

Dual 10G Cybersecurity Gateway with 4-Port 10/100/1000T

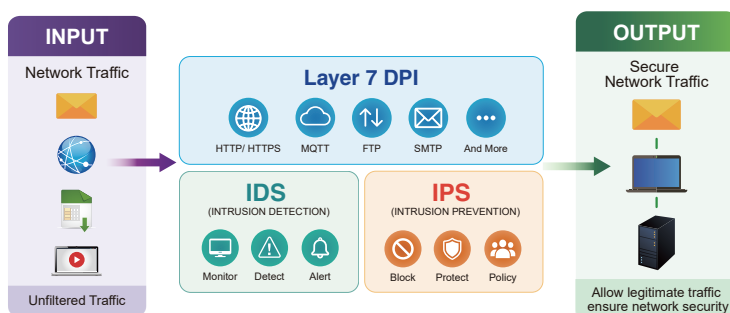


Enterprise Cybersecurity Gateway for Intelligent Threat Protection

The PLANET **CSG-800** is an enterprise-grade cybersecurity gateway designed to protect modern business, industrial, and critical infrastructure networks through comprehensive threat protection, identity-based access control, and high-performance VPN connectivity. By integrating built-in **IDS/IPS**, **Layer 7 Deep Packet Inspection (DPI)**, **security monitoring**, **Zero Trust authentication**, and **Hybrid VPN** into a unified security platform, the CSG-800 enables organizations to proactively defend against cyber threats while ensuring secure and reliable network communications. Powered by a high-performance quad-core processor with dual 10G WAN interfaces, Secure Boot, Hardware TRNG, and **PQC-ready TLS** architecture, it delivers enterprise-class performance, trusted platform security, and flexible deployment for distributed enterprise environments.

Advanced Threat Protection with Built-in IDS/IPS and Layer 7 Deep Packet Inspection

The **CSG-800** integrates built-in **Intrusion Detection and Prevention (IDS/IPS)** with **Layer 7 Deep Packet Inspection (DPI)** to continuously inspect network traffic and identify malicious activities before they impact business operations. By analyzing application-layer traffic in real time, the gateway detects known threats, blocks suspicious connections, enhances application visibility, and helps organizations minimize cyber risks while maintaining stable, reliable, and high-performance network operations.



Highlights

- Enterprise threat protection with built-in IDS/IPS, Layer 7 DPI, SPI firewall and content filtering
- Continuous security monitoring with security logs, event reports and Scheduled Signature Updates
- Zero Trust access control with FIDO2 Passkey, TOTP MFA and certificate-based authentication
- Hybrid VPN (IPSec, OpenVPN, WireGuard, GRE, PPTP and L2TP)
- Dual 10G WAN interfaces with Dual-WAN load balancing and automatic failover
- High Availability (HA)
- AP Controller, Captive Portal and RADIUS
- IPv6, SNMP, PLANET DDNS and CloudNMS support
- Supports up to 100 concurrent SSL VPN connections

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
- Desktop installation or rack mounting

IP Routing Feature

- Static Route
- Dynamic Route
- OSPF

Firewall Security

- Secure Boot to ensure trusted firmware integrity
- Hardware TRNG (True Random Number Generator) for high-entropy cryptographic key generation
- Stateful Packet Inspection (SPI) firewall
- Intrusion Detection and Prevention (IDS/IPS)
- Layer 7 Deep Packet Inspection (DPI)
- Blocks DoS/DDoS attack
- Content Filtering

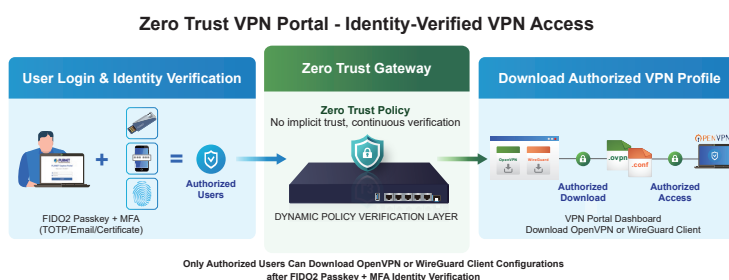
Continuous Security Monitoring with Security Log and Scheduled Signature Updates

The **CSG-800** provides comprehensive **security logs**, **event reports**, and **Scheduled Signature Updates** to simplify cybersecurity management and improve threat visibility. Administrators can efficiently monitor network activities, analyze security incidents, and quickly identify potential threats, while continuously updated threat signatures ensure protection against newly emerging cyber attacks without manual intervention, maintaining an up-to-date security posture with reduced management effort.



Zero Trust–Protected VPN Access with Identity-Based Authentication

The **CSG-800** adopts a Zero Trust architecture by verifying every administrator, user, and device before granting access to enterprise resources. Supporting **FIDO2 Passkey authentication**, **TOTP-based MFA**, **certificate-based authentication**, and optional **RADIUS integration**, it strengthens identity verification and enables secure VPN access while reducing the risks of credential compromise, unauthorized access, and lateral movement across distributed enterprise environments.



Secure Boot for Trusted System Integrity

The **CSG-800** incorporates **Secure Boot** technology to ensure that only authenticated and trusted firmware is executed during system startup. Combined with a built-in **Hardware True Random Number Generator (TRNG)** for secure cryptographic key generation and **Post-Quantum Cryptography (PQC)-ready TLS** architecture, it establishes a trusted hardware foundation that protects against firmware tampering and strengthens long-term cybersecurity resilience.

- Application-level traffic visibility
- Zero Trust access control
- Identity-based access policy
- MAC Filtering and IP Filtering
- NAT ALGs (Application Layer Gateway)
- Blocks SYN/ICMP Flooding
- Security log and event reporting
- Automatic threat signature updates
- Security design follows EU Cyber Resilience Act (CRA) principles

VPN Features

- Zero Trust-protected VPN access
- Identity-based VPN authentication
- 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) readiness for future-proof encryption

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 system and security monitoring
- Security log viewer
- Event reports

Automatic Failover between Dual WAN

Featuring **10GBASE-T RJ45** and **10GBASE-X SFP+** WAN interfaces, the CSG-800 supports intelligent **Dual-WAN failover** to maintain uninterrupted Internet connectivity. When the primary WAN connection becomes unavailable, the secondary WAN interface automatically takes over, ensuring continuous network operation and minimizing downtime for business-critical applications.

Flexible WAN Interface Enables Extension of Network Deployment

The CSG-800 provides flexible WAN deployment through its **10G RJ45** and **10G SFP+** interfaces, allowing administrators to choose copper or fiber connectivity according to deployment requirements. Supporting long-distance fiber transmission and high-speed Ethernet connectivity, it enables secure, scalable, and flexible network expansion for headquarters, branch offices, data centers, and industrial facilities.

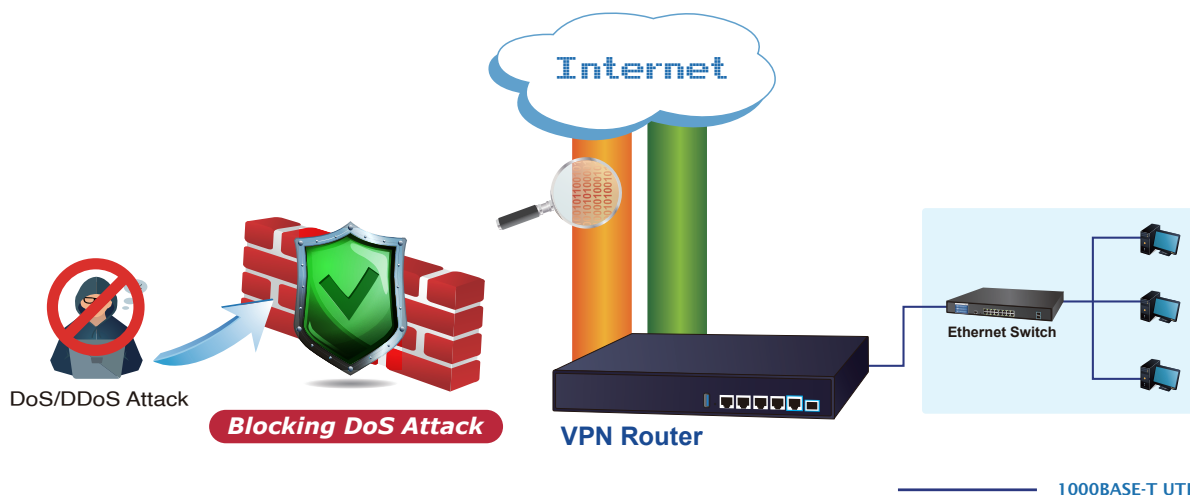
Cybersecurity Network Solution to Minimize Security Risks

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 CSG-800 is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the CSG-800 offers an easy-to-use, platform independent management and configuration facility. The CSG-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 CSG-800 ensures long-term protection against evolving cyber threats, including quantum-era attacks.

Excellent Ability in Threat Defense

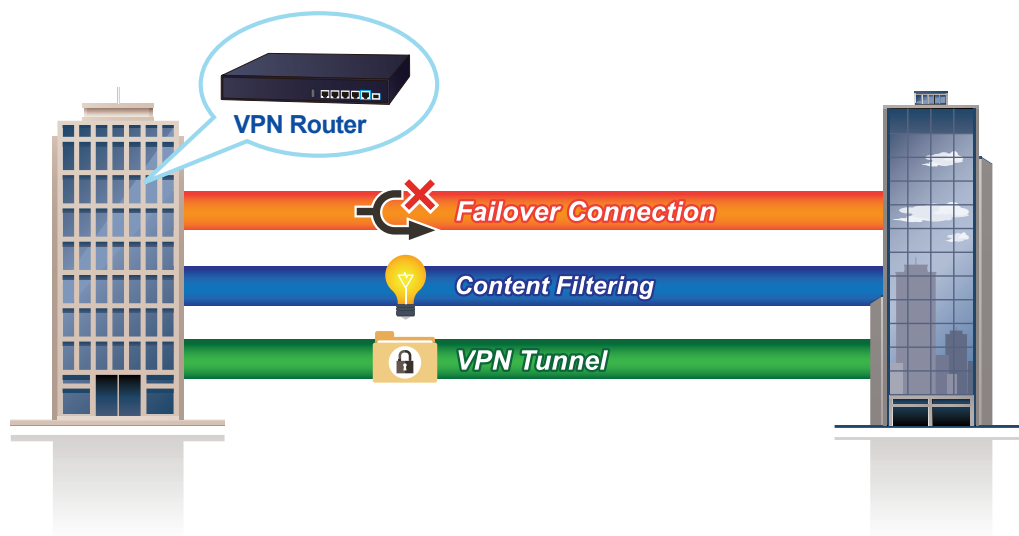
The CSG-800 integrates Stateful Packet Inspection (SPI), Intrusion Detection and Prevention (IDS/IPS), Layer 7 Deep Packet Inspection (DPI), and DoS/DDoS mitigation technologies to provide comprehensive threat protection. Thus, virtual server and DMZ functions can let you set up servers in the Intranet and still provide services to the Internet users.

- Scheduled Signature Updates
- 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



High-Availability VPN Security Router Designed for SMB Applications

The CSG-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 CSG-800 provides secure, flexible, and resilient connectivity for branch sites, remote workers, and sensitive business operations.



Flexible Routing with NAT Disable Capability

The CSG-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 CSG-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

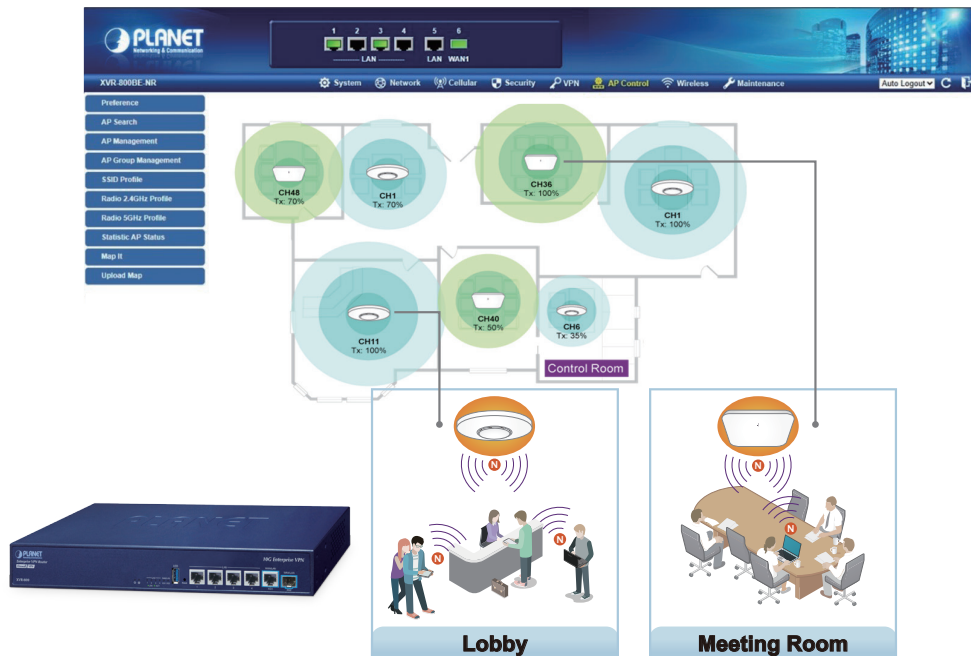
The CSG-800 integrates an AP Controller, Captive Portal, RADIUS authentication, and DHCP server to streamline Wi-Fi deployment for small and medium-sized businesses. These built-in services eliminate the need for external servers, enabling administrators to centrally manage APs, enforce access policies,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

Captive Portal



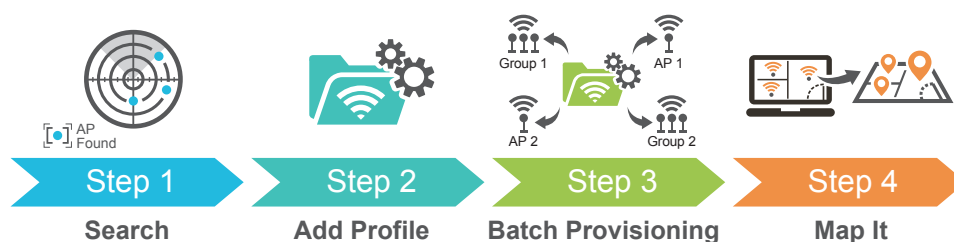
Centralized Remote Control of Managed APs

Through its intuitive web-based interface, the CSG-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.



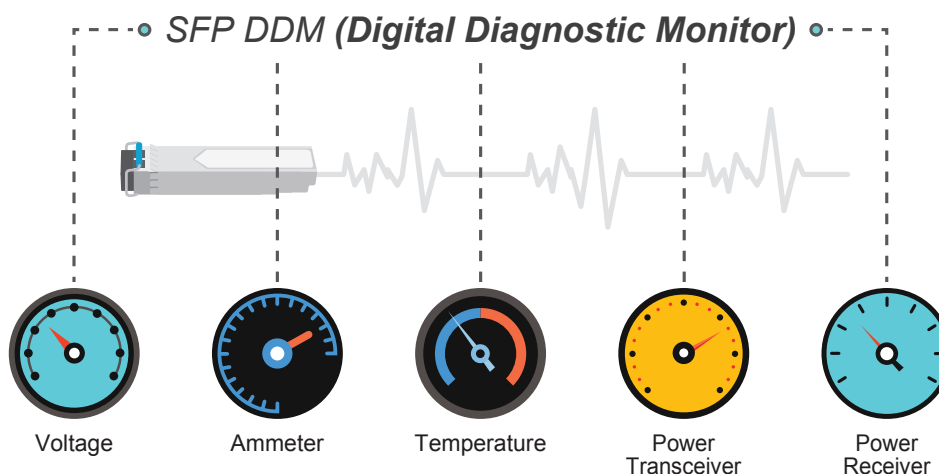
Administrators can cluster APs of the same model for unified management, flexibly expand or remove APs, and perform bulk provisioning or firmware upgrades—all from a single control point. This ensures scalable, efficient, and low-maintenance Wi-Fi management.

Simplified Cluster Management with 4 Steps



Intelligent SFP Diagnosis Mechanism

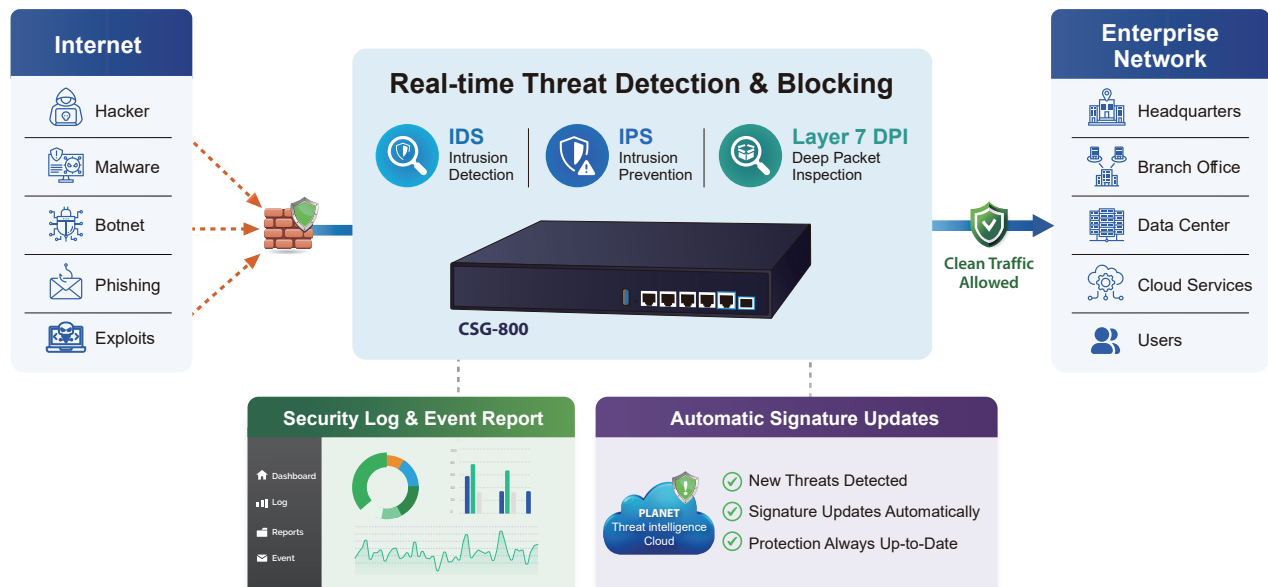
The CSG-800 supports SFP-DDM (digital diagnostic monitor) function that greatly helps network administrator to easily monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.



Applications

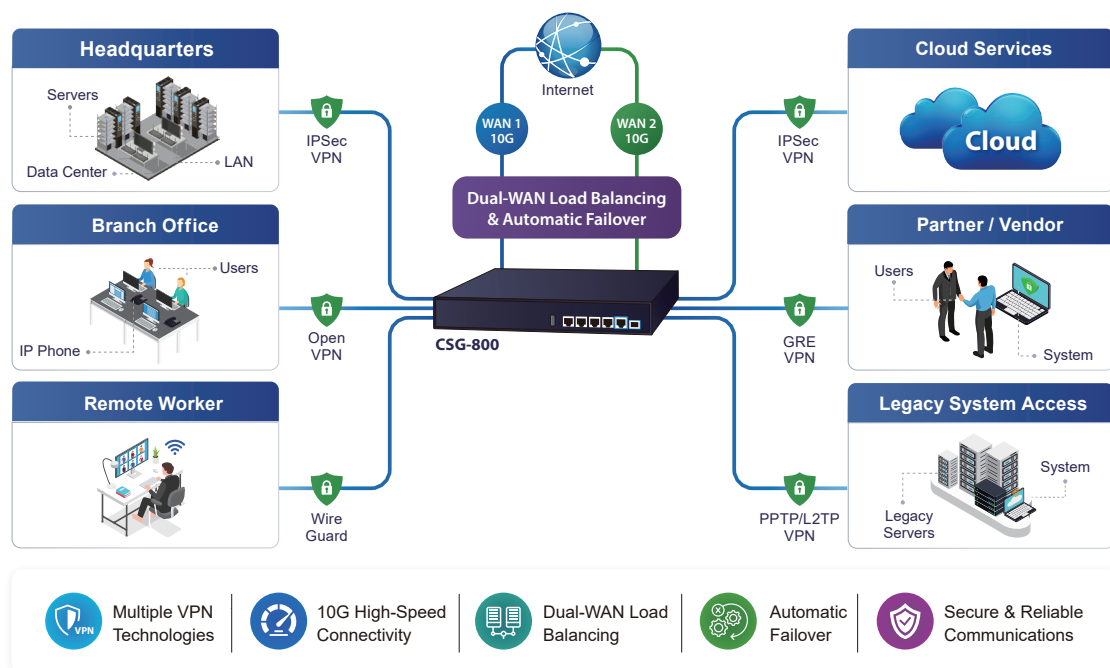
Intelligent Threat Detection for Enterprise Network Security

The **CSG-800** provides comprehensive cybersecurity protection for enterprise headquarters, branch offices, and industrial networks by continuously inspecting inbound and outbound traffic with built-in **IDS/IPS** and **Layer 7 Deep Packet Inspection (DPI)**. It automatically detects malicious activities, blocks cyber threats, and provides application-level visibility, while **security logs**, **event reports**, and **Scheduled Signature Updates** enable administrators to monitor security events and respond quickly to newly emerging threats. This proactive security architecture helps organizations maintain continuous protection without interrupting normal network operations.



Secure Hybrid VPN Connectivity for Distributed Enterprise Networks

The **CSG-800** enables secure communications between headquarters, branch offices, remote workers, and cloud services through comprehensive **Hybrid VPN** technologies, including IPSec, OpenVPN, WireGuard, GRE, PPTP, and L2TP. Combined with **Dual-WAN load balancing**, **automatic failover**, and high-speed **10G WAN** connectivity, it ensures uninterrupted access to business applications while maintaining secure and reliable communications across distributed enterprise environments.

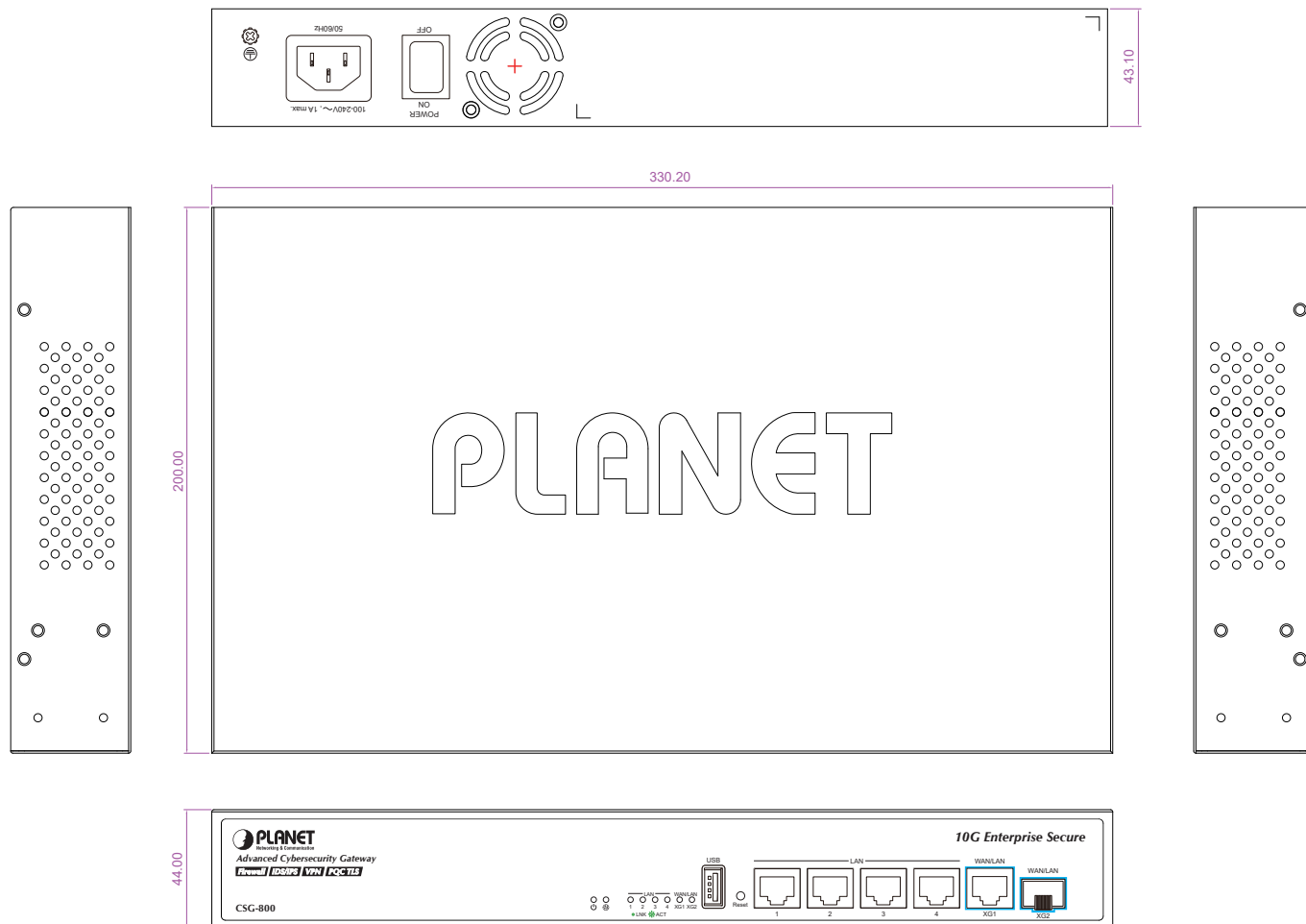


Specifications

Model	CSG-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) <i>Supports WAN port mode or LAN port mode over software configuration</i>
Fiber	One 1G/2.5G/10GBASE-X SFP+ port (Port 6) <i>Supports WAN port mode or LAN port mode over software configuration</i>
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 (WxDxH)	330.2 x 200 x 43.1mm, 1U height
Enclosure	Metal
Security Service	
Firewall Security	Hardware TRNG for secure cryptographic key generation Stateful Packet Inspection (SPI) Security log and event reporting Automatic threat signature updates Blocks DoS/DDoS attack Role-based access policy enforcement
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)
Zero Trust	Zero Trust access control with identity verification Multi-factor authentication via external hardware security key support
Intrusion Prevention System	Intrusion Detection and Prevention (IDS/IPS) Layer 7 Deep Packet Inspection (DPI) Application-level traffic visibility
Secure Boot	Establishes a Chain of Trust (CoT) across all boot stages via cryptographic image signature verification
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	Max. 9.4Gbps
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 (Net-to-Net, Host-to-Net) IPSec Remote Server GRE PPTP Server L2TP Server SSL Server SSL Client (Open VPN, Surfshark, NordVPN, PureVPN) WireGuard VPN Server/Client
VPN Tunnel Capacity by Protocol	IPSec: 16 GRE: 5 PPTP: 100 SSL VPN: 100
VPN Throughput	L2TP (1Gbps): 145~463Mbps L2TP (10Gbps): 483~885Mbps L2TP/IPsec (1Gbps): 150~334Mbps L2TP/IPsec (10Gbps): 438~496Mbps IPsec/AES128 (1Gbps): 894~910Mbps IPsec/AES128 (10Gbps): 1,110~1,310Mbps IPsec/AES256 (1Gbps): 752~842Mbps IPsec/AES256 (10Gbps): 864~1,060Mbps WireGuard (1Gbps): 815~883Mbps WireGuard (10Gbps): 1,430~1,890Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encryption PQC TLS (Post-Quantum Cryptography TLS) ready Supports Hybrid Post-Quantum TLS key exchange using ML-KEM (Kyber)
Authentication Methods	SHA-256/SHA-384/SHA-512 authentication algorithm TLS_KYBER_RSA_WITH_AES_256_GCM_SHA384 FIDO2 Passkey authentication Certificate-based authentication TOTP MFA RADIUS authentication
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 Security Log Event Report Scheduled Signature Update
Others	Setup wizard Dashboard System status/service Statistics Security Monitoring Dashboard 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)

Dimensions



Dimensions (W x D x H): 330.2 x 200 x 43.1 mm

Ordering Information

CSG-800	Dual 10G Cybersecurity Gateway with 4-Port 10/100/1000T
---------	---

Related Products

CSG-800BE	Dual 10G Cybersecurity Gateway with Wi-Fi 7 5100BE
XVR-800	Enterprise Dual 10G VPN Security Router with 4-Port 10/100/1000T
XVR-800P	Enterprise Dual 10G VPN Security Router with 4-Port 10/100/1000T 802.3at PoE+
XVR-800BE	Enterprise Wi-Fi 7 5100BE + Dual 10G VPN Security Router with 4-Port 10/100/1000T
XVR-800BE-NR	Enterprise 5G NR Cellular + Wi-Fi 7 5100BE + Dual 10G VPN Security Router with 4-Port 10/100/1000T
ZT-800	Dual 10G Zero Trust Security Gateway with 4-Port 10/100/1000T
ZT-800BE	Dual 10G Zero Trust Security Gateway with Wi-Fi 7 5100BE
CoreTrust Key	PUF-Powered FIDO2 Security Key for Zero Trust Access

PLANET Technology Corporation

11F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231,
Taiwan (R.O.C.)

Tel: 886-2-2219-9518

Email: sales@planet.com.tw

Fax: 886-2-2219-9528

www.planet.com.tw



PLANET reserves the right to change specifications without prior notice. All brand names and trademarks are property of their respective owners. Copyright © 2026 PLANET Technology Corp. All rights reserved.

CSG-800