VATROZIDI I PRIMJERI NJIHOVE PRIMJENE

Gudelj, Ivan

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni preddiplomski studij računarstva

VATROZIDI I PRIMJERI NJIHOVE PRIMJENE

Završni rad

Ivan Gudelj

Osijek, 2021.

SADRŽAJ

1. UVOD

Pojam vatrozid izvorno se odnosio na zid namijenjen da ograniči vatru ili potencijalni požar unutar zgrade, kasnije se odnosio na slične strukture, kao što je lim koji razdvaja motor u autu ili na avionu od putničke kabine. Vatrozidna tehnologija kojom se koristimo danas, nastala je kasnih 1980-ih godina kada je internet još uvijek bio prilično nova tehnologija u smislu globalnog korištenja i povezivanja.

Svakog dana dođe do velikog broja napada hakera na određeno računalo ili određeni uređaj. Osim toga mnoga računala nisu zaštićena antivirusom te se služe internetom pa također jedan od čestih problema jest zaraženost uređaja sa raznim virusima. Postavlja se pitanje kako se zaštititi od navedenih napada. Za realizaciju zaštite od navedenih problema u mrežnu strukturu potrebno je implementirati vatrozid.

U drugom poglavlju će sam pojam vatrozida biti detaljno objašnjen kao i njegove ranije tehnologije i primjene istih. Za istinsko razumijevanje rada vatrozida potrebno je proučiti i vrste mogućih napada na mrežu kako bi pravilno konfigurirali postavke vatrozida, što će biti obrađeno u trećem poglavlju. Četvrto poglavlje će opisati samu instalaciju i primjenu Endian vatrozida za jednu lokalnu mrežu koja će se sastojati od nekoliko računala, servera i telefonske centrale.

1.1. Zadatak završnog rada

U završnom radu potrebno je detaljno opisati i objasniti pojam vatrozida (pojam, vrste, načela rada, doprinos sigurnosti). Prikazati primjere njihove primjene kroz implementaciju (od instalacije i podešavanja do praćenja i nadzora rada) u različitim realnim situacijama.

2. VATROZID I NJEGOVE PRETHODNE TEHNOLOGIJE

2.1. Što je vatrozid?

Vatrozid (eng. *firewall*) je moguće definirati kao sigurnosni element smješten između neke lokalne mreže i javne mreže (Interneta) čije je namjena zaštita povjerljivih, korporativnih i korisničkih podatka od neautoriziranih korisnika. Navedeno se provodi blokiranjem i zabranom prometa po pravilima koja definiraju usvojena sigurnosna pravila. Vatrozid bi trebao imati mogućnosti upravljanja i kontrole mrežnog prometa, autorizacije pristupa, očuvanja resursa te snimanja i obavještavanja u slučaju nekog događaja tj. napada i sposobnost brzog izvršavanja svih zadataka kako ne bi postao *bottleneck* odnosno smetnja u mreži.

Za dobrobit organizacije ne moraju svi korisnici unutar mreže imati jednaka prava pristupa Internetu. Moguće je kontrolirati prava pristupa korisnika u određenim dijelovima mreže na način da se postavi vatrozid između dva ili više mrežnih dijelova. Pri navedenome, vatrozid je implementiran tako da dopušta pristup valjanim zahtjevima, dok blokira ostale zahtjeve.

Moguće je definirati dvije vrste vatrozida; softverski i hardverski. Kada je riječ o softverskom vatrozidu, zaštićeno je jedno računalo s iznimkom računala predodređenih za zaštitu čitave mreže. U slučaju iznimke, potrebno je implementirati vatrozid na računalo koje je spojeno na dvije mreže, odnosno između vanjske mreže (nezaštićeni dio) i unutarnje mreže (zaštićeni dio). U navedenom slučaju, postoji mogućnost smanjene brzine mrežnog prometa zbog obavljanja različitih provjera paketa. Posljedično, poželjno je koristiti računalo koje omogućava brzo filtriranje paketa. S druge strane, danas se sve češće koriste hardverski vatrozidi kod kojih se maksimizira brzina promjene dok se u isto vrijeme olakšava konfiguracija samog vatrozida. Kako bi vatrozid radio bez poteškoća, nužno je definirati niz pravila koja će odrediti koje vrste prometa su dopuštene, a koje zabranjene.

Većina operacijskih sustava osobnih računala sadrži vatrozide (u obliku programske podrške) za zaštitu protiv prijetnji sa Interneta, također većina usmjerivača (eng. Router) koji šalju podatke između mreža sadrže vatrozidne komponente i, obrnuto, većina vatrozida može obavljati osnovne funkcije routera.

2.2. Povijest Vatrozidne tehnologije

2.2.1. Prva generacija: “stateless” filteri paketa

Prema [1] prvi članak objavljen u vezi vatrozidne tehnologije bio je u 1988, kada su inženjeri firme Digital Equipment Corporation (DEC) [1] razvili filterski sustav poznat kao filter paketa. Ovaj osnovni sustav bio je prva generacija onoga što je danas tehnička mogućnost internet sigurnosti. U kompaniji AT&T Bell Laboratories, Bill Cheswick i Steve Bellovin nastavljali su svoje istraživanje u filterima paketa i razvili radni model za svoju vlastitu kompaniju osnovanu na njihovoj originalnoj ideji arhitekture prve generacije.

Paketni filtri vrše ulogu inspekcije "paketa" koji su razmijenjeni između računala na Internetu. Ako se paket slaže sa skupom filtrirajućih pravila filtera paketa, paketni filter će propustiti, tiho odbaciti ili ga odbaciti (odbaciti, te poslati "poruku greške" izvoru). Ovaj tip filtriranja paketa ne posvećuje pažnju bilo da je paket dio postojećeg prometnog toka (npr. ne sadrži informacije ili "stanje" veze). Paketni filteri obično dozvoljavaju ili odbijaju promet bazirano na:

- Izvornoj i odredišnoj IP adresi
- Protokolima, kao što su TCP, UDP ili ICMP
- Izvornim i odredišnim portovima i ICMP tipovima i kodovima
- Oznakama u TCP zaglavlju, kao što je da li je paket zahtjev za povezivanje
- Smjeru (ulazni ili izlazni)
- Kroz koje fizičko sučelje paket prolazi

Vatrozidi paketnog filtriranja rade uglavnom na prva tri sloja OSI modela, što znači da je većina rada obavljena između mreže i fizičkih slojeva, sa malo "provirivanja" u transportni sloj radi saznavanja izvornih i odredišnih brojeva porta. Kada paket dolazi od pošiljaoca i filtrira se kroz vatrozid, uređaj provjerava sličnosti sa bilo kojim od paketa koji su podešeni u pravilima vatrozida, a zatim propušta ili odbija paket u skladu s tim. Kada paket prolazi kroz vatrozid, on filtrira paket prema protokol/port brojevnoj bazi (GSS)[1]. Npr., ako pravilo u vatrozidu postoji da blokira „telnet“ pristup, tada će vatrozid blokirati TCP protokol za port broj – 23

Svi paketi filtera imaju zajednički kriterij a to je da se povjerenje bazira na IP adresama. Iako ovaj tip zaštite nije dovoljan za cijelu mrežu, prihvatljiv je na razini komponente.Većina IP paketnih filtera je bez stanja, što znači da oni ne pamte ništa o paketima koje su prethodno

obradili. Paketni filter sa stanjem može čuvati neke informacije o prethodnom prometu, što nam daje mogućnost konfiguracije da su s interneta dozvoljeni samo odgovori na zahtjeve s unutarnje mreže. Paketni filteri bez stanja su osjetljivi na podvale, zato što se izvorna IP adresa i ACK bit u zaglavlju paketa mogu lako probiti.

2.2.2. Druga generacija: "stateful" filteri paketa

Od 1989–1990. tri kolege sa AT&T Bell Laboratories, Dave Presetto, Janardan Sharma i Kshitij Nigam, razvili su drugu generaciju vatrozida koji nastavljaju rad prethodnika prve generacije ali operiraju do sloja 4 Open Systems Interconnection (OSI) modela – transportnog sloja. Prema [1], osnovna razlika između prve i druge generacije vatrozida jest ta da vatrozidi druge generacije pohranjuju stanja veze odnosno prate uspostavljene tokove podataka i sve pakete koji pripadaju istim. To se dobija zadržavanjem paketa sve dok dovoljno informacija nije dostupno da se napravi sud o cjelokupnom stanju. Vatrozid s pamćenjem stanja snima sav promet i određuje da li je paket početak nove veze, dio postojeće veze, ili pak nije paket niti jedne veze.

Kod donošenja odluke o tome hoće li se paket propustiti ili odbaciti se u obzir uzima i prijašnja inspekcija odgovarajućih paketa odnosno paketa s iste IP adrese ili paketa na istom portu. Temeljna pravila za prihvaćanje ili odbijanje paketa su ista kao i kod vatrozida bez mogućnosti pamćenja stanja.

Najveću prednost vatrozida druge generacije predstavlja automatizirano pisanje pravila za protok ulaznih i povratnih podataka tj. ukoliko ste administrator mreže ne morate pisati brojna (također i nesigurna zbog mogućnosti pogreške) pravila za svaki port ili izvor podataka kako biste dopustili povratne podatke. Nadalje prednosti predstavlja i mogućnost definiranja veze koristeći se jednim pravilom (za definiranje veze koristeći se vatrozidom bez mogućnosti pamćenja bila su potrebna minimalno dva pravila) što predstavlja manje posla za administratora.

2.2.3. Treća generacija: Proxy vatrozid / vatrozid aplikativnog sloja

Gene Spafford sa Purdue Sveučilišta, Bill Cheswick iz AT&T Bell Laboratories i Marcus Ranum su definirali vatrozid treće generacije kao vatrozid na aplikacijskom sloju čija je prva inačica lansirana u prodaju 1991. godine.

Proxy vatrozid se može ponašati kao posrednik između klijenta i servera (primatelja i pošiljaoca podataka), spremati (*cache-ati*) web stranice kako bi se smanjio broj zahtjeva u protoku podataka, sažeti podatke, filtrirati promet te uočavati viruse koji štete mreži klijenta. Bitno je spomenuti i da se proxy vatrozid može koristiti za skrivanje korisničkih podataka od servera što znači da se proxy vatrozid može i ponašati kao proxy server (ima vlastitu IP adresu te podaci prvo stižu na njega, potom se analiziraju i predaju ostatku mreže ukoliko ih vatrozid propusti)

Ključna korist filtriranja aplikativnog nivoa je ta da on "razumije" određene aplikacije i protokole kao što su File Transfer Protocol (FTP), Domain Name System (DNS) ili Hypertext Transfer Protocol (HTTP), što je korisno jer je u mogućnosti da otkrije ukoliko neka neželjena aplikacija pokušava zaobići vatrozid na dozvoljenom portu, ili da otkrije ako se protokol zloupotrebljava u bilo kojem štetnom načinu. Od 2012, tzv. next-generation firewall (NGFW) nije ništa drugo nego proširena inspekcija u aplikacijskom nivou. Postojeća inspekcija paketa modernih vatrozida je proširena da sadržava preventivni sistem intruzije (IPS), integraciju korisničkog identiteta (povezivanje ID-ova sa IP ili MAC adresama radi "stvaranja reputacije").

Proxy vatrozidi su najsigurniji od navedenih zbog toga što imaju mogućnost sprječavanja direktnog mrežnog povezivanja sa drugim sustavima sa kojima je ostvarena veza budući da imaju vlastitu IP adresu. Imaju i mogućnost procjene prijetnje od strane nekog napada ukoliko dođe do istog te svojom primjenom uvelike smanjuje broj napada u organizacijama koje su ga implementirale. Uvjerljivo najveći nedostatak predstavlja to što ukoliko dođe do njegovog zakaženja, zakazao je cijeli sustav (Single point of failure). Također je jedan od nedostataka usporavanje ostatka mreže što se tiče performansi zbog analize više podataka [3] .

2.3. Vrste vatrozida i njihovi principi rada s obzirom na način pregleda paketa

Sve vatrozide možemo podijeliti na one sa:

- Statičkim filtriranjem paketa (primijenjeni kod prve generacije vatrozida)
- Dinamičkim filtriranjem paketa

2.3.1. Statičko filtriranje paketa (eng. stateless inspection)

Temeljni dio svakog vatrozida predstavlja filtriranje paketa. Filtriranje paketa određuje treba li mrežni paket biti proslijeđen na drugu mrežu. Pri obavljanju ovog dijela, moguće je definirati različite vrste podataka kao što su broj fragmentiranih paketa, odredišni port, informacije o tablici usmjeravanja paketa, vrsta protokola i IP adrese odredišta i izvorišta.

Filtriranje paketa ovisno o vrsti protokola

Protokolno filtriranje paketa temeljeno je na sadržaju IP protokolnog polja. Korišten protokol namijenjen je za određivanje hoće li se paket proslijediti ili ne, pri čemu postoje različite vrste protokola kao što su User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP).

Filtriranje paketa ovisno o IP adresama odredišta tj. izvorišta

IP filtriranje razlikuje se od ostalih vrsta filtriranja prema tome što omogućava zabranu povezivanja prema određenim mrežama i/ili računalima, ovisno o njihovim IP adresama. U slučaju kada je potrebno zaštititi mrežu od neovlaštenih korisnika, moguće je zaustaviti promet mrežnih paketa čije odredište sadrži određene IP adrese. S druge strane, navedeni pristup nije učinkovit jer neovlašteni korisnici imaju mogućnost promjene IP adrese. Učinkovitiji pristup ovoj vrsti filtriranja je stvaranje IP tablica s poznatim IP adresama te omogućavanje prometa paketima koji dolaze s IP adresa koje se nalaze u tablici. Ukoliko neovlašteni korisnici mreže dođu do sadržaja navedene tablice, mogu koristiti neku od IP adresa iz iste.

Filtriranje paketa ovisno o odredišnim tj. izvorišnim portovima

Pri spajanju dvaju računala, oba računala koriste određene pristupne portove, kojih je ukupno 65536. Prva 1024 porta su osigurana su predviđene aplikacije i nije ih moguće koristiti za neke druge. Primjer navedenog je sljedeće; HTTP koristi port 80, FTP koristi portove 20 i 21, DNS koristi port 53 itd.. Administrator ima mogućnost limitirati pristup mrežnim paketima ovisno o aplikacijama. Određeni aplikacijski protokoli vrlo su ranjivi na mrežne napade zbog čega je nužno zabraniti pristup istima (Telnet, NetBIOS Session, POP, NFS, X Window i sl.). Nadalje, navedeni portovi mogu biti izloženi napadima zbog velike razine kontrole koju pružaju neovlaštenom korisniku.

Filtriranje paketa ovisno o ruti usmjeravanja paketa (eng. Source Routing)

Proces rutiranja mrežom kojom paket treba proći prilikom putovanja prema cilju i/ili prilikom povratnog putovanja naziva se *Source routing*. Prvenstveno se koristio za analiziranje paketa koji se kreću mrežom kako bi se optimizirala brzina prijenosa, no danas ovu metodu koriste neovlašteni korisnici. Ukoliko se neovlašteni korisnik uključi u mrežu i koristi se *Source routing*-om ima mogućnost prepravljanja polja izvorišne IP adrese koje može postaviti tako da mu se paket iz mreže vrati koristeći vlastitu IP adresu. Tijekom tog procesa, neovlašteni korisnici imaju nadzor nad cijelom mrežom budući da *Source routing* prikazuje sve element mreže

Filtriranje paketa ovisno o broju fragmentiranog paketa

U slučaju kada je potrebno prenijeti poruke koje su prevelike, one se raščlanjuju u manje pakete. Definirana veličina paketa za prijenos predodređena je putem IEEE 802.3 standarda jer ograničena sa maksimalnom veličinom od 1500 okteta. Prvotno raščlanjenu poruku na izvorištu moguće je dodatno rasčlaniti koristeći usmjerivače preko kojih ona prelazi. Raščlanjeni paketi na odredištu se ponovno povezuju u odaslanu poruku.

Filtriranje na vatrozidu provodi se na način da se odbaci početni raščlanjeni paket koji jedini sadržava port aplikacije koja ostvaruje vezu, pri čemu se pretpostavlja da će ostali paketi biti neupotrebljivi jer neće imati pristup aplikaciji. Ova vrsta filtriranja danas se ne koristi zbog mogućnosti neovlaštenih korisnika da na prvom poslanom raščlanjenom paketu umjesto broja 0 dodjele broj 1 zbog čega poruka može preći preko vatrozida i doći do željene aplikacije.

2.3.2. Dinamičko filtriranje paketa (eng. Stateful packet filtering)

Stateless inspection predstavlja najčešći način provjere mrežnih paketa od strane vatrozida, no ima mnogo sigurnosnih rupa. Ovom metodom vatrzoid analizira pakete kao jedinice pri čemu ne postoji način utvrđivanja je li riječ o početnim paketima ili su oni dio već postojeće veze. S druge strane, *stateful inspection* vrsta je provjere mrežnih paketa putem kojeg je moguća detaljna analiza. Koristeći ovu metodu, moguće je ustanoviti jesu li paketi dio već uspostavljene veze ili nisu**.** Primjer ove metode bio bi korisnik koji se iz zaštićene mreže pokuša spojiti na nezaštićeno, pri čemu će mu vatrozid to dozvoliti. U tom slučaju paketi koje prima korisnikovo računalo sadržaj su uspostavljene veze, uključujući i one sa nezaštićene mreže te ih vatrozid propušta na određeni port. U slučaju kada računalo iz nezaštićene mreže pokuša poslati paket na računalo na zaštićenoj mreži, on će biti dio nove veze i vatrozid neće dopustiti prijenos.

Dinamičko filtriranje razlikuje se od statičkog filtriranja prvenstveno po mogućnosti analize paketa samo na temelju njihovih zaglavlja pri čemu *stateful inspection* utvrđuje i sve uspostavljene veze između pojedinih mrežnih sučelja na temelju čijih stanja obavlja provjere. Zbog navedenog, vatrozid koji koristi dinamičko filtriranje trebao bi redovito ažurirati tablice stanja koje sadrže veze s pridruženim odgovarajućim stanjima. Posljedično, odluke o filtriranju bazirane su na administratoski definiranim pravilima (statičko filtriranje), ali i na sadržajima već proslijeđenih paketa (dinamičko filtriranje).

Jedan od glavnih nedostataka vatrozida koji koriste statičko filtriranje je što većina njih ima otvoren pristup na mrežnim portovima iznad adrese 1024. Navedeni portovi ostavljaju se otvorenima zbog odgovora koji se primaju sa nezaštićenog dijela mreže. Otvoren pristup preko portova iznad adrese 1024 može predstavljati rupu u sigurnosti mreže budući da u trenutku korištenja otvorenog porta neovlašteni korisnik može poslati modificiran mrežni paket te vatrozid koji radi na principu statičkog filtiranja nema mogućnost sprječavanja takvog upada. S druge strane, vatrozid s dinamičkim filtriranjem paketa zabranjuje pristup preko portova iznad adrese 1024 te će provjeriti sve pakete budući se radi o novoj vezi unutar mreže. Postoje iznimke kada je potrebno dopustiti pristup putem određenog porta iznad adrese 1024 kod vatrozida s dinamičkim filtriranjem, no tada on gubi svoju funkcionalnost.

3. MOGUĆE VRSTE I TIPOVI NAPADA I TEHNOLOGIJE PROTIV NJIH

Kako bi zaštitili mrežu od napada potrebno je poznavati i same napade. Sve napade na mrežu odnosno pokušaje stjecanja određenih informacija i resursa od strane klijenta, možemo podijeliti u dvije skupine; pasivni napadi i aktivni napadi. Također je napade bitno grupirati u četiri glavne skupine mrežnih napada a to su; *Denial of Service* (DoS), *Probing, Remote to User Attacks* (R2L) i *User to Root Attacks* (U2R)

3.1. Aktivni napadi

Ukoliko se napadač koristi aktivnim napadom možete očekivati otkrivanje vlastitih podataka te u gorim slučajevima promjenu ili čak potpuni gubitak istih, kvar sigurnosnih aplikacija itd.. Dakle napadač tijekom napada izvršava neke akcije koje direktno utječu na vaš sustav i time ga mijenjaju prema vlastitim potrebama.

3.2. Pasivni napadi

U slučaju pasivnog napada, napadači pokušavaju doći do vaših povjerljivih informacija ali bez utjecaja na vaše resurse. To se obavlja koristeći se alatima za njuškanje (eng. *sniffer tools*) kojima se pokušavaju uhvatiti podaci koje klijent npr istipka preko tipkovnice ili podatci vezani za sigurnosne postavke napadnutog računala. Pasivne napade je moguće podijeliti na *Release message of contents* i *Traffic analysis* napade.

3.3. Najčešći korišteni napadi kroz povijest

3.3.1. Denial of Service (DoS) i Distributed Denial of Service (DDoS)

DoS napad je dizajniran s namjerom da napadač dobije kontrolu nad resursima ciljanog računala odnosno ciljanog uređaja do te mjere da klijent više nije u mogućnosti odgovoriti na valjane upite. DDoS čini istu stvar samo što je napad organiziran od strane nekoliko drugih računala koja su prethodno zaražena zlonamjernim softverom odnosno *malware*-om te se u teoriji izvodi brže nego napad s jednog računala budući da više računala pošalje veći broj nevažećih odnosno zlonamjernih upita [4].

DoS i DDoS napadi su drugačiji od ostalih napada koji pružaju napadaču pristup resursima ciljanog računala jer napadač pravovremeno ima korist od svog rada te samim time

može pripremiti računalo za sljedeći napad kojim bi preuzeo, izmjenio ili uništio podatke ciljanog računala. Rješenje protiv ovakvog napada jest vatrozid koji ima mogućnost "pronalaska" zlonamjernih upita te mogućnost da ih odstrani.

3.3.2. Man-in-the-middle (MITM)

Napad "Čovjeka u sredini" se osvrće na sigurnosni proboj u kojem se napadaču omogućuje prisluškivanje podataka koji se šalju između dvaju mreža odnosno dvaju strana. Odvija se tako što napadač "upadne" negdje u mrežu te svi podaci prelaze prvo preko njega i potom idu do odredišta [4].

MITM napade je moguće negirati korištenjem bolje enkriptiranih pristupnih točki odnosno bolje zaštićenih certifikata ili korištenjem VPN-a.

3.3.3. Krađa identiteta (eng. Phishing)

Napad krađe identiteta se odvija tako što napadač šalje meti mail koji se čini kao i svaki drugi pouzdan mail koji sadrži neki zlonamjerni softver čiji je cilj preuzeti informacije o meti. Ova vrsta napada je zapravo kombinacija socijalnog inženjerstva i tehnologije kojim se mete "namame" u neko zabranjeno područje u kojem napadač ima kontrolu korištenjem mamca odnosno lijepo složenog maila. U slučaju da se napada cijela organizacija (npr. neka tvrtka), napadači imaju običaj poslati pojedinom radniku mail s nekim vremenskim razmakom kako mailovi ne bi bili sumnjivi.

Ukoliko mail prođe kroz vatrozid i dođe do računala jedina zaštita je razumijevanje mailova i "čitanje malih slova" odnosno bolje obraćanje pozornosti na mailove koji dolaze iz sumnjivih izvora i imaju neke linkove ili priloge. Potrebno je proučiti zaglavlje svakog mail-a odnosno adresu pošiljatelja budući da na taj server napadač mora biti povezan.

3.3.4. Napad s iznuđivanjem (eng. Ransomware)

Ovakav napad je sve češći u današnje vrijeme budući da mete dobivaju ultimatum; ili platiti ili ostati bez podataka. Dakle napadač se domogne resursa računala i zabrani pristup pravom korisniku računala sve dok se ne izvrši uplata. Uobičajeno napadač do resursa računala dolazi preko neke datoteke koju meta preuzme kao prilog maila. Nakon preuzimanja zlonamjernog softvera napadač enkriptira sve podatke koje je dobio na raspolaganju. Mete napada mogu postati i ostala računala u već postojećoj mreži te na kraju i centralni server.

Ransomware napad je moguće spriječiti koristeći se *Next-Generation Firewall*-om (NGFW) koji ima mogućnosti pronalaska *ransomware*-a koristeći se softverom koji traži karakteristike *ransomware*-a na ulazu podataka u mrežu .

3.3.5. *SQL Injection*

Napad čija se tehnika sastoji od umetanja zlonamjernog softvera u obliku teksta u polja obrazaca koja koriste neke aplikacije u sustavu koristeći se SQL upitima. Metoda se temelji na pokušaju i grešci budući da je cilj napadača pogoditi imena tablica i atributa kao i strukturu SQL upita.

Napad je moguće zaobići provjeravajući ulazne podatke kako bi se osiguralo da nema opasnih kodova, projektirajući dobru infrastrukturu mreže za zaštitu od krađe resursa.

3.3.6. Napadi na zaporke

Napadi na zaporke su vjerojatno i dalje najčešće korišten napad a osnovna metoda jest pogađanje lozinke. Metodu je moguće proširiti koristeći se socijalnim inženjeringom i navođenjem mete da unese zaporku kako bi riješila neki naočigled važan kviz ili upitnik.

Uobičajena metodologija napada je korištenje Brute-force tehnike koja predstavlja uzastopno unošenje različitih lozinki koristeći se razvijenim softverom. Taj softver sadrži biblioteke sa velikim brojem mogućih kombinacija znakova koje se koriste za zaporke te ih upisuje kao lozinku (automatizirano pogađanje).Također razvijeniji brute-force programi se koriste vašim podacima kao što su interesi i osobne informacije kao što su informacije o poslu, školi, društvenim mrežama te ih iskorištavaju kako bi jednostavnije prilagodili traženje po bibliotekama [4].

3.3.7. Lažiranje Domain Name System-a (DNS) (eng. *DNS Spoofing*)

Koristeći se *DNS Spoofing-om* napadač mijenja DNS zapis u izlazećem prometu kako bi metu odveo na lažiranu stranicu na kojoj bi ona unijela svoje osjetljive podatke koji kasnije napadač obrađuje i profitira od njih. Napadač kako bi izveo napad mora imati pripremljenu lažiranu stranicu koja mora biti dovoljno uvjeravajuća kako bi meta unijela podatke.

Najjednostavniji način sprječavanja ovog napada je redovita provjera ažuriranja DNS servera jer napadačima je potrebno neko vrijeme da razviju softver za pristup DNS serveru, tako najnovija ažuriranja sadrže “zakrpe” za moguće otkrivene rupe u sigurnosti.

3.3.8. Skriptiranje (XSS) (eng. *Cross-site scripting*)

Napadači skriptiranje koriste tako što meta klikom na neki sadržaj na web-stranici pokrenu skriptu koja se izvrši na njihovom računalu te počinje snimati promet i vaše podatke te ih mogu mijenjati.

Kao primjer se može uzeti napad na online bankarstvo; meta klikne na bezazleni link koji ju vodi na naizgled njoj poznatu stranicu te time pokreće skriptu napadača. Nakon što shvati da je stranica "srušena" tijekom iste sesije web aplikacije pokrene internet bankarstvo i izvrši transakciju. Svi podaci ostaju u rukama napadača čija je skripta preuzela osjetljive informacije vidljive tijekom transakcije.

3.4. Tehnologije korištene kao dio sigurnosti protiv napada na mrežu

3.4.1. Sustav za sprječavanje upada (eng. *Intrusion Prevention System* (IPS))

IPS je oblik mrežnog osiguranja koje radi na način da konstantno prati određenu mrežu, tražeći mogući zlonamjerni softver i dohvaća informacije o njemu kako bi isti mogao biti uklonjen iz vaše mreže.

Ukoliko dođe do pronalaska zlonamjernog softvera, IPS prvo blokira resurse zlonamjernog softvera te potom obavještava administratora kako bi administrator obavio preventivne akcije te postavio vatrozid tako da u budućnosti ne bude sličnih propusta u sigurnosti sustava. Najčešće akcije se pokreću u slučaju na DoS napad, DDoS napad te razne viruse ili crve.

IPS prvo ukida TCP sesiju u kojoj je pronađena rupa u sigurnosti te blokira pristup IP adrese na kojoj se nalazi napadač ili server koji zaprima podatke. Preprogramira automatski vatrozid kako bi bio spreman na takve napade u budućnosti te uklanja ili izmjenjuje sav zlonamjerni sadržaj koji preostaje prepakirajući pakete koji dolaze [5].

Postoji razlika između IPS i *Intrusion detection system* (IDS) tehnologije budući da IDS tehnologija ima mogućnost samo nadzora mreže i obavještenja ukoliko pronađe zlonamjerni softver bez mogućnosti blokiranja resursa i samim time zaustavljanjem zlonamjernog softvera.

3.4.2. Duboko pregledavanje paketa (eng. *Deep packet inspection* (DPI))

DPI kod nas poznatiji pod pojmom "njuškanje paketa" je sigurnosna značajka implementirana u današnjim vatrozidima koja se očituje u pregledavanju sadržaja svakog paketa podataka koji uđe u mrežu odnosno prođe određeni dio mreže. Dok kod "stateful" provjere podataka se čita samo zaglavlje odnosno izvorišni i odredišni IP i broj porta, kod DPI-a se pregledaju i metapodaci koji su povezni sa sadržajem svakog paketa odnosno DPI provjerava i zaglavlje i sadržaj paketa. Ovakav način pregleda rezultira boljoj sigurnosti što se tiče primanja zlonamjernog softvera te također ima mogućnost pronalaska nekih od skrivenih prijetnji kao što je pokušaj izvlačenja podataka i sl. [6].

Administrator ili *Internet Service Provider* (ISP) postavljaju određena pravila po kojima DPI filtrira sadržaj koji dolazi u korisničku mrežu, odnosno po tim pravilima odlučuje kako će postupati sa prijetnjom koja se otkrije. Također, budući da može pročitati i zaglavlje i sadržaj paketa, DPI može otkriti izvor slanja paketa čime je moguć sukob sa napadačem. DPI je moguće pronaći u NGFW koje ubrajamo u treću generaciju vatrozida kao proširena sigurnosnu značajku.

3.4.3. Upravitelj pružanja sigurnosnih usluga (eng. *Managed security service provider* (MSSP))

Prije svega je bitno napomenuti kako se MSSP može smatrati posebnom kategorijom vatrozida budući da predstavlja korištenje online cloud vatrozida kao posrednika u mreži. MSSP nadzire promet koji ulazi u mrežu kao i promet koji treba izaći iz mreže kako ne bi došlo do slanja povjerljivih podataka s unutarnje strane mreže.

Sav promet koji treba ući u mrežu prvo se šalje na pregled cloud vatrozidu odnosno MSSP-u koji nakon pregleda podatke prihvaća ili odbija ovisno o tome koja je administrator pravila postavio unutar tog vatrozid. Ovo je odlično rješenje ukoliko korisnici nemaju mogućnost implementiranja vatrozida na neko od vlastitih računala odnosno uređaja ili imaju manjak resursa u sigurnosnom dijelu.

4. NAJPOZNATIJE KOMERCIJALNE DISTRIBUCIJE VATROZIDA

Prateći nekoliko izvora [7] [8] [9] [10] i uspoređivanjem rezultata, kao najbolje ocjenjeni i najčešće korišteni vatrozidi pokazali su se; pfSense, Cisco ASA Firewall, Fortinet FortiGate, Palo Alto Networks, Check Point te Huawei.

4.1. pfSense

pfSense je distribucija vatrozida koja je besplatna i *open sourced* što znači da izvornom kodu odnosno *kernel*-u mogu pristupiti svi korisnici, kreirana s namjerom da bude korištena i kao ruter i kao vatrozid. Konfiguracija pfSense-a se odvija koristeći se web GUI sučelje.

pfSense na raspolaganju ima nekoliko funkcija od kojih su neke; statičko/dinamičko praćenje i označavanje putanje prometa, *stateful* provjeru paketa, virtualnu privatnu mrežu (VPN), DHCP, DNS, sposobnost balansiranja opterećenja. Također kao dodatke moguće je instalirati; Snort (dodatak koji implementira IPS i IDS), Squid (mogućnost korištenja proxy servera) itd.

Samim time što je pfSense besplatan softver za sigurnost, napadači mogu također jednostavnije doći do greški u sustavu jer imaju na raspolaganju *kernel* datoteke samog softvera. Osim toga, većina "ozbiljnijih" organizacija kao što su NASA, neke vlade i slične ustanove koriste vatrozide bez GUI-a odnosno bez grafičkog sučelja koja također mogu činiti propuste u sigurnosnom pogledu sustava.

4.2. Fortinet FortiGate

Trenutno možda i najunosniji vatrozid koji je probio industriju koristeći se svojom umjetnom inteligencijom i strojnim učenjem kako bi obranio sustav od napada, dakle što više napada primi to će se bolje pripremiti za buduće napade. Kao i ostali vatrozidi omogućuje filtriranje ulaznog i izlaznog prometa na temelju IP adresa, IPS, IDS, IoT IDS, Antivirusne usluge kao i brojne druge.

Kao i Cisco ASA vatrozid dolazi uz plaćenu licencu za koju će korisnik morati izdvojiti od 300 do 600 dolara koja pokriva 10 računala u mreži (najmanji paket).Prednost FortiGate vatrozida jest ta što može biti pokrenut i kao softver na zasebnom računalu odnosno virtualnoj mašini ili kao usluga na oblaku (eng. *cloud service*). Napredno rutiranje podataka vam pruža visok stupanj integracije u veliku mrežu odnosno koristeći se *Routing Information Protoco*l (RIP), *Open Shortest Path First* (OSPF), *Border Gateway Protocol* (BGP) i *Policy-based Routing* (PBR) protokolima.

4.3. Cisco ASA firewall

Budući da je Cisco jedan od svjetski najpoznatijih distributera mrežne opreme, moraju i dobro poznavati sigurnost prijenosa informacija putem mreža a time i načine zaštite istih. Uobičajena primjena Cisco ASA vatrozida se obavlja implementiranjem softvera, za koji korisnik kupi licencu, na zasebno računalo koje postaje vatrozid u mreži i stavlja se na ulazu odnosno izlazu iz mreže.

Mogućnosti koje Cisco ASA vatrozid pruža ubrajaju filtriranje ulaznog i izlaznog prometa prema IP adresama, zaštitu od zlonamjernog softvera, IDS i IPS, VPN te pristupačnu podršku budući su svjetski poznata tvrtka i vode dobru skrb o svojim korisnicima. Ukoliko korisnici već koriste nešto od Ciscove opreme, vrlo velika šansa je da će se odlučiti za Cisco ASA vatrozid. Moguće je softver pokrenuti i na virtualnoj mašini ukoliko resursi ne dozvoljavaju implementiranje na zasebnom uređaju. Nedostatke korištenja Cisco ASA vatrozida predstavlja ponajprije cijena, budući se radi o oko 500 dolara za najmanji paket koji sadrži licence za povezivanje 10 računala. Osim što osnovni paket košta mnogo novca, svaki oblik dodatne zaštite koju korisnik želi implementirati se plaća. Također je bitno napomenuti da ovaj vatrozid nema GUI te je znanje podešavanja Cisco uređaja potrebno kako bi konfigurirali vatrozid i njegova sigurnosna pravila.

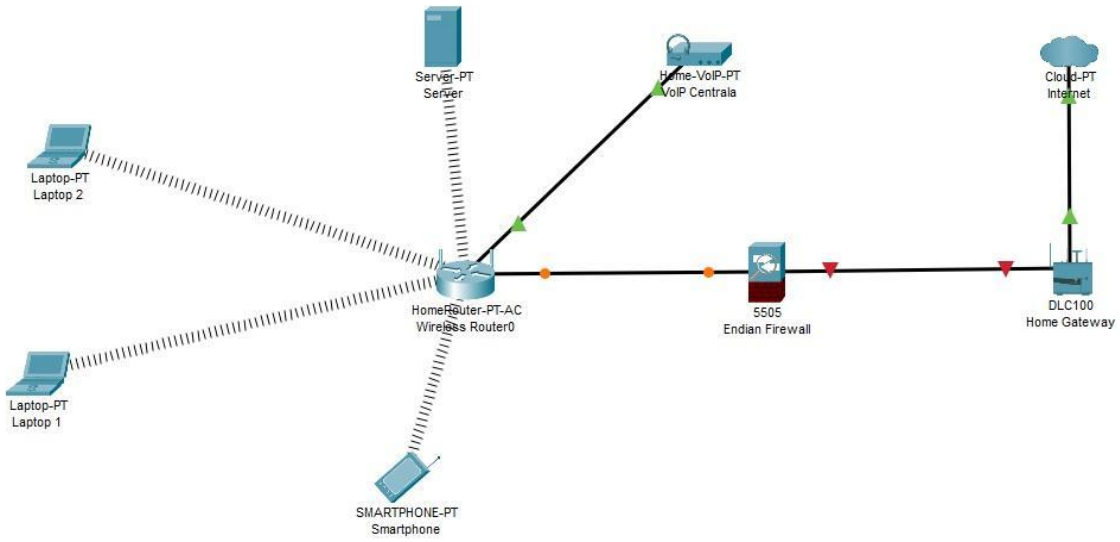
4.4. Palo Alto Networks vatrozid

Još jedan velikan u razgovoru o vatrozidima koji se na tržište probio 2009. godine uz pomoć velikog broja mogućnosti koje sam softver pruža. Također ga je moguće pokrenuti i na zasebnom uređaju kao i uslugu na oblaku.

Ovaj vatrozid se sastoji od četiri glavna dijela a to su NGFW, Panorama, Traps i Wildfire. NGFW pruža sve uobičajene mogućnosti današnjih vatrozida kao što su IPS i IDS, VPN i antivirus te osim toga koristi i Panoramu koja predstavlja kontrolni centar za mrežnu sigurnost koja omogućuje korisnicima upravljanje svim licencama odjednom iz konzole. Uz to Traps značajka vatrozida pruža mogućnost antivirusa, no ne uobičajenog antivirus koji prati potpise nego antivirus koji pomno analizira ponašanje programa. Sve informacije su podijeljene i primljene od strane usluge Wildfire koja predstavlja analizu prijetnje na cloud sustavu koja sprječava i uklanja prijetnje.

5. KONKRETAN PRIMJER PRIMJENE VATROZIDA

Kako bi što realnije i što bolje opisali primjenu vatrozida smo se odlučili za besplatnu verziju Endian vatrozida - *Endian Firewall Community 3.3.2* [11]. Scenariji je takav da je vatrozid namijenjen kao zaštita za dva računala, telefonsku centralu i server. Koristeći se alatom *Cisco Packet Tracer* je mreža dizajnirana da bude kao na slici ispod (Slika 5.1)



Slika 5.1 Dizajn mreže u *Cisco Packet Tracer*-u

5.1. Tehnički podaci virtualnih mašina i korištena programska podrška

5.1.1. Oracle VM VirtualBox

Oracle VM VirtualBox [12] je slobodan softver za x86 virtualizaciju koji je razvijen od strane Oracle Corporation-a. VirtualBox podržava stvaranje i upravljanje virtualnih mašina s operacijskim sustavima po željama administratora. Neki od podržanih operativnih sustava su: Windows, macOS, Linux, BSD, OS/2, Haiku i OSx86.

5.1.2. Tehnički podaci virtualnih mašina korištenih u scenariju

Kako bismo virtualizirali operativne sustave, potrebno je zauzeti resurse računala. U scenariju su korišteni sljedeći operativni sustavi s pripadajućim zauzetim resursima:

Windows Server 2019 Evaluation [13] (WS2019) - softver čija licenca traje 180 dana kako bi korisnik utvrdio da je to ono što mu treba te na kraju kupio trajnu licencu. Tehnički podaci se nalaze u tablici 5.1

Tablica 5.1. Usporedba minimalnih hardverskih zahtjeva i korištenih resursa za WS2019

Komponenta	Minimalni hardverski zahtjevi	Korišteni resursi u izvođenju rada
Radna memorija	512 MB	3 GB
Slobodan prostor na tvrdom disku	32 GB	75 GB
Procesor	1.4 GHz 64-bit (dual-core 2 GHz preporučeno)	2 x quad-core 2.3GHz

Issabel PBX je besplatan softver koji pruža vrlo jednostavno korisničko sučelje za web konfiguraciju i menadžment telefonskih usluga. To je *open-source* verzija Elastix-a razvijena od strane zajednice programera kada je 3CX kupio Elastix i izdao plaćenu verziju. Tehnički podaci se nalaze u tablici 5.2.

Tablica 5.2. Usporedba minimalnih hardverskih zahtjeva i korištenih resursa za Issabel

Komponenta	Minimalni hardverski zahtjevi	Korišteni resursi u izvođenju rada
Radna memorija	1 GB	2 GB
Slobodan prostor na tvrdom disku	20 GB	50 GB
Procesor	1 GHz (dual-core 2 GHz preporučeno)	1 x quad-core 2.3GHz

5.2. Instalacija vatrozida

Instalacija započinje pripremom virtualne mašine (VM) na kojoj će softver Endian vatrozida biti instaliran. VirtualBox je softver koji koristimo za podešavanje i pokretanje VM. VM na kojoj će vatrozid biti instaliran mora biti u stanju podržavati ga u vidu potrebne radne

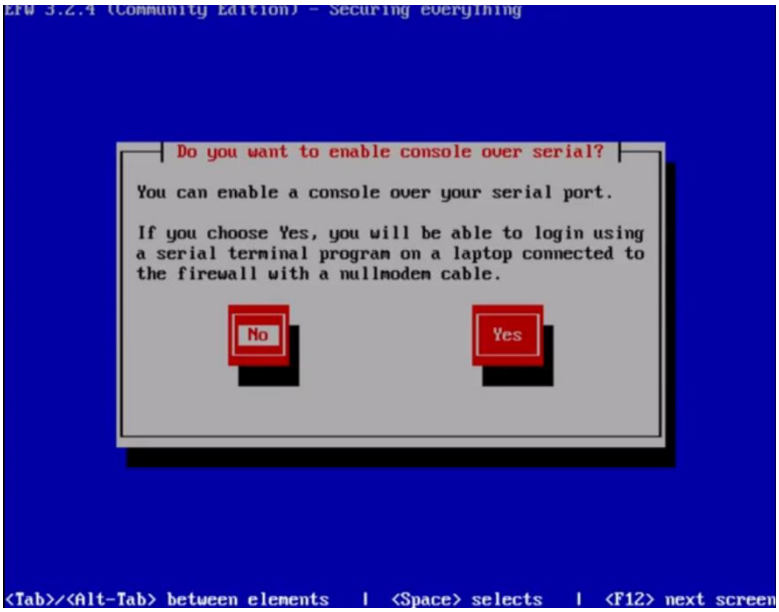
memorije te u vidu brzine procesora. Ukoliko bi uzeli računalo koje ne postiže minimalne zahtjeve vatrozida koji se na njega instalira može doći do kvara računala ili nemogućnosti pokretanja softvera.

VM mora podržavati minimalne zahtjeve softvera koji se instalira na računalo. Za konkretnu instalaciju Endian vatrozida koristimo prosječno računalo čiji se tehnički podaci u usporedbi s minimalnim hardverskim zahtjevima softvera nalaze u tablici 5.3.

Tablica 5.3. Usporedba minimalnih hardverskih zahtjeva i korištenih resursa

Komponenta	Minimalni hardverski zahtjevi	Korišteni resursi u izvođenju rada
Radna memorija	2GB	2 GB
Slobodan prostor na tvrdom disku	8	15 GB
Procesor	1GHz (dual-core 2 GHz preporučeno)	2 x quad-core 2.3GHz

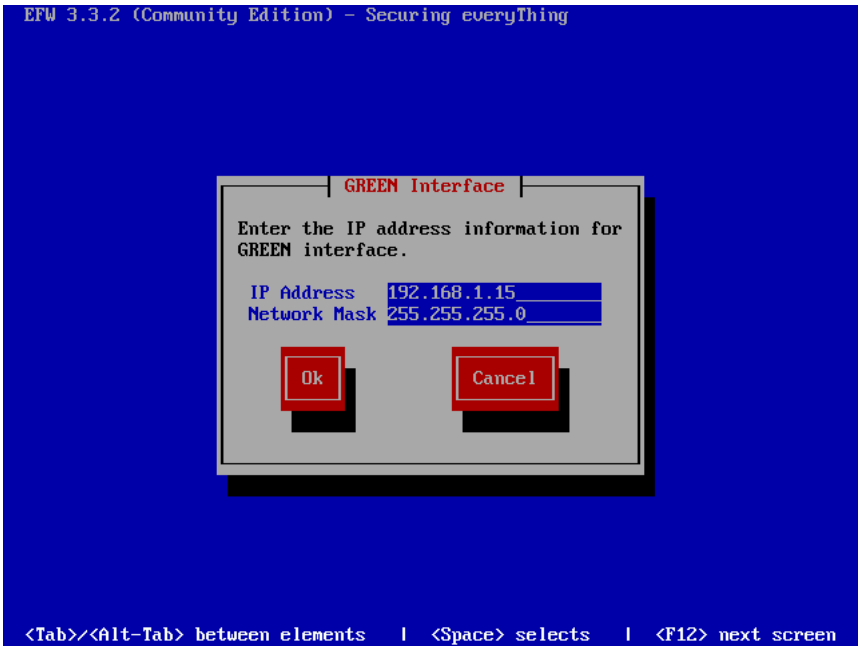
Kako bi se zaštitili od gubitka podataka bilo pogodno da se koristi RAID 1 tehnologija čiji se princip sigurnosnog pohranjivanja podataka očituje u istovremenom pohranjivanju podataka na dva ili više tvrdih diskova te ukoliko otkaže jedan svi podaci se nalaze na preostalim tvrdim diskovima. Instalacija se nastavlja uz podešavanje izvora ISO datoteke Endian vatrozida kao optičkog diska kako bi se pri prvom pokretanju računala pokrenula instalacija. Ista se vrši u DOS-u odnosno operativnom sustavu u kojem se koristi isključivo tipkovnica. Dakle pri pokretanju instalacije, nakon formatiranja tvrdog diska, dolazimo do prvog interaktivnog dijela (Slika. 5.2) u kojem korisnik može omogućiti/onemogućiti serijsku vezu prema vatrozidu.



Slika 5.2 Omogućavanje spajanja putem serijske veze

To je danas rijetko primjenjena tehnologija jer se svakom vatrozidu može pristupiti iz unutrašnjosti mreže na koju je on spojen te se time smanjuje mogućnost ulaska u vatrozid preko serijskog kabla odnosno fizičkim pristupom vatrozidu.

Nakon što korisnik omogući ili onemogući pristup vatrozidu preko serijskog porta dolazimo do podešavanja prvog mrežnog adaptera odnosno podešavanju strane vatrozida koja će biti ukopčana u korisničku mrežu. U našem scenariju ta kartica će biti mrežnim kablom spojena na pristupnu točku (eng. *Access Point*) na koji su spojeni svi uređaji u mreži. Dakle karticu koja je spojena na unutarnji dio mreže nazivamo „GREEN“ karticom (Slika 5.3). Bitno je negdje spremiti konfiguraciju ove kartice jer se putem IP-adrese koju dodijelimo toj kartici pristupa vatrozidu putem mreže i grafičkog korisničkog sučelja.



Slika 5.3 Osnovne mrežne postavke *GREEN* kartice

Postavimo da je adresa GREEN kartice 192.168.1.15 (mora biti u različitom mrežnom opsegu od RED kartice - djela mreže koji je okrenut prema internetskom smjeru). Možemo shvatiti djelovanje vatrozida kao djelovanje po zonama odnosno, vatrozid može djelovati u više zona od kojih su najčešće GREEN, RED i DMZ.

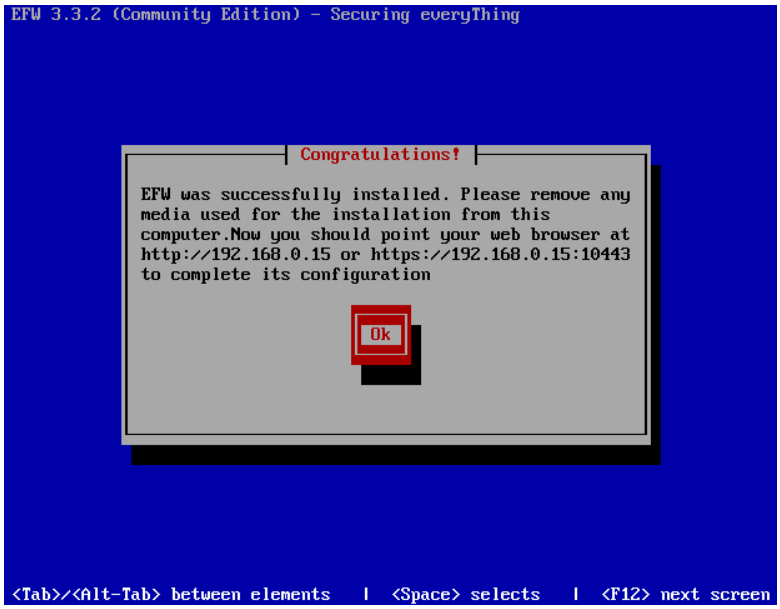
RED zona predstavlja stranu vatrozida koja će biti okrenuta prema usmjerivaču koji prima podatke od strane svjetske mreže i šalje podatke prema istoj. Najčešće se povezuje žičanim putem, no u slučaju ovog scenarija, povezivanje će biti bežično. Uobičajena pravila za RED zonu su ta da se svi korišteni portovi i IP adrese neprestano analiziraju kako ne bi došlo do napada na mrežu. U našem scenariju RED kartica poprima IP adresu 192.168.0.2.

GREEN zona predstavlja unutarnju mrežu odnosno lokalnu mrežu u kojoj se nalaze korisnici. Pristupna točka mreže će biti usmjerivač koji može raditi u *Access Point* modu. Pravila za GREEN zonu postavlja administrator te on ovisno o potrebni omogućuje/onemogućuje korištenje određenih portova i IP adresa. To znači da, ukoliko administrator dobije naređenje od šefa da zabrani korištenje npr. Facebook-a, administrator mora uvesti novo pravilo kojim zabranjuje IP adresu odnosno adrese preko kojih je moguće pristupiti toj društvenoj mreži.

Treća zona je demilitarizirana zona odnosno DMZ, čiji pripadnici moraju koristiti resurse sa interneta za obavljanje vlastite funkcije. Takvim uređajima možemo smatrati mail, web ili aplikacijske servere. Vidimo da primjenom vatrozida možemo “odvojiti” vlastitu mrežu od dijela

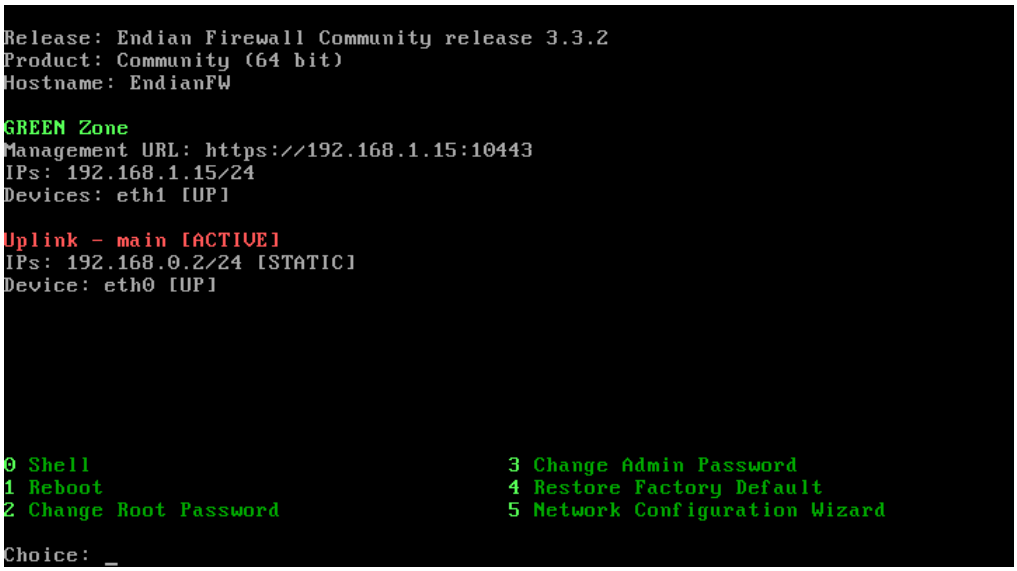
u kojem je potreban stalin i nesmetan pristup internetu te time smanjiti rizik od pristupa korisničkim podacima.

Time smo završili instalaciju vatrozida te mu od sada pristupamo putem mreže i grafičkog korisničkog sučelja (Slika 5.4). Nakon završetka instalacije potrebno je odstraniti prenosivi mediji preko kojeg smo instalirali vatrozid kako se pri njegovom ponovnom pokretanju ne bi ponovno pokrenula instalacija.



Slika 5.4 Pristupne informacije vatrozida

Sada kada je vatrozid spreman i spojen na mrežu, daljnje konfiguriranje nastavljamo putem grafičkog korisničkog sučelja do kojeg se dolazi putem IP-adrese *GREEN* kartice gdje dolazimo do dijela za prijavu te na vatrozid može ući samo osoba koja zna korisničko ime i lozinku vatrozida (koji su bili postavljeni pri samom instaliranju softvera). Nakon uspješne instalacije bi trebali dobiti prizor kao na slici ispod (Slika 5.5) te potom prelazimo na prijavljivanje tj dolazimo do GUI odnosno do grafičkog korisničkog sučelja.



Slika 5.5 Početni zaslon nakon pokretanja vatrozida na VM

5.3. Mogućnosti Endian vatrozida i njegovo podešavanje putem grafičkog korisničkog sučelja

Uobičajeno korisničko ime za prijavu na vatrozid je “admin” dok je lozinka za prijavu ona koju smo podesili za vrijeme instalacije vatrozida. Ukoliko ste odlučili ostaviti standardnu (*default*) lozinku ona glasi “endian”. Nakon što smo se prijavili na vatrozid dolazimo do kontrolne ploče (eng. *Dashboard*) (Prilog 1).

Sada na raspolaganju imamo sve mogućnosti vatrozida od zatvaranja portova do nadgledanja paketa koji dolaze odnosno izlaze iz mreže. Bitno je naglasiti kako postoje pravila za pregled paketa ovisno iz kojih zona paketi dolaze i u koje zone idu. Za primjer ćemo uzeti RED sučelje koje blokira sav promet “izvana” odnosno od strane interneta osim ukoliko je poslan odgovor na neki od zahtjeva s unutarnje strane mreže. Ne samo da RED sučelje blokira promet nego i ne dozvoljava povezivanje odnosno sesiju između vanjske i unutarnje mreže čime napadači imaju vrlo male šanse za dohvaćanje informacija iz mreže.

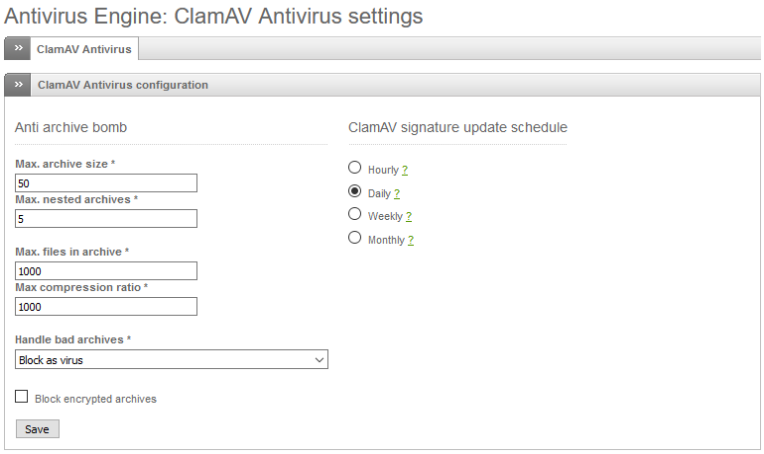
U kartici *Services* je moguće pronaći sljedeće funkcije: DHCP server, *Antivirus engine*, *Time server*, *Spam Training*, I*ntrusion Prevention*, *Network Traffic Analyzer (NTA)*, *Simple Network Management Protocol* (SNMP) server. Za slučaj scenarija nećemo koristiti SNMP server koji radi na principu slanja paketa uređajima koji ga razumiju te odgovorima na iste administrator u mreži može virtualno pratiti sve podatke koje dobije kao odgovor i *Time Server* koji služi za izjednačavanje vremena na svim uređajima u mreži što je veoma važno za neke od mrežnih protokola kao i za sigurnost sustava u vidu obavještavanja da se dogodio napad.

U ovom scenariju će biti aktivan DHCP server uz koji ćemo postaviti fiksne IP adrese za poznate uređaje (pristupna točka, server, telefonska centrala i dva računala). DHCP server smo podesili da dijeli IP adrese od 192.168.1.20 do 192.168.1.50. Fiksne IP adrese će biti postavljene kao što je prikazano u Tablici 5.4.

Tablica 5.4. Popis uređaja s pripadajućim fiksnim IP adresama

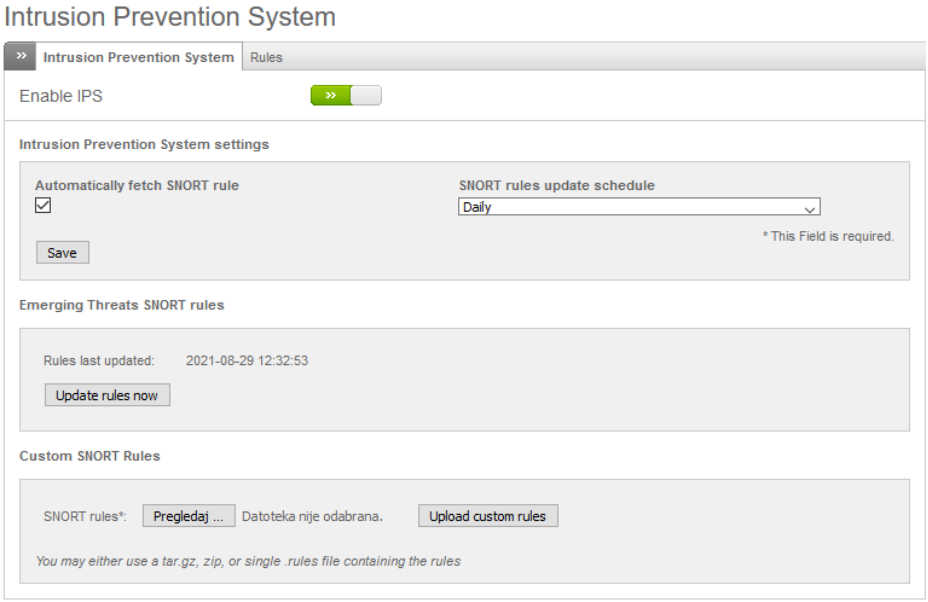
Uređaj	Fiksna IP adresa
Pristupna točka (*Access Point*)	192.168.1.20
Windows 2019 server	192.168.1.21
Issabel PBX	192.168.1.22
Računalo 1	192.168.1.23
Računalo 2	192.168.1.24
Smartphone	192.168.1.25

Antivirus engine, koji se bavi inspekcijom paketa i arhiva koje uđu u mrežu, će biti pokrenut uz naznaku da je akcija, u slučaju pojave sumnjivog paketa ili arhive, blokirati taj paket kao virus te mu ne dopustiti daljnje kretanje unutar mreže. Također je naznačeno da se lista s digitalnim potpisima (lista akoja sadrži formate digitalnih potpisa mrežnih protokola i aplikacija) koja antivirusu služi za usporedbu s digitalnim potpisima nadolazećih paketa, ažurira jednom dnevno (Slika 5.6).



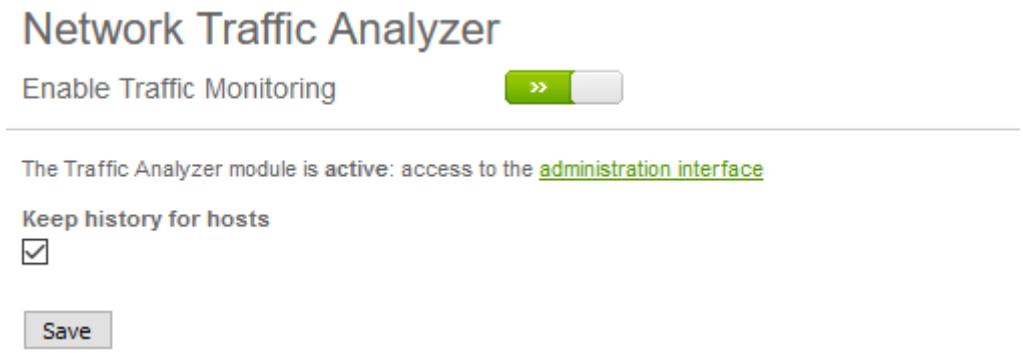
Slika 5.6 Postavke servisa *Antivirus engine*

IPS kao što je spomenuto u poglavlju 3.4.1 služi za pronalaženje i suzbijanje zlonamjernog softvera unutar mreže čije postavke na Endian vatrozidu izgledaju kao na slici ispod (Slika 5.7). IPS zaštita se postiže korištenjem SNORT pravila odnosno popisa pravila s kojima se uspoređuje ponašanje mrežnih paketa i obavještava administratora o pronađenom zlonamjernom ili neodgovarajućem paketu. Postoji javni popis pravila koji je korišten i u predstavljenom scenariju te je podešeno da se taj popis ažurira svakodnevno. Ukoliko je administrator dovoljno kompetentan, može i sam napisati odgovarajuća SNORT pravila po kojima će IPS pratiti digitalne potpise paketa.



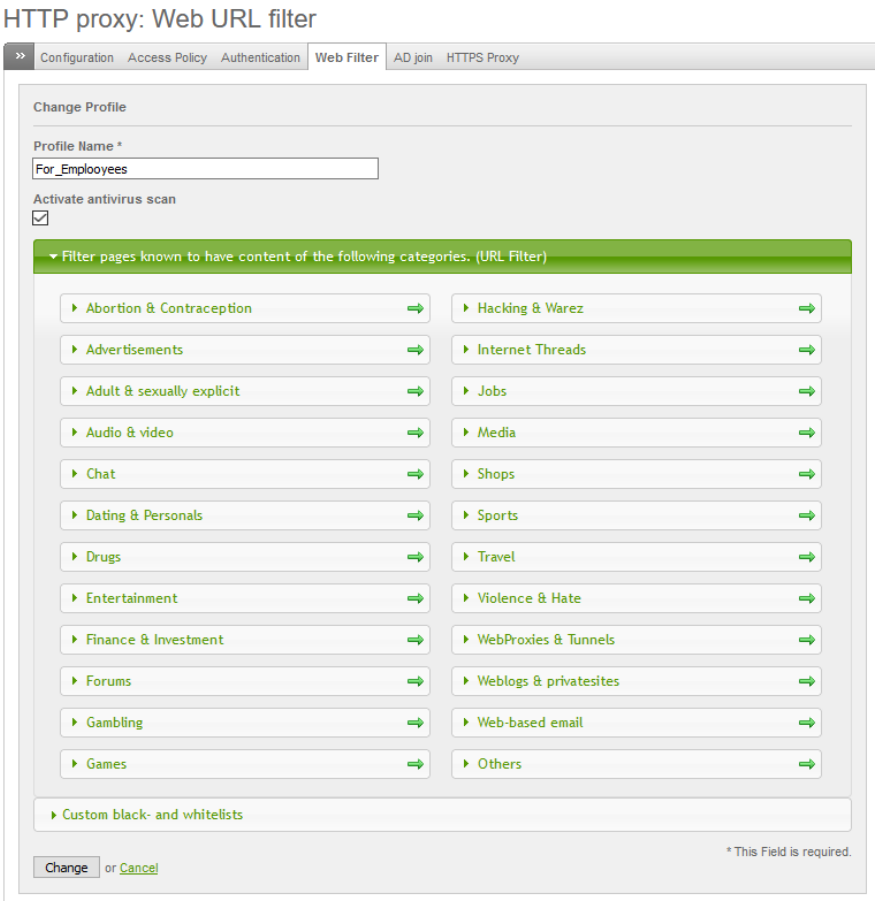
Slika 5.7 Podešavanje IPS postavki na Endian vatrozidu

Još jedan od servisa koji je korišten u scenariju jest *Network Traffic Analyzer* (NTA) koji skuplja sve trenutne i povijesne podatke o tome što se događa u mreži te otkriva zlonamjerni softver u obliku *ransomware*-a. Moguće ga je koristiti i kako bi imali uvid u performanse mreže odnosno kako bi optimizirali iste no korišten je iz razloga dodatne sigurnosti kako bi minimizirali napade i time što bolje osigurali povjerljive informacije (Slika 5.8).



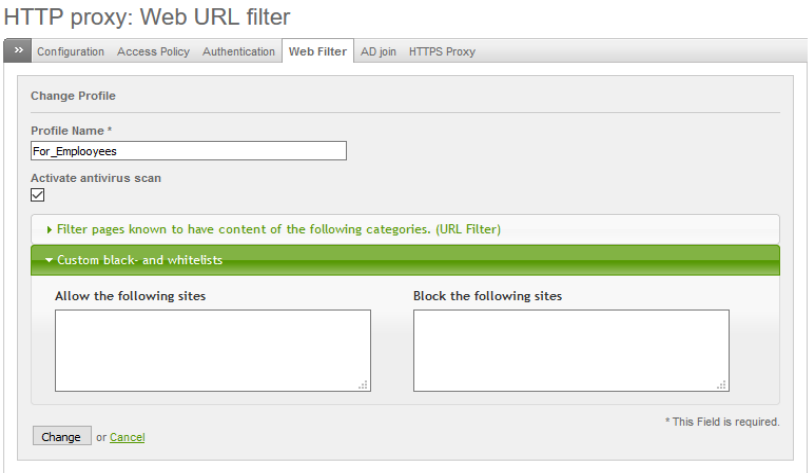
Slika 5.7 Podešavanje NTA postavki na Endian vatrozidu

Ukoliko pretpostavimo da administrator vatrozida radi u maloj tvrtci čija je mreža simetrična onoj u opisanom scenariju i dobije naređenje od direktora tvrtke da zabrani korisnicima i zaposlenicima pristup mrežnim mjestima koja sadrže npr. nasilje, neprimjereni sadržaj, kockanje, videoigre i slično. Administratoru mreže je tada potrebno napraviti profil Web-Filtera po kojem će se mreža filtrirati odnosno potrebno je podesiti HTTP Proxy server sa Web URL filtrom. Endian vatrozid ima mogućnost kreiranja HTTP Proxy servera te primjer kreiranja profila izgleda kao na slici 5.8.



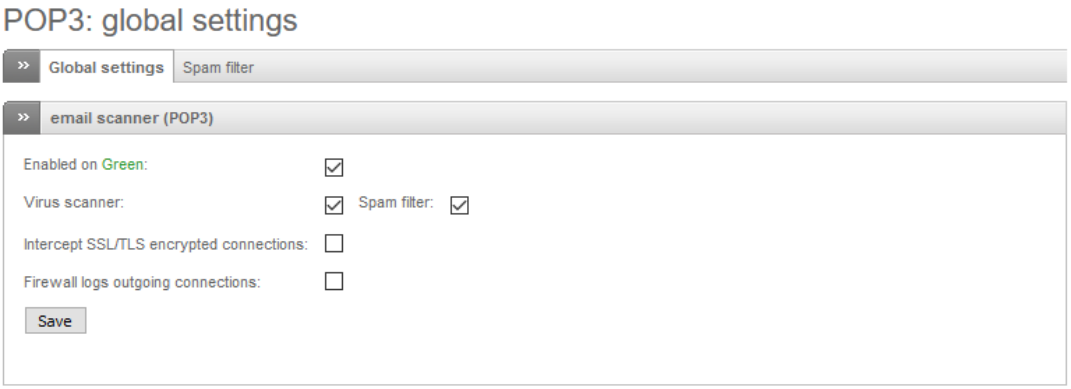
Slika 5.8 Podešavanje URL filtera na Endian vatrozidu prema sadržaju web lokacije

Također je moguće da administrator zabrani pristup određenim web lokacijama koristeći se prilagođenom crnom listom kao na slici 5.9. Potrebno je u desno polje unijeti web mjesta koja administrator želi zabraniti te nakon unosa svih pravila, spremiti profil i postaviti ga kao aktivan.



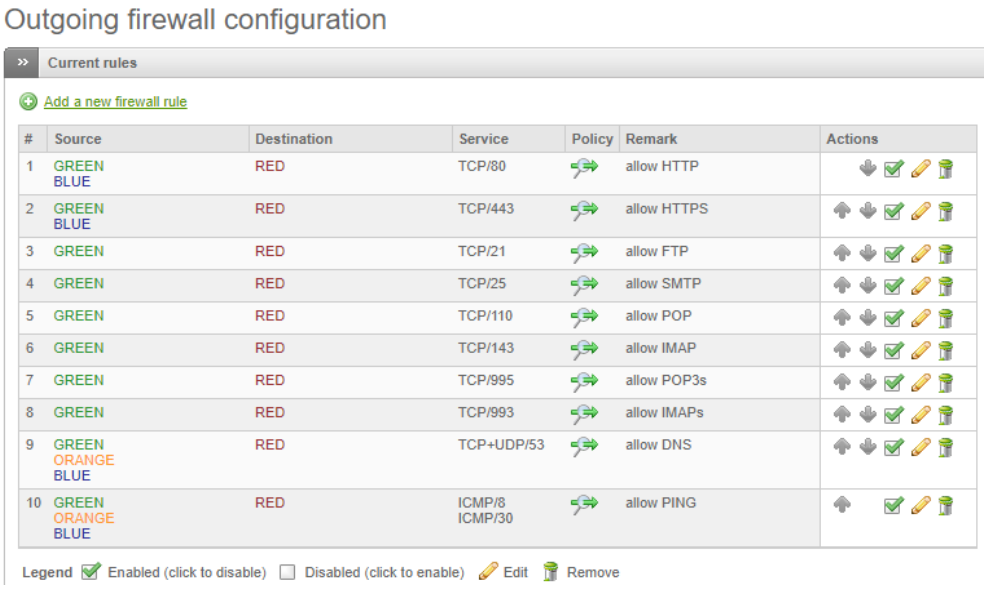
Slika 5.9 Podešavanje URL filtera na Endian vatrozidu prema određenoj web lokaciji

Naposljetku je potrebno konfigurirati POP3 filter unutar GREEN zone kako ne bi došlo do preuzimanja zlonamjernog softvera kroz e-mail usluge. Uz sam e-mail skener u scenariju je korišten i spam filter kao i virusna zaštita kao funkcija POP3 sigurnosne značajke (Slika 5.10).



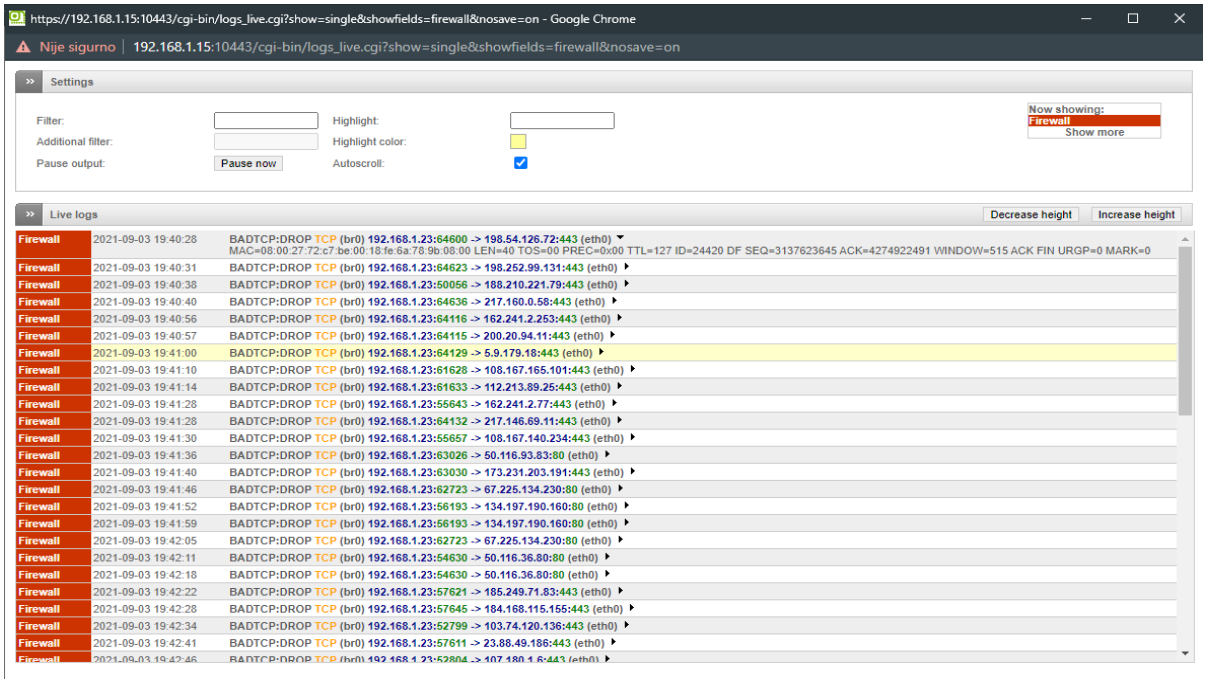
Slika 5.10 Podešavanje e-mail sigurnosnog skeniranja na Endian vatrozidu

Postavljanje pravila za prosljeđivanje portova je gotovo nužno za pravilno funkcioniranje mreže. U scenariju je pretpostavljeno da se koriste osnovni portovi kao što su 25, 80, 443, 110 te se svi navedeni koriste TCP protokolom. Postoje unaprijed postavljena pravila za prosljeđivanje portova (Slika 5.11) te osim njih, za osnovnu zaštitu mreže, nije potrebno implementirati druga pravila. Naravno administrator može uvesti pravilo za bilo koji port koji je moguće koristiti u mreži.

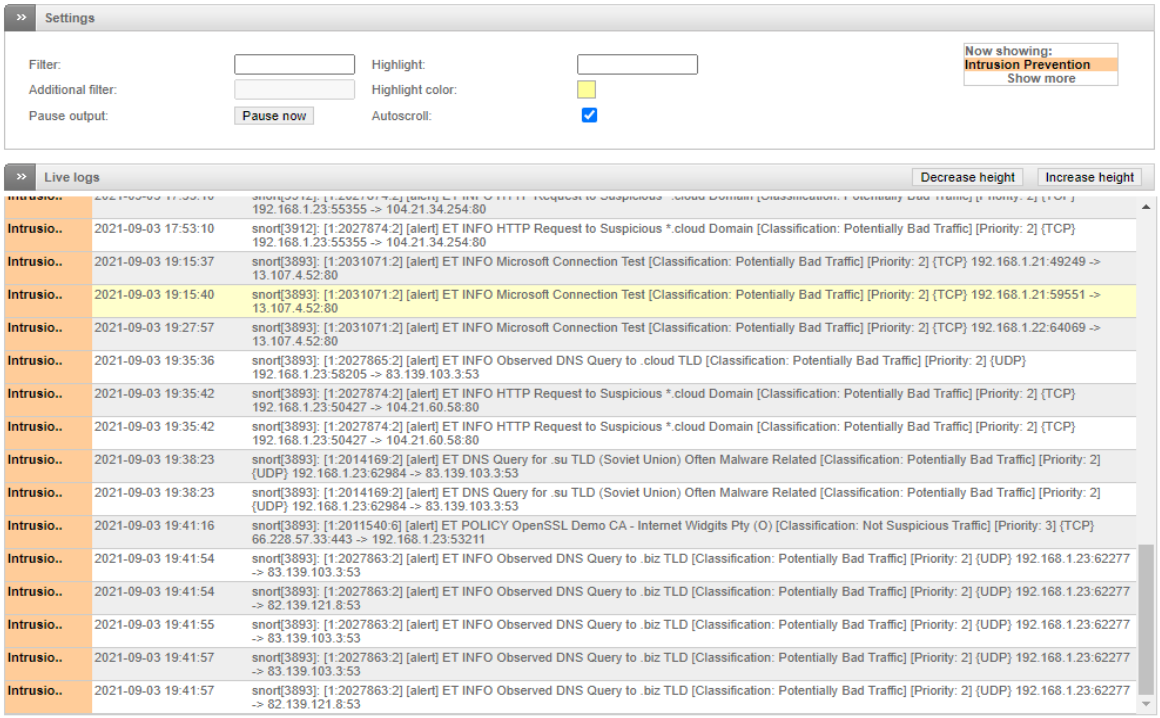


Slika 5.11 Podešavanje pravila prosljeđivanja portova između RED i GREEN zona

Sve sigurnosne značajke moraju biti nadgledane u slučaju napada ili nekog drugog događaja u mreži. Endian pruža mogućnost izvještavanja o pronađenom zlonamjernom softveru, pojavama paketa iz sumnjivih izvora (Slika 5.12, Slika 5.13)



Slika 5.12 Izvještaj o prijenosu paketa kroz mrežu



Slika 5.13 Izvještaj o IPS servisu Endian vatrozida.

Jedna od također bitnijih sigurnosnih značajki Endian vatrozida je mogućnost praćenja paketa te prikaz atributa kao što su: izvorišna IP adresa, izvorišni port, odredišna IP adresa, odredišni port, korišteni protokol, status te vrijeme istjecanja sesije (Prilog 2).

ZAKLJUČAK

Jedan od najvećih problema današnjice predstavlja internetska sigurnost. Iz dana u dan se razvijaju novi zlonamjerni softveri čiji je cilj doći do osjetljivih informacija. Iz tog razloga bitno je posvetiti se sigurnosti vlastite mreže.

Uvođenje vatrozida kao sigurnosne komponente je jedan od najboljih metoda zaštite. Primjena vatrozida ne samo da zaustavlja zlonamjerni softver nego i omogućuje administratoru neprestano promatranje unutarnje mreže, praćenje napada i analizu istih te samim time priprema administratora na moguće nove tehnologije napada.

Iako danas većina uređaja koje ljudi svaki dan koriste ima implementirane osnovne metode zaštite koje se koriste i u vatrozidu, implementacija posebnog vatrozida u mrežu pruža znatno bolju zaštitu. Primjena znatno smanjuje rizik od mrežnih napada i gubitka informacija ali samim time uvodi i ograničenja na unutarnju mrežu tako što opterećuje mrežu svojim servisima, blokira određene portove i sl. Najčešća primjena vatrozida se vrši kao što je opisano u radu, koristeći se virtualnim mašinama jer to omogućuje administratoru dodatnu sigurnost budući da je virtualnoj mašini pristup ostatku tvrdog diska zabranjen. Naravno kao dodatna mjera sigurnosti moguće je sve zaposlenike (ukoliko se radi o mreži unutar tvrtke) i ostale korisnike mreže obavijestiti o mogućim opasnostima pri spajanju na mrežu.

LITERATURA

[1] K.Ingham, S. Forrest, *A History and Survey of Network Firewalls*, The University of New Mexico Computer Science Department Technical Report 2002-37. https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf

[2] A. Wool , *Packet Filtering and Stateful Firewall*s, School of Electrical Engineering, Tel Aviv University, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.146.5044&rep=rep1&type=pdf .

[3] R. Zalenski, *Firewall technologies*, *IEEE Potentials*, vol. 21, no. 1, pp. 24-29, Feb.-March 2002, https://ieeexplore.ieee.org/abstract/document/985324 .

[4] Prowell, S., Kraus, R., & Borkin, M., *Seven deadliest network attacks*. Elsevier, 2010.

[5] R. Koller , *Anatomy of a Real-Time Intrusion Prevention System , 2008 International Conference on Autonomic Computing*, 2008, pp. 151-160

[6] C.Parsons, *Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials*. Queen's University, Surveillance Studies Centre, 2011.

[7] C.BasuMallick, *Top 10 Firewall Hardware Devices in 2021*, 2021. https://www.toolbox.com/it-security/network-security/articles/top-10-firewall-hardware-devices/

[8] P.Shread, *Top Next-Generation Firewall (NGFW) Vendors for 2021*. https://www.esecurityplanet.com/products/top-ngfw/

[9] S.Hodge, *The best enterprise level firewalls: Rating 10 top products*, 2018. https://www.networkworld.com/article/3313344/the-best-enterprise-level-firewalls-rating-10-top-products.html

[10] https://www.itcentralstation.com/categories/firewalls

[11] Download link za softver "*Endian Firewall Community*" https://www.endian.com/de/community/download/

[12] Download link za softver "*Oracle VM VirtualBox*", https://www.virtualbox.org/

[13] Download link za softver "*Microsoft Windows Evaluate Server 2019*" https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

SAŽETAK

Korištenje uređaja koji je povezan na internet korisnike automatski izlaže mogućem napadu i gubitku osobnih podataka koji su pohranjeni na tom uređaju. Potrebno je implementirati metode zaštite protiv mogućih napada. U radu je opisan postupak implementacije vatrozida u običnu korisničku mrežu te podešavanje njegovih mogućnosti. Vatrozid je najbolje sigurnosno rješenje budući da ima mogućnosti prijavljivanja uljeza i/ili zlonamjernog softvera u sustavu kao i mogućnost njihovog zaustavljanja. Implementacijom vatrozida je admnisnitrator dobio nadzor nad cjelokupnom mrežom.

Ključne riječi: mreža, mrežna sigurnost, mrežni napadi, Oracle VirtualBox, vatrozid

ABSTRACT

FIREWALLS AND EXAMPLES OF THEIR APPLICATION

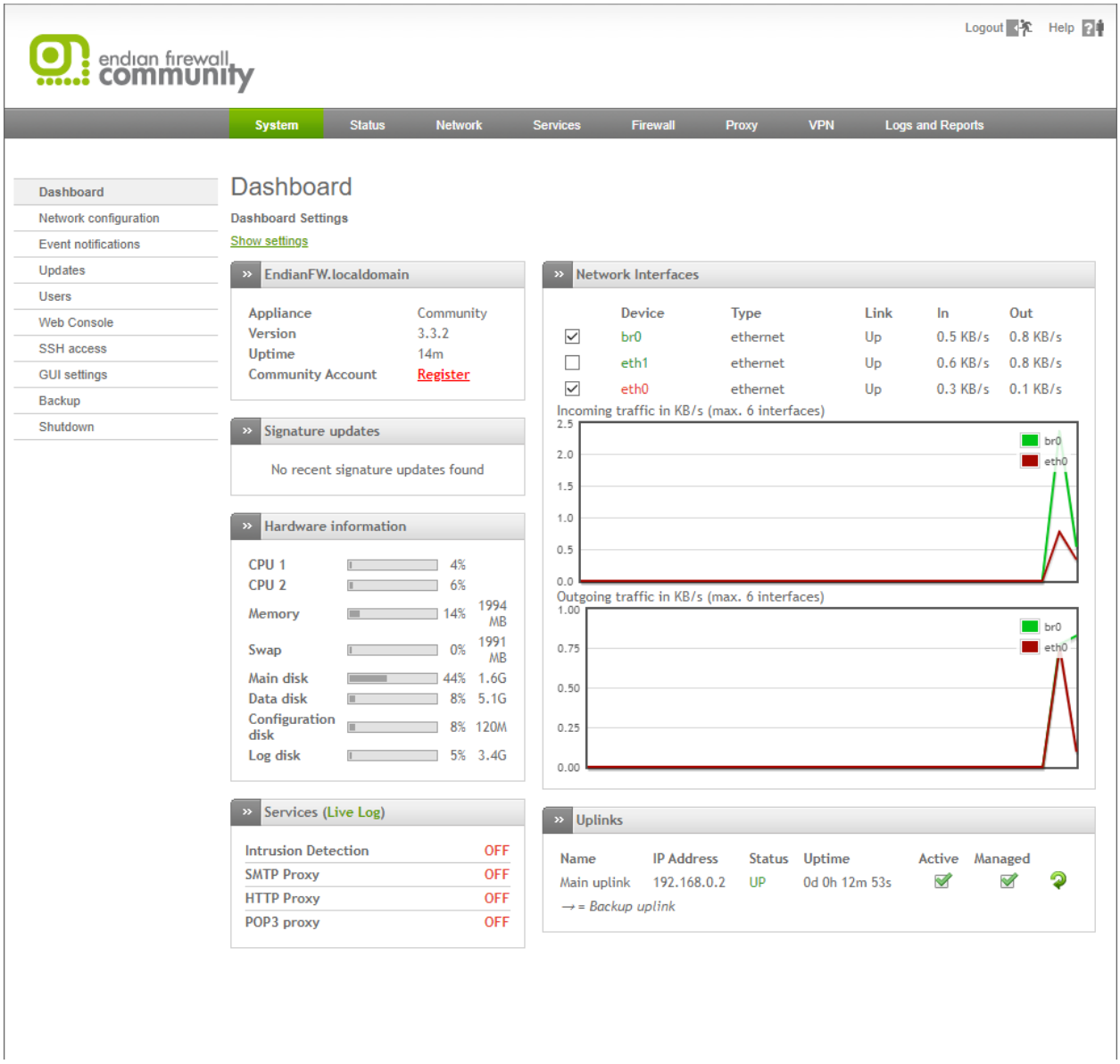
Usage of devices that have the ability to connect to the internet automatically puts users in danger by exposing them to cyber-attacks. It is necessary to implement security methods against possible cyber-attacks. This paper explains the firewall implementation procedure as well as modification of its services. Firewall is the best security solution because of its ability to locate and stop attackers and their malware. By implementing the firewall, administrator gains control of the entire network.

Usage of device connected to the Internet automatically exposes

Keywords: cyber-attacks, firewall, network, network security, Oracle VirtualBox

PRILOZI

Prilog 1 - Glavni izbornik Endian vatrozida (*Dashboard*)



Prilog 2 - Prikaz servisa za praćenje paketa

Connections

» IPTables connection tracking

Legend: LAN | INTERNET | DMZ | Wireless | Endian Firewall | VPN (IPsec)

Source IP	Source port	Destination IP	Destination port	Protocol	Status	Expires
127.0.0.1	57688	127.0.0.1	6379	tcp	ESTABLISHED	119:59:59
192.168.1.23	59310	192.168.1.15	10443	tcp	ESTABLISHED	119:59:59
192.168.1.21	50947	161.53.201.4	443 (HTTPS)	tcp	ESTABLISHED	119:59:59
192.168.1.23	50315	89.46.110.73	443 (HTTPS)	tcp	ESTABLISHED	119:59:59
192.168.1.23	59877	172.67.158.210	443 (HTTPS)	tcp	ESTABLISHED	119:59:58
192.168.1.21	65208	172.217.16.106	443 (HTTPS)	tcp	ESTABLISHED	119:59:57
192.168.1.23	53794	216.58.214.206	443 (HTTPS)	tcp	ESTABLISHED	119:59:56
192.168.1.23	50027	85.17.88.174	443 (HTTPS)	tcp	ESTABLISHED	119:59:54
192.168.1.21	51562	69.171.250.15	443 (HTTPS)	tcp	ESTABLISHED	119:59:52
192.168.1.23	59875	50.87.147.73	443 (HTTPS)	tcp	ESTABLISHED	119:59:51
192.168.1.23	59874	104.21.91.205	443 (HTTPS)	tcp	ESTABLISHED	119:59:51
192.168.1.21	61008	69.171.250.15	443 (HTTPS)	tcp	ESTABLISHED	119:59:50
192.168.1.23	59870	79.170.44.148	443 (HTTPS)	tcp	ESTABLISHED	119:59:49
192.168.1.23	62717	172.217.20.3	443 (HTTPS)	tcp	ESTABLISHED	119:59:49
192.168.1.23	61865	20.199.120.85	443 (HTTPS)	tcp	ESTABLISHED	119:59:46
192.168.1.23	55642	142.250.184.206	443 (HTTPS)	tcp	ESTABLISHED	119:59:46
192.168.1.21	52329	142.250.102.188	443 (HTTPS)	tcp	ESTABLISHED	119:59:46
192.168.1.23	57932	142.250.201.202	443 (HTTPS)	tcp	ESTABLISHED	119:59:45
192.168.1.23	59110	172.217.16.100	443 (HTTPS)	tcp	ESTABLISHED	119:59:45
192.168.1.23	63282	142.250.201.194	443 (HTTPS)	tcp	ESTABLISHED	119:59:45
192.168.1.23	58941	87.98.239.24	443 (HTTPS)	tcp	ESTABLISHED	119:59:33
192.168.1.23	64270	104.21.89.27	443 (HTTPS)	tcp	ESTABLISHED	119:59:33
192.168.1.23	50303	104.21.35.247	443 (HTTPS)	tcp	ESTABLISHED	119:59:33
192.168.1.23	50300	52.51.227.131	443 (HTTPS)	tcp	ESTABLISHED	119:59:32
192.168.1.23	64269	104.21.13.53	443 (HTTPS)	tcp	ESTABLISHED	119:59:29
192.168.1.23	58256	70.32.23.18	443 (HTTPS)	tcp	ESTABLISHED	119:59:27
192.168.1.23	60155	194.110.177.98	443 (HTTPS)	tcp	ESTABLISHED	119:59:27
192.168.1.23	58972	69.160.38.2	443 (HTTPS)	tcp	ESTABLISHED	119:59:26
192.168.1.23	53684	172.217.20.3	80 (HTTP)	tcp	ESTABLISHED	119:59:26
192.168.1.23	51407	172.217.16.100	443 (HTTPS)	tcp	ESTABLISHED	119:59:25
192.168.1.23	53314	172.67.180.9	443 (HTTPS)	tcp	ESTABLISHED	119:59:21
192.168.1.23	49953	142.250.27.188	443 (HTTPS)	tcp	ESTABLISHED	119:59:21
192.168.1.23	50294	104.21.77.76	443 (HTTPS)	tcp	ESTABLISHED	119:59:21
192.168.1.23	58971	109.234.162.20	443 (HTTPS)	tcp	ESTABLISHED	119:59:07
192.168.1.23	58974	149.126.6.120	443 (HTTPS)	tcp	ESTABLISHED	119:59:06
192.168.1.23	60151	120.138.17.201	443 (HTTPS)	tcp	ESTABLISHED	119:59:03
192.168.1.23	58975	89.46.105.31	443 (HTTPS)	tcp	ESTABLISHED	119:59:02
192.168.1.23	60153	172.67.205.94	443 (HTTPS)	tcp	ESTABLISHED	119:59:02
192.168.1.23	60148	172.67.144.19	443 (HTTPS)	tcp	ESTABLISHED	119:59:01
192.168.1.23	58962	89.46.106.64	443 (HTTPS)	tcp	ESTABLISHED	119:58:57
192.168.1.23	58965	66.235.200.146	443 (HTTPS)	tcp	ESTABLISHED	119:58:55
192.168.1.23	58967	54.72.3.133	443 (HTTPS)	tcp	ESTABLISHED	119:58:54
192.168.1.6	49673	20.199.120.182	443 (HTTPS)	tcp	ESTABLISHED	119:58:53