Dual 10G Zero Trust Security Gateway with 4-Port 10/100/1000T

Dual-10G Zero Trust VPN Gateway with FIDO2 Passwordless Management Access and Secure ZTNA Overlay Connectivity

The PLANET ZT-800 is an enterprise-grade Dual-10G VPN gateway designed to strengthen identity-based access control for secure gateway administration and encrypted inter-site connectivity. By integrating **FIDO2 passkey authentication**, **TOTP- based MFA (multi-factor Authentication)**, and **certificate-based login** protection, the ZT-800 enforces Zero Trust principles at the management access layer—ensuring that only verified administrators can control critical network infrastructure.

To support secure connectivity across distributed deployments, the ZT-800 enables Zero Trust Network Access (ZTNA) overlay networking, allowing authenticated gateways to establish encrypted peer-to-peer tunnels without exposing internal services to the public Internet. This architecture simplifies secure branch-to-branch communication while reducing reliance on traditional perimeter-based VPN models.

Powered by a high-performance quad-core platform with dual 10G WAN interfaces, the ZT-800 delivers high-throughput encrypted networking for enterprise branches, infrastructure sites, and industrial edge environments. It supports multiple VPN technologies—including **IPSec**, **OpenVPN**, **WireGuard**, GRE, PPTP, and L2TP—ensuring flexible interoperability across hybrid network architectures.

With **Secure Boot** protection and **Post-Quantum Cryptography (PQC)-ready TLS** architecture, the ZT-800 strengthens platform trust integrity and prepares organizations for long-term cryptographic resilience against emerging quantum-era security risks.

Designed for secure distributed network deployments, the ZT-800 also provides:

- Dual-WAN failover and load balancing
- Advanced routing and segmentation capability
- IPv4/IPv6 dual-stack readiness
- Secure gateway deployment for branch, industrial, and infrastructure networks

Highlights

- One 1G/2.5G/5G/10GBASE-T RJ45 Port for WAN/LAN interface
- One 1G/2.5G/10GBASE-X SFP+ slot for WAN/LAN interface
- Dual-WAN failover and dual-WAN load balancing
- SSL VPN and robust hybrid VPN (IPSec/PPTP/L2TP over IPSec/OpenVPN/WireGuard)
- Stateful Packet Inspection (SPI) firewall and content filtering
- Blocks DoS/DDOS attack, port range forwarding
- Zero Trust access control with identity authentication and policy enforcement Support hardware security key authentication such as CoreTrust Key for MFA protection
- High Availability, AP Controller, Captive Portal and RADIUS
- IPv6, SNMP, PLANET DDNS and Universal Network Management System
- Planet NMS controller system and CloudNMS platform supported

Hardware

- 4 10/100/1000BASE-T RJ45 ports
- 1 1G/2.5G/5G/10GBASE-T RJ45 Port for WAN/LAN interface
- 1 1G/2.5G/10GBASE-X SFP+ slot for WAN/LAN interface
- 1 USB port for system configuration backup and restoration
- Reset button and fanless design
- Desktop installation or rack mounting

IP Routing Feature

- Static Route
- Dynamic Route
- OSPF

Firewall Security

- Secure Boot to ensure trusted firmware integrity
- Cybersecurity
- Stateful Packet Inspection (SPI) firewall
- Blocks DoS/DDoS attack
- Content Filtering
- Zero Trust access control

Zero Trust–Protected VPN Access with Passkey Authentication and MFA Enforcement

The ZT-800 introduces a secure VPN Portal designed to strengthen identity verification before VPN connectivity is established. By supporting FIDO2 passkey authentication, multi-factor authentication (MFA), and optional external RADIUS integration, the portal ensures that only verified users can obtain authorized OpenVPN or WireGuard client configurations.

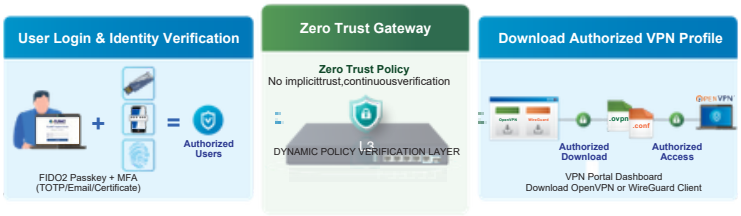
Unlike traditional VPN deployment models where credentials alone grant tunnel access, the ZT-800 enforces identity validation at the profile provisioning stage—reducing the risk of unauthorized VPN distribution and strengthening access control across remote users and distributed teams.

This identity-aware VPN onboarding mechanism enables organizations to implement Zero Trust principles for remote connectivity while maintaining compatibility with widely deployed VPN client infrastructures.

Secure Boot for Trusted System Integrity

The ZT-800 incorporates a Secure Boot mechanism to ensure that only authenticated and trusted firmware can be executed during system startup. This hardware- based protection prevents unauthorized or tampered firmware from being loaded, safeguarding the device against malicious attacks at the system level and ensuring a trusted foundation for network security.

Zero Trust VPN Portal - Identity-Verified VPN Access



Only Authorized Users Can Download OpenVPN or WireGuard Client Configurations after FIDO2 Passkey + MFA Identity Verification

Automatic Failover between Dual WAN

With its fiber and copper dual WAN interfaces—10GBASE-X SFP+ and 10GBASE-T — the ZT-800 ensures continuous Internet connectivity through automatic failover. Administrators can freely set the WAN priority, and when the primary link becomes unavailable, the secondary WAN interface takes over instantly. This design guarantees reliable, always-on network uptime for mission-critical applications.

Flexible WAN interface Enables Extension of Network Deployment

The ZT-800 is equipped with both copper and fiber WAN interfaces, featuring an SFP+ slot that supports a wide range of SFP+ and SFP transceivers for FTTx and long-distance extensions. Administrators can select SFP+ and SFP modules according to distance requirements:

- Multi-mode fiber: 550 m to 2 km
- Single-mode / WDM fiber: 10 km, 20 km, 30 km, 40 km, 50 km, 60 km, 70 km, up to 120 km

This capability allows the device to efficiently uplink to backbone switches or monitoring centers over long distances.

- Identity-based access policy
- MAC Filtering and IP Filtering
- NAT ALGs (Application Layer Gateway)
- Blocks SYN/ICMP Flooding

VPN Features

- IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (OpenVPN, compatible with VPN services such as Surfshark and NordVPN), WireGuard
- Encryption methods: DES, 3DES, AES, AES-128/192/256
- Authentication methods: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- PQC TLS (Post-Quantum Cryptography TLS) ready

Networking

- Outbound load balancing
- Failover for dual-WAN
- High Availability
- Captive Portal
- RADIUS Server/Client
- Static IP/PPPoE/DHCP client for WAN
- DHCP server/NTP client for LAN
- Protocols: TCP/IP, UDP, ARP, IPv4, IPv6
- Port forwarding, QoS, DMZ, IGMP, UPnP, SNMPv1,v2c, v3
- MAC address clone
- DDNS: PLANET DDNS, Easy DDNS, DynDNS and No-IP
- NAT disable support for pure routing mode deployment

Others

- Setup wizard
- Dashboard for real-time system overview
- SFP-DDM (Digital Diagnostic Monitor)
- Supported access by HTTP or HTTPS
- Auto reboot
- PLANET NMS System and Smart Discovery Utility for deployment management
- PLANET CloudNMS app for real-time monitoring

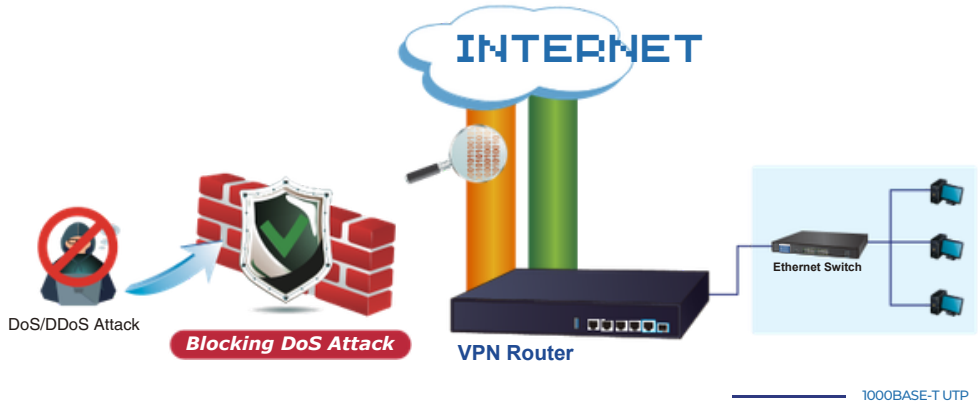
Cybersecurity Network Solution to Minimize Security Risks

The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the ZT-800 is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the ZT-800 offers an easy-to-use, platform independent management and configuration facility. The ZT-800 supports SNMP and it can be managed via any management software based

on the standard SNMP protocol. With support for advanced security mechanisms such as Secure Boot and PQC TLS readiness, the ZT-800 ensures long-term protection against evolving cyber threats, including quantum-era attacks.

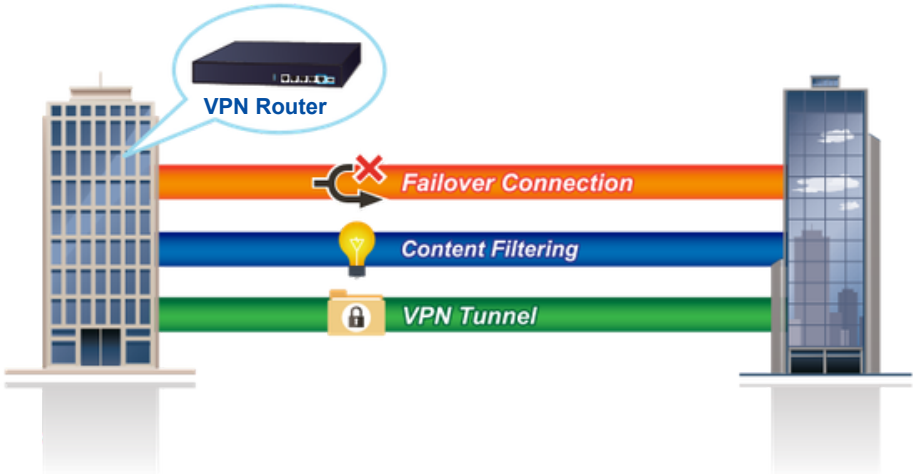
Excellent Ability in Threat Defense

The ZT-800 with built-in SPI (stateful packet inspection) firewall and DoS/DDoS attack mitigation functions provides high efficiency and extensive protection for your network. Thus, virtual server and DMZ functions can let you set up servers in the Intranet and still provide services to the Internet users.



High-Availability VPN Security Router Designed for SMB Applications

The ZT-800 ensures strong data privacy and secure remote access through its comprehensive VPN suite. It supports IPSec VPN with DES/3DES/AES encryption and MD5, SHA-1, SHA-256, SHA-384, and SHA-512 authentication, as well as GRE tunneling, SSL VPN, PPTP, L2TP, and WireGuard for modern, lightweight, high-speed encrypted connections. With this extensive VPN capability, the ZT-800 provides secure, flexible, and resilient connectivity for branch sites, remote workers, and sensitive business operations.



Flexible Routing with NAT Disable Capability

The ZT-800 supports NAT disable functionality, allowing it to operate in pure routing mode for advanced network deployment scenarios. This feature is particularly beneficial for environments requiring end-to-end IP transparency, such as enterprise backbone networks, data centers, or integration with upstream security systems. By disabling NAT, administrators can achieve greater control over traffic flow and routing policies.

Maximizing Work Efficiency with PLANET SD-WAN Gateway

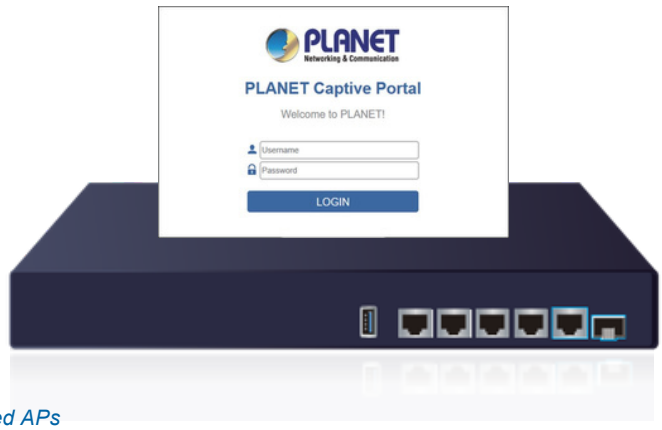
PLANET ZT-800 incorporated in SD-WAN (software-defined wide area network) function can greatly increase WAN optimization for multiple WAN links to be managed. With SD-WAN, users can connect any application across all available network connections at every site. It improves application performance and provides

a high-quality user experience for increasing business productivity and reducing IT costs.

Integrated Wi-Fi Management for Secure and Easy Deployment

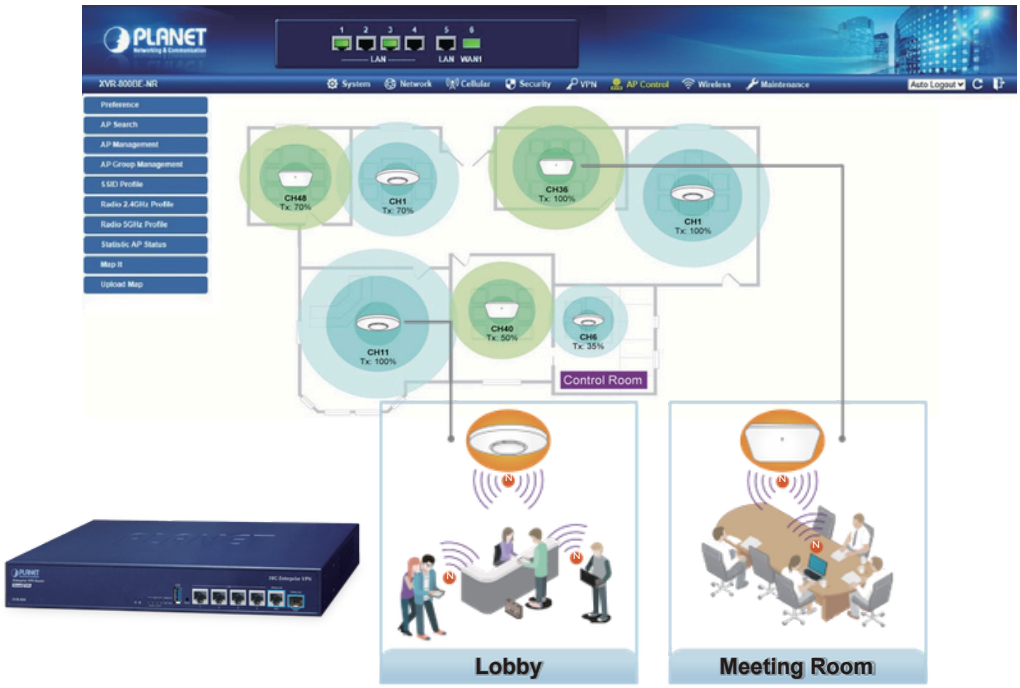
The ZT-800 integrates an AP Controller, Captive Portal, RADIUS authentication, and DHCP server to streamline Wi-Fi deployment for small and medium-sized businesses. These built-in services eliminate the need for external servers, enabling administrators to centrally manage APs, enforce access policies, and deliver secure employee and guest Wi-Fi networks with reduced setup complexity.

Captive Portal



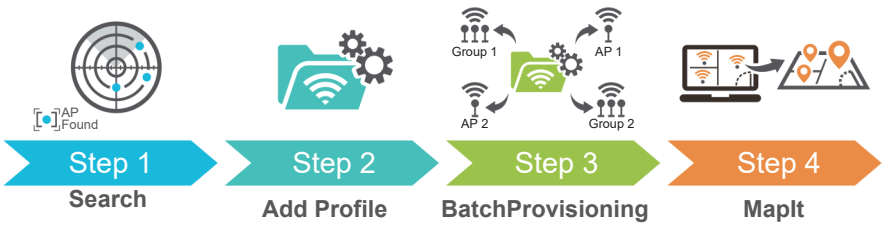
Centralized Remote Control of Managed APs

Through its intuitive web-based interface, the ZT-800 allows easy centralized control of PLANET Smart APs, with simple configuration of SSIDs, radio settings, and security policies. A quick four-step setup pushes wireless profiles to multiple APs or groups at once, enabling fast rollout and reduced deployment cost.



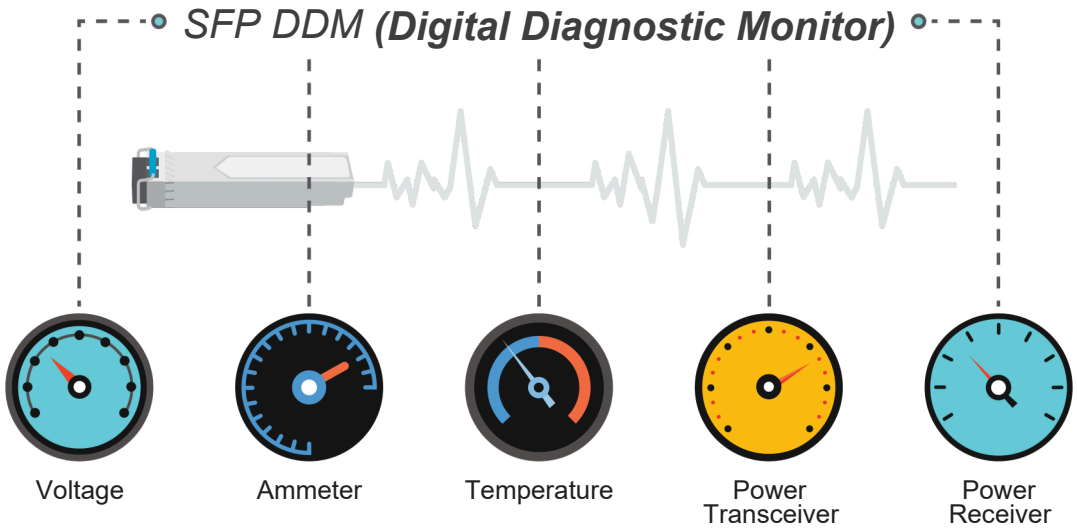
Administrators can cluster APs of the same model for unified management, flexibly expand or remove APs, and perform bulk provisioning or firmware upgrades—all from a single control point. This ensures scalable, efficient, and low-maintenance Wi-Fi management.

Simplified Cluster Management with 4 Steps



Intelligent SFP Diagnosis Mechanism

The ZT-800 supports SFP-DDM (digital diagnostic monitor) function that greatly helps network administrator to easily monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

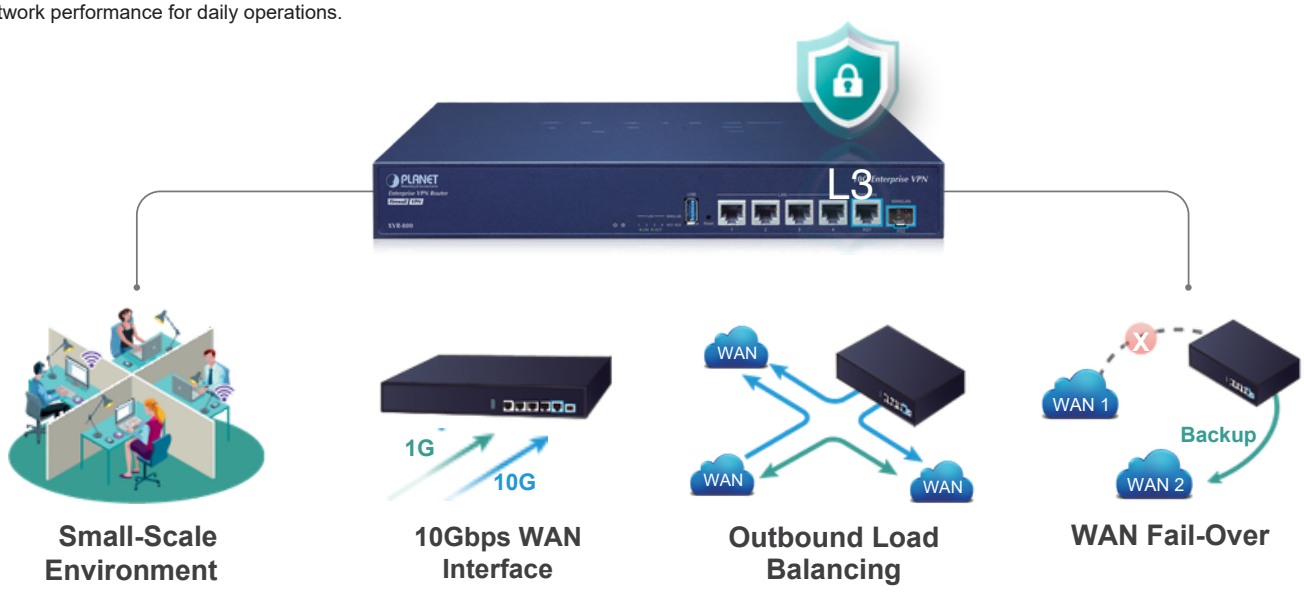


Applications

High-PerformanceNetwork Reliability with Dual-WAN and Load Balancing

The ZT-800 is ideal for small to medium-sized businesses that require stable and efficient network connectivity. With dual-WAN load balancing and automatic failover,

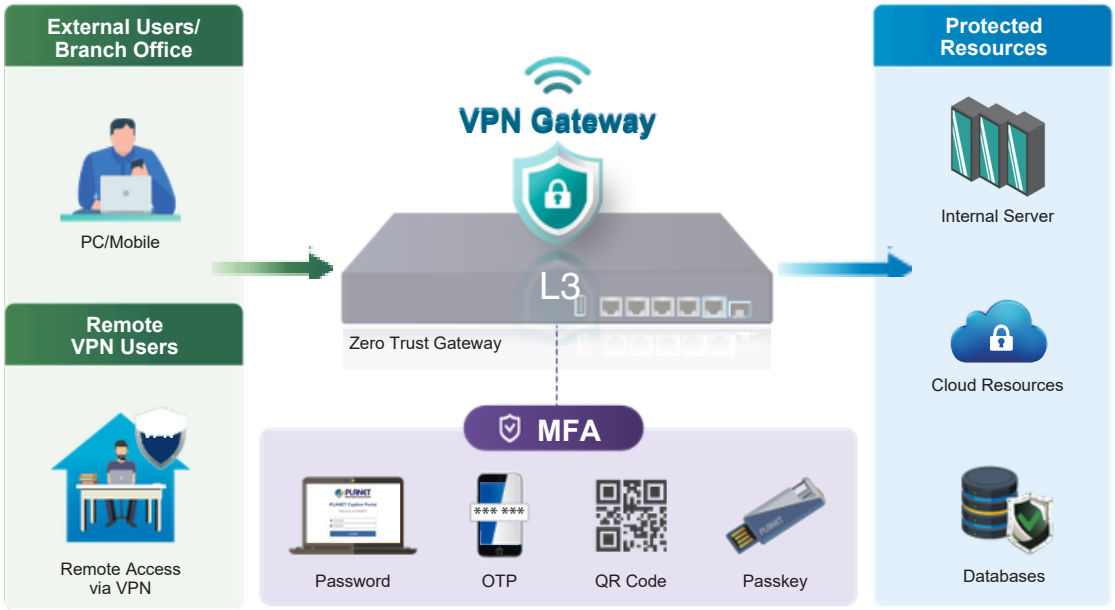
it ensures continuous Internet access by intelligently distributing traffic and switching to a backup link when needed. Combined with high-speed Gigabit and 10G interfaces, QoS, and VPN capabilities, it supports critical applications such as VoIP, video conferencing, and cloud services, delivering reliable and optimized network performance for daily operations.



Zero Trust Access Control for Identity-Based Network Security

The ZT-800 adopts a Zero Trust architecture to secure modern enterprise and hybrid work environments. By verifying every user, device, and connection through identity authentication, MFA, and policy enforcement, it prevents unauthorized access regardless of network location. With built-in RADIUS, Captive Portal, and VPN access control, administrators can enforce role-based policies across wired, wireless, and remote connections, effectively protecting sensitive resources and minimizing lateral movement within the network.

Zero Trust + VPN Secure Access



Specifications

Model	ZT-800
Hardware Specifications	
Ethernet	4 10/100/1000BASE-T RJ45 Ethernet ports (Port 1 to 4) 1 1G/2.5G/5G/10GBASE-T RJ45 port (Port 5) *Supports WAN port mode or LAN port mode over software configuration*
Fiber	One 1G/2.5G/10GBASE-X SFP+ port (Port 6) *Supports WAN port mode or LAN port mode over software configuration*
USB Port	1 USB 2.0 port for system configuration backup and restoration
Reset Button	Reset to factory default
Thermal Fan	1
LED Indicators	System: PWR, Internet, (Green) Ethernet Interfaces (Port 1-4): 10/100/1000 LNK/ACT (Green) Ethernet Interfaces (Port 5): 1G/2.5G/5G/10G LNK/ACT (Green) Fiber Interfaces (Port 6): 1G/2.5G/10G LNK/ACT (Green)
Installation	Desktop installation or rack mounting
Power Requirements	100~240V AC, 50/60Hz, auto-sensing
Power Consumption / Dissipation	Max. 3.3 watts/10.92BTU (Power on without any connection) Max. 11 watts/37.53BTU (Full loading)
Weight	1725g
Dimensions (W x D x H)	330.2 x 200 x 43.1mm, 1U height
Enclosure	Metal

Security Service	
Firewall Security	Cybersecurity Secure Boot Stateful Packet Inspection (SPI) Blocks DoS/DDoS attack Zero Trust access control with identity verification Role-based access policy enforcement Multi-factor authentication via external hardware security key support
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP
NAT	Port forwarding DMZ Host UPnP NAT disable (supports routing mode)
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)
Networking	
Operation Mode	Routing mode
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF
VLAN	802.1q Tag-based, Port-based, Multi-VLAN
Multicast	IGMP Proxy
NAT Throughput	Up to 9Gbps
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, PPPoE, SNMPv1/v2c/v3
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control
VPN	
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net) GRE PPTP Server L2TP Server SSL Server/Client (Open VPN) WireGuard Server/Client
VPN Tunnel Capacity by Protocol	IPSec: 16 GRE: 5 PPTP: 100 SSL VPN: 100
VPN Throughput	Max. 1.3Gbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encryption PQC TLS (Post-Quantum Cryptography TLS) ready
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm
Management	
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported PLANET NMS System/CloudNMS
Secure Management Interfaces	SSHv2, TLSv1.3, SNMP v3
System Log	System Event Log
Others	Setup wizard Dashboard System status/service Statistics Connection status Auto reboot Diagnostics

Standards Conformance	
Regulatory Compliance	CE, FCC
Environment Specifications	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)