Simplifying IT Security

HaltDos Falcon

(Enterprise DDoS Protection Solution)

DATASHEET

HaltDos Falcon is a high-performance DDoS detection and mitigation solution, leading industry in precision, scalability, intelligent automation, and performance. HaltDos is certified EAL 2+ solution under Common Criteria Certification Scheme.

First and Last Line of Smart and Automated DDoS Defense Against Cyber Attacks

Falcon at a glance:

AI-Enabled: Employs AI to automatically detect and effectively respond to cyber-attacks in real time without any human intervention.

High-Performance: Industry standard in latency by DDoS appliance is around 200 microseconds, HaltDos provides < 60 microseconds latency. 3x faster than traditional hardware-based solutions.

Bi-Directional: Ensure protection against both inbound and outbound traffic and decrease the attack degree.

Transparent Layer 2 Solution: Deploy-and-forget appliance. No need for IT security experts for management. Ready to deploy in any network environment.

Protect Your Business

DDoS attacks are increasing in scale and complexity and threatening to damage businesses around the globe. These attacks combine high-volume traffic with stealthy, low-and-slow, application-targeted techniques. There is almost an unlimited array of tools that hacktivists and cyberterrorists can exploit to prevent customers access to your web services.

Sophisticated DDoS attacks are much smaller in size, making it nearly impossible for traditional ISP-based mitigation methods to detect them. To combat these attacks from reaching the enterprise network, organizations need a solution that is equally dynamic and broad-based.

HaltDos is available when you need help most. HaltDos uses signature-based pre-emption, entropy-based detection, and anomaly-based detection and mitigation techniques to accurately and automatically detect and mitigate attacks at lightning speed. Also, HaltDos mitigation appliance features full protection from traditional vulnerability-based attacks through proactive signature updates, preventing the already known attacks.

HaltDos mitigation appliance uses signature-based pre-emption, entropy-based detection, and anomaly-based detection and mitigation techniques to accurately and automatically detect and mitigate attacks at lightning speed.

HaltDos is a real-time DDoS protection hardware device, which maintains business continuity by protecting the application infrastructure against existing and emerging network- based threats that cannot be detected by traditional Intrusion Prevention Systems.

Support

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

TALK WITH HALTDOS

Web haltdos.com/products/ddos

Call 1800-120-2394

Reach haltdos.com/contact

Amidst fierce competition, your business cannot afford to slow down. With HaltDos, you don’t have to sacrifice productivity and performance to get leading-edge security.

HaltDos provides multi-layer, multi-vector protection to ensure that your IT network stays online and always accessible to your customers.

Get peace of mind for your online business with HaltDos - real-time, all the time network protection solution.

Why Trust HaltDos Falcon?

360° Security

All round protection from simple to sophisticated zero-day attacks.

Real-Time Metrics

Audit report on Attack, application health, customer interaction and more

Maintains Business Operational

Attack or no attack, HaltDos ensures your business stays operational all the time.

Multi-Vector Attack Protection

Detect and mitigate DDoS attacks of many types, including volumetric, protocol, and application-level attacks

Security Simplified

100% customizable with on the fly updates. Easy to scale and takes no more than a few minutes to set up.

No Human Policy

"Hands-off" solution with self-learning capability that adapts to changing network conditions and requires minimal tuning.

Accurate Attack Mitigation

Stateful and/or Stateless DDoS appliance providing best in class attack detection and mitigation in the most demanding operational environments.

DDoS Mitigation Techniques
(How to Prevent DDoS Attacks)

Deep Packet Inspection

(Look within the application payload of packet)

- Accurate detection of malicious packets
- Serves real-time network monitoring
- Enhances the capability of ISPs to prevent the exploitation of IoT devices in DDOS attacks

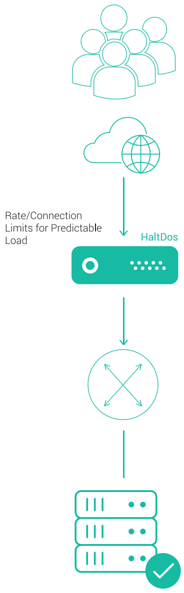
Checks:

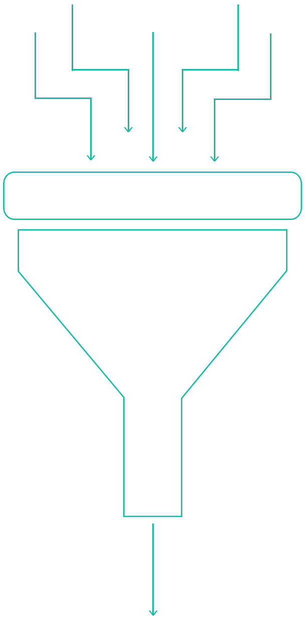
- Connection State
- Attack Signature
- Packet Payload Content
- Packet Headers

Whitelisting / Blacklisting

(Manual operations to perform on IP prefixes)

- Filter legitimate/malicious incoming requests that are coming from any geographical region
- Ensure regulatory compliance regimes
- Prevent inbound flood attacks from the multiple IP resources
- Prevent outbound flood attacks from your IPs





Traffic Shaping

(Improve Latency)

- Stream optimization and increased network performance
- Prevent False Positives

Traffic Rate Control

(Monitoring and Rate Limiting Traffic)

- Prevents Volumetric attacks, Protocol and Resource attacks
- Network and Application level enforcement

Examples

- Connection Limit
- Connection Rate Limit
- Packet Rate Limit
- HTTP Request Limit

Aggressive Aging

(Connection Timeout for Idle / half-open connections)

- Prevent against the Open connection and Slow connection attacks.
- Prevents idle connections to fill up the connection tables in servers.
- Much sooner Timeout for Inbound and Outbound Connections.

- Slow connection attacks aim to make a service unavailable or increase latency to a service.

Anomaly Detection

(Automatic detection based on the traffic behavior)

- Enables quick attack mitigation response.
- Accurately detects the abnormal behavior of the traffic.
- Prevents Zero-day DDoS

Checks

- Traffic Pattern
- Packet Analysis

HaltDos DDoS attack mitigation appliance is a dedicated, specially designed device to detect and mitigate an array of DDoS attacks.

UDP | ICMP | IGMP | Smurf | TCP FIN | TCP ACK | Teardrop | Slowloris | Spoofing | DNS flood | TCP RESET | HTTP Flood | Brute Force | Ping of Death | TCP SYN+ACK | TCP ACK + PSH | TCP Fragment | Connection Flood | Zero-day DDoS attacks | Reflected ICMP and UDP | Attacks targeting DNS servers | Mixed SYN + UDP or ICMP + UDP flood | Attacks targeting Apache Windows or Open BSD vulnerabilities And more...

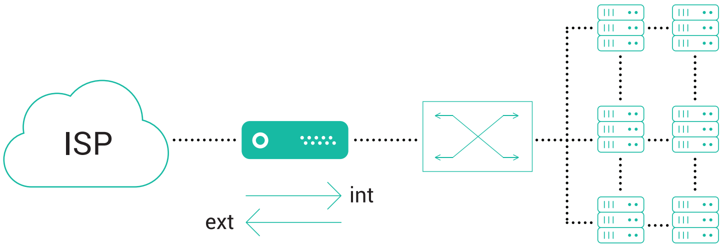
Deployment Modes

Inline Mode

Inline DDoS Mitigation mode inspects all the traffic in real-time and can identify, analyze and mitigate within seconds.

HaltDos supports flexible inline mode deployments:

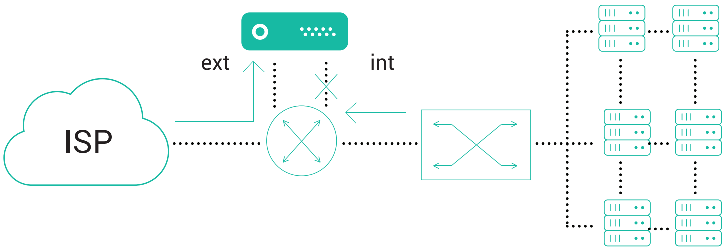
- Standalone deployment
- High Availability 1:1 deployment with separate management
- Stack deployment with separate management



In inline mode, the solution also supports the "inactive" protection mode where only attack detection is enabled and "active" protection mode where attack detection, as well as mitigation, are enabled. In "inactive" protection mode, the solution analyzes traffic and monitor attacks without performing any mitigations. Protection mode can be changed on-the-fly by configuring software bypass setting.

Offline Mode

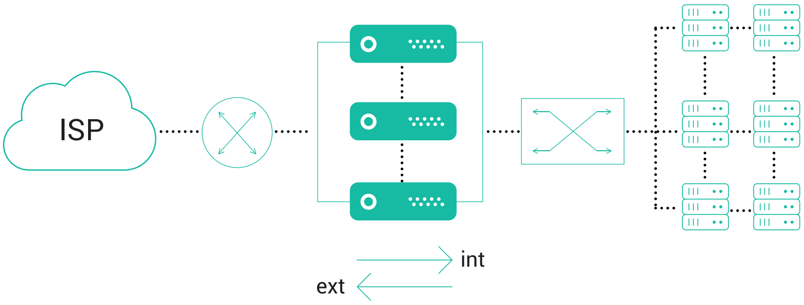
HaltDos is deployed out-of-line through a span port or a network tap. Offline mode, in general, is for trial implementation. For example, before deploying HaltDos inline mode and allowing it to affect the enterprise network traffic, you can deploy it in offline mode for evaluation purposes. The generated information further helps in creating enterprise policies for attack detection and mitigation.



High Availability Mode

High-availability settings allow configuring multiple HaltDos Mitigation servers to run in a cluster (sharing states, parameters and behaviour). This also ensures reliability & service continuity. To set this, you need to fulfil the following two conditions:

- Availability of minimum of two HaltDos mitigation appliances
- Ensure both devices are in direct connection with each other over a dedicated HA port



STAY ONLINE AND ALWAYS AVAILABLE WITH HALTDOS FALCON!

To learn more about our Enterprise DDoS Protection Solution and to ensure 360° protection for your IT network resources, please visit: www.haltdos.com

HaltDos™ FALCON

● *We are GDPR Compliant!* ●