CIP-005 R2: Understanding the Security Requirements for Secure Remote Access to the Bulk Energy System

Purpose

CIP-005-5 R2 is focused on ensuring that the security of the Bulk Energy System is not compromised by remote access. The general access control policy defined in section R1 is further augmented by the requirements of R2 for all remote access. This paper discusses the requirements and approaches to meeting the challenge of Remote Access Management for the Bulk Energy System (BES).

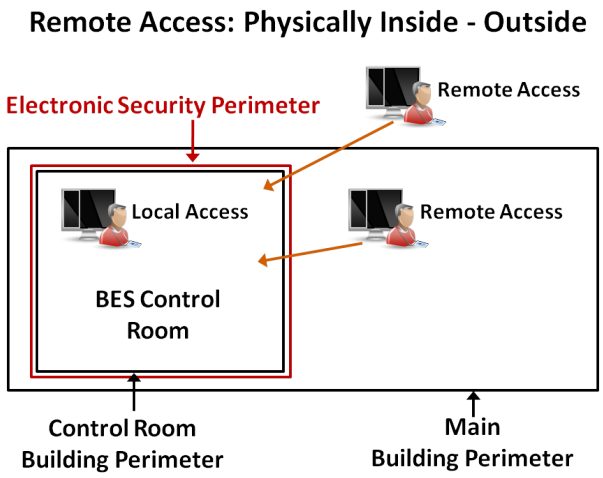
Introduction

The NERC-CIP standards are the primary knowledge resource used by the Utility industry to ensure our nation's power grid is protected from unintentional (accidental) and intentional (malicious) disruption. While the NERC-CIP standard takes a comprehensive approach to cyber security, there remain areas where the specific implications of security vulnerabilities are not understood by the industry at large. This whitepaper looks at the specific area of Remote Access Management as covered by NERC-CIP-005-3a R2.

What is Secure Remote Access?

Remote access occurs anytime an asset inside the electronic security perimeter (ESP) is accessed by a user that is outside of the ESP whether the asset is classified a Critical Cyber Asset (CCA) or not. This includes access from within a physical security perimeter and access from outside all physical security perimeters.

The focus is on user access to the assets or CCA controlling the Bulk Electric Supply (BES). As



depicted in the diagram to the right, users may be inside a physical security perimeter yet outside the actual Electronic Security Perimeter of the BES or they may be at a remote location (i.e. – traveling, working from home, etc.) outside all physical and logical security. Only personnel inside the physical security of the ESP or BES control room (or other secured cyber asset location) would not be considered *remote*.

This is a new requirement for Utility organizations that was not included in previous versions of NERC-CIP. From NERC, it addresses "vulnerabilities for remote access methods and technologies that were previously thought secure and in use by a number of large electric security entities" (NERC-CIP-005-3a R2 - Rationale).

While NERC does not currently provide any requirements or guidance documents on how to accomplish secure remote access, NERC does define the key requirements that must be met by a secure remote access practice or solution in CIP-005.

The key requirements of CIP-005-3a R2 include:

1) Implementing an Intermediate Device for Remote Access
2) Encryption for all Interactive Remote Sessions
3) Multi-factor authentication
4) Up-to-date anti-malware software on user devices
5) Up-to-date patch levels on user devices

Intermediate Device (ID) Explained

A firewall or other electronic access point (EAP) device provides access denial, unless authentication is accomplished, and limited access based on roles. Once authentication is accomplished, it allows the user to directly connect to one or more cyber assets, networks, or other logical elements. In the simplest terms, it is a locked door on the perimeter to the BES that must be opened to gain access.

★★★★★★★★★★

Security Perspective: Personnel remotely accessing the BES must be managed per CIP-005 R2, but they also must be managed per CIP-007 (strong role-based access control, logging, and real-time event /incident detection).

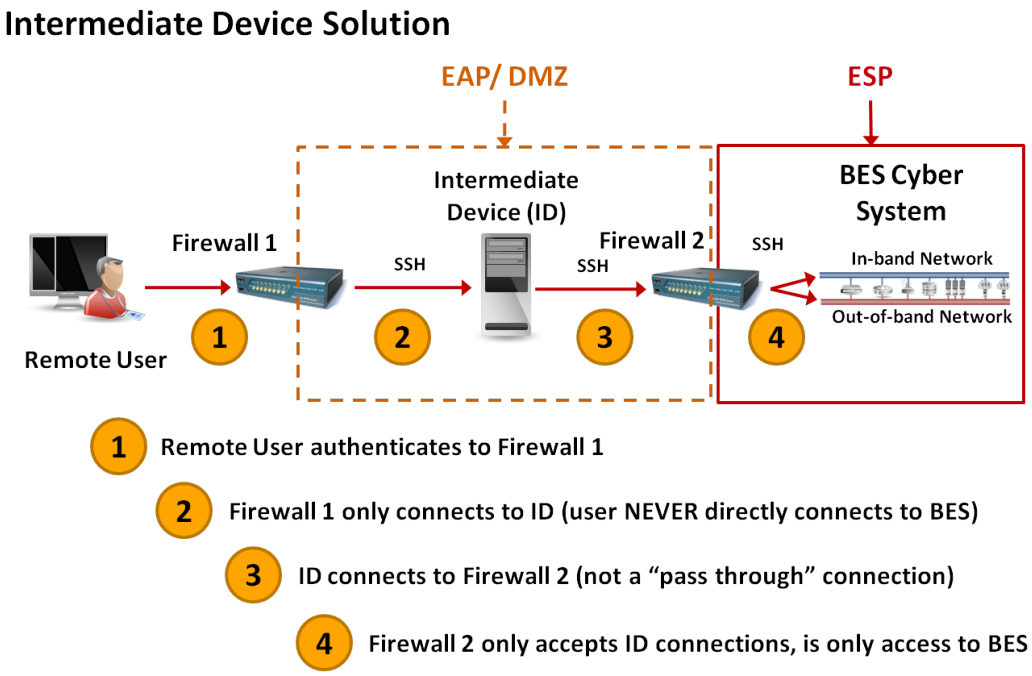
From this perspective, even personnel inside the ESP should be utilizing the same controls for access as those outside the ESP. This ensures that a consistent view, method and process is used for control of the BES - all the while having command and control of the BES that is logged and audited in such a manner as to thwart an insider attack or insider unintentional impact to the BES.

CIP-005 R2 should be considered in the broader scope of the NERC-CIP regulations when formulating an overall security strategy. Addressing the new requirements for Remote Access Management in isolation can result in a fragmented security solution with gaps that can have a significant impact on the ability of the Utility organization to support reliability and security - *its primary objective*.

★★★★★★★★★★

With Remote Access Management there is another step between the EAP and the BES that is required to meet the CIP-005 R2 requirements. Instead of gaining access to the BES through the EAP, the user gains access to an Intermediate Device (ID). The ID is connected to the BES cyber network inside the ESP. In this configuration, there is no direct connection between the remote user and the BES or CCA. This kind of Intermediate Device is often called a jump box or bastion host. The jump box provides an added layer or buffer to the security of the BES, never directly exposing a BES cyber system to a remote cyber asset.

Compared to the EAP "locked door" analogy, CIP-005 R2 can be viewed as two locked doors, with the second door opening from a secure 'room' to the BES cyber network. Authenticated users enter the secure room where they can issue commands that the room can then carry out to the BES cyber asset. In this scenario, the user is never directly connected to the BES cyber system or network. The Remote Access Management solution is presented in the following diagram.



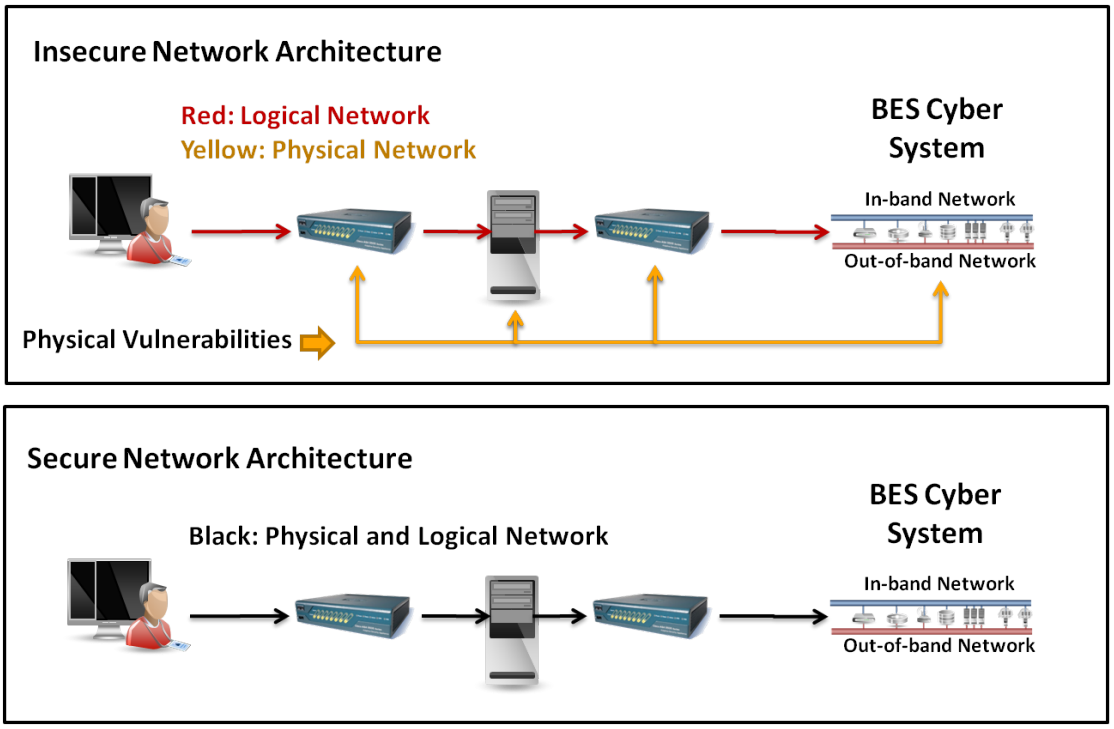
In this scenario, the remote user connects to an EAP through a firewall (Firewall 1), probably with a VPN. The remote user must now authenticate against the Intermediate Device (ID) using a multi-factor (username, password and an additional method) authentication. Once authenticated, the Intermediate Device provides the specific connectivity to the BES CCA through the next firewall (Firewall 2) needed for the remote user to do their work.

The result is a DMZ (De-Militarized Zone) that acts as a composite EAP (combination of Firewall 1, ID, and Firewall 2).

Additional Requirements:

1) Networking between Firewall 1 and the ID is both physical and logical
2) Networking between ID and Firewall 2 is both physical and logical
3) Firewall 1 and Firewall 2 are NOT the same device type

Employing physical networking between Firewall 1 and the ID, and the ID and Firewall 2 (as depicted in the Intermediate Device Solution diagram above) ensures that NO connection can be made to the BES or a CCA without going through the composite EAP.



By deploying defense-in-depth with layering of firewalls, role-based access management, and high availability failover of security status monitoring and event logging, entities can be assured of data integrity, rapid incident response and disaster recovery..

Intermediate Device Advanced Capabilities

Intermediate Devices can provide advanced capabilities to harden the security footprint without impacting user performance – a major drawback in many Intermediate Device approaches.

The major performance impact derives from RDP (Remote Desktop Protocol) sessions[1] that are heavy bandwidth consumers that cannot be comprehensively audited. CLI (Command Line Interface) sessions are much lighter (and auditable) but can still affect performance depending on their technical implementation.

Advanced capabilities in Intermediate Devices can include:

1) Role-based access and control that limits each user's access to a predefined set of cyber assets in the BES
2) Least privilege by user and/or role, limiting privileges to lowest level needed to perform the work the user is authorized to perform

[1] RDP sessions are used with GUI applications and are primarily an artifact of Windows servers

3) Capture of all user activity down to the keystroke (CLI). (usage of video or graphics based interfaces do not allow capture of meaningful keystroke activity for auditing purposes as it allows the mixture of "Button Pushes", "Check Box" and keystrokes.)
4) Capture of system messages from application logs , SNMP alerts, SYSLOG and other sources
5) Management of all BES assets in the ESP – not just servers. Support of more than just a single OS, application or interface.
6) Support for normal and emergency operations including power reset, firmware management, BIOS Configuration as well as multi-user privileged access.
7) Event detection and alerting – predefined and admin configurable
8) Single pane-of-glass oversight
9) Business rules that restrict, alert, or control user activity

★★★★★★★★★★

Additional resources:

One reference that can help in assessing or designing a secure network is available from the Defense Information System Agency:
http://iase.disa.mil/stigs/downloads/pdf/network_management_security_guidance_at-a-glance_v8r1.pdf

Other resources that discuss network design/topology, security practices and security process include ITIL V3, ISO270001, NIST, FEMA, and SANS 20 Critical Security Controls for Effective Cyber Defense.

★★★★★★★★★★

10) Coverage for all privileged interfaces, in-band (production) network and out-of-band (maintenance) network

The items in the list above (in particular items 1,2,3,7,8) are common security practices typically falling under the practice of Privileged Access Management (PAM).

Privileged Access Management

Privileged Access Management is a highly appropriate value-added role for an Intermediate Device for NERC-CIP-005-3a R2. Restricting access to specific cyber assets, networks, or other logical elements at each EAP (the traditional approach) is valuable, but it does not provide fine-grained control over what a user can access or the privileges granted for each. Intermediate Devices should serve as the fine-grained control mechanism for the Remote Access Management practice.

Supporting the Role of People

The most secure access profile eliminates remote access altogether. This, however, is unreasonable as it would require that all staff needed to service the BES - address security threats, perform IT maintenance, and respond to emergencies - would be required to be physically present inside the physical security of the BES ESP at all times (24/7/365).

This brings up an extremely important point. When personnel are accessing the BES remotely, they are typically doing so under conditions demanding fast response and expert skill. This most commonly occurs in one of the following two scenarios: 1) issues that threaten availability of the BES (alarm, outage, service issues, etc.) and 2) security threats.

An Intermediate Device can serve multiple purposes by addressing the context of the people needing remote access with supporting capabilities that improve their ability to resolve operational or security issues.

To do this, the Intermediate Device must have very good situational awareness of the complete BES CCA inside the ESP – from hardware to the application and all points in-between. This way, when the remote or local user accesses the ID they will not need to look in multiple places to gain a forensic understanding of failures, degradation or other issues affecting BES availability (which cause remote access to be used by remote personnel). This directly supports the primary objective of Availability while providing the appropriate level of security.

Forensic capture and logging down to the keystroke of privileged user activity provides another important security and compliance function. Capturing privileged user activity actively deters out-of-policy behavior while the information it contains is often critical to resolving issues and mitigating security threats caused by human error or malicious intent by Insider threat.

Remote access to both in-band and out-of-band networks is a requirement. The out-of-band network is the only network and interface where emergency operations and actions can be taken to resolve hardware or software failures, including configuration issues related to hardware, operating system, network and often applications.

Where the Intermediate Device can capture system messages (application logs, SYSLOG, SNMP and privileged actions for single user and multi-user access et. al.), it can serve a dual purpose by automatically producing compliance records and for retaining information needed by remote users to troubleshoot issues, confirm operations, and be alerted to potential problems.

This ability also has impact on mean-time-to-repair (MTTR) since forensic information needed to repair or

★★★★★★★★★★

In-band and out-of-band networks:

The In-band network is commonly referred to as the production network. It uses the normal networking ports on devices that require each device to be functional, healthy, and fully operational with network services running before communications can be established.

The out-of-band network is commonly referred to as the maintenance network. It uses special ports including baseboard management controllers (iLO, DRAC, ALOM, etc.) and serial privileged interfaces to establish communications. These ports (often called Configuration Ports – see whitepaper CIP-007 R1: Understanding the Importance and Relevance of Configuration Ports to Utility Cyber Security) are always on as long as there is power to the chassis of the device.

★★★★★★★★★★

correct the BES configuration would be at-hand in the event of an outage or degradation. Having the information readily at-hand, eliminates the need to look in multiple places and find available logs messages (assuming they still exist or in some cases may have been a single last gasp alert not stored or no longer available).

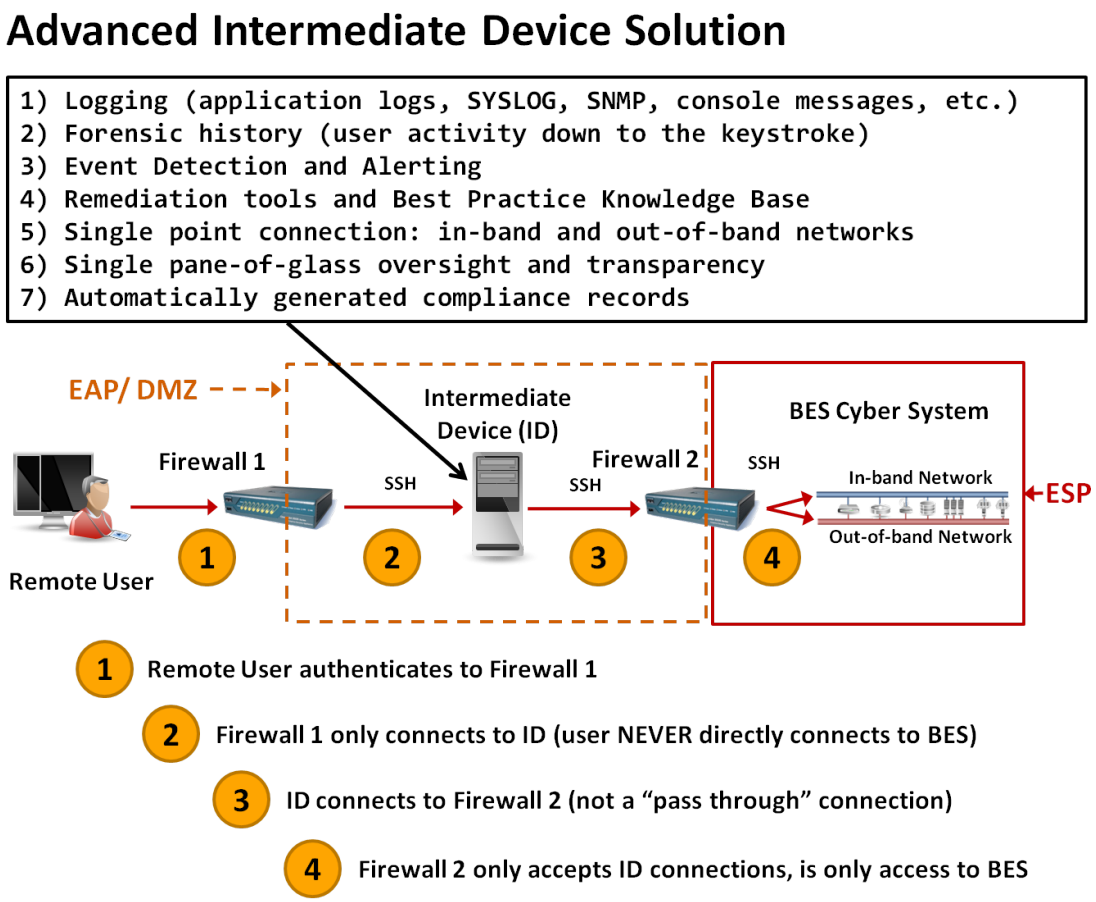
From a management perspective, the Intermediate Device with the capabilities listed here provides comprehensive oversight and transparency. Because the Intermediate Device is effectively a single point of connection for remote and local users to the BES cyber system, it has access to all of the information needed to provide a single source of all Remote Access activity. This makes the Intermediate Device the ideal source for single pane-of-glass oversight and situational awareness.

Ideally, the Intermediate Device would automatically confirm the user's device has met malware and patch level requirements before allowing the user to connect to it – although this may be instituted as a separate security procedure.

The challenge here is that the remote cyber asset is responding to queries by the Intermediate Device and as such, if infected, could very well be malware responding to queries by the Intermediate Device.

Instead of the Intermediate Device querying an agent on the remote device, it is better for the Intermediate Device to simply eliminate the ability to communicate (other than human communication) to the BES through its connections. In other words, no direct, outside protocol is allowed to communicate past the Intermediate Device.

The diagram below depicts an advanced Intermediate Device solution:



While there is concern that the Intermediate Device requirement in CIP-005 R2 may impose additional work on Utility organizations - conflicting with the challenge of delivering affordable electricity with high availability

– this does not need to be the case. The challenge of Privileged Access Management is well understood and commercial solutions exist that do not impact performance. They actually improve user performance (by simplifying the user experience).

Best Practice Guidance

The best practice guidance for Remote Access Management is to look at the problem holistically, including in that view, the perspective of Privileged Access Management. Utility organizations should recognize upfront that performance penalties are not a trade-off they must make, but that due diligence will likely be required on their part to ensure that performance degradation does not become part of the outcome of the Remote Access Management practice.

Specific consideration for Intermediate Device solutions should be given to:

1) Define a strategy that will achieve security goals without negatively impacting performance or availability of the BES but instead increasing the efficiency of the remote user and their situational awareness of the BES
2) Ensure the solution covers both in-band and out-of-band interfaces / networks – both REQUIRE remote access
3) Institute a fine-grained, role-based access and control model for all users (restrict access, least privilege)
4) Ensure the Intermediate Device can encrypt communications from the remote or local user to the BES CCA cyber system
5) Ensure the Intermediate Device supports multi-factor authentication
6) Include all user activity logging in the solution. It provides additional security, can eliminate manual compliance reporting work, and enables oversight
7) Review other potential benefits an Intermediate Device may have, such as automating portions of the security and compliance practice (event management, etc.)
8) Consider a solution that can capture system messages. There may be an opportunity to further reduce compliance report generation costs while improving user performance and provide better situational awareness of the BES to the remote user responding to issues related to security, availability or performance of the BES
9) Consider the solution from the Privileged Access Management perspective. A well-architected solution increases performance and can be applied to ALL users, reducing or potentially thwarting insider threats
10) Consider the ability of the solution to perform configurable alerting and alarming and how that might be used to gain further oversight and proactive notification of security-related events
11) Have a solution that has persistent agent-less monitoring – not polled solutions. Polling introduces windows of invisibility
12) Look for a Vendor supported complete solution – Hardware, Operating System, Application. Training and installation – Turnkey
13) Never provide command line access to the Intermediate Device.

In the case of Intermediate Devices, there are quite a number of different hardware and software solutions that can address at least a portion of the best practices outlined here. Some strategies may require multiple components to be used – noting that this may require additional work to properly harden the resulting Intermediate Device - while others may use a single solution (which may still need to be hardened).

The most important mistake to avoid is to take a minimalist approach that is focused on simply meeting the stated requirements of CIP-005 R2. While a properly designed strategy can deliver advanced security without negatively affecting performance (probably improving it), a less considered approach can have significant negative consequences to performance.

About This Whitepaper

This whitepaper was written to help address a security vulnerability that is often overlooked and misunderstood in the Utility industry. The recommendations provided are believed to be accurate in their applicability and support for NERC-CIP-005 R2. The areas of the NERC-CIP Version 5 standard that we will be discussing in our whitepapers include: CIP-005, 007 and 010.

Full Disclosure

This whitepaper was written and produced by TDi Technologies, a software vendor that provides security, compliance and operations software solutions to the Utility industry and other vertical markets. The information presented here represents our best understanding of the security issues associated with Remote Access Management, which is a problem area our company focuses on. The whitepaper is intended to provide useful and educational content that can assist Utility companies in providing secure, dependable power to our Nation without interruption.

Additional Reference Material from TDi Technologies

For more information on TDi Technologies solution offerings, see NERC CIP Requirements Mapping and Additional Utilities Whitepapers at
http://www.tditechnologies.com/products/nerc-cip-smart-grid-solutions