haltdos

TECHNICAL SPECIFICATION

Haltdos Canary:
Application Delivery Controller

Fast . Scalable . Reliable

Haltdos hardware appliances deliver a hardened and scalable, reliable platform to power Haltdos solutions. Haltdos Hardware Appliances offer exceptional performance, allowing organizations to consolidate device management and address future bandwidth requirements. Haltdos appliances can manage heavy traffic loads without impacting application or network performance.

Fault Tolerant Hardware Design

With multi-gigabit throughput, fail open interfaces, secure out-of-band management, and low latency, Haltdos appliances are high assurance, fast and easy to manage. To maximize system uptime, Haltdos appliances offer redundant, hot-swappable components including redundant power supplies and hard drives. In the event of a hardware failure, the redundant component will automatically take over, providing continuous system operations.



Support

- 24 x 7 x 365 Support
- On-Site Warranty Support
- Twice a Year Site Visit Assurance
- Centralised Helpdesk

CONNECT WITH HALTDOS

https://www.haltdos.com/appsec/enterprise-web-application-firewall

1800-120-2394

https://www.haltdos.com/contact

Flexible Expansion Options to Address Unique Business Needs

The appliances are built on a common hardware platform with flexibility in mind. Haltdos appliances can be extended to provide remote, out-of-band management and monitoring, performance acceleration, and more with expansion modules. Expansion modules include:

- Network Cards (copper or optical)
- Hardware Security Module (HSM) (non-FIPS and FIPS-140-2)
- SSL acceleration card
- Disk Space & RAM

Copyright Haltdos. All rights reserved

Product Specifications

MITIGATION PERFORMANCE		HD-CAN-550	HD-CAN-1100	HD-CAN-4100	HD-CAN-4600
1.1	Layer 4 Throughput	500 Mbps	1 Gbps	5 Gbps	24 Gbps
1.2	Layer 7 Throughput	500 Mbps	1 Gbps	4 Gbps	25 Gbps
1.3	SSL/TLS Throughput	500 Mbps	1 Gbps	4 Gbps	20 Gbps
1.4	Compression Throughput	500 Mbps	1 Gbps	4 Gbps	20 Gbps
1.5	Decompression Throughput	500 Mbps	1 Gbps	5 Gbps	20 Gbps
1.6	L4 Connections Rate (cps)	1M	1.5M	3M	5M
1.7	L7 Request Rate (rps)	250 K	500 K	1 M	3 M
1.8	Concurrent Connections	7 M	12 M	24 M	32 M
1.9	SSL/TLS RSA 2K Rate (tps)	10K	22K	22K	40K
1.10	SSL/TLS ECC Rate (tps)	5K	15 K	15 K	25K
1.11	VM Supported	Yes	Yes	Yes	Yes
1.12	Induced Latency	< 1 ms			
HARDWARE DETAILS					
2.1	Processor	Intel Xeon			
2.2	CPU Cores	6	8	8	24
2.3	Memory *	8 GB	16 GB	16 GB	64 GB
2.4	Hard Disk *	128 GB SSD	128 GB SSD	256 GB SSD	512 GB SSD
2.5	Form Factor	1U/2U/4U Rack mount server (19-inch mounting) with panel indicators			
		Option available for RAID or dual partition			
2.6	Operating Temperature & Humidity	0 - 40 C with 8%-95% humidity (non-condensing)			
2.7	Power Supply and Fans	Redundant Power Supply (Hot Swappable)AC 170-240V,50 Hz and Redundant fans.			
2.8	Virtual ADC Supported	N/A	upto 5	upto 8	upto 15
2.9	Additional Specs	Built-in TPM Chip and Hardware HSM for SSL offloading & compression optimization Option available for FIPS-140-2 (additional charge) or non-FIPS compliant HSM			
2.10	Inspection Ports *				
	1 GE Ports	4	8	8	8
	10 GE Ports	-	-	-	4
	25 GE Ports	-	-	-	-
	40 GE Ports	-	-	-	-
	100 GE Ports	-	-	-	-
2.11	Out Of Band Ports				
	1 GE (RJ-45) Ports	1	2	2	2
	Console (RS232/RJ45) Ports	-	1	1	1
	HA Ports (RJ-45/SFP/SFP+)	1	1	1	1
	Input/Output (USB)	2	2	2	2

* Customizable Components

Copyright Haltdos. All rights reserved

Product Specifications

MITIGATION PERFORMANCE		HD-CAN-5100	HD-CAN-5400	HD-CAN-6200	HD-CAN-6700
3.1	Layer 4 Throughput	48 Gbps	72 Gbps	120 Gbps	150 Gbps
3.2	Layer 7 Throughput	40 Gbps	60 Gbps	100 Gbps	120 Gbps
3.3	SSL/TLS Throughput	40 Gbps	50 Gbps	100 Gbps	200 Gbps
3.4	Compression Throughput	24 Gbps	37 Gbps	66 Gbps	132 Gbps
3.5	Decompression Throughput	30 Gbps	54 Gbps	120 Gbps	240 Gbps
3.6	L4 Connections Rate (cps)	7M	10M	12M	15M
3.7	L7 Request Rate (rps)	7 M	10 M	15 M	18 M
3.8	Concurrent Connections	56 M	96 M	160 M	192 M
3.9	SSL/TLS RSA 2K Rate (tps)	80K	140K	180k	240K
3.10	SSL/TLS ECC Rate (tps)	40K	80K	140K	200K
3.11	VM Supported	Yes	Yes	Yes	Yes
3.12	Induced latency	< 1 ms			
HARDWARE DETAILS					
4.1	Processor	Intel Xeon			
4.2	CPU Cores	32	40	64	64
4.3	Memory *	64 GB	128 GB	256 GB	512 GB
4.4	Hard Disk *	1 TB SSD	1 TB SSD	2 TB SSD	2 TB SSD
4.5	Form Factor	1U/2U/4U Rack mount server (19-inch mounting) with panel indicators			
		Option available for RAID or dual partition			
4.6	Operating Temperature & Humidity	0 - 40 C with 8%-95% humidity (non-condensing)			
4.7	Power Supply and Fans	Redundant Power Supply (Hot Swappable)AC 170-240V,50 Hz and Redundant fans.			
4.8	Virtual ADC Supported	upto 25	upto 30	upto 50	upto 50
4.9	Additional Specs	Built-in TPM Chip and Hardware HSM for SSL offloading & compression optimization Option available for FIPS-140-2 (additional charge) or non-FIPS compliant HSM			
4.10	Inspection Ports *				
	1 GE Ports	-	-	-	-
	10 GE Ports	4	8	8	8
	25 GE Ports	-	-	-	2
	40 GE Ports	2	2	4	-
	100 GE Ports	-	-	-	2
4.11	Out Of Band Ports				
	1 GE (RJ-45) Ports	2	2	2	2
	Console (RS232/RJ45) Ports	1	1	1	1
	HA Ports (RJ-45/SFP/SFP+)	1	1	1	1
	Input/Output (USB)	2	2	2	2

***** Customizable Components

Copyright Haltdos. All rights reserved

Centralized Management

Depending upon the chosen deployment as standalone or cluster, Haltdos also offers a centralized management solution for management of Haltdos products. The centralized management is API first solution that comes in the following flavors:

- HD-MGT-ST: This model is a single tenant centralized management solution that supports only one license dedicated to a single customer.
- HD-MGT-MT: This model is a multi-tenant centralized management solution that supports multiple licenses that can be used by one or more customers.

Like the products, Haltdos Centralized Management solution can be deployed in Hardware or virtual form factor.

Virtual Appliances

All Haltdos products are built on top of Haltdos platform and can be deployed as SaaS, hardware, or virtual appliances, with the same features and security capabilities across all deployment models. However, mitigation performance depends on the underlying hardware or infrastructure specifications. No additional software-based limitations are imposed, apart from the licensed Net WAF throughput.

Standalone Virtual Models	Cluster Virtual Model	Throughput (Mbps)
HD-CAN-25/VM	HD-VC-25	25
HD-CAN-50/VM	HD-VC-50	50
HD-CAN-100/VM	HD-VC-100	100
HD-CAN-200/VM	HD-VC-200	200
HD-CAN-500/VM	HD-VC-500	500
HD-CAN-750/VM	HD-VC-750	750
HD-CAN-1000/VM	HD-VC-1000	1000
HD-CAN-2500/VM	HD-VC-2500	2500
HD-CAN-7500/VM	HD-VC-7500	7500
HD-CAN-10000/VM	HD-VC-10000	10000

Cloud WAAP

EDGEO-WAAP is a cloud-delivered WAAP solution for securing web applications and APIs through a scalable, low-latency architecture. It is licensed based on the number of protected FQDNs and requires no customer-managed hardware or virtual appliance.

Product Model	Deployment	Licensing	Product
EDGEO-WAAP	Cloud / SaaS	FQDN Based	Web Application & API Protection (WAAP)

Copyright Haltdos. All rights reserved

PRODUCT OVERVIEW & DEPLOYMENT SPECIFICATIONS

The Haltdos Web Application and API Security, API Discovery Module provides advanced protection for web applications and APIs, including automated API discovery, threat detection, and centralized visibility. The solution is available in virtual machine and cloud deployment models to meet different infrastructure and security requirements.

TECHNOLOGY & CERTIFICATION

SPECIFICATION	HD-CAN-550/VM-API	HD-CLOUD-API
Product	Haltdos API Security, API Discovery Module	Haltdos API Security, API Discovery Module
Deployment Mode	On-premises / Private Cloud / Virtual Machine	Cloud-delivered / SaaS
Feature Differentiation	Dedicated instance with customer-controlled deployment, API Security and API Discovery.	Cloud-managed API Security and API Discovery with centralized visibility and scalable protection.
Licensing Model	Instance / Capacity-based licensing, as per quoted BOM.	Subscription-based licensing, as per protected FQDNs / APIs and applicable data consumption.

Product Features

TECHNOLOGY & CERTIFICATION

5.1	Platform & Technology	Haltdos Platform with Signature from Threat Intelligence & Machine Learning
5.2	License	Unlimited applications. Bandwidth capped by license. Upgrade possible without hardware replacement up to max supported hardware bandwidth
5.3	Additional Licenses	Optional license for GSLB, LLB, DDoS and SSL VPN
5.4	Certifications	FCC, ROHS, CE compliant, EAL 2+, IPv6 Ready Gold certifications
5.5	Support	24x7 via Online, Email , Telephone and Dedicated Account Manager
5.6	Warranty	1 year warranty. Additional charges for extended warranty
5.7	TAC Support	TAC support in India

Copyright Haltdos. All rights reserved

INTEGRATION FEATURES		
6.1	Custom Threat Intel	Integration with 3rd party Threat Intelligence (TI) feeds
6.2	Storage and Export	Local retention of logs, reports and events. Support for export to 3rd party storage
6.3	NIMS Integration	Support for SNMP, NTP / SNTP, DNS, Web Proxy integration
6.4	3rd Party Integration	Notification & Logging via SNMP, SMTP, SMS Gateway, and 3rd party integration via API hooks, CI/CD, Kubernetes
6.5	SIEM Integration	Support for integration with SIEM and Syslog services
6.6	AAA Integration	Support for integration via RADIUS and TACACS+
6.7	Identity Management	Inbuilt with support for integration with AD / SAML / LDAP
6.8	Security Tools Integration	Support for integration with SAST/DAST/IAST tools. Integration with 3rd party Threat Intelligence (TI) feeds
6.9	Export IOCs	Support for exporting attacking IOCs via STIX / TAXII
OPERATION MODE		
7.1	Network Operations	Offline, Inline Reverse Proxy, Inline Forward Proxy, Inline Bridge, Inline Router Mode, Inline L2 Transparent
7.2	Inline Modes	Proxy or Direct Server Return, Immediate or Delayed Binding
7.3	Deployment Modes	1-Arm or n-Arm, Support for Virtual Matrix Architecture & Direct Access Mode
7.4	Binding	Immediate or Delayed binding
7.5	IP Stack	Dual IPv4 & IPv6 stack
7.6	Supported HTTP Protocols	HTTP 0.9,1.0,1.1,2.0,3.0 (QUIC) with translation
7.7	Web Socket Support	Yes
7.8	Virtual Matrix Architecture	Yes
7.9	Direct Access Mode	Yes
7.10	Mitigation Modes	Bypass, Record (Report Only), Learning, Mitigation (Block & Report)
7.11	Tunnelling Protocols	VLAN, MPLS, GRE, L2TP, GTP, IPinIP
7.11	Dynamic Routing	BGP, OSFP, RIPv1/v2
7.12	Networking	VLAN, VXLAN, Link Aggregation & Trunking (LACP), Multiple Routing Tables, ARP Table etc
7.13	Block Actions	Drop Request, Terminate Connection / Session, Rate Limiting, Blacklist (Temporary or Permanent), Send Challenge, Tarpit
7.14	Virtualization	Multi-tenancy with isolated VMs with dedicated CPU, RAM and Disk. Support for multiple OS templates for customized deployments
7.15	Supported Flow Ingestion	Netflow v5, Netflow v9, sFlow, IPFIX

Copyright Haltdos. All rights reserved

HIGH AVAILABILITY		
8.1	Multiple Appliances	N + 1 Active - Active or Active – Passive (VRRP) with floating MAC
8.2	Management Modes	Standalone / Centralized Management (VM or appliance)
8.3	Secure Communication	Secure communication between centralized management and HA appliances for full state synchronization
MANAGEMENT FEATURES		
9.1	Graphical User Interface (GUI)	Secure web interface over HTTPs with support for all modern browsers
9.2	API Integration	Yes (XML or JSON)
9.3	Command Line Interface (CLI)	Command Line Interface over SSH or console port
9.4	System Management	IPMI 2.0 Compliant
9.5	Audit Trail, Logging & Recovery	Centralized logging of system, services, MIS, incidents. Built-in MIS with policy recovery
9.6	Dashboards & Reporting	Real-Time & historical dashboards with custom duration. Support for custom dashboards. Status dashboard for 1-click health check. Periodic daily, weekly or monthly reports in PDF or Excel
9.7	RBAC Administration	Configurable user profiles with role based access control
9.8	Policy Management	On the fly configuration updates on mitigation appliances
9.9	Backup, Restore & Snapshots	Automatic or manual backup and restore. CLI tool for pushing current snapshot to Haltdos Cloud for diagnostics
9.10	Certificate Management	SSL/TLS certificate management with support for Let's Encrypt certificate generation
9.11	Events / Alerts	Detailed event and alert reporting on attack, health, etc.
9.12	Network Forensics	Network forensic with packet capture and traceroute. Built-in utilities for investigating attacks, payloads and managing false positives
9.13	Updates	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos. Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates
9.14	Snapshorts & Cloud Sync	Automatic and/or manual policy snapshot for diagnosis, policy creation & enforcement using AI/ML via Haltdos cloud
9.15	Backup & Restore	Automatic or Manual Backup and restore. CLI tool for pushing current snapshot to Haltdos cloud for diagnostic.
9.16	Haltdos Threat Stream	Periodic threat intel update (signatures, Geo IP, Bad IP,TOR IP, Anon Proxy,etc from Haltdos.
ADC FEATURES		
10.1	Enforce RFC Compliance	Protection against invalid HTTP, MQTT requests
10.2	NAT & Routing	Support for client, server or full NAT, static routing for IPv4 & IPv6
10.3	Advanced Load Balancing	Content based load balancing with upstream rules
10.4	Load Balancing	Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported

Copyright Haltdos. All rights reserved

10.5	SSL/TLS Management	Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc
10.6	Virtual Contexts	Support for multiple virtual contexts along with resource allocation
10.7	Load Balancing Algorithms	Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc.
10.8	Network Optimization	Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts
10.9	HTTP Optimization	Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients
10.10	Failover Management	Automatic failover & recovery. Support for marking servers up / down / backup
10.11	Health Check	Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script
10.12	Client Visibility	Embedding Real IP information in X-* headers, client cert information, etc
10.13	Redirection Rules	REGEX based redirection rules to rewrite URLs
10.14	Variable Rules	Support for embedding and using variables for A/B testing or custom load balancing
10.15	Script Rules	Embedding user defined custom code for advanced routing
10.16	Error Handling	Error rules for custom error handling
10.17	Content Transformation	Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response JSON to XML, HTTP to MQTT & vice versa
10.18	End-User Fingerprinting & Monitoring	Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring
10.19	DDoS Protection	Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests
10.20	Compliance	PCI DSS 2.0 section 6.6 enforcement
10.21	API Security	Built-in API gateway for authentication, rate limiting, transformation, documentation and discovery
10.22	Authentication	Support for Single SignOn with multiple Auth type like Basic Auth, Form Auth, NTLM, LDAP, SAML, etc.
10.23	Forwarding Rule	Support traffic chaining, decrypt traffic forwarding to one or more devices.
WAF FEATURES		
11.1	Comprehensive Security	OWASP Top 10 Web Application Security Risks, OWASP Top 20 Automated Threats and SANS 25 Software Errors
11.2	Security Profiles	Multiple security profiles with support for different security status per application based on url, source, country, regex, etc.
11.3	Positive Security Model	Support for Form Rules for positive security model
11.4	Negative Security Model	Support for user defined Firewall Rules for REGEX based negative security model
11.5	Multi-Factor Authentication (MFA)	Additional verification factors, such as Email based OTP, TOTP, while accessing resources remotely

Copyright Haltdos. All rights reserved

11.6 Virtual Patching	Support for virtual patching through built-in web security scanner or upload of 3rd party SAST / DAST / IAST scan results
11.7 Built-in Signatures	Over 4000+ built-in signatures on various technologies, platforms and frameworks with pre-defined templates
11.8 Bot Management	Anti-bot protection with AI classification and scoring of bots based on advanced browser fingerprinting
11.9 0-day Protection	Automatic learning and profiling application structure. Threat scoring and baseline creation for AI driven 0-day attack protection
11.10 Anti-Automation Protection	Protection against known and 0-day bots, account takeover attempts, brute force attempts, scraping, reconnaissance, cloaking, etc
11.11 Mobile App Protection	Anti-Bot mobile SDK for Android & iOS for protecting mobile apps and communication between apps and web APIs
11.12 AV Scanning	Built-in AV scanner for malicious file upload. Support for ICAP integration for 3rd party scanners
11.13 Minimize False Positives	Support for REGEX based whitelist rules and signature staging and deploy policies to minimize signature based false positives
11.14 HTTP Validations	Protocol validations, request normalization (encoding & evasion techniques) before inspection, managing security headers and cookies etc
11.15 Policy Inspection	Policy validation such as HTTP methods, file extension, request size, etc
11.16 Blacklist / Whitelist	Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, url, country, etc
11.17 Challenge-Response	Support for JS, Crypto and CAPTCHA challenge on suspicious user activity or known bots or malicious IPs
11.18 Rate Limiting	Rate Limit rules for implementing request, bandwidth or connection limits per source, IP prefix or user defined policy
11.19 API & WebSocket Protection	Built-in XML firewall, validation of XML / JSON / Ajax requests and WebSocket requests
11.20 Security Breach Prevention	Built-in support for data leak prevention, response filtering for sensitive personal identifiable information
11.21 Tamper Proofing	Tamper rules for URL / parameter tamper protection, website defacement, hidden form field protection, cookie signing and encryption, etc.
11.22 Correlation Engine	Advanced correlation engine with support for custom correlation rules for detecting attack across user requests and sessions
11.23 Variables & Scripting	Support for user defined variables and scripts for building custom application specific security policy
11.24 Deception Technology	Implement decoys in web application to protect against advanced bots, profile attacks and trap attackers
11.25 L3-L7 DDOS PROTECTION	Protection against volumetric and low & slow DDos attacks
11.26 Sensitive Data Masking	Support for Log Rules for masking sensitive information such as passwords in logs and events
11.27 Malicious Source Protection	Protection against TOR IP, Bad Reputation IP, dark IP, known Bots, proxies, spammers provided by Haltdos or user defined threat intel
11.28 Enforced Browsing	Protection against forceful browsing, access to pctable resources, unauthorized navigation with additional security enforcement with Two factor authentication (2FA)
11.29 DDoS Detection & Mitigation	Attack detection & mitigation in less than 18s and 10s respectively
11.30 Captcha Challenge	Support for JS or Captcha challenge on suspicious user activity or known bots or Malicious IPs.

Copyright Haltdos. All rights reserved

11.31	API Security	Built-in API gateway for authentication, rate limiting, transformation, documentation and discovery
11.32	Misc. Protection	Support for protection against buffer overflow attacks, man-in-the-middle attacks, blocking malware payload, buffer overflow, SQL, SSI, LDAP injection, etc
ANTI-DDoS FEATURES (ADDITIONAL LICENSING)		
12.1	Comprehensive Security	Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks
12.2	Block Actions	Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting
12.3	Hybrid DDoS Integration	Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services
12.4	Bi-Directional	Support for both inbound and outbound traffic protection
12.5	Deep Packet Inspection	Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.)
12.6	Enforce RFC Compliance	Protection against misbehaving clients sending invalid or out of state packets
12.7	Bot Protection	Automatic detection and blocking of bot traffic with support for manual bot policy
12.8	Behavior Analysis	Network behavior analysis for anomaly detection and packet scoring technology
12.9	Multiple Security Profiles	Support for multiple security profiles for enforcing different policy for different sub - networks (Src, Dst IP Prefix, VLAN). Default Global security profile
12.10	Port Mirroring	Mirror traffic / specific traffic to another NIC port
12.11	Rate Limit & QoS Management	Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.)
12.12	Blacklist / Whitelist	Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc
12.13	Malicious Source Protection	Protection against TOR IP, Bad Reputation IP, dark IP, known Bots, proxies, spammers provided by Haltdos or user defined threat intel
12.14	Custom Signatures	Support for user defined custom rules with support for REGEX and byte matching
12.15	SYN Flood Protection	TCP SYN flood protection with SYN Proxy and connection aging
12.16	Challenge & Response	Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources
12.17	Connection Based Protection	Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc
12.18	DNS Protection	Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDoS attacks (Water Torture, NXDomain, etc.)
12.19	L7 DDoS Protection	Protection against low & slow attacks such as Slowloris, R.U.D.Y., slow HTTP GET / POST, etc
12.20	Machine Learning Protection	Automatic learning counter measures and dynamic signature creation upon attack detection
12.21	Signatures for Known Vulnerabilities	Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, etc.)
12.22	DDoS Protection & Mitigation	Attack detection & mitigation in less than 18s and 10s respectively.
12.23	Adaptive Packet Scoring Engine	High-performance software-defined packet processing engine with an NPU-inspired packet processing architecture, utilizing adaptive packet scoring, behavioral analysis, machine learning, and threat intelligence for real-time Layer 3–Layer 7 traffic inspection and attack mitigation.

Copyright Haltdos. All rights reserved

LLB FEATURES (ADDITIONAL LICENSING		
13.1	Load Balancing & Path Selection	Round robin (RR), weighted round robin, minimum packet loss, persistent hash, tuneable hash, least connections, least response time, least bandwidth, minimum jitter, etc.
13.2	NAT Rules	Support for static NAT, dynamic NAT, SNAT, DNAT, PAT, Full NAT
13.3	Wan Configuration	Supports multiple WAN connectivity such as Static IP, DHCP, PPPoE, Bridge, tranparent mode etc.
13.4	Health Monitoring	Link monitoring with instant failover (<1s). Support for TCP, HTTP, DNS, ICMP or script based monitoring
13.5	Routing Rules	Custom rules for Static and Policy based routing
13.6	Dual Stack Lite	Support for NAT 46 / 64 and DNS 46 / 64 with DNS Proxy
13.7	Traffic Shaping	Traffic shaping and QoS on inbound and outbound links
GSLB FEATURES (ADDITIONAL LICENSING)		
14.1	Global Load Balancing	Routing traffic across multiple data centers based on health checks
14.2	WAN Load Balancing	Outbound WAN link selection based on link health
14.3	Load Balancing Algorithms	Support for Least connection, Proximity, Round Robin, Weighted RR, Persistent Hash, Geo, etc.
14.4	Operation Mode	Option for Authoritative or Recursive operationalmodes with supportfor various DNS record typessuch as A, AAAA, MX, TXT, PTR, etc.
14.5	Routing Rules	Custom rules for Static and Policy based routing
14.6	Network Mode	Support DNS over HTTP, UDP, TCP &SSL as well as DNSSEC
14.7	DNS Firewall	Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy
14.8	Blacklist / Whitelist	Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc.
14.9	Custom Signatures	Support for user defined custom rules with support for pattern, suffix, domain, etc.
VPN FEATURES (ADDITIONAL LICENSING)		
15.1	HTTP Protocols	HTTP 0.9/1.0/1.1/2.0 with translation
15.2	Client Support	Provides access for Windows, Linux, Mobile Apps (Android and iOS), and Web (via browser-based solutions)
15.3	Authentication	Supports Password, SAML, AD/LDAP, SSO, AAA, OAuth, Step-up Authentication and third-party integrations via Webhooks
15.4	NAT & Routing	Enables client, server, or full NAT and static routing for IPv4 and IPv6
15.5	User Grouping	Allows creation of multiple users and user groups with granular access control
15.6	Clientless Access	Offers secure resource access via web browsers without additional client installation
15.7	Granular Access Control	Configurable policies to control user access to specific resources and applications based upon time, country, user-group and IP addresses
15.8	Endpoint Security	Validates the security posture of devices before granting access by performing Antivirus and Malware Scan of the devices, Windows Registry checks etc
15.9	Concurrent User/ Scalability	Scalable architecture supporting expansion to 4000+ concurrent users through vertical/horizontal scaling.
15.10	Multi-Factor Authentication (MFA)	Additional verification factors, such as Email based OTP, TOTP, while accessing resources remotely
15.11	Split Tunneling	Configurable options for routing only specific traffic through the secure tunnel
15.12	Zero Trust Principles	Strict verification of users and devices before granting access

Copyright Haltdos. All rights reserved

15.13	Dual Stack Lite	Support for NAT 46 / 64 and DNS 46 / 64 with DNS Proxy
15.14	SSL/TLS Management	Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher cuites. Client certificate-based authentication also supported, proxy SSL/TLS Connections.
15.15	IP Address Management	Dynamic IP allocation from configurable network pools (IPv4/IPv6) with automated lease management
15.16	VPN Protocol &Encryption	Modern VPN protocol utilizing Noise protocol framework with Curve25519 for key exchange, ChaCha20 for encryption, Poly1305 for authentication, and BLAKE2s for hashing
15.17	Networking	Support for VLAN, Link Aggregation & Trunking(LACP)
15.18	Policy Rules	HTTP request interception with policy-based traffic filtering with comprehensive request logging at VPN authentication layer
15.19	Dynamic Routing Protocols	BGP, OSPF, RIP v1, RIP v2

API SECURITY

16.1	Discovery	Static and Dynamic endpoint discovery using source code scan, swagger/open-api, SPAN traffic traffic etc.
16.2	Static Discovery	Scanning of source code repositories across major languages and common frameworks for endpoint discovery. Import of existing OpenAPI / Swagger specifications and Postman collections
16.3	Dynamic Discovery	Continuous API discovery from live traffic from WAF / gateway and web server access logs
16.4	Documentation & posture	Documentation of the discovered endpoints
16.5	On-Deman Scan	Support for on-demand or scheduled scans
16.6	Supported Protocol	Support for HTTP 1.0 / 1.1 / 2.0, gRPC, SOAP / XML-RPC and GraphQL APIs
16.7	Shadow & Unknown APIs	Automatic detection of hosts and endpoints outside the documented inventory with request volume, source clients, destination servers and first / last seen. One-click addition to API inventory
16.8	Traffic Discovery Sources	Continuous API discovery from live traffic and from WAF / gateway and web server access logs
16.9	Traffic Sensor	Discovery through out-of-band through mirror/SPAN port or virtual switch, SYSLOG, agent-based discovery
16.20	HTTP & HTTPS Visibility	Support for HTTP/gRPC visibility on any configured port. HTTPS inspection using SSL certificates for RSA key exchange sessions
16.21	API Inventory	Complete endpoint record including method, path, normalized path with version, collection, discovery source, request volume, consumers, destination service, authentication type, content type, technology and tags
16.22	Inventory Organization	Grouping of APIs into business collections with hostname based mapping. Support for separation per environment and per tenant
16.23	Drift Detection	Detection of undocumented changes in request and response structures. Version-wise tracking of each API against its previous version
16.24	API Lifecycle	Lifecycle tracking from discovery through documentation, change, deprecation and retirement. Detection of zombie and orphan endpoints still receiving traffic
16.25	Sensitive Data & PII Discovery	Identification of personal and regulated data in API fields across 20 data classes such as email, phone, national ID, card number, bank account, credentials, health and biometric data with per-endpoint flags. Support for masking values at capture so no sensitive content is retained

Copyright Haltdos. All rights reserved

16.26	OWASP API Security Top 10	Findings mapped to OWASP API Security Top 10 (2023) including Broken Object Level Authorization (BOLA), Broken Authentication, Broken Object Property Level Authorization (excessive data exposure), Broken Function Level Authorization (BFLA) and related risks, each with severity and evidence. Active and passive scan findings mapped to OWASP API Security Top 10 with severity, evidence and remediation guidance
16.27	Custom Rules & Updates	Support for customer-specific and sector-specific rules with OWASP mapping and severity. Rule updates without product upgrade
16.28	Risk Scoring	Risk score per API and per field based on exposure, authentication, sensitive data and known findings. Support for analyst override
16.29	Vulnerability Scan	Support for scanning with authenticated and unauthenticated point based on the application information
16.30	Passive Scan	Passive scanning of live traffic and access logs with no impact on production traffic.
16.31	Active Scan	Active scanning of API endpoints on demand or on schedule, with throttling and exclusion controls for safe testing
16.32	Vulnerability lifecycle	Tracking of findings from detection and remediation through revalidation and closure
16.33	Security Misconfiguration	Detection of missing security headers, CORS misconfiguration, and weak TLS

HARDWARE FLEXIBILITY

Haltdos appliances are built on a common hardware platform with flexibility in mind. The appliances can be extended to provide remote, out-of-band management and monitoring, performance acceleration, and more with expansion modules

Expansion Module includes:

- Network Cards (copper or optical)
- Hardware Security Module (HSM) (non-FIPS and FIPS-140-2)
- SSL acceleration card
- Hard Disk & RAM

Hard Disk		
16.1	HD-DSK-128G-SSD	128 GB SSD Hard Disk
16.2	HD-DSK-256G-SSD	256 GB SSD Hard Disk
16.3	HD-DSK-512G-SSD	512 GB SSD Hard Disk
16.4	HD-DSK-1T-SSD	1 TB SSD Hard Disk
16.5	HD-DSK-1T-HDD	1 TB HDD Hard Disk
16.6	HD-DSK-2T-HDD	2 TB HDD Hard Disk
16.7	HD-DSK-4T-HDD	4 TBHDD Hard Disk

Copyright Haltdos. All rights reserved

SSL Cards

	Part Code	Throughput			SSL TPS
17.1	HD-SSL-25G	SSL	25 Gbps	RSA	40
		Compression	20 Gbps	ECC	25K
17.2	HD-SSL-50G	SSL	50 Gbps	RSA	95K
		Compression	37 Gbps	ECC	48K

NIC Cards

18.1	Part Code	Description	Copper/Fiber	Hardware Bypass
18.2	HD-NIC-1x4C	Quad Port 1 Gbps	Copper	No
18.3	HD-NIC-1x4CB	Quad Port 1 Gbps	Copper	Yes
18.4	HD-NIC-1x4F	Quad Port 1 Gbps	Fiber (Single / Multi-Mode)	No
18.5	HD-NIC-10x2C	Dual Port 10 Gbps	Copper	No
18.6	HD-NIC-10x2CB	Dual Port 10 Gbps	Copper	Yes
18.7	HD-NIC-10x2F	Dual Port 10 Gbps	Fiber (Single / Multi-Mode)	No
18.8	HD-NIC-10x2FB	Dual Port 10 Gbps	Fiber (Single / Multi-Mode)	Yes
18.9	HD-NIC-10x4F	Quad Port 10 Gbps	Fiber (Single / Multi-Mode)	No
18.10	HD-NIC-10x4FB	Quad Port 10 Gbps	Fiber (Single / Multi-Mode)	Yes
18.11	HD-NIC-25x2F	Dual Port 25 Gbps	Fiber (Single / Multi-Mode)	No
18.12	HD-NIC-25x2FB	Dual Port 25 Gbps	Fiber (Single / Multi-Mode)	Yes
18.13	HD-NIC-25x4F	Quad Port 25 Gbps	Fiber (Single / Multi-Mode)	No
18.14	HD-NIC-25x4FB	Quad Port 25 Gbps	Fiber (Single / Multi-Mode)	Yes

Copyright Haltdos. All rights reserved

NIC Cards

18.15	HD-NIC-40x2F	Dual Port 40 Gbps	Fiber (Single / Multi-Mode)	No
18.16	HD-NIC-40x2FB	Dual Port 40 Gbps	Fiber (Single / Multi-Mode)	Yes
18.17	HD-NIC-40x4F	Quad Port 40 Gbps	Fiber (Single / Multi-Mode)	No
18.18	HD-NIC-40x4FB	Quad Port 40 Gbps	Fiber (Single / Multi-Mode)	Yes
18.19	HD-NIC-100x2F	Dual Port 100 Gbps	Fiber (Single / Multi-Mode)	No
18.20	HD-NIC-100x2FB	Dual Port 100 Gbps	Fiber (Single / Multi-Mode)	Yes
18.21	HD-NIC-100x4F	Quad Port 100 Gbps	Fiber (Single / Multi-Mode)	No
18.22	HD-NIC-100x4FB	Quad Port 100 Gbps	Fiber (Single / Multi-Mode)	Yes

RAM

19.1	HD-RAM-8G	8 GB DDR4 RAM
19.2	HD-RAM-16G	16 GB DDR4 RAM
19.3	HD-RAM-32G	32 GB DDR4 RAM
19.4	HD-RAM-64G	64 GB DDR4 RAM

Copyright Haltdos. All rights reserved