CASE STUDY

NSFOCUS
SECURITY MADE SMART AND SIMPLE

Cloud DPS – Guaranteed Mitigation Effect by Tailored Policy Tuning

About NSFOCUS

NSFOCUS is an iconic network and cyber security provider for telecom carriers, BFSI, enterprises, healthcare, retail and SMBs. It has a proven track record of protecting over 25% of the Fortune Global 500 companies, including four of the five largest banks and six of the world's top ten telecommunications companies.

NSFOCUS delivers a holistic suite of security products powered by industry leading threat intelligence. These security products work in concert to protect you from massive volumetric DDoS attacks, Web threats and advanced persistent threats (APTs).

A CRITICIAL THING TO THINK WHEN CHOOSING YOUR CLOUD DDOS MITIGATION SERVICE

Today, more and more ISPs, IDCs, enterprises, governments and SMBs choose cloud-based DDoS mitigation services to protect their business as these services can be ordered and deployed easily, offers more scrubbing capacity and financial flexibility comparing to traditional on-premises DDoS protection hardware and software.

Anyway, before ordering, customers need to look into the market carefully and try to identify the most suitable cloud DDoS mitigation service supplier as the service itself can vary a lot. Different supplier could mean different scrubbing capacity, clean traffic injection route, platform/service availability, time-to-mitigate, utilization frequency of blackholing or rate limit, and the most important above all – mitigation effect.

WHY MITIGATION EFFECT IS IMPORTANT

Going back to the essence of the Distributed denial of service (DDoS) attack, it brings negative impact to internet service by generating flood traffic towards the target. So an effective mitigation service shall be able to guarantee that the traffic reaching the target must be limited under the certain level that the target can bear, thus business will not be disrupted.

The above-mentioned guarantees are often mentioned as Mitigation Effect, which describes the ratio between malicious traffic successfully mitigated and total incoming traffic, E.g.:

- During a DDoS incident, incoming traffic reaches 10 Gbps;
- After mitigation, 500 Mbps traffic arrives at the target;
- Among the 500 Mbps, 50 Mbps are legitimate traffic while 450 Mbps are malicious traffic;

Mitigation Effect = (10Gbps - 450Mbps) / 10Gbps = 95%

From customers' view, a guaranteed Mitigation Effect of 95% means its

internet service will survive under a 10Gbps DDoS attack as long as it could bear 500Mbps of traffic. This brings a series of benefits for customers to plan their resources and service availabilities.

CLOUD DPS - HOW MITIGATION EFFECT IS GUARANTEED

Mitigation Effect actually reflected the efficiency and accuracy of the mitigation policies. We have discovered in practices that mitigation effect cannot be guaranteed when there is only one or few global policy templates for all customers. Each customer shall have its own policies which reflects its unique business and traffic characteristics to get the best mitigation effect.

NSFOCUS has built an experienced expert team with sufficient know-how in its security operations center (SOC), experts will do the following for our customers:

- Before attack:

  Detailed investigation to the customer's business and traffic characteristics and tune the policies accordingly to ensure the legitimate traffic could go through with minimum false-positive.

- During attack:

  Observe DDoS attack vectors and tune the policies accordingly to reach the best false-negative rate. In most incidents the attacker will use mixed attack vectors and may change during difference period of an attack so the tuning has to be constant and dynamic.

ANOTHER NEGATIVE IMPACT WHEN INEFFECT POLICY

In case the protection policy does not good enough and lead to remarkable traffic leakage or the supplier's network/scrubbing resources are going to exhaust, the supplier may trigger rate limit or blackholing to protect their network resources which is not good for customers, as that means the attacker has reached its goal to interrupt customers' service.

NSFOCUS performs well in policy tuning and also reserves abundant network resources for its customers. As a result, customers have rare chance of encountering blackholing and/or rate limit.

CASE A: CUSTOMER WITH ITS POLICY TUNED

The customer on-boarded NSFOCUS Cloud DPS normally.

Peak malicious traffic reached 634 Gbps;

For more information, please contact:

U.S.

Tel: + 1 408-907-6638

EMEA

Tel: +44 (0) 20 3882 7025

LATAM

Tel: +55 11 3521-7124

Email: contato@nsfocusglobal.com

APAC

Email: apmarketing@nsfocusglobal.com

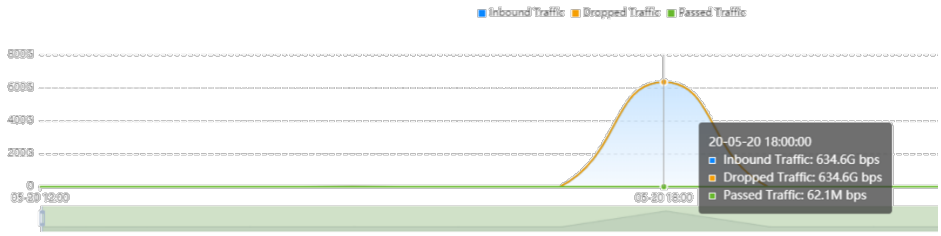
GCR:

Email: gcrmarketing@nsfocusglobal.com

NSFOCUS
SECURITY MADE SMART AND SIMPLE

After mitigation, only 62 Mbps of traffic reached the customer.

Mitigation Effect = (634Gbps – 62Mbps) / 634Gbps = 99.99%



CASE B: CUSTOMER WITH ITS POLICY UNTUNED DUE TO EMERGENCY ON-BOARD

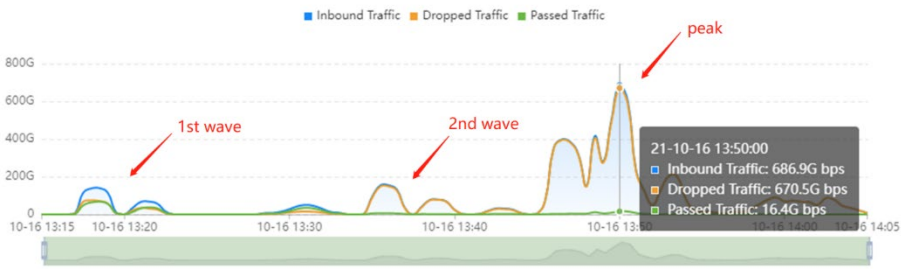
The customer on-boarded NSFOCUS Cloud DPS in emergency when it was already under attacks. NSFOCUS didn't have data and knowledge of its legitimate traffic and patterns of malicious traffic, thus no preliminary tuning was possible.

1. The first wave of attack arrived at 100-150 Gbps peak and almost half of them passed to the customer due to no policy tuning. Mitigation Effect ≈50%.
2. NSFOCUS SOC team managed to do immediate investigate to attack patterns and mitigate effect improved a lot during the 2nd wave arriving in 20 minutes;
3. In the peak moment of the incident, traffic reaches 686.9 Gbps and passed traffic stayed at 16.4 Gbps.

Mitigation Effect = (686.9Gbps – 16.4Gbps) / 686.9Gbps = 97.61%

Here we could see that a tailored policy tuning will significantly improve Mitigation Effect to a satisfactory level.

Furthermore, if we compare this emergency case with normal case A in the similar size of an attack, when customer stayed with NSFOCUS in long-term, mitigation effect will keep involving during daily SOC operations and passed traffic could go minimum and no pressure will be brought to the customer infrastructure.



Connect with NSFOCUS:

Blog: nsfocusglobal.com/blog/

LinkedIn @nsfocus

Twitter @NSFOCUS_Intl

Facebook @nsfocus

FOR MORE INFO:

www.nsfocusglobal.com/products/cloud-ddos-protection-service-cloud-dps/

NSFOCUS Website:

www.nsfocusglobal.com