Network **Security** Solutions

PolyNet DDoS Defense Mitigation System

The safest choice against DDoS attacks

POLYNET
Perfect Timing

In an ever-changing cybersecurity landscape where the types and intensities of Distributed Denial of Service (DDoS) attacks can vary significantly, data center operators, network providers and enterprises need a defense that is not only effective, cost-efficient, and easy to manage, but also adaptable to different network architectures and security strategies. **PolyNet's DDoS Defense Mitigation System** combines these key features to protect against DDoS attacks and ensure the continuous availability and security of your online services.

Benefits

- Protection against attack varieties, including volumetric, application layer, and protocol-based attacks
- Cost savings by minimizing the need for emergency response and recovery efforts
- Enhanced service availability
- Helps you meet compliance requirements and data protection regulations by maintaining service availability and data integrity
- Improved user experience

Key Features

- Easy integration, ensuring minimal disruption to existing infrastructure
- Flexible deployment without any inline components
- On-site traffic scrubbing ensures that only clean data reaches your network
- Swift response time: More than 99% of all DDoS attacks are detected and mitigated within milliseconds
- Automatic mitigation, enabling immediate action without human intervention

POLYNET
Perfect Timing

Network **Security** Solutions

PolyNet DDoS Defense Technical Data

Simultaneous Sessions	Not limited
Detection Modes	SPAN monitor, ERSPAN monitor, Passive Inline
Mitigation Modes	BGP redirect, BGP Flowspec redirect to scrubber, BGP Flowspec rate-limiting, BGP community-based filtering
Transit Link Mitigation	Automatic eBPG signaling (BGP/Flowspec)
Attack Protections	Reflection floods: DNS, mDNS, NTP, SQL, CLDAP, RIP, WSD, CHARGEN, SSDP, SNMP, ICMP, CoAP, NetBIOS, Memcached, TFTP, Sentinel, RPC, RDP, IPsec, L2TP Fragmentation floods: Generic, Nestea, Jolt, Targa, Teardrop TCP floods: SYN flood, RST, FIN, ACK, PSH-ACK, URG, Anomalies Basic app floods: HTTP get, post, SIP, SQL
Scrubbing Actions	Filtering/rate-limiting: Malformed packets, Geo IP, User-defined black/whitelists through RESTapi (Maximum 500,000 user defined IP range) Threat intelligence exchange: Curated, aggregated threat intelligence feed from multiple exchanges. Automatic daily update TCP authentication: Transparent TCP Syn proxy, only requests from RFC compliant TCP stacks are forwarded to the end-point. TCP flag filtering Per-client and per-server transaction rate-limits: DNS, SYN, HTTP, HTTP2 Malformed application request filtering: HTTP
Detection interface	Nx4x10Gbps 14.88Mpps/10GbE or Nx2x40/100Gbps 110Mpps/100GbE Maximum of 400Gbps/server
Mitigation interface	Any combination of 10(10Mpps)/25/40(30Mpps)/50(30Mpps)/100(50Mpps)GbE interface Maximum of 800Gbps/server
Average detection lag	10ms
Scrubbing added e2e lag	1ms
Power Requirements	Two 2200W redundant PSU
Power consumption	600W-1200W based on configuration
Dimensions	Chassis: 2U Weight: 20-25kg Dimensions (D x W x H): 32.71" x 17.25" x 3.43" (831 x 438.4 x 87mm)
Management Interfaces	2x 1/10GbE + 1GbE IPMI
Sample Storage	2TB NVMe SSD storage for network traffic
Environmental	10°C ~ 35°C (50°F ~ 95°F) Max 90% Humidity
Regulatory	FCC (SDoC) Class A CE (DoC) Class A CB/LVD Yes RCM Class A VCCI Class A

PolyNet Telecommunications Consulting and Contractor Ltd.
Bojtar utca 17, Budapest, 1037 Hungary | Phone/Fax: +36 1 250 7725 | www.polynet.eu | Email: info@polynet.eu