

FIREWALL AS A SERVICE

Enterprise-grade network security for cloud and colocation

Protect your workloads with a dedicated firewall instance — without the cost and complexity of owning the underlying hardware.

How does Firewall as a Service work?

Your team controls its security policies while Ilkari manages the underlying platform, high availability and updates. **The service is delivered from Ilkari-owned data centres, bringing your infrastructure, billing and support together with one trusted provider.**



Sovereign by design

Keep your data and network traffic within the applicable local jurisdiction, hosted in Ilkari-owned data centres across Europe and Latin America.



Hardware-backed isolation

Benefit from greater separation through a dedicated firewall instance with hardware-backed VDOM isolation.



No CAPEX, predictable costs

Avoid upfront hardware investment and pay a predictable monthly fee based on the protection and capacity your organisation needs.



Advanced threat protection

Add protection against intrusions, malware, malicious websites and threats within encrypted traffic by selecting the Advanced tier.



Security that scales with you

Increase your protection level and capacity as your organisation's requirements evolve.



Local expert support

Get direct support from Ilkari specialists who understand your infrastructure and local operating environment.

Who is it for?

Designed for organisations that need enterprise-grade network security.

Mid-market organisations

Access enterprise firewall capabilities without the cost and operational burden of owning and maintaining firewall hardware.

Enterprises and regulated industries

Protect business-critical environments with security capabilities that support demanding governance, audit and compliance requirements.

Colocation customers

Add enterprise-grade network security to infrastructure already hosted within Ilkari data centres.

TIERS AND CAPACITY

Choose your level of protection

Select Essential for core enterprise firewall capabilities or Advanced for enhanced threat protection. Then choose the capacity that best fits your organisation's requirements.

MID-MARKET ORGANISATIONS

Essential

ENTERPRISE FIREWALL

- ✓ Hardware-backed VDOM isolation
- ✓ Stateful firewall traffic control
- ✓ NAT and DHCP plus static routing
- ✓ IPsec site-to-site VPN connectivity
- ✓ Self-service administration through the Ilkari portal

ENTERPRISES AND REGULATED INDUSTRIES

Advanced

ENTERPRISE FIREWALL WITH ADVANCED THREAT PROTECTION

Includes everything in Essential, plus:

- ✓ Intrusion prevention system (IPS)
- ✓ Antivirus and anti-malware protection
- ✓ Web and DNS filtering and application control
- ✓ SSL/TLS traffic inspection
- ✓ Compliance-ready logging and SD-WAN

INCLUDED

Self-service virtual firewall included with Ilkari Cloud, providing an accessible starting point for traffic control before moving to a enterprise firewall service.

Choose your capacity

Select the capacity that best matches your organisation's performance requirements, independently of your chosen protection tier.

Small

Firewall **up to 500 Mbps**
Protection **up to 150 Mbps**

Medium

Firewall **up to 1 Gbps**
Protection **up to 350 Mbps**

Large

Firewall **up to 2 Gbps**
Protection **up to 700 Mbps**

Advanced threat protection

Strengthen your defences against malware, intrusions and threats concealed within encrypted traffic with the Advanced tier.



Ransomware



Phishing
and fraud



Malware
and viruses



Unauthorized
accesses



Encrypted
threats

Protect your infrastructure without compromising sovereignty

Contact us to discuss the right protection tier and capacity for your organisation: sales@ilkari.tech



www.ilkari.tech