Managed Firewall Service

(Using Zyxel Firewalls with Gold Pack UTM Security)

1. Service Overview

Our Managed Firewall Service provides end-to-end management, monitoring, and maintenance of your perimeter firewalls, using Zyxel next-generation firewall appliances licensed with the Gold Security Pack. The service is designed to protect your network from external and internal threats, ensure secure connectivity for users and sites, and maintain a compliant, auditable security posture.

This document defines the functional areas covered under the service. It is intended to sit alongside your Master Services Agreement and specific SLA schedule.

2. Hardware & Platform Management

- Procurement advice and sizing of Zyxel firewall models to meet current and projected requirements (users, throughput, VPN, UTM load).
- Initial deployment and configuration (rack/desktop installation, basic network integration, WAN configuration, LAN/VLAN layout, basic routing).
- Ongoing firmware management: evaluation, scheduling and installation of vendor firmware updates and security patches, including rollback if required.
- Management of device inventory, serial numbers, license status, and renewal dates for Gold Security Pack subscriptions.

3. Core Firewall Policy Management

- Design and implementation of firewall rule sets aligned to your security policy (inbound, outbound, inter-VLAN, DMZ).
- Creation and maintenance of network objects, address groups, service groups, and zones.
- Change management for firewall rules (adds, moves, changes, deletions), including risk assessment and documentation.
- NAT configuration and management (static NAT, PAT, one-to-one and many-to-one translations, hair-pinning as required).
- Policy optimisation and cleanup, including removal of redundant rules and consolidation of overlapping policies to maintain a **hardened** posture.

4. Unified Threat Management (UTM) Features

All UTM features listed below are included in the Zyxel Gold Security Pack and are configured, tuned, and monitored as part of this service.

4.1 Intrusion Prevention System (IPS)

- Enablement and tuning of IPS profiles to detect and block known network attacks, exploits, and protocol anomalies.
- Selection of appropriate IPS signatures based on your environment and risk profile (e.g. server roles, exposed services).
- Regular review and adjustment of IPS policies based on alerts, false positives, and emerging threats.

4.2 Anti-Malware

- Configuration of gateway anti-malware scanning for HTTP/HTTPS (where SSL inspection is used), SMTP/POP3 and other supported protocols.
- Policy definition for block/log actions, file size limits, and response to confirmed detections.
- Periodic review of detection statistics and tuning to reduce false positives while maintaining strong protection.

4.3 Sandboxing (Advanced Threat Protection)

- Activation and policy configuration of cloud sandboxing for suspicious or unknown files to protect against zero-day malware.
- Review of sandboxing reports and investigation of high-risk events, with containment actions where required.
- Feedback of sandbox intelligence into other policies (e.g. blocklists, reputation filtering).

4.4 Reputation Filtering (IP/URL/DNS)

- Configuration of reputation-based blocking for malicious IPs, URLs and domains, using Zyxel's threat intelligence feeds.
- Ongoing tuning and whitelisting of legitimate sites incorrectly categorised to prevent business disruption.
- Periodic review of reputation filter hits to identify recurring threats or mis-configured applications.

4.5 Web Filtering

- Implementation of category-based web filtering (e.g. malware, phishing, adult, gambling, illegal content).
- Definition of time-based or group-based internet usage policies where supported (e.g. stricter for guests vs staff).
- Configuration of safe search enforcement and file-type control (e.g. blocking risky downloads).
- Review of web activity reports and adjustment of policies in line with HR/acceptable-use requirements.

4.6 Application Patrol / Application Control

- Configuration of application control policies to identify and manage traffic from thousands of applications (e.g. social media, streaming, remote access tools).
- Enforcement of allow/deny/shape policies per application or application group, aligned with your business and bandwidth priorities.
- Review of application-level reports and refinement to address shadow IT and unsanctioned services.

4.7 Email Security (Where Used on Firewall)

- Enablement of firewall-based email security features (anti-spam, malware scanning, basic content filtering) where mail flows traverse the device.
- Tuning of spam thresholds, block/allow lists, and quarantine behaviour.
- Coordination with your mail platform (e.g. cloud email security) to avoid duplication or gaps in coverage.

5. Secure Connectivity & VPN

- Design, configuration, and management of site-to-site VPN tunnels between your locations and approved third parties.
- Configuration and ongoing management of remote access VPN (IPsec/SSL) for staff and contractors, including user and group policies.
- Integration with directory/identity services where supported (RADIUS/LDAP/AD/SSO) for user authentication.
- Monitoring of VPN stability, throughput, and failover behaviour, with remediation of issues as they arise.

6. Identity, Access & Network Segmentation

- Configuration of user and device authentication policies on the firewall, including captive portal or integrated authentication where applicable.
- Support for network segmentation via VLANs and security zones (e.g. staff, guest, IoT, servers) and appropriate inter-zone rules.
- Policy enforcement based on user/group identity (where supported) in addition to IP/subnet, providing more granular **control**.
- Implementation of guest/visitor access policies and basic captive portal options available via the platform.

7. Monitoring, Logging & Reporting (SecuReporter / Cloud)

- Continuous health and security monitoring of firewall appliances (CPU, memory, interfaces, tunnels, license status).
- Centralised logging of security events and traffic flows using Zyxel's SecuReporter and/or Nebula cloud management.
- Scheduled delivery of summary security and usage reports (e.g. top threats, blocked sites, bandwidth consumers) at agreed intervals.
- Ad-hoc investigation of incidents and provision of evidence for audits or compliance requests.

8. Incident Detection & Response

- Detection of security incidents via alerts from IPS, anti-malware, sandboxing, reputation filtering, and web filtering.
- Initial triage and validation of alerts to reduce noise and identify genuine threats.
- Containment actions on the firewall, such as blocking IPs/domains, adjusting rules, or isolating affected network segments.
- Communication of incident details, impact assessment at network level, and recommended remediation steps on endpoints/servers.
- Post-incident review of policies to reduce likelihood or impact of recurrence.

9. Change Management & Requests

- Managed change process for firewall and UTM policy modifications, including request validation and security impact assessment.
- Implementation of approved changes within agreed timescales, including out-of-hours where required by prior arrangement.
- Documentation of significant changes (new services, new VPNs, major rule revisions) for audit trail purposes.
- Emergency changes in response to active threats or outages, followed by retrospective documentation.

10. Compliance & Governance Support

- Provision of firewall and security configuration information to support audits (e.g. ISO 27001, Cyber Essentials, PCI-DSS scoping).
- Assistance with defining and aligning firewall policies to your internal security standards and regulatory requirements.
- Retention of logs and reports for an agreed period to support investigations and compliance evidence.

11. Exclusions

Unless explicitly stated in your order or agreement, the Managed Firewall Service does **not** include:

- Supply of firewall hardware, licenses, or subscriptions (these may be billed separately).
- Management of third-party security products (non-Zyxel firewalls, separate web filters, endpoint AV).
- Incident response on internal endpoints/servers beyond firewall containment and network-level guidance.
- Penetration testing or formal security assessments (these can be quoted as separate services).
- On-site engineering visits except where specifically included in your contract.

12. Service Hours & SLA

Please note that the timescales stated are target maximum mins/hours and that most requests will be responded to and resolved well within the specified timeframes.

INCIDENT	EXAMPLE DEFINITION	INITIAL RESPONSE TARGET	RESOLUTIONTARGET
P1 – Critical	Full outage/sever degradation affecting multiple users/key business functions	30 mins	4 hours to restore to an operational state. (may be interim workaround)
P2 - High	Major functional impact/single critical user unable to work	Within 1 bus.hr	Same business day or within 8 hours
P3 – Medium	Moderate impact, work can continue using a workaround, non-critical services affected	Within 2 bus. hours	Within 1-2 working days
P4 – Low	Low impact, minor issues, how-to/informational or scheduled change requests	Within 4 bus. hours	Within 5 business days

Service operation: Business hours monitoring/support 08:30–17:30 UK time, Monday–Friday (excluding public and bank holidays).