network Communication Encryption
Network communication encryption used within electricity sector control systems can introduce significant design challenges because encryption, authentication, or encapsulation (or a combination of these three) adds complexity and potential operational limitations to the environment. If not properly implemented, network communication encryption may only provide the illusion of security, while introducing additional risk.

The Registered Entity should secure its implementation of selected encryption technologies consistent with vendor recommendations and guidelines on the use of evaluated cryptography. Registered Entities should select evaluated cryptographic modules that support strong algorithms for encryption, authentication, key exchange, and hash functions.[9]

Registered Entities may deploy cryptographic systems with or without the use of encryption. Without encryption, either authentication or encapsulation maybe used to authenticate users and ensure the integrity of data while in transit without the added overhead of encryption. If the data is sensitive, then encryption should also be used. The sensitivity of the data should govern the decision by the Registered Entity to use encryption or not.

The Registered Entity should protect cryptographic systems from physical tampering and uncontrolled electronic connections. The cryptographic systems should have remote key management capabilities.

Understanding the various options and implementation examples listed in the reference material in this document can help a Registered Entity decide which encryption technologies, algorithms, and key lengths can best serve as an appropriate security control within a specific control systems environment.

Vendor Risks

As a cost-saving measure, Registered Entities contract technology services out to maintain and support their Cyber Assets. Organizations outside the Registered Entity performing these maintenance and support functions increase risks to interactive remote access security. Some risks include vulnerabilities to systems caused by other assets not connected to or controlled by the Registered Entity. Outsourcing services does not relieve

[9] The employment of cryptography consistent with that found in Federal Information Processing Standard (FIPS) 140 is one accepted method to ensure adequate protection of sensitive data, authentication, non-repudiation, and secure key exchanges. Many of the cryptographic algorithms used in commercial cryptographic modules and cipher suites may not meet the criteria for FIPS-approval and should not considered for use since they could not be configured to be compliant with FIPS.

the Registered Entity of the responsibility to ensure that appropriate controls are in place to protect its Cyber Assets.

Contractual Language to Address Security Concerns

To ensure security controls are in place with contracting organizations, the Registered Entity may use specific contract language identifying minimum performance and cybersecurity requirements to which the vendor must adhere. The contract should address the vendor's security responsibilities for the Registered Entity's resources, including protecting against malicious software by using Registered Entity approved malicious software prevention solutions (e.g., anti-virus, whitelisting, etc) and by installing security patches.

The following section is an example of contractual language for patching and malicious software protection:

> Patching and Malicious Software Protection
>
> Vendor represents and warrants that it has used commercially-reasonable efforts to ensure against introduction of any malicious software into <<Registered Entity>>'s systems. These efforts include the implementation of security patches and antivirus or anti-malware solutions to remediate vulnerabilities. Where Vendor does not apply patches or utilize virus or other malicious software prevention solutions, Vendor represents and warrants it has used alternate means that provide the same or better level of protection.
>
> Vendor shall immediately advise <<Registered Entity>>, in writing, upon reasonable suspicion or actual knowledge that the Application may contain a virus or other malicious software. If a virus or other malicious software is found to have been introduced into <<Registered Entity>>'s systems by Vendor, Vendor will, at its own expense, repair or restore the Application within 10 business days thereafter. Vendor shall use all reasonable commercial efforts, at no additional charge, to assist <<Registered Entity>> in reducing the effects of the virus or other malicious software if introduced by Vendor and, if a virus or other malicious software introduced by Vendor causes a loss of operational efficiency or loss of data, to assist <<Registered Entity>> to the same extent to mitigate and restore such losses.

Appendix A: Secure Interactive Remote Access Architecture Overview

Today, the two most prominent options for secure interactive remote access are the traditional IPSec VPN and the SSL VPN. The IPSec VPN requires client based software that is typically proprietary and requires a compatible host to connect to. This solution is generally best suited for a site-to-site connection, for example connecting where a regional office to the main office. The IPSec VPN is a network layer protocol that, once connected, gives connectivity to the remote network as if the user were locally connected.

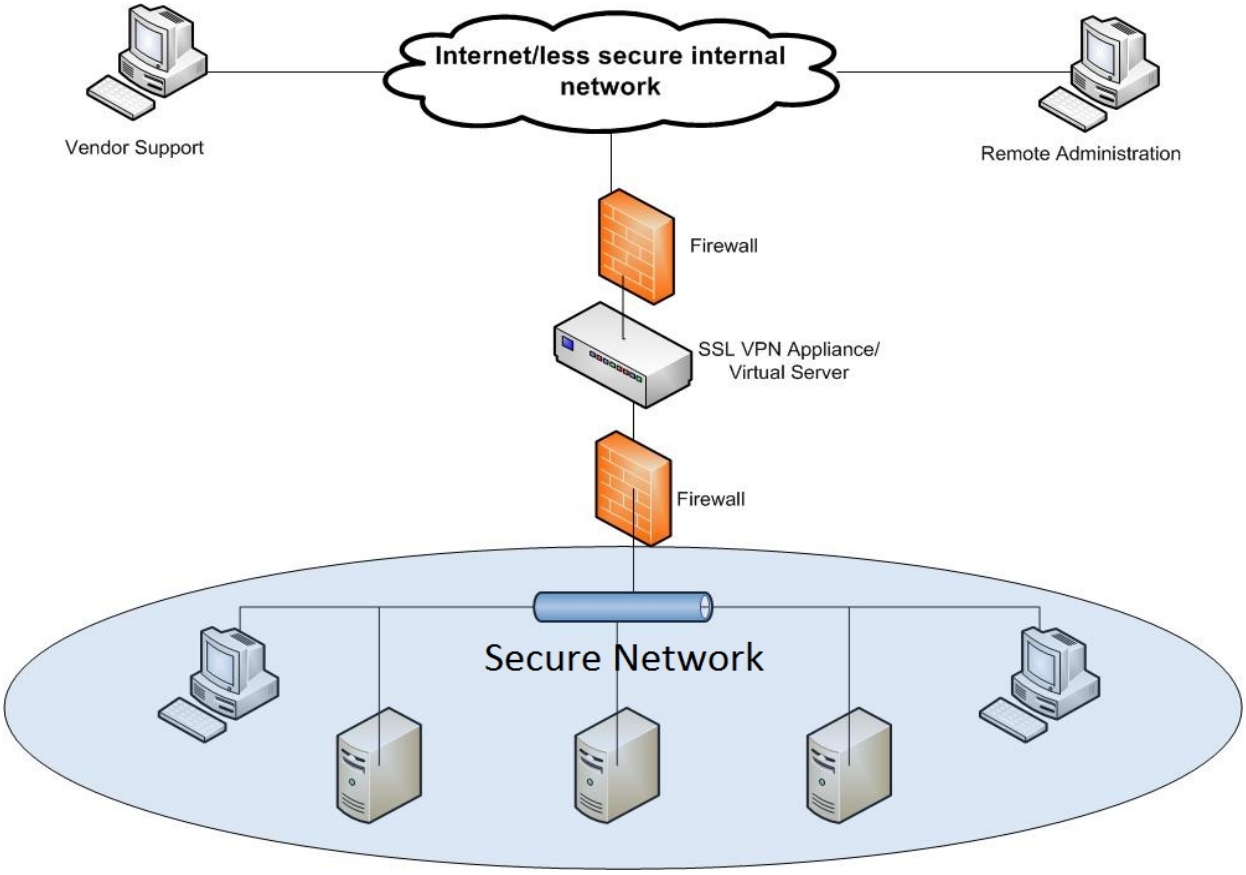
The SSL VPN can be a client-less VPN alternative that runs at the application layer. This type of secure connection usually connects to a VPN appliance (or virtual server) that is hosted at the company's site. Because SSL VPNs run in application layer, very restrictive policies can be applied to remote users allowing access only to specific applications. They commonly support at least two-factor authentication and are able to produce session access logs. Some implementations are able to record command line (ssh) and RDP sessions that can be played back or archived, or both.

If the VPN appliance offers application services such as ssh or VNC (Virtual Network Computing) clients, the VPN appliance itself may serve the function of an intermediate server. The VPN appliance acts as a proxy, and the connection into the secure network from the DMZ appears to originate at the appliance, not at the remote computer. If the VPN appliance does not have this feature, or if more flexible methods of access are required, a separate VPN appliance can be added to the configuration to provide an intermediate server.

Since several vendors offer secure interactive remote access solutions, client-less SSL VPNs can be a cost-effective solution for utilities of differing sizes and resources.

Below is a diagram of a basic SSL VPN implementation:

Figure 1: Generic Interactive Remote Access Drawing using SSL VPN



Appendix B: Use Cases and Case Studies

Use Cases

This guidance document seeks to provide real-life examples—or case studies—of protective defense-in-depth methods to secure interactive remote access for support and maintenance to ensure adequate cybersecurity measures are in place to minimize risk to the BPS. These methods include examples of connectivity for functions such as:

Support and Maintenance Functionality

- Hardware, Operating System, and Application Programming Support – Includes connectivity to Cyber Asset systems for maintenance and support staff, and vendor access to provide troubleshooting and resolution of issues such as problems with underlying operating system software and other third party layered application software.

- Maintenance of Power System Applications, Data, and Modeling – Includes connectivity to Cyber Asset systems for maintenance and support staff, and vendor access to provide troubleshooting and resolution of issues such as debugging power system applications, databases, and data models. This could include applications such as Supervisory Control and Data Acquisition (SCADA), automatic generation control, state estimator, or contingency analysis, or a combination of these applications.

Read-only Monitoring

- This common configuration utilizes a unidirectional (outbound from the Cyber Asset network) logical connection to a read-only system. By its configuration, read-only monitoring prevents any access to, or control of, the BPS from occurring. This external system would typically reside on a corporate network environment that would still be protected from direct Internet access by firewalls and other protective measures. Read-only monitoring is commonly used to grant those individuals not involved in the real-time operation of the BPS the ability to view data in a near real-time mode. This viewing access increases BPS situational awareness beyond the boundaries of the normally-authorized set of users with access to the Cyber Assets.

Case Studies – Introduction

The following case studies were solicited from industry participants, and describe actual implementations of secure interactive remote access that are in use at their companies. The descriptions and network drawings are reproduced here as the industry participants submitted them, with minor modifications to clarify terms and to provide anonymity.

The case studies present a range of implementation methods and expected purchase and support costs for both small and large entities. While the case studies differ somewhat (e.g., two-factor authentication vs. multi-factor authentication; specific products or architectures; etc.), they provide a reference of methods that the Registered Entity can implement to secure interactive remote access.

Case Study 1 – External Interactive Access to Cyber Assets within an Electronic Security Perimeter

Purpose:
Interactive remote access (access from locations other than company facilities) is required for the following activities:

- Off-hours and emergency support and troubleshooting by company support and maintenance personnel
- Vendor support

Overview
This solution uses the corporate VPN (i.e., the VPN system used by the entire company) to allow access from the public Internet. A VPN dedicated to Electronic Security Perimeter access could be used, but in this case the corporate VPN implementation provides a high level of security, and allows control of which corporate subnets a user can traverse based on their authentication, so providing a dedicated VPN solution for Electronic Security Perimeter interactive remote access was not necessary. Once VPN access is established, the user connects to a jump host using remote control or remote desktop technology. The jump host is a computer that serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly.[10]

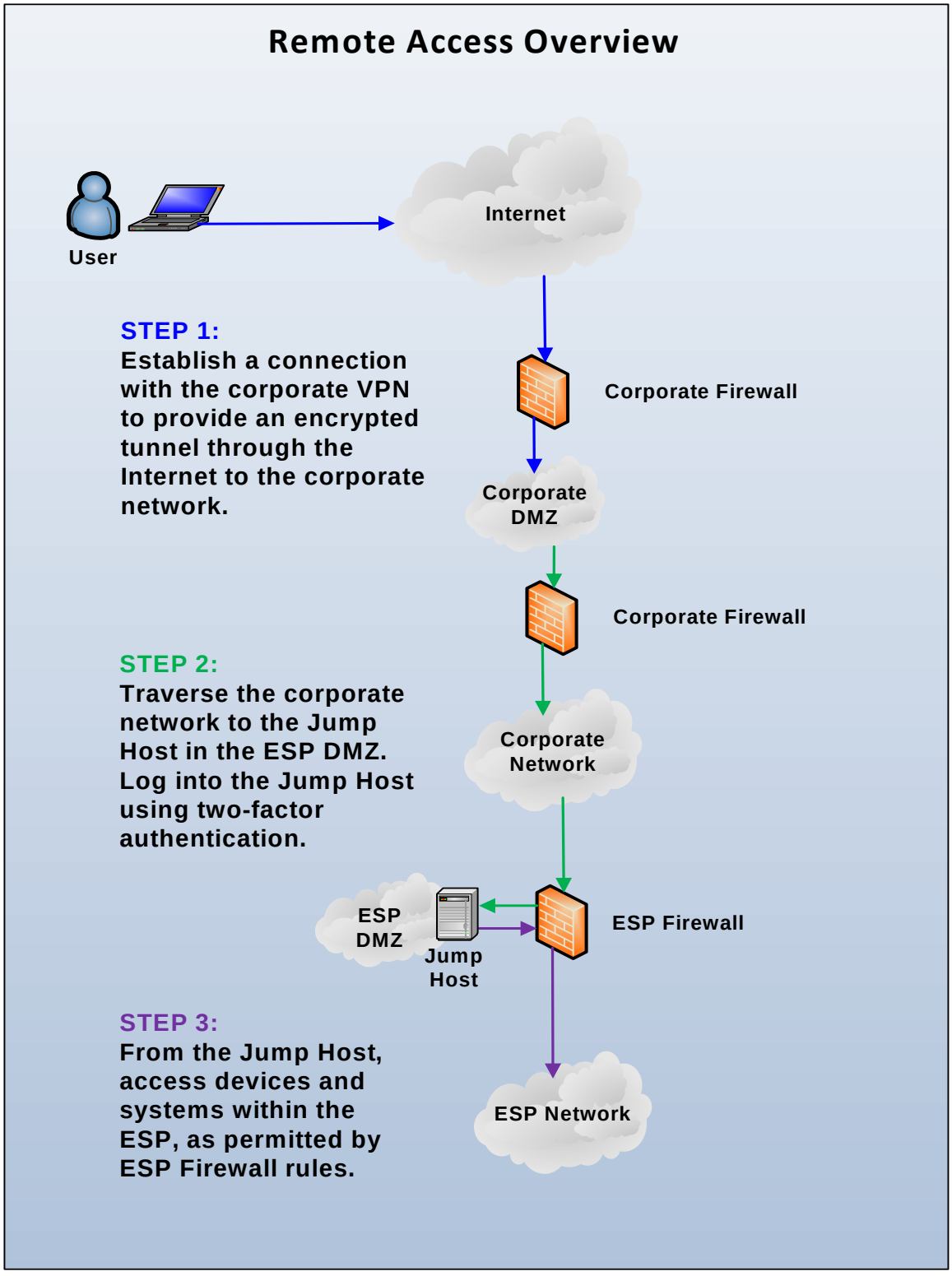
Two-factor authentication is required to log into the jump host. The two-factor authentication is provided by a system installed specifically for and dedicated to authentication to and within the Electronic Security Perimeter. Although not specifically required by the NERC CIP standards, a dedicated system was installed for ease of administration and to facilitate compliance with CIP-005-4, Requirement R1.5 and CIP-007-4, Requirement R5 and its sub-requirements.

Finally, the jump host is in a DMZ, separate from Critical Cyber Assets in the Electronic Security Perimeter, further protecting the Critical Assets by allowing only required protocols to specific Cyber Asset addresses from the jump host through the Electronic Security Perimeter DMZ firewall.

[10] This also simplifies maintaining ongoing compliance. Per CIP-005-4, Requirement R2.2, all ports and services enabled on Electronic Security Perimeter access points must be documented. Using a jump host eliminates protocols that might otherwise be required to access devices within the Electronic Security Perimeter, and also reduces the number of changes that will occur to the protocol list.

A diagrammatic overview of the process is provided in **Error! Reference source not found.**, below. Details of the procedures for employee and vendor support access are provided in the Procedure Details section, and in the flow chart diagrams (**Error! Reference source not found.** and **Error! Reference source not found.**).

Figure 2: Interactive Remote Access Overview



Note that this solution includes logging of successful and unsuccessful login attempts using a Security Information Event Monitoring (SIEM) system installed specifically to support NERC CIP compliance. The SIEM allows event correlation across multiple systems to detect suspicious activity, and can generate alerts when such activity occurs. For example, a successful login to the jump host that is not followed by a successful login to a Cyber Asset within the Electronic Security Perimeter from the jump host may indicate suspicious activity, i.e., someone is connecting to the jump host for reason other than its intended purpose.

While a SIEM system provides an additional layer of security and contributes to defense-in-depth, it is not specifically required by the NERC CIP standards. It was installed to facilitate ongoing compliance, in particular with CIP-005-3, Requirement R3 and CIP-007-3, Requirement R6 and their sub-requirements. (Note: The use if a SIEM is equally applicable to CIP-005-4, Requirement R3 and CIP-007-4, Requirement R6.)

Procedure Details:

Company Employee

1. The employee uses the corporate VPN to gain access to the corporate network.
    a. Pursuant to corporate policy, VPN access to the corporate network requires two-factor authentication.
    b. The authentication factors are a PIN and a one-time passcode from a hardware token.
2. The employee connects from the VPN through the corporate network to a jump host computer inside a DMZ between the corporate network and the Electronic Security Perimeter network.
    a. The DMZ is an Electronic Security Perimeter network itself but does not hold any Critical Cyber Assets, just covered assets (Cyber Assets used for authentication and monitoring)
    b. Only necessary and authorized protocols are allowed into the DMZ, and only to specific addresses.
    c. The jump host challenges for two-factor authentication. The authentication factors are a PIN and a one-time passcode from a token. The user uses the same token as for the corporate VPN[11], but the infrastructure for the two-factor authentication to the Electronic Security Perimeter is completely separate from the corporate infrastructure and maintained inside the Electronic Security Perimeter.
    d. Multiple unsuccessful login attempts will lock out the account.
    e. The jump host is part of an Electronic Security Perimeter directory service domain, separate from the corporate domain. All components of this

[11] The same token is used for user convenience. Token information is exported from the corporate system to the Electronic Security Perimeter system. Accounts on the Electronic Security Perimeter system are maintained in accordance with applicable CIP standards.

directory service are maintained inside the company's Electronic Security Perimeters. The user must log into the Electronic Security Perimeter domain after successful two-factor authentication.

f. Successful and unsuccessful login attempts are logged to the Electronic Security Perimeter SIEM.

g. The Electronic Security Perimeter domain accounts and the two-factor authentication credentials are authorized and maintained pursuant to CIP-007.

h. The user accounts in the Electronic Security Perimeter domain are not privileged accounts. They have only user-level access to the jump host machine.

i. Sessions are automatically disconnected after a period of inactivity.

3. From the jump host, the user accesses Cyber Assets within the Electronic Security Perimeter using the preferred access method for the Cyber Assets. The necessary clients or remote access software are installed on the jump host.

4. Access from the jump host to Electronic Security Perimeter Cyber Assets is controlled by a firewall. Access is only allowed from the jump host, and only to computers authorized for external access, and only on specific ports.

Vendor Support

1. The company support and maintenance personnel or control room staff member requesting support or initiating a previously arranged support session places a telephone call to the vendor support team member (vendor). Note that the call is always initiated from the company to the vendor. This protects against social engineering attacks.

2. The vendor initiates a connection to the corporate VPN.

   a. There is a hardware token assigned to each vendor. The token is held by the control room supervisor. The PIN is maintained by the vendor.

   b. The support and maintenance personnel or control room staff member requesting support or initiating a previously arranged support session obtains the appropriate token from the Control Room Supervisor.

   c. The staff member provides the vendor with the current passcode from the token. This way the vendor is provided with a one-time passcode.

3. The vendor then proceeds as above for Company Employee starting with Step 2 and follows the same steps as the company employee, except that the support and maintenance personnel or control room staff member requesting support provides the passcode.

4. The Electronic Security Perimeter directory services account may be an account dedicated to the individual vendor staff member, a one-time use account set up just for this session, or a shared account. In any event, it is managed in accordance with CIP-007.

5. When the support call is complete, the hardware token is returned to the Control Room Supervisor.

Figure 3: Interactive Remote Access Procedure for Employees

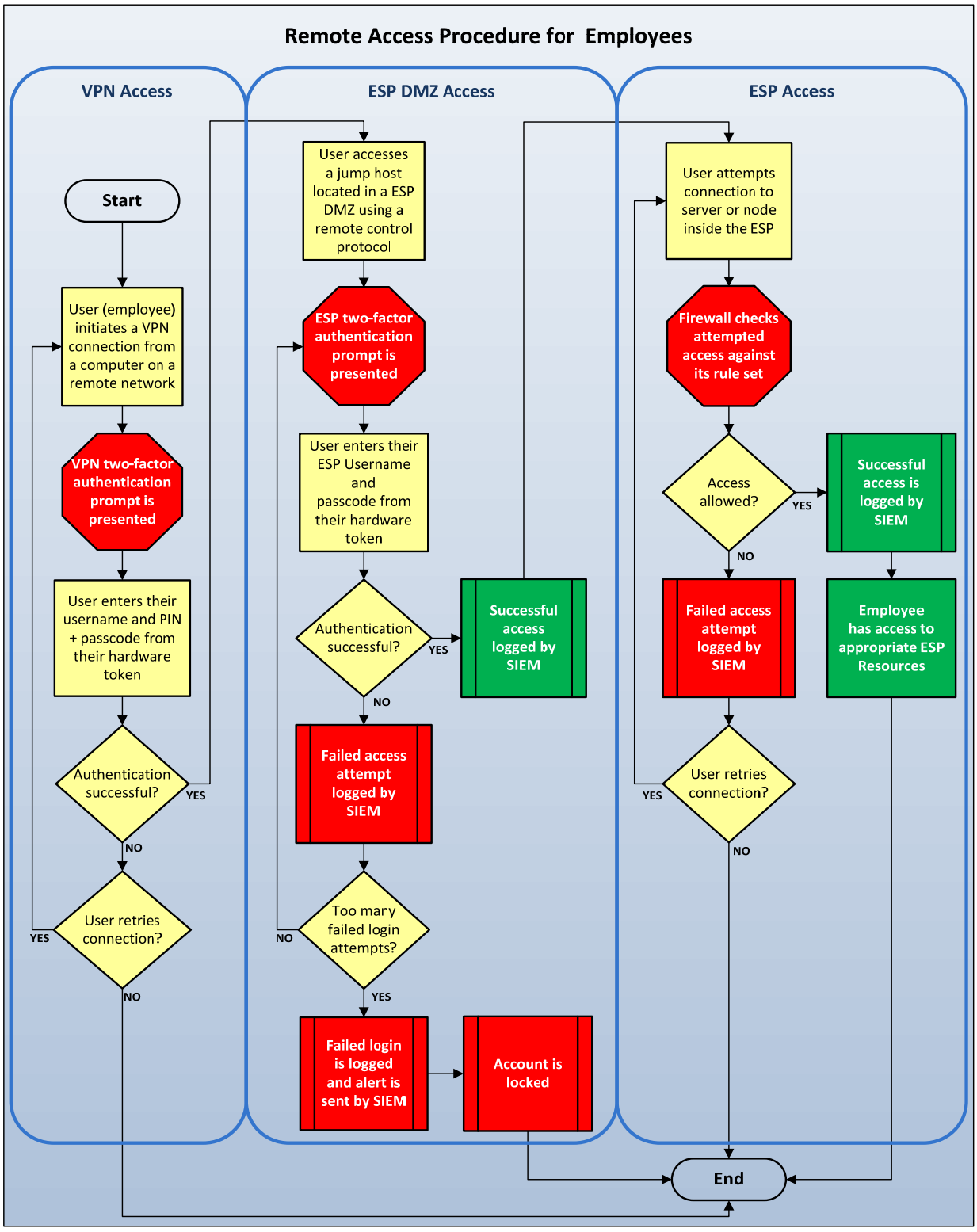
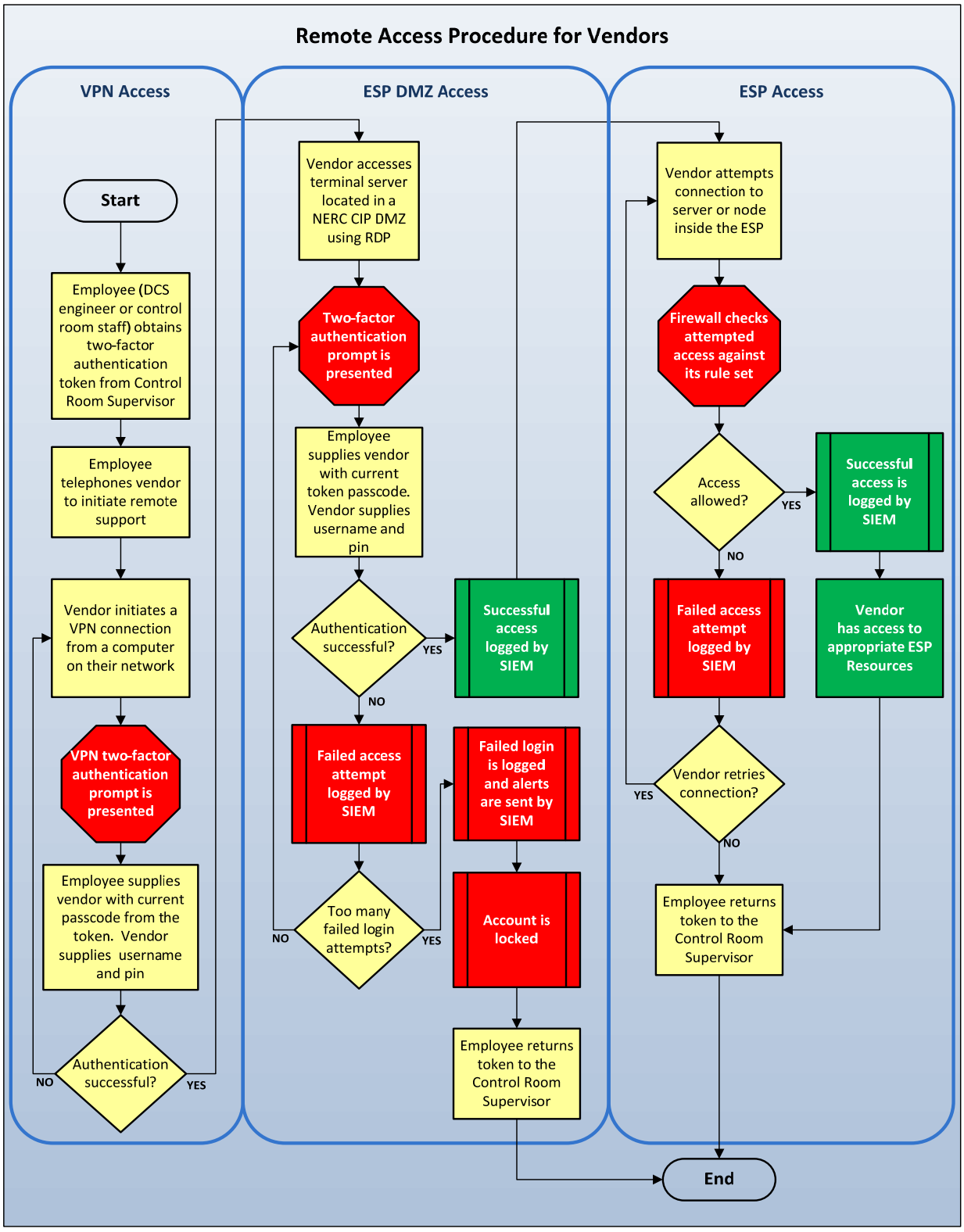


Figure 4: Interactive Remote Access Procedures for Vendors



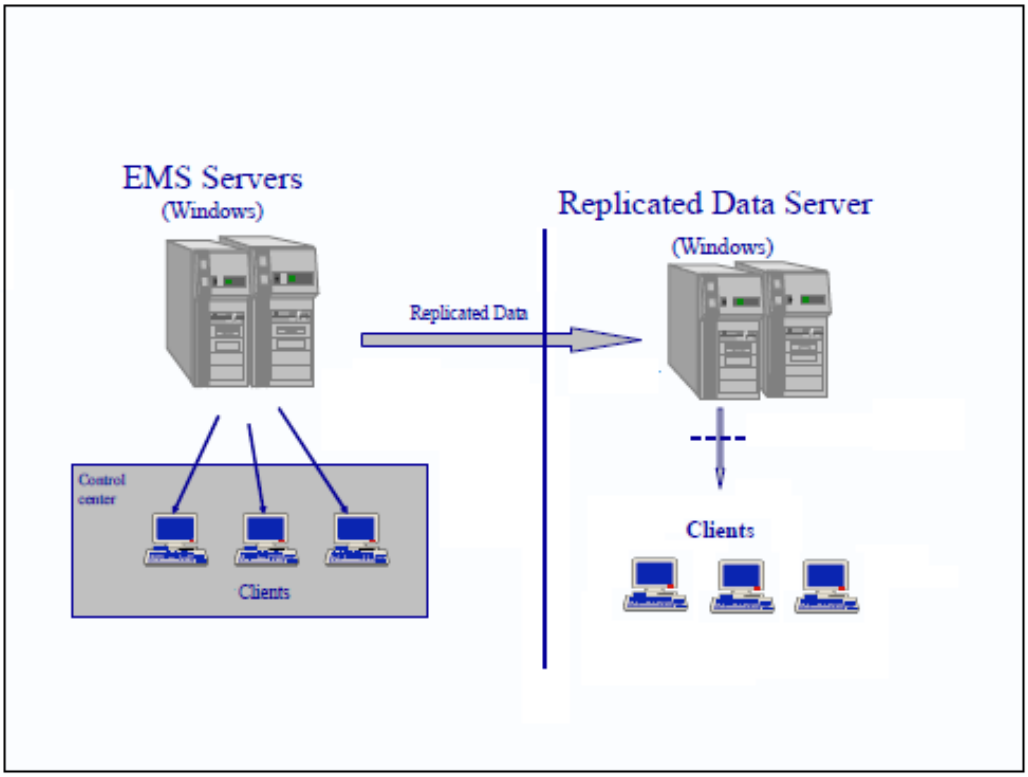
Case Study 2 – EMS Read-only Access via Replicated Data Servers

In addition to clients accessing displays directly from the EMS servers, clients can access read-only displays from servers called replicated data servers which are also know as corporate data servers. These servers contain clones of the EMS database to which data is replicated from the EMS servers. They reside outside of the Secure EMS network. This configuration offers two advantages:

- **Security:** Users can call up displays, but they cannot connect to the EMS computers or issue controls. The displays are read-only.
- **Scalability:** Replication places a predictable, relatively static load on the EMS computer. Large numbers of clients can access displays without placing any additional load on the EMS servers.
- **Advantages:** The replicated system uses identical software to the real EMS, so any updates to configuration or presentation can be readily copied to the replicated data servers providing the same "look and feel" to all users.

The corporate data servers have the same authorization software as the EMS servers to allow users to access only the displays which they are required to view. Below is an overview diagram of a replicated data server.

Figure 5: Replicated Data Server



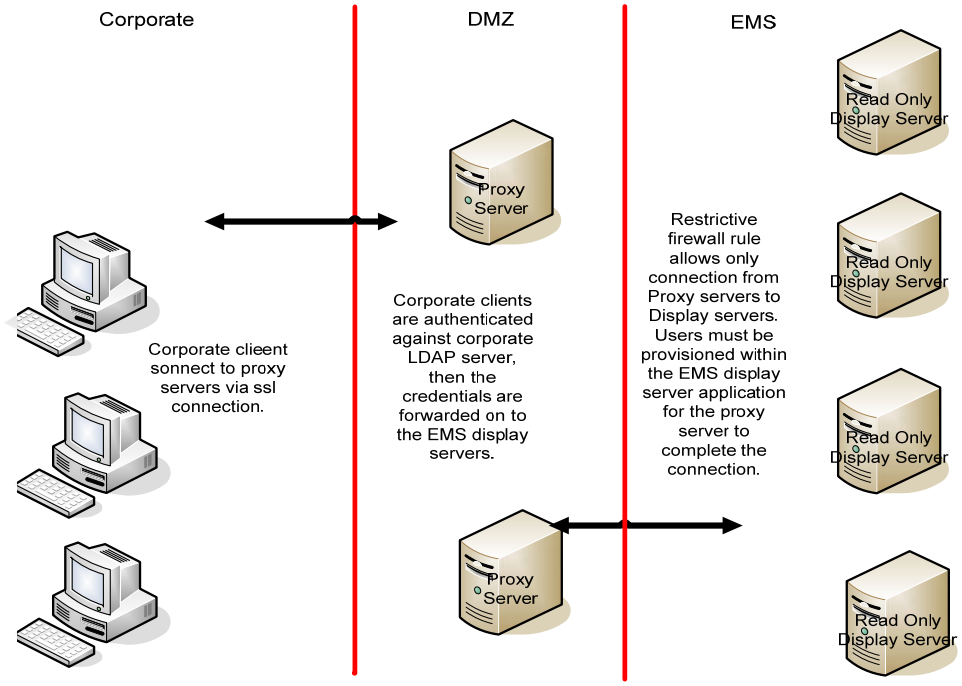
Case Study 3 – EMS Read-only Access via Proxy Servers

In addition to clients accessing displays directly from the EMS servers, clients can access read-only displays from servers called proxy servers. These servers act as intermediaries providing access control and monitoring (ACM) functionality as well as secure encrypted communication between the corporate users and the read only display servers. They reside in the DMZ between the corporate network and the secure EMS network. This configuration offers multiple advantages:

- **Security:** Users can call up displays, but they cannot connect to the EMS computers or issue controls. The displays are read-only.
    - Provides secure encrypted connection from the corporate network into the DMZ.
    - Secures the internal network from malware, allows for traffic monitoring
- **Scalability:** Allows for one proxy server to many display server relationship. Large numbers of clients can access displays while spreading the load on to multiple EMS display only servers.

The proxy servers introduce a stronger user authorization as the users must first authorize against the corporate domain, allowing for corporate access polices to be enforced (password strength, change periodicity, etc.) then have to be defined within the EMS display server restricting which displays they are allowed to view. Below is an overview diagram of a Proxy server.

Figure 6: EMS Access using Proxy Servers



Case Study 4 – Smaller Utility interactive Remote Access

Purpose:

Interactive remote access (access from locations other than company facilities) is required for the following activities:

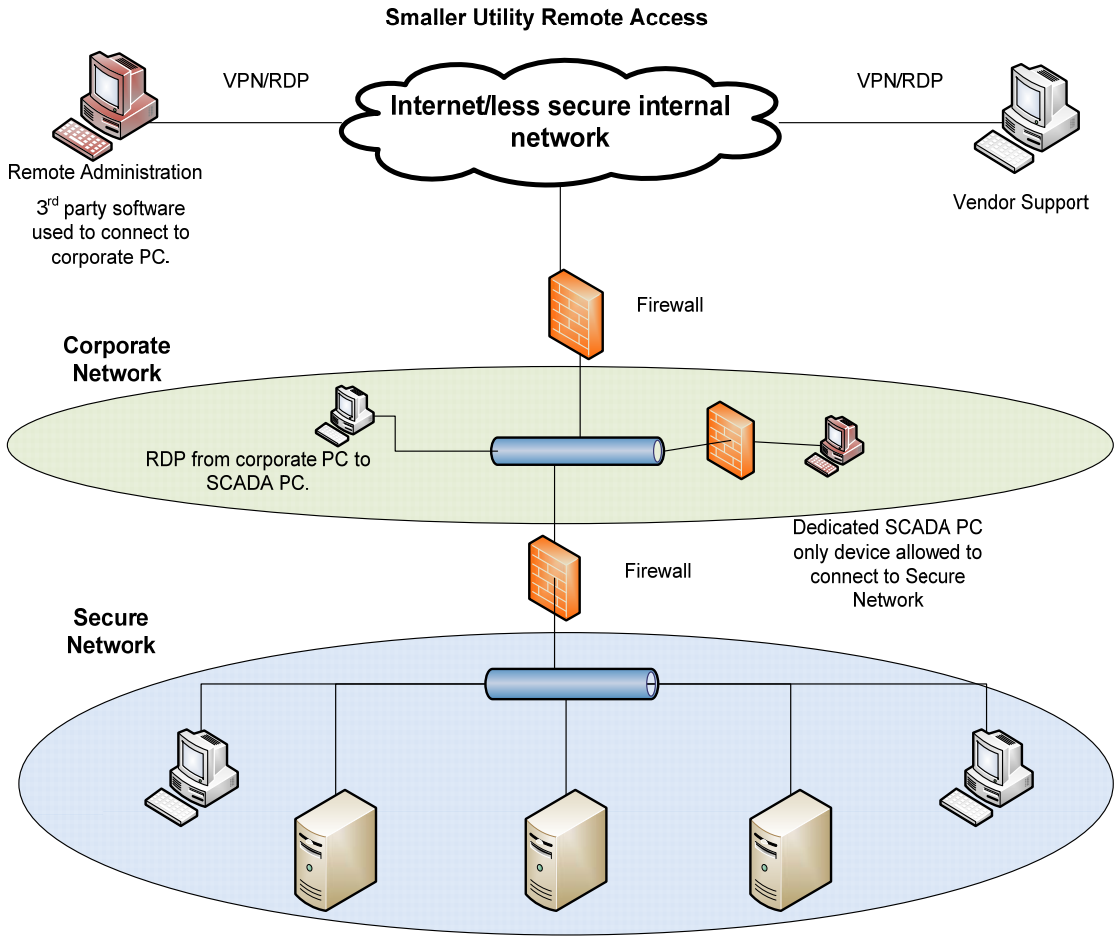
- Off hours and emergency support and troubleshooting by support and maintenance personnel
- Vendor support

Overview:

The following write-up describes the steps and security measures that are used to allow secure interactive remote access into an Electronic Security Perimeter. The following configuration has been found to be a secure and cost-effective solution for allowing interactive remote access.

- SCADA support programmers have 2 sets of workstations at their desk. One for corporate connectivity and one for dedicated SCADA support functions. The SCADA workstations are connected to a separate and secure network with only software installed and ports and services allowed for necessary operation.
- Interactive remote access is accomplished via Microsoft Intelligent Application Gateway (IAG); an SSL VPN solution that allows only "permitted" application access. A secure connection is established to the corporate PC. A Remote Desktop Protocol (RDP) connection is made from the corporate workstation to the secure dedicated SCADA workstation. Only the IP address of the corporate workstation is allowed to make an RDP connection to the SCADA workstation.
- The dedicated SCADA workstation sits behind a firewall and is the only remote connection allowed into the SCADA network inside the Electronic Security Perimeter. This "Jump Host" configuration denies direct access to the SCADA network inside the Electronic Security Perimeter) network from a remote VPN connection.

Figure 7: Small Utility Interactive Remote Access



Case Study 5 – Mid-Sized IOU Example

The overall mitigation approach denies a full VPN to computers which are not owned by XXX. This approach is supported today through the use of the Corporate XWA (XXX Web Access) for access to general computing on the corporate network. The XWA configuration uses a remote desktop protocol (RDP) session using a Microsoft Terminal Services server proxied using a reverse https proxy, which implements strong authentication and URL inspection. The approach further mitigates risks associated with RDP by denying sharing of local client resources.

For corporate laptops, access to the High Value Network(s) (Control-Nets) is only allowed using designated, hardened servers from which access will be authorized (i.e., the "Jump Hosts"). Firewall rules on the edge of the Control-Net only allow the Jump Hosts through using RDP and 2-factor authentication.

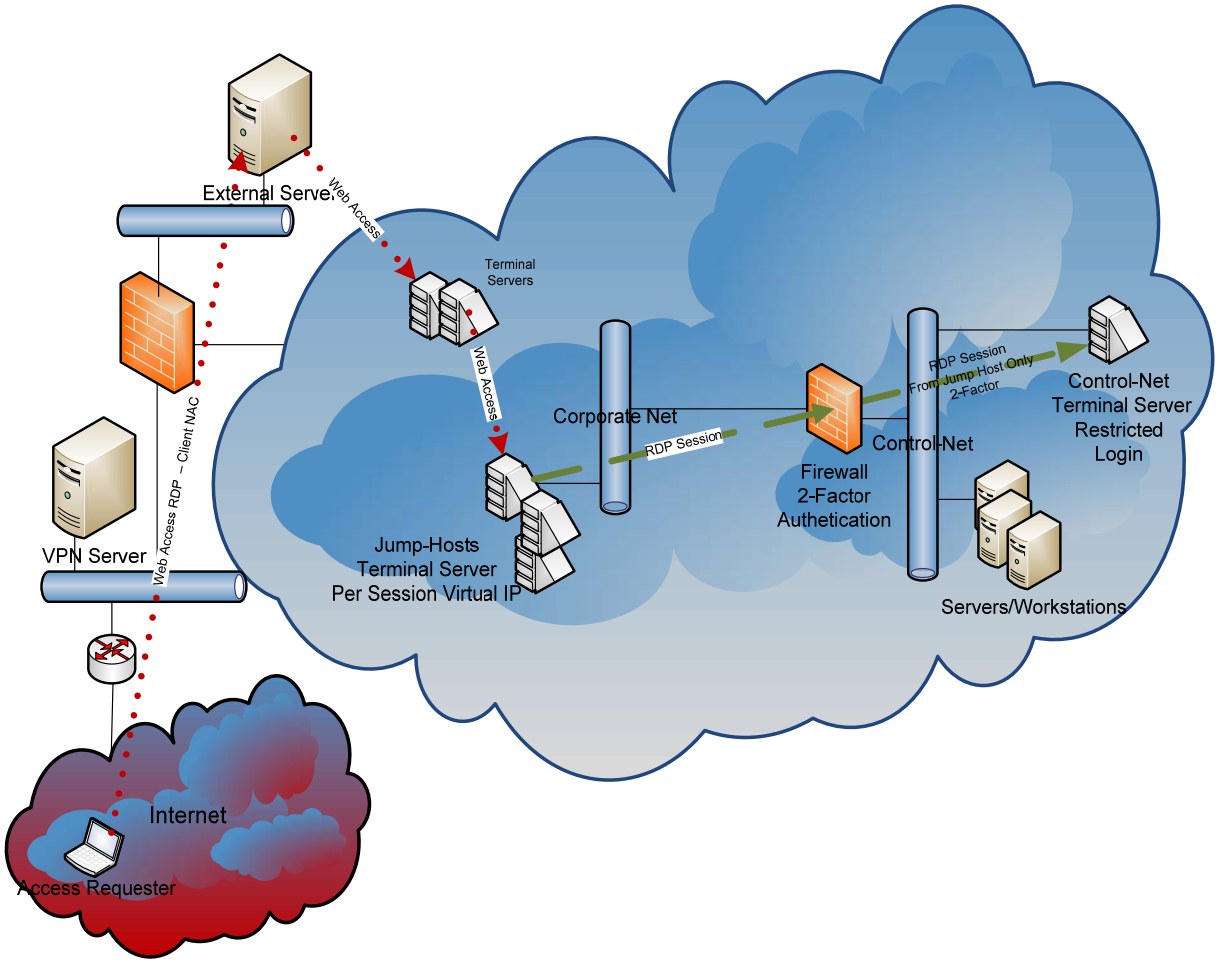
The approach to XWA is replicated for access to Control-Nets and their hosts across one or more firewalls using a dedicated set of Terminal Services servers capable of providing separate Virtual IP addresses for each RDP session. A separate IP address is required for each session because each RDP client will be authenticated using 2-factor authentication by IP address for the session to the target Terminal Services server on the Control-Net.

The following measures provide mitigations from potentially compromised clients:

- To mitigate the risks of full VPNs into target High Value networks and hosts, non-corporate PCs and laptops are only provided with RDP (MS Terminal Services/Remote Desktop Services) access using a set of dedicated Terminal Services servers which act as Jump Hosts (TS-JH) connected to the Corporate network. Corporate PCs and laptops must use the Jump Hosts to access the Terminal Services server(s) on the target Control-Net.
- External access to these Jump Hosts servers will be provided through XWA: external users will open a Terminal Services session with XWA and from there, access the Jump Hosts in the same way internal users access the Jump Hosts.
- The Jump Hosts will implement a session based IP Virtualization, which provides a separate IP address for each session (supported in Remote Desktop Services in Server 2008 R2). Separate IP addresses are required to allow discrete access across the firewall for each session separately using 2-factor authentication. Note that Network Interface Card (NIC) Teaming is not supported in this configuration at this time.
- Jump Hosts will be locked down to allow Terminal Service Client/Remote Desktop and Telnet applications only.
- Users will use the Jump Hosts to establish a separate RDP session to a Terminal Services server in the target Control-Net.
- Two-factor authentication is required for access across the firewall to the target Terminal Services server on the Control-Net. (TS-CN). Provisioning of authorized users will be performed by the Control-Net administrators.

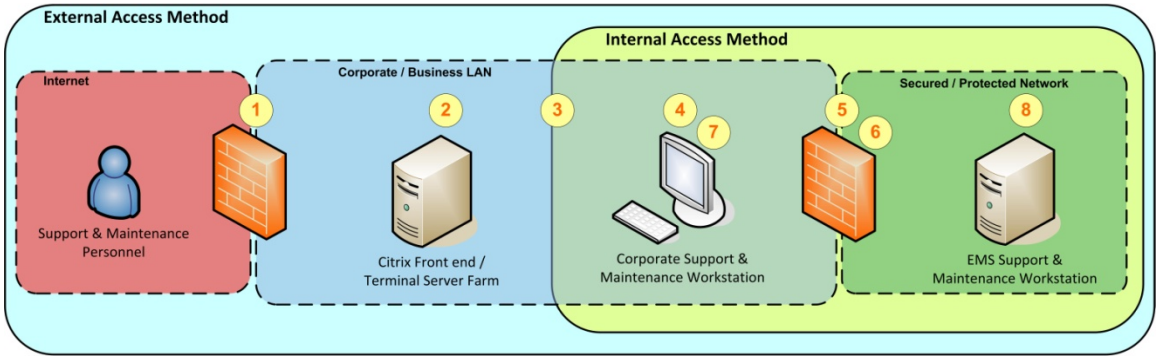
- The Control-Net firewall rule will allow only RDP sessions from the Jump Hosts to the target Terminal Services server(s) only on the Control-Net after 2-factor authentication.
- The TS-CN server(s) on the Control-Net(s) will only allow authorized users (using local host accounts, or Control-Net local Active Directory).
- All Terminal Services server users have non-administrative privileges on the Terminal Services servers.
- All Terminal Services servers have client local resource sharing disabled.
- Two-factor authentication is used to get from the Jump Host into the target Terminal Services server inside the Control-Net.
- All Jump Hosts and TS-CN servers are denied outbound Internet access on the Corporate and Control-Net perimeter firewalls.
- Control-Net interactive remote access is hardened with additional procedural controls, for example:
    - Explicit Control-Net operator configuration action is required to enable RDP access (e.g., through radius provisioning restrictions).
    - Only the Control-Net Operator can initiate a request for remote access.
    - Ad-hoc requests initiated by remote personnel should require explicit GM/Director level authorization.
    - Robust out-of-band procedural authentication is implemented prior to enabling RDP rule.

Figure 8: Mid-sized IOU Interactive Remote Access



Case Study 6 – Interactive Remote Access to Critical Cyber Assets within an Electronic Security Perimeter

Figure 9: Interactive Remote Access to Critical Cyber Assets within an Electronic Security Perimeter



Secure Access Methods into Protected Networks

External Access Method

1. Support and maintenance personnel connect remotely to corporate interactive remote access solution via multi-factor authentication:
    a. Utilize an SSL VPN with limited access (not full network access).
2. Connect to Citrix (Jump Host 1), logging in with Corporate Active Directory (AD) credentials.
3. Launch remote desktop from Citrix to connect to a specific corporate support and maintenance workstation.

...Proceed to Internal Access Method

Internal Access Method

4. Log into the specific corporate support and maintenance workstation (with AD credentials) which has been identified and configured to access secured/protected network (Electronic Security Perimeter) via uniquely defined Access Lists.
5. Authenticate to Electronic Security Perimeter with multi-factor authentication.
6. Launch ssh to connect to EMS support and maintenance workstation within the Electronic Security Perimeter:
    a. Authenticate via certificate based authentication.
    b. Restrict EMS workstation to specific corporate workstation and user.

7. Launch application, such as remote desktop and tunnel through the ssh connection to uniquely identified EMS support and maintenance workstation within the Electronic Security Perimeter.
8. Log into the EMS support and maintenance workstation via multi-factor authentication.

Appendix C: Sample Interactive Remote Access Policy Guidelines

Secure Interactive Remote Communications for Individual Remote Cyber Assets to Cyber Assets residing within a Registered Entity

The following sample interactive remote access policy guideline was extracted from and based on material from NIST SP 800-77, Appendix A.

Registered Entities that establish a secure or trusted communications path (or VPN) to protect communications between individual remote Cyber Assets used by employees or approved vendors, and Cyber Assets residing within the Registered Entity, must include an Interactive Remote Access Policy as part of the policy requirement. Secure or trusted communications path must be created by the deployment of remote gateway Cyber Assets or management Cyber Asset servers, or both, which allow remote users secure access and communications with Cyber Assets within the Registered Entity. Remote Cyber Assets used by employees or vendors must first be configured with appropriate and approved client application software such that the establishment of secure tunnels between the remote Cyber Assets and the gateway Cyber Asset or management Cyber Asset server is controlled and communications are limited to approved uses. Secure access from remote Cyber Assets to gateway Cyber Assets or management Cyber Asset servers is to protect the Cyber Assets within the entity and must be configured to support the following: confidentiality, integrity, authentication and non-repudiation of all transactions with the Cyber Assets within the entity.

This sample policy should only be considered as an “example” for remote Cyber Assets and the organization’s gateway Cyber Assets and management Cyber Asset servers.

Interactive Remote Access Policy

The Registered Entity must have an interactive remote access policy that clearly specifies the type of secure or trusted communications usage allowed employees from both organization-controlled Cyber Assets (and privately-owned remote Cyber Assets, if allowed) to the remote gateway Cyber Assets or management Cyber Asset servers.

Examples of “secure or trusted” communications usage may be found in the table below. Each Registered Entity must assess their operational needs, network configurations and requirements for interactive remote access prior to selecting the particular level of protection and applications appropriate to meet their requirements.

Comparison of Secure Trusted Network Alternatives to IPsec VPNs -- Extracted from NIST SP 800-77

Name	Primary Strengths	Primary Weaknesses	Potential Cases for Use Instead of IPsec
IPsec Network Layer	• Already supported by most operating systems • Can provide strong encryption and integrity protection • Transparent to clients in gateway-to-gateway architecture • Can use a variety of authentication protocols	• Can only protect IP-based communications • Requires client software to be configured (and installed on hosts without a built-in client) for host-to-gateway and host-to-host architectures • Does not protect communications between the clients and the IPsec gateway in gateway-to-gateway architectures	N/A
PPTP Data Link Layer	• Can protect non-IP protocols	• Requires client software to be configured (and installed on hosts without a built-in client) • Has known security weaknesses • Does not offer strong authentication • Only supports one session per tunnel	None
L2TP Data Link Layer	• Can protect non-IP protocols • Can support multiple sessions per tunnel • Can use authentication protocols such as RADIUS • Can use IPsec to provide encryption and key management services	• Requires client software to be configured (and installed on hosts without a built-in client)	Protecting dial-up communications
L2F Data Link Layer	• Can protect non-IP protocols • Transparent to clients • Can use authentication protocols such as RADIUS	• Requires each ISP.s participation • Does not protect communications between the clients and the ISP • Does not offer encryption; must rely on PPP encryption services, which have known weaknesses	None
SSL/TLS Transport Layer	• Already supported by all major Web browsers • Can provide strong encryption	• Can only protect TCP-based communications • Requires application servers and clients to support SSL/TLS • Typically implemented to authenticate the server to the client, but not the client to the	Protecting communications for a small number of HTTP-based applications that do not require strong authentication or provide their own

Name	Primary Strengths	Primary Weaknesses	Potential Cases for Use Instead of IPsec
		server	strong authentication mechanism
SSL/TLS Proxy Server Application Layer	• Already supported by all major Web browsers • Can provide strong encryption • Can provide multiple layers of authentication	• Can only protect TCP-based communications • Requires clients to support SSL/TLS • Does not protect communications between the proxy server and application servers	Protecting communications for a substantial number of HTTP-based applications
PGP/SSH Application Layer	• Can provide finely-grained protection for application communications	• Can only protect some or all of the communications for a single application • Often cannot be incorporated into off-the-shelf software • Often use proprietary encryption or authentication mechanisms that may have serious weaknesses	Protecting communications for individual applications that are designed to use proven encryption and authentication algorithm implementations

The Registered Entity should also require that each employee and vendor who will use the Secure Interactive Remote Access implementation must sign an interactive remote access agreement or a copy of the interactive remote access policy prior to being granted access to the Registered Entity's remote gateway Cyber Assets and management Cyber Asset servers.

(Note: There is considerable discussion about whether this policy and agreement could also be enforced for non-employees who use of the Secure Interactive Remote Access gateway server or management server. Depending on the details of the Registered Entity's interactive remote access policy and agreement, along with the contractual terms and conditions with vendor/contractor agreements, changes will be needed to make the policy/agreement suitable to address non-employees.)

Items that are typically found in an interactive remote access policy include the following:

- Description of appropriate and inappropriate usage of the remote connection (e.g., forbidding personal use, forbidding use by other individuals).
- Pointers to other Registered Entity policies that apply to interactive remote access, such as an acceptable use policy or a remote network access policy.
- Interactive remote access authentication requirements, such as two-factor authentication or strong/complex passwords.
- Required network and remote Cyber Asset configuration profiles; for example, the policy might forbid a remote Cyber Asset from being connected to the Registered Entity's network and any other network at the same time—dual homed, as well as forbidding split tunnels; this should be enforced and monitored

from the remote gateway Cyber Asset or management Cyber Asset server, not the remote Cyber Asset.

- Minimum hardware and software requirements for remote Cyber Assets to including acceptable operating systems and current software/firmware patches
- Required security controls for remote Cyber Assets, such as: up-to-date anti-malware software and signatures, personal firewalls and host integrity checks.
- The remote Cyber Asset should also be configured periodically check for vulnerabilities, malware, or other security problems and to scan any/all files prior to uploading them to the gateway Cyber Asset or management Cyber Asset server.

Registered Entities might also wish have the interactive remote access policy require that each remote Cyber Asset to be automatically checked for vulnerabilities, malware, or other security problems immediately after establishing a secure or trusted connection and prior to connecting to any other Cyber Assets. This should be stated in the interactive remote access policy.

Gateway Cyber Assets and Management Cyber Asset Servers

Items that are typically part of a remote network access policy for gateway Cyber Assets and management Cyber Asset servers include the following:

- Roles and responsibilities related to gateway Cyber Assets and management Cyber Asset server operations.
- Definition for where secure trusted communication tunnels should terminate (e.g., between the border router and firewall, on the firewall) prior to allowing communications with Cyber Assets within the entity.
- Requirement for creating and maintaining of a list of authorized users, disabling access for individual users as soon as it is no longer needed, and auditing the list of authorized users periodically.
- Network-based intrusion detection and prevention systems and anti-malware applications should be placed in the network architecture in such a manner that they may monitor unencrypted network traffic and alarm to network monitoring systems.
- Authentication requirements for administrators of the gateway Cyber Asset or management Cyber Asset servers should be at least two-factor authentication.
- There should be requirements to change all default manufacturer passwords on the gateway Cyber Assets and management Cyber Asset servers to complex passwords as permitted by the Cyber Asset.
- Each Administrator must have a separate user/admin account, change administrator passwords on a periodic basis, and the Administrator accounts must be disabled or deleted consistent with appropriate CIP Standards when it is no longer needed.
- Authentication requirements for secure interactive remote access users should include a periodic requirement user account monitoring and review and authentication requirements to access the gateway Cyber Assets or management Cyber Asset servers.

- Network Security Architecture requirements for a remote gateway Cyber Assets or management Cyber Asset servers might require a firewall to be deployed between the gateway Cyber Asset or management Cyber Asset server, and the Cyber Assets within the Registered Entity. The firewall should be configured to block all traffic not explicitly approved for use with the protected Cyber Assets. The Registered Entity should also specify what security controls should be on the gateway Cyber Assets and management Cyber Asset servers, such as host-based firewalls, anti-malware software and remote monitoring clients.
- What information should be kept in audit logs, how long logs should be maintained, and how the log information should be reviewed.
- Requirements for remediating new vulnerabilities affecting the gateway Cyber Assets and management Cyber Asset servers.
- Which types of traffic should be protected by the secure tunnels, and what types of protection should be applied to each type of traffic.
- What types of protection should be applied to communications between an IPsec gateway and an IPsec management server.
- Automatic termination and disconnection of idle connections after X minutes.

Cyber Assets and People Using the Secure Protected Tunnel

The Policy should state whether the Cyber Asset and people using the secure protected tunnel are required to use remote Cyber Asset equipment and network components owned by the Registered Entity, or if they are allowed to use personally owned Cyber Asset to communicate with Cyber Assets within the Registered Entity.

The user must agree to support configuration policies related to remote Cyber Asset configuration and use when connected to the organization over the secure tunnel. Examples policies include:

- Cyber Asset access requirements and authentication,
- risk mitigation requirements such as OS and application software patching of known vulnerabilities,
- technical controls such as anti-malware, personal firewalls, and platform scanning by the Registered Entity's remote gateway Cyber Assets and management Cyber Asset servers,
- Minimum acceptable configuration of and compliance with all technical controls.

If connectivity is allowed using personally owned Cyber Assets, then the users must agree to acceptable use of their Cyber Assets consistent with above when connected to the Registered Entity's networks. There should be no expectation of personal privacy if using personally owned Cyber Assets to access the organization's remote gateway Cyber Asset servers and management Cyber Asset servers for communications with Cyber Assets within a Registered Entity.

Appendix D: References and Bibliography

The following list is a brief compilation of documents and Internet references that the reader may find useful. Inclusion in this list does not imply any endorsement of NERC or the authors. Exclusion from this list does not imply anything by NERC or the authors.

NIST Computer Security Division Computer Security Resource Center:
http://csrc.nist.gov/

NIST Special Publications:
http://csrc.nist.gov/publications/PubsSPs.html

NIST Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

NIST Guide to IPSEC VPNs
http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

National Security Agency Central Security Service Security Configuration Guidelines:
http://www.nsa.gov/ia/guidance/security_configuration_guides/

US CERT Control Systems Security Program:
http://www.us-cert.gov/control_systems/

National SCADA Test Bed publications:
http://www.inl.gov/scada/publications/index.shtml

Sandia National Laboratory Center for SCADA Security:
http://www.sandia.gov/ccss/

Federal Financial Institutions Examination Council
Authentication in an Internet Banking Environment
http://www.ffiec.gov/pdf/authentication_guidance.pdf

NIST Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Defense Security Administration Agency (DISA) Secure Remote Computing (SRC) Security Technical Overview
http://iase.disa.mil/stigs/downloads/zip/unclassified_secure_remote_computing_v2r3_stig_20100827.zip

DISA Security Technical Implementation Guides (STIGs)
http://iase.disa.mil/stigs/stig/

Encryption Resources

Department of Homeland Security: Control Systems Communications Encryption Primer
http://www.us-cert.gov/control_systems/pdf/Encryption%20Primer%20121109.pdf

NIST Federal Information Processing Standard (FIPS) 140: Security Requirements for Cryptographic Modules – the most current version of FIPS 140-X may be found at:
http://csrc.nist.gov/publications/PubsFIPS.html

NIST Special Publication 800-21: Guideline for Implementing Cryptography In the Federal Government
http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

NIST Special Publication 800-53, Rev 3: Recommended Security Controls for Federal Information Systems and Organizations
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

NIST Special Publication 800-77: Guide to IPsec VPNs
http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

NIST Special Publication 800-113: Guide to SSL VPNs
http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

NIST Special Publication 800-114: User's Guide to Securing External Devices for Telework and Remote Access
http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf

NIST Special Publication 800-131 A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

Appendix E: Terms

Interactive remote access: Refers to user interactive access by a person to support or maintain a system. Interactive remote access originates from a Cyber Asset that is not an intermediate server and is not located within any of the Registered Entity's control system network, whether network-based or dial-up access. Interactive remote access can be initiated from: 1) Cyber Assets used or owned by the Registered Entity; 2) Cyber Assets used or owned by employees; and 3) Cyber Assets used or owned by vendors, contractors, or consultants.

Intermediate server: A Cyber Asset that: 1) is used to provide the required multi-factor authentication for the interactive remote access; 2) is a termination point for the required encrypted communication; and 3) restricts the interactive remote access to only authorized users. Intermediate servers are sometimes called proxy systems or "jump hosts." The functions of an intermediate server may be implemented on one or more Cyber Assets. The intermediate server may be located outside of a protected network (e.g., the control system network) in a perimeter network, sometimes called a Demilitarized Zone (DMZ) network.

Support or maintenance: Includes non-operational activities associated with the upkeep, testing, and modification of Cyber Assets or control system networks. Examples of support or maintenance activities include (but are not limited to): configuration changes, power system model maintenance, extraction of disturbance data, vulnerability assessments, incident response, troubleshooting, computer system monitoring, and application of software patches.

Revision History:

Date	Version Number	Reason/Comments
9/17/2010	1.0	Initial posting
10/25/2010	2.0	Updates after initial posting
5/23/2011	0.9	Convert to standalone guidance document
6/2/2011	0.91	Release for initial external review
7/15/11	1.0	Release as alert reference document