NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Secure Remote Access
Draft

to ensure the reliability of the bulk power system

September, 2010

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

Table of Contents

Figures:

Disclaimer

This supporting document may explain or facilitate implementation of reliability standard CIP-005-4 Requirement R6, but this supporting document does not contain mandatory requirements subject to compliance review.

Executive summary

Secure remote access to Critical Cyber Assets (CCAs) has become a "hot topic" lately. Recent release of Compliance Application Notices (CANs) from NERC, as well as joint intelligence products from the Department of Defense (DOD), Department of Energy, Department of Homeland Security and NERC have indicated that there are potential security problems when secure remote access is not properly authorized, designed, or configured.

This guidance document addresses securing remote access that is used for support and maintenance purposes. A properly secured remote access implementation can be used to provide non-operational access to CCAs to troubleshoot and repair operating systems, hardware and application software issues, as well as to provide a mechanism to troubleshoot and repair data and modeling problems which cause application errors. Secure remote access can also provide a mechanism for read-only monitoring of power system operations and status, allowing view-only access of the power system status beyond the boundaries of normally authorized users and access requiring escort.

Training, policy, and processes are necessary to ensure that security is not compromised inadvertently through the introduction of unsecured computers or unsecured access. Proper software configuration of the computers used to access the CCAs, along with securely designed and implemented network architectures are crucial to the continued security of the CCAs themselves. Also essential are secure methods of authentication (proving a user is who they say they are) once they have identified themselves to the system.

An overview of secure remote access architectures is presented to introduce a set of remote access case studies. Six case studies, submitted by different Electric Sector entities, are presented and discussed. 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 implementation, and a network architecture diagram to aid readers in designing their own secure remote access architecture.

Finally, the guideline concludes with a brief list of recommended references which the technical reader may use to further explore the topic of secure remote access and secure authentication.

Background

Scope

This Guideline is intended to assist a Responsible Entity in applying secure approaches for remote access to previously identified Critical Cyber Assets (CCAs) within a defined Electronic Security Perimeter (ESP), in compliance with requirement CIP-005-4, Requirement R6. The guideline is intended to apply to the use of network-level remote access to CCAs across an ESP (i.e., access that uses a "routable protocol" rather than a "dial-up connection").

Remote access for the purpose of Bulk Electric System (BES) operations is beyond the scope of this guideline.

Audience

This Guideline is directed toward those responsible for developing the appropriate technical solutions regarding remote access to CCAs for their entity. It may also be useful to appropriate management personnel involved in identifying different solution options and determining corporate direction based on criteria such as risk, financial, security, etc.

Strategy

NERC Standard CIP-005-4, Requirement R6 requires that Responsible Entities implement protections around devices, procedures, and processes used to remotely access CCAs for the purpose of support and maintenance.

The term Critical Cyber Assets is defined in the NERC Glossary as "Cyber Assets essential to the reliable operation of Critical Assets." This Guideline provides guidance and practical examples for implementing secure methods of remote access to CCAs for maintenance and support for both internal responsible entity personnel as well as vendor support.

CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)

A restricted distribution (For Official Use Only) NERC CIP Awareness Bulletin was issued on March 31, 2010 on the subject of "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)". The Awareness Bulletin addressed all aspects of remote access and the use of VPNs in the electricity sector. Within the Awareness Bulletin there are several supporting arguments for the type of remote access addressed in this guideline. While the Awareness Bulletin was in reference to generic VPN-based remote access without specific reference to its application, the

principles in the bulletin apply to the remote access methods covered in this guideline. Even though this guideline focuses on remote access for the purpose of support and maintenance, the following excerpt from the Awareness Bulletin applies:

During exigent circumstances, remote VPN access provides essential value to support business continuity as follows:

a. *Remote VPN access permits many personnel to work from home during pandemic outbreaks, significantly reducing the number of critical personnel that would need to come to the workplace and possibly an area of greater exposure threats. Additionally, during pandemics VPN capabilities would allow the bulk power system to operate when travel restrictions could be imposed in communities, counties, and states.*
b. *Remote VPN access provides bulk power system operators the ability to virtually configure their organizational support processes following the loss of a control center (fire, flood damage, or attack).*
c. *Remote VPN access permits bulk power organizations to keep personnel off of roads during periods of dangerous weather conditions, yet they can continue to support bulk power system reliability from their homes. This reduction of travel risks during such conditions permits the Electric Sector to protect some of their most critical assets, their people.*
d. *Remote VPN access allows bulk power organizations to limit the number of personnel at their facilities during periods of heightened physical security threats. During heightened security postures, bulk power organizations should significantly limit the number of personnel entering their facilities so that these people can undergo far greater scrutiny screening and fewer staff would be possibly at risk to a physical attack on the facility. Without VPN – organizations would lose this ability to better tailor their physical security postures in response to increased threat exposures.*

Compliance Application Notice (CAN)-0005:

CAN-0005 also addresses the topic of remote access to CCAs. Where the specific focus of that notice was targeted at remote access for purposes of operation of the BES, this guideline is focused on remote access for the purpose of maintenance and support for both internal responsible entity personnel as well as vendor support. This guideline, therefore, compliments, rather than conflicts with, CAN-0005.

Use Cases

This guidance document seeks to provide real-life examples or "Use Cases" of methods of providing remote access for support and maintenance that provide protective defense-in-depth measures to ensure adequate cyber security to minimize risk to the BES. This includes examples of connectivity for functions such as:

Support & Maintenance Functionality

- Hardware, Operating System & Application Programming Support – Connectivity to CCA systems for maintenance & support staff as well as vendor access to provide troubleshooting and problem resolution of issues such as problems with underlying operating system software and other third party layered application software critical to proper operation of the CCA.

- Maintenance of Power System Applications, Data, and Modeling – Connectivity to CCA systems for maintenance & support staff as well as vendor access to provide troubleshooting and problem resolution of issues such as debugging power system applications, databases, and data models for successful operation of the CCA. This could include applications such as SCADA, automatic generation control, state estimator and/or contingency analysis.

Read-only Monitoring

- This a common configuration that utilizes a one-way-direction connection through the ESP boundary to replicate data from a CCA within the ESP to a read-only system outside the ESP that, by its configuration, prevents any access to, or control of, the BES 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. This configuration is commonly used to grant those not involved in the real-time operation of the BES the ability to view data in a near real-time mode thereby increasing the situational awareness of the state of the BES beyond the boundaries of the normally authorized set of users with unescorted access to the CCAs.

Remote Access Concepts

This section addresses integrating people, processes, and technology – the three key elements to successfully protecting critical assets.

People:

People are the heart of it all. Organizations must ensure Senior Management buy-in and commitment is in place; without this you will fail. Having the right people in place to execute the processes will deliver the expected value and results. Organizations must invest in continuous training to ensure 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 technology that best meets their needs. It is important that organizations build continuous auditing and monitoring into their processes. Continuous auditing and monitoring can deliver regular insight into the status of controls, enhancing risk and control oversight capability through monitoring and detection. It can also enable organizations to amortize the resource expenditures over the life time of the solution. Once the process has been established it is critical to invest in continuous training to ensure employees know what is expected of them. Training should include the testing of the employees' understanding of the processes.

Technology: Protecting Computers Used for Remote Access

Most organizations have standards and policies to protect their computers against malware and other compromises. The NERC CIP standards require that covered assets be protected by firewalls and anti-malware software, and that security patches be kept up to date. These are sound practices that should be followed by any computer owner. However, what happens when access from outside networks is enabled using Virtual Private Network (VPN) technology? A VPN can be thought of as a tunnel, in which information (data from one network or computer) is encrypted and sent to another network, perhaps using the public Internet. The information is decrypted when it gets to the destination network, and information from the destination network is likewise encrypted before it is sent back to the originating network or computer. The encryption protects the information as it travels across the network. However, VPNs by themselves do not limit the protocols that can be sent or detect malicious code or behavior. If the remote computer or a machine on the remote network is infected or compromised, then an attack can be mounted from it to devices accessible across the VPN.

Ideally, any computer allowed remote access via a VPN should have anti-malware software installed with current signatures, have up-to date security patches, and have a client firewall installed.

What steps can be taken to ensure remote computers using a VPN do not threaten the organization's network or the ESPs themselves?

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

- Educate remote users on the importance of anti-malware, of keeping patches current, and maintaining a personal firewall in both protecting their own computers and the information on them, and protecting the company's assets as well. Implement a policy requiring, or include in the corporate computer use policy, a requirement that anti-malware, current patches, and a client firewall be installed on machines used for remote access.

- Include language in maintenance contracts obligating vendors to maintain anti-malware and current patches on, and protect with firewalls, computers they use for remote control.

- Configure the VPN system to check for the presence of anti-malware software on connecting machines, and only allow connections from machines with approved versions. This is sometimes referred to as "user access control," and solutions are available from several different vendors.

- Configure the VPN such that split tunneling[1] is not allowed by technical policy.

- Force VPN traffic through a firewall and/or an intrusion prevention system after it is unencrypted, so that malicious content or behavior can be detected and dealt with.

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

Another approach is to provide remote access users with a bootable CD that includes the VPN client and the tools necessary to access internal resources remotely (e.g., secure shell – ssh, Remote Desktop protocol – RDP 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 (e.g., all unnecessary services removed) operating system from read-only media. The operating system is configured with no disk drivers, so it

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

impossible to read or write data to the local hard disk with it. The Air Force research Laboratory developed such a solution for the DOD.[2] Detailed instructions for implementing a boot CD solution with Linux have been published[3]. It is also possible to implement a boot CD solution using Microsoft Windows, if Windows is required for remote access.

Multi-Factor Authentication

Definition

A multi-factor authentication system is a system that uses authentication factors from at least two of three generally accepted categories[4]: something known (e.g., a password or PIN), something possessed (e.g., a one-time password token or a smart-card) and something unique about you (e.g., fingerprint or iris pattern). Any system that uses two or more factors may be referred to as multi-factor authentication; systems that use only two factors are often referred to as two-factor authentication. Note that a User ID is *not* considered one of the factors in a multi-factor authentication system.

Examples

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

Something Known

- Password
- PIN
- Passphrase

Something Possessed

- One-time password tokens
- Soft tokens
- Magnetic cards
- Smart cards
- USB tokens
- Hybrid USB/One-time password tokens
- Grid card or Scratch card (description below)
- Dynamic grid card (description below)
- Out-of-band One-time password (description below)
- Challenge-response systems (description below)

[2] See https://spi.dod.mil/COOP/DoD_reg_SSL.htm
[3] Waddell, Jeffery Douglas, "Secure Boot CDs for VPN HOWTO", June 15, 2007, http://www.linux.com/learn/docs/ldp/732-Secure-BootCD-VPN-HOWTO.
[4] Additional categories, such as location are occasionally used, but not very often

Something Unique About You

- Fingerprint
- Facial features
- Iris (has replaced retina)

Grid cards or scratch cards are inexpensive alternatives to one-time password tokens. The user is provided with a credit-card format 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 is provided with a random row and column number and asked to provide the code associated with the designated cell in the grid. A variation is to have a single number in each cell in the grid. The user is provided the starting cell on the grid. The user then follows a predetermined, user chosen path through the grid to determine the rest of the code (i.e., one cell to the right, one up, two to the right, one down, etc.) This provides another layer of security because only the user knows the correct path through the grid.

Dynamic grid cards are a variation where the grid or other pattern of numbers and characters is displayed on the screen when logging in. There is a scheme by which the users select numbers or characters based on something they know (such as the path method described previously). The advantage is the grid changes each time the user logs in, and there is no card to misplace.

Out-of-band one-time passwords are passwords that are delivered real-time via SMS (text messaging). They are secure because a separate communication channel is used to deliver the password to the user.

Challenge-response systems are 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). Some dynamic grid cards are one example of a challenge-response system. However, a more common example sends a cryptographically generated number associated with a specific user, which is entered into a calculator token to generate a corresponding number which 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

Passwords can be guessed, stolen, hijacked, found and are often 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, which is really a simple password designed to be used on devices with only numeric input) 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.

Drawbacks

Hardware tokens are popular but are expensive, especially with the costs of the logistical problems they present. They must be associated with a user by an administrator and then delivered to a user. A policy and procedure must be set up to handle lost tokens. All of these are labor intensive.

Software tokens are less secure than hardware tokens – the software can be cloned and the device clock moved forward to predict future passwords or to analyze the password generation algorithm.

Grid cards and out-of-band delivered one-time passwords are less expensive alternatives to tokens.

Costs

The cost of deploying two-factor authentication can be substantial, but it does not need to be. There are two-factor authentication solutions available that are simple to deploy (the server can be a software appliance or a hypervisor[5] system appliance) with pricing starting at $240 for ten users per year.[6]

[5] See http://en.wikipedia.org/wiki/Hypervisor
[6] See http://www.wikidsystems.com/

Case Studies

Secure Remote Access Architecture Overview

Today, the two most prominent options for secure remote access are the traditional IPSec VPN and the SSL VPN. The IPSec VPN requires client base 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 where you might connect 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 you 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 utility's site. Due to the fact that 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 and/or archived.

If the VPN appliance offers application services such as ssh or VNC (Virtual Network Computing) clients, the appliance itself may serve the function of an intermediate device or system, pursuant to CIP-005-4, Requirement R6.4 (these devices are sometimes called "jump hosts"). The appliance acts as a proxy, and the packets allowed into the secure network from the DMZ originate at the appliance, not at the remote computer. If the appliance does not have this feature, or if more flexible methods of access are required, a separate jump host can be added to the solution to provide an intermediate system.

Since there are several vendors that offer secure remote access solutions, this can be a cost-effective solution for utilities of differing sizes and resources.

Below is a diagram of a basic implementation:

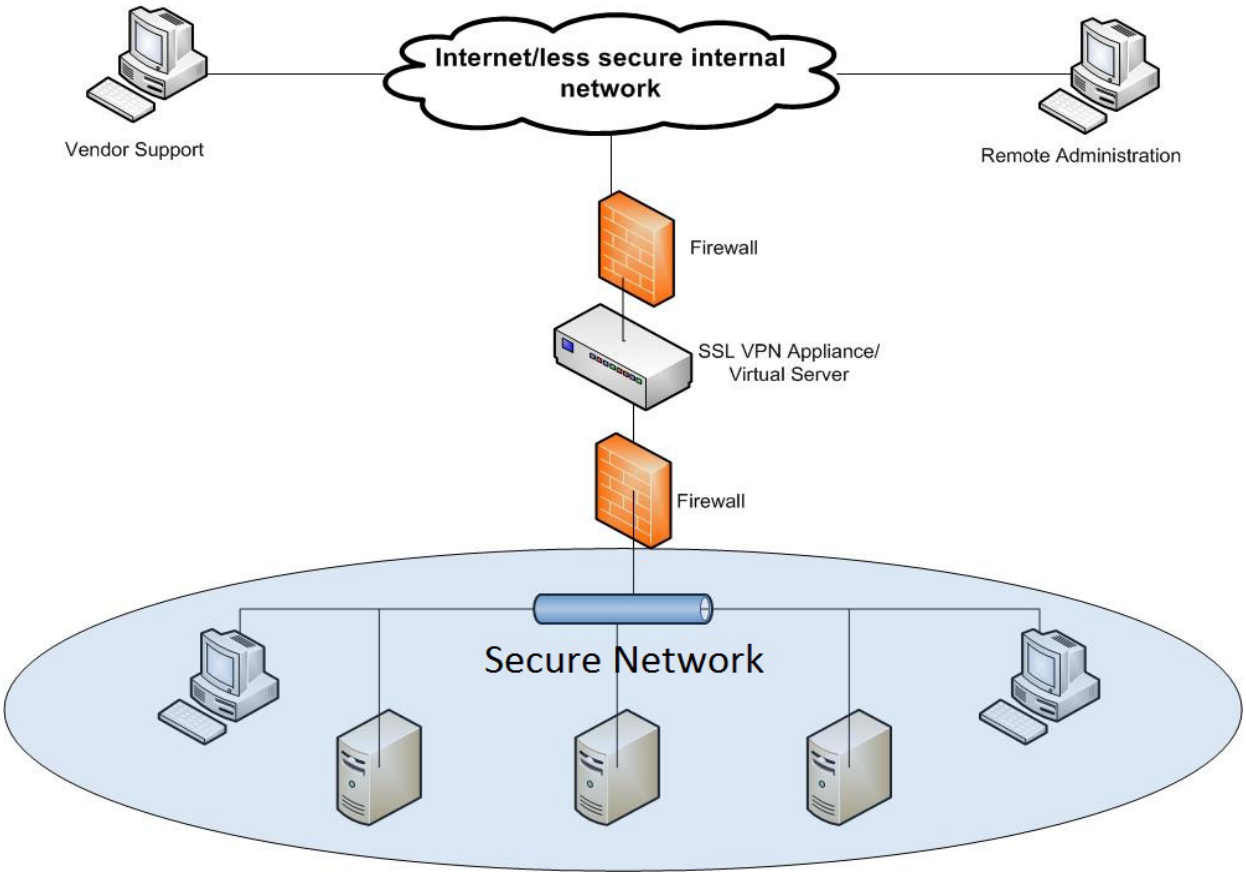

Figure 1: Generic Remote Access Drawing

Case Studies – Introduction

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

A range of implementations is presented, from large entities to small entities, providing a range of expected purchase and support costs.

While the implementations may differ somewhat from the specific wording of CIP-005-4 Requirement R6 (i.e., two-factor vs. multi-factor, and including specific product or architectures), they provide a reference or acceptable methods that can be employed to implement secure remote access.

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

Purpose:
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 ESP 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 (ESP) 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 devices or systems inside the ESP to traverse from the ESP 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 devices and systems within the ESP directly.[7]

Two-factor authentication is required to log into the jump host, as required by CIP-005-4, Requirement R6.2.1. The two-factor authentication is provided by a system installed specifically for and dedicated to authentication to and within the ESP. 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 ESP, further protecting the Critical Assets by allowing only required protocols to specific device addresses from the jump host through the ESP DMZ firewall.

A diagrammatic overview of the process is provided in Figure **2**, below. Details of the procedures for employee and vendor support access are provided in the Procedure Details section, and in the flow chart diagrams (Figure **3** and Figure **4**).

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

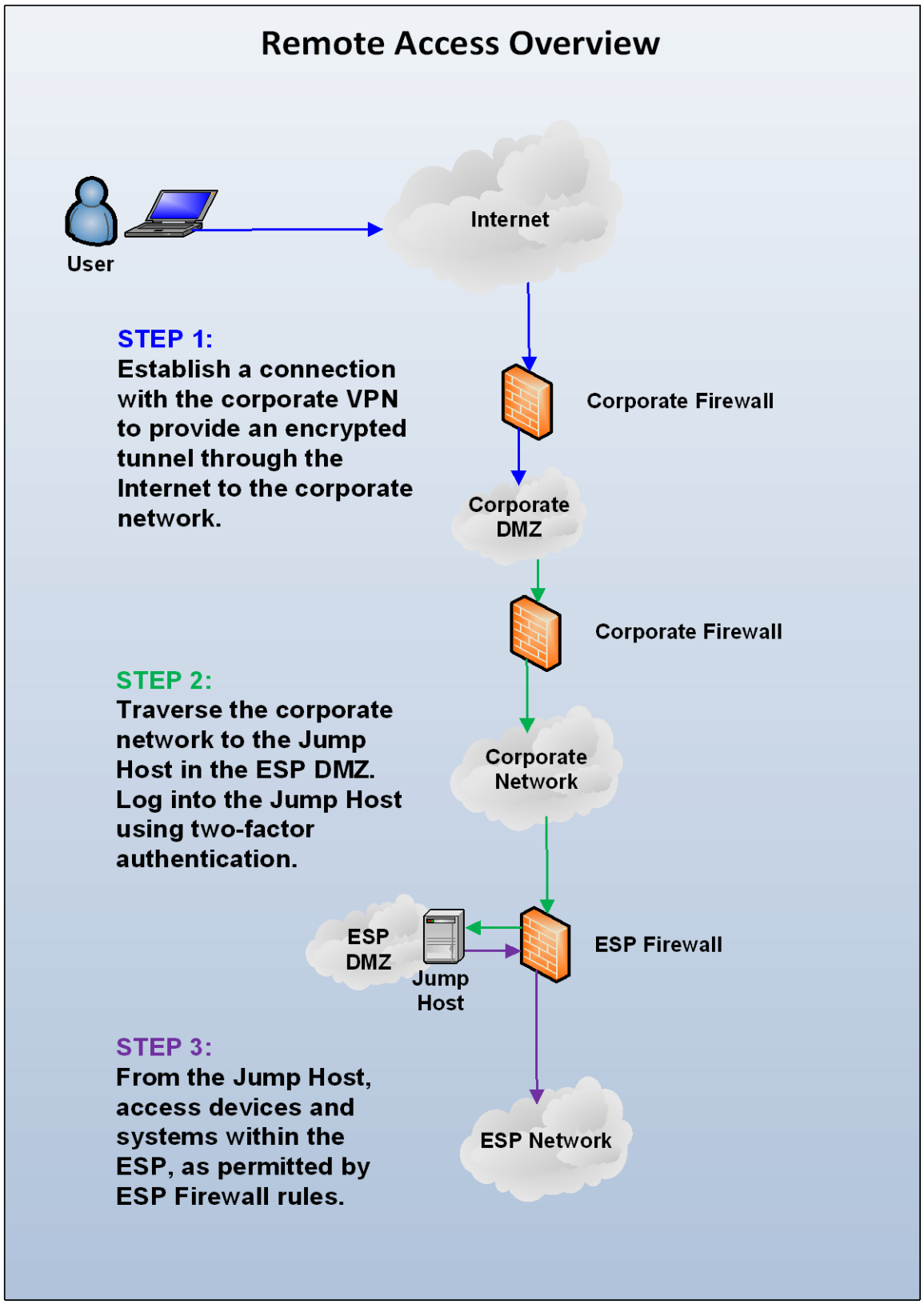

Figure 2: Remote Access Overview

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 device or system within the ESP 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 ESP network.
    a. The DMZ is an ESP 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[8], but the infrastructure for the two-factor authentication to the ESP is completely separate from the corporate infrastructure and maintained inside the ESP.
    d. Multiple unsuccessful login attempts will lock out the account.
    e. The jump host is part of an ESP directory service domain, separate from the corporate domain. All components of this directory service are maintained inside the company's ESPs. The user must log into the ESP domain after successful two-factor authentication.
    f. Successful and unsuccessful login attempts are logged to the ESP SIEM.

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

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

h. The user accounts in the ESP 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 devices within the ESP using the preferred access method for the device or system. The necessary clients or remote access software are installed on the jump host.

4. Access from the jump host to ESP devices is controlled by a firewall. Access is only allowed from the jump host, and only to devices 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 ESP 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.

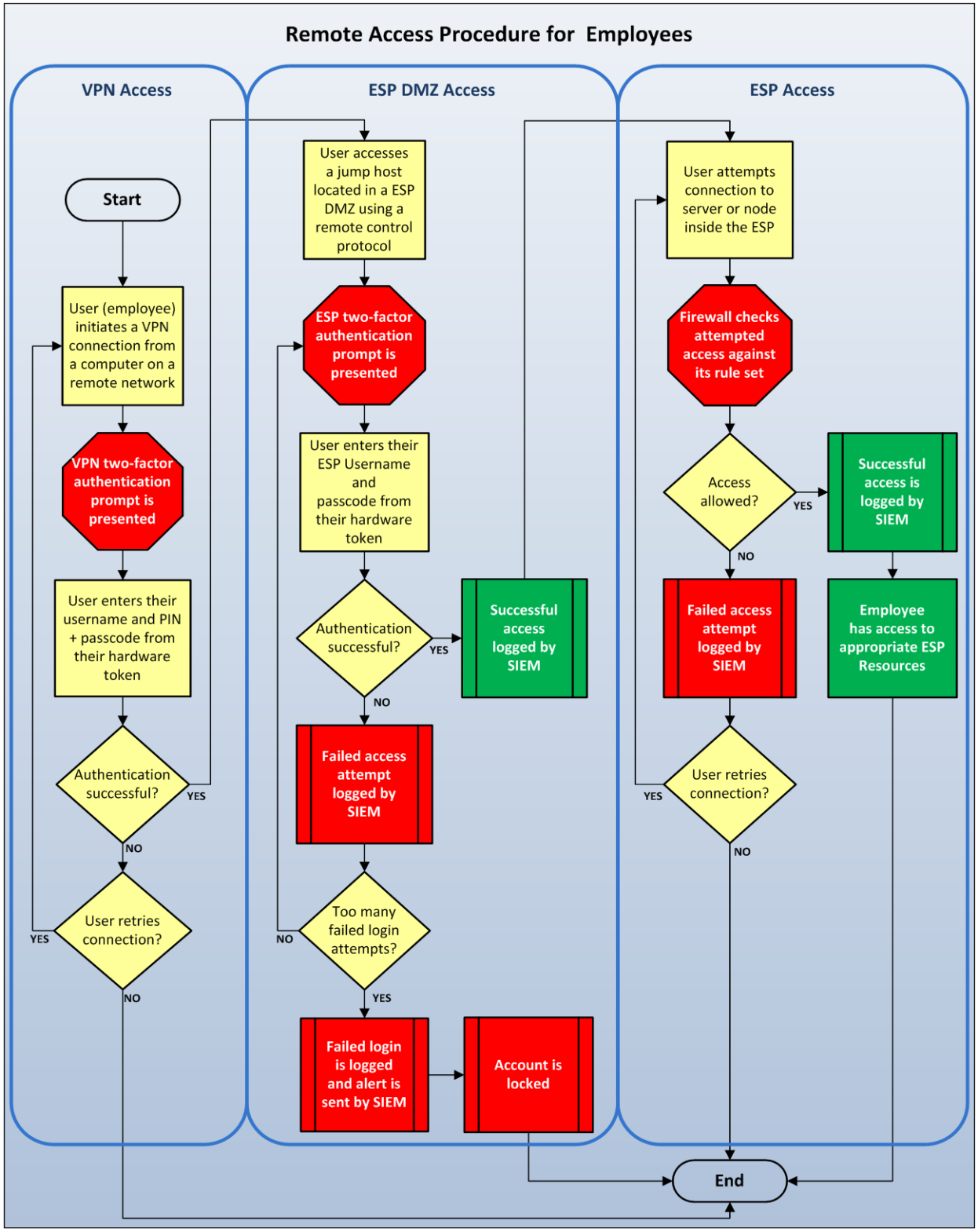

Figure 3: Remote Access Procedure for Employees

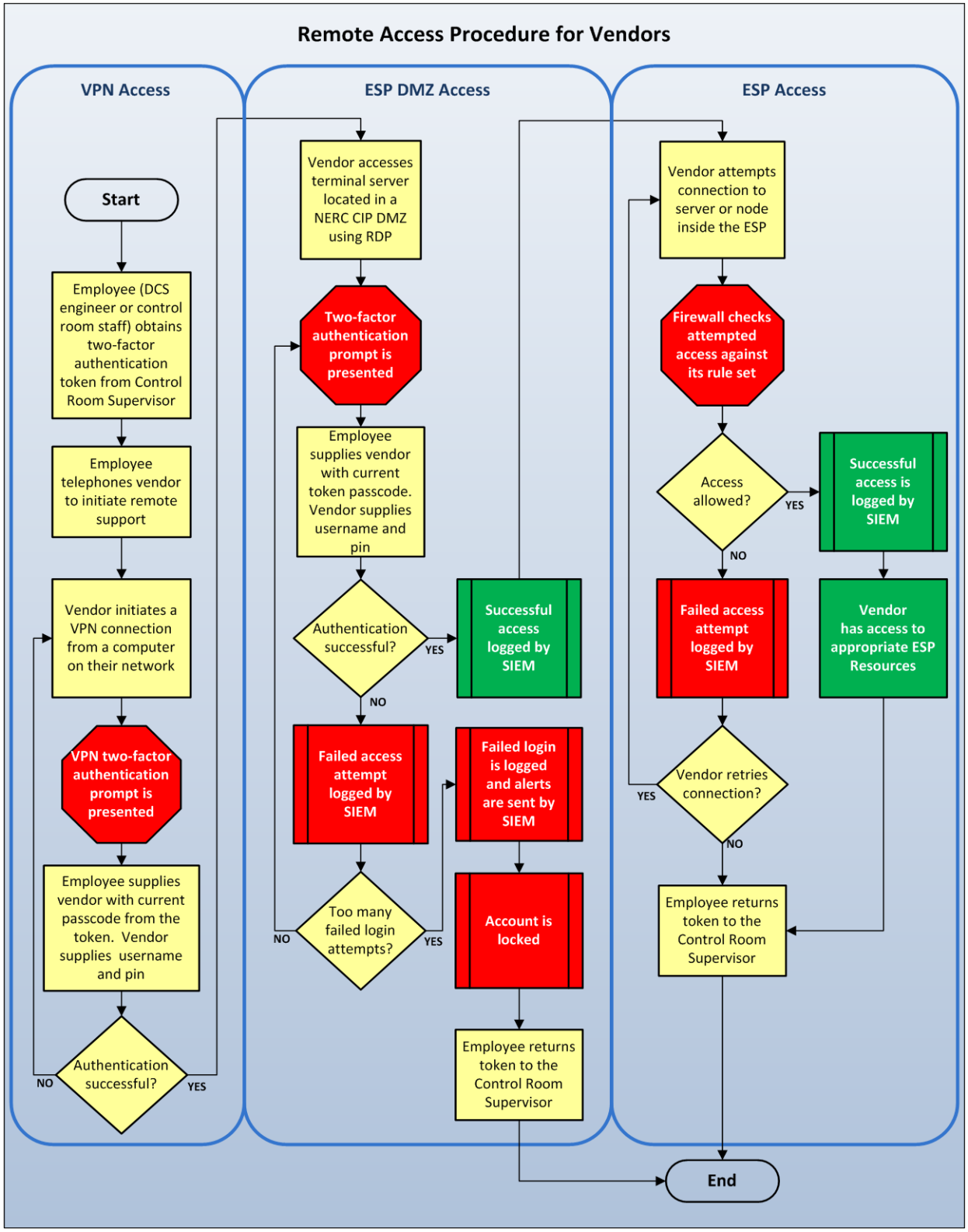

Figure 4: Remote Access Procedures for Vendors

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.

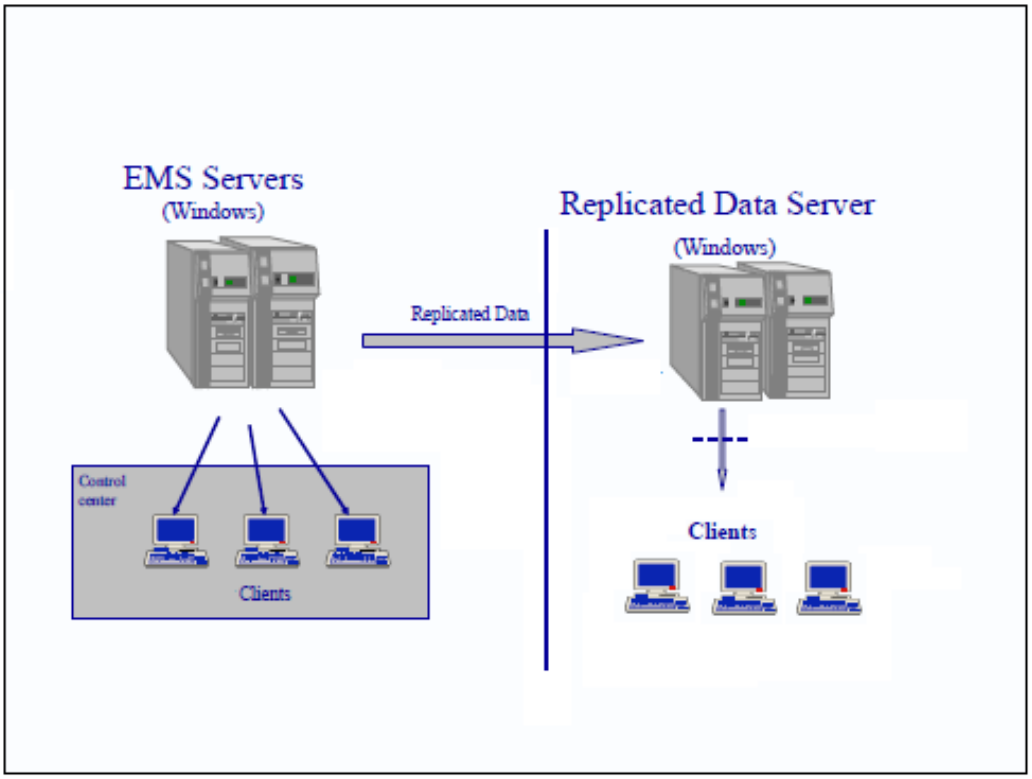

Figure 5: Replicated Data Server

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.

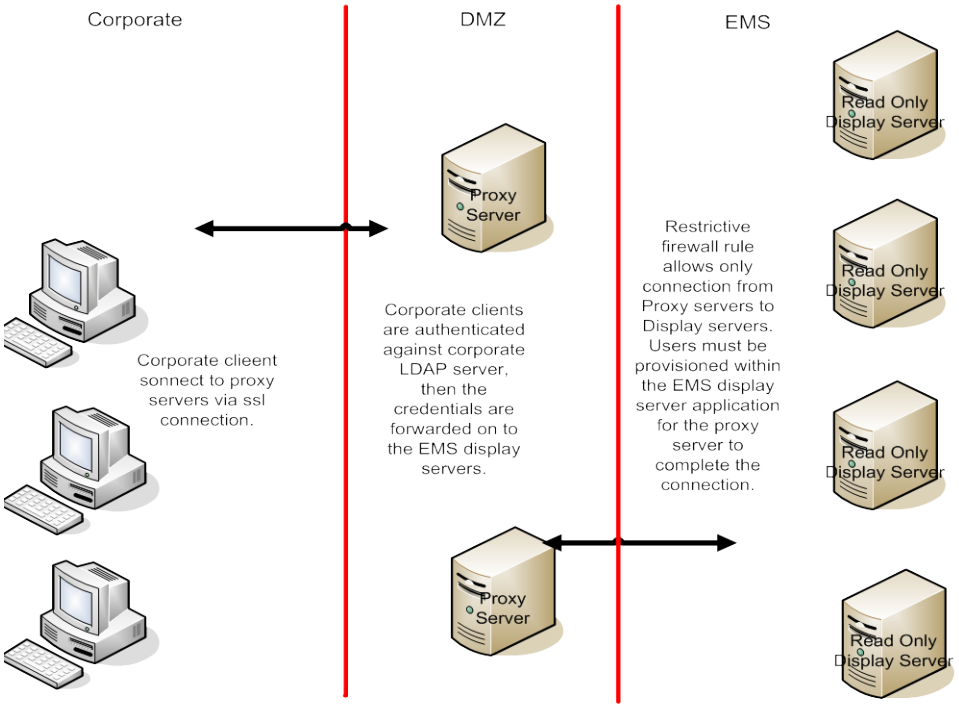

Figure 6: EMS Access using Proxy Servers

Case Study 4 – Smaller Utility Remote Access

Purpose:

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 remote access into an ESP. The following configuration has been found to be a secure and cost-effective solution for allowing 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.
- 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 (ESP). This "Jump Host" configuration denies direct access to the SCADA (ESP) network from a remote VPN connection.

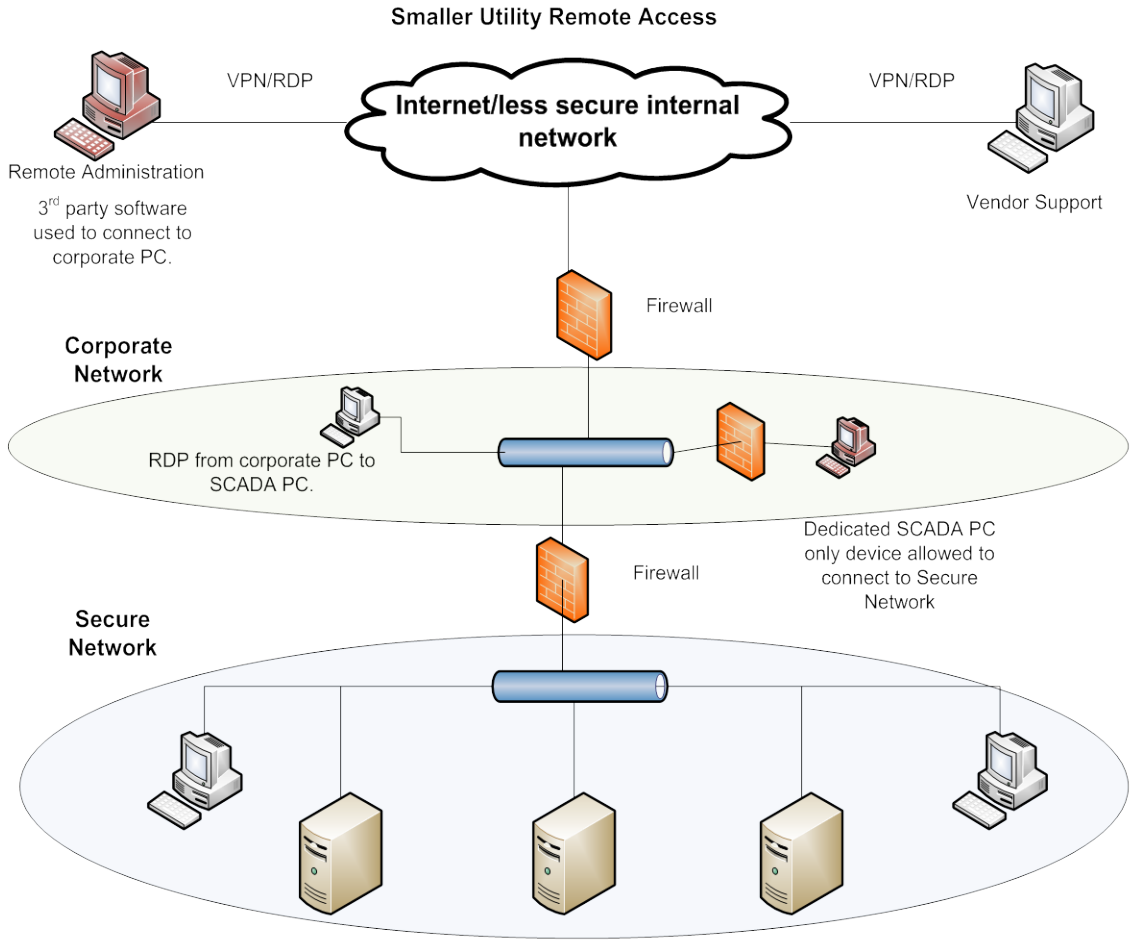

Figure 7: Small Utility Remote Access

Case Study 5 – Mid-Sized IOU Example

The overall mitigation approach denies a full VPN to devices 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 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.

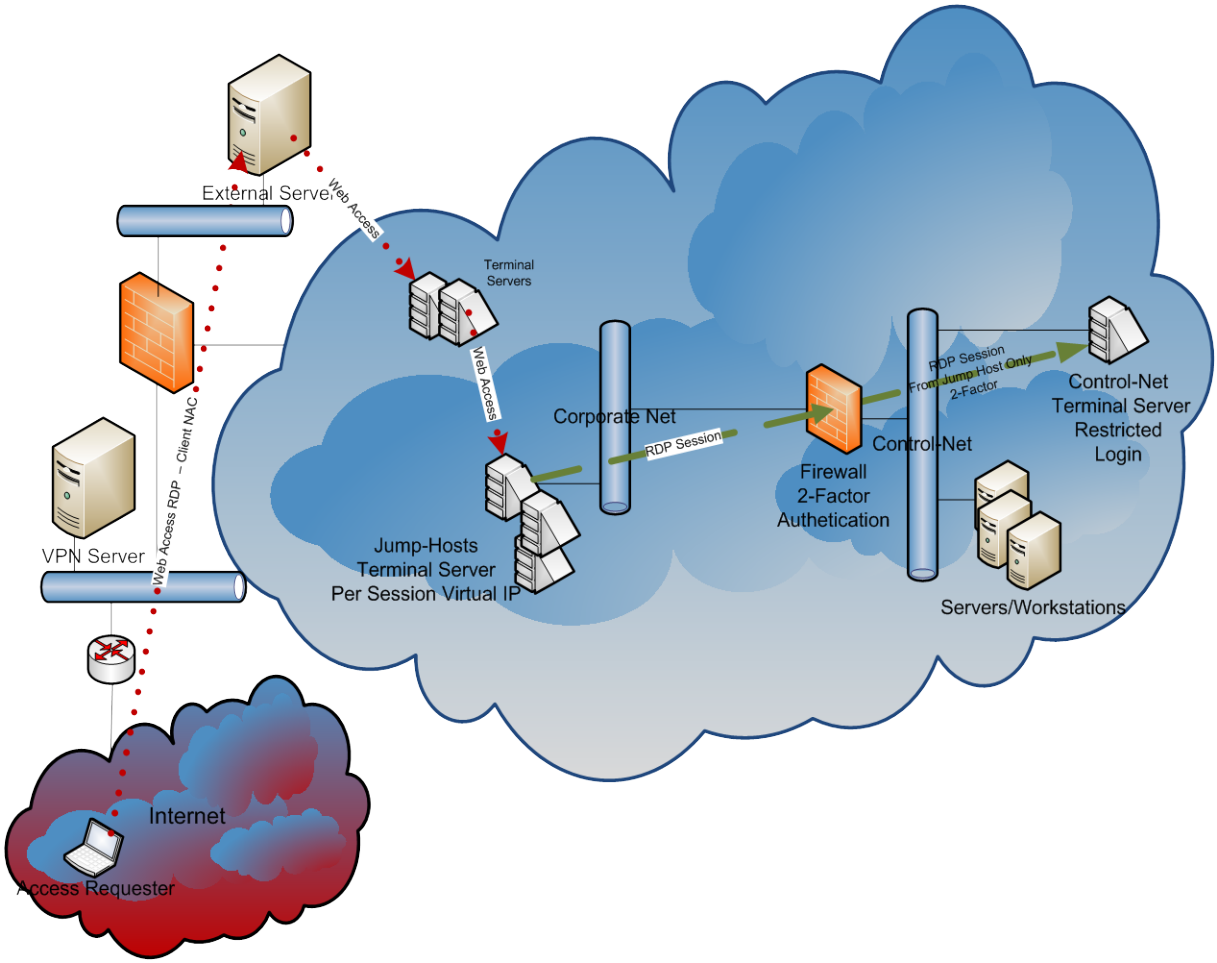

Figure 8: Mid-sized IOU Remote Access

Case Study 6 -- Remote Access to CCAs within an ESP

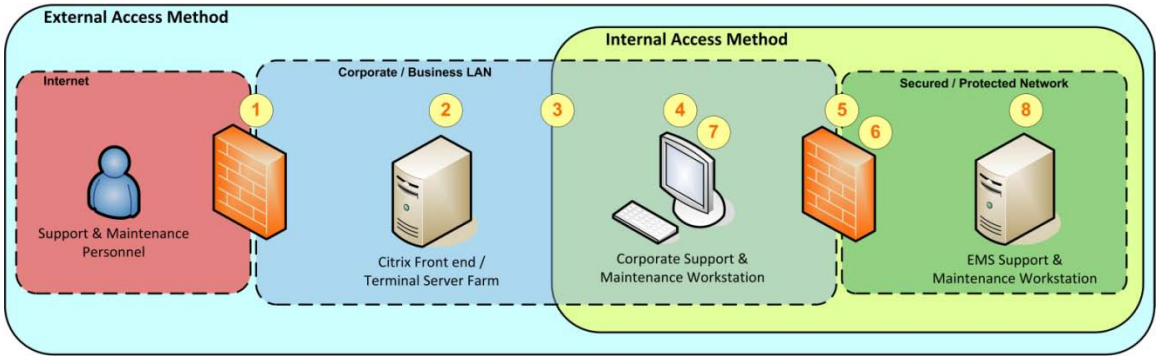

Figure 9: Remote Access to CCAs within an ESP

Secure Access Methods into Protected Networks

External Access Method

1. Support & maintenance personnel connect remotely to corporate 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 & maintenance workstation.

...Proceed to Internal Access Method

Internal Access Method

4. Log into the specific corporate support & maintenance workstation (with AD credentials) which has been identified and configured to access secured/protected network (ESP) via uniquely defined Access Lists.
5. Authenticate to ESP with multi-factor authentication.
6. Launch ssh to connect to EMS support & maintenance workstation within the ESP:
    a. Authenticate via certificate based authentication.
    b. Restrict EMS workstation to specific corporate workstation & user.
7. Launch application, such as remote desktop and tunnel through the ssh connection to uniquely identified EMS support & maintenance workstation within the ESP.
8. Log into the EMS support & maintenance workstation via multi-factor authentication.

References & Bibliography

The following list is a brief compilation of documents and Internet references which 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.

http://www.niap-ccevs.org/pp/draft_pps/archived/remote_accessHA.pdf

http://www.gdc4s.com/documents/D-RAS-6-0507_p1.pdf

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

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

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/

A good government reference on multifactor authentication: 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

Revision History:

Date	Version Number	Reason/Comments
9/17/2010	1.0	Initial posting