SEL-3620 Ethernet Security Gateway

Major Features and Benefits

The SEL-3620 Ethernet Security Gateway is a router, virtual private network (VPN) endpoint, and firewall device that can perform security proxy services for serial and Ethernet-based intelligent electronic devices (IEDs). The SEL-3620 helps create a user audit trail through strong, centralized, user-based authentication and authorization to modern and legacy IEDs. The SEL-3620 secures your control system communications with a stateful deny-by-default firewall, strong cryptographic protocols, and logs for system awareness. The SEL-3620 also manages protected IED passwords, ensuring that passwords are changed regularly and conform to complexity rules for stronger security. The integrated security proxy also provides user-based single sign-on access to Ethernet and serial devices.

- **Secure Architecture and Malware Protection.** Maximize reliability with integrated exe-GUARD® whitelist antivirus and other malware protections, eliminating costly patch management and signature updates.
- **Centralized User-Based Access to Protected IEDs.** Provide strong, centralized access control and user accountability to all protected devices with Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS). Simplify compliance with accurate logging.
- **Automated Management of IED Passwords.** Migrate away from shared passwords and accounts with the SEL-3620 acting as a password manager for protected devices.
- **Security Proxy Services.** Connect securely with identity based access controls to command line interfaces.
- **Detailed Connection Reports.** Receive detailed connection reports that make user activity audits a snap.
- **Secure Ethernet Communications.** Use Internet Protocol Security (IPsec), Media Access Control Security (MACsec), Secure Shell (SSH), and Transport Layer Security (TLS) to provide confidential communications and maintain message integrity among devices.
- **Stateful Deny-by-Default Firewall.** Prevent unauthorized traffic from entering or exiting your private network. Log all successful or blocked connections to the firewall, and receive alerts indicating the presence of unauthorized network communication attempts.
- **Syslog.** Log events for speedy alerts, consistency, compatibility, and centralized collection. For slow communications links, the SEL-3620 can throttle the number of outgoing syslog messages.
- **Integrated Port Switch.** Map one or more of the serial ports to any other serial ports, or to Ethernet TCP or UDP connections.
- **Modbus Protocol Conversion.** Convert Modbus TCP to Modbus RTU and Modbus RTU to Modbus TCP.
- **Script Engine.** Perform any sequence of command-driven tasks with a single push of a button, and restrict users to specific scripted tasks.
- **X.509 Certificates.** Ensure strong authentication with third-party validation of incoming connection requests over the IPsec VPN, Active Directory connection, or Web management interface.
- **Online Certificate Status Protocol.** Use OCSP to verify validity of X.509 certificates.
- **Time Synchronization.** Synchronize events and user activity across your system with IRIG or NTP.
- **Virtual Local Area Networks (VLANs).** Segregate traffic and improve network organization and performance.

- **Ease of Use.** Simplify configuration and maintenance with a secure web interface that allows for convenient setup and management.
- **Reliability.** Rely on the SEL-3620, built for availability, hardened for the substation, and backed by a 10-year warranty.
- **Ethernet Port Bridge.** Support a reliable Ethernet ring topology.
- **Encrypted Terminal Communications.** Securely communicate with IEDs via Secure Shell (SSH)-encrypted terminal programs.
- **5 V Pin One Power on Serial Ports.** Directly power 5 V devices from the serial ports.
- **Bit-Based Conversion.** Transform Conitel and other bit-based protocols to Ethernet and reduce reliance on expensive analog circuits.
- **Service Port.** Automate base-lining of the device settings with a basic command-line interface.

Functional Overview

The SEL-3620 is a router, VPN endpoint, and firewall device that can perform security proxy services to serial and Ethernet-based IEDs. The SEL-3620 is an access control solution for control systems environments with both Ethernet and serial communications. The SEL-3620 filters all incoming and outgoing traffic with a deny-by-default stateful firewall that only allows authorized traffic. IPsec VPNs protect all site-to-site communications.

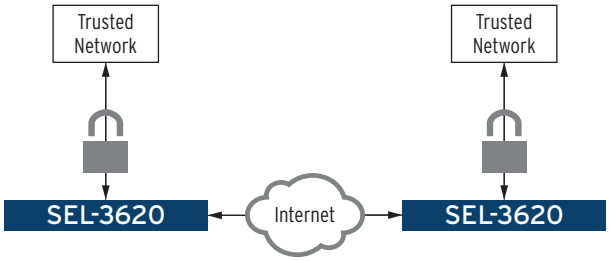


Figure 1 Site-to-Site Virtual Private Network

The authentication proxy technology integrated in the SEL-3620 provides single sign-on engineering access to protected IEDs. The strong authentication in the SEL-3620 includes centralized user-based credentials and verification of the source of user communications. Thorough logging of all user activities on protected devices provides simple audit reports from which you can know who did what when.

Figure 2 Protected Engineering Access

An integrated stateful, deny-by-default firewall prevents unauthorized communications from entering or exiting the protected network. The SEL-3620 filters incoming and outgoing TCP, UDP, ICMP, AH, and ESP communications based on a user-configurable set of rules.

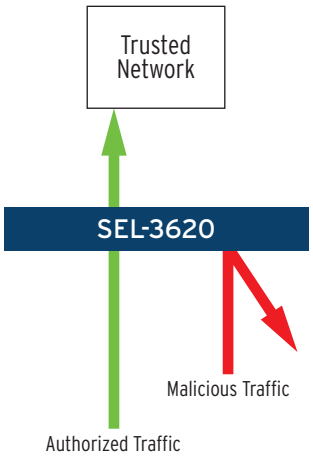


Figure 3 Deny-by-Default Firewall

User-based accounts increase log granularity and make password management easy and effective. The SEL-3620 includes support for centralized authentication and authorization to simplify management of user accounts, passwords, and user privileges for all your protected devices from an active directory server.

Figure 4 Centralized User Management

The port switch integrated in the SEL-3620 allows users to create mappings for serial-to-serial, serial-to-Ethernet, Ethernet-to-serial, and Ethernet-to-Ethernet communications. Through use of these mappings you can use such different modes of communications as one-to-one, one-to-many, and many-to-many.

The SEL-3620 formats, stores, and forwards logs according to the syslog specification to enable quick notification, central collection, and interoperable reporting of security events. IRIG-B and NTP synchronizes these events. The SEL-3620 records user activity on IEDs to provide you with auditable tracking of user activity within your system.

Authentication for the web management interface, VPN peers, and directory servers relies on X.509 certificates. The Online Certificate Status Protocol (OCSP) verifies the legitimacy of any certificates the SEL-3620 receives.

The SEL-3620 streamlines user-configurable options and uses an HTTPS web interface for a simplified user experience. SEL ACSELERATOR QuickSet® SEL-5030 Software with connection directory software provides configuration of the proxy services. A command line interface on the integrated SSH server provides access to protected IEDs.

The SEL-3620 exe-GUARD feature provides whitelist architected antivirus and other malware protections, including a secure kernel that prevents unauthorized access or modification of system data and monitors critical system services to detect unexpected activity caused by unauthorized modifications to the device program.

The SEL-3620 is built for installations that require high levels of availability. The device contains no moving parts, operates over a wide temperature range from –40°C to +85°C, and uses a flash-based hard drive for maximum durability.

The SEL-3620 secures traffic by using MACsec. MACsec is a non-routable “hop-by-hop” cryptographic protocol that protects Ethernet frames starting at the data-link layer (OSI Layer 2). The MACsec protocol provides confidentiality, integrity, authenticity, and replay prevention to communications. Automated key management is provided by the MACsec Key Agreement (MKA) protocol. The goal of the MKA protocol is to facilitate and automate the commissioning, management, and scalability of MACsec on a LAN.

Applications

The SEL-3620 is ideally suited for electronic access point routing, message encryption, packet authentication, and user authentication. The authorization and serial capabilities of the SEL-3620 provide a strong solution for user-based access to legacy IEDs that have shared user accounts.

Routing and Masquerading

The SEL-3620 forwards communications among separate Ethernet networks. Any device that has access to the SEL-3620 can use it to forward Ethernet packets to a destination on a different network.

The SEL-3620 supports Network Address Translation (NAT) for a wide variety of dynamic network applications. Port forwarding enables the use of similar remote address space without re-architecting IP subnets, and outbound NAT supports Internet access for those applications that require it.

Secure Communications Over Untrusted Networks

The SEL-3620 secures all communication by establishing IPsec VPN tunnels with other SEL-3620 gateways and IPsec-enabled devices. It can also be used to secure local communications with MACsec.

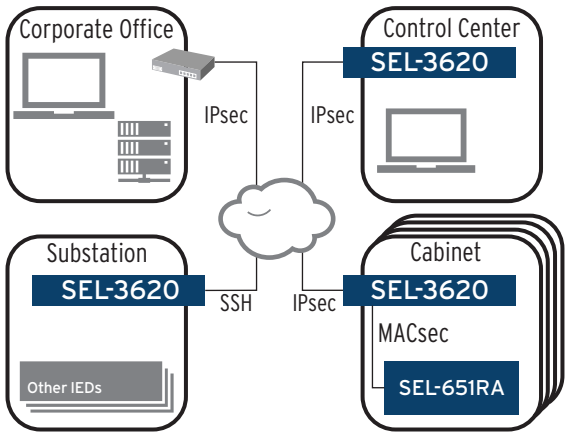


Figure 5 SEL-3620 Encrypts Communications

Point-to-Point Serial Over Ethernet Network

Figure 6 shows the SEL-3620 in a point-to-point application in which bit- and byte-based serial devices can communicate with each other across an Ethernet network. The SEL-3620 supports IPsec and SSH for encrypted and authenticated communications. This provides an easy transition from existing costly analog serial lines to Ethernet transport networks without having to upgrade remote terminal units (RTU) or communication front ends (CFE).

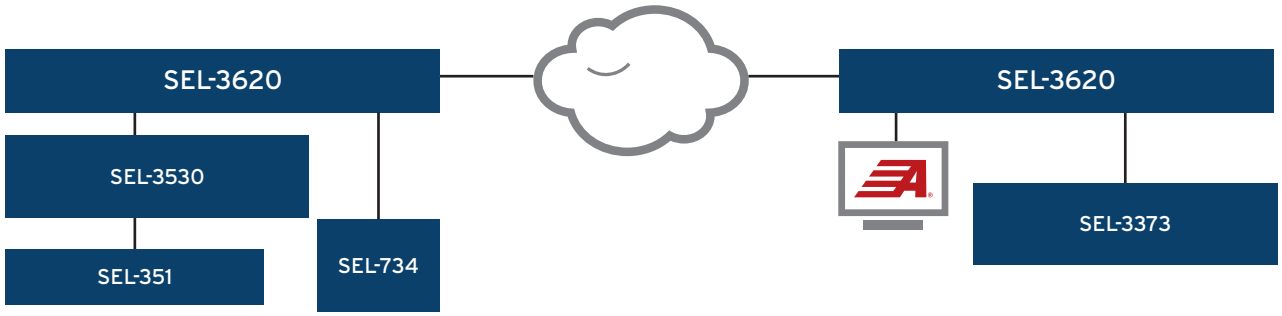


Figure 6 SEL-3620 Protects Serial Over Ethernet

User-Based Access to IEDs

The authentication proxy feature in the SEL-3620 provides user-based access to serial and Ethernet devices within the secured network. The SEL-3620 records and logs all user activity, to provide an audit trail and user accountability.

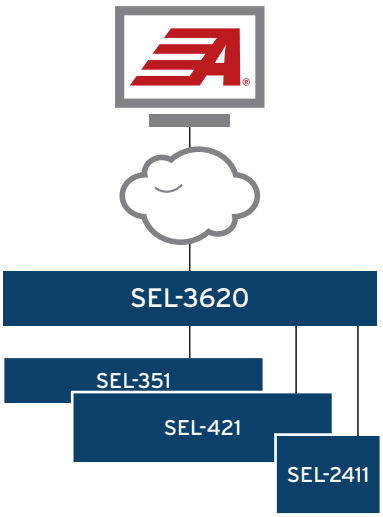


Figure 7 SEL-3620 Authenticates Users

Ethernet to Serial Conversions

Gain Ethernet-based access to your serial devices through the SEL-3620. The SEL-3620 performs both bit- and byte-based serial-to-Ethernet media conversions for Telnet, SSH, Raw TCP, and UDP protocols.

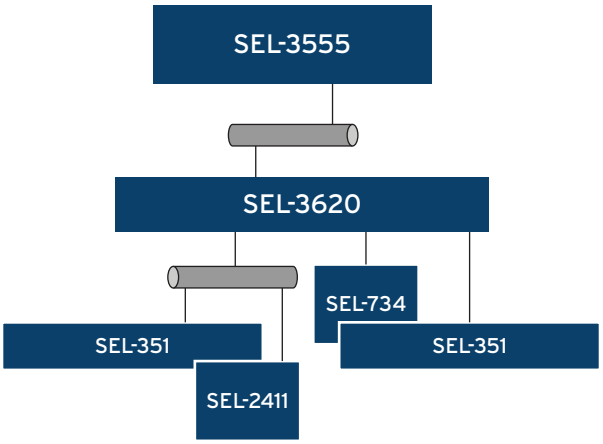


Figure 8 SEL-3620 Converts Serial to Ethernet

Password Management

The SEL-3620 is uniquely designed to manage the passwords of all your protected IEDs. The single sign-on capabilities of the authentication proxy require that the SEL-3620 be aware of the passwords of all protected IEDs. The combination of the script engine with this password knowledge gives the SEL-3620 the ability to manage your passwords, enforce strong passwords, and provide audit reports of password changes.

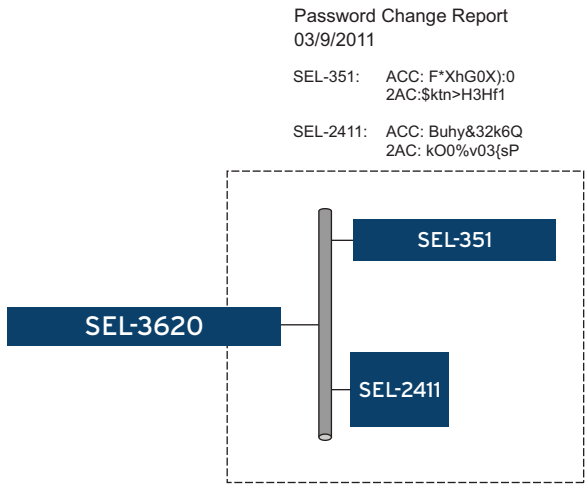


Figure 9 SEL-3620 Manages Passwords

Time Distribution

Synchronize all your devices with the SEL-3620, regardless of whether these devices understand NTP or IRIG. The SEL-3620 synchronizes to and sources both IRIG-B and NTP.

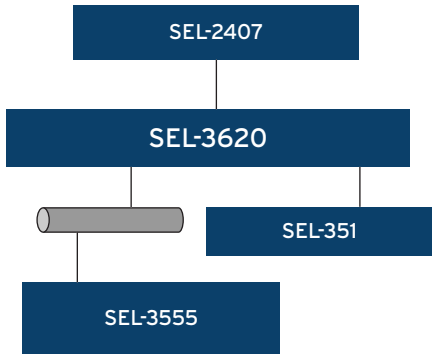


Figure 10 SEL-3620 Distributes Time

Functional Description

Cryptographic Message Protection

IPsec

IPsec VPN initiation requires that three tasks be performed: the two peers must authenticate each other, the IKE security associations (SAs) must be established, and the IPsec SAs must be established. Upon establishment of the IPsec SAs, the SEL-3620 transmits all messages that route through this "tunnel" within an Encapsulating Security Payload. The SEL-3620 performs all of these steps when it connects to any peer IPsec-enabled device.

Security associations are shared pieces of information that we can use to secure communications channels. An SA includes the encryption and authentication algorithms the channel uses along with their respective keys. An Internet Key Exchange (IKE) SA defines the secure channel on which IPsec SA negotiation takes place. An IPsec SA defines the communications parameters that will be in use for communication across a VPN. The SEL-3620 contains preconfigured settings in "Profiles" to simplify connecting to non-SEL devices.

Figure 11 VPN Establishment

Encryption ensures that communications are confidential and only readable by authorized parties. The SEL-3620 uses the IPsec Encapsulating Security Protocol to protect the entire original packet, including both the header and the payload. This prevents the possibility of information leakage about the structure of your protected networks. The hardware-accelerated encryption algorithms the SEL-3620 supports are AES, 3DES, and Blowfish.

MACsec

MACsec provides industry-standard security through the use of secured point-to-point Ethernet LAN links. The point-to-point links are secured after matching security keys are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption. Encryption ensures that communications are confidential and only readable by authorized parties. The SEL-3620 uses MACsec Security Protocols to protect the communication. This prevents the possibility of information leakage.

The SEL-3620 performs all these steps when it connects to any peer MACsec-enabled device. The device will participate as an MKA key server only, not as a client. MACsec is configured in connectivity associations. Key management is automated for simplicity with MACsec and MKA.

Figure 12 Layer Two Tunnel Establishment

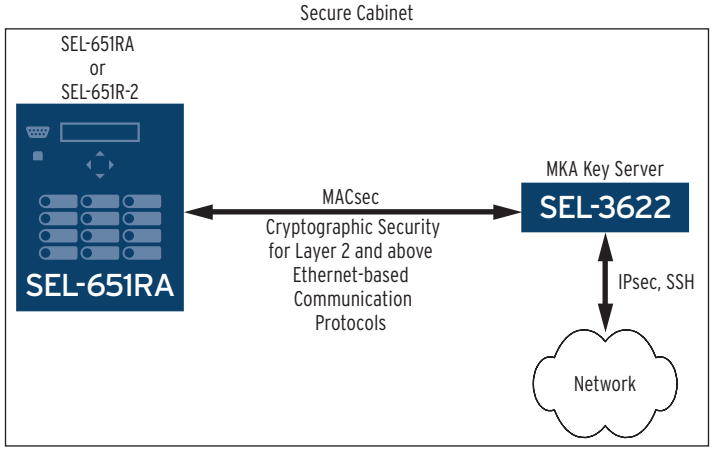


Figure 13 Secure Cabinet

Device Authentication

The SEL-3620 can use either X.509 certificates or preshared keys for authentication of another party over a network. The X.509 certificate confirms that the party at the opposite end of the tunnel is an entity with whom the SEL-3620 has approval to communicate. The SEL-3620 accepts both self-signed X.509 certificates and X.509 certificates that have been signed by a Certificate Authority (CA).

The SEL-3620 uses OCSP to check the status of X.509 certificates. When the SEL-3620 receives a connection request along with a certificate signed by a CA, it will poll an OCSP server to verify that the certificate is good. There are three possible responses the OCSP server can supply: good, revoked, and unknown. If the SEL-3620 receives a response other than good, it will deny the connection request.

Centralized User-Based Access Control

The security proxy services in the SEL-3620 provide user-based access to protected serial and Ethernet IEDs. *Figure 14* illustrates this process. A user needing to access a protected IED will first access the SEL-3620. The SEL-3620 will then prompt for the user's username and password. The SEL-3620 will verify the provided credentials with a centralized server and obtain the user's permissions. These permissions then determine which devices and access levels the user has authorization to access. The SEL-3620 connects to the IED which the user wants to access, and joins the sessions with the user and the IED. Alternately, if the user needs direct relay access, such as for calibration testing purposes, the user can checkout the device. Device checkout resets the device access level passwords, which the user has authorization to access, to their initial values for a preconfigured amount of time.

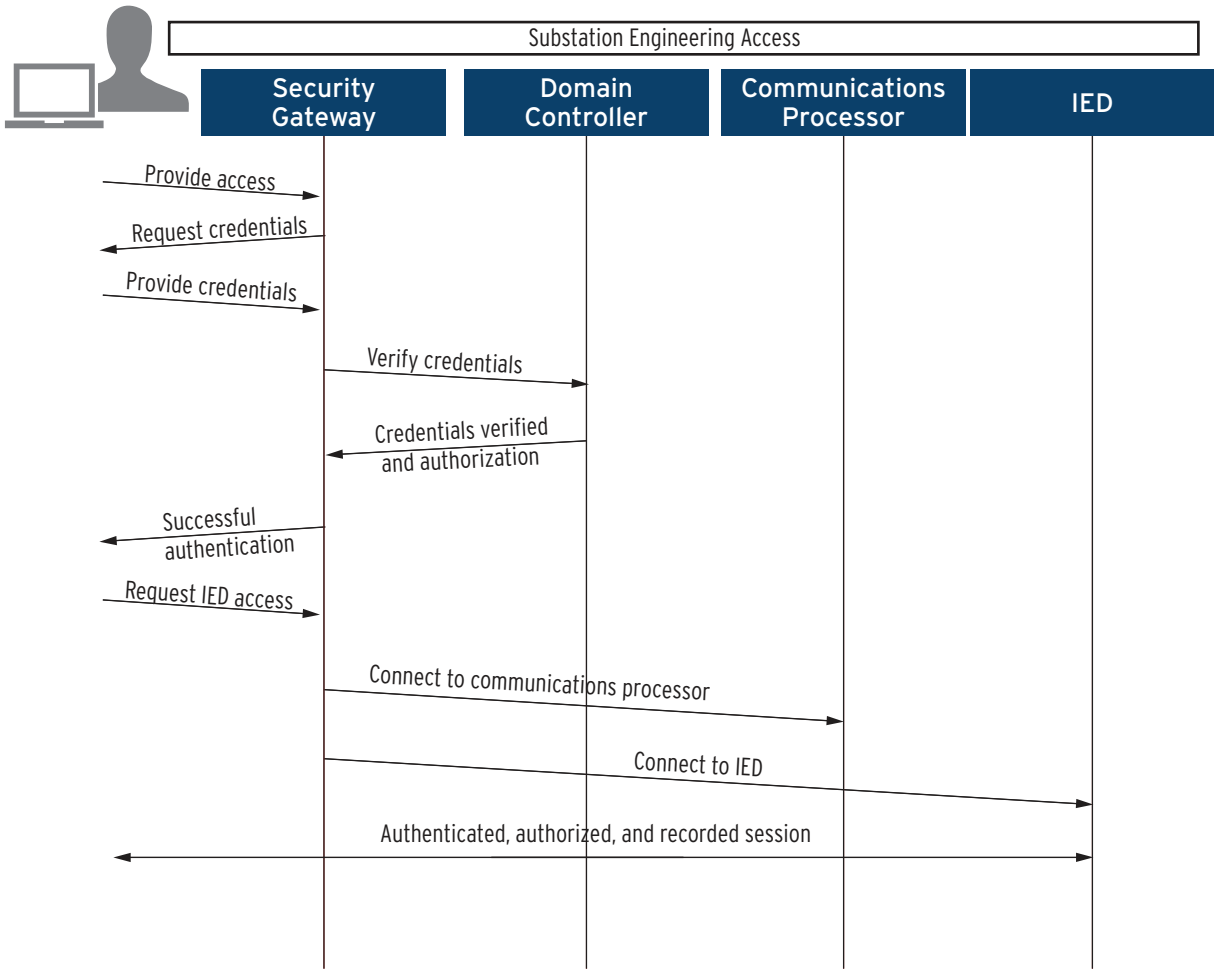


Figure 14 Central User Authentication

Maintaining logs of user activity is very important for auditing purposes. The SEL-3620 monitors all user activity and logs each session to a locally stored file. At the same time, the SEL-3620 generates syslog messages, indicating the start of a session and the end of a session, to alert that activity has taken place. Users with appropriate privileges can export the user log files for later examination as necessary.

Password Management

The SEL-3620 manages the passwords for all managed devices. It maintains an internal list of all the managed devices, their current states, their initial passwords, their currently used passwords, and their proposed passwords. Password change cycles are broken into three steps:

Step 1. Password generation creates a new list of proposed passwords for all selected managed devices.

Step 2. Report generation and download creates and stores a list of all the currently used and proposed passwords for all managed devices.

Step 3. Password application changes the passwords of all managed device accounts/access levels which have proposed passwords.

The web interface provides a manual method to perform these tasks as needed. The master port self-controller provides a method to easily script these steps for automated systems, such as TEAM Security. The flexibility of the web interface provides a means to enable or disable managed devices so they are not included in bulk operations, as well as the ability to select which devices to generate passwords for. Finally, the web interface provides the ability to set persistent and shared passwords that are never changed as part of a bulk operation.

Multiple Access Methods

Users have multiple methods of accessing IEDs to provide flexibility for various types of software. SSH and Telnet provide a command line interface to protected devices through the SEL-3620. You can also map specific TCP and UDP ports to physical serial ports.

Syslog

The SEL-3620 uses the syslog format to log events. These logs contain several fields that indicate event severity, event origin, the type of event that occurred, and details regarding the cause of the event. Additionally, the event message contains such event tracking information as the entity that triggered the event and the time and date of the event. The SEL-3620 maintains an internal record of as many as 60,000 event logs in nonvolatile memory, and it generates, stores, and forwards syslog messages to multiple destinations.

SNMP

Simple Network Management Protocol (SNMP) support on the SEL-3620 allows administrators to query some state information from the device, as well as to receive notifications (traps) for events that indicate a device integrity fault, such as Mandatory Access Control audit messages, and whitelist integrity failures. The Management Information Base (MIB) provides information about data and traps available via SNMP. The MIB can be downloaded as a zip file from the SEL-3620 from the SNMP Settings page on the web management interface.

Firewall

To protect your private network from malicious traffic, the stateful firewall in the SEL-3620 denies all traffic by default. Explicitly identifying traffic that the SEL-3620 permits makes it far less likely that the SEL-3620 will overlook specific types of traffic.

Secure Management

Configuration of the SEL-3620 occurs through a secure web management interface that uses HTTPS incorporating transport layer security (TLS). Mutual authentication takes place before a secure web management session opens. The device uses an X.509 server-side certificate to authenticate to the user, and the user uses a username and password to authenticate to the device. The SEL-3620 then restricts users to actions for which they have authorization through their account assignments. There are two roles: administrator and technician. The technician may perform any task on the SEL-3620 except create or edit user accounts, modify date/time settings, or reset, halt, or restart the device. Administrators may perform any action on the SEL-3620, including creating and editing all accounts on the box.

Web management provides simple-to-use graphic configuration pages that display the gateway configuration through network diagrams. You can use this to confirm that all configurations are as you intend. The web interface supplies you a single place from which you can retrieve all communications channel information and network diagrams associated with the SEL-3620. The device also features a basic command-line interface service port that allows for the automation of configuration base-lining. The service port is read-only and requires administrative credentials to access.

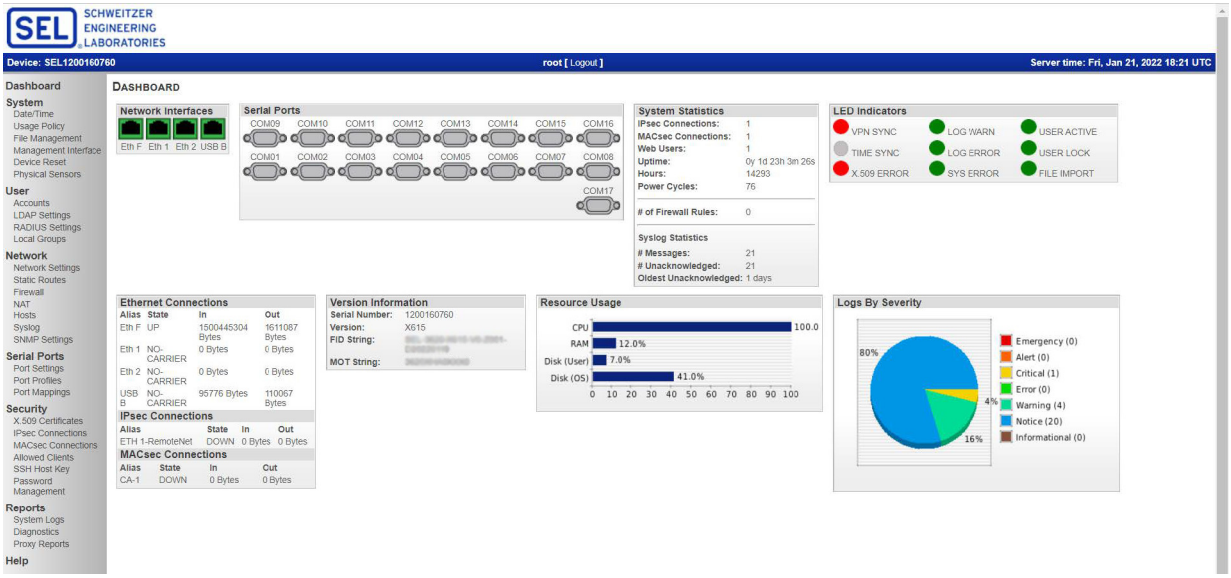
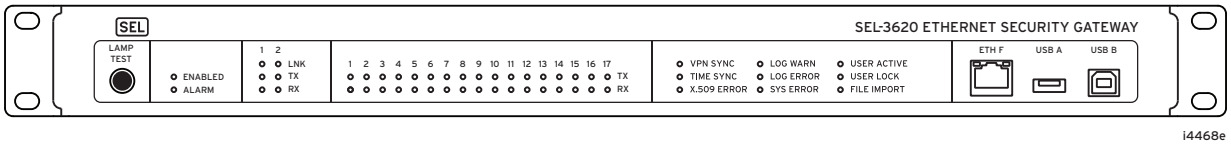


Figure 15 Web Management Dashboard

Mechanical Diagrams and Dimensions

Rack Mount



Panel Mount

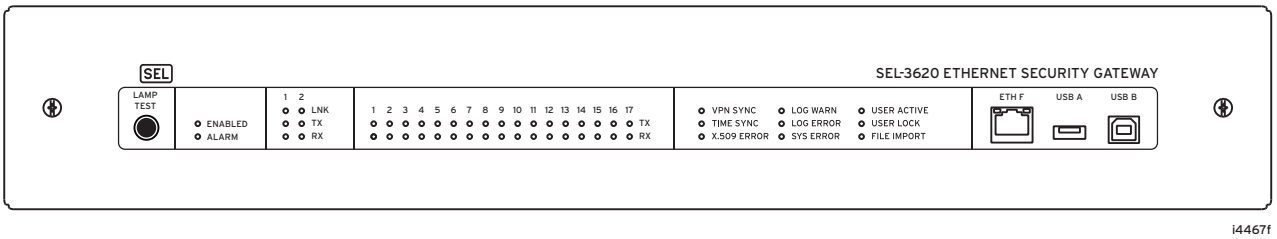
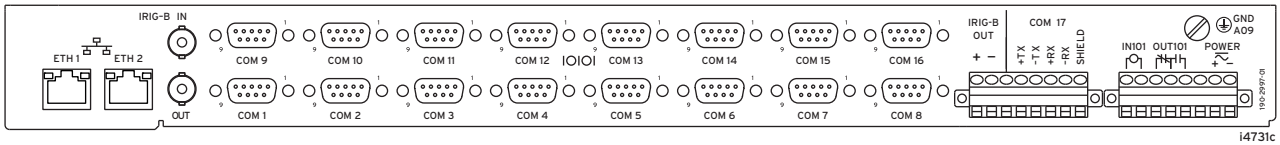
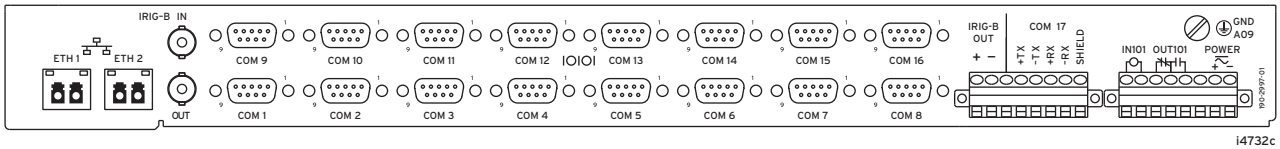


Figure 16 Front-Panel Diagrams

Copper Ethernet



Fiber Ethernet



Mixed Ethernet

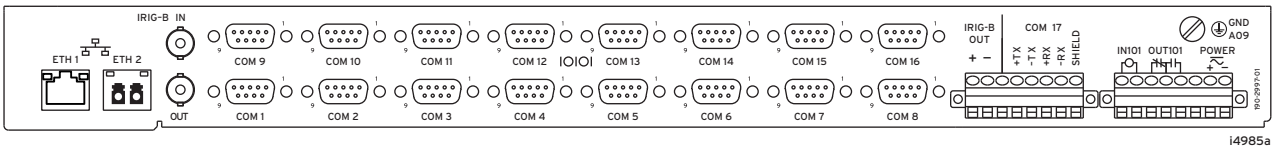


Figure 17 Rear-Panel Diagrams

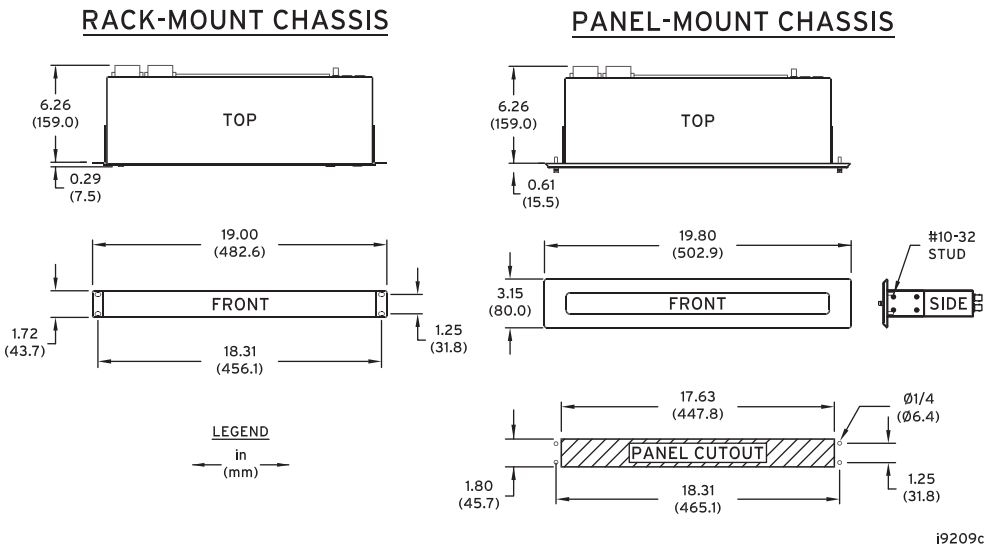


Figure 18 SEL-3620 Dimensions

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

47 CFR 15B, Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at their own expense.

UL Listed to U.S. and Canadian safety standards (File E220228; NRAQ, NRAQ7)

CE Mark
UKCE Mark
RCM Mark

Networking

Web Management

Protection Protocols:	HTTPS, TLSv1.2, TLSv1.3
Authentication:	X.509 and Username/Password
Encryption Key Strength:	128-bit, 256-bit

Virtual Private Networks

Maximum Throughput:	30 Mbps
Maximum Concurrent Sessions:	16
Protection Protocols:	IPsec
Key Exchange:	IKEv1, IKEv2
Authentication:	Passphrase, X.509, OCSP
Accelerated Encryption Algorithms:	AES
Nonaccelerated Encryption Algorithms:	3DES, Blowfish
Encryption Key Strength:	128-bit, 256-bit, 512-bit

Routing Functions

Static Routing

Network Address Translation: Port Forwarding (DNAT) as many as 200 user-specified rules

Network Address Translation: Outbound NAT (SNAT)

Ethernet Protocols

Address Resolution Protocol (ARP)

Dynamic Host Configuration Protocol (DHCP) Client

Dynamic Host Configuration Protocol (DHCP) Server (USB-B Only)

Encapsulating Security Payload (ESP)

File Transfer Protocol (FTP)

Hypertext Transfer Protocol Secure (HTTPS)

Internet Control Message Protocol (ICMP)

Internet Key Exchange (IKEv1/v2)

Internet Protocol Security (IPsec) Protocol Suite

Internet Secure Association and Key Management Protocol (ISAKMP)

Lightweight Directory Access Protocol (LDAP) Client

MACsec Key Agreement (MKA)

Media Access Control Security (MACsec)

Modbus TCP/IP

Network Time Protocol (NTP) Client/Server

Online Certificate Status Protocol (OCSP)

Remote Authentication Dial-In User Service (RADIUS)

Secure Shell version 2 (SSHv2) Client/Server

Simple Network Management Protocol (SNMP)

Spanning Tree Protocol (STP)

Syslog

Telnet

Transmission Control Protocol (TCP)

Transport Layer Security (TLS)

User Datagram Protocol (UDP)

VLAN

Maximum number of VLANs per physical interface:	4

Security

User-Based Accounts

Maximum Local Accounts:	256
Password Length:	8–128 characters
Password Set:	All printable ASCII characters
User Roles:	Administrative and Technician

Syslog

Storage for 60,000 messages

Forwarding to 3 destinations

Firewall

Implementation:	iptables

As many as 1000 user-specified rules supported

Proxy Services

Maximum number of simultaneous users:	10
Maximum number of managed devices:	150
Time to generate 1050 passwords	<20 minutes

MACsec

Connectivity Associations:	One per physical Ethernet port
Encryptions Key:	GCM-AES-128

General

Operating Temperature Range

–40° to +85°C (–40° to +185°F)
Note: Not applicable to UL applications.

Operating Environment

Pollution Degree:	2
Overvoltage Category:	II
Relative Humidity:	5%–95%, non-condensing
Maximum Altitude:	2000 m

Dimensions

1U Rack Mount:	482.6 mm W x 43.7 mm H x 159 mm D (19" W x 1.72" H x 6.26" D)
1U Panel Mount:	502.9 mm W x 80 mm H x 159 mm D (19.8" W x 3.15" H x 6.26" D)

Weight

2.35 kg (5.2 lb)

Warranty

10 Years

Processing and Memory

Processor Speed:	533 MHz
Memory:	1024 MB DDR2 ECC SDRAM
Storage:	4 GB

System Speeds

Firmware Update Time (Varies):	10 min
Cold Boot-Up Time:	2 min

Time-Code Input

IRIG accuracy depends on external GPS source

Input Type:	IRIG-B000 or B002, Even or Odd parity

NTP accuracy depends on network conditions

Modulated IRIG-B (BNC)

On (1) State:	$V_{ih} \geq 3.3\ V_{p-p}$
Off (0) State:	$V_{il} \leq 0.1\ V_{p-p}$
Input Impedance:	2.5 kΩ
Accuracy:	500 µs

Demodulated IRIG-B (BNC)

On (1) State:	$V_{ih} \geq 2.2$ V
Off (0) State:	$V_{ih} \leq 0.8$ V
Input Impedance:	2.5 kΩ
Accuracy:	250 ns

Network Time Protocol (Ethernet)

Accuracy:	10 ms (varies)

Time-Code Output

IRIG accuracy depends on source accuracy

NTP accuracy depends on network conditions

Demodulated IRIG-B000 Even Parity (BNC and Serial)

On (1) State:	$V_{oh} \geq 2.4$ V
Off (0) State:	$V_{ol} \leq 0.8$ V
Load:	50 Ω

Output Drive Levels

Demodulated IRIG-B:	TTL 120 mA, 3.5 Vdc, 25 Ω
Serial Port:	TTL 2.5 mA, 2.4 Vdc, 1 kΩ

Network Time Protocol (Ethernet)

Accuracy:	250 µs (ideal on LAN)

Communications Ports

Ethernet Ports

Ports:	2 rear, 1 front
Data Rate:	10 or 100 Mbps
Front Connector:	RJ45 Female
Rear Connectors:	RJ45 Female or LC Fiber (single-mode or multimode, 100 Mbps only)
Standard:	IEEE 802.3

Fiber Optic

100BASE-FX Multimode Option (to 2 km)

Maximum TX Power:	–14 dBm
Minimum TX Power:	–19 dBm
RX Sensitivity:	–30 dBm
System Gain:	11 dB
Source:	LED
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

100BASE-LX10 Single-Mode Option (to 15 km)

Maximum TX Power:	–8 dBm
Minimum TX Power:	–15 dBm
RX Sensitivity:	–25 dBm
System Gain:	10 dB
Source:	Laser
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

Serial Ports

Type:	EIA-232/EIA-422/EIA-485 (software selectable)
Data Rate:	1200 to 115200 bps
Connectors:	DB-9 Female (Ports 1–16), Isolated 8 pin (Port 17)
Power:	+5 Vdc power on Pin 1 (500 mA maximum cumulative for 16 ports)

USB Ports

1 Host Port:	Type A (nonfunctional, for future use)
1 Device Port:	Type B Supports USB Networking with DHCP server for out-of-band management access (driver downloadable from selinc.com)

Power Supply

Input Voltage

Rated Supply Voltage:	125–250 Vdc; 110–240 Vac, 50/60 Hz 48–125 Vdc; 120 Vac, 50/60 Hz 24–48 Vdc
Input Voltage Range:	85–300 Vdc or 85–264 Vac 38.4–137.5 Vdc or 88–132 Vac, 18–60 Vdc polarity dependent

Power Consumption

AC:	<40 VA
DC:	<30 Watts

Input Voltage Interruptions

20 ms @ 24 Vdc
20 ms @ 48 Vdc
50 ms @ 125 Vac/Vdc
100 ms @ 250 Vac/Vdc

Digital Inputs

Contact Input

125 Vdc:	Pickup: 105–150 Vdc Dropout: <75 Vdc

Digital Outputs

DC Ratings

Rated Operational Voltage (U_e):	24–250 Vdc
Rated Voltage Range:	19.2–275 Vdc
Rated Insulation Voltage (U_i):	300 Vdc
Continuous Carry:	6 A at 70°C 4 A at 85°C
Make:	30 A @ 250 Vdc per IEEE C37.90
Thermal:	50 A for 1 s
Contact Protection:	360 Vdc, 40 J MOV protection across open contacts
Leakage Current in a 500 Ω load at Rated Voltage:	<0.02 mA
Impedance of a Closed Output, in D.C.:	<1 Ω
Bouncing Measured in Resistive Load of 10 kW at Rated Voltage:	<5 ms
Operating Time (Coil Energization to Contact Closure, Resistive Load):	Pickup time ≤5 ms typical Dropout time of ≤5 ms typical
Breaking Capacity (10,000 Operations):	Per IEC 60255-0-20: 1974: 24 V 0.75 A L/R = 40 ms 48 V 0.50 A L/R = 40 ms 125 V 0.30 A L/R = 40 ms 250 V 0.20 A L/R = 40 ms
Cyclic Capacity (2.5 Cycles/Second):	Per IEC 60255-0-20: 1974: 24 V 0.75 A L/R = 40 ms 48 V 0.50 A L/R = 40 ms 125 V 0.30 A L/R = 40 ms 250 V 0.20 A L/R = 40 ms
Mechanical Durability:	10 million no-load operations

AC Ratings

Operational Voltage (U_e):	250 Vac/Vdc
Rated Insulation Voltage (U_i):	300 Vac/Vdc
Utilization Category:	AC-15 (control of electromagnetic loads >72 VA)
Contact Rating Designation:	B300 (B = 5 A, 300 = rated insulation voltage)
Rated Operational Current (I_e):	3 A @ 120 Vac 1.5 A @ 240 Vac.
Conventional Enclosed Thermal Current (I_{the}) Rating:	5 A
Operate Current:	>1 mA
Rated Operational Voltage (U_e):	240 Vac
Voltage Protection Across Open Contacts:	270 Vac, 40 J
Pickup/Dropout Time:	≤16 ms (coil energization to contact closure).
Electrical Durability Make VA Rating:	3600 VA, cos j = 0.3
Electrical Durability Break VA Rating:	360 VA, cos j = 0.3
Mechanical Durability:	10,000 no-load operations
Rated Frequency:	50/60 ± 5 Hz

Type Tests

Electromagnetic Compatibility (EMC)

Emissions:	IEC 60255-25:2000 Canada ICES-001 (A) / NMB-001 (A)

Electromagnetic Compatibility Immunity

Conducted RF Immunity:	IEC 60255-22-6:2001 10 Vrms IEC 61000-4-6:2008 10 Vrms
Digital Radio Telephone RF Immunity:	ENV 50204:1995 10 V/m at 900 MHz and l.89 GHz
Electrostatic Discharge Immunity:	IEC 60255-22-2:2008 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEC 61000-4-2:2008 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEEE C37.90.3-2001 2, 4, and 8 kV contact; 4, 8, and 15 kV air
Fast Transient/Burst Immunity:	IEC 60255-22-4:2008 Class A: 4 kV at 5 kHz, 2 kV at 5 kHz on comm ports IEC 61000-4-4:2004 + CRGD:2006 4 kV at 5 kHz
Magnetic Field Immunity:	IEC 61000-4-8:2001 1000 A/m for 3 s, 100 A/m for 1 min IEC 61000-4-9:2001 1000 A/m
Power Supply Immunity:	IEC 60255-11:2008 IEC 61000-4-11:2004 IEC 61000-4-29:2000
Radiated Radio Frequency Immunity:	IEC 60255-22-3:2007 10 V/m IEC 61000-4-3:2008 10 V/m IEEE C37.90.2-2004 35 V/m

Surge Immunity:	IEC 60255-22-5:2008 1 kV Line-to-Line 2 kV Line-to-Earth IEC 61000-4-5:2005 1 kV Line-to-Line 2 kV Line-to-Earth
Surge Withstand Capability:	IEC 60255-22-1:2007 2.5 kV peak common mode 1.0 kV peak differential mode IEEE C37.90.1-2002 2.5 kV oscillatory 4 kV fast transient waveform

Environmental Tests

Cold:	IEC 60068-2-1:2007 16 hours at –40°C
Damp Heat, Cyclic:	IEC 60068-2-30:2005 25°C to 55°C, 6 cycles, 95% relative humidity
Dry Heat:	IEC 60068-2-2:2007 16 hours at +85°C
Vibration:	IEC 60255-21-1:1988 Class 1 Endurance, Class 2 Response IEC 60255-21-2:1988 Class 1 Shock Withstand, Bump Class 2 Shock Response IEC 60255-21-3:1993 Class 2 Quake Response

Safety

Dielectric Strength:	IEC 60255-5:2000 2500 Vac on contact inputs and contact outputs, 1 min 3100 Vdc on power supply, 1 min IEEE C37.90-2005 2500 Vac on contact inputs and contact outputs, 1 min 3100 Vdc on power supply, 1 min
Impulse:	IEC 60255-5:2000, 0.5 Joule 5 kV IEEE C37.90-2005, 0.5 Joule 5 kV
IP Code:	IEC 60529:2001 + CRGD:2003 IP20

Notes

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
selinc.com • info@selinc.com

PDS3620-01