SANS

Analyst Program

Product Review

Let's Get Serious: Protecting Industrial Control Systems Is Mission-Critical

Written by **Dean Parsons**

October 2022

SIEMENS

Today's ICS Threat Landscape

Cyber attackers are targeting critical infrastructure, industrial control systems (ICSs), and operating technology (OT) environments. Adversaries have developed and deployed ICS-capable attack tools to gain access via network or other vectors, giving them the potential to impact engineering operations and safety.

The good news is ICS defense is doable, even in the face of modern ICS attack tactics and techniques. Today's adversaries are able to pit existing legitimate engineering systems and applications, such as human-machine interfaces (HMIs) and engineering workstations, against the control system itself. Doing so means attackers have to bring less toolkits into a victim environment and perform less custom. Defenders therefore need more than endpoint-only technologies to protect OT devices running traditional operating systems such as Windows, Linux, and Unix. Network architecture and network firewall controls are required. Effective technologies that defend against network lateral movement and the pre-positioning of attack tools have the advantages of controlling all network traffic and can also assist with incident response.

Although the Siemens SCALANCE SC600 series does not attempt to be a full-blown next-generation firewall (NGFW) that can handle an organization's edge traffic to and from the internet, it is well suited for minor enforcement boundary security and cell protection in accordance with the SANS ICS410 SCADA reference architecture.[1] Once SCALANCE S firewalls are in place to segment the network and securely route traffic, security programs can leverage the Siemens Network Management System (SINEC NMS) to centrally manage them, as well as Siemens SIBERprotect to move further toward the active defense posture on the sliding scale of cybersecurity.[2]

Our testing found the SIEMENS SCALANCE S Industrial Firewall Appliances to be very flexible and capable in their ability to segment and control traffic to protect ICS networks, even starting with a previously unsegmented, or flat, network.

The Siemens SCALANCE S family of industrial appliances is commonly relied on for ICS network security in industries such as oil and gas, transportation, automotive, electric power distribution, and others. For example, the appliances can be deployed at water management sites for remote monitoring and control of pumping stations, in critical manufacturing to provide remote third-party access for monitoring of equipment, and in chemical facilities for protecting and controlling traffic in engineering network zones located in potentially hazardous environments.

This paper explores how SCALANCE S Industrial Security Appliances can protect against security challenges and assist with ICS network segmentation, asset protection, access control, and stateful packet inspection (SPI) for traffic control.

[1] ICS410: ICS/SCADA Security Essentials registration, SANS Institute, www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

[2] "The Sliding Scale of Cyber Security," SANS Institute, September 1, 2015, www.sans.org/white-papers/36240

Lessons Learned

ICS Ransomware: How Industrial Firewalls Can Help

The EKANS[3] ransomware targets ICS Windows domain controllers, disables host-based endpoint protections, encrypts files, and works from its kill-list to forcibly stop engineering applications running on traditional endpoint operating systems. EKANS has been used against several industrial sectors, causing significant operational disruptions in production networks at companies including Honda and European energy company Enel Group.[4]

ICS firewalls can enforce access control lists, ensure segmentation, assist with incident response containment efforts at network boundaries, and detect the pre-positioning of these types of attacks from a network perspective before endpoint systems are compromised. Additionally, weak network security configurations can be hardened for zone or cell network segmentation.

The Oldsmar Water Facility Hack: Why Secure Remote Access Is Best

In 2021, an adversary obtained unauthorized remote access to the HMI at a drinking water facility in Oldsmar, Florida.[5] The weak configuration of remote network access from the internet to the control systems allowed the attacker to change the engineering settings of the production facility, altering the acidity of the water so that it was toxic to humans. Fortunately, the change was noticed by the engineering staff as part of an ICS incident response effort and they were able to correct the acidity of the water immediately.

In a security advisory regarding the event, the Cyber Security and Infrastructure Security Agency (CISA) cited several security practices for ICSs including the use of multiple-factor authentication to enable secure remote access, the auditing of network connections, and the isolation of vulnerable systems, which can be achieved with ICS firewalls.[6]

What Can Be Done?

Organizations can detect and improve response to such threats or stop them in their tracks by having a strong network architecture. Good network architecture is the necessary foundation for any technologies or processes that are subsequently deployed. For example, a segmented ICS network will perform better than a flat one during the containment phase of responding to a DDoS attack, network-based transient device contaminants, or malware propagating on a network.

---

[3] "This is how EKANS ransomware is targeting industrial control systems," ZDNet, July 2, 2020, www.zdnet.com/article/this-is-how-ekans-ransomware-is-targeting-industrial-control-systems

[4] "Honda and Enel impacted by cyber attack suspected to be ransomware," Malwarebytes, June 9, 2020, www.malwarebytes.com/blog/news/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware

[5] "ICS Hot Take: Oldsmar, FL Water Facility Event," SANS Institute, February 25, 2021, www.sans.org/blog/ics-hot-take-oldsmar-fl-water-facility-event

[6] Alert (AA21-042A), "Compromise of U.S. Water Treatment Facility," Cybersecurity & Infrastructure Security Agency, February 12, 2021, www.cisa.gov/uscert/ncas/alerts/aa21-042a

ICS Network Security and Scalance S Appliances

Deployment in Multiple Sectors

The Siemens SCALANCE S Industrial Security Appliances seek to address ICS network challenges through network segmentation, SPI firewall capabilities, and flexible security features that scale for management across sites, while integrating with ICS network network architectures—even a flat control network, because SCALANCE S Industrial Security Appliances will provide the needed segmentation.

The devices can be deployed by an organization in any ICS sector by either building a new network or adding security to an existing network that aligns with the Purdue Enterprise Reference Architecture.[7]

SECURITY PRO TIP

The Purdue Enterprise Reference Architecture has six logical levels to organize ICS assets. Level 5 references the internet and cloud services; Level 4 is for enterprise IT business networks and systems; Level 3 is for an ICS plant-wide site and SCADA controls; Level 2 refers to HMIs and engineering workstations; Level 1 is for process control elements, programmable logic controllers (PLCs), and field devices; and Level 0 is sensors and hardware actuators. Levels 2, 1, and 0 can be implemented in their own cells or in separated zones specifically for a part of an engineering process.

Network Fortification: Minor Enforcement Boundaries and Cell Protection

We mapped the Purdue levels to the SANS ICS410 SCADA architecture reference model to determine where the SCALANCE S devices would be best suited.

We found the SC600 devices are better suited for lower levels of the control network than for use as an internet firewall or between a corporate environment and the industrial environment. Those positions require NGFWs with full deep packet inspection (DPI); Siemens has several partners to help it meet these use cases.[8] The SCALANCE S devices are suited as firewalls in ICS networks at minor enforcement boundaries, say between Purdue Level 3 and Level 2, and for cell protection, as shown in Figure 1.

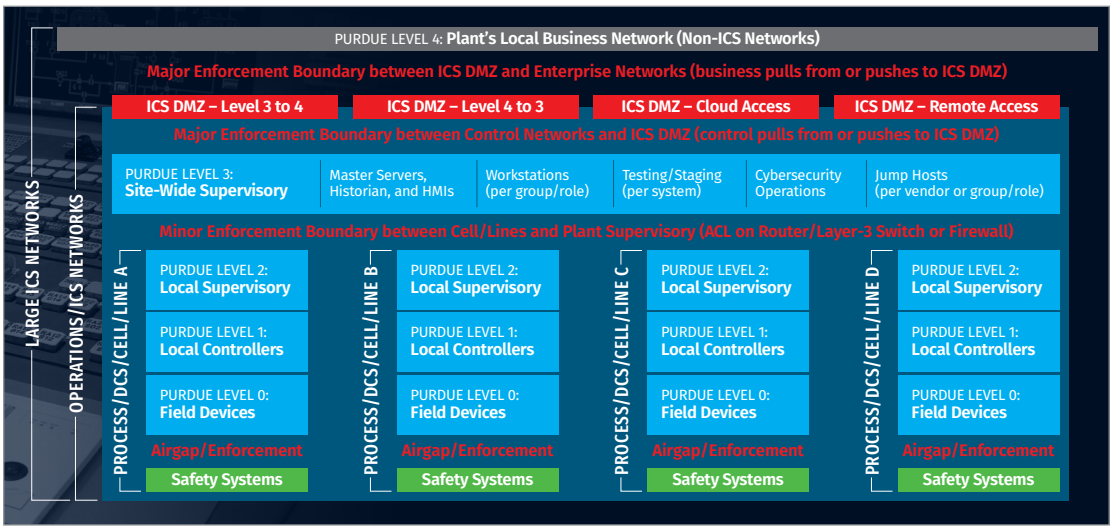

Figure 1. SANS ICS410 SCADA Reference Architecture – Major, Minor and Cells[9]

[7] Purdue Enterprise Reference Architecture, Wikipedia, https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

[8] Siemens NGFW and DPI options, https://new.siemens.com/global/en/products/automation/industrial-communication/rugged-communications/technology-highlights/cybersecurity.html

[9] ICS410: ICS/SCADA Security Essentials registration, SANS Institute, www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

Figure 2. SCALANCE S Devices

Exploring the SCALANCE SC646-2C In Depth

There are several variations of the SCALANCE S devices (see Figure 2).

We've focused this product review on the SC646-2C (see Figure 3),[10] which falls in line with security recommendations from IEC-62443.

The SCALANCE family of interoperable devices includes the SCALANCE X Industrial Ethernet Switches and Routers,[11] SCALANCE M Mobile Industrial Routers, and SCALANCE W Industrial Wireless LAN,[12] but those are all out of the scope of this review.

The SC646-2C is multifaceted. It can be configured as a network routing device or a bridged firewall. It can participate fully as an IP-based SPI industrial firewall to inspect both the egress and ingress of network traffic. For example, with the SPI firewall features turned on, we increased security in our lab by setting the device to make access control decisions based on rulesets that inspect the 5-tuple network data (source IP address, destination IP address, source port, destination port, and protocol) of any IP-based connection it sees.

Figure 3. The SCALANCE SC646-2C Industrial Security Appliance

[10] IEC-62443, Wikipedia, https://en.wikipedia.org/wiki/IEC_62443

[11] Siemens industrial Ethernet switches, https://new.Siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/industrial-ethernet-switches-scalance-x.html

[12] SCALANCE W770 access points and W730 client modules, https://new.Siemens.com/global/en/products/automation/industrial-communication/industrial-wireless-lan/scalance-w770-access-point-scalance-w730-client-module.html

Partially simulated in our lab with the SC646-2C, a defendable network was architected using the SCALANCE SC646-2C, M, and X devices (see Figure 4).

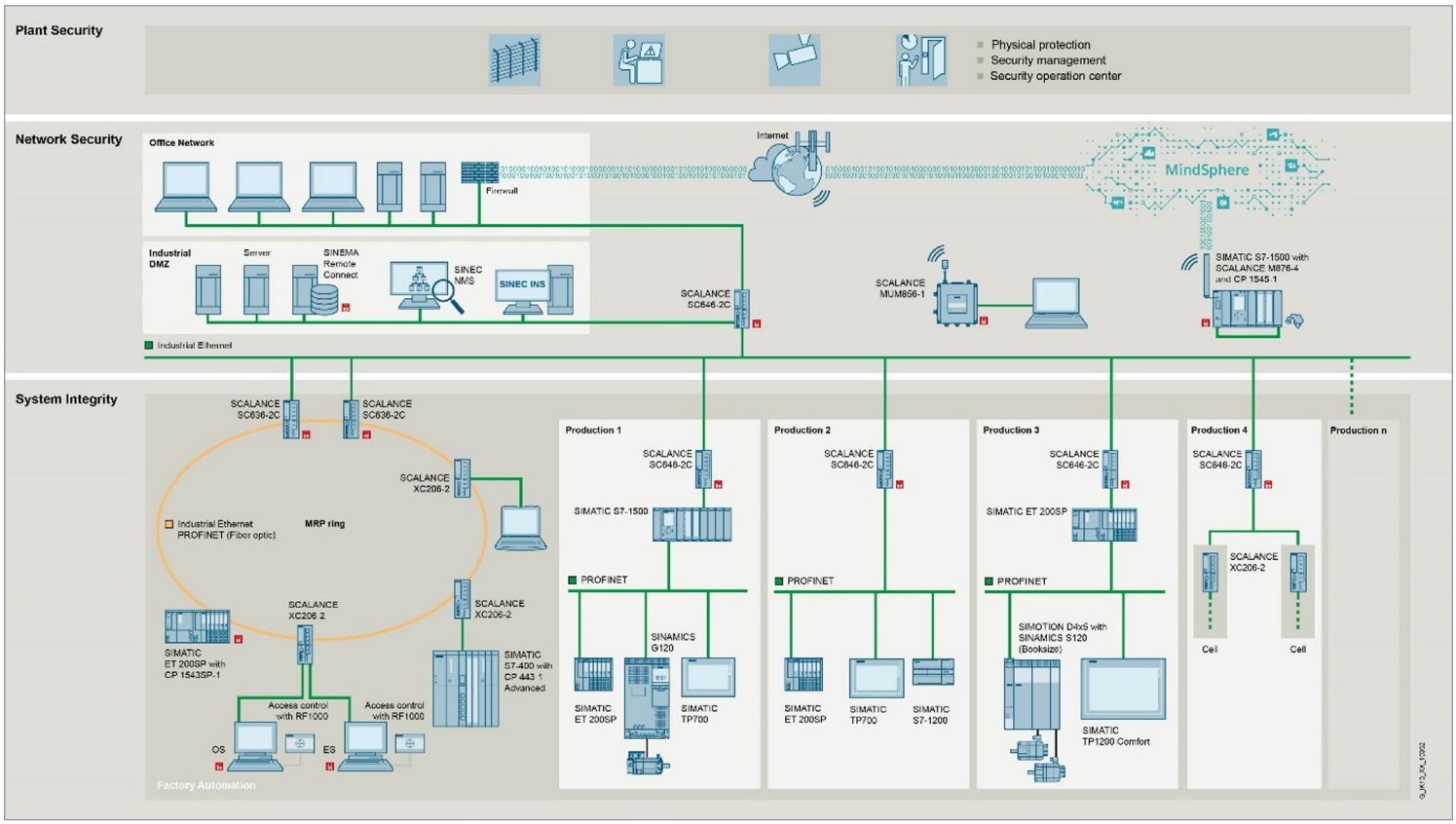

Figure 4. SCALANCE S, M, and X Devices Deployed for a Holistic View of Network Security

Notice that the SCALANCE SC646-2C protects engineering cells Production 1, Production 2, and Production 3. This would be a common deployment for most organizations to secure traffic to or from a cell while also protecting internal communications. For internal communications, we could allow and protect specific protocols, such as Profinet and S7, between devices such as the SIMATIC TP1200 and TP700 panel HMIs, the SIMATIC S7-1200 controllers, and the SIMATIC ET 200SP input/output modules.

SC646-2C Operating Environment

The SCALANCE X, M, W, and S device family is ruggedized for use in industrial settings such as assembly plants, mining operations, mills, foundries, power generation facilities, refineries, and manufacturing plants. It has physical port security using RJ45 Port Locks (see Figure 5).

Figure 5. SCALANCE SC646-2C with Key-Entry RJ45 Port Locks

It has an ambient operating temperature range of -40 to 70 °C (-40 to 158°F) and approval for operation in hazardous zones specified by EN 60079-0: 2006, EN60079-15: 2005, II 3 G Ex nA IIC T4 Gc, and KEMA 07ATEX0145 X. See Figure 6 for layout and interfaces.

Standard Security Features

Our review checked all features, including User-Specific Security, MAC-Based Security, and Bridged Mode, but we focused mostly on what we considered the main security feature, IP-Based Security.

While not being a full DPI-capable device, the SCALANCE SC646-2C does extend the features of a basic IP-only firewall by checking additional connection information with its IP-Based Security SPI capabilities. The SC646 SPI feature maintains a dynamic status table of connections to pass only what is explicitly allowed to pass through the appliance. We established a controllable enforcement boundary to protect sensitive or vulnerable assets behind the appliance, where SPI features allow only valid and specified connections based on IP address, MAC address, communication protocols, and ports, configured through the web-based management (WBM) interface or command-line interface (CLI) firewall rules.

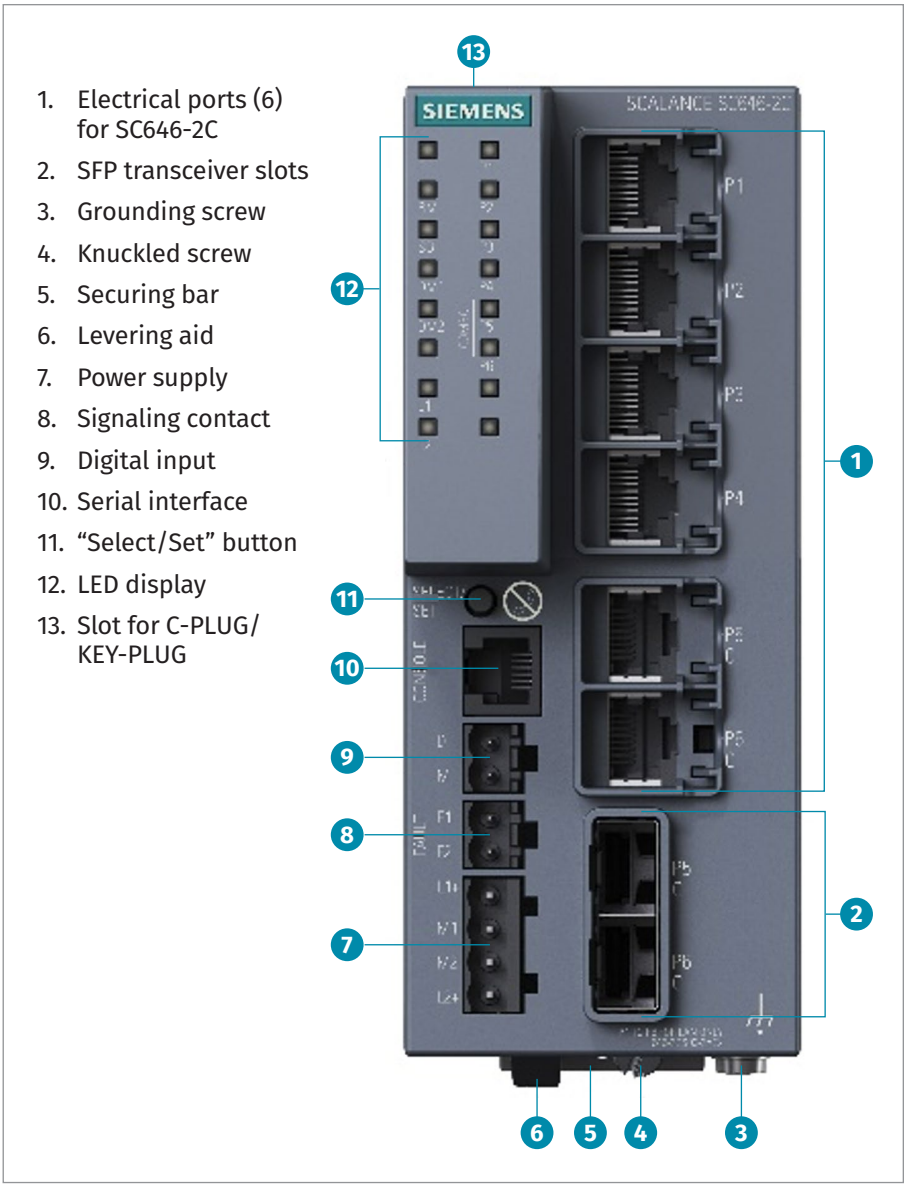

Figure 6. SCALANCE SC646-2C Layout and Interfaces

User Interfaces

We used the web-based management (WBM) user interface through a browser. Upon logging in with administration access, users are presented with the start page, which illustrates basic device status for easy reference: system name, device type, power line status, and fault status, if any (see Figure 7).

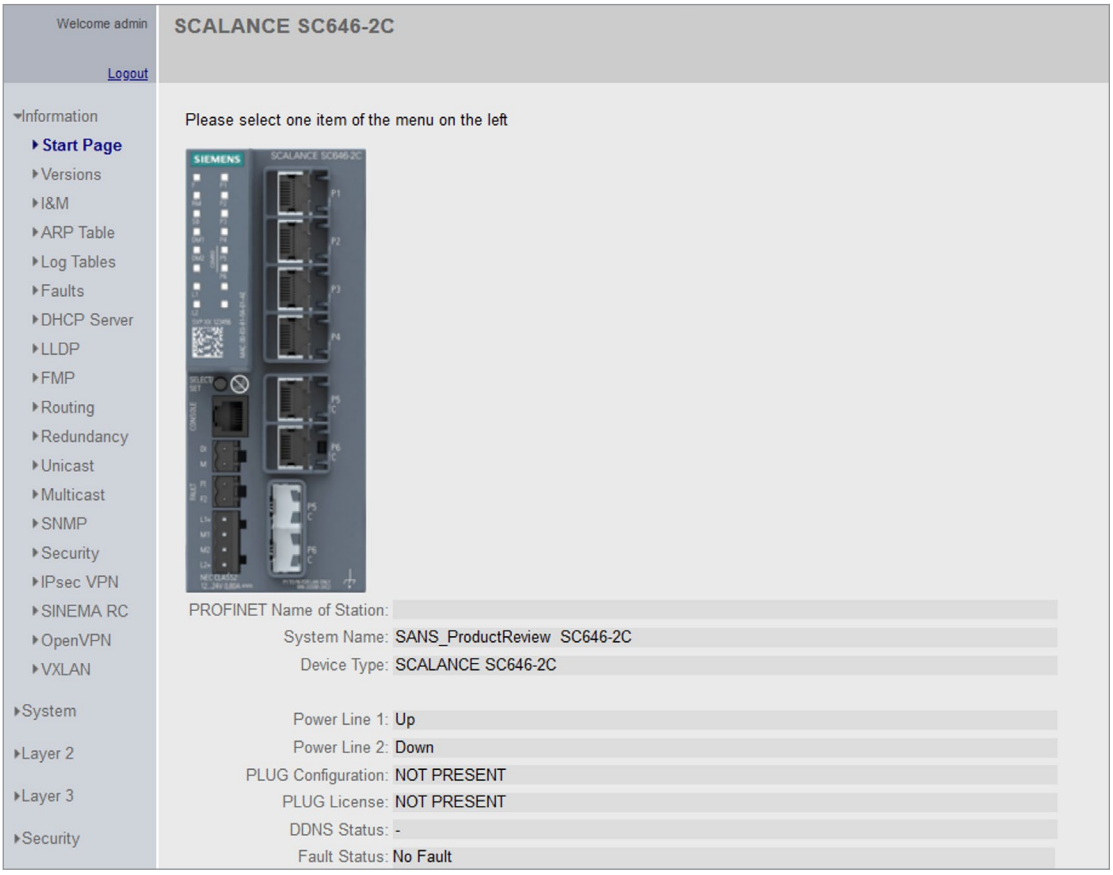

Figure 7. SC646-2C Start Page

A command line interface (CLI) is also available for device administration, configuration changes, and device management. It has modes for various levels of access rights to different groups of commands. For example, administrators would probably use the CLI for "Privileged EXEC" mode, especially when local physical access is possible; it allows them to display or change configuration data. The "Global Configuration" mode does not provide as much access but allows for making basic changes. It is important to note that we found both the CLI and WBM interface to be fully functional; all the configuration settings for the device can be made through either the CLI or WBM interface.

SC646-2C Users, Roles, and Hardening

The Siemens product documentation provides excellent guidance on system setup, hardening, and industry security practices that should be considered by administrators prior to production. If administrators want to follow the NIST advice to use passphrases rather than passwords[13] or if they have to meet long-password specifications, the SC646-2C password policy allows up to 128 characters.

We established several accounts for various individual roles. For example, "SecurityTest" is a general account for reviewing the interface and settings and provides just a read-only view, "ICS_IncidentResponse" is for ICS/OT security team members to conduct log analysis during incident response cases and provides no access to change configurations, and "EngineeringOperator" is for checking firmware versions and planning device updates in scheduling maintenance windows. We also set up an account called "Backup" for checking the system configuration and monitoring for configuration changes. We gave a long passphrase to the admin account, the only one with access to all device configuration for making changes. All of our accounts and roles are shown in Figure 8.

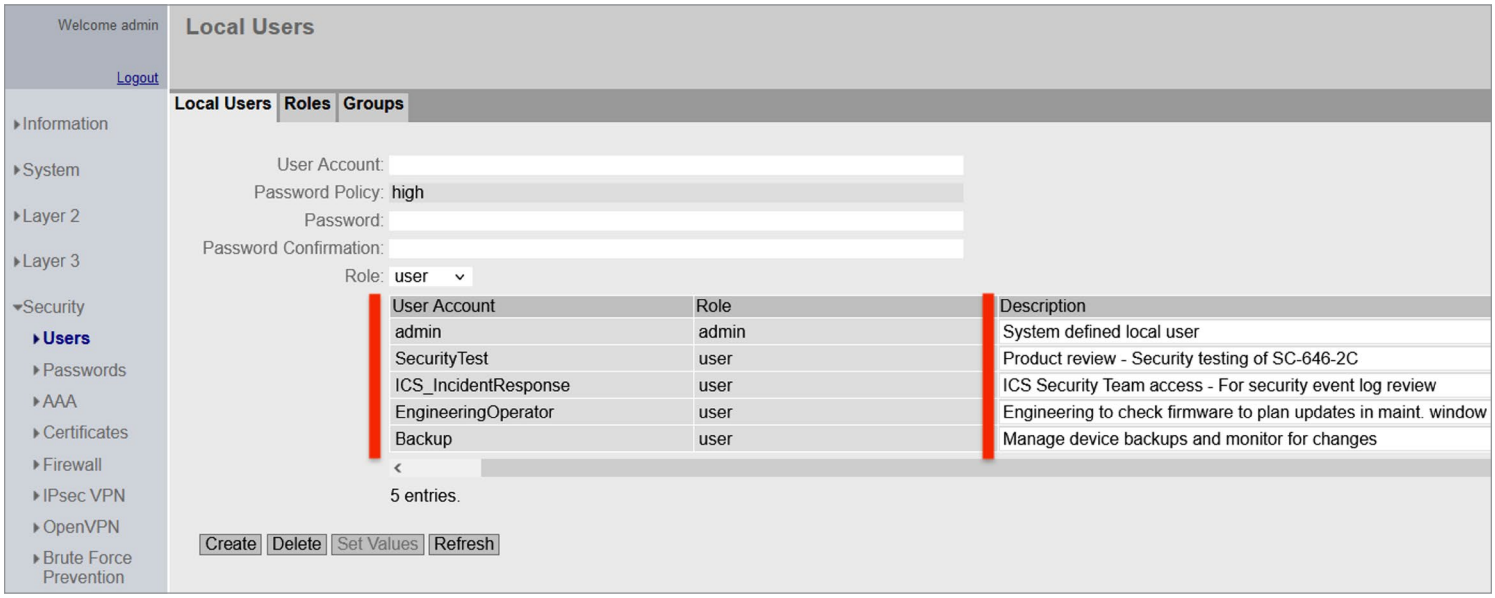

Figure 8. Accounts for a Variety of Tasks

In creating roles, we considered how to best set up function rights for access control. Function Right 1 provides general read-only administration to users who should be able to read device parameters but not change them. At the other extreme, Function Right 15 grants full administration capabilities to users who need to both read and change device parameters. We experimented with Function Right 0, for users who cannot be authenticated and therefore must be denied access to a device. Because the admin account is used for all major changes, it was given Function Right 15, and the newly created "SecurityReviewTest" role was set up with Function Right 1, allowing new users to manage their tasks.

[13] "NIST Has Spoken - Death to Complexity, Long Live the Passphrase!" SANS Institute blog, July 27, 2017, www.sans.org/blog/nist-has-spoken-death-to-complexity-long-live-the-passphrase

An item of note is the device protection features help devices to protect themselves. We tested the "Brute Force Prevention" feature on several of our accounts and reviewed the related events in the logs, shown in Figures 9 and 10.

User Specific BFP:

User	Failed Logins	Last Failed[s]	Blocked[s]	Clear
Unknown User	6	1444	not blocked	Clear
admin	0	0	not blocked	Clear
SecurityTest	0	0	not blocked	Clear
ICS_IncidentRespon:	11	1357	not blocked	Clear
EngineeringOperator	0	0	not blocked	Clear
Backup	5	1408	not blocked	Clear

6 entries.

Figure 9. "Brute Force Prevention" Log

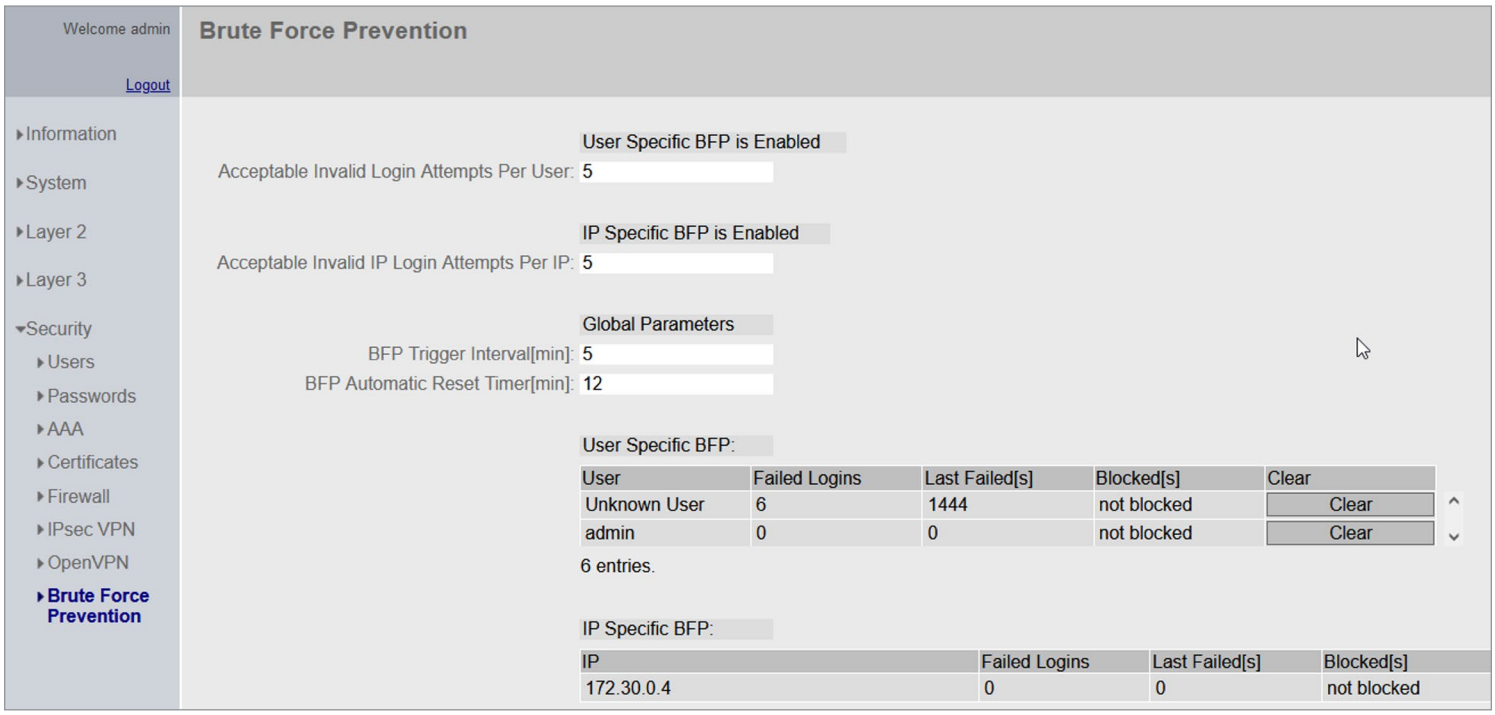

Figure 10. "Brute Force Prevention" Settings

The settings shown, such as "Acceptable Invalid Login Attempts" and "Brute Force Prevention Trigger Interval" are configurable and can be applied at the account or the IP address level.

Firewall Mode Activation

Establishing foundational security rules is straightforward using the WBM interface. But first we needed to make sure the firewall was activated by selecting "Active Firewall." We accepted the default settings for TCP, UDP, and ICMP Idle Timeout[s] and clicked "Set Values" for the changes to take place (see Figure 11).

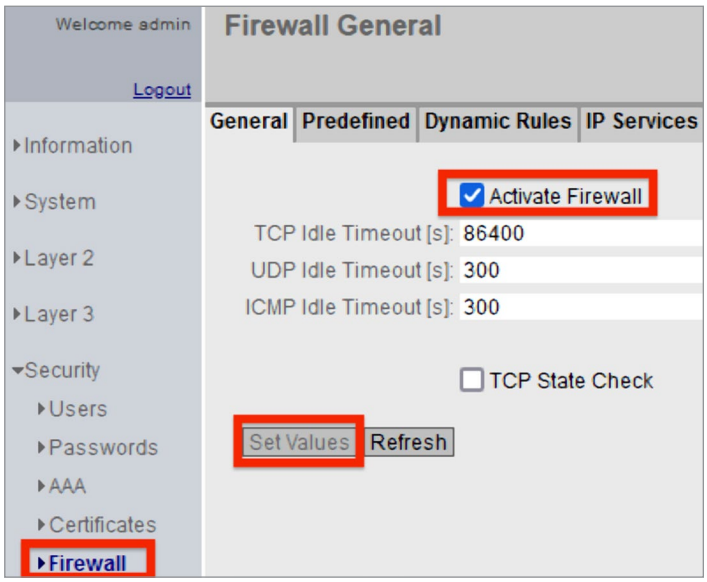

Figure 11. Firewall Mode Enabled with Default Settings

Once submitted, changes take place immediately because they are saved to nonvolatile RAM (NVRAM) within 60 seconds. Saving to NVRAM can be accelerated if desired. Figure 12 shows that with the current configuration, "Changes will be saved automatically in 27 seconds." This option will lead a user with administration-level access directly to the system configuration screen to submit the change using the "Write Setup Config" button.

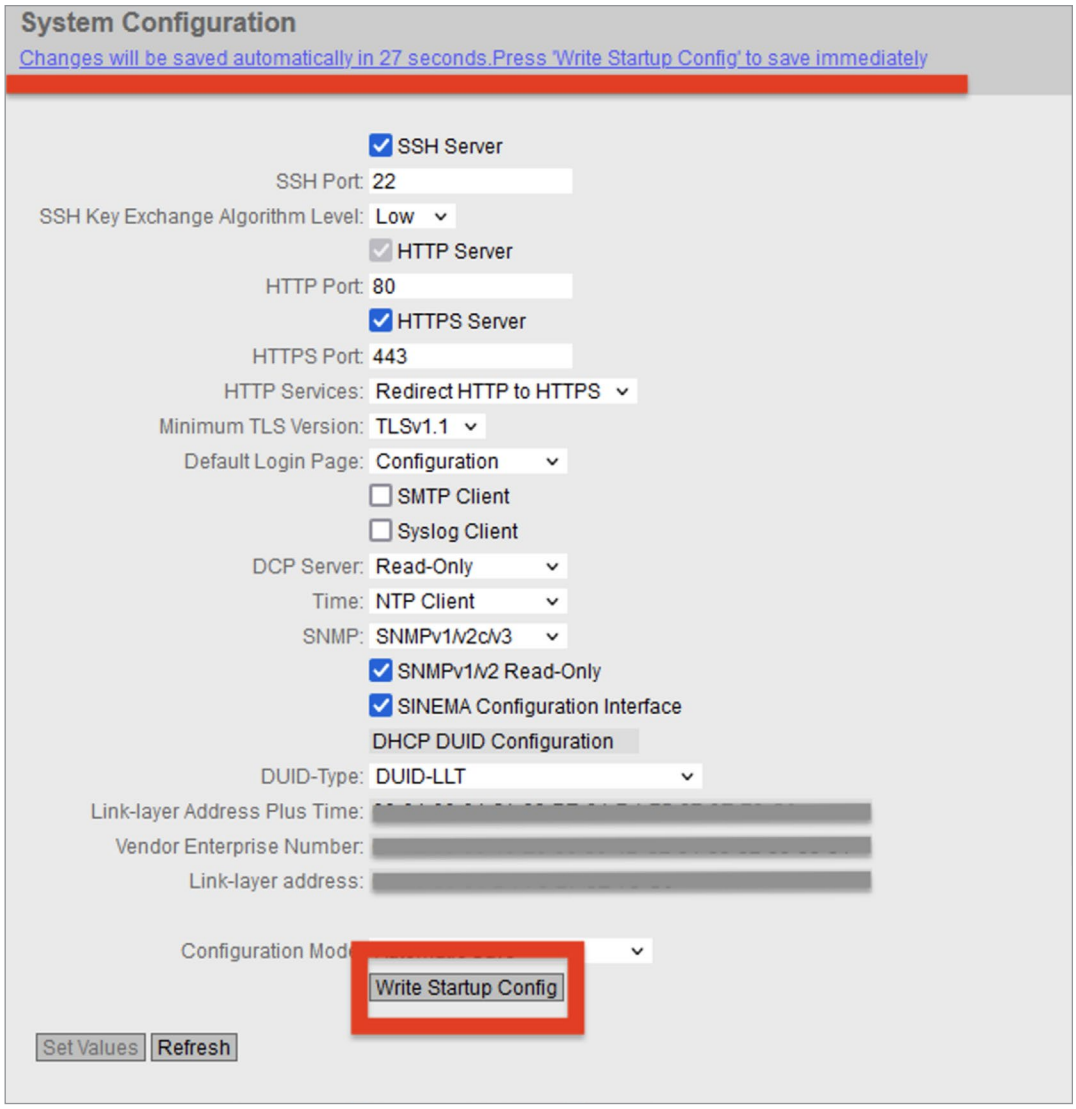

Figure 12. Saving Changes to NVRAM

Confirmation of the changed configuration is verified with a notification just after the change is pushed (see Figure 13).

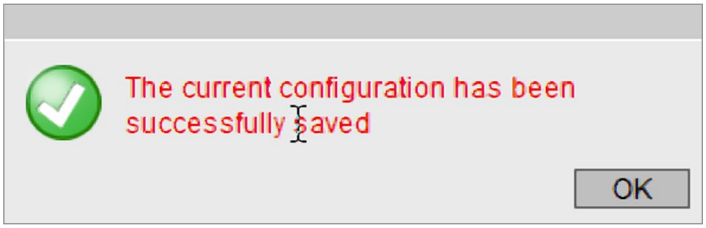

Figure 13. A Change Verification

Predefined Packet Filters: IP-Services

In the “Firewall General” section, we discovered a helpful set of rules available through the “Predefined” tabs. Facility staff can leverage both IP- and MAC-based packet filters to quickly enable or disable commonly used security services. For example, we experimented with several interfaces to apply IP-based predefined rules such as HTTP, HTTPS, DNS, SNMP, IPsec VPN, SSH, DHCP, Ping, and others. These can be applied individually to different interfaces or enabled or disabled all at once for a defined interface. Figures 14 and 15 show IP- and MAC-based predefined rules, respectively.

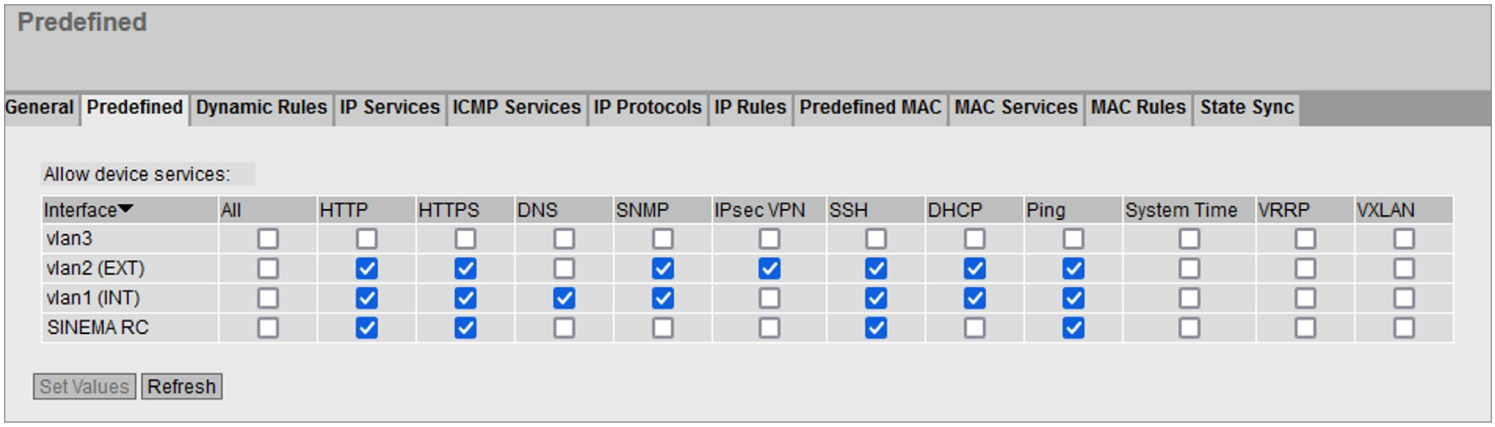

Figure 14. Predefined IP Packet Filters for the SC646-2C

Ruleset Scenario

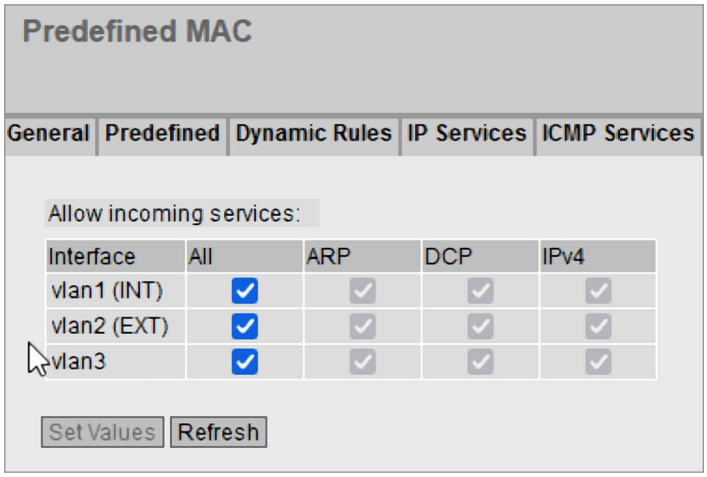

Figure 15. Predefined MAC Filters for the SC646-2C

After defining our test cases, we worked to create and deploy a firewall ruleset in the lab environment. The general approach to configuring a firewall ruleset is to define external and internal networks, activate the firewall, and review predefined “enable/disable” firewall rules.

We created common services, then defined inbound and outbound firewall rules based on IP, ports, and protocol. This scenario protects a network segment while allowing protected internal communications, remote connectivity for management, and only specific allowed device communication through the SC646-2C to or from the 192 and 10 networks, specifically for just 192.168.1.2 and 192.168.1.3 assets (see Figures 16 and 17 on the next page).

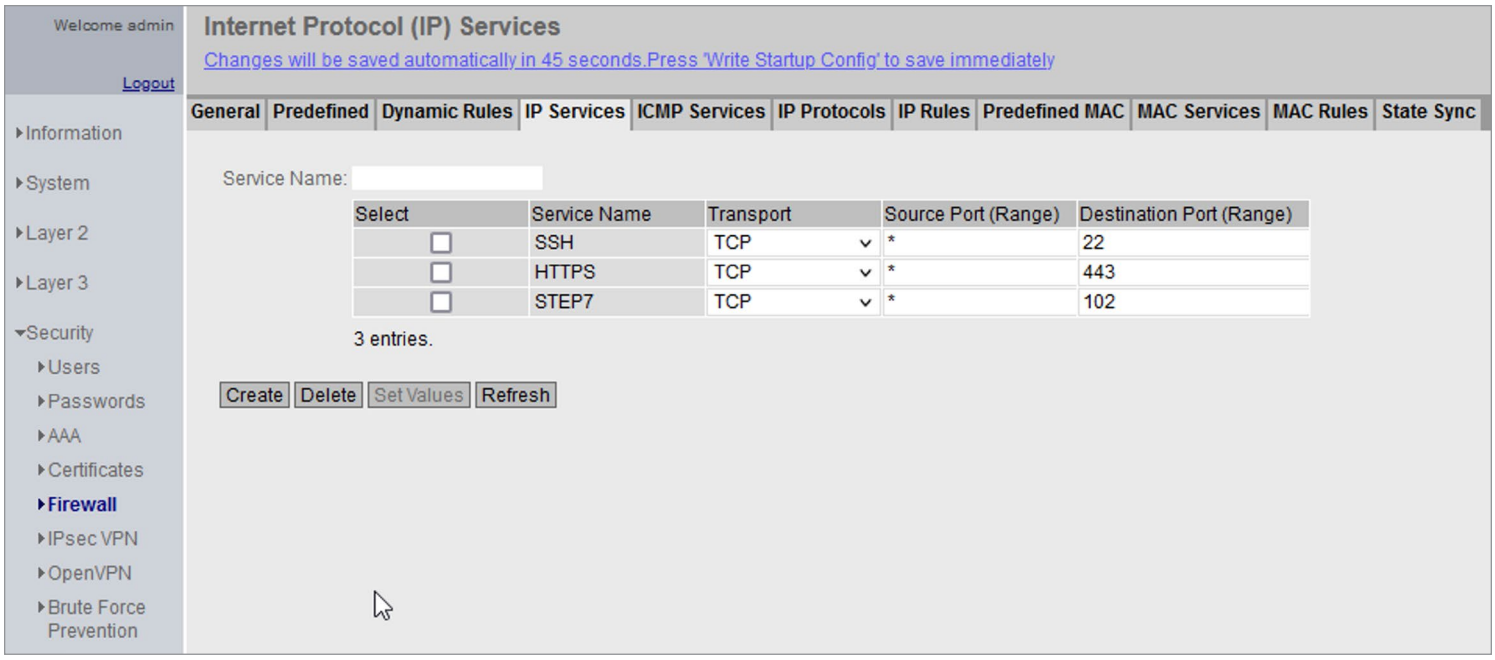

Figure 16. IP Services Set for Only Secure and Required Traffic

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.2	HTTPS
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.2	SSH
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.3	HTTPS
☐	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.10	192.168.1.3	STEP7

Figure 17. Example Ruleset for Specific Devices for SSH, HTTPS, and Step 7 Services

The WBM interface was used to activate the IP-based firewall features. Finally, we implemented a simple yet effective protection ruleset based on the access requirements outlined here (and shown in Figures 16 and 17):

- Secure communication for terminal interface for SSH and TCP 22
- Secure communication for management via the WBM (HTTPS and TCP 443)
- Step 7 (S7) communications for devices inside this minor enforcement boundary (S7 102)
- Protection of devices by preventing all other connection or protocols

Security Events and Logging

The logging capabilities of the SC646-2C include standard options where analysis can be done across three main log event types: event log, security log, and firewall log.

First, in the lab we generated events by creating firewall rules, modifying access control lists, attempting brute-force logins, and applying different device configuration settings on several occasions.

Then we took a proactive threat hunting approach in reviewing logs on the device. We leveraged recent ICS threat intelligence in an exercise to scope the SC646-2C event logs looking for network-based indicators of compromise (IoCs).

Event, firewall, and security log types can be accessed and downloaded from within the WBM interface through "Load & Save," with data save options using HTTP, TFTP, and SFTP. We performed the log download via HTTP and scoping through both the firewall and security logs. These were exported in CSV file format, and we ran a quick search in a CSV editor for recently identified malicious IP addresses from our ICS threat intel sources. While we fortunately did not find any real security threats in our test environment, we were able to illustrate the process of scoping for malicious IP addresses. This example works for a small deployment of SC646-2C devices without centralized management capabilities. Figure 18 shows the logs in a CSV editor and reveals our hacking exercise of testing the "Brute Force Prevention" feature. The review showed that the SC646-2C and it's "Brute Force Prevention" feature performed as expected, locking out an account and the IP from our hacking server.

Restart;SystemUpTime;SystemTime;Severity;Message
66;03:04:58;09/02/2022 14:10:45 ;4 - Warning;"WBM: User ICS_IncidentResponse failed to log in from X.X.X.X"
66;03:04:54;09/02/2022 14:10:42 ;4 - Warning;"WBM: User ICS_IncidentResponse failed to log in from X.X.X.X"
66;03:04:17;09/02/2022 14:10:05 ;6 - Info;"Time synchronized via 'NTP' with server IP X.X.X.X"
66;03:04:11;09/02/2022 14:09:59 ;4 - Warning;"WBM: User Backup failed to log in from X.X.X.X"
66;03:04:06;09/02/2022 14:09:54 ;4 - Warning;"WBM: User hackersRhere failed to log in from X.X.X.X"
66;03:03:40;09/02/2022 14:09:28 ;4 - Warning;"WBM: User secretaccount failed to log in from X.X.X.X"
66;03:03:38;09/02/2022 14:09:26 ;4 - Warning;"User unknown user account is locked for 12 minutes after 5 unsuccessful login attempts."
66;03:03:38;09/02/2022 14:09:26 ;4 - Warning;"IP X.X.X.X is locked for 12 minutes after 5 unsuccessful login attempts."
66;03:03:05;09/02/2022 14:08:53 ;6 - Info;"WBM: User admin has logged out from X.X.X.X"
66;03:02:00;09/02/2022 14:07:48 ;6 - Info;"Device configuration changed."
66;02:59:53;09/02/2022 14:05:41 ;6 - Info;"WBM: User admin has logged in from X.X.X.X"
66;02:59:35;09/02/2022 14:05:23 ;4 - Warning;"WBM: User ICS_IncidentResponse failed to log in from X.X.X.X"
66;02:59:10;09/02/2022 14:04:57 ;4 - Warning;"WBM: User ICS_IncidentResponse failed to log in from X.X.X.X"
66;00:00:25;09/02/2022 11:06:31 ;6 - Info;"Link up on P0.5."
66;00:00:14;09/02/2022 11:06:20 ;6 - Info;"Update DNS: X.X.X.X(manual) Y.Y.Y.Y(manual) "
66;00:00:09;09/02/2022 11:06:15 ;6 - Info;"Ring ID 1 is configured to ring off."
66;00:00:00;09/02/2022 11:06:14 ;6 - Info;"Cold start performed"

Figure 18. Log Review (with Redactions)

It is important to note that during an incident response scenario, another separate ruleset could be enabled by using the Digital Input (DI) on the front panel of the SC646-2C, thus changing the network security in a certain defined condition. This means organizations can operationally and procedural pursue this further to limit or change available attack vectors from the network in the event of a compromise, for example.

Another use case is allowing *data acquisition* traffic allowed to come in through the firewall in normal operating conditions. So, controls traffic can be disabled in the main ruleset by default, disallowing the state changes of the engineering process such as changing the position of an actuator, pressure from a pump, or other manipulation of the engineering process.

When *control* traffic is needed it can be allowed using the SC646-2C DI at only specific times determined by operators. This can be achieved if the DI is connected to a physical button, for example, as an operator can press a button to change the ruleset to temporarily allow *control* traffic on a control timer which will timeout and reset the firewall ruleset to data acquisition only again.

Notable in the logging features is the local log table and the syslog options to forward logs to a syslog service or ICS/OT SIEM device (see Figure 19).

Event	E-mail	Trap	Log Table	Syslog	Fault	Digital Out	VPN Tunnel	Firewall
Cold/Warm Start	☐	☐	☑	☑	☐			
Link Change	☐	☐	☑	☑				
Authentication Failure	☐	☐	☑	☑				
Power Change	☐	☐	☑	☑				
Fault State Change	☐	☐	☑	☑		☐		
Security Logs				☑				
Firewall Logs				☑				
DDNS Client Logs	☐	☐	☑	☑				
802.1X Port Authentication State Change	☐	☐	☑	☑				
Digital In	☐	☐	☑	☑	☐	☐	☑	☑
VPN Tunnel	☐	☐	☑	☑		☐		
FMP Status Change	☐	☐	☑	☑				
Secure NTP	☐	☐	☑	☑				
Configuration Change	☐	☐	☑	☑				
Service Information	☐	☐		☑				
DHCP Server Log	☐		☑	☑				

Figure 19. Logging Capabilities

Of particular note, syslog forwarding of security and firewall logs can be done for easier security incident correlation and large-scale investigations.

Additionally, some logs were reviewed in the security log table by selecting both “Warning” and “Critical.” This then displayed system uptime, restart status, system time, severity, and log messages (see Figure 20).

Because of our remote test connections, the security log shows SINEMA Remote Connect connections and several entries where we changed configurations—a notable event to track from a security perspective to ensure all changes are approved prior to implementation.

Security Log Table

Event Log | Security Log | Firewall Log

Severity Filters

☐ Info
☑ Warning
☑ Critical

System Up Time	Restart	System Time	Severity	Log Message
4d 01:03:07	65	08/12/2022 21:43:35	4 - Warning	SINEMA RC - OpenVPN terminated.
4d 01:02:35	65	08/12/2022 21:43:02	4 - Warning	SINEMA RC - OpenVPN terminated.
4d 01:02:01	65	08/12/2022 21:42:29	4 - Warning	SINEMA RC - OpenVPN terminated.
05:34:02	65	08/09/2022 02:13:05	4 - Warning	SINEMA RC - OpenVPN terminated.
05:30:52	65	08/09/2022 02:09:55	4 - Warning	SINEMA RC - OpenVPN terminated.
00:00:09	65	08/08/2022 20:39:09	2 - Critical	SINEMA-RC: Device configuration has been changed.
00:01:31	64	08/08/2022 14:01:04	2 - Critical	SINEMA-RC: Device configuration has been changed.

Figure 20. Main Security Log filtered for Warning and Critical Events

Centrally Managing a Fleet

We investigated how the SC600 series can be managed at scale, looking in particular at which changes can be managed across several networks and leveraged for active defense. Among the centralized managed changes accessible through SINEC NMS[14] is bulk policy-based configuration changes for switch settings, NAT configuration, security firewall rules, firmware patching, and central configuration backups, with periodic verification for change detection at the device level. SINEC NMS can be used to contain a compromise by pushing a set of lockdown firewall rules to a fleet of devices to further limit traffic and only allow a subset of traffic, ports, or protocols, or it can be set during an active attack to a traffic shutdown in selected zones to reduce impact.

SECURITY PRO TIP

It is a good practice to investigate events that indicate device changes or access control changes, such as the "Device configuration has been changed" warning shown in Figure 20. Such events can be viewed locally or through log exports to an ICS/OT SIEM using syslog, for example.

Device Vulnerability Management

We reviewed the SC646-2C for its ability to manage disclosed vulnerabilities and patch its firmware. For local firmware version checks, we navigated to Information > Versions to display the details needed to understand what versions were loaded and which were running (see Figure 21).

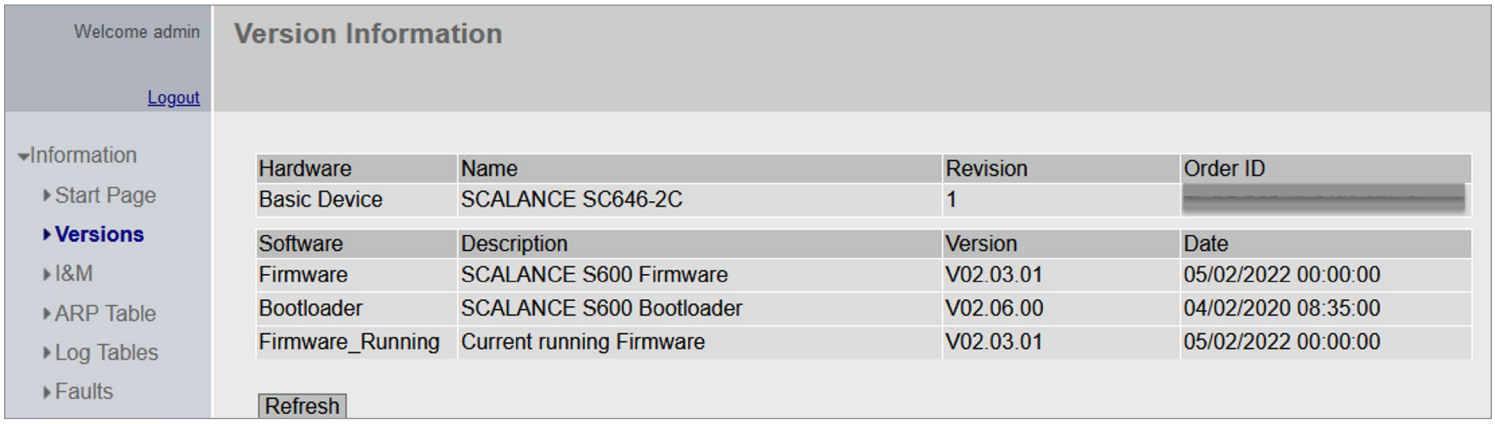

Figure 21. Checking Firmware Revisions

At scale, the Siemens Industrial Vulnerability Manager[15] can be leveraged by administrators to keep abreast of disclosed device vulnerabilities because it provides details on software versions in use, vulnerability details, and recommendations for remediation.

[14] Siemens, https://new.Siemens.com/global/en/products/automation/industrial-communication/sinec-networkmanagement.html

ICS Incident Response and Innovation with SIBERprotect

We were interested to find out how the SCALANCE SC646-2C could be leveraged during an evolving or active threat in the control system community. Through central device management with NMS, SCALANCE SC646-2C custom firewall rules can be pushed to a fleet of devices at once for rapid containment if a threat is imminent or has been realized on the network.

Furthermore, but beyond the scope of this review, Siemens SIBERprotect can also be leveraged. SIBERprotect[17] is a security solution utilizing security and engineering assets for rapid automatic incident response for OT and ICS environments. It can take input from devices such as an IDS, an NGFW, a PLC, an HMI, or cell/zone firewalls such as the SC600 appliances. SIBERprotect utilizes a PLC for security event detection and response in milliseconds, with the advantage of it being equipment that should be familiar to ICS/OT security or engineering staff.

SECURITY PRO TIP

SINEMA Remote Connect

Remote access can be securely deployed with SINEMA Remote Connect (RC).[16] It is a server-based application installed to enable the secure management of VPNs between main facilities, service technicians, and other trusted parties that require secure remote connectivity to manage, monitor, change, or troubleshoot key devices. SINEMA RC supports multifactor authentication and provides VPN solutions such as IPSec and OpenVPN, supporting proven encryption.

Threat Intelligence and the SC646-2C

In reviewing how SCALANCE SC600 devices can be used to reduce risks, we mapped several mitigations cited by the Mitre ATT&CK ICS framework,[18] including employing access management (M0801), filtering network traffic (M0937), using network allow lists (M0807), and implementing network segmentation (M0930). Additionally, a resource to consider for immediate response to security threats and issues affecting Siemens devices is the Siemens ProductCERT Computer Emergency Response Team.[19]

[15] Siemens, https://support.industry.Siemens.com/cs/sc/4990/industrial-vulnerability-manager?lc=en-US

[16] Siemens, https://new.siemens.com/us/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks/sinema-remote-connect-access-service.html

[17] Siemens, https://Siemensgovt.com/assets/documents/SIBERprotect.pdf

[18] Mitre ATT&CK framework, https://attack.mitre.org

[19] Siemens, https://new.Siemens.com/global/en/products/services/cert.html

Conclusion

Our testing found the SIEMENS SCALANCE S Industrial Firewall Appliances to be very flexible and capable of segmenting and controlling traffic to protect ICS networks, even starting with a previously unsegmented, or flat, network.

The WBM interface is straightforward to use and can be configured for user-based access control to suit many roles, such as device administrators, to network security teams that need to set up traffic filtering, and incident responders to do security event log reviews. We found that the predefined IP- and MAC-based rulesets jump-start deployment, and creating rules for settings, services, and the firewall is intuitive, making rapid network security changes possible.

While not attempting to be a full-blown next generation firewall to handle organization's edge traffic to and from the Internet, the SC-600 series are well suited for Minor and Cell enforcement boundary security in accordance with the SANS ICS410 SCADA Reference Architecture.[20] Once SCALANCE S firewalls are in place to segment the network and securely route traffic, maturing security programs can leverage SINEC NMS to centrally manage them, and look to SIBERprotect to move further towards the Active Defense posture on the Sliding Scale of Cyber Security.[21]

The SCALANCE SC646-2C meets the needs for performing control system network segmentation, asset protection, role-based access control, and traffic control using SPI. It excels as an industrial, ruggedized ICS firewall well suited to secure minor enforcement boundary and operational cell protection using its SPI features and SINEC NMS for scalable deployment to manage a large fleet. The devices are suitable for multiple sectors including but not limited to oil and gas, chemical facilities, critical manufacturing, water and wastewater management, power facilities, automotive manufacturing, etc.

We recommend the SCALANCE SC600 devices to organizations looking to build a secure control network from the ground up, to improve the security of their existing control networks, or to align with network segmentation best practices. This approach would benefit organizations in the short term but also in the long term because technologies and processes can be built atop a trustworthy and flexible, strong network foundation.

Sponsor

SANS would like to thank this paper's sponsor:

SIEMENS

[20] SANS ICS410 SCADA Reference Architecture www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

[21] Sliding Scale of Cyber Security: www.sans.org/white-papers/36240