For
Small
Business

All-in-One Security for Your Small Business

Secure your business network with a single, flexible, affordable solution.

In today's connected world, businesses that preserve the integrity of their network gain a powerful advantage. When a company can protect itself against intruders, spam, phishing, and other viral hazards, it avoids the costly pitfalls of other, less secure networks. The Cisco® SA 500 Series Security Appliances, part of the Cisco Small Business Pro Series, are designed to help small businesses do just that. By guarding every component of your network—at the mobile, gateway, server, and client levels—the Cisco SA 500 Series helps ensure that productivity never gets interrupted and business can keep moving.

As the worldwide leader in networking and communications, Cisco is dedicated to empowering small businesses like yours. The Cisco SA 500 Series is a simple, flexible solution that fits neatly into your network—and your business strategy. By fortifying your network with the Cisco SA 500 Series, you gain more than absolute security and transparent connectivity for your network. You lay a foundation for robust business performance, now and in the future.

The Cisco SA 500 Series provides:
· **Improved business resiliency:** Prevent disruption of business-critical applications and services due to security breaches by implementing a robust business-grade firewall, along with support for IPS, email and web security.

· **Enhanced authentication security for remote users:** Prevent unauthorized access to your business network by using hardware- or software-generated one-time-use passwords.

· **Increased employee productivity:** Prevent the loss of employee productivity by protecting your network against spam, spyware, and inappropriate web browsing, using the optional Cisco ProtectLink Gateway.

· **Reduced IT costs:** Free up IT support resources and avoid the costly process of cleaning up infections due to spyware, viruses, and other malware by preventing them from occurring.

· **Easy-to-deploy remote access:** Allow employees and partners to quickly and easily connect to the business with SSL VPN.

· **Improved business efficiency:** Reduce costs associated with deployment, ongoing management, and monitoring of the security solution by using a single, easy-to-install, easy-to-use solution.

· **Decreased liability:** Reduce the company's exposure to liability due to compromised data or inadequate corporate controls by implementing comprehensive access control and threat protection services in a single device.

· **Peace of mind:** Get maximum value from your Cisco solution with the Cisco Small Business Pro Service.

Service and Support
The Cisco SA 500 Series is backed by the Cisco Small Business Pro Service, which provides affordable coverage for any small business owner. Delivered by Cisco, this comprehensive service includes software upgrades and updates, extended access to the Cisco Small Business Support Center, and next-business-day hardware replacement when needed.[*] In addition, it provides community-based support that allows small businesses to connect and collaborate via online forums and wikis.

For more information about the Cisco SA 500 Series, visit www.cisco.com/go/sa500.

[*] Where available.

Comprehensive gateway security and VPN connectivity.

With its combined firewall, email, and web security capabilities, the Cisco SA 500 Series stops threats before they enter the network and affect business operations.

Cisco SA 500 Series Security Appliances

	SA 520	SA 520W	SA 540
SKU	SA520-K9	SA520W-K9	SA540-K9
Firewall			
Stateful packet inspection throughput*	200 Mbps	200 Mbps	300 Mbps
Firewall + email + web security throughput	200 Mbps	200 Mbps	300 Mbps
Connections	15,000	15,000	40,000
Rules	100	100	100
Schedules	●	●	●
IPS	●	●	●
Peer-to-peer and IM blocking	●	●	●
VPN			
3DES/AES VPN throughput*	65 Mbps	65 Mbps	85 Mbps
IPsec VPN tunnels	50 max	50 max	100 max
SSL VPN tunnels	2 seats included; license required to upgrade to 25 seats (max)	2 seats included; license required to upgrade to 25 seats (max)	50 seats (max) included
	●	●	●
Dead peer detection	●	●	●
IPsec NAT traversal	●	●	●
NetBIOS broadcast over VPN	●	●	●
Cisco ProtectLink Gateway			
URL filtering	80+ categories	80+ categories	80+ categories
Web threat protection	●	●	●
Antispam protection	●	●	●
Virus patterns	More than 3 million	More than 3 million	More than 3 million
Spyware patterns	More than 420,000	More than 420,000	More than 420,000
Wireless			
802.11b/g/n	○	●	○
2 x 3 multiple input, multiple output (MIMO)	○	●	○
2.4 GHz	○	●	○
Wi-Fi Multimedia quality of service	○	●	○
Unscheduled automatic power save delivery	○	●	○
MAC filtering	○	●	○
WEP, Wi-Fi Protected Access Pre-Shared Key	○	●	○
Basic service set identifier (BSSID)	○	●	○
Ability to dynamically or manually adjust transmit power	○	●	○
Wi-Fi Protected Setup (WPS)	○	●	○
Other			
Routing	Static, RIP v1, v2	Static, RIP v1, v2	Static, RIP v1, v2
VLANs	16	16	16
IPsec/Point-to-Point Tunneling Protocol	●	●	●
Message digest	MD5/SHA1/SHA2	MD5/SHA1/SHA2	MD5/SHA1/SHA2
Encryption	DES/3DES/AES	DES/3DES/AES	DES/3DES/AES
User database	100	100	400
Dynamic DNS (DDNS)	●	●	●
Load balancing	●	●	●
Integrated and automated failover and failback	Yes, using optional port for dual WAN	Yes, using optional port for dual WAN	Yes, using optional port for dual WAN
VeriSign VIP support	●	●	●
Physical Interfaces	· All Ethernet ports 10BASE-T, 100BASE-TX, 1000BASE-T capable · 4 LAN ports · 1 WAN port · 1 optional port for use as LAN, WAN, or DMZ port · 1 USB 2.0 port · 1 power switch	· All Ethernet ports 10BASE-T, 100BASE-TX, 1000BASE-T capable · 4 LAN ports · 1 WAN port · 1 optional port for use as LAN, WAN, or DMZ port · 1 USB 2.0 port · 1 power switch · 3 external antennas	· All Ethernet ports 10BASE-T, 100BASE-TX, 1000BASE-T capable · 8 LAN ports · 1 WAN port · 1 optional port for use as LAN, WAN, or DMZ port · 1 USB 2.0 port · 1 power switch

○ – Not Included   ● – Included

* Performance test methodology: Maximum performance based on RFC 2544. All results are aggregate bidirectional. Actual performance may vary upon network environment and configuration.