Cisco Secure Firewall ISA3000

Contents

Developed specifically to withstand the harshest industrial environments, these industrial firewalls offer uncompromising end-to-end security with industrial design and operation in mind.

Product overview

The Cisco® Secure Firewall ISA3000 is a true industrial firewall that provides OT-targeted protection based on proven enterprise-class security.

The ISA3000, with four data links, is a DIN rail mount, ruggedized appliance that provides the widest range of access, threat, and application controls for the harshest and most demanding industrial environments.

Figure 1.
Cisco Secure Firewall ISA3000 with two copper and two fiber ports (left) or four copper ports (right)

The ISA3000 bundles the proven security of the Cisco Secure Firewall with the visibility and control of industrial protocols and applications developed by leading automation vendors such as Omron, Rockwell, GE, Schneider, Siemens, and others. The ISA3000 is key as you start converging IT and OT security and capturing the benefits of your industrial digitization efforts.

As a foundational component of your IoT/OT security journey, the ISA3000 is the ideal ruggedized firewall to segment industrial networks, protect OT assets from potential threats, and build compliance with a variety of industrial standards, regulations, and guidelines such as NERC-CIP, ISA99/IEC62443, CFATS, ANSI/AWWA G430, and others.

Certified for deployment in the most demanding industries (power utilities, oil and gas, transportation, mining, manufacturing, water utilities, and more), the ISA3000 is widely used as a DMZ firewall to connect small, distributed industrial sites, enforce segmentation of large internal networks, and manage VPN connections to enable secure management of remote assets and seamless distributed operations.

The ISA3000 protects industrial processes and vulnerable control equipment. It leverages industry-leading threat detection and vulnerability exploit protection rules developed by Cisco Talos®, including thousands of industrial-focused rules. Using OpenAppID and Deep Packet Inspection (DPI) of industrial protocols, it even lets you write your own custom detectors to create alerts and block or allow traffic based on the industrial application flows you most care about. Cisco Advanced Malware Protection (AMP) is also built in to continuously track suspect file propagation.

Managed through either a user-friendly on-box device manager, on-premises centralized management, or a cloud-based management solution, the ISA3000 provides industrial-focused, out-of-the-box configuration and simplified operational management. And because these management tools are the same you already use with Cisco firewalls in your IT domain, it is easy to extend IT security to OT and enforce consistent security policies across domains.

As part of Cisco's comprehensive security portfolio, the ISA3000 interacts with your existing tools to deliver an integrated IT/OT security workflow. Cisco Cyber Vision provides host attribute information to enable construction of meaningful and contextual security policies. Cisco Identity Services Engine (ISE) can be leveraged to exchange unified policy updates as well as host context information using Security Group Tags (SGTs) for security enforcement. The ISA3000 can also exchange NetFlow information with Cisco Stealthwatch® to provide network-level context information. The ISA3000 provides insights and alerts to Cisco SecureX™ to streamline event triage and correlation, enabling coordinated, single-click defenses.

With the ISA3000, you can build a secure IoT/OT infrastructure and leverage your existing IT security tools and expertise to help ensure production integrity, continuity, and safety.

Your ruggedized choice for industrial firewall deployments

The Cisco Secure Firewall ISA3000 offers:

- Controlled traffic to, from, and between manufacturing cells or industrial zones
- Secured WAN connectivity for power substations and isolated industrial assets
- Flexible and secure enterprise-class remote access
- Critical network infrastructure services such as IP routing, NAT, DNS, DHCP, and more
- Unequaled threat protection for every level of networking and computing — from the switch, router, OS, and compute infrastructure to industrial control systems
- Wide support for industrial protocols for visibility and control over every level of your applications in both the industrial and enterprise space
- More levels of traffic continuity safety than other offerings in the industrial space
- Common Criteria for IT security certification.

Table 1. General capabilities of Cisco Secure Firewall ISA3000

Capability	Features
Robust industrial design	• Built for harsh environments and temperature ranges (-40° to 158°F; -40° to 70°C) • Hardened for vibration, shock, surge, and electrical noise immunity • Four Gigabit Ethernet uplink ports, providing multiple resilient design options (4 copper or 2 copper plus 2 fiber) • Complies with multi-industry specifications for industrial automation, Intelligent Transport Systems (ITS), and electrical substation environments • Improves uptime, performance, and safety of industrial systems and equipment • Compact DIN rail unit design with industrial LED features, allowing easy monitoring • Fanless and convection cooled with no moving parts for extended durability • IEEE 1588v2 Precision Time Protocol (PTP) clock synchronization (default profile is supported) • Alarm I/O for monitoring and signaling to external equipment.

Capability	Features
User-friendly GUI device manager	• On-device management for local awareness and immediate control using Cisco Firepower® Device Manager • Centralized management configuration, logging, monitoring, and reporting using Cisco Firepower Management Center • Cloud-based management option available with Cisco Defense Orchestrator • Multidevice management that handles hundreds of devices • User-specific access and control customizations
Traffic continuity and protection	• Full “lights out” traffic bypass copper ports • Default passive deployment learning mode • Software updates without traffic loss • Connection limitations to protect from denial-of-service-causing traffic • Latency detection and mitigation functions • Quality-of-service policies
OT and ICS protocol support	• BACnet • Common Industrial Protocol (CIP) (AppID for individual CIP applications available) • Companion Specification for Energy Metering (COSEM) • Connection Oriented Transport Protocol (COTP) • Distributed Network Protocol (DNP3) • EtherNet/IP • Generic Object Oriented Substation Events (GOOSE) • Generic Substation Events (GSE) • Emission Control Protocol • Fujitsu Device Control • Honeywell Control Station/NIF Server • Honeywell Esperion DSA Server Monitor • IEC 60870-5-104 (AppID for individual commands available) • IEC 61850 MMS (AppID for individual commands available) • ISO Manufacturing Message Specification (MMS) • Modbus • Omron FINS • OPC Unified Architecture (OPC-UA) • Q.931 • Siemens S7 • SRC • TPKT

Table 2. Access control capabilities

Capability	Features
Proven, extensible access control	• Enforces ISA99/IEC 62443 segmentation needs • Stateful inspection (Layers 2 through 7) • Transparent and routed firewall operation modes • Provides features to enable electronic security perimeter (ESP) for NERC-CIP compliance • Next-Generation Intrusion Prevention System (NGIPS) • Identity-based access control policies (users, devices, SGTs, etc.) • VPN: Remote Access, site-to-site
Application control	• Visibility and control of all DMZ infrastructure • Visibility and control of industrial applications • Visibility and control of individual protocol commands and values • ICS/OT protocol visibility and/or control
Remote access enablement and control	• Network access control via Cisco AnyConnect® • Cisco ISE support • Site-to-site VPN • Remote Access VPN • Cisco Secure Desktop • Support for Citrix and VMware clientless connections
Multilevel access controls	• Global block lists – automated or manual • Global allow lists • Third-party intelligence feed utilization • File allow lists • File block lists • Application-level access control • 802.1X support
Cisco TrustSec® controls	• In-band and out-of-band identity • Active Directory integration • Policy based on SGTs • 802.1X support • MACsec and MAC Authentication Bypass (MAB) support • Enforces endpoint security state for remote access

Table 3. Intrusion detection and protection capabilities

Capability	Features
Uncompromising threat detection and protection	• Leverages industry-leading rules developed by Cisco Talos research teams • Over 55,000 rules, providing the widest range of protection anywhere • Hundreds of industrial-focused rules • Industrial equipment exploit protection rules • Protocol abuse identification • Protection for web-based control systems • Network behavior analytics • Passive device discovery
Threat network mapping	• Passive device identification • Mobile device identification • Application host network mapping • Vulnerability/host network mapping • User/host network mapping
Threat discovery	• Indicators of Compromise (IoC) tracking • OpenAppID – open community ID system • Correlation policies and responses • Traffic variance detection • Router-based remediation actions • NetFlow tracking • 55,000+ threat identifiers • Customizable identifiers • Can create wholly new identifiers • Widest identifier contributorship
File tracking	• Approved file trace • Suspect file trace • Malware match

Table 4. Networking capabilities

Capability	Features
DMZ infrastructure	• DNS services • Dynamic Host Configuration Protocol (DHCP) services • Authentication, authorization, and accounting (AAA) support • IP routing (v4 and v6)
Layer 3 routing	• IPv4 static routing • Dynamic routing (Routing Information Protocol [RIP], Enhanced Internet Gateway Routing Protocol [EIGRP], Intermediate System to Intermediate System [IS-IS], Open Shortest Path First [OSPF], and Border Gateway Protocol [BGP])

Capability	Features
Network Address Translation (NAT)	• Static NAT • With port translation, one-to-many, nonstandard ports • Dynamic NAT • Dynamic Port Address Translation (PAT) • Identity NAT
Layer 2 IPv6	• IPv6 host support, HTTP over IPv6, Simple Network Management Protocol (SNMP) over IPv6
Trunking	• 802.1q trunks supported
Logging	• Local logs, syslog, Security Analytics and Logging (SAL), eStreamer, and Log in the management application • Proven integration with leading security information and event management (SIEM) systems (QRadar, Splunk, etc.)
Clock synchronization	• IEEE 1588 (hardware-enabled PTP)

Performance specifications

Table 5. Performance using Cisco Firepower Threat Defense (FTD)

Feature	Performance
Throughput: NGIPS (1024B)	500 Mbps
Throughput: Firewall (FW) + Application Visibility and Control (AVC) (1024B)	375 Mbps
Throughput: FW + AVC + Intrusion Prevention System (IPS) (1024B)	350 Mbps
Maximum concurrent sessions, with AVC	50,000
Maximum new connections per second, with AVC	2700
IPsec VPN throughput (1024B TCP with Fastpath)	50 Mbps
Maximum VPN peers	25
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications as well as geo locations, users, and websites
URL filtering	More than 80 categories More than 280 million URLs categorized

Feature	Performance
Defined interfaces	200, 400 (with SecPlus license on ASA), 400 (FTD)
VLAN counts	5, 100 (with SecPlus license on ASA), 100 (FTD)
IPv4 MACsec Access Control Entries (ACEs)	1000 with default TCAM template
NAT	Bidirectional, 128 unique subnet NAT entries, which can expand to tens of thousands of translated entries if designed properly

Security feature specifications

Table 6. Security features

Feature	Support information
Transport Layer Security (TLS) decryption	Yes
AVC: OpenAppID support for custom, open-source application detectors	Standard
Cisco security intelligence	Standard, with IP, URL, and DNS threat intelligence
Cisco Firepower NGIPS	Available; can passively detect endpoints and infrastructure for threat correlation and IoC intelligence
Cisco Secure Firewall (formerly Cisco AMP for Networks)	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco Secure Endpoint (formerly Cisco AMP for Endpoints) is also optionally available
Cisco Secure Malware Analytics (formerly Cisco Threat Grid) sandboxing	Available
Automated threat feed and IPS signature updates	Yes: class-leading Collective Security Intelligence (CSI) from the Cisco Talos group (https://www.cisco.com/c/en/us/products/security/talos.html)
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats
High availability and clustering	Active/standby failover
Cisco Trust Anchor technologies	Includes Trust Anchor technologies for supply chain and software image assurance

Hardware specifications

Table 7 lists physical specifications, Table 8 lists safety standards and compliance specifications, and Table 9 gives information about networking standards.

Table 7. Physical specifications

Description	Specification
Hardware	• 4-core Intel® Atom® processor (industrial temp.) • 8-GB DRAM (soldered down) • 16-GB onboard flash memory • mSATA 64 GB • 1-GB removable SD flash memory card (industrial temp.) • Mini-USB connector for console • RJ-45 traditional console connector • Dedicated 10/100/1000 management port • Hardware-based anti-counterfeit, anti-tamper chip • Factory reset option
Alarm I/O	• Two alarm inputs to detect dry contact open or closed • One Form C alarm output relay
Dimensions (WxHxD)	• 11.2 x 13 x 16 cm (4.41 x 5.12 x 6.30 in.)
Weight	• 1.9 kg (4.2 lb)
Power supply and ranges	• Dual internal DC • Nominal: ± 12V DC, 24V DC, or 48V DC • Maximum range: 9.6V DC to 60V DC • Power consumption: 24W
Mean time between failures (MTBF)	• ISA-3000-4C: 398,130 hours • ISA-3000-2C2F: 376,580 hours

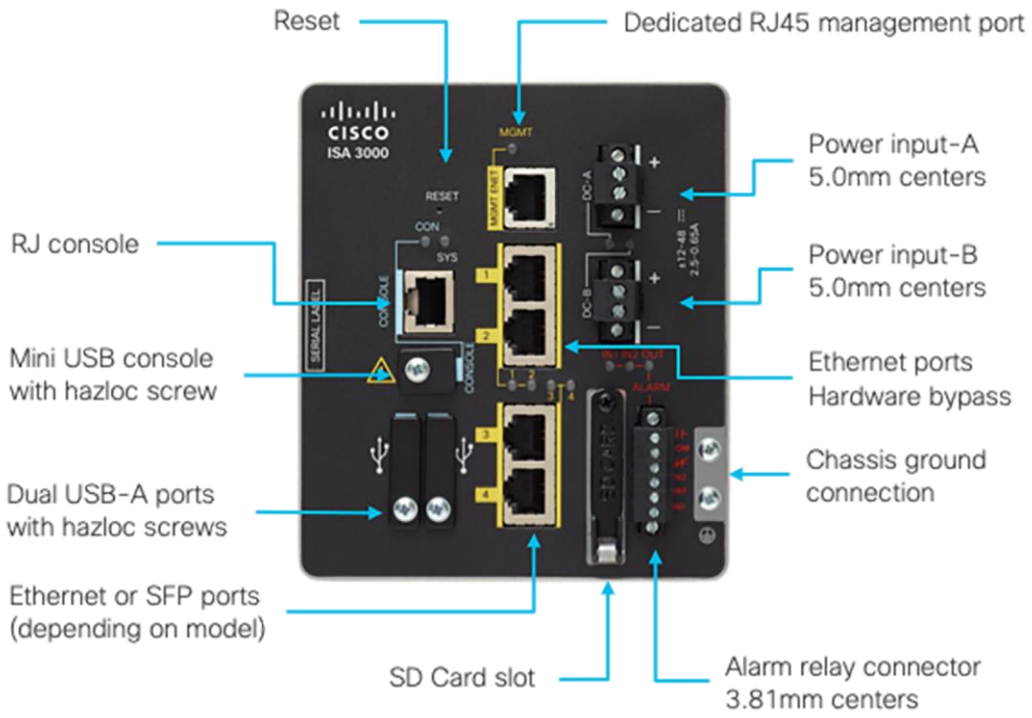

Figure 2.
Cisco Secure Firewall ISA3000 ports overview

Table 8. Safety standards and compliance specifications

Type	Standards
Electromagnetic emissions	FCC 47 CFR Part 15 Class A EN 55022A Class A VCCI Class A AS/NZS CISPR 22 Class A CISPR 11 Class A CISPR 22 Class A ICES 003 Class A CNS13438 Class A KN22

Type	Standards
Electromagnetic immunity	EN55024 CISPR 24 AS/NZS CISPR 24 KN24 EN 61000-4-2 Electro Static Discharge EN 61000-4-3 Radiated RF EN 61000-4-4 Electromagnetic Fast Transients EN 61000-4-5 Surge EN 61000-4-6 Conducted RF EN 61000-4-8 Power Frequency Magnetic Field EN 61000-4-9 Pulse Magnetic Field EN 61000-4-18 Damped Oscillatory Wave EN-61000-4-29 DC Voltage Dips and Interruptions IEC/AS/NZS 62368.1
Industry standards	EN 61000-6-1 Immunity for Light Industrial Environments EN 61000-6-2 Immunity for Industrial Environments EN 61000-6-4 Emission Standard for Industrial Environments EN 61326 Industrial Control EN 61131-2 Programmable Controllers IEEE 1613 Electric Power Stations Communications Networking IEC 61850-3 Electric Substations Communications Networking NEMA TS-2 EN 50121-3-2 EN 50121-4 EN 50155

Type	Standards
Safety standards and certifications	Information technology equipment: • UL/CSA 60950-1 • EN 60950-1 • CB to IEC 60950-1 with all country deviations • NOM to NOM-019-SCFI (through partners and distributor) Industrial floor (control equipment): • UL 508 • CSA C22.2, No 142 • EN/IEC 61010-2-201 • UL/CSA 61010-1 Hazardous locations:* • ANSI/ISA 12.12.01 (Class I, Div 2 A-D • CSA C22.2 No 213 (Class 1, Div 2 A-D) • UL/CSA 60079-0, -15 • IEC 60079-0, -15 (IECEx test report Class I, Zone 2, group II gases) • EN 60079-0, -15 ATEX certification (Class I, Zone 2, group II gases) *Must meet deployment requirements such as with IP54 enclosure described in the "Product Documentation and Compliance Information for the Cisco ISA 3000" https://www.cisco.com/c/dam/en/us/td/docs/security/Firewalls/ISA3000/ISA3000-PDOC.pdf
Operating environment	Operating temperature: -40° to +74°C (-40° to +165°F) -40° to +70°C (-40° to +158°F) (vented enclosure operating) -40° to +60°C (-40° to +140°F) (sealed enclosure operating) -40° to +75°C (-40° to +167°F) (fan or blower-equipped enclosure operating) EN 60068-2-21 EN 60068-2-2 EN 61163
Storage environment	Temperature: -40° to +85°C (-40° to +185°F) Altitude: 0 to 15,000 ft (0 to 4572 m) IEC 60068-2-14
Humidity	Relative humidity of 5% to 95% noncondensing IEC 60068-2-30

Type	Standards
Ingress Protection (IP) rating	IP30
Shock and vibration	IEC60068-2-6 and IEC60068-2-27 MIL-STD-810, Method 514.4 Marine EN60945 Industrial EN61131-2/IEC61131-2 Railway EN61373 CAT 1B Smart Grid EN61850-3 IEEE 1613
Corrosion	ISO 9223: Corrosion Class C3-Medium Class C4-High EN 60068-2-52 (Salt Fog) EN 60068-2-60 (Flowing Mixed Gas)
Others	RoHS compliance China RoHS compliance TAA (Government) CE (Europe) Regulatory Compliance Mark (RCM)
Warranty	5-year limited hardware warranty on all ISA3000 product IDs See link at end of data sheet for more details on warranty

Table 9. Networking standards

Description	Specification	
IEEE standards	• IEEE 802.1D MAC Bridges, Spanning Tree Protocol (STP) • IEEE 802.1p Layer2 class-of-service (COS) prioritization • IEEE 802.1q VLAN • IEEE 802.1s Multiple Spanning-Trees • IEEE 802.1w Rapid Spanning-Tree • IEEE 802.1x Port Access Authentication • IEEE 802.1AB Link Layer Discovery Protocol (LLDP) • IEEE 802.3ad Link Aggregation (LACP)	• IEEE 802.3ah 100BASE-X single-mode fiber (SMF)/multimode fiber (MMF) only • IEEE 802.3x full duplex on 10BASE-T • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • IEEE 1588v2 PTP

Description	Specification	
RFC compliance	• RFC 768: User Datagram Protocol (UDP) • RFC 783: Trivial FTP (TFTP) • RFC 791: IPv4 • RFC 792: Internet Control Message Protocol (ICMP) • RFC 793: TCP • RFC 826: Address Resolution Protocol (ARP) • RFC 854: Telnet • RFC 951: BOOTP • RFC 959: FTP • RFC 1157: SNMPv1 • RFC 1901,1902-1907 SNMPv2 • RFC 2273-2275: SNMPv3 • RFC 2571: SNMP Management • RFC 1166: IP Addresses • RFC 1256: ICMP Router Discovery	• RFC 1305: NTP • RFC 1492: TACACS+ • RFC 1493: Bridge MIB Objects • RFC 1534: DHCP and BOOTP interop. • RFC 1542: Bootstrap Protocol • RFC 1643: Ethernet Interface MIB • RFC 1757: RMON • RFC 2068: HTTP • RFC 2131, 2132: DHCP • RFC 2236: IGMP v2 • RFC 3376: IGMP v3 • RFC 2474: DiffServ Precedence • RFC 3046: DHCP Relay Agent Information option • RFC 3580: 802.1X RADIUS • RFC 4250-4252 SSH Protocol

Ordering information

Table 10 and Table 11 show the available ISA3000 product IDs, Table 12 lists the SFP modules, and Table 13 lists the power supplies available for the ISA3000.

Table 10. Cisco Secure Firewall ISA3000 models

Product number	Base software	Copper 10/100/1000 (all bypass enabled)	SFP fiber ports
ISA-3000-2C2F-K9	ASA	2	2
ISA-3000-4C-K9	ASA	4	0
ISA-3000-2C2F-FTD	FTD	2	2
ISA-3000-4C-FTD	FTD	4	0

Table 11. Optional orderable features

Note – Cisco Firepower Services 7.0 is the last Firepower Services release to run on Cisco ASA Firewall.

Product number	Feature
Optional orderable features (ASA+Firepower Services)	
L-ISA3000SEC+-K9	Security Plus – HA enablement, SSL VPN, greater connection count, VLAN trunking
Threat/Application subscription licenses	
L-ISA3000-TA-1Y	1 Year Subscription Threat/Application
L-ISA3000-TA-3Y	3 Year Subscription Threat/Application

Product number	Feature
L-ISA3000-TA-5Y	5 Year Subscription Threat/Application
Threat Defense Malware Protection licenses	
L-ISA3000-AMP-1Y	1 Year Subscription Threat Defense Malware Protection
L-ISA3000-AMP-3Y	3 Year Subscription Threat Defense Malware Protection
L-ISA3000-AMP-5Y	5 Year Subscription Threat Defense Malware Protection
Threat Defense URL Filtering licenses	
L-ISA3000-URL-1Y	1 Year Subscription Threat Defense URL Filtering License
L-ISA3000-URL-3Y	3 Year Subscription Threat Defense URL Filtering License
L-ISA3000-URL-5Y	5 Year Subscription Threat Defense URL Filtering License
Threat Defense Threat and URL Filtering licenses	
L-ISA3000-TC-1Y	1 Year Subscription Threat Defense Threat and URL Filtering License
L-ISA3000-TC-3Y	3 Year Subscription Threat Defense Threat and URL Filtering License
L-ISA3000-TC-5Y	5 Year Subscription Threat Defense Threat and URL Filtering License
Threat Defense Threat and Malware Protection licenses	
L-ISA3000-TM-1Y	1 Year Subscription Threat Defense Threat and Malware Protection License
L-ISA3000-TM-3Y	3 Year Subscription Threat Defense Threat and Malware Protection License
L-ISA3000-TM-5Y	5 Year Subscription Threat Defense Threat and Malware Protection License
Threat Defense Threat, Malware Protection, and URL Filtering licenses	
L-ISA3000-TMC-1Y	1 Year Subscription Threat Defense Threat, Malware Protection, and URL License
L-ISA3000-TMC-3Y	3 Year Subscription Threat Defense Threat, Malware Protection, and URL License
L-ISA3000-TMC-5Y	5 Year Subscription Threat Defense Threat, Malware Protection, and URL License
Optional orderable features (FTD)	
Threat/Application subscription licenses	
L-ISA3000T-T-1Y	1 Year Subscription Threat/Application
L-ISA3000T-T-3Y	3 Year Subscription Threat/Application
L-ISA3000T-T-5Y	5 Year Subscription Threat/Application

Product number	Feature
Threat Defense Malware Protection licenses	
L-ISA3000T-AMP-1Y	1 Year Subscription Threat Defense Malware Protection
L-ISA3000T-AMP-3Y	3 Year Subscription Threat Defense Malware Protection
L-ISA3000T-AMP-5Y	5 Year Subscription Threat Defense Malware Protection
Threat Defense URL Filtering licenses	
L-ISA3000T-URL-1Y	1 Year Subscription Threat Defense URL Filtering License
L-ISA3000T-URL-3Y	3 Year Subscription Threat Defense URL Filtering License
L-ISA3000T-URL-5Y	5 Year Subscription Threat Defense URL Filtering License
Threat Defense Threat and URL Filtering licenses	
L-ISA3000T-TC-1Y	1 Year Subscription Threat Defense Threat and URL Filtering License
L-ISA3000T-TC-3Y	3 Year Subscription Threat Defense Threat and URL Filtering License
L-ISA3000T-TC-5Y	5 Year Subscription Threat Defense Threat and URL Filtering License
Threat Defense Threat and Malware Protection licenses	
L-ISA3000T-TM-1Y	1 Year Subscription Threat Defense Threat and Malware Protection License
L-ISA3000T-TM-3Y	3 Year Subscription Threat Defense Threat and Malware Protection License
L-ISA3000T-TM-5Y	5 Year Subscription Threat Defense Threat and Malware Protection License
Threat Defense Threat, Malware Protection, and URL Filtering licenses	
L-ISA3000T-TMC-1Y	1 Year Subscription Threat Defense Threat, Malware Protection, and URL License
L-ISA3000T-TMC-3Y	3 Year Subscription Threat Defense Threat, Malware Protection, and URL License
L-ISA3000T-TMC-5Y	5 Year Subscription Threat Defense Threat, Malware Protection, and URL License

Table 12. Supported Cisco ruggedized SFPs*

Product number	Type
GLC-SX-MM-RGD=	1000 BASE-SX Ruggedized
GLC-LX-SM-RGD=	1000 BASE-LX/LH Ruggedized
GLC-FE-100FX-RGD=	100 BASE-FX Ruggedized
GLC-FE-100LX-RGD=	100 BASE-LX Ruggedized

*For the complete list of supported SFP models, please refer to https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html.

MM = multi-mode fiber

SM = single-mode fiber

Table 13. Suggested power supply

Product number	Details
PWR-IE50W-AC-IEC	AC to DC 24V/2.1A DIN Rail power supply, input 100-240VAC/1.25A 50-60Hz, output 24VDC/2.1A, IEC Plug
PWR-IE50W-AC	AC to DC 24V/2.1A DIN Rail power supply, input 100-240VAC/1.25A or 125-250VDC/1A, output 24VDC

Warranty information

Warranty information is available at https://www.cisco-servicefinder.com/warrantyfinder.aspx.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environmental Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environmental Sustainability" section of the CSR Report) are provided in the following table.

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco and Partner Services

At Cisco, we're committed to minimizing our customers' TCO, and we offer a wide range of services programs to accelerate customer success. Our innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services helps you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Some of the key benefits our customers can get from Cisco Services follow:

- Mitigating risks by enabling proactive or expedited problem resolution
- Lowering TCO by taking advantage of Cisco expertise and knowledge
- Minimizing network downtime
- Supplementing your existing support staff so they can focus on additional productive activities

For more information about Cisco Services, refer to Cisco Technical Support Services or Cisco Advanced Services at https://www.cisco.com/web/services/.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation, and stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about the Cisco Secure Firewall ISA3000, visit https://www.cisco.com/go/isa3000 or contact your local account representative.

Document history

New or Revised Topic	Described In	Date
Updates related to new OS version		Jan 20, 2020
New available licenses	Table 10 and Table 11	Jan 20, 2020
Reorganized feature lists		Feb 6, 2021
Updated performance data	Table 5	April 8, 2021
Updated product name		April 8, 2021
Mentioned end of Firepower Services on ASA	Table 10 and Table 11	July 7, 2021

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-735839-05 07/21