Datasheet

ANTI DDOS VOLUME - BASED SERVICE

viettel security

Service Introduction

Anti DDoS Volume-Based is an anti-DDoS attack service with large bandwidth that blocks the customer's internet channel, which helps to ensure good quality for the customer's transmission channel in normal conditions as well as when under DDoS attack.

Why the service should be deployed?

DDoS attacks are increasingly diverse in size and purpose (personal, economic and political motives). Attack types are also increasingly diverse and complex, causing disruption to infrastructure services.

In addition, hackers can take advantage of vulnerabilities in terminals to use many forms of attacks to mobilize large bandwidth flows from a few tens to hundreds of Gbps, heavily blocking the customer's transmission channel.

Therefore, the anti-DDoS attack service was developed to ensure disabling DDoS attacks to the customer's infrastructure, protecting the best transmission channel for customers against targeted attacks, thereby protecting customer's production and business activities.

Highlights

- Quickly detect, process and immediately notify customers of Volume-Based DDoS attacks.
- Automate the entire process and features.
- Meet professional 24/7 operation, monitoring and customer support team throughout the service life.
- Support a variety of real-time warning channels via Email, SMS, Portal.
- Handle all popular DDoS attacks with bandwidth up to hundreds of Gbps, quickly and regularly update new attack patterns.
- Provide an intuitive and convenient Portal interface for customers to track information.
- Use advanced technologies to detect and block attacks such as DPI, Profiling, Machine learning, BGP flowspec, Remote trigger black hole, etc.

Key Features

The service quickly detects and handles Volume-Based DDoS attacks:

- ✓ Quickly detect most types of Volume-Based DDoS attacks in less than 3 minutes
- ✓ Delay packet passing through filter < 3 ms
- ✓ Protect against volumetric attacks, up to more than 100 Gbps
- ✓ Detect and handle common attacks:

TCP stack attack (SYN Flood, FIN, RST, ACK, SYN-ACK...)

Reflection/Amplification Flood Attacks (ICMP, DNS, mDNS, Memcached, SSDP, NTP, Chargen...)

Volumetric Attacks (UDP Flood, ICMP Flood...)

Fragmentation (Teardrop)

Invalid packet

- ✓ **Flexible handling methods:** Clean attack traffic to return clean traffic to customers or block traffic to hacked IP according to domestic traffic, international traffic options...

The service automatically notifies customers by Email, SMS, Portal as soon as the attack is detected.

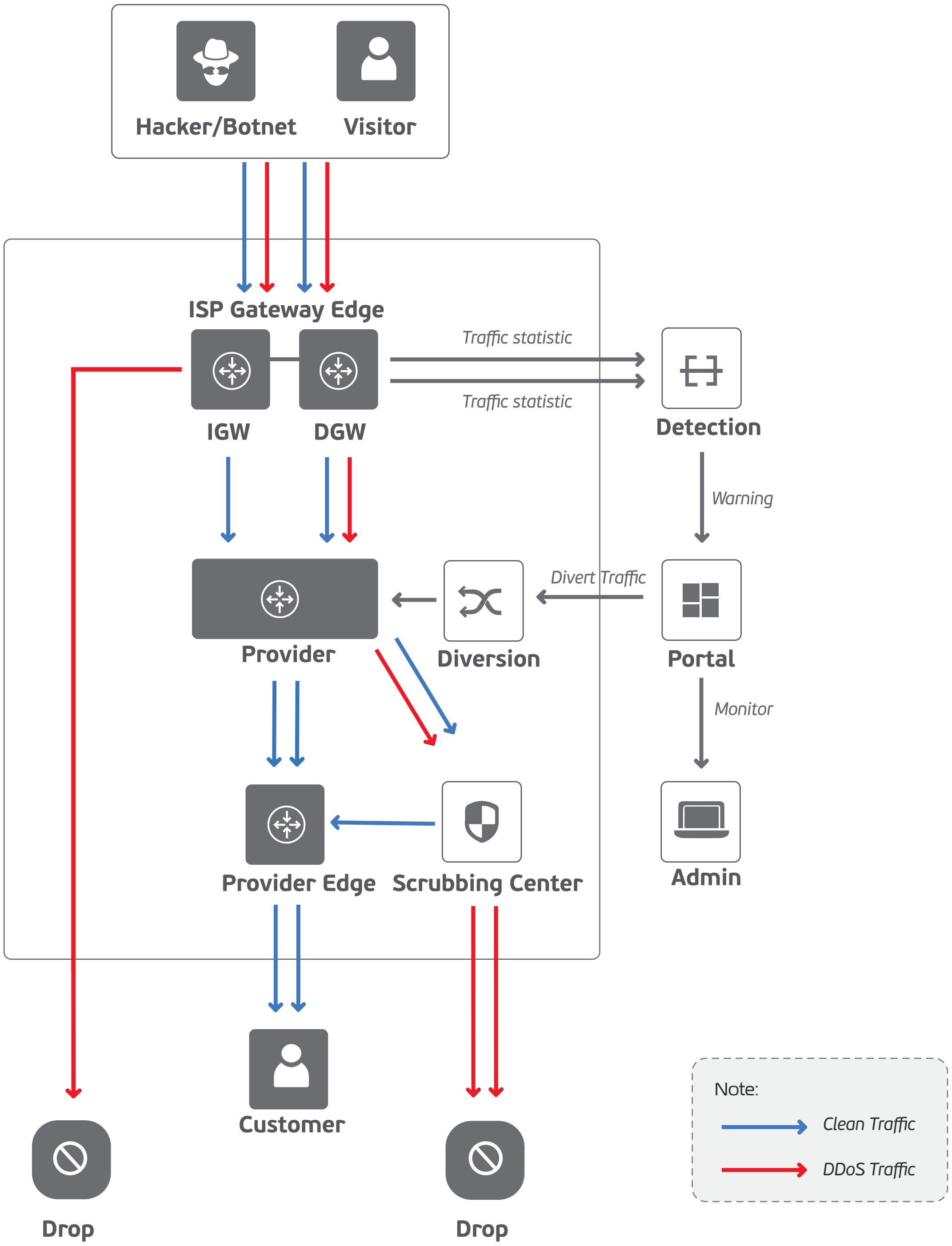
Portal provides friendly interface for customers to monitor and look up detailed information about attacks that have happened and are happening.

Datasheet

ANTI DDOS VOLUME - BASED SERVICE

viettel security

Solution Model



Service level agreement

- ✓ **System stability:** The system is always active and provides customers with full features stably 24/7.
- ✓ **Attack detection and automatic processing of attack traffic time:** Maximum within 3 minutes.
- ✓ **Time to send notifications to customers (Email, SMS, Portal):** Maximum within 5 minutes.
- ✓ **Traffic cleaning efficiency:** At least 95% of 'clean' traffic is returned to the customer after going through the traffic cleaning system.