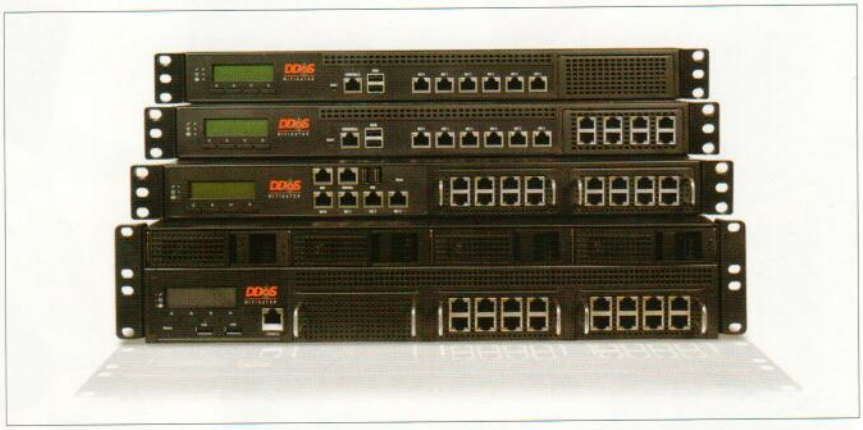
Get Protected Against the Most Disruptive Cyber Warfare Tool with DDOS Mitigator

As Turkey's #1 Cyber Security vendor, Labris Networks Inc. is proud to announce its latest cyber warfare defence tool: DDOS Mitigator Appliance

Distributed Denial of Service (DDOS) attacks have been evolving over the last 10 years. The impact of these attacks on critical infrastructures have been increasing day by day. Such impact is created by many elements such as the intelligence level of the attackers, strong attack motives and advancement of the attack technologies which is claimed to be backed by the governments.



What to know about DDOS Attacks

A basic denial of service (DOS) attack involves bombarding an IP address with large amounts of traffic. If the IP address points to a Web server, then it may be overwhelmed. Legitimate traffic heading for the Web server will be unable to contact it, and the website becomes unavailable. Service is denied.

A distributed denial of service (DDOS) attack is a special type of denial of service attack. The principle is the same again, but the malicious traffic is generated from multiple sources – although orchestrated from one central point. The fact that the traffic sources are distributed – often throughout the world – makes a DDOS attack much harder to block than one origination from a single IP address.

How to get protected against DDOS Attacks

The DDOS attack seemed to be an unsolved issue because of its chaotic structure however recent technological developments led cyber security teams to mitigate the risk of online unavailability. "Mitigation" is the right word because one should keep in mind that there can be always a huge attack to make your services unavailable for some time.

Although many local Internet Service Providers (ISP) provides the DDOS mitigation service whereby DDOS attack identification and mitigation occurs within ISP's IP backbone before it reaches the customer's network, now it's widely accepted that it's not enough to rely on ISP only. Recently, the commonly accepted concept is the hybrid approach which combines the advantages of network perimeter based solutions – dedicated DDOS Mitigator Appliances – as well as ISP-based solutions. The reason of using DDOS Mitigator Appliances is the insufficiency of ISP solutions about preventing the malicious traffic under 1 Gbps. ISP Scrubbing Centers were designed to mitigate the attacks over 1 Gbps or what we call "volumetric attacks" where the threshold values are used to identify the malicious DDOS traffic, however according to the latest researches, around 40% of the attacks worldwide are named as non-volumetric attacks under 1Gbps.

Identifying DDOS traffic is the first stage of defence. DDOS Mitigator Appliances are not only using threshold values on inbound-outbound traffic, but also using the advantage of 34+ different data sensors (TCP, UDP, ICMP, HTTP GET, HTTP POST, TCP SYN etc..) for the first phase of decision-making process. The worldwide IP reputation databases identifies the black IP's and dropping the packets which is the second phase. In this phase, the geographical traffic blocking allows you to block the traffic originated from irrelevant countries/regions which can help much during state-sponsored cyber-attacks. The third and the most important phase is performed by the Anomaly Engine having unique Deep DDOS Inspection technology which is scanning the traffic with heuristic / non-heuristic algorithms, network memory and timely averages, deciding if the traffic is benign or not, in only milliseconds.

After the attack, the evidence file can be printed out from management interface screen on which you can work. The IP addresses, countries of the attackers or the attack type, target service, start-end time can be seen for further investigation.

In order to mitigate the DDOS attack, the IT security tools are not always sufficient; focused Security Emergency Response Teams should be established and kept up-to-date for today's latest attack scenarios. Moreover, Advanced Persistent Threat (APT) level attacks force victims to get in direct touch with the vendor's research labs during the attack. The customer and the vendor are advised to get in touch not only during the attacks but also before the attack. The chosen vendor should be transferring the necessary knowledge to the customer

DDOS MITIGATOR