Service Datasheet
Firewall as a Service

Executive Summary

Maxtel's Firewall as a Service (FWaaS) provides organizations with advanced, fully managed protection for their networks, applications, and workloads. Designed for companies that require enterprise-level security without the complexity of managing physical appliances or maintaining internal firewall policies, FWaaS delivers a robust, flexible, and scalable security layer integrated directly into Maxtel's infrastructure. With next-generation firewall technology, deep traffic inspection, and intelligent access controls, our service helps your organization defend against modern threats, enhance visibility, and maintain continuous compliance, all through a simple, service-based model.

Key Features

- Next-Generation Firewall (NGFW): Deep packet inspection (DPI), application-aware filtering, port and protocol control, content inspection, and malicious traffic blocking.

- Flexible, centralized policies: Rules defined by segment, service, VLAN, user, or application, with real-time updates.

- Threat protection: Intrusion Detection and Prevention (IDS/IPS). DDoS mitigation. Malware and suspicious traffic blocking. Sandboxing to detect anomalous behavior.

- Advanced segmentation: Logical isolation across environments (production, QA, development, databases, containers, etc.).

- High availability: Redundant firewall instances with automatic failover to ensure uninterrupted operations.

- Integrated with Maxtel's network: Distributed firewalling at the perimeter and within Maxtel's backbone, optimizing both latency and security.

- 24/7 monitoring: Continuous oversight of traffic flows, security alerts, and real-time reporting.

- Regulatory compliance: Controls aligned with ISO 27001, PCI-DSS, GDPR, and Latin American data protection standards.

- Expert-managed service: Maxtel engineers handle configuration, policy management, updates, and threat signature maintenance.

Business Benefits

- Enterprise-grade security without upfront investments in specialized hardware.

- Reduced risk exposure against advanced threats, unauthorized access, and network attacks.

- Complete visibility into network traffic, supporting better decision-making.

- Immediate scalability, adapting effortlessly to growing infrastructure demands.

- Predictable costs through a clear, service-based pricing model.

- Lower operational burden, with security management delegated to experts.

- Enhanced performance, with protection embedded in a low-latency network architecture.

Datacenter