WEB SECURITY APPLIANCE

Pramod Kaler, Eshita Patni and Akshita Lodha
Department of computer Engineering, Govt Polytechnic College, Sikar
Department of Information Technology Jaipur Engineering College and Research Center Jaipur

Abstract - In our highly connected and increasingly mobile world, more complex and sophisticated threats require the right mix of security solutions. Cisco delivers security for all layers of network infrastructure with the strong protection, complete control, and investment value businesses need. They also offer a broad set of web security deployment options, along with market-leading global threat intelligence. The Cisco Web Security Appliance (WSA) simplifies security with a high-performance, dedicated appliance and the Cisco Web Security Virtual Appliance (WSAV) lets businesses deploy web security quickly and easily, wherever and whenever it’s needed. The Cisco WSA is the first secure web gateway to combine leading protections to help organizations address the growing challenges of securing and controlling web traffic. You get advanced malware protection, application visibility and control, acceptable use policy controls, insightful reporting, and secure mobility all on a single platform. The Cisco WSA enables simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs. “Set and forget” technology frees up staff once initial automated policy settings go live and automatic security updates are pushed to network devices every three to five minutes. Flexible deployment options and integration with your existing security infrastructure help you meet quickly evolving security requirements.

1. INTRODUCTION
Web access is a requirement for the day-to-day functions of most organizations. The challenge is maintaining appropriate web access for everyone in the organization while minimizing unacceptable or risky use. A solution is needed to control policy-based web access to ensure employees work effectively and confirm that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk. One risk associated with Internet access for the organization is the pervasive threat that exists from accessing sites and content. As the monetary gain for malicious activities on the Internet has grown and developed, the methods used to affect these malicious and illegal activities has grown and become more sophisticated.

Botnets, one of the greatest threats that exist in the Internet today, are malicious Internet servers (mostly web) being used to host content that then attacks innocent user’s browsers as they view the content. These types of attacks have been used very successfully by “bot herders” to gather in millions of infected members that are subject to the whims of the people who now control their machines. Other threats include the still popular and very broad threats of viruses and trojans, in which a user receives a file in some manner and is tricked into running it, and the file then executes malicious code. The third variant uses directed attacks over the network. Examples of these attacks are the Internet worms that gathered so much attention in the early to mid-2000s. Cisco IT achieved the goal of protecting against zero-day threats without changing the user experience using the Cisco IronPort S670 Web Security Appliance (WSA). The IronPort WSA is a web proxy that inspects and then either forwards or drops web traffic based on reputation filters or the outcome of inline file scanning. The IronPort WSA combines many technologies in one platform. Cisco initially is using two capabilities: Web-Based Reputation Filters (WBRS) and the Webroot and McAfee antimalware scanning engines.

Unlike many companies, Cisco is not using the IronPort WSA’s web-filtering capabilities to block entire website categories, such as gambling or shopping. The company’s policy is to trust employees to use their time productively. Cisco has always had a permissive web-access policy because of its engineering and development focus.

2. WEB SECURITY APPLIANCE
Manage the Safe Use of Web-Based and Social Networking Applications with an On-premise Security Appliance—All web traffic from the primary-site and remote-site networks accesses the Internet through a centralized Cisco Adaptive Security Appliance (ASA) firewall. Cisco Web Security Appliance (WSA) complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security using a dedicated on-premises appliance. All web traffic from the primary site and any remote-site networks access the Internet through a centralized Cisco ASA firewall. Cisco Web Security Appliance (WSA) complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security using a dedicated on-premises appliance. This design guide enables the following security capabilities:
• Transparent redirection of user web traffic—Through the seamless integration with the Cisco ASA firewall, web traffic is transparently redirected to Cisco WSA service. No configuration changes are required on user devices.
• Web filtering—Cisco WSA supports filters based on predefined content categories, as well as custom categories. The filtering rules can be configured to block, monitor or warn based on the specific web usage policies of an organization.
• Malware protection—Cisco WSA analyzes every web request to determine if content is malicious. Cisco WSA updates its malware protection policies by using the Cisco Security Intelligence Operations (SIO), which is designed to help organizations secure business applications and processes through identification, prevention, and remediation of threats.

3. BENEFITS OF WEB SECURITY APPLIANCE

• Single Appliance Security and Control The Cisco IronPort S-Series offers a single appliance solution to secure and control the three greatest web traffic risks facing enterprise networks: security risks, resource risks and compliance risks.
• Mitigate Malware Risks and Costs With malware infecting approximately 75 percent of corporate desktops, there is considerable overhead around managing infected desktops, ensuring minimal downtime to the end-user and minimizing the risk of information leakage. By stopping these threats at the network perimeter with Cisco IronPort web security appliances, enterprises can significantly reduce the administrative costs, prevent attacker “phone-home” activity on networks, reduce support calls, enhance worker productivity and also eliminate the business exposure that accompanies these threats.
• Complete, Accurate Protection Cisco IronPort S-Series appliances are designed from the ground up to address the broadest range of web-based malware threats, including those from the use of FTP and dynamic Web 2.0 sites. A multi-layered defense that includes Cisco Security Intelligence Operations, Cisco IronPort URL Filters, Cisco IronPort Web Reputation Filters and Cisco IronPort DVS technology (with multiple anti-malware scanning engines running simultaneously), ensures industry-leading accuracy. This multi-layered protection is based on a deep content application-layer inspection, as well as network-layer pattern detection, checking both inbound and outbound activities. These innovations make the Cisco IronPort S-Series the industry’s most secure web gateway.
• Enforce Acceptable Use Policies (AUP) By implementing acceptable use web policies, enterprises can not only conserve resources for work-related web usage, but also inform end-users to help shape web access behavior over time. enterprises can increase the amount of time that employees spend on business-oriented activities, reducing misuse of enterprise networks and bandwidth.
• Simplified Data Security The data loss problem extends well beyond malware. employees can easily use webmail to send a message including proprietary information, post confidential data on social networks and blogs, or transfer financial documents over FTP to a server outside the corporate network. Making sure that sensitive data does not leave the corporate boundary – while allowing users to leverage the full power of the Internet – is an important and challenging issue to solve. Cisco IronPort web security appliances enable organizations to take quick, easy steps to enforce common sense data security policies for outbound traffic on HTTP, HTTPS and FTP.
• Reporting Visibility The Cisco IronPort S-Series appliances deliver real-time and historical security information, allowing administrators to quickly understand web traffic activity. Real-time reports let administrators identify and track issues such as policy violations and security violations as they occur. Historical reports allow administrators to identify trends and report on efficacy and ROI.
• Enterprise-Scale Performance Cisco IronPort web security appliances scale to meet the unique scanning needs of web traffic, thereby ensuring that the end-user experience is maintained. Cisco offers industry-leading performance through its proprietary IronPort AsyncOS platform, an enterprise-grade web proxy and cache file system as well as an intelligent, multi-core engine for rapid content scanning. Consequently, the Cisco IronPort S-Series is a platform that can address the capacity requirements of even the largest of enterprises.
• Low Total Cost Of Ownership Legacy solutions typically require multiple appliances or servers to protect against security, resource and compliance risks. Unlike other solutions, the Cisco IronPort S-
Series provides a single platform that contains a complete, in-depth defense – along with all the necessary management tools – significantly reducing initial and ongoing TCO.

- **Reduced Administrative Overhead** Designed to minimize administrative overhead, Cisco IronPort web security appliances offer easy setup and management with an intuitive graphical user interface, support for automated updates, and comprehensive monitoring and alerting. The solution is also easy to deploy and configure to match corporate-specific policies.

4. DESIGN OVERVIEW

Cisco Web Security Appliance (WSA) addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection.

The Cisco WSA family is a web proxy that works with other Cisco network components such as firewalls, routers, or switches in order to monitor and control web content requests from within the organization. It also scrubs the return traffic for malicious content.

Cisco WSA is connected by one interface to the inside network of the Cisco Adaptive Security Appliance (ASA). In the Internet edge design, Cisco WSA connects to the same LAN switch as the Cisco ASA appliance and on the same VLAN as the inside interface of the appliance. Cisco ASA redirects HTTP and HTTPS connections to Cisco WSA by using the Web Cache Communication Protocol (WCCP).

5. CONCLUSION

The number of security threats introduced by web traffic has reached epidemic proportions. Traditional gateway defenses are proving to be inadequate against a variety of web-based malware, leaving corporate networks exposed to the inherent danger posed by these threats. According to industry estimates, approximately 75 percent of corporate PCs are infected with spyware, yet less than 10 percent of corporations have deployed perimeter malware defenses. Additionally, 87 percent of today’s web-based threats are delivered through legitimate websites. The speed, variety and maliciousness of web-based malware attacks highlight the importance of a robust, secure platform to protect the enterprise network perimeter from such threats.

In addition to the security risks introduced by web-based malware and spyware, web traffic also exposes an organization to compliance and productivity risks introduced by inappropriate usage of the web within an organization.

The Cisco® IronPort S-Series web security appliance is the industry’s first and only secure web gateway to combine traditional URL filtering, reputation filtering, malware filtering and data security on a single platform to address these risks. By combining innovative technologies, the Cisco IronPort S-Series helps organizations address the growing challenges of both securing and controlling web traffic.

Customers enjoy low total cost of ownership (TCO), as these powerful applications are integrated and managed on a single appliance. Robust management and reporting tools deliver ease of administration, flexibility and control, as well as complete visibility into policy- and threat-related activities.

6. REFERENCES


[9] Parmar, B” Protecting against spear-phishing. Computer Fraud Secure” 2018

AUTHOR INFORMATION
Eshita Patni, Department of Information technology, Jaipur Engineering College and Research Centre

Akshita Lodha, Department of Information technology, Jaipur Engineering College and Research Centre