superloop

Managed Firewall Service Schedule

This Service Schedule forms part of the Agreement between You and Superloop and is applicable to Services entered into between You and Superloop from 1 April 2026.

1. Service Description

1.1 General

The Service is comprised of the following items ("Managed Firewall as a Service" or "Service"):

(a) Managed Firewall Device (or Devices, as per the Service Order);

(b) Software licences for the use of the Managed Firewall Device and cloud services;

(c) The provisioning of the Managed Firewall Device in accordance with the agreed architecture;

(d) Each site's Managed Firewall Device installation and configuration will consist of:

(i) On-site installation, deployment and testing;

(ii) Securinge and baselininge the firewall – harden administrative access (role-based access, MFA, restricted management interfaces), configure core system settings, and prepare certificates where SSL/TLS inspection is required;

(iii) Establishing network and connectivity – define security zones, routing, and high availability (if applicable), and deploy secure remote access and site-to-site VPN connectivity;

(iv) Implementing policy and protection – design or optimise a least-privilege rulebase and apply next-generation security services (IPS, anti-malware, web filtering, application control, DNS security) with appropriate SSL inspection;

(v) Enablinge visibility and integration – integrate with identity services, configure centralised logging (to the standard cloud logging service), and enable monitoring, alerting, and reporting;

(vi) Remote testing with Superloop provisioning Engineers;

(e) Establish remote support standards and testing including:

(i) Ensuring the device is connected and reachable;

(ii) Ensuring monitoring standards are configured and functioning as expected;

(iii) Working with Your site contact and Your IT staff to complete Your acceptance testing;

(iv) Troubleshooting and resolving any issues with Your acceptance testing;

(f) Site handover and go live;

(g) Configuration and Access for you to the Managed Firewall Device Management Portal (where applicable);

(h) Establish configuration backup of the Managed Firewall, and;

(i) Establishing the schedule for ongoing software upgrades to the Managed Firewall Device as needed and determined by Superloop.

1.2 Managed Firewall Device Management Portal

The Managed Firewall Device Management Portal allows Superloop to:

(a) Configure the Managed Firewall Device;

(b) Provide some of the monitoring and analysis of your Managed Firewall Device; and

(c) Identify issues, inefficiencies or delays with the network.

1.3 Managed Firewall Device Licensing

(a) All Managed Firewall Devices are licensed based on the ability to provide at a minimum, Advanced and Unified Threat Protection.

(b) Your Advanced and Unified Threat Protection License is as listed on your Service Order.

(c) Vendor support to provide RMA service.

(d) Managed Firewall Device Management Portal licensing.

1.4 Assessment and Release of Liability

(a) You must make your own assessment of the information and any recommendations provided by Us and must satisfy Yourself as to its appropriateness for Your specific requirements, prior to implementing any recommendation We provide.

(b) For the avoidance of doubt, Superloop's obligations are strictly limited to the Services described in this Service Schedule. Superloop has no liability whatsoever for any service, scope of works, activity or matter that is not listed in this Service Schedule.

(c) Furthermore, The Customer agrees and acknowledges that Superloop will configure the Service as per your guidance. You are responsible for providing the information needed and for approving the design of the Service.

(d) Superloop excludes all liability for any and all direct Loss and Consequential Loss, including in relation to any negligent act or omission of Superloop in installing, configuring, deploying or maintaining the Services for the Customer.

1.5 Logging

(a) Superloop's standard logging and analytics platforms are based on the chosen vendor's platform. This is FortiGate Cloud, FortiAnalyzer Cloud or Strata Cloud Manager, Superloop will setup and confirm the platform as per the Service Order which includes where licensed basic ingestion.

(b) As Standard Superloop Provides FortiGate Cloud and Strata Cloud Manager Essentials without SLS.

(c) FortiGate Cloud provides 1 year of log retention.

(d) Strata Cloud Manager Essentials does not provide any logging capability without an SLS add-on. If an SLS add-on or SCM Pro is chosen by the customer, these add-ons provide 1 year of log retention.

(e) If FortiAnalyzer Cloud is required and listed on your Service Order, this service is licensed per device and requires at least 1 device with FortiAnalyzer Cloud licensing within Your environment to setup the baseline FortiAnalyzer Cloud environment.

(f) To deliver centralised logging and threat visibility with FortiAnalyzer Cloud without requiring additional log ingestion licenses (which can be purchased in addition to the standard device license), Superloop are required to advise all customers of the following logging limitations which Fortinet have enforced based on daily ingestion entitlements per FortiGate form factor:

Form Factor/Mode	Device Class	FAZ Cloud Logging Entitlement
FG-40F to FG-90G	Small (Desktop)	200 MB/day
FG-100F to FG-600F	Medium (1RU)	1 GB/day
FG-1000F & above	Large / Enterprise (2RU)	5 GB/day

(g) Superloop are ~~NOT~~ not responsible for ensuring all logs are ingested into the required logging platform, especially if any limits enforced are reached by You, as each customer, site and usage differs.

(h) Log Ingestion Add-ons (for all Vendor environments) and log analytics can be added to a customer environment if required.

2. Provision of Services

2.1 Feasibility Study for related Internet Access (if any)

If a related ~~S~~service of a different type to the Managed Firewall Service requires a successful Feasibility Study to proceed and the relevant Feasibility Study is not successful, then Superloop may stop work on and may cancel, the Service Order for the relevant Managed Firewall Service.

2.2 Provisioning

(a) Superloop will endeavour to provision the Managed Firewall Service to the Site by the Ready for Service (RFS) Date in accordance with Good Industry Practice.

(b) The Managed Firewall Device LAN Interface is Superloop's demarcation point with You.

(c) Where a Third-Party network is used, the Service demarcation location within the Site will be confirmed with You and the Third Party prior to installation and provisioning of the Managed Firewall Service.

(d) The deployment and delivery of the Service is limited to a single on-site or remote visit conducted during standard business hours (Monday to Friday, excluding public holidays). Any additional visits, after-hours work, or extended engagements outside this scope may be subject to additional costs.

(e) The following table outlines the Managed Firewall standard setup limits, these limits are applied as standard without additional costs and are not reflective of any technical limitations;

Category	Standard Limit / Best Practice
Security Profiles / Security Services	Use vendor-recommended default security profiles (Fortinet UTP / Palo Alto Security Profiles) with minimal tuning. Apply to all outbound and inbound security-relevant traffic.
URL Filtering	Block malicious, high-risk, and phishing categories by default. Optionally block Acceptable Use (AUP) categories such as gambling or adult content based on customer requirements.
SSL Inspection	Minimum standard: inspect high-risk or unknown categories. Avoid full TLS inspection in baseline configuration unless explicitly required due to performance and privacy considerations.
Logging	Log all security events and session summaries. Enable enhanced logging only when required. Packet captures are for troubleshooting only and not part of standard operations.
Outbound Policies	No more than 3 consolidated outbound rules (LAN → Internet) with all required security services enabled (UTP/Security Profiles). Avoid granular per-application rules in the baseline build.
Inbound Policies	Only include business-required published services. Apply full security profiles to all inbound policies. Use VIPs/NAT policies according to vendor best practice.
VPN – Remote Access	Standard: no more than 2 user groups/pools (e.g., staff, admin). Enforce MFA where supported. Limit access strictly to approved subnets and services.
VPN – Site-to-Site (IPSec)	Standard: no more than 3 sites, each with redundant tunnels. Use route-based VPNs on both platforms. Apply relevant security profiles where feasible.
Rulebase Size	Maintain a clean policy set with no more than 50 rules in standard deployments. Aggregate rules by business function rather than per-application or per-user rules.
Profiles / Objects	Maintain one global set of security profiles (UTP profiles / Palo Alto Security Profiles) reused across policies. Avoid creating rule-specific or duplicated profiles.

3. Your obligations

3.1 Address information

(a) You must provide accurate and complete Site address information to Superloop for deploying the Managed Firewall Service. You may be liable for any costs incurred by Superloop due to any incorrect, false or misleading information You provide.

(b) If You change the Site prior to the delivery of the Service, You must pay Superloop's reasonable costs and fees (if any) arising from the change of Site.

3.2 Provisioning

In order for Superloop to provision the Service, you must:

(a) Install and maintain any cabling between the Managed Firewall Device and Customer Equipment and if you are unable to do so, You may request that Superloop do so on Your behalf, at Your cost, and any such cabling is deemed Customer Equipment for the purposes of the Agreement.

(b) Prepare and maintain the Site(s) for the installation of the Managed Firewall Device, including:

(i) providing a suitable and safe operational environment for the Managed Firewall Device, including connection points and a secure, accessible continuous power supply at the Site(s) for the operation and maintenance of the Managed Firewall Device, in accordance with Superloop's reasonable instructions and applicable installation standards; and

(ii) ensuring the required space at appropriate network facilities and a specified location for the Managed Firewall Device, in time to allow Superloop to meet its obligations, and to undertake any necessary installation or maintenance.

(c) Acknowledge and agree that You are responsible for ensuring the operational health and safety of all network infrastructure provisioned under this Service Schedule, including the safety of any persons installing, maintaining, or working on the infrastructure, in compliance with applicable laws, regulations, and industry standards.

(d) The deployment and delivery of the Service is limited to a single on-site or remote visit conducted during standard Business Hours (Monday to Friday, excluding public holidays). Any additional visits, after-hours work, or extended engagements outside this scope may be subject to additional costs.

3.3 Superloop Equipment

Superloop Equipment refers to all physical or virtual Managed Firewall Devices located on Your premises or located in your Azure environment.

3.4 Rack space, Power and Heating / Cooling

You must provide an adequate and suitable space, power supply and environment for all equipment used in connection with the Service.

3.5 Ownership of Superloop Equipment

Superloop Equipment will remain Superloop's property at all times, any risk in Superloop Equipment will pass to you upon delivery, whether or not the Superloop Equipment has been installed.

3.6 Virtual Devices

(a) For the avoidance of doubt, our responsibilities under this Service Schedule extend only to the supported virtual device itself, including its configuration, policy management, and any associated service levels relating to configuration and operation of the device.

(b) We do not provide, manage, or support the underlying infrastructure on which the virtual device resides, whether such infrastructure is hosted on-premises, within a public cloud environment, or on any third-party platform. All responsibilities relating to the provision, operation, maintenance, availability, patching, and backup of the supporting infrastructure shall remain the sole responsibility of You.

3.7 Use of Equipment

In relation to Superloop Equipment You will:

(a) Keep the Superloop Equipment safe, without risk to equipment health;

(b) Only use the Superloop Equipment, or allow it to be used for the purpose for which it is was provided under the Agreement;

(c) Not move the Superloop Equipment or any part of it from the Site(s) except as detailed in clause 7.1;

(d) Not make any alterations or attachments to, or otherwise interfere with, the Superloop Equipment, nor permit any person to do so, without Superloop's prior written consent;

(e) Not sell, charge, assign, transfer or dispose of or part with possession of the Superloop Equipment or any part of it;

(f) Ensure that the Superloop Equipment appears in Superloop's name in your accounting books;

(g) Where an Insolvency Event applies to you, immediately advise Superloop so that Superloop may take action to repossess the Superloop Equipment;

(h) Notify any interested third parties that Superloop owns the Superloop Equipment; and

(i) In addition to any other rights that Superloop may have, You must reimburse Superloop for any losses, costs, or liabilities arising from your use or misuse of the Superloop Equipment or where the Superloop Equipment is damaged, stolen or lost, except where the loss or damage to Superloop Equipment is a result of fair wear and tear or caused by Superloop.

3.8 Equipment related actions upon expiry or termination

At the expiry of the Service Term or upon a valid termination of the Managed Firewall Service by either party, You will:

(a) Provide Superloop with all reasonable assistance necessary to remove the Superloop Equipment from the Site(s);

(b) Disconnect any Customer Equipment from Superloop Equipment located at the Site(s);

(c) Not dispose of or use the Superloop Equipment other than in accordance with Superloop's written instructions or authorisation; and

(d) Promptly return or delete any confidential information that you have received from Superloop during the term of the Contract.

3.9 Co-management Obligations

Where You are granted any Write Access to the Managed Firewall platform the following applies:

(a) You will be responsible for managing your End User accounts. You must advise Superloop in writing when an End User exits Your business or otherwise no longer requires access.

(b) Where You are responsible for causing a Fault that results in the Service being down, this downtime will be counted as Excused Downtime for the purpose of Service Availability.

(c) Resolutions of Faults caused by You may attract a Time and Materials fee which will be payable by You to Superloop.

(d) Repeated Faults caused by You may result in the Write Access being revoked from that individual End User or Your whole organisation.

(e) Where possible, Roles Based Access Control will be used by Superloop to limit the Write Access, in relation to specific access requirements.

3.10 Access Risk

(a) Superloop excludes all liability for any and all direct Loss and Consequential Loss, including in relation to any negligent act or omission of Superloop in relation to Superloop's access to Your data and systems.

4. Maintenance

4.1 Planned Outage Periods

Superloop will, wherever reasonably practical in the circumstances, give You at least 10 days prior notice of any Planned Outage Period (Proposed Outage) and will consider any reasonable representations and requests by You in respect of that Proposed Outage. You acknowledge that such prior notice will not always be reasonably practicable, and that Your requests in respect of a Proposed Outage may not be acted on.

4.2 Minimise Disruption

Superloop will use its reasonable endeavours to minimise disruption to any affected Service arising from any Planned Outage Periods.

5. Faults and Fault Tickets

5.1 Reporting Faults

The Managed Firewall Device will notify the Superloop Support team of alerts and alarms which will be triaged to identify Faults. If you become aware of a fault which has not been identified by the Managed Firewall Device, you must promptly report that Fault to the Superloop Support team within the Agreed Coverage Period.

5.2 Fault classification

Faults are classified by Superloop in accordance with the following table:

Priority Matrix			
Impact	Urgency		
	High	Medium	Low
Managed Firewall	P1	P2	P3

High: 3+ services impacted or predefined Critical Customer Site offline

Medium: 1 or 2 services impacted

Low: Degradation (errors, congestion, packet loss, high latency)

5.3 Fault Tickets

Upon receiving a notification from the Managed Firewall Device of an issue that is identified as a Fault or upon receiving a Fault report from You, the Superloop Support team will assign a reference number to the Fault (Fault Ticket) and will issue that reference number to You.

5.4 Closure of Fault Tickets

When Superloop has remedied a Fault, it will notify You that the Fault Ticket is "closed".

5.5 Faults reported in error

If You report a Fault to the Superloop Support team in circumstances where the Service disruption is not due to a Fault within the Superloop Network (for example where the Service is unavailable due to an issue with Customer Equipment or a Third-Party network) or the Fault is due to an issue or damage caused by You, You will bear any and all costs incurred by Superloop to investigate the reported Fault.

5.6 Fault restoration target

Superloop will use its best endeavours to remedy each Fault within the Fault Restoration Targets (unless otherwise stated) in accordance with the Fault table set out below:

Fault	Response	Restoration Target (No Site Visit Required)	Restoration Target (Site Visit Required)
P1	15 minutes	4 hours	4 hours
P2	30 minutes	8 hours	8 hours
P3	4 hours (during business hours)	24 hours	End of next business day
P4	8 hours (during business hours)	3 Business Days	3 Business Days
Service Request	2 Business Days	n/a	n/a

5.7 Information updates

During the Remedy Period, the Superloop Support team will provide updates in respect of the progress of any Fault resolution to You where such information is reasonably available to Superloop.

6. Service Availability

6.1 Service Availability Target

(a) The Service Availability Target is calculated according to the Service Availability of the Managed Firewall Service only. For services offered in combination with network connectivity, SLAs for the network apply in accordance with the respective Service Schedules. For the avoidance of doubt, Customers' other Services as well as Excluded Services, which may include upstream or downstream functions, are not covered by this clause 6.1.

(b) Service Availability is calculated as per the equation below.

$$\textit{Service Availability} = \frac{\textit{Uptime - Excused Downtime}}{\textit{Total - Excused Downtime}} \times 100$$

Total = the total number of minutes in a calendar month.

Uptime = the number of minutes in each month where the link state of the Service is 'up', rounded to the nearest minute.

Excused Downtime = as defined in this Agreement.

(c) The Service Availability Target is 99.95% in a calendar month and Superloop endeavours to meet the Service Availability Target in any given month during the Service Term. No Service Credits will apply in relation to this Service if the Service Availability Target is not achieved.

7. Change Management

7.1 Relocations

(a) In the event You require a relocation of a Service to a new location, You must make a written request to Superloop in a manner nominated by Superloop. You acknowledge that not all Services can be relocated.

(b) Superloop will respond to Your request and advise, in its absolute discretion, whether the Service can be relocated.

(c) Where the Service can be relocated, a once-off fee may apply as well as a change to the Charges.

(d) Where the Service can't be relocated, or where You opt to terminate instead of relocate, Cancellation and other fees and charges may apply under the Agreement.

7.2 Upgrades / Changes

(a) You may at any time make a written request in a manner nominated by Superloop to upgrade the Service or to change the Service. Superloop will respond to Your request and advise, in its absolute discretion, whether the Service can be upgraded or changed. You acknowledge that additional fees and/or Charges may apply.

(b) We will upgrade the firmware of the Managed Firewall Device on a quarterly basis, subject to the availability of a new version. Before proceeding with any upgrade, we will assess the applicability of the new firmware version to your environment based on Superloop's recommendation and guidance. Should a firmware version address a critical security vulnerability or other urgent risk, the upgrade will be performed promptly to ensure the ongoing protection of your infrastructure. All upgrades will be scheduled with you in advance to minimise potential disruption to your operations.

7.3 Service Order

Where You make a request under clauses 7.1 or 7.2 which is accepted by Superloop, the parties will give effect to that change by signing the relevant change request form. In circumstances where the changes are substantial or involve an extension of the Service Term, the parties will enter into a new Service Order which, upon execution, will replace or amend the previous Service Order.

7.4 Variations by Third Parties

Without limiting Superloop's rights under any other clause of the Agreement, Superloop may, on written notice to You, vary this Service Schedule or a Service Order (excluding the Charges) if a Third-Party's supply terms or agreement with Superloop is varied, terminated or replaced and as a result Superloop considers (on reasonable grounds) that a variation to this Service Schedule or the Service Order is necessary.

8. Defined terms

Any capitalised terms in this Service Schedule, which are not defined below, have the meaning given to those terms in the Agreement. All other capitalised terms in this Schedule have the following meaning, unless the context otherwise requires:

Agreed Coverage Period means 24 hours a day, 7 days a week, 52 weeks a year.

Agreement means the agreement between Superloop and You (incorporating the General Terms, this Service Schedule, and any applicable Service Order) in relation to the supply of Services by Superloop to You, which is available at https:// superloop.com/legal/terms/.

Critical Customer Site or Critical Business Service means a Head Office, Data Centre, or any other site or business service expressly designated as critical in the Services Agreement.

Customer Equipment means all of the equipment used by You, including, but not limited to, cross-connects and cables, in connection with the Service that is not provided by Superloop.

Excluded Services refers to Services provided via Third Party network or Services which are qualified in a Service Order as being excluded.

Excused Downtime means the number of minutes in month, rounded to the nearest minute that the link state of the Service is 'down' due to:

(a) Your acts or omissions or the acts or omissions of Your End Users, agents, contractors or anyone You are responsible for;

(b) the acts or omissions of any Third Party or a fault on a Third Party's network;

(c) any failure, incompatibility or error in the configuration of Customer Equipment;

(d) Superloop suspending the Service in accordance with the Agreement;

(e) a Planned Outage Period as notified to You by Superloop or a third-party; or

(f) a Force Majeure Event.

Facility means each data centre where Superloop will provide the Service, as listed in the relevant Service Order.

Fault has the meaning given in clause 5.2, but excludes circumstances arising as a result of a Force Majeure Event or as a result of damage caused by You or Your staff, agents or contractors. For the avoidance of doubt:

(a) except to the extent that a Planned Outage Period exceeds the planned outage window notified in accordance with clause 4.1, Planned Outage Periods are not Faults for the purposes of the Agreement; and

(b) the failure of multiple Services over a single Fibre or device is treated as a single Fault.

Fault Restoration Target has the meaning given in clause 5.6.

Fault Ticket has the meaning given in clause 5.3.

Feasibility Study refers to a service qualification or Site survey.

Fibre means the optical fibre cable used to provide Services.

Good Industry Practice means the practice of a reasonable and prudent operator in the same business as the party required to comply with good industry practice.

Managed Firewall Device means a network security appliance that is actively monitored, configured, and maintained by a managed service provider (MSP) or security operations team. It enforces security policies, filters traffic, and protects against cyber threats while ensuring compliance with organisational and regulatory requirements. As part of a managed security service, the device receives regular updates, performance optimisation, and threat intelligence to safeguard network infrastructure against evolving threats.

Managed Firewall Device Management Portal means a centralised, web-based or software-driven interface that enables administrators and managed service providers (MSPs) to configure, monitor, and manage firewall devices remotely. It provides real-time visibility into security policies, threat activity, network traffic, and device performance. The portal typically includes functionalities such as rule management, logging, reporting, firmware updates, and automated alerts to ensure continuous security, compliance, and operational efficiency across managed firewall deployments.

Planned Outage Periods means the period during which Superloop, or a party on behalf of Superloop, may carry out work on its facilities, networks or systems for any reason, including arising out of or in connection with:

(a) installation of infrastructure;

(b) maintenance requirements (including scheduled maintenance);

(c) infrastructure upgrades; and

(d) Network relocation.

Ready for Service (RFS) Date means the requested date for delivery of the Service, as agreed between Superloop and You **and specified in the relevant Service Order.**

Remedy Period means the period that:

(a) commences on the earlier of when the Fault is reported to the Superloop Support team, or when Superloop otherwise becomes aware of the Fault; and

(b) ends when the Fault is closed by Superloop.

Roles Based Access Control means when access to view data **or edit configurations in the Service may be limited based on** the user accessing the Service.

Service means the Managed Firewall Service as described in clause 1 and specified in a Service Order.

Service Availability is calculated each month as Uptime divided by the number of minutes in the month, less Excused Downtime, expressed as a percentage.

Service Availability Target has the meaning given at clause 6.1(c).

Site means each of Your physical premises, including Facilities, located at the site addresses specified in the Service Order.

Super Port is a port hand off in a Facility where Superloop has a network presence.

Superloop Equipment means devices and appliances owned by Superloop used in the solution design deployed at Your premises.

Superloop Support team means a service offered by Superloop accessed by a telephone number or email address, as advised by Superloop from time to time, which may be used to convey potential fault information to Superloop.

Uptime means the number of minutes in each month where the link state of the Service is 'up', rounded to the nearest minute.

Write Access means an account with the ability to make any modification to configuration within the Service.