

 FourNet	4net Technologies Ltd Network Services 2 (RM3808) Service Offering	Crown Commercial Service <i>Supplier</i>
--	---	---

1. Service Offer Reference No: RM3808-Lot 1-4net-033
2. Lot(s): 1
3. Service Offer Effective Date: 5th June 2023
4. Service Offer Expiry Date: 16th August 2023
5. Service Description: Fortinet Firewall Infrastructure

The Service is provided pursuant to RM3808 Framework Agreement.

This service offer is to provide the hardware to create a Secure SDWAN capable Managed WAN service to replace existing firewalls currently installed across the Buyer's Network.

Business Level expected outcomes / compelling events

- Provide a resilient Firewall solution for main Datacenters with the ability to failover
- Provide the ability for datacenter failover of services were appropriate.
- Provide a solution to integrate with current connectivity from ISP's and MPLS with the flexibility to intergrade SDWAN in the future.
- Provide flexibility for local internet break-out or centralized internet break-out to minimize the time taken to access the internet.
- Provide SD-WAN and MPLS hybrid network, allowing flexible routing across MPLS or secure SD-WAN routing across the internet.
- Allow for the provision of local services such as DHCP, DNS, and secure Guest access where appropriate.
- Centralised data analysis and management of SDWAN hardware

Proposed Solution & Technical Specification

FourNet has designed an SD-WAN overlay utilising Fortinet appliances and services. Central to the Fortinet service is the security fabric, which provides many tools and features to ensure the SD-WAN is secure regardless of the locations, devices or services in use. The security-driven Fortinet SD-WAN is an end-to-end solution, providing an accessible, intuitive solution with an advanced level of control and management capabilities.

Each Datacentre will receive two physical Fortinet FortiGate devices whereas all other sites will receive a single device. The size of device varies dependant on size of site and use case. Where appropriate, 3rd party SFP will be used within the appliances.

Topology Diagram



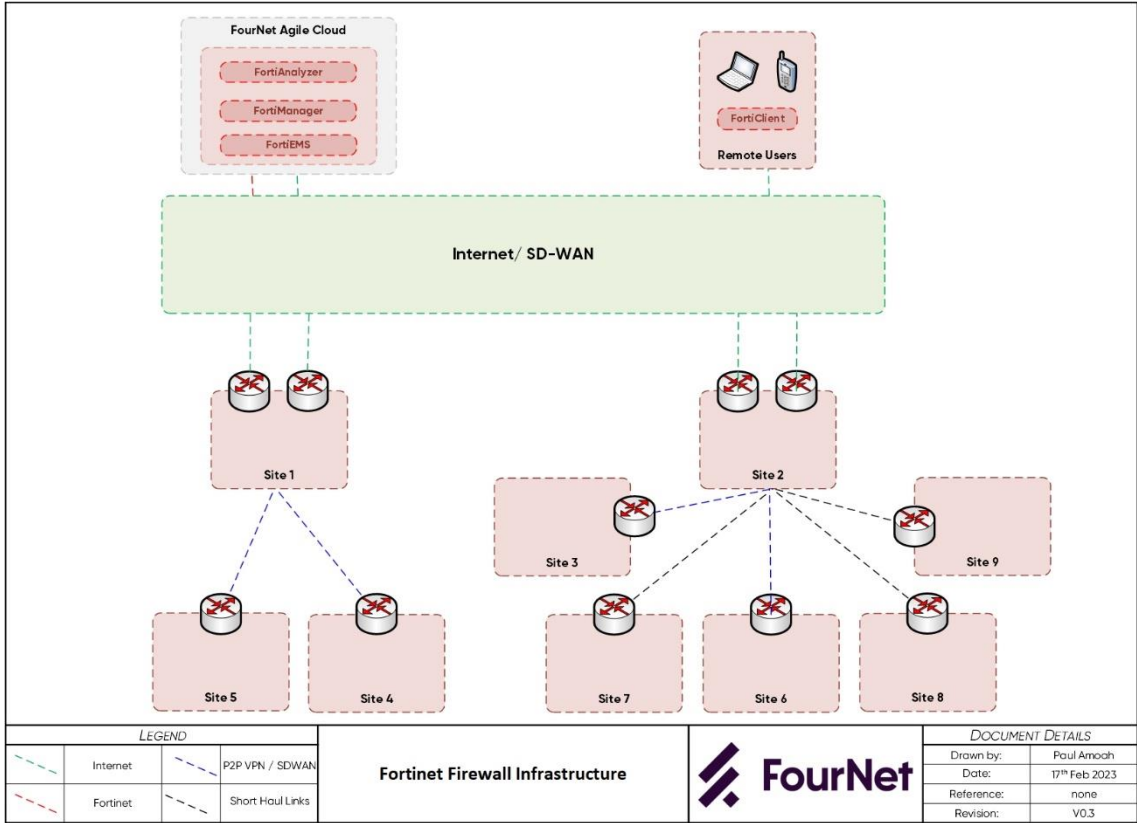
4net Technologies Ltd

Network Services 2 (RM3808)

Service Offering

Crown
Commercial
Service
Supplier

The final topology for the service will be agreed with the Buyer on completion of the Order Form.



Based on the Topology diagram above the proposed appliance, for each site, is shown in the following table:

Example Site	Priority	FortiGate Appliance
Site 1	1	400F
Site 2	2	400F
Site 3	3	100F
Site 4	4	100F
Site 5	5	60F
Site 6	5	70F
Site 7	6	60F
Site 8	6	60F
Site 9	6	70F

The "Priority" in the table above is an example of the order in which the deployment will be completed, the final order of priority will be agreed with the Buyer on completion of the Order Form.



4net Technologies Ltd Network Services 2 (RM3808) Service Offering

Crown
Commercial
Service
Supplier

Each Firewall includes FortiGate Unified Threat Protection (UTP). This enables the Buyer to consolidate their IT security services into one device, simplifying the protection of the network. As a result, all threats and security-related activity can be managed through a single pane of glass. The following features are also included within each Firewall deployment, which can be utilised to further enhance the security of the environment.

Antivirus

Antivirus software that can monitor your network, then detect and stop viruses from damaging your system or its connected devices. This is done by leveraging the information in signature databases, which are storehouses containing the profiles of viruses, to check if any are active within your system or are trying to gain access.

Some of the threats the antivirus software within a UTP can stop include infected files, Trojans, worms, spyware, and other malware.

Anti-malware

Unified threat protection protects your network against malware by detecting it and then responding. A UTP can be preconfigured to detect known malware, filtering it out of your data streams and blocking it from penetrating your system. UTP can also be configured to detect novel malware threats using heuristic analysis, which involves rules that analyse the behaviour and characteristics of files. For example, if a program is designed to prevent the proper function of a computer's camera, a heuristic approach can flag that program as malware.

UTP can also use sandboxing as an anti-malware measure. With sandboxing, a cell inside the computer is confined to a sandbox that captures the suspicious file. Even though the malware is allowed to run, the sandbox prevents it from interacting with other programs in the computer.

Intrusion Prevention

A UTP system can provide an organization with intrusion prevention capability, which detects then prevents attacks. This functionality is often referred to as an intrusion detection system (IDS) or intrusion prevention system (IPS). To identify threats, an IPS analyses packets of data, looking for patterns known to exist in threats. When one of these patterns is recognized, the IPS stops the attack.

In some cases, an IDS will merely detect the dangerous data packet, and an IT team can then choose how they want to address the threat. The steps taken to stop the attack can be automated or performed manually. The UTP will also log the malicious event. These logs can then be analysed and used to prevent other attacks in the future.

Virtual Private Networking (VPN)

The virtual private network (VPN) features that come with a UTP appliance function similarly to regular VPN infrastructure. A VPN creates a private network that tunnels through a public network, giving users the ability to send and receive data through the public network without others seeing their data. All transmissions are encrypted, so even if someone were to intercept the data, it would be useless to them.


FourNet

4net Technologies Ltd Network Services 2 (RM3808) Service Offering

Crown
Commercial
Service
Supplier

Web Filtering

A UTP's web filtering feature can prevent users from seeing specific websites or Uniform Resource Locators (URLs). This is done by stopping users' browsers from loading the pages from those sites onto their device. You can configure web filters to target certain sites according to what your organization aims to accomplish.

Data Loss Prevention

The data loss prevention you get with a UTP appliance enables you to detect data breaches and exfiltration attempts and then prevent them. To do this, the data loss prevention system monitors sensitive data, and when it identifies an attempt by a malicious actor to steal it, blocks the attempt, thereby protecting the data.


A virtual instance of FortiManager, FortiAnalyser and FortiEMS will be hosted in FourNet's core network, Agile Cloud. MPLS and internet connectivity into FourNet's Agile Cloud platform will also be provided free of charge, as this will provide access to the hosted devices. FortiClient licenses for up to 800 remote-user devices are included in the design, which will provide secure remote access to the SD-WAN, such as for homeworkers or users working out of the office. FortiClient will provide Zero-Trust Network Access to these users, ensuring only authorised devices access the network remotely and securely.

FortiManager is a next generation, automation driven, management solution, which will allow the Buyer to manage all the FortiGates and FortiClients. This will provide a single dashboard with a suite of tools for managing the SD-WAN and security, the Buyer to control the network and the resources accessible via the network, for example setting policies around who has access, what they can access and how much bandwidth they can utilise. It will also provide tools that manage the connections themselves, with features such as right-path selection which routes traffic over the best performing connection, load balancing traffic to fully utilise all available, as well as visibility of network metrics (latency and jitter to name a few).

FortiAnalyser is a security driven, analytics and log management solution that will collect and analyse logs from different sources (FortiGates, FortiSwitch and FortiAP), helping to identify and eliminate threats across the Fortinet Security fabric.

6. Conditions on the Buyer:

- The Buyer will provide any structured cabling at their expense
- The Buyer will complete any data capture documentation as required in a timely manner
- The Buyer will provide all environmental requirements specified by FourNet, including rack space and power outlets
- The Buyer will provide an appropriate Network Time Protocol (NTP) service . NTP is required to synchronize the time on all elements of the solution to ensure consistency across all logs and to provide a good user experience
- The Buyer will deploy the FortiClient software on user devices: FourNet will provide a download link for the FortiClient software


 FourNet	4net Technologies Ltd Network Services 2 (RM3808) Service Offering	Crown Commercial Service Supplier
<ul style="list-style-type: none"> • The Buyer will provide FourNet with appropriate IP addresses of all sites • The Buyer will dispose of all redundant/retired equipment, removed from the current environment as the new service is deployed • The Buyer will dispose of all packaging and waste, as applicable. • The Buyer will provide an appropriate level of knowledgeable resource to support FourNet with the integration between the FourNet supplied equipment and other Buyer systems/services • The Buyer will be responsible for completing the software/application Integration between the FourNet service and other customer third-party systems • The Buyer will ensure timely attendance of appropriate personnel at scheduled training and workshops. • The Buyer will agree and complete User Acceptance Testing (UAT) and the sign-off the UAT documentation prior to any Training takes place • The Buyer will agree to an appropriate means of remote access to enable FourNet support services to remotely implement and subsequently support the service. • The Buyer will provide FourNet engineer(s) with internet access whilst working on site • The Buyer will designate a single point of contact. The individual will have a thorough understanding of the Buyer's business/operational requirements and technical environment, and will be authorised to make binding decisions on the Buyer's behalf 		

7. Outline Implementation Plan:

Due to the complex nature of the delivery of a Secure SDWAN capable Managed WAN service it is not possible, without consultation with the Buyer, to offer a confirmed Implementation plan. However, the Outline Implementation Plan below is indicative of the delivery and payment milestones.

The Qualified Implementation Plan will be agreed with the Buyer as soon as possible after the Contract Ward and before the start of the delivery of the services.

Task	Deliverable	Estimated End Date	Milestone Payment
Contract Award	Signed Order Form and Buyer Purchase Order	Week 1	50% of Capital Price
Deliver Site 1 and 2	Configure, Installation and UAT complete	Week 6	10% of Capital Price
Deliver Site 3 and 4	Configure, Installation and UAT complete	Week 12	20% of Capital Price
Deliver Site 5 and 6	Configure, Installation and UAT complete	Week 18	10% of Capital Price

 FourNet	4net Technologies Ltd Network Services 2 (RM3808) Service Offering		Crown Commercial Service Supplier
Deliver Site 7, 8 and 9	Configure, Installation and UAT complete	Week 26	10% of Capital Price

8. Service Level Agreement:

This Service Level is offered as an operating level agreement, the applicable service levels are subject to the terms of the RM3808 Call Off Schedule 14: Service Levels which can be varied by the agreement of both parties pursuant to the terms of that agreement. This service is available at Service Maintenance Level 4.

This Service Level is offered as an operating level agreement, the applicable service levels are subject to the terms of the RM3808 Call Off Schedule 14: Service Levels which can be varied by the agreement of both parties pursuant to the terms of that agreement. This service is available at Service Maintenance Level 4.

9. Service Offer Price Card


The Service Offer Price Card below defines the price for Services made available to Buyer through this Service Offer.

9.1. Hardware (Capital), Professional Services (Capital) and Support (Operational) Charges

Site Name	Priority	Proposed Gate	Quantity	FourNet Hardware Including 5 Years FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	FourNet Professional Services	FourNet Managed Service (Per Year)
Site 1	1	400F	2	£52,959.00	£19,362.00	£10,416.17
Site 2	2	400F	2	£52,959.00	£19,362.00	£10,416.17
Site 3	3	100F	1	£7,454.00	£2,656.00	£744.00
Site 4	4	100F	1	£7,454.00	£2,656.00	£744.00
Site 5	5	60F	1	£1,855.00	£1,842.00	£744.00
Site 6	5	70F	1	£2,133.00	£1,884.00	£744.00
Site 7	6	60F	1	£1,855.00	£1,842.00	£744.00
Site 8	6	60F	1	£1,855.00	£1,842.00	£744.00
Site 9	6	70F	1	£2,133.00	£1,884.00	£744.00
Sub-Total Cost				£130,657.00	£53,330.00	£26,040.33

9.2. Application (Capital) Charges

Description	Quantity	FourNet Software Including 5 Years FortiCare Premium
FortiAnalyzer-VM Subscription License with Support aligned to Managed Service term Subscription license for 50 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service.	1	£31,240.00
FortiManager-VM Subscription License with Support and BPS aligned to managed service contract term including Subscription	1	£5,340.00

 FourNet	4net Technologies Ltd Network Services 2 (RM3808) Service Offering	Crown Commercial Service Supplier
license for 10 devices/vdoms managed by FortiManager VM S-series. FortiCare Premium support plus FortiCare Best Practice services included.		
Endpoint-based Licenses – VPN/ZTNA (On Premise Deployments) aligned to Managed Service contract term, including FortiClient VPN/ZTNA Agent Subscriptions for 800 endpoints , includes on-prem EMS and FortiCare Premium.	1	£30,652.00
Sub-Total Cost		£67,232.00

9.3. Total Contract Value

Description	Price
FourNet Hardware – Including 5 Years FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	£130,657.00
FourNet Professional Services	£53,330.00
FourNet Software – Including 5 Years FortiCare Premium	£67,232.00
FourNet Managed Service (Year 1)	£26,040.33
FourNet Managed Service (Year 2)	£26,040.33
FourNet Managed Service (Year 3)	£26,040.33
3-Year Total Contract Value	£329,339.99

9.4. Notes:

1. The Managed Service calculation covering all sites has been split as follows, Site 1: 40%, Site 2: 40%, All other sites equally share the remaining 20%. Service maintenance charges shall commence upon delivery of the equipment to the relevant site.
2. Where FourNet purchases items in currencies other than GBP, costs may vary due to fluctuation in exchange rates and FourNet reserve the right to reflect this upon order and/or contract renewal/extension
3. All costs are exclusive of VAT
4. This Service Offering has an Initial Call Off Period of 3 years with an optional 2-year extension.
5. Payment Milestones are as follows:
 - a. Capital Expenditure invoiced following acceptance of the agreed Milestone Deliverable
 - b. Operational Expenditure invoiced yearly in advanced. The Managed Service calculation covering all sites will be split as follows, Site 1: 40%, Site 2: 40%, all other sites equally share the remaining 20%. Service maintenance charges shall commence upon delivery of the equipment to the relevant site.
6. Schedule 8 (Guarantee) does not apply to this Service Offer.

10. Supporting Documents

1. RM3808-Lot 1-4net-033 – Fortinet EULA

----- End of Document -----