Cisco Small Business ISA500 Series Integrated Security Appliances

Q. What is the Cisco® Small Business ISA500 Series Integrated Security Appliance?

A. The Cisco Small Business ISA500 Series Integrated Security Appliance is an all-in-one security solution. It combines highly secure Internet, wireless, site-to-site, and remote access with a breadth of unified threat management (UTM) capabilities that include firewall, email, and web security, and application control to provide the peace of mind you need in order to know your small or medium business is protected. Optimized specifically for small and medium businesses, it 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 provide unrivaled 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, helps keep your organization secure, and increases both uptime and employee productivity while minimizing risk and operational costs.

General Cisco ISA500 Product Information

Q. What are the primary differences between the ISA550 and ISA570 appliances?

A. Listed below is a table that outlines the primary differences between the ISA550 and IS570 appliances. The key differences between the two models is their performance and VPN scalability (refer to the Table 1). Thus, selecting between the two models should be based on the customers' traffic volume and the number of remote offices and mobile workers that need to be supported. Generally speaking, for a site with total protected users of more than 25, we suggest the ISA570 because of its higher UTM throughput. Also, if a business is expecting to interconnect more than three remote offices to each other, we recommend the ISA570 because it supports a larger number of site-to-site VPN tunnels than the ISA550. Similarly, if a business needs to provide more than ten remote workers with VPN access, we recommend the ISA570.

Table 1. Cisco ISA500 and ISA570 Comparison Chart

Security Appliance UTM Models		ISA550		ISA570	
		ISA550	ISA550W	ISA570	ISA570W
Hardware	Ports	7 GE		10 GE	
	Wireless (802.11b/g/n, 2.4 GHz)	Yes (on ISA550W)		Yes (on ISA570W)	
	Security Acceleration HW	No		Yes	
Performance	Firewall	200 Mbps		500 Mbps	
	VPN	75 Mbps		130 Mbps	
	AV	50 Mbps		80 Mbps	
	IPS	60 Mbps		90 Mbps	
	UTM *	45 Mbps		75 Mbps	
	Maximum Connections	15,000		40,000	
	IPsec VPN Site-to-Site Tunnels	25		100	
	IPsec Remote Access Tunnels	10		75	

		ISA550	ISA570
	SSL VPN Tunnels	10	50

Q. What security services are included in the security subscription services in ISA500?

A. ISA500 offers the following seven subscription based security services:

Table 2. Cisco ISA500 Subscription Security Services Summary

Subscription Security Services	Description
Anti-Virus & Anti-Spyware	Prevent wide spread and active viruses, spyware and malware at networks
Spam Filter	Stop spam at the connection level
IPS (Intrusion Prevention Systems)	Block malicious attacks on businesses
Application Access Control	Block unproductive application usage
Network Reputation Filter	Block malicious senders
Web URL Filter	Block unwanted web site access by category, domain, and URL
Web Reputation Filter	Prevent dangerous web site access

Q. Do I need to buy a separate license to use security subscription services?

A. Cisco ISA500 comes standard with both hardware and UTM security services. Customers do not need to purchase a separate license for the security services. Listed below are eight SKUs for the ISA500. Each of the SKUs is a "bundle" SKU that includes both hardware and a comprehensive security subscription service suite. Customers will need to buy a "renewal" license to continue using security services when their subscription term expires.

Table 3. Cisco ISA500 Bundles and SKUs

	Package Selection			SKU
Product Bundle	Low-end	Wired	1-year	ISA550-BUN1-K9
			3-year	ISA550-BUN3-K9
		Wireless	1-year	ISA550W-BUN1-K9
			3-year	ISA550W-BUN3-K9
	High-end	Wired	1-year	ISA570-BUN1-K9
			3-year	ISA570-BUN3-K9
		Wireless	1-year	ISA570W-BUN1-K9
			3-year	ISA570W-BUN3-K9

Q. Can I use security subscription services right away or do I need to activate the security subscription license first?

A. While ISA500 will come with a security subscription license, customers will need to activate the license first before they can use security subscription services. The license term will start only after the license is activated not after the unit is purchased.

Q. Does the gateway anti-virus supported on the ISA500 prevent malware from web traffic only?

A. The Cisco ISA500 gateway anti-virus prevents the wide spread virus, spyware, and malware that may come from various applications, including web, email, and file transfer applications. The solution scans traffic from not just HTTP (web) but also SMTP, FTP, NetBIOS, and CIFS protocols to identify and prevent infected files from downloading into users' devices. In addition to the gateway anti-viurs, Cisco ISA500 also supports web reputation filter which prevents users from accessing web sites that may contain malware. By combining both

gateway anti-virus and web reputation filter, Cisco ISA500 can effectively protect businesses from the most active malicious malware.

Q. Can I use ISA500 as an Internet gateway or do I need to put another router in front of it?

A. Cisco ISA500 comes with many Internet features, such as dual WAN, PPPoE, DHCP, NAT, PAT, routing, VLAN, inter-vlan routing, etc. features. Thus, it can be used as a Internet gateway.

Q. Does ISA500 support wireless to allow my iPhone, iPad, laptop, and other wireless devices to connect?

A. Yes, Cisco ISA500 provides 802.11b/g/n capability in its wireless models, which can allow different mobile wireless devices to connect to the network. It also supports multiple SSIDs and guest wireless Internet access to the secure intranet from guest networks.

Q. Can ISA500 support WAN redundancy?

A. ISA500 supports different types of WAN redundancy, such as the following to improve business continuity:

- Failover
- Load balancing based on bandwidth
- Load balancing based on remaining bandwidth
- Policy based routing (PBR)

Q. Can you customize IPS signatures on the ISA500?

A. ISA500 is designed for simplicity. It does not provide customization support so that administrators can tune their IPS signatures. However, you can disable and enable certain types of signatures to improve performance. For example, you can select signatures that are relevant to Unix operating systems and disable them if there are no Unix based servers and devices on your networks.

Q. When IPS is enabled, what is the throughput on the ISA500?

A. Table 1 provides a high-level performance comparison of the ISA550 and ISA570. Both offer superior performance compared to third-party vendors like SonicWALL and Fortinet (see the Cisco ISA500, Fortinet and SonicWALL comparison table later in this document).

Q. Does the ISA500 provide both onbox and cloud-based management options? Does it support reporting?

A. The ISA500 can be managed using the embedded Security Appliance Configuration Utility, a powerful yet easy-to-use browser-based management and monitoring interface. It provides browser-based configuration GUI that uses a simplified configuration flow with default settings (i.e. step-by-step configuration wizards). 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 intervals and times. 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.

Please contact your sales representative for availability

Q. Do I need to purchase Cisco OnPlus to use OnPlus Advanced Security Services?

A. Yes. Cisco OnPlus Advanced Security services are advanced services provided on top of Cisco OnPlus. In order to use them, customers need to have Cisco OnPlus. However, OnPlus Advanced Security Services is provided free of charge along with Cisco OnPlus.

Q. What kind of support does Cisco provide for the ISA500?

A. The Cisco ISA500 service option is the Small Business Support Contract. It's supported by a dedicated Cisco Small Business Support team. Its service option is the Small Business Support Services – CON-SBS-SVC2. This service provides:

- Three year 'peace-of-mind' support
- Call and online chat support
- Software updates
- Next-business-day hardware replacement

Q. What are typical use cases supported by the ISA500?

A. The ISA500 supports a wide variety of use cases that include multi-site businesses, businesses with multiple departments that want to segregate traffic by department in addition to remote and mobile workers. Some sample use cases are:

- Multi-site businesses, businesses with multiple departments that want to segregate traffic by department and secure VPN
- Secure VPN gateway for remote workers and remote offices to securely connect to offices
- A 75 employees manufacturing firm that wants to separate traffic by business groups and applies different access rules among the groups
- Teleworker devices for executive or remote workers

A typical multi-site retail use case is shown in Figure 1. See Appendix A for application diagrams and additional use cases.

Figure 1. Cisco ISA500 Use Case: Security Gateway at Multiple Company Locations
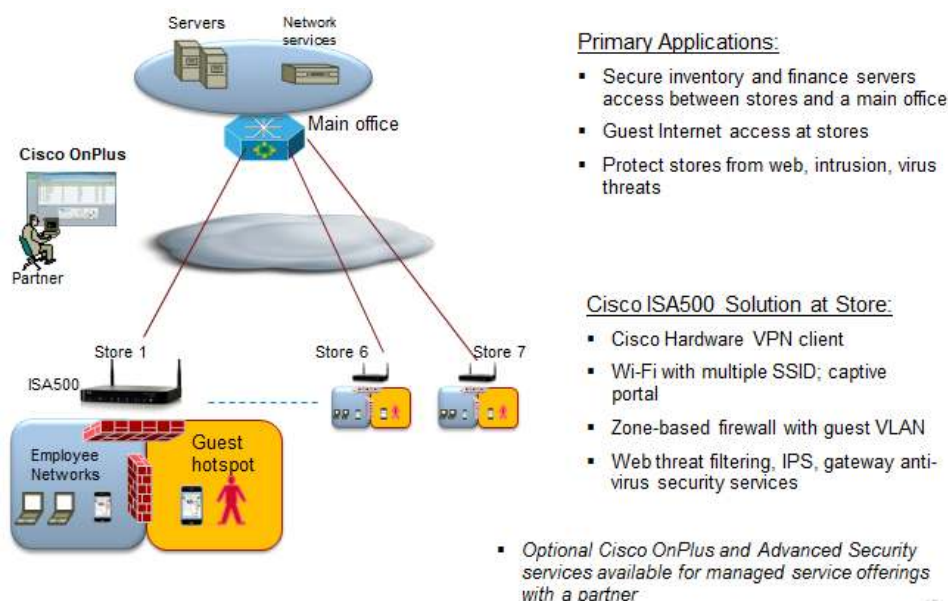
Primary Differences between the New Cisco ISA500 and Cisco SA500

Q. Is the Cisco SA500 still available?

A. The Cisco SA500 is being replaced by the new Cisco ISA500.

Q. What are the primary differences between the Cisco SA500 and the new Cisco ISA500?

A. Cisco ISA500 is built with brand new hardware and software architectures compared to the SA500. It provides more advanced and deeper security services than the Cisco SA500. Table 4 summarizes the primary feature differences.

In addition to the feature differences, ISA500 has adopted many Cisco security solutions. For example, instead of using the Trend Micro Protectlink product for web blocking and filtering, ISA500 uses Cisco Security Intelligence Operations (SIO), which provides strong threat intelligence to deliver superior threat protection. It also uses 75 TB of threat telemetry per day from market-leading email, web, firewall, IPS, and endpoint clients. This allows it to provide unparalleled global threat intelligence, and to protect infrastructure and applications from advanced persistent threats (APTs) and other sophisticated attacks. This does not only enhance threat protection, but also makes the support experience better with faster turnaround times. Cisco ISA500 will also take full advantage of Cisco AnyConnect for VPN clients – both IPSec and SSL.

Table 4. Primary Feature Differences between the New Cisco ISA500 and Cisco SA500

Feature Highlights	SA500	ISA500 (New)
Firewall	Stateful firewall	Zone-based stateful firewall
Gateway Anti-virus	No	Yes
Web Reputation	Trend Micro	Cisco
Web URL filtering	Trend Micro	Cisco
Network Reputation	No	Yes
Spam Filtering	Trend Micro	Cisco
Application Control	No (basic IM/P2P)	Yes, more than 100 applications

Feature Highlights	SA500	ISA500 (New)
Rogue Access Point Detection	No	Yes
Remote User IPSec VPN	Open VPN client	Cisco VPN client
Remote User SSL VPN	Non Cisco	Cisco AnyConnect VPN client
Teleworker VPN client (EzVPN Client Mode)	No	Yes
802.1x Support	No	Yes
IPS Performance	Less than 30 Mbps	60 Mbps on ISA550 and 90 Mbps on ISA570
UTM Performance	Less than 30 Mbps	45 Mbps on ISA550 and 75 Mbps on ISA570
Guest Access Management	No	Yes, guest VLAN isolation and captive portal support
DMZ	Either dual WAN or 1 Wan and 1 DMZ	Up to 4 DMZ; supports both dual WAN and DMZ together
IPS Hardware Acceleration	No	Yes on ISA570 and ISA570W
Configuration Wizards	No	Yes, six wizards
QoS	Basic	Advanced, including low latency queuing
Dual WAN	Yes	Advanced, with weighted load balancing
Network Address Translation (NAT)	Basic	Advanced
Virtual Router Redundancy Protocol (VRRP)	No	Yes (one VLAN only)
Spanning Tree	No	Yes
OnPlus Advanced Security Services	No	Yes
Onbox Security Reports	No	Yes

Q. What is the performance of the Cisco ISA500 compared to Fortinet and SonicWALL?

A. The Cisco ISA500 has equal to or better than throughput performance compared to Fortinet and SonicWALL. In particular, it outperforms both of these competing offerings when the full breadth of UTM services is enabled (see Table 5).

Primary Cisco ISA500 Competitive Differentiators

Table 5. Cisco ISA500 Comparison with Competitive Offerings

Performance Area	Cisco ISA550	Cisco ISA570	Fortinet FG-20C	Fortinet FG-40C	Fortinet FG-60C	SonicWALL TZ105	SonicWALL TZ205	SonicWALL TZ215
Firewall Throughput	200 Mbps	500 Mbps	20 Mbps	200 Mbps	1 Gbps	200 Mbps	500 Mbps	500 Mbps
VPN Throughput	75 Mbps	130 Mbps	20 Mbps	60 Mbps	70 Mbps	75 Mbps	100 Mbps	130 Mbps
Anti-Virus Throughput	50 Mbps	80 Mbps	20 Mbps	40 Mbps	40 Mbps	40 Mbps	60 Mbps	70 Mbps
IPS Throughput	60 Mbps	90 Mbps	20 Mbps	135 Mbps	135 Mbps	60 Mbps	80 Mbps	110 Mbps
UTM Throughput	45 Mbps	75 Mbps	<20 Mbps	<40 Mbps	<40 Mbps	25 Mbps	40 Mbps	60 Mbps

Q. Why choose Cisco ISA500 over SonicWALL?

A. See Table 6 for a listing of Cisco advantages.

Table 6. Cisco Advantages over SonicWALL TZ Series

Cisco Advantages	Cisco ISA500	SonicWALL TZ Series
Superior Internet Access and Security Solution	• Superior security threat protection by unrivaled global security threat intelligence from Cisco SIO • Higher UTM performance	• Security R&D investment is only a fraction of Cisco's • Lower UTM performance
Easy to Use and Fast to Deploy	• Easy to navigate; simplified setup flow • Interoperability tested with other Cisco products	• Cumbersome navigation • More steps required to set up

Cisco Advantages	Cisco ISA500	SonicWALL TZ Series
Simplified Pricing, Cost Effective to Deploy and Manage	• Simplified packaging – eight SKUs, only one license, consistent features • Manageable by Cisco hosted cloud-based management services – OnPlus, and Cisco Advanced Security Services • Pay-as-you-go pricing model with Cisco OnPlus	• Complicated packaging • Requires higher upfront cost ($7000 or more for GSM security appliance) and can only manage the security solution • Requires resources to host and manage its management appliance

Q. Why choose Cisco ISA500 over Fortinet?

A. See Table 7 for a listing of Cisco advantages.

Table 7. Cisco Advantages over Fortinet Fortigate 20/40/60

Cisco Advantages	Cisco ISA500	Fortinet Fortigate 20/40/60
Superior Internet Access and Security Solution	• Superior security threat protection by unrivaled global security threat intelligences from Cisco SIO • Higher security service (UTM) performance	• Security R&D investment is only a subset of Cisco's • Its claimed "ASIC" performance disappears with security services enabled
Easy to Use and Fast to Deploy	• Easy to navigate; simplified setup flow • Interoperability tested with other Cisco products	• "Fit" to SMB (not designed for SMBs) • No built-in wizard; More steps required to set up security services
Simplified Pricing, Cost Effective to Deploy and Manage	• Simplified packaging – eight SKUs, only one license, consistent features • Manageable by Cisco hosted cloud-based management services – OnPlus and Advanced Security Services • Pay-as-you-go pricing model with Cisco OnPlus	• Requires high upfront cost • Managed service offerings • Requires resource to host and manage its management appliance

Cisco ISA500 Purchasing Information and Additional Resources

Q. How can I buy the Cisco ISA500?

A. A: The Cisco ISA500 is sold via Cisco partners. To purchase it, please contact a Cisco Partner. A list of Cisco partners can be found at: http://tools.cisco.com/WWChannels/LOCATR/openBasicSearch.do?smb=Y

Q. How can I learn more about the Cisco ISA500?

A. For more information about the Cisco Small Business ISA500 Series Integrated Security Appliance, contact your local Cisco partner or visit www.cisco.com/go/isa500resources.

For more information about Cisco OnPlus, visit www.cisco.com/en/US/products/ps11792/index.html.

For more information about Cisco Small Business Support Services, visit www.cisco.com/go/isa500resources.

Appendix A. Cisco Small Business ISA500 Series Use Cases

**Figure 2.** Cisco ISA500 Use Case: Internet Gateway at Small Advertising Firm

Primary Applications:

- Protect business from web threat, intrusion, and virus/malware threats
- Block employees from accessing gaming web sites and Facebook through company Internet
- Keep business running in the case of an Internet failure

Cisco ISA500 Solution:

- Web reputation filtering, gateway, anti-virus, stateful firewall, network reputation filter, IPS
- Web URL filtering, and application control
- Dual Gigabit Ethernet WAN with load balance, Policy Based Routing, failover support

Figure 3. Cisco ISA500 Use Case: VPN Gateway at Multiple Company Locations
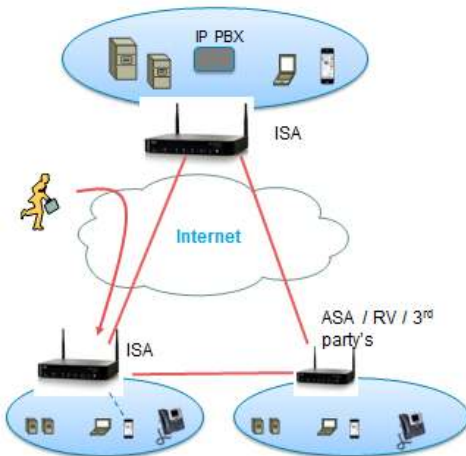
Primary Applications:

- Site-to-site secure data and voice communication
- Mobile workforce secure remote access to offices

Cisco ISA500 Solution:

- Site-to-Site IPSec VPN (AES-256)
- Session Initiated Protocol (SIP) Application Layer Gateway (ALG)
- QoS over VPN
- AnyConnect™ VPN / Cisco VPN

Figure 4.   Cisco ISA500 Use Case: Secure Internet and Intranet Gateway
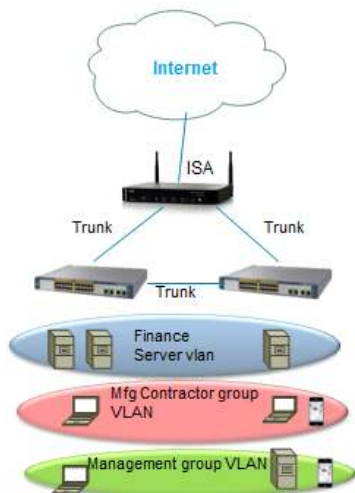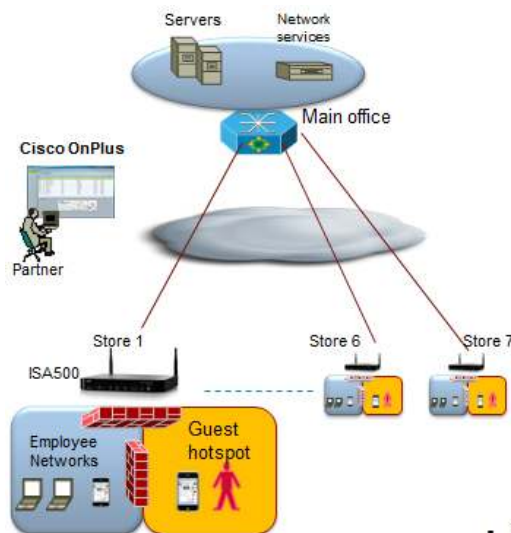

Primary Applications:

- Separate traffic among different use groups
    - Allow management VLAN access to finance server but not manufacturing contractor group
- Apply different security policies to different groups
    - Block manufacturing contractor group from accessing gaming web sites and Facebook
    - Protect all employees from web and virus/malware threats
- Switching network integration

Cisco ISA500 Solution:

- Zone Firewall
- DHCP server per VLAN
- Web URL filtering, application control, Web threat filtering, gateway anti-virus, IPS
- 802.1Q Trunking; Single Transfer Point (STP)

Figure 5.   Cisco ISA500 Use Case: Security Gateway at Multiple Company Locations
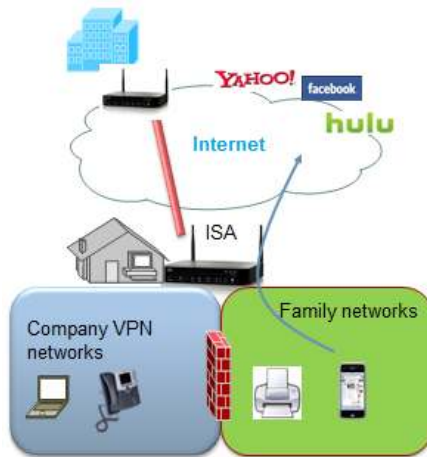

Primary Applications:

- Secure inventory and finance servers access between stores and a main office
- Guest Internet access at stores
- Protect stores from web, intrusion, virus threats

Cisco ISA500 Solution at Store:

- Cisco Hardware VPN client
- Wi-Fi with multiple SSID; captive portal
- Zone-based firewall with guest VLAN
- Web threat filtering, IPS, gateway anti-virus security services
- *Optional Cisco OnPlus and Advanced Security services available for managed service offerings with a partner*

Figure 6.   Cisco ISA500 Use Case: Teleworker Support
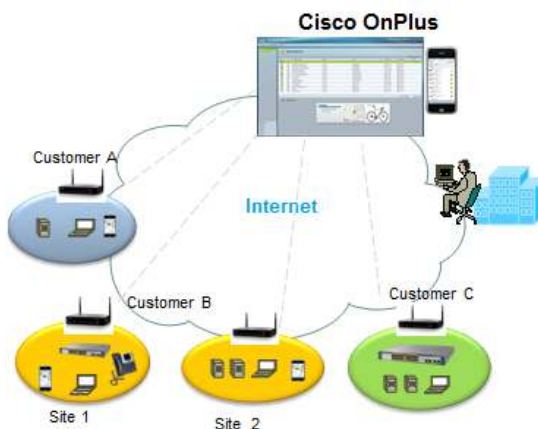

Primary Applications:

- Secure always-on connection to company network
- Company and family networks isolation and policy support

Cisco ISA500 Solution:

- Cisco EzVPN hardware client
- Split tunneling support
- Zone-based firewall
- 802.1x
- UTM multi-threat protection

Figure 7.   Cisco ISA500 Use Case: Security Services Managed by Partners

Primary Applications:

- Managed network and security service offerings

Cisco ISA500 Solution:

- Cisco ISA500 with term-based security license
- OnPlus management services – multi-sites and multi-tenants
- Security services reports with OnPlus Advanced Security Services

CISCO

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 **www.cisco.com/go/offices.**

Printed in USA

C67-719997-00   11/12