

Cisco Web Security Appliance



In a highly connected and increasingly mobile world with more and more complex and sophisticated threats, Cisco delivers the strong protection, complete control, and investment value businesses need. We offer the broadest set of web security deployment options in the industry, combined with market-leading global threat intelligence. The Cisco® Web Security Appliance simplifies security with a high-performance, dedicated appliance, and the Cisco Web Security Virtual Appliance enables businesses to deploy web security wherever and whenever it's needed.

Product Overview

The Cisco Web Security Appliance (WSA) is the first highly secure web gateway to combine advanced malware protection, application visibility and control, acceptable use policy controls, insightful reporting, and secure mobility on a single platform. Helping organizations address the growing challenges of securing and controlling web traffic, the Cisco WSA provides continuous monitoring and analysis across the extended network and throughout the full attack continuum-before, during, and after an attack.

With its simplified architecture, it enables faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs than separate competing products. "Set and forget" technology frees up staff once initial automated policy settings go live. Automatic security updates are pushed to network devices every three to five minutes. Flexible deployment options and integration with the existing security infrastructure help customers meet demanding business needs.

Virtual Appliance

With the growth of video and other rich media, traffic has become less predictable. To address capacity overages and prevent drops in performance, administrators need to allow for long lead times, remote installation challenges, customs duties, and other logistical issues involved with buying and installing hardware, especially in multinational organizations.

The Cisco Web Security Virtual Appliance (WSAV) significantly lowers the cost of deploying web security, especially in highly distributed networks, by letting administrators create security instances where and when they are needed. The Cisco WSAV is a software version of the Cisco WSA that runs on top of a VMware ESXi hypervisor and Cisco Unified Computing System™ (Cisco UCS®) servers. A Cisco WSAV license is included in all Cisco web security software bundles and can be used for as many virtual machines as needed.

With the Cisco WSAV, administrators can respond instantly to traffic spikes and eliminate capacity planning. There is no need to buy and ship appliances; new business opportunities can be supported without adding complexity to a data center or requiring additional staff.

Features and Benefits

Real-time Threat Intelligence	<p>Receive fast and comprehensive web protection backed by the largest threat detection network in the world, with the broadest visibility and largest footprint, including:</p> <ul style="list-style-type: none"> • 100 TB of security intelligence daily • 1.6 million deployed security devices, including firewall, IPS, web, and email appliances • 150 million endpoints • 13 billion web requests per day • 35 percent of the world's enterprise email traffic <p>Cisco Security Intelligence Operations (SIO) provides a 24x7 view into global traffic activity to analyze anomalies, uncover new threats, and monitor traffic trends. SIO prevents zero-hour attacks by continually generating new rules that feed updates to the WSA every three to five minutes, providing industry-leading threat defense hours and even days ahead of competitors.</p>
Zero-Day Threat Protection	<p>Defend against malware and advanced persistent threats using multiple layers of anti-malware technologies. Cisco Web Reputation Filters analyze more than 200 different web traffic- and network-related parameters to provide a powerful outer layer of malware defense from zero-day threats. Administrators can then run multiple anti-malware scanning engines in parallel on a single appliance. Adaptive scanning dynamically selects the most relevant scanner based on URL reputation, content type, and efficacy of the scanner and improves the catch rate by scanning high-risk objects first during increased scan loads.</p>
Advanced Malware Protection	<p>Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco Web Security customers. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis and retrospective alerting. It leverages the vast cloud security intelligence networks of both Cisco and Sourcefire (now part of Cisco).</p> <p>AMP augments the anti-malware detection and blocking capabilities already offered in Cisco Web Security with enhanced file reputation capabilities, detailed file behavior reporting, continuous file analysis, and retrospective verdict alerting. Learn more.</p>
Layer 4 Traffic Monitoring	<p>The Layer 4 Traffic Monitor continuously scans activity, detecting and blocking spyware “phone-home” communications. By tracking all network applications, the Layer 4 Traffic Monitor effectively stops malware that attempts to bypass classic web security solutions. It dynamically adds IP addresses of known malware domains to its list of malicious entities to block.</p>
Web Usage Controls	<p>Combine traditional URL filtering with dynamic content analysis to mitigate compliance, liability, and productivity risks. Cisco's continuously updated URL filtering database of over 50 million blocked domains provides exceptional coverage for known websites, and the Dynamic Content Analysis (DCA) engine accurately identifies 90 percent of unknown URLs in real time. It scans text, scores the text for relevancy, calculates model document proximity, and returns the closest category match. Administrators can also select specific categories for intelligent HTTPS inspection.</p>
Granular Application Visibility and Control	<p>Easily control the use of hundreds of Web 2.0 applications and more than 150,000 micro applications. Granular policy control allows administrators to permit the use of applications such as Dropbox or Facebook while blocking users from activities such as uploading documents or clicking the “Like” button. The Cisco WSA supports visibility of activity across an entire network.</p>
Data Loss Prevention (DLP)	<p>Prevent confidential data from leaving the network by creating context-based rules for basic data loss prevention (DLP). The Cisco WSA also uses Internet Content Adaptation Protocol (ICAP) to integrate with third-party DLP solutions for deep content inspection and enforcement of DLP policies.</p>
Roaming User Protection	<p>Safeguard data requested by roaming laptop devices. Provides web security to remote clients by initiating a VPN tunnel that redirects traffic back to the on-premises solution, analyzing traffic in real time before permitting access.</p>
User Authentication	<p>The Cisco WSA offers a choice of options for authenticating users. That includes authentication via Lightweight Directory Access Protocol (LDAP), NT LAN Manager (NTLM) Protocol, and Kerberos - a third-party authentication mechanism. Using Kerberos, WSA can authenticate clients that have joined the domain transparently. Kerberos provides better performance and interoperability than NTLM, including compatibility with non-Windows clients.</p>

IPv6 Support	Cisco WSAs running the latest version of AsyncOS (Version 8.0 and above) have the ability to proxy, monitor, and manage IPv6 traffic. IPv6 proxy capabilities can be deployed via Web Cache Communication Protocol (WCCP) and Explicit mode. The ability to monitor and manage IPv6 traffic is beneficial, even for customers that have not migrated to IPv6, as IPv6 traffic may still be running on their network.
Centralized Management and Reporting	Receive actionable insights across threats, data, and applications. The Cisco WSA provides an easy-to-use, centralized management tool to control operations, manage policies, and view reports. The Cisco M-Series Content Security Management Appliance provides central management and reporting across multiple appliances and multiple locations, including virtual instances. The Cisco WSA also enables a custom Splunk application with an interface that's similar to on-appliance reporting for scalability and flexibility.
Flexible Deployment	The Cisco WSAV offers all the same features as the Cisco WSA, with the added convenience and cost savings of a virtual deployment model, including instant self-service provisioning. With a Cisco WSAV license, businesses can deploy web security virtual gateways without being connected to the Internet by applying the license to a new Cisco WSAV virtual image file stored locally. Pristine virtual image files can be cloned, if needed, to deploy several web security gateways immediately. Run hardware and virtual machines in the same deployment. Small branch offices or remote locations can have the same protection the Cisco WSA provides without having to install and support hardware at that location. Custom deployment is easily managed with the Cisco M-Series Content Security Management Appliance.

Product Specifications

Tables 1 and 2 show the performance and hardware specifications, respectively, for the Cisco WSA. Table 3 shows the specifications of various Cisco WSAV models, and Table 4 shows the number of users supported by models in the Cisco M-Series Content Security Management Appliance portfolio.

Table 1. Cisco Web Security Appliance Performance Specifications

	Users*	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large enterprise	6,000-12,000	S680	4.8 TB (8 x 600 GB SAS)	Yes (RAID 10)	32 GB	16 (2 octa-core) 2.70 GHz
Midsize office	1,500-6,000	S380	2.4 TB (4 x 600 GB SAS)	Yes (RAID 10)	16 GB	6 (1 hex-core) 2.00 GHz
		S370	1.8 TB (4 x 450 GB SAS)	Yes (RAID 10)	4 GB	4 (1 quad-core) 2.26 GHz
SMB and branch	Less than 1,500	S170	500 GB (2 x 250 GB SATA)	Yes (RAID 1)	4 GB	2 (1 dual-core) 2.80 GHz

* Please confirm sizing guidance with a Cisco content security specialist to help ensure your solution will meet your current and projected needs.

Table 2. Cisco Web Security Appliance Hardware Specifications

	Cisco S680	Cisco S380	Cisco S370	Cisco S170
Hardware platform				
Form factor	2RU	2RU	2RU	1RU
Dimensions	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm)	3.5 x 17.75 x 29 in. (8.9 x 45.1 x 73.7 cm)	1.64 x 19 x 15.25 in. (4.2 x 48.3 x 38.7 cm)
Redundant power supply	Yes	Yes	Yes	No
Remote power cycle	Yes	Yes	No	No
DC power option	Yes	Yes	No	No
Hot-swappable hard disk	Yes	Yes	Yes	Yes
Fiber option	Yes (accessory)	No	No	No
Ethernet	4 gigabit network interface cards (NICs), RJ-45	4 gigabit NICs, RJ-45	4 gigabit NICs, RJ-45	2 gigabit NICs, RJ-45
Speed (Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate

Table 3. Cisco Web Security Virtual Appliance Models

Web Users				
Web Users	Model	Disk	Memory	Cores
Less than 1000	S000v	250 GB	4 GB	1
1000-2999	S100v	250 GB	6 GB	2
3000-6000	S300v	1024 GB	8 GB	4
Servers				
Cisco UCS			ESXi 4.0 X 5.0 Hypervisor	

Table 4. Cisco M-Series Content Security Management Appliance, Number of Supported Users by Model

Model	Cisco M1070	Cisco M680	Cisco M670	Cisco M380	Cisco M170
Users (approx.)	More than 10,000	More than 10,000	Up to 10,000	Up to 10,000	Up to 1,000

Deployment

The Cisco WSA is a forward proxy that can be deployed in either Explicit mode using proxy automatic configuration (PAC) files and Web Proxy Auto-Discovery (WPAD) browser settings, or Transparent mode using Web Cache Communication Protocol (WCCP) with policy-based routing (PBR) load balancers. WCCP-compatible devices reroute web traffic to the WSA. These devices include Cisco Catalyst® 6000 Series Switches, Cisco ASR 1000 Series Aggregation Services Routers, Cisco Integrated Services Routers (ISRs), and Cisco ASA 5500-X Series Next-Generation Firewalls.

The WSA can proxy HTTP, HTTPS, SOCKS, native FTP, and FTP over HTTP traffic to deliver additional capabilities such as data loss prevention, mobile user security, and advanced visibility and control.

Licensing

A Cisco WSAV license is included in all Cisco web security software bundles (Cisco Web Security Essentials, Cisco Web Security Anti-Malware, and Cisco Web Security Premium). This license has the same term as the other software services in the bundle and can be used for as many virtual machines as needed.

Term-Based Subscription Licenses

Licenses are term-based subscriptions of one, three, or five years.

Quantity-Based Subscription Licenses

The Cisco web security portfolio uses tiered pricing based on a range of users, not devices. Sales and partner representatives can help to determine the correct sizing for each customer deployment.

Web Security Software Licenses

Four web security software licenses are available: Cisco Web Security Essentials, Cisco Anti-Malware, Cisco Web Security Premium, and McAfee Anti-Malware. The major components of each software offering are provided below:

Bundles	Description
Cisco Web Security Essentials	Provides protection and control of an organization's web traffic using URL filtering, reputation and application visibility and control technologies (Cisco Web Usage Controls, Cisco Web Reputation, and software subscription support). Includes a license for Cisco Web Security Virtual Appliance.
Cisco Web Security Anti-Malware	Combines Cisco Web Reputation with deep content scanning (Cisco Web Reputation, Sophos Anti-Malware, Webroot Anti-Malware, and software subscription support). Includes license for Cisco Web Security Virtual Appliance.

Bundles	Description
Cisco Web Security Premium	Combines URL filtering defense with deep content scanning (Cisco Web Usage Controls, Cisco Web Reputation, Sophos Anti-Malware, Webroot Anti-Malware, and software subscription support). Includes license for Cisco Web Security Virtual Appliance.
McAfee Anti-Malware	Includes both virus and malware signature scanning and can perform both signature- and heuristics-based scanning.
A-la-Carte Offerings	Description
Advanced Malware Protection	Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco Web Security customers. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis and retrospective alerting. It leverages the vast cloud security intelligence networks of both Cisco and Sourcefire (now part of Cisco). AMP augments the anti-malware detection and blocking capabilities already offered in Cisco Web Security Appliance with enhanced file reputation capabilities, detailed file behavior reporting, continuous file analysis, and retrospective verdict alerting.

Software License Agreements

The Cisco End-User License Agreement (EULA) and the Cisco Web Security Supplemental End-User License Agreement (SEULA) are provided with each software license purchase.

Software Subscription Support

All Cisco web security licenses include software subscription support that is essential to keeping business-critical applications available, highly secure, and operating at peak performance. This support entitles customers to the services listed below for the full term of the purchased software subscription:

- Software updates and major upgrades to keep applications performing optimally at the most current feature set
- Access to the Cisco Technical Assistance Center (TAC) for fast, specialized support
- Online tools to build and expand in-house expertise and boost business agility
- Collaborative learning for additional knowledge and training opportunities

Services

Cisco Branded Services	<p>Cisco Security Planning and Design: Enables deployment of a robust security solution quickly and cost effectively</p> <p>Cisco Web Security Configuration and Installation: Mitigates web security risks by installing, configuring, and testing appliances to implement:</p> <ul style="list-style-type: none"> • Acceptable-use-policy controls • Reputation and malware filtering • Data security • Application visibility and control <p>Cisco Security Optimization Service: Supports an evolving security system to address security threats, design updates, performance tuning, and system changes.</p>
Collaborative/Partner Services	<p>Cisco Network Device Security Assessment: Helps maintain a hardened network environment by identifying gaps in network infrastructure security.</p> <p>Cisco Smart Care: Provides actionable intelligence gained from highly secure visibility into a network's performance.</p> <p>Additional services: Cisco partners provide a wide range of valuable services across the planning, design, implementation, and optimization lifecycle.</p>
Cisco Financing	<p>Cisco Capital[®] can tailor financing solutions to business needs. Access Cisco technology sooner and see the business benefits sooner.</p>

Cisco SMARTnet Support Services

Customers have the option to purchase Cisco SMARTnet™ for use with Cisco Web Security Appliances. Cisco SMARTnet helps customers resolve network problems quickly with direct, anytime access to Cisco experts, self-help support tools, and rapid hardware replacement. For more information, visit <http://www.cisco.com/go/smartnet>.

Warranty Information

Find warranty information on Cisco.com at the [Product Warranties](#) page.

For More Information

Find out more at <http://www.cisco.com/go/wsa>. Evaluate how the Cisco Web Security Appliance will work for you with a Cisco sales representative, channel partner, or systems engineer.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)