CIP Version 5 Supports Unidirectional Security Gateways

Paul Feldman
Independent Director
MISO & WECC

Lior Frenkel
CEO and Co-Founder
Waterfall Security Solutions

May, 2013

Abstract
The NERC CIP Version 5 draft standard was recently submitted to FERC for approval. The submitted draft recognizes that Unidirectional Security Gateways provide security which is stronger than firewalls, and the draft includes measures to encourage the deployment of this strong security technology. The standard also changes how firewalls must be managed and mandates network intrusion detection systems as a second level of defense when control centers deploy firewalls.

Introduction
The electric power sector leads North American industry and the world in the implementation of strong, enforceable cyber-security standards. Both NEI and NRC standards in nuclear generation and the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards in the Bulk Electric System are seen as among the strongest cyber-security regimes enforced anywhere in the world. The NERC-CIP standards in particular are seen as a model of cyber security for other industries.

The NERC CIP Version 5 draft standard was recently submitted to FERC for approval. The submitted draft includes many changes, including significant changes to network perimeter protection rules. This article describes new perimeter protection rules and concepts, and explores new support in the draft standard for hardware-enforced Unidirectional Security Gateways.

Critical Assets vs. Asset Impact

The CIP standards are a set of documents numbered 002-009 in versions 1-4, and 002-011 in the V5 draft. Before any discussion of cyber-security protections begins, the standards all first define what equipment is in scope for the standard, in the CIP-002 rules.

CIP-002 V1-4 defined the concept of Critical Asset (CA) as a physical asset in the Bulk Electric System (BES), such as a generator or a substation, which was essential to the reliability of the BES. Cyber assets were computers, network devices, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs) or any other equipment with a CPU in it. Cyber assets which were essential to the operation of Critical Assets were candidates for classification as Critical Cyber Assets (CCAs).

A cyber asset became a Critical Cyber Asset only if the cyber asset met at least one of three criteria:

- The cyber asset was part of a BES Control Center – a site dispatching transmission or generation capacity - and the cyber asset used routable protocols, such as the Internet Protocol (IP) or Transmission Control Protocol (TCP),
- The cyber asset was dial-up accessible, or
- The cyber asset used a routable protocol to communicate through an Electronic Security Perimeter (ESP).

The CIP standards recognize that BES Control Centers are key targets for malware or for adversaries bent on damaging the power grid. While the term "Control Center" was not strictly defined in the CIP V1-V4 standards, the term is generally understood to mean a site which dispatches generation at multiple sites, or dispatches transmission resources at multiple substations. In particular, a generator control room is almost never a BES Control Center.

In addition, the standards recognize that cyber assets are at greater risk of attack if they are connected to public switched telephone networks, or if those assets can be reached directly or indirectly by IP communications.

In the new, draft, CIP V5 standards, CIP-002 V5 replaces the concept of CCA with that of High-Impact, Medium-Impact and Low-Impact BES Cyber Systems. High-Impact systems are sets of cyber assets essential to the operation of BES Control Centers. Medium-Impact systems are pretty much

all other cyber systems that were called Critical Cyber Assets in the V1-V4 standards.

A key difference between the V1-4 and V5 standards is that in the V5 standards, communications characteristics are no longer part of determining what "impact" level to assign to BES cyber assets. Impact is assessed purely by whether and how the cyber assets can affect the reliable operation of the BES.

Network Intrusion Detection Systems

A second important change in the V5 standards is the requirement for network intrusion detection systems at BES Control Centers. The 2008 FERC "Order 706" indicated that firewalls alone are not strong enough security to ensure the reliability of BES Control Centers. The order required NERC to create rules for a second level of defense for when firewalls are breached. CIP-005 V5 specifies network perimeter protections and requirement R1.5 requires some sort of network intrusion detection system or application-layer firewall implemented as a second level of defense behind vulnerable firewalls.

This is a significant expense for BES Control Centers, since intrusion detection systems are worthless unless someone monitors the alert stream. When alerts are raised, each alert must be investigated to determine whether it represents a real intrusion, or represents a "false alarm" – eg: an alarm due to benign traffic accidentally matching some signature and triggering an alert. On-going labor costs for monitoring and false-alarm investigation costs generally dwarf firewall and intrusion detection purchase costs.

Remote Access Protections

CIP-005 V5 contains new requirements for remote access systems as well. Remote access systems are any systems by which an external user can initiate access to a BES Cyber System. CIP-005 V5 R2.1 requires intermediate "jump hosts" for all remote access. The workstation or laptop initiating the remote access is not permitted to log into BES Cyber Assets directly, but must log into an intermediate system instead. This system may be a separate Windows Terminal Server or Linux "ssh" server, so long as the jump host is not itself a cyber asset essential to the reliability of the BES.

Other new rules in the CIP-005 V5 remote access standards are rules requiring that remote access traffic be encrypted, and that two-factor authentication be used to control access to jump hosts.

External Routable Connectivity

Very nearly all of the V5 CIP-005 perimeter protection provisions though, apply only to BES Cyber Systems with External Routable Connectivity (ERC). While routable communications are no longer used as a criterion for determining what impact BES Cyber Systems have on the reliability of the BES, the concept of routable communications is still important to the V5 standards.

CIP V5 defines External Routable Connectivity as:

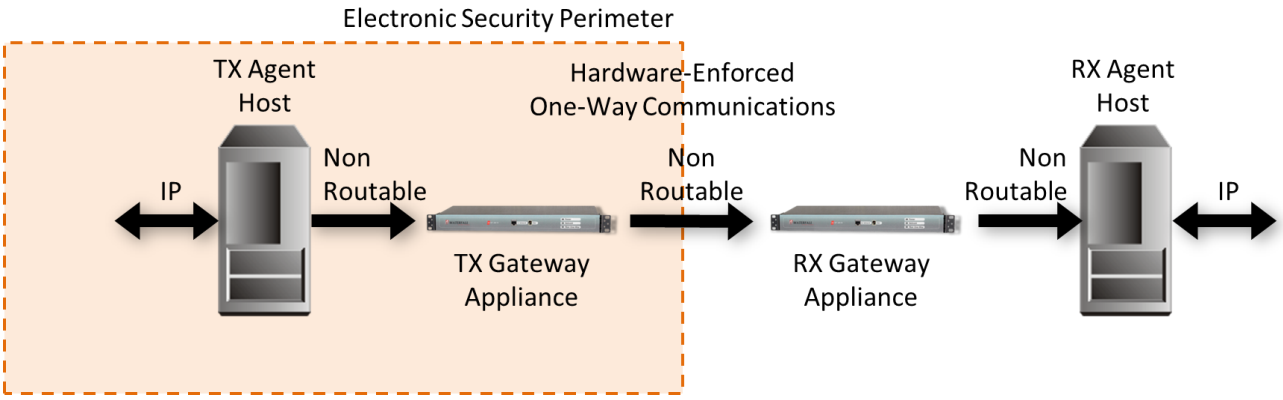
> *"The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."*

Fully 37 out of 103 requirements and sub-requirements in the CIP V5 standard, including nearly all of the CIP-005 perimeter protection rules, apply only to Cyber Systems with External Routable Connectivity. Systems without such connectivity are exempt from these 37 requirements.

This, in the V5 standards, routable connectivity is no longer used to classify BES Cyber Systems or cyber assets as to their impact on the BES, but routable connectivity is still important. Cyber Systems with no routable connectivity are still seen as representing a lower risk than assets with External Routable Connectivity, and so assets without ERC are required to comply with only 66 of the 103 requirements in the standard.

Unidirectional Security Gateways

There is a word that is easy to miss in the definition of External Routable Connectivity and that word is "bi-directional." The word is entirely new in the CIP V5 standards – the word did not appear at all in versions 1-4 of the standards. What does "bi-directional" mean in this definition?



The Hardware/Software Unidirectional Security Gateway Solution

When members of the CIP V5 drafting team are asked this question, they respond that the term refers to hardware-enforced unidirectional communications equipment, more commonly called Unidirectional Security Gateways. The drafting team reports that these gateways are being deployed widely in the BES and provide much stronger security than firewalls are able to. The team deliberately inserted the word "bi-directional" into the definition of ERC in order to encourage the use of these gateways in protecting BES Cyber Systems.

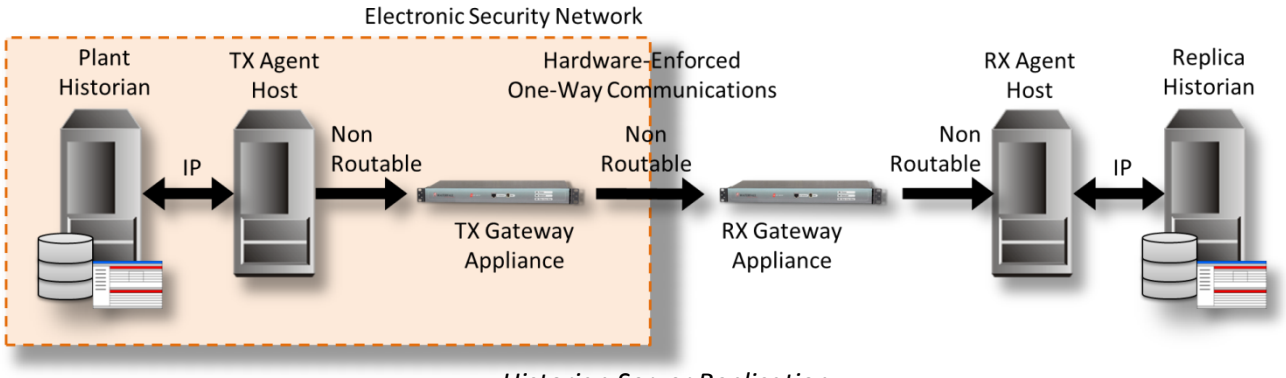
Communications are External Routable Communications only if those communications are bi-directional, and communications through Unidirectional Security Gateways are strictly unidirectional. As a result, BES Cyber Systems protected by Unidirectional Security Gateways are exempt from the 37 requirements and sub-requirements that apply only to Cyber Systems with External Routable Connectivity. With fewer rules to follow for equipment protected by Unidirectional Gateways, deploying the gateways reduces the cost of V5 CIP compliance programs.

How do the gateways work? Security practitioners not familiar with the gateways might initially be confused by the new "bi-directional" term in the V5 standard. Some practitioners regard TCP connections as "unidirectional outbound" for example, if those connections are initiated inside the ESP, and if they exist primarily to send data out of the ESP into external systems.

However, such connections are not truly unidirectional. TCP/IP is a bi-directional transport and application protocols such as HTTP, OPC-UA, Modbus and DNP3 are all bi-directional at the application layer on top of the TCP transport. These protocols all issue queries, commands and poll commands to servers and devices, and receive responses from those systems. Bi-directional communications cannot simply send data out of an ESP. Every bi-directional communications channel through a firewall at an ESP exposes the source BES Cyber System to attack as well, through that same communications channel. With a pair of bi-directionally communicating systems, either system can launch attacks at the other.

The CIP V5 definition of ERC refers to bi-directional communications in the sense of being the opposite of truly unidirectional communications. Truly unidirectional communications is hardware-enforced. A common design for hardware-enforced Unidirectional Gateways uses two network appliances: the transmit (TX) appliance contains a fiber-optic laser, and the receive (RX) appliance contains a fiber-optic receiver. The two appliances are joined by a fiber-optic cable. The appliances are oriented so that they can send information out of an ESP-protected network without exposing the protected Cyber Systems to any kind of attack at all.

Unidirectional Gateways are not just hardware though. The gateways are a combination of hardware and software. The unidirectional hardware provides security, making it impossible for any system on an external network to attack the protected systems. The gateway software replicates



Historian Server Replication

industrial servers, making the total gateway solution a plug-and-play replacement for firewalls.

Take for example a generating plant historian replicated to a business network. The gateway software takes the form of a transmit (TX) agent and a receive (RX) agent, each running on a conventional Windows or Linux computer. The TX agent connects to the plant historian using conventional communications protocols, and queries the plant historian for data. The TX agent sends that data to the RX agent via the TX and RX hardware appliances.

The RX agent receives the data and establishes a conventional connection to a historian on the external business network. The RX agent instructs this replica historian on the business network to store the historical data received from the TX agent. The replica historian, now populated with data, is available for users and applications on the business network to use when they need access to plant data.

The replica historian is maintained by the gateway solution as a faithful replica of the plant historian. The replica has all of the historical data, back to "the beginning of time," and it has all of the latest data, less than a second old. Business users generally think they are still connected directly to the plant historian.

That is, they think they are connected to the plant historian until a virus infects the business network and affects the replica historian. Corporate IT deals with the virus, rebuilds the historian machine from clean media, restores the historical database from business-network backups, and presses a few buttons on the TX agent user interface to resend the last day of historical data, and so fill in any gaps in the replica historian's records.

The whole time the infection and clean-up were under way, the plant historian and plant systems are completely unaware of whatever havoc might be wrought on the business network. No signal can pass back from the RX gateway hardware to the TX gateway hardware - there is after all no laser in the RX gateway, and no fiber-optic receiver in the TX gateway. The hardware is unable to send any signal at all back into the protected network.

When Unidirectional Security Gateways are the only communications configured between a protected BES Cyber System and an external network, the gateways provide absolute protection from attacks originating on external networks. The gateways eliminate the online attack threat vector entirely. Other parts of the CIP standard are still needed in order to deal with other threat vectors, but security practitioners no longer need spend any time or mind-share dealing with the risk of network-based attacks from the business network.

Making the World a Safer Place

Unidirectional Security Gateways are being deployed widely in the BES, especially in power generation applications. The strong security provided by these gateways is being recognized by steadily increasing numbers of security practitioners over time. For example, at a recent cyber-security conference Tim Roxey, the CSO of the NERC ES-ISAC, was heard to observe:

> *"When you are considering security for your control networks, you need to keep in mind innovative security technologies such as unidirectional gateways."*

Later in his address, Mr. Roxey repeated his encouragement to entities to "*embrace the technology.*"

A variety of industry market analysts are advising their clients to become familiar with the gateway technology. Unidirectional Security Gateways are a technology whose time has come - industrial security practitioners should all be familiar with the technology, with where it fits, where it does not fit, and with truly unidirectional approaches to remote support and other apparently bi-directional problems.

Other industries are taking note as well - water and wastewater utilities, chemical plants and oil & gas production and refining operations in particular. The Bulk Electric System and the world at large are becoming measurably safer, more secure and more reliable as a result of the widespread deployment of Unidirectional Security Gateways.

Paul Feldman is an experienced executive in the technology, telecommunica-tions, and energy industries. Mr. Feldman is a director and past chairman of the MISO, where he chairs the System Planning Committee He is also an independent director at WECC where is the chair of the Compliance Committee the Compliance Hearing Body and as a member of the Governance committee.

Lior Frenkel is the CEO and Co-Founder of Waterfall Security Solutions. Waterfall is the recognized market leader for Unidirectional Security Gateways and for the secure integration of industrial control systems with business systems. Please feel free to contact Waterfall directly for additional information on this topic or on any topic related to Unidirectional Gateways at any of +1-212-714-6058, info@waterfall-security.com or http://www.waterfall-security.com