Cisco Small Business ISA500 Series Integrated Security Appliances

An All-in-One Internet Access and Security Solution to Safeguard Your Small Business

The Cisco® Small Business ISA500 Series Integrated Security Appliance is an all-in-one internet access and security solution that combines highly secure Internet, wireless, site-to-site, and remote access with a breadth of Unified Threat Management (UTM) capabilities. These capabilities include firewall, email, and web security, and application control to provide the peace of mind you need in order to know your small business is protected. Optimized specifically for small and medium businesses, the ISA500 is an affordable and easy-to-use solution that can be set up to start protecting your business in minutes. It takes full advantage of Cisco Security Intelligence Operations (SIO), which provides global threat intelligence to deliver superior threat protection. The combined power of the ISA500's comprehensive UTM security capabilities, easy-to-use design, and superior threat intelligence keeps your organization more secure, and increases both uptime and employee productivity, while minimizing operational costs and the risk of business disruption.

The Cisco ISA500 Series utilizes a cloud-based approach to email and web security that minimizes management tasks and can enable responsive, agile protection against new threats. This in-depth inspection helps increase employee productivity by controlling web access, reducing spam emails, and minimizing phishing attacks, unauthorized intrusions, and other emerging threats. It also uses the 75 TB of threat telemetry from 1.6M devices per day from Cisco SIO to provide superior global threat intelligence and protection from sophisticated attacks. This comprehensive approach to threat protection helps free IT resources up from time-consuming virus eradication and system cleanup activities.

In addition to the many capabilities already outlined, the Cisco ISA500 provides several other features that can help optimize business uptime. It offers WAN redundancy that supports failover, load balancing, and policy based routing (PBR) to keep businesses running when failures occur due to either a failed Internet connection or a failure within an ISP itself. Also, as part of the Cisco Small Business product portfolio, the Cisco ISA500 Series has been tested to ensure it works with other Cisco Small Business products and the uptime of the overall solution is increased.

The ISA500 is also designed for today's dynamic organizations. It can enable mobile employees and business partners to more securely connect to networks over the Internet using IP Security (IPsec) or Secure Socket Layer (SSL) VPN services. With a Cisco ISA500 Series solution protecting your network, you can focus on serving customers and growing your business, instead of worrying about security issues.

Challenge

Small businesses need a simple, affordable and easy-to-deploy solution that provides Internet access in addition to all the security they need to ensure that this internet access is used safely and doesn't disrupt business productivity. They need a simple, straight forward way of providing the internet access they need and want to provide, but they don't want a solution that's so simplistic that they're left vulnerable. As they open up their networks and applications to

become more collaborative, mobile, and engaged they need to make sure this doesn't make them an open target for security threats like unauthorized access, viruses, internet threats and spyware. Here are some more detailed explanation of these challenges and the impact they can have:

- Multi-box solutions for Internet access and comprehensive security can be cumbersome and drive up expenses
- Unauthorized access can lead to loss of company data, unplanned downtime, unstable networks, and related liability concerns
- Viruses can infect office networks, resulting in outages and lost revenue
- Internet threats can hamper your ability to meet regulatory and compliance requirements
- Email threats such as spam and phishing can make critical information available unintentionally and contribute to a loss of employee productivity
- Spyware provides a view into your network and data that can lead to identity theft and business data loss
- Cloud technology and applications require robust security and encryption to avoid exposing sensitive business information to risks
- Businesses are increasingly opening their networks to customers, partners, and public users through wireless and guest access, creating the potential for new security risks
- Browsing of non-work-related and harmful websites and social media leads to lost productivity, exposure to viruses and spyware, and possible legal issues

Solution

The ISA500 Cisco Small Business ISA500 Security Appliance Series provides small businesses with an all-in-one solution for secure Internet access with comprehensive UTM security backed by Cisco's superior SIO that's easy-to-deploy and provides VPN support for mobile and geographically dispersed employees. With its combined zone-based firewall, content security and highly secure access capabilities, the Cisco ISA500 Series stops threats before they enter the network and impact business operations. The Cisco ISA500 Series:

- **Provides an all-in-one solution for internet access and security**
- **Safeguards your business from Internet threats** – The Cisco ISA500 Series provides critical perimeter security services for comprehensive protection.
  - **Valid business traffic flows; unwelcome visitors locked out** – The Cisco ISA500 Series features a zone-based firewall that lets you apply flexible, policy-based control over who can access your network. It also supports a publicly accessible network area, known as a demilitarized zone (DMZ), to safely host file, web, and other Internet-accessible servers without exposing the business's internal LAN network to threats.
  - **Web blocking and filtering** – Reputation-based web and URL filtering can be used to control employee Internet usage by blocking access to dangerous or inappropriate sites. This sophisticated control helps minimize web-based security threats, while improving employee productivity and limiting the risk of legal action by employees exposed to offensive content.
  - **Antivirus** – Advanced gateway antivirus technology uses up-to-date data feeds to shield your internal network resources from the most wide spread and active virus attacks, at the most effective point in your infrastructure, the Internet gateway. Filtering your email and web traffic at the perimeter eliminates the need for costly, time-consuming infection cleanups and helps ensure business continuity.

- **Antispyware** – Blocking the most wide spread and active spyware at the gateway prevents it from entering your network through Internet traffic (HTTP and FTP) and email, avoiding costly spyware removal procedures and improving employee productivity.

- **Spam limiting** – Robust reputation-based spam filtering helps restore the effectiveness of email so that communication with customers, vendors, and partners continues uninterrupted.

- **Antiphishing** – Identity theft protection guards against phishing attacks, thereby preventing employees from inadvertently disclosing company or personal details that could lead to financial loss.

- **Proactive prevention of intrusions and blockage of dangerous peer-to-peer communications** – The Cisco ISA500 Intrusion Prevention System (IPS) capabilities can identify possible intrusions into the business network and take action to stop the intrusion and prevent further risk. The Cisco ISA500 Series can also block peer-to-peer and instant messaging traffic, and perform protocol inspection to help increase network security, enhance employee productivity, and keep the network available for business traffic.

- **Inclusion of Cisco SIO for Unrivalled Threat Protection** – The Cisco ISA500 uses the 75 TB of threat telemetry per day from Cisco SIO to provide unparalleled global threat intelligence that is combined with local threat defense. This helps to protect against sophisticated attacks and to provide a comprehensive approach to threat protection.

- **Protection against internal threats and management of access control** – To help protect your business from internal threats, the Cisco ISA500 provides zone-based firewall and security services, including IPS and antivirus capabilities. It helps protect wireless environments through secure wireless LAN (WLAN) support with robust authentication options and guest access management.

- **WAN Redundancy** – The Cisco ISA500 provides WAN redundancy that supports failover, load balancing, and policy based routing (PBR) to keep businesses running when failures occur due to either a failed Internet connection or a failure within an ISP itself

- **Secure VPN access** – The Cisco ISA500 Series makes it easy for remote and mobile employees to establish secure VPN connections with IPsec or SSL encryption. A site-to-site IPsec VPN is ideal to secure communications between offices and provides complete network access. Mobile workers can use Cisco AnyConnect™ or Cisco VPN Client to establish SSL based VPN or IPsec based VPN connections to main offices while they are at customer sites, cafés, or the airport.

- **Highly secure wireless connectivity** – To provide untethered access to employees as they roam around the office, select models of the Cisco ISA500 Series support highly secure mobility with 802.11b, g, and n wireless connectivity with WPA encryption and 802.11x authentication. Rogue access point detection helps you reduce the risk of unauthorized wireless users and maintain control of your network infrastructure.

- **Easy cloud-based or onbox management with Cisco OnPlus and the ISA500 embedded management utility** – The Cisco ISA500 Series can be managed using the embedded Security Appliance Configuration Utility, a powerful yet easy-to-use browser-based management and monitoring interface. In addition to supporting management and monitoring, the Configuration Utility provides security and network usage reports so administrators can quickly and easily review security activities and network operation status. Your partner can also manage the Cisco ISA500 for you through the Cisco OnPlus™ Service. This cloud-based platform provides discovery and monitoring of the entire small business network. It also lets you offload network management tasks to your trusted partner, so you're free to focus on your core business instead of network management. Cisco OnPlus also provides reporting services via its Advanced Security Services capabilities. With Advanced Security Services, partners can generate security, network usage, and

system status reports such as intrusion attack events and WAN bandwidth utilization at a scheduled interval and time. These reports can be stored in a PDF file format and shared via email. All combined, the Cisco ISA500 provides a variety of management capabilities and options that support proactive network service and support that can help increase your network availability and give you peace of mind.

Business Benefits

The Cisco ISA500 Series provides security and connectivity that helps you:

- **Support your business with security, increase uptime** – Apply comprehensive security to protect your most important business processes, such as company storefronts, websites, services, and customer communication. Broad security helps keep your critical network resources accessible, resilient against attacks, and with increased uptime.
- **Increase employee productivity** – Improve employee productivity by limiting spam and spyware and controlling inappropriate web browsing. Advanced application control lets you minimize the use of distracting non-business applications.
- **Improve business resiliency** – Prevent disruption of business-critical applications and services due to security breaches by implementing a comprehensive, all-in-one security solution.
- **Decrease liability risks** – Reduce your company's exposure to liability related to compromised data or inadequate corporate controls by applying comprehensive access control and unrivaled threat protection provided by services that take full advantage of Cisco SIO. Advanced risk mitigation and monitoring help you comply more effectively with government and industry regulations, protect customer data, and safeguard human resources and other sensitive business data.
- **Reduce IT costs** – Free up IT support resources and avoid the costly process of cleaning up infections due to spyware, viruses, sophisticated attacks and other malware by preventing them from occurring.
- **Stay productive with safe remote access** – Enable employees and partners to more securely access the network from home, on the road, or at branch offices with flexible, easy-to-use built-in VPN support. With highly secure remote access and robust content protection, your employees can reach the tools and people they need anytime, anywhere, to work more effectively and respond to customers and colleagues faster. Mobile employees can use the Cisco AnyConnect client to enjoy always-on intelligent VPN access with consistent, context-aware security, using a laptop or smartphone.
- **Improve operational efficiency** – Simplify installation and reduce ongoing monitoring and management costs with an intuitive browser-based interface and sophisticated configuration wizards.
- **Enjoy peace of mind** – Get maximum value from your Cisco solution through an affordable, subscription-based service offering. The Cisco Small Business Support Service extends device level support for three years, protecting your investment with software upgrades and updates, access to the Cisco Small Business Support Center and support community, and next-business-day hardware replacement.

These benefits make the Cisco ISA500 Series the right choice to address your security needs and enable your network and employees to deliver maximum value to your business.

Product Specifications

Table 1.   Cisco Small Business ISA500 Series Security Appliance Models and Specifications

Features	ISA550	ISA550W	ISA570	ISA570W
Firewall				
Stateful Packet Inspection Throughput [1]	200 Mbps	200 Mbps	500 Mbps	500 Mbps
Zone-Based Firewall	Yes	Yes	Yes	Yes
Maximum Connections	15,000	15,000	40,000	40,000
Maximum Rules	100	100	100	100
Sessions Per Second (cps)	2500	2500	3000	3000
Schedules	Yes	Yes	Yes	Yes
Denial-of-Service Attack Protection	Yes	Yes	Yes	Yes
IPS Throughput [1]	60 Mbps	60 Mbps	90 Mbps	90 Mbps
AV Throughput [1]	50 Mbps	50 Mbps	80 Mbps	80 Mbps
UTM Throughput [1]	45 Mbps	45 Mbps	75 Mbps	75 Mbps
VPN				
IPsec VPN Throughput (Data Encryption Standard [DES] / Triple DES [3DES] / Advanced Encryption Standard [AES]) [1]	75 Mbps	75 Mbps	130 Mbps	130 Mbps
IPsec VPN Site-to-Site Tunnels	25	25	100	100
IPsec VPN Remote Access Tunnels	10	10	75	75
SSL VPN Tunnels	10	10	50	50
Encryption	DES/3DES/AES (128,192,256 bit)	DES/3DES/AES (128,192,256 bit)	DES/3DES/AES (128,192,256 bit)	DES/3DES/AES (128,192,256 bit)
Authentication	MD5, SHA-1, SHA2 (256,384,512 bit)	MD5, SHA-1, SHA2 (256,384,512 bit)	MD5, SHA-1, SHA2 (256,384,512 bit)	MD5, SHA-1, SHA2 (256,384,512 bit)
IPsec Dead Peer Detection	Yes	Yes	Yes	Yes
IPsec Network Address Translation (NAT) Traversal	Yes	Yes	Yes	Yes
IPsec NetBIOS Broadcast over VPN	Yes	Yes	Yes	Yes
VPN Pass-Through	IPsec/Point-to-Point Tunneling Protocol (PPTP)/Layer 2 Tunneling Protocol (L2TP)	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP
Cisco VPN client Support	Yes	Yes	Yes	Yes
Cisco VPN Client Mode Support	Yes	Yes	Yes	Yes
Cisco VPN Network Extension Mode Support	Yes	Yes	Yes	Yes
Cisco VPN Split Tunneling Support	Yes	Yes	Yes	Yes
Cisco AnyConnect SSL VPN Client Support	Yes	Yes	Yes	Yes
SSL VPN Split Tunneling Support	Yes	Yes	Yes	Yes
SSL VPN Certificates	Yes	Yes	Yes	Yes
Teleworker VPN Client (Cisco Hardware VPN Client)	Yes	Yes	Yes	Yes
L2TP Server	Yes	Yes	Yes	Yes

Features	ISA550	ISA550W	ISA570	ISA570W
Security Services				
Intrusion Prevention System (IPS)	Yes	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes
Web URL filtering	Yes	Yes	Yes	Yes
Web Threat Protection	Yes	Yes	Yes	Yes
Anti-Phishing	Yes	Yes	Yes	Yes
Anti-Virus	Yes	Yes	Yes	Yes
Anti-Spyware	Yes	Yes	Yes	Yes
Spam Filter	Yes	Yes	Yes	Yes
Network Reputation Filter	Yes	Yes	Yes	Yes
Networking				
IP Address Assignment	Static, Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol over Ethernet (PPPoE), L2TP, and PPTP	Static, DHCP, PPPoE, L2Tp, PPTP	Static, DHCP, PPPoE, L2Tp, PPTP	Static, DHCP, PPPoE, L2Tp, PPTP
DHCP	Server and relay	Server and relay	Server and relay	Server and relay
VLANs	16	16	16	16
Trunking (802.1Q)	Yes	Yes	Yes	Yes
Network Address Translation (NAT)	Yes	Yes	Yes	Yes
Port Forwarding	Yes	Yes	Yes	Yes
Port Triggering	Yes	Yes	Yes	Yes
Routing	Static, Routing Information Protocol (RIP) v1, v2	Static, RIP v1, v2	Static, RIP v1, v2	Static, RIP v1, v2
DMZ	Yes	Yes	Yes	Yes
Dual WAN	Yes	Yes	Yes	Yes
Load Balancing	Symmetric	Symmetric	Symmetric	Symmetric
Policy-Based Routing (Protocol Binding)	Yes	Yes	Yes	Yes
Integrated and Automated Failover and Failback	Yes	Yes	Yes	Yes
Weighted Load Balancing	Yes	Yes	Yes	Yes
Dynamic DNS (DDNS)	Yes	Yes	Yes	Yes
Voice over IP Support	SIP, H.323, compatible with most VoIP gateway and communication devices	SIP, H.323, compatible with most VoIP gateway and communication devices	SIP, H.323, compatible with most VoIP gateway and communication devices	SIP, H.323, compatible with most VoIP gateway and communication devices
SIP ALG Support	Yes	Yes	Yes	Yes
H.323 ALGP Support	Yes	Yes	Yes	Yes
QoS	Yes	Yes	Yes	Yes
Strict Priority Queuing	Yes	Yes	Yes	Yes
Weighted Round Robbin Queuing	Yes	Yes	Yes	Yes
Low Latency Queuing	Yes	Yes	Yes	Yes
DSCP Marking	Yes	Yes	Yes	Yes
Rate-Limiting	Yes	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes	Yes	Yes

Features	ISA550	ISA550W	ISA570	ISA570W
Internet Group Management Protocol (IGMP) Proxy	Yes	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes	Yes
Wireless				
802.11b/g/n, 2.4 GHz, 2 x 2 Multiple Input Multiple Output (MIMO)	No	Yes	No	Yes
Multiple SSIDs	4	4	4	4
Wi-Fi Multimedia (WMM) Quality of Service (QoS)	No	Yes	No	Yes
Unscheduled Automatic Power Save Delivery (U-APSD) (WMM Power Save [WMM-PS])	No	Yes	No	Yes
MAC Filtering	No	Yes	No	Yes
Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access Pre-Shared Key (WPA2-PSK), WPA2-ENT	No	Yes	No	Yes
Basic Service Set Identifier (BSSID) or Virtual Access Points	No	Yes	No	Yes
Dynamically and Manually Adjustable Transmit Power	No	Yes	No	Yes
Wi-Fi Protected Setup (WPS)	No	Yes	No	Yes
Guest Access	No	Yes	No	Yes
Captive Portal	No	Yes	No	Yes
Rogue Access Point Detection	No	Yes	No	Yes
Administration				
Automatic Firmware Check to See if a New Version is Available	Yes	Yes	Yes	Yes
Local User Database	100	100	100	100
Authentication	Local, RADIUS, Active Directory, Lightweight Directory Access Protocol (LDAP)	Local, RADIUS, Active Directory, LDAP	Local, RADIUS, Active Directory, LDAP	Local, RADIUS, Active Directory, LDAP
Diagnostics	Ping, DNS lookup, Packet Capture	Ping, DNS lookup, Packet Capture	Ping, DNS lookup, Packet Capture	Ping, DNS lookup, Packet Capture
Discovery Protocols	Cisco Discovery Protocol (CDP), Bonjour, universal plug and play (uPnP)	Cisco Discovery Protocol (CDP), Bonjour, uPnP	Cisco Discovery Protocol (CDP), Bonjour, uPnP	Cisco Discovery Protocol (CDP), Bonjour, uPnP
Logging and Monitoring	Local log, syslog	Local log, syslog	Local log, syslog	Local log, syslog
Status Reporting	Network usage status, security service status, network operation status	Network usage status, security service status, network operation status	Network usage status, security service status, network operation status	Network usage status, security service status, network operation status
Hardware Specifications				
Total Interface	7 GE	7 GE	10 GE	10 GE
LAN Ports (10/100/1000)	up to 6	up to 6	up to 9	up to 9
WAN Ports (10/100/1000)	up to 2	up to 2	up to 2	up to 2
DMZ Port (10/100/1000)	up to 4	up to 4	up to 4	up to 4
USB 2.0 Ports	1	1	1	1
Form Factor	1 RU, 19-in. rack mountable, wall mountable	1 RU, 19-in. rack mountable, wall mountable	1 RU, 19-in. rack mountable, wall mountable	1 RU, 19-in. rack mountable, wall mountable

Features	ISA550	ISA550W	ISA570	ISA570W
Dimensions (W x D x H)	308mm x 180mm x 49mm or 12.1 in. x 7.1 in. x 1.9 in. (with rubber pads)	308mm x 180mm x 49mm or 12.1 in. x 7.1 in. x 1.9 in. (with rubber pads)	308mm x 180mm x 49mm or 12.1 in. x 7.1 in. x 1.9 in. (with rubber pads)	308mm x 180mm x 49mm or 12.1 in. x 7.1 in. x 1.9 in. (with rubber pads)
Weight	1.2 Kg	1.3 Kg	1.3 Kg	1.4 Kg
Power On/Off Switch	Yes	Yes	Yes	Yes
Antennas	None	2	None	2
Environmental Operating Temperature	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)
Storage Temperature	–4 to 158°F (–20 to 70°C)	–4 to 158°F (–20 to 70°C)	–4 to 158°F (–20 to 70°C)	–4 to 158°F (–20 to 70°C)
Voltage Range	100–240 VAC	100–240 VAC	100–240 VAC	100–240 VAC
Input Frequency	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Output Voltage	11.4 V ~ 12.6 V	11.4 V ~ 12.6 V	11.4 V ~ 12.6 V	11.4 V ~ 12.6 V
Output Current	MAX 1.667 A	MAX 1.667 A	MAX 2.5 A	MAX 2.5 A

[1] Performance test methodology: Maximum performance based on RFC 2544. All results are aggregate bidirectional. Actual performance may vary depending upon network environment and configurations.

Ordering

Table 2.   Cisco Small Business ISA500 Integrated Security Appliance Product and License Part Numbers

Product	SKU
Cisco Integrated Security Appliance 550 with one year comprehensive security subscription	ISA550-BUN1-K9
Cisco Integrated Security Appliance 550 with wireless and one year comprehensive security subscription	ISA550W-BUN1-K9
Cisco Integrated Security Appliance 570 with one year comprehensive security subscription	ISA570-BUN1-K9
Cisco Integrated Security Appliance 570 with wireless and one year comprehensive security subscription	ISA570W-BUN1-K9
Cisco Integrated Security Appliance 550 with three years comprehensive security subscription	ISA550-BUN3-K9
Cisco Integrated Security Appliance 550 with wireless and three years comprehensive security subscription	ISA550W-BUN3-K9
Cisco Integrated Security Appliance 570 with three years comprehensive security subscription	ISA570-BUN3-K9
Cisco Integrated Security Appliance 570 with wireless and three years comprehensive security subscription	ISA570W-BUN3-K9

License	SKU
Cisco Comprehensive Security Subscription for ISA550 Series – 1 Year	L-ISA550-CS-1YR=
Cisco Comprehensive Security Subscription for ISA570 Series – 1 Year	L-ISA570-CS-1YR=
Cisco Comprehensive Security Subscription for ISA550 Series – 3 Year	L-ISA550-CS-3YR=
Cisco Comprehensive Security Subscription for ISA570 Series – 3 Year	L-ISA570-CS-3YR=

Service and Support

The Cisco Small Business ISA500 Integrated Security Appliance Series is backed by the Cisco Small Business Support Service, which provides affordable coverage that offers peace of mind. This affordable, subscription-based service includes software upgrades and updates, extended access to the Cisco Small Business Support Center, and next-business-day hardware replacement as necessary. It provides community-based support to enable you to share knowledge and collaborate with peers using online forums and wikis. The Cisco Small Business Support Service helps you reduce risks, deliver better service to colleagues and customers, and enjoy peace of mind.

For More Information

For more information about the Cisco Small Business ISA500 Series Integrated Security Appliances, visit www.cisco.com/go/isa500resources or contact your local Cisco provider. For more information about Cisco OnPlus, visit www.cisco.com/en/US/products/ps11792/index.html or contact your local Cisco provider.

For more information about the Cisco Small Business Support Service, visit www.cisco.com/cisco/web/solutions/small_business/services/index.html.

Printed in USA

C78-717565-00   10/12