DATA SHEET

ThingzFirewall Enterprise

TE-300U/ TE-500U

Next Generation Firewall
Secure SD_WAN
Secure Web Gateway

TE-300U

TE-500U

ThingzEye Enterprise-Firewall is the true Next-Generation Firewall (NGFW) which provides *360° network security*. We offer scalable solutions for different performance requirements yet full range of threat protection. The solution is built with a lot of enthusiasm to deliver a solution for the futuristics enterprise networks which are blends of traditional machines with Internet of things (IoT) devices. The solution is powered with AI/ML technologies to provide defense against the threats yet to be developed as zero-day attacks. ThingzFirewall offers users a friendly interface to manage and monitor their network security at an affordable cost with the ambition of protecting every network. The detailed list of features and hardware specifications are given in the following tables.

FEATURES

Intrusion Detection/ Prevention System (IDS/IPS)

Packet analyzer

- Process of intercepting and logging traffic for analysis.

Layer 7 applications detection

- Identification of Layer 7 applications on the basis of analysis of their communication patterns such as signatures and parsing information.

Emerging threats database

- *Emerging Threats Database* provides timely and accurate threat intelligence which integrates seamlessly with the firewall to enhance security decision making

IP blacklist database

- Maintains an *IP Blacklist Database* for filtering out illegitimate or malicious IP addresses from accessing your network

Deep packet inspection (DPI)

- It evaluates the data part and the header of a packet that is transmitted through an inspection point

Firewall and Routers

Stateful packet inspection (SPI)

- Monitors the state of active connections and uses this information to determine which network packets to allow through the firewall

GeoIP blocking

- It blocks web traffic from entire countries, and can be an effective way to stop hackers from attacking your business

Anti-spoofing

- Identifying and dropping packets that have a false source address

Connection limits

- Firewall connection limit policy allows or denies traffic based on a matching tuple: source address, destination address, service type, and connection count

Captive portal guest network

- A captive portal is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources

Supports concurrent IPv4 and IPv6

- You can now specify up to ten IPv4 and IPv6 DNS servers in a single client settings configuration

NAT mapping (inbound/outbound)

- NAT is configured in two directions: inbound and outbound. Outbound NAT defines how traffic leaving a local network destined for a remote network, such as the Internet is translated. Inbound NAT refers to traffic entering a network from a remote network

Configurable static routing

- A form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. It reduces the overhead from network sources

PPPoE server

- PPPoE is a client-server protocol that means PPPoE client (IP devices such as Desktop, Laptop, wireless Router etc.) will request for IP information to PPPoE server providing security information (username and password) and PPPoE server will provide IP information by matching that security information

IPv6 router advertisements

- The RADVD (Router Advertisement Daemon) is used for IPv6 auto-configuration and routing. When enabled, messages are sent by the router periodically and in response to solicitations. A host uses the information to learn the prefixes and parameters for the local network

Multiple IP addresses per interface

- Multiple IP addresses per interface is very useful for setting up multiple virtual sites on Apache using one single network interface with different IP addresses on a single subnet network

Dynamic DNS

- Automatically updates a name server in the Domain Name System (DNS), often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information

Reverse proxy

- A reverse proxy server is a type of proxy server that typically sits behind the firewall in a private network and directs client requests to the appropriate backend server. A reverse proxy provides an additional level of abstraction and control to ensure the smooth flow of network traffic between clients and servers.

DHCP server

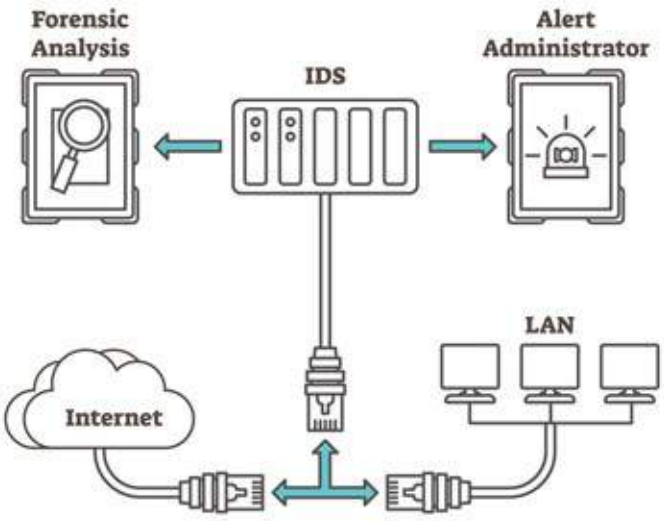
- A network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients

DNS forwarding

- The process by which particular sets of DNS queries are handled by a designated server, rather than being handled by the initial server contacted by the client

IPv6 network prefix translation

- IPv6-to-IPv6 Network Prefix Translation (NPTv6 or NAT66) is a specification for IPv6 to achieve the address-independence at the network edge, similar to network address translation (NAT) in Internet Protocol version 4



(Intrusion Detection System)

Virtual Private Network (VPN)

- IPsec and OpenVPN
- Site-to-site and remote access VPN support
- SSL encryption
- VPN client for multiple operating systems
- L2TP/IPsec for mobile devices
- Multi-WAN for failover
- IPv6 support
- Split tunneling
- Multiple tunnels
- VPN tunnel failover
- NAT support
- Automatic or custom routing
- Local user authentication or RADIUS/LDAP

Enterprise Reliability

Optional multi-node high availability clustering

- To ensure that a multi-node cluster remains available

Multi-WAN load balancing

- Dual WAN or Multi WAN routers give you a reliable Internet at all times coupled with load balancing and security. Load balancing enables traffic to be directed to an optimal path.

Automatic connection failover

- Automatic connection failover automates the process of re-establishment of an asynchronous replication connection to another sender of the sender list

Bandwidth throttling

- Bandwidth throttling is the intentional slowing or speeding of an internet service by an Internet service provider (ISP). It is a reactive measure employed in communication networks to regulate network traffic and minimize bandwidth congestion

Traffic shaping wizard

- Traffic shaping wizards can be used for prioritizing a certain application traffic and deprioritize the other application traffic when required

Reserve or restrict bandwidth based on traffic priority

- Restricts bandwidth on the basis of priority assignment.

Fair sharing of bandwidth

- Fair bandwidth allocation in the network devices or entities

User data transfer quotas

- Network Traffic Quota allows you to specify the data transfer limit for a specific user

User Authentication

- Local user and group database
- User and group-based privileges
- Optional automatic account expiration
- External RADIUS authentication
- Automatic lockout after repeated attempts

Proxy and Content Filtering Features

- HTTP and HTTPS proxy
- Non Transparent or Transparent caching proxy
- Do Anti-virus filtering
- Main/URL filtering
- Safe Search for search engines
- HTTPS URL and content screening
- Website access reporting
- Domain Name blacklisting (DNSBL)
- Usage reporting for daily, monthly, etc.

System Configurations

- Web-based configuration
- Setup wizard for initial configuration
- Remote web-based administration
- Customizable dashboard
- Easy configuration backup/restore
- Configuration export/import
- Encrypted automatic backup to Netgate server
- Variable level administrative rights
- Multi-language support
- Forward-compatible configuration
- Serial console for shell access and recovery options

Security

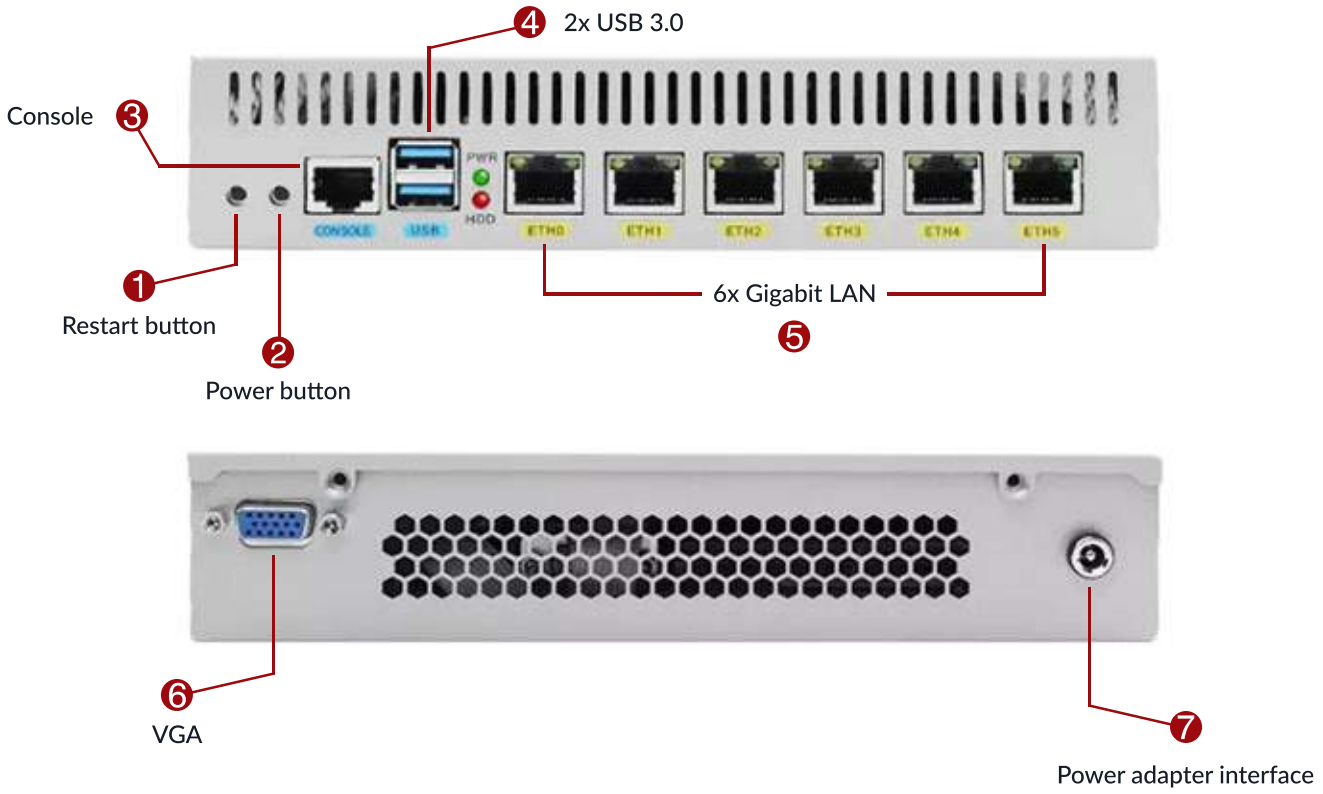
- Web interface security protection
- CSRF protection
- HTTP Referer enforcement
- DNS Rebinding protection
- HTTP Strict Transport Security
- Frame protection
- Optional key-based SSH access

Reporting & Monitoring

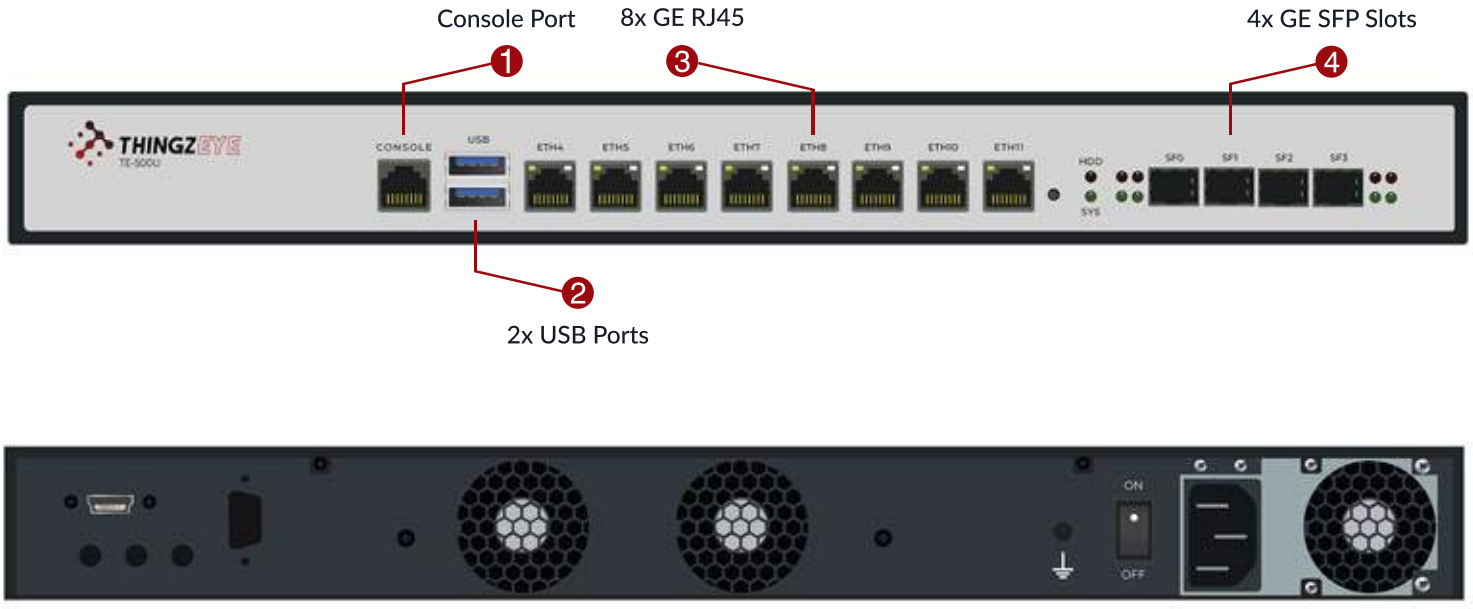
- Dashboard with configurable widgets
- Local logging
- Remote logging
- Local monitoring graphs
- Real-time interface traffic graphs
- SNMP monitoring
- Notifications via web interface, SMTP, or Growl
- Hardware monitoring
- Networking diagnostic tools

Hardware

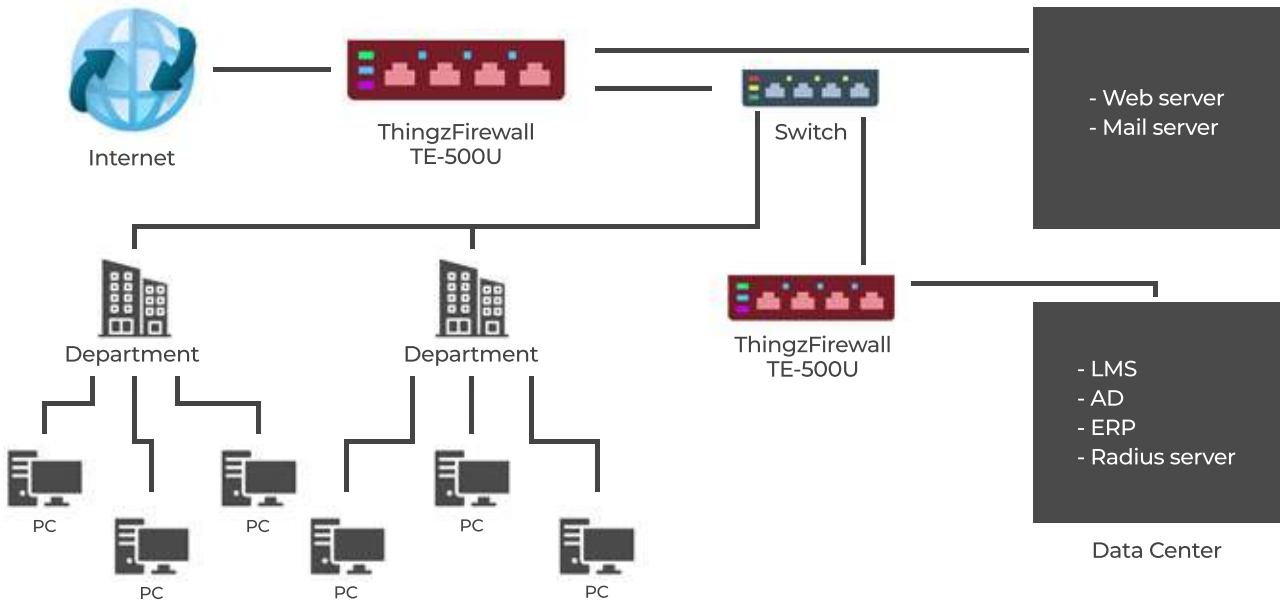
ThingzFirewall TE-300U



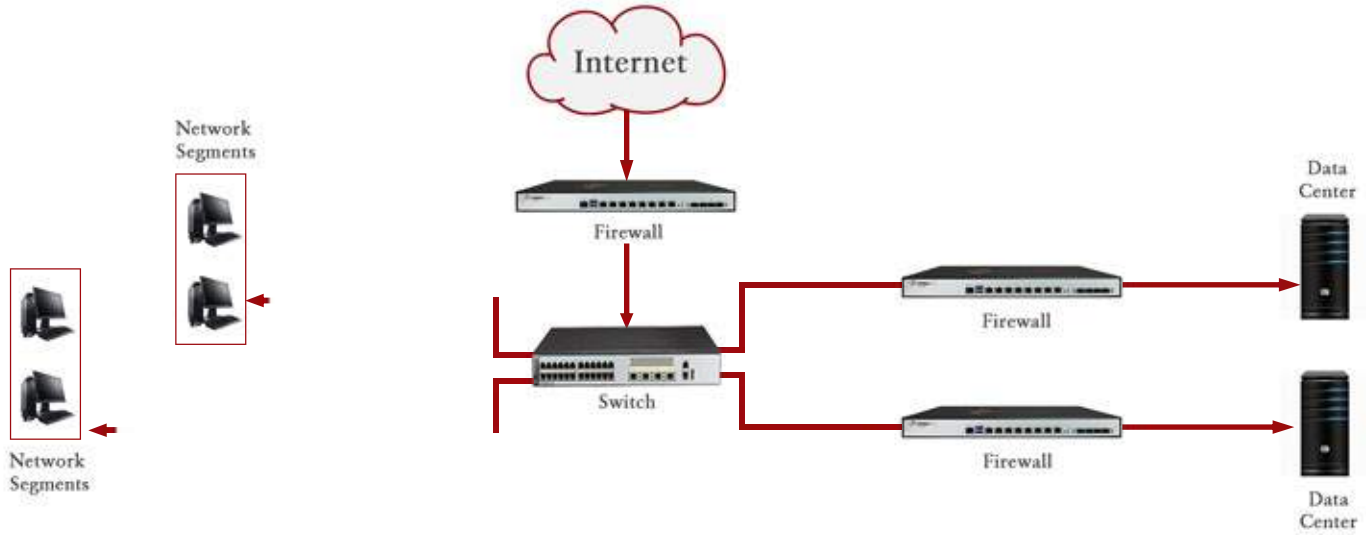
ThingzFirewall TE-500U



Deployment Architecture



(Deployment Architecture 1.1)



(Deployment Architecture 1.2)

SPECIFICATIONS	TE-300U/ TE-500U
CPU	Intel Core i7-7600U, 2.8 GHz Processor, 4 MB Smart Cache / Intel Core i9-9900, 5 GHz Processor, 16 MB Smart Cache
Memory	16GB RAM / 32GB RAM DDR4 2666
Storage (SSD)	128GB / 256GB
Display Chip	Intel HD Graphics
Display Connection	VGA Display connector
CPU Fan	Silent Fan
Power Source	Mingwei power supply, 110V-240V 50-60Hz AC Input (Outta power source 12V 4A)
No. of Cores / Threads	2 / 4 / 8 / 16
Safety Certification	CE/CCC/FCC Class A/ROHS
TDP	15W / 65 W
Front I/O	6* Gigabit LAN 2* USB 3.0, 1*console port / 4*intel X710 Gigabit optical port, 8*RJ45 GE (1Gbps), 2*USB 2.0, 1*console port
Product Measurements	210*200*45mm / 250*440*45mm (W*L*H)
Working Temperature / Humidity	0° C-60° C / 0-60%

Performance Statistics

THROUGHPUT SPECIFICATIONS (@ 1 GBPS LINK)	TE-300U/ TE-500U
Firewall throughput	910.21 / 937.0 Mbps
VPN throughput	355.43 / 365.89 Mbps
VPN + IPS throughput	298.36 / 307.15 Mbps
IPS throughput	676.64 / 696.56 Mbps
Concurrent sessions	upto 1 Million

FEATURES

Network Security

- Stateful Packet Firewall
- Demilitarized Zone (DMZ)
- Intrusion Detection and Prevention (Snort)
- Multiple Public IP Addresses
- Multiple WAN
- Quality of Service and Bandwidth Management
- SNMP Support
- VoIP/SIP Support
- SYN/ICMP Flood Protection
- VLAN Support (IEEE 802.1Q Trunking)
- DNS Proxy/RoutingAnti-Spyware
- Phishing Protection

WAN Failover

- Automatic WAN Uplink Failover
- Monitoring of WAN Uplinks
- Uplink Types: Ethernet (Static/DHCP), PPPoE, PPTP, WiFi 802.11abgn/ac

Network Address Translation

- Destination NAT
- Incoming Routed Traffic
- One-to-One NAT
- Source NAT (SNAT)
- IPsec NAT Traversal

Routing

- Static Routes
- Source-Based Routing
- Destination-Based Routing
- Policy-Based Routing (Based on Interface, MAC Address, Protocol or Port)

Bridging

- Firewall Stealth ModeOSI Layer 2
- Firewall Functionality
- Spanning Tree
- Unlimited Interfaces per Bridge

Virtual Private Networking

- Encryption: Null, AES
- 128/192/256-bit,
- IKEv1 & IKEv2
- Dead Peer Detection (DPD)
- NAT Traversal
- Compression
- Perfect Forward Secrecy (PFS)
- VPN Site-to-Site
- VPN Client-to-Site (Roadwarrior)
- L2TP User Authentication
- XAuth User Authentication

OpenVPN

- True SSL/TLS VPN
- Authentication: Pre-Shared Key, X.509 Certificates
- PPTP Passthrough
- VPN Client-to-Site (Roadwarrior)
- VPN Client for Microsoft Windows, Mac OS X and Linux
- VPN Failover
- Multiple Server Support Scalability
- Support for Mobile Devices (Android, iOS)

User Management & Authentication

- Unified User Management for OpenVPN, L2TP, x`
- Group Management
- Integrated Certificate Authority
- External Certificate Authority Support
- User Password and Certificate Management (Two-factor Authentication)
- Multiple Authentication Servers (Local, LDAP, Active Directory)

Serial Communication

- Serial over IP

Event Management

- More Than 30 Individually Configurable Events
- Email Notifications
- SMS Notifications
- Powerful Python Scripting Engine

Extra Services

- NTP (Network Time Protocol)
- DHCP Server
- SNMP Server
- Dynamic DNS

Logging and Reporting

- Reporting Dashboard
- Detailed System and Attack

Reports

- Live Network Traffic Monitoring (powered by ntopng)
- Live Log Viewer
- Network/System/Performance

Management / GUI

- Easy Web-Based Administration (SSL)
- Multi-Language Web-Interface (English, Italian, German, Japanese, Spanish, Portuguese, Turkish, Chinese, Russian)
- Secure Remote SSH/SCP Access
- Serial Console
- Centralized Management through Endian Network

Statistics

- Rule-Based Logging Settings (Firewall Rules)
- Syslog: Local or Remote
- OpenTSA Trusted Timestamping

Updates and Backups

- Scheduled Automatic Backups
- Encrypted Backups via E-mail
- Instant Recovery / Backup to USB Stick (Endian Recovery Key)
- Centralized Updates through SSL