Service Definition

Firewall (Fortigate) | Managed

1. Operational Services

1.1. Service Description

Normal Business Hours = 9:00 -17:30, Monday to Friday (excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

1.1.1. ANS Service

Service	Service Description	Service Hours
Incident Management		
Service Desk - Non Business Critical Faults	The Supplier provides access with relevant phone and email contact details to the Supplier Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4).	Normal Business Hours
Service Desk - Business Critical faults	The Supplier provides 24/7 access with relevant phone contact details to the Supplier Service Desk for critical system down scenarios (P1) only.	24 x 7
Priority Escalation to Microsoft or Fortinet for faults	Priority escalation to Microsoft Premier Support or Fortinet Support	Normal Business Hours
High Priority Escalation to Vendor	High Priority escalation to Microsoft Premier Support or Fortinet Support for Priority 1 business critical faults.	24 x 7
Change Management & Advisory		
Access Control List Configuration & Management	The supplier will configure and manage Access Control Lists to suit your requirements via change management	Normal Business Hours
NAT Configuration & Management	The supplier will configure and manage inbound and outbound Network Address Translation (NAT) rules to suit your requirements via change management	Normal Business Hours
VPN Configuration & Management	The supplier will create, configure and manage VPN configurations via change management, including Site to Site VPN and Client VPN Configurations.	Normal Business Hours
Routing Changes	The supplier will provide Change Management for Static and Dynamic routing changes.	Normal Business Hours
Web Proxy Configuration	The supplier will provide Change Management for Proxy Configuration changes.	Normal Business Hours

VIP and Port Forwarding Configuration	The supplier will create, configure and manage VIP and port forwarding configurations via change management.	Normal Business Hours
Authentication Server Configuration	The supplier will create, configure and manage Authentication Server Configurations via change management, including: • RADIUS • LDAP • SSO	Normal Business Hours
Security Profile Configuration	Where the relevant Security Profile features have been licensed the supplier will provide Change Management on the following: • Intrusion Prevention Systems • Application Control • Antivirus • Web Filtering • AntiSpam	Normal Business Hours
Patch Management & Updates	The supplier will apply dot releases, patches & updates via change management	Normal Business Hours
Security Profiles		
Intrusion Prevention System	Where the Intrusion Prevention System (IPS) is licensed the Supplier will deploy the module. IPS protects your network from outside attacks using anomaly-based and signature-based defences	24 x 7
Application Control	Where Application Control is licensed the Supplier will deploy the module. Application Control detects and takes action against network traffic depending on the application generating the traffic	24 x 7
Antivirus	Where Antivirus is licensed the Supplier will deploy the module. The Antivirus Security Profile applies antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions.	24 x 7
Web Filtering	Where Web Filtering is licensed the Supplier will deploy the module. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources.	24 x 7
AntiSpam	Where AntiSpam is licensed the Supplier will deploy the module. AntiSpam provides mail filtering for IMAP, POP3, and SMTP email. Email filtering includes both spam filtering and filtering for any words or files you want to disallow in email messages.	24 x 7
High Availability & Recovery		
HA Configuration	Where a high-availability solution has been deployed the Supplier will configure and manage your FortiGate failover to standard specifications	Normal Business Hours

Failover Management & Recovery	Where a high-availability solution has been deployed, the Supplier will help manage switchover during failure.	Normal Business Hours
Monitoring & Event Management		
Platform Monitoring	• Availability Monitoring • OS Monitoring thresholds CPU/Memory/Disk IO • Intrusions Blocked and Detected • Viruses Blocked and Detected • HTTP Requests/Sessions/URLs Blocked	24 x 7
Alert Configuration and Response	The Supplier will configure Alerts for the FortiGate environment and respond to Alerts. Alerts will be handled as Incidents within the Incident Management process	Normal Business Hours
Service Operations		
Enterprise Monitoring Portal Access	Customer read-only access to a portal providing visibility of all Customer Supported Assets covered by the Enterprise Monitoring service.	24 x 7
GLASS Portal Access	Customer access to ANS GLASS portal providing visibility of all Service related tickets, alerts and performance dashboards.	24 x 7
Problem Management	ANS Problem Management processes are adhered to for incident, change and event reduction. Problems are reviewed during the Service Management Review.	Normal Business Hours
Service Reviews	Service Management Review (SMR) Reports will be distributed at regular intervals and discussed via a meeting between the Supplier and the Customer. The SMR Report will cover the previous period. Please refer to your Service Statement for SMR frequency and meeting type.	Normal Business Hours
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken to identify the underlying cause. Where applicable a Service Disruption Report will be created.	Normal Business Hours
Change Management Process	The Supplier will take full ownership of the Change Management Process for the Customer Supported Assets.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes.	24 x 7

1.2. Incident Management

1.2.1. Incident Priority Table:

Affect	Business Impact		
	Minor	Moderate	Major
System/Service Down	P3	P2	P1
System/Service Affected	P4	P3	P2
User Down/Affected	P5	P4	P3

1.2.2. Incident Response and Escalation Table:

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	30 Minutes	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	4 Hours	None	GLASS Portal	1 Day
P3	4 Hours	1 Day	2 Days	None	GLASS Portal	10 Days
P4	1 Day	Never	Never	None	GLASS Portal	30 Days
P5	2 Days	Never	Never	None	GLASS Portal	None

For an Incident, "Response" is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call or in person. For detailed process flow see the current Managed Services Handbook. Support to provide a resolution shall be provided within Service Hours from the time of Response until the Incident has been resolved.

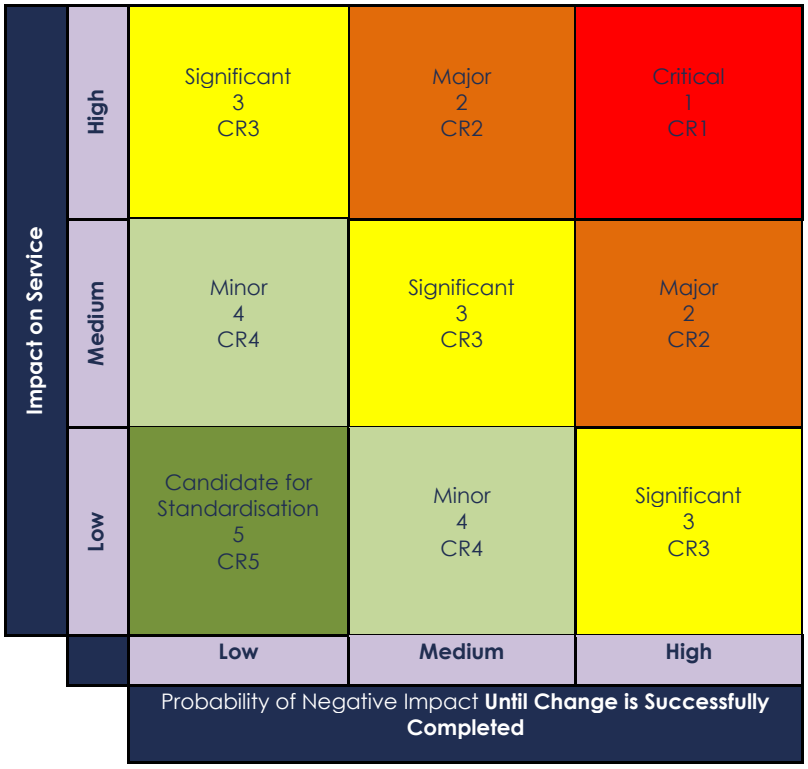
From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in the table above.

1.3. Change Management

All Changes require a Request for Change (RFC) form to be completed on the Suppliers GLASS Portal and submitted detailing the required Change. The Supplier will reject unapproved or incomplete RFC forms.

Changes will follow the Change Management Process as defined in the ANS Managed Services Handbook. It should be noted that Emergency Changes will only be carried out in the event of a P1 scenario (either pro-active or reactive) and/or a major Security Incident where the Supplier deems appropriate.

1.3.1. Change Risk Assessment Matrix



1.3.2. Change implementation targets Table:

Change Type	Implementation Start Date
Normal CR1	1 Working Day from CAB Approval
Normal CR2	2 Working Days from CAB Approval
Normal CR3	3 Working Days from CAB Approval
Normal CR4	4 Working Days from CAB Approval
Normal CR5	5 Working Days from CAB Approval
Normal CR6	Project Changes (Informational and Approval only)
Standard	Change to be completed within 4 Working days from logging on ANS ITSM Tool
Emergency	Change to completed in conjunction with Incident Management Process (P1)

Emergency Changes are dealt with in conjunction with the Incident Management Process; further details of this and all other change types are detailed within the Managed Services Handbook.

Standard and Emergency Changes to the Service within the scope of this Contract will be completed by the Supplier at no additional cost.

2. Service Levels, Key Performance Indicators and Service Credits

Category	Service Level Target	Minimum Service Level	Service Credits
P1 Incidents	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.	100%	1st incident missed response time – 5% Service Credit 2nd incident missed response time – 10% Service Credit
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.	Service credits apply from 2nd failure within a calendar Month	1st incident missed response time – 0% Service Credit 2nd incident missed response time – 5% Service Credit 3rd incident missed response time – 10% Service Credit
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.	80%	<80% - 5% Service Credit
P4 Incidents	100% of Incidents responded to within 1 Working Day.	None	No Service Credit
P5 Incidents	100% of Incidents responded to within 2 Working Days.	None	No Service Credit
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution	None	No Service Credit
CR1 Change	100% of Changes start implementation within 1 Working Day from CAB Approval	100%	1 Change Missed Implementation time - 5% Service Credit 2 Changes missed Implementation times - 10% Service Credit

CR2 Change	90% of Changes start implementation within 2 Working Days from CAB Approval	85%	5% Service Credit
CR3 Change	90% of Changes start implementation within 3 Working Days from CAB Approval	None	No Service Credit
CR4 Change	90% of Changes start implementation within 4 Working Days from CAB Approval	None	No Service Credit
CR5 Change	90% of Changes start implementation within 5 Working Days from CAB Approval	None	No Service Credit
Standard Change	100% of changes implemented within 4 Working Days	90%	5% Service Credit

Service Credits are calculated as a percentage of the monthly Base Charge and in any event, shall not exceed 10% of the monthly Base Charge in the month that the Service Credit arose. Where a Service Credit is due it shall not accumulate with any other Service Credit and only one Service Credit can be offered within the monthly period.

3. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the Terms and Conditions should be consulted.

a. Issues resulting from misconfiguration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
c. Issues resulting from misconfiguration or development by the Customer and/or the Customers chosen 3rd Party Application provider.
d. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets.
e. End User or 1st Line support.
f. Technical Advice to any persons not listed as a Named Contact.
g. Failure to meet SLA due to Public Cloud provider outages or local environment factors such as Power and Cooling.
h. Normal Changes requiring more than 2 hours of implementation time are excluded from the service and will be subject to Additional Service Charges.
i. Project Changes (Normal CR6) are excluded from the service and will be subject to Additional Service Charges. Project Changes are recorded within the Supplier ITSM Tool for Informational and approval purposes only.
j. Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges.
k. Major Version Releases will be subject to Additional Service Charges as only dot releases and patches are included as part of the service.

4. Customer Responsibilities

Including but not limited to:

a. The Customer shall have an established end user support function that may be validated by the Supplier.
b. Where required, the Customer shall make available appropriately skilled Employed persons while an Incident is being managed.
c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
    a. Affected Services
    b. Business Impact
    c. Number & Type of users affected
    d. Recent changes on Supported Assets (regardless of perceived impact)
    e. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected (where required)
    f. The Customer shall check LED status of equipment onsite (where required)
d. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed.
e. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have (where required) Supplier recommended hardware and vendor support in place.
f. The Customer is responsible for all configuration backups outside of the Supported Assets without exception.
g. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process.
h. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook.
i. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier).
j. The Customer shall ensure 24x7x365 availability of a suitable Escalation Contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions.
k. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
l. The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Assets and/or Supplier Assets from the address specified in the Contract. Any asset that has been moved without notification to ANS will be subject to Additional Service Charges.
m. During investigations into a potential hardware or software fault it may be required to reseat certain elements of the device/infrastructure onsite or require a device inspection for LED status. This task sits with the Customer (unless the Supported Asset is located within the Suppliers Data Centres).
n. If the Customer requires the Supplier to provide onsite hands and eyes support then this will be subject to Additional Service Charges.
o. It should be noted that the Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels or Service Credits for Business-Critical Incidents raised via email.

5. Assumptions

a. All Customer Supported Assets and Production AWS and Azure Accounts within the Customer Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.
c. All Customer specific pre-requisites have been completed before contract commencement.
d. The Customer will provide a suitable specification platform, operating system and connectivity for the Enterprise Monitoring collector server.

6. Pre-Requisites

a. On-Boarding Health Check and Documentation.
b. Deployment of ANS Monitoring and Fortinet Cloud Tooling.
c. Platform and where applicable WMI access for all monitored services.
d. Registered Partner of Record and/or AWS Associated Partner registration (where required).
e. Administrative Access Permissions for ANS Engineers on supported Subscriptions/Accounts and Customer Supported Assets.

7. Partner of Record

ANS' Managed Cloud for Azure incorporates Microsoft Signature Cloud Support for any issues that require escalation to Microsoft. In order for this to be able to be fulfilled, Microsoft leverage information collected from the Partner of Record (PoR) system to assign back end support rights. As such ANS must be registered as the digital PoR on any Subscriptions that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the PoR on all Subscriptions that contain or contribute to assets under support or management for the entire duration of this agreement.

8. Amazon AWS Associated Partner

Amazon AWS' partnership status is heavily reliant on demonstrating working relationships with AWS consumers, Amazon leverage information collected from the associated partner system to assign partnership status. As such ANS must be registered as the associated partner on any accounts that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the associated partner on all accounts that contain or contribute to assets under support or management for the entire duration of this agreement.