Pico-UTM 100

Network Security Filter
SMB, Home & Individual

Highlights

- Enterprise-level Security Features:
  Anti-Virus, Anti-Intrusion, Anti-WebThreat and Firewall
- 3 minutes setup while keeping the original network topology.
- Live update signature database protects your network from the latest threat and virus.
- Optional CMS (Central Management System) for remote management of multiple Pico-UTM.

Features

Enterprise-level security features for various scenarios

With Deep Packet Inspection (DPI), Pico-UTM 100 offers comprehensive and enterprise-level protections, including Anti-Virus, Anti-Intrusion, Anti-WebThreat and Firewall. These features assist users in destroying viruses or blocking malicious contents and attacks effectively.

Seamless integration to the original network topology

3 minutes installation in bridge mode with 1 WAN and 1 LAN. Plug-n-play without changing oroginal network topology.

Sustained protection against growing threats

Live update signature database is able to identify the latest threat and virus including variants.

Remote management with Central Management System (CMS)

Administrator can monitor the real-time status of all Pico-UTM devices and configuration via CMS.

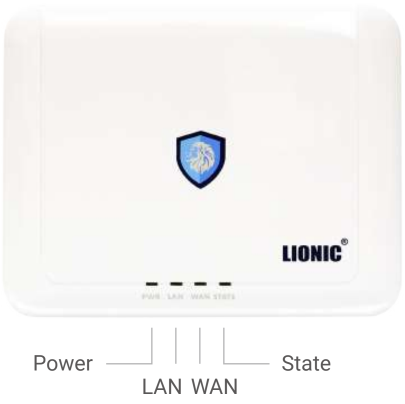
* License or subscription may be required for signature database or CMS.

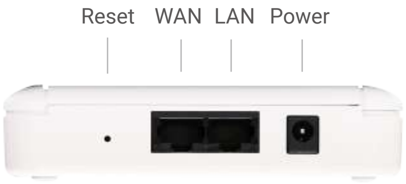
Performance

Enabled Features	
Throughput (Pure Forwarding _all disabled)	*833 Mbps*
Throughput (All Features)	*700 Mbps*
Concurrent Sessions	*30K*

Testing Tool : IXIA IxLoad HTTP Download 1MB.exe
Remarks : The test result may be varied due to the test environment and test devices.

Hardware Overview





Hardware Specifications

Product Name	Pico-UTM 100
Hardware	CPU : Qualcomm IPQ4018, 4 ARMv7 cores, 716 MHz
	RAM : 256MB
	Flash : 512MB
Interface	Gigabit Ethernet WAN x 1 Port, Gigabit Ethernet LAN x 1 Port
Power Required	Universal Switching Power Adapter 100-240V AC IN, 12V DC
Reliability	Operating Temperature : 0-40°C (32-104°F)
	MTBF (hrs) : 2,041,392
Dimensions	116 W x 25 H x 91 D (mm)
Maximum Weight	135g

Feature List

Security

Security features for various scenarios

- Virus detection on common protocols: FTP, HTTP, SAMBA, etc.
- Hybrid virus scan
- Virus files destruction
- Executable files scan
- Office documents scan
- Compressed files scan
- Emails and attached files scan
- Enhanced ransomware detection
- Enhanced trojan detection
- 1-to-many virus signature
- Virus cloud database
- Cyber-attacks blocking
- Brute-force attack detection
- Port scan detection
- DoS attack detection
- Abnormal protocol behavior detection
- SAMBA intrusion detection
- Botnet attack detection
- Prompt-updated virtual patch
- Unsafe website access blocking
- Domain name checking
- URL checking
- IPv4 & IPv6 checking
- Malicious and phishing website cloud database
- Customized whitelist for security policy
- User-defined firewall for both TCP & UDP protocols
- Always-allow/deny website list
- Detected threat detailed information listing
- Threat log exporting (CSV)
- Threat log reporting to cloud log server

Network

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
- User-defined proxy server setting to access Lionic cloud services

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
- Inspected traffic summary
- Detected threat statistics
- System resource monitor
- Security policy and system setting backup/restore
- Lionic cloud service license management
- 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

CMS

Central Management System (CMS)

Remote management with CMS

- Visualized operating status summary
- Defense situation dashboard
- Remotely configure Pico-UTM
- Creating and applying security policy for Pico-UTM groups
- Summarized threat log exporting (CSV)
- Alternative signature update service
- Remotely firmware update triggering
- Threat-detected notification mail
- System user activity history
- System user permission management

Pico-UTM 100
Makes Security Simple

LIONIC
Security Solution Provider

Sales Contact
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com
https://www.pico-utm.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.