HARPP
ddos mitigator

www.harppddos.com

HARPP DDoS Mitigator Appliances and DDoS CERT

provide cyber warfare intelligence with its best-of-breed DDI™ (Deep DDoS Inspection) technology for full protection of your network, web applications and services ensuring your online operations' continuity.

Cyber Warfare Intelligence

How to protect a million dollar?

DDoS attacks have evolved for over the last 10 years becoming more sophisticated and significant threat to critical public-facing web operations. Ultimately, the perpetrators' motivations are more alarming for a wide range of organizations including online money-making operations, critical public infrastructures, enterprise networks, e-government operations and agencies.

Any organization that conducts online business or has distinctive investments in their online reputation is a potential target. While many organizations are highly concerned about the DDoS threat, few organizations have specific tools for detecting and defeating the attacks completely.

Despite popular belief, the traditional stand-alone measures such as Firewall/IPS appliances implemented within most organizations or the recommended solutions of Internet Service Providers (ISP) and cloud scrubbing centers are insufficient to detect and mitigate today's highly sophisticated attacks.

Wisdom is The Power

A Dedicated Appliance + Security Intelligence

As the sophistication of the DDoS attacks is increasing day by day, the intelligence level of detection and defense systems gain much importance to be protected against these cyber weapons. The three main features of the DDoS attacks are frequency, size and complexity. Since the frequency can be controlled only by the attackers, DDoS protection solutions focus on the remaining two challenging attack features: size and complexity. The best solutions to solve the size issue are bandwidth over provisioning and service providers' traditional and limited protection tools that ignore sophisticated application level – Layer 7 attacks. When we have a deep look at the size issue, the researches show that 75% of the DDoS attacks are “Low and Slow Attacks" under 1 Gbps attack traffic which is enough to make your web infrastructure down. To avoid the devastating results of such DDoS attacks, there need to be a dedicated appliance and service which is capable of detecting and mitigating a wide variety of DDoS attacks including TCP, UDP, HTTP, ICMP, SMTP, VOIP and application level specific attacks.

Detection

DDI™ (Deep DDoS Inspection) Technology

DDoS Mitigator's DDI (Deep DDoS Inspection) Technology is designed to be your intelligent shield against DDoS attacks with Advanced Persistent Threat (APT) capabilities. By its Best-Of-Breed anomaly engine with heuristic andnon-heuristic algorithms supported by 34+ data sensors an innovative proportions feature based on historical data collections and timely averages, unpredictable DDoS traffics can be detected on real-time for cleaning.

Real-time Inspection	Real time traffic analysis In time decision before DDoS floods reaches to firewall
Data Sensors	34+ data sensor groups under 4 categories Advanced configuration tool to make sensors fully controllable L7, application level sensors
Static Thresholds	By default generic static thresholds experienced in different types of networks, traffics and attacks
Dynamic Threshold Optimization	Automatic optimization of sensor thresholds based on *threat level *historical records archived on sensors
Proportions	Network Memory (Historical Data Collections) Averages (annual, seasonal, monthly, daily,..)

Anomaly Engine	Heuristic and non-heuristic algorithms that use data sensor averages Source determination of anomalous traffics
Geographical Traffic Classification	Country based filtering IP Block based filtering
IP Reputation	IP reputation database queries 5 level exception lists (white and black lists)
DOS IPS	DDoS pattern signatures for attacks using application and system vulner abilities
Deep Packet Inspection Firewall	L7 Packet Inspection Stateful Packet Inspection Bandwidth Management Ipv6 support

Data Sensor Categories

TOTAL PACKETS	TOTAL CONNECTIONS	TOTAL CLIENTS	DEEP DoS/DDoS INSPECTION (DDI)
Incomming packets	TCP connections	TCP clients	DNS deep DoS/DDoS inspection
Outgoing pockets	UDF 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	TimeWait connections	TimeWait clients	L7 IPS sensors
IPv4 packets	TCP SYN connections	FinWait clients	
IPv6 packets	TCP other flags	TCP SYN clients	
Incoming bandwidth		TCP other flagged clients	
Outgoing bandwidth			

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

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

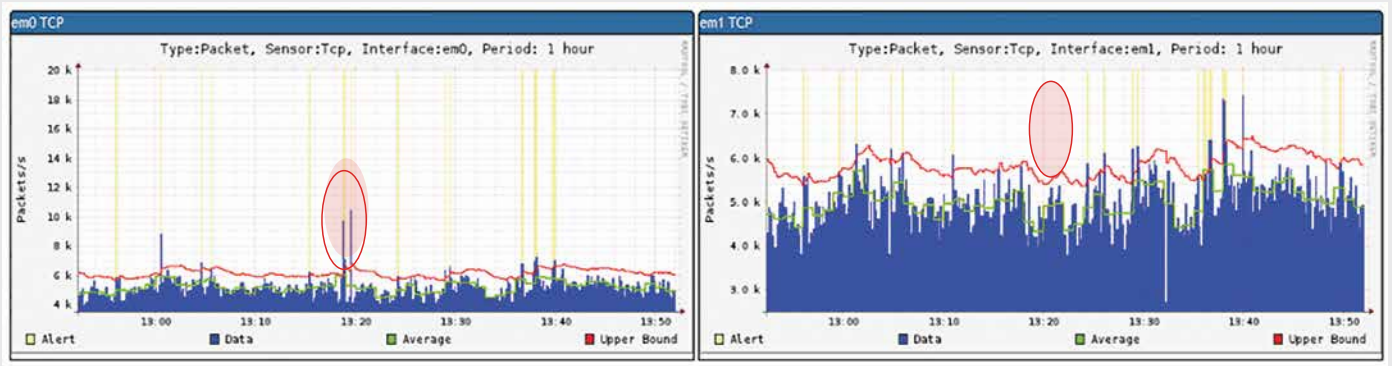
IP Version Stack

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.



Defence

DDoS Mitigator Appliance is the first level of protection for your network against cyber attacks ensuring online business continuity with minimum TCO. In addition to state-of-the-art defense functions providing high-level protection to your web and DNS infrastructure by its normalization, protection and protocol-specific security tools, preemptive defense functions are continually active day and night. DDoS Mitigators all around the world create a wide security intelligence network you can access in real-time which is one of the key-differentiators.

Management

One of the key-advantages of DDoS Mitigator is its steerable and instantly tunable structure. During an intelligently-designed and complex DDoS attack, having a dynamic dashboard that visualizes the dynamic attacks is extremely important. DDoS Mitigator's AVS™ (Attack Visualization System) provides multidimensional graphics where the deep attack characteristics can be fully monitored and analyzed to take the right steps in the possible shortest time.

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, dynamicaly identified frequent users if the emergency level is exceeded Challenge Respose 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

Management and Reporting

Installation	Installation without changing the topology or any other device configuration (no-change-deploy™) 'Install-as-a-router' Support Interoperable with all standards-compatible network ' devices
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

"While many organizations are highly concerned about the DDoS threat, few of them have dedicated tools for detecting and defeating the attacks completely. Despite popular belief, the traditional stand-alone measures such as Firewall/IPS systems and reliance on Internet Service Providers (ISP) or Cloud Scrubbing Centers are insufficient to detect and mitigate today's highly sophisticated attacks."

HARPP DDoS Mitigator

Defence

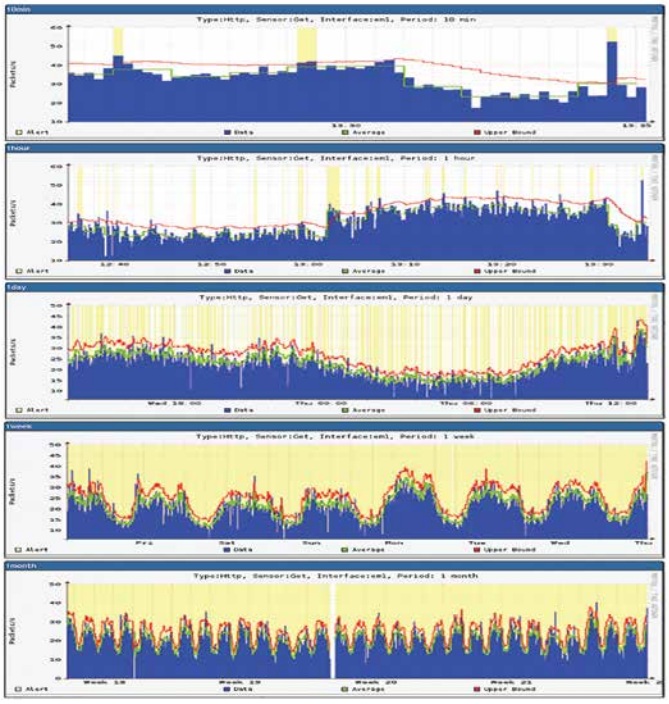
Case Evidences & Forensic Analysis

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 by E-mail Support Customizable alarms

Management

Management and Reporting

Central Management	Remote Syslog Support SNMP Support
Backup	Automatic configuration backups Restore the needed configuration easily



Popular Misconceptions

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

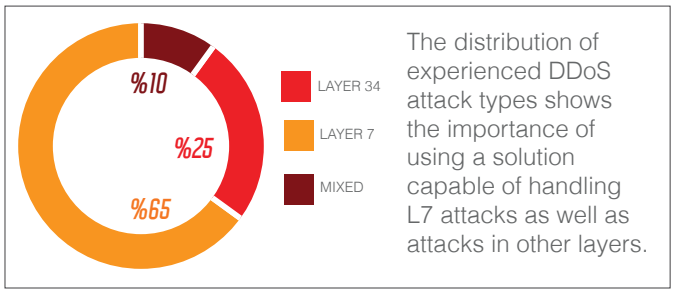
You're not safe. Actually, you've already been a part of the problem. Since the the DDoS attack is caused by overloading, the inline appliances that you trust such as Firewall or IPS with limited processing performance and number of concurrent sessions will cause the bottle-neck. You need a dedicated high-performance DDoS appliance to stop DDoS attacks before reaching interior network 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

It's better to fully outsource the DDoS protection job.

The reality: DDoS Attacks are the latest warfare tools based on cyber world. Whether you're an organization in military sector or a mediumsized enterprise there is always a high-risk to outsource the IT security issue, especially DDoS. Considering the fact that today the cyberattacks are used or backed by governments, directing your internet or web traffic to the cloud data centers located in other countries doesn't sound secure and solution to rely on.

Cloud or ISP Scrubbing Centers can protect my web infrastructure.

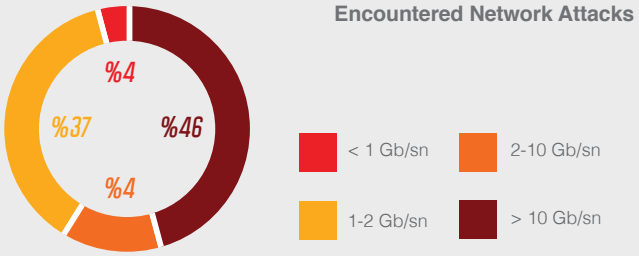


The distribution of experienced DDoS attack types shows the importance of using a solution capable of handling L7 attacks as well as attacks in other layers.

You're not safe. Actually, you've already been a part of the problem. Since the the DDoS attack is caused by overloading, the inline appliances that you trust such as Firewall or IPS with limited processing performance and number of concurrent sessions will cause the bottle-neck. You need a dedicated high-performance DDoS appliance to stop DDoS attacks before reaching interior network appliances.

Organizations need to be ready for enormous volumetric attacks.

Recent studies show that attackers today are a lot more sophisticated requiring providers to become increasingly resourceful in their countermeasures. Although some online businesses incur intensive DDoS attacks (over 1 Gbps), many more organizations never experience a high-level volumetric attack. These organizations are taken down by less intensive, but equally critical attacks.



cyber warfare lab

In information security, speed is the most important point to take measures and build solution against the threats by anticipating emerging threats beforehand. Due to very widespread use of the internet and reduction of the prevalence of closed-circuit networks, we observe that “Cyber War” concept that we were watching in science fiction movies previously became a part of our daily lives from now on. Not only individuals or corporations, but also countries are trying to harm each other or obtain valuable information by this way.

It is essential to improve yourself constantly, keep your knowledge up to date and take measures in advance in order to eliminate the threats. It is required to move faster and before the enemy, eliminate the dangers by thinking like it. In “Cyber Warfare Lab”, we are developing the most important analysis and decision components of cyber defense tools, specific to Turkey, by following other cyber threats and propagations in the world. Our aim is to take measures by anticipating developments beforehand and prevent to be caught unprepared against threats. HARPP DDoS Mitigator which is Turkey’s first anti-DDoS appliance has come out of this laboratory and is developed by our R & D team. Our expert team especially qualified in points where attackers are threatening the institutions or governments via the internet with the DDoS attacks, stands by the customer with all its expertise.

Winner Solution

A Dedicated Appliance + Security Intelligence

DDoS MITIGATOR APPLIANCE	MODEL T	MODEL T1	MODEL E	MODEL C
Appliance Form	Rackmount	Rackmount	Rackmount	Rackmount
PPS (PacketsPerSecond)	100.000	250.000	600.000	3.000.000
Max Concurrent Sessions	10.000.000	10.000.000	20.000.000	50.000.000
100/1000 Ethernet (PCS)	6 (Max 10)	6 (Max 10)	12 (Max 20)	8 (Max 24)
Gigabit SFP Port (PCS)	Op (Max 2)	Op (Max 2)	Op (Max 8)	Op (Max 12)
10 GIGABIT (PCS)	Op (Max 2)	Op (Max 2)	Op (Max 4)	Op (Max 12)
Internal Log Capacity	500 GB	500 GB	500 GB	1 TB(RAID 0+1)
LCD Panel	20x2 LCM, 4 buttons	20x2 LCM, 4 buttons	20x2 LCM, 4 buttons	20x2 LCM, 4 buttons
Redundant Power Supply	Optional	Optional	Redundant(275W)	Redundant(500W)
Dimensions (WxHxD)	431 x 44.4 x 415 mm	431 x 44.4 x 415 mm	431 x 44 x 550 mm	442x88x660 mm
Weight (kg)	8	8	12	22

www.harppddos.com

Cyber Warfare Intelligence

Galyum Binası, 1. Kat, No:23, Teknokent-ODTÜ Ankara/Türkiye
T . +90 312 2101490 (Pbx) F . +90 312 2101492 info@harppddos.com

7 • 24 • 365
GLOBALSUPPORT

HARPP
ddos mitigator