Seven Key Features to Help You Stop Advanced Evasion Techniques at the Firewall

by Binh Phan, Senior Security Architect, McAfee

Computer networks are built to facilitate the flow of communication, not stop it. Unfortunately, data packets can be manipulated to look normal yet contain an exploit. These techniques evade standard security measures and, in most cases, can deliver a malicious payload without detection. Often, these advanced evasion techniques (AETs) take advantage of rarely used protocol properties in unexpected combinations. Most network security devices are not capable of detecting them. While many pass industry tests with high ratings, those ratings are based on protection against a limited number of threats. The exact number of AETs is unknown, but it is close to hundreds of millions.

To defend against AETs, your network security should incorporate seven critical features.

1. Dynamic Security Updates

One of the most significant challenges for every enterprise is keeping up with the threat landscape. The current thinking is that being proactive, not reactive, is the best strategy. Unfortunately, this can easily exhaust your security operations team. The only solution is advanced threat intelligence that researches and updates your organization continuously with new responses to threats that are automatically pushed out to all locations (including remote locations), without the need for physical access.

2. HTTPS/TLS Inspection

HTTPS uses the transport layer security (TLS) protocol to encapsulate HTTP connections, providing what is generally believed to be a secure means of communication. That security goes out the window when that same encrypted connection is used to hide malicious traffic. HTTPS/TLS inspection lets you inspect TLS connections the same way you inspect unencrypted traffic. This is a must-have feature for protecting your network from both incoming and outgoing TLS connections.

Look for integrated HTTPS/TLS inspection as a feature of your next-generation firewall. Make sure it maintains an acceptable level of performance when this is running. This inspection component also gives you an automatic means of thwarting possible attacks over your secured web services, a growing component of most new regulations for transactions.

3. Data Normalization and AET Readiness

Normalizing data traffic 100% and then activating evasion detections once all data is normalized as a constant stream is critical to protecting your business from the growing number of AETs. Testing for evasions using data snapshots instead of streams is not sufficient, and neither are solutions that have limited visibility to data packets or pseudo-packets where evasions can remain invisible. Missing any evasion type opens the door for a hacker to use an entire class of exploits to get around security products, basically making them useless. Old-school devices may instead use security shortcuts to optimize throughput performance, providing only partial normalization and inspection and putting your entire network at risk.

4. Full Stack Inspection

When the only focus is performance and price, the easy way to win is to sacrifice your level of security. Packet inspection is not enough. The traffic must be normalized, and the full stack must be analyzed to identify threats. Full stack inspection instead decodes and normalizes traffic on all protocol layers, giving you full-stack visibility

and maximum detection accuracy. Application-specific normalization broadens the coverage to higher layers while your network maintains its high level of overall performance.

Most next-generation firewall products still rely only on signatures and pattern matching using non-normalized traffic. Since the number of possible evasions is in the hundreds of millions, this approach does not work. To be sure you are protected, ask your current security vendors about how they plan to stop AETs and what techniques they are using. Then test using freely available tools such as Evader, now available from McAfee. (Download at www.mcafee.com/evader.)

5. Evasion and Anomaly Detection and Reporting

You can't protect what you can't see. It may seem obvious, but constant awareness of real-time threats requires strong reporting on what is being detected, logged, and acted upon. Large enterprises require more than just standard reports. Visualizations of users, servers, networks, threats, responses, bandwidth usage, application usage, and anomalies give your network security operations team the ability to see pending issues and act quickly.

6. Unified Software Core

If your enterprise is still relying on a hardware-based or blade-based solution, keeping up with the rapidly evolving threat landscape can be both costly and difficult. Expensive, forklift upgrades may be your only option when attempting to keep up with emerging threats or the latest feature upgrades.

Switching to a security solution that features a unified software core provides the flexibility to quickly and easily scale to your needs. Relying on a software solution further enables you to respond to new requirements and implement new features in a shorter deployment timeframe. An additional advantage is the ability of the functions to communicate with each other to optimize overall performance.

7. Endpoint Protection

Keeping your endpoints protected against advanced threats is as vital as keeping your network protected. One of the most critical aspects of endpoint protection is the ability to move beyond the typical range of threats and defend against emerging threats. Superior endpoint protection will do exactly that, working on all endpoints, including ever-evolving mobile devices and virtualized environments.

About the Author

Binh Phan is currently a senior security architect at McAfee, where he helps customers design and implement security solutions to protect their critical infrastructures. Phan has more than 16 years of experience in IT and holds a master's degree in management in information technology and numerous industry certifications, including ISC2 CISSP, SANS GCIH, and Cisco CCIE.

60792brf_7-features-aet_0114_fnl_ETMG

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com