



GLOBALCOM
DATA SERVICES

GLOBALCOM
DATA SERVICES

DDOS PROTECTION

Prevent **DDOS** attacks and
stay online
with our advanced
security service



The Distributed Denial of Service (DDOS) attacks have become more complex and easier to launch than ever before. These attacks combine high volume traffic, with slow, low and application-targeted techniques.

GDS DDOS mitigation is a service delivered via the cloud to detect and mitigate all types of attacks in real time. This occurs in coordination with our partners: Arbor/BT, an industry leading for DDOS attack mitigation. GDS security experts are available 24x7x365 to keep your business online during a DDOS attack with comprehensive multi-layered L3-L7 DDOS attack protection.

KEY BENEFITS

Keep your business online during a DDOS attack

By using real-time, DDOS attack detection and mitigation in GDS cloud, you can stop DDOS attacks before they affect your network and your business.

Protect against all DDOS attack vectors

GDS service is engineered to respond to the increasing threats and complexity of DDOS attacks – and, to offer multi-layered L3–L7 DDoS attack protection against all attack vectors. GDS service offers also offers a daily update for the protection plan implemented on GDS platform to preserve the same level of security.

Get details of the attack mitigation

A customer portal is built on GDS cloud to provide transparent attack mitigation visibility and reporting before, during, and after an attack.

Get expert service

GDS in coordination with Arbor/BT Security Operations Center (SOC) experts are available 24x7x365 with optimum service SLAs for uptime and prompt response to DDOS attacks.

COMPREHENSIVE GDS DDOS FEATURES

Complete Attack Protection

GDS DDOS Solution provides a protection against a wide variety of attacks including the below:

DEFENSIBLE ATTACKS

VOLUMETRIC

ICMP and UDP Flood, spoofed-packet floods, NTP, DNS and Chargen amplification...

STATE EXHAUSTION/PROTOCOLS

SYN flood, Teardrop, Smurf, Ping of Death, Mixed Flood, Fin Flood, RST Flood, fragmented packet attacks...

APPLICATION AND LAYER 7

Slow-and-low attacks, GET/POST Flood, DNS, SMTP, SIP, Slowloris, known signature attacks... attacks that target webserver and operating system vulnerabilities

The size of the volumetric attacks can reach up to 700Gbps without affecting your network.

Service Subscription

GDS DDOS solution provides a 1-to-3-year service subscription with flexible options:

DEPLOYMENT AND SERVICE METHODS

ALWAYS ON

The Always On subscription blocks bad traffic from reaching your network.

It continuously processes all traffic through the cloud-scrubbing center, and only returns legitimate traffic to your site.

ALWAYS AVAILABLE WITH LIMITED NUMBER OF MITIGATION

The Always Available subscription runs on standby – and can be initiated when under attack [for a specific number of monthly attacks].

ALWAYS AVAILABLE WITH UNLIMITED NUMBER OF MITIGATION

The unlimited number of mitigation services per subnet prevents you from paying additional fees if you encounter more attacks than originally defined.

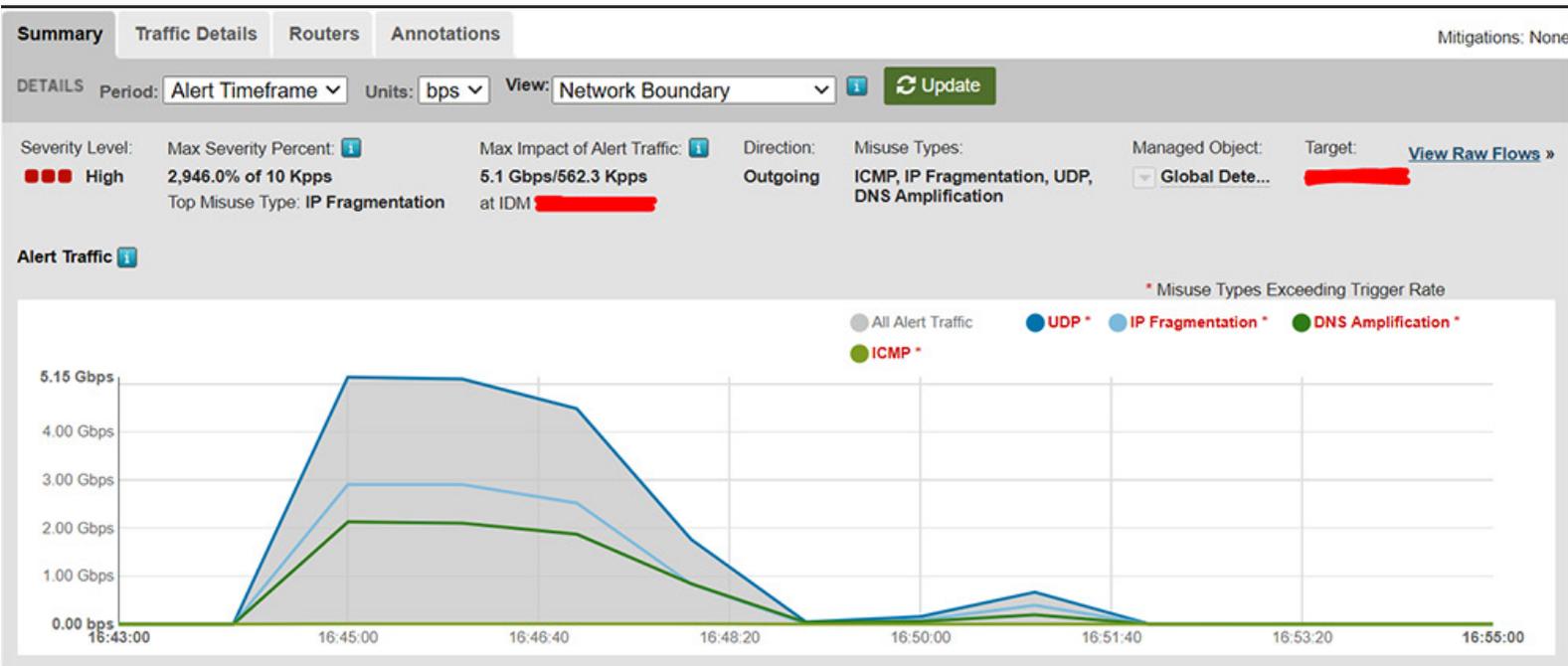
IP BLOCKING

Blocks the IPs based on customer request.

PROACTIVE MONITORING

Monitors the mitigation start-up and notifies the customer [during 24x7 hours] about the status of the process.

Reporting and Visibility

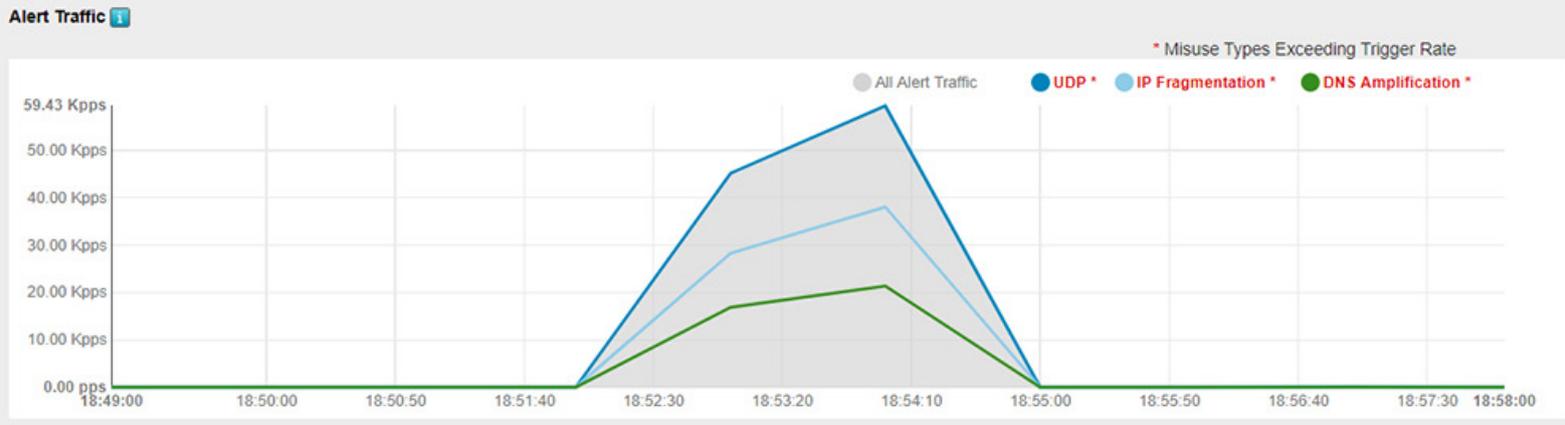


With transparent attack visibility and mitigation, GDS provides a web portal to check the details of the attacks as it occurs – the web portal also checks the type and size, IP origin, attack vector mitigation process and all actions taken by GDS security teams.

In addition, access to a portal is provided to the customer (or automated reports) that includes similar information with regard to the volumetric attacks.

With a combined service [report and access to portal], the customer will have full visibility on the attack status and details.

DETAILS Period: **Alert Timeframe** Units: **pps** View: **Network Boundary** Update
 Severity Level: **High** Max Severity Percent: **525.0% of 10 Kpps** Max Impact of Alert Traffic: **877.7 Mbps/84.4 Kpps** Direction: **Incoming** Misuse Types: **IP Fragmentation, UDP, DNS Amplification** Managed Object: **IDM-Supernets** Target: **[REDACTED]** [View Raw Flows >](#)
 Top Misuse Type: **IP Fragmentation** at **[REDACTED]**



Alert Characterization

Misuse Types	UDP (9)	100.00%
Misuse Types	IP Fragmentation (1)	63.35%
Misuse Types	DNS Amplification (11)	36.55%
Source IP Addresses	Highly Distributed	99.90%
Destination IP Addresses	[REDACTED]	100.00%
Protocols	udp (17)	100.00%
Source UDP Ports	0	63.35%
Source UDP Ports	53 (domain)	36.55%
Destination UDP Ports	0	63.35%
Destination UDP Ports	1024-65535 (Dynamic)	36.05%
Source ASNs	NULL (0)	100.00%
Destination ASNs	NULL (0)	100.00%

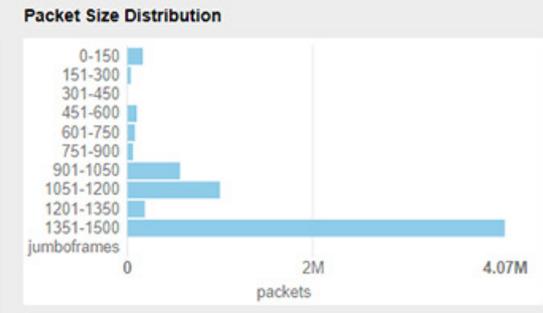


Figure-1: Reports regarding a volumetric attack

Products Available and Service SLA

The available products offered with combined service are listed below:

MITIGATION TYPE	ATTACK TYPE	SLA	NUMBER OF ATTACKS	SIZE OF THE ATTACKS	LOCATION OF THE SCRUBBING CENTER
Always ON	Slow and Low	Immediate - 1 Minute	Unlimited	Unlimited	On GDS data center
Always available	Volumetric	Layer 7 attacks < 7 minutes	Unlimited	Unlimited	On Arbor Cloud

GDS STRONG PARTNERSHIP



Since 2015, GDS has extended its expertise to its enterprise and corporate customers by offering fully a managed security solution. GDS collaborated with a BT, a cooperative and respectful partner, for two main reasons:

- Due to the increase in complex attacks in Lebanon
- To facilitate engagement of security as a service for managing infrastructure security

About BT Security

With a global network incorporating over 195 countries, BT has an enviable view of the trends and types of activities that occur over the Internet. This telemetry allows a unique level of analysis. A significant cyber-capability is created when this visibility is combined with a team of highly skilled and well-funded cyber-experts. This manifests itself in disciplines, including threats cape mapping, cyber-response and cyber-operations development.

BT has a network of 14 Security Operations Centers (SOCs) across several locations around the world. Customer devices are managed and monitored – and security analysts are available to provide around the clock, real time support and response services to protect your networks. BT SOC's have maintained 100% uptime since operations began. To provide the assurance of the highest quality of service, the SOC's are accredited and audited variously to (ISO 27001) and auditing (SSAE16 and ISAE3402) standards, and where appropriate to Government information assurance standards.

BT, in coordination with Arbor, provides GDS the best combined DDOS mitigation solution.

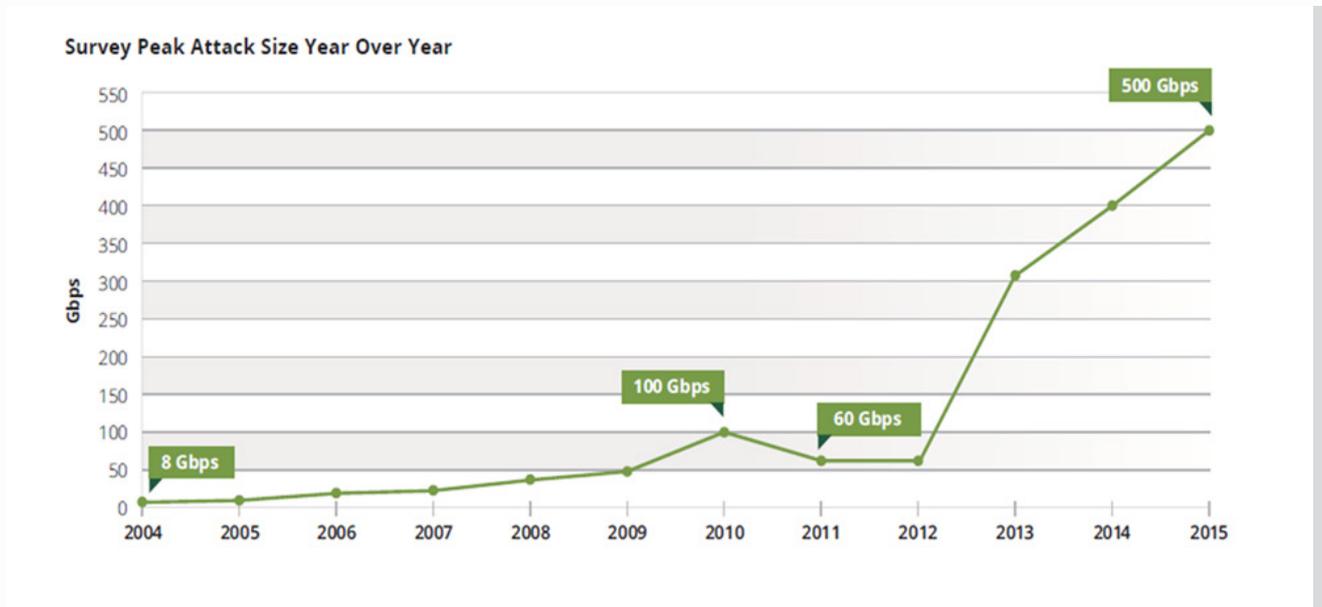


About Arbor Security

Arbor provides the most comprehensive suite of DDoS attack protection products and services for the Enterprise, Cloud / Hosting and Service Provider markets.

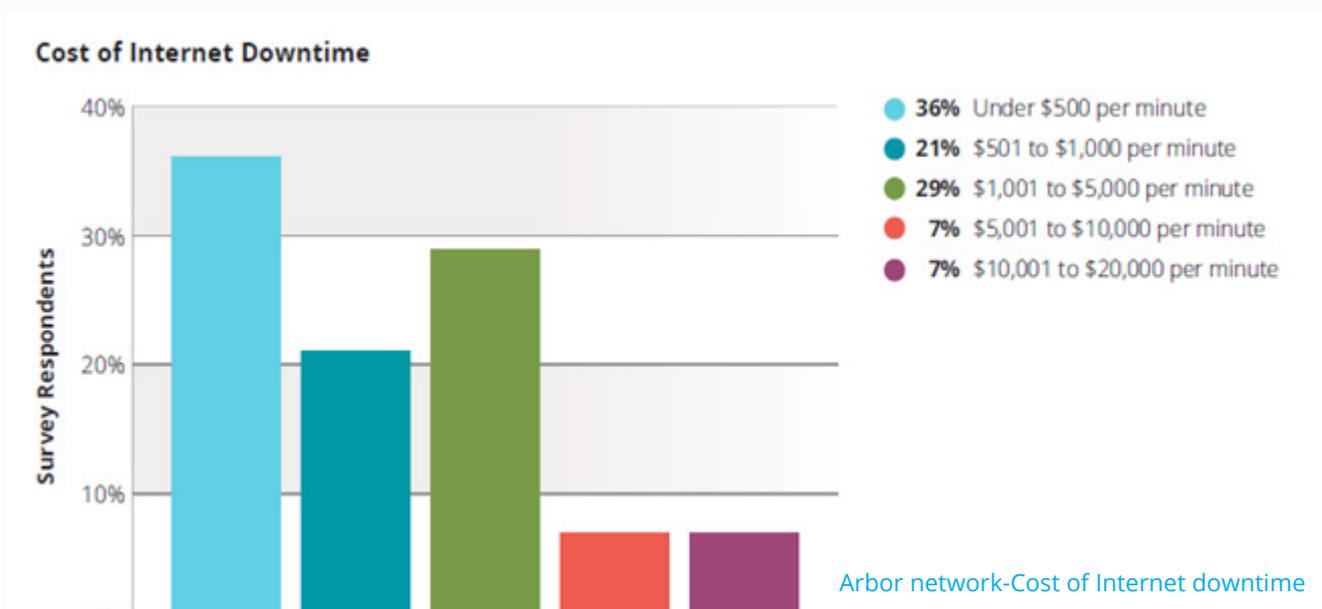
Facts and Figures from Arbor

- The peak volumetric attack detected by Arbor is 500 Gbps



Arbor network-Peak attack Size

- The consequences of a successful DDOS attack can be devastating – e.g., millions of dollars in lost revenue or damage to a company's brand.



Arbor network-Cost of Internet downtime

- The number of threats continue to grow: Approximately 50 million attacks per year, resulting in one or two attacks per second

GDS GLOBAL SERVICES

GDS offers advanced support, training and consultancy to help you get the most out of GDS DDOS service.

For more information about the service, please contact: sales@gds.com.lb



To learn more about GDS and our security portfolio, visit www.gds.com.lb

Globalcom Data Services sal
Holcom Bldg., 4th floor
Corniche Al Nahr, Beirut, Lebanon
Tel: +961 1 59 52 59
info@gds.com.lb

About Globalcom Data Services sal

Operating since 1996, GDS is deemed one of the first Data Service Providers in Lebanon to provide modern and fast connectivity across the country.

GDS leads the way to the future by consistently supporting new technologies for over 20 years.

GDS provides a comprehensive security services portfolio by building on its extensive network and security expertise.

A team of security experts is available to assist customers with complex security threats and cyber-attacks that may potentially affect their businesses long-term.