LANEX

EDGE Firewall Series

Next-Generation Network Security Solutions

In today's fast-paced digital landscape, protecting your business infrastructure requires security that is powerful, flexible, and simple to manage. IPEDGE Firewalls deliver a comprehensive, all-in-one network security platform that perfectly balances high performance with robust threat protection. Built to scale with your business and fit your budget, this unified solution eliminates complexity by providing consistent security management across appliance firewall and virtual firewall in cloud environments.



© 2017 TeleSource Solutions. All rights reserved.



Edge Network Security Features

provides end-to-end threat prevention and intelligent network monitoring to neutralize advanced cyber risks before disruption. With highly adaptable policy management and dynamic traffic control, they ensure maximum security coverage without compromising performance.

Advanced Routing & SD-WAN

- Dynamic & Policy Routing: Full support for BGP, OSPF, IS-IS, RIP, and policy-based routing to handle complex network paths.
- SD-WAN & Overlay Networks: Integrates DMVPN, MPLS, and Segment Routing (SR-MPLS/SRv6) for multi-site traffic engineering.
- Multicast & Network Isolation: Built-in VRF and multi-topology routing allow safe network segmentation on a single device.

Comprehensive VPN & Remote Access

- Multi-Protocol Support: Combines high-speed WireGuard, IPsec/IKEv2 (with hardware acceleration), and OpenVPN for flexible site-to-site and remote user connections.
- High-Capacity Concentrator: Supports thousands of concurrent VPN tunnels, making it ideal as a central hub or regional concentrator.
- Resilient Failover: Built-in dead-peer detection and dynamic routing over VPN interfaces ensure zero-downtime WAN redundancy.

Stateful Firewall & NAT

- Enterprise Security Engine: Powered by Linux nftables for high-speed, multi-gigabit stateful packet inspection across IPv4 and IPv6.
- Zone-Based Control: Granular security policies isolate traffic by zone, source, destination, and service with full event logging.
- Flexible NAT Support: Full support for SNAT, DNAT, 1:1 NAT, port forwarding, and NPTv6 for seamless network address translation.

Network Services & Automation

- Core Infrastructure Services: Built-in DHCP, DNS forwarding, NTP, and advanced QoS traffic shaping (FQ-CoDel, DSCP marking).
- Automated Management: Fully controllable via REST API, NETCONF, Ansible, and Terraform for Infrastructure-as-Code (IaC) workflows.
- Zero-Touch & Safe Deploys: Features cloud-init for automated provisioning and instant single-command configuration rollbacks.

Key Features

Core Security & Performance

- **Complete Protection:** Includes a built-in firewall, web/content filtering, VPN, and threat prevention (IDS/IPS).
- **Application-Aware Filtering:** Uses Deep Packet Inspection (DPI) to identify specific apps, letting you prioritize business-critical traffic over non-essential applications.
- **Flexible Licensing:** Choose subscription options that match your business needs for threat protection and website access control.

Remote Access & Management

- **Secure Remote VPNs:** Connects branch offices to headquarters and safely encrypt traffic for remote or traveling workers.
- **Intuitive Dashboard:** Features an easy-to-use graphical interface to monitor traffic, check security status, and manage rules at-a-glance.
- **Cost Savings:** Reduces training time, speeds up incident response, and slashes overall network management costs.

Simple Management

- **Intuitive Dashboard:** Features an easy-to-use web interface to monitor traffic, check security status, and manage rules at-a-glance.
- **Cost Savings:** Reduces network management time & operational costs.

Network Security Features	
DPI firewall engine	
Deep Packet Inspection engine	The high-performance inspection engine performs stream-based bi-directional traffic analysis, identifying individual applications, while blocking intrusion attempts and malware.
Bi-directional inspection	Protect your network by scanning threats in inbound traffic, while protecting your business reputation by scanning for threats in outbound traffic.
Single-pass inspection	Multiple threat detection and protection capabilities are integrated within a purpose-built solution that provides single-pass low-latency inspection and protection for all network traffic.
Application and Web control	
Application control	Application-aware visibility delivers precise control over applications, content, and users across your network. Choose between a built-in application list or a regularly updated subscription database for maximum coverage.
Application bandwidth management	Manage application bandwidth to support business requirements, while limiting non-essential applications.
Web control	Web Control feature enables easy management of user website access by selecting which content categories to allow or deny globally. Any URL can be checked to view its web control category, to ensure website management aligns with business policies. Proxy-based or Deep Packet Inspection (DPI) options provide flexibility.
URL filtering	Enables http/https access to particular websites to be allowed/blocked with user-defined lists.
Unified threat management	
DoS attack protection	Protection against Denial of Service (DoS) attacks, which are designed to consume resources and therefore deny users network and application access.
Zone-based protection	Internal security is increased with the network segmented into multiple security zones, with boundaries that block the propagation of threats.
Advanced IPS (Intrusion Protection System)	Advanced IPS detects and blocks threats. The subscription-based service is updated daily, and protects against malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies.
Virtual Private Networking	
WireGuard VPN Remote Access and Site-to-Site	WireGuard VPN offers modern, high-speed, and low-latency encryption for remote users and branch connections with minimal firewall overhead.
IPSec VPN for site-to-site and multi-site connectivity	High-performance IPSec VPN allows firewalls to act as a VPN concentrator for other large sites, branch offices or home offices. Multipoint VPN uses a single VPN to connect a head office to multiple branch offices.
Dynamic routing through VPN tunnels	Dynamic routing over VPN links ensures no loss of connectivity, as traffic is routed through an alternate link in the event of a tunnel failure.



Flexible Deployment

A comprehensive firewall security lineup available in different flexible deployment options. Deploy high-performance hardware appliances using **Enterprise Firewall** for standard corporate edge or the **Data Center Firewall** for high-density modular capacity. For virtualized datacenters and public cloud networks, the **Virtual Firewall** delivers identical security and control in a software-only edition.

Flexible Deployment Options

The Edge Network Firewall series features two versions built on the exact same operating system, the hardware-based NG Firewall and the software-based Virtual Firewall. Because they share an identical codebase, their commands, features, and automation tools are completely interchangeable.



High-Performance Appliance Security for Enterprise Edge and Datacenters

EDGE Firewall is a 1U/2U rack-mountable appliance powered by enterprise Intel Xeon processors and high-speed Intel network interfaces. Built for organizations seeking full network stack control without proprietary licensing fees, it delivers wire-rate 10GbE forwarding, advanced routing, VPN, and firewall capabilities in a compact footprint. EDGE provides an open, transparent platform that is easy to automate, audit, and customize to your operational needs.

Software-Defined Network Security for Cloud, Edge, and Virtualized Datacenters

EDGE Virtual Firewall delivers complete edge security in a software-only, ready-to-deploy virtual machine for leading hypervisors and public clouds. Running the exact same codebase as physical EDGE appliances, it provides 100% feature and interface parity—including CLI, Web GUI, and automation workflows. This consistency allows teams to standardize management, configuration templates, and troubleshooting across physical, virtual, and cloud environments.

- **One Unified Experience:** Unlike legacy vendors that require different software for branches, datacenters, and cloud, Edge Network provides a single, uniform system across appliance, virtual, and public cloud environments (like AWS).
- **Seamless Automation:** Configurations and automation scripts (like Ansible playbooks or Terraform providers) work perfectly on both form factors without any modifications.
- **Multi-Instance Deployment:** Runs on the Edge Network Appliance, allowing you to run multiple independent firewalls to safely isolate different parts of your network.

EDGE FIREWALL

EDGE Firewall Series— Three Editions, One Codebase. All models are based on EDGE-Network LTS codebase.



Deployment Scenarios

- Enterprise Branch and SD-WAN Edge.
- Data Center Edge and Internet Gateway.
- Secure Remote Access Connector.

Deployment Scenarios

Enterprise Branch & SD-WAN Edge

- Multi-WAN & Auto-Failover: Bonds multiple ISP uplinks with dynamic routing and policy-based steering to keep branch connections resilient.
- Granular Security & QoS: Uses zone-based firewalls to isolate Corporate, Guest, and WAN segments while prioritizing VoIP and real-time traffic.
- Zero-Touch Provisioning: Cloud-init automation allows branch devices to be shipped unconfigured, auto-fetch settings on boot, and join the network instantly.

Datacenter Edge & Internet Gateway

- Enterprise BGP Peering: Accepts full or partial BGP tables with RPKI validation to block hijacked routes and maintain high-availability internet access.
- Multi-Tenant Isolation: Leverages front-door VRFs and stateful security zones to separate enterprise workloads, management, and internet traffic.
- High-Density & Flexible Connectivity: The Data Center Firewall is equipped with 4 modular expansion slots supporting up to 32 ports, featuring customizable 10G and 40G NIC modules to handle redundant ISP uplinks and high-speed core switches.

Secure Remote Access Concentrator

- Combines high-performance IPSec and ultra-fast WireGuard for site-to-site connectivity, alongside OpenVPN (TLS/Certificates) for user devices.
- Enterprise Identity Integration: Connects seamlessly with RADIUS and TACACS+ for Multi-Factor Authentication (MFA).
- Role-Based Access: Automatically applied dynamic, group-based firewall policies based on user identity and privilege levels.

LANEX

LANEX is a leader in cloud-native networking software and network disaggregation solutions. Powered by TeleSources Solutions, founded in 2015 based in London. For more information, visit us at www.lanex.uk