

Cisco Web Security Appliance



For security, your network needs malware protection, application visibility and control, acceptable use policy controls, insightful reporting and secure mobility. Cisco offers this protection, all on a single platform: the Cisco® Web Security Appliance (WSA).

In our highly connected and increasingly mobile world, more complex and sophisticated threats require the right mix of security solutions. Cisco delivers security for all layers of network infrastructure with the strong protection, complete control, and investment value businesses need. We also offer a broad set of web security deployment options, along with market-leading global threat intelligence. The Cisco WSA simplifies security with a high-performance, dedicated appliance, and the Cisco Web Security Virtual Appliance (WSAV) lets businesses deploy web security quickly and easily, wherever and whenever it's needed.

The Cisco WSA was one of the first secure web gateways to combine leading protections to help organizations address the growing challenges of securing and controlling web traffic. It enables simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs. "Set and forget" technology frees staff after initial automated policy settings go live, and automatic security updates are pushed to network devices every 3 to 5 minutes. Flexible deployment options and integration with your existing security infrastructure help you meet quickly evolving security requirements.

Virtual Appliance

With the growth of video and other rich media, traffic has become less predictable, resulting in overages and degraded performance. Addressing these and other issues, administrators face long lead times when buying and installing hardware, remote installation challenges, customs duties, and other logistical issues, especially in multinational organizations.

The Cisco 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 or KVM hypervisor and Cisco Unified Computing System™ (Cisco UCS®) servers. You will receive an unlimited license for the Cisco SMAV with the purchase of any of the Cisco Email or Web Security software bundles, along with the corresponding SMA software license.

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

Talos Security 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% of the world's enterprise email traffic <p>Providing a 24x7 view into global traffic activity to analyze anomalies, uncover new threats, and monitor traffic trends. Talos prevents zero-hour attacks by continually generating new rules that feed updates to the WSA every three to five minutes, enabling industry-leading threat defense hours and even days ahead of competitors.</p>
Cisco 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 sites 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>
Advanced Malware Protection	<p>Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco WSA customers. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting. It takes advantage of the vast cloud security intelligence networks of both Cisco and Sourcefire® technology. AMP augments the malware detection and blocking capabilities already offered in the Cisco WSA with enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. The Cisco AMP Threat Grid delivers malware protection through an on-premises appliance for organizations that have compliance or policy restrictions on submitting malware samples to the cloud. 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>
Cognitive Threat Analytics	<p>Cisco Cognitive Threat Analytics is a cloud-based solution that reduces time to discovery of threats operating inside the network. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection. Take advantage of Cisco Cognitive Threat Analytics with a simple add-on license to your Web Security solution. Reduce complexity while gaining superior protection that evolves with your changing threat landscape.</p>
Cloud Access Security	<p>Cisco can protect you from the hidden threats lurking in cloud apps. We have partnered with leading CASB providers to deliver new visibility by monitoring your cloud app usage in real time, extending your control in a cloud-first, mobile-first world, and combating evolving threats through intelligent protection powered by data science. Ecosystem partners such as Elastic integrate smoothly with your customer's existing security architecture to extend on-premises protection into the cloud. Cloud Access Security solutions provide full visibility of your cloud app environment; classify all cloud traffic passing through the gateway to detect intrusions and data leakage; and automatically enforce any new global security policies across all sanctioned and unsanctioned apps.</p>
Application Visibility and Control (AVC)	<p>Easily control the use of hundreds of Web 2.0 applications and 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 WSA supports visibility of activity across an entire network. New: Customers can deploy customized bandwidth and time quotas per user, per group, and per policy.</p>
Data Loss Prevention (DLP)	<p>Prevent confidential data from leaving the network by creating context-based rules for basic 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. The Cisco WSA also supports Secure ICAP to encrypt the traffic exchanged between WSA and third-party DLP solutions.</p>

Roaming-User Protection	<p>The Cisco WSA protects roaming users by integrating with the Cisco AnyConnect® Secure Mobility Client, which provides web security to remote clients by initiating a VPN tunnel that redirects traffic back to the on-premises solution. Cisco AnyConnect technology analyzes traffic in real time prior to permitting access.</p> <p>The Cisco WSA is also integrated with Cisco Identity Services Engine (ISE). With this exciting enhancement, customers can now take advantage of the power of Cisco ISE for Cisco WSA upon request. Cisco ISE integration allows admins to create policy on the Cisco WSA based on profile or membership information gathered by Cisco ISE through its single sign-on process.</p>
Centralized Management and Reporting	<p>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.</p> <p>The Cisco M-Series Content Security Management Appliance provides central management and reporting across multiple appliances and multiple locations, including virtual instances.</p> <p>Cisco® Web Security Reporting Application is a reporting solution that rapidly indexes and analyzes logs produced by Cisco Web Security Appliances (WSA) and Cisco Cloud Web Security (CWS). This tool provides scalable reporting for customers with high traffic and storage needs. It allows reporting administrators to gather detailed insight into web usage and malware threats.</p>
Flexible Deployment	<p>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.</p> <p>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.</p>

Product Specifications

Tables 1 and 2 give Cisco WSA performance and hardware specifications, respectively.

Table 1. Cisco WSA Performance Specifications

	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large Enterprise	S690	4.8 TB (8x600 GB SAS)	Yes (RAID 10)	64 GB, DDR4	2 x 2.5 Ghz, 24C
Large Enterprise	S690X	9.6TB (16x600 GB SAS)	Yes (RAID 10)	64 GB, DDR4	2 x 2.5 Ghz, 24C
Large Enterprise	S680	2.4 TB (8x300 GB SAS)	Yes (RAID 10)	32 GB, DDR3	2 x 2.7 Ghz, 16C
Midsized Office	S390	2.4 TB (4x600 GB SAS)	Yes (RAID 10)	32 GB, DDR4	1 x 2.4 Ghz, 8C
Midsized Office	S380	2.4 TB (4x600 GB SAS)	Yes (RAID 10)	16 GB, DDR3	1 x 2.0 Ghz, 6C
SMB and Branch	S190	1.2TB (2x600 GB SAS)	Yes (RAID 1)	8 GB, DDR4	1 x 1.9 Ghz, 6C
SMB and Branch	S170	500 GB (2x500 GB SATA)	Yes (RAID 1)	4 GB, DDR3	1 x 2.8 Ghz, 2C

* 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 WSA Hardware Specifications








	Cisco S690	Cisco S690X	Cisco S680	Cisco S390	Cisco S380	Cisco S190	Cisco S170
Hardware Platform							
Form Factor	2RU	2RU	2RU	1RU	2RU	1RU	1RU
Dimensions	3.4" x 19" x 29"	3.4" x 19" x 29"	3.5" x 19" x 29"	1.7" x 19" x 31"	3.5" x 19" x 29"	1.7" x 19" x 31"	1.64" x 19" x 15.25"
Redundant P/S	Yes	Yes	Yes	Yes	Yes	Yes, Accessory Option	No
Remote Power Cycle	Yes	Yes	Yes	Yes	Yes	No	No
DC Power Option	Yes	Yes	Yes	No	Yes	No	No
Hot-Swappable H/D	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ethernet interfaces	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	2 port 1G Base-T copper network interface (NICs), RJ - 45	2 port 1G Base-T copper network interface (NICs), RJ - 45
Speed (Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate
Fiber Option	Yes, separate SKUs 6 port 1G Base-SX Fiber: WSA- S690-1G 6 port 10G Base-SR Fiber WSA- S690-10G	Yes, separate SKUs 6 port 1G Base-SX Fiber: WSA- S690-1G 6 port 10G Base-SR Fiber WSA- S690-10G	Yes, separate SKUs 6 port 1G Base-SX Fiber: WSA- S680-1G 6 port 10G Base-SR Fiber WSA- S680-10G	No	No	No	No

Table 3 lists specifications of the Cisco WSAV, and Table 4 lists those for the Cisco M-Series Content Security Management Appliance.

Table 3. Cisco WSAV



Web Users				
Web Users	Model	Disk	Memory	Cores
<1000	S000v	250 GB	4 GB	1
1000-2999	S100v	250 GB	6 GB	2
3000-6000	S300v	1024 GB	8 GB	4
Servers		Hypervisor		
Cisco UCS Red Hat Enterprise Linux 7.0 Ubuntu 14.04.1 LTS		ESXi 5.0, 5.1, and 5.5 KVM: QEMU 1.5.3 KVM: QEMU 2.0.0		

Table 4. Cisco M-Series Content Security Management Appliance

Model	Cisco M680	Cisco M380	Cisco M170
Users (approximately)	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 (proxy automatic configuration [PAC] files, Web Proxy Auto-Discovery [WPAD], browser settings) or Transparent mode (Web Cache Communication Protocol [WCCP], Policy-Based Routing [PBR], load balancers). WCCP-compatible devices, such as Cisco Catalyst® 6000 Series Switches, Cisco ASR 1000 Series Aggregation Services Routers, Cisco Integrated Services Routers, and Cisco ASA 5500-X Series Next-Generation Firewalls, reroute web traffic to the Cisco WSA.

The Cisco 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 Antimalware, 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 follow:

Cisco Web Security Essentials

- Threat Intelligence via Cisco Talos
- Layer 4 traffic monitoring
- Application Visibility and Control (AVC)
- Policy management
- Actionable reporting
- URL filtering
- Third-party DLP integration via ICAP

Cisco Anti-Malware

- Real-time malware scanning

Cisco Web Security Premium

- Web Security Essentials
- Real-time malware scanning

Advanced Malware Protection

- AMP augments anti-malware detection and blocking capabilities with file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for continuous analysis of threats.

Cognitive Threat Analytics

- CTA relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

Cloud Access Security

- Cisco with Elastica enables organizations to embrace the benefits of cloud apps while maintaining security policies through SaaS Visibility, Extended Granular Control, and Intelligent Protection.

McAfee Anti-Malware

- McAfee real-time malware scanning is available as a single, a-la-carte license.

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 essential to keeping business-critical applications available, secure, and operating at peak performance. This support entitles customers to the following services 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 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

Table 5 lists Cisco Web Security services.

Table 5. Cisco Web Security 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>Network Device Security Assessment: Helps maintain a hardened network environment by identifying gaps in network infrastructure security.</p> <p>Smart Care: Provides actionable intelligence gained from secure visibility into the performance of a network</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>

SMARTnet Support Services

Customers have the option to purchase Cisco SMARTnet® support for use with Cisco WSAs. Cisco SMARTnet support 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>.

Ordering Cisco WSAV

Do the following to order Cisco WSAV:

1. Go to <http://www.cisco.com/go/wsa>. At right, under “Support”, click “Software Downloads, Release, and General Information”. Click “Download Software”, then click on any model to see the downloadable virtual-machine images available. You will also see a downloadable XML evaluation license. You need to download one of the images and the XML evaluation license.
2. Download the following documentation from Cisco.com:
 - a. Cisco Security Virtual Appliance Installation Guide
 - b. Documentation for AsyncOS® 9.0
3. Follow the instructions in the Cisco Security Virtual Appliance Installation Guide to get started. Please note that content security virtual appliance evaluations are not covered under SMARTnet support and are therefore unsupported.

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 WSA 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)