Understanding NERC CIP compliance solutions with Phoenix Contact

By Mariam Coladonato, Lead Product Marketing Specialist, Networking and Security, Phoenix Contact USA

INSIDE:

Introduction

The Internet phenomenon stands out because it facilitates rapid access to infinite amounts of information at a relatively low cost. In other words, the concept of distance has no rationale in this new society, because it seems we have all the information we want at our fingertips.

Indeed, the Internet revolution has changed and improved many processes. It has united the world in its connection capacity and represents an opportunity for new creations. However, like all revolutions, it has as many detractors as defenders. There are both positive and negative attributes that impact the social, political, and economic aspects.

One example that can affect the entire chain is the Industrial Internet of Things (IIoT), also known as "Smart Industry" and similar to the German project called "Industrie 4.0." This concept is making a fully automated industrial world a reality. Imagine complete industrial production plants like power or water, providing services automatically, connected to the Internet, and all operating without any human intervention.

The biggest, most meaningful impact falls within the political spectrum, as cyberspace becomes a new expanded nation without borders, created without any absolute laws. The Internet revolution has facilitated the diffusion of power, and not from one state to another. This power is falling outside the control of even the most powerful governments, and these entities must learn to share it with others that may be difficult to control. Following the above scenario, consider the risk of power plants connected to the Internet and the possible consequences if a cyberattack were to happen.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Email: info@phoenixcon.com • Website: www.phoenixcontact.com

The Aurora Project works as a perfect illustration. This project was funded by the Department of Homeland Security (DHS) in 2015 and exposed a common vulnerability around electrical devices like power plant generators. Can you imagine the next world war as a digital affair? Unfortunately, there are malicious and unethical people who could use their knowledge and resources to attack a nation-state by targeting its electric utility. Although it's scary to think about, we must keep in mind that it is feasible, as proven by the Russians in the cyberattack against Ukraine's power grid that caused outages all over the country back in 2015.

The utility owners' need for connectivity and the high risks that the bulk electric system (BES) in the US faces daily are the main reasons why the FERC granted NERC the authority to form the CIP committee. This committee is in charge of helping advanced physical and cyber security around the North American critical electricity infrastructure.

"The vision for the Electric Reliability Organization Enterprise, which is comprised of NERC and the seven Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid."

The NERC CIP plan is a set of standards developed to secure all physical and cyber assets. The federal government has established this plan as mandatory and enforceable for registered owners and operators of North America's bulk electric system (BES). The plan covers assets like control centers, BES transmission and generation facilities, black start resources, special protection systems, and load-shedding. The responsible entity must name a CIP Senior Manager (CSM), a single authority with full responsibility for leading and managing the implementation of and continuous adherence to requirements within NERC CIP.

The current NERC CIP set, version 6, consists of 11 listed standards and a series of requirements mainly covering the protection of physical and cyber security. Additionally, these standards incorporate the basics of critical asset identification, employee awareness and training, emergency preparedness and response, business continuity plans and recovery from disastrous events with the urgency to focus on deterring, preventing, limiting, and recovering from any possible cyberattack.

- **CIP-002-5.1a: Cyber Security — BES Cyber System Categorization:** The objective is to identify and categorize all BES Cyber Systems as low, medium, or high impact.
- **CIP-003-6: Cyber Security — Security Management Controls:** This is primarily a policy-focused standard, where responsibility and accountability of BES Cyber System protection is noted. However, there is an exception, as the requirements for Low Impact BCS are grouped in four main topics: security awareness, physical security, electronic access, and incident response.
- **CIP-004-6: Cyber Security — Personnel & Training:** The purpose is to provide security training and manage individuals with direct access to the BES Cyber System.
- **CIP-005-5: Cyber Security — Electronic Security Perimeter(s):** This section defines all requirements regarding the defensive boundary around the electronic systems in the BES Cyber Systems for routable communications.
- **CIP-006-6: Cyber Security — Physical Security of BES Cyber Systems:** The goal is to appropriately plan and manage all physical security access to the BES Cyber Systems.
- **CIP-007-6: Cyber Security — System Security Management:** The target is to manage the system security of the BES Cyber Systems at technical, operational, and procedural levels.
- **CIP-008-5: Cyber Security — Incident Reporting and Response Planning:** This standard mainly deals with the teams and appropriate response plans to a cybersecurity incident.
- **CIP-009-6: Cyber Security — Recovery Plans for BES Cyber Systems:** This aims for a reliable recovery of all the functions performed by the BES Cyber System following a recovery plan.
- **CIP-010-2: Cyber Security — Configuration Change Management and Vulnerability Assessments:** The overall approach is to prevent and detect any unauthorized changes to the BES Cyber

Systems by applying controls of change management and vulnerability assessments.

- **CIP-011-2: Cyber Security — Information Protection:** It applies to the protection of information to prevent unauthorized access and distribution that could be useful to a potential attacker.
- **CIP-014-2: Physical Security:** The point is to design and implement physical security plans around transmission stations, substations, and their primary control centers.

With time, NERC CIP has made the CIP standards easier to digest for the CIP senior manager, as each standard is separated in multiple sections:

- Introduction: Includes the specific purpose of the current standard.
- Requirements and Measures: Explains the actual mandatory requirement and the associated measure.
- Attachments: Serves as additional support documentation for the standard requirements.
- Guidelines and Technical Basis: Discusses the technical reasons behind the need or the standard requirement, with additional guidance for appropriate compliance.
- Violations: Describes the Violation Security Level (VSL) and Violation Risk Factor (VRF) at multiple degrees in which a requirement can be violated and the relative risk factor that it represents if the requirement it is not met.

At Phoenix Contact, we have found greater simplicity in the compliance process by dividing these 11 standards into four groups:

Identify, categorize, classify, and continuously monitor all your assets and information

One of the most basic but important steps that any critical industry owner could take toward better cybersecurity is to fully understand what assets exist within their networks (device names, serial numbers, baseline configuration, firmware levels, and patches) and the specific location within the entire infrastructure. Furthermore, owners can categorize and rank them by vulnerabilities, essentialness to the operation, and even possible impact rating if something happened.

Additionally, this group isn't restricted to devices. Asset owners must understand the flow of critical information, either in storage, in use, or in transit, and implement security control mechanisms for data transfer, data encryption, data loss prevention, and appropriate disposal and sanitation if needed.

To be more precise, CIP-002, CIP-010, and CIP-011 could touch a variety of these points. For more specific information regarding each CIP requirements, visit https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Look after the physical security of your assets and the employees who work around them

While many asset owners already attend physical security within their assets, standards CIP-006 and CIP-014 require a level of detail that might prove their measures to be insufficient and out of compliance by default. Physical access control systems such as cameras, biometrics, badging technologies, and alarms are widely used; however, the standard also implies that the proper physical security plans are being implemented and documented to keep these entry/departure logs on record for a period of time, for employees and third parties alike. Additionally, physical security mechanisms extend to cabinets, cabling, and components used for connections between cyber assets within the electronic security perimeter (ESP).

Personnel management is another factor in the NERC CIP equation for CIP-004, which governs security awareness and training for employees who have authorized electronic or unescorted physical access to the BES systems. General security awareness could come in the form of emails, posters, presentations, etc., depending on individual roles. Security training would be geared toward the specific functions and responsibilities. This standard also extends to pre-hiring screening processes and background checks, properly addressing access management controls, and revocation at the time of employees' terminations.

For more specific information regarding each CIP requirement, visit https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Email: info@phoenixcon.com • Website: www.phoenixcontact.com

Formulate plans to protect your cyber assets and systems

Both CIP-005 and CIP-007 present requirements and guidance for securing a variety of assets within a system. For example, there are rules governing electronic access points (EAPs) required in each electronic security perimeter (ESP) with inbound and outbound communication. These rules refer to technologies like firewalls, as well as the implementation of processes to detect malicious communications crossing these paths. These processes may be embedded within the firewall, or additional software like intrusion detection systems might be applied at that level. When remote access is needed, Virtual Private Network (VPN) equipment with strong authentication and encryption is part of the requirement. Furthermore, malicious software risks are to be treated with anti-virus products or any kind of anti-malware feature. Also, patch management and security logging and alerting requirements fall within these standards.

For more specific information regarding each CIP requirement, visit https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

It is all about the policies and procedures

Applying all the mentioned standards is not enough for NERC CIP, as the proper documentation of policies and procedures around each CIP is also a requirement. CIP-003 is a policy-focused standard that looks to review and obtain approvals periodically, identify a CIP senior manager by name, and document processes of delegation of authority. CIP-008 revolves around the response plans and procedures after a cybersecurity incident has happened, how it would be handled, the responsible individuals who must come together, and the proper gathering and analysis of forensic evidence for the investigation. CIP-009 deals with the recovery plans for BES Cyber Systems, where the recovery of all the affected functions after the incident much be achieved concerning the stability, operability, and reliability of the system.

For more specific information regarding each CIP requirement, visit https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

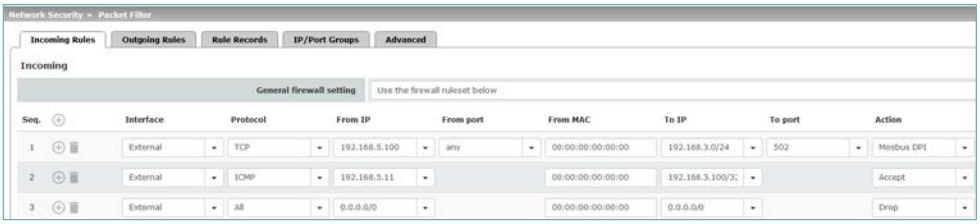
Phoenix Contact can help

If your company is identified as an asset owner within NERC CIP, most if not all, of the responsibility to determine the policies and procedures for these critical steps will fall on the shoulders of your IT department. They'll need to understand and register your applicability, define your system categorization, plan the most efficient ways to achieve, and document your compliance. However, from a product perspective, Phoenix Contact already offers multiple solutions and services that can help you fulfill some of the NERC CIP requirements. Below you will find a list of a some of these:

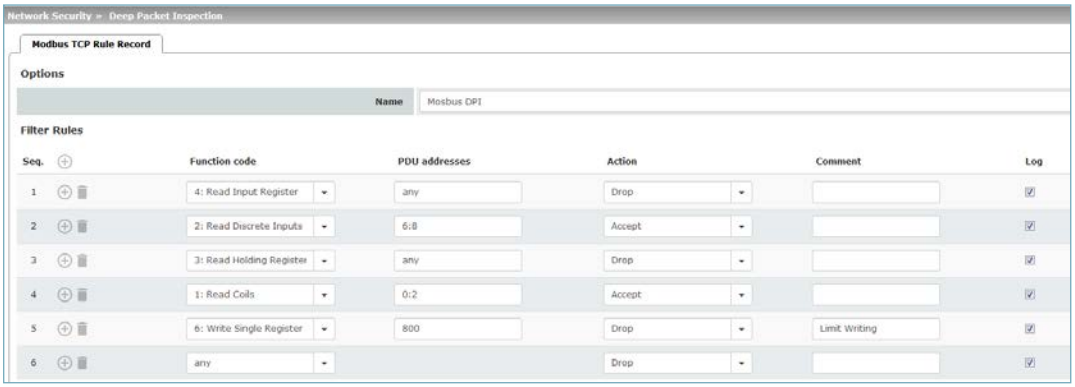
- CIP-002 contains obligations with respect to the identification of BES Cyber Systems. The FL Network Manager from Phoenix Contact is a software product that identifies network participants, MAC addresses, and IP parameter assignments regardless of the vendor. It also could list firmware level and device type, depending on the response to the SNMP message request, and even do some basic device configuration and firmware updates. Additionally, the FL Network Manager can be programmed to continuously monitor your devices' availability within the network. This software also allows you to export these devices' data in multiple file formats to maintain the logs needed for NERC CIP audits.
- CIP-003, CIP-006, and CIP-014 touch on points regarding physical security controls and implementations. Phoenix Contact offers low-cost, easy-to-install, self-locking security elements for Ethernet cables and sockets that protect against intentional or accidental release of cabling and restrict adding new network components. For example, the image below shows a Phoenix Contact unmanaged switch (the FL Switch SFN), which does not have the capabilities to virtually protect or disable ports. However, with the FL Plug Guard protecting cabling and unused ports, you can still achieve physical security requirements inside the control cabinet for NERC CIP. Additional parts like the FL Patch Guard would achieve the same level of security for unmanaged switches from other vendors by physically protecting the Ethernet cables from unwanted physical release.

FL Plug Guard in a FL SFN Switch

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Email: info@phoenixcon.com • Website: www.phoenixcontact.com



Stateful Packet Inspection Firewall Screen Shot from FL mGuard: User can configure options, including protocol, Source/Destination IP, port, action, and logging. Implicit deny ensures that traffic not matching any rules gets dropped.



Modbus Inspector Firewall screen shot from the FL mGuard: User can specify actions based on function code and coil/register address range.

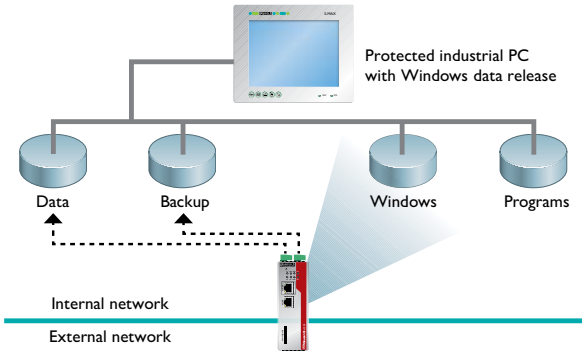
- CIP-003 and CIP-005 consist of multiple requirements around electronic access permissions, focusing on restrictions in the inbound/outbound communication through an EAP, which is a natural market for firewall devices. The Phoenix Contact FL mGuard security devices can protect your systems against unauthorized access with an out-of-the-box stateful packet inspection firewall that can filter based on rules, MAC and IP addresses, ports, and some protocols.

  Furthermore, advanced firewalls with the ability to perform application-level security and monitoring can aid in protection against malicious communication crossing inside the ESP boundary. For example, the FL mGuard with its Deep Packet Inspection (DPI) firewalls can analyze and filter the network packets at the Modbus TCP and OPC Classic application layers.

  The mGuard security devices also support additional features like IP and Port Groups, which make the entire firewall configuration and management simpler to use. Furthermore, the built-in User Firewall feature also provides easy access to your authorized employees into the ESP boundary, still applying the firewall rules needed. However, these rules would be enabled after a user is authenticated locally or through a RADIUS authentication server.

- CIP-005 also refers to the need and usage of secure remote access into the ESPs. This can also be addressed with the FL mGuard, which can serve as a VPN gateway that supports both IPsec VPN (client/server) and OpenVPN (client only) technologies, conforming with the highest encryption standard of AES-256, hash algorithms of SHA-512, and certificate authorities for the authentication of peers. The product family also offers additional features within the VPN functionality:

  - Firewall filtering after an authenticated VPN: This means that you can restrict traffic for authorized users inside the tunnel.
  - Conditional VPN: The VPN tunnel doesn't need to be enabled at all times. The mGuard devices can be configured to enable/disable VPN tunnels with the closure of a digital contact embedded in the hardware. For example, it can be a switch or a push button. This allows VPN security controls at the ESP level for remote users, as well as monitoring and logging of when authorized users were remotely connected.
  - Multi-Factor Authentication: Remote access users can use two-factor authentication when connecting through an mGuard VPN. One factor is something they have, which is the VPN certificate used. The second factor is something that they know, such as a password. The mGuard uses a built-in feature called User Firewall. Even though the VPN is authenticated through certs, the traffic won't be allowed in until the user is authenticated using a login and password inside the VPN traffic.



CIFS Integrity Monitoring

- CIP-007 has a variety of requirements touching on several points. One of them is for the risk management of malicious software; it calls for deployment methods to deter, detect, or prevent malware in order to protect operating systems (OS) sitting inside the control systems' environments. The FL mGuard family has an optional license that can be added into the devices called Common Internet File Systems Integrity Monitoring (CIFS IM). CIFS IM can detect whether Windows-based systems, such as controllers, operator interfaces, or PCs, have been manipulated, for example, by malware, without the need to load virus patterns.

  CIFS IM regularly checks Windows systems against a reference status to determine whether certain files (e.g., .exe or .dll) have been changed. If a file system to be checked is reconfigured or modified, a reference or integrity database must be created. This database contains the checksums of all files to be checked and is used as a basis for comparison. It is created either on the first check or explicitly due to a specific reason. If the checksum of a file has changed, this means that the file has been modified. If an authorized user did not perform this change, it may have been modified by malware. It also detects the deletion or addition of a file. When CIFS IM detects a checksum change, it generates an alarm via either email or SNMP trap. The integrity database itself is protected against manipulation.

- CIP-007 also requires collection and monitoring of the security event logs around a Security Information and Event Management (SIEM) system. Phoenix Contact doesn't offer a SIEM system; however, all of our industrially managed products, like the FL mGuard or FL Switches, do offer logs for plenty of functions locally, which can even be sent to a central log server. Additionally, a list of product features can generate alarms in the form of emails, SMS text messages (if using cellular modems), and SNMP packets.

Conclusion

It is a privilege to witness the social, political, and economic changes that are happening due to the information revolution. The Internet has affected and will continue to affect everything inside our civilization: the way we live, work, and relate. The process is irreversible, but the faster adapters can survive and succeed in this revolution.

The NERC CIP compliance is a perfect example of cybersecurity regulations that are being reviewed and enforced at a fast pace. If companies and users do not adapt quickly, they will face sanctions and fines accordingly. The most effective security is holistic, flexible, adaptable, and sensitive to the changing circumstances NERC CIP envisions. It should cover component security, device-specific features, system and network characteristics, communication management procedures, and personnel awareness and training. Compliance with NERC CIP regulations ensures the reliability and availability of the power grid, which serves our homes and businesses throughout the entire country.

Owners and operators of the BES covered under NERC CIP can rest assured that partnering with Phoenix Contact can help them fulfill multiple requirements through device-level unique features and configurations. This partnership can also help you distribute the resources and training you might need, depending on the engineering services level you're looking to achieve.

References

https://www.nerc.com/Pages/default.aspx

Attachments

Attachment 1

Attachment 2

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Email: info@phoenixcon.com • Website: www.phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

ABOUT PHOENIX CONTACT

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect, and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 50 international subsidiaries, including Phoenix Contact USA in Middletown, Pa.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com,** call technical service at **800-322-3225,** or e-mail **info@phoenixcon.com.**

This article expresses the personal views of the author and does not represent the opinions of any employer or business entity, (the "Company") with which the author is affiliated.

The information in this article is intended solely for informational, educational, and personal non-commercial use only. The information contained in this article is general in nature and should not be considered as the provision of consulting services or the rendering of any other professional advice. The reader's adherence to the examples or information contained within this article does not constitute compliance with the NERC Compliance Monitoring and Enforcement Program ("CMEP") requirements, NERC Critical Infrastructure Protection ("CIP") Reliability Standards, or any other NERC Reliability Standards or rules. This article should not be treated as a substitute for any such Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the reader should rely on the language contained in the applicable Reliability Standard itself, and consult with a professional who is familiar with the reader's particular factual situation for advice or guidance concerning compliance with these Reliability Standards before making any decision. The information contained in this article is provided on an "as is" basis with no guarantees of completeness, accuracy, or usefulness

Neither the author nor the Company assumes any responsibility or liability for any errors or omissions in the content of this article. The reader accepts full responsibility and assumes all risk for his or her use or actions taken upon his or her receipt of any of the information. Neither the author nor the Company will be liable for any losses or damages sustained by a reader or any third party in connection with the reader's use of this article.

P.O. Box 4100
Harrisburg, PA 17111-0100
Phone: (717) 944-1300
Fax: (717) 944-1625
www.phoenixcontact.com

Removable Media Declaration of Usage for the mGuard devices

To whom it may concern:

Depending on the hardware, the mGuard product line has embedded various types of removable media inserts, such as an SD card for TC and FL variants, or memory plugs for GT/GT variants. Supporting functions removable media allows for easier configuration management and/or firmware updates.

1. Using the removable media as external configuration storage

Configuration profiles stored on mGuard devices can be exported to external configuration storage (ECS), from where they can be imported onto other mGuard devices. The configuration can be automatically loaded, decrypted, and used as the active configuration when the device is started or loaded and activated via the web interface.

- Technical requirements of SD card: FAT file system on the first partition and maximum recommended size of 2 GB.
- The memory plug is available in two versions with different memory capacity. Listed under the specific accessories page for the product.
- When a configuration profile is saved, the passwords used for authenticating administrative access to the mGuard (Root password, Admin password, SNMPv3 password) are saved in a hashed, i.e. not human-readable, format.
- It is possible to load and activate a configuration profile that was created under an older firmware version. However, profiles created with newer firmware will not load on a device running older firmware.
- From mGuard firmware version 7.6.1, all configuration profiles can be encrypted when stored on any ECS device, not supported on FL MGUARD GT/GT.

2. Using the removable media for flashing the firmware

Firmware updates can be done on mGuard devices using the external configuration storage (ECS) and the flashing procedure.

- No settings like VPN tunnels, firewall rules, or passwords will be retained after the flash update. The mGuard device will be reset to factory default.
- Firmware Flash Procedure (SD card):
    a) Users can download the necessary firmware files from the Phoenix Contact website.
    b) Create a folder in the ECS called Firmware.
    c) Copy and paste the needed files into the ECS Firmware directory.
    d) Safely eject the ECS from the PC and insert it into the mGuard device.
    e) Hold the reset button for about 3 seconds, release when all top LEDs light up.
    f) The complete process will take 5–7 minutes total and will show the top LEDs blinking in unison.
    g) Power cycle the mGuard.

If you have any questions about any of the mGuard product lines, their capabilities and features, or how they relate to NERC-CIP compliance, please don't hesitate to contact me.

Sincerely,

Mariam Coladonato
Lead Product Marketing Specialist, Networking and Security

P.O. Box 4100
Harrisburg, PA 17111-0100
Phone: (717) 944-1300
Fax: (717) 944-1625
www.phoenixcontact.com

To whom it may concern,

The FL mGuard product line, as a properly configured security appliance, has several features and functions that support the attainment of NERC-CIP compliance in many of the required areas. The table below lists the NERC-CIP sections, descriptions of the section requirements, and the mGuard feature(s) that can be utilized to help address these requirements.

Note: for the FL mGuard RS4000 and GT/GT series with additional security licenses

Section	Description	mGuard Feature(s)	How it helps meet compliance
CIP-003-6 - Attachment 1 –Section 3	Electronic Access Controls	Stateful Packet Inspection firewall and optional Deep Packet Inspection Firewall for Modbus TCP and OPC Classic, User Firewall w/ RADIUS, X509 with CRL.	These are all features in the firewall that limit what TCP/IP and Ethernet traffic is allowed to pass through the mGuard. The ability to restrict traffic operates in both directions and can filter based on MAC, IP, and TCP/UDP headers as well as Modbus and OPC data payloads. All unspecified traffic is denied.
CIP-003-6 - Attachment 1 –Section 4	Cyber Security Incident Response	CIFS Integrity Monitoring (CIM) to identify incidents in OS.	CIM is an additional mGuard license that alerts operators and/or admins to any changes to the Windows/Linux file system of a protected system. These changes include new files, modified files, and deleted files.
CIP-005-5 R1 Part 1.3	ESP: inbound and outbound access permissions	Stateful Packet Inspection firewall and optional Deep Packet Inspection Firewall for Modbus TCP and OPC Classic.	These are all features in the firewall that limit what TCP/IP and Ethernet traffic is allowed to pass through the mGuard. The ability to restrict traffic operates in both directions and can filter based on MAC, IP, and TCP/UDP headers, as well as Modbus and OPC data payloads. All unspecified traffic is denied.
CIP-005-5 R1 Part 1.5	ESP: inbound and outbound access permissions	Optional Deep Packet Inspection Firewall for Modbus TCP and OPC Classic, Local and remote Logging.	The application-layer firewall in the FL mGuard can filter traffic for Modbus TCP and OPC Classic protocols. Within this functionality, the mGuard has the ability to log "traffic hits" against it. For example, both an employee **allowed** FTP request *and* the dropping of an **unauthorized** HTTP request could be logged. The logging can be done locally and/or redirected remotely to a central log server or System Information Event Manager server.

Section	Description	mGuard Feature(s)	How it helps meet compliance
CIP-005-5 R2 Part 2.2	Interactive Remote Access Management: Encryption Termination	IPsec VPN (server and client) or OpenVPN (client only) terminates at the mGuard device; additionally, the VPN firewall can filter traffic inside the VPN.	VPN traffic is limited to the LAN/DMZ network. It is not permitted to be decrypted and routed to the WAN. Further VPN tunnel firewall and network configuration can limit the traffic to only certain IPs and/or networks over a VPN (an example of split tunneling).
CIP-005-5 R2 Part 2.3	Interactive Remote Access Management: multi-factor authentication	IPsec VPN (server and client) or OpenVPN (client) with Certificates and User Firewall through VPN interface	First, to establish a VPN would require an X.509 certificate (i.e., "something they have"). Second, to pass data through the VPN, including the mGuard itself or any end devices, would require a second authentication to the mGuard using User Firewall username and password (i.e., "something they know"), also supported with RADIUS authentication.
CIP-007-6 R3 Part 3.1	Malicious Code Prevention	Optional CIFS Integrity Monitoring License	CIM is an additional mGuard license that alerts operators and/or admins to any changes to the Windows/Linux file system of a protected system. These include new files, modified files, and deleted files. This is a type of "whitelisting" technology that does not require malware signatures or malware database updates, external server access, etc.
CIP-007-6 R4 Part 4.1	Security Event Monitoring	Logs are available around most mGuard functions. Logs can be maintained locally or be sent to a central log server.	Logging is available for successful logins and failed logins via Web GUI, CLI/SSH, SNMP, or Serial interfaces. CIM will log successful scans as well as detecting file system changes/unknown files (for malware prevention). VPN will log the tunnel being established, or a disconnected mGuard will log configuration parameter changes. Firewall functions can log all allowed or denied traffic across any interface or tunnel. The logging can be done locally and/or redirected remotely to a central log server or Security Information and Event Management server.

Section	Description	mGuard Feature(s)	How it helps meet compliance
CIP-007-6 R4 Part 4.2	Security Event Monitoring: Alerts	A list of mGuard features can generate alarms in the form of emails and SNMP packets to a server.	SMTP traps, SMS text messages (if using a cellular mGuard), and SNMP emails can be generated for a more limited number of events, including input/output contacts and VPN-based events.
CIP-007-6 R5 Part 5.1	System Access Control: Authentication enforcement	User Firewall w/ RADIUS or user password, X509 with CRL.	Firewall rules can be activated only upon successful authentication to the mGuard via User Firewall account (username + password or RADIUS authentication). Web GUI and SSH access to the mGuard itself can be granted only via administrative password and/or X.509 certificate. Validity of certificates can be enforced via CRL database.
CIP-008-5 R1 Part 1.1	Cyber Security Incident Response Plan Specifications: Identification	Syslog, SNMP Trap, Firewall log info.	These events and triggers serve as the input to initiate a CSIRP. They use industry standard protocols and formats such as SNMP trapping to ensure broad compatibility with SIEMs and other monitoring/alerting systems.
CIP-008-5 R1 Part 1.4	Cyber Security Incident Response Plan Specifications: Recovery	SD Card Backup, Local ATV configuration downloads, MDM software for configuration.	These ensure that the mGuard configuration can be easily recovered/restored in case of corruption and accidental or malicious modification.
CIP-008-5 R2 Part 2.3	Cyber Security Incident Response Plan: Implementation and Testing	Syslog, SNMP Trap, Firewall log info.	These artifacts can be sent and stored on a centralized server for later forensic analysis or incident review.
CIP-009-6 R1 Part 1.3	Recovery Plan Specifications: Backup and Storage	SD Card Backup, Local ATV configuration downloads, MDM software for configuration.	These allow for the mGuard (and its firewall rules, routing table, and VPN connections) to quickly be backed up/restored either via local means (e.g., via SD card) or via centralized management server (e.g., MDM or central configuration server). These backups can be "human readable" or encrypted for an additional layer of security.

Section	Description	mGuard Feature(s)	How it helps meet compliance
CIP-009-6 R1 Part 1.5	Recovery Plan Specifications: data preservation	Syslog, SNMP Trap, Firewall log info.	While not preserving user or application data per se, this allows for the capture and preservation of certain metadata, such as time stamp of configuration changes, authentication events, and source/destination and traffic information of logged firewall events.
CIP-010-2 R1 Part 1.1	Configuration Change Management	SD Card Backup, Local ATV configuration downloads, MDM software for configuration.	Both baseline and fully customized configurations can be stored in standard asset-management systems. Other configuration parsers, including Skybox and RedSeal, are supported and can be used to record original and modified mGuard configurations. MDM software provides a "history" report to show modifications to the configuration and when they were deployed.
CIP-011-2 R1 Part 1.2	Information Protection	Stateful and Deep Packet Inspection Firewalls for sensitive information at rest/use. Additional IPsec VPN and OpenVPN for information security while in transit.	The firewall functionality ensures the limiting of traffic through the mGuard. The VPN ensures the limiting of traffic but also provides a layer of encryption (up to AES-256) to protect the traffic from sniffing or man-in-the-middle attacks when data is in transit.

It is important to remember that mGuard features and functions are the ***tools*** that help your network achieve compliance; however, like all tools, they must be properly configured and utilized to realize these benefits. If you have any questions about any of the mGuard product lines, their capabilities and features, or how they relate to NERC-CIP compliance, please don't hesitate to contact me.

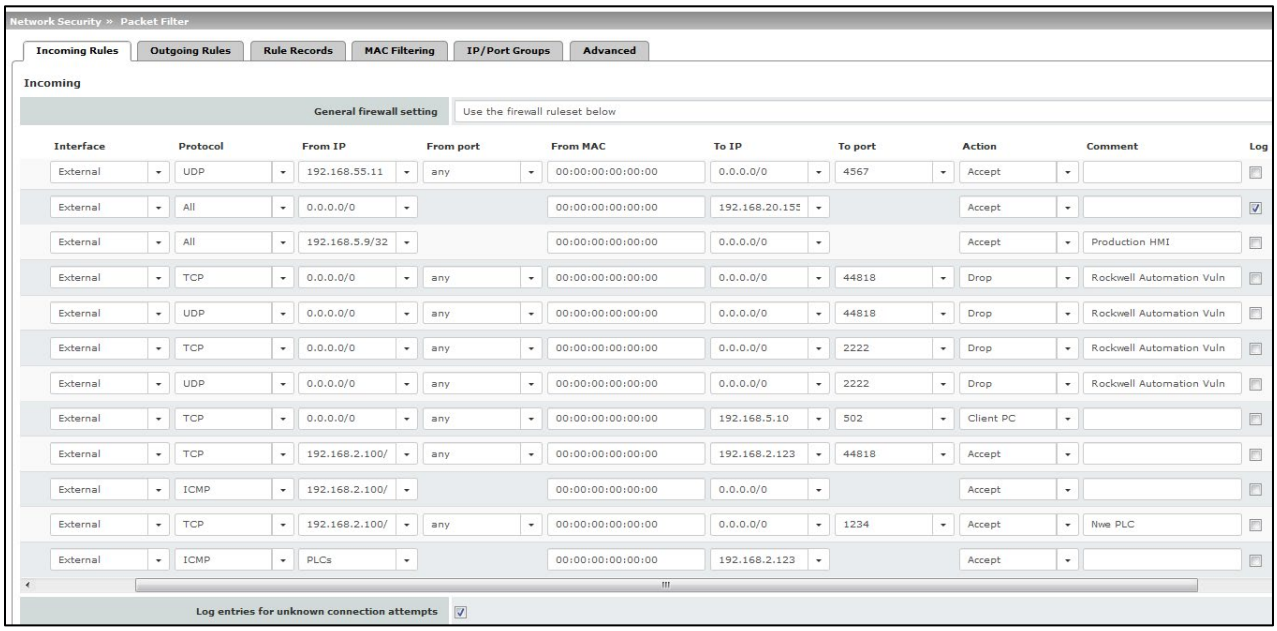
Sincerely,

Mariam Coladonato
Lead Product Marketing Specialist, Networking and Security

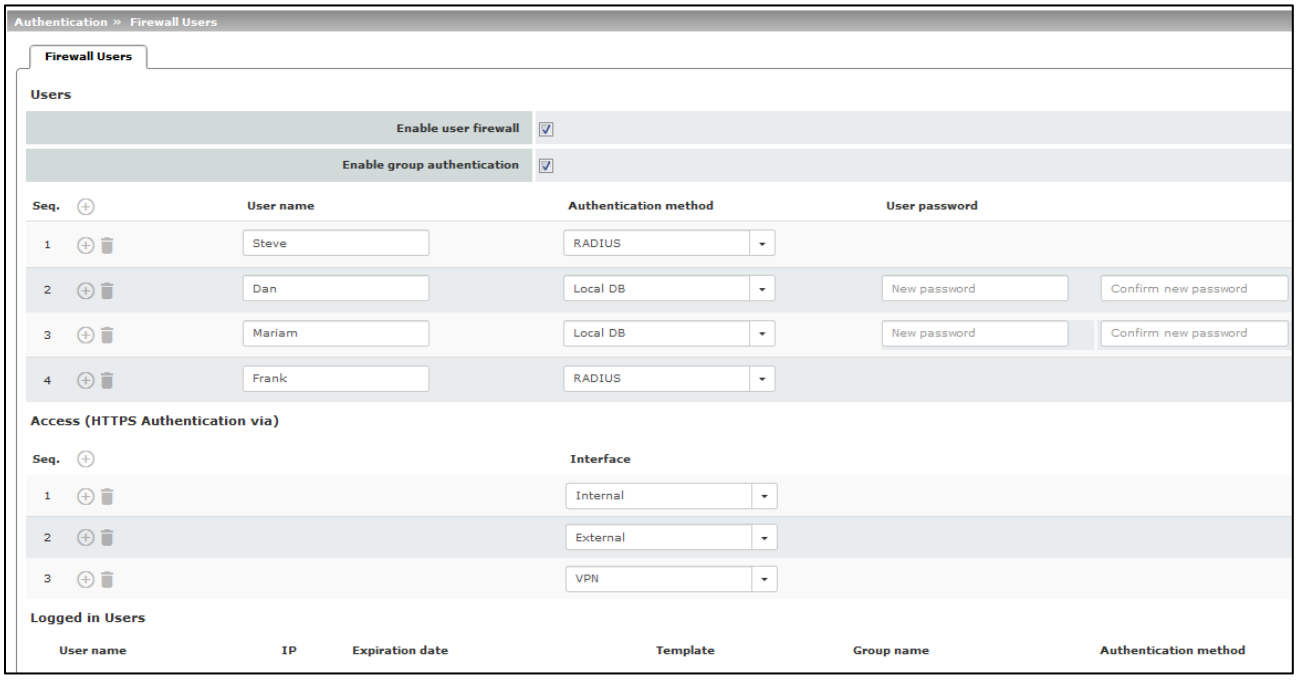
Appendix

Relevant screenshots of various mGuard configuration pages

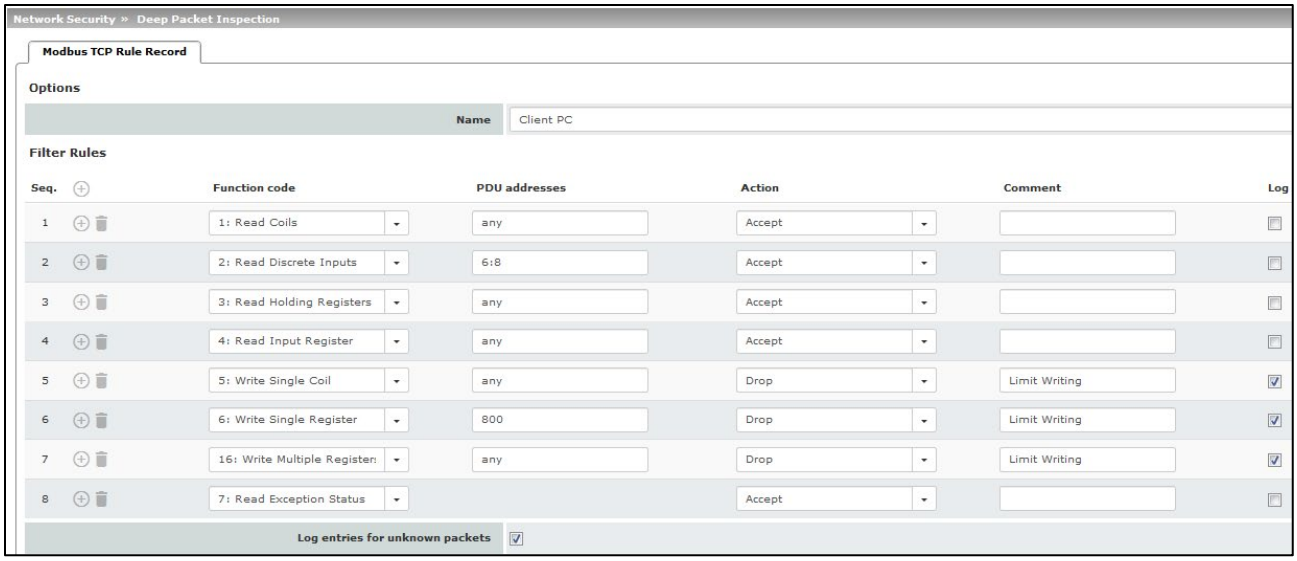
For easier understanding and reference, several screenshots of the above-described mGuard features are included here. Please note that all images used are taken on an mGuard RS4000 running firmware version 8.7 with the optional CIM and DPI licenses installed. Please contact the author, or a member of the Phoenix Contact Sales, Marketing, or Tech Support teams, for a deeper description.



Screenshot 1 – Stateful Inspection Firewall options, including protocol, src/dst IP, port, action, and logging. Implicit deny ensures that traffic not matching any rules gets dropped.



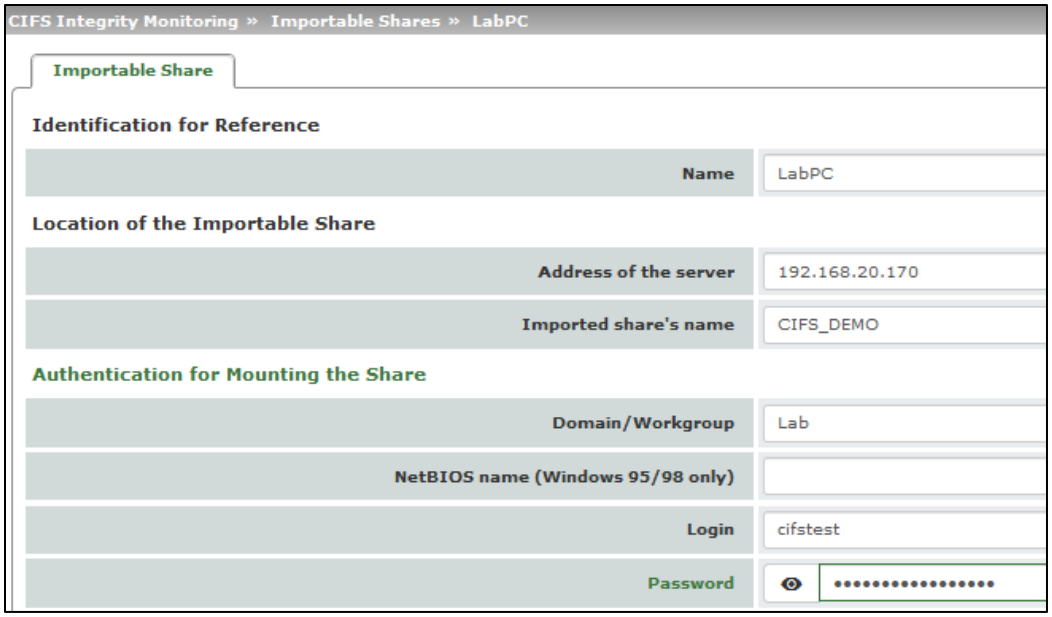
Screenshot 2 – User Firewall setup, including Local vs RADIUS authentication.



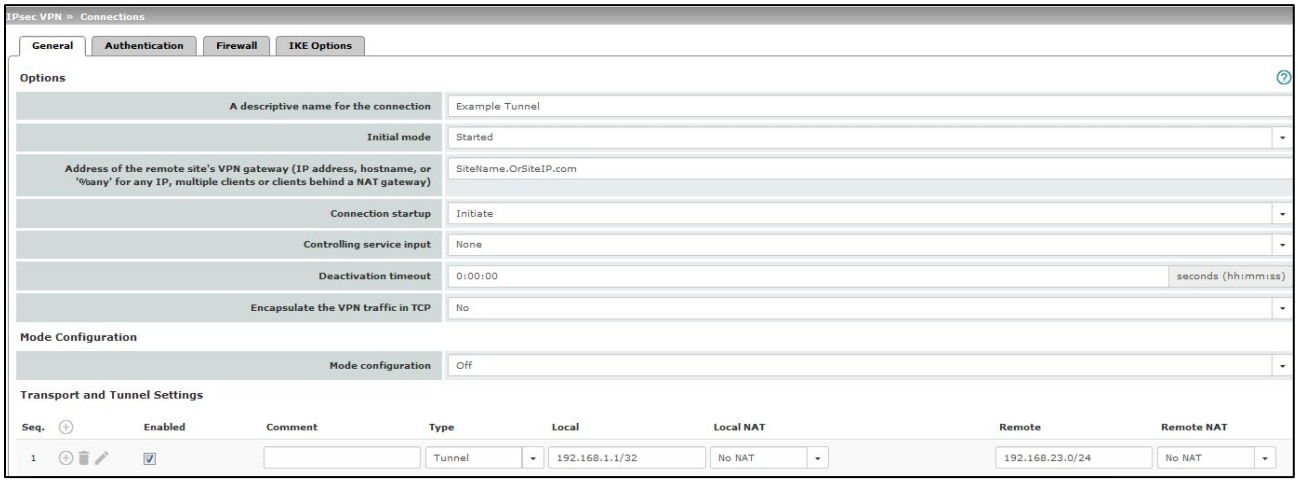
Screenshot 3 – Modbus/TCP DPI setup. Specify actions based on function code and coil/register address range. Optional logging for all traffic rules.

Screenshot 4 – RADIUS server configuration setup. Can to be used for firewall users and local Web GUI or SSH authentication.

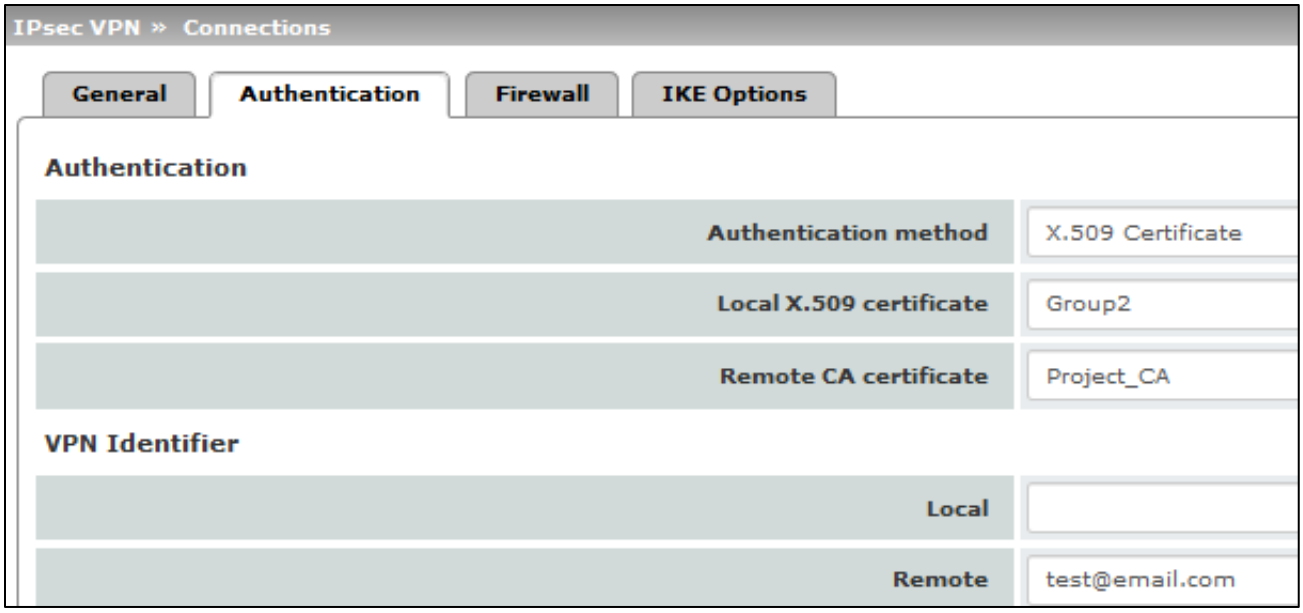
Screenshot 5 – CIFS Integrity Monitoring (CIM) main setup screen showing PC share and email notification setup.



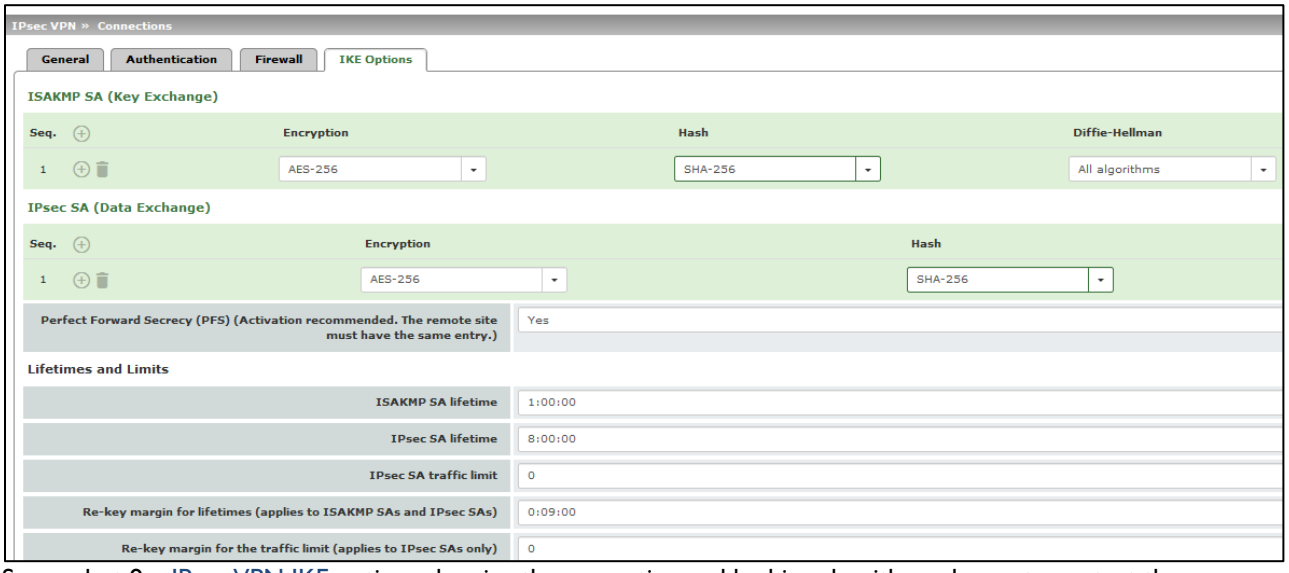
Screenshot 6 – CIM Share configuration, showing monitored PC's IP address and file system information.



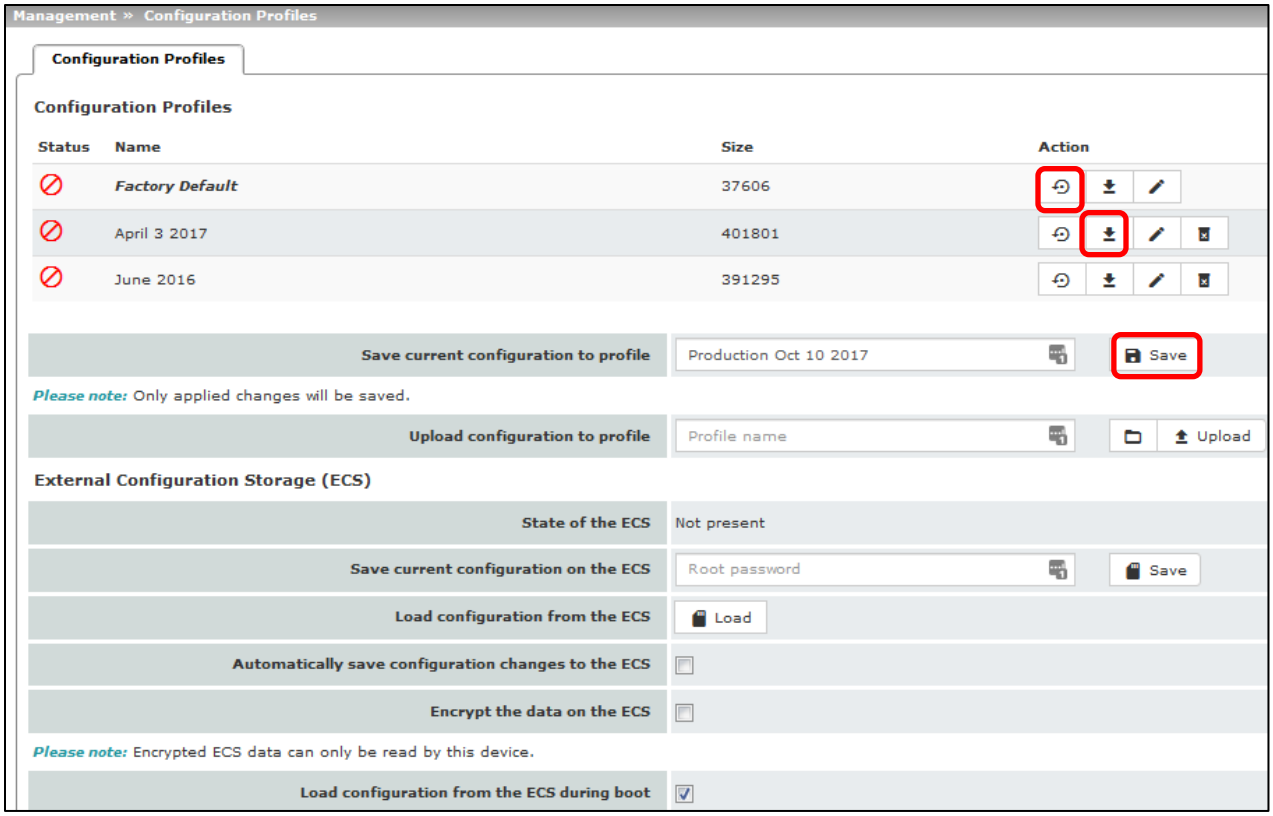
Screenshot 7 – Main IPsec VPN configuration screen showing Peer Address, default state, and participating network/IPs as well as Network Address Translation rules.



Screenshot 8 – IPsec VPN Authentication showing use of Local X.509 certificate and trusted signing CA certificate of VPN Peer.



Screenshot 9 – IPsec VPN IKE options showing the encryption and hashing algorithms chosen to protect the traffic. Also shown are rekeying and advanced configuration options.



Screenshot 10 – Configuration Profiles management page, showing the ability to activate/restore and download existing configurations. Also used to save the running parameters as a new saved config. Additional parameters for saving a configuration (encrypted or normally) to an SD memory card for backup.