UPC ANTI-DDOS

Bezpečnosť vášmu podnikaniu

Služba UPC Anti-DDoS chráni pred volumetrickými útokmi a útokmi zameranými na protokol a aplikácie. UPC Anti-DDoS je cenovo dostupné riešenie, použiteľné so službami Internet alebo IP konektivita. Táto služba ponúka nepretržitú podporu, ktorá pomáha zákazníkom chrániť dostupnosť ich sieťovej infraštruktúry a minimalizovať postoje tým, že zmierňuje útoky vedené na sieť zákazníka. Ak si zákazník zvolí UPC ako primárneho (alebo jediného) poskytovateľa pripojenia, môže uvoľniť zdroje svojho IT oddelenia aj manažmentu na podporu iných potrieb nevyhnutných na podnikanie.

ČO JE DDOS ÚTOK

DDoS je technika preťažovania prostriedkov siete alebo servera poskytovateľa služieb alebo jednotlivých zákazníkov, ktoré spôsobia, že ich služba nie je na internete dostupná. Útoky DDoS môžu byť hrubou silou využité tak, aby zahltila schopnosť procesora alebo pamäte reagovať na veľa falošných požiadaviek. Útoky DDoS prebiehajú kvôli podnecovaniu mnohých napadnutých počítačov zákazníkov (zombie) alebo dokonca cloudových služieb na odoslanie požiadaviek na obsah v obrovských množstvách z určitého cieľa. Na vyvolanie DDoS možno tiež zneužiť slabiny protokolov IP alebo zle nakonfigurovaných zariadení. Napríklad útok amplifikáciou DNS môže z jediného pripojenia generovať 10 – 350x väčšiu prevádzku. Vinou DDoS útoku je napadnutá služba nedostupná a pri útoku na podnikovú infraštruktúru sú v mnohých prípadoch hlásené aj straty dát.

PREČO SLUŽBU UPC ANTI-DDOS

- UPC ponúka plne spravovanú nepretržitú službu, ktorá umožňuje zákazníkom zabrániť/prekonať väčšinu prekážok súvisiacich s útokmi DDoS.
- Využitie služby UPC Anti-DDoS môže znížiť prípadné kapitálové a prevádzkové výdavky a zaistiť predvídateľné prevádzkové náklady súvisiace s bezpečnosťou siete.
- So službou UPC Anti-DDoS môžu zákazníci očakávať minimalizáciu neočakávaných výdavkov a problémov s výkonom siete súvisiacich s útokmi DDoS.
- Služba UPC Anti-DDoS umožňuje preniesť zodpovednosť za zmiernenie útokov DDoS zo zákazníka na spoločnosť UPC.
- Sieťová prevádzka k aplikáciám účastníka prechádza sieťou poskytovateľa, preto je UPC logickým umiestnením na implementáciu služby zmiernenia útokov DDoS.
- Volumetrické útoky sú zaisťované tiež na hraniciach celej siete Liberty Global a môžu byť vyriešené už tam, ešte kým dorazia do siete UPC SK.
- Služba UPC Anti-DDoS funguje automaticky bez závislosti od ľudského rozhodovania a bez omeškania
  - Nie sú potrebné zmeny vo vašej sieťovej topológii
  - Možnosť individuálneho nastavenia vyhodnotenia prevádzky
  - K službe pripojíme aj zákazníkov s vlastným AS

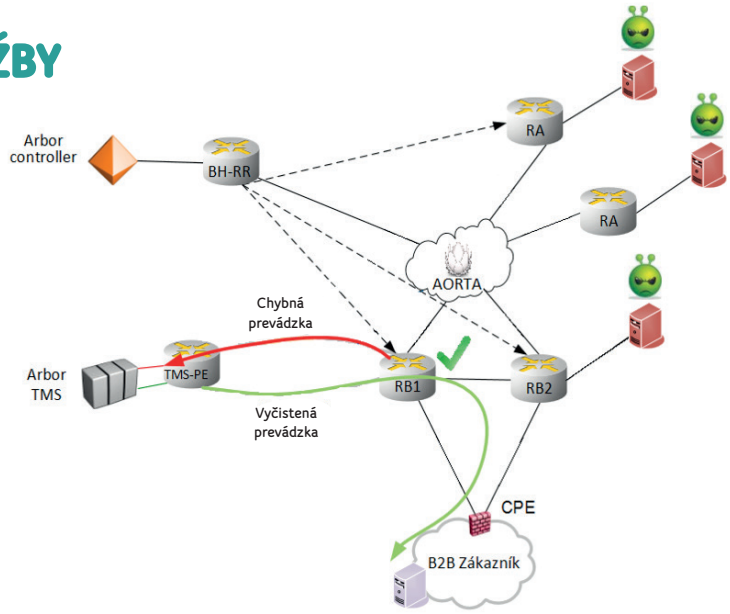
UPC Anti-DDoS
Power by ARBOR NETWORKS

Business upc

AKO TO FUNGUJE

Prevádzka sa meria pomocou Acces routerov a odosiela sa do centrálneho zberača. Prítomnosť škodlivej prevádzky je zistená na základe prahových hodnôt a vzorcov. Automatická reakcia na útok sa spustí pri dosiahnutí nastaviteľnej (pre každého účastníka na mieru) hornej prahovej hodnoty v danom časovom intervale pri útoku. Pri útoku je dátová prevádzka presmerovaná na čistiaci server TMS. Presmerovaná je však iba prevádzka, kde je vedený útok (špecifická IP adresa, určitý port, ...). Ostatná prevádzka je smerovaná bez zmeny. Škodlivá prevádzka je v TMS odfiltrovaná a legitímna prevádzka je vedená späť k zákazníkovi.
Chránime proti viacnásobným a simultánnym (veľa útokov je kombináciou rôznych spôsobov) hrozbám a spôsobom, ako sú volumetrické útoky obrovským dátovým tokom, amplifikácie a nakazenia DNS, ICMP, fragmenty IP, aplikácie SQL, amplifikácie NTP, amplifikácie SNMP, amplifikácie SSDP, rôzne typy TCP a zneužitie UDP.
Naše riešenie umožňuje aplikovať jemnú detekciu zneužívania a presmerovať len zasiahnutú prevádzku. Nástroje ako Flowspec nám umožňujú identifikovať zasiahnuté porty a protokoly a čistiť iba tie. To zaručuje oveľa väčšiu kapacitu ochrany.
Protiopatrenia zahŕňajú kontrolu neplatených paketov, zoznamy zakázaných a povolených IP adries, filtrovanie podľa polohy, filtrovanie záhlavia paketov, detekciu zombií, ochranu podľa zahltenia pripojenia, overovanie TCP Syn, riadenie DNS (posudzovanie, detekcia nesprávnych formátov, obmedzovanie počtu a overovania), riadenie HTTP (nesprávny formát, posudzovanie, obmedzovanie počtu), riadenie SIP (nesprávny formát, obmedzenie požiadaviek), obmedzovanie a resetovanie pripojení TCP.

FUNGOVANIE SLUŽBY



TECHNICKÉ PARAMETRE SLUŽBY

PARAMETER	HODNOTA
Reakčná doba v prípade útoku	Menej než 60 sekúnd
Garantovaná ročná dostupnosť služieb (Platforma Arbor)	99,9 %
Dopad na latenciu, jitter a stratu paketov v internetovej službe počas čistenia prevádzky	Pri útoku je prevádzka presmerovaná cez čistiace centrum – dopad na reakčnú dobu v prípade zmierňovania dopadov útoku: <3 až 6 ms.
Maximálna doba čistenia prevádzky po skončení útoku DDoS	5 minút
Maximálna prevádzková kapacita scrubing centra	3 x 80 Gb/s = 240 Gb/s
Minimálna prenosová rýchlosť pre čistenie	100 Mb/s

www.upc.sk/business/firmy

Business upc