The bridge to possible

Cisco Secure Firewall ISA3000 Industrial Security Appliances

Prevent threats and secure your industrial control systems

Businesses in manufacturing, energy, transportation, and other industries are transforming their operations through digitization. This deeper integration between IT, cloud, and industrial networks is creating many security issues that are now putting production integrity, continuity, and safety at risk.

As industrial organizations connect more devices, enable more remote access, and build new applications, the air gap approach to protecting industrial networks against cyber threats is no longer sufficient. Operational Technologies (OT) have specific threat protection needs, requiring a ruggedized solution and a perfect understanding of industrial protocols.

The Cisco® Secure Firewall ISA3000 industrial security appliances deliver on these needs with the proven enterprise firewall, intrusion protection, and network security policies of Cisco's next generation firewall software. Developed specifically for deployment in the harshest industrial environments, these industrial firewalls are the foundation to enable secure industrial operations and regulatory compliance.

Benefits

- **Reduce risk with application awareness:** Control industrial network traffic to help ensure production uptime and integrity. The ISA3000 understands proprietary and standard OT protocols
- **Protect OT computers from malware:** Block malicious traffic before it's too late. The ISA3000 leverages Talos® threat intelligence to continuously analyze files and uncover stealthy threats
- **Extend IT security to OT:** Enforce consistent security policies across OT and IT. The ISA3000 is part of the Cisco Firepower® family and leverages the same management tools
- **Simplify compliance and reduce audit scope:** Build a secure industrial network that complies with regulatory requirements. The ISA3000 helps you conform to NERC-CIP, ISA99, IEC 62443, CFATS, ANSI/AWWA G430, and others

The bridge to possible

Key features

Robust industrial design

Built for extreme temperature, vibration, shock, surge, and electrical noise. Certified for deployment in the most demanding industries.

Reliable and durable operation

Fanless, convection cooled, with no moving parts. Dual power inputs, hardware bypass, and high availability design.

OT/IT traffic visibility and control

Cisco's leading firewall capabilities plus wide support for industrial protocols to control industrial process communications.

Advanced threat detection

Leverages industry-leading rules developed by Cisco Talos, including thousands of industrial-focused rules and rules to protect against vulnerability exploits.

Converged IT/OT security workflow

Fully integrated with Cisco's security portfolio including Cyber Vision, Identity Services Engine (ISE), Stealthwatch® and SecureX™ enabling coordinated defenses.

Easy to use and manage

On-device or centralized management for rapid provisioning of multiple devices, deploying consistent security policies across OT and IT and monitoring threat status while providing actionable reports.

Use cases

Build your industrial DMZ

Secure your small distributed industrial sites. The ISA3000 is the ideal DMZ firewall to connect utility substations, pipeline networks, remote control units, or street cabinets. It filters traffic flowing through the WAN and manages VPN connections to enable seamless and secure distributed operations.

Secure production with network segmentation

Prevent any threats or malicious actors from moving unchallenged laterally through the network. The ISA3000 separates different parts of the network in your manufacturing cells, zones, or utility substations so that attacks are contained and business-critical processes are kept safe.

Protect vulnerable assets from malicious activities

Block threats and exploits to vulnerable control equipment and save on downtime. The ISA3000 leverages threat intelligence from Cisco Talos to detect malicious activity or harmful traffic and protect industrial assets that cannot be patched.

Connect machines with duplicate IP addresses

Enable communications between different machines and cells without changing IP addresses. The ISA3000 translates IP addresses and secures communications so you don't have to modify duplicate addresses and can easily connect prebuilt systems.

Next steps

Visit cisco.com/go/isa3000 or contact your local Cisco account representative to learn more.

C45-744711-01 04/21