

Application Note

DDOS MITIGATION WITH EXAWARE

Exaware DDoS Mitigation Solution

Protect your network from the most aggressive DDoS attacks using Exaware Dynamic Filtering at the Peering Point (DFPP)

Exaware DFPP is a solution enabling Communication Service Providers to extend their DDoS mitigation capabilities at the edge of their network.

DFPP comes to complement your existing lines of defense against DDoS attacks to ensure that most of the unwanted traffic stays out of your network and that your customers can continue to enjoy their services.

The Challenge

Medium Businesses, Global Organizations and Communications Service Providers are constantly challenged by repetitive cyber-attacks, which cost massive amounts of money in lost revenues and reputation, compensation for unhappy customers and heavy manpower to address these attacks.

Today's mitigation systems often work in isolation from the other elements in the network. They hardly combine to provide a global view and understanding of the source and the nature of the attack. Security teams are also separated from network teams making it harder to coordinate actions at times of cyber-attacks.

These issues result in challenges to identify the attacks and properly stop them.

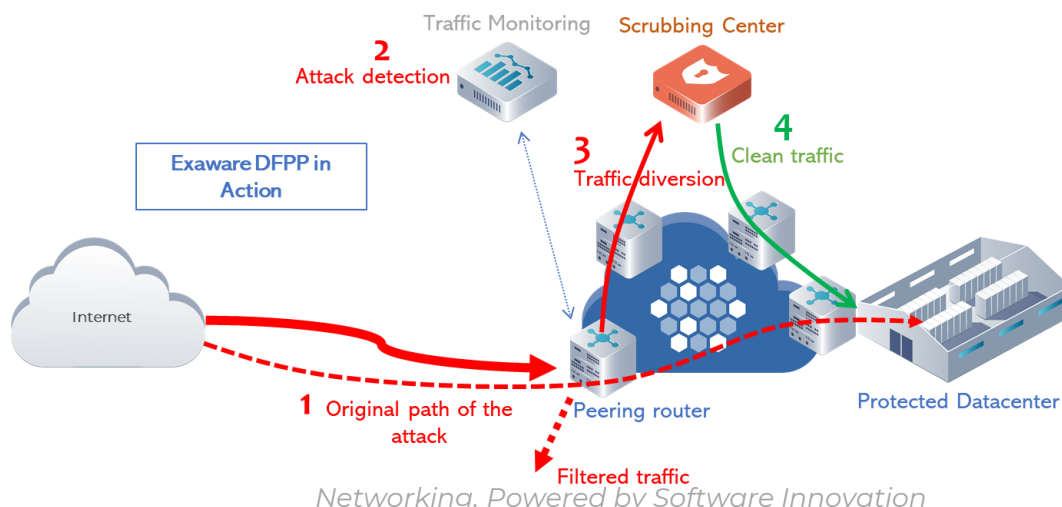
Exaware DFPP Solution

Exaware has developed a solution to enable its peering routers to filter identified attacks at the peering points, in real-time, at scale and supporting rapid changes, to match the rapidly changing conditions of DDoS attacks.

All traffic identified by your current DDoS mitigation systems as being attacks are filtered on the peering router and dropped outside of the network, before they can even get in and impact your customers.

DFPP Benefits

- Efficient against all DDoS Volumetric attacks
- Keeps your network clean of unwanted traffic
- Provides visibility into DDoS attacks
- Time to mitigation under 1 minute
- Adaptive filtering changes rapidly to block new attacks



You can choose between fully automatic, semi-automatic or manual filtering and decide how much control you want to keep.

You define the network segments you want to protect and set your own rules for each segment. Each segment can be one of your customers or a set of servers in your Datacenter, in order to set different priorities based on the sensitivity of the segment and apply different policies.

The system monitors the traffic and triggers the mitigation when the volume of traffic exceeds a defined threshold, above the baseline traffic. DFPP will monitor both bit per second and packet per second.













When the attack is identified, DFPP will send filter commands on the source IP address, destination IP or both to Exaware peering routers.

A whitelist is also available, on IP addresses or AS numbers.

DFPP offers a number of mitigations on the router:

- Policy-Based Routing (PBR); routing configuration is dynamically changed based on the attacks identified and the router can typically send the traffic to a scrubbing center.
- BGP Flowspec; the router will filter or throttle traffic based on Flowspec commands coming from the mitigation systems.
- RTBH (Remotely-Triggered Black Hole); the attack traffic will simply be discarded by the router before it gets into the network.

DFPP provides detailed reports of the attacks, such as time of the attack, duration and statistics on the traffic.

Attack list									
All <input type="text" value=""/>									
Active attacks 1									
ID	STATUS	TIME		TARGET	ACTION STATUS			ACTION	
#1245	Active	12:38 2019-11-01	NOW	 AS Numbers autodetect GENERAL	Detected	Not Active	Detected	 START MITIGATION	
Attacks with active mitigation 0									
Ended attacks 1232									
ID	STATUS	TIME		TARGET	ACTION STATUS			ACTION	
#1244	Ended	12:10 - 12:14 2019-11-01		 AS Numbers autodetect GENERAL	Detected	Not Active	Ended	 ATTACK DETAIL	
#1243	Ended	11:28 - 11:31 2019-11-01		 AS Numbers autodetect GENERAL	Detected	Not Active	Ended	 ATTACK DETAIL	
#1242	Ended	11:08 - 11:17 2019-11-01		 AS Numbers autodetect GENERAL	Detected	Not Active	Ended	 ATTACK DETAIL	

Exaware Internet Peering solutions

ExaDOS is the powerful Network Operating System behind Exaware routing solutions. Built from its inception with carrier scale in mind, ExaDOS delivers all the features and the performance required for the most demanding peering points.

ExaDOS is an Open NOS, which means you can connect your applications with your network and enable brand new services.

Non-Redundant “Pizzabox”

800G, 2.4T (Q-MX/2C, Q2A)
4T (Jericho2)



800G to 4T

Redundant Back-to-back

Active/Standby solution for
mid-size bandwidth.

Jericho/Jericho2C/2C+



4.8T to 8T

Redundant Distributed Chassis

High scale based on DNX technology
Modular line cards - J2/J2C/J2C+
Modular fabric - Ramon



Up to 1300T



Cloud architecture

- Modern software architecture
- Cloud architecture for flexibility and dynamic scale



Complete set of Peering Solution

- Multiple hardware platforms from major Hardware vendors
- Flexibility to customize your network to your needs



Carrier Grade

- ExaDOS is the result of a decade of development
- Deployed among several Tier1 service providers



Reduced TCO

- From plan-ahead (chassis) to Pay-as-you-grow
- Generate new stream of revenues, with 3rd party Applications
- Break the chains of vendor lock-in

CONTACT US



www.exaware.com



info@exaware.com



+972-73-2124500