Industrial Next Generation Firewall

Product Details

SIEMENS

Continuous network protection
with Industrial Next Generation Firewall

Automation environments have evolved from isolated islands into highly complex networks – often without proper segmentation of untrusted cyber networks (such as office or internet).

Industrial Next Generation Firewall serves as perimeter protection in accordance with security requirements for industrial automation and has been tested and approved for use with the Siemens process control system.

Solution and Service

- State-of-the-Art Next Generation **Firewall Appliances**
- Additional **Security Subscriptions** for Threat Prevention, URL Filtering and WildFire
- **Support Package** (3 or 5 years) with Premium Support

Your value

Continuous protection against known and unknown threats

Tested and approved for SIMATIC PCS 7 and SIVaaS

Excellent price-performance ratio

SIEMENS

Insufficient perimeter protection means taking risks

Operative Challenges

- Shop-floor landscape evolved from isolated islands to highly complex and flat networks without any segmentation from untrusted cyber networks (e.g. office or internet).
- Often there is no perimeter protection at all or perimeter protection only for the office environment.
- If perimeter protection for the automation network exists, it is often controlled by office IT without automation know-how.
- Industrial automation networks require a perimeter protection based on the IEC 62443 zones and conduits model.

Flat industrial networks without segmentation from untrusted cyber networks are easy targets for hackers.

Possible consequences

High risk of cyber attacks due to missing perimeter protection for the automation network

High risk of cyber attacks due to inconsistent configuration of protection measures due to lack of automation expertise

Unplanned downtimes and/or data loss due to cyberattacks, time consuming troubleshooting

SIEMENS

Continuous network protection with Industrial Next Generation Firewall

Solution and Service

Industrial Next Generation Firewall is a perimeter protection solution in line with security requirements for industrial automation, tested and approved for usage with Siemens products. It serves as the first line of defense against unauthorized access from untrusted cyber networks.

The solution includes:

- State-of-the-art Next Generation Firewall appliances from Palo Alto Networks
- Additional security subscriptions for Threat Prevention, Advanced URL Filtering and WildFire
- Service Package (3 or 5 years) with Premium Support

SIEMENS

Next Generation Firewall appliances from Palo Alto Networks

Palo Alto Networks provides a large range of Next Generation Firewalls and is the leader in Gartner Magic Quadrant for Enterprise Network Firewalls – already for the 11th consecutive year.

The partnership of Palo Alto Networks as leader for enterprise network firewalls and Siemens service experts with combined expertise in automation and cybersecurity makes this offering

the best-in-class firewall solution for IT/OT network segmentation

based on the IEC 62443 zone and conduits model.

Product features:

- Application layer and stateful inspection firewall
- Classifies all applications, on all ports, all the time
- Enforces security policies for any user, at any location
- Prevents against known and unknown threats
- Intrusion detection / prevention system (IDS/IPS)
- IPSec VPN gateway
- High availability (active/active and active/passive modes)
- Hardened operating system (PanOS is Linux based)
- Capable of inspecting layer 7 traffic such as S7 protocol (detecting: start, stop, read, write) or OPC
- Secure System Architecture
- Cloud-based security subscriptions: Threat Prevention, Advanced URL Filtering, WildFire

SIEMENS

Next Generation Firewalls – different options for different needs

	PA-440	PA-450	PA-460	PA-1410
Firewall throughput (HTTP/Appmix)	2,9 / 2,2 Gbps	3,6 / 3,0 Gbps	5,1 / 4,4 Gbps	8,9 / 6,8 Gbps
Use cases	Enterprise branch offices, retail locations and midsize businesses	Enterprise branch offices, retail locations and midsize businesses	Enterprise branch offices, retail locations and midsize businesses	Organisations' branch offices and midsize businesses High-speed internet gateway deployments
Max sessions	200,000	300,000	400,000	945,000
Onboard interfaces (copper)	10/100/1000 (8x)	10/100/1000 (8x)	10/100/1000 (8x)	10/100/1000 Mbps (8x) 1/2,5/5 Gbps PoE (4x)
Optional interfaces (SFPs)	-	-	-	1G-SFP (6x) 1G/10G-SFP+ (4x)
Redundant power supply	optional	optional	optional	optional
Dimensions in inch (HxDxW)	1,74 x 8,83 x 8,07 (5,0lbs / 7,8lbs)	1,74 x 8,83 x 8,07 (5,0lbs / 7,8lbs)	1,74 x 8,83 x 8,07 (5,0lbs / 7,8lbs)	19" standard rack 1,70" x 14,15" x 17,15"
Dimensions in cm (HxDxW)	4,42 x 22,43 x 20,5 (2,27kg / 3,54kg)	4,42 x 22,43 x 20,5 (2,27kg / 3,54kg)	4,42 x 22,43 x 20,5 (2,27kg / 3,54kg)	19" standard rack 4,32 x 35,94 x 43,56

PANW FWs not listed here can be requested as individual offerings

SIEMENS

Premium Support and optional subscriptions

Premium Support

Premium Support provides you with services for maintaining your Palo Alto Networks deployment. Premium Support includes e.g. following features:

- Premium support hours: 24/7 for all severities
- Next business day delivery for parts and hardware replacement
- Feature releases and software updates, subscription services updates
- Documentation and FAQ, online customer-support portal, etc.

TP

Threat Prevention Subscription

The Threat Prevention subscription adds integrated protection against network-borne threats, including exploits, malware, command and control traffic, and a variety of hacking tools, through IPS functionality and stream-based blocking of millions of **known malware samples**.

UF

Advanced URL Filtering Subscription

Advanced URL Filtering provides you with granular, user-based controls over Web activity through **URL categories** and customizable allow- and deny-lists, as well as protection from Web-borne threats through malicious categories like “malware” and “phishing”.

WF

WildFire™ Subscription

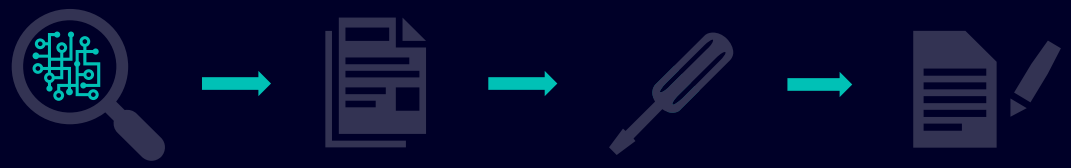
The WildFire™ subscription **actively analyzes unknown threats,** including malware, websites, and command and control traffic, and delivers automatically created protections and intelligence back to subscribed firewalls all over the world for proactive global prevention.

SIEMENS

Industrial Next Generation Firewall installation service

Combined expertise in automation and cybersecurity

Siemens industrial security experts combine years of expertise in automation and cybersecurity to accompany you with your perimeter protection from review and concept creation over the installation and configuration of your firewall up to the commissioning and documentation.



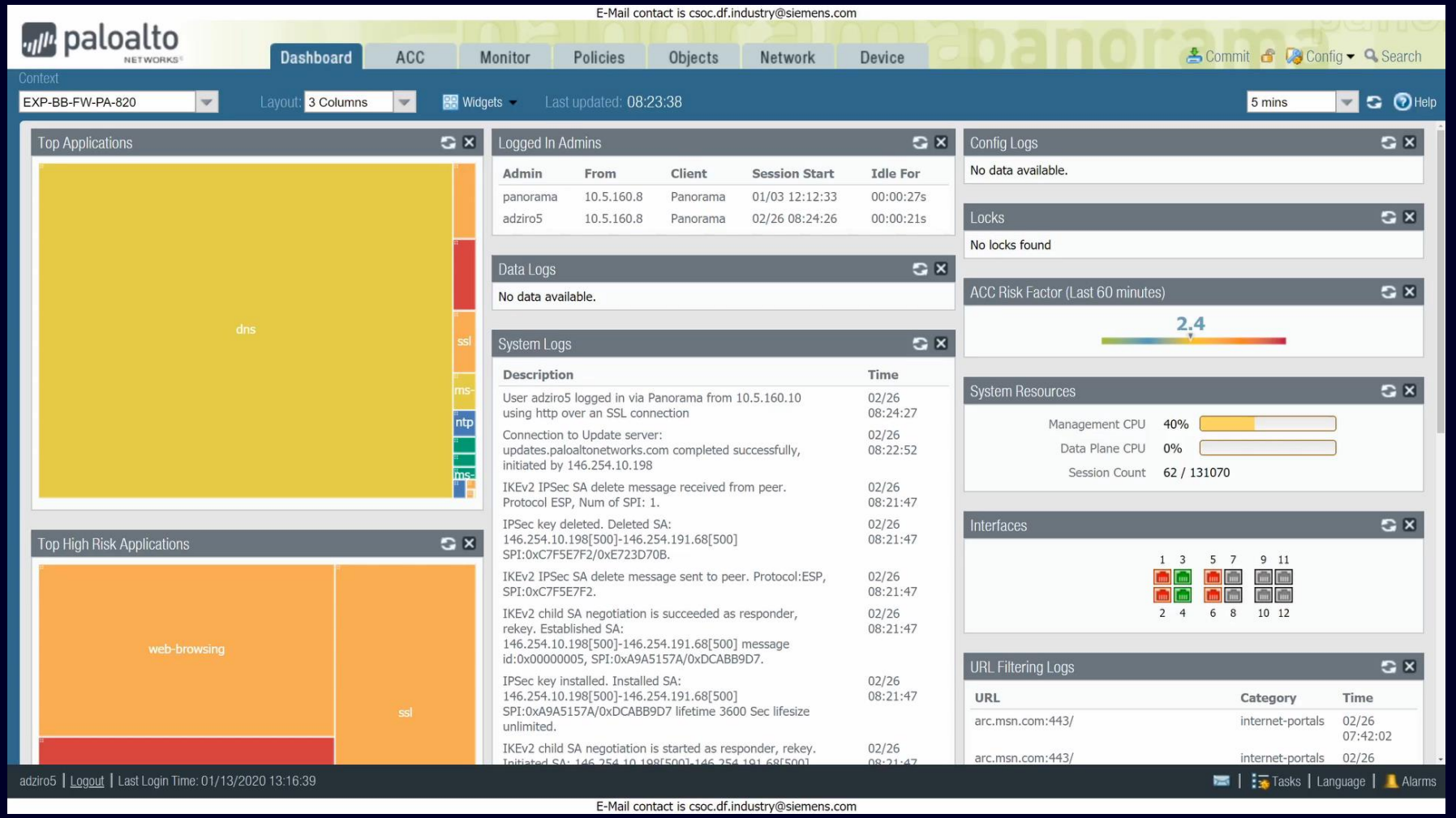
Furthermore, the solution has been tested and approved for usage with the Siemens process control system SIMATIC PCS 7 and SIVaaS (SIMATIC Virtualization as a Service).

How does it work?

1. **Review of plant network layout**
   Basis of the service is a review of your current plant network layout.
2. **Creation of a perimeter firewall concept**
   On this basis, the service expert creates a perimeter firewall concept tailored to your individual plant.
3. **Installation and configuration of firewall**
   While installing and configuring the firewall in line with industrial security requirements, customer-specific applications are also considered by the service expert (e.g. fine-tuning of intrusion detection / prevention system (IDS/IPS)).
4. **Documentation of firewall configuration**
   After the commissioning and test of the firewall system and traffic rules, the service expert will hand over the documentation and configuration backup.

SIEMENS

Application overview



SIEMENS

Why should you choose Industrial Next Generation Firewall?

Continuous protection

against known and unknown threats thanks to Application Layer firewall with Deep Package Inspection

Best-in-class firewall solution

for IT/OT network segmentation based on IEC 62443

Tested and approved

for Siemens products

SIEMENS

Siemens AG, SIMATIC Systems Support, Germany
Secure connections through Industrial Next Generation Firewall

Siemens AG, Germany

With over 100 employees Siemens SIMATIC Systems Support is a prime example of a Siemens internal testing environment for customer projects. This is largely a virtualized environment with a large number of servers and hardware components. This includes S7-1500, S7-1200, and the use of TIA-Portal and WinCC.

Customer objectives

- One consequence of digitalization is the growing connectivity of industrial plants. On the one hand, this increasing networking enables companies to make their production processes more flexible and efficient, while cutting costs. On the other, it also increases the risk of cyber attacks. Production processes in particular are a frequent target for attacks and therefore require an especially high level of protection.
- The SIMATIC Systems Support has a virtual environment with more than 500 virtual machines and a fully networked automation environment. Also, they have access between Siemens Networks (SNX) and special test networks Hence, a firewall service with next-Generation functionality was needed.

Solution and Service

- The solution was a Next Generation Industrial Next Generation Firewall including:
  - Industrial Security Monitoring installation and management
  - Perimeter Firewall installation and management
  - Network Security consulting resulting in VLAN network separation

Customer value

- Solid, in-depth security information thanks to Industrial Security Monitoring
- Secured connections between SNX and Special networks with the Industrial Next Generation Firewall
- An accepted network configuration approved by Siemens Global IT

Siemens References ID: 18623

SIEMENS

Hindalco Industries Ltd., Renukoot, India
Metals, Transforming IT-OT Infrastructure for Cybersecurity

Hindalco Industries Ltd., Renukoot, India

Hindalco Industries Ltd. (HIL) is the Indian largest Aluminum manufacturing company with around 17 locations spread across the country. The biggest plant is located at Renukoot and is an integrated plant. The biggest power plant supporting Renukoot's plant is located at Renusagar, with a capacity of ~800 MW.

Customer objectives

- HIL had a flat network without appropriate OT-IT segregation, no Industrial DMZ, no OT perimeter protection and no backup management
- HIL's objective was to create a dedicated OT backbone with OT Network Management System, infra for Anti virus, WSUS, dedicated Active Directory for OT, syslog server and backup management solution
- Deploy Continuous Threat Detection (CTD) and Secured Remote Access (SRA) from Claroty and integration with OT SOC.

Solution and Service

- IEC62443 based architecture (Purdue Model) for the OT area, OT perimeter protection through NGFW,
- Network management through SINEC NMS, Syslog server through SINEC INS
- Backup management solution through Acronis
- Infra for Anti virus Server, WSUS, Active Directory for OT
- Continuous Threat Detection and Secured Remote Access through Claroty

Customer value

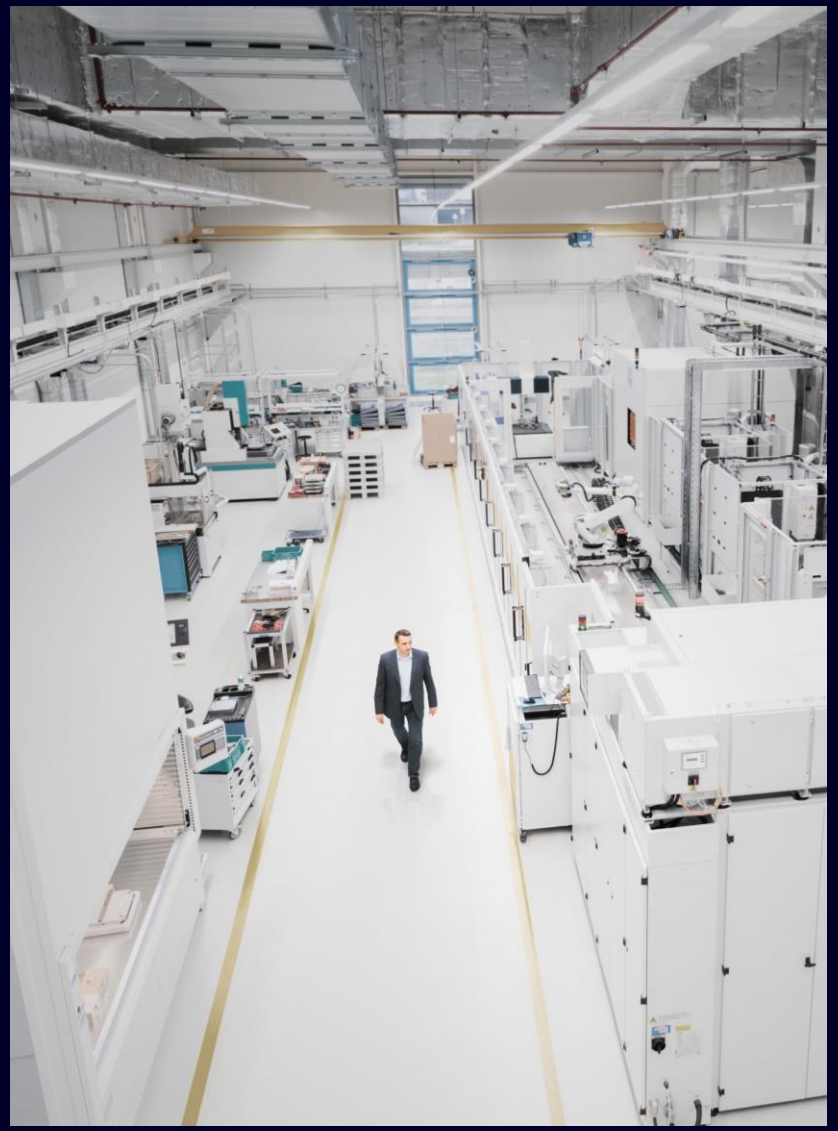
- Best in class OT infrastructure and OT-IT integration in line with IEC62443 standard
- Enhanced lifecycle support for existing system
- Better availability of systems thereby ensuring business continuity, adherence to OT security policies
- Reliable operation through centralized user access management

Siemens References ID: 39814

"The project was completed on time and exceeded our expectations. The integration of IT and OT systems has greatly improved our operational processes and security posture."

Mr. Rahul Kene and Mr. Manish Negi, Hindalco Industries Limited

SIEMENS



You want to find out **more**?

Webpage

Siemens Contact Database

Webinar

SIEMENS

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

SIEMENS

Security Information

Siemens provides products and solutions with industrial security functions
that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats,
it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept.
Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks.
Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent
such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity

SIEMENS