



**Next Generation Firewalls:
ciberseguridad para infraestructuras
críticas industriales.**

**¡Bienvenidos!
Hora de Inicio 9:35
12 de Febrero de 2021**

Zona de registro y próximos Webinars

Si está interesado puede registrarse en alguno de los próximos Webinars en:

<https://siemens.es/workshops>

SIEMENS - Webinars 2021

SOLICITUD DE ASISTENCIA

En primer lugar, queremos agradecer su interés por participar en alguno de los Webinars 2021 que hemos previsto para el próximo semestre.

.....

Podrá indicar 1 único Webinar / Registro, pudiendo realizar tantos registros como Nº de Webinars a los que desea asistir.

.....

LEY DE PROTECCIÓN DE DATOS

Los datos que nos aporte en el momento de su registro se incorporarán en la Base de datos de SIEMENS, S.A. para los siguientes fines:

- Gestión integral del evento o la campaña referidos, así como el envío de información sobre eventos o campañas similares del responsable.
- El envío de información sobre otros productos y servicios.

Legitimación: Consentimiento del interesado.

Destinatarios: No se cederán datos a terceros, salvo obligación legal.

Derechos: Acceder, rectificar, suprimir los datos y otros derechos, como se explica en la información adicional.

* Obligatorio

1. Indique el Webinar para el que solicita el registro. *

☒

03/11/20 - Webinar - SIMATIC Ecosystem. Completa Solución de Automatización para la Industria 4.0. Horario: 16:00-17:00 h

☒

06/11/20 - Webinar - SIMATIC Ecosystem. Completa Solución de Automatización para la Industria 4.0. Horario: 09.30-10.30 h

1. Indique el Webinar para el que solicita el registro.

Selecciona la respuesta

24/11/20 - Webinar - TIA Portal Ecosystem. Concepto y aplicación en la I4.0 Horario: 16.00-17.00 h

27/11/20 - Webinar - TIA Portal Ecosystem. Concepto y aplicación en la I4.0 Horario: 09.30-10.30 h

01/12/20 - Webinar - Eficiencia Energética enfocada al uso de variador de velocidad. Horario: 16:00-17:00 h

04/12/20 - Webinar - Eficiencia Energética enfocada al uso de variador de velocidad. Horario: 09.30-10.30 h

09/12/20 - Webinar - Ejemplos de digitalización en instrumentación. Horario: 16:00-17:00 h

11/12/20 - Webinar - Ejemplos de digitalización en instrumentación. Horario: 09:30-10:30 h

15/12/20 - Webinar - SIMATIC Drive Controller basado en S71500T: Solución ultra compacta Horario: 16:00-17:00 h

18/12/20 - Webinar - LOGO! 8.3. El Mini PLC de siempre, ahora con conexión a la nube !!! Horario: 09.30-10.30 h

Soluciones de Comunicaciones de Conectividad Digital de SIEMENS

Cyber Security,
Edge, Cloud, IoT,
Software

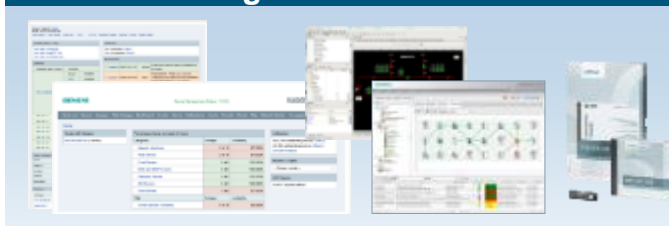
Cyber Security Solutions



IoT, Edge Computing, Cloud



Network Management Software

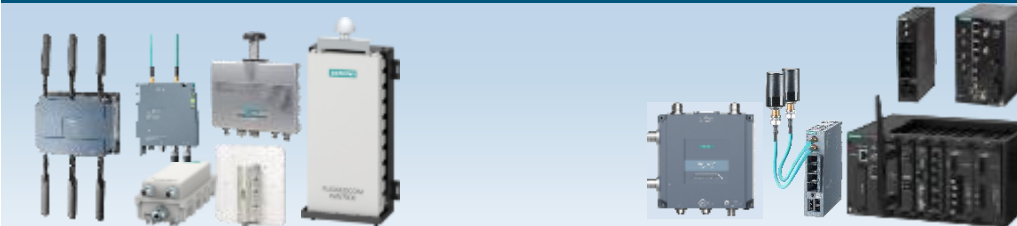


WAN and
Backhaul

Layer 3 Multiservice Platform and Routing



Wireless – Private & Public Solutions



Advanced LAN,
Digital
Substation &
Process Bus

Redundant Networks with PRP/HSR



Time Synchronization with IEEE1588



Substation LAN,
Legacy Support

Layer 2 Ethernet Switches



Media Converters, Serial Servers, Modems, Cables & Connectors





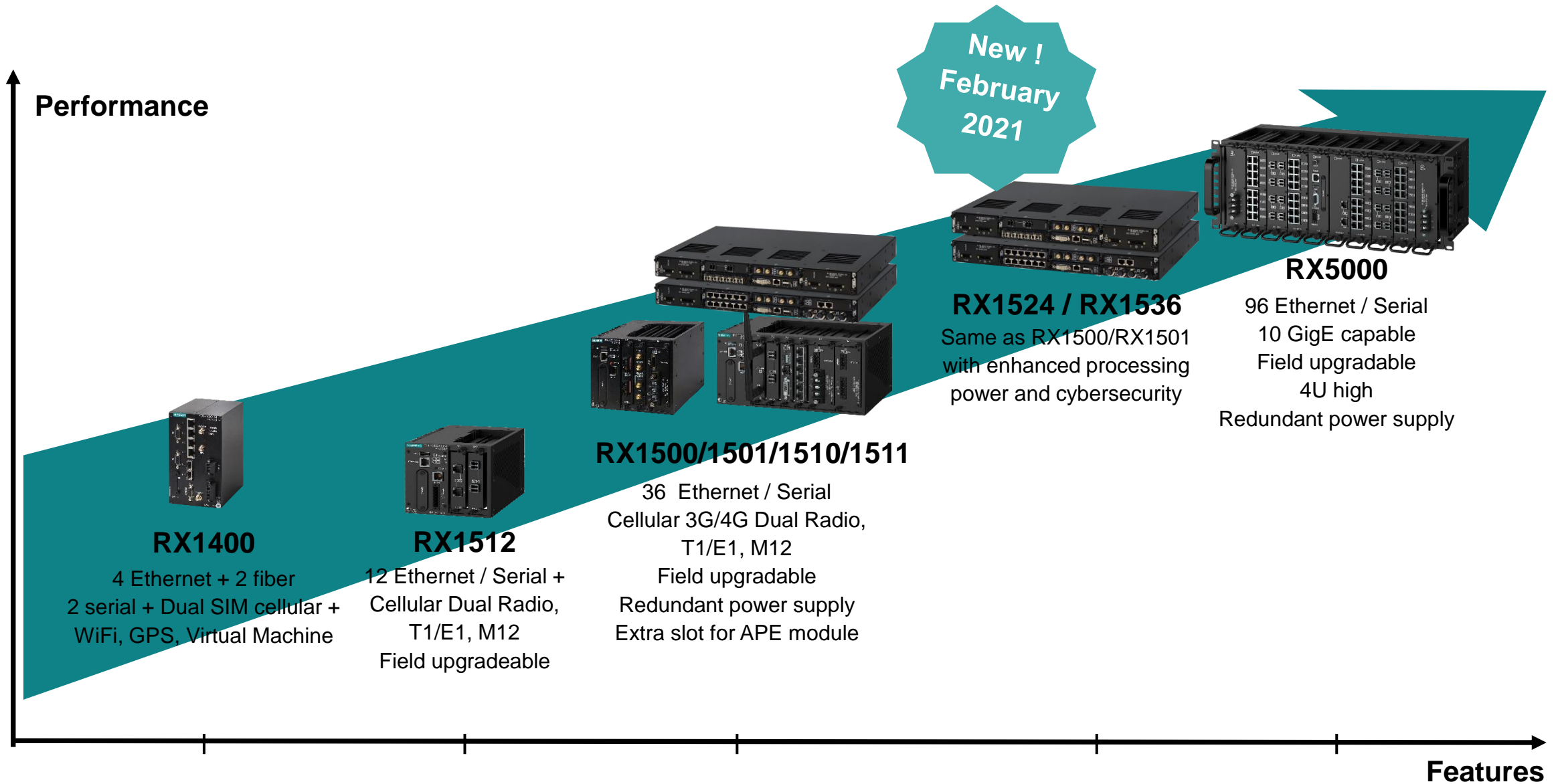
RUGGEDCOM: Plataformas multiservicio

ROX Operating System - Common Features

- Combines IP routing (Layer 3) and Ethernet managed switch (Layer 2)
- “Telecom standard” command line interface (CLI)
- Modular design with hot-swappable modules, high port density
- VRRP, OSPF, RIPv2, BGP, IS-IS, MPLS, VRF
- **R-GOOSE** (Routable GOOSE) New
- **Netflow support**
- Traffic prioritization
- VPN/IPSec, DMVPN, L2TPv3, GRE
- Radius, TACACS+, **Stateful Firewall CAPA 4**
- IP Multicast (IGMPv3, PIM-SM, PIM-SSM)
- Frame Relay, T1/E1, PPP, PAP, CHAP
- 3G/4G Cell modem with dual SIM, single radio and dual radio



RUGGEDCOM Layer 3 Multi-Service Platform portfolio



RUGGEDCOM RX1524/RX1536: Product highlights

New members of
world well known
RX1500 family!

February 2021

Enhanced hardware
supports up to 20,000 routes
per device ✓

Cyber improvements,
eMMC, TPM for key storage,
and up to **100 Mbit/s** IPsec
capacity ✓



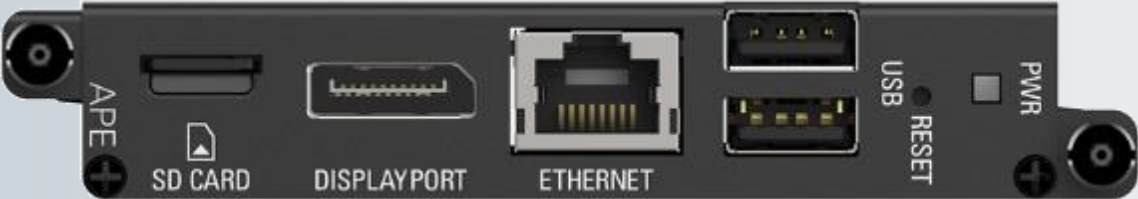
Lower latency while
interacting and utilizing
ROX features on the unit ✓

Significant edge processing
improvements to support IIoT
trends in the market ✓

Hot swappable hardware
compatible with the
existing RX15xx Multi-
Service Platform devices ✓

Hardware Platform: RUGGEDCOM APE1808 for RX15xx

A utility-grade line module that plugs directly into RUGGEDCOM RX15xx family and runs Siemens as well as third party software applications



	APE 1808
Specifications	
CPU	Intel x5-E3940 – 4 cores (x86_64)
CPU speed	1.6Ghz and higher
RAM	8GB DDR3 with ECC
Storage	64 GB pseudo-SLC
Front Network Ports	1x 10/100/1000mbps RJ45
Backplane Network Ports	1x 1000mbps
Graphics	Intel HD 500 (DisplayPort)
USB Ports	2x USB 3.0
MicroSD Reader	1x micro-SDHC
Audio	Intel HD Audio through DisplayPort
OS Support	Debian Linux and Windows 10 IoT Ent.

RUGGEDCOM Multi-Service Platform with APE1808

Rugged design

Certified reliability in harsh environments of electric power, transportation, O&G



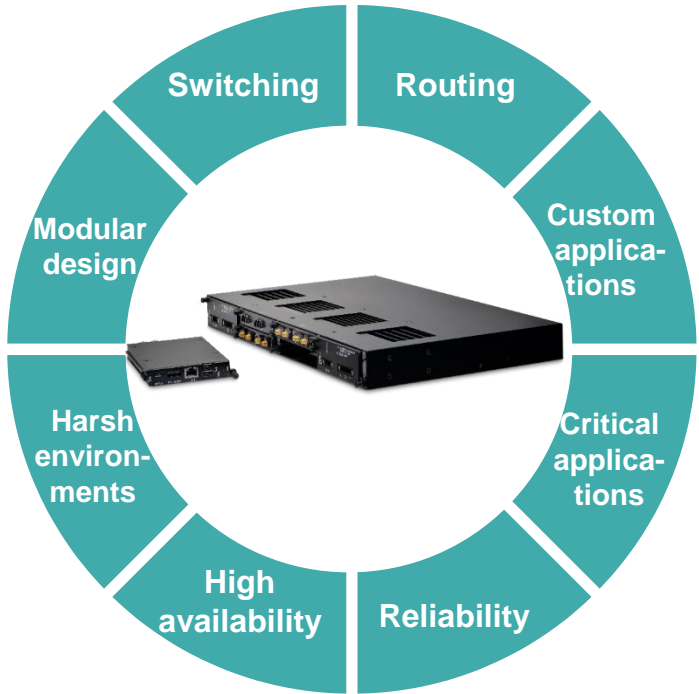
Integrated single or redundant power supplies ensure high availability



Operation in industrial temperature range with fan-less design



RX15xx with APE1808



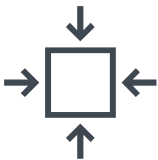
Maximum flexibility



Field swappable modules guarantee flexibility and easy maintenance



Cybersecurity partnerships offer customized solutions of various security levels



Field proven, industry accepted platform for critical applications

We offer rugged and flexible cybersecurity solutions to maximize our customers' benefits

Cybersecurity Solutions Overview

IDS



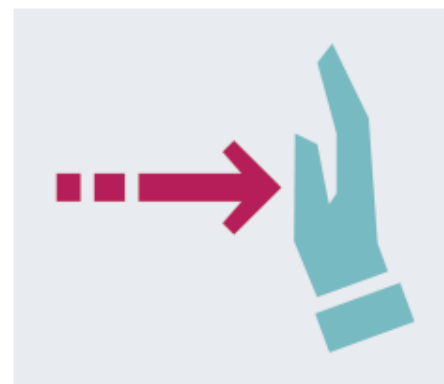
Non-intrusive, anomaly-based signature-less Intrusion Detection System software for mission-critical operational networks, operating on RUGGEDCOM hardware, provides early warning notification and alerting on vulnerabilities and sophisticated cyber threats that may be undetectable by conventional IT security tools

DPI



Deep Packet Inspection (DPI) on the RUGGEDCOM RX1500 with the APE1808 examines data packets utilizing a non-intrusive methodology for mission-critical networks. DPI helps to secure the communication to control centers and IT networks

IPS



An Intrusion Prevention System (IPS) is a capability available on the RUGGEDCOM hardware if equipped with a NGFW solution. IPS is located between the WAN and the LAN to deny the traffic that represents known threat based on a security profile

NGFW



RUGGEDCOM switching and routing platform with leading Next-Generation Firewall functionality on a single integrated appliance provides for additional integrated DPI/IPS functionalities, as well as security when connecting non-critical IT networks to critical deterministic operational networks.

Applications for complex OT requirements

IDS/DPI Third Party Solutions

	Secure-NOK	Nozomi Networks	Claroty	Kaspersky
Technology	IDS	IDS with DPI	IDS with DPI	IDS with DPI
IDS Detection Method	Anomaly based	Anomaly based, capable of supporting signatures	Anomaly based	Anomaly based
DPI	N/A	With support for OT protocol inspection*	With support for OT protocol inspection*	With support for OT protocol inspection*
Firewall Features	N/A	N/A	N/A	N/A
IPS	N/A	N/A	N/A	N/A
Platform	APE14xx, APE1808	APE1808	APE1808	APE1808

Tested solutions for the APE1808

**Check with vendor on OT protocol inspection support*

NGFW/IPS Third Party Solutions

	Fortinet	Check Point
Technology	NGFW	NGFW
IDS Detection Method	Signature based if equipped with IDS features	Signature based if equipped with IDS features
DPI	IT level inspection with support of OT Protocols*	IT level inspection with support of OT Protocols*
Firewall Features	Packet & Application filtering IPSec VPN NAT & more	Packet & Application filtering IPSec VPN NAT & more
IPS	Available, based on signatures and predetermined policies	Available, based on signatures and predetermined policies
Platform	APE1808	APE14xx, APE1808

Tested solutions for the APE1808

**Check with vendor on OT protocol support*

APE1808 with Fortinet FortiGate VM

Top Highlights



NGFW with Application Control



- Blocks and restricts access to resources
- Granular control using security policies
- Bandwidth optimization
- Visibility & control over network communication
- Full SSL inspection capabilities



Advanced Malware Protection



- Real-time malware detection and prevention
- Comprehensive Botnet and Antispam protection
- Continuous signature updates

FORTINET



Intrusion Prevention System (IPS)



- Built-in IPS functionality
- Threat detection and prevention
- Real-time threat intelligence
- Extensive database of IPS signatures



Industrial Security Service (ISS)



- DPI capability for ICS/SCADA protocols
- Granular control and visibility for ICS/SCADA communication
- Broad support for industrial protocols and applications

Comprehensive solution that delivers real-time security to protect and defend against the evolving threat landscape

APE1808 with Nozomi Networks Guardian

Top Highlights



Asset Discovery & Network Visualization



- Discover assets
- Visualize OT network
- Options for passive & active monitoring*



Anomaly & Threat Detection



- Identify anomalous and suspicious behavior
- Detect threats in real-time



Vulnerability Assessment



- Assessment of network vulnerabilities
- Identification of gaps in your assets



ICS Risk Monitoring



- Continuous monitoring
- Improve security posture
- Meet compliance regulations



Deep Packet Inspection



- Gain insights of the network communications
- Non-intrusive protocol analysis

Unified Intrusion Detection System for Industrial Control Systems and Operational Visibility

** Smart Polling add-on required for active discovery and monitoring*

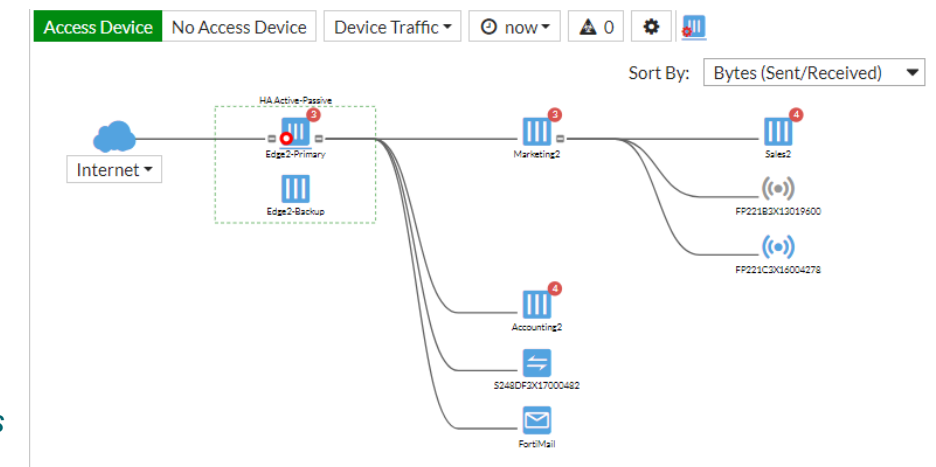
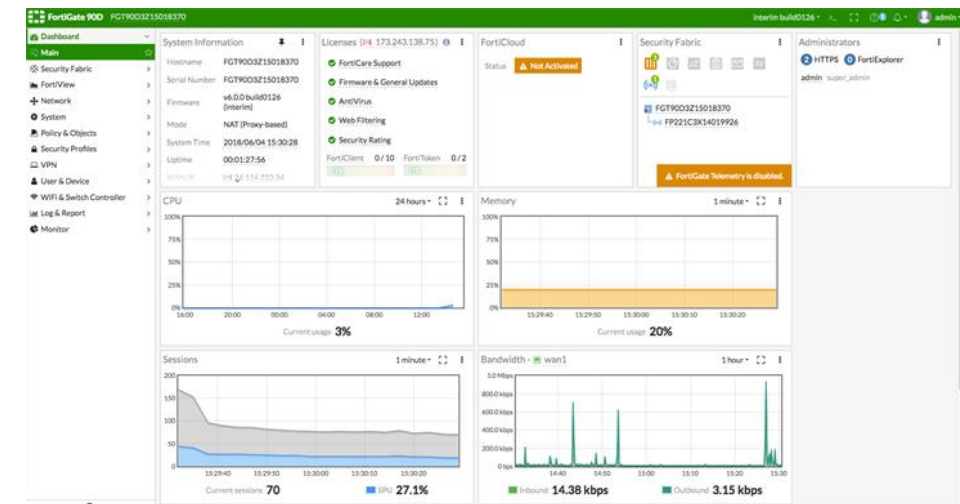
Example RX15xx with APE1808 and Fortinet FortiGate VM

Siemens RUGGEDCOM Multi Service Platform with Fortinet FortiGate	
Form factor	Rack Mounted or DIN Form
Line Modules	Up to 5 modules
Monitoring Ports	Up to 30 ports, mixed RJ45/Fiber/Serial Port
Power Supply Options	24VDC, 48VDC, 88-300 VDC or 85-264 VAC
Degree of Protection	IP30
Certification	61850-3, IEEE 1613, NEMA TS-2, KEMA Cert
Computing Platform	APE1808 module with Quadcore 1.6 GHz CPU, 64 GB SSD storage & 8 GB DDR3
Ambient Conditions	
Temperature Range	-40° C to +85° C
Solution Highlights	
IPv4 Firewall Throughput ¹⁾	600 Mbps
IPSec VPN Throughput ²⁾	74 Mbps
Threat Prevention	Active ³⁾

¹⁾ V1518 UDP for 512 Frame Size

²⁾ Depending on applications and protocols

³⁾ ISS and IPS subscription required

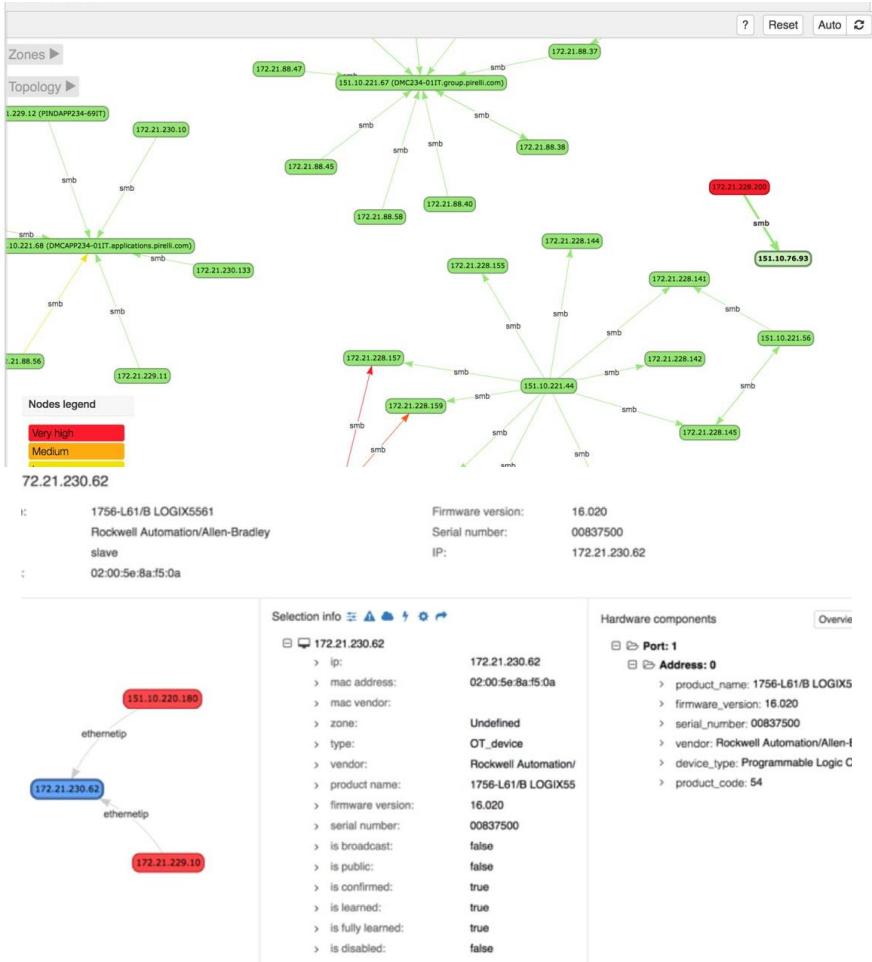


Example RX15xx with APE1808 and Nozomi Networks Guardian

Siemens RUGGEDCOM Multi Service Platform with Nozomi Networks Guardian	
Form factor	Rack Mounted or DIN Form
Line Modules	Up to 5 modules
Monitoring Ports	Up to 30 ports, mixed RJ45/Fiber/Serial Port
Power Supply Options	24VDC, 48VDC, 88-300 VDC or 85-264 VAC
Degree of Protection	IP30
Certification	61850-3, IEEE 1613, NEMA TS-2, KEMA Cert
Computing Platform	APE1808 module with 4 core - 1.6 GHz CPU, 64 GB SSD storage, 8GB DDR3, 2 x USB 3.0
Ambient Conditions	
Temperature Range	-40° C to +85° C
Solution Highlights	
Maximum Protected Nodes	500
Maximum Throughput ¹⁾	15 Mbps - 195 Mbps
Protocol Support*	61850, Goose, MMS, S7/S7+, common SCADA protocols, etc..
Threat Detection	Passive and Active ²⁾

¹⁾ Depending on applications and protocols

²⁾ Via Smart Polling Subscription



Example RX1536 with Fortigate and Nozomi Guardian

Siemens RUGGEDCOM Multi Service Platform with Nozomi Networks Guardian and Fortigate	
Switching	VLANS, QoS, RSTP, Link Aggregation and much more
Routing	VRRP, OSPF, PIM-SM, PIM-SSM, VRF and much more
Stateful Firewall	Layer 4 FW, VPN
Redundant Power Supply Options	24VDC, 48VDC, 88-300 VDC or 85-264 VAC
Modular solution	mixed RJ45/Fiber/Serial Port/celullar
Certification	61850-3, IEEE 1613, NEMA TS-2, KEMA Cert
Computing Platform	APE1808 module with 4 core - 1.6 GHz CPU, 64 GB SSD storage, 8GB DDR3, 2 x USB 3.0
Ambient Conditions	
Temperature Range	-40° C to +85° C
Cybersecurity NGFW	
Anomaly & Threat Detection	<ul style="list-style-type: none">Identify anomalous and suspicious behaviorDetect threats in real-time
Deep Packet Inspection	<ul style="list-style-type: none">Gain insights of the network communicationsNon-intrusive protocol analysis
Intrusion Prevention System (IPS)	<ul style="list-style-type: none">Built-in IPS functionalityThreat detection and preventionReal-time threat intelligenceExtensive database of IPS signatures
NGFW with Application Control	<ul style="list-style-type: none">Blocks and restricts access to resourcesGranular control using security policiesBandwidth optimizationVisibility & control over network communicationFull SSL inspection capabilities

Ruggedcom RX1536 (24 ports available, Hi power Supply)










| Contacto

Published by Siemens, S.A.

Javier Sánchez Lobón
Ruggedcom Sales Manager

Phone +34 675 79 25 27

E-mail javier.sanchez_lobon@siemens.com