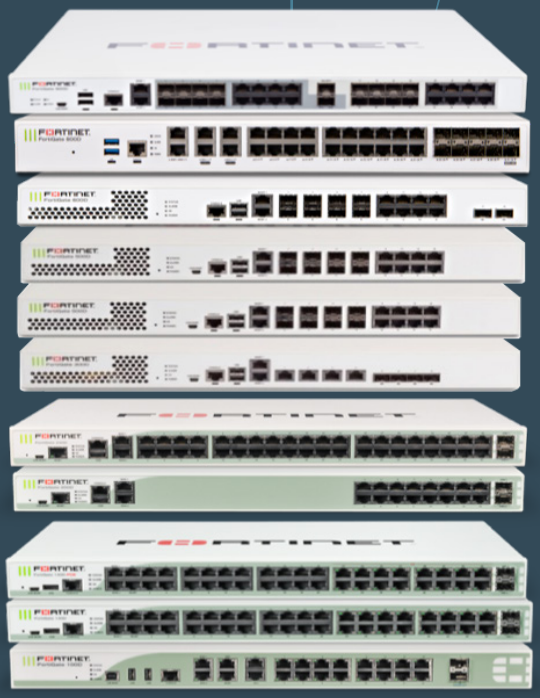


FORTIGATE KICK STARTER PACKAGE

MID-RANGE LEVEL

www.insoftservices.uk

insoft services | FORTINET

FortiGate
Kick Starter Package
(Mid-Range Level)

Table of Contents

Introduction **3**
- Solution Scoping 3
- Devices covered 4
- Assumptions 5

Activity Execution **7**
- Work Description 7
- Work Plan 8
- Deliverables 9
- Optional Deliverables 10

Introduction

Each firewall project and its implementation is always unique, adapting to the right customer situation.

However, when planning and implementing firewall projects, many similar services and configurations, which can be integrated into stand-alone Professional Service Packages. Note: The FortiGate Kick Starter Package (Mid-Range Level) **is not suitable for all firewall installations**. It is important to evaluate in advance and to check if this package suits for the planned deployment.

Solution Scoping

The following firewall project requirements would correspond to the FortiGate Kick Starter (Mid-Range Level)

Configuration Requirements

- Static routes - up to 35
- Policy Routes - up to 10
- Firewall policies - up to 100
- Address Objects - up to 250
- Custom Service Objects - up to 80
- Source NAT - up to 50
- Destination NAT - up to 50
- Security profiles (AV, IPS, Web filtering, application control, etc.)
  - up to 5 for each category
- Remote Authentication
  - up to 3 AD / LDAP Server / Radius Server
- Authentication - up to 100 users
- IPsec VPN tunnel - up to 20
- SSL VPN portals - up to 10

Larger projects or more customized and complexed configurations can be pre-screened with **Insoft System Engineering Team** (Professional Services) to find a solution that meets your specific needs.

Any task or activity **not explicitly listed** in the deliverables or agreed to via an additional scoped agreement shall be considered out of scope for the purposes of this engagement. This includes, but is not limited to:

- **HyperVisor Setup & vNIC Setup** – It is expected that any HyperVisor platform and its associated virtual Network be pre-configured and working prior to the deployment of a virtual Wireless LAN controller.

• **Configuration of FortiGate Wi-Fi or Switch Controller and FortiAPs**, FortiSwitches. Extra Fortinet Wireless and Fortinet Switching Kick-Starter Packages can be purchased separately.

• **Captive Portal Setup or Authentication** – Integration with or set up of any 3rd party Captive Portal system for user authentication is outside the scope of this engagement.

• **Switch Configuration** – Our team can advise on the correct logical switch configuration for best practice, however the actual configuration of any 3rd Party switching infrastructure will not be Insoft's responsibility. Insoft can optionally configure FortiSwitches. (See Fortinet Switching Kick-Starter Package)

• **QoS** – Outside of marking CoS/DSCP values for applications, Insoft will not be responsible for ensuring Quality of Service on the network.

• **Interface Link Aggregation** – If link aggregation is required (i.e. LACP configuration), Insoft will not be responsible for its configuration or any potential bridging loops arising from mis-configured STP or similar.

• **Physical FortiGate mounting & cabling** – The physical installation of FortiGate and related cabling will be performed by a 3rd party to Insoft.

• **Authentication Server** (Active Directory, RADIUS Server) **configuration** – Insoft will not be responsible for configuring any 3rd Party Network Enforcement devices.

• **Configuration and set up** of iPerf server is not part of the scope

• **Firewall, Routing, DNS & DHCP server** configuration delivered by 3rd Party Devices – Unless specifically stated, Insoft will not be responsible for any network configuration components that fall outside of the configuration of the FortiGate Firewall and related components.

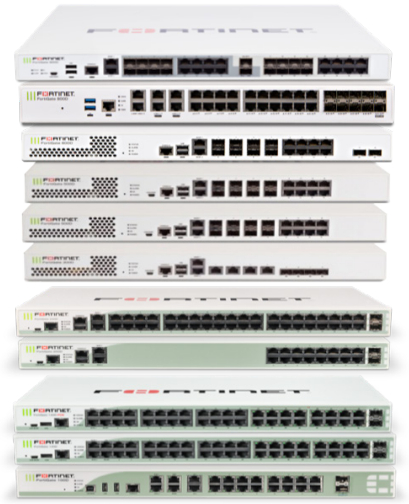
• **IPsec VPN Configuration on Remote Sites** – Insoft can advise and provide the needed IPsec VPN Parameters for Remote Site to be configured for IPsec Tunnels with the FortiGate on the customer side; however the actual configuration of any 3rd party Firewalls or VPN Gateways will not be Insoft's responsibility.

Devices Covered

FortiGate Kick Starter – Mid-Range Level Package is designed for FortiGate Mid-Range Level Firewall Solutions. It is important to know the Performance and Feature requirements to be able **to size the best-suited solution to your needs**.

Please work with your IT-Security Consultant / Engineer to determine which Appliance is suitable.

Insoft can also provide a Pre-Sale IT - Security Consultant, who will help you to size and design a suitable FortiGate Appliance for your needs.



FortiGate Mid-Range Level Series – Feature-rich Security Appliances for Small/Home Offices & Small Branch Offices

The FortiGate Kick Starter Package (Mid-Range Level) is recommended when you buy any of this Appliances:

- **FG-900D**
- **FG-800D**
- **FG-600D**
- **FG-500E**
- **FG-400D**
- **FG-300E**
- **FG-200E Series**
- **FG-100E Series**

Assumptions

All aspects that need to be clarified are listed hereunder, be this related to the work, the infrastructure, or preliminary work/phases, which are required for safe package execution.

- Access to site
- Availability of staff
- Availability of information
- Certain configuration rules or concepts, which are requisites for our work to be done

The following assumptions have been made concerning the FortiGate Kick Start Package:

- It is assumed that the analysis of requirements and sizing has already been done.

• It is also assumed that a physical data-centre/server-room visit has been done to ensure that FortiGate Appliances can be placed in Server Rack and have a free power socket.

• We assume that the customer will provide a nominated sponsor to provide unhindered access to all relevant server rooms, cabinets and racks as required to set up and install the FortiGate Appliance and associated components.

• The customer is responsible for the internal change management processes.

• The customer is responsible for any relevant end-user communications.

In addition, the following technical assumptions have also been made:

• The customer will provide all relevant networking details (e.g. Network Diagram, Vlans, IP addresses for the interfaces and Adress Objects, etc).

• The customer will provide all the back-end switching (VLAN trunking, tagged/untagged VLANs, DHCP helpers as necessary etc).

• The customer or their contractor will physically mount and secure the FortiGate.

• If virtual machines are used, the customer will provide virtual resources (vCPU, Memory, Disk) from an on-site Hypervisor with dedicated NICs per the specs in the Virtual Controller Guide.

Activity Execution

The FortiGate Kick Start package (Entry-Level) provides the customer with specialist FortiGate Professional services for a fixed duration of time. All services will be delivered by skilled, trained and certified Professional Services consultants.

The scope of the professional services engagement is limited to the in scope deliverables listed below.
Requests for the optional deliverable items, (also listed below) will be provided upon agreement for services beyond the duration or scope of the standard Kick Starter.

All optional deliverable items shall be clearly defined in the package ordering under as 'advanced' or add-on items.

Work Description

The Service Package workflow consists of the following Phases:

Design
• Verifying and approving of the Requirements and Sizing that has already been done by the customer in Pre-Sale Phase
• High-Level Design
• Detailed Design
  - Topology
  - Interfaces / Zones
  - Routing
  - Policies
  - VPN
  - Authentication Servers
  - Use cases
  - Etc.

Basic Config
• Registration and licensing
• Firmware Upgrade
• High Availability Cluster setup (optional)
• Interface configuration
• Live on LAN and WAN

Main Config / Implementation
• FortiGate detailed configuration as defined by design and customer conditions.

Tests
• Configuration Tests
  - Connectivity Tests (Internet, LAN, DMZ, etc.)
  - Destination NAT (VIP) Tests
  - VPN Tests
  - Security Profiles working
  - High Availability Cluster Fail-over Test (optional)

Fine Tuning
• Fine tuning of FortiGate configuration (best practice)
• FortiGate Hardening (best practice)

User Acceptance Tests
• Live-Test User use-cases
• Addressing and remedial of possible issues that have been found during Live-Test
• User acceptance sign-off

Knowledge Transfer Workshop
• FortiGate Knowledge Transfer Workshop for internal Administrators

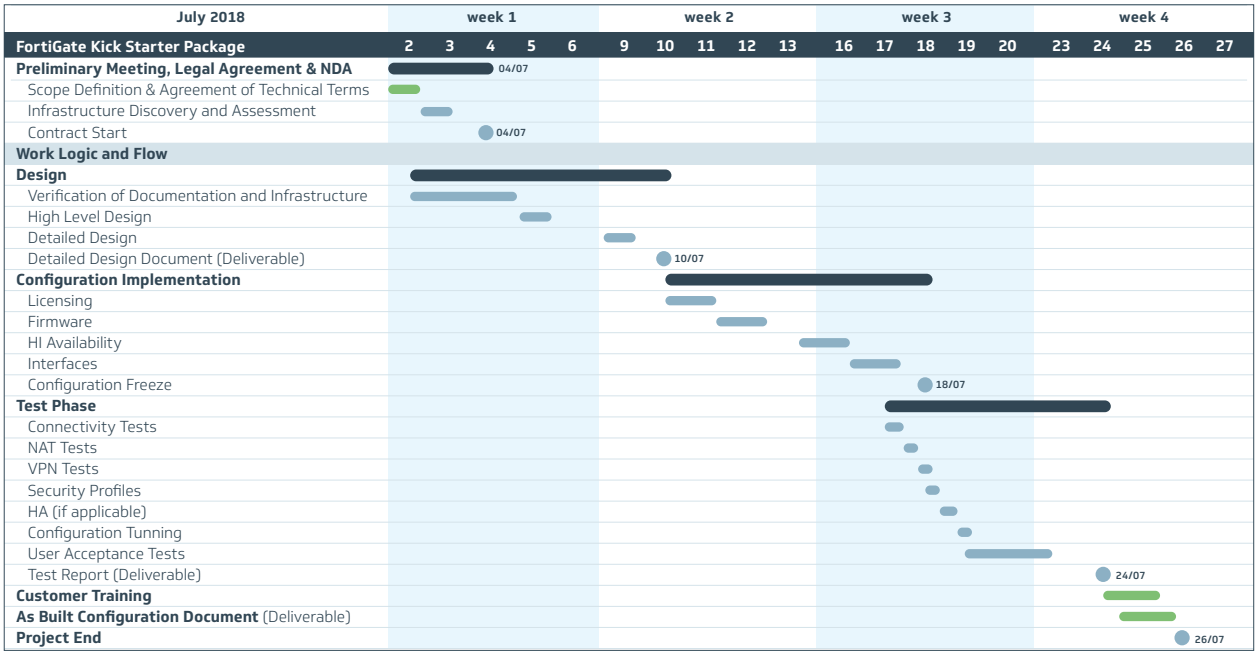
Documentation
• As built documentation
• Visio FortiGate Design overview

FortiGate handing over to customer
• Internal Administrators take over and are responsible for the Firewall

Work Plan

The work plan is based on the Work Description and can be graphically summarised in the following chart. Activities and milestones are listed and differentiated. The overall project time is an example, since the overall duration is depending on Customer availability.

However, the overall duration cannot be more than 45 working days.



Deliverables

This section describes the Deliverables in general terms, including configuration activities and features, as listed hereafter. Project contractual deliverables are the following, and are provided in paper format:

1. Detailed Design Document
2. Test Report
3. As Built Documentation

Activities that can be considered as deliverables since they are part of the work flow are the followings:

• **Design of the FortiGate-Firewall** will logically describe the proposed Perimeter-Design based on the requirements determined during pre-sales.

• **FortiGate Initial Setup** – Rack and stack of the FortiGate and the setup of the FortiGate on the network.
• Fortinet Virtual Machine Basic Config (Only required if using virtual FortiGate Appliances).

• **Registration and licensing** of FortiGate Appliances

• **FortiGate Firmware updates** – Once initially set up, Insoft will ensure that the firmware is updated to the most current and stable release available.

• **FortiGate Configuration** per customer requirements with this scope:

- Static routes - up to 35
- Policy Routes - up to 10
- Firewall policies - up to 100
- Address Objects - up to 250
- Custom Service Objects - up to 80
- Source NAT - up to 50
- Destination NAT - up to 50
- Security profiles (AV, IPS, Web filtering, application control, etc.) - up to 5 for each category
- Remote Authentication - up to 3 AD/ LDAP Server/Radius Server
- Authentication - up to 50 users
- IPsec VPN tunnel - up to 15
- SSL VPN portals - up to 10

• **Post Implementation**, Best Practice Configuration, Fine Tuning and Hardening.

• **Testing** – Insoft will test all aspects of the Firewall Design and Configuration in consultation with User Acceptance plans developed in conjunction with the customer.

• **As Built Documentation** – Insoft will document the new Firewall as built. This includes but is not limited to: FortiGate configuration, IP addresses, Admin access, Visio Firewall Design Overview

Optional Deliverables

The following items can be optionally negotiated as deliverable items.
This is an incomplete list and more can be added/negotiated via an additionally scoped agreement. All optional deliverable items shall be clearly defined in the package order.

- **Performance testing** - requires a testing server such as iPerf. If an on-site-testing server is available then Insoft will conduct throughput testing as part of the post-implementation validation.

- **The configuration of FortiGate VDOMs** (Route, Transparent Mode).

- **The configuration of FortiGate Virtual Wire Pair** Interfaces and FortiGate in Transparent Mode.

- **High Availability** (Nplus1) **setup & fail-over testing** – If multiple FortiGates have been purchased, Insoft will set up a High Availability cluster and perform fail-over testing to ensure network resilience in the case of hardware or link failure.

- **FortiGate SD-WAN Configuration.**

- **Configuration and testing** of dynamic routing Protocols (OSPF, RIP, BGP).

- **Fortinet Security Fabric Configuration** – configuring the FortiGate to be a part of Fortinet Security Fabric of the customer company.

- **IPv6 Configurations** – Interfaces, Policies, Routing, NAT46 and NAT64.

- **The configuration of IP Pools** and Virtual/ Real Servers.

- **The configuration of Explicit Web Proxy** and SSL Inspection Full Mode.

- **The configuration of FortiTokens**.

- **The configuration of FortiGate Single Sign-On** in DC and Pooling Modes.