McAfee Web Gateway

Security. Control. Performance.

McAfee Web Gateway

- Common criteria EAL2+ and FIPS 140-2 Level 2 certified.
- Number one-rated anti-malware solution on the market (AV-TEST).

Organizations can do more over the web today than ever before. Today's web offers a dynamic, real-time user experience. However, the web has also become a more dangerous place, with increasingly sophisticated attacks released every day. The McAfee® Web Gateway appliance is the first line of defense for any organization to protect against evolving malware threats. It empowers organizations to enable employee access while greatly reducing an organization's risk with an advanced security approach that combines powerful, local intent analysis with cloud-based protection powered by McAfee Labs.

As web application use and sophistication increases, so does the need for flexible access coupled with advanced web security because even seemingly "safe" sites can be targeted for malware distribution.

In today's world, simply blocking known viruses or restricting access to "known bad" websites is not enough. Reactive techniques, such as signature-based antivirus and category-only URL filtering, while necessary, are insufficient to protect access to cloud applications or combat today's exploits.

Since these solutions focus on known content and malicious objects or executables, they can't prevent today's attacks that hide malicious code within seemingly trustworthy HTTP or HTTPS traffic, or provide protection against unknown or emerging threats. The ability to enable secure, granular access to cloud applications while proactively blocking unknown, as well as known, threats is now crucial.

Intel Security understands the security needs of the web-enabled world like no other vendor and offers the industry's most effective, proven proactive solution: McAfee Web Gateway.

Complete Inbound and Outbound Protection

McAfee Web Gateway delivers comprehensive security for all aspects of web traffic, regardless of location or device. For user-initiated web requests, McAfee Web Gateway first enforces an organization's Internet use policy. For all allowed traffic, it then uses local and global techniques to analyze the nature and intent of all content and active code entering the network via the requested web pages, providing immediate protection against malware and other hidden threats. And, unlike basic packet inspection techniques, McAfee Web Gateway can examine SSL traffic to provide in-depth protection against malicious code or inappropriate applications that have been disguised through encryption.

Inbound protection also mitigates risks for organizations hosting websites that accept data or document uploads from external sources. McAfee Web Gateway in reverse proxy mode scans all content before it is uploaded, securing both the server and the content.

To secure outbound traffic, McAfee Web Gateway uses our industry-leading DLP technology to scan user-generated content on all key web protocols—including HTTP, HTTPS, and FTP—and protect against loss of confidential, sensitive, or regulated information leaking from the organization through social networking sites, blogs, wikis, or online productivity tools such as web-based mail, organizers, and calendars. McAfee Web Gateway also safeguards against unauthorized data leaving the organization through "bot-infected" machines attempting to phone home or transmit sensitive data.

McAfee Web Gateway Delivers the Industry's Best Protection

As the number one-rated[1] malware protection, McAfee Web Gateway uses a patent-pending approach to signature-less intent analysis with the McAfee Gateway Anti-Malware Engine. Proactive intent analysis filters out malicious content from web traffic in real time. By scanning a web page's active content, emulating and understanding its behavior, and predicting its intent, McAfee Web Gateway proactively protects against zero-day and targeted attacks as they occur.

McAfee Web Gateway integrates with McAfee Advanced Threat Defense—advanced anti-malware detection technology with innovative sandbox capabilities that combine static and dynamic analysis. The result is greater accuracy and stronger protection against advanced, dynamic malware threats.

We combine this local, real-time intent analysis with comprehensive McAfee antivirus protection to quickly block known viruses and several cloud-based technologies—all powered by McAfee Labs. Use of multiple technologies enables McAfee Web Gateway to provide greater protection while optimizing security on a single platform with different, yet complementary, technologies—something many organizations want for their defense-in-depth security approaches.

- **McAfee antivirus with real-time McAfee Global Threat Intelligence (McAfee GTI) file reputation**: With cloud-based McAfee GTI file reputation look-up capabilities, McAfee closes the gap between virus discovery and system update/protection.
- **McAfee GTI web reputation and web categorization**: McAfee Web Gateway delivers enhanced web filtering functionality and protection through the powerful combination of both reputation and category-based filtering. McAfee GTI creates a profile of all Internet entities—websites, email, and IP addresses—based on hundreds of different attributes gathered from the massive, global data collection capabilities of McAfee Labs. It then assigns a reputation score based on the security risk posed, enabling administrators to apply very granular rules about what to permit or deny.

McAfee Web Gateway offers expanded, cloud-based web reputation capabilities that now include geo-location, enabling geographic visibility and policy management based on the web traffic's originating country. For both web categorization and security-focused web reputation, organizations can now choose between on-premises and cloud lookups or a combination of both. Cloud lookups eliminate protection gaps between discovery/change and system updates and offer significantly enhanced coverage with data on hundreds of millions of unique malware samples.

Protection for encrypted traffic
Sophisticated cybercriminals have turned to SSL traffic (HTTPS) as the new back door through the enterprise's security barrier. Ironically, a protocol designed to provide security must now also be secured against abuse, just as traditional HTTP traffic must be secured. McAfee Web Gateway is the first security product to fully integrate malware detection, SSL inspection, and certificate validation. There's no need to route encrypted traffic to a separate box for malware inspection. McAfee Web Gateway directly scans all SSL traffic to ensure the complete security, integrity, and privacy of encrypted transactions and to enforce acceptable usage policy.

Data loss prevention
McAfee Web Gateway protects organizations from outbound threats—such as leakage of confidential information—by scanning outbound content over all key web protocols, including SSL. This makes it an essential tool for preventing intellectual property loss, ensuring and documenting regulatory compliance, and providing forensic data in the event of a breach. Leveraging the power of the McAfee Data Loss Prevention (DLP) solution, McAfee Web Gateway supports predefined DLP dictionaries and enables custom dictionaries to be created through keyword matching and/or regular expressions.

Built-in file encryption protects data that is uploaded to file sharing/collaboration sites against unauthorized access. Users cannot retrieve and view the data without going through the Web Gateway.

Mobile filtering for remote users
As the workforce becomes more distributed and mobile, the need for web filtering and protection to seamlessly transition from the office to the road becomes increasingly important. McAfee Client Proxy, a tamperproof client agent, enables roaming users to seamlessly authenticate and redirect to either a McAfee SaaS Web Protection solution in the cloud or an on-premises Web Gateway located in a DMZ. This enables Internet access policy enforcement and full security scanning to be applied to roaming or remotely located users, even if their Internet access is via a public portal, such as at a coffee shop, hotel, or other Wi-Fi hotspot.

McAfee Web Gateway also allows enterprises to extend and enforce their security policies on mobile devices. Today's popular smartphones and tablets can direct web traffic to McAfee Web Gateway which, through standard device management and security controls, ensures that mobile devices are secured with advanced anti-malware protection and corporate web filtering policies. McAfee Web Gateway also extends protection to mobile devices accessing content that is traditionally available on internal corporate servers such as intranets, wikis, Microsoft SharePoint servers, and other web-based solutions. While this information is generally not made available to certain mobile devices due to security concerns, McAfee Web Gateway deployed as a reverse proxy can enable controlled and secure access to these internal resources.

Taking Control with McAfee Web Gateway

McAfee Web Gateway protects today's web-centric enterprises with a powerful rules-based engine for optimal policy flexibility and control. To streamline policy creation, McAfee Web Gateway offers an extensive pre-built rules library with common policy actions. Organizations can pick and choose various rules, easily modify these rules, and share their own rules through an online community. Interactive rules tracing simplifies rules debugging.

The McAfee Web Gateway platform extends acceptable usage policy and control to web applications as well, enabling granular, proxy-based control over how web applications are used. Organizations can control more than 1,000 popular web applications, enabling or disabling specific functionality as needed, controlling who uses a web application and how it is used. Do you want to enable access to Facebook but not allow chat? No problem.

Flexibility and control also extend to user authentication and access. McAfee Web Gateway supports numerous authentication methods, including NTLM, RADIUS, AD/LDAP, eDirectory, cookie authentication, Kerberos, or a local user database. The McAfee Web Gateway authentication engine allows administrators to implement flexible rules, including the use of multiple authentication methods. For example, McAfee Web Gateway can try to transparently authenticate a user and, based on the result, prompt the user for credentials, use another authentication method, apply a restrictive policy, or simply deny access.

McAfee Web Gateway Identity, an optional add-on, includes single sign-on (SSO) connectors for hundreds of popular cloud-based applications. McAfee Web Gateway Identity provides today's web-centric enterprises with the ability to improve security and reduce password-related help desk calls using an SSO launch pad where users can access authorized cloud applications with a simple click of the mouse.

Support for both HTTP POST and Security Assertion Markup Language (SAML) connectors provide coverage for a wide range of applications. Provisioning connectors enable system administrators to create and terminate user accounts on select SaaS applications.

McAfee Web Gateway extends access control to streaming content through native streaming proxy support as well, providing bandwidth savings and reduced latency.

Agile Infrastructure and Performance with McAfee Web Gateway

McAfee Web Gateway is a high-performance, enterprise-grade proxy that provides the caching, authentication, administration, and authorization controls required by today's most demanding enterprises. Offering a scalable family of appliance models with integrated high availability, support for virtualized machines, and in-the-cloud service with McAfee SaaS Web Protection, McAfee Web Gateway delivers the deployment flexibility and performance you need, along with the scalability to easily support hundreds of thousands of users in a single environment. (For more information on SaaS, see **McAfee SaaS Web Protection** on McAfee.com.)

You can mix deployment options as well. For example, you can offload portions of web traffic to the cloud during peak times for added high-availability performance or use this hybrid model as a cost-effective fail-over option. Automated policy synchronization and reporting for hybrid on-premises and cloud deployments help streamline management, ensure consistent policy enforcement, and simplify reporting, tracking, and investigation.

McAfee Web Gateway offers numerous implementation options—from explicit proxy to transparent bridge and router modes—to ensure that your network architecture is supported.

With support for numerous integration standards, McAfee Web Gateway is designed to work in your unique environment. From the web cache communication protocol (WCCP) to the Internet content adaptation protocol (ICAP/ICAPS) to the socket secure (SOCKS) protocol, McAfee Web Gateway efficiently communicates with other network devices and security appliances.

Additionally, McAfee Web Gateway now offers IPv6 support, helping larger organizations and federal institutions comply with regulations. McAfee Web Gateway bridges the gap between internal IPv4 and external IPv6 networks and applies all available security and infrastructure features and functions to the traffic.

Value and a Platform for the Future

McAfee Web Gateway combines and integrates numerous protections that would otherwise require multiple stand-alone products. Web filtering, anti-malware, antispyware, SSL scanning, data loss prevention, and content control filtering—you can get all of these protections in a single, cost-effective appliance. And a simplified management footprint means that a single security policy can be shared across protections and protocols, saving you valuable time and money.

Security Risk Management and Reporting

The most popular and respected security management technology, the McAfee ePolicy Orchestrator® (McAfee ePO™) platform, is supported by McAfee Web Gateway. As the single source for consolidated information, the McAfee ePO platform helps you quickly identify and mitigate problems and improve compliance management.

McAfee ePO software supports detailed web reporting through the McAfee Content Security Reporter extension. McAfee Content Security Reporter gives you the information and forensic tools you need to understand how your organization is using the web, identify instances of unknown or rogue "shadow IT" applications, comply with regulations, identify trends, isolate problems, document inappropriate web activity, and tailor your filtering settings to enforce your web usage policies. It combines dashboard views and drilldowns into web traffic with powerful offline processing—everything you need in one easy-to-use solution. McAfee Content Security Reporter offers an external, stand-alone report server designed to offload resource-intensive data processing and storage from the existing McAfee ePO server, enabling it to scale to meet the reporting needs of even the largest global corporations.

Licensing

For the ultimate in deployment flexibility and to help future-proof your investment, McAfee offers all features of the McAfee Web Gateway and McAfee SaaS Web Protection Service in a single suite: **McAfee Web Protection**. Deploy on premises, in the cloud, or both for added flexibility and high availability—the choice is yours. You'll find award-winning McAfee anti-malware protection and comprehensive web filtering with either option.

McAfee Web Gateway hardware is sold separately.

1. In tests conducted by AV-TEST, McAfee Web Gateway detected 94.5% of zero-day malware, 99.8% of malicious Windows 32 portable executable (PE) files, and 98.63% of non-PE files. "McAfee Web Gateway Security Appliance Test," AV-TEST GmbH.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com