Cisco Web Security Appliance

BENEFITS

- **Strong protection:** Protect every device through a sophisticated, global threat intelligence infrastructure, which includes Cisco Talos Security Intelligence and Research Group.
- **Complete control:** Provide advanced control of all web traffic, including dynamic web content such as social media applications.
- **Investment Value:** Get more for your security investment and lower your total cost of ownership (TCO) for web security with flexible deployment options, smooth integration with existing security and network infrastructure, and world-class 24-hour support.

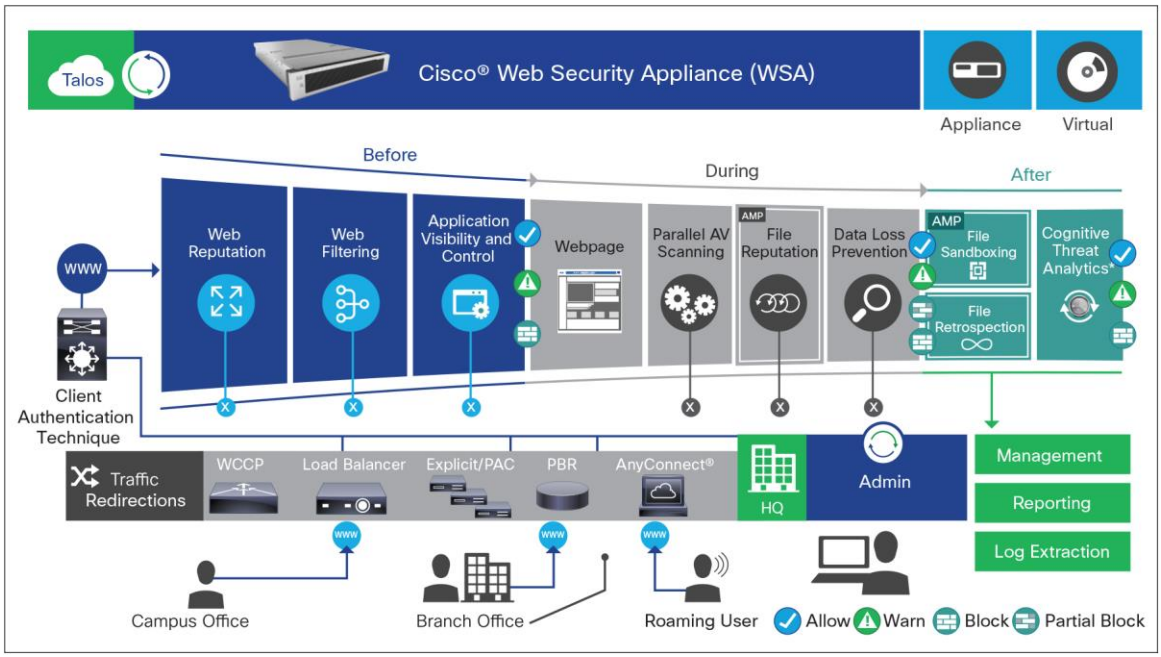
The World Wide Web is insecure. You're likely to contract a virus or download malware through legitimate websites. So here's how to protect your devices and resources accessing social media and Web 2.0 applications in the office and on the go.

To protect against the growing breadth and diversity of threats in today's business climate, you need a modern approach. That means a variety of protections that can block hidden malware from both suspicious and legitimate sites before it reaches you. We think the best Web security solutions today should be backed by the best real-time security intelligence available to help you stay abreast of this changing threat landscape and prevent the latest exploits from turning into issues. And modern Web security should be able to support policies that give employees access to the sites they need to use to do their jobs while selectively denying the use of undesired sites and features like web-based file-sharing.

You get all of those features and more with the Cisco® Web Security Appliance (WSA), Figure 1. Cisco WSA safeguards businesses through broad threat intelligence, multiple layers of malware defense, and vital data loss prevention (DLP) capabilities across the attack continuum. It's an all-in-one web gateway that brings you broad protection, extensive controls, and investment value. It also offers an array of competitive web security deployment options, each of which includes Cisco's market-leading global threat intelligence infrastructure.

Figure 1. Cisco Web Security Appliance

Figure 2. Protection from Cisco Web Security



Before an Attack: Cisco Security Intelligence Operations

Cisco WSA detects and correlates threats in real time by tapping into the largest threat-detection network in the world, Cisco Talos. To discover where threats are hiding, Cisco Talos pulls massive quantities of information across multiple vectors - firewall, IPS, web, email, and VPN. Cisco Talos constantly refreshes information every 3 to 5 minutes - adding intelligence to and receiving intelligence from Cisco WSA and other network security devices. This enables Cisco WSA to deliver industry-leading defense hours and even days ahead of competitors. Then the intelligence of Cisco Talos is combined with resources from the Sourcefire Vulnerability Research Team, which offers additional benefits, including:

- More than 180,000 file samples processed per day
- Access to the Advanced Malware Protection (AMP) community
- Advanced Microsoft and industry disclosures
- Snort® and ClamAV open-source communities
- Honeypots
- Sourcefire Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) program
- Private and public threat feeds
- Dynamic analysis

Web Reputation Filters

Cisco WSA analyzes and categorizes unknown URLs and blocks those falling below a defined security threshold. The instant a web request is made, Web reputation filters analyze more than 200 different web traffic- and network-related parameters to determine the level of risk associated with a site. After checking the domain owner, the server where the site is hosted, the time the site was created, and the type of site, the site is assigned a reputation score. Based on that reputation score and selected security policies, the site is blocked, allowed, or delivered with a warning. Cisco Talos updates Web reputation filtering intelligence every 3 to 5 minutes.

Cisco Web Usage Controls

We combine traditional URL filtering with real-time dynamic content analysis. This can be used to shut down access to sites known to host malware with specific policies for URL filtering, which checks against a list of known websites from Cisco's database of more than 50 million blocked sites. We can accurately identify inappropriate content in real time for 90 percent of unknown URLs using the Dynamic Content Analysis (DCA) engine. The DCA engine scans text, scores the text for relevancy, calculates model document proximity, and returns the closest category match. Cisco Talos updates the URL database with information from multiple vectors: firewall, IPS, web, email and VPN. Talos constantly refreshes information every 3 to 5 minutes - adding intelligence to and receiving intelligence from Cisco WSA and other network security devices.

During an Attack: Real-Time Antimalware Scanning

Cisco WSA enhances malware defense coverage with multiple signature scanning engines run in parallel on a single appliance. It includes the most robust antimalware inspection on the market that optimizes processing speeds and prevents traffic bottlenecks. The Adaptive Scanning feature dynamically selects the most relevant scanner based on URL reputation, content type, and scanner efficacy and improves the catch rate by scanning high-risk objects first during increased scan loads. You receive information on the latest coverage with automated updates.

Layer 4 Traffic Monitor

Cisco WSA scans all traffic, ports, and protocols to detect and block spyware "phone-home" communications with the integrated Layer 4 traffic monitor. Based on this scanning, it identifies infected clients to help stop malware that attempts to bypass classic web security solutions. In addition, the Layer 4 traffic monitor is able to dynamically add IP addresses of known malware domains to its list of malicious entities to block. Using this dynamic discovery capability, the Layer 4 traffic monitor can monitor the movement of malware in real time.

Third-Party DLP Integration with Internet Control Adaptation Protocol

For richer DLP functionality, Cisco WSA uses Internet Control Adaptation Protocol (ICAP) to integrate with DLP solutions from leading vendors. By directing all outbound traffic to the third-party DLP appliance, content is allowed or blocked based on the third-party rules and policies. Deep content inspection is also available for regulatory compliance and intellectual property protection. Powerful engines inspect outbound traffic, analyze it for content markers, such as confidential files, credit card numbers, customer data, etc., and prevent this data from being uploaded to the web.

Cloud Access Security

Cisco can protect you from the hidden threats lurking in cloud apps. We have partnered with leading Cloud Access Security Broker (CASB) providers to deliver new visibility by monitoring your cloud app usage in real time. We extend your control in a cloud-first, mobile-first world, and help combat evolving threats through intelligent protection powered by data science. Ecosystem partners such as Elastica integrate seamlessly with your existing security architecture to extend on-premises protection into the cloud.

Cloud Access Security solutions provide full visibility of your cloud app environment; letting you classify all cloud traffic passing through the gateway to detect intrusions and data leakage; and automatically enforcing any new global security policies across all sanctioned and unsanctioned apps.

File Reputation and Analysis with Cisco AMP

With WSA, you can assess files using the latest threat information from Cisco Talos, which is updated every 3 to 5 minutes. Cisco WSA captures a fingerprint of each file as it traverses the gateway and sends it to Cisco's cloud-based threat intelligence network for a reputation verdict checked against zero-day exploits. You can also Identify malware and breaches as they affect your system. When malware is detected, AMP gleans precise details about a file's behavior and combines that data with detailed human and machine analysis to determine the file's threat level in a sandbox.

After an Attack: File Retrospection

Cisco WSA inspects the network continuously for instances of undetected malware and breaches. After an initial detection, Cisco WSA continues to interrogate files over an extended period of time with the latest detection capabilities and collective threat intelligence, allowing for the rendering of an updated disposition and further analysis.

Cognitive Threat Analytics

With Cisco WSA, you reduce time to discovery to stop the spread of attacks with behavioral-driven threat detection. Cisco WSA spots symptoms of infection using behavioral anomaly detection algorithms and trust modeling. An add-on license, Cisco Cognitive Threat Analytics (CTA) uses machine learning to adapt over time. No rule sets are required; CTA discovers threats on its own.

Use Case: Acceptable Use

Combine application visibility and control (AVC), acceptable-use policy controls, insightful reporting and secure mobility on a single appliance with Cisco WSA. You can control global security infrastructure from a single interface consistently across on-premises and mobile environments. With Cisco WSA, you can also enforce policy and provide precise control over application and usage behavior using context-aware inspection. Protect data with built-in Cisco WSA features or advanced DLP through integration with leading vendors.

Policy Management

Centralized Management and Reporting

You can control security and network operations from a simple-to-use, centralized tool built into the Cisco WSA appliance. Insightful and actionable reporting simplifies analysis, speeds troubleshooting, and identifies potential security policy refinements. Alternatively, manage multiple locations and appliances, including virtual instances, with central management and reporting through the M-Series Content Cisco Security Management Appliance (SMA).

Cisco AVC

For deep visibility into evolving application content, Cisco AVC provides the most precise control over application and usage behavior, identifying and classifying hundreds of the most relevant and widely used Web 2.0 and mobile applications such as Facebook and more than 150,000 microapplications such as Facebook games. Permit applications such as Facebook or Dropbox but block users from activities such as clicking the Like button or uploading documents. For personal webmail use, block all use, allow users to read and send but not upload documents, or decrypt transactions and send them to a third-party DLP solution.

Cisco Identity Services Engine

The integration of Cisco WSA with Cisco Identity Services Engine (ISE) allows the WSA to supplement web security policy attributes with identity and network context information, enabling a better user experience through better visibility and more granular control over user access to specific web sites. Customers that deploy the two solutions provide a better end user content delivery experience by utilizing Cisco ISE device-type and network-access contextual information to understand how, when, and from what devices users access web resources. You can improve web access policy based on the user role or user device and gain better control over granting user access to approved or sensitive content. Create device-specific web access policies that allow or deny access to web-based content with an understanding of the whether the endpoint is compliant with IT usage policies.

> "The [Cisco] WSAs blocked 1 percent of all web transactions, or 30 million, in just the first three months. These could have been commands to or from botnets, retrieval or leaking of user passwords and other personal information, and malware downloads."
>
> **— Jeff Bollinger, Senior Information Security Investigator, Cisco IT**

Compliance

Cisco Web Usage Controls

Using Cisco WSA, you mitigate risks related to compliance, liability, and productivity with traditional URL-filtering and real-time DCA. You get exceptional coverage for known websites with Cisco's URL-filtering database containing more than 50 million blocked sites. Identify 90 percent of unknown URLs in real time. The DCA engine scans text, scores the text for relevance, calculates model document proximity and returns the closest category match. Cisco Talos updates the URL database with information from multiple vectors - firewall, IPS, web, email and VPN. Cisco Talos constantly refreshes information every 3 to 5 minutes - adding intelligence to and receiving intelligence from WSA and other network security devices. Administrators can also select specific categories for intelligent HTTPS inspection.

Data Loss Protection

With Cisco WSA, you can allow or block content to meet business requirements for regulatory compliance and intellectual property protection. Prevent confidential data from leaving the network by creating context-based rules for basic DLP or easily integrating through ICAP into any third-party DLP solution for deep content inspection and enforcement of DLP policies. Protect data with onboard DLP capabilities by scanning uploaded content by title, metadata, and size and preventing uploading to webmail and file-share services in the cloud (such as Dropbox). Build custom policies according to the desired degree of restriction. For example, choose to block all use of personal webmail or allow users to read and send personal webmail without the ability to upload documents or decrypt transactions and send them to a third-party DLP solution for analysis.

Remote Device Management

Cisco AnyConnect Secure Mobility Client

Extend always-on web security protection to mobile users with the Cisco AnyConnect Secure Mobility Client. When users leave the corporate network, Cisco AnyConnect automatically detects that the user is roaming and redirects traffic back to Cisco WSA on the corporate network. The Cisco AnyConnect client requires traffic redirection through a VPN tunnel back to the on-premises router or firewall and on to the Cisco WSA for analysis. Cisco WSA then applies all web security features.

Cisco Services

Cisco Branded Services

- **Cisco SMARTnet™ Service for Web Security Appliance** helps you resolve network problems quickly with direct anytime access to Cisco experts, self-help support tools, and rapid hardware replacement.
- **Cisco Security Planning and Design** helps you assess which Cisco WSA model is appropriate for your needs. Deploy a robust security solution quickly, easily, and cost-effectively with this service.
- **Cisco Web Security Configuration and Installation** helps you mitigate web security risks through installation, configuration, and proper testing of your security solution.
- **Cisco Optimization Service for Security** is for customers that may already have a web appliance and want to optimize or enhance it with features such as those in AMP. It helps you proactively evaluate and strengthen your networks, helping you to better respond to evolving security threats and unexpected incidents.

Cisco Financing

Cisco Capital® can tailor financing solutions to your customers' business needs. That means they can access Cisco technology sooner and see the business benefits sooner.

Market Leadership

- Gartner positioned Cisco Web Security as a challenger in its 2015 Magic Quadrant for Secure Web Gateways
- Cisco is the market share leader in the overall security appliance market, according to IDC (June 2015)
- Gartner also positioned Cisco as a leader in the 2015 Gartner Magic Quadrants for Network Access Control and for Email Security

Why Cisco?

With Cisco you get broad threat coverage through Talos, zero-day, advanced threat protection, and multiple antimalware engines all on one device. Centralized management and reporting offers deep visibility. Flexible deployment options let you take advantage of physical or virtualized resources. Our 24-hour worldwide award-winning support means there is always a Cisco specialist available to help resolve questions or issues quickly. And Cisco WSA integrates with other Cisco products such as ISE and AMP, extending the value of investments and delivering security without affecting network performance. Finally, Cisco's "set and forget technology" greatly lessens the time required for an administrator once configuration is set and initial policy settings go live.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps

Find out more about Cisco WSA at http://www.cisco.com/go/wsa.

A Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco WSA with AMP and other Cisco security products will best meet your pressing security needs and requirements.

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.

Printed in USA C22-732948-02 01/16