LOGICALIS
Architects of Change

Intelligent Connectivity

Secure Firewall

Protect users, apps, and networks, with efficiency, unification and visibility.

The Logicalis Managed Secure Firewall solution offers a comprehensive managed service that provides adaptive threat protection and zero-trust enforcement. It ensures real-time visibility into users, traffic, and applications, helping customers maintain security in a digital-first world.

With employees, data, and offices spread across the country and globally, your firewall needs to be prepared for any situation. Secure Firewall assists in planning, prioritizing, closing security gaps, and recovering from disasters with greater resilience.

LOGICALIS

The benefits of Secure Firewall

By leveraging Logicalis Secure Firewall, you can ensure a robust and adaptive security infrastructure that keeps your organisation protected in a digital-first world.

Lean on AI that simplifies policy management

Streamlining workflows, finding misconfigurations. Auto-generating rules. With 1000s of policies to manage, we can simplify your firewall policies.

Achieve superior visibility

Regain visibility and control of your encrypted traffic and application environments. Detect more with Threat Intelligence and leverage billions of signals across your infrastructure with security resilience.

Drive efficiency at scale

Secure Firewall supports advanced clustering, high availability and multi-instance capabilities. Bring scalability, reliability and productivity to your teams across hybrid environments.
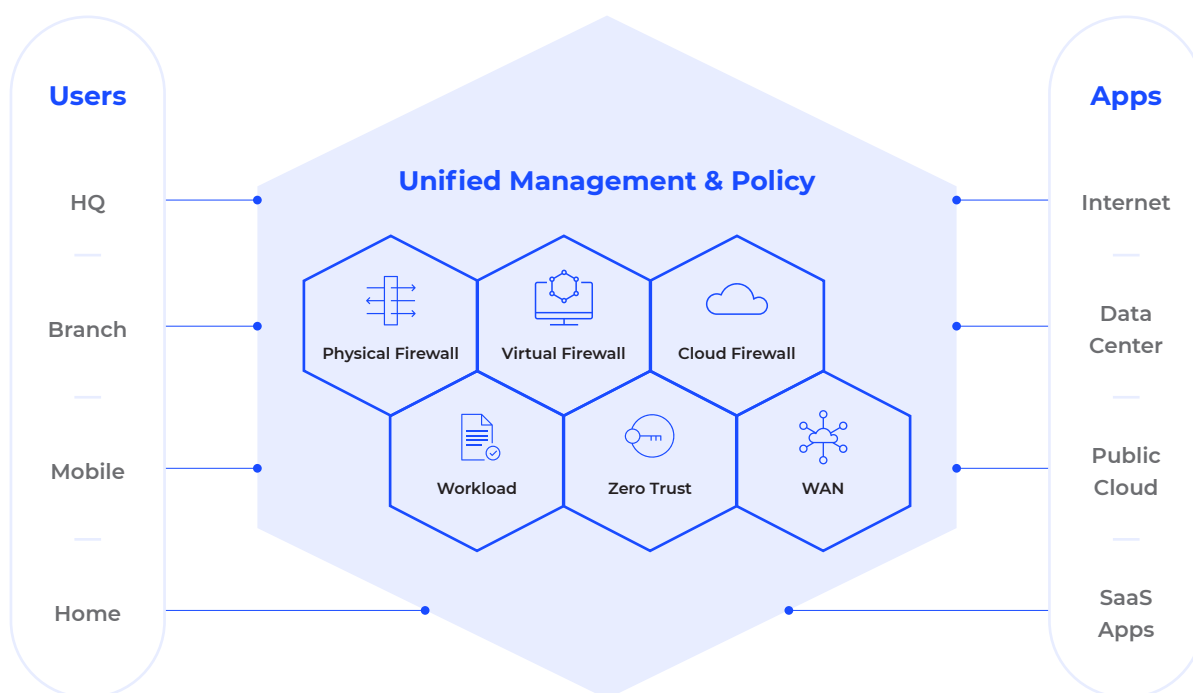
Make zero trust practical

Secure Firewall makes a zero-trust posture achievable and cost effective with network, micro segmentation and app security integrations. Automate access and anticipate what comes next.

Modernise your defense with Logicalis Secure Firewall

Harmonising the firewall across all form factors, the solution expands its capabilities to encompass applications, networking, and users. It offers unified identity, management, and policy to provide choice, consistency, and control. Additionally, it augments deep packet inspection with AI/ML-based inference and contextual insights. The flexible consumption model ensures easy migration, making it adaptable to various organisational needs

Users

HQ

Branch

Mobile

Home

Unified Management & Policy

Physical Firewall

Virtual Firewall

Cloud Firewall

Workload

Zero Trust

WAN

Apps

Internet

Data Center

Public Cloud

SaaS Apps

Secure Campus

Provide network zero trust to protect users, devices and thing in the office.

· Deploy robust network security with the most up-to-date Threat Intelligence.

· Identify and block threats and malware before they hit firewall.

· Ensure remote worker security, anywhere.

· Work together with our Migration Services to ensure successful deployment.

Secure Branch

Secure the branch and remote networks.

· Deploy the same level of security at branches and remote locations as found at headquarters.

· Ensure remote worker security, anywhere.

· Work together with our Migration Services to ensure successful deployment.

Secure Hybrid Datacenter

Secure data, applications, workloads and resources across a hybrid datacenter architecture.

· Protect applications, data and workloads across datacenters and clouds.

· Deliver a consisted user experience regardless of where they are working.

· Work together with our Migration Services to ensure successful deployment.

How we get you there

We help you along the journey towards achieving Intelligent Security - with speed and efficiency, using our tried and tested methodology.

Phase 1
Foundation and Visibility

- Deploy core firewall functions (stateful inspection, basic L3/L4 policies)
- Enable secure access (VPN, remote access if needed)
- Establish visibility using tools like Cisco Secure Firewall Management Center (FMC) or Cisco Defense Orchestrator (CDO)
- Integrate with identity sources (e.g., AD/LDAP)
- **Goal:** Establish basic perimeter security and visibility.

Phase 2
Advanced Threat Protection

- Enable next-gen features:
- IPS (Snort)
- Advanced Malware Protection (AMP for Networks)
- URL filtering
- Fine-tune policies based on users, apps, and threat intelligence
- **Goal:** Strengthen protection with threat-centric policies.

Phase 3
Automation & Policy Optimisation

- Integrate with Cisco SecureX for incident response and automation
- Leverage policy recommendations and automation from FMC/CDO
- Begin segmentation (macro or micro) aligned to Zero Trust
- **Goal:** Reduce manual overhead and optimize for scale.

Phase 4
Integration with Broader Architecture

- Integrate with SASE stack (Umbrella, Duo, SD-WAN)
- Integrate with XDR ecosystem (Cisco XDR or 3rd party)
- Integrate with SIEM/SOAR tools (Splunk, Palo Alto XSOAR, etc.)
- Enable dynamic policies based on identity, behaviour, device posture
- **Goal:** Achieve adaptive and integrated security posture.

> **"**
>
> We generate about 170,000,000 events a month. There is no way our internal security team would be able to review that amount of data without partners and their threat intelligence to help identify potential threats.

Global CISO, Global Enterprise Organisation

Be the guardian of your digital future

Innovate and advance. Be where you want to be, following an Intelligent Connectivity blueprint for success with Logicalis by your side.

Get in contact with us today