Cisco Cloud Web Security

Cisco IT Methods

Introduction

Malicious scripts, or malware, are executable code added to webpages that execute when the user visits the site. Many of these seemingly harmless websites lead to unnoticed computer infection, pop-up advertisements, a blocked browser, redirection to other sites, or other potentially harmful or unwanted activities. Many more complex and targeted attacks leverage malware to gain access to user devices.

Remediating the disruptions caused by malware infections creates significant workloads and costs for IT. For example, in a nine-month period from late 2012 to early 2013, malware infections generated more than 200 cases for virus remediation and more than 2700 help desk cases, for a total cost of more than US$4 million to Cisco IT. These factors are why defense against malware has become an integral part of Cisco IT's security strategy.

Malware can enter the Cisco network when an infected user PC connects over a direct link in the office or a VPN link from a remote location. For these connections, Cisco IT uses the Cisco® Web Security Appliance (WSA) to protect the network from malware intrusion.

However, WSA protection is not available when a user connects to the Internet directly, without connecting via the Cisco network, such as when using a public Wi-Fi service in a coffee shop. In this case, the user's PC can become infected with malware, which may disrupt the user's activity, spread to other networks and devices, and present the risk of a data security or privacy breach. Cisco IT uses the Cisco Cloud Web Security (CWS) solution to help protect user PCs from these malware infections.

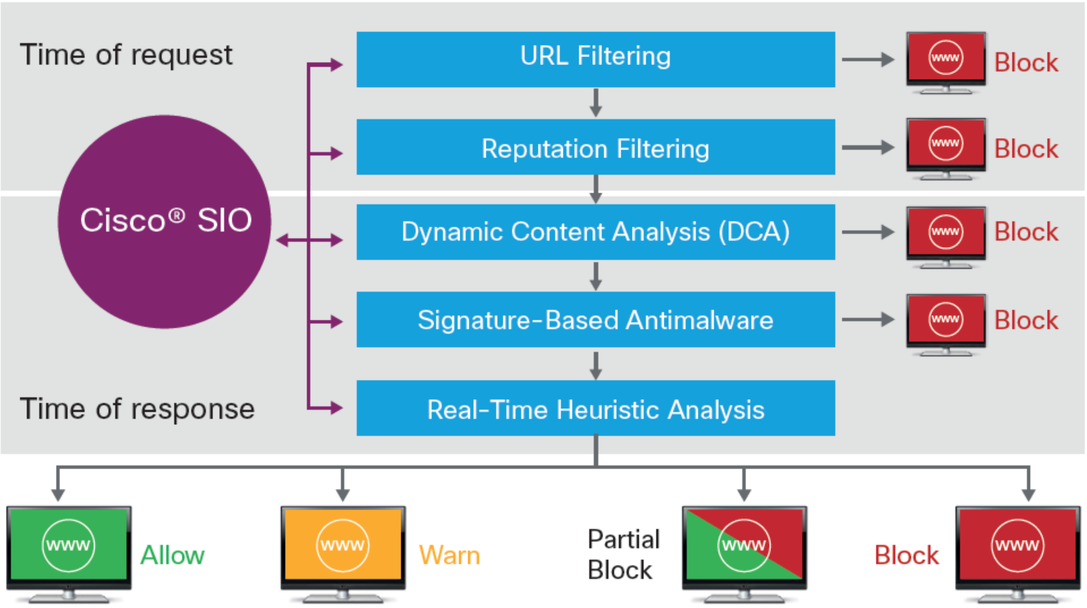
Together, Cisco WSA and Cisco CWS give Cisco IT a comprehensive way to reduce malware and the associated impacts in the Cisco network. More specifically, Cisco IT's deployment of Cisco CWS delivers advantages that address several business challenges:

- **Reducing the number of malware infections:** The strong protection of user devices offered by Cisco CWS means fewer malware infections enter the Cisco network. This protection reduces the potential for data theft, productivity loss, as well as the direct costs of IT resources needed to remediate these infections.
- **Management overhead:** Cisco CWS helps Cisco IT avoid the costly overhead of managing malware infections in a decentralized mode, especially as Cisco IT supports more remote and mobile workers.
- **Consistent policy enforcement:** Because Cisco CWS supports complete control of web traffic on user devices, Cisco IT gains better visibility and reporting of off-premises infections through consistent policies about user access to risky websites.
- **Network complexity:** The flexible options for Cisco CWS deployment helps Cisco IT cost-effectively serve the security demands of its complex global network.

Solution

The Cisco CWS solution, previously known as Cisco ScanSafe, enforces secure communication to and from the Internet. It uses the Cisco AnyConnect® Secure Mobility Client 3.0 to provide remote workers the same level of security as onsite employees when using a laptop issued by Cisco. Cisco CWS incorporates two main functions, web filtering and web security, and both are accompanied by extensive, centralized reporting. Figure 1 provides a conceptual view of the Cisco CWS solution.

Figure 1. Cisco Cloud Web Security Key Functionality [NOTE: Place caption above figure.]



The web-filtering service in Cisco CWS creates, enforces, and monitors web usage policies by applying real-time, rule-based filters and checking an up-to-date and accurate database for categorizing websites. By enforcing an organization's acceptable usage policy and reducing the volume of inappropriate content, Cisco CWS helps avoid potential legal liabilities, reduces bandwidth congestion, and improves employee productivity.

When a user enters a URL in a web browser, that request is routed to the nearest Cisco CWS data center where the Cisco Security Intelligence Operations (SIO) service applies correlated detection technologies, automated machine-learning heuristics, and multiple scanning engines to detect and block known and unknown malware on websites. Cisco CWS operates independently from the user device; all control over URL access and malware detection is carried out in the cloud.

Deployment

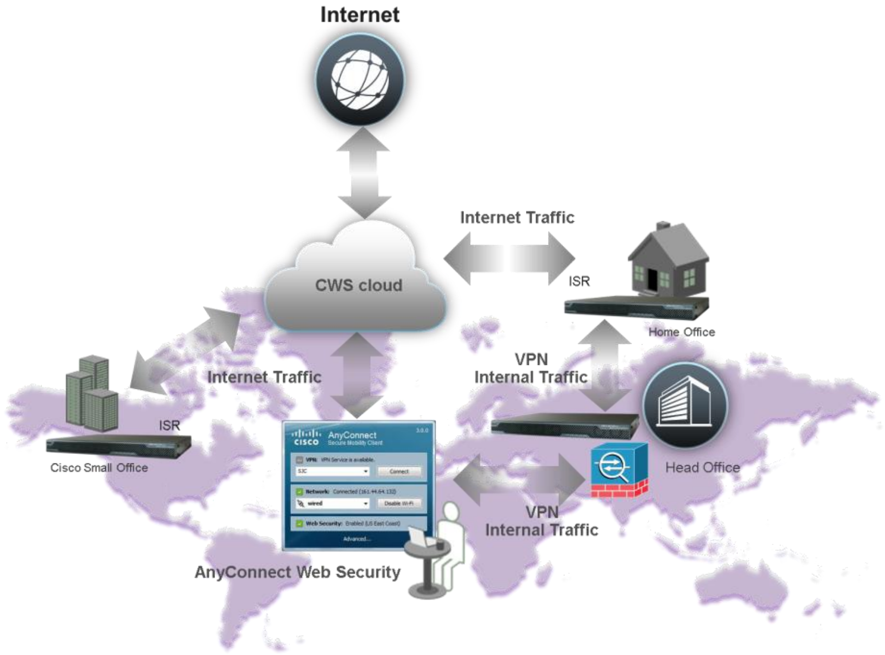
Cisco IT has deployed Cisco CWS as a complement to the Cisco Web Security Appliance. All Internet traffic on the corporate network that arrives via VPN or on-premises connection uses Cisco WSA. Internet traffic from employee laptops that is sent over a public network uses Cisco CWS via the Cisco AnyConnect client.

In the Cisco IT pilot deployment, Cisco CWS has three main components:

- Cisco AnyConnect client for individual user connections
- Cisco Cloud Web Security cloud, which is hosted in Cisco data centers
- CWS database and reports

The CWS service runs on scanning proxy servers, located in Cisco data centers around the world. The Cisco AnyConnect client and Cisco ISR G2 routers automatically route user traffic to the data center with the fastest response time to minimize latency. (Figure 2)

Figure 2. Traffic Flow in the Cisco CWS Cloud Deployment



The network traffic bypasses scanning proxies only when the Cisco AnyConnect client detects that it is connected to the trusted corporate network. In this scenario, all web traffic destined to the Internet will be subject to inspection by the WSA. The servers should be added in the Cisco AnyConnect client profile, because proxy exceptions and all HTTP traffic generated to or from them will be excluded from evaluation by the Cisco CWS service.

Implementation of Cisco CWS within the Cisco corporate network will be accomplished in two phases. As of late 2013, the deployment is in a pilot phase of 250 users, which allows for service testing, documenting the architecture and design, and validating the full deployment plans.

Users who had previously installed the Cisco AnyConnect client received instructions for downloading and configuring the CWS upgrade. The CWS feature is already configured for new users of the client.

One issue that needed to be resolved before deployment was Cisco IT’s policy on associating usernames with the URL requests stored in the CWS database. Cisco could face potential legal risks if the company chose to monitor who is making specific URL requests. With different local laws around the world, Cisco IT decided to make all user data anonymous.

Table 1 shows results from the Cisco IT pilot project for Cisco CWS from January 2013 to May 2013.

Table 1. Cisco CWS Results from a 250-User Pilot Project

Highest number phishing sites per day	17
Bandwidth of virus sites per day	77 Mb
Highest number of viruses blocked per day	400
Highest number of adware blocked per day	1800
Top site adware blocked site	router.tlvmedia.com
Top site blocked application site	Youku
Top Three Blocked Categories	Computers and Internet; Advertisements; Infrastructure and Content Delivery
Highest number of blocks per day for all apps	3300
Top applications that consumed most bandwidth	YouTube, Flash Video, Netflix, MPEG, Youku

Remediating the disruptions caused by malware infections creates significant workloads and costs for IT. For example, in a nine-month period from late 2012 to early 2013, malware infections generated more than 200 cases for virus remediation and more than 2700 help desk cases, for a total cost of more than US$4 million to Cisco IT.

Management

Cisco CWS offers the ScanCenter management portal that integrates all management and reporting capabilities.

Cisco CWS reporting provides a centralized database of user URL requests for a clear picture into the threats and breaches presented by off-premises devices. By analyzing this data over time, Cisco IT identifies policy adjustments that will increase the benefits of Cisco CWS.

Service and Support

The internal Cisco WebEx® Social site offers users an FAQ document and self-support tips for configuring the CWS service in the Cisco AnyConnect client. The Cisco IT help desk also provides full user support for the internal CWS service.

Security

Cisco CWS operates within the standard security architecture and procedures for the Cisco network.

Lessons Learned

Based on the pilot project, Cisco IT offers the following insights for implementing Cisco CWS:

- Run a limited pilot project and form a user team to identify any needed changes in the user experience.
- Integrate Cisco CWS into the overall remote access solution to help users adapt to the changes in how they access the Internet.
- Identify whether to use Cisco CWS only for Windows and Macintosh clients, or for all types of mobile devices.
- Review policies that govern user access to websites to verify that they are up-to-date with current laws and security concerns.

- Determine whether you will allow users to override CWS when it blocks access to a particular website.
- Be prepared to answer user questions about why corporate policies restrict access to certain websites and about how their data is tracked and used in the CWS reports.

For More Information

Read more information about the Cisco products discussed in this document:

- Cisco Cloud Web Security: http://www.cisco.com/web/products/security/cloud_web/index.html
- Cisco AnyConnect Secure Mobility Client: www.cisco.com/go/anyconnect
- Cisco Web Security Appliance: http://www.cisco.com/en/US/products/ps10164/index.html

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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.**