Ako se odlučite za samostojeći uređaj, to je kutija standardnih serverskih gabarita, ukrašena šarenim listićima, koji su dio Arborova vizualnog identiteta

Jamac vaše dostupnosti

Rajko Plečko

Nedavno smo pisali o skupini rješenja pod imenom Availability Protection System (APS), Arbor Edge Defense (AED) te ATLAS Intelligence Feed (AIF), tvrtke Arbor Networks. Prema istraživanju nezavisne tvrtke Quadrant Knowledge Solutions za 2017. godinu, u branši kompanija koje se bave umanjivanjem utjecaja DDoS napada, Arbor je usamljen u gornjem desnom kutu. Za one koji nisu familijarni s kvadrantnim prikazima uspješnosti, to znači da tvrtka ima najveći tržišni udio i vrhunsku tehnologiju za svoju grupu proizvoda.

SAMOSTOJEĆI UREĐAJ

O čemu se zapravo radi? Proizvod na kojem leži Arborov uspjeh u najjednostavnijoj inačici jest samostojeći uređaj koji se načelno postavlja između *routera,* koji vas (vašu tvrtku) povezuje s Internetom, te *firewalla,* koji bi vas trebao štititi od neželjenog prometa u oba smjera. Budući da procesorski snažna i brza računala, koja su u virtualnom okruženju u stanju pogoniti veći broj servera raznih operacijskih sustava, nisu više nedostupna ni manjim kompanijama, Arborovo rješenje može se implementirati i kao virtualni uređaj na jednom od vaših *hostova* koji vrte i sve ostale vaše servise. No zaštitu od DoS odnosno DDoS napada nije moguće implementirati samostalno i bez pomoći izvana. Naime, DDoS napad prema definiciji je tip napada gdje se ciljani sustav (mreža) zasipa ogromnom količinom prometa, koji ni po čemu osim po količini ne mora

Arbor Networks APS2600

Kućište	**2U *rack mount***
Napajanje	**2x redundantno**
Diskovi	**2x 120 SSD (2x 240 SSD)**
Memorija	**32 GB**
CPU	**2x Intel Xeon (12 jezgri)**
OS	***Proprietary embedded* ArbOS**
Upravljački priključci	**2x10/100/1000 BaseT + serijski *port***
Štićeni priključci	**1Gx4, 8 ili 12 (bakar, sx fiber, lx fiber), 4x10G *portovi***

+ Nakon instalacije i inicijalnog podešavanja ne zahtijeva naročitu pažnju, ima pregledne ekrane za nadzor i brzo uočavanje nepravilnosti

– Ako vas ne muči činjenica da će u trenutku obrane od velikih napada vaš promet trebati proći kroz Arbor Cloud koji nije pod vašim nadzorom, drugih zamjerki nema

Dojam: Moćan sustav za obranu od DDoS-a, iza kojeg stoji ogroman i kompleksan *cloud*

Cijena **7.092 USD** godišnje
(APS Virtual Subscription License -100 Mbps Tier)

Ustupio Veracomp, www.veracompadria.com

Nakon nedavnog druženja sa specijalistima Arbor Networksa, gdje je postojećim i budućim korisnicima predstavljeno napredno rješenje za borbu protiv DDoS napada, došli smo u priliku i pobliže se upoznati s proizvodom koji se već neko vrijeme na svjetskoj razini uspješno nosi s napadima raznih intenziteta, koji za cilj imaju ograničiti ili onemogućiti dostupnost servisima većih i manjih kompanija

biti problematičan. U takvoj situaciji ciljani sustav nije u stanju odgovoriti na sve upite koji dolaze do njega i postaje nedostupan. Bilo kakvo samostalno i izolirano rješenju u takvoj je situaciji nemoćno jer neželjeni promet je već na ulazu u našu mrežu i količina prometa je takva da je u potpunosti zagušila našu vezu sa svijetom. Tu se pokreće mehanizam koji odmah nakon detekcije napada sav promet prema napadnutoj mreži preusmjerava na servere u Arborovom *cloudu*, koji su u stanju sav sadržaj pregledati i u realnom vremenu ga, očišćenog od "smeća" korištenjem GRE tunela, vratiti prema nama.

Kako bi takva redirekcija prometa bezbolno i trenutačno funkcionirala, potrebno je zadovoljiti neke preduvjete. Jedno od rješenja je da krajnji korisnik bude "vlasnik" svojih javnih IP adresa, što znači da ih mora zatražiti od nadležnih tijela kako bi nakon dobivanja AS broja od *providera* mogao dobiti *routanje* prometa BGP protokolom.

BGP je jedan od najvažnijih *routing* protokola i upravo na njemu se temelji kičma Interneta. Jedna od značajki mu je da "svoje adrese" možete preseliti bilo kuda i zadržati ih neovisno o *provideru*. Isto tako nam u slučaju detektiranog napada omogućuje spomenutu redirekciju prometa prema Arborovom *cloudu* i prije nego što promet dođe do naših mrežnih uređaja.

Ako korisnik nije vlasnik dodijeljenih javnih IP adresa, nego su one u vlasništvu *service providera*, onda se on, *provider*, mora složiti da će u slučaju potrebe raditi redirekciju adresa.

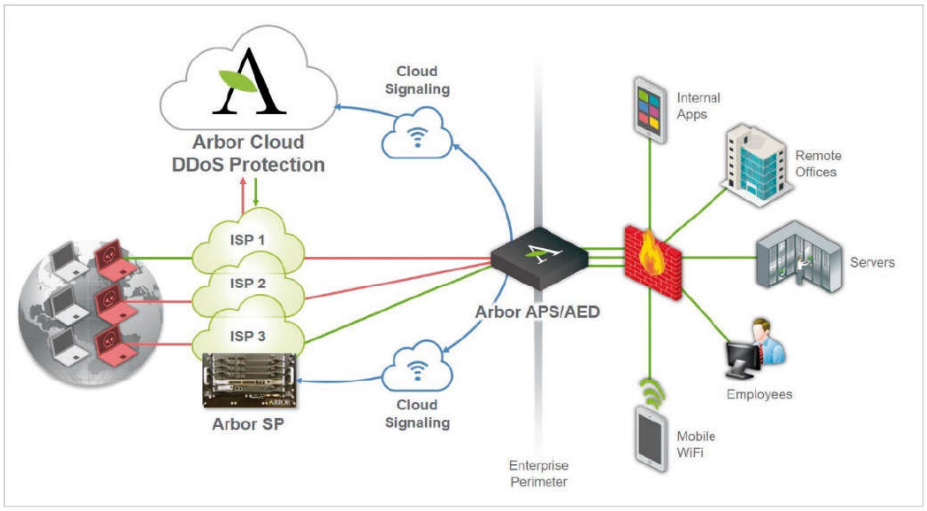
Postoji i mogućnost DNS redirekcije, ali ona funkcionira samo za servise bazirane na DNS-u. Dakle, napad prema IP adresi, a ne prema FQDN-u, ovako ne možemo odbiti.

Ako smo zadovoljili neki od spomenutih preduvjeta, možemo se upustiti u instalaciju i konfiguraciju Arborova sustava, koju ćemo ukratko opisati. U stvarnom životu dobar će dio biti unaprijed konfiguriran, a fino podešavanje će za vas vjerojatno napraviti specijalisti ovlaštenog partnera, a možete računati i na pomoć od strane ovlaštenog distributera, pa čak i samog vendora, jer je za to potrebno dosta specifičnih znanja i iskustava.

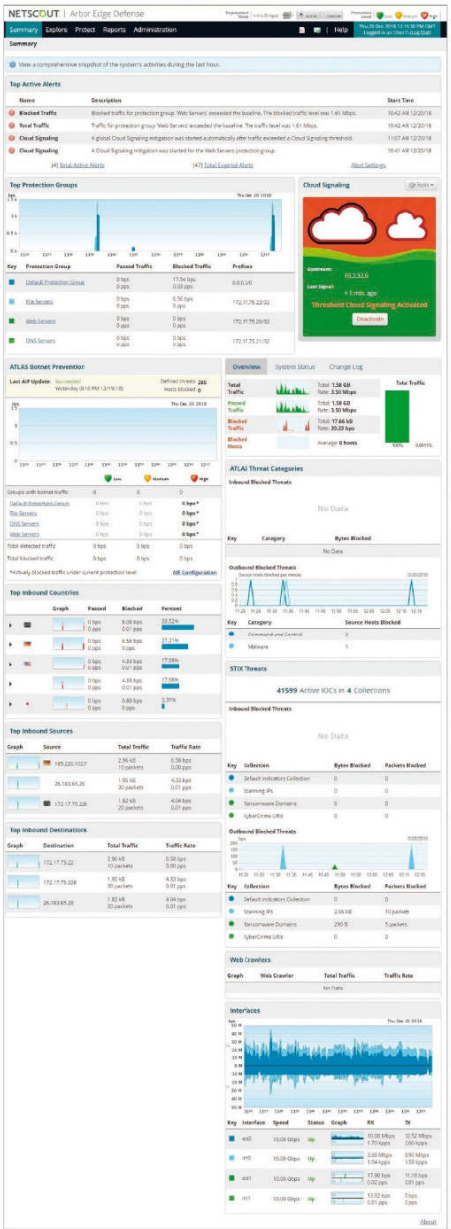
KORAK PO KORAK

Na inicijalnom ekranu prije svega možemo dobiti informaciju o načinu rada uređaja i primijenjenoj razini zaštite. Način rada može biti pasivan ili aktivan. U pasivnom načinu rada uređaj će samo detektirati problematične situacije, a u drugom i reagirati na unaprijed određeni način. Razine zaštite su unaprijed postavljeni pragovi iznad kojih će uređaj podrazumijevati da se radi o nekom neželjenom prometu ili akciji, a koji se nakon provedene analize prometa i postavljenih *baselineova* mogu i fino podesiti prema potrebama korisnika. Možemo ih prilagoditi prema svakom definiranom objektu ili grupi objekata. Iako pragovi reagiranja na pojedine tipove ugroza dolaze preddefinirani, tek nakon procesa finog podešavanja doći ćemo do stvarnih, na naš sustav primjenjivih, vrijednosti. Do njih ćemo doći tako da instalirani uređaj desetak dana ostavimo u takozvanom "*profile capture*" načinu rada, u kojem će samo analizirati svakodnevni promet i opterećenje te tako stvoriti profil normalnog rada. Nakon što pregledamo i dodatno ručno podesimo rezultate razdoblja učenja, uređaj možemo pustiti u rad.

U okviru "Cloud Signaling" vidljiv je status povezivanja s Cloud Scrubing centrom, koji



Pozicioniranje Arbor APS/AED uređaja na rubu mreže, Cloud Signaling i povezivanje s Arbor Cloudom



Inicijalni ekran s obiljem informacija nad kojim će administratori provesti najviše vremena jer objedinjuju informacije o svim funkcionalnostima sustava

će nam biti od pomoći pri volumetrijskim napadima, prevelikim da bismo im se othrvali na licu mjesta (*on-premise*). Cloud Signaling je točka u kojoj se nakon premašenih pragova odlučuje (u dogovoru s Cloudom) o redirekciji prometa, a ako za to postoji razlog, može se i isključiti.

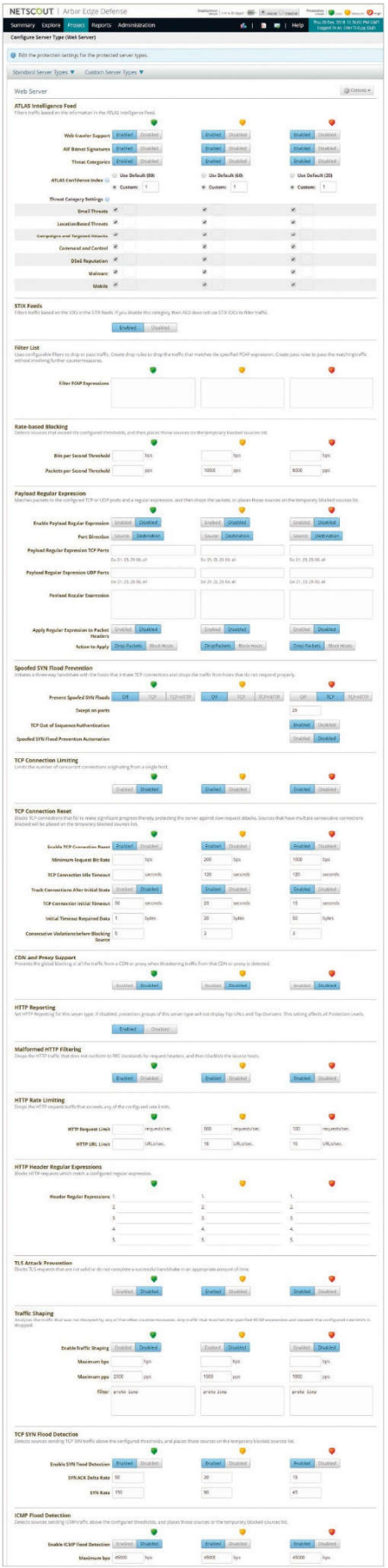
Na istom ekranu na raspolaganju je još cijeli niz informacija koji će administrativnom osoblju vrlo brzo otkriti da se radi o nekakvoj nelegalnoj situaciji, pokazati što se trenutačno radi na otklanjanju problema i mnoge druge.

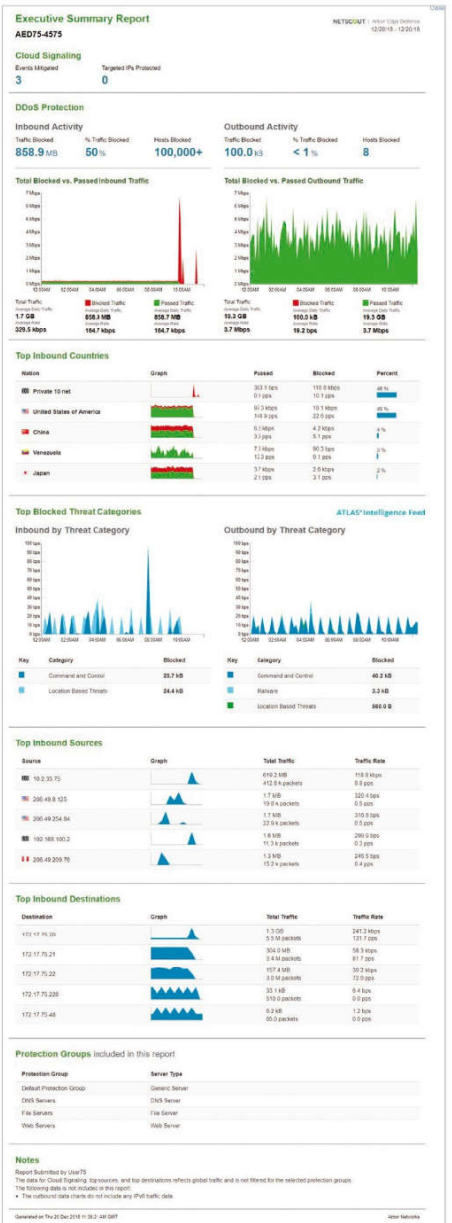
Sljedeća važna kartica zove se Protect, i to je mjesto na kojem će administrator podesiti način i parametre povezivanja s Cloudom te konfigurirati *inbound* i *outbound* zaštitu. I tu većina parametara dolazi unaprijed podešena, ali to nikako ne znači da takva treba i ostati. Radi se o velikom broju parametara koji će s jedne strane pomoći čuvanju mreže od vanjskih napadača, a s druge spriječiti iniciranje neželjenih aktivnosti s računala u lokalnoj mreži prema Internetu, ako se dogodilo da imamo "zaraženih" računala koja bi se željela povezati sa svojim kontrolnim centrom (CNC) i sudjelovati u DDoS napadu na nekog drugog.

Još jedna funkcionalnost koju je vrijedno spomenuti je vrlo opsežan i detaljan "Executive Summary Report" koji je, kako mu ime kaže, namijenjen menadžmentu, kako bismo na brz, jednostavan i pregledan način dobili sve potrebne informacije o radu sustava, kao što je količina blokiranog prometa ili *hostova*, lista napadača prema državi ili IP adresi s koje je napad došao, lista blokiranih prijetnji prema kategoriji, popis grupa zaštite i mnoge druge.

Uređaj, odnosno softver, licencira se prema količini prometa koji u realnom vremenu želimo provjeravati, tako da imamo razne "*tierove*" – za 100 i 500 Mbit/s te 1, 2, 5, 10, 15 i 20 Gbit/s. APS licenca za najniži, 100-megabitni *tier* košta oko 7.000 USD godišnje.

Radi se o vrlo korisnoj "napravi", iza koje stoji ogroman i kompleksan Arbor Cloud. Dotični se u dosadašnjem radu pokazao sposobnim "sažvakati" napade i do 1,7 Tbit, s obećanjem proizvođača da je to tek dvadesetak posto prometa koji je *cloud* spreman podnijeti. Ako vaše poslovanje ovisi o internetskoj dostupnosti, a imajući u vidu lakoću i cijenu za koju se DDoS napad na crnom tržištu može kupiti i usmjeriti na koga god želite, život na internetskoj vjetrometini postaje sve teže zamisliti bez ovakvog uređaja.





Report je izvrstan i sažet pregled svih akcija koje je sustav poduzeo u proteklom vremenu, namijenjen menadžmentu

U kartici Protect nalaze se svi "podesivi" parametri sustava za koje je uputno angažirati profesionalnu pomoć