McAfee Client Proxy

Web Protection for users everywhere

Q. How does McAfee protect mobile workers when they are off the network?

A. We extend web security to users working outside the corporate network by redirecting web traffic from laptops to a McAfee® Web Protection solution—either McAfee Web Gateway Cloud Service or an on-premises McAfee Web Gateway—both part of the McAfeeproduct offering. We redirect off-network web traffic with McAfee Client Proxy.

Q. What happens when my mobile workers are in the office/on the network?

A. McAfee Client Proxy software is location-aware and recognizes its environment, whether inside the corporate network, connected to it by VPN, or external to it. To determine location, McAfee Client Proxy performs a TCP connect to the address of the McAfee Web Gateway or other network device. During the connect phase, McAfee Client Proxy initiates a test or a SYN toward the McAfee Web Gateway. If the McAfee Web Gateway acknowledges, McAfee Client Proxy stands down since the device is connected to the internal network. The client software intercepts the TCP connections but lets them pass to the original destination without modifying the traffic.

If there is no reply because McAfee Client Proxy is outside the network, it becomes active and redirects traffic to the designated McAfee Web Protection solution, most likely McAfee Web Gateway Cloud Service. McAfee Client Proxy can be configured to connect to the closest McAfee Web Gateway Cloud Service data center or the one with the lowest latency. Policy is managed centrally across McAfee Web Gateway and McAfee Web Gateway Cloud Service, enabling users off-network to receive the same level of protection as they would on-network.

Q. What type of traffic is redirected? Is any data or identification information attached to the traffic?

A. McAfee Client Proxy primarily redirects HTTP and HTTPS traffic. As it does so, the client software adds metadata to the request. Identification token, Microsoft Windows domain username, and the list of Windows Active Directory groups that the user belongs to are examples of metadata that is added and encrypted. McAfee Web Gateway and McAfee Web Gateway Cloud Service use this data to verify that McAfee Client Proxy is redirecting the traffic and to identify the user and transparently apply matching policy without requiring the user to authenticate. It also identifies protocols such as FTP

Connect With Us

and SNMP by port numbers and redirects this data, without adding any metadata to the traffic.

Q. How is McAfee Client Proxy configured and deployed?

A. McAfee Client Proxy is typically configured from McAfee® ePolicy Orchestrator® (McAfee ePO™) software. The client software can also be distributed to client computers with McAfee ePO software. Additional options are also available using McAfee ePO Cloud and Microsoft Systems Management Server (SMS).

Q. Can end users disable the McAfee Client Proxy and connect directly to the Internet?

A. A user cannot easily remove the software or bypass the traffic redirection without an administrator-generated security key. If managed with McAfee ePO software, the administrator can create and issue a bypass key, which is valid for a specified time period.

Q. What operating systems are supported?

A. Currently supported Windows operating systems and Macintosh OS X 10.8 and higher are supported.

Q. Do administrators create a separate web security policy for the McAfee Client Proxy?

A. McAfee Client Proxy software does not define or enforce a security policy. It defines when and how to connect to a McAfee Web Protection security solution. The security policy is defined and enforced by the security solution.

Q. What policy is defined with the McAfee Client Proxy?

A. McAfee Client Proxy policy can consist of the following:

- **Proxy server lists**: Proxy server locations to redirect traffic to such as McAfee Web Gateway Cloud Service or McAfee Web Gateway.
- **Bypass lists**: Domain names, network addresses, network ports, and process names that a user can connect to directly. These web destinations are considered safe and connecting to them does not activate redirection to a McAfee Web Gateway or McAfee Web Gateway Cloud Service solution. An example would be VPN software.
- **Block lists:** A list of applications or processes that are blocked immediately without being redirected. For example, an administrator could put non-corporate approved browsers on the block list. McAfee Client Proxy would forward traffic from approved browsers and block all traffic generated by browsers on the block list.

Q. How do customers get the McAfee Client Proxy software?

A. For McAfee Web Gateway/McAfee Web Gateway Cloud Service customers, it is available on the McAfee Cloud and Content Security Portal (https://contentsecurity.mcafee.com). For McAfee Web Gateway Cloud Service, it is also available through ePO Cloud.

TECHNICAL FAQ

Q. How much does McAfee Client Proxy cost?

A. It is available at no cost to McAfee Web Gateway and McAfee Web Gateway Cloud Service customers with active licenses.

Q. If an organization is only using McAfee Web Gateway Cloud Service, can the McAfee Client Proxy be used to direct all traffic—whether they're in the office or on the road?

A. McAfee Client Proxy can be configured to always redirect traffic to the McAfee Web Gateway Cloud Service solution, making the software active when users are both on and off the network.

Q. Does McAfee Client Proxy work in a captive portal situation—for example, when a user must input credentials at a hotel for Internet access?

A. McAfee Client Proxy remains passive until Internet access is available. When it is, McAfee Client Proxy will direct traffic to the appropriate McAfee solution.

Q. Do users have to interact with McAfee Client Proxy?

A. Users do not interact with McAfee Client Proxy. All location determination and traffic routing is done automatically.

Q. If I use McAfee Web Gateway Cloud Service for roaming users and McAfee Web Gateway appliances for network users, can I consolidate reporting?

A. McAfee Web Protection solutions use Content Security Reporter software to report on all web traffic. Content Security Reporter enables organizations to consolidate logs from McAfee Web Protection solutions, whether on-premises or cloud, and has a single, consolidated view into web traffic and use trends.

Q. McAfee Web Filtering for Endpoint (McAfee SiteAdvisor® Enterprise software) is offered for mobile users along with McAfee Client Proxy. Are there any advantages of using McAfee Client Proxy over McAfee Web Filtering for Endpoint?

A. McAfee Web Filtering for Endpoint provides URL filtering in addition to McAfee SiteAdvisor software's security ratings. McAfee Client Proxy provides tamper-resistant traffic redirection to McAfee Web Gateway and/or McAfee Web Gateway Cloud Service for full web policy enforcement, including URL filtering, proactive anti-malware, and granular web control.

Q. What technology does the McAfee Client Proxy replace, and what are the benefits of doing so?

A. Alternatives to the McAfee Client Proxy include technology such as proxy auto configuration (PAC) files, cookies, a browser plug-in, backhauling all web traffic through a centralized hub, or manually setting browser proxy settings.

These alternatives are typically browser-dependent and can be either modified or disabled by the user. Benefits include:

- A hardened client
- Tamper-resistant, so users cannot easily disable
- Browser independence
- Managed via McAfee ePO software
- Simplified transparent authentication
- One solution for both on- and off-network devices

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847 8766
www.mcafee.com

1761_0916
SEPTEMBER 2016