

G-Cloud 15 Lot2a Service Definition for Fortinet Fortigate Managed Firewall Service



1 Introduction

The Fortinet FortiGate Managed Firewall Service is a cloud-enabled, managed network security service designed to protect organisational network perimeters, cloud environments, and hybrid infrastructures. The service uses Fortinet FortiGate next-generation firewall technology, combined with Quadris-delivered design, configuration, monitoring, and operational support.

The service provides centralised firewall management, threat prevention, traffic inspection, and security policy enforcement, reducing operational burden while improving security posture. It is suitable for UK public sector organisations requiring a managed, scalable firewall service aligned to security and compliance requirements.

2 Service Scope

The service delivers managed firewall capabilities using Fortinet FortiGate technology, including:

- Firewall policy management
- Intrusion prevention
- Traffic inspection and monitoring
- Web filtering and application control
- Secure remote access and VPN support
- Ongoing operational management and reporting

The service can be delivered for on-premises, cloud, or hybrid environments.

3 Supported Environments

- On-premises networks
- Cloud-hosted environments
- Hybrid infrastructures
- Branch offices and data centres
- Internet-facing network perimeters

4 Functional Capabilities

4.1 Firewall and Network Security

- Next-generation firewall (NGFW) functionality using Fortinet FortiGate
- Stateful firewalling and traffic inspection
- Application-aware traffic control
- Web filtering with granular policy enforcement

- Intrusion Prevention System (IPS) to detect and block known and zero-day threats
- Detection of command-and-control and ransomware “call-home” activity

4.2 Centralised Management

- Centralised policy management across multiple firewall devices
- Securely hosted FortiManager for configuration and policy control
- Securely hosted FortiAnalyzer for logging, analytics, and reporting
- Automated configuration backups

4.3 Monitoring and Visibility

- Traffic monitoring and analysis
- Security event logging and reporting
- Network mapping and visibility of connected sites
- Customised dashboards and filtered reporting views

5 Service Features

- Fully managed Fortinet FortiGate firewall solution
- Bespoke firewall design and configuration
- Centralised firewall policy management
- Quarterly firewall updates and rule reviews
- Automated backups and configuration management
- Traffic inspection and suspicious activity reporting
- Customised security and web-filtering reports
- Optional 24x7 support by qualified Fortinet engineers
- Single monthly service cost

6 Service Benefits

- Improved network perimeter security
- Reduced operational overhead through managed service delivery
- Centralised visibility and control across firewall estate
- Faster response to security threats and policy changes
- Consistent firewall configuration and governance
- Lower total cost of ownership compared to self-managed solutions
- Support for security assurance and audit activities

7 Service Management

7.1 Management Interface

- Secure access to firewall management and reporting platforms
- Centralised service request and change management via the Quadris EyeQ portal
- Role-based access to reports and dashboards

7.2 Monitoring and Oversight

- Continuous monitoring of firewall health and activity
- Regular review of security events and traffic trends
- Proactive identification of misconfiguration or anomalous behaviour

8 Security

8.1 Data and Network Security

- Deep packet inspection and intrusion prevention
- Encrypted management access
- Secure handling of configuration and log data
- Logical separation of customer environments

8.2 Platform Assurance

- Service built on Fortinet FortiGate technology
- Regular updates to security signatures and threat intelligence
- Integration with Fortinet Security Fabric where applicable

9 Onboarding and Implementation

9.1 Onboarding

- Initial assessment of customer network environment
- Firewall design aligned to security and operational requirements
- Deployment or onboarding of FortiGate devices
- Configuration of policies, logging, and reporting

9.2 Transition

- Validation of firewall rules and traffic flows
- Testing and handover into managed service operation

10 Quadris Support Services

Quadris provides optional support services for the Fortinet FortiGate Managed Firewall Service to assist organisations in the effective operation, management, and ongoing assurance of their firewall environments. These support services are designed to align with differing public sector operating models, ranging from assisted self-managed operation to a fully managed, Quadris-operated firewall service.

Quadris support services are provided in addition to the underlying Fortinet FortiGate technology, licences, and hosting components.

10.1 Base Support Service – Assisted Self-Managed Operation

The Base Support Service is intended for organisations that wish to retain day-to-day operational control of their Fortinet FortiGate firewall(s) while receiving structured onboarding, guidance, and access to experienced Quadris network and security engineers.

Under this model, the buyer performs routine firewall administration and monitoring activities, with Quadris providing advisory support, best-practice guidance, and escalation assistance where required.

10.2 Inclusions

- Initial service onboarding support, including:
 - Validation of firewall deployment and connectivity
 - Review of baseline firewall configuration and policies
 - Confirmation of FortiManager and FortiAnalyzer integration
- Administrator guidance covering:
 - Firewall rule and policy management
 - Use of intrusion prevention, web filtering, and application control
 - Log review, traffic analysis, and reporting
 - Backup and configuration management
- Advisory support for:
 - Firewall policy optimisation and security hardening
 - Change planning and impact assessment
 - Audit preparation and security assurance activities
- Liaison with Fortinet technical support where required

10.3 Buyer Responsibilities

- Day-to-day firewall administration and monitoring
- Review and approval of firewall rule changes
- Execution of approved configuration changes
- Maintenance of network architecture and connectivity
- Compliance with internal security, governance, and change management processes

10.4 Intended Use

This service is suitable for organisations with in-house network or security capability that wish to retain operational control while reducing risk through access to expert support and structured guidance.

10.5 Managed Support Service – Quadris-Operated Service

The Managed Support Service is intended for organisations that require Quadris to operate and manage their Fortinet FortiGate firewall service on their behalf. Quadris assumes responsibility for configuration management, monitoring, maintenance, and operational oversight of the firewall environment in accordance with agreed policies and procedures.

The buyer retains accountability for business risk, security policy decisions, and approval of material changes.

10.6 Inclusions

- Full service onboarding and configuration
- Ongoing management of the firewall service, including:
 - Firewall rule and policy management
 - Intrusion prevention, web filtering, and application control configuration
 - Centralised management via FortiManager
 - Log collection, analysis, and reporting via FortiAnalyzer
- Operational activities, including:
 - Continuous monitoring of firewall health and security events
 - Quarterly firewall rule and configuration reviews
 - Proactive identification of misconfiguration or anomalous traffic
- Change and incident support, including:
 - Implementation of approved firewall changes
 - Investigation of suspected security events
 - Escalation and coordination with Fortinet technical support
- Regular service reporting and operational summaries

- Support for audits, compliance reviews, and assurance activities

10.7 Intended Use

This service is suitable for organisations seeking to reduce internal operational overhead, where in-house network or security capability is limited, or where a fully managed firewall service is required.

10.8 Buyer Responsibilities

- Defining firewall security policies and risk appetite
- Authorising firewall rule changes and exceptions
- Maintaining ownership of network architecture and connected systems
- Ensuring compliance with data protection and regulatory obligations

10.9 Service Boundaries and Assumptions

- Quadris support services do not replace the underlying Fortinet FortiGate licences or hardware
- Quadris does not manage non-firewall network infrastructure unless explicitly agreed
- Quadris does not provide endpoint or server administration unless explicitly agreed
- All services are delivered remotely unless otherwise agreed
- Firewall migrations and associated networking device changes are not included in this service and must be charged for as additional consultation services based off the Lot3 daily rate card depending on the roles involved.

10.10 Support Service Responsibility Matrix (RACI)

Key:

R – Responsible (performs the activity)

A – Accountable (owns the outcome / approval)

C – Consulted (provides guidance or input)

I – Informed (kept informed)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Service onboarding and initial configuration	R (Quadris) / A (Buyer)	R (Quadris) / A (Buyer)
Firewall architecture and design	R (Buyer) / C (Quadris)	R (Quadris) / A (Buyer)

Activity	Base Support Service (Assisted Self-Managed)	Managed Support Service (Quadris-Operated)
Firewall rule and policy definition	A (Buyer) / C (Quadris)	A (Buyer) / C (Quadris)
Firewall rule implementation	R (Buyer)	R (Quadris)
Change management execution	R (Buyer)	R (Quadris)
Firewall health monitoring	R (Buyer)	R (Quadris)
Security event review and investigation	R (Buyer) / C (Quadris)	R (Quadris)
Intrusion prevention and threat tuning	R (Buyer) / C (Quadris)	R (Quadris)
Backup and configuration management	R (Buyer)	R (Quadris)
Quarterly firewall review	I (Buyer)	R (Quadris) / I (Buyer)
Reporting and dashboards	R (Buyer)	R (Quadris) / I (Buyer)
Liaison with Fortinet support	C (Quadris)	R (Quadris)
Network ownership and connectivity	A (Buyer)	A (Buyer)
Compliance and governance	A (Buyer)	A (Buyer)

11 Service Constraints and Dependencies

- Requires Fortinet FortiGate firewall hardware or virtual appliances
- Internet connectivity required for management and updates
- The service does not replace broader network or endpoint security controls
- Firewall effectiveness depends on accurate network design and traffic visibility

12 Pricing and Licensing Model

Pricing is subscription-based and typically includes:

- Managed service fees
- Fortinet licences for FortiGate, FortiManager, and FortiAnalyzer
- Optional support tiers

Hardware ownership and lifecycle terms can be defined per contract.

13 Exit Management

- Firewall configurations can be exported on service termination
- Managed services are withdrawn in a controlled manner
- Support for planned service exit in line with G-Cloud requirements

14 Intended Users

- Central government departments
- Local authorities
- NHS and healthcare organisations
- Education and research institutions
- Other UK public sector bodies

15 Summary

The Fortinet FortiGate Managed Firewall Service provides a secure, centrally managed firewall capability that reduces operational complexity while improving network security. Delivered using Fortinet technology and Quadris operational expertise, the service supports resilient, scalable network protection aligned with G-Cloud 15 expectations.