



Service description document: Managed Fortinet SASE Secure Access Service (Managed SaaS)

Introduction to eir Business

eir Business is a leading provider of advanced network, cloud, and IT managed services, supporting public and private sector organisations across the UK and Ireland for almost 30 years. We design, implement, and manage next-generation solutions that strengthen resilience, enhance security, and enable organisations to work seamlessly and securely from anywhere.

Every engagement starts with listening, understanding your environment, your priorities, and the outcomes you need to achieve. From there, we shape solutions that deliver genuine value, long-term performance, and measurable operational impact.

As a trusted managed service provider, we bring together specialist engineering, proactive service management, and a 24×7 operations capability. Our tightly integrated teams work across the full IT and network landscape, including cloud, cybersecurity, WAN/LAN, connectivity, digital workplace, AI and automation, data centre services, and unified communications.

Our managed services are built on industry best practice and underpinned by ITIL principles, ensuring consistency, accountability, and continual improvement. We combine rigorous processes with real human engagement: our service managers, engineers, and analysts work side-by-side with customers to anticipate needs, resolve issues quickly, and identify opportunities for ongoing optimisation.

Our goal is simple: To give customers complete confidence that their technology is in expert hands, enabling them to focus on delivering essential public services and organisational objectives.

Our Fortinet capability

eir Business has extensive experience delivering secure connectivity and cloud security solutions using Fortinet technologies. We provide the full lifecycle of Fortinet services from design and configuration to ongoing management and optimisation, enabling organisations to adopt modern cloud security models with confidence.

Our security engineers are skilled in the deployment and management of Fortinet's secure access, firewall, SD-WAN, and cloud security portfolio. We combine Fortinet's cloud-delivered SASE capabilities with our MSP expertise to provide highly resilient, scalable, and user-centric security services.

Through our 24×7 Security and Network Operations Centres, based in Belfast and Dublin, we monitor and manage customer environments using industry-leading tools and methodologies. Our teams ensure continuous service health, rapid incident response, and proactive improvements across Fortinet-based solutions.

Service introduction

Fortinet Secure Access Service Edge (FortiSASE) is a cloud-delivered security platform that provides secure, consistent access to the internet, cloud applications and private services for remote and hybrid users. This service combines the following cloud security capabilities into a single, unified service:

- Secure Web Gateway
- CASB
- ZTNA
- IPS, anti-malware
- DNS security
- Traffic inspection

eir Business delivers FortiSASE as a managed SaaS service, providing licensing, onboarding, configuration, policy setup and ongoing support. The service helps organisations improve security, reduce complexity, and give users fast, reliable access from any location or device.

We combine Fortinet's cloud-delivered SASE capabilities with our managed service approach to deliver a complete, end-to-end security service

This service is suitable for public sector bodies looking to modernise remote access, enhance cloud security controls, or transition away from traditional VPN solutions.

Key service features

Cloud-delivered security

- Secure Web Gateway with real-time web filtering
- Intrusion Prevention System (IPS)
- Anti-malware scanning and SSL inspection
- DNS security and application control

Secure access to cloud applications

- Cloud Access Security Broker (CASB)
- Inline and API-based inspection for SaaS applications
- Visibility of risky behaviour or policy violations

Zero Trust Network Access (ZTNA)

- User identity-based access instead of traditional VPN
- Application-level access controls
- Encrypted tunnels between users and private services

Secure Private Access (SPA)

- Secure IPSec connectivity from FortiSASE cloud to on-premises firewalls
- Supports access to company-hosted or private applications

Unified management and insight

- Central dashboard for policy management, usage, activity and threat visibility
- Real-time and historical analytics

Scalable and cloud-native model

- No hardware required
- Scales up or down based on user numbers
- Supports up to three devices per user

Key service benefits

Improved security for remote and hybrid workers

Consistent security policies applied everywhere users work (at home, on the move or in the office).

Reduced operational overhead

The service removes the need to run on-premise VPN concentrators or distributed security hardware.

Faster and safer access to cloud apps

Traffic is inspected in the cloud, reducing latency and improving user experience.

Supports digital transformation

Moves organisations away from legacy VPN to a modern Zero Trust model.

Backed by local eir Business expertise

2nd and 3rd line support is delivered by eir Businesses Northern Ireland-based network and security teams, with escalation to vendor TAC when required.

Service scope

Included	FortiSASE licensing (Standard or Advanced)
	Design and configuration of security policies
	Setup of Secure Internet Access (SIA)
	Setup of Secure SaaS Access (SSA / CASB)
	Setup of Secure Private Access (SPA / ZTNA)
	Integration with on-premises firewalls (e.g., FortiGate)
	Integration with identity providers such as Entra ID or Active Directory
	User onboarding guidance
	Access to portal dashboards and reporting
	Ongoing 3rd-line support delivered by eir Business
Optional add-ons	Additional public IPs for whitelisting
	Additional data transfer allowances
	Increased support hours
	Additional training sessions
	Extended consultancy for policy optimisation
Not Included	User acceptance testing
	Endpoint installation (customer responsibility)
	Custom integrations or bespoke software development
	Ongoing client upgrades (customer responsibility)

Onboarding

eir Business follows a structured onboarding approach, typically including:

1. Discovery and design review

Understanding your environment, remote access policies, firewall setup and user requirements.

2. Configuration and deployment

- Configure FortiSASE policies
- Enable SWG, CASB, SPA and ZTNA functions
- Integrate with firewalls and identity services

3. Testing and validation

- Remote access tests
- Policy enforcement checks
- SPA tunnel testing

4. Knowledge transfer

A short training and handover session for your technical teams.

5. Transition to live service

Service desk activation and ongoing support arrangements.

Support

Support is delivered from eir Businesses Northern Ireland operations centre:

- **Hours:** 09:00–17:00 Monday–Friday (standard)
- **Escalation:** 24×7×365 for major incidents
- **Channels:** Phone, email, service desk portal
- **Levels:**
 - 1st line support by customer
 - 2nd and 3rd line support by eir Business
 - Vendor TAC engagement where necessary

Incident handling includes logging, diagnosis, escalation, and service reporting, following ITIL and ISO 20000 processes.

Dependencies

- The customer must install and maintain FortiClient on endpoints
- The customer must provide firewall access for SPA tunnel configuration
- The customer must provide identity provider details for SSO
- The customer must approve final security policies

Service constraints

- Connectivity relies on customer internet performance
- Maintenance windows may cause short interruptions (1–2 minutes)
- Data transfer limits apply per licence (e.g., 25TB for 100 users)
- Policy changes may require testing before going live

