Cisco Web Security Appliance

Powerful, All-in-One Network Security

To combat advanced web security threats, you need strong protection and consistent control across all endpoints and everywhere in between. That includes mobile devices, web-enabled and mobile applications, and web browsers. You need the Cisco® Web Security Appliance. With it, you can address the challenges of securing and controlling web traffic easily and quickly.

The Web Security Appliance combines Advanced Malware Protection (AMP), Cognitive Threat Analytics (CTA), Application Visibility and Control (AVC), acceptable-use policies, insightful reporting, and highly secure mobility (Figure 1). It's all available on a single easy-to-manage platform.

As a physical appliance, the Web Security Appliance has few maintenance requirements, for low operational costs along with reduced latency. For highly distributed networks, the Cisco Web Security Virtual Appliance lets you deploy the same stringent web security when and where it's needed in a virtual version.

Benefits

- **Get advanced threat detection** through integration with Cisco Advanced Malware Protection, Cisco Cognitive Threat Analytics, and cloud access security products.
- **Easily deploy the solution** with fast, flexible options and automatic updates.
- **Enhance security with highly detailed web-access control** with the industry-leading Cisco Identity Services Engine.
- **Reduce costs** with easy integration into your existing security infrastructure.
- **Get an all-in-one solution** with web security and proxy capabilities supported within a single box.

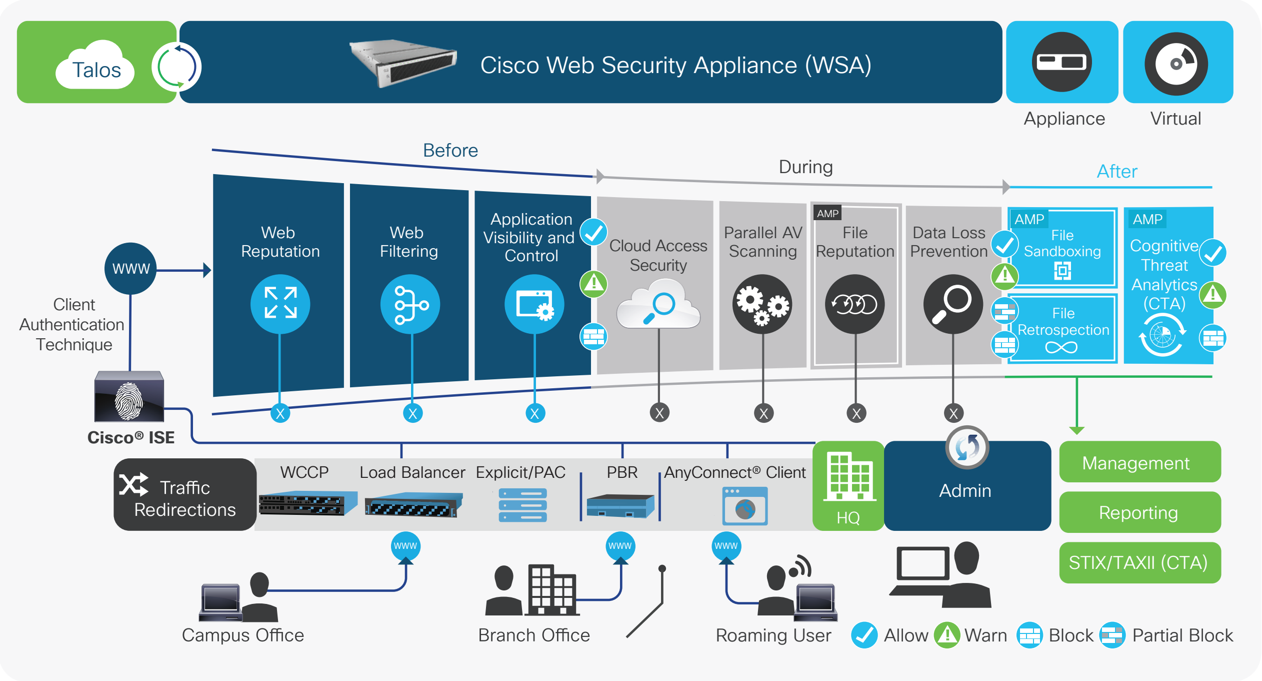
Application Visibility and Control

With the Web Security Appliance, you can enforce policy and provide precise control over application and user behavior using context-aware inspection from a single easy-to-use management interface. You can easily set policies to control the use of hundreds of applications and more than 150,000 microapplications. You can permit the use of applications such as Facebook or Dropbox while blocking users from activities such as chatting or uploading documents. You can also deploy customized bandwidth and time quotas per user, group, and policy. Integration with cloud access security addresses “shadow IT” (IT systems and solutions built and used inside organizations without explicit organizational approval) by controlling user access to cloud applications.

Web-Usage Controls

The Web Security Appliance lets you combine traditional URL filtering with a dynamically updated URL database to reduce compliance, liability, and productivity risks. The Cisco Dynamic Content Analysis engine evaluates page content on unknown URLs to categorize them in real time. Categorizations are dynamically updated every 3 to 5 minutes from the Cisco Talos Security Intelligence and Research Group. Talos is staffed by leading threat researchers who tap into sophisticated systems that analyze threats, malware, and intrusions from around the world.

Figure 1. Threat-Centric Security Before, During, and After an Attack



Protect Roaming Users

The Web Security Appliance protects the data requested by roaming laptops. Before granting access to the network, it initiates a VPN that directs sensitive traffic to the primary web access point for real-time analysis. And by integrating the appliance with the Cisco Identity Services Engine (ISE), administrators can create policies on the appliance based on user profile or membership information gathered by engine. You gain a new level of user control and reporting. You also provide a much better user experience in bring-your-own-device (BYOD) environments through streamlined capabilities such as integrated single sign-on.

Data Loss Prevention

You can prevent confidential data from leaving your network by creating context-based rules for basic data loss prevention (DLP). The Web Security Appliance uses the Internet Content Adaptation Protocol (ICAP) to integrate with third-party DLP solutions for advanced protection.

Additional features and benefits of the physical and virtual appliances are shown in Table 1.

Table 1. Features and Benefits

Feature	Benefit
Talos	Get early-warning insights and vulnerability analysis with the industry's largest collection of real-time threat intelligence: 100 terabytes of security data processed daily from 13 billion web requests, 150 million endpoints, and 1.6 million deployed security devices. Talos sends automatic updates every 3 to 5 minutes, giving you continuous real-time threat protection.
Web reputation filters	Together with threat intelligence from Talos, web reputation filters defend against zero-day web malware through dynamic reputation analysis. The feature selects the most relevant scanner in real time—based on URL reputation, content type, and the efficacy of the scanner—and improves the catch rate by scanning high-risk objects first during higher scan loads.
Advanced Malware Protection (AMP)	AMP is an additionally licensed feature available to all Web Security Appliance customers. It builds on the malware detection and blocking capabilities already offered in the appliance. You get enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. AMP now supports the AMP Threat Grid appliance, which delivers malware protection through an on-premises appliance for organizations that have compliance or policy restrictions on submitting malware samples to the cloud.
Cognitive Threat Analytics (CTA)	Turn your web proxy into a security sensor with cloud-based breach detection and analytics. Cisco Cognitive Threat Analytics (CTA) is a cloud-based solution that reduces the 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 (CTA), which is now part of the AMP add-on license to your Cisco Web Security Appliance. Reduce complexity while gaining superior protection that evolves with your changing threat landscape. For more detailed information on Cisco Cognitive Threat Analytics (CTA), go to www.cisco.com/go/cognitive.

Next steps

Learn more about the Cisco Web Security Appliance at https://www.cisco.com/go/wsa.

A Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco products will work for you.

Feature	Benefit
Command-and-control traffic monitoring	The Layer 4 traffic monitor continuously scans activity to detect and block spyware “phone home” communications. By tracking all network applications, the feature effectively stops malware that attempts to bypass classic web security solutions. It also dynamically updates its list of malicious entities with the IP addresses of known malware domains.
Simplified deployment	The Web Security Appliances (physical and virtual) are all-in-one solutions that simplify deployment by aggregating several web security features in a single appliance. With their simplified architecture, they reduce IT costs because you have fewer devices to manage, support, and maintain.