Know What’s on Your Network:
Deep Packet Inspection
McAfee® Next Generation Firewall

Data flowing across enterprise networks is susceptible to malicious intervention that can compromise those networks with disastrous results. Every application, email, web page, and Internet connection relies on the information encapsulated into a discernible packet that can be easily distributed across data networks. These packets include information about the sender and receiver, as well as the actual contents, or payload. By manipulating pieces of the packet data, criminals can infiltrate networks, applications, data centers, and individual computers.

McAfee Next Generation Firewall—part of the Intel® Security product offering—relies on deep packet inspection (DPI) capabilities to examine thoroughly the various pieces of each packet to identify errors, malformed packets, known attacks and other anomalies. The goal is to quickly identify viruses, Trojans, spam, intrusion attempts, and other violations of normal protocol communications that are then blocked. DPI also forms the basis for application control, user authentication, and quality of service functions.

McAfee Next Generation Firewall employs multiple means of analyzing packet data:

- Protocol identification and data normalization.
- Data stream-based inspection.
- Clear-text HTTP and encrypted HTTPS connections.
- Vulnerability signatures.
- Policy configurations and web filtering.

Key Advantages
Full protection
Protect vulnerable applications and operating systems from threats against client and server vulnerabilities.

Complete inspection capable
Uses protocol identification, normalization, and data stream-based inspection technology to detect and block threats in both clear-text HTTP and inside encrypted HTTPS connections.

Dynamic updates
Always up-to-date, vulnerability-based protection fingerprints and recommended policy configurations are updated regularly via dynamic updates. Administrators have the option to automate the entire process when needed.

Use across all next-generation firewall roles
Inspection can be shared between firewall, IPS, and layer 2 firewall roles.
Full Protection
Traditional firewalls and intrusion prevention systems are not enough to protect against these threats. Sophisticated inspection capabilities are required. McAfee Next Generation Firewall enables deep packet inspection to eliminate threats inherent in web traffic (HTTP/HTTPS) and open encrypted web traffic, and treats it with the same inspection as clear-text HTTP data, eliminating a critical blind spot in network protection.

Web Filtering
With this capability, you can allow or block users from accessing specific websites. The practice has become an essential one on enterprise networks, with the goal of blocking employees from accessing content that would be a detriment to their productivity or the company as a whole. Blocked sites may include those that threaten the security of the organization, have objectionable content, or are bandwidth-intensive enough to strain company resources.

Catch Advanced Evasion Techniques
Deep packet inspection also helps you defend against sophisticated anti-evasion techniques, typically used by well-resourced, motivated attackers to obtain access into protected networks and launch advanced persistent threats. Always up to date, this layer of protection is critical to stop emerging network-based attacks that can bypass most security solutions by distributing payloads across multiple protocols.

Application and User Control
DPI gives you full user and application identification and security enhanced with additional controls. Expand user groups, domain names, applications, TLS matches, URL categories, and zones. These elements are also available in logs, statistics, and reports, offering increased user and application awareness.