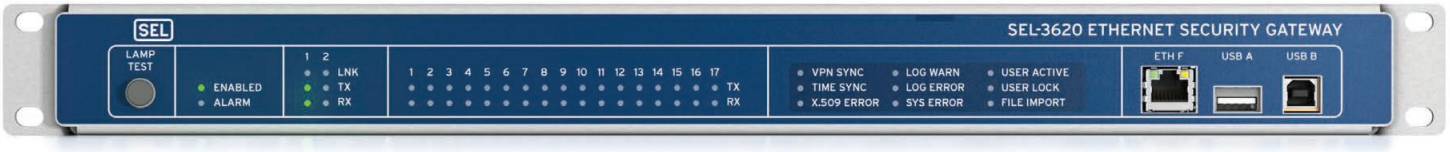
SEL-3620

Ethernet Security Gateway



Secure entire substation networks, and simplify device management.

- Integrated IED password management simplifies organizational compliance efforts.
- Multifactor authentication keeps engineering access to all devices secure.
- Deny-by-default firewall and IPsec VPN encryption protect all traffic entering and leaving the substation network.
- Embedded allowlist antivirus technology reduces zero-day virus threats.
- Analog bit-based protocol conversion to Ethernet eliminates reliance on costly leased analog circuits.
- Best-in-class encryption and authentication of information packets is provided with four IPsec profiles to choose from, including 2022 Secure with updated cipher suites.

Key Features

Secure Electronic Access Point to Electronic Security Perimeters

Use the SEL-3620 Ethernet Security Gateway to provide a central point of entry to bulk cyber systems with user-based access controls and detailed activity logs. Log onto the SEL-3620 jump host functionality, not individual IEDs. Manage user accounts and group memberships centrally using Lightweight Directory Access Protocol (LDAP)-accessible systems, such as Microsoft Active Directory. Additional Remote Authentication Dial-In User Service (RADIUS) functionality enables the use of multifactor authentication technology, such as RSA tokens.

Embedded Allowlist Anti-Malware

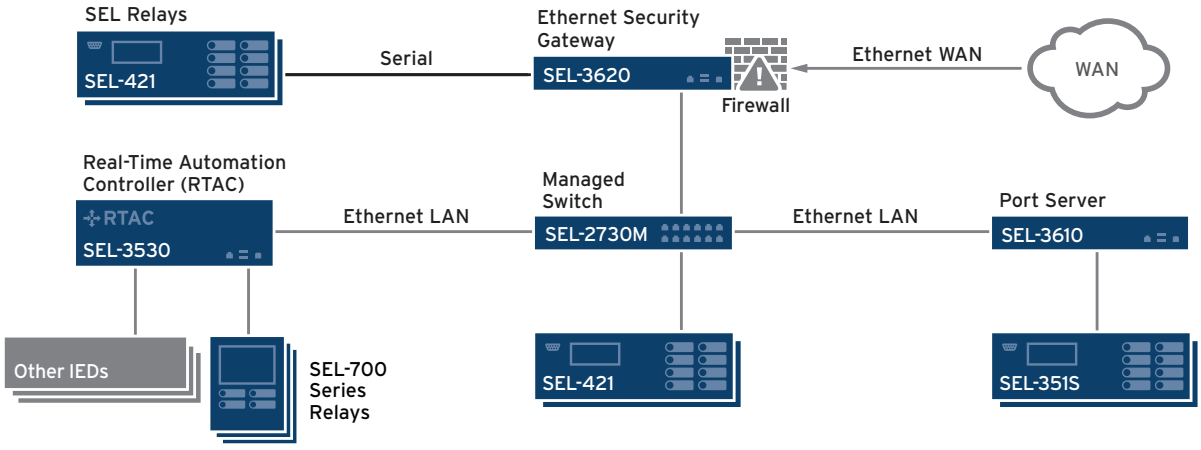
Resist known and unknown malware attacks with exe-Guard® embedded antivirus. Powerful rootkit resistance technology, embedded Linux mandatory access controls, and process allowlisting help mitigate attacks against the gateway itself and eliminate costly patch management and antivirus signature updates.

Substation Firewall and IPsec VPN Endpoint

Secure your substation network from malicious traffic with a powerful deny-by-default firewall. Manage status and configuration with an intuitive, menu-driven interface. Securely connect critical networks to the control center using IPsec VPNs. Use X.509 certificates with Online Certificate Status Protocol (OCSP) to centrally manage trust. The SEL-3620 is interoperable with Lemnos-compliant devices.

Strong Auditability and User Activity Reports

Log and time-stamp user access and every command entered on critical IEDs. Integrate event records into existing log management systems using Syslog. Protect IEDs with strong passwords, and block shared or default accounts. Granular access controls limit users' access to their assigned roles on individual IEDs. Log all successful or blocked connections to the firewall, and be alerted to the presence of unauthorized network communications attempts.



The SEL-3620 provides strong access control for your electronic security perimeter.

IED Password Management

Enforce strong passwords on IEDs, and have them automatically changed on a configurable schedule. Satisfy regulatory password requirements, and ensure that no weak or default passwords are in use. Manage passwords on IEDs that use command-line interfaces and on devices that use the Modbus protocol, such as GE UR series relays.

NERC CIP Requirement Support

Implement strong user-based access control to the electronic security perimeter (ESP) while protecting IEDs with strong passwords and blocking shared or default accounts. Granular access control limits a user's access to assigned roles on individual IEDs. Log all user activity, and quickly alert system operators via remote Syslog destinations.

Serial-to-Ethernet Transceiver

Expand your protocol compatibility by converting serial DNP3 and Modbus to Ethernet DNP3 TCP or UDP and Modbus TCP on the fly. Establish an Ethernet connection using Secure Shell (SSH), Telnet, TCP, or UDP encapsulation to create a persistent tunnel between a logical Ethernet port and a physical serial port. The device can also convert most bit-based protocols (Conitel, Tejas, Van Comm, etc.) to Ethernet to help replace analog links without disrupting existing systems.

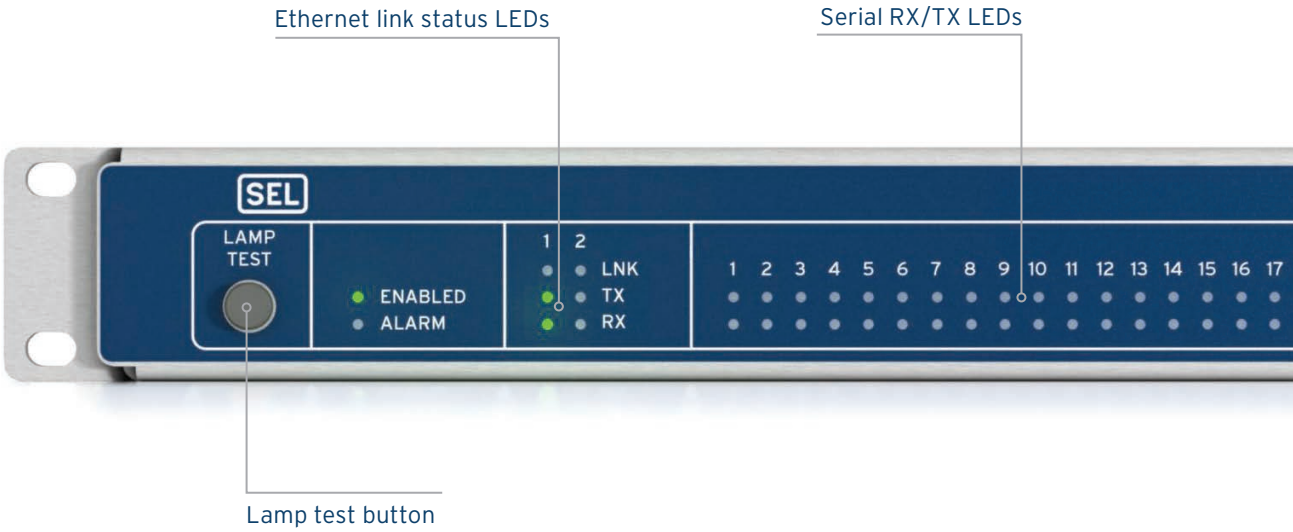
Virtual Software Client Support

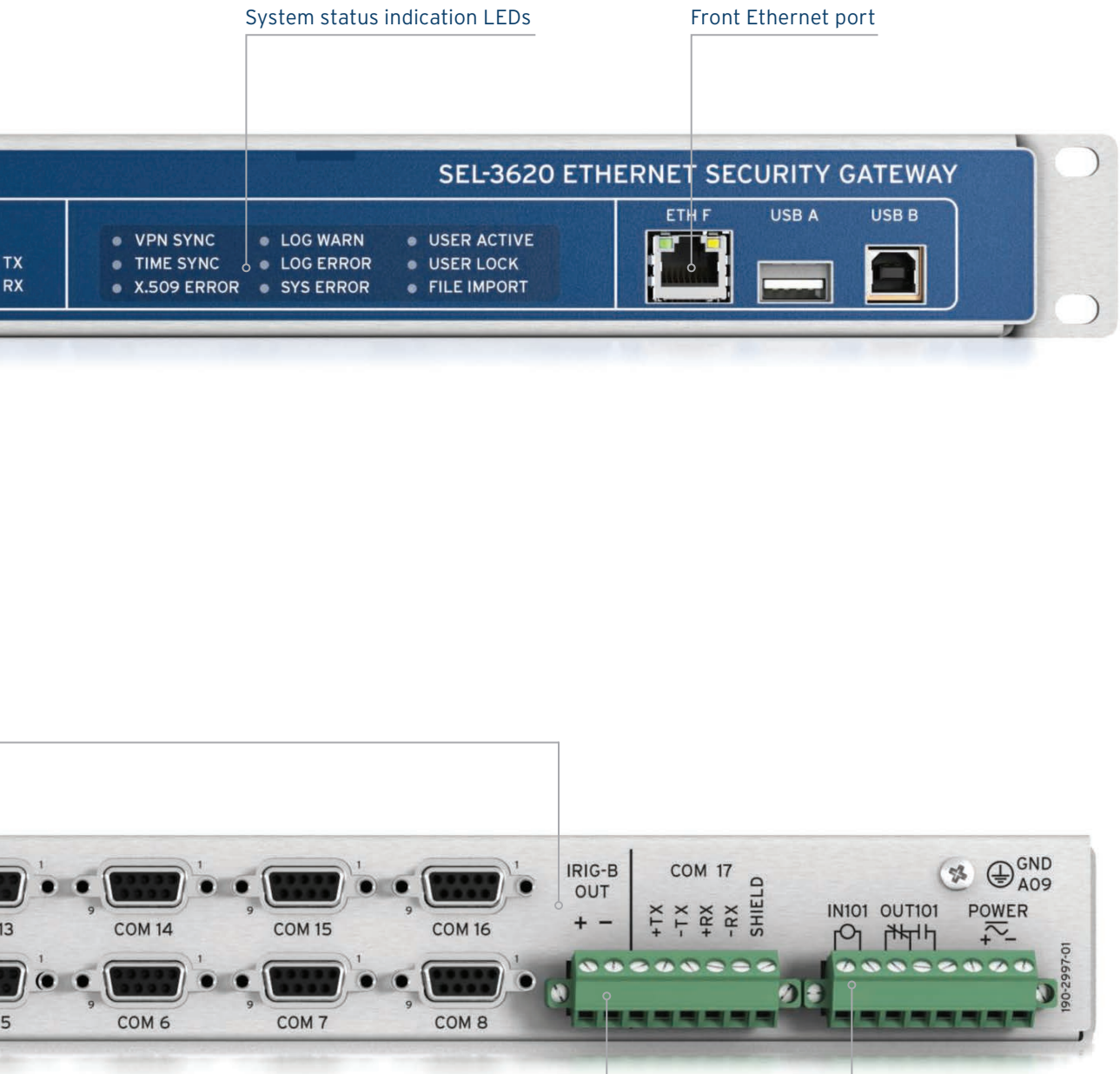
Transform unsecure serial or legacy Ethernet communications on Windows computers to cryptographically secure channels by using SEL-5827 Virtual Connect Client or SEL-5828 Virtual Port Service Software. These applications are provided free by SEL to make remote SEL-3620 ports available for existing software and terminal applications on your PC, including those using Modbus TCP/RTU. Data are secured using SSH with SEL-3620 port groups, master ports, and serial ports.

Secure Recloser Communications With MACsec

Use Media Access Control Security (MACsec) to enhance the existing cybersecurity of the SEL-651R and SEL-651RA recloser controls and reduce operation and maintenance expenses. MACsec secures Ethernet traffic (except IEC 61850 GOOSE and Parallel Redundancy Protocol [PRP] traffic) between an SEL-651R/651RA and SEL-3620 or Key Server MACsec-enabled routers/radios, providing confidential communication and maintaining message integrity between devices. Key management is automated via the MACsec Key Agreement (MKA) to simplify commissioning and improve the overall user experience.

Product Overview




System status indication LEDs
Front Ethernet port
SEL-3620 ETHERNET SECURITY GATEWAY
VPN SYNC
TIME SYNC
X.509 ERROR
LOG WARN
LOG ERROR
SYS ERROR
USER ACTIVE
USER LOCK
FILE IMPORT
ETH F
USB A
USB B
COM 14
COM 15
COM 16
COM 6
COM 7
COM 8
IRIG-B OUT
+ –
COM 17
+TX
-TX
+RX
-RX
SHIELD
IN101
OUT101
POWER
GND A09
190-2997-01
Isolated COM Port 17
Input contact

Applications

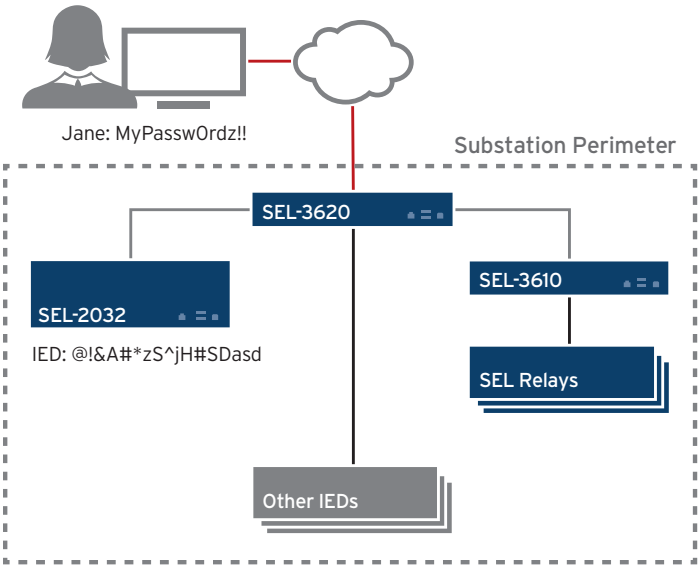
Sensible, Manageable, Scalable Cybersecurity Solutions

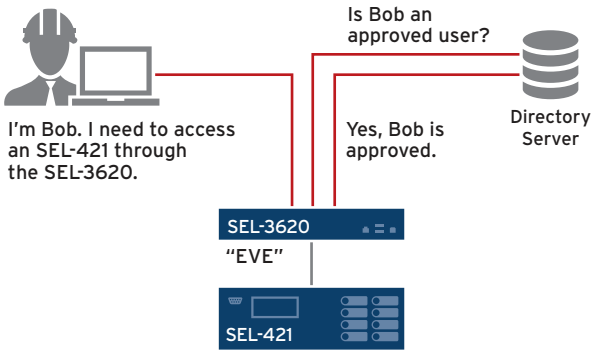
Protected Device Password Management

Manage IED passwords quickly and efficiently with the SEL-3620. Enforce strong passwords on IEDs that automatically change on a configurable schedule, and ensure that no default or weak passwords are in use on critical networks. Users only need to know their own password, not the IED's.

User Access Control

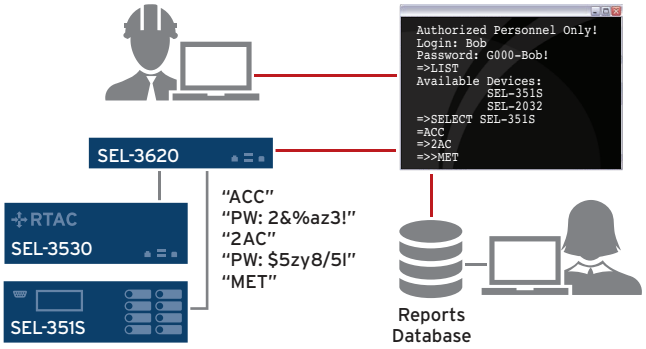
Query Microsoft Active Directory using LDAP or RADIUS. System administrators can easily add and remove user-based account access and authorized access levels to specific devices from a central location.





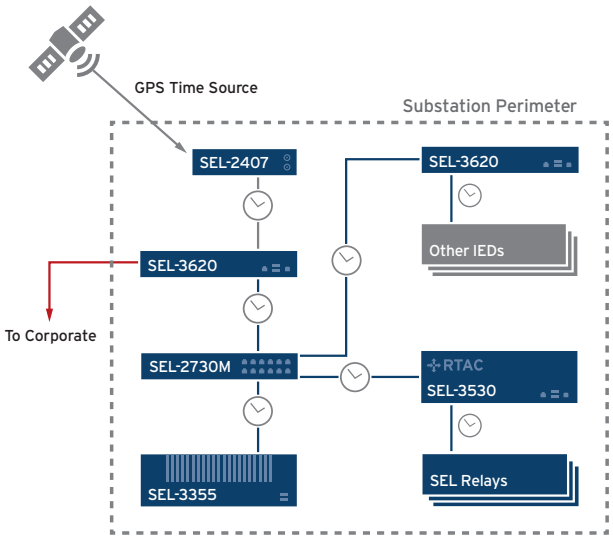
User Activity Reports

Provide granular reports that correlate unique users to individual IED commands. Thoroughly log all user activities on protected devices to know exactly who did what and when. Users with appropriate privileges can download connection reports for detailed user activity audits and to provide maximum user accountability.



Time Synchronization

Provide time synchronization to all your protected substation IEDs, data concentrators, and rugged computing devices. Distribute highly accurate time over both IRIG-B and the Ethernet-based Network Time Protocol (NTP). Should a satellite time source be disrupted temporarily, the SEL-3620 will synchronize substation time using its own internal clock.



SEL-3620 Specifications

General	
Network Interfaces	Ports: 2 rear, 1 front
	Data Rates: 10/100 Mbps
	Front Connector: RJ45 female
	Rear Connectors: RJ45 female or LC fiber (single-mode 100BASE-LX10 or multimode 100BASE-FX)
	VLANs: Up to 4 per physical interface
	Data Throughput: 100 Mbps
Routing Functions	Routing Protocol: Static routes
	Network Access Translation (NAT): Outbound NAT (SNAT), port forwarding (DNAT)
	Firewall: Stateful
Serial Ports	Ports: 17 rear
	Type: EIA-232/EIA-485 (software-selectable)
	Data Rate: 1200 to 115200 bps
	Connector: DB-9 female (Ports 1—16), isolated 8-pin (Port 17)
	Power: +5 Vdc power on Pin 1 (500 mA maximum)
	Protocol Support: Byte- and bit-based serial protocols
Time Synchronization	NTP: Server and client
	IRIG-B Input: BNC connector, IRIG B000 or B002, even or odd parity
	IRIG-B Output: BNC connector, serial ports (Pins 4 and 6), IRIG B000 even parity
User Authentication	Local Accounts: 256 maximum local accounts, requires strong passwords (8—128 characters)
	LDAP: v3, TLS-secured
	RADIUS: PAP, EAP-PEAP/MSCHAPv2, EAP-TTLS/PAP
Logging and Alerting	SNMP Traps: v1/v2c/c3
	Syslog: UDP transport
	RADIUS: Accounting packets
Physical Tamper Detection	Input Contact: 1 (pickup/dropout depends on source)
Additional Cybersecurity Controls	IED Password Management: Suggested maximum 100 devices
	IED Authentication Proxy: Suggested maximum 100 devices
	IPsec VPNs: Tunnel mode, IKEv1/IKEv2, passphrase or X.509
	IPsec Throughput: 30 Mbps
	Embedded Antivirus: exe-GUARD allowlisting antivirus
	Authorization Levels: Technician and Administrator
	SSH: Server and client
Power Supply Options	125/250 Vdc or 110/240 Vac, 50/60 Hz
	85—300 Vdc or 85—264 Vac
	48/125 Vdc, 120 Vac, 50/60 Hz
	38.4—137.5 Vdc, 88—132 Vac
	24/48 Vdc
	18—60 Vdc (polarity-dependent)
	<30 Watts
Operating Temperature	−40° to +85°C (−40° to +185°F)

SEL SCHWEITZER ENGINEERING LABORATORIES

Making Electric Power Safer, More Reliable, and More Economical
+1.509.332.1890 | info@selinc.com | selinc.com

PF00197 • 20221010