F5 BIG-IP AFM INTRUSION PREVENTION SYSTEMS

AFM IPS SUPPORTED PROTOCOLS (LIST SUBJECT TO CHANGE)

- CoAP
- DHCP
- Diameter
- DNS
- FTP
- GTP
- HTTP
- IMAP
- IPSEC
- IRC
- MQTT
- MYSQL
- NETBIOS_NS
- NETBIOS_SSN
- NNTP
- Oracle
- PFCP
- POP3
- RADIUS
- RDP
- RSH
- SMTP
- SNMP
- SS7
- SSH
- SSL
- SUNRPC
- TELNET
- TFTP
- WINS

CHALLENGE

Service provider and enterprise networks operate using a number of different protocols that enable connectivity to a large number of applications. Most of these networks operate on legacy protocols that have weak or non-existent built-in security, and which can be exploited by an attacker to impact services or steal information. For service providers delivering 5G-based services, the new 5G architecture introduces exponentially more new entry points into network infrastructure. To deliver an experience that meets customers' expectations in a competitive marketplace, protecting the networks is a must.

A FLEXIBLE, MODERN PROTOCOL INSPECTION SOLUTION

F5 intrusion prevention system (IPS), natively a part of F5® BIG-IP® AFM, performs Layer 5-7 inspection of all incoming traffic and protects more than 25 protocols and infrastructure applications against security incidents and exploits. BIG-IP AFM's IPS reviews traffic for adherence to protocol standards, matching it against hundreds of known attack signatures. It protects DNS infrastructure against protocol attacks and exploits that can impact performance. For service providers, BIG-IP AFM IPS does even more, protecting the network edge and performing traffic inspection and protocol adherence for prevalent service provider protocols such as SS7, Diameter, HTTP/2, GTP, SCTP and SIP traffic coming into the network over UDP, TCP, and SCTP. The system ensures that these application services are not attacked or exploited.

The threat landscape becomes even more challenging when you consider the millions of IoT devices sold each year which connect to consumer and business networks. Many of these IoT devices have weak, or even no, security. This makes them targets for hacking, adding them to attack networks. BIG-IP AFM IPS inspects the widely used IoT protocols MQTT and CoAP to mitigate attacks on IoT services servers.

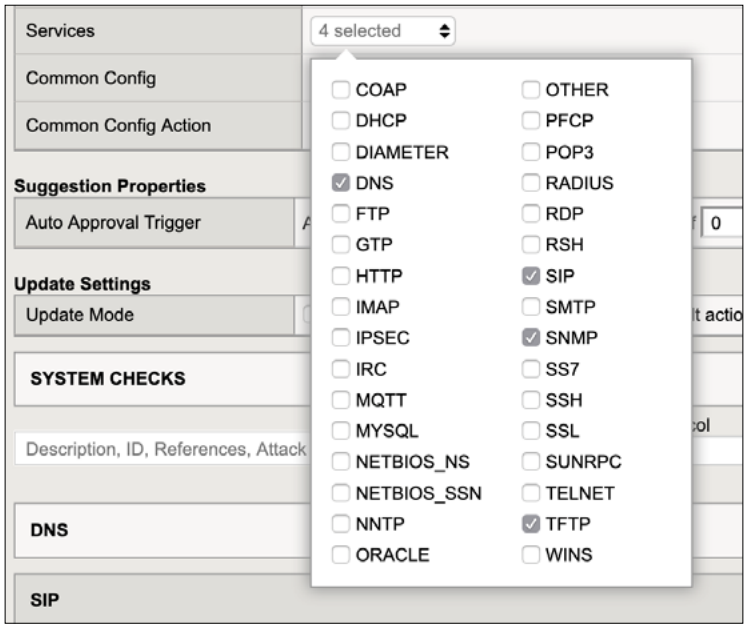

FIGURE 1: The simple GUI enables fast instantiation of IPS services to secure network services.

Quick, easy, and flexible

In order for BIG-IP AFM IPS to quickly respond to attacks and exploits aimed at networks and protocols, BIG-IP Standard virtual servers and access control lists (ACL), plus FastL4, are supported. F5® iRules® can also be used to swiftly apply policies to incoming traffic. iRules is leveraged by the F5 DevCentral™ community of over 250,000 users, who collaborate and create custom rules that mitigate less-common threats. These rules are shared by the community to give other administrators the flexibility to expand the functionality of their BIG-IP AFM deployments.

SNORT-compliant rules consumption and protection

BIG-IP AFM's IPS engine uses SNORT, an industry-standard, domain-specific language (DSL), to apply rules on incoming traffic to detect and block attacks and exploits. BIG-IP AFM's IPS can ingest and use SNORT rules from third party sources to ensure consistent protection based on existing policies. F5 provides out of the box, pre-built rules specifically tuned for service provider network protocols to further extend inspection and protection for subscriber traffic. To protect against new and evolving attacks and exploits, the BIG-IP AFM IPS subscription service delivers new signatures on a continual basis.

Near real-time risk visibility

BIG-IP AFM IPS features high-speed logging (HSL) for almost real-time visibility on incoming traffic to help network personnel respond quickly to attacks. F5® BIG-IQ™ Security complements this by providing correlated visibility of threats and provides actionable responses. Log data can be transmitted to supported third-party security information and event management (SIEM) solutions for analysis and historical comparison.

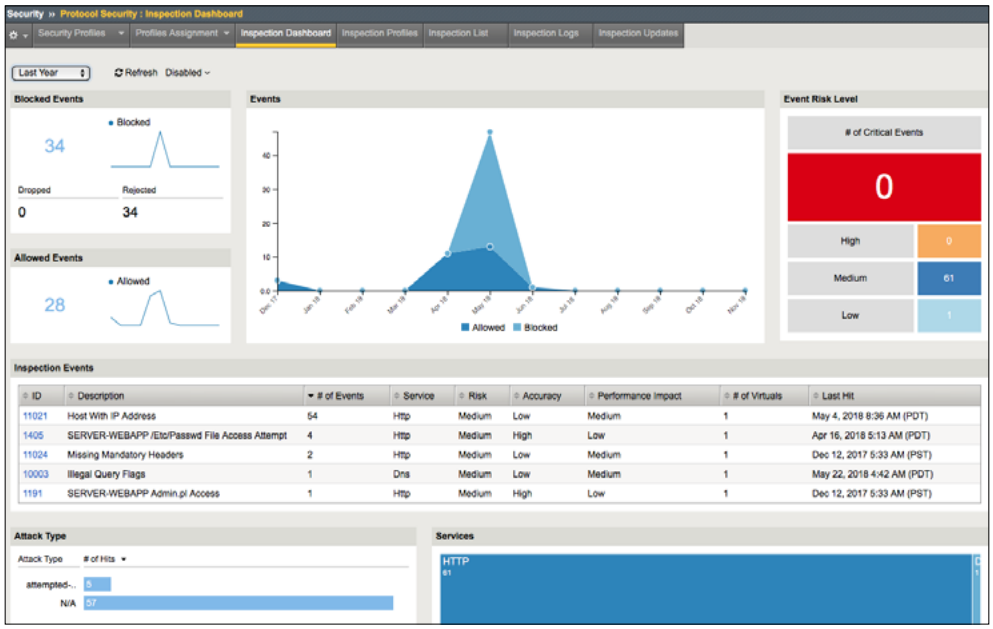

FIGURE 2: F5 AFM IPS provides visibility into and protection against attacks.

Built-in learning and rule suggestion

BIG-IP AFM IPS contains a policy suggestion engine that enables administrators to keep up with evolving attacks and exploits without having to extensively monitor and develop rules. The policy suggestion engine builds rules based on traffic patterns that can be accepted or denied, either manually or automatically, to easily add protection without expertise or overhead. It can also provide feedback on when a rule might be delivering a lot of false positives and should be disabled.

Multi-threaded for performance and scalability

BIG-IP AFM IPS is built upon the F5 BIG-IP platform, and is designed for native multi-threaded processing that makes it easy to scale in response to traffic spikes or planned growth without compromising services. The multi-threaded architecture also provides high availability and enables hit-less software upgrades—so your business operations can continue uninterrupted, and your exposure to risk is reduced.

Operational flexibility

BIG-IP AFM virtual edition's IPS is easy to run on AWS, Azure, and Google Cloud platforms, as well as in VMware/KVM private cloud environments to enable protection in any application infrastructure and NFV end points. Deployments can be managed by F5 BIG-IQ, located in either a public or private cloud for ease of management and visibility.

Services consolidation platform

BIG-IP AFM IPS enables service providers to consolidate and protect their infrastructure with an IPS that is integrated with Gi-firewall and load-balancing services in a single platform. BIG-IP AFM IPS is optimized to protect data center core and edge and the underlying protocols that enable subscriber services. For networks that require high scalability and performance, IPS on BIG-IP iSeries appliances and VIPRION chassis provides industry-leading throughput and reliability to ensure secure network services delivery.

Learn more about how BIG-IP AFM and BIG-IQ can help secure your infrastructure.