McAfee Web Gateway

Security. Connected Intelligence. Performance.

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. McAfee® Web Gateway is a critical defense for any organization to protect against emerging malware threats. It empowers organizations with secure internet access while greatly reducing risk through an advanced security approach that combines powerful, local intent analysis with cloud-based protection powered by McAfee Labs.

As internet use and sophistication increases, so does the need for advanced web security. 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 crucial.

Comprehensive Inbound and Outbound Protection

McAfee Web Gateway delivers comprehensive security for all aspects of web traffic in one high-performance appliance software architecture. 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 secure sockets layer (SSL) traffic to provide in-depth protection against malicious code or control applications that have been hidden through encryption.

McAfee Web Gateway

- Available in multiple hardware models and as a virtual machine supporting VMware and Microsoft Hyper-V
- Integrated with complementary McAfee solutions including McAfee Endpoint Security, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, McAfee Cloud Data Protection, and McAfee Cloud Visibility—Community Edition
- Common criteria EAL2+ and FIPS 140-2 Level 2 certified
- Support for multiple cryptographic key storage options, including Gemalto SafeNet Hardware Security Module (HSM), Thales nShield HSM, and Thales PCIe cards
- Rated number one anti-malware in a secure web gateway (AV-TEST)

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

To secure outbound traffic, McAfee Web Gateway uses industry-leading McAfee Data Loss Prevention technology to scan user-generated content on all key web protocols, including HTTP, HTTPS, and FTP. It also protects 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 further 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] web security solution in malware protection, McAfee Web Gateway uses a patented approach to signatureless intent analysis with the McAfee Gateway Anti-Malware Engine. Proactive intent analysis filters out previously unknown, or zero-day 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 prevents the delivery of zero-day malware to endpoints, dramatically reducing the costs associated with system cleanup and remediation.

We combine this analysis with McAfee antivirus and global reputation technologies from McAfee Labs to quickly block known malware and malicious sites. 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 demand for their layered defense security approaches.

- **McAfee antivirus with real-time McAfee Global Threat Intelligence (McAfee GTI) file reputation:** Cloud-based McAfee GTI file reputation look-up closes the gap between virus discovery and system update/protection.
- **McAfee GTI web reputation and web categorization:** McAfee Web Gateway delivers 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.
- **Geolocation:** McAfee Web Gateway features geolocation, enabling geographic visibility and policy management based on the web traffic and user's originating country.

For both web categorization and web reputation, organizations can choose between on-premises and cloud lookups, or a combination of both. Cloud lookups eliminate protection gaps between discovery/change and system updates, along with delivering broad coverage through data on hundreds of millions of unique malware samples.

Advanced Threat Analysis integration

McAfee Web Gateway integrates with McAfee Advanced Threat Defense—our advanced malware detection technology that combines customizable sandboxing with in-depth static code analysis. McAfee Advanced Threat Defense and the in-line scanning capabilities of the Gateway Anti-Malware Engine in McAfee Web Gateway provide the strongest protection available for internet-delivered threats. Organizations that want a lower cost, simplified advanced threat analysis option can integrate McAfee Cloud Threat Detection, a cloud-based sandbox with multiple additional threat analysis layers.

Threat Intelligence sharing

Today, many security tools exist in silos and are not built to share threat intelligence, despite the fact that key intelligence is available at the endpoint, network, security information and event management (SIEM) solution, gateway, and more. When shared, this intelligence can be utilized for better protection against threats, detection of existing breaches, and improved incident response through efficient correction of compromised systems. Through McAfee Threat Intelligence Exchange, McAfee solutions—including McAfee Web Gateway—share intelligence with each other to bridge these gaps.

McAfee Web Gateway delivers immense value in this process by creating and sharing new file reputations for zero-day malware discovered by the Gateway Anti-Malware engine, allowing, for example, endpoint devices to be protected before a new .DAT is released. Additionally, more threats are stopped by McAfee Web Gateway with expanded threat intelligence delivered from McAfee Threat Intelligence Exchange.

Insight and protection within encrypted traffic

Sophisticated cybercriminals have turned to SSL traffic (HTTPS and HTTP/2) as a backdoor through the enterprise security barrier. Ironically, a protocol designed to provide security must also be assessed for risk. McAfee Web Gateway integrates malware detection, SSL inspection, and certificate validation together for a comprehensive approach to encrypted traffic inspection.

There's no need for an additional investment in SSL scanning hardware—McAfee Web Gateway performs all of this in a single hardware or virtual appliance architecture. McAfee Web Gateway directly scans all SSL traffic to ensure the complete security, integrity, and privacy of encrypted transactions.

Organizations that want to take the initiative to go deeper into their inspection of SSL traffic can offload the entire stream of unencrypted traffic or individual streams by policy through the SSL tap within McAfee Web Gateway. This software-enabled feature allows a full or partial mirror of decrypted SSL traffic to be sent to additional security solutions such as intrusion prevention systems (IPS) or network-based data loss prevention (DLP) solutions.

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 a powerful 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 solution set, McAfee Web Gateway includes built-in, predefined DLP dictionaries and enables custom dictionaries to be created through keyword matching and/or regular expressions.

For organizations that utilize cloud-based storage, 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 McAfee Web Gateway.

Protection for off-network users

As the workforce becomes more distributed and mobile, the need for web filtering and protection while seamlessly transitioning from the office to the road becomes increasingly important. McAfee Client Proxy, a tamper-resistant client agent, enables roaming users to seamlessly authenticate and redirect to either an on-premises McAfee Web Gateway located in a demilitarized zone (DMZ) or the McAfee Web Gateway Cloud Service. 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 by directing web traffic to McAfee Web Gateway. Through our partnerships with mobile device management providers AirWatch and MobileIron, McAfee Web Gateway ensures that Apple iOS and Google Android mobile devices are secured with advanced anti-malware protection and corporate web filtering policies.

Ultimate Flexibility with McAfee Web Gateway

McAfee Web Gateway features a powerful, rules-based engine for policy flexibility and control. To streamline policy creation, McAfee Web Gateway offers an extensive prebuilt rules library with common policy actions. Organizations can pick and choose various rules, easily modify these rules, and share their own rules through our online community. For advanced administration, a unique combination of context-based rule criteria and shared lists opens the door to unlimited possibilities for problem solving and web security optimization. Interactive rules tracing simplifies rules debugging.

McAfee Web Gateway extends control to cloud applications, enabling granular, proxy-based control over how web applications are used. Organizations can apply thousands of controls to cloud 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 Dropbox but not allow uploads? No problem.

Flexibility and control also extend to user authentication and access. McAfee Web Gateway supports numerous authentication methods, including NT LAN manager (NTLM), remote authentication dial in user service (RADIUS), Active Directory (AD)/lightweight directory access protocol (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 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 one click. Support for both HTTP power-on self-test (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 Software-as-a-Service (SaaS) applications.

McAfee Web Gateway extends access control to streaming content through native streaming proxy support as well, providing bandwidth savings and reduced latency. Additional bandwidth controls can be set to enforce minimums, maximums, and prioritization for defined classes of traffic, allowing organizations to optimize use of their available bandwidth.

Agile Infrastructure and Performance with McAfee Web Gateway

McAfee Web Gateway is a high-performance, enterprise-grade proxy offered in a scalable family of appliance models with integrated high availability, virtualization options, and hybrid deployment with McAfee Web Gateway Cloud Service. McAfee Web Gateway delivers deployment flexibility and performance, along with the scalability to support hundreds of thousands of users in a single environment.

You can mix deployment options as well. For example, you can route all web traffic to the on-premises appliance for on-network users, and route all off-network users to the cloud service, dramatically reducing the cost of backhauling traffic over multiprotocol label switching (MPLS) lines or virtual private network (VPN). 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), internet content adaptation protocol (ICAP/ICAPS), and WebSocket protocol to the socket secure (SOCKS) protocol, McAfee Web Gateway efficiently communicates with other network devices and security appliances.

Additionally, McAfee Web Gateway 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.

Unified Platform for the Future

McAfee Web Gateway combines and integrates numerous protections that would otherwise require multiple standalone products. URL filtering, antivirus, zero-day anti-malware, SSL scanning, data loss prevention, and central management—all are unified in one appliance software architecture. Managing deployments is unified across all form factors, so one policy can be extended to on-premises appliances, clusters of appliances, virtual appliances, and the cloud service all from one single management console.

Security Risk Management and Reporting

The popular and respected security management technology, McAfee ePolicy Orchestrator® (McAfee ePO™) software, is supported by McAfee Web Gateway as a single source for all security reporting.

McAfee ePO software delivers detailed web security reporting through the McAfee Content Security Reporter extension. McAfee Content Security Reporter gives you information and forensic tools to understand how your organization is using the web, comply with regulations, identify trends, isolate problems, and tailor your filtering settings to enforce your web security policies. McAfee Content Security Reporter offers an external, stand-alone reporting 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 organizations.

Additionally, McAfee Web Gateway integrates with McAfee Cloud Visibility—Community Edition, a free service for McAfee Data Loss Prevention, encryption, and McAfee Web Protection customers that brings visibility to cloud application usage and risk. Employees are using cloud applications, but IT only knows about some of them, and that lack of visibility creates risk. A simple dashboard into all cloud application access, risk levels, and data classification takes this burden away so security professionals can focus their time and effort around actually protecting the data moving to the cloud along with controlling cloud access, which will reduce risk for the organization.

McAfee Cloud Visibility—Community Edition is also included as a free service with McAfee Cloud Data Protection, the next step in safeguarding data in the cloud.

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 Web Gateway Cloud 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
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com