Solution Brief

McAfee Next Generation Firewall

Built-in SSL VPN

McAfee® Next Generation Firewall offers a complete suite of tools for securing network traffic between corporate campuses, branch offices, remote sites, and end users. In addition to unique McAfee Multi-Link capabilities and powerful management tools, McAfee Next Generation Firewall provides robust virtual private networking (VPN) technologies, including IPsec VPN and SSL VPN. The McAfee SSL VPN solution offers lightweight, fine-grained connectivity to remote and mobile enterprise network resources. Client-based and clientless SSL VPN alternatives enable customers to secure traffic across a wide variety of use cases. All of these powerful features are included with McAfee Next Generation Firewall, allowing customers deploy them as needed with no additional licensing costs.

Key Advantages

- Built into McAfee Next Generation Firewall.
- Client and clientless access options.
- Consolidated VPN management via McAfee SMC.

Powerful SSL VPN Capabilities

SSL VPN is often used to provide remote users with secure access to network resources from a variety of endpoints or client machines, including shared computers. Deploying dedicated SSL VPN appliances can solve the problem temporarily, but multiple appliances can be costly and difficult to maintain. McAfee Next Generation Firewall's built-in SSL VPN technology provides immediate operational and cost benefits by consolidating visibility of your VPNs and network security into a single centralized management system, McAfee Security Management Center (McAfee SMC). Additionally, McAfee Next Generation Firewall offers high availability and clustering features that enable in-service upgrades while maintaining full business continuity.

Our SSL VPN technology allows customers to enable secure connectivity to enterprise networks and other specific resources in two ways:

- Client-based access.
- Clientless (or portal-based) access.

Both of these options are native to McAfee Next Generation Firewall, whether physical or virtual appliance, with no specific licensing needs.

intel Security

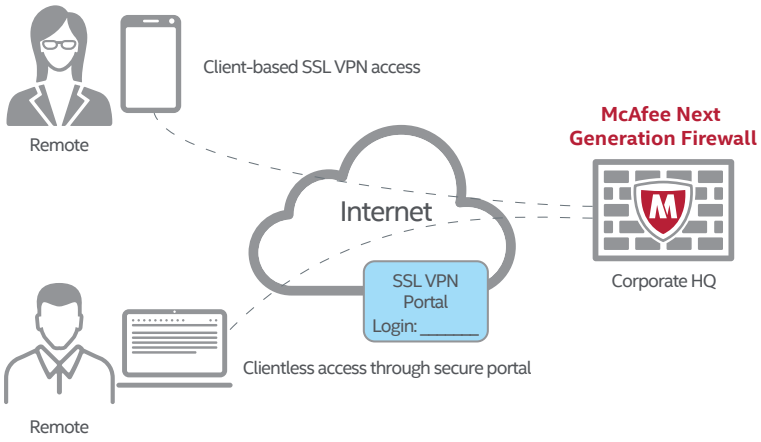

Figure 1. SSL VPN access options.

McAfee SMC provides full control of SSL VPN settings and related access policies, as well as SSL VPN portal customization. All VPN configurations, whether IPsec- or SSL-based, follow the same workflow, saving administrators time and headaches.

Client-Based Access from Multiple Platforms

Client-based access is a good fit for mobile remote users and supports leading client platforms including Google Android, Apple Mac, and Microsoft Windows. Client software versions are conveniently downloadable via their respective web stores.

Users are authenticated, for example, via external LDAP or RADIUS servers, which then provide the client with an IP address for SSL VPN tunnel setup. The Windows client, shared for both IPsec and SSL VPN, may perform additional local security checks before traffic is allowed. Local checks can ensure that additional security features, such as antivirus, host firewall, and Windows updates, are enabled. Administrators can allow or deny user access to applications and services by setting policies in the management console. As the SSL VPN tunnel transports IPv4 packets, the remote user can flexibly use services, which may be based on HTTP/HTTPS or other protocols. Administrators can also define preferred security levels by choosing from a variety of encryption algorithms.

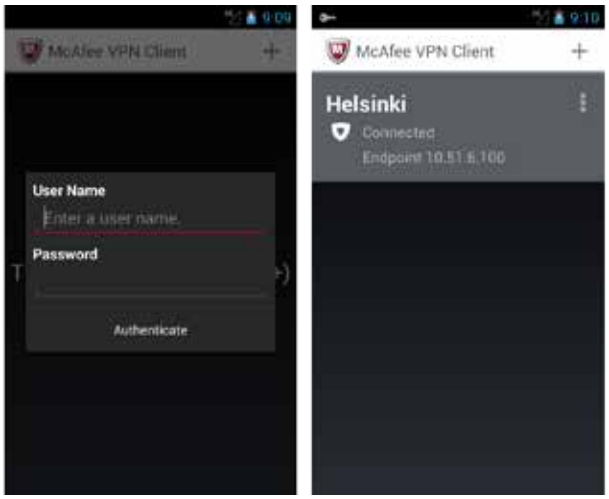

Figure 2. SSL VPN client login with Android device.

User-Friendly Portal-Based Access to Select Services

Clientless SSL VPN provides portal-based access so administrators don't need to install or maintain host clients. It also permits secure access from any operating system that can support a standard web browser, such as Firefox, Internet Explorer, Google Chrome, and Safari. Logging in from a home computer or an ad hoc location requires only a web browser and Internet connection.

Upon login, users are presented with a clearly organized portal of internal web applications or web-based email. The SSL VPN portal acts as a proxy between the user and the services—authenticating users, requesting pages from backend servers, and providing pages for clients.

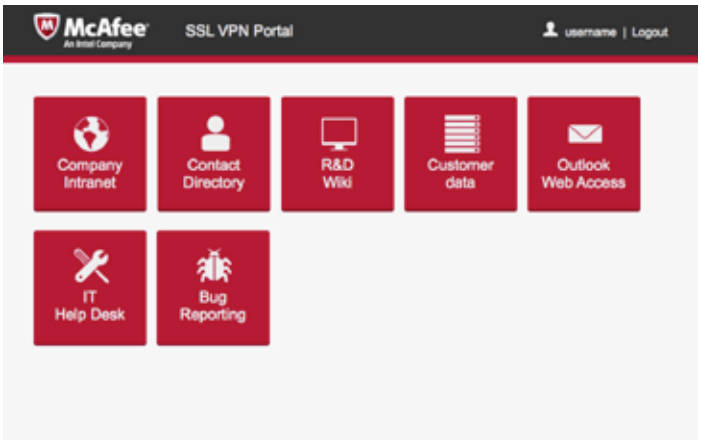

Figure 3. Example of SSL VPN portal.

Portal-based access provides an easy way for administrators to configure highly granular access to specific services for individuals or user groups. The look and feel of all SSL VPN portal configurations, including policies for user access and services, are customizable through the McAfee SMC.

Conclusions

McAfee Next Generation Firewall provides advanced, enterprise-grade protections, including AET prevention, application control, deep packet inspection, and robust VPN capabilities in a fully integrated, easy-to-manage security solution. Both IPsec and SSL VPN features are included with McAfee Next Generation Firewall as part of the standard license. Using either an SSL VPN client or clientless portal enables easy access for mobile users, as well as administrators.

	Client-Based	Portal-Based
Specific use cases	Personal mobile or other device	Application-specific use Access from shared computers
Accessible services	IPv4 based services	HTTP- and HTTPS-based
Platform support	Platform specific clients (Android, Mac, and Windows)	Any web browser
Granularity of access control to the services	Typically network level	Service URL, user identity, and group-specific

Table 1. SSL VPN access option comparison.

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