

GIỚI THIỆU DỊCH VỤ

Anti DDoS Volume-Based là dịch vụ chống tấn công DDoS bằng thông lớn làm nghẽn kênh truyền internet của khách hàng, giúp đảm bảo chất lượng tốt cho kênh truyền của khách hàng trong điều kiện bình thường cũng như khi bị tấn công DDoS.

VÌ SAO CẦN TRIỂN KHAI DỊCH VỤ

Các cuộc tấn công DDoS ngày càng đa dạng về quy mô và mục đích (động cơ cá nhân, kinh tế và chính trị). Các kiểu tấn công cũng ngày càng đa dạng, phức tạp, gây hậu quả gián đoạn cho dịch vụ hạ tầng.

Bên cạnh đó, hacker có thể lợi dụng lỗ hổng của các thiết bị đầu cuối để sử dụng nhiều hình thức tấn công huy động được các luồng băng thông lớn từ vài chục tới hàng trăm Gbps làm nghẽn nặng kênh truyền của khách hàng.

Chính vì vậy, dịch vụ chống tấn công DDoS ra đời đảm bảo vô hiệu hóa các cuộc tấn công DDoS tới hạ tầng của khách hàng, bảo vệ kênh truyền tốt nhất cho khách hàng trước những cuộc tấn công chủ đích, qua đó bảo vệ hoạt động sản xuất kinh doanh của khách hàng.

CÁC TÍNH NĂNG CHÍNH

Phát hiện và xử lý nhanh tấn công DDoS Volume-Based:

- ✓ Phát hiện nhanh hầu hết các loại hình tấn công DDoS Volume-Based trong thời gian dưới 3 phút
- ✓ Delay gói tin đi qua bộ lọc < 3 ms
- ✓ Chống tấn công volume lớn, lên đến hơn 100 Gbps
- ✓ Phát hiện và xử lý các tấn công phổ biến:

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

- ✓ **Các hình thức xử lý linh hoạt:** Làm sạch lưu lượng tấn công để trả về lưu lượng sạch cho khách hàng hoặc chặn lưu lượng đến IP bị tấn công theo các tùy chọn lưu lượng trong nước, lưu lượng quốc tế...

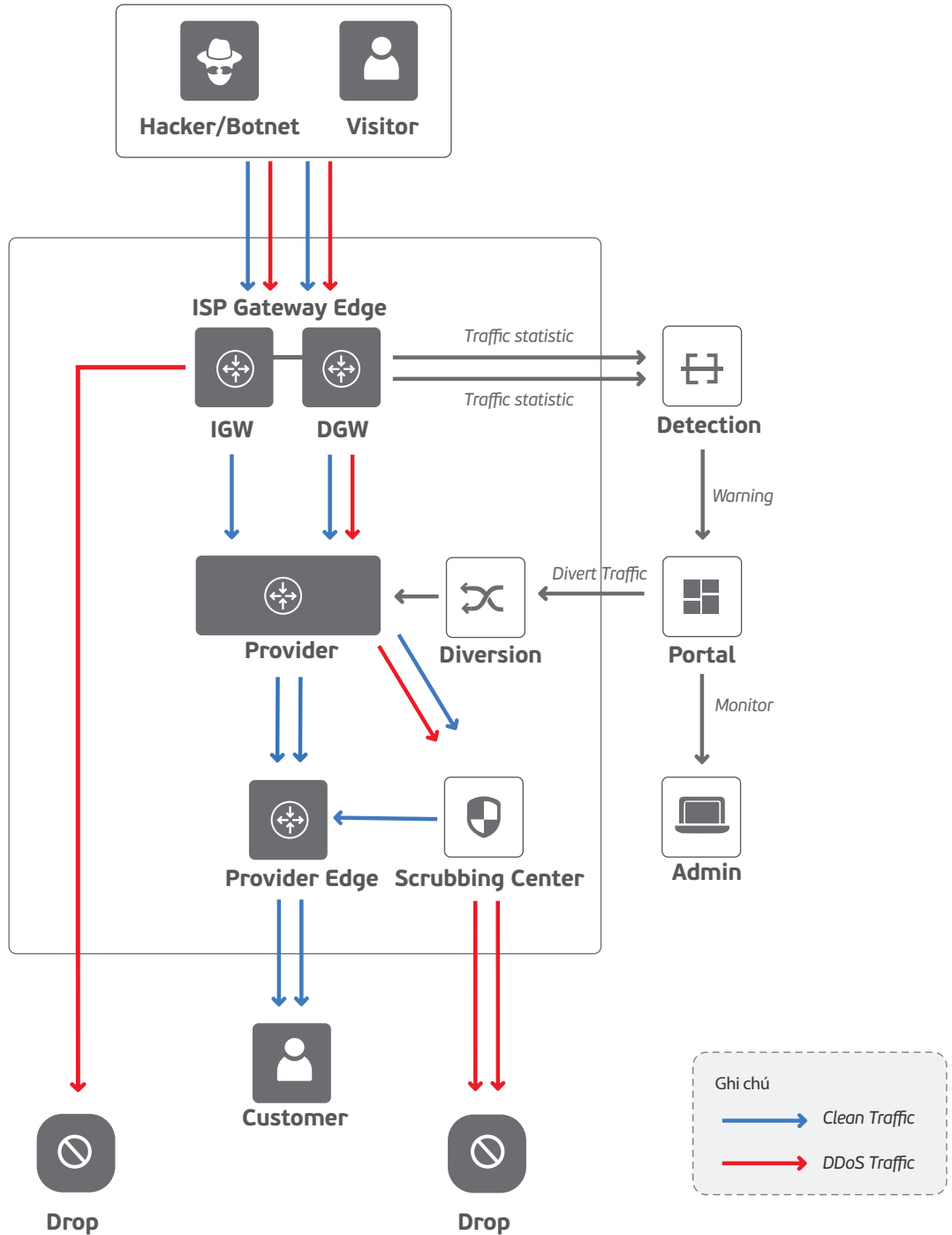
Tự động thông báo đến khách hàng bằng Email, SMS, Portal ngay khi cuộc tấn công được phát hiện.

Portal cung cấp giao diện thân thiện cho khách hàng theo dõi, tra cứu thông tin chi tiết các cuộc tấn công đã và đang xảy ra.

ƯU ĐIỂM NỔI BẬT

- Phát hiện, xử lý nhanh, thông báo tức thời đến khách hàng các cuộc tấn công DDoS Volume-Based.
- Toàn bộ quy trình, tính năng được tự động hóa.
- Đội ngũ vận hành, giám sát, hỗ trợ khách hàng 24/7 chuyên nghiệp trong suốt thời gian sử dụng dịch vụ.
- Hỗ trợ đa dạng các kênh cảnh báo realtime qua Email, SMS, Portal.
- Xử lý được toàn bộ các kiểu tấn công DDoS phổ biến với băng thông lên đến hàng trăm Gbps, cập nhật nhanh chóng và thường xuyên các hình thái tấn công mới.
- Cung cấp giao diện Portal trực quan, tiện lợi cho khách hàng theo dõi thông tin.
- Sử dụng các công nghệ tiên tiến để phát hiện và chặn lọc tấn công như: DPI, Profiling, Machine learning, BGP flowspec, Remote trigger black hole...

MÔ HÌNH GIẢI PHÁP



CAM KẾT CHẤT LƯỢNG DỊCH VỤ

- ✓ **Độ ổn định của hệ thống:** Luôn luôn hoạt động và cung cấp đầy đủ tính năng cho khách hàng ổn định 24/7.
- ✓ **Thời gian phát hiện tấn công và tự động xử lý lưu lượng tấn công:** Tối đa trong vòng 3 phút.
- ✓ **Thời gian gửi thông báo đến khách hàng (Email, SMS, Portal):** Tối đa trong vòng 5 phút.
- ✓ **Hiệu quả làm sạch lưu lượng:** Tối thiểu 95% lưu lượng sạch được trả về cho khách hàng sau khi đi qua hệ thống làm sạch lưu lượng tấn công.