Cisco Web Security Appliance

In a highly connected and increasingly mobile world with more complex and sophisticated threats, only Cisco delivers the strong protection, complete control, and investment value businesses need. Cisco offers 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.

Overview

The Cisco Web Security Appliance (WSA) is the first 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 enables simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs. "Set and forget" technology frees up staff once initial automated policy settings go live, and 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 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 WSAV is a software version of the WSA that runs on top of a VMware ESXi hypervisor and Cisco UCS® servers. Customers receive an unlimited license for the WSAV with the purchase of any Cisco web security software bundle.

With the 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

Security Intelligence Operations (SIO)	Receive fast and comprehensive web protection backed by the largest threat detection network in the world, with the broadest visibility and largest footprint, including: • 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 Cisco 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.
Cisco Web Usage Controls	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.
Real-Time Malware Defense	Defend against malware and advanced persistent threats using multiple layers of antimalware 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. Administrators can then run multiple antimalware 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. 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.
Application Visibility and Control (AVC)	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.
Data Loss Prevention (DLP)	Prevent confidential data from leaving the network by creating context-based rules for basic DLP. The WSA also uses Internet Content Adaptation Protocol (ICAP) to integrate with third-party DLP solutions for deep content inspection and enforcement of DLP policies.
Cisco AnyConnect® Secure Mobility Client	The 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. AnyConnect analyzes traffic in real time prior to permitting access.
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 Web Security Virtual Appliance (WSAV) offers all the same features as the 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 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 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

Table 1.   Cisco Web Security Appliance Performance Specifications

	Users[*]	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large Enterprise	6000-12000	S680	4.8 TB (8x600 GB SAS)	Yes (RAID 10)	32 GB	16 (2 Octa Core) 2.70 Ghz
		S670	2.7 TB (6x450 GB SAS)	Yes (RAID 10)	8 GB	8 (2 Quad Core) 2.80 GHz
Midsize Office	1500-6000	S380	2.4 TB (4x600 GB SAS)	Yes (RAID 10)	16 GB	6 (1 Hexa Core) 2.00 Ghz
		S370	1.8 TB (4x450 GB SAS)	Yes (RAID 10)	4 GB	4 (1 Quad Core) 2.26 GHz
SMB & Branch	< 1500	S170	500 GB (2x250 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 S670	Cisco S380	Cisco S370	Cisco S170
Hardware Platform					
Form Factor	2U	2U	2U	2U	1U
Dimensions	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.)	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 P/S	Yes	Yes	Yes	Yes	No
Remote Power Cycle	Yes	No	Yes	No	No
DC Power Option	Yes	No	Yes	No	No
Hot-Swappable H/D	Yes	Yes	Yes	Yes	Yes
Fiber Option	Yes (Accessory)	No	No	No	No
Ethernet	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	2 Gigabit NICs, RJ-45
Speed (mbps)	10/100/1000, auto-negotiate	10/100/1000, auto-negotiate	10/100/1000, auto-negotiate	10/100/1000, auto-negotiate	10/100/1000, auto-negotiate

Table 3.   Cisco Web Security Virtual Appliance

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				
Cisco UCS			**ESXi 4.0 X 5.0 Hypervisor**	

Table 4.   Cisco M-Series Content Security Management Appliance

Model	Cisco M1070	Cisco M680	Cisco M670	Cisco M380	Cisco M170
Users (Approx.)	10,000+	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 (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 WSA.

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 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 are provided below:

Cisco Web Security Essentials

- Threat Intelligence via Cisco Security Intelligence Operations (SIO)
- 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

McAfee Anti-Malware

- McAfee real-time malware scanning 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 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 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	Cisco Security Planning & Design: Enables deployment of a robust security solution quickly and cost effectively.
	Cisco Web Security Configuration and Installation: Mitigates web security risks by installing, configuring, and testing appliances to implement:
	• Acceptable-use-policy controls
	• Reputation and malware filtering
	• Data security
	• Application visibility and control
	Cisco Security Optimization Service: Supports an evolving security system to address security threats, design updates, performance tuning, and system changes.
Collaborative/Partner Services	Network Device Security Assessment: Helps maintain a hardened network environment by identifying gaps in network infrastructure security.
	Smart Care: Provides actionable intelligence gained from secure visibility into a network's performance.
	Additional services: Cisco partners provide a wide range of valuable services across the planning, design, implementation, and optimization lifecycle.
Cisco Financing	Cisco Capital® can tailor financing solutions to business needs. Access Cisco technology sooner and see the business benefits sooner.

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.

Ordering WSAV

1. Go to http://www.cisco.com/go/wsa. At right, under "Support," click on "Software Downloads, Release, and General Information." Click on "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 will 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® 7.7.5

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 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 Web Security Appliance will work for you with a Cisco sales representative, channel partner, or systems engineer.

Printed in USA   C78-729630-01   10/13