

Contexte de la mission :

Intégrer l'équipe sécurité du groupe Accor avec pour objectif principal la prise en charge de l'ensemble des proxy (McAfee) et Reverse Proxy/WAF (F5 ASM)

Proxy McAfee:

McAfee Web Security:

- McAfee Web Protection
- McAfee Web Gateway
- McAfee Web Gateway Cloud Service

McAfee Endpoint Security:

McAfee Network Security:

- McAfee Network Security Platform
- McAfee Virtual Network Security Platform
- McAfee Advanced Threat Defense

ReverseProxy/WAF (F5 ASM):

Ownership: F5 Network Inc. US.

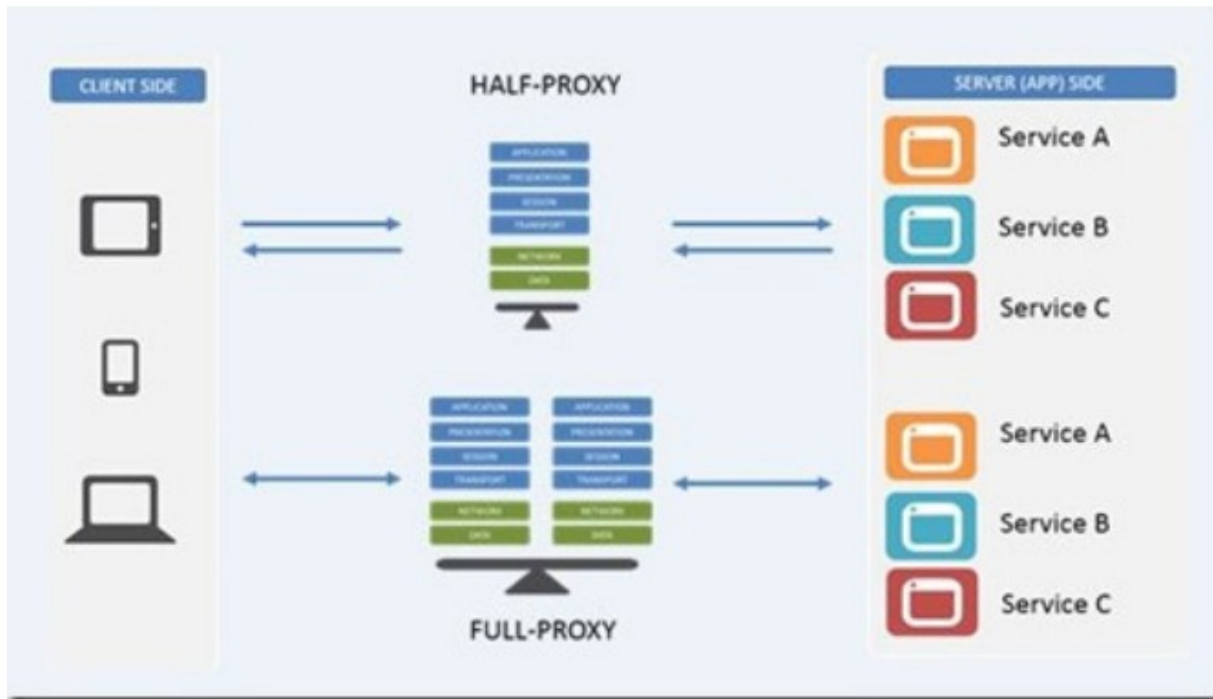
Definition:

- Reverse Proxy is a device /service placed between a client and a server. Incoming requests are handled by this reverse proxy, which interacts on behalf of the client with the server.
- WAF: Web Application Firewall.
- F5 ASM: Application security Manager.
- F5 LTM: Local Traffic Manager
- F5 APM : Access Policy Manager
- F5 TMOS : Traffic Management Operating System
- F5 CA: Certified Administrator
- F5 CTP : Certified Technical Professional
- F5 CTS : Certified Technology Specialist
- F5 CSE : Cerfited Solution Expert

Purpose:

Why should I use this Reserse Proxy?

- To provide Load Balancing for web applications and APIs. This is a way to improve performance through TLS acceleration, intelligent compression and caching.
- To manage traffic. A full Reverse Proxy (**F5 BIG-IP system**) is capable of intercepting, inspecting and interacting with requests and responses, along with services such as Application Layer Security, Web Acceleration, Page rouing and Secure remote access.
- To enforce web application security through web application firewall, application delivery firewall and deep contect inspection.



Half proxy: DSR (Direct Server Return), L4 port switching, routing and NAT (nothing intelligent other than passing traffic).

Full proxy: Traditional load balancing, optimization, SSL offloading, server side caching, and security functionality.

Forward proxy: Client side caching (grabbing a video and storing locally) , filtering (blocking certain time-wasting sites or macilous contents) along with privacy (masking internal resources) along with security.

Full application proxy (Standard Virtual Service): This service fully terminates the transport layer connections (typically TCP) and establishes completely separate transport layer connections to the applications. It's used to inspect payloads(JSON, XML,HTML,etc...) or steer requests based on HTTP headers (URL, cookies, custom variables, etc...).

Packet by Packet Proxy (Performance L4 Virtual Service): SDN Openflow (highest layer), simple load balancing, and policy network routing.

Router (IP Forwarding Virtual Service): Rewrite @IP_SRC

Bridge (L2 Forwarding Virtual Service):

Application Delivery Firewall: This isolates users from applications and infrastructure by transparently applying the appropriate security, performance, and availability policies to inbound and outbound traffic.

Description de la mission :

- Prise en charge du Run et Build de l'infrastructure Proxy McAfee et Reverse Proxy/WAF (F5 ASM)
- Prise en charge du Run et Build des alertes sécurité
- Gestion des incidents (réactivité et investigation avancées)
- Amélioration continue des processus et des services - Force de proposition - Automatisation des tâches récurrentes
- Création et évolution des dashboards sous Splunk

Compétences techniques :

- Infrastructure - Sécurité