# haltdos

# HALTDOS FALCON TECHSPECS

| Base Models | HD-FAL-4120 | HD-FAL-4620 | HD-FAL-5120 | HD-FAL-5420 | HD-FAL-6220 | HD-FAL-6700 |
|---|---|---|---|---|---|---|
| **MITIGATION PERFORMANCE** | | | | | | |
| Throughput Range | upto 4 Gbps | upto 24 Gbps | upto 48 Gbps | upto 64 Gbps | upto 120 Gbps | upto 150 Gbps |
| Supported TCP Sessions | Unlimited | | | | | |
| DDoS Attack Flood Prevention Rate | 1M – 5M | 5M – 20M | 10M – 30M | 25M – 50M | 30M – 80M | 30M – 80M |
| SSL / TLS Connections per Second | 22K (RSA 2K) 15K (ECC) | 40K (RSA 2K) 25K (ECC) | 40K (RSA 2K) 25K (ECC) | 95K (RSA 2K) 48K (ECC) | 95K (RSA 2K) 48K (ECC) | 95K (RSA 2K) 48K (ECC) |
| SSL Throughput | 4 Gbps | 20 Gbps | 40 Gbps | 50 Gbps | 100 Gbps | 100 Gbps |
| TCP Connection Tracking | 1M – 4M | 4M – 10M | 10M – 15M | 10M – 25M | 20M – 35M | 20M – 35M |
| L4 Connection per Second | 600 K | 1.5 M | 1.5 M | 2 M | 4 M | 4.2 M |
| L7 Request per Second | 1 M | 3 M | 7 M | 10 M | 15 M | 18 M |
| Induced Latency | < 50 microseconds (μs) | | | | | |
| Attack Detection Time | < 18s | | | | | |
| Attack Mitigation Time | < 10s | | | | | |
| **HARDWARE SPECS** | | | | | | |
| Processor | Intel Xeon | Intel Xeon | Intel Xeon | Intel Xeon | Intel Xeon | Intel Xeon |
| CPU Cores | 12 | 24 | 32 | 40 | 48 | 48 |
| Minimum Memory | 32 GB | 64 GB | 64 GB | 96 GB | 128 GB | 128 GB |
| Minimum Hard Disk | 256 GB SSD | 512 GB SSD | 1 TB SSD | 2 TB SSD | 2 TB SSD | 2 TB SSD |
| 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 | | | | | |
| Form Factor | 1U/2U Rack Mount Server (19 inch mounting) | | | | | |
| Power Supply | Redundant Power Supply (Hot Swappable) AC 170-240V, 50 Hz | | | | | |
| Operating Temperature | 0° – 40° C | | | | | |
| Humidity | 8% - 95% (non-condensing) | | | | | |
| **Hard Disk and Memory can be customized over the base model** | | | | | | |
| **INSPECTION PORTS** | | | | | | |
| 1G | 8 | 8 | - | - | - | - |
| 10G | - | 2 | 4 | 8 | 8 | 8 |
| 25G | - | - | - | - | - | 2 |
| 40G | - | - | 2 | 2 | 4 | - |
| 100G | - | - | - | - | - | 2 |
| **No. of ports can be customized over the base model** | | | | | | |
| **OUT OF BAND PORTS** | | | | | | |
| 1 GE (RJ-45) Ports | 2 | 2 | 2 | 2 | 2 | 2 |
| Console (RS232/RJ45) Ports | 1 | 1 | 1 | 1 | 1 | 1 |
| HA Ports (RJ-45/SFP/SFP+) | 1 | 1 | 1 | 1 | 1 | 1 |
| Input/Output (USB) | 2 | 2 | 2 | 2 | 2 | 2 |
| **TECHNOLOGY, CERTIFICATION & SUPPORT** | | | | | | |
| Platform | Haltdos Platform – hdPlatform (EAL 2+ Certified) | | | | | |
| Technology | Signature with Threat Intelligence, Machine Learning | | | | | |
| Bandwidth License | Bandwidth capping on provided license. Upgrade possible without hardware replacement upto max supported bandwidth on hardware | | | | | |
| Additional Licenses | Optional license for WAF, LLB, GSLB, SLB & DNS Firewall | | | | | |
| Certification | FCC, ROHS, CE compliant, Common Criteria EAL 2+ | | | | | |
| Support | 24x7 Support with dedicated Account Manager | | | | | |
| Warranty | 1 year software and hardware maintenance | | | | | |
| TAC Support | TAC support in India | | | | | |
| **OPERATION MODE** | | | | | | |
| Network Operations | Transparent L2 or Inline L3 | | | | | |
| Stateful Mode | Stateful (Symmetric) or Stateless (Asymmetric) mode | | | | | |
| Deployment Modes | Offline (SPAN port or Flow), Inline, Out-of-path | | | | | |
| Supported Flow Ingestion | Netflow v5, Netflow v9, sFlow, IPFIX | | | | | |
| IP Stack | Dual IPv4 & IPv6 stack | | | | | |
| IP Fragmentation | IP defragmentation & TCP stream assembly | | | | | |
| Jumbo Frames | Yes | | | | | |
| Mitigation Modes | Bypass, Record (Report Only), Learning, Mitigation (Block and Report) | | | | | |
| Tunnelling Protocols | VLAN, MPLS, GRE, L2TP, GTP, IPinIP | | | | | |
| Dynamic Routing Protocols | BGP, OSFP, RIP v1, RIP v2 | | | | | |
| Link Aggregation | Support for link bundling via LACP | | | | | |
| Block Actions | Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting | | | | | |
| **HIGH AVAILABILITY** | | | | | | |
| Hardware Bypass | Internal or External | | | | | |
| Software Bypass | Yes | | | | | |
| Multiple Appliances | N + 1 Active - Active or Active – Passive with VRRP equivalent | | | | | |
| Management Modes | Standalone / Centralized Management (VM or appliance) with Haltdos Hawk | | | | | |
| Secure Communication | Secure communication between centralized management and HA appliances for state synchronization | | | | | |
| **INTEGRATION FEATURES** | | | | | | |
| Custom Threat Intel | Integration with 3rd party Threat Intelligence (TI) feeds | | | | | |
| Storage and Export | Local retention of logs, reports and events. Support for export to 3rd party storage | | | | | |
| NIMS Integration | Support for SNMP, NTP / SNTP, DNS, Web Proxy integration | | | | | |
| Notification Integration | Notification & Logging via SNMP, SMTP, SMS Gateway and 3rd party integration via API hooks, CI/CD, Kubernetes | | | | | |
| SIEM Integration | Support for integration with SIEM and Syslog services | | | | | |
| AAA Integration | Support for integration via RADIUS and TACACS+ | | | | | |
| Identity Management | Inbuilt with support for integration with AD / SAML / LDAP | | | | | |
| Hybrid DDoS Integration | Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services | | | | | |
| Export IOCs | Support for exporting attacking IOCs via STIX / TAXII | | | | | |
| **MANAGEMENT FEATURES** | | | | | | |
| Graphical User Interface (GUI) | Secure web interface over HTTPs with support for all modern browsers | | | | | |
| Command Line Interface (CLI) | Command Line Interface over SSH or console port | | | | | |
| API Integration | Yes (XML or JSON) | | | | | |
| System Management | IPMI 2.0 Compliant | | | | | |
| Logging | Centralized logging of system, services, MIS, incidents | | | | | |

| | |
|---|---|
| Dashboards | Real-Time & historical dashboards with custom duration. Support for custom dashboards |
| System Status Dashboard | Status dashboard for 1-click health check |
| Reporting | Periodic daily, weekly or monthly reports in PDF or Excel |
| RBAC Administration | Configurable user profiles with role based access control |
| Backup | Automatic or manual backup and restore |
| Policy Management | On the fly configuration updates on mitigation appliances |
| Events / Alerts | Detailed event and alert reporting on attack, health, etc. |
| Network Forensic | Network forensic and packet capture capability for traffic examination and diagnosis |
| Attack Forensic | Built-in utilities for investigating attackers, attack payloads and identifying false positives |
| Haltdos Threat Stream | Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos |
| Updates | Update and upgrade management on version releases and patch updates from Haltdos |
| **DDOS MITIGATION FEATURES** | |
| Comprehensive Protection | Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks |
| Bi-directional | Support for both inbound and outbound traffic protection |
| Deep Packet Inspection | Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) |
| Enforce RFC Compliance | Protection against misbehaving clients sending invalid or out of state packets |
| Bot Protection | Automatic detection and blocking of bot traffic with support for manual bot policy |
| Behaviour Analysis | Network behaviour analysis for anomaly detection and packet scoring technology |
| Multiple Security Profiles | Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN) |
| Rate Limit & QoS Management | Rate limit capability for bandwidth and QoS management |
| Blacklist / Whitelist | Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc |
| Malicious Source Protection | Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc |
| Custom Signatures | Support for user defined custom rules with support for REGEX and byte matching |
| SYN Flood Protection | TCP SYN flood protection with SYN Proxy and connection aging |
| Challenge & Response | Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources |
| Connection Based Protection | Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc |
| DNS Protection | Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDoS attacks (Water Torture, NXDomain, etc.) |
| L7 DDoS Protection | Protection against low & slow attacks such as Slowloris, R.U.D.Y., slow HTTP GET / POST, etc |
| Machine Learning Protection | Automatic learning counter measures and dynamic signature creation upon attack detection |
| Signatures for Known Vulnerabilities | Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, etc.) |
| **LLB FEATURES (ADDITIONAL LICENSING)** | |
| NAT Rules | Support for static NAT, dynamic NAT, SNAT, DNAT, PAT, Full NAT |
| Health Monitoring | Link monitoring with instant failover (<1s). Support for TCP, HTTP, DNS, ICMP or script based monitoring |
| Routing Rules | Custom rules for Static and Policy based routing |
| Dual Stack Lite | Support for NAT 46 / 64 and DNS 46 / 64 with DNS Proxy |
| Traffic Shaping | Traffic shaping and QoS on inbound and outbound links |
| **GSLB FEATURES (ADDITIONAL LICENSING)** | |
| Global Load Balancing | Routing traffic across multiple data centers based on health checks |
| Local Load Balancing | Outbound WAN link selection based on link health |
| Operation Mode | Option for Authoritative or Recursive operational modes |
| Routing Rules | Custom rules for Static and Policy based routing |
| Network Mode | Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC |
| DNS Firewall | Protecting DNS infrastructure from bot attacks |

Version: v6.1