

Managed Firewall-

Service Level Agreement

SLA

SERVICE DESK			
CATEGORY	DESCRIPTION	STANDARD	ADVANCED
Incident Management	Incident/Problem detection, recording, classification, investigation and diagnosis. Manage and co-ordinate incidents. Serves as a single point of contact, entry and exit for customers keeping a customer informed of progress and advising on workarounds. Restore normal service operation as quickly as possible and minimize the adverse effect on business operations	24 x 7 Mean time to respond: 1 hr Business General Desk Feedback- Issue Resolved Troubleshooting: Best effort	24 x 7 Mean time to respond: 30 min Dedicated Support Desk Feedback: Hourly Updates to resolution Troubleshooting: 1 hr Remote Support Escalation: On Site Support
	On Site Support (*)	On Site Engineer Visits: Included: Vox issue Billable: Client issue	On Site Engineer Visits: Included: Vox issue Billable: Client issue Mean time to Site*: P1- 4 hrs P2- 8 hrs P3- 24 hrs
	Reporting: Monthly Service SLA Report - Product Specific reporting (as long as the Firewall is publicly available from the Vox management IP prefixes)	On request Reports on request: - Firewall Sessions - Firewall CPU - Firewall Memory	Included Reports Available - Firewall Sessions - Firewall CPU - Firewall Memory - Firewall SSL Login - Firewall SSL AV stats - Firewall IPS stats
Request Fulfillment	First line management of basic user change requests which are often minor (standard) changes which includes:	8 x 5 Business General Desk	24 x 7 Dedicated Support Desk
		Mean Time to Respond: 1 hr	Mean Time to Respond: 30 min
		Feedback: request fulfilled	Feedback: Hourly updates to request fulfillment
SLA Stock	Hardware Replacement in event of a Vox owned and managed unit needing to be replaced because of system errors but excludes negligence and damage	Best Effort	30 – 100 Series 24 Business hours 200 Series and above (subject to a 24x7 Forti care support contract)

Managed Firewall-

Service Level Agreement

SLA

MONITORING AND REPORTING

CATEGORY	DESCRIPTION	STANDARD	ADVANCED
Event Management	Monitoring against uptime / downtime	8x5 (uptime availability only)	24x7 (uptime availability only)
Capacity Monitoring	Performance monitoring against configured capacity of Network, CPU, RAM, Storage utilization, Application etc.	N/A	N/A

SERVICE OPERATION

CATEGORY	DESCRIPTION	STANDARD	ADVANCED
Problem Management	Resolve the root causes of incidents to minimize the adverse impact of incidents and problems on business caused by errors within Vox infrastructure, and to prevent recurrence of incidents related to these errors.	Notification Alerts 24x7 Updates to Resolution 8x5 P1 - 1-2 business hrs P2 - 2-3 business hrs P3 - 3-4 business hrs P4 - 3-4 business hrs	Notification Alerts 24x7 Updates to Resolution 8x5 P1 - 1-2 business hrs P2 - 2-3 business hrs P3 - 3-4 business hrs P4 - 3-4 business hrs
Change management	Change Management, Maintenance Emergency maintenance	8x5 notification alerts	8x5 notification alerts

Managed Firewall-

Service Level Agreement

SLA

NOTE: Managed Services are an optional extra and are billable by product

MANAGED SERVICES															
CATEGORY	DESCRIPTION	DELIVERABLE - FULL													
Request Fulfillment	First line management of basic user change requests which are often minor (standard) changes which includes: <ul style="list-style-type: none"> - Moves additions and changes to policies on request - Reporting requests - Requested Firmware updates - User Integration 	Included													
Support	Access to Basic and Advanced support	Included dependent and service SLA selected													
Event Management	Pro Active Performance monitoring against pre-defined thresholds of Network, CPU, RAM, Storage utilization, Application etc.	24x7 Monitoring 8x5 Remediation													
	Thresholds are customizable but will be configured as below by default: <table border="1" data-bbox="419 1055 928 1223"> <thead> <tr> <th>Service</th> <th>Warning</th> <th>Fail</th> </tr> </thead> <tbody> <tr> <td>CPU usage</td> <td>80%</td> <td>97%</td> </tr> <tr> <td>Session count</td> <td>80%</td> <td>97%</td> </tr> <tr> <td>Memory</td> <td>80%</td> <td>97%</td> </tr> <tr> <td>Uptime</td> <td>Alerts</td> <td>Alerts</td> </tr> </tbody> </table> Alerts will be generated and sent to the helpdesk for attention on Managed Services customer.		Service	Warning	Fail	CPU usage	80%	97%	Session count	80%	97%	Memory	80%	97%	Uptime
Service	Warning	Fail													
CPU usage	80%	97%													
Session count	80%	97%													
Memory	80%	97%													
Uptime	Alerts	Alerts													
Capacity Management	Capacity Management Monitoring of capacity criteria to predict capacity problems on the firewall.	Monitoring and Alert setup, with reporting at month end													
Advanced Reporting	Scheduled default reports	Reports include: <ul style="list-style-type: none"> Web Usage Report Fortigate Performance Report Security Overview 360 Degree Security Review SaaS Application Usage Report Application and Risk Analysis Security Analysis Threat Report Cyber Threat Assessment 													
Asset and Configuration Management	Management and traceability of every asset configuration.	Daily backups of the firewall configuration													
		All rule changes are verified with audit trails													
Release and Deployment Management	Ensures the availability of licensed, tested, and version certified software and hardware <ul style="list-style-type: none"> - Evaluates the impact of new software upgrades on the environment 	Quarterly – One version behind latest firmware													

Managed Firewall-

Service Level Agreement

SLA

	<ul style="list-style-type: none"> - Service Validation and testing to ensure the deployed releases and the resulting services meet expectations, and verify that the IT operations can support the new service 	
Audits and Assessments	<p>Quarterly 1 Hr VCIO (Virtual CIO) Engagement (Physical or Video Conference): Improvement initiatives typically follow a seven-step process: *</p> <ul style="list-style-type: none"> - Capacity review - includes environment growth, review of users and recommended improvements - Change review and vulnerability to discuss breaches and concerns - Quarterly Lan / Wan Assessment will provide a holistic IT review of the environment with emphasis on security 	Quarterly
	<p>Vulnerability Testing: Run a vulnerability test on the Firewall to ensure risk is mitigated includes a consultation to unpack</p>	Billable (20% discount)

Definitions

- 1.1. "8x5" refer to hours 8h30 to 16h30 Monday to Friday, excluding public holidays.
- 1.2. "24x7" refer to hours 00h00 to 23h59 every day, including weekends and public holidays.
- 1.3. Incident is used interchangeably with Fault.
- 1.4. "Fault is defined as a system affecting interruption that is logged by a customer via Vox's ticket logging process.
- 1.5. "Mean Time to Respond" The average time taken to contact the customer. This is calculated based on a calendar month.
- 1.6. "Mean Time to Site" (MTTS): The average time taken for an Engineer to get to the customer's premises. This is calculated based on a calendar month.
- 1.7. "P1": Priority 1 – Major system outage with all users affected. Customer cannot continue with normal operations
- 1.8. "P2": Priority 2 – Major system failure with many users affected. Business can continue but is impaired.
- 1.9. "P3": Priority 3 – Minor fault or operational problem, causing user problems but not affecting day to day operation.
- 1.10. *P4*: Priority 4 – Vox Internal System changes.

Service Level Agreement Terms and Conditions

- 1.11. Quarterly engagement": Virtual CIO to meet with the client quarterly. Based on a 50km radius from Vox Main offices (Johannesburg, Pretoria, Cape Town, Durban, Port Elizabeth, East London, Bloemfontein and Kimberley). *Subject to change based on Product and Client SLA's.