Mobile Device Web Filtering

Use McAfee® Web Gateway and McAfee Enterprise Mobility Management to filter web content on mobile devices.
Table of Contents

Introduction .................................................................................................................. 3
McAfee Web Gateway ................................................................................................. 3
McAfee EMM Software ............................................................................................... 3
  Use cases .................................................................................................................. 4
  Mobile devices ......................................................................................................... 4
  Web traffic ............................................................................................................... 7
  Non-web traffic ........................................................................................................ 8
Authentication ............................................................................................................ 9
  Mobile browsing ..................................................................................................... 11
  Mobile applications (apps) ...................................................................................... 12
Summary .................................................................................................................... 13
Introduction
Mobile devices, such as smartphones and tablets, proliferate in today's corporate environments. While there are significant opportunities to leverage these devices to increase the effectiveness of mobile workers, there are also significant concerns about the privacy of sensitive corporate data stored on the devices. Corporate IT organizations are not so much worried about the threat of losing the device, likely owned by the employee, but the threat of a targeted attack stealing sensitive corporate data stored on these mobile devices. As a first line of defense, an increasing number of companies rely on mobile device management software and web filtering.

This paper will explore ways to implement web filtering of mobile devices through McAfee Web Gateway and discuss ways that McAfee Enterprise Mobility Management (McAfee EMM™) software can be leveraged in an integrated manner to assist with web filtering.

The focus is to explore use-cases as it relates to mobile devices such as Apple iPad/iPhone using iOS 6, with some information regarding various versions of the Android operating system. However, most of the topics apply to PCs as well.

McAfee Web Gateway
McAfee Web Gateway is an industry-leading product used in the enterprise to provide:

- URL filtering.
- Anti-malware.
- Data loss prevention (DLP).
- Application control.
- Secure sockets layer (SSL) scanning.
- Authentication.
- Web caching.

McAfee Web Gateway has always been able to perform this filtering on web traffic no matter what device connects to it—desktop, mobile, or otherwise.

McAfee EMM Software
McAfee EMM software is used to protect mobile devices and data.

McAfee EMM software can be leveraged to provide access to the assets by:

- Defining wireless access points.
- Defining VPN settings.
- Defining APNs.
- Defining proxy settings on iOS.
- Defining connection to email.
- Defining X509 certificates for user/device for authentication to wireless/VPN/proxy.

McAfee EMM software also has a variety of other features for the management of devices and applications. This paper limits the discussion to only that of web filtering—not all of the McAfee EMM software capabilities possible.
Use cases
The two most requested use cases where mobile device web filtering is desired are in the BYOD in the enterprise and a completely managed environment. This document will discuss web filtering in both of these environments.

*Bring your own device (BYOD)*
The BYOD scenario is where an enterprise infrastructure exists and employees are able to use their personal devices to use corporate infrastructure assets. These assets might include the internal wireless network, intranet web servers and applications, Internet access, and corporate email.

These devices could also be company-owned, but issued to users for individual use. That is, one device per person.

*Managed environment*
In the managed environment scenario, devices are typically owned by the organization and shared among users. These may be for shared use in a classroom, single-purpose applications like PoS, Kiosks, or other captured usage. The assumption is all traffic from these managed devices must be filtered at all times.

*Mobile devices*
Much of the challenge with filtering web traffic on mobile devices has been the ability to get the traffic to the filter. The most common method of intercepting web traffic on PCs is with explicit proxy. Explicit proxies have long been supported by the operating systems, browsers, and some applications as a formalized way to connect to the web. Generally speaking, the majority of web traffic can be explicitly proxied with only some minor configuration to the host. However, not all applications will honor the proxy method and will have to be considered in the overall implementation.

Mobile devices have had spotty support for proxies at the operating system and application level. Some operating systems support it globally per device; others only support it per connection (wireless, VPN, or APN). Application support for the operating system's proxy setting is dependent on the application developer.

Another popular technique is by using protocols such as WCCP on Cisco equipment. This can intercept all HTTP/HTTPS traffic and force it through a gateway in a transparent manner. Challenges with this method are introduced when you try to instantiate authentication or SSL decryption/scanning. These challenges are not specific to mobile devices, but to any host or application that doesn't recognize the interception and redirection of the web traffic where none is expected.
Apple iOS Global HTTP Proxy

iOS 5 and below only had settings for per-wireless connection, VPN connection, or APN connection. This can be defined manually in the connection setting itself.

iOS 6 has per-connection settings, but also has a new Global HTTP Proxy setting. This setting is used globally on the device and, when activated, disables the per-connection settings.

Supervision mode

In order to activate Supervision mode, the Apple Configurator 1.2 software must be used. This software only works on Mac OS X 10.7.5 or later.

Things to note:

- The device must be tethered to the configurator computer via USB, and once the device is supervised, it cannot be connected to any other computer to sync or backup with iTunes.
- Enabling Supervision Mode will erase the device’s entire configuration.
- Despite the restrictions imposed by the Apple Configurator software, there is nothing that prevents a user from resetting and erasing all content and data, including the supervision profiles.
- This feature is best used in a managed environment and not recommended for BYOD.

Once Supervision Mode is activated, either Apple Configurator or McAfee EMM software can change the Global HTTP Proxy Settings.
Figure 2. Apple Configurator: Global Proxy Setting.

Figure 3. McAfee EMM Software: Global Proxy Setting.
Web traffic

Explicit proxy settings
Both iOS and certain versions of Android have some sort of proxy settings.

iOS has two types of settings: Manual and Automatic. These can be assigned either globally or on a per-connection basis like the wireless or VPN setting. As previously noted, Global Proxy settings apply to all HTTP traffic on the device. When the global settings are active, the per-connection proxy settings are unavailable.

Manual settings specify the IP address or FQDN and port number of the proxy and, optionally, the user name and password. Manual settings cannot specify exclusions to proxying. All applications that honor the proxy setting will be forced through the proxy, including internal web traffic.

If the username and password are left blank in the setting itself, the user will be prompted to supply them if the proxy requires them (see “Authentication”).

Automatic settings specify a URL where a PAC file can be located. If used, the automatic settings cannot specify a username/password. Automatic settings can be used if you need exclusions to proxying. PAC files can be formed so that specific destinations can be bypassed, typically internal addresses, hosts, and domains.

If Automatic is specified, but no value is entered into the URL, then Windows Proxy Automatic Detection (WPAD) is enabled. At that point, the device first queries DHCP for option 252, then if that fails a DNS lookup of wpad.domain.tld (where domain.tld is the search suffix assigned by the DHCP server), it goes direct if neither of the first two queries produces results.

Because username and password cannot be specified with the automatic method, the user will always be prompted for credentials when accessing the network for the first time (see “Authentication”).

Android support for explicit proxy settings is dependent on the version of the OS, device manufacturer, cellular carrier, and support in the application. Early versions of Android had little or no support for proxies. Version 3.1 (Honeycomb) was the first to introduce proxy support on wireless connections. Settings are manual and allow you to specify an IP Address/FQDN and port of the proxy, but also provide ability to enter bypass setting to prevent proxying of internal hosts. Username and passwords are not assigned in the proxy settings and will be prompted within the application that uses the proxy.

McAfee EMM software is able to specify and manage proxy settings on iOS mobile devices, but the capabilities of Android do not permit for the remote management of proxy settings. They must be entered manually by the user.

Transparent proxies
Although the recommended way to do web filtering is typically through explicit proxy, other methods exist that can transport web traffic through a proxy. The most common way to do this is via the WCCP protocol present on most Cisco firewalls and core routers. Other methods to accomplish similar results are via transparent bridging/routing on the McAfee Web Gateway itself or some sort of layer 2 redirection from a load balancer or policy-based routing. When using one of these methods, web traffic is intercepted by a routing device or McAfee Web Gateway is placed in line with the route of web traffic.

By using transparent proxies in such a manner, settings are not required on the device (mobile devices or PCs) to redirect the web traffic, but challenges are introduced with authentication and SSL scanning when you use any form of traffic interception. It is an invalid assumption that transparent proxying is completely “touchless” to the device. If using SSL Scanning, a trusted certificate authority must be installed on the device. McAfee EMM software can assist in this for managed devices.
Captive portals
Captive portals use techniques to force a device on a network to display a special web page before using the Internet. These are common on public Wi-Fi hotspots, hotels, and enterprise guest wireless networks. When a device has a hard-coded proxy setting that cannot be changed by the user, access to the hotspot is prevented. This is because the device's browser is used to access the portal web page, but the proxy setting is trying to redirect all web traffic through the web filter and the web filter cannot access the portal.

iOS has some provision to detect captive portals, but it does not interact properly with proxy settings, thus preventing portal access when proxies are enabled.

Using iOS-supervised Global HTTP Proxy setting prevents connection to most captive portals. The Global HTTP Proxy setting should typically only be used when the devices are only allowed to connect to an internally maintained Wi-Fi network. An example of this would be shared student devices that are not allowed to leave campus or PoS devices that are not allowed to leave the premise.

Non-web traffic
Web traffic is defined as HTTP or HTTPS protocols. These typically use TCP ports 80 and 443, respectively, but can arbitrarily use other TCP ports. Although the majority of traffic on a mobile device is HTTP protocol, not everything is.

Traffic that is not web traffic includes FaceTime, Skype, AirPlay, FTP, RDP, SSH, or POP/IMAP/SMTP email. These cannot be proxied or filtered by a web filter because they are not truly web protocols that use HTTP or HTTPS.

Also, even if the network is using port 80 or 443, that does not mean it's actually HTTP or HTTPS protocol. Some applications expect these ports to be open and attempt to use them without regard to the formal protocol specifications.

Further, it is common for some traffic on port 443 to appear as HTTPS, but when the SSL is decrypted, it does not conform to the HTTP protocol inside. These types of connections may be transported but cannot be SSL scanned and must be bypassed in a whitelist.
Authentication
When web traffic is being filtered, it is usually desirable to know the identity of the user or device. By knowing the user, policy decisions can be made to allow or deny certain types of traffic. For example, teachers may be able to use webmail, while students may not.

There are a number of techniques used to authenticate users, as shown in the following table (see Table 1 below).

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Authentication</td>
<td>When using explicit proxies, a formalized process within the HTTP protocol is defined to ask the browser for credentials. Technically, the proxy returns a 407 status code to the browser to inform it that authentication is required, hence the term &quot;407 Auth.&quot;</td>
<td>Credentials are stored separately for HTTP and HTTPS, so even though credentials are saved for the HTTP site, when a user goes to an HTTPS site for the first time, they will be prompted again. Once they are entered, they will be saved as well for future use.</td>
<td>It may be a challenge to switch users on a device, if needed, because save credentials are not prompted for afterwards.</td>
</tr>
<tr>
<td>Try-Authentication</td>
<td>When using Proxy Authentication (407 Auth), it is often desirable to attempt authentication, but if there is no user in the directory, allow it to proceed anyway. This method of attempting to authenticate, but accepting whatever credentials are offered is called Try-Auth.</td>
<td>Try-Auth is generally best used in a guest environment with a minimal policy applied. Do not use Try-Auth on any Internet-facing proxy. This will effectively turn it into an anonymous open proxy for the world to use since any username that is entered will be accepted.</td>
<td>Try-Auth may have the unwanted side effect of disabling a user's account because invalid credentials could be presented too many times and cause multiple authentication failures and account lockouts.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>McAfee Web Gateway has other built-in methods to identify users. These are commonly used when traffic is being transparently redirected via a method like WCCP, but may also be used with explicit proxying as well.</td>
<td>The advantage to using the Authentication Server is it provides alternative methods for transparently redirected traffic where 407 Auth cannot be used. Most web browsers will be able to process the 302 redirects to McAfee Web Gateway, authenticate, and redirect back to the original URL without any noticeable effect on the user.</td>
<td>The disadvantage is that apps and other non-web browser user agents will not understand the redirection and will usually fail to operate properly.</td>
</tr>
<tr>
<td>Time/IP-Based</td>
<td>When Time/IP-based is used, McAfee Web Gateway authenticates and identifies the user and sets a timer for the client IP address. All traffic coming from that client IP during this period is associated with that user.</td>
<td>Once the authentication has occurred, there are no further interactions with the client until the timer expires.</td>
<td>The disadvantage to using this method is when multiple sessions are coming from a shared IP address, such as from behind a NAT router or behind a Wi-Fi hotspot, the proxy cannot distinguish among the clients and will not be able to apply user-specific policy.</td>
</tr>
<tr>
<td>Cookie-Based</td>
<td>When Cookie-based authentication is used, the client is redirected to McAfee Web Gateway and it sets an encrypted cookie in the browser session after the credentials have been validated. This occurs once for each site (host name) that is visited because cookies are set on a per-site basis.</td>
<td>Cookie-based authentication is best used on browser-only traffic.</td>
<td>Cookie-based authentication is not very effective with mobile devices where the majority of traffic is application based.</td>
</tr>
</tbody>
</table>
### Authentication Type

#### Form-Based
When Form-based authentication is desired, a user is redirected to a browser form with fields to enter username and password. These credentials are posted back to the proxy, validated, and the user is allowed to proceed.

**Advantages**
- Using Form-based logon is a convenient way to allow shared devices to explicitly prompt for credentials after a period of time, like a classroom teaching period.

**Disadvantages**
- There is no way to log off. Once you are logged on, the time must expire in order to de-authenticate.

#### Authorized Override
Authorized override is intended to provide temporary access to a blocked site for short periods of time. It presents a block page to the user when they access a site that is not allowed, but the block page also includes form fields for entering the username and password of a user that does have access to the site.

**Advantages**
- Once credentials are entered, surfing to that site can continue for a short period of time.
- Credentials could potentially be OTP-based.

**Disadvantages**
- If the expiration time is set too short, the block page re-prompts before continuing and may interrupt an existing session.

#### Credential Validation
While the above authentication techniques describe characteristics of interaction between the device and the proxy, it doesn't describe how credentials are validated with the proxy itself.

**Advantages**
- Generally speaking, McAfee Web Gateway may use a variety of authentication methods to validate credentials. On mobile devices, the available methods include NTLM, User Database, LDAP, X509 client certificates, and RADIUS.

**Disadvantages**
- There are other methods McAfee Web Gateway can use, like Kerberos and Novell eDirectory, but those are not possible with mobile devices because they rely on membership to the domain, and mobile devices are not capable of doing that like PCs are.

#### NTLM
In a Windows network, NTLM (NT LAN Manager) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users.

**Advantages**
- Most popular browsers on most operating systems support NTLM, the encrypted challenge/response method used to securely pass credentials.

**Disadvantages**
- On non-Windows hosts like OS X, iOS, Android, and Linux, you will always get prompted for credentials. You may have to remember passwords in the browser to suppress future prompting.

#### X509 Client Certificates
McAfee Web Gateway has features that allow the proxy to use X509 certificates issued to the user or device in order to authenticate and authorize web traffic. McAfee EMM software can integrate with an organization’s Active Directory Certificate Authority to authenticate, enroll, install, and use client certificates on mobile devices. These certificates may then be utilized for authentication and identification on the McAfee Web Gateway.

**Advantages**
- (See “Time/IP-based advantages.”)

**Disadvantages**
- Client Certificate enrollment is not supported by any MDM solution on Android platforms, only iOS.
- (See for “Time/IP-based disadvantages.”)

#### SSL Scanning/Decryption
One of McAfee Web Gateway’s strongest features is the ability to securely intercept HTTPS-encrypted traffic for scanning. This is primarily used to prevent the transmission of malware, sensitive information, and web application control.

**Advantages**
- In order for SSL scanning to occur, McAfee Web Gateway acts as a Certificate Authority (CA) to regenerate web certificates for the intercepted sites. The McAfee Web Gateway CA certificate must be installed and trusted in the device’s key store to prevent warnings from occurring from an unrecognized certificate. The CA certificates can be installed on the device either manually or using McAfee EMM software for device management.

**Disadvantages**
- Not all web browsers and web applications will use the certificates in the iOS key store. Some browsers and applications maintain their own list of trusted CAs and will not operate properly if alternative certificates are presented. This usually results in the necessity to whitelist traffic from SSL Scanning to the various destinations they communicate with.

---

**Table 1. Authentication techniques.**
Mobile browsing
The native web browser built into iOS is the Apple Safari browser. It comes standard across all of Apple's platforms. However, alternative browsers are available for iOS devices from the Apple App Store, most notably Google Chrome and Opera Software's Opera Mini. These alternative browsers offer additional features over Safari but don't behave completely the same with the operating system and can create some problems with the user experience.

Safari
Apple Safari is the standard browser native to iOS. It has deep integration with most all iOS components, including the proxy settings and certificate key stores. It is the most compatible browser for use with the various proxy and authentication methods.

- **Explicit Proxy**: Yes. Safari honors and uses the HTTP Proxy settings that are set either globally or per-connection.
- **Transparent Proxy**: Yes.
- **SSL Scanning**: Yes. The trusted CA certificate stored in the iOS key store is used with SSL Scanning.
- **Authentication**
  - **407 Auth**: Yes. Safari prompts user for credentials first, but stores them on its keychain for future use.
  - **NTLM**: Yes. Safari will encrypt credentials for presentation to the proxy.
  - **X509 Authentication**: Yes. Client certificates in the iOS key store will be presented to the authentication server.
  - **Cookie Authentication**: Yes. Accept Cookies>Always must be set in the Safari settings.
  - **Try-Auth**: Yes.

Google Chrome
Google Chrome is a popular alternative browser for many OS platforms like Android, Windows, Mac, and Linux. However, the iOS version does not have complete functionality as it does with other platforms because of constraints placed on it by Apple. In essence, Chrome is using the AppleWebKit engine that Safari uses with a few more front-end features, but lacking some key components that inhibit its functionality with a proxy, especially with authentication and SSL scanning.

- **Explicit Proxy**: Yes. Chrome honors and uses the HTTP Proxy settings that are set either globally or per connection.
- **Transparent Proxy**: Yes.
- **SSL Scanning**: Partial. The trusted CA certificate stored in the iOS key store is not used by the Chrome application. Any SSL-encrypted site will be warned by Chrome that the certificate is not trusted. Some sites that use Authority Information Access, like Google.com or Twitter.com, will not be able to access the site because of a presumed bug in Chrome for iOS AIA chasing capability.
- **Authentication**
  - **407 Auth**: Yes. Chrome prompts user for credentials first, but stores them on its keychain for future use.
  - **NTLM**: Yes. Chrome will encrypt credentials for presentation to the proxy.
  - **X509 Authentication**: No. Client certificates in the iOS key store will not be presented to the authentication server and thus cannot properly authenticate with X509 certificates issued to the device.
  - **Cookie Authentication**: Yes. Content Settings >Accept Cookies be set to yes in the Chrome settings.
  - **Try-Auth**: Yes.
Opera-Mini
Opera Software’s Opera-Mini is a popular alternate browser to iOS Safari. It has taken a different approach than Chrome in that it uses its own engine and doesn’t rely on iOS itself to provide core services. Because of this approach, Opera-Mini tunnels all of its network connections to opera-mini.net which, in turn, forwards it to the destination site. This method creates a problem with any kind of web content filtering in that the actual network connections are not HTTP connections to the destination website, but tunnel connections to its own network. By default, the tunneled connections are transported through a pseudo SOCKS-like connection on port 1080, but can be HTTP proxied. However, when proxied, they do not honor proxy authentication or any kind of filtering.

Opera-mini is not recommended for iOS mobile devices because it has no capability to be proxied, authenticated, content scanned, or policy enforced in any way.

Mobile applications (apps)
The majority of network traffic from a mobile device is not browser-centric, but originates from mobile apps. Apps come from various vendors and deliver a variety of functionality to the device. The ability to control and filter content for apps is entirely up to the developer’s discretion as to how the app interacts with the operating system and the network. Each app must be taken on a case-by-case basis to see what interoperability it may have with any filtering and control solution.

App proxy awareness
Well-behaved apps that use the HTTP/S protocols have the option to honor iOS proxy settings. When they do, there is a good chance that explicit proxy settings on the device will be able to authenticate, control, and filter content to the network. For apps that do not honor proxy settings, but still are using HTTP/S protocols, it may still be possible to filter content with transparent proxy methods like WCCP. Much of the filtering ability will be dependent on the app’s tolerance for SSL scanning and ability to authenticate using the authentication server.

App authentication
Well-behaved apps that recognize the proxy settings will generally be able to use 407 Auth. Whether the cached credential the browsers default to will be used is up to the application itself. Some will and not prompt the user for logon information, but many will prompt for the proxy credentials.

Non-proxy-aware apps will generally not be able to understand or use most forms of transparent authentication like Cookie Auth or X509 Auth. Usually, this is because the app won’t honor 302 redirection used by the authentication server. Using Time/IP-based authentication in the browser (with either credentials or X509 certificates) is a good alternative. In this scenario, a user would open the Safari browser, authenticate, and set a timer. Once set, the user can switch to the app and use it for the period of time until the timer expires. After expiration, the app usually ceases to function, and the user must switch back to the browser and repeat the process.

App network protocols
Not all network traffic from a mobile device is HTTP/S-based. Many apps use a mix of other protocols to perform their duties. Examples of non-HTTP/S apps would include FaceTime, Skype, Email, Streaming media, RDP clients, and others. Additionally, some apps may use a mix of web and non-web protocols. Often the logon and presentation of the app may be web-based, but the transport of the content is not. For example a streaming-media app may require web logon and ad content from the network, but audio or video data itself is not web-based. Many times, the web-based portion of the app may be filtered enough to prevent access to the non-web based portion of the content.
App SSL scanning
As previously described, HTTPS traffic has the opportunity to be SSL decrypted and scanned. Doing so requires trusting a CA that performs the decryption. Not all apps will use the trusted certificate authority key store and allow for this decryption and scanning. Many apps will embed the certificates within the app itself and expect HTTPS server to be signed by a specific CA.

Many of the Apple native apps behave in this manner. Apple iTunes, Apple AppStore, and Apple iCloud have specific CAs embedded in the app itself and will fail to operate if presented with an alternate certificate.

Summary
With companies becoming increasingly mobile, IT administrators have to balance their users’ desire to stay connected while maintaining mobile-device security and safeguarding corporate data. McAfee mobile-device management and web filtering helps reduce the risks of corporate data loss, unauthorized access, and business-data leakage from employee-owned devices.

About McAfee
McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security’s mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.