LionFilter 200

Next-Generation Firewall

- 10Gbps WAN Port and 4 2.5Gbps LAN Ports for high-speed networking.
- Enterprise-level cyber security features: Anti-Virus, Anti-Intrusion, Anti-WebThreat, Anti-DoS, and Network Behavior Management.
- Use the latest threat database with AI-powered engine to provide real time protection from 0-day virus threat.
- Support IPSec Site-to-Site VPN to establish secure connections among local networks from different locations.
- Low-Latency protection mode ensures both network stability and cybersecurity protection.
- LTE failover ensures automatic switch during WAN outage for stable connectivity.
- Ensures uninterrupted and reliable network connection with High Availability (HA).
- Provide Central management system (CMS) for managing lots of LionFilter 200.

Features

High-speed Network Content Inspection.

LionFilter 200 is equipped with 1x 10Gbps WAN Port and 4 x 2.5Gbps LAN Ports, providing high speed packets transfer. It features a comprehensive suite of enterprise-grade security functions, including Anti-Virus, Anti-Intrusion, Anti-WebThreat, Anti-Region, Anti-Spam, Firewall, and SSL/TLS encrypted traffic security. These capabilities are powered by patented Deep Packet Inspection (DPI) technology, helping users stop viruses and prevent from malicious content and attacks in various scenarios.

Use AI technology to detect 0-day virus and Botnet C&C server

Through cloud AI technology, it can identify zero-day viruses and dynamically changing malicious URLs. This provides comprehensive protection against attacks from malware and botnet connections, ensuring the completeness of cybersecurity.

IPSec Site-to-Site VPN, WireGuard Client-to-Site VPN

LionFilter 200 supports for IPSec and WireGuard protocols enables the establishment of secure encrypted channels over the internet, providing protection against eavesdropping or tampering of important information during transmission. These protocols cater to different scenarios, specifically for interconnecting different branch offices' local area networks (LANs) and allowing remote employees to securely access internal company resources.

LTE Failover ensures reliable connectivity during WAN outages.

When the primary WAN connection is interrupted, the system automatically switches to LTE via a USB dongle or smartphone hotspot to maintain seamless connectivity. Once the WAN connection is restored, it automatically performs failback to the primary WAN, ensuring stable and continuous network service.

Enhancing network reliability with High Availability (HA)

Supports High Availability (HA) with two or more devices. In the event of a failure, the standby unit seamlessly takes over from the active unit, ensuring uninterrupted network connectivity. (HA configuration is required.

Network Behavior Management and Smart QoS

LionFilter 200 allows monitoring and managing the applications used by devices within a specific IP range, and controlling the categories of web content accessible by these devices, including blocking advertisements. It also monitors the network traffic of the devices and provides QoS bandwidth management, assigning priority levels to specific traffic for designated devices.

Low-Latency protection mode ensures both network stability and cybersecurity protection.

The low-latency protection mode enables real-time packet scanning and threat interception without affecting the original network connection latency. Suitable in latency sensitive fields, like Smart Factory or Automated Production Line. It ensuring fast response and real-time data processing to maintain system stability.

Remotely managing multiple devices with the Central Management System (CMS).

Network administrators can use a Centralized Management System (CMS) to simultaneously configure and monitor multiple devices. This system allows them to manage various functions such as:

- **Signature Updates:**
  Ensuring that all devices are using the latest security definitions and signature files to protect against new threats.
- **License Activation and Renewal*:**
  Enabling or renewing licenses across multiple devices, ensuring continuous service and security features are available.
- **Device Firmware Updates:**
  Managing and pushing firmware updates to devices to ensure they are running the latest and most secure versions, minimizing vulnerabilities.

* License or subscription may be required for live-updated signature database or cloud AI functions.

Performance

Enabled Features	
Throughput (All)	*4 Gbps*
Concurrent Sessions	*500K*

All: Anti-Virus, Anti-Intrusion, Anti-WebThreat enabled

Hardware Overview

1. PWR (Power)
2. MGMT(Management)
3. CMS (Centrally managed)
4. AUTH (License)
5. NET (Internet)
6. WAN
7. 8. LAN (1-4)
8. MGMT
9. USB (LTE Failover)
10. RESET
11. Power switch
12. DC IN

Hardware Specifications

Product Name	LionFilter 200
Hardware	RAM : 2GB
	Flash : 4GB
	WAN : 1 x RJ45 (10 Gbps)
	LAN : 4 x RJ45 (2.5 Gbps, 1 of them can configure as MGMT Port)
Indicator	PWR, MGMT, CMS, AUTH, NET
Power	Type C DC 12V / 2A
Max Power Consumption	10W
Operation Temperature	0~40°C
Dimension	210 W x 40 H x 150 D (mm)
Weight	850 g
Certification	VCCI/BSMI/CE/FCC

Feature List

Security

Security features for various scenarios

- Virus detection on common protocols: FTP, HTTP, SMB, etc.
- Multiple engines virus scan
- Virus files destruction
- Executable files scan
- Office documents scan
- Compressed files scan
- Emails and attached files scan
- HTTPS Deep Inspection
- Ransomware detection
- Trojan detection
- Cloud virus scan
- Cyber-attacks blocking
- Brute-force attack detection
- Port scan detection
- DoS attack detection
- Abnormal protocol behavior detection
- Server Message Block (SMB) intrusion detection
- Botnet attack detection
- Prompt-updated virtual patch
- Unsafe website access blocking
- Domain name checking
- URL checking
- IPv4 & IPv6 checking
- Malicious links checking in Email content
- Malicious and phishing website cloud database
- Customized whitelist for security policy
- Threat source analysis and geo-blocking
- User-defined firewall for both TCP & UDP protocols
- Firewall rules scheduling
- Always-allow/deny website list
- Detected threat detailed information listing
- Threat log exporting (CSV)
- Online threat encyclopedia for Anti-Intrusion
- External user-defined malicious websites
- Dynamic malicious URLs detection with AI
- 0-day virus identification with AI
- Real-time Protection Mode
- Low-Latency Protection Mode

Network Configuration

Seamless integration to the original network topology

- Intuitive installation in Bridge Mode (default)
- DHCP server and port forwarding for Router Mode
- VPN server for mobile devices protection
- Support VLAN
- User-defined proxy server setting to access Lionic cloud services
- Advanced routing configuration for static route and NAT
- Customized DHCP setting
- Site-to-Site VPN(IPSec)
- Supports LTE failover during WAN outages
- Support HA: High availability with 2 or more devices

Network Usage Management

Internet Behavior Management & Intelligent Bandwidth Allocation

- Quality of Service (QoS) management
- Monitor Network traffic
- Asset recognition and management
- Website content categorizing and filtering
- Application identification and blocking
- Blocks advertisements embedded in web pages.

Monitor & Control

Sustained protection against growing threats

- Intuitive web user interface
- Remote access with DDNS
- Access granting for remote administrators
- Secure access with encrypted connection
- 2-factor authentication for VPN server accessing
- Inspected traffic summary
- Detected threat statistics
- System resource monitor
- Lionic cloud service license management
- Auto-generated summary report
- Self-diagnosis rating for system load
- Network security risk estimation
- Security policy and system setting backup/restore
- Reboot scheduling
- System user activity history
- Firmware & signature auto-update
- User-defined syslog server setting to collect detailed system status
- Customized NTP server setting
- Threat-detected notification mail
- Network diagnosis tools
- System log exporting
- Monitor system status with SNMP
- Dedicated Management Port

Central Management System (CMS)

Remote management with CMS

- Visualized operating status summary
- Defense situation dashboard
- Remote configuration
- Creating and applying security policy for device groups
- Summarized threat log exporting (CSV)
- Alternative signature update service
- Remotely firmware update triggering
- Threat notification via email
- System user activity history
- System user permission management
- Batch operations for multiple devices
- Remote system log exporting
- Batch remote Activate/Update license

LionFilter 200
Makes Security Simple

LIONIC
Security Solution Provider

Sales Contact
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com

Lionic Corp.
https://www.lionic.com/
1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.

© Copyright 2025 Lionic Corp. All rights reserved.