CARNET

Zaštita od DDoS napada

CERT.hr-PUBDOC-2022-10-408

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

1.1 Što su DDoS napadi: DoS i DDoS

DoS (engl. *Denial of Service*) je kibernetički napad na računalni sustav (npr. *web* poslužitelj), s ciljem uskraćivanja usluga (engl. *denial of service*). Time je računalna usluga, primjerice *web* sjedište, nedostupna legitimnim korisnicima. Napadač može pokrenuti DoS napad koristeći jedno računalo.

Za razliku od DoS napada, DDoS (engl. *Distributed Denial of Service*) napad se pokreće s mnogo računala, obično fizički rasprostranjenih diljem svijeta. Ta računala ne pripadaju napadaču, već drugim korisnicima koji nisu svjesni da njihova računala sudjeluju u napadu. Tu skupinu računala nazivamo *botnet*.

Botnet je skupina zaraženih, tzv. „zombi" računala ili „botova", kojima napadač upravlja na daljinu (engl. *remotely*). Nakon što je računalo zaraženo, ono se spoji na C&C poslužitelj (engl. *command and control server*) kako bi primalo nove naredbe od napadača. Isto tako, *malware* koji je zarazio računalo nastavlja se širiti na druga računala na različite načine poput *spam* poruka elektroničke pošte ili iskorištavajući ranjivosti uređaja ili programa kojeg želi zaraziti kako bi *botnet* stalno rastao, tj. kako bi C&C imao sve više računala pod kontrolom.

Struktura *botneta* može biti slična klijent-poslužitelj strukturi, gdje su botovi povezani na jedan ili više C&C poslužitelja. Nedostatak ovakve strukture je taj što se rad *botneta* može zaustaviti ometanjem samo C&C poslužitelja koji upravlja botovima. Primjerice, francuska policija i firma Avast su zaustavili Retadup *botnet* preuzimanjem kontrole nad njihovim C&C poslužiteljima (1). Druga vrsta strukture, koja je otpornija na ovakav napad jest P2P (engl. *peer to peer*) struktura. U ovakvoj strukturi, svaki zaraženi uređaj komunicira s drugim zaraženim uređajima te od njih može primati naredbe.

Zaštita od DDoS napada nije jednostavan posao budući da je teško razlikovati legitimni promet *web* poslužitelja od prometa uzrokovanog DDoS napadom.

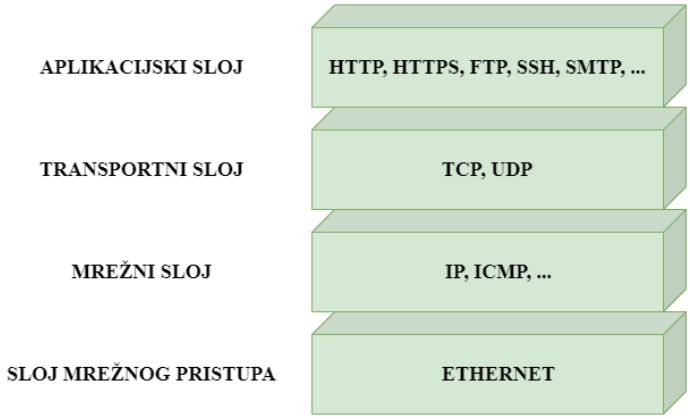
Trajanje DDoS napada ovisi o tome koliko je meta napada uložila u zaštitu protiv ove vrste napada te koliko su napadači motivirani za napad. Primjerice, 2015. je izveden veliki DDoS napad na *web* sjedište Githuba. Neki sigurnosni stručnjaci vjeruju da je napad izvela Kina, kako bi prisilila Github da ukloni alate za pristup *web* sjedištima koja su zabranjena u Kini. Ovaj napad je trajao čak 5 dana te su napadači mijenjali tehnike ovisno o tome kakve mitigacije bi Github primijenio (2). S druge strane, 2022. dogodio se DDoS napad na Andorra Telecom, pružatelja internetskih usluga u Andori. Taj napad je kratko trajao. Sumnja se da je razlog kratkog trajanja taj što ga je izveo napadač koji nije imao pristup vlastitom *botnetu* nego je unajmio pristup tuđem *botnetu* (3). Sumnja se da je cilj ovog napada bio sabotirati *gaming* natjecanje koje se održavalo u Andori, pa nije trebao trajati dugo da ispuni svoj cilj (trebao je trajati samo u terminu natjecanja). Prema Cloudflareu, devet od deset napada prestane unutar sat vremena (4).

DDoS napad na računalne sustave može napraviti financijsku štetu, naštetiti reputaciji kompanije čiji je sustav napadnut ili dugoročno smanjiti povjerenje korisnika.

Kako bi se konceptualno lakše objasnilo na koji način različiti DDoS napadi funkcioniraju, tj. koji točno dio *web* sjedišta napadaju, koristi se OSI model (engl. *Open Systems Interconnection Model*) (5). Osim OSI modela, postoji i TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*) kojeg ćemo više objasniti. On za razliku od OSI modela nije konceptualan, već je više praktičan model.

1.1.1 TCP/IP model

TCP/IP model je hijerarhijski model koji definira uspostavljanje veze između različitih računala i način komuniciranja preko mreže. Protokoli koji su dio TCP/IP modela su bili napravljeni prije samog modela. Također, TCP/IP je nastao prije OSI modela, pa se ne podudara s njim potpuno, ni u cijelosti ni u dijelovima, ali su dovoljno slični u namjeni. Na Slika 1 je prikazan TCP/IP model te je na svakom sloju modela prikazan protokol koji se u njemu koristi. Kao što je već rečeno, TCP/IP model je praktičan model.



Slika 1 *TCP/IP model*

Za razliku od OSI modela, TCP/IP model se sastoji od 4 sloja:

- aplikacijski sloj (engl. *application layer*) – zadužen je za razmjenu podataka i kontrolu sučelja, omogućuje korisniku interakciju s aplikacijom
- transportni sloj (engl. *transport layer*) – zadužen za komunikaciju i kontrolu podataka koji se šalju preko mreže
- mrežni sloj (engl. *network layer*) – zadužen za slanje paketa preko mreže
- sloj mrežnog pristupa (engl. *network access layer*) – definira kako bi se podaci trebali fizički slati preko mreže

1.1.2 Svojstva UDP i TCP protokola

Prije opisivanja primjera napada, a za njihovo lakše razumijevanje, potrebno je objasniti što je to TCP, a što UDP i koja je razlika između njih. Naime, neki od napada se oslanjaju na neka svojstva tih protokola koji su nastali u doba kad nitko nije očekivao njihovu ovako široku primjenu pa ni razmišljao o njihovoj zloupotrebi.

Nije se razmišljalo da će neprijatelj biti legitimni korisnik mreže, uključen u nju i da će ju napadati softverski, slanjem zlonamjernih paketa zato što je Internet nastao s idejom izgradnje, zapravo privatne, mreže koja će biti otporna na fizičke napade.

UDP (engl. *User Datagram Protocol*) je protokol koji služi za brzo i „nepouzdano" slanje informacija između uređaja. Pri slanju paketa koji sadrže informacije, uređaji ne uspostavljaju vezu, konekciju. Također, ne postoji garancija da će svi poslani paketi sigurno stići na svoje odredište, ili da će stići onim poretkom kojim su poslani. Upravo zato, ovaj protokol koriste programi kojima je bitno brzo prenošenje podataka bez obzira na moguće gubljenje paketa. „Nepouzdan" (engl. *unreliable*) se zapravo odnosi na svojstvo da protokol ne omogućava potvrdu prijema paketa, tj. sam protokol pošiljatelju ne daje povratnu informaciju je li primatelj primio poruku. Još jedna karakteristika ovog protokola je ta što on nema mehanizme koji vode računa da primatelj paketa neće njima biti zagušen.

TCP (engl. *Transmission Control Protocol*) je protokol koji služi pouzdanom prijenosu informacija između uređaja. Kako bi dva uređaja slala podatke putem TCP-a potrebno je uspostaviti konekciju, što se postiže tzv. „trostrukim rukovanjem" (engl. *three way handshake*).

Uređaj koji želi uspostaviti konekciju pošalje prvo SYN paket. Nakon toga, drugi uređaj s kojim se konekcija pokušava ostvariti pošalje natrag ACK, SYN paket. I rukovanje završi sa zadnjim SYN paketom kojeg prvi uređaj, pozivatelj, pošalje natrag pozvanom.

Nakon što završi rukovanje i nakon što se uspostavi konekcija, uređaji mogu pouzdano slati podatke bez straha da će neki paket biti izgubljen ili dostavljen u krivom redoslijedu.

Naime, sam protokol vodi brigu da se primatelju isporuče svi paketi i u ispravnom redoslijedu. Ako je potrebno, od pošiljatelja će tražiti ponovno slanje nedostajućih ili neispravnih paketa.

Nakon što prijenos završi, uređaji prekidaju konekciju.

1.2 Vrste DDoS napada

Napadi se događaju na mrežnom, transportnom te aplikacijskom sloju mrežnih protokola. DDoS napade možemo podijeliti obzirom na koji način uzrokuju uskraćivanje usluga.

Razlikujemo tri vrste DDoS napada:

a) volumetrički napad – cilj napada je zauzeti cijeli kapacitet propusnosti (engl. *bandwidth*) između žrtve napada i ostatka interneta;

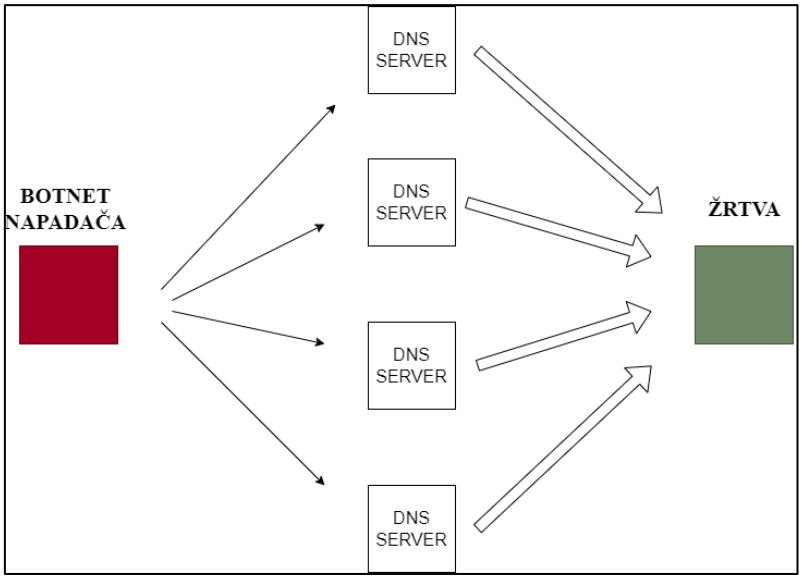
b) napad na aplikacijskom sloju – cilj napada je potrošiti sve resurse dodijeljene nekoj specifičnoj aplikaciji;
c) napad na razini mrežnog protokola – cilj napada je potrošiti sve resurse, no meta nisu specifične aplikacije.

1.2.1 Volumetrički napad

Cilj volumetričkih napada je zauzeti sav komunikacijski kapacitet žrtve ili puteva do nje koristeći veliku količinu podataka. Komunikacijski kapacitet se zauzme slanjem velike količine neželjenog prometa zbog čega legitiman promet ne može doći do svog odredišta. Veliki promet se može stvoriti izravno ili nekim pojačanjem (engl. *amplification*), nakon čega se usmjeri prema meti napada kako bi se zagušio promet između mete i ostatka interneta.

U volumetričke napade spadaju:

- UDP amplifikacija – napadač kreira zahtjev s lažiranom izvorišnom (engl. *source address*) IP adresom koja je postavljena na IP adresu žrtve (engl. *IP spoofing*) i pošalje ga nekom UDP servisu, primjerice DNS[1] poslužitelju. Primatelj poruke misli da mu je zahtjev došao od mete napada, pa njoj šalje odgovor i tako, efektivno, sudjeluje u stvaranju velike količine podataka koja preopterećuje žrtvu. Napadač se pobrine da zahtjev bude tako oblikovan da odgovor na upit bude bitno veći (otuda „amplifikacija“) od samog upita. Koristeći *botnet*, napadač može poslati više takvih zahtjeva na više DNS poslužitelja. Komunikacijski kanal mete će biti zagušen velikom količinom prometa kojeg šalju DNS poslužitelji vjerujući da odgovaraju na legitimne upite mete napada. Jedna od najčešćih UDP amplifikacija je DNS amplifikacija koja je prikazana na Slika 2. No, mogu se koristiti i drugi legitimni servisi. Problem obrane od tog napada leži upravo u tome što se ta vrsta prometa i ti servisi ne smiju filtrirati na komunikacijskim putovima prema žrtvi, jer onda žrtva neće ni sama moći koristiti te servise koji su ključni za njen rad.



Slika 2 *DNS amplifikacija*

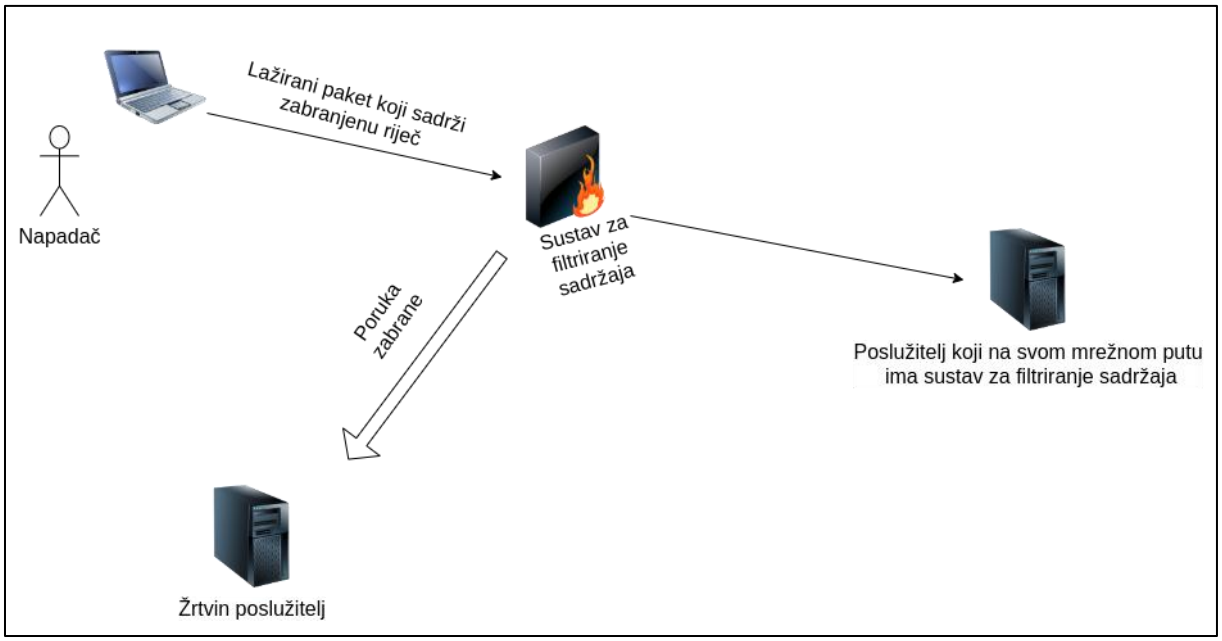
- TCP amplifikacija – napadač šalje SYN pakete s lažiranom IP adresom mete prema reflektirajućim IP adresama, tj. reflektorima koji su izabrani na temelju

[1] engl. *Domain Name System*

toga ignoriraju li RST ili ICMP kontrolne poruke koje bi rezultirale prekidom konekcije. Reflektori će poslati SYN-ACK paket prema žrtvi, misleći da je to bio izvor SYN paketa. Ako dođe npr. do gubitka paketa, žrtva će poslati neke kontrolne RST ili ICMP poruke kako bi prekinula rukovanje. No, budući da reflektori ignoriraju te poruke, oni će zatim više puta probati ponovno poslati SYN-ACK pakete, što može rezultirati amplifikacijom, i na kraju uskraćivanjem usluga.

- TCP *middlebox* amplifikacija – ovaj napad je sličan UDP amplifikaciji, no napadač umjesto UDP servisa koristi sustave za filtriranje sadržaja (engl. *content filtering*). Neke države blokiraju pristup pojedinim tipovima sadržaja unutar zemlje, primjerice pristup društvenim mrežama. Ako korisnik unutar zemlje pokuša pristupiti zabranjenoj društvenoj mreži, sustav blokira sadržaj i pošalje korisniku odgovor s porukom zabrane koja objašnjava kako ne smije pristupiti tom sadržaju. Takvi sustavi ponekad ne gledaju je li paket koji prolazi kroz njega dio uspostavljene TCP veze već će odgovoriti i na lažirane pakete koji nisu dio uspostavljene TCP veze ako smatra da ti paketi pokušavaju doseći resurs koji je zabranjen.

  Napad koji iskorištava način na koji sustavi za filtriranje sadržaja rade objašnjen je Slika 3[2].

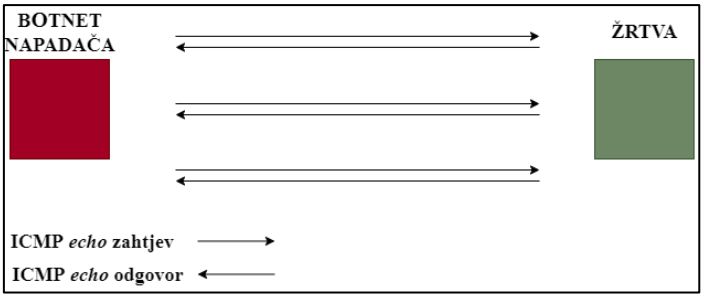


Slika 3 *TCP middlebox amplifikacija*

- ICMP[3] poplavljivanje (engl. *ICMP flood)* – napad znan još i kao ping poplavljivanje, koristi ICMP *echo* zahtjeve (u normalnim situacijama ICMP *echo* zahtjevi služe za provjeravanje dostupnosti uređaja prema kojemu je bila poslana poruka). Napadač pomoću *botneta* šalje veliki broj ICMP *echo* zahtjeva, tzv. pingova žrtvi, a

[2] Za dodatno objašnjenje, na sljedećoj poveznici može se pronaći odličan dijagram u *gif* formatu: https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/
[3] engl. *Internet Control Message Protocol*

ona pokušava odgovoriti na sve njih čime se na kraju zaguše oba smjera komunikacijskog kapaciteta žrtve.



Slika 4 *ICMP poplavljivanje*

- UDP poplavljivanje (engl. *UDP flood*) – napadač šalje pakete s UDP datagramima na nasumično odabrane priključke (engl. *port*) poslužitelja kako bi uzrokovao nedostupnost žrtve drugim korisnicima. Nakon što poslužitelj primi UDP paket, on najprije provjeri postoji li neki servis koji očekuje konekcije na tom priključku. Ako ne postoji, tada poslužitelj šalje natrag ICMP poruku kako bi javio da odredište nije dostupno.

  Napadač slanjem velikog broja UDP paketa (najčešće s lažiranom IP adresom izvora) može zagušiti komunikacijski kapacitet budući da poslužitelj šalje ICMP poruku kao odgovor na svaki UDP paket. Napad se može izazvati s relativno malo resursa budući da ne postoji ugrađen mehanizam koji ograničava protok UDP paketa zbog karakteristika tog protokola. Naime, kao što je prethodno objašnjeno [1.2], UDP je protokol bez konekcije i bez sjednice te ne zahtjeva trostruko rukovanje poput TCP-a.

1.2.2 Napad na aplikacijskom sloju

Napadi se izvršavaju na sedmom sloju (OSI modela) i troše resurse poslužitelja kao i resurse mreže. Može se dogoditi sljedeći scenarij: napadač pošalje poslužitelju upit zbog kojeg poslužitelj mora pristupiti bazi podataka kako bi došao do podataka koje mora poslati napadaču. Ako napadač koristi *botnet*, takvih zahtjeva može biti puno budući da svaki bot unutar *botneta* može sudjelovati u slanju upita poslužitelju, što rezultira uskraćivanjem usluga poslužitelja. Dakle, iako komunikacijski put ne mora biti potpuno zagušen, poslužitelj je toliko preopterećen da ne može odgovoriti na sve upite, pa tako ni na upite legitimnih korisnika.

Vrste napada na aplikacijskom sloju su:

- HTTP[4] poplavljivanje (engl. *HTTP flood*) – napadač koristeći *botnet* šalje veliki broj HTTP zahtjeva zauzimajući resurse *web* poslužitelja. Primjerice napadač slanjem velikog broja HTTP GET zahtjeva traži slike, datoteke i ostale moguće podatke. Poslužitelj pokuša odgovoriti na sve zahtjeve koje je primio, no budući da ih je puno, dolazi do uskraćivanja usluge. Osim napada HTTP GET zahtjevima, postoji i napad HTTP POST zahtjevima.

[4] engl. *Hypertext Transfer Protocol*

- Spori DDoS napadi – napadač otvara veći broj konekcija između sebe i žrtve šaljući parcijalne HTTP zahtjeve. Žrtva koristi dretve (engl. *thread*) za svaki od zahtjeva. U normalnim situacijama, dretva bi se oslobodila ako bi spajanje predugo trajalo. U ovom slučaju, napadač povremeno šalje parcijalne HTTP zahtjeve kako bi i dalje dretva bila zauzeta. Budući da žrtva ima samo ograničen broj dretvi za posluživanje zahtjeva, ovim načinom bi se sve dretve zauzele, i ne bi bilo moguće napraviti nove konekcije, tj. došlo bi do uskraćivanja usluga.

  Jedan od primjera ovakvog napada je „*Slowloris*“. *Slowloris* je zapravo alat koji omogućuje napad uskraćivanja usluga time što održava veliki broj konekcija između sebe i žrtve, upravo na način kako je i prethodno opisano. Jedna ranjivost gdje se napad može izazvati *Slowloris* alatom je CVE-2021-3909 ranjivost.

- Poplavljivanje DNS upitima (engl. *DNS query flood*) – kibernetički napad sedmog sloja koji uključuje slanje paketa s lažiranim IP adresama izvora na DNS poslužitelj neke domene s ciljem izazivanja uskraćivanja usluge. Dakle, meta napada je sam DNS poslužitelj. Za razliku od DNS amplifikacije, koja je asimetrični napad (što znači da se koristi manje resursa za uzrokovanje veće štete), ovo je simetrični napad (šteta je proporcionalna količini poslanih paketa). Napadač šalje pakete pomoću UDP protokola putem *botnet* mreže. Svaki paket ima lažiranu nasumično odabranu adresu izvora, zbog čega je teže detektirati ovaj napad pa filtriranje može biti beskorisno.

  Jedna vrsta ovih napada je i DNS NXDOMAIN napad poplavljivanjem – napadač šalje zahtjeve za rezoluciju domena za koje to nije moguće. Time se troše resursi DNS poslužitelja te on ne može odgovarati na zahtjeve legitimnih korisnika.

- Napadi uzrokovani nepažljivim programiranjem aplikacije: vrsta napada do koje može doći ako primjerice u aplikaciji postoji funkcionalnost koja blokira dretvu poslužitelja na dugo vremena (npr. pozivanjem funkcije *sleep*). Napadač lako može zauzeti sve raspoložive dretve (ili *worker* procese poslužitelja) tako da više puta pozove tu funkcionalnost.

  Slično tome, ako se ne postavi gornji limit na veličinu učitane (engl. *upload*) datoteke ili broj učitanih datoteka, napadač može zauzeti sav prostor na disku što također može dovesti do uskraćivanja usluge.

1.2.3 Napad na razini mrežnog protokola

- *Smurf attack* – napad sličan ICMP poplavljivanju, ali paket se šalje na razašiljačku adresu (engl. *broadcast address*) te ga primaju svi uređaji u mreži. Svaki uređaj u mreži tada šalje žrtvi odgovor na lažirani ping zahtjev kojeg je poslao napadač.

- IP/ICMP fragmentacija – napad koji iskorištava fragmentaciju paketa. Naime, prije nego što se paket pošalje, ako je veći od dozvoljene maksimalne veličine prijenosa (engl. *maximum transmission unit*), tada se on mora rastaviti, fragmentirati u manje dijelove koji se onda šalju do primatelja, svaki u svom paketu, koji ih onda mora ponovno spojiti u cjelinu. Napadač koristeći *botnet* ubacuje lažne fragmente paketa koji se ne mogu ponovno spojiti.

- TCP SYN poplavljivanje – napadač iskorištava dio TCP trostrukog rukovanja. Kao što je prethodno već pojašnjeno, u normalnom povezivanju između klijenta i poslužitelja, klijent pošalje serveru SYN paket. Poslužitelj kao odgovor pošalje SYN-ACK paket te čeka odgovor klijenta, tj. ACK paket kako bi se uspostavila konekcija. Na kraju klijent šalje ACK paket.

  Međutim, kod ovog napada, napadač šalje veliki broj SYN paketa prema poslužitelju žrtve, koji odgovara SYN-ACK paketima te iščekuje ACK pakete kao odgovor kako bi se uspostavila konekcija. No napadač nikad ne pošalje te pakete, ili jednostavno ne primi ni SYN-ACK pakete ako je adresa s kojom je bio poslan SYN paket bila lažirana. Zbog takvih poluotvorenih veza gdje se nikad nije uspostavila konekcija, poslužitelj će odbijati uspostaviti nove veze koje pripadaju pravim korisnicima te će doći do uskraćivanja usluga.

- Ping smrti (engl. *Ping of Death*) – napadač šalje prevelike ili neispravne pakete koristeći ping naredbu. Cilj napada je izazvati neočekivano ponašanje računala ili servisa kojemu je poslana ping naredba. Paketi se šalju fragmentirano. Nakon što žrtva napada pokuša ponovno sastaviti fragmente, može doći do izvanrednog gašenja (engl. *crash*). Napad iskorištava stariju ranjivost koja je vjerojatno zakrpana (engl. *patched*) u novijim sustavima, ali još uvijek može doći do ovakve vrste napada u starijim, nezakrpanim sustavima.

2 Sigurnosne preporuke za zaštitu od DDoS napada

Kako bi se uspješno zaštitili od DDoS napada potrebno je pravovremeno otkriti napad i odmah započeti njegovo rješavanje i ublažavanje. Za to je potrebno prethodno pripremiti odgovarajuće softvere ili uređaje ili cijele sustave.

Kako bi napadnuta usluga i dalje bila dostupna pravim korisnicima, potrebno je propustiti promet pravih korisnika, a blokirati neželjeni promet. Najveći izazov jest razlikovanje prometa pravih korisnika od neželjenog prometa čiji je izvor *botnet*.

U prošlom poglavlju je objašnjena razlika između tri vrste DDoS napada. U nastavku su navedene metode zaštite za svaku od navedenih vrsta.

2.1 Zaštita od DDoS napada na aplikacijskom sloju

Napad HTTP poplavljivanjem se može ublažiti blokiranjem IP adresa s kojih napad dolazi. Za neke od servisa postoje i dodaci (engl. *plugin*) koji blokiraju IP adresu ako detektiraju da jedna IP adresa šalje previše zahtjeva u prekratkom vremenu (npr. Apache modul *„mod_evasive“*).

„Spori“ DDoS napadi poput *Slowloris* napada [1.2.2] se mogu ublažiti tako da se prekinu zahtjevi koji traju predugo. Apache HTTP poslužitelj primjerice ima modul „*mod_reqtimeout*“ u čijoj se konfiguracijskoj datoteci može postaviti koliko dugo HTTP zahtjev smije trajati. Za vrijeme napada, ti parametri se mogu i postrožiti, no treba uzeti u obzir da bi to moglo utjecati na korisnike koji imaju sporu internetsku vezu pa se stroga konfiguracija ne preporučuje u „mirna“ vremena. Kao i kod napada HTTP poplavljivanjem, blokiranje IP adresa s kojih napad dolazi može ublažiti ovakav napad.

DDoS napadi na aplikacijskom sloju se mogu otežati i tako da se servisu dopusti da zauzme veću količinu resursa nego što mu je to omogućeno po zadanim postavkama. Primjerice kod Apache HTTP poslužitelja moguće je povećati postavku „*MaxRequestWorkers*“ kako bi se dopustilo više istovremenih HTTP zahtjeva. Tada je za DDoS napad potrebno više resursa, a servis će pritom moći podnijeti i više istovremenih legitimnih korisnika (6). Pri povećavanju takvih postavki potrebno je uzeti u obzir i druge servise koji se pokreću na poslužitelju. Servis ne smije zauzeti previše resursa, kako to ne bi utjecalo na druge servise.

Postoje razna softverska i hardverska rješenja koja mogu filtrirati promet prepoznavanjem poznatih uzoraka napada kako bi se spriječili neki DoS napadi na aplikacijskom i mrežnom sloju. Pritom treba uzeti u obzir da je to još jedan resurs kojim treba upravljati i redovito ga ažurirati te da nije zamjena za pravilnu konfiguraciju servisa.

Kao što je već spomenuto, sam DDoS napad može biti izazvan i nepažljivim programiranjem aplikacije. U tom slučaju, potrebno je ispraviti dijelove kôda aplikacije koji rezultiraju uskraćivanjem usluga. Neki primjeri nepažljivog programiranja aplikacije su navedeni u prethodnom poglavlju [1.2.2].

2.1.1 WAF – Aplikacijski vatrozid (engl. *Web Application Firewall*)

Aplikacije se od napada sedmog sloja mogu zaštititi i korištenjem aplikacijskog vatrozida (skraćeno „WAF“). Aplikacijski vatrozid služi kao obrnuti *proxy* (engl. *reverse-proxy*). Sav promet koji putuje od klijenata prema *web* sjedištu je filtriran, dakle potencijalni neželjeni promet koji iskorištava neke ranjivosti *web* aplikacije ili *web* poslužitelja se filtrira pomoću tog vatrozida. Između ostalog, WAF može filtrirati i promet koji pokušava iskoristiti ranjivosti čije bi iskorištavanje učinilo *web* sjedište nedostupnim, primjerice *billion laughs attack* (7) ili *slowloris* napade.

WAF se može implementirati na razne načine obzirom na dostupne resurse:

- mrežni vatrozid (engl. *network-based WAF*): lokalno instaliran vatrozid, najčešće kao *hardver*, što ga čini najskupljim rješenjem. Prednost je brzina i visoka performansa (eng. *performance*) budući da je blizu poslužitelja i može brzo filtrirati pakete.

- vatrozid baziran na poslužitelju (engl. *host-based WAF*): vatrozid koji može biti direktno integriran s aplikacijom, budući da se pokreće na istom poslužitelju kao i web aplikacija, zauzima lokalne resurse poslužitelja, što može negativno utjecati na performanse aplikacije.

- vatrozid baziran na oblaku (engl. *cloud-based WAF*): jeftiniji od prethodne dvije opcije, i jednostavan za koristiti, no nedostatak može biti taj što njime upravlja treća strana (engl. *third-party*), što znači da korisnik ovisi pružatelju ove vrste vatrozida.

2.2 Zaštita od DDoS napada na mrežnom sloju

Moderni operacijski sustavi već po zadanim (engl. *default*) postavkama imaju mjere koje mogu ublažiti ili čak spriječiti neke od DDoS napada na mrežnom sloju.

Primjerice kod napada TCP SYN poplavljivanjem, Linux koristi mehanizam SYN kolačića (engl. *SYN cookies*) koji sprječava alociranje memorija za TCP vezu dok klijent ne odgovori s ACK paketom. Zbog toga, napadač ne može zauzeti resurse slanjem SYN paketa s lažiranom izvornom IP adresom. Windows OS također ima sličan mehanizam zaštite (8).

Moderne verzije Linux i Windows operacijskih sustava su po zadanim postavkama konfigurirane da ne odgovaraju na ICMP ping pakete, ako je izvorišna adresa razašiljačka. Tako se sprječavaju prethodno spomenuti *smurf* napadi [1.2.3].

Što se tiče pinga smrti i fragmentacijskih napada, proizvođači operacijskih sustava uglavnom izdaju sigurnosnu zakrpu (engl. *security patch*) kada se pojave takve vrste ranjivosti. Takve ranjivosti se rijetko pojavljuju u novijim verzijama operacijskih sustava. Zbog toga je važno redovito ažurirati operacijski sustav.

Kao i kod napada na aplikacijskom sloju, softversko ili hardversko rješenje može pomoći pri detekciji i blokiranju ovakvih napada.

2.3 Zaštita od volumetričkih napada

Za razliku od napada na aplikacijskom i mrežnom sloju, volumetrički napadi se **ne mogu** riješiti konfiguracijom poslužitelja koji je pod napadom ili filtriranjem zlonamjernog prometa neposredno prije nego što dođe do poslužitelja (npr. pomoću WAF-a). Dovoljno veliki volumetrički napad će zagušiti kapacitet propusnosti bez obzira na konfiguraciju poslužitelja.

Ipak, postoje neke mjere koje mogu ublažiti i volumetričke DDoS napade.

2.3.1 Čišćenje (engl. *scrubbing*)

Neželjeni promet koji je namijenjen nekom računalnom sustavu (npr. *web* poslužitelju) se može preusmjeriti prema centru za čišćenje (engl. *scrubbing center*) kako bi se očistio. Na taj način samo promet koji je prethodno očišćen dolazi do računalnog sustava.

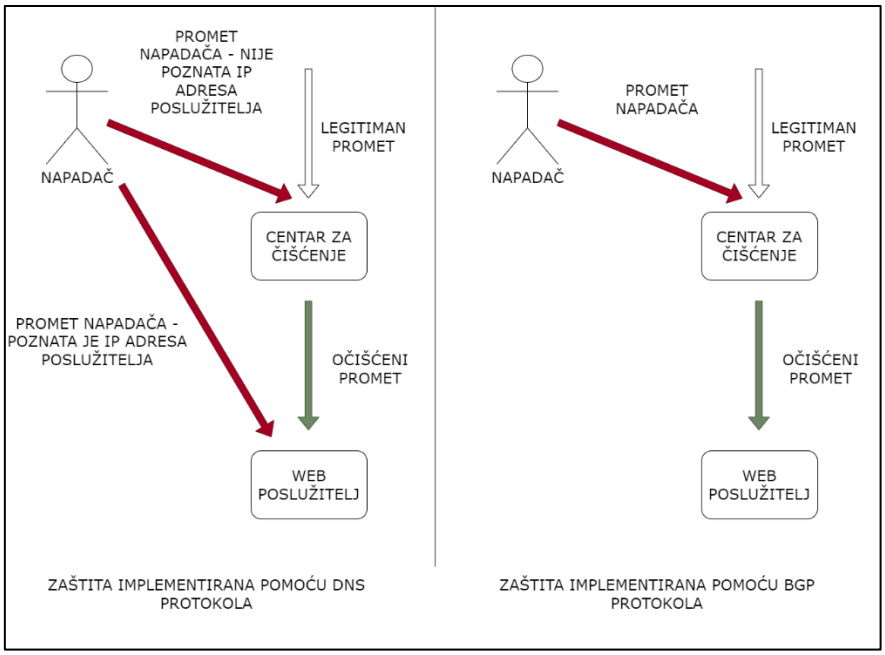
Čišćenje se obavlja u mreži većeg kapaciteta propusnosti u javnom ili privatnom oblaku.

Ovakva zaštita može biti implementirana pomoću DNS-a ili pomoću BGP (engl. *Border Gateway Protocol*) protokola.

Zaštita implementirana pomoću DNS-a se temelji na tome da se skriva prava IP adresa poslužitelja - žrtve. Napadač pomoću DNS upita može saznati samo IP adresu pružatelja usluga zaštite od DDoS napada, koji prosljeđuje očišćeni promet prema poslužitelju. No, ako napadač ipak nekako sazna IP adresu poslužitelja i napadne ju volumetričkim DDoS napadom, poslužitelj neće biti zaštićen. Primjerice, ako je DDoS zaštita implementirana tek naknadno, napadač može pregledom povijesnih DNS zapisa otkriti pravu IP adresu.

Kod zaštite temeljene na BGP protokolu, sav mrežni promet se preusmjerava kroz centar za čišćenje. Budući da promet prolazi kroz centar za čišćenje, poznavanje prave IP adrese poslužitelja nije baš korisno, zato što će promet svejedno prolaziti kroz centar za čišćenje (uvijek ili tek kad napad počne, ovisno o konfiguraciji). Ova metoda zaštite je namijenjena većim organizacijama koje imaju svoj „autonomni sustav“.

Autonomni sustav je skup usmjernika koji imaju zajedničku politiku usmjeravanja prema drugim autonomnim sustavima. Njima upravlja jedan entitet poput vladine agencije ili tijela, pružatelja internetskih usluga (skraćeno „ISP“), velikog sveučilišta ili neke velike komercijalne organizacije. AS broj može dobiti svatko tko dobro obrazloži potrebu za njim. Svaki autonomni sustav ima svoj jedinstveni broj kao oznaku. Kako bi objavio svoju politiku usmjeravanja drugim autonomnim sustavima ili usmjernicima, koristi se BGP protokol. Više detalja o BGP-u može se pronaći u zasebnom dokumentu.



Slika 5 ***Usporedba zaštite implementirane pomoću DNS i BGP protokola***

Pružatelji usluga zaštite obično nude sljedeće dvije moguće konfiguracije:

- *on-demand* konfiguracija: promet teče normalno do poslužitelja bez ikakvih preusmjeravanja. Tek nakon što započne DDoS napad, promet se preusmjerava prema centrima za čišćenje.

  Ova opcija se preporuča za računalne sustave kojima ne prijete stalni DDoS napadi te za one koji neće biti teško pogođeni ako dođe do kašnjenja (engl. *latency*) ili kratkog pada usluge (engl. *downtime*) nakon što započne DDoS napad. Naime, u vremenu dok ne traje DDoS napad, budući da promet teče izravno prema poslužitelju, nema kašnjenja. Jednom kad započne DDoS napad, tada može doći do malog kašnjenja jer promet više ne ide izravno prema poslužitelju. Isto tako, u vremenu između početka napada, detektiranja i preusmjeravanja prometa prema centrima za čišćenje, poslužitelj koji je žrtva DDoS napada je izložen neko vrijeme što može rezultirati i kratkim zastojem u pružanju usluge.

- *always-on* konfiguracija: promet se cijelo vrijeme preusmjerava prema centrima za čišćenje, a prema poslužiteljima dolazi samo očišćeni promet.

  Ova opcija je obično skuplja od prethodno spomenute opcije budući da se koristi više kapaciteta propusnosti. Isto tako, ovisno o lokaciji centara za čišćenje, korisnika *web* sjedišta i samog poslužitelja, može postojati određeno kašnjenje kojeg nema ako se koristi opcija *on-demand.*

Pri odabiru opcija za čišćenje potrebno je uzeti u obzir neke čimbenike kako bi se izabrala bolja opcija:

1. Koliko je računalni sustav osjetljiv na kašnjenje?

2. Koja je učestalost DDoS napada?

3. Zadovoljavajući omjer cijena i usluge koju određena opcija pruža.

Neki od poznatijih pružatelja ovakvih usluga zaštite su: Cloudflare, Imperva, Akamai Technologies i DataDome.

2.3.2 CDN – Mreža za dostavljanje sadržaja (engl. *content delivery network*)

CDN je naziv za mrežu distribuiranih poslužitelja koji služe za brzo i pouzdano dostavljanje sadržaja korisnicima.

Pružatelj neke usluge ne koristi svoje poslužitelje za dostavljanje sadržaja svojim krajnjim korisnicima, već sadržaj predaje CDN-u koji ga dostavlja krajnjim korisnicima.

Konkretno, CDN pomaže u olakšavanju posljedica HTTP poplavljivanja budući da omogućuje pohranjivanje statičkih resursa na CDN poslužiteljima. Jednom kada korisnik zatraži neki resurs, poslužitelj koji je dio CDN-a i koji je najbliži korisniku dohvaća taj resurs s njegove originalne lokacije ili ga, u slučaju da se resurs već nalazi kod njega, jednostavno šalje korisniku. Nakon toga, čuva taj resurs kod sebe neko vrijeme ili dok god ga korisnici traže. Zbog pohranjivanja, sustav je otporniji na taj napad.

S druge strane, CDN može funkcionirati i kao obrnuti *proxy* (engl. *reverse proxy*), što između ostalog služi za skrivanje IP adresa. Na taj način, ako napadač pokuša napasti žrtvu volumetričkim napadom, on će zapravo napasti CDN poslužitelje, a ne pravu žrtvu.

CDN poslužitelji raspoređuju promet između sebe te tako održavaju dostupnost usluge čak i kad je jedan ili više poslužitelja nedostupno. Svaki CDN poslužitelj je postavljen na nekoj drugoj lokaciji diljem svijeta te se koristi onaj „najbliži“ (ne geografski, već komunikacijski) korisniku kako bi se dostavio traženi sadržaj. U slučaju povećanja prometa, tj. u slučaju DDoS napada, velika količina prometa koja je namijenjena *web* sjedištima žrtve ne dolazi do njih, već se raspoređuje između CDN poslužitelja. Time je opterećenje svakog poslužitelja manje i očekuje se da je manje od njegovog kapaciteta, pa poslužitelj neće biti potpuno zagušen.

Između ostalog, ono što dodatno može pomoći u olakšanju DDoS napada jest balansiranje opterećenja (engl. *load balancing*). Metoda je korisna jer se njome promet ravnomjerno distribuira između svih poslužitelja.

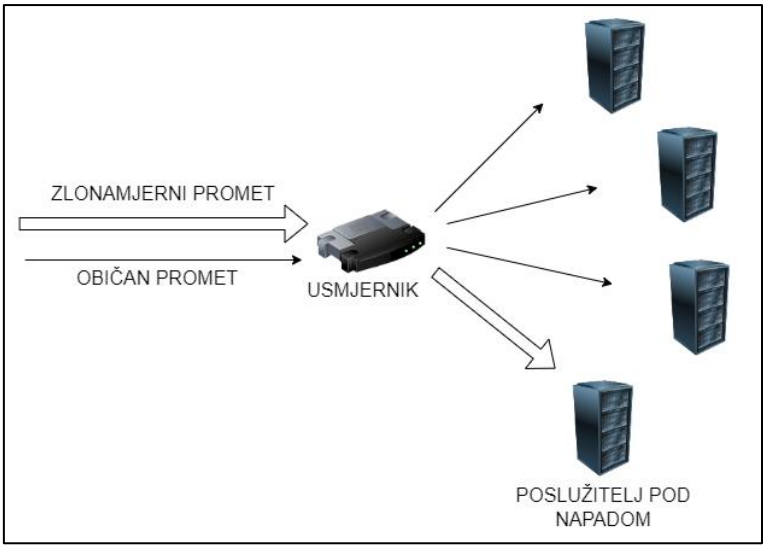
Ova zaštita je automatska, tj. djeluje odmah čim započne napad i ne treba ljudsku intervenciju.

2.3.3 Blackhole routing

Blackhole routing ili *null routing* predstavlja potpunu zabranu mrežnog prometa prema nekoj IP adresi. Pomoću BGP protokola se konfigurira ruta na rubnim usmjernicima (engl. *router*) pružatelja internetskih usluga koja preusmjerava sav promet koji ide prema žrtvi u „crnu rupu“, tj. odbacuje se.

Iako napadač tako zapravo ostvaruje svoj cilj, budući da uskraćuje uslugu legitimnim korisnicima, ovo je ipak ponekad nužno napraviti. Naime, veliki volumetrički napadi mogu zagušiti kapacitet propusnosti infrastrukture kojom prolazi mrežni promet.

Budući da dijelove te infrastrukture koriste i drugi klijenti, *blackhole routingom* se sprječava da i oni budu pod utjecajem napada.



Slika 6 ***Količina prometa koja opterećuje usmjernik ispred poslužitelja pod napadom može biti smetnja i drugim poslužiteljima koji nisu pod napadom, a nalaze se iza istog usmjernika***

Slika 6 prikazuje primjer situacije u kojoj bi *blackhole routing* mogao biti korisna mitigacija (ublažavanje, olakšavanje). Jedan od poslužitelja u mreži je pod volumetričkim DDOS napadom. Na putu do poslužitelja maliciozni promet prolazi kroz usmjernik koji koriste i drugi poslužitelji. Ako je volumetrički napad dovoljno velik usmjernik bi mogao imati problema s obrađivanjem legitimnog prometa namijenjenog za druge poslužitelje koji nisu pod napadom. Korištenjem tehnike „*blackhole routinga*" sav promet namijenjen za poslužitelj koji je pod napadom se može odbaciti na rubnim usmjernicima autonomnog sustava u kojem se poslužitelj nalazi. Cijeli taj proces može biti i automatiziran (engl. *remotely triggered blackhole routing*).

Ova zaštita je reaktivna, nije automatska, tj. treba intervenciju administratora mreža i žrtve i svih uključenih pružatelja komunikacijskih usluga, čim se otkrije napad.

2.3.4 Egress filtriranje

Pružatelji internetskih usluga mogu spriječiti korisnike da šalju mrežne pakete s lažiranom IP adresom. Tako bi se napadi koji se oslanjaju na lažiranje IP adresa (npr. DNS amplifikacijski napad) spriječili na samom izvoru.

Ovo je vrlo učinkovita preventivna mjera, ali problem je u tome što uvođenje te mjere može biti zahtjevno, a samom pružatelju internetskih usluga ne pruža osobitu korist. Zbog toga, iako su napadi koji se oslanjaju na lažiranje izvorne IP adrese poznati već desetljećima, dio ISP-eva i dalje ne sprječava lažiranje IP adresa (21% autonomnih sustava u vrijeme pisanja dokumenta (9)). Ako ISP ne sprječava lažiranje IP adresa, napadač može poslati paket s izvornom IP adresom žrtve, koja se može nalaziti i u nekom drugom ISP-u. To se može koristiti za amplifikacijske napade, koji su detaljnije objašnjeni u poglavlju [1.2.1].

Pružatelji internetskih usluga koji žele spriječiti lažiranje IP adresa mogu na svojim usmjernicima omogućiti RPF (engl. *Reverse-path forwarding*) protokol. Pomoću ovog protokola se odlučuje hoće li se paket prihvatiti ili odbaciti s obzirom na izvorišnu IP adresu paketa te puta kojim je prolazio. U slučaju da put kojim je paket prolazio ne odgovara izvorišnoj IP adresi, u smislu da taj put nije moguć s te izvorišne IP adrese, može se zaključiti da je ona lažirana i paket će biti odbačen.

Ovo je preventivna mjera i zahtijeva jednokratnu aktivnost administratora mreža pružatelja komunikacijskih usluga.

2.3.5 Ograničenje broja javno izloženih UDP servisa

Ograničenje broja javno izloženih (da ga bilo tko može koristiti) UDP servisa ili konfiguriranje tih servisa na način da se ne mogu lako koristiti za amplifikacijske napade bi otežalo takve napade.

Primjerice, uglavnom ne postoji razlog da Memcached servis[5], koji se može koristiti za jake amplifikacijske DDOS napade bude izložen (na raspolaganju bilo kojem korisniku). S druge strane postoje legitimni razlozi da DNS servis bude javno izložen, no u tom slučaju se može konfigurirati *Response Rate Limiting* kako bi se otežalo iskorištavanje DNS servisa za amplifikacijske napade.

Slično prethodnoj mjeri, ova mjera ne štiti izravno organizaciju koja ju je provela, ali može zaštiti ostale organizacije koje bi mogle biti žrtve DNS amplifikacijskih napada.

2.4 Open source alat: Gatekeeper

Gatekeeper[6] je *open source* sustav za zaštitu protiv DDoS napada. Nije namijenjen za osobno korištenje, već je namijenjen raznim institucijama, servisima i pružateljima nekog sadržaja.

Autonomni sustav (u nastavku AS) koji želi koristiti Gatekeeper kao sredstvo zaštite treba postaviti i pokrenuti Gatekeeper i njegove komponente. Na više različitih geografskih lokacija je potrebno strateški postaviti „*Vantage Points*“ (u nastavku VP). VP-ovi mogu primjerice biti točke internetske razmjene (engl. *Internet Exchange Point*) ili data centri u oblaku. VP-ovi mogu podnijeti veliku količinu prometa.

Na VP-u se instalira Gatekeeper komponenta koja odlučuje hoće li promet biti poslan prema odredištu (AS-u) ili ne. Gatekeeper serveri oglašavaju putem BGP-a put do AS-a kojeg je potrebno zaštititi. Na taj način, promet će biti preusmjeren prema najbližem VP-u. Ako dođe do DDoS napada, sav zlonamjerni promet će biti distribuiran po VP-ovima koji su najbliži izvoru tog prometa. Primjerice, po raznim lokacijama u Europi i Sjevernoj Americi su distribuirani VP-ovi. Računala koji su dio *botneta* napadača koji izvršava DDoS napad se nalaze na različitim kontinentima. U tom slučaju će promet zombi računala iz Europe ići kroz njima najbliži VP u Europi, dok će promet zombi računala iz Sjeverne Amerike ići kroz njima najbliži VP u Sjevernoj Americi. Naravno, VP kao i zombi

[5] Softver otvorenog koda koji služi za spremanje podataka u međuspremnik (engl. *cache*)
[6] Detaljnije o Gatekeeperu se može pročitati na GitHub stranici.

računala se mogu nalaziti i na ostalim kontinentima, ali je za lakše razumijevanje dan primjer s Europom i Sjevernom Amerikom. Budući da je promet distribuiran po VP-ovima, teže će biti opteretiti jednog.

Grantor komponenta koja se instalira u AS-u odlučuje o politikama koje će se izvršavati na VP-u. Ona aktivno komunicira sa Gatekeeper komponentom.

Za osnovni rad se preporučuje da su AS i VP povezani privatnom rutom koja ne sadrži neku javnu IP adresu. Ovo se može ostvariti na više načina, a koji način će točno biti odabran ovisi o korisnicima koji koriste Gatekeeper. Na taj način, nad usmjernicima između AS-a i VP-a se neće moći izvršiti DoS napad.

Iz svega navedenog se može primijetiti da Gatekeeper može izdržati DDoS napade velikih volumena. Za detaljnije objašnjenje treba proučiti GitHub stranicu Gatekeepera na kojoj se nalaze i detaljne upute kako ga instalirati.

3 Zaključak

Postoje razne metode i rješenja koja pomažu u zaštiti protiv DDoS napada, kao i u ublažavanju DDoS napada ako dođe do njega.

Napadi na aplikacijskom i mrežnom sloju se mogu ublažiti pažljivom konfiguracijom servisa i redovitim ažuriranjem operacijskog sustava. Razna softverska ili hardverska rješenja također mogu pomoći u detekciji i ublažavanju napada.

S druge strane volumetrički napadi se moraju rješavati prije nego što promet dođe do poslužitelja, u mreži većeg kapaciteta propusnosti (mreži pružatelja internetskih usluga, javnom ili privatnom oblaku).

4 Literatura

1. **Cimpanu, Catalin.** Avast and French police take over malware botnet and disinfect 850,000 computers. [Mrežno] 28. kolovoza 2019. [Citirano: 10. listopada 2022.] https://www.zdnet.com/article/avast-and-french-police-take-over-malware-botnet-and-disinfect-850000-computers/.

2. **Shankland, Stephen.** How startup GitHub survived a massive five-day network attack (Q&A). [Mrežno] 17. travnja 2015. [Citirano: 10. listopada 2022.] https://www.cnet.com/news/privacy/how-startup-github-survived-a-massive-five-day-network-attack-q-a/.

3. **Cluley, Graham.** DDoS attack on Minecraft Twitch tournament disruted Andorra's internet access. [Mrežno] 28. siječnja 2022. [Citirano: 10. listopada 2022.] https://www.bitdefender.com/blog/hotforsecurity/ddos-attack-on-minecraft-twitch-tournament-disrupted-andorras-internet-access/.

4. **Pritchard, Stephen.** What is DDoS? A complete guide. [Mrežno] 16. prosinca 2021. [Citirano: 19. svibnja 2022.] https://portswigger.net/daily-swig/what-is-ddos-a-complete-guide.

5. **Cloudflare.** What is the OSI Model? [Mrežno] [Citirano: 10. listopada 2022.] https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/.

6. **Apache.** Apache Performance Tuning. [Mrežno] [Citirano: 28. lipnja 2022.] https://httpd.apache.org/docs/2.4/misc/perf-tuning.html.

7. **Sullivan, Bryan.** Security Briefs - XML Denial of Service Attacks and Defences. [Mrežno] 13. kolovoza 2015. [Citirano: 10. listopada 2022.] https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/november/xml-denial-of-service-attacks-and-defenses.

8. **SANS Institute.** Global Information Assurance Certification Paper. [Mrežno] [Citirano: 28. lipnja 2022.] https://www.giac.org/paper/gsec/2013/syn-cookies-exploration/103486.

9. **Caida.** State of IP Spoofing. [Mrežno] [Citirano: 10. listopada 2022.] https://spoofer.caida.org/summary.php.

10. **Imperva.** DDoS attacks. [Mrežno] [Citirano: 13. svibnja 2022.] https://www.imperva.com/learn/ddos/ddos-attacks/.

11. —. Distributed Denial of Service. [Mrežno] [Citirano: 13. svibnja 2022.] https://www.imperva.com/learn/ddos/denial-of-service/.

12. **Cloudflare.** What is a DDoS attack? [Mrežno] [Citirano: 13. svibnja 2022.] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

13. —. What is DDoS blackhole routing? [Mrežno] [Citirano: 26. svibnja 2022.] https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/.

14. —. What is rate limiting? [Mrežno] [Citirano: 26. svibnja 2022.] https://www.cloudflare.com/learning/bots/what-is-rate-limiting/.

15. **Datadome.** How does DDoS protectio work. [Mrežno] 22. lipnja 2019. [Citirano: 31. svibnja 2022.] https://datadome.co/learning-center/how-does-ddos-protection-work/.

16. **Cisco.** Cisco Secure DDoS Protection: Global Scrubbing Centers Data Sheet. [Mrežno] 25. lipnja 2021. [Citirano: 31. svibnja 2022.] https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-scrubbing-center-ds.html.

17. **Cloudflare.** What is a CDN? [Mrežno] [Citirano: 31. svibnja 2022.] https://www.cloudflare.com/learning/cdn/what-is-a-cdn/.

18. —. [Mrežno] [Citirano: 31. svibnja 2022.] https://www.cloudflare.com/learning/cdn/glossary/anycast-network/.

19. —. What is a Web Application Firewall (WAF)? [Mrežno] [Citirano: 31. svibnja 2022.] https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/.

20. **Graham-Cumming, John.** No Scrubs: The Architecture That Made Unmetered Mitigation Possible. [Mrežno] 25. rujna 2017. [Citirano: 8. lipnja 2022.] https://blog.cloudflare.com/no-scrubs-architecture-unmetered-mitigation/.

21. **Radware.** Threat Alert: TCP Amplification Attacks. [Mrežno] 9. studenog 2019. [Citirano: 15. lipnja 2022.] https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/.

22. **Cloudflare.** Slowloris DDoS attack. [Mrežno] [Citirano: 15. lipnja 2022.] https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/.

23. **Imperva.** Border Gateway Protocol (BGP). [Mrežno] [Citirano: 28. lipnja 2022.] https://www.imperva.com/learn/ddos/border-gateway-protocol-bgp/.

24. **Stowm Wall.** Protecting your network from DDoS attacks using BGP. [Mrežno] [Citirano: 28. lipnja 2022.] https://stormwall.network/network-protection.

25. **Caida.** Spoofer: FAQ. [Mrežno] [Citirano: 28. lipnja 2022.] https://www.caida.org/projects/spoofer/faq/.

26. **Huawei.** NE40E V800R010C10SPC500 Configuration Guide - Security 01. [Mrežno] [Citirano: 28. lipnja 2022.] https://support.huawei.com/enterprise/en/doc/EDOC1100055025/621e8ebd/urpf-overview.

27. **Cloudflare.** What is a DNS flood? [Mrežno] [Citirano: 21. lipnja 2022.] https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/.

28. **Java T point.** TCP/IP model. [Mrežno] [Citirano: 9. kolovoza 2022.] https://www.javatpoint.com/computer-network-tcp-ip-model.

29. **Mary E. Shacklett, Amy Novotny, Kate Gerwig.** TCP/IP. [Mrežno] [Citirano: 9. kolovoza 2022.] https://www.techtarget.com/searchnetworking/definition/TCP-IP.

30. **GeeksforGeeks.** TCP/IP Model. [Mrežno] 30. rujna 2020. [Citirano: 9. kolovoza 2022.] https://www.geeksforgeeks.org/tcp-ip-model/.

31. **ISC.** What is the Response Rate Limiting Feature in BIND? [Mrežno] 20. srpnja 2021. [Citirano: 9. kolovoza 2022.] https://kb.isc.org/docs/aa-01148.

32. **Cloudflare.** Memcached DDoS attack. [Mrežno] [Citirano: 9. kolovoza 2022.] https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/.