McAfee Next Generation Firewall
Botnet prevention

Millions of poorly protected consumer and corporate computing devices, such as PCs and mobile devices, have inspired hackers and criminal organizations to create botnets. A botnet is a collection of compromised Internet-connected hosts, or “bots” that are enslaved by a “bot-master” for criminal use, such as denial-of-service (DoS) attacks, spamming, espionage, and financial fraud. Bot-masters typically orchestrate botnet activity through centralized “command and control” (C&C) servers. The globally distributed and complex nature of botnets makes them very difficult to detect and eliminate. Thus there is a correspondingly strong need to protect both end-user hosts and enterprise networks against botnet infection. McAfee® Next Generation Firewall includes advanced anti-botnet technologies that detect and block botnet malware and communications.

1. Attacker infects endpoint devices with botnet malware to create bots.

2. Bots are typically controlled by a bot-master through a C&C server.

3. Bot master conducts spam, phishing, malware, DoS attacks, or sells illegal botnet services to others.

Figure 1. Botnet malware infects millions of hosts across the Internet for illegal purposes.
Discovering Advanced Botnets Requires Advanced Inspection Techniques.

Large, valuable botnets take time to set up, so bot-masters are continually seeking ways to delay discovery and extend their useful lives as long as possible. To this end, botnet creators use evasive tactics such as:

- Frequently changing the location and IP addresses of C&C servers.
- Communicating with botnets using “channel hopping” peer-to-peer protocols.
- Communicating with botnets using encryption and obfuscation techniques.

Combating these advanced techniques requires coordinated defenses that encompass both endpoints and networks. The Security Connected ecosystem provides tight integration and coordination of threat defenses across multiple security solutions, including McAfee® ePolicy Orchestrator® (McAfee ePO™) software on the endpoint and McAfee Next Generation Firewall on the network side. McAfee Next Generation Firewall goes beyond basic discovery capabilities, such as botnet signatures and reputation-based detection, to provide advanced in-line protection against botnet malware and attacks. Advanced protection methods include:

- **Full traffic normalization with botnet protocol decoding**: Defeats peer-to-peer and obfuscation techniques.
- **Decryption of botnet traffic**: Enables proper inspection.

**Inspection Efficiency Brings Speed.**

Inspection methods applied in an inefficient serial fashion can severely impact network performance. McAfee Next Generation Firewall combines multiple inspection technologies that focus on the most relevant botnet families to optimize botnet detection and traffic throughput. Combined botnet inspection technologies include:

- Botnet traffic decryption.
- Message length sequence analysis.
- Botnet fingerprint signature matching.

**Figure 2.** McAfee Next Generation Firewall combines multiple anti-botnet technologies
McAfee Next Generation Firewall anti-botnet technologies efficiently identify network traffic that carries botnet communications between C&C servers and bots. Incoming traffic is decrypted and examined in depth for known botnet communication characteristics, such as ports, protocols, and encryption keys. Once the obfuscation method or encryption key used by the botnet has been determined by reverse engineering, fingerprint signatures can be used to identify actual botnet-related messages.

Additionally, McAfee Next Generation Firewall performs message-length sequence analysis on TCP/UDP streams to identify known botnet family traits. Message-length sequence fingerprinting can be used to identify botnet C&C traffic, even when traffic is encrypted. Fingerprint signature matching is combined with decryption-based and message length sequence analysis detection methods to ensure accurate and efficient botnet traffic detection with minimal false positives.

### Table 1. McAfee Next Generation Firewall detects highly evasive botnets.

<table>
<thead>
<tr>
<th>Botnet evasive technique</th>
<th>Intel Security anti-botnet technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing C&amp;C server location and IP address.</td>
<td>C&amp;C traffic identification and analysis.</td>
</tr>
<tr>
<td>Peer-to-peer control channel.</td>
<td>C&amp;C traffic identification and analysis.</td>
</tr>
<tr>
<td>Obfuscated control channel.</td>
<td>Traffic decryption with botnet keys and message sequence analysis.</td>
</tr>
<tr>
<td>Encrypted control channel.</td>
<td>Traffic decryption with botnet keys.</td>
</tr>
</tbody>
</table>

**Full Visibility and Reporting Aids Detection.**

McAfee Security Management Center provides easy-to-use tools for administrators to specify inspection policies and view network events including detected botnets. Built-in reporting tools allow administrators to define botnets separately for use in standard or custom reports.

McAfee Next Generation Firewall can automatically download security updates, including botnet fingerprints, to ensure the best protection against the latest threats.

**Eliminate Protection Gaps.**

In addition to strong threat detection and advanced evasion prevention capabilities, McAfee Next Generation Firewall helps organizations eliminate security gaps and blind spots with advanced anti-botnet technologies. McAfee offers a complete suite of botnet detection solutions for network and endpoint.