SERVICE DEFINITION DOCUMENT

SonicWall Managed Security Service

1.Service Overview

Flotek's SonicWall Managed Security Service provides organisations with enterprise-grade perimeter protection, advanced threat defence, and secure multi-site connectivity using SonicWall Next-Generation Firewalls (NGFWs). The service delivers real-time inspection of all network traffic, proactive threat prevention, secure remote access, and centralised firewall management, ensuring robust cybersecurity and reliable network performance.

This service is suitable for SMEs, multi-site operations, public-sector bodies, and organisations requiring continuous protection against cyber threats, compliance with security standards, and high-availability network connectivity.

2. Key Features

Next-Generation Firewall Security

Deep packet inspection of all incoming and outgoing traffic to block malicious activity.

Advanced Threat Protection (ATP)

Protection against zero-day attacks, ransomware and emerging threats.

Gateway Anti-Virus & Anti-Spyware

Continuous scanning of network traffic to prevent malware infiltration.

Intrusion Prevention System (IPS)

24/7 monitoring for suspicious activity with automatic mitigation.

Application & Traffic Control

Granular visibility and control over applications, services, and protocols.

Content Filtering

Blocking of harmful, inappropriate, or non-business-related websites.

Secure Remote Access (VPN)

Support for SonicWall NetExtender and Mobile Connect for hybrid and remote working.

Enterprise-grade SD-WAN

Optimised performance and inter-office connectivity without complex VPN setups.

Centralised Management & Monitoring

Unified configuration, policy deployment and real-time monitoring.

High-Performance Networking

Hardware designed to prevent bottlenecks and maintain fast, reliable connectivity.

3. Service Benefits

✓ Strong security posture

Provides layered, real-time protection against sophisticated cyber threats.

✓ Lower risk of downtime

Threat prevention, IPS, and 24/7 monitoring significantly reduce disruption.

✓ Improved compliance & control

Content filtering and application rules enforce safe and compliant internet usage.

✓ Enhanced connectivity

SD-WAN links offices securely and efficiently with no traditional VPN overhead.

✓ Scalable architecture

Supports growth, additional sites and future infrastructure changes.

✓ Simplified security management

Centralised monitoring reduces administrative burden on internal IT teams.

✓ Better remote working

Secure VPN access ensures safe and seamless home-working experiences.

✓ Operational efficiency

Automated policy enforcement reduces manual intervention and speeds up responses.

✓ Increased visibility

Advanced analytics and reporting support better decision-making.

✓ Faster incident response

Real-time detection, alerting and remediation reduce the impact of threats.

4. Service Constraints

Complex configuration changes require specialist engineers

Firewall rule changes, VPN modifications and advanced security policies must be handled by Flotek's IT specialists, which may require scheduling.

Certain support tickets may require escalation

SonicWall errors or high-risk security incidents may need senior technical involvement, which can affect resolution time.

Remote access configuration dependency

VPN access depends on accurate client configuration (NetExtender / Mobile Connect), correct authentication setup, and supported devices.

SD-WAN requires coordinated deployment

Multi-site architecture relies on proper configuration across all participating offices.

Performance depends on customer infrastructure

Weak connectivity, outdated equipment, or misconfigured internal networks can impact achievable performance.

Security services require active licensing

Advanced features (ATP, IPS, etc.) require valid SonicWall subscription services.

5. Service Levels

Flotek provides the following service levels:

Helpdesk Hours

- **Mon–Fri:** 08:00–18:00
- **Sat–Sun:** 08:30–17:00

Standard SLA Response Times

- P1 (Critical outage): Immediate response
- P2 (Major impact): Fast-track response
- P3 (Minor issue): Standard response
- P4 (General request): As scheduled

Monitoring

24/7 device monitoring (where installed and connected).

6. Onboarding & Implementation

Onboarding Includes:

- Requirements gathering
- Network assessment
- Appliance selection and provisioning
- Installation and configuration
- Policy design (firewall rules, content filtering, VPN)
- Testing and validation
- User and admin guidance

Optional:

- Multi-site SD-WAN configuration
- VPN deployment and remote-access rollout
- Documentation and IT Glue integration

7. Offboarding

Offboarding includes:

- Configuration export (where permissible)
- Firewall removal and device wiping
- Transfer of administrative rights (if supported)
- Documentation handover
- Termination of licensing and monitoring

8. Technical Requirements

- Stable internet connectivity
- Supported SonicWall hardware or virtual appliance
- Appropriate licensing bundle (Essential, Advanced or APSS)
- For remote access: compatible OS and authentication methods

9. Roles & Responsibilities

Flotek

- Supply, configure and manage SonicWall devices
- Maintain security policies and firmware updates
- Provide monitoring and incident response
- Deliver support and escalations

Customer

- Provide accurate network information
- Maintain internal infrastructure (cabling, switching etc.)
- Approve policy changes
- Ensure user devices meet security prerequisites

4 Old Field Road
Pencoed
Bridgend
CF35 5LJ

T: 02921 50 8000
E: Hello@Flotek.io
W: www.Flotek.io

Flotek Group Limited is Registered in England & Wales | Company Number: 13882299 | VAT Registration Number: GB 4060 18239