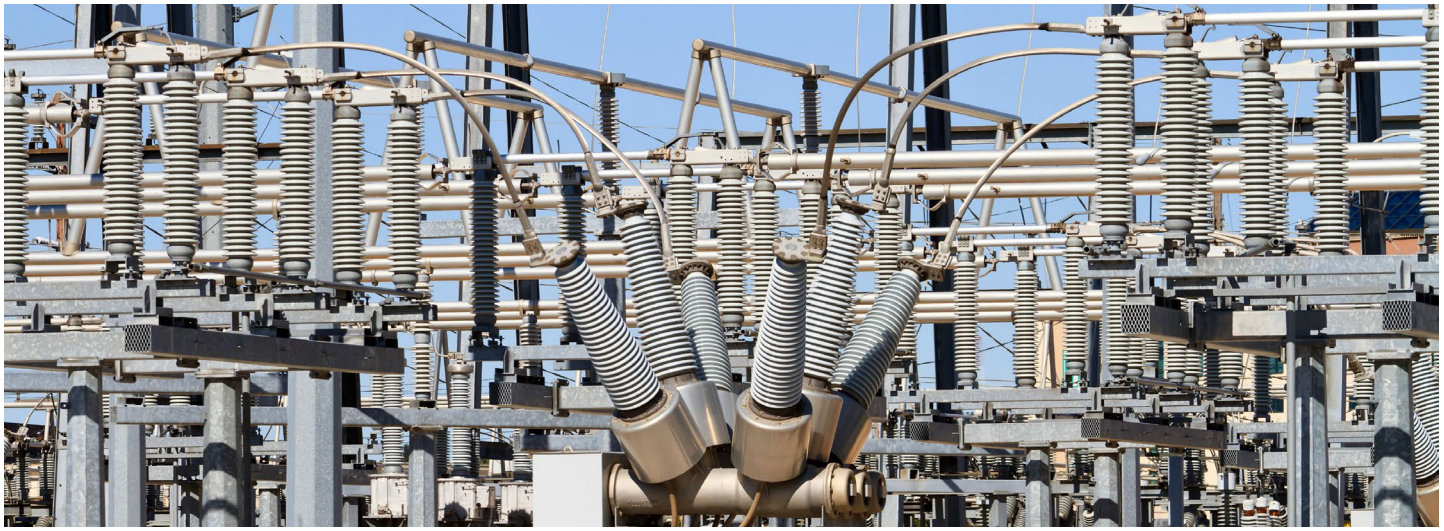
VIRTUAL ACCESS

CRITICAL APPLICATION CONNECTIVITY

Substation Security

Virtual Access Support for NERC CIP



Overview

Virtual Access' cyber-security capabilities help power utilities to comply with North American Electric Reliability Corporation reliability standards for critical infrastructures. Commonly known as NERC-CIPv5 Standards, the NERC's compliance program is a set of requirements designed to improve the reliability of North America's bulk power system by imposing standards covering the security of electronic perimeters and the protection of critical cyber assets, security management, disaster recovery planning as well as personnel and training. NERC standards are designed to ensure correct practices are set up and implemented so the chances and severity of possible future disturbances are greatly reduced.

NERC CIP Version 5 Compliance Mapping

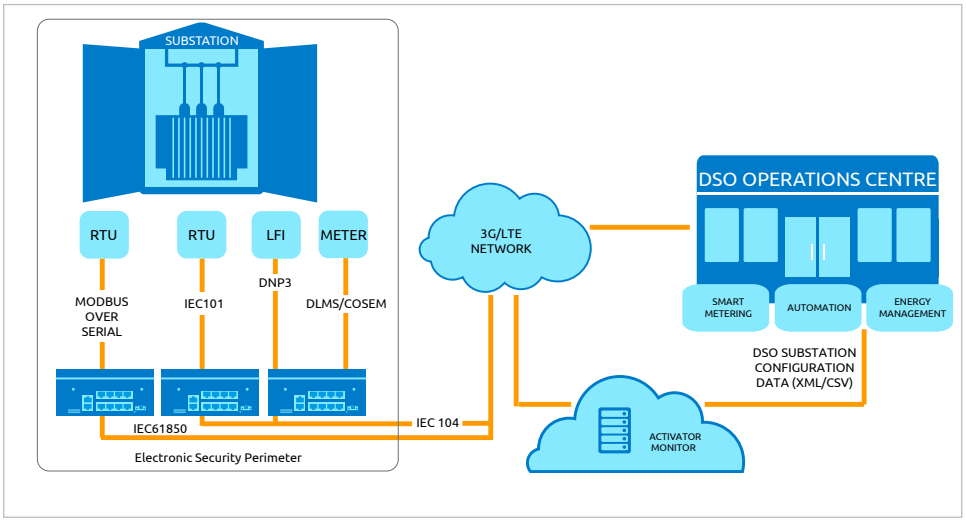
The table shows a mapping of Virtual Access' industrial routers features to NERC CIP 5 standards CIP-005-5 and CIP-007-5. The wide range of Virtual Access routers, combined with the embedded Activator and Monitor deployment and management system, ensures lifecycle security and compliance readiness.

CIP005-5 Electronic Security Perimeter(s)

The purpose of CIP005-5 (electronic security perimeter) is to manage electronic access to BES cyber systems by specifying a controlled Electronic Security Perimeter. Methods and evidence for ensuring compliance include documented processes and measures that address the requirement.

CIP-007-5 System Security Management

The focus of CIP007-5 (system security management) is on port control and access, patch management, malicious code detection and prevention, incident log capabilities, and access controls.



CIP-005-5 R1 Part1.3				
Applicable Systems	**Requirements**	**Measures**	**VA Router Features**	**Additional Information**
Electronic Access Points for High Impact BES (Bulk Electric System/Substation) Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems.	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.	Stateful firewall and access control system to manage both user access and solicited and unsolicited traffic	Firewall: • Stateful • IP filters • MAC filters • DOS protection
Part1.4				
Applicable Systems	**Requirements**	**Measures**	**VA Router Features**	**Additional Information**
High impact BES cyber systems with dial-up connectivity and their associated: • PCA (Protected Cyber Assets) Medium impact BES cyber systems with dial-up connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing dial-up Connectivity with applicable cyber assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible entity is providing authenticated access through each dial-up connection.	Access control system to manage both user access and solicited and unsolicited traffic.	Access control: • Secure access with SSH and HTTPs • RADIUS support • TACACS support • 802.1x • Multi user router access • Event system monitors malicious access
Part 1.5				
Applicable Systems	**Requirements**	**Measures**	**VA Router Features**	**Additional Information**
Electronic access points for high impact BES cyber systems Electronic access points for medium impact BES cyber systems at control centers.	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.	Stateful firewall to manage solicited and unsolicited traffic.	Firewall: • Stateful • IP filters • MAC filters • DOS protection
CIP-005-7 R5 Part 2.1				
Applicable Systems	**Requirements**	**Measures**	**VA Router Features**	**Additional Information**
High impact BES cyber systems with dial-up connectivity and their associated: • PCA Medium impact BES cyber systems with dial-up connectivity and their associated: • PCA	Utilize an intermediate system such that the cyber asset initiating Interactive remote access does not directly access an applicable cyber asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.	Stateful firewall and access control system to manage both user access and solicited and unsolicited traffic	Firewall and access control: • Stateful • IP filters • MAC filters • Secure access with SSH and HTTPs • RADIUS support • TACACS support • 802.1x • Event system monitors
Part 2.2				
Applicable Systems	**Requirements**	**Measures**	**VA Router Features**	**Additional Information**
High impact BES cyber systems with dial-up connectivity and their associated: • PCA Medium impact BES cyber systems with dial-up connectivity and their associated: • PCA	For all interactive remote access sessions, utilize encryption that terminates at an intermediate system.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.	Comprehensive VPN solutions.	• IPSec • OpenVPN • SSL • AES256 • SHA512 • MODP8192
Part 2.3				
Applicable Systems	**Requirements**	**Measures**	**VA Router Features**	**Additional Information**
High impact BES cyber systems with dial-up connectivity and their associated: • PCA Medium impact BES cyber systems with dial-up connectivity and their associated: • PCA	Require multi-factor authentication for all interactive remote access sessions.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable cyber assets and electronic access points, individually or by group. • Listings of the listening ports on the cyber assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host based firewalls or other device level mechanisms that only allow needed ports and deny all others.	Stateful firewall to manage solicited and unsolicited traffic	Access control: • Secure Access with SSH and HTTPs • RADIUS support • TACACS support • 802.1x • Multi user router access • Event system monitors malicious access • X.509 certificate support

CIP-007-5 R1 Part1.1				
Applicable Systems	Requirements	Measures	VA Router Features	Additional Information
High impact BES cyber systems and their associated: 1. EACMS (Electronic Access Control & Monitoring System); 2. PACS (Physical Access Control System); and 3. PCA Medium impact BES cyber systems with external routable connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable cyber assets and electronic access points, individually or by group. • Listings of the listening ports on the cyber assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host based firewalls or other device level mechanisms that only allow needed ports and deny all others.	Stateful firewall to manage solicited and unsolicited traffic	Firewall: • Stateful • IP filters • MAC filters • DOS protection • SCADA itegrity checking
Part1.2				
Applicable Systems	Requirements	Measures	VA Router Features	Additional Information
High impact BES cyber systems Medium impact BES cyber systems at control centers.	Protect against the use of unnecessary physical input/ output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.	Access control system to manage both user access and solicited and unsolicited traffic	Access control: • Secure access with SSH and HTTPs • RADIUS support • TACACS support • 802.1x • Multi user router access • Event system monitors malicious access • X.509 certificate support