HARPP
ddos mitigator

www.harppddos.com

HARPP DDoS Mitigator Appliances and DDoS CERT

The HARPP DDoS Mitigator's unique DDI™ (Deep DDoS Inspection) and AVS™ (Attack Visualization System) provide unparalleled protection of your network, web applications and services - from DDoS attacks.

Cyber Warfare Intelligence

Are you safe from DDoS attacks?

Any organization offering online services to potential customers, employees and/or business partners are a potential target.

Volumetric attacks-target the bandwidth of an organization's internet pipe with the intent to saturate it with unwanted traffic-reducing the available capacity and causing web application performance to be slowed or even closed down for extended periods of time.

Exhaustion attacks-focus on specific devices such as Firewalls, Load balancers, IPS appliances and web servers in order to exhaust their limitations in concurrent connections by attempting to establish incomplete connections, ultimately causing the slowing or actual halting of these devices and therefore impacting internet and in some cases internal network connectivity.

Application layer attacks - target a specific application or database with application calls, slowing or even closing down your business applications.

DDoS diversion attacks - can be Volumetric, Exhaustion or Application DDoS attacks which are used to divert attention from the penetration of another threat which could ultimately lead to the theft of critical business intelligence information, or even funds.

Concurrent attacks - a combination of volumetric, exhaustion and application level attacks which are increasingly used to overcome situations whereby an organization might have some existing protection devices which are only able to protect against specific attack forms. Any of the above can and most often will, significantly impact your on-line reputation & revenue generation activities.

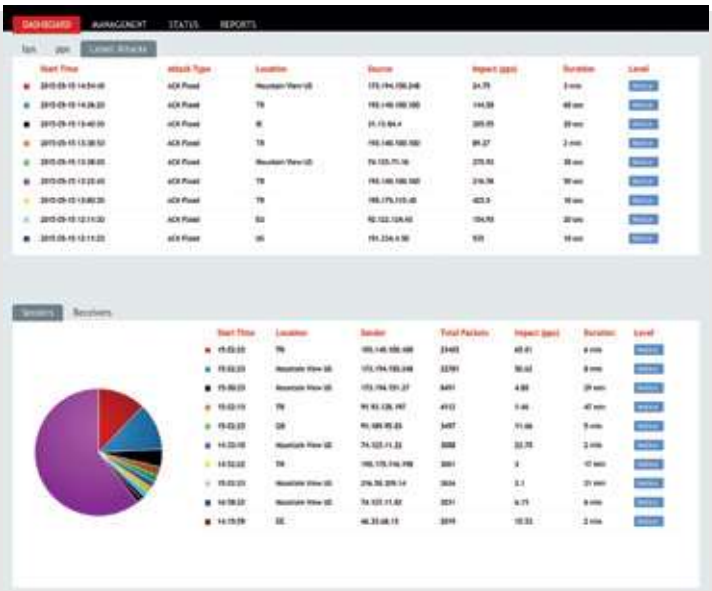
Few organizations have implemented the sufficient level of protection needed to detect and defeat these ever increasing and sophisticated attacks. Traditional "stand-alone measures" such as Firewall/IPS/UTM appliances, or even solutions provided by Internet Service Providers (ISP) and cloud scrubbing centers, are insufficient to detect and mitigate many of today's highly sophisticated attacks.

As the frequency, size and sophistication of DDoS attacks increase, the intelligence level of any

and defense system is key. Less than 1 Gbps of attack traffic (historical statistics show 75% of DDoS attacks are at or under 1 GBps) is sufficient to halt most web services with ease. Whilst the ability to defend against a simple “volumetric or exhaustion attack” is critical, perhaps even more important is the ability to detect and defend against the “emerging more targeted & advanced” application layer & concurrent attacks.

To avoid the devastating results of either, there is a need for a high performance and high availability hardware appliance, with the intelligence and supporting services needed to detect and then mitigate both known and previously unknown DDoS attack forms including TCP, UDP, HTTP, ICMP, SMTP, VOIP and application layer specific attacks.

» Management & Reporting



A key design objective was to produce a solution that was simple to install and administrate – which is why our HARPP DDoS Mitigator starts protecting your business immediately upon connection - minimizing your cost of implementation & ownership. A key-advantage over alternative products is in the HARPP DDoS Mitigator’s unique ability to dynamically learn and then tune its protection configuration.

During a sophisticated and complex DDoS attack, the ability to visualize historical and real-time traffic data provides important total insight and security. The HARPP DDoS Mitigator’s AVS™ (Attack Visualization System) provides multi-dimensional graphics through which the deep attack characteristics can be fully monitored and analyzed.

» Your Trusted Defense From The DDoS Threat

The HARPP DDoS Mitigator Appliance should be your first level of protection from cyber attacks. State-of-the-art performance & functionality provide the highest-level of protection for your web, DNS infrastructure, servers and applications through normalization, protection and protocol-specific security tools. Pre-emptive defense functions (without the requirement of administrator intervention), are continually active 24 hours a day, 365 days a year ensuring your online business continuity with the absolute minimum Total Cost of Ownership. Our network of HARPP DDoS Mitigators installed worldwide creates a wide cyber intelligence network (IP Reputation Network) from which you gain additional intelligence and benefits in real-time.

Popular Misconceptions

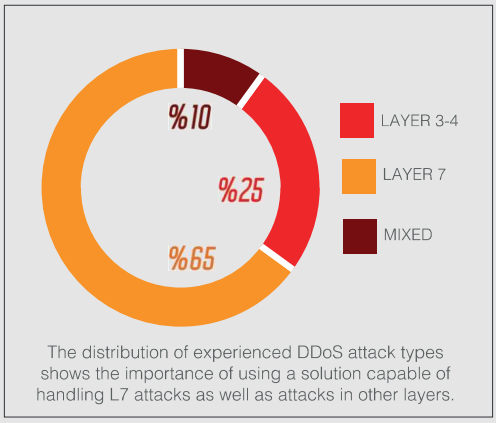
"There are Firewall and IPS appliances in my network. So, I'm safe."

Unfortunately you really are not safe. Those inline appliances, which you trust can actually be part of the problem! UTM, Firewall and IPS appliances have limited processing performance and number of concurrent sessions, and since DDoS attacks are targeted to overload systems/applications etc. your appliances can often be the first bottleneck in any attack forcing your network offline, or making your systems vulnerable to other threats.

You require a dedicated high-performance HARPP DDoS Mitigator appliance to stop DDoS attacks prior to reaching your existing interior security appliances.

Sample FW/IPS Specs	Product A	Product B	Product C
Concurrent Sessions	1.000.000	2.000.000	10.000.000
Sessions per Second	23.000	40.000	175.000

"Cloud or ISP Scrubbing Centers can protect my web infrastructure."



The distribution of experienced DDoS attack types shows the importance of using a solution capable of handling L7 attacks as well as attacks in other layers.

Resource: Labris SOC

There are a number of potential problems for organizations electing to use a solely off-premises scrubbing center approach. One example is where the attacker is using SSL. The scrubbing center typically cannot handle HTTPS attacks as it is, in most cases, unable to decrypt the traffic as it does not hold the SSL certificate. A further drawback is in the time delay to divert traffic to the scrubbing center. DDoS attacks can be shorter than the period it takes for BGP to converge and advertise the new routes. So frequent short attacks are often used to target this weak - ness. Also latency must be considered as if the scrubbing center is located far from your datacenter, it will add latency to your traffic which can be a problem in some environments.

We even see basic DNS method to get traffic in some scrubbing center solutions. It is easy for the attacker to get real IP addresses of the servers and bypass scrubbing center in such solutions.

Superior performance & intelligence

Given the ever-increasing frequency & evolving complexity of DDoS attacks, the need for a fast and sophisticated detection & prevention engine is paramount. HARPP DDoS Mitigator's industry leading DDI™ (Deep DDoS Inspection) anomaly engine includes both heuristic and non-heuristic algorithms together with true real-time traffic analysis to ensure that detection & prevention occur prior to any attack reaching your network.

The HARPP DDoS Mitigator's integral Advanced Persistent Threat (APT) identification capability ensures that even the most stealthy and continuous computer hacking processes are identified. Greater than 34 traffic sensors are continuously monitored and our unique predetermined & self-learning sensor algorithms utilise proportioning, historical and real-time data to ensure often previously unpredictable DDoS attacks are detected for cleaning, prior to any disruption.

» HARPP DDoS Mitigator Features & Benefits

Designed for working in non-blocking working principle which does not use any proxy which leads to high latencies.	
It does not require any Telco backbone complement and provide independence to network security teams.	
Provides plugin framework and plugin ecosystem for any third party applications.	
Wire-speed real-time inspection provided by a family of highly tuned software appliances.	Ensures DDoS attacks are detected prior to impacting your network.
34+ Data sensor groups including layer 7 application level sensors plus an advanced configuration tool, which provides even greater control & customized signature creation capability.	The Industry leading large number of sensors plus customization ability provide the capability to detect the most sophisticated attack forms.
Default generic thresholds developed from our knowledge & experience, plus dynamic threshold optimization providing automatic optimization of sensor thresholds based on current threat levels and historical data archived from our world-wide deployment of HARPP DDoS Mitigator sensors (IP Reputation Network).	Starts protecting your business immediately - minimizing your cost of implementation & ownership.
Ultra-fast and advanced anomaly engine uses AI, heuristic and non-heuristic algorithms which use data sensor averages and source determination of anomalous traffic.	Provides complete protection against evolving, as well as network and application layer attacks.
Unique proportioning ability based upon historical data, averages (yearly, seasonal, monthly, weekly, daily etc) aids accuracy.	Reduces administrator overhead and time consuming false alarms.
Geographical traffic classification provides both Country based and IP block based filtering abilities.	Provides the ability for an organization to reduce the risk of attack by blocking potential attack sources.
Integral DOS Intrusion Prevention System pattern signatures & Deep Packet Inspection Firewall with Layer 7 packet inspection, Stateful Packet Inspection, bandwidth management and full IPV6 support provide protection from all attack types including those seeking to exploit application and system vulnerabilities.	Total protection ensures business confidence no matter the size of the organization.

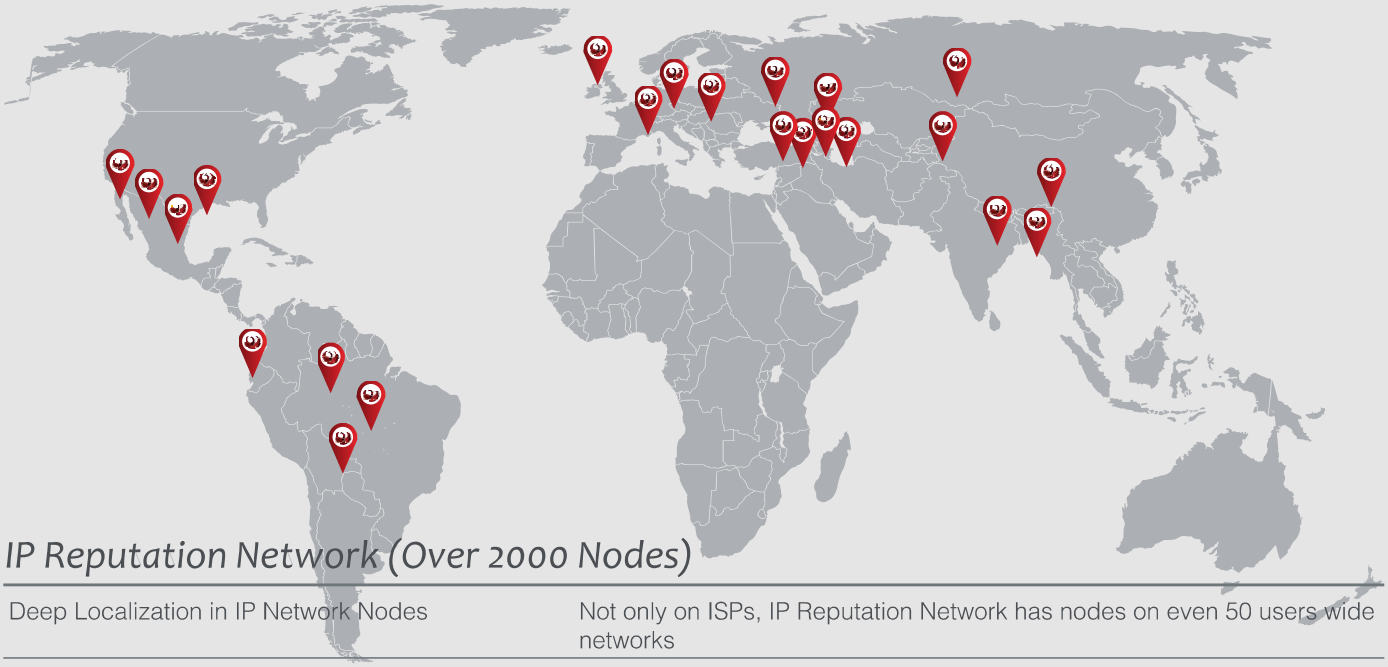
» Specifications

› *Data Sensor Categories*

TOTAL PACKETS	TOTAL CONNECTIONS	TOTAL CLIENTS	DEEP DoS/DDoS INSPECTION (DDI)
Incoming packets	TCP connections	TCP clients	DNS deep DoS/DDoS inspection
Outgoing packets	UDP connections	UDP clients	Commonly used ports inspections
TCP packets	ICMP connections	ICMP clients	HTTP GET sensor
UDF packets	Other connections	Other clients	HTTP POST sensor
ICMP packets	Established TCP connections	TCP established clients	HTTP other words
Other packets	Time Wait connections	Time Wait clients	L7 IPS sensors
IPv4 packets	TCP SYN connections	Fin Wait clients	DNS deep DoS/DDoS inspection
IPv6 packets	TCP other flags	TCP SYN clients	
Incoming bandwidth	TCP connections	TCP other flagged clients	
Outgoing bandwidth	UDF connections	TCP clients	

Mitigated Attack Types

TCP DoS/DDoS	SYN, ACK, FIN, URG, PUSH, SYNACK, ACKPUSH Flood, Fragmented Attacks, Connection / Session Flood	
UDP DoS/DDoS	DNS Flood, Generic UDP Flood	
HTTP DoS/DDoS	GET Flood, POST Flood	
Others	ICMP DoS/DDoS	Brute Force Attacks
	SMTP DoS/DDoS	Pre-attack
	VOIP DoS/DDoS	Vulnerability Analysis
	L7 Application Specific DoS	(Ex: Folder Checks, Application Vulnerability Scans)



IP Reputation Network (Over 2000 Nodes)

Deep Localization in IP Network Nodes	Not only on ISPs, IP Reputation Network has nodes on even 50 users wide networks
Inspected Traffics for IP Determination	Malicious traffics like spam, virus, malware outbreaks, open proxy
Historical Background	Reputation Database aged for years

Winner Solution

A Dedicated Appliance + Cyber Intelligence

Appliance Form	Rackmount (1U)				Rackmount (2U)				Rackmount (2U)	
PPS (PacketsPerSecond)	600.000				3.000.000				26.000.000	
Full Traffic Throughput (up to)	0.5 Gbps	1 Gbps	1.5 Gbps	2 Gbps	4 Gbps	6 Gbps	8 Gbps	10 Gbps	20 Gbps	40 Gbps
Max Concurrent Sessions	20.000.000				50.000.000				50.000.000	
100/1000 Ethernet (PCS)	8 Port (Max 24)				4 Port (Max 12)				4 Port (Max 32)	
Gigabit SFP Port (PCS)	Op (Max 8)				Op (Max 12)				Op (Max 32)	
10 GIGABIT (PCS)	Op (Max 4)				Op (Max 12)				Op (Max 16)	
40 GIGABIT (PCS)	Op (Max 4)				Op (Max 12)				Op (Max 16)	
Bypass Interfaces	Copper Interfaces				✓				✓	
Transparent- L2 Operation	✓				✓				✓	
LCD Panel	20×2 LCM, 4 Button				20×2 LCM, 4 Button					
Redundant Power Supply	Redundant(275W)				Redundant (600W)				Redundant(850W)	
Dimensions (WxHxD)	431 x 44 x 550 mm				442 x 88 x 660 mm				438 x 88 x 600 mm	
Weight (kg)	8				22				28	
	MODEL E5	MODEL E10	MODEL E15	MODEL E20	MODEL C4	MODEL C6	MODEL C8	MODEL C10	MODEL C20	MODEL C40

Dynamic Threshold Optimization

Threat Level
5 threat levels to decide the configuration hardening
Threat levels set by considering
- attack type
- attack duration
- attack strength

Time
0 minutes depth in optimization

Date
Day of the year optimization
Day of the week optimization

L7 Application Layer Inspection

DDoS IPS
L7 Packet Inspection

IP Classification

IP Reputation Network
Geographical Traffic Classification

Real Time Data Sensors

Anomaly Engine
Proportions
Static Thresholds
Dynamic Thresholds Optimization

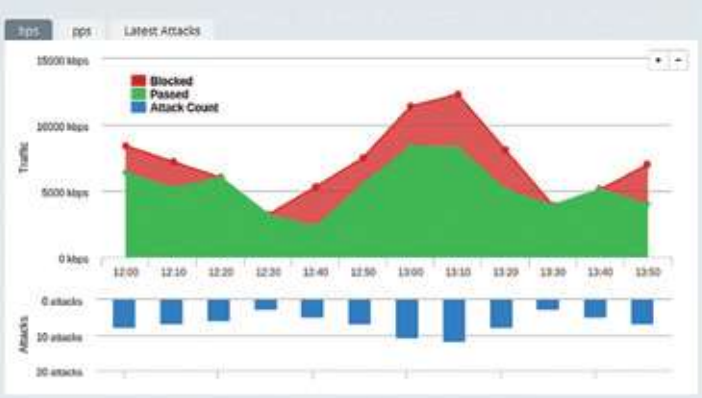
IP Version Stack

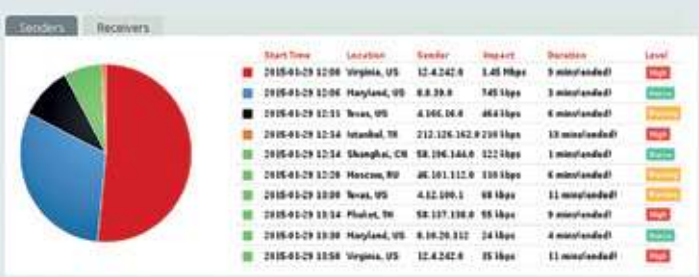
IPv4
IPv6

"HARPP DDoS Mitigator can detect DDoS traffics on real-time for cleaning."

HARPP DDoS Mitigator

During or after the cyber attack, DDoS Mitigator gives you the chance to deeply analyze the attack using the deductive case evidences including attacker IPs, attacker country, attack type and duration.





Defense Functions

Normalization	IP spoof scrubbing Bogon IP scrubbing Botnet zombie determination TCP/IP protocol anomaly scrubbing Packet defragmentation DOS/DDoS packet generator tool blocking Traditional DOS/DDoS tools blocking (Teardrop, land, smurf, fruggle, winnuke, ping of death, oversized ICMP vb.) URPF Automatic aggressive session time-out
Mitigation/ Prevention	Time-out based on attack magnitude Rate limiting Packet dropping IP/Network/Country blocking Ability to provide automatic access only to: specific countries, white list, dynamically identified frequent users if the emergency level is exceeded Challenge Response Page
Protocol-Specific Methods	Robot detection and prevention methods for TCP, UDP and DNS protocols

Preemptive Defense Functions

Coordinated Mitigators	Coordination of associated DDoS Mitigators State, alarm, data, log sharing Automatic ISP notification IP reputation feedbacks Setting Trap IP and port
Individual Mitigators	IP reputation feedbacks Automatic ISP notification Setting Trap IP and port

Case Evidences & Forensic Analysis

Attack Lists	Chronological attack list Chronological subattack list Attack filtering by - interfaces - attack type - attack duration - the beginning of the attack - the end of the attack
Blocked IP Lists	Searchable Blocked IP lists
Case Evidences	Case evidence log file Availability of evidence logs on management screen for investigation Evidence log file (pcap) download support Attacker IP list
Filtering of block lists	Filtering current blockages list by - attacker IP - attacker country - attack type - the beginning of blockage
Alarms and Notifications	E-mail/SMS notification Attack reporting byh e-mail suport Customizable alarms

Management and Reporting

Installation	Installation without changing the topology and any other appliance configuration (L2 inline mode). Installation within complex topologies with L3 router mode installation.
User Interface	Web based dynamic user interface for configuration and monitoring AVS™ (attack visualization system) HTTPS/SSH Secure management support Multilingual management interface Operating system free management platform
Instant Monitoring	Dynamic dashboard with pre-configured graphs (both for WAN and LAN interfaces) Quick picture of the system - Number of connections - Number of states - Number of unique IPs - Packet per second value - Bandwidth per second value - System load
Reports	Ready report templates Reporting engine with parameters
Updates	IP reputation database DDoS signature database DDI™ engine Advanced firmware (Partially Upgradable) No system interruption for firmware/database updates
Logging	Internal logging area Internal evidence collection area Trusted time stamp
Central Management	Remote Syslog Support SNMP Support
Backup	Automatic Configuration Backups Restore The Needed Configuration easily

DDoS CERT

HARPP DDoS CERT is a DDoS specific premium Computer Emergency Response Team (CERT) Service for protecting your business.

There are 6 defined activities in the scope of HARPP DDoS CERT.

Service Activation: Analyzing the existing environment as a whole and plan for HARPP DDoS Mitigator placement.

Tuning: Aim of tuning is to generate Application Anomaly Signatures (AAS) specific to customer services to prevent DDoS and minimalize the false positives.

7x24x365 Monitoring: All HARPP DDoS Mitigator devices are connected to HARPP SOC as a part of this service for ensuring continuous monitoring. Service levels are continuously monitored and incident handling is done with the agreed SLA's.

Attack Mitigation: If there is an incident recognized as DDoS attack, this is immediately seen by HARPP DOS CERT Team and attack mitigation starts.

Monthly Service Review: This part of service ensures that HARPP DDoS protection is updated with the changes on the applications itself and the user/client characteristics.

HARPP CERT Team reviews customer environment on a monthly basis and ensures that DDoS protection is effective and not causing false positives.

Post Incident Reporting: After major incidents, there is a specific report prepared as a result of that event.

CWL
cyber warfare lab

In information security, speed is an important aspect in order to rapidly take appropriate measures to develop a solution against current threats, and also in anticipating emerging threats.

Due to the very widespread use of the internet, and reduction in the prevalence of closed-circuit networks, we can observe that the "Cyber War" concept (once seen only in science fiction movies) has become a part of our daily lives. Not just individuals or Corporations, but also Countries are trying to harm each other, or obtain valuable information through cyber crime.

It is therefore essential to continually improve your protection systems, ensure your knowledge is relevant and up-to-date, and to take appropriate measures in advance in order to eliminate the constantly changing threat. There is a need to move faster and keep ahead of the "Cyber enemy", anticipate & eliminate potential dangers by thinking like them. In our "Cyber Warfare Intelligence Lab" we are researching, simulating and then developing the most important analysis and decision components of our cyber defense tools, specific to your environment.

Our aim is to develop and prepare measures by anticipating future developments and to avoid being caught unprepared of new threats. The HARPP DDoS Mitigator anti-DDoS appliance comes from this laboratory and is developed by our extensive R&D team. Our highly qualified and expert team will continue to anticipate future threats and enhance our security products appropriately, providing you with a level of support that you can trust.

Security Operations Center

In our Security Operations Center (SOC), we closely monitor your devices, cyber attacks, and security events. Our teams that include Cyber Warfare Lab (CWL) staff , analyze possible security vulnerabilities and make provisions. Thus, we protect what's valuable for you with our provisions and the technology developed by us.

www.harppddos.com
Cyber Warfare Intelligence

7 • 24 • 365
GLOBALSUPPORT

HARPP
ddos mitigator