

Un atac DDoS (Distributed Denial of Service) este o acțiune coordonată a unei persoane sau a unui grup prin care se încearcă oprirea funcționării unui server pentru o perioadă.

Motivul acestora variază de la concurență neloială pentru discreditarea serviciului atacat în fața vizitatorilor până la teribilism și motivații politice.

Orice serviciu existent pe Internet poate fi victima unui asemenea atac care poate dura de la câteva secunde până la zile sau chiar săptămâni. Protecțiile oferite de sistemele de operare sunt neputincioase în fața unui atac bine coordonat.

Un atac DDoS constă în trimiterea la capacitate maximă, simultan de pe servere din diferite locații de cereri de acces la serviciul atacat. Aceste cereri sunt simulate de diferite programe și doar volumul neobișnuit de mare le face să difere de cererile utilizatorilor reali.

Soluția este dată de capacitatea furnizorilor de Internet și hosting în a-și folosi echipamentele de rutare și filtrare de mare capacitate pentru oprirea acestor atacuri.

Limehost are 3 niveluri automate de protecție disponibile clienților:

1. Protecție împotriva atacurilor DDoS nedistribuite (gratuit)

Un atac originat de o adresă IP care trimite un *număr foarte mare* de pachete (IP, UDP, ICMP etc) către un server este blocat după 10-60 secunde.



Simultan, Limehost are implementate împreună cu furnizorii de Internet diferite reguli de transfer de trafic pentru a evita anumite anomalii.

Protecția este eficientă împotriva serverelor compromise de pe Internet la care atacatorii au obținut acces ilegal și pe care le folosesc să origineze asemenea atacuri.

2. Protecție împotriva atacurilor DDoS distribuite (8€ / luna, fără TVA)

Un atac originat de la mii de adrese IP care trimit fiecare un *număr mediu* de pachete către un server este blocat instantaneu.



Protecția este eficientă împotriva atacurilor originare prin programe de file-sharing sau viruși instalați pe calculatoare personale, folosite de atacatori fără știința utilizatorilor.

3. Protecție împotriva atacurilor DDoS de orice fel (15€ / luna, fără TVA)

Atacurile cu pachete TCP_SYN, UDP flood sau *orice alt tip care nu reprezintă trafic real* este blocat de firewallul Limehost. Include filtrele de mai sus pentru a asigura maximul de protecție a unui serviciu.

Se activează în 2-4 secunde de la începerea atacului și rămâne activă încă 10 minute după încetarea acestuia.

Protecția este ideală împotriva oricărei forme de atac a unui serviciu deoarece se bazează pe analiza traficului anterior al serverului și permite accesul doar al adreselor IP care anterior au accesat cu bună intenție serverul.

Contactează-ne acum la noc@limehost.ro sau 021.2074780
pentru activarea protecțiilor sau pentru relații suplimentare!

Întrebări frecvente

1. *Îmi protejeaza serverul radio care îmi pică la flood?*

Da, orice fel de tip de flood este blocat si radioul nu va suferi nici o întrerupere. Dacă poți bloca SYN-urile pe server, atunci ai nevoie doar de protecția împotriva atacurilor DDoS distribuite (8€/lună) altfel va trebui să activezi Protecție împotriva atacurilor DDoS de orice fel (15€ / lună)

Limehost găzduiește multe posturi de radio care ne-au ales exact pentru acest motiv și pentru banda de Internet de 1Gbps.

2. *Protecțiile sunt eficiente împotriva Supernova, floodului de hub si UDP?*

Da! Nu vei observa nici o problemă de funcționare a serverului în timpul acestor atacuri cu condiția să nu trimiți flood de pe propria adresă de IP.

3. *Pot să testez aceste protecții?*

Da. Contactează-ne pentru a testa gratuit protecția pentru serverul tău de la Limehost.

4. *De unde știu că sunt floodat?*

Dacă aveți activate protecțiile noastre, veți primit automat un email care vă anunță sursa atacurilor si măsurile luate împotriva lor.

5. *Costul e pe server sau per IP?*

Costul lunar menționat este per server și include toate IP-urile găzduite pe acel server.

6. *Mai am nevoie de firewall pe server?*

Nu pentru protecția la flood. Dacă nu aveți cunoștințe foarte avansate de configurare a acestuia, atunci vă recomandăm să-l dezactivați. Majoritatea problemelor raportate sunt în fapt configurări greșite ale propriului firewall.

7. *Pot obține mai multe relații despre sistemul de protecție?*

Nu. Nu putem dezvălui tehnologiile folosite pentru a proteja sistemul la potențiale vulnerabilități pe care nu le cunoaștem. Va invităm în schimb să le testați eficiența! (si nu uitați să nu trimiteți trafic de flood de pe propriul IP!!)