

CONFIDENTIAL



Signals

Maldives National Defence Force
Republic of Maldives

Terms of Reference (TOR)
REQUEST FOR PROPOSAL
Wide Area Network (WAN)

06 June 2024

1. Introduction

The Maldives National Defence Force (MNDF) is seeking proposals from qualified vendors for the comprehensive upgrade of its Wide Area Network (WAN) infrastructure. The objective is to enhance our network's performance, security, and scalability to support our operational needs. This document outlines the requirements for licenses, devices, connectivity, configurations, and training.

2. Scope of Work

The scope of work includes the provision of specified hardware and software licenses, establishment of connectivity across various MNDF sites, Configurations and relevant professional certification and training for MNDF personnel on the infrastructure and the devices.

3. Licenses and Devices Requirement

This section outlines the necessary licenses and devices required for the MNDF WAN architecture. The requirements are categorized into two main sections: "License Only" and "License with Appliance."

3.1. License Only

Table 1 shows the products that require only licenses for their operation. These licenses are for the devices and virtual machines (VMs) that will be used to manage and analyze network traffic and security within the MNDF WAN infrastructure.

Table 1

#	Product Model Name	QTY	Licenses	Duration
1	FortiManager VM S-Series	1	VM License 100 Devices	3 Years
2	FortiAnalyzer 300G	1	FortiCloud (180 Vdoms)	3 Years
3	FortiGate 400E	2	UTP	3 Years
4	FortiGate 80F	3	UTP	3 Years
5	FortiWifi 60F	17	UTP	3 Years
6	FortiWifi 60F	8	FortiCare Essential Support	3 Years
7	FortiGateRugged 60F 3G4G	3	UTP	3 Years
8	FortiGateRugged 60F 3G4G	20	FortiCare Essential Support	3 Years
9	FortiWifi 40F 3G4G	4	UTP	3 Years

3.2. License with Appliance

Table 2 details the products that require both the appliance and associated licenses. These are hardware devices bundled with the necessary licenses for their operation within the MNDF WAN infrastructure.

Table 2

#	Product Model Name	QTY	Licenses	Duration
1	FortiWifi 60F	1	FortiCare Essential Support	3 Years
2	FortiWifi 40F 3G4G	1	UTP	3 Years

4. Connectivity Requirements

All sites of the MNDF WAN must be able to communicate directly with each other, despite using different connectivity types (WAN Links or LTE). The Links should be designed to facilitate this through a hybrid mesh topology.

4.1. WAN Connections

- The service provider must ensure the integration of WAN Links to enable efficient and scalable routing within WAN-connected sites.
- The WAN links must provide the bandwidths according to **Table 3** and **Table 4** to handle peak traffic loads and maintain low latency to support real-time communications and critical applications.
- **MNDF KK (Backup)** Link mentioned in **Table 3** should be a redundant link which should work as an active-active scenario.

4.1.1 Headquarters (WAN Links)

Table 3

#	Site	WAN Links Bandwidth/Type
1	MNDF MALE HQ	No Less than 375 Mbps
2	MNDF KK (Backup)	No Less than 100 Mbps
3	MNDF S.GAN	50 Mbps
4	MNDF Lh. Maafilaafushi	50 Mbps
5	MNDF L. Kahdhoo	50 Mbps
6	MNDF H. Dh Hanimadhoo Post	50 Mbps

4.1.2 Other Sites (WAN Links)

Table 4

#	Site	WAN Links Bandwidth/Type
1	MNDF Thilafushi	15 Mbps
2	MNDF Uligamu Post	15 Mbps
3	MNDF Kulhudhufushi Post	15 Mbps
4	MNDF Maamigili Post	15 Mbps
5	MNDF Kudahuvadhoo Post	15 Mbps
6	MNDF Gdh. Kaadedhoo Post	15 Mbps
7	MNDF Fuvahmulah Post	15 Mbps
8	MNDF S. Hithadhoo Fire Station	10 Mbps
9	MNDF Lh. Naifaru Fire Station	10 Mbps
10	MNDF Gdh. Thinadhoo Fire Station	10 Mbps
11	Ga. Villingili Radar Station	10 Mbps
12	Makunudhoo Radar Station	10 Mbps
13	Kaashidoo Radar Station	10 Mbps
14	Mulee Radar Station	10 Mbps

4.2. LTE Connections

- The service provider must ensure extensive LTE coverage and provide adequate bandwidth to support necessary communication needs.
- The LTE links must provide the bandwidths according to **Table 5** to handle peak traffic loads and maintain low latency to support real-time communications and critical applications.

4.2.1 Mobile Sites

Table 5

#	Site	QTY	LTE Bandwidth/Type
1	MNDF MALE HQ	1	No Less than 200 Mbps Upload/Download from all the other LTE sites (Dedicated Private IP)
2	LTE connection (SIM) for Fortigate Devices	12	10 Mbps / Unlimited (Dedicated Private IP)
3	LTE connection (SIM) for Fortigate Devices	16	5 Mbps / 50GB (Dedicated Private IP)

5. General Requirements

1. Service providers are required to do any configuration required for any **device** in the process of **migration, device upgrading, implementation of redundant connections** and **license upgrading** process.
2. All sites must be interconnected and must be reachable via direct route (Mesh Topology).
3. The Links must support multicast traffic, enabling it to flow seamlessly across all sites.
4. Fiber optic cable must be used for last mile connectivity to ensure high-speed and reliable communication.
5. Links must be provisioned to meet the required bandwidth specifications for all sites.
6. The service provider's devices and links must fully support multicast traffic.
7. The service provider is responsible for providing and setting up all necessary equipment in accordance with the specifications outlined in this RFP.
8. The service provider must identify a technical focal point to offer prompt technical assistance to MNDF as required.
9. The service provider must notify MNDF SIGNALS of any major technical works scheduled or any significant technical faults that may lead to service interruptions and MNDF SIGNALS should be informed promptly upon the completion of such work or the resolution of faults, ensuring services are back to normal operation.

CONFIDENTIAL

6. Training Requirements

The selected vendor must provide Fortinet training and certification for Eight (8) MNDF staff members according to following: The Training should be conducted in 2 separate batches.

1. **Fortinet Certified Professional (Network Security)** for MNDF two (2) staff.
2. **Fortinet Certified Professional (Security Operations)** for MNDF two (2) staff.

The training should be conducted by an authorized Fortinet trainer at an authorized Fortinet Training Center.

-- End of Document --

