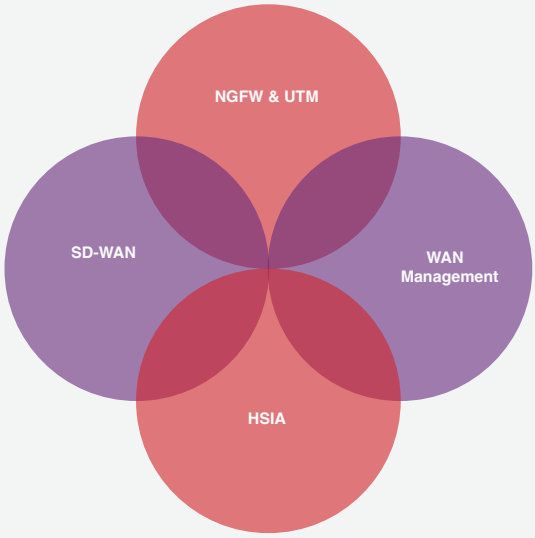
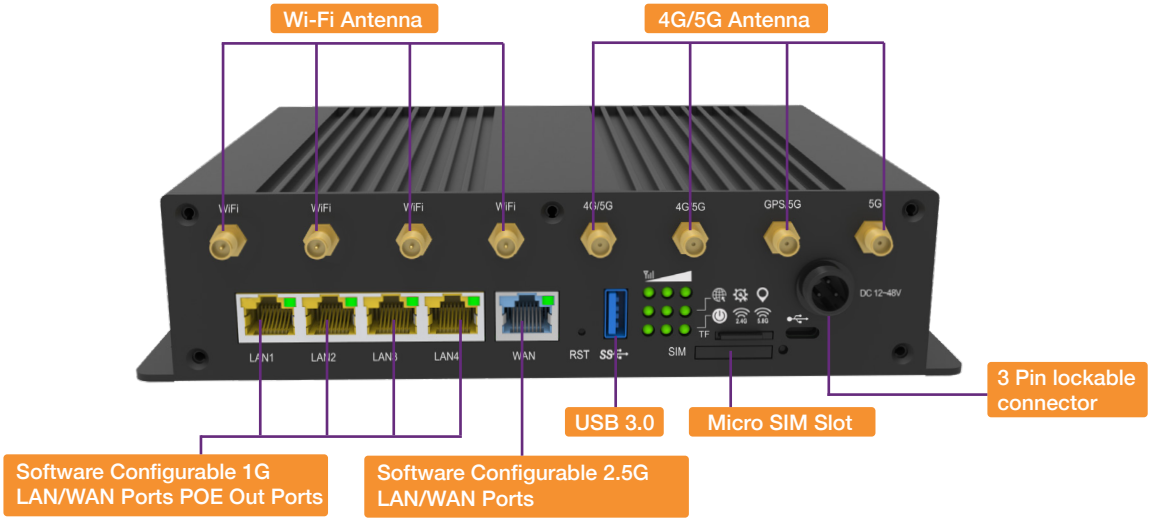
OVERVIEW

Ray Edge is a unique product that spans multiple product lines and solves the key Gateway issues of an Enterprise. The four key pillars of the Ray Edge Gateway are:

- SD-WAN
- Multi-WAN Management
- HSIA
- Firewall





Ray Edge Gateway as a Firewall

Use Case

The Ray Edge Gateway as a Firewall

Features

Web Protection & Control
Ray Edge Gateway with built in URL Filtering Engine provides full visibility and control over the web traffic. Protection against Phishing, SPAM and malicious websites in a real-time basis. Advance Web Filtering based on the website category with local caching creates an Enterprise Secure Web Gateway (SWG) and ensures a quick and easy Enterprise compliance.

DNS Filtering
Ray Edge Gateway powered by the Ray Platform hosts a Secure DNS server. DNS Queries can be segregated to provide 3 levels of responses. Level 1 enables Phishing, SPAM and malicious control with Level 2 adding Porn control and Level 3 adding Safe search and VPN control.

Application Filtering
Ray Edge Gateway powered by Layer 7 Deep Packet Inspection (L7 DPI) enables complete application visibility and control over thousands of applications. The application control can be enforced on a user or group and on both wired and wireless users. Traffic Shaping (QoS) enables/disables applications based on schedule, prioritizes bandwidth allocation to critical applications and limits bandwidth for non-business applications.

Core Networking
Ray Edge Gateway offers the most advanced enterprise-grade networking technology available for NAT (Gateway), routing, and bridging. Create powerful object-based NAT rules, 802.1Q VLAN support, flexible bridging options, PPPoE and Static IP Support and dual stack with IPv4 and IPv6 Support.

Firewall & Segmentation
Ray Edge Gateway provides powerful segmentation. VLANs provide ways to separate levels of trust on your network. Intranet Firewall enables added protection against lateral movement between different parts of your network.

Ray Edge Gateway as an SD-WAN

Use Case

The Ray Edge Gateway as an SD-WAN

enables the below Use Cases:

1. Connecting multiple sites/branches & datacenters to one virtual private network
2. Enabling secure access of private applications hosted on private/ public cloud
3. MPLS/Lease line replacement for multi-branch connectivity
4. Remote working & business continuity for modern enterprise
5. Zero Trust Network Access for in-office and WFH employees

Features

Achieve Network Intelligence
Automate operations using machine learning and artificial intelligence of IT operations (AIOps). Enable dynamic steering of all traffic for optimized application and data delivery. Ray Secure SD-WAN provides visibility into traffic traversing the network between users, applications, and devices regardless of their location. Deep application visibility, with Layer 7 intelligence helps simplify network policy creation and traffic engineering. It offers visualized performance insights into the underlying SD-WAN network for actionable insights.

Secure Networking (SASE) Foundations
Ray Edge Gateway includes ZTNA that enables edge-to-cloud security. The Ray SD-WAN controller can be used to create virtual network segments to isolate data, including PCI data, to ensure data integrity and for PCI audit compliance. Micro-segmentation across the entire network to reduce risk zones and lateral movement. Context-based network and security policies, and traffic steering, based on users, devices, locations, and applications

Agile Networks
Ray Secure SD-WAN with zero-touch deployment and orchestration reduces setup to just minutes. Ray Secure SD-WAN supports all topologies including full mesh, partial mesh, hub-and-spoke and other arbitrary topologies. Cloud-delivered and software-based, it allows for quick adaptation to changing needs, including adding access to cloud-based services, standing up new branches or remote offices.

Lower TCO
Increase agility and reduce costs for bandwidth by augmenting existing MPLS and leased line infrastructure with broadband, LTE, and other connection types. Off-load non-critical business apps to broadband as an alternative to MPLS. AIOps reduces problem identification and associated remediation costs; central management and control of network activity through Ray Platform eliminates the need to send out, trained technicians to assess issues and repair them.

Advanced QoS features
Ray Edge ensures there is a fair sharing of bandwidth among users. The Link Monitoring feature ensures optimum bandwidth utilization and informs the IT Admin of High Link Utilization. It enables differentiated class of services for different group of users and applications, ensuring the best internet experience.

Ray Edge Gateway as an HSIA

Use Case

The Ray Edge Gateway as a HSIA enables the below Use Cases:

1. Welcome the guests in your enterprise securely
2. Give a personal touch with a branded Captive Portal
3. Provide seamless internet to your guests connected with a PMS system
4. Stay compliant with Cyber laws whilst providing guest internet
5. Monetize Wi-Fi by showing advertisements
6. Capture user data or feedback by means of a survey
7. Visitor Management System for the enterprise

Features

Captive Portal
Ray Edge has one of the most advanced Captive Portal systems with 8 built-in Captive Portals. The multi-language capable Captive Portal itself can be configured with a step-by-step wizard to match the design aesthetics of the customer. The resulting captive portal is mobile friendly and responsive. The Captive Portals supported are Click to Login, SMS & Email OTP, Voucher, Username & Password, Social Media, Survey and Advertisement.

Cluster/Site Management
Ray Edge with its Hierarchical Multi-Site Management feature allows the owners to create and manage multiple properties centrally in the Ray Platform. Integrated with the Google Maps, the Site Management gives a bird's eye view on the status of all sites while the User & Role management controls granular access to the site. The hierarchical nature of the site management provides an ease of publishing configurations to hundreds of locations with a click of a button.

Advance Plan Management
Ray Edge with built-in radius offers robust (Authentication, Authorization and Accounting) AAA functionalities which allows the IT admins to configure advanced plans. The Edge offers granular control on the speed, quota, price, concurrency, content, usage time, validity, etc. It allows IT admins to create flat or flexible plans to be offered to the customers.

Wi-Fi Monetization via Advertisement
Ray Edge with the built-in Advertisement enables the property owners to create a revenue stream from Wi-Fi. The Advertisement Server supports both picture and Video advertisements and displays detailed statics on the clicks or views.

Wi-Fi Monetization via Survey
Ray Edge with the built-in Survey engine enables the property owners to use survey as an authentication mechanism to the internet. The customizable surveys can include questions, single select, multi-select, star ratings etc. which can be verified with pre-defined templates. The surveys can be used as a feedback mechanism, Visitor Management for guests or simply to gather customer information.

Compliance & Log Management
Ray Edge with built-in URL filtering ensures non-compliant sites can be blocked through categories or manual entry. Ray Edge stores IP Log for all browsing sessions via the Guest Captive Portal. The logs are stored for a period of 1 year. The IT admin can search, retrieve, and export the IP Logs for Guest Captive Portal browsing sessions.

Ray Edge Gateway as a Multi-WAN

Use Case

The Ray Edge Gateway a Multi-WAN enables the below Use Cases:

1. Business criticality requiring multiple internet connections
2. MPLS replacement with single or multiple alternatives
3. Remote sites depending on cellular connectivity

Features

Multi-WAN & Link Failover/Balancing
Ray Edge Gateway intelligently manages multiple internet transports (MPLS, Broadband, 3G, 4G, LTE, 5G) from any of your service providers. Edge is a proactive router that can monitor, detect, and adapt to the fluctuations in your ISP performance as well as your changing traffic profile. This means Edge will solve the network problems automatically and will avoid interruptions to your internet services and applications.

Aggregated Downlink Capacity in Standalone Mode
When not peered with another Edge device, all HTTP downlink sessions can be configured to use the aggregated bandwidth of the combined internet access links, even in the case of a single HTTP session. For non-HTTP downlink sessions and all uplink sessions, Edge provides session-based intelligent load balancing across the access links if not peered with another Edge device or service.

Cellular Gateway
Ray Edge Gateway with its LTE and 5G modems offers connectivity via cellular network. This network can be used as a primary internet or as a failover/secondary internet in case of connectivity failures. The industrial built of the Edge ensures that it can be used in rugged environments.

Dimensions & Interfaces

Model	Physical Dimensions (mm)	Weight (kg)	10/100/1000 Base-T	10/100/1000/2500 Base-T
Edge Micro	L=285, B=540, H=235	2.03	4	1

Performance	
FIREWALL	3,700 Mbps
TLS INSPECTION	› 375 Mbps
IPS	› 1,015 Mbps
IPSEC VPN	› 2,800 Mbps
NGFW	› 700 Mbps
THREAT	› 240 Mbps
LATENCY (64 BYTE UDP)	› 6 µs
Power Specifications	
DC	› 12V~48V DC
PoE IN	› WAN: 48V Passive PoE in › LAN: 48V active PoE out
PoE Out	4 * 10/100 / 1000Mbps RJ45 LAN Ports (Support 48V active PoE out if powered by DC)
Max Power Consumption	≤ 60W
Other Interfaces	
USB	› 1 * USB3.0 Port
SD-Card	› 1 * SD Card Slot
Cellular	
SIM Slot	› Built-In Micro SIM Slot
Frequency Bands	› LTE FDD: B1/B3/B8 › LTE TDD:B38/B39/B40/B41 › TDSCDMA: B34/B39 › WCDMA: B1 › CDMA 1x/EVDO: BC0 › GSM: 900/1800MHz
LTE Version	› 3GPP E-UTRA Release 9
Bandwidth	› 1.4/3/5/10/15/20MHz
Throughput	› LTE: › LTE FDD: Max 100Mbps (DL)/Max 50Mbps (UL) › LTE TDD: Max 61Mbps (DL)/Max 18Mbps (UL) › DC-HSPA+: Max 42Mbps (DL)/Max 5.76Mbps (UL) › UMTS: Max 384Kbps (DL)/Max 384Kbps (UL) › TD-SCDMA: Max 4.2Mbps (DL)/Max 2.2Mbps (UL) › EVDO: Max 14.7Mbps (DL)/Max 5.4Mbps (UL) › EDGE: Max 236.8Kbps (DL)/Max 236.8Kbps (UL) › GPRS: Max 85.6Kbps (DL)/Max 85.6Kbps (UL)
Management	
Single Pane of Glass	"Single Pane of Glass" feature to centrally cloud manage all the switches along with other Networking components like Wi-Fi Access Point and Gateways across multiple locations on a single Cloud UI.
Firmware Update	› Automatic firmware upgrades with scheduling control › Firmware upgrade by HTTP/TFTP protocol through Ethernet network
Log Integration	› SNMP v1, v2c, v3 Integration › SYSLOG Integration (Remote & Local)
Standards	› Simple Network Management Protocol (SNMP) v1, v2c, v3 › RFC 854 Telnet › RFC 1155 Management Information for TCP/IP-Based Internets › RFC 1156 MIB › RFC 1157 SNMP › RFC 1213 SNMP MIB II › RFC 1350 TFTP › RFC 1643 Ethernet MIB › RFC 2030 SNTP › RFC 2616 HTTP › RFC 2665 Ethernet-Like Interface types MIB › RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions › RFC 2819 RMON MIB › RFC 2863 Interfaces Group MIB › RFC 3164 Syslog › RFC 3414 User-Based Security Model (USM) for SNMPv3 › RFC 3418 MIB for SNMP › RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs
Interfaces	› Web-based (HTTPS) › Secure Shell (SSH) Protocol

Wireless Specifications	
Wi-Fi Standards	› 802.11 ax/ac/b/g/n/a
AP Type	› Industrial, dual radio, 5GHz and 2.4GHz 802.11ax 2x2 MIMO
Wi-Fi 6 (802.11ax) Features	› UL/DL-OFDMA › Target Wake Time (TWT) › Spatial Frequency Reuse (BSS Coloring)
Max aggregate frame rate	› Max aggregate frame rate: 1.8 Gbps › 2.4GHz: 574 Mbps › 5GHz: 1201 Mbps
Supported Channels	› Available channels dependent on configured regulatory domain › 2.4GHz: 1-13 › 5GHz: 36-64, 100-144, 149-165
Supported frequency bands	› 2.412-2.484 GHz › 5.150-5.250 GHz (UNII-1) › 5.250-5.350 GHZ (UNII-2) › 5.470-5.600, 5.660-5.725 GHz (UNII-2e) › 5.725-5.850 GHz (UNII-3) › Country-Specific restrictions apply.
MIMO	› 2x2:2 streams SU/MU MIMO 5GHz › 2x2:2 streams SU/MU MIMO 2.4GHz
Channelization	› 802.11n high-throughput (HT) support: HT20/40 › 802.11ac very high throughput (VHT) support: VHT20/40/80 › 802.11ax high efficiency (HE) support: HE20/40/80
Supported modulation types	› 802.11b: BPSK, QPSK, CCK › 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension) › 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (proprietary extension)
Beamforming	› Transmit Beamforming and Maximal Ratio Combining
Mesh	› SON based Mesh
Beaconing	› Transmit Only › Transmit/Receive (Attached Devices) › Transmit/Receive (Unattached Devices)
WI-FI OFFLOAD	› Passpoint Wi-Fi (Release 2) (Hotspot 2.0) for Seamless cellular-to-Wi-Fi › Access Network Discovery and Selection Function (ANDSF) Integration
Other Wi-Fi Standards	› 802.11d › WMM/802.11e › 802.11h › 802.11n › 802.11k › 802.11r › 802.11u › 802.11w
Wireless Intrusion Detection (WIDS/ WIPS)	› Rogue AP detection / prevention › Evil-twin/AP spoofing detection › Ad hoc detection
Wi-Fi Channel Management	› Intelligent Radio Resource Management (iRRM)
Client Density Management	› Adaptive Band Balancing › Client Load Balancing › Airtime Fairness › Airtime-based WLAN Prioritization
Wireless Performance	
Maximum number of associated client devices	› Up to 256 associated client devices per radio › Up to 512 clients per AP
Wi-Fi Channel Management	› 16 BSSIDs per radio › Up to 31 per AP

Networking	
IP	IPv4, IPv6, dual stack
VLAN	› 802.1Q (1 per BSSID or dynamic per user based on RADIUS) › VLAN Pooling › Port-based
802.1x	› Authenticator & Supplicant
Tunnel	› L2TP › GRE/EoGRE › Openvpn › L2TP/IPSEC › PPTP
Policy Management Tools	› Application Recognition and Control › Access Control Lists › Device Fingerprinting › Rate Limiting › Integrated Layer 7 firewall with mobile device policy management › Flexible guest access with device isolation
Quality of Service	› WMM Access Categories with DSCP and 802.1p support › QoS-based scheduling › Directed Multicast › L2/L3/L4 ACLs
Mobility	› 802.11r for fast Layer 2 roaming › Centralized Layer 3 roaming
Modes	› Gateway Mode › Bridge & Firewall › Bridge No Firewall
Radius	› Authentication via Radius › Radius Option 82 Support
SD-WAN	

Topology	› SD-WAN
	  › Hub & Spoke Topology
	  › Mesh Topology
	› Application based Routing
	› Application Priority
	› Multi-WAN Support
	  › Link Failover
	  › Link Balancing
	  › Link Bonding/Aggregation

Security	
Security	› WEP, WPA, WPA2-PSK, WPA2-Enterprise with 802.1X, WPA3 - Personal, WPA3 - Enterprise, WPA3 - Enhanced Open (OWE) › Personal PSK › EAP-TLS, EAP-TTLS, EAP-MSCHAPv2, EAP-SIM
Encryption	› Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys) › Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) › Data Encryption Standard (DES): DES-CBC, 3DES › Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit › DTLS: AES-CBC › IPsec: DES-CBC, 3DES, AES-CBC › 802.1AE MACsec encryption

Authentication	
Authentication, Authorization, and Accounting (AAA)	› IEEE 802.1X › RFC 2548 Microsoft Vendor-Specific RADIUS Attributes › RFC 2716 PPP EAP-TLS › RFC 2865 RADIUS Authentication › RFC 2866 RADIUS Accounting › RFC 2867 RADIUS Tunnel Accounting › RFC 2869 RADIUS Extensions › RFC 3576 Dynamic Authorization Extensions to RADIUS › RFC 5176 Dynamic Authorization Extensions to RADIUS › RFC 3579 RADIUS Support for EAP › RFC 3580 IEEE 802.1X RADIUS Guidelines › RFC 3748 Extensible Authentication Protocol (EAP) › Web-based authentication › TACACS support for management users
Security	
Authentication	› RADIUS Authentication, Authorization, Accounting › TACACS+ Authentication › IEEE 802.1X port-based authentication › IEEE802.1x AAA
DHCP	› IPv4/IPv6 DHCP Client › IPv4/IPv6 DHCP Relay › DHCP Option 82 › DHCP Option 37/38 › IPv4/IPv6 DHCP Server › IPv4/IPv6 DHCP Snooping, Detection and Blocking
Other Security Features	› Sticky MAC, MAC Whitelisting › IP-MAC port binding › MAC filtering › Static MAC Address › Port Isolation › DoS/DDoS attack prevention › ARP inspection › IP source guard › Storm control support › Broadcast/unknown unicast/unknown multicast › Secure Management Interfaces (SSH, SSL, SNMP v3)] › Storm Control based on packets and bytes › Port Security, MAC Limit based on VLAN and Port › Anti-ARP-Spoofing, Anti-ARP-Scan, ARP Binding › ND Snooping › DAI
Green Energy	
Green Energy	› IEEE 802.3az (Energy Efficient Ethernet) › LED Shut-off
Physical Characteristics	
Operating Temperature	› -20 °C ~ 60 °C
Storage Temperature	› -40 °C ~ 70 °C
Operating Humidity	› 5% ~ 90% non-condensing
Storage Humidity	› 5% ~ 95% non-condensing
Vibration	› Vibration Proof
IP Rating	› IP60
Surge Protection	› Common mode ±6KV Differential mode ±4KV;
MTBF	› >50000 hour
Electrostatic standard	› Contact 6KV, air 8KV
Green Energy Saving	› Support IEEE (802.3az)

Standards	
Standards	› IEEE 802.3 10BASE-T › IEEE 802.3u 100BASE-TX/100BASE-FX › IEEE 802.3z Gigabit SX/LX › IEEE 802.3ab Gigabit 1000BASE-T › IEEE 802.3x flow control and back pressure › IEEE 802.3ad port trunk with LACP › IEEE 802.1D Spanning Tree Protocol › IEEE 802.1w Rapid Spanning Tree Protocol › IEEE 802.1s Multiple Spanning Tree Protocol › IEEE 802.1p Class of Service › IEEE 802.1Q VLAN Tagging › IEEE 802.1x Port Authentication Network Control › IEEE 802.1ab LLDP › RFC 768 UDP › RFC 793 TFTP › RFC 791 IP › RFC 792 ICMP › RFC 2068 HTTP › RFC 1112 IGMP version 1 › RFC 2236 IGMP version 2 › RFC 3376 IGMP version 3 › RFC 2710 MLD version 1 › RFC 3810 MLD version 2 › IEEE802.3ah › IEEE 802.1ag › RFC 768 UDP › RFC 791 IP › RFC 2460 IPv6 › RFC 792 ICMP › RFC 793 TCP › RFC 826 ARP › RFC 1122 Requirements for Internet Hosts › RFC 1519 CIDR › RFC 1542 BOOTP › RFC 2131 DHCP › RFC 5415 CAPWAP Protocol Specification › RFC 5416 CAPWAP Binding for 802.11 › RFC 1321 MD5 Message-Digest Algorithm › RFC 1851 ESP Triple DES Transform › RFC 2104 HMAC: Keyed Hashing for Message Authentication › RFC 2246 TLS Protocol Version 1.0 › RFC 2401 Security Architecture for the Internet Protocol › RFC 2403 HMAC-MD5-96 within ESP and AH › RFC 2404 HMAC-SHA-1-96 within ESP and AH › RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV › RFC 2407 Interpretation for ISAKMP › RFC 2408 ISAKMP › RFC 2409 IKE › RFC 2451 ESP CBC-Mode Cipher Algorithms › RFC 3280 Internet X.509 PKI Certificate and CRL Profile › RFC 4347 Datagram Transport Layer Security › RFC 5246 TLS Protocol Version 1.2
Ordering Information	
Model	› Product information
Ray Edge Micro	› Ray Edge Micro with Standard Hardware Support
Ray Edge Micro – P	› Ray Edge Micro with Priority Hardware Support

Specifications

Routing & Network Services	
IPv4 / IPv6 Routing	Dual Stack Routing, Static Routing, OSPFv2/v3, BGP4+
Traffic Engineering	Policy Based Routing (PBR), VRF Multi-Tenant Segmentation
High Availability	VRRP High Availability
LAN Services	IEEE 802.1Q VLAN (4K VLANs), LACP Link Aggregation
Multicast	PIM-SM/DM Routing, IGMP / MLD Snooping

WAN & Multi-WAN	
WAN Interfaces	Ethernet / SFP / 4G / 5G WAN (Model Dependent)
WAN Protocols	Static IP, DHCP, PPPoE
Cellular Services	APN Selection, SIM Failover, USB Modem Backup
Load Balancing	Weighted, Priority and Session Based Load Balancing
Link Reliability	Automatic Failover/Failback, Packet Duplication, FEC

Secure Connectivity	
VPN	IPSec VPN, WireGuard VPN
Tunneling	GRE / EoGRE, L2TP / PPTP, MPLS CE Support
Network Services	NAT, DHCP Server/Relay, DNS Forwarder, NTP Services

Native Secure SD-WAN	
Topology	Hub-Spoke, Full Mesh and Hybrid
Routing Intelligence	Application Aware Routing, Dynamic Path Selection
Monitoring	Latency, Jitter, Loss Monitoring, Brownout Detection
Optimization	Ray Link Bonding, Packet/Session Multipath
Encryption	AES-256, ChaCha20-Poly1305

Next Generation Firewall & Security	
Firewall	Stateful Firewall, Application Identification & Control
Threat Protection	IDS/IPS, Anti Malware, Anti Phishing, Anti Spam
Web Security	URL Filtering, DNS Filtering
Protection	DoS/DDoS Protection, Zero-Day Protection
Segmentation	Trust Zone Based Security Policies

Identity & Management	
Authentication	802.1X, RADIUS, LDAP, Microsoft AD, OAuth
Policy Control	MAC/IP/User Based Policy Mapping
Administration	AAA Server, RBAC Multi-Admin Control
Management	Ray ONE Cloud / On-Prem Controller
Monitoring	SNMP v1/v2/v3, NetFlow/IPFIX, CLI, SSH

Certifications	
Product Compliance	TEC/MTCTE (Applicable Models)
Company Certifications	ISO 9001:2015, ISO 14001:2015, ISO 20000-1:2018, ISO 27001:2022, ISO 27017:2015, ISO 27018:2014

Ray Pte. Ltd.
ray.life | sales@ray.life | Suite #09-01, 20 Collyer Quay, Singapore 049319

© Copyright 2022 Ray Pte. Ltd. All Rights reserved. Ray, Ray.life and the Ray logo are trademarks of Ray Pte. Ltd. in Singapore, India and other countries. This product is protec ed by Singapore and international copyright and intellectual property laws. The information contained herein is subject to change without notice.The only warranties for Ray Pte. Ltd. products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warran ty. Ray Pte. Ltd. shall not be liable for technical or editorial errors or omissions contained herein.