

Cisco Secure Web Appliance

March 2024

Contents

Virtual Appliance	3
Features and benefits	4
Product specifications	5
Deployment	7
Licensing	7
Services	9
SMARTnet Support services	10
Warranty information	10
Cisco Capital	10
For more information	10
Acknowledgments	11

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: Cisco Secure Web Appliance (formerly 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 Secure Web Appliance deployment options, along with market-leading global threat intelligence. Cisco Secure Web Appliance simplifies security with a high performance, dedicated appliance, and the Secure Web Appliance Virtual Appliance (SWAV) lets businesses deploy Secure Web Appliance quickly and easily, wherever and whenever it's needed.

Secure Web Appliance 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 SWAV significantly lowers the cost of deploying Secure Web Appliance, especially in highly distributed networks, by letting administrators create security instances where and when they are needed. The Cisco SWAV is a software version of the Secure Web Appliance that runs on top of a VMware ESXi, KVM hypervisor, Microsoft Hyper-V and Cisco Unified Computing System™ (Cisco UCS®) servers. You will receive an unlimited license for the Cisco SWAV with the purchase of any of the Cisco Secure Web Appliance software bundles.

Additionally, the purchase of any of the Cisco Secure Web Appliance and/or Cisco Secure Email software bundles also grants entitlement to unlimited licenses for the [Cisco Content Security Management Appliance virtual \(SMAv\)](#).

Note: SMA licenses still need to be purchased separately.

With the Cisco SWAV, 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

Feature	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 Secure Web Appliance every three to five minutes, enabling industry- leading threat defense hours and even days ahead of competitors.</p>
Secure Web Appliance 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 Secure Web Appliance 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 Secure Web Appliance with enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. The 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 Secure Web Appliance solutions. It dynamically adds IP addresses of known malware domains to its list of malicious entities to block.</p>
Cognitive Threat Analytics	<p>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 Cognitive Threat Analytics with a simple add-on license to your Secure Web Appliance solution. Reduce complexity while gaining superior protection that evolves with your changing threat landscape.</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 Secure Web Appliance supports visibility of activity across an entire network. New: Customers can deploy customized bandwidth and time quotas per covered user, per group, and per policy.</p>

Feature	Benefits
Data Loss Prevention (DLP)	Prevent confidential data from leaving the network by creating context-based rules for basic DLP. The Secure Web Appliance also uses Internet Content Adaptation Protocol (ICAP) to integrate with third-party DLP solutions for deep content inspection and enforcement of DLP policies. The Secure Web Appliance also supports Secure ICAP to encrypt the traffic exchanged between Secure Web Appliance and third-party DLP solutions.
Remote Browser Isolation (RBI)	By isolating web traffic from the user device and the threat, the Secure Web Appliance RBI delivers an extra layer of protection to the Secure Web Appliance so that users can safely access risky websites without the risk of malware infections. With RBI, the Secure Web Appliance isolates web content in a remote surrogate browser in the cloud, separate from the endpoint and the corporate network, and renders it safely to the end user providing a seamless end user experience.
Roaming-User Protection	<p>The Secure Web Appliance protects roaming users by integrating with the Cisco AnyConnect Secure Mobility Client, which provides Secure Web Appliance 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 Secure Web Appliance 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 Secure Web Appliance upon request. Cisco ISE integration allows admins to create policy on the Secure Web Appliance 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 Secure Web Appliance 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 Advanced Secure Web Appliance Reporting is a reporting solution that rapidly indexes and analyzes logs produced by Secure Web Appliance and Cisco Umbrella. 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>

Product specifications

Tables 1 and 2 give Secure Web Appliance performance and hardware specifications, respectively.

Table 1. Secure Web Appliance performance specifications

	Model	Disk Space	Raid Mirroring	Memory	CPUs	
Large Enterprise	S696	12 TB (10x1.2TB SAS)	Yes (RAID 10)	128 GB, DDR4	2 x 3.1	Ghz, 16C
Midsize Office	S396	4.8 TB (4x1.2TB SAS)	Yes (RAID 10)	64 GB, DDR4	1 x 2.9	Ghz, 16C
SMB and Branch	S196	2.4 TB (2x1.2TB SAS)	Yes (RAID 1)	16 GB, DDR4	1 x 2.3	Ghz, 10C

Table 2. Secure Web Appliance hardware specifications




Hardware Platform	Cisco S696	Cisco S396	Cisco S196
Form Factor	 2RU	 1RU	 1RU
Dimensions	3.4" x 16.9" x 29.5"	1.7" x 16.89" x 29.8"	1.7" x 16.89" x 29.8"
Redundant P/S	Yes	Yes	Yes, Accessory Option
Remote Power Cycle	Yes	Yes	Yes
DC Power Option	No	No	No
Hot- Swappable H/D	Yes	Yes	Yes
Power Consumption	3,262 BTU/hr 3,412 BTU/hr (Fiber)	2,060 BTU/hr	1,765 BTU/hr
Power Supply	1050W	1050W	1050W
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
Fiber Option	Yes, separate SKU, 6-port 1G Base-SX Fiber or 10GBASE-SR Fiber selectable upon ordering (modules included): SWA-S696F	No	No
HD Size	Ten 1.2 TB hard disk drives (2.5" 12G SAS 10K RPM) are installed into front- panel drive bays that provide hot- swappable access for SAS drives	Four 1.2 TB hard disk drives (2.5" 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot- swappable access for SAS drives	Two 1.2 TB hard disk drives (2.5" 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot- swappable access for SAS drives
CPU	Two 3.1GHz 16c 3200MHz processor	One 2.9GHz 16c 3200MHz processor	One 2.3GHz 10c 2666MHz processor
RAM	Four 32GB DDR4-3200 RDIMM	Two 32GB DDR4-3200 RDIMM	One 16GB DDR4-3200 RDIMM

Table 3 lists specifications of the Cisco SWAV.

Table 3. Cisco SWAV

Model	Disk	Memory	Cores
S100v	250 GB	8 GB	3
S300v	1024 GB	12 GB	5
S600v	2.4 TB	24 GB	12
S1000v	2.4 TB	48 GB	24
Servers		Hypervisor	
Cisco UCS		ESXi 6.5, 6.7, and 7.0	
Red Hat Enterprise Linux 7.0 Ubuntu 14.04.1 LTS		KVM: QEMU 1.5.3	
		KVM: QEMU 2.0.0	
		Microsoft Hyper-V	

Deployment

The Cisco Secure Web Appliance 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 SWA.

The Cisco SWA 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 SWAV license is included in all Secure Web Appliance software bundles (Secure Web Appliance Essentials, Secure Web Appliance Antimalware, and Secure Web Appliance 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 Secure Web Appliance 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.

Secure Web Appliance Software Licenses

Three Secure Web Appliance software licenses are available: Cisco Secure Web Appliance Essentials, Cisco Secure Web Appliance Advantage, and Cisco Secure Web Appliance Premier. The major components of each software offering follow.

Secure Web Appliance 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 ICA

Secure Web Appliance Advantage

- Secure Web Appliance Essentials
- Real-time malware scanning

Secure Web Appliance Premier

- Secure Web Appliance Advantage
- Advanced malware protection
- Cognitive threat analytics
- Threat Grid file analysis

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.

McAfee Anti-Malware

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

Software License Agreements

The Cisco General Terms and the Cisco Secure Web Appliance Supplemental General Terms are provided with each software license purchase.

Software Subscription Support

All Cisco Secure Web Appliance 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 4 lists Cisco Secure Web Appliance services.

Table 4. Cisco Secure Web services

Cisco Branded Services	<p>Cisco Security Planning and Design: Enables deployment of a robust security solution quickly and cost-effectively.</p> <p>Cisco Secure Web Appliance Configuration and Installation: Mitigates Secure Web Appliance risks by installing, configuring, and testing appliances to implement:</p> <ul style="list-style-type: none">• Acceptable-use-policy controls• Data security• Reputation and malware filtering• 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 Secure Web Appliance.

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 <https://www.cisco.com/go/smartnet>.

Ordering Cisco SWAV

Do the following to order Cisco SWAV:

1. Go to <https://www.cisco.com/go/swa>. 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® 14.5
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 support and are therefore unsupported.

Warranty information

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

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. [Learn more](#).

For more information

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

Acknowledgments

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: (<https://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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 <https://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: <https://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)