Cisco Web Security Appliance (WSA)

Web Security Challenges

Today's interactive web technologies enable innovative ways to market products, reach customers and suppliers, and reduce costs. Unfortunately, many of these technologies contain security threats that can expose companies to significant business risks.

Cisco Web Security Appliance

The Cisco® Web Security Appliance (WSA) combines advanced malware protection, application visibility and control, acceptable use policies, insightful reporting, and secure mobility on a single platform, helping to address the growing challenges of securing and controlling web traffic.

This all-in-one solution results in simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs.

Strong Protection

Safeguards every device, everywhere, all the time

Cisco Security Intelligence Operations (SIO) provides zero-day threat protection to all users, regardless of location. SIO integrates with Cisco's family of network security offerings, enabling the WSA to deliver continuous real-time threat protection.

Cisco Security Intelligence Operations

The broadest worldwide threat telemetry network

Cisco SIO receives automatic updates every three to five minutes and provides a 24x7 view into global traffic activity, enabling Cisco to analyze anomalies, uncover new threats, and monitor traffic trends.

Cisco SIO delivers the industry's largest collection of real-time threat intelligence, including:

- 100 TB of security intelligence daily
- 1.6 million deployed security devices, including firewall, IPS, web, and email appliances
- 13 billion daily web requests
- 150 million endpoints
- 35 % of worldwide email traffic

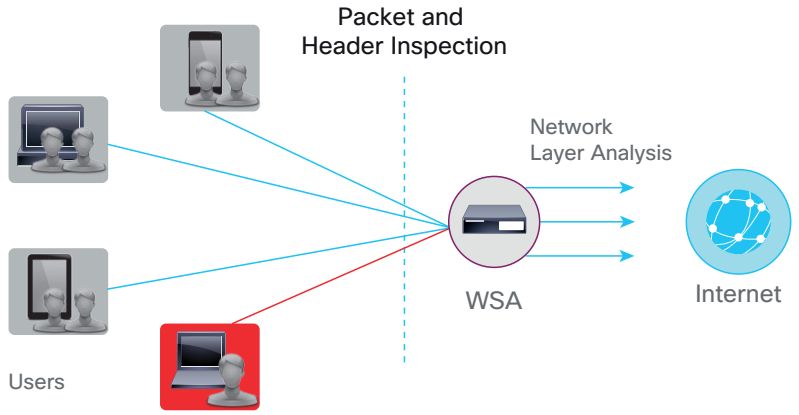
Real-Time Malware Defense

Multilayer scanning and Layer 4 Traffic Monitoring

The Cisco WSA offers multiple layers of antimalware protection. Cisco Web Reputation Filters analyze web traffic and block URLs that fall short of an acceptable threshold. Adaptive Scanning then 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.

Figure 1. On-Premises Layer 4 Traffic Monitor



Preventing "Phone-home" Traffic

- Scans all traffic, all ports, all protocols
- Detects malware bypassing port 80
- Preventing botnet traffic

Preventing Anti-malware Data

- Automatically updated rules
- Generates rules in real time using "dynamic discovery"

Complete Control

Enables control of all web traffic on all devices

Enforce policy and provide granular control over application and user behavior using context-aware inspection from a single, easy-to-use management interface.

Cisco Web Usage Controls

Includes URL filtering and Dynamic Content Analysis (DCA)

Combine traditional URL filtering with a dynamically updated URL database to defend against compliance, liability, and productivity risks. The proprietary Cisco Dynamic Content Analysis engine analyzes page content on unknown URLs to categorize them in real time. Categorizations are dynamically updated every three to five minutes from Cisco SIO.

Application Visibility and Control (AVC)

Ensures acceptable use and security policy enforcement

Easily set policy and control usage 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 Facebook or Dropbox while blocking users from activities such as uploading documents or clicking the “Like” button.

Cisco AnyConnect® Secure Mobility Client

Extends protection to roaming users

Safeguard data requested by roaming laptop devices. AnyConnect dynamically initiates a VPN that directs sensitive traffic to the primary web access point for real-time analysis prior to permitting access.

Data Loss Prevention (DLP)

Prevents leaks and data loss

Prevent confidential data from leaving your network by creating context-based rules for basic DLP. The WSA uses Internet Content Adaptation Protocol (ICAP) to integrate with third-party DLP solutions for advanced protection.

Investment Value

Delivers more for your investment

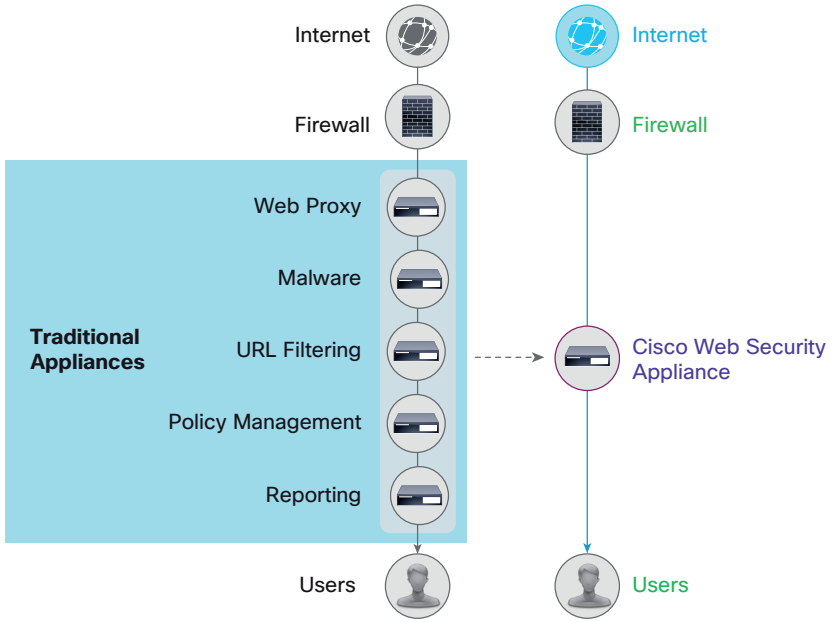
Get the benefits of several web security solutions on a single appliance. While other solutions require complex multidevice deployments, the Cisco WSA operates as a standalone solution, deployed alone or integrated with existing infrastructure. Multiple WSAs can be controlled using the Cisco S-Series Management Appliance (SMA).

All-in-One Solution

Simplifies deployment

Simplify web security deployment by aggregating several web security features in a single appliance. With its simplified architecture, the WSA reduces IT costs by having fewer devices to manage, support, and maintain.

Figure 2. All-in-One Solution



Learn More

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

Evaluate how Cisco products will work for you with a Cisco sales representative, channel partner, or systems engineer.

C45-716641-01 09/13