Tera-UTM 12

Industrial Level Network Security Filter

- Industrial level cyber security + Industrial control systems protection: Anti-Virus, Anti-Intrusion, Anti-WebThreat, Anti-Region, Firewall and ICS protocol inspection.

- Prevent Tera-UTM 12 from causing network interruptions due to maintenance, downtime or power outages with Hardware Bypass.

- Easy setup and intuitive user interface with robust design.

- Live update threat database, protecting your network from the latest virus and intrusion.

- Central management system (CMS) for monitoring multiple Tera-UTM 12.

Features

Industrial level security protection for various scenarios

With Deep Packet Inspection (DPI), Tera-UTM 12 offers comprehensive and Industrial level protections, including Anti-Virus, Anti-Intrusion, Anti-WebThreat, Anti-Region and Firewall. These features assist users in destroying viruses or blocking malicious contents and attacks effectively.

Advanced protection for industrial control systems (ICS)

Tera-UTM 12 is able to inspect packets transfering in ICS protocols, such as Modbus, DNP3, etc. Users can define their own rules based on their requirement, and Tera-UTM 12 can help them control and protect their ICS.

Enhanced inspection for SSL / TLS traffic

Tera-UTM 12 can decrypt, inspect and re-encrypt the SSL / TLS traffic in order to provide full protection when browsing HTTPS websites. Users can also set a whitelist with URL, IP address or website categories to keep the connection encrypted.

Sustained protection against growing threats

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

Remote management with Central Management System (CMS)

Administrator can monitor the real-time status of all linked Tera-UTM 12 devices and configure by group on CMS.

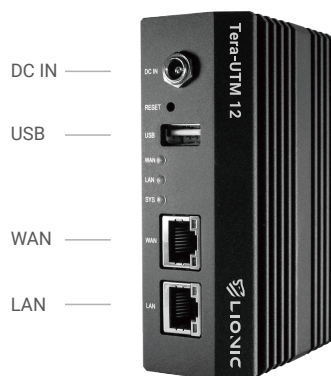* License or subscription may be required for signature database or CMS.

Performance

Enabled Features	
Throughput (Pure Forwarding)	*910 Mbps*
Throughput (All)	*890 Mbps*
Throughput (All+SSL/TLS Inspection)	*355 Mbps*
Concurrent Sessions	*1000K*

Pure Forwarding: All features disabled
All: Anti-Virus, Anti-Intrusion, Anti-WebThreat enabled

Hardware Overview

Hardware Specifications

Product Name	Tera-UTM 12
Hardware	CPU: NXP i.MX 8M PLUS
	Memory : 4G LPDDR4, 4000MT/s
	Flash : 8GB eMMC NAND Flash for O.S.
Ethernet	Chipset : 2 x AR8035-AL1A
	Speed : 2 x 10/100/1000 Mbps
	Support Hardware Bypass (Controlled By Cortex-M7)
Indicator	2 x Ethernet Active, 1 x Power Status (Green/Red 2color)
Power	7V~36V DC-in Lockbale
Environment	Operation Temperature : 0-60°C
	Storage Temperature : -40~85°C 5%~95% Relative Humidity, non-condensing
Dimension	108 W x 72 H x 38 D (mm)
Certification	BSMI

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
- SSL/TLS scan in HTTPS
- User-defined website whitelist for HTTPS 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
- ICS protocol anomaly dectection
- User-defined ACL for ICS protocols
- Threat source analysis and geo-blocking

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
- 2-factor authentication for VPN server accessing
- Inspected traffic summary
- Detected threat statistics
- System resource monitor

- System user activity history
- Reboot scheduling
- 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

- Security policy and system setting backup/restore
- Lionic cloud service license management
- Auto-generated daily / weekly report
- Self-diagnosis rating for system load
- Network security risk estimation

- Network diagnosis tools
- System log exporting
- Network traffic analysis

CMS

Central Management System (CMS)
Remote management with CMS

- Visualized operating status summary
- Defense situation dashboard
- Remotely configure Tera-UTM 12
- Creating and applying security policy for Tera-UTM 12 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

Tera-UTM 12
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.