PRODUCT ANNEXURE - FIREWALL SERVICES

1. INTRODUCTION

This Annexure sets out the legal framework for the provision and use of Firewall Services provided by the Supplier. This Product Annexure is subject to and must be read in conjunction with the Supplier terms and conditions located at https://saicom.io/. The nomenclature used in the Agreement shall apply to this Product Annexure.

2. DEFINITIONS

2.1. **Application Control** - protects servers by allowing or denying network application usage based on policies established by the network administrator. Enterprise applications, databases, web mail, social networking applications, IM/P2P, and file transfer protocols can all be identified accurately by sophisticated detection signatures. Application Control signature updates are provided via the global distribution network.

2.2. **IPS** - Intrusion Prevention System detects threats against the network and/or hosted environment to proactively block attacks. The IPS Service is an integrated hardware and software platform based on best of breed architecture. IPS delivers protection from known, zero day and denial of service (DoS) attacks including malware and underlying vulnerabilities.

2.3. **Layer 2** - The data link layer, or layer 2, is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment.

2.4. **UTM** - Unified Threat Management consolidates multiple security and networking functions with one unified appliance that protects businesses and simplifies infrastructure.

2.5. **VDOM** - Virtual Domains are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units.

2.6. **VPN** - Virtual Private Network. A configuration that allows remote users to connect to the Firewall, and access resources behind it securely.

3. HOSTED FIREWALL SERVICES

3.1. The Fortinet Hosted Firewall service is provided by a virtualized Fortigate Firewall device hosted on the Supplier's network that provides access control (firewalling) for a Customer that connects to the Supplier network via Layer 2 fibre services and/or Layer 2 wireless services.

3.2. The Service comprises 1 x VDOM (Virtual Domain) which equates to 1 Firewall instance.

3.3. The ruleset to be applied by the Supplier is dictated by the Customer. As the enforcer of the IT security policy, which the Customer dictates, the Supplier takes no responsibility for rules which are requested via the official channels, even if those rules lead to undesired effects.

3.4. All changes to the ruleset must be communicated via email. Only changes from authorised technical contacts will be enacted.

3.5. The Customer may have read-only access to their VDOM, upon request.

3.6. Unified Threat Management (UTM) services are an optional extra. The UTM services offered by the Supplier are:

3.6.1. Web Filtering

3.6.2. Application Control

3.6.3. Intrusion Prevention System (IPS)

3.6.4. User authentication (for Customers with Microsoft Active Directory)

3.6.5. Up to 3 IPSEC tunnels per VDOM

4. DEDICATED / ONSITE FIREWALL SERVICES

4.1. The Onsite Firewall service is an appliance provided by the Supplier to facilitate access control (firewalling) for a Customer’s Internet access. The firewall is placed in-line and forms the gateway between the private network and the public Internet.

4.2. The Service comprises of a physical Fortinet Firewall device.

4.3. The ruleset to be applied by the Supplier is dictated by the Customer. As the enforcer of the IT security policy, which the Customer dictates, the Supplier takes no responsibility for rules which are requested via the official channels, even if those rules lead to undesired effects.

4.4. All changes to the ruleset must be communicated via email to our Support Desk. Only changes from authorised technical contacts will be enacted.

4.5. The Customer may have read-only access to their FortiNet, upon request.

4.6. Unified Threat Management (UTM) services are an optional extra if not purchased with the original firewall solution. The UTM services offered by the Supplier are:

4.6.1. Web Filtering as defined by the Fortinet Model specifications

4.6.2. Application Control as defined by the Fortinet’s Model specifications

4.6.3. Intrusion Prevention System (IPS) as defined by the Fortinet Model specifications

4.6.4. User authentication (for Customers with Microsoft Active Directory)

4.6.5. IPSEC Tunnels as defined by the Fortinet Model specifications

5. FIREWALL REPORTING - VFAZ

5.1. Firewall reporting is an optional extra, which can be provided by the Supplier’s Virtual FortiAnalyzer (VFAZ) service.

5.1.1. Live logs are stored for 30 days, and archived logs are available for a further 30 days.

5.1.2. Should longer retention be required, the Supplier can facilitate on a case-by-case basis.

5.1.3. The amount of logs determines the monthly cost for log storage. Please refer to the Supplier price list for log volume costing.

5.2. For onsite firewalls, transmission of logs from the firewall to the VFAZ service inherently utilises some of the customer’s available WAN bandwidth.

6. REMOTE ACCESS SERVICES - VPN CUSTOMER

6.1. Should Remote Access Services be required, secure VPN customer functionality would be supplied by Supplier. This service allows remote users to securely connect to corporate resources, behind the firewall, over the public Internet. This functionality would be provided by the Forticustomer software.

6.1.1. For Hosted Firewall services, the service is based on a per-user billing model. Each additional user would require their own account configured on the FortiGate firewall. No sharing of user accounts is permitted.

6.1.2. For Dedicated/onsite firewall services, the Firewall’s capability determines the number of user accounts that can be accommodated. In other words there is no charge for additional VPN users, provided the Firewall’s performance is not hindered by the additional VPN users.

6.1.3. Forticustomer must be downloaded and installed by the end user (or Customer IT administrator) and installed onto a supported version of Windows / MacOS / Linux / Apple IOS / Android.

6.1.4. The configuration profile will be supplied by the Supplier to the authorised Security Technical Contact/s. This will include the public IP address of the Firewall. It is the Customer’s responsibility to create a DNS entry for this IP address if required.

6.1.5. Static (local) usernames and passwords will be configured on the Customer's FortiGate VDOM. Should LDAP integration into Microsoft Active Directory be required, this would incur an additional installation cost, which will be quoted case by case basis prior to project commencement.

6.1.6. End user support would be performed by the Customer's IT administrator. The Supplier will support the administrator as part of the normal technical support process. Password resets should be logged by the authorised IT administrator, via email. New passwords may be sent directly to end-users via email.

6.1.7. SSL certificate not included by default, can be provided on a case-by-case basis, at an additional cost.

7. SERVICE FEES AND CHARGES

7.1. Service Fees shall be provided at the rates set out in the Supplier pricing plan at the time of subscription, plus applicable taxes. The Supplier may from time to time modify the Service Fees.

END OF ANNEXURE