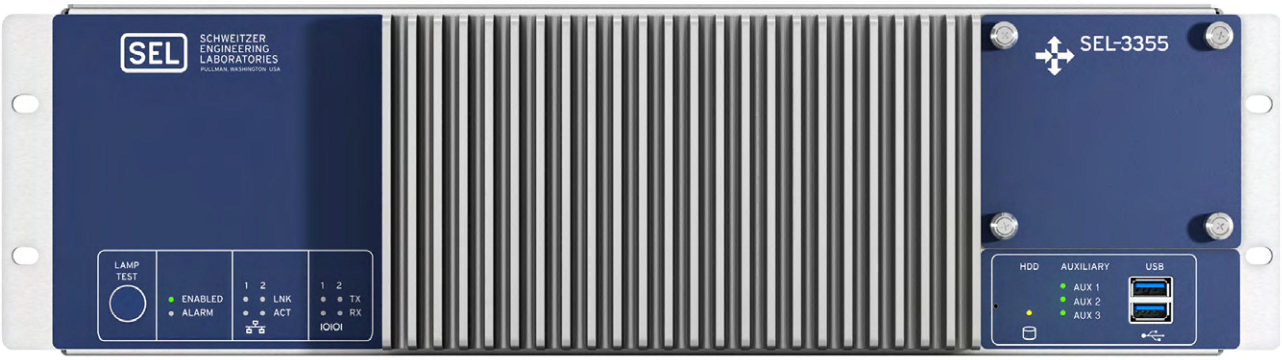
SEL Unified Threat Management Firewall

Rugged Solution for Threat Management



Key Features and Benefits

The SEL-3355 Unified Threat Management (UTM) Firewall is an OPNsense-based, state-of-the-art firewall and router purposely built for substation and industrial environments. With advanced routing capabilities, this device offers complete and scalable edge-router solutions for small and large substations. The robust and reliable hardware and excellent redundancy features ensure low downtime and provide maximum data security. The SEL-UTM offers several high-end features:

- **Flexible and Rugged Hardware.** The SEL-UTM is designed and tested to withstand vibration, electrical surges, fast transients, and extreme temperatures. The standards to which it is built meet or exceed protective relay standards. The SEL-UTM is built with a modular design that supports up to 10 Ethernet ports and an option for dual redundant power supplies. The device contains no moving parts and operates over a wide temperature range from –40°C to +75°C.
- **High Availability.** The SEL-UTM uses the Common Address Redundancy Protocol (CARP) for hardware failover or for load balancing. Two or more firewalls can be configured as a failover group. For failover setup, if one interface fails on the primary firewall or the primary firewall goes offline entirely, the secondary firewall becomes active. Using this powerful feature creates a fully redundant firewall system with automatic and seamless failover that allows for updating and making changes to the firewall settings. While switching to the backup, network connections remain active with minimal interruption for throughput communications. For a load balancing group, multiple firewalls will share the communications load. Load balancing can be used to split the portion of outbound traffic between two SEL-UTM firewalls. The traffic can be divided equally or weighted. This enhances the total available bandwidth and lowers the load on each SEL-UTM.
- **Dynamic Routing.** The SEL-UTM supports adaptive routing protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Routing Information Protocol (RIP). These routing protocols improve configurability and fault tolerance; in the case of a connection break, the SEL-UTM finds an alternate route.
- **Stateful Firewall.** A *stateful firewall* is a network firewall that keeps track of the state of network connections (such as TCP streams, UDP communication, etc.) traveling across it. This tracking increases firewall filtering capabilities while reducing configuration needs. The SEL-UTM firewall has flexible configuration options that use categorizations, aliases, and groupings for demanding architectures through an intuitive web-based graphical interface.
- **Flexible Network Address Translation (NAT).** The SEL-UTM supports multiple flexible network address translation (NAT) options, such as one-to-one, port forwarding, and outbound NAT, and supports multiple public interfaces.

- **Network Intrusion Detection/Prevention System.** Based on Suricata by the Open Information Security Foundation, the SEL-UTM built-in Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS) provide a state-of-the-art packet acquisition and threat-detection engine, with input and output support for popular security information and event management (SIEM) solutions. Deployed as an edge router, the SEL-UTM actively records, filters out, and detects malicious code in incoming packets. This powerful deep-packet inspection system can be used to mitigate security threats at wire speed.
- **Network Management System Integration Technologies.** The SEL-UTM supports seamless integration with third-party network management software (NMS) using Simple Network Management Protocol (SNMP), SNMPTraps, and Representational State Transfer application program interfaces (REST APIs). The SEL-UTM also supports syslog for remote management and logging capabilities and MONIT, which provides extensive monitoring capabilities with the ability to send email. In modern networking solutions, a centralized management device is often an optimal solution for monitoring of other gateways, receiving updates, notifications, and alerts, across the network.
- **Flexible Interface Assignments.**
  - Bridge Mode: Connect two or more subnet branches with SEL-UTM bridged interfaces. The SEL-UTM bridged interfaces are loop resistant and fault tolerant through the use of Rapid Spanning Tree Protocol (RSTP).
  - VxLAN: Use virtual extensible local area networks (VxLANs) to overlay virtualized Layer 2 networks over Layer 3 networks, as described by RFC7348.
  - VLAN: Create VLAN interfaces to segregate and manage traffic that shares the same physical links.
  - Generic Routing Encapsulation (GRE): Encapsulate a wide variety of network layer protocols for safe transmission, such as in passing routing information between connected networks in conjunction with a VPN.
  - Link Aggregation (LAGG): Combine multiple physical interfaces together virtually as one logical interface using LAGG—such a combination provides higher speeds and increased fault tolerance.
  - Virtual IP (VIP): Create an address that does not correlate to a physical interface. Such an address is useful for one-to-many NAT, fault tolerance (to provide a backup for when an interface fails). and mobility, providing virtual IDs to share among live services as necessary.
- **Virtual Private Networks (VPN).** Protect WAN communications with IPsec or OpenVPN-based VPNs. IPsec is great at securing site-to-site communications, while OpenVPN excels at protecting host-to-site communications. Using the SEL-UTM as a VPN terminator allows multiple users and services to obtain confidential, authenticated, disruption-free access to the protected network.
- **Captive Portal.** Implement access control for transient devices and users through the SEL-UTM captive portal. This helps to achieve and maintain compliance with many utility cyber security standards such as NERC CIP. The SEL-UTM captive portal enables continuous monitoring of local user access attempts and the transient devices they use.

Product Overview

You can place the SEL-UTM as a Level 5 device (as shown in *Figure 1*)within an energy control system defense-in-depth model to provide logical separation between the industrial control system and the WAN; the convergence of informational technology (IT) and operational technology (OT) networks remains protected. As a Level 3 device, as shown in *Figure 1*, the SEL-UTM provides both a tiered system of access and separation between the automation and protection systems and their less secure computers and configuration tools.

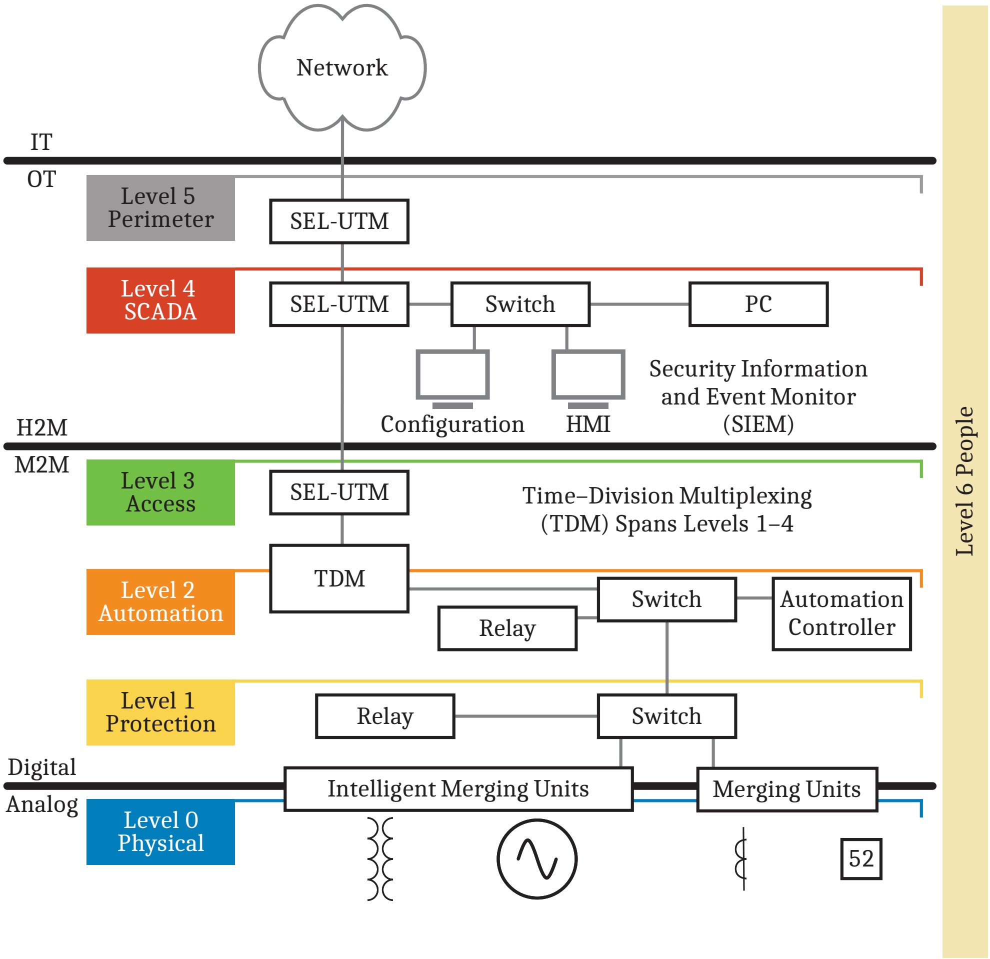


Figure 1 The Energy Control Systems (ECS) Defense-In-Depth Model

Security controls can be implemented with the SEL-UTM at these levels. The deny-by-default stateful firewall allows only authorized traffic and IPsec virtual private networks to secure all site-to-site communications. The properly configured firewall can then bolster the security posture of the industrial control system (ICS) environment by providing confidentiality, integrity, and the encryption of mission-critical information through the following:

- Protecting mission-critical infrastructure by preventing any direct access from external networks.
- Providing seamless IT/OT convergence with industrial-grade reliability at the edge of the substation using IT features such as BGP, HA, and load balancing for multiple protected LANs and DMZs.
- Securing the private network inside the substation through deep-packet inspection: detecting and intercepting viruses and other malicious traffic.
- Preventing information leaks through the ability to block egress based on protocol.
- Imposing a secure management configuration of the SEL-UTM through a secure web management interface by using either a web browser or REST APIs.
- Logging the events, made available for remote viewing by forwarding messages to a centralized syslog server or federated network management system, for forensics and troubleshooting.

Features

Virtual Private Network. The SEL-UTM offers a wide range of VPN technologies such as Transport Layer Security (TLS) and IPsec and supports site-to-site and road-warrior configurations.

Intuitive GUI. The modern user interface provides an intuitive user experience with multi-language support, built-in help, and fast navigation through use of the search box.

Time Synchronization. The SEL-UTM supports time synchronization using Network Time Protocol (NTP).

Secure Ethernet Communications. Secure Shell (SSH) and TLS provide confidential authenticated communications and device management.

Centralized User-Based Access. Enforce strong, centralized access control and user accountability with Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS). The SEL-UTM simplifies compliance with accurate logging.

Anti-Malware Protection. Protects HTTP and HTTPS connections against ransomware, trojans, viruses, and other malware.

Reporting and Monitoring. Remote and local logging capabilities with the ability to create real-time graphs.

Comprehensive Diagnostics and Reporting. Built-in tools such as packet captures, pings, and port probes to diagnose and troubleshoot networking issues.

Remote Network Management. Use various interfaces such as a web-based GUI, REST API, and a command line to manage a fleet of UTM firewalls.

Additional Features.

- Stateful packet inspection (SPI)
- Traffic shaping
- GeoIP blocking
- Anti-spoofing
- Time-based rules
- Connection limits
- Dynamic DNS
- Reverse proxy
- Captive portal
- Support for concurrent IPv4 and IPv6
- NAT mapping
- Configurable static routing
- Multiple IP addresses per interface
- DHCP server
- DNS forwarding

Application Examples

Perimeter Firewall to Secure Communications Over Untrusted Networks

The SEL-UTM secures all-substation-to-substation or substation-to-control-center communications over the public or private wide area network (WAN) by establishing secure IPsec VPN tunnels with other IPsec-enabled devices as shown in *Figure 2*.

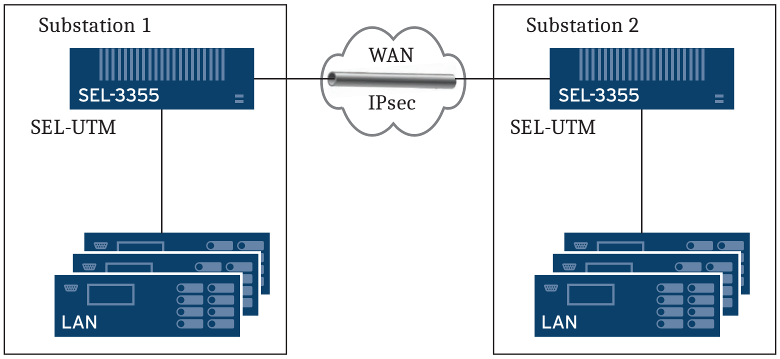


Figure 2 Using SEL-UTM to Secure Substation-to-Substation Communication Over Public WAN Through Use of IPsec

Secure Electronic Perimeter With the Ability to Detect and Prevent Attacks

You can use the SEL-UTM to create a DMZ, a buffer zone between the substation LAN and external WAN. You can use the built-in Suricata-based IDS/IPS of the SEL-UTM to detect and deter cyber attacks.

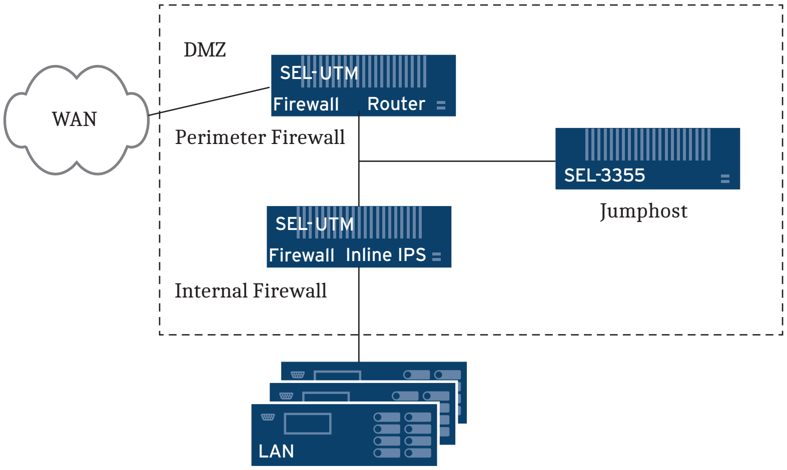


Figure 3 Using SEL-UTM in a Dual Firewall DMZ Setup to Secure a Substation LAN

Use Traffic Shaping to Limit Bandwidth and Prioritize Message Exchange

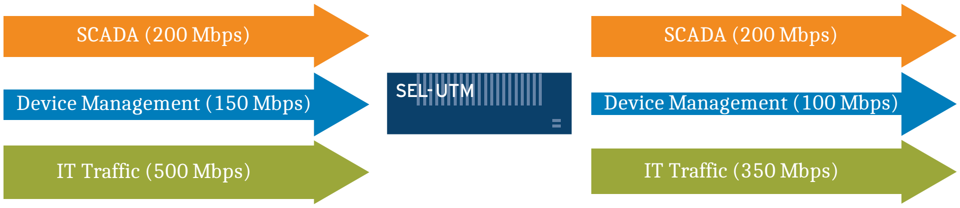


Figure 4 Using Traffic Shaping to Prioritize OT Traffic

SEL-UTM traffic shaping is a reliable way to limit bandwidth for various IT and OT applications, prioritize the network traffic, or both. SEL-UTM provides flexibility for configuring bandwidth limitations based upon the interface(s), IP source and destination, direction of traffic (in/out) and port numbers (application). Users can use pipes to define the allowed bandwidth, queues to determine a weight within each pipe, and rules to apply the shaping to a certain package flow.

Diagrams and Dimensions

Figure 5 shows dimensions for the SEL-3355.

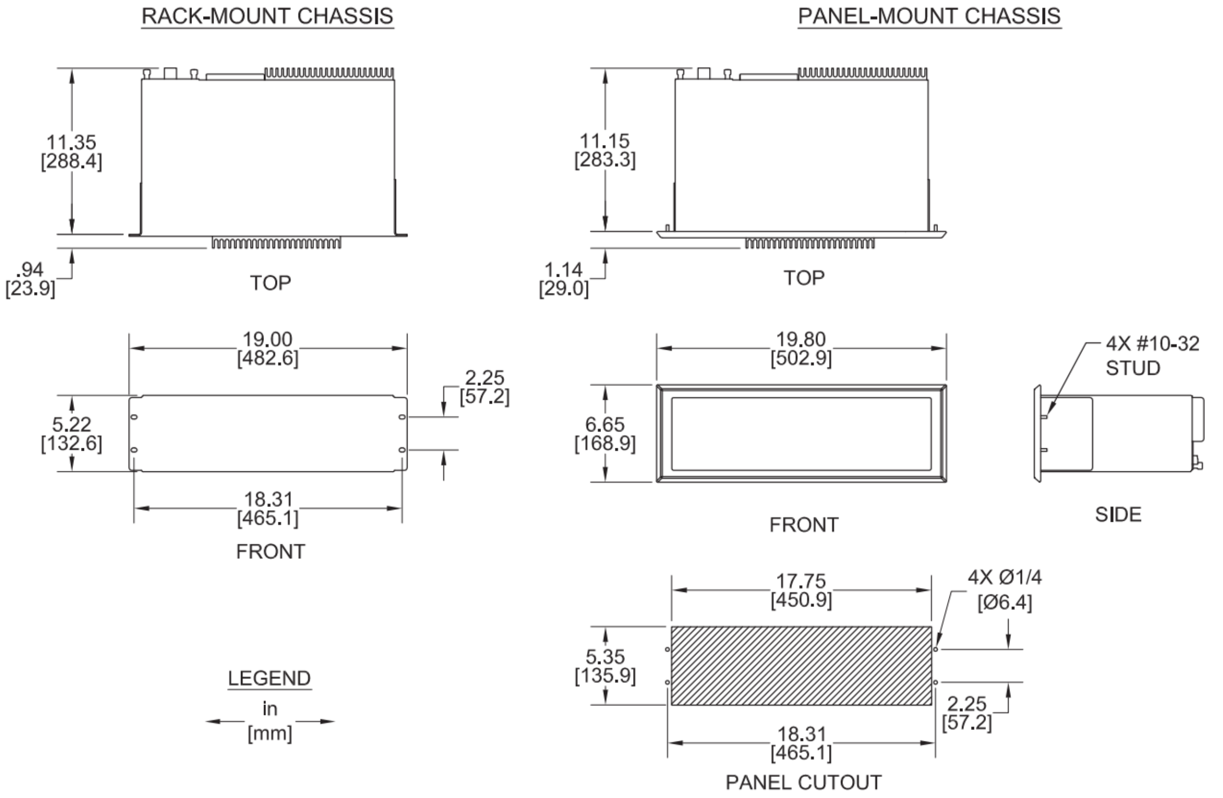


Figure 5 SEL-3355 Dimensional Drawings

SEL-3355 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 his own expense.

CE Mark
RoHS Compliant

General

CPU

Intel Xeon E3-1505L Quad-Core

Speed:	2.0 GHz base, 2.8 GHz turbo
Cache:	1 MB L2, 8 MB L3

RAM

8–16 GB DDR4 ECC PC4-17000 (2133 MHz)

Chipset

Intel CM236 Chipset

Mass Storage

Internal Drive Bay:	One 2.5 inch SSD SATA II 3.0 Gb/s
Optional SATA Drives:	Industrial-Grade SLC SSD 30–250 GB 10-year warranty Industrial-Grade iMLC SSD 120–480 GB 5-year warranty

Video

Intel P530 Graphics Controller

Audio

TSI (IDT) 92HD91 HD Audio Codec
3 Analog 3.5 mm TRS

USB

4 Rear-Panel Ports, 2 Front-Panel Ports

USB 3.1 Compliant

2000 mA Maximum Current Each

Cable Length <2 m

2 Internal Ports on 1 Main Board Header

USB 2.0 Compliant

Fuse Ratings

LV Power Supply Fuse Rating:	15 A
Maximum Rated Voltage:	500 Vdc, 500 Vac
Breaking Capacity:	20 kA at 500 Vdc
Type:	Time-lag T
HV Power Supply Fuse Rating:	5 A
Maximum Rated Voltage:	250 Vdc, 277 Vac
Breaking Capacity:	1500 A at 277 Vac
Type:	Time-lag T
Heater Fuses F2, F3:	5 A, 125 V slow blow 125 Vdc/50 A break rating Fuses are not serviceable.

Alarm Output Contact

Per IEC 255-0-20:1974, using the simplified method of assessment Output Type:	Relay, Form C, break-before-make
Power Supply Burden:	<1 W maximum
Mechanical Life:	2,000,000 operations
Operational Voltage:	250 Vac/Vdc
Make:	30 A at 250 Vdc
Carry:	6 A continuous at 70°C
1 s Rating:	50 A
MOV Protection:	270 Vac/360 Vdc, 75 J
Insulation Voltage:	300 Vac/Vdc
Pickup Time:	<8 ms
Dropout Time:	<8 ms

Breaking Capacity (10000 operations):

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

Terminal Connections

Compression Screw Terminal

Power Wiring Insulation:	300 V minimum
Size:	12–18 AWG
Alarm Wiring Insulation:	300 V minimum
Size:	12–18 AWG
Tightening Torque	
Minimum:	0.6 Nm (5 in-lb)
Maximum:	0.8 Nm (7 in-lb)

Crimp Ferrule Recommended.

Mounting Ear Tightening Torque	
Minimum:	0.18 Nm (1.6 in-lb)
Maximum:	0.25 Nm (2.2 in-lb)

Grounding Screw

Ground Wiring Insulation:	300 V minimum
Size:	12 AWG, length <3 m
Tightening Torque	
Minimum:	0.9 Nm (8 in-lb)
Maximum:	1.4 Nm (12 in-lb)

Ring Terminal Recommended.

Serial Port

Tightening Torque	
Minimum:	0.6 Nm (5 in-lb)
Maximum:	0.8 Nm (7 in-lb)

Video Port

Tightening Torque

Minimum:	0.6 Nm (5 in-lb)
Maximum:	0.8 Nm (7 in-lb)

Temperature Range

Operating

With E3-1505L CPU:	–40° to +75°C (–40° to +167°F)
With E3-1505M CPU:	–40° to +60°C (–40° to +140°F)

Note: UL ambient 40°C. See *Safety Information* in the SEL-3355 Instruction Manual for additional restrictions.

Storage

–40° to +85°C (–40° to +185°F)

Relative Humidity

5% to 95% noncondensing

Maximum Altitude

5000 m

Atmospheric Pressure

80–110 kPa

Overvoltage Category

Category II

Insulation Class 1

Pollution Degree 2

Weight

9.072 kg (20 lb) maximum

Product Standards

Communications Equipment in Utility Substations:	IEC 61850-3:2013 IEEE 1613-2009 Severity Level: Class 1
Industrial Environment:	IEC 61000-6-2:2005 IEC 61000-6-4:2006
Electrical Equipment for Measurement, Control, and Laboratory Use:	IEC 61010-1:2013 UL 61010-1:2016, C22.2 No. 61010-1:12 IEC 61010-2-201:2013 UL 61010-2-201:2017, C22.2 No. 61010-2-201:14
Measuring Relays and Protection Equipment:	IEC 60255-26:2013 IEC 60255-27:2013

Type Tests

Note: To ensure good EMI and EMC performance, type tests were performed using shielded Ethernet and serial cables with the shell grounded at both ends of the cable, and the USB, video, and audio cables with ferrite chokes. Double-shielded cables are recommended for best EMI and EMC performance.

Electromagnetic Compatibility Emissions

Conducted and Radiated Emissions:	CISPR 11:2009 + A1:2010 CISPR 22:2008 CISPR 32:2015 IEC 61000-6-4:2006 IEC 61850-3:2013 FCC 15.107:2014 FCC 15.109:2014 Severity Level: Class A Canada ICES-001(A) / NMB-001(A)
Harmonic Current:	IEC 61000-3-2:2014
Severity Level:	Class A
Voltage Flicker:	IEC 61000-3-3:2013

Electromagnetic Compatibility Immunity

Conducted RF:	IEC 61000-4-6:2013 Severity Level: 10 Vrms
Electrostatic Discharge:	IEC 61000-4-2:2008 IEEE C37.90.3-2001 Severity Level: 2, 4, 6, 8 kV contact discharge; 2, 4, 8, 15 kV air discharge
Fast Transient/Burst:	IEC 61000-4-4:2012 Severity Level: Class A 4 kV, 5 kHz on power supply and outputs; 2 kV, 5 kHz on communications lines
Magnetic Field:	IEC 61000-4-8:2009 Severity Level: 1000 A/m for 3 s 100 A/m for 1 m
Power Supply:	IEC 61000-4-11:2004 IEC 61000-4-17:1999+A1:2001 +A2:2008 IEC 61000-4-29:2000
Radiated Radio Frequency:	IEC 61000-4-3:2006+A1:2007 Severity Level: 10 V/m
Surge Withstand Capability:	IEC 61000-4-18:2006+A1:2010 Severity Level: Power supply and outputs 2.5 kV peak common mode 1.0 kV peak differential mode Communications ports 1.0 kV peak common mode
	IEEE C37.90.1-2012 Severity Level: 2.5 kV oscillatory 4 kV fast transient
Surge Immunity:	IEC 61000-4-5:2005 1 kV line-to-line 2 kV line-to-earth 2 kV communications ports

Environmental

Change of Temperature:	IEC 60068-2-14:2009 Severity Level: 5 cycles, 1°C per minute ramp –40°C to +60°C (E3-1505M CPU) –40°C to +75°C (E3-1505L CPU)
Cold, Operational:	IEC 60068-2-1:2007 Severity Level: 16 hours at –40°C
Cold, Storage:	IEC 60068-2-1:2007 Severity Level: 16 hours at –40°C
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 12 + 12-hour cycle 25° to 55°C, 6 cycles, >93% r.h.
Damp Heat, Steady:	Severity Level: 40°C, 240 hours, >93% r.h.
Dry Heat, Operational:	IEC 60255-1:2009 IEC 61850-3:2013 IEC 60068-2-2:2007 Severity Level: 16 hours at 60°C (E3-1505M CPU) 16 hours at 75°C (E3-1505L CPU)
Dry Heat, Storage:	IEC 60255-1:2009 IEC 61850-3:2013 IEC 60068-2-2:2007 Severity Level: 16 hours at 85°C

Free Fall:	IEEE 1613-2009 Severity Level:100 mm
Vibration:	IEC 60255-21-1:1988 Severity Level: Endurance Class 2 Response Class 2
	IEC 60255-21-2:1988 Severity Level: Shock Withstand, Bump Class 1 Shock Response Class 2
	IEC 60255-21-3:1993 Severity Level: Quake Response Class 2

Safety

Enclosure Protection:	IEC 60529:2001 + CRGD:2003 Severity Level: IP30
Dielectric Strength:	IEC 60255-27:2013 IEEE C37.90-2005 Severity Level: 3600 Vdc on power supply 2500 Vac on contact output 1500 Vac Ethernet ports Type tested for one minute
Impulse:	IEC 60255-27:2013 IEEE C37.90-2005 Severity Level: 5 kV common mode, power supply, contact outputs 1.5 kV Ethernet ports

Performance

Unencrypted Throughput:	885 Mbps (approx.)
Encrypted Throughput:	835 Mbps IPsec

Core Features

Stateful Firewall

Filter By:	Source Destination Protocol Port OS (OSFP)

Limit Simultaneous Connections On a Per-Rule Basis

Log Matching Traffic On a Per-Rule Basis

Policy-Based Routing

Packet Normalization

Option to Disable Filter for Pure Router Mode Granular Control State Table

Adjustable State Table Size

On a Per-Rule Basis:	Limit simultaneous client connection Limit states per host Limit new connections per second Define state time-out Define state type
State Types:	Keep Sloppy Modulate Synproxy None
Optimization Options:	Normal High latency Aggressive Conservative

2-Factor Authentication

Supports TOTP

Google Authenticator

Support Services:	Captive Portal Proxy VPN GUI

802.1Q VLAN Support

Max 4096 VLANs

Network Address Translation

Port Forwarding

1:1 of IPs and Subnets

Outbound NAT

NAT Reflection

Network Prefix Translation

Traffic Shaping

Limit Bandwidth

Share Bandwidth

Prioritize Traffic

Rule Based Matching:	Protocol Source Destination Port Direction

IGMP Proxy

For Multicast Routing

Universal Plug and Play

Fully Supported

Dynamic DNS

Selectable From a List

Custom

RFC 2136 Support

DNS Forwarder

Host Overrides:	A records MX records

Access Lists

DNS Filter

Supports OpenDNS

DHCP Server

IPv4 and IPv6

Relay Support

BOOTP Options

Multi WAN

Load Balancing

Failover

Aliases

Load Balancer

Balance Incoming Traffic Over Multiple Servers

Network Time Server

Intrusion Detection and Prevention

Inline Prevention

Integrated Rulesets:	SSL Blacklists Feodo Tracker Geolite2 Country IP Emerging Threats ETOpen

SSL Fingerprinting

Auto Rule Update Using Configurable Cron

Captive Portal		
	Typical Applications:	Transient Device Network Template Management Multiple Zones
	Authenticators:	LDAP Radius Local User Manager Vouchers / Tickets
	Voucher Manager:	Multiple Voucher Databases Export vouchers to CSV
	Timeouts and Welcome Back	
	Bandwidth Management:	Share evenly Prioritize Protocols Ports IP
	Portal Bypass:	MAC and IP whitelisting
	Real-Time Reporting:	Live top IP bandwidth usage Active Sessions Time left Rest API
Virtual Private Networks		
	IPsec:	Site to Site
	OpenVPN:	Site to Site Road Warrior Easy client configuration exporter
High Availability		
	Automatic Hardware Failover	
	Synchronized State Table	
	Configuration Synchronization	
Caching Proxy		
	Multi Interface	
	Transparent Mode	
	Access Control Lists	
	Blacklists	
	Category-Based Web-Filter	
	Traffic Management	
	Auto Sync for Remote Blacklists	
	ICAP (Supports Virus Scan Engine)	
System Health		
	Round Robin Data	
	Selection and Zoom	
	Exportable	
Backup and Restore		
	History and Diff Support	
	File Backup	
SNMP		
	Monitor and Traps	
Diagnostics		
	Filter Reload Status	
	Firewall Info (pfInfo)	
	Top Users (pfTop)	
	Firewall Tables:	Aliases Bogons
	Current Open Sockets	
	Show All States	
	State Reset	
	State Summary	
	Wake on LAN	
	ARP Table	
	DNS Lookup	
	NDP Table	
	Ping	
	Packet Capture	
	Test Port	
	Trace Route	
	Traffic Graph	
Network Monitoring		
	Netflow Exporter	
	Network Flow Analyzer:	Fully Integrated CVS Exporter
REST API		
	ACL Support	

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

© 2020–2021 by Schweitzer Engineering Laboratories, Inc. All rights reserved.

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders. No SEL trademarks may be used without written permission. SEL products appearing in this document may be covered by U.S. and Foreign patents.

Schweitzer Engineering Laboratories, Inc. reserves all rights and benefits afforded under federal and international copyright and patent laws in its products, including without limitation software, firmware, and documentation.

The information in this document is provided for informational use only and is subject to change without notice. Schweitzer Engineering Laboratories, Inc. has approved only the English language document.

This product is covered by the standard SEL 10-year warranty. For warranty details, visit selinc.com or contact your customer service representative.

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

ISO 9001 CERTIFIED

WORLDWIDE 10 years WARRANTY

PDSUTM-01