

McAfee Enterccept Web Server Edition

Proven Intrusion Prevention for Web Servers

The Challenge

Web servers present difficult and unique security challenges. By nature, Web servers must be externally accessible, placing them in easy reach of attackers anywhere in the world. Furthermore, hundreds of vulnerabilities have been discovered in Web servers, making them an easy target for attackers. Additionally, Web page defacement has become increasingly popular as a method for attackers and subversive groups to gain attention.

Firewalls and perimeter security are no longer enough to protect today's enterprise. Increasingly knowledgeable hackers have discovered ways around firewalls and existing detection systems to launch attacks, such as buffer overflows and worms, directly against servers and applications. For example, the Code Red worm bypassed firewalls and network-based IDS to cause enormous damage. Computer Economics estimates the worldwide economic impact of the Code Red worm to be \$2.62 billion. Today's Web servers need protection from a growing battery of threats: Web defacement, buffer overflows, worms, previously unknown attack methods, etc. Additional security is required to protect Web servers from the threats of today as well as tomorrow.

The McAfee Enterccept Web Server Edition Solution

McAfee® Enterccept® Web Server Edition (WSE) identifies attacks and prevents unauthorized access to Web server resources before any unauthorized transactions occur. Building on the capabilities of the McAfee Enterccept Standard Edition, the Web Server Edition proactively protects the host by evaluating HTTP requests to the Web server (even when SSL-encrypted), the application programming interface (API), and the operating system before they are processed. McAfee Enterccept combines operating system and application protection, giving an unparalleled depth of security against known and unknown attacks.

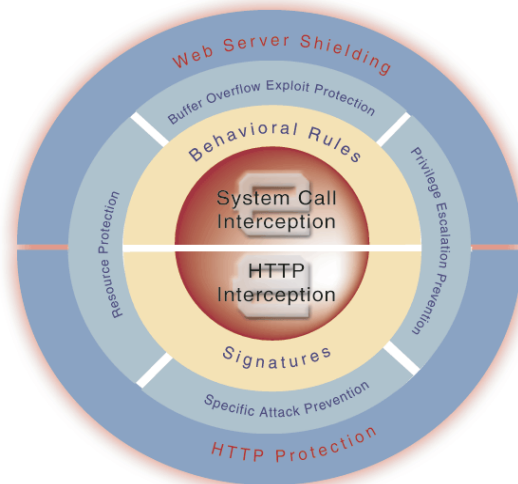
Benefits

Decreases Downtime

- Blocks Web defacement
- Prevents server compromise
- Protects against buffer overflow exploits

Reduces Security-Related Costs

- Minimizes recovery costs associated with downtime
- Reduces need for specialized personnel



McAfee Enterccept's multi-layered solution provides in-depth defense for critical Web servers.

Protects Assets

- Protects customer data
- Prevents attackers from using the Web server as a launch point for attacking other servers

Safeguards Reputation

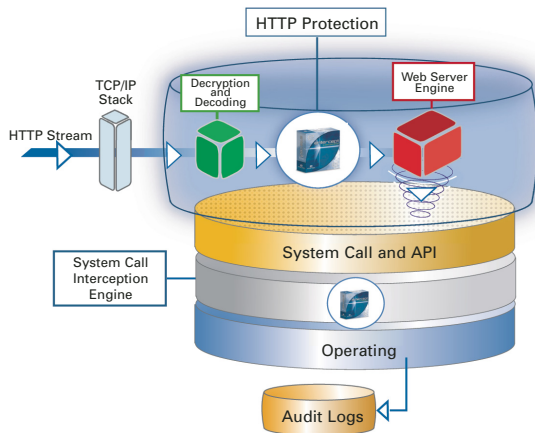
- Blocks Web defacement

How McAfee Enterccept WSE Works

McAfee Enterccept combines several core technologies to protect enterprise servers. Using a distributed architecture, McAfee Enterccept agents are installed on each server in an enterprise. These agents intercept system calls to the operating system and API and block calls that would result in malicious behavior. McAfee Enterccept determines, among other things, the process making the call, the user making the call, the resource being accessed by the call, and the user permissions related to the call. Using this information, calls are matched against the appropriate behavioral rules and known attack signatures. McAfee Enterccept then blocks calls that attempt malicious behavior or match any specific attack signature. All preventive activity is logged to the McAfee Enterccept Management System for review and reporting.

The policy database ships with a fully configured default template that incorporates powerful customization features, allowing false positives to be virtually eliminated. The default policy ensures rapid deployment. Agents are deployed per server and are controlled and updated from the McAfee Enterccept Management System.

Agents are completely self-contained protective units and not reliant on the management system to function. This approach improves both reliability and security. Agents retrieve updates from the management system, including code updates and new attack definitions. RC4 encryption and Diffie-Hellman key exchange agreements are used for all communications.



The McAfee Enterecept Web Server Edition resides on the server, protecting the operating system and applications.

Web Server Shielding—Web Server Shielding creates a protective shield around Apache, iPlanet, and Microsoft® IIS Web servers. It protects the Web server application and its resources, including data. The shield is installed after an adaptive auditing process automatically determines the configuration of the server. The shield then provides a protective envelope of operation that prevents both outside penetration and malicious use of the Web server. As a result, both known and unknown attacks are prevented in real time before they reach the Web server and cause harm. Would-be intruders cannot deface Web pages, gain access to confidential data, or modify operational parameters—even if they managed to gain privileged access to the server

HTTP Protection—HTTP Protection blocks attacks directed against Apache, iPlanet, or Microsoft IIS Web servers via HTTP requests. A parsing process checks the HTTP stream, identifies malicious requests, and blocks them from reaching the Web server before they can cause damage. This technology prevents popular Web server attacks such as remote code execution, directory traversal, and file disclosure even if intruders try to evade detection with data obfuscation or with application-level encryption such as SSL, which is

widely used by e-commerce Web sites. Full application protection is only achieved in conjunction with other McAfee Enterecept defense methodologies.

All Features of McAfee Enterecept Standard Edition—The McAfee Enterecept Web Server Edition includes the features described above, as well as all the features present in the Standard Edition: known and unknown attack prevention, buffer overflow exploit prevention, resource protection, prevention of privilege escalation, and SecureSelect.

Features

- Unique shielding giving total Web server protection
- Proactive attack response allows McAfee Enterecept WSE to prevent an exploit before any damage is done
- Eliminates need for constant security monitoring
- Secure, self-contained agents
- Pre-configured policy templates, including full customization options
- Ability to prevent malicious access to system resources
- Complements existing security infrastructure, no integration required

Installation Requirements

Windows® Web Server (English OS versions only)

- 200MHz Pentium III or faster
- 128MB RAM minimum
- Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2003 Server
- Windows NT 4 Server or Enterprise Server, Service Pack 6a or higher
- IIS 4 on NT 4
- IIS 5 on Windows 2000
- IIS 6 on Windows 2003

Solaris Web Server

- Solaris 7 (32-bit or 64-bit kernel)
- Solaris 8 (32-bit or 64-bit kernel)
- Solaris 9 (32-bit and 64-bit kernel)
- Apache 1.3.6 and higher
- Apache 2.0.42 and higher
- iPlanet 4.0/4.1 and SunOne 6
- Netscape Enterprise Server 3.6

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766), www.mcafeesecurity.com

Network Associates® products denote years of experience and commitment to customer satisfaction. The PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects—all with service levels to meet the needs of every customer organization. McAfee® Research, a world leader in information systems and security, continues to spearhead innovation in the development and refinement of all our technologies.

Network Associates, McAfee, Enterecept and PrimeSupport are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Sniffer® brand products are made only by Network Associates, Inc. All other registered and unregistered trademarks herein are the sole property of their respective owners. ©2004 Networks Associates Technology, Inc. All Rights Reserved. 1-sps-ent-wse-002-0304