Fact Sheet

Cogito Group

F5 Big-IP

F5 Big-IP

BIG-IP is a collection of F5's hardware platforms and software solutions providing services focused on security, reliability, and performance.

BIG-IP Primary Software Modules

- **BIG-IP Local Traffic Manager (LTM**) - Central to F5's full traffic proxy functionality, LTM provides the platform for creating virtual servers, performance, service, protocol, authentication, and security profiles to define and shape your application traffic.
- **BIG-IP DNS** - Formerly Global Traffic Manager, BIG-IP DNS provides similar security and load balancing features that LTM offers but at a global/multi-site scale. BIG-IP DNS offers services to distribute and secure DNS traffic advertising your application namespaces.
- **BIG-IP Access Policy Manager (APM)** - Provides federation, SSO, application access policies, and secure web tunneling. Allow granular access to your various applications, virtualised desktop environments, or just go full VPN tunnel.
- **Secure Web Gateway Services (SWG)** - Paired with APM, SWG enables access policy control for internet usage. You can allow, block, verify and log traffic with APM's access policies allowing flexibility around your acceptable internet and public web application use.
- **BIG-IP Application Security Manager (ASM)** - This is F5's web application firewall (WAF) solution. Traditional firewalls and layer 3 protection don't understand the complexities of many web applications. ASM allows you to tailor acceptable and expected application behavior on a per application basis. Zero day, DoS, and click fraud all rely on traditional security device's inability to protect unique application needs; ASM fills the gap between traditional firewall and tailored granular application protection.

- **BIG-IP Advanced Firewall Manager (AFM)** - AFM is designed to reduce the hardware and extra hops required when ADC's are paired with traditional firewalls. Operating at L3/L4, AFM helps protect traffic destined for your data center. Paired with ASM, you can implement protection services at L3 - L7 for a full ADC and Security solution in one box or virtual environment.

Jellyfish integration with F5 BIG-IP

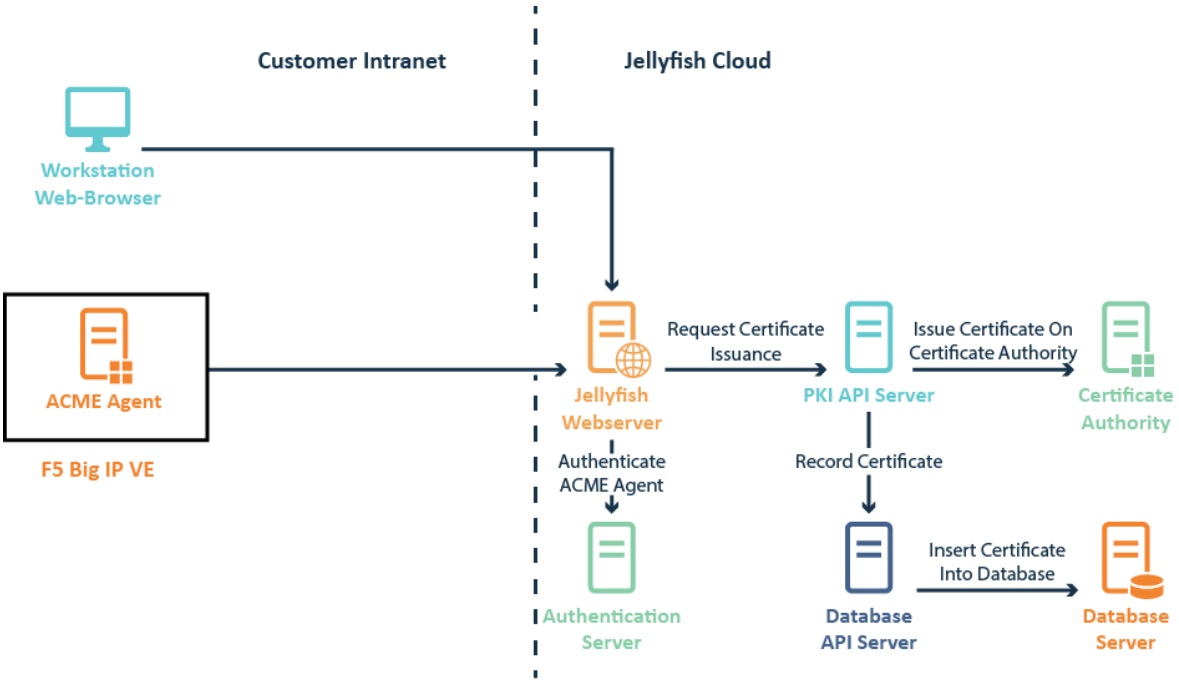
F5's Big-IP is a networking appliance that provides features for managing networks, traffic, and applications. Big-IP can be configured with an ACME (Automatic Certificate Management Protocol) client to perform automated certificate renewal with a Jellyfish ACME server.

How it works

Big-IP uses F5's Traffic Management Operating System (TMOS). TMOS is designed to inspect network and application traffic and make real time decisions based on service requirements and configuration.

The system uses SSL (TLS) certificates and keys for administrative tasks, communication, and deployment. Big-IP can be configured to act as an SSL (TLS) intercept server, securely monitoring communication between servers and their clients to increase transparency, threat detection, and auditability.

An ACME protocol client is installed into the Big-IP system and is configured to renew certificate with the Jellyfish ACME server. Renewed certificates through Jellyfish ACME are loaded into TMOS, enabling standard management of certificates with Big-IP's tools and features.



F5 Big- IP benefits

The Big-IP system can be configured with SSL profiles to perform the SSL handshake that destination servers normally perform. The purpose of this, is to offload the SSL processing from a destination server as an SSL intercept.

Jellyfish ACME support enables the automated renewal of SSL certificates for these profiles, allowing for Big-IP users to manage their certificates without operator support and with confidence in their timely renewal.

Jellyfish ACME also provides Big-IP users control and visibility of their issued certificates through the Jellyfish application. This includes cost management, searching and reporting tools, support services, and other certificate maintenance features.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.