White Paper

# Cisco ASA and Cloud Web Security: Best-in-Class Network Security Combined with Best-in-Class Web Security

## Introduction

Organizations that want to harness the power of the web must deal with a consequence: becoming vulnerable to web-based threats that can negatively impact data, reputation, and operations. Trends such as social networking and Bring Your Own Device (BYOD) add to the challenge of securing the safety of network traffic and increase the attack footprint. Many current "all-in-one" appliance solutions do not offer the predictable performance and solution flexibility that today's enterprises demand.

Cisco® ASA Software Release 9.0, integrated with Cisco Cloud Web Security (formerly ScanSafe), and powered by Cisco Security Intelligence Operations (SIO), solves the combined problems of performance and breadth of security—without affecting network complexity or business agility. Web security is managed in the cloud and tightly integrated with the network, placing no additional load on existing systems.

This white paper explains how Cisco uses the advantages of the cloud to protect enterprises from web-based threats and to apply comprehensive policies to web content and web-application visibility within the enterprise.

## Managing Threats in a Web-Centric World

The ever-growing sophistication of malware creators—including their skill at evading detection—puts unprecedented pressure on organizations to protect their information and their employees from web-based threats.

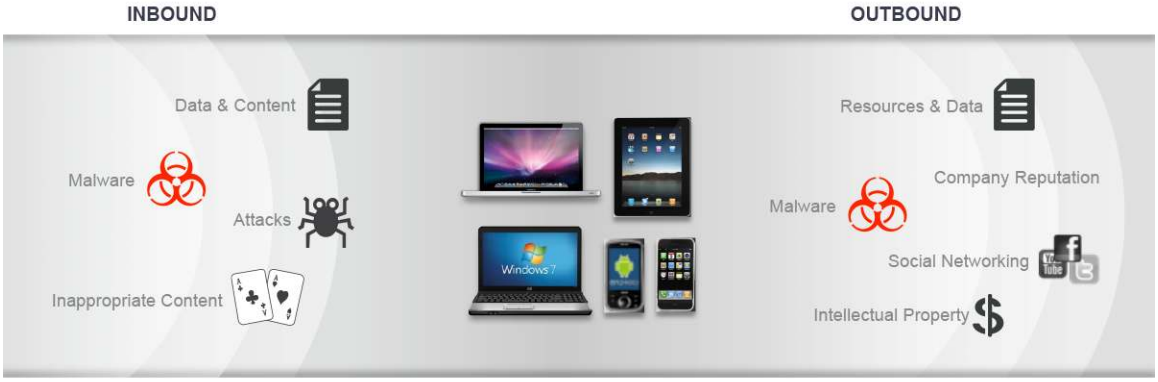
Adding to this pressure is workers' reliance on the web to do their jobs and grow the business, no matter where they're working or what devices they're using. Businesses fear the impact of poor threat protection and of unmonitored and unregulated web access.

Web trends such as the growth of social media and user-generated content increase these risks. For malware creators, social networks and their users offer rich opportunities to launch threats, particularly those that involve social engineering and exploiting the trust of a target. Because these threats are triggered by the actions of unsuspecting web users, they are not as easily blocked at the points at which traffic enters the network.

The BYOD revolution has further complicated the task of securing an organization against threats. Workers access the web from desktop computers in their offices, from laptops in airports, and from smartphones and tablets at home and on the road, which requires security professionals to secure traffic that is beyond their network perimeter.

These challenges add up to demands on security professionals to manage the varied pressures on their data centers. They need to protect and manage web traffic to and from users and their devices; they need to maintain high levels of performance and data availability; they need to migrate enterprise applications and online business activity to the web; and they need to invest in cost-effective, long-term solutions for web security.

**Figure 1.** The World of Web-Based Threats




## Limitations of "All-in-One" Solutions

Security vendors have typically offered "all-in-one" appliances that are limited in their capabilities and pose performance problems. For instance, all-in-one systems generally suffer in performance in situations where web traffic increases and demand for scanning is high. In addition, the all-in-one approach to web security is often limited in terms of its depth—for example, usually only one antivirus solution is available in these appliances.

Besides these limitations in the breadth and depth of solution choices, organizations taking an all-in-one approach are often advised to reduce the maximum allowed file size for scanning. Unfortunately, this means that if a compromised file is over a certain size, most of these all-in-one appliances will allow those files to pass through.

The other key disadvantage of all-in-one appliances is that as soon as an organization enables the breadth of services available—including features such as antivirus and URL filtering—the performance of the appliance drops significantly, as much as 95 percent of rated performance. All security features compete for fixed computing resources. The unpredictability of these solutions' performance levels can cause problems for an organization. For example, this unpredictability can force businesses to constantly revisit capacity planning goals and increase investments in security products.

Because of these caveats, customers are forced to choose between security and performance. In some cases customers are forced to disable these services to get around the performance limitations.

In addition to searching for appliances that can manage their traffic, monitoring, and performance demands, organizations need to aggressively enforce web security policies for their branch offices, remote locations, and remote users. There are ways this challenge can be addressed, although both have disadvantages:

- Backhaul web traffic to headquarters from branch offices
- Deploy dedicated web security solutions for each branch office

Backhauling web traffic to headquarters is an inefficient process that can cause application latency and increase bandwidth costs. Deploying web security solutions at each branch is not only costly, but also highly dependent on the availability of skilled security administrators in each location.

Given these disadvantages, following are the requirements for an ideal web security solution for a decentralized network:

- Provide localized network security while maintaining centralized web security

- Provide web security, including content scanning, with no loss of performance and without placing too much load on existing systems
- Apply granular policies and filtering on a centralized basis

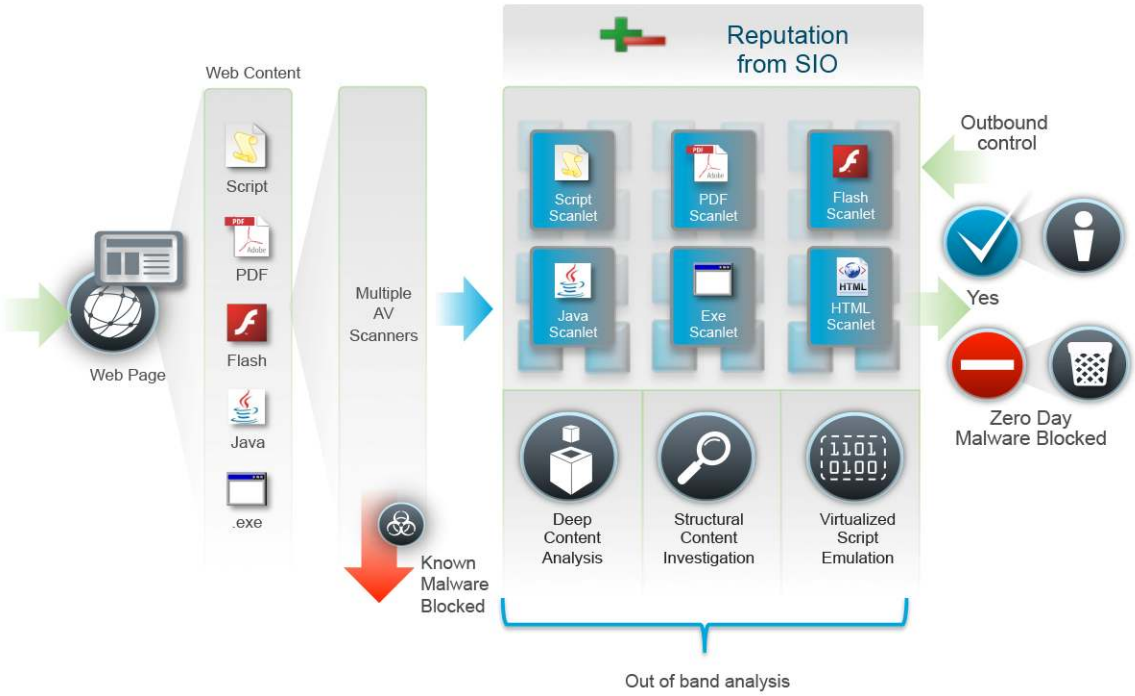
## The Solution: Cisco ASA Software Release 9.0, Integrated with Cisco Cloud Web Security

Cisco ASA Software Release 9.0 includes integration with Cisco Cloud Web Security (formerly ScanSafe), which provides a centralized content security solution combined with localized network security. Since all content scanning is offloaded to Cisco's cloud, there is little to no impact on the performance of ASA devices.

Administrators can choose to perform deep content scanning on a subset of traffic, based on network address, Microsoft Active Directory user or group name, or hosts residing inside a specific security context. The cloud infrastructure is built on high-availability and high-performance data centers spread throughout the globe. This infrastructure has a proven track record for availability and provides visibility and security without the need for on-premise devices.

Unlike all-in-one approaches to security that compete for computing resources, Cisco Cloud Web Security executes antivirus and web security on the scalable Cisco cloud and executes network security on the Cisco ASA. As a result, both services achieve maximum security efficacy with little or no performance impact.

**Figure 2.** Offloading Content Scanning to the Cloud




With Cisco ASA Software Release 9.0, Internet traffic is redirected to the Cisco Cloud Web Security service, where it is scanned for malware and user-based policy is enforced. The outbound traffic can be classified based on user name, user group, source, or destination. The destination aspect can be further classified into three broad categories:

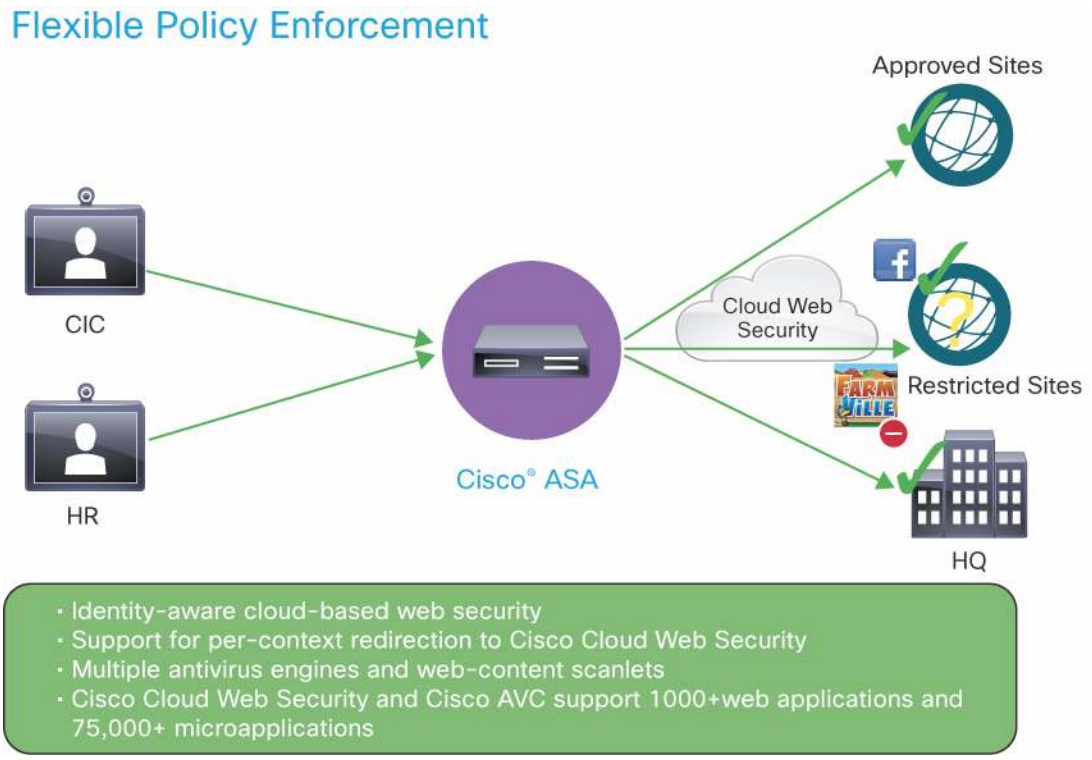
- **Approved traffic:** Traffic from known, safe websites that is automatically approved by corporate policy
- **VPN traffic:** Traffic flowing through a site-to-site VPN tunnel
- **Traffic redirected to Cisco Cloud Web Security:** Traffic sent to Cisco Cloud Web Security for granular web policy control, including URL filtering, antivirus scanning, web content scanning, and web application visibility and control

This process optimizes traffic for internal networks and for branch offices, and applies security and policy enforcement for all users, regardless of their location.

Cisco Cloud Web Security capabilities are extended to remote users via the Cisco AnyConnect® Secure Mobility Client, which performs split-tunneling of web and VPN traffic. This eliminates the need to backhaul Internet traffic to company headquarters, thereby enabling complex remote access use cases.

For example, if a user is traveling from the United States to Japan, AnyConnect will automatically find the closest Cisco Cloud Web Security tower in Japan, even if the VPN tunnel is terminated to the U.S. headquarters location.

**Figure 3.** Flexibility in Applying Acceptable Use Policies




Cisco Cloud Web Security uses industry-leading Cisco SIO threat defense technology to provide proven, zero-day threat protection to all users wherever they are. Cisco SIO uses the largest threat detection network in the world:

- Over 75 TB of web data per day
- More than 1.6 million deployed devices
- More than 150 million endpoints
- More than 13 billion web requests per day

- Over 35 percent of the world's email traffic

## Cisco ASA and Cisco Cloud Web Security: Benefits

The integration of Cisco ASA Software Release 9.0 with Cisco Cloud Web Security helps to create the following benefits for organizations:

- **Lower cost of ownership:** The integrated firewall and cloud solution helps avoid costs associated with deployment and maintenance of on-premise software and hardware.
- **Industry-leading security with no impact on firewall performance:** Real-time cloud-based scanning blocks malware and inappropriate content before it reaches the network.
- **Scalability and availability:** Cisco's global network processes high volumes of web content at high speeds, everywhere, for a true global solution that is always available.
- **Integration with other Cisco security products:** The Cloud Web Security Solution integrates with Cisco ISR branch office routers and Cisco AnyConnect to offer a web security solution, enabling flexible deployments.
- **Consistent, unified policy:** Acceptable use policies can be applied to all users regardless of location, simplifying management.
- **Predictable operational expenses:** Clients can plan capacity and budget.

## Sizing Guide for Cisco Cloud Web Security with the ASA 5500 Series Adaptive Security Appliances

Small Office and Branch Office

| ASA Platform | 5505 | 5510 | 5512-X | 5515-X |
|---|---|---|---|---|
| |  |  |  |  |
| Maximum CWS Users | 25 | 75 | 100 | 250 |

Internet Edge

| ASA Platform | 5520 | 5525-X | 5540 | 5545-X | 5550 | 5555-X |
|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |
| Maximum CWS Users | 300 | 500 | 1,000 | 1,500 | 2,000 | 3,000 |

Enterprise Data Center

| ASA Platform | 5585-X SSP10 | 5585-X SSP20 | 5585-X SSP40 | 5585-X SSP60 |
|---|---|---|---|---|
| |  |  |  |  |
| Maximum CWS Users | 7,500 | 7,500 | 7,500 | 7,500 |

**Note on sizing:**

a. Sizing for Cloud Web Security (CWS) is based on named users. This isn't concurrent users but total number of users who may browse the internet

b. Tests used HTTP traffic with 32K object size—every single HTTP GET was answered by an object 32K in size

c. Peak bandwidth per seat is 20 Kbps (measured on a 95th percentile basis)

d. Traffic profile: HTTP—88% and HTTPS—12%

e. Tests were run with authentication using IDFW and the test setup designed such that every GET request would make the ASA apply a header to each request

f. Actual internet traffic profile may vary based on usage, but Cisco strongly recommends that customers adhere to the sizing guidelines above

## For More Information

- http://www.cisco.com/go/websecurity

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 C11-715169-01 10/12