The Roadblock for Malicious Traffic

Peter Silva, 2016-07-03

I am sure you are aware, the business computing environment is evolving. From all of us and the multitude of devices we now carry and interact with, along with the various ways we access information…to all of the applications and the interdependency among those applications that we request information from…to the infrastructure needed to secure those applications and information being delivered to us. Maintaining security throughout is a challenge.

In a business environment, security is all about risk: Assessment, analysis, management and mitigation. The many IT security trends like IoT, cloud, device proliferation, disappearing perimeter, and so forth are all potential risks to the business. To reduce their risk, organizations need to ensure they can scale to meet the global workforce's and customer's data demand; they need to secure their data from targeted attacks, unauthorized access, inadvertent leakage or to comply with regulatory rules; and they need to keep their operational infrastructure simple and efficient.

The BIG-IP platform offers the scale and capacity to meet the deluge, the full proxy security to protect the applications and infrastructure and the operational efficiency to consolidate functions within an application centric security model. The BIG-IP platform is a full proxy architecture – establishing a TCP connection with the client to the BIG-IP and a separate TCP connection from the BIG-IP to the resources themselves. It is able to apply policies on both ends, anywhere along the stack. This allows organizations to inspect, manipulate or simply drop traffic – on the way in or on the way out - if it does not adhere to the policy. Plus, iRules extensibility gives you the power to do almost anything with the traffic.

BIG-IP Advanced Firewall Manager (AFM) is a stateful, full-proxy, ICSA-certified firewall and brings additional network firewall capabilities at a fine granular level allowing administrators to easily protect their infrastructure and understand what types of attacks are infiltrating the network. Logging and reporting are built-in. BIG-IP AFM can be added to any BIG-IP platform and can help reduce those business risks.

Bringing together security and deep application fluency, BIG-IP AFM delivers the most effective network-level security for enterprises and service providers alike. Whether on-premises or in the cloud, BIG-IP AFM tracks the state of network sessions, maintains application awareness, and mitigates threats based on attack details that most traditional network firewalls simply do not have. It helps you respond to threats quickly and with a full understanding of your security posture. In addition, AFM protects your organization from the most aggressive DDoS attacks before they ever reach your data center.

F5 DevCentral has a whole AFM series coming your way over the next few weeks! The schedule includes:

- **March 15th**: Foundational / Provisioning – This will kick of the series, taking what John tackled in AFM Provisioning and Policy Building and fleshing out more of the finer details in provisioning and basic policy functionality.
- **March 17th:** Architectural Context – We'll dive deep into the architecture to define global and local contexts, work through precedence decision trees, and introduce the programmability entrance points.
- **March 22nd:** Policy Building – Harder, stronger, balanced and more flexible policies to combat all those bad actors out there! Lessons learned and best practices will help you wield a more powerful weapon in the battle.
- **March 29th:** DDoS Capabilities: AFM shines with DDoS mitigation. You'll see the many attack vectors handled auto-magically for you, as well as walk through some demos of attack mitigations in action.
- **March 30th**: Blacklisting Magic - As the title says...
- **March 31st:** IP Intelligence - Blocking bad actors at the core.
- **April 12th:** Full stack protection – Where does AFM end and ASM begin? You'll see how these two modules complement each other and provide synergistic protection for all layers of your application and delivery infrastructure.
- **April 14th:** iRules extensions - Programmability to help stop those tricky attacks.
- **April 19th:** DNS firewall deployments - We'll show you how to make one mighty powerful firewall for your DNS

infrastructure.

Stay tuned for more insight on how to protect your critical infrastructure.

ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com