Technology Brief

Preventing Sophisticated Attacks: Anti-Evasion and Advanced Evasion Techniques

McAfee® Next Generation Firewall

Networking communication protocols make it possible for the Internet to work. Unfortunately, criminals can use those trusted systems to obfuscate malicious data and penetrate your network defenses undetected. An advanced evasion technique (AET) is a method of delivering an exploit or malicious content into a vulnerable target so that the traffic looks normal and security devices will pass it through. By combining attacks using several protocol layers, these advanced evasions bypass most existing security solutions. McAfee Next Generation Firewall applies sophisticated analysis techniques specifically to detect this type of attack. After years of research and development, it is the only network security equipment that reconstructs the data stream, normalizing it to detect attempts at evasions. Signature and behavioral defenses are unable to keep up with the myriad attack modes of an evasion technique. Using full stack, multilayer traffic normalization, McAfee Next Generation Firewall has been successfully tested against more than 800 million AET variants.

McAfee Next Generation Firewall applies the following capabilities to detect and defeat AETs:

- Full stack, multilayer traffic normalization deconstructs and decodes packets.
- Stream-based data inspection and detection works better than individual packet inspection.
- Vulnerability-centric fingerprint detects exploits in normalized data streams.
- Evasions are removed and evasion characteristics logged in matching context.
- Continual process analysis looks at layers 2 through 7 and all protocols (TCP, UDP, and others).
- Provides low false-positive alerts and reports on advanced evasions.

Key Advantages

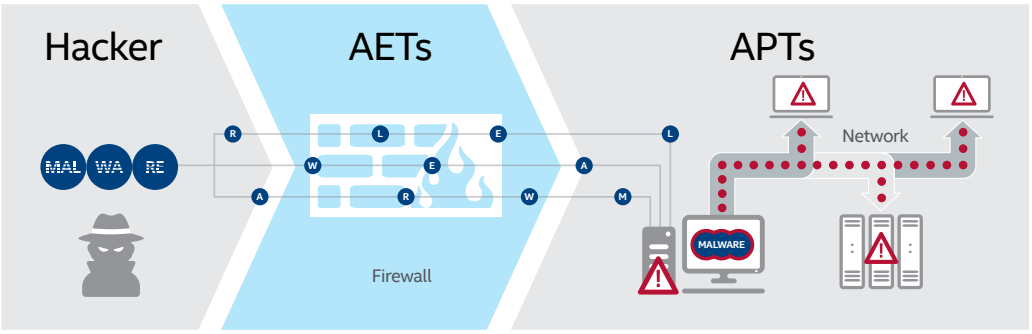
Included in all McAfee Next Generation Firewall products
AET protection is included in all McAfee Next Generation Firewall products at no extra cost.

No impact to throughput
By designing the inspection process right into the core of the product, data normalization and analysis does not affect performance.

Works in any configuration
McAfee anti-evasion technology adapts to physical, virtual, or hybrid network environments.

Free self-test lab
Find out how secure your company is doing with AETs by using our free Evader testing tool at **evader.mcafee.com**.

intel Security



Hackers apply AETs to disguise their attack, including splitting up malicious payloads into pieces, and sending them across multiple and rarely used protocols.

AETs are methods of disguise used to penetrate target networks undetected. Once inside, AETs reassemble to unleash malware and continue an (APT) attack.

Advanced Persistent Threats (APTs) are precisely targeted attacks on a business or political entity that require a high degree of stealth over a prolonged duration of operation in order to be successful.

Figure 1. McAfee anti-evasion and advanced evasion techniques.

Data Normalization for True Evasion Identification

A thorough and comprehensive data normalization process is the most effective way to protect networks from AETs and other threats that may otherwise disguise themselves and be undetected. Data normalization is the process of intercepting and storing incoming data so it exists in one form only. This eliminates redundant data and protects the data's integrity. McAfee Next Generation Firewall ensures that evasions are removed through the normalization process before the data stream is even inspected. This normalization is successful because it combines a data stream-based approach, layered protocol analysis, and protocol specific normalization at different levels. It helps fortify a network's three weakest points—traffic handling, inspection, and detection.

Figure 2. Full traffic inspection across all layers of the OSI.

Full Stack Inspection

Traditional security defenses try to optimize throughput and performance by relying on partial inspection of normalized data. For more accurate detection, it is necessary to analyze and decode the data layer by layer. Since the attack may be obfuscated by evasions at many different layers, normalization and careful analysis must be carried out on the appropriate layer. McAfee Next Generation Firewall decodes and normalized traffic on all protocol layers, giving you full stack visibility for maximum detection accuracy. And there is minimal performance impact.

Only Available with McAfee Next Generation Firewall

Most security vendors still rely on an exploit-based approach relying on packet-oriented pattern matching. These are significantly more vulnerable to evasions and pose a concrete risk and long-term security liability. The fact is, it is impossible to create signatures for every evasion combination.

Free AET Test Lab

Find out how well your network is prepared to defend against AETs using our free McAfee Evader tool. The Evader test lab launches controlled AET attacks against your network security device to deliver an exploit to a target machine. See how well your existing defenses can identify, log, and prevent a variety of AET attacks. Download it at **evader.mcafee.com**.

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