Technology Blueprint

McAfee
An Intel Company

INSPECT ENCRYPTED WEB TRAFFIC

Secure and enforce HTTPS traffic compliance

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL 1 2 **3** 4 5

Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Secure and enforce HTTPS traffic compliance

The Situation

As web usage escalates to be one of the highest risk attack vectors, many organizations are enhancing security protection at the proxy or web gateway. This is a positive step; however, one area of security that is frequently neglected during these infrastructure improvements is the inspection, validation, and enforcement of HTTPS (or SSL) traffic. In many organizations, HTTPS traffic represents between 10 and 30 percent of the total outbound web traffic. Without appropriate controls and inspection, this channel places security policy decisions at the hands of the end user and lies open to abuse from insider threats, data leakage, and malicious content.

Driving Concerns

An ever-increasing proportion of business applications, social networking, forums, and other web-enabled services leverage HTTPS to protect data and ensure privacy. Although many organizations have upgraded their web proxy infrastructure to a level where SSL inspection and decryption could be performed, many deployments do not leverage this functionality today.

HTTPS traffic browsing poses the following challenges:

- **SSL certificate control**. Traditionally, SSL certificates are managed and accepted by each user during the process of visiting a site. IT has no central oversight or control over these certificates, or their acceptance by the user. For example, when a spear phishing attack routes the user to a site that presents a self-signed certificate, the user will often simply accept the certificate presented, without realizing that the certificate is fake. With the rise of SSL certificate-related incidents such as the recent Diginotar compromise, it is imperative that SSL certificate policy be in the hands of the security team, not the end user.
- **Privacy and compliance concerns regarding scanning of encrypted content**. Human Resources (HR) policies and varying regional and geographical privacy regulations make it imperative to be able to scan content selectively. Regulators want to prevent scanning and inspection of HTTPS traffic that would expose protected health and personally identifiable information (PHI/PII). Many solutions either lack flexible criteria for bypassing inspection, or will allow a bypass without enforcing certificate checks.
- **Protection from malicious or infected websites, content, and "command and control" sites**. Malicious and compromised sites appear on a constant basis, thanks to automated website vulnerability tools and SQL injection. Once legitimate sites are infected, they deliver malicious HTML, mobile code, executables, and zero-day malware. Sites that leverage SSL are not exempt from such attacks, since SSL secures the transport, not the site itself.
- **Lack of enforcement of corporate executable, file, and media policies**. Realizing that many customers have a simple web filtering solution or gateway, attackers have developed their malware to leverage this outbound access point. Often, browser attacks are split into two parts: an initial exploit will then download malware such as a Trojan over a web-based channel. Unfortunately, many customers rely on a policy that restricts file downloads purely based on file extension (such as .jpg). An attacker can simply rename a file to a permitted format to bypass this filtering. For file sharing resources or webmail services, this loophole allows users to download executable content—both encrypted and not—without being scanned for malware at the gateway.
- **Application control**. Developers write some applications such as instant messaging clients and file transfer software to leverage HTTPS proxies as a mechanism to bypass security controls and tunnel outside the corporate network.

Until these challenges are overcome, most organizations are leaving themselves open to unnecessary risk, or are unable to sufficiently protect and meet the demands for web access from the business.

Solution Description

Key requirements for holistic HTTPS protection include:

- **SSL certificate control**. To reduce the risk of data leakage and uncontrolled access via HTTPS, it is important to leverage certificate validation technology. Before any HTTPS traffic is allowed from your clients, the presented server SSL certificate should be validated and compared against corporate policy. This allows the security team to approve or deny specific certificate authorities and apply appropriate policy to self-signed certificates. Should a certificate authority or certificate become compromised, you can rapidly protect your desktops by updating the policy. A mature solution will offer the following functionality:
  - » Flexibility on grace period for expired server certificates. Many organizations allow their server certificates to expire accidentally. The ability to define an acceptable grace period allows business continuity over the 24 to 48 hours it typically takes the site owner to renew the SSL certificate
  - » Control over presented self-signed certificates
  - » Fine-grained control over trusted and untrusted certification authorities
  - » Control of acceptability of overly long certificate chains
- **Encrypted content**. It is important that the solution has the ability to selectively decrypt and inspect content as required. A mature solution will offer the capability to:
  - » Select the organization's allowed ciphers, such as 3DES or AES, ensuring appropriate protection
  - » Present differing intermediate certificates dependent on location or organization. This feature is especially useful during acquisition periods.
  - » Define ports that are allowed to be connected via the proxy to prevent abuse or "tunneling"
- **Privacy features**. The solution should be able to selectively disable certificate verification or HTTPS decryption as required. Potential situations include users in specific groups, in specific countries or locations, or using healthcare and financial sites. Advanced solutions will also allow the ability to bypass auditing of specific hosts if required.
- **Protection from malicious or infected websites**. The technology must include both categorization and reputation-based technology as an initial defense mechanism. Ideally, the solution should apply context as part of additional antimalware scanning to identify sophisticated attacks.
- **Protection against dynamic malware or "Web 2.0" threats**. Traditional desktop AV engines are not designed with web content in mind. Instead, analysis should adapt to the individual request conditions (such as category or reputation). (Note: Inline IPS devices can provide additional layers of protection to detect and prevent application exploits.)
- **Enforcement of corporate executable, file, and media policies**. Best practice dictates that we should not allow every user to run or install every kind of executable content downloaded via the Internet. Enforcement by policy and by *validated* and *enforced* media type is mandatory for today's web content.
- **Integration with data loss prevention (DLP) solutions**. The ability to inspect SSL traffic allows the business to also enforce DLP or regulatory requirements on both HTTP and HTTPS traffic.
- **Application control**. Solutions should include the ability to restrict applications that are attempting to leverage HTTPS ports to bypass security controls. Advanced solutions offer predefined application definitions and include the ability to detect and offer policy controls for the HTTP/HTTPS application.
- **Detection and blocking of command and control ("phone home") communication**. Complete solutions should also include traffic flow analysis for additional validation of protocols and applications leveraging the outbound web channel available for communication. This analysis can also include command and control communication, as well as applications that attempt to tunnel that are not legitimate HTTP traffic.
- **Protection of off-premises workstations**. Solutions should offer technology to suit differing mobile workforce requirements, protecting systems when they leave the corporate network.

Decision Elements

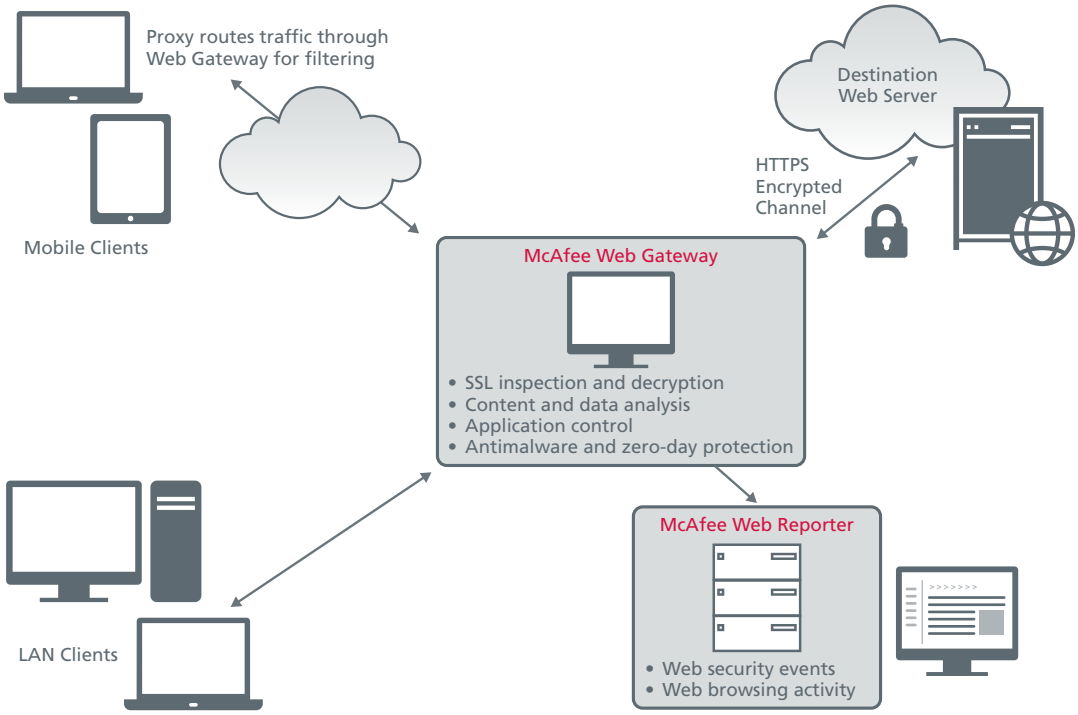
These factors could influence your architecture:

- Do you have an Internal Certification Authority you can leverage for HTTPS decryption?
- Is your web browsing centralized, or do regional offices have direct Internet connectivity?
- Do you operate in countries where privacy regulations would restrict the level of filtering or SSL decryption that can be performed?
- Do you already have a DLP solution today? Does it support ICAP or ICAPS?

Technologies Used in the McAfee Solution

To provide secured, encrypted HTTP traffic that follows corporate guidelines, the McAfee solution uses McAfee® Web Gateway for HTTPS decryption, certificate management, and deep content and malware inspection. McAfee Web Reporter provides reporting detail across certificate, malware, and content violations. Finally, the McAfee Client proxy protects remote and traveling clients such as laptops when they are outside the corporate network.

McAfee Web Gateway is often deployed within the DMZ or within the corporate LAN, and may require connectivity to authentication services, McAfee Web Reporter, and any third party operational monitoring systems that leverage email, SNMP, or SYSLOG as communication channels.



Traffic from both mobile and LAN-connected clients traverses the McAfee Web Gateway so that encrypted content can be inspected.

McAfee Web Gateway

The McAfee Web Gateway delivers HTTP and HTTPS content scanning in a single appliance. This full-featured solution can give you the controls required to inspect encrypted traffic deeply and appropriately.

HTTPS Decryption

McAfee Web Gateway offers HTTPS decryption of traffic and full inspection of content. This operation is facilitated by presenting signed certificates to the client that are trusted by a common certification authority, such as an internal Microsoft Certificate Authority (CA). If you have not yet deployed a PKI infrastructure, the McAfee Web Gateway certificate can be deployed to the browser.

McAfee Web Gateway offers a high level of flexibility including selective *bypassing* of decryption to support privacy and Human Resource regulations. You can inspect based on a wide variety of criteria such as destination host, category, a specific name presented in the common name of the certificate (CN), or if client certificates are requested from the remote server.

Certificate/Certification Authority management

McAfee Web Gateway makes it possible to ensure that appropriate and trusted HTTPS web services are leveraged by the browsing client, enforcing a security control traditionally left in the hands of the end user. You have the option to define and enforce policies on:

- Certificates that have expired, including the ability to define a grace period for cases where the webmaster has not installed or renewed the web certificate promptly
- How self-signed certificates should be handled
- Trusted root certification authorities, allowing the security team to define which certificate authorities are able to be trusted by the corporation and revoke these trusts at any time in the event of compromise

Protection from malicious content and websites

Comprehensive, contextual content coverage and policy control reduce your exposure to malicious web applications, content, and behavior. The McAfee Web Gateway uses several protection techniques:

- True media analysis and detection of file or stream content type—regardless of the MIME content type presented—to enforce correct corporate policy on downloaded or uploaded content
- Granular category-based URL filtering with reputation and geolocation awareness—McAfee Labs™ research delivers comprehensive protection from infected and malicious websites or hosts
- Two different antimalware engines for customers that wish to leverage more than one engine for policy requirements
- In addition to these malware engines, McAfee Web Gateway includes the McAfee Gateway Anti-Malware Engine. This engine delivers intent- and behavior-based detection for mobile code, web threats, and executable content, plus detection of potentially malicious shellcode. The McAfee Gateway Anti-Malware Engine also detects malicious outbound "phone home" behavior. All three antimalware engines can be layered to provide comprehensive protection.

McAfee Web Gateway is unique in that policies can be conjoined to deliver context-based content filtering. For example, if a site is hosted in an embargoed country, has an "unverified" reputation, and is providing executable content, McAfee Web Gateway can apply a more aggressive behavioral scan of the delivered content.

Application control

The administrator can define policy around specific web applications without a requirement to leverage specific URL or HTML filtering rules. For example, you may define a rule set for: the detection of anonymous proxies or tunneling applications over HTTPS; the ability to restrict posting of content to social media sites; or the upload of documents or content to "Google Docs." This functionality allows the security administrator granular control over the applications that would traditionally be bypassed over SSL channels. Application control can be defined according to the specific application or the risk posture of that application as defined by McAfee Labs™.

DLP integration and functionality

Natively—without the addition of external DLP—McAfee Web Gateway can define and detect specific content (such as credit card numbers) through the use of regular expression lists. For comprehensive DLP coverage, McAfee Web Gateway also integrates with ICAP or ICAPS (ICAP over SSL) DLP solutions including McAfee Data Loss Prevention.

McAfee Web Reporter

McAfee Web Reporter provides scalable reporting of both web security events *and* web browsing activity. For enterprise scalability, it leverages external database integration (Oracle, MySQL, and Microsoft SQL). McAfee Web Reporter allows security teams to report on certificate and Certification Authority violations, URL, application, and detailed content activity including detected malicious content. Usually, McAfee Web Reporter is deployed in a management LAN segment with connectivity to McAfee Web Gateway.

McAfee Client Proxy

For off-network content filtering and SSL scanning of laptops, McAfee provides a client proxy technology that allows transparent redirection of browsing traffic to a hosted McAfee Web Gateway. This solution will only enable the redirection function when the client is outside of the corporate network.

Management and deployment of the McAfee Client proxy is available via McAfee ePolicy Orchestrator® (McAfee ePO™) or using SMS or other package deployment solutions.

Impact of the Solution

Efficient and appropriate inspection of encrypted traffic will help your organization better protect itself and its data while enabling safe business transactions via web channels. As you enforce compliance of HTTP and HTTPS traffic, you can significantly reduce your risk and the attack surface available to web-based attacks.

The McAfee solution includes both HTTP and HTTPS content inspection in flexible deployment platforms to suit the requirements of your business. You can decommission and consolidate any existing proxy infrastructure and web controls to reduce your hardware requirements and remediation costs. In addition, our integrations help you leverage existing DLP solutions to reduce the risk of data theft.

Q&A

Do I need to have deployed an internal Certificate Authority (CA) to perform HTTPS scanning?
The McAfee Web Gateway is able to utilize a subordinate CA certificate if a certificate authority is already present. If no certificate authority is present on your network, McAfee Web Gateway is able to present its own certificate.

How does the gateway anti-malware work? Is it the same as the McAfee desktop engine?
No. The McAfee Gateway Anti-Malware Engine is a specific technology developed to focus on attacks that are often initially seen at the web gateway. It leverages custom, patented technology that allows analysis of the intent of code without specific signatures. For detailed information see Understanding the McAfee Gateway Anti-Malware Engine.

Do I need a separate management appliance to manage multiple McAfee Web Gateways?
No you do not. Centralized management is included in the appliance, with enterprise-class features such as centralized AV and URL filtering updates. If you wish to deploy an appliance in a separate VLAN or management segment, this can be facilitated with either a virtual or physical appliance.

Am I required to deploy any agents to leverage Active Directory authentication for the McAfee Web Gateway?
McAfee Web Gateway integrates directly into the domain and is seen by the Active Directory servers as a workstation within the domain.

Does the McAfee Web Gateway perform reputation and categorization only on the appliance?
McAfee Web Gateway will leverage the optimal configuration for performance. If the categorization or reputation is not available on the local appliance, the Web Gateway has the ability to query global threat intelligence for further reputation and categorization information.

Does the McAfee Client Proxy work when behind Wi-Fi hotspots or captive portals?
The McAfee Client Proxy is designed to work in such conditions. It allows the user to login to the hotspot or hotel Wi-Fi registration system before redirecting traffic to a hosted McAfee Web Gateway.

Additional Resources

www.mcafee.com/webgateway
www.mcafee.com/webreporter
www.mcafee.com/epo
www.mcafee.com/producttrials
www.mcafee.com/kb

About the Author

Jon Paterson is part of the enterprise solutions architecture team in the network business unit at McAfee, consulting with the largest customers globally to find solutions to web and email challenges. Jon is also an avid security and malware researcher. Jon holds several industry certifications including CISSP and SANS GIAC incident handler and reverse engineering malware certifications.

McAfee
An Intel Company

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

41800bp_encrypted-web-L3_0212_ETMG_fnl