Datasheet

# Viettel Anti DDoS Volume Based Solution

viettel security

## Viettel Anti DDos Volume Based Solution

Anti DDOS Volume Based is the solution to minimize bandwidth denial-of-service attacks that congest uplink traffic of clients and affect services or network leading to widespread service loss.

## Necessity of Anti DDOS volume based solution

DDOS attacks have been increasingly diverse in scale and purpose, which are not merely acts of sabotage against systems for personal purposes but also organized attacks fueled by economic and political motivations. Types and scale of attacks are increasingly diverse and complex.

Hackers may use terminal errors, launch various types of attacks to mobilize high-volume attack streams ranging from a few Gbps to several tens of Gbps:

- Types of attacks includes UDP flood, ICMP flood, SYN Flood, DNS Amplification, NTP Amplification, SSDP, etc
- Attacks may target a FTTH client, a Leaseline client, a business or even a network operator, etc.

Anti DDOS Volume Based system is an all-in-one solution which protects users and organizations from the said DDOS attacks by blocking illegitimate traffic at the ISP's network.

## HIGHLIGHTS

1. Detect and alarm high-bandwidth DDOS attacks to administrator via SMS or email
2. Mitigate types of high-bandwidth attacks such as: UDP flood, ICMP flood,SYN Flood, DNS Amplification, NTP Amplification
3. Process high-bandwidth attacks of up to several tens of Gbps, or illegitimate traffic of up to 10 million pps.
4. Detect and alarm attacks that congest uplink by each interface, process link congestion directly through portal
5. Operate and process in an easy manner
6. Implement easily and be compatible with a variety of network infrastructures.

## Key features

**Detecting DDoS Volume Based attack:**

- Detect attacked IP based on client's actual traffic profile for any anomalies. Detect attacked IP by threshold.
- Types of attack detected: Volumed based: UDP & ICMP Flood, SYN Flood, Volume-based, regardless of protocol.
- Detection time less than 2 minutes.
- Verify good IP list for the whole network and for each client (a reliable IP list that the client regularly connects with at normal state)
- Issue ACL (Access List) of attacked IP.

**Block 1 bad IP:**

Block quikcly 1 bad IP and send order to Router RTBH.

**Portal for monitoring and processing attacks:**

- Monitor ongoing attacks: Detailed information of the attacks (IP, bandwidth, type of attack).
- Process attacks: Route attacked IP to null/Scrubber. Modify the Access list of the attack.
- Further monitoring: View the In/Out pcap data packets if the attacked IP runs through scrubber to evaluate the effectiveness of detection/prevention

**Preventing DDoS Volume Based attack:**

Situation 1: Deal with direct attack stream on the portal: International link flood, IDC-VTNET link flood, Allot overload: Send order to router RTBH to solve the attack

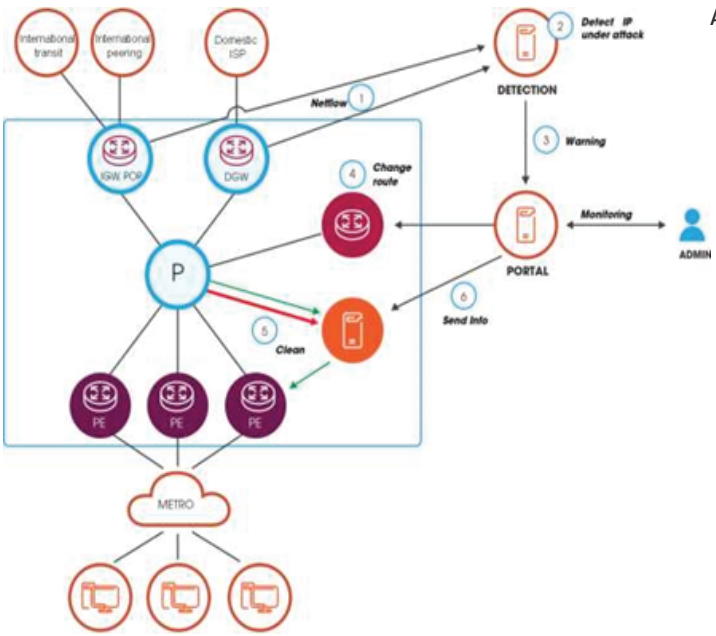
Situation 2: Route the illegitimate traffic of DDOS attack to Scrubber system to filter the illegitimate traffic, upholding services for clients:

- Block invalid packet.
- Permit Good IP: allow good IP to pass through quickly without further processing (ACL, bandwidth reduction), etc
- Drop bad ACL: Block illegitimate traffic by ACL from Detection.
- Bandwidth limit by IP dest: Bandwidth limit by preset threshold.
- Capture pcap data packets before and after processing for further monitoring
- Deal with attack at max 20 Gbps/ 01 physical server.

# Viettel Anti DDoS Volume Based Solution

viettel security

## Deployment model




Anti DDOS Volume Based system is comprised of 4 main components:

**Detection**

Detect and send warnings of the IP under DDoS attacked.

**Diversion**

Route traffic to scrubber system, change routing and receive command from portal.

**Scrubber**

Filter illegitimate traffic, return clean traffic to client.

**Portal**

View warning information, attack status, command to diversion system for routing change.

## Hardware description

| Model | Anti DDoS 60 Gbps | Anti DDoS 120 Gbps | Anti DDoS 180 Gbps | Anti DDoS 240 Gbps |
|---|---|---|---|---|
| Maximum traffic anti-attack | <60 Gbps | <120 Gbps | <180 Gbps | <240 Gbps |
| Server configuration | • 01 Server 2 x E5-2687Wv4<br>• 128GB DDR<br>• 4x 1.2TB SAS 10K rpm HDD<br>• 3 x back plane PCI<br>• 3 x 4 port ethernet 10Gbps quang<br>• 12 modul single mode 1310mm | • 02 Server 2 x E5-2687Wv4<br>• 128GB DDR<br>• 4x 1.2TB SAS 10K rpm HDD<br>• 3 x back plane PCI<br>• 3 x 4 port ethernet 10Gbps quang<br>• 12 modul single mode 1310mm | • 03 Server 2 x E5-2687Wv4<br>• 128GB DDR<br>• 4x 1.2TB SAS 10K rpm HDD<br>• 3 x back plane PCI<br>• 3 x 4 port ethernet 10Gbps quang<br>• 12 modul single mode 1310mm | • 04 Server 2 x E5-2687Wv4<br>• 128GB DDR<br>• 4x 1.2TB SAS 10K rpm HDD<br>• 3 x back plane PCI<br>• 3 x 4 port ethernet 10Gbps quang<br>• 12 modul single mode 1310mm |