

ITogether Service Definition Document – Managed Firewall & Secure Connectivity Services

Detailed Description
Managed Firewall & Secure Connectivity Services provides the ongoing management and operation of firewall and secure connectivity technologies that protect organisational networks, users, and services. The service helps organisations maintain secure, reliable connectivity across on-premise, cloud, and hybrid environments. The service includes day-to-day administration of firewall platforms, secure remote access, and site-to-site connectivity. It focuses on maintaining strong security controls while ensuring network performance and availability are not compromised. Delivered by experienced security and network specialists, the service removes the operational burden of managing complex firewall and connectivity environments. Configurations are maintained in line with security best practice, organisational policy, and changing operational requirements. Managed Firewall & Secure Connectivity Services is suitable for public sector organisations with distributed sites, remote users, and internet-facing services. It supports both traditional perimeter-based architectures and modern zero trust and cloud-first models.
Business Benefits
Reduced security risk • Consistent enforcement of network security controls. • Reduced exposure from misconfiguration or unmanaged changes. Improved availability and reliability • Secure connectivity maintained without unnecessary disruption. • Faster resolution of firewall and connectivity issues. Operational efficiency • Day-to-day administration handled externally. • Internal teams focus on strategic and service improvement activities.



The information in this document is the property of Network Integration Technologies Ltd t/a ITogether. The contents of this document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Network Integration Technologies Ltd t/a ITogether.

Access to specialist expertise

- Experienced engineers across firewall and connectivity technologies.
- Support for complex and evolving architectures.

Scalable and adaptable

- Supports growth in sites, users, and cloud services.
- Adapts to changing security and connectivity models.

Improved visibility and assurance

- Clear reporting on changes, incidents, and service health.
- Supports governance, audit, and risk management.

Standard Service Components

Service onboarding and discovery

- Review of firewall estate, connectivity, and architecture.
- Identification of critical services, dependencies, and risks.
- Agreement of scope, responsibilities, and escalation paths.

Firewall configuration and policy management

- Ongoing management of firewall rules and policies.
- Secure change implementation and validation.
- Regular review of rules to reduce risk and complexity.

Secure connectivity management

- Management of site-to-site and remote access VPNs.
- Support for secure connectivity to cloud services.
- Oversight of zero trust and secure access technologies.

Monitoring and incident response

- Monitoring of firewall health and connectivity status.
- Investigation and resolution of security and connectivity incidents.
- Coordination with customer teams and third-party providers.

Change and release support

- Support for planned changes and network developments.
- Validation of connectivity and security post-change.
- Rollback support where required.



The information in this document is the property of Network Integration Technologies Ltd t/a ITogether.
The contents of this document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Network Integration Technologies Ltd t/a ITogether.

Reporting and service reviews

- Regular reporting on changes, incidents, and trends.
- Insight into policy usage and improvement opportunities.
- Scheduled service review meetings.

Service governance and support

- Defined service levels and operational processes.
- Clear communication and escalation routes.
- Alignment with public sector security and operational requirements.

Optional Service Components

To be discussed during scoping exercise.

Service Exclusions

Anything not specifically included in either the above or when the project is formally scoped.

Standard Support Services

8x5 support, Monday to Friday 9am to 5pm

Assumptions

Any and all information will be provided by the customer to enable the full onboarding of the product without hinderance

Contact

Name	Role	Tel	Email
Tim Ripper	Account Director	0113 341 0123	tim@itogether.co.uk
Simon Richardson	Director	0113 341 0123	simon@itogether.co.uk



The information in this document is the property of Network Integration Technologies Ltd t/a ITogether.
The contents of this document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Network Integration Technologies Ltd t/a ITogether.