Master Services Agreement:

Annexure C: Service Schedule – Secure Cloud Gateway Services V10-11

GLOBAL MICRO
Intelligent Technology

This Service Schedule for **Secure Cloud Gateway Services V10-11** (the "Service") replaces all previously signed/incorporated version(s) of the Service Schedule(s) for Secure Cloud Gateway Services (if any). It forms part of the Master Services Agreement and Master Services Schedule. Its provisions are an integral part of the Master Services Agreement. Words and expressions defined in the General Conditions and Master Services Schedule shall (unless otherwise defined in this Services Schedule) bear the same meanings where used in this Service Schedule. In this Service Schedule, the following words and phrases shall have the following meanings unless the context otherwise requires:

1. Interpretation

1.1. "**Secure Cloud Gateway Suites**" means a collection of Services, options and showcase features that have been bundled together and provide (i) a convenient way to order and (ii) at a lower fee than when ordered separately;

1.2. "**SD-WAN**" means Software-Defined Wide Area Network;

1.3. "**SOC"** or "**Security Operations Centre**" means SP's helpdesk;

1.4. "**SOC Analyst"** means an SP's Tier 2 or Tier 3 support engineer.

2. Service Overview

2.1. Secure Cloud Gateway Services provides **Secure Cloud Gateway Appliances** based on Fortigate™ technology. SP will provide device management, health monitoring, security analysis and customer reporting.

3. Standard Features of Secure Cloud Gateway Appliances

3.1. The Secure Cloud Gateway Appliance includes installation, management and support for the following components:

3.1.1. Intrusion Prevention Service;

3.1.2. Firewall;

3.1.3. Anti-Virus Protection;

3.1.4. Application Intelligence and Control;

3.1.5. Anti-Spyware;

3.1.6. Content & URL Filtering (CFS);

3.1.7. Wireless LAN support;

3.1.8. VPN Tunnels (subject to additional charges);

3.1.9. Multi-WAN Support.

4. Secure Cloud Gateway Appliance Management

4.1. **Pooled Support Units**

4.2. Customer shall be entitled to **up to 1000 (one thousand) Pooled Support Units per month per Secure Cloud Gateway Appliance** ('**Pooled Support Allocation**').

4.2.1. Once the monitoring agent(s) are successfully installed, SP will only allocate Support.

4.2.2. After that, SP will decrement Pooled Support units from the Pooled Support Unit Allocation for work performed in response to monitoring alerts and/or on an as-needed basis or according to the areas of SP responsibility outlined in paragraphs 4.3 to 4.15 below:

4.3. **Availability Monitoring**

4.3.1. SP must be able to connect to the device via the Internet using HTTPS & IPSEC protocols.

4.3.2. SP will perform availability monitoring of the Secure Cloud Gateway Appliance. SP monitors availability via periodic polling of the device. If regular polling checks indicate that the device has become unavailable, the SP is altered, which generates a service ticket. If the root problem of device failure is Customer-related, such as a network change, outage, or Customer-managed device, SP will provide the Customer with troubleshooting information upon Customer request. SP is not responsible for troubleshooting issues not directly related to the Secure Cloud Gateway Appliance under management.

4.4. **Appliance Event Monitoring**

4.4.1. The SP's Global Management System gathers log data.

4.4.2. The data is parsed, correlated, and prioritized.

4.4.3. SP categorizes the relevant security events based on the severity level.

4.4.4. Malicious and unknown events are correlated, which raises alerts.

4.4.5. SP will provide access to service ticket requests, reporting capabilities, and ongoing enterprise security event aggregation and reporting for each Secure Cloud Gateway Appliance.

4.4.6. Note: Incident response, forensics and ticket requests associated with security event analysis are **not included** and must require a separate Reserved Support Services Subscription.

4.5. **Software Upgrade and Patch Maintenance**

4.5.1. As security-related software patches and upgrades are released, SP assesses each release's applicability to the Customer's environment. SP will work with the Customer to schedule any necessary remote upgrades.

4.5.2. Upgrades are implemented by SP so long as the following conditions apply:

4.5.2.1. The upgrade can be performed remotely, independently, or with minimal on-site assistance from the customer.

4.5.2.2. The upgrade does not require a change to the underlying hardware.

4.5.3. SP will communicate new platform migration options when the vendor or SP discontinues support for a product or product version. To be assured of uninterrupted service, the Customer must complete the migration process within 60 (sixty) days. The customer bears any costs for procuring new hardware or components and re-provisioning devices.

4.5.4. SLAs do not apply during maintenance work. SLAs cannot be guaranteed if the Customer does not make the changes SP requires or if the Customer otherwise prevents SP from making the changes necessary for continued service.

4.6. **Firewall Policies**

4.6.1. An Authorised Technical Contact may submit change requests for firewall policies via the Support Desk.

4.6.2. The following defines the type of policy changes that may be requested:

4.6.2.1. Adding, deleting, or modifying up to three individual Network Address Translations (NAT) (incoming, outgoing and loop-back), including object creation;

4.6.2.2. Adding, deleting, or modifying up to two access control list changes (such as to permit or deny changes), including the creation of up to 6 policy objects creation (Hosts, Groups, Networks, Ranges and Service objects);

4.6.2.3. Adding, deleting, or modifying up to two individual network routes within the firewall;

4.6.3. The standard policy change may comprise one or more of the above bullets. SP may complete any change request not explicitly listed above on a time and materials basis. SP reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of the Customer's service.

4.6.4. Note: Design or validation of rule sets or troubleshooting related to rule sets is **not included** and requires a separate Reserved Support Services Subscription.

4.7. **Intrusion Prevention System**

4.7.1. SP manages the policy on the device. The SP will review updated policies when vendors release them.

4.7.2. The following defines what one policy change is:

4.7.2.1. Adding, deleting, or modifying IDS/IPS signatures, not including routine signature updates;

4.7.3. Note: Any change request not explicitly listed above is **omitted** and requires a separate Reserved Support Services Subscription.

4.8. **Application Intelligence and Control**

4.8.1. SP can enable application control per the Customer's request. Over 1600 applications are supported by the Secure Cloud Gateway Appliance. Therefore, it is the Customer's responsibility to specify all required application control and application rule settings. SP will configure the appliance per the Customer's specifications.

4.8.2. Note: SP does not offer application debugging in the event of unexpected consequences from application control settings. SP's application control responsibilities are limited to turning the application control settings on or off. Application Intelligence and Control are turned off at the initial deployment. SP may (in its sole discretion) offer application debugging as part of a separate Support Services Subscription.

4.9. **Anti-Virus Protection support**

4.9.1. SP can enable Gateway anti-virus ("**GAV**" hereafter) functionality on Secure Cloud Gateway Appliances. As a service component, SP will work with the manufacturer to update GAV policies regularly as SP releases and reviews updates. Security-relevant AV events are logged but will not result in ticket creation or viewing by an SP's SOC Analyst.

4.9.2. Note: Enforced Client AV protection is not supported.

4.10. **Anti-Spyware**

4.10.1. SP can enable Gateway anti-spyware ("**GAS**" hereafter) functionality on Secure Cloud Gateway Appliances. As a component of this service, SP will regularly update GAS policies as updates are released and reviewed by SP.

4.10.2. Security-relevant GAS events are logged but will not result in ticket creation or viewing by an SP's SOC Analyst.

4.11. **Content & URL Filtering (CFS) support**

4.11.1. When the Subscription includes a CFS license, SP shall deploy the default categorization policy by zone or internet protocol ("IP") range as specified by the Customer. Websites specified within a category will be blocked. Customers who wish to challenge a categorization shall contact the Appliance manufacturer directly.

4.11.2. Customers can request a change of category as a standard policy change request. Requests for allow-listing or deny-listing of domains are standard policy change requests. User authentication for the CFS service is not supported.

4.12. **Wireless LAN support**

4.12.1. SP will deploy a trusted network, a guest network (2 SSIDs), and up to 8 Wireless Access Points (subject to an additional Subscription and charges).

4.12.2. The following defines what one policy change is:

4.12.2.1. Addition/deletion of a Wireless Access Point;

4.12.2.2. Modification of an SSID;

4.12.2.3. Modification of a pre-shared key;

4.12.3. The customer is responsible for configuring the LAN infrastructure connecting to Wireless Access Points. SP will not perform wireless LAN availability monitoring and cannot assist with individual wireless client connectivity issues.

4.13. **Multi-WAN Support**

4.13.1. The Customer can specify a single WAN (Ethernet) or multi-WAN (Ethernet and 3G) at set-up time. It is the Customer's responsibility to provide and maintain the 3G service. SP shall set up and test multi-WAN functionality.

4.13.2. The following defines what one policy change is:

4.13.2.1. Change of ISP connection or network preference.

4.13.3. Note: SP is not responsible for advising Customers about network priority changes. SP may (in its sole discretion) offer application debugging as part of a separate Support Services Subscription.

4.14. **VPN Configuration**

4.14.1. SP configures VPN connections for Secure Cloud Gateway Appliance, which is contractually managed by SP, and troubleshoots the device during an outage. SP requires management of all appliances when providing this Service. The Secure Cloud Gateway Appliance model and Subscription govern the number of VPN tunnel configurations permitted. Site-to-site VPN configuration uses SP standard VPN templates. SP does not warrant the Secure Cloud Gateway Appliance's ability to interwork with 3rd party firewalls managed by other parties. SP is not required to assist with remote device configuration.

4.14.2. SP can configure the Secure Cloud Gateway Appliance to accept Global VPN Client ('GVC') connections. It is the Customer's responsibility to set up the GVC.

4.15. **Secure Cloud Gateway Appliance Exclusions**

Any other services are out-of-scope. Examples of such out-of-scope support include but are not limited to:

4.15.1. On-site installation and provisioning of the device;

4.15.2. Integration of complementary products that SP does not manage (e.g., encrypted email, web reporting software);

4.15.3. Custom analysis or custom reports;

4.15.4. Forensics;

4.15.5. Any change requests not specified above;

4.15.6. Configuration of any tunnel end-points which do not terminate on an SP-managed device;

4.15.7. Ruleset design, validation, and troubleshooting;

4.15.8. Firewall policy auditing, policy/rule utilization, and security best practice consulting;

4.15.9. Development of customized signatures;

5. Secure Cloud Gateway Appliance Implementation

5.1. Each new Secure Cloud Gateway Appliance shall be shipped directly to the customer from SP. The Customer shall bear responsibility for the shipping costs.

5.2. The Secure Cloud Gateway Appliances shall be deployed and configured remotely by SP with a standard deployment configuration and on-site support from the customer.

5.3. Existing equipment is provisioned remotely, with on-site support from the Customer.

5.4. Secure Cloud Gateway Appliance remote start-up and configuration includes the following configuration deliverables. Not all deliverables may be applicable based on the appliance model, firmware version or Customer requirements. Any configuration requests not included in the standard configuration deliverable will require an approved change request.

5.4.1. Loading the latest firewall firmware;

5.4.2. Activating the service license keys and enabling security services;

5.4.3. Configuring administrator accounts;

5.4.4. Specifying mode of operation, zones, IP address, subnet mask, hostname, static routes, DNS, SYSLOG;

5.4.5. Setting up the firewall policy consists of the following elements. Firewall access rules, Network address translation rules, VLAN creation and Object creation (Hosts, Groups, Networks, Ranges and Service objects) up to the maximum number of policy elements included in the Subscription;

5.4.6. Enabling wireless security features (wireless appliances only) – intrusion detection and wireless guest services.

5.4.7. Service **does not include** wireless configuration on end Customer devices (e.g. Laptops or Mobile devices);

5.4.8. Setting up VPNs: site-to-site and Customer-to-site (subject to the provisions of 4.14);

5.4.9. Setting up SSL VPN for remote access (on-firewall local user authentication database is not supported). Setting up user-level authentication using external authentication servers where the customer has provided all the required authentication server parameters;

5.4.10. Setting up a single WAN interface only;

5.5. SP provides telephone support to Customer contact at the implementation site while installing all Customer premises equipment.

5.6. Once the Customer's premises equipment is in place, SP will access the device(s) remotely and perform the remaining configuration and service activation tasks, which may require device downtime.

5.7. Customers must provide SP with exclusive administrative privileges. Firewall policy migration services are not part of the Secure Cloud Gateway Appliance Service.

5.8. SP will provide the Customer with a notice of service commencement, which identifies the service commencement date when the following conditions have been met: SP has (a) established communication with the relevant Customer device(s), (b) verified the availability of customer data on the portal, and (c) confirmed connections via SP's Global Management System.

6. Additional Conditions for Secure Cloud Gateway Appliances

6.1. The Service provides the Customer with robust device management, security event analysis and performance monitoring. The Service does not achieve the impossible goal of risk elimination. Therefore, SP does not guarantee that intrusions, compromises, or other unauthorized activity will not occur on the Customer's network.

7. Technical requirements

7.1. The minimum system requirements, as described in the schedules, are incorporated by reference.

7.2. The customer will provide access to Customer-premises and relevant appliance(s) necessary for SP to manage and monitor the contracted Secure Cloud Gateway Appliances. Additionally, the Customer should communicate any network or system changes that could impact service delivery to the SP. Service activation, which may require device downtime, will depend on customer deliverables such as on-site assistance with the appliance's initial configuration to connect the Customer's site to SP's data centres. SLAs will not apply to devices that are experiencing Customer-caused connectivity issues.

8. Service Availability

8.1. Service Availability, as described in the schedules, is incorporated by reference.