

NEXT GENERATION FIREWALL IMPLEMENTATION

PROFESSIONAL SERVICES

Fortinet Next Generation Firewall Professional Service

Code: PS-IMP-FORT-ADV-01

Advanced

Overview

It is no secret that organizations across the globe are facing a growing volume of cyber-attacks. Attackers are highly skilled, well organized and tenacious, whilst many organizations are under-skilled and undermanned. To help combat these attacks, organizations continue to invest heavily in technology, many making the move to next generation firewalls.

Fortinet delivers unparalleled protection, ease of use and performance from its Next Generation Network Security platforms to protect against sophisticated Cyber Threats. Fortinet a leading global provider of network security appliances available in both hardware and virtualized form factors to fit unique requirements of Carriers, Data Centers, Enterprises and Distributed offices.

Fortinet combine the most advanced threat intelligence from FortiGuard Labs with our FortiOS Operating System and purpose-built FortiASIC processors to provide consistently top-rated security, deeper visibility, and superior performance. Industry leading threat management from the edge to the endpoint, and all points in between – consolidated, simplified security without creating performance bottlenecks.

We are PT. Autojaya Idetech offering Fortinet Next Generation Firewall (NGFW) Professional Service, enables an organizations to confidently invest in the latest firewall technologies, to ensure that the business is as secure as can be. We work with you to minimize complexity and the resources required for the configuration and integration of the new solution, ensuring it is ready to plug into the network for the security zones and policies to be configured and deployed. Customers that choose this service benefit from the knowledge and experience of our Professional Services team, with expert planning, specialized tools, continual analysis and tuning.

Benefits of our approach

- Configuration of cyber security technology to industry standards without tying up limited resources
- Reduce the impact of a breach by ensuring the basics are covered
- Freedom to upgrade to the latest technology and firewall functionality without impacting security
- Reduced pressure on the IT security team to immediately become experts in new technology

Spectrum Analysis / RF Interference

The Professional Services Engineer will work with the customer to:

- Mount & power up appliance
- Upgrade to latest firmware || if required
- Register unit & apply license in Fortinet Portal
- Admin profile settings for Administrators (max 5 profiles)
- Network configuration : IP Address, Default Gateway, DNS, Static Route, DHCP Server
- Create VLAN or Trunk || if necessary (max 10 VLANs)
- Basic firewall policies & traffic shapers (max 20 policies, 5 shapers)
- Configure Virtual IP || if required (max 5 VIP profiles)
- Configure NGFW profile : Web Filter/AntiVirus/AntiSpam/Application Control/IPS (max 8 profiles)
- Configure WAN Link Load Balancing || if necessary (up to 4 ISP)
- Configure High Availability (HA), fail-over configuration || if necessary
- Create Virtual Domain (VDM) || if necessary (max 2 VDM)
- Configure Policy Routes & Dynamic Routing || if necessary (max 7 policy routes)
- Configure IPSec & SSL VPN || if necessary (max 3 IPSec policies)
- Create local user & addresses object (max 20 objects)
- Custom services & service group object (max 20 objects)
- Logging, report & event mail notification
- Backup/Restore configuration
- Register unit & apply license in Fortinet Portal

Knowledge Transfer

Prior to concluding the engagement, our professional service engineer will conduct a knowledge transfer session with your staff. We will review how to administer and use the Fortinet NGFW system with the customer's staff. We will provide a network security check and review common security events and performance.

Deliverables and Leave-behind Items

The following deliverables will be left with the customer at the conclusion of the engagement:

- ▶ User Acceptance Test (UAT) check list
- ▶ End of engagement report out
- ▶ Comprehensive configuration documentation including a spreadsheet that details:
 - Login and password summary
 - Fortinet product serial numbers
 - IP addressing scheme
 - Complete NGFW profile configuration settings
 - License keys, etc
- ▶ Backup running configuration
- ▶ Project management documentation

