SCHEDULE N: SERVICE DEFINITION FOR CENTRALISED FIREWALL SERVICE

1. Service Description for Centralised Firewall Service

Vysiion will provide to the Customer and manage a dedicated virtual instance on Vysiion's multi-tenant Next Generation Unified Threat Management (NG UTM) virtual firewalls. The Centralised Firewalls are Vysiion Equipment; ownership will not pass to the Customer. The Centralised Firewall Service comprises of the following mandatory components, to the extent set out on the Order Form:

- Provision of a Centralised Firewall Virtual Instance on Vysiion's Firewall Appliances (in the form of a Virtual Domain (VDOM));
- Vysiion Management.

1.1 Centralised NG UTM Firewall

Vysiion offers a managed Centralised Next Generation Unified Thread Management (NG UTM) Firewall Service as an add-on to an Internet VLAN over a Smart Wires Service. The Service comprises of a configured High Availability (HA) pair of virtual firewall devices within Vysiion data centres with NG UTM licensing, providing resiliency as part of the standard service. The Customer will be setup with (i) a dedicated virtual firewall(s) instance with NG UTM licensing on the Vysiion physical infrastructure and (ii) a connection to the Customer's LAN as part of an Internet Virtual Circuit (VC) over a Smart Wires service (subject to contract). Vysiion maintains full access to the firewall and carries out management using secure protocols (SSH, HTTPS etc.) via the Vysiion management infrastructure. The Customer recognises that a managed firewall is part of an overall security policy and does not guarantee total security (for example, vulnerabilities may exist in traffic flows that are permitted by the firewall policy).

The NG UTM consists of configurable services on the devices that can provide:

- Threat Prevention
- Anti-Virus
- Application Control
- User Identity
- Intrusion Prevention
- Content Filtering

1.1.1 Centralised NGUTM Features

The feature specifications for this service are detailed in the following table.

Centralised NGUTM Features Per VDom	
Maximum Firewall Throughput (Mbps)	500
Maximum Concurrent Sessions	20,000
IPSec VPNs	15
Remote Access SSL VPN users	100
Maximum number of Zones	3*
Maximum number of Firewall Policies	500**
MAC address limit	64

**Additional Zones are subject to additional charges.*

*** Subject to chosen Implementation Package (See section 1.2 Vysiion Implementation)*

1.2 Vysiion Implementation

For implementation of Centralised firewall, the Customer will be required to contract with Vysiion for its Next Generation Managed Firewall Implementation Service (see Schedule D).

1.3 Vysiion Management

A total of ten (10) hours of engineering time per calendar month to effect changes to the Customer's vDom shall be provided at no additional charge, with each change accounting for at least 1 hour of engineering time. For additional engineering hours or priority changes that sit outside change request target lead times, the Vysiion Service Desk will

advise the cost and will need customer acceptance via email that the cost has been accepted before proceeding with the Change. Changes requested will normally only be carried out during Normal Business Hours.
Change request target lead times as follows:

- Standard and Normal changes – 48 hours
- Emergency – 24 hours*

**Emergency Changes should be reserved to restore service, prevent a service impact, or restore a degraded service as determined by Vysiion acting reasonably.*

2 Centralised NGUTM Service Demarcation Point (SDP)

The SDP for the Centralised NGUTM Service is the SDP of the associated Smart Wires Service.

3 Centralised NGUTM Service Level Agreement

Target Availability

Availability is defined as the firewall service appliance(s) being able to process a network packet (not blocked by firewall policy), maintain a firewall session and remain connected to Vysiion's management platform.

	Target Availability
Centralised Firewall Service	99.99%

Service Credits

	Measure	Service Credit*
Availability	>0.1 Below Target	10%
	>1 Below Target	20%

** The Service Credit is applied as a percentage of the Monthly Charge for the Centralised Firewall Service only.*

4 Remote Access VPN

The Centralised Firewall Service includes a Remote Access VPN capability, where users can establish a connection to the firewall appliance(s) over the internet to provide an on-demand connection to the Customer corporate network over an encrypted connection, relying on IPSec or SSL VPN technologies, as the vendor software allows.

Any Remote Access VPN connection should only be established using a secure method supporting multi-factor authentication (additional charges may apply), integrating an external identity provider via RADIUS, LDAP, or SAML. Configuring the Remote Access VPN capability with local accounts, or other single-factor authentication solutions, is not permissible and shall not be done by the Customer.

It is the Customer's responsibility to ensure the client software and end user device is configured correctly, maintained, and updated. Where FortiClient is used to initiate a connection to the Remote Access VPN, Vysiion is unable to provide FortiClient software support without the Customer ordering the FortiClient Enterprise Management Server Service (see Schedule I).