Mogućnosti primjene vatrozida nove generacije u zaštiti pristupa informacijsko - komunikacijskim sustavima

Juss, Luka

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:610405

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-17**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Luka Juss

MOGUĆNOSTI PRIMJENE VATROZIDA NOVE GENERACIJE U ZAŠTITI PRISTUPA INFORMACIJSKO KOMUNIKACIJSKIM SUSTAVIMA

DIPLOMSKI RAD

Zagreb, 2016.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

MOGUĆNOSTI PRIMJENE VATROZIDA NOVE GENERACIJEU ZAŠTITI PRISTUPA INFORMACIJSKO KOMUNIKACIJSKIM SUSTAVIMA

APPLICATION OF NEXT GENERATION FIREWALLS IN PROTECTING INFORMATION SYSTEMS

Mentor: Izv. prof. dr. sc. Dragan Peraković
Student: Luka Juss, 0246033286

.

ZAGREB, 2016.

Sažetak

Radi razvoja *web* 2.0 aplikacija i promjene ponašanja korisnika tradicionalni vatrozidi postaju nedovoljni za zaštitu modernih informacijsko-komunikacijskih sustava. Dolazi se do potrebe za razvojem novih sigurnosnih rješenja. Vatrozidi nove generacije predstavljaju standardne vatrozide sa brojnim unaprijeđenim funkcijama. Rad vatrozida nove generacija bazira se na 3 komponente: identifikaciji aplikacija, identifikaciji korisnika i identifikaciji sadržaja. Svrha ovog rada je prikaz mogućnosti vatrozida nove generacije Cilj diplomskog rada je provesti testiranje mogućnosti vatrozida nove generacije. U ovome radu prikazane su funkcionalnosti 2 vatrozida nove generacije: *Palo Alto* PA-500 i *Fortigate* D60. Provedenim testiranjima utvrđeno je da oba vatrozida mogu ostvariti visok stupanj zaštite informacijsko-komunikacijskih sustava.

KLJUČNE RIJEČI: vatrozidi, vatrozidi nove generacije, zaštita informacijskih sustava, identifikacija

Summary:

Because of development of web 2.0 applications and change in user behavior traditional firewalls failed to protect modern information systems. All that leads to need for development of new security solutions. New generation firewalls represents standard firewalls with numerous improvements. Work of new generation firewalls is based on three components: application identification, user identification and content identification. The purpose of this paper is to present the possibilities of a new generation firewalls. The goal of this paper is to test the possibilities of a new generation firewalls. In this paper are shown the functionalitys of two next generation firewalls: Palo Alto PA-500 and Fortigate D60. It was found that both firewalls can achieve a high level of protecting the information systems.

KEYWORD: firewall, next generation firewall, protection of inormation systemes, identification

SADRŽAJ

1.UVOD 1

2. Povijesni razvoj vatrozida 3

2.1 Vatrozidi prve generacije 3

2.2 Vatrozidi druge generacije 5

2.3 *Proxy* vatrozid 6

2.4 Sustavi za sprječavanje neovlaštenih aktivnosti i sustavi za otkrivanje neovlaštenih aktivnosti 7

3. Vatrozidi nove generacije 10

3.1 *Web* 2.0 aplikacije 10

3.2 Slabosti tradicionalnih sigurnosnih rješenja 13

3.3 Mogućnosti vatrozida nove generacije 15

3.3.1 Identifikacija aplikacija 17

3.3.2 Identifikacija korisnika 18

3.3.3 Identifikacija sadržaja 19

3.3.4 Politike kontrole prometa 20

3.3.5 Arhitektura visokih performansi 21

4.Arhitekture vatrozida 23

4.1 *Bastion host* 23

4.2 *Dual homed* arhitektura 23

4.3 *Screened host* arhitektura 24

4.4 *Screened subnet* arhitektura 25

5. Implementacija vatrozida nove generacije 28

5.1 Kontrola zaposlenika 28

5.2 Kontrola radne površine 29

5.3 Mrežne kontrole 29

5.4 Definiranje korisničkih zahtjeva za uvođenje vatrozida nove generacije 30
5.5 Segmentacija mreže i sigurnosne zone 33
6. Mogućnosti primjene vatrozida nove generacije 34
6.1 Prikaz mogućnosti i testiranje Palo Alto Pa-500 vatrozida nove generacije . 34
6.1.1 Palo Alto tehnologije 34
6.1.2 *Palo Alto* PA-500 38
6.1.3 Opis testnog okruženja 39
6.1.4 Konfiguracijsko Sučelje *Palo Alto* PA-500 vatrozida 40
6.1.5 Konfiguracija sučelja i mrežnih postavki 43
6.1.6 Konfiguracija zona i osnovnih politika 47
6.1.7 Blokiranje sadržaja 52
6.1.8 Kreiranje aplikacijskog potpisa 53
6.1.9 Identifikacija korisnika 54
6.1.10 Ostale mogućnosti *Palo Alto* PA-500 vatrozida 56
6.2. Prikaz mogućnosti i testiranje *Fortigate* 60D vatrozida nove generacije 57
6.2.1 *Fortinet* servisi 57
6.2.2 *Fortigate* D60 vatrozid nove generacije 58
6.2.3 Opis testnog okruženja 59
6.2.4 Konfiguracijsko sučelje *Fortigate* D60 vatrozida 60
6.2.5 Konfiguracija mrežnih sučelja i DHCP servera 63
6.2.5 Konfiguracija sigurnosnih politika 64
6.2.6 Konfiguracija blokiranja servisa 67
6.2.7 Identifikacija korisnika 70
6.2.8 Konfiguracija ostalih opcija vatrozida 70
6.2.8.1 Konfiguracija blokiranja datoteka 70
6.2.8.2 Konfiguracija aplikacijskog potpisa 71
6.2.8.3 Konfiguracija blokiranja aplikacija 72

6.2.8.4 SSL inspekcija 72
6.2.8.5 Konfiguracija rasporeda obavljanja 73
6.2.8.6 Konfiguracija QoS parametara 73
6.2.8.7 Konfiguracija *web* filtra 73
6.2.8.8 Ostale opcije 74
8. Zaključak 75
Zahvale 76
Popis literature 77
Popis kratica 79
Popis slika 80

1.UVOD

U današnje vrijeme svjedoci smo sve većeg razvoja, primjene i korištenja elektroničkog poslovanja. Gotovo je nemoguće zamisliti ozbiljnu organizaciju koja ne koristi određeni oblik *web* aplikacije u svome poslovanju za ostvarivanje poslovnih funkcija. Korištenjem sve većeg broja aplikacija kao i digitalizacijom određenog dijela poslovanja pojavljuje se potreba za stvaranjem velikih i kompleksnih informacijsko-komunikacijskih sustava. Razvojem informacijsko-komunikacijskih sustava dolazi se do sve veće količine informacija koje se pohranjuju unutar samog sustava. Iz razloga da svaka informacija predstavlja određenu vrijednost za samu organizaciju pojavljuje se potreba za kontrolom tko, kako i na koji način pristupa i koristi te informacije. Zaštita pristupa informacijsko-komunikacijskom sustavu predstavlja ključan čimbenik u osiguravanju visoke razine sigurnosti informacijsko-komunikacijskih sustava. Cilj zaštite pristupa je kontrolirati pristup sustavu i informacijama s ciljem očuvanja cjelovitosti, povjerljivosti i integriteta sustava. Za osiguravanje zaštite pristupa sustava koriste se vatrozidi. Vatrozidi kao uređaji razvijali su se kroz više generacija što će biti opisano kasnije u radu. U današnje vrijeme mijenja se način korištenja aplikacija sa strane korisnika. Pojavljuje se problem klasifikacije aplikacija i kontrole prometa kojeg generiraju te aplikacije. S povećanjem broja aplikacija dolazi se i do povećanja broja napada na te aplikacije, koji postaju sve softiciraniji i kompleksniji. Vatrozidi prve i druge generacije nisu se mogli nositi s tim problemima. Kao rješenje za te probleme počinju se razvijati vatrozidi nove generacije. Vatrozidi nove generacije predstavljaju tradicionalne vatrozide ali sa nadodanim brojnim poboljšanjima i sustavima zaštite. Rad vatrozida nove generacije bazira se na 3 komponente:

- identifikaciji aplikacija,
- identifikaciji korisnika i
- identifikaciji sadržaja.

Kombiniranjem tih tri komponenti pojavljuje se mogućnosti kreiranja softiciranijih sigurnosnih kontrola i politika. Primjenom tih kontrola i politika ostvaruje se visoki stupanj zaštite pristupa današnjim informacijsko-komunikacijskim sustavima.

Diplomski rad sastoji se od 8 povezanih poglavlja:

1. Uvod
2. Povijesni razvoj vatrozida
3. Vatrozidi nove generacije
4. Arhitekture vatrozida
5. Implementacija vatrozida nove generacije
6. Mogućnosti primjene vatrozida nove generacije
7. Zaključak

U drugom poglavlju opisan je povijesni razvoj vatrozida do vatrozida nove generacije kao i razlike između različitih tipova vatrozida.

Treće poglavlje opisuje razloge zašto je došlo do potrebe za vatrozidima nove generacije. Nadalje opisuju se tri ključne komponente svakog vatrozida nove generacije: identifikacije aplikacija , identifikacije korisnika i identifikacije sadržaja.

U četvrtom poglavlju opisuju se mogućnosti postavljana vatrozida nove generacije u mreže, kao i prednosti i nedostaci pojedine arhitekture.

U petom poglavlju opisani su kriteriji koji se moraju uzeti u obzir prilikom odabira vatrozida nove generacije.

U šestom poglavlju prikazane su i opisane konfiguracije i testiranja mogućnosti dva vatrozida nove generacije.

Svrha rada je prikaz mogućnosti vatrozida nove generacije te uočavanje prednosti i nedostataka testiranih vatrozida u osiguravanju pristupa informacijsko-komunikacijskim sustavima.

Cilj diplomskog rada je provesti testiranje performansi i mogućnosti vatrozida nove generacije. Provedbom različitih scenarija u radu će se testirati sigurnosne performanse vatrozida.

Istraživanje i testiranje mogućnosti vatrozida nove generacije provedeno je u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava na Fakultetu prometnih znanosti korištenjem prave opreme.

2. Povijesni razvoj vatrozida

Vatrozidi kao uređaji povijesno su se razvijali u nekoliko faza. Raniji modeli vatrozida bili su jednostavni uređaji. Radi razvoja *web* 2.0 aplikacija kao i promjene načina korištenja interneta dolazi se do potrebe za razvojem učinkovitijih metoda i načina zaštite pristupa mreži. U ovome poglavlju biti će prikazan razvoj vatrozida od prve generacije do vatrozida nove generacije kao i karakteristike svih vrsta vatrozida, također opisati će se uloga i princip IDS i IPS sustava koji su sastavni dijelovi vatrozida nove generacije.

2.1 Vatrozidi prve generacije

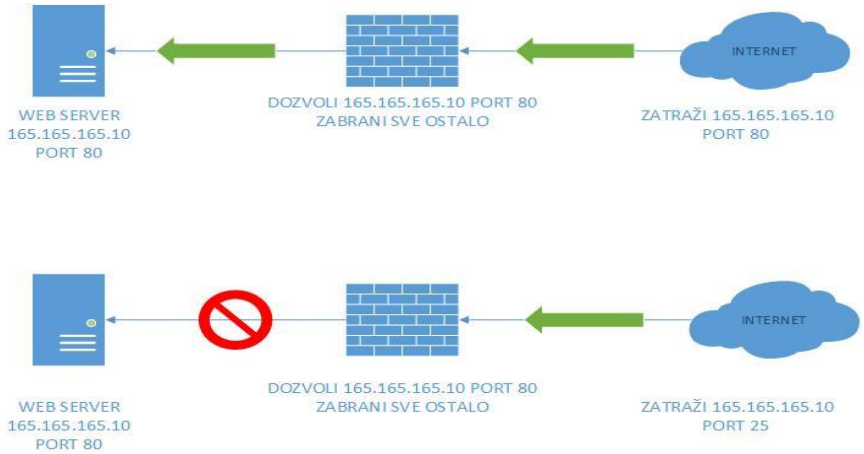
Prvu generaciju vatrozida predstavljaju paketni filtri. Paketni filtri vrše filtriranje paketa na temelju sadržaja zaglavlja paketa mrežnog sloja i zaglavlja segmenta transportnog sloja. Nakon pregleda zaglavlja IP paketa i zaglavlja segmenta vatrozidi donose odluku koja može biti dozvola ili odbijanje prolaska paketa. Filtriranje paketa može se vršiti prema sljedećim kriterijima [1]:

- izvorišnoj i odredišnoj IP [1]adresi,
- izvorišnom i odredišnom portu,
- vrsti protokola (TCP[2] ili UDP[3]) i
- smjeru prometa (ulazni ili izlazni).

Paketni filtri mogu biti implementirani unutar graničnog usmjernika ili kao zasebni uređaji. Ova vrsta vatrozida implementira se u obliku pristupnih lista (*acess list)*. Pristupna lista predstavlja skup pravila postavljenih na određeno mrežno sučelje i primijenjenih na sav promet koji prolazi kroz to mrežno sučelje. Kada paket pristigne na mrežno sučelje vatrozid pregledava zaglavlja paketa i uspoređuje ga sa pravilima

[1] IP (*Internet protocol*): mrežni protokol koji se koristi za komunikaciju unutar računalne mreže. Nalazi se na 3 sloju OSI modela i koristi IP adrese za adresiranje uređaja i usmjeravanje prometa u mreži.
[2] TCP (*Transmission Control Protocol*): konekcijski protokol za prijenos podataka. Radi na 4 sloju OSI modela.
[3] UPD (*User Datagram Protocol*): bez konekcijski protokol za prijenos podataka. Radi na 4 sloja OSI modela.

pristupne liste. Pravila se pregledavaju od početka sve do podudaranja nakon čega se paket odbija ili propušta. Nakon pozitivnog podudaranja s određenim pravilom sva ostala pravila se zanemaruju. Ukoliko ne postoji podudaranje s nijednim pravilom paket se najčešće odbija ali je moguće i propuštanje paketa ovisno o proizvođaču vatrozida [1]. Primjer načina rada paketnog filtra prikazan je slikom 1.



Slika 1 Primjer rada paketnog filtra

Ova vrsta filtriranja paketa još se naziva bez konekcijskom inspekcijom jer vatrozid nema mogućnosti razumjeti cijeli tijek komunikacije koja se odvija između dva sustava, već je orijentiran isključivo na karakteristike pojedinog paketa koji analizira. Prednosti paketnih filtra je jednostavna, jeftina i lagana implementacija kao i potreba za malim resursima. Nedostaci paketnih filtra su nemogućnost gledanja sadržaja paketa što omogućava brojne napade. Najčešća primjena paketnih filtra je kao prva linija obrane tj. za filtriranje mrežnog prometa s poznatih adresa napadača [2].

2.2 Vatrozidi druge generacije

Paketni filtri donose odluke o propuštanju ili odbacivanju paketa po principu paket po paket tj. kada se paket propusti ili odbije paketni filtar zaboravlja na taj paket. Paketni filtri ne posjeduju mogućnost provjere je li paket koji dolazi na provjeru dio postojeće konekcije ili je inicijalni paket određene konekcije. Zbog potrebe za kontrolom je li određeni paket dio postojeće konekcije ili je inicijalni paket konekcije počinju se razvijati napredniji oblici zaštite. Kompanija *Check Point* 1994. godine patentira i predstavlja prvi vatrozid stanja naziva *FireWall* 1 [3]. Vatrozidi stanja posjeduju sve mogućnosti vatrozida prve generacije ali donose unaprjeđenje u način rada tako da održavaju tablice stanja (*state table*). Tablica stanja prikazana je slikom 2 i sadrži u sebi popis svih konekcija kao i pridružena stanja tih konekcija. Također u tablici stanja mogu se nalaziti brojne varijable vezane uz konekcije kao i prošla stanja konekcija. Vatrozidi stanja ne donose odluke samo na temelju definiranih pravila, već se uzimaju u obzir i sadržaji prethodno proslijeđenih paketa. Paketi moraju slijediti pravilan redoslijed stanja konekcije i zadovoljiti pravila da bi bili propušteni. Vatrozid stanja naziva se još i dinamičkim filtrom paketa.

Src_IP	Src_Prt	Dst_IP	Dst_Prt	IP_prot	Kbuf	Type	Flags	Timeout
192.168.1.202	1783	192.168.1.207	137	17	0	16386	ffffff00	18/40
192.168.1.202	1885	192.168.1.207	80	6	0	28673	ffffff00	43/50
192.168.1.202	1884	192.168.1.207	80	6	0	28673	ffffff00	43/50
192.168.1.202	1797	192.168.1.207	23	6	0	16385	ffffff00	35/50
192.168.1.202	1796	192.168.1.207	22	6	0	16385	ffffff00	35/50

Slika 2 Primjer tablice stanja, [1]

Vatrozid stanja radi na principu da se u slučaju dolaska inicijalnog paketa konekcije, vrši tzv. duboka inspekcija (*deep packet inspection*). Dubokom inspekcijom pregledava se sadržaj svih slojeva poruke, zatim se unosi nova konekciju u tablicu stanja kao i sve informacije o toj konekciji i sesiji kojoj pripada. U tablicu stanja pohranjuju se izvorišna i odredišna IP adresa, izvorišni i odredišni portovi, vrsta protokola, zastavice iz zaglavlja, slijedni broj, QoS. parametri, vremenska oznaka itd.

Kada se prođe inicijalna provjera paketa i ona zadovolji uvjete za ostale pakete iz sesije pregledava se samo zaglavlje paketa mrežnog sloja i zaglavlje segmenta transportnog sloja. Prilikom dolaska novog paketa već uspostavljene konekcije, u tablici stanja za tu konekciju unose se promjene. Također provjerava se dali taj paket slijedi definirani redoslijed stanja za tu aplikaciju. Ukoliko je sigurnosna provjera uspješna paket se propušta i unosi se promjena u tablicu stanja gdje se mijenja stanje konekcije. Prednost ovakve vrste vatrozida je da su na puno sigurnijoj razini, ako se uspoređuje sa njihovim prethodnicima. Ova vrsta vatrozida održava i zapisuje u *log* datoteke sve radnje koje poduzima te postoji mogućnost praćenja konekcija i kontrole prometa. Nedostatak ove vrste vatrozida je de je konfiguracija i održavanje puno kompleksnije jer je potrebno znanje o radu aplikacija, također nedostatak je što je ova vrsta vatrozida pogodna za *DoS*[4] napade na tablice stanja čime postoji mogućnost onemogućavanja rada ovog vatrozida [2].

2.3 *Proxy* vatrozid

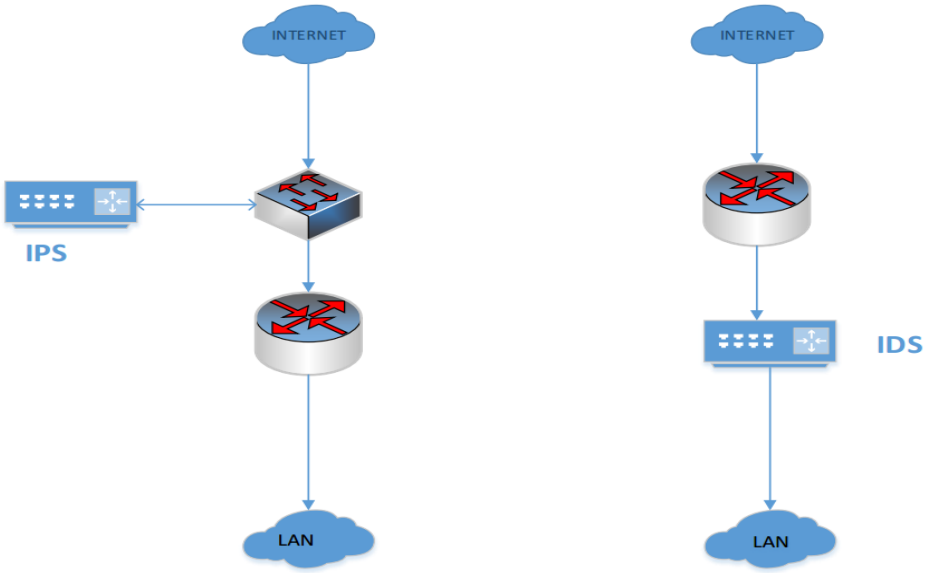
Proxy kao pojam predstavlja svakog posrednika u određenoj komunikaciji koji presreće i pregledava poruke prije dostavljanja poruke. *Proxy* vatrozidi rade na principu prekidanja direktne komunikacije između pošiljatelja i primatelja. Ne postoji direktna komunikacija između uređaja koji komuniciraju već se komunikacija vrši između pošiljatelja i *proxy*-a, kao i primatelja i *proxy*-a. Kada paket dođe na *proxy* vatrozid on prekida sesiju, vrši sigurnosnu kontrolu i ukoliko se prođe kontrola započinje sesiju s drugom stranom. *Proxy* vatrozid može raditi na različitim OSI[5]slojevima. *Circuit level proxy* radi na sloju sesije i provjerava promet prije dozvole prolaska kroz vatrozid. Ova vrsta vatrozida prekida direktnu komunikaciju između pošiljatelja i odredišta. Kada paket dolazi na vatrozid prvo se vrši inspekcija na temelju zaglavlja mrežnog i transportnog sloja, kao i podataka o sesiji. Ukoliko se provjera zadovolji vatrozid ostvaruje konekciju i šalje pakete. Mana ove vrste vatrozida je da se ne provjerava sadržaj paketa već samo sadržaj zaglavlja mrežnog i transportnog sloja.

[4] DoS (*Denial of Service*): vrsta napada u kojem se šalje veliki broj lažnih zahtjeva na određeni dio s infrastrukture ciljem onemogućavanja usluge
[5] OSI: najkorišteniji i najpoznatiji referentni model za apstraktni prikaz računalnih mreža. Sastoji se od 7 slojeva.

Aplikacijski *proxy* vatrozid vrši inspekciju paketa na aplikacijskoj razini i može donijeti odluku na temelju samog sadržaja određenog paketa. Aplikacijski *proxy* vatrozid poznaje aplikacijske protokole i servise kao i način na koji komuniciraju, npr. aplikacijski vatrozid razumije razliku između *http_get* i *http_post* naredbe i može donijeti odluku samo na temelju ove informacije. Ova vrsta vatrozida specijalizira se samo za određeni protokol i servis koji se želi štititi. Ako postoji potreba za zaštitom više različitih aplikacijskih protokola tada se mora implementirati više različitih *proxy* vatrozida. Glavni nedostatak *proxy* vatrozida predstavlja prekid direktne komunikacije. Prekid komunikacije može uzrokovati probleme u radu nekih aplikacija kao npr. kod aplikacija za stvarno vremensku komunikaciju. Korištenjem aplikacijskih vatrozida povećava se cijena i kompleksnost cijeloga sustava jer postoji potreba za implementacijom više uređaja u slučaju zaštite više različitih aplikacija [2].

2.4 Sustavi za sprječavanje neovlaštenih aktivnosti i sustavi za otkrivanje neovlaštenih aktivnosti

Paralelno s razvojem vatrozida počinju se razvijati uređaji za otkrivanje i sprječavanje malicioznih aktivnosti unutar sustava. Tokom vremena počele su se pojavljivati nove vrste napada na mrežu. Napadači su iskorištavali poznate propuste, a tehnike napada postajale su sve pametnije i kompleksnije. Da bi se zaštitili informacijsko-komunikacijski sustavi razvijeni su *Intrusion Detection System* (IDS) i *Intrusion Protection System* (IPS) sustavi .Zajednička uloga IDS i IPS sustava je da prepoznaju napade, međutim ono što će napraviti s tom informacijom je ono što razlikuje IDS i IPS. Uloga IDS-a je da detektira napad i o tome generira obavijest (alarm). Uloga IPS-a je da detektira i na vrijeme spriječi napad. Sukladno tome, IDS i IPS se različito postavljaju u mrežu [4]. Smještaj IPS i IDS sustava u mreži prikazan je slikom 3.



Slika 3 IPS i IDS postavljanje u mreži

Unutar mrže IDS je postavljen na način da samo promatra promet koji prolazi kroz njega. Ukoliko se primijeti anomalija u prometu, obavijest o tome će biti poslana odgovarajućoj osobi i/ili uređaju. IPS se postavlja na način da kroz njega prolazi sav promet koji ulazi u mrežu i koji izlazi iz mreže. IPS ima mogućnost utjecaja na promet do te mjere da ga, ako je potrebno, i u potpunosti zabrani. Tehnike otkrivanja malicioznih aktivnosti biti će opisane u nastavku. Metoda prepoznavanja uzoraka radi na način da se pretražuje paket te se uspoređuju nizovi *bytova*[6] i traži točni uzorak koji ukazuje na neželjenu radnju. Ova metoda radi samo ako se koriste određeni portovi i protokoli. Problem kod ove metode je šte se određeni uzorci detektiraju kao lažno pozitivni iii lažno negativni tj. ako se željeni promet detektira kao negativni i obrnuto. Ako se uzorak detektira kao lažno negativni posljedice po sustav mogu biti katastrofalne. Heuristička analiza prometa odnosi se na primjenu naprednih algoritama za statističku obradu prometa koji prolazi kroz IPS uređaj. Algoritam analizom podataka dobiva određeni uzorak ponašanja i ukoliko se ustvrdi da određena radnja odstupa od uzorka ponašanja tada se može detektirati kao prijetnja. Metoda anomalije temelji se na tome da su definirana normalna ponašanja aplikacija i protokola. Normalna ponašanja određuju se temeljem različitih parametara, ukoliko određeno

[6] 1 *byte*: 8 bita

ponašanje odstupa od normalnog detektira se kao prijetnja. Mana ove metode je da se moraju unaprijed odrediti normalna ponašanja. Ukoliko se pojavi protokol ili aplikacija kojoj nije definirano ponašanje ova metoda ne može se primjenjivati [5].

3. Vatrozidi nove generacije

Kao posljedica sve većeg razvoja *web* 2.0 aplikacija kao i promjene ponašanja i navika korisnika kod korištenja interneta, pojavljuje se sve veći broj prijetnji i napada. Iz razloga da vatrozidi prve i druge generacije nisu mogli zaštiti informacijsko-komunikacijske sustave počinju se razvijati vatrozidi nove generacije. U ovome poglavlju biti će opisani trendovi koji su doveli do razvoja vatrozida nove generacije kao i funkcionalnosti koje bi svaki vatrozid nove generacije trebao imati.

3.1 *Web* 2.0 aplikacije

Tradicionalna sigurnosna podjela aplikacija bila je na „dobre“ i „loše“. Poslovne aplikacije smatrane su dobrima i bile su propuštane kroz vatrozide, a većina ostalog prometa smatrana je lošim i bila blokirana. Problem s ovakvom klasifikacijom prometa je što je danas sve više aplikacija negdje između, tj. aplikacije su korisne za poslovanje ali je bitno tko i na koji način ih koristi. Unutar zadnjeg desetljeća način izrade i primjene aplikacija se znatno promijenio za organizacije. Korporativne aplikacije počinju dobivati sve više funkcionalnosti te se počinju u njih dodavati neke funkcionalnosti osobnih aplikacija .Konvergencija korporativne infrastrukture i osobnih tehnologija pogonjena je trendom konzumerizacije koji je prema *Gartneru*[7] najznačajniji IT trend u 2015. godini [6]. Proces konzumerizacije javlja se kada korisnici počinju shvaćati da su neke osobne aplikacije jednostavnije i praktičnije za upotrebu nego napredna i kompleksa korporativna rješenja. Primjer tog trenda je sve veća želja korisnika za korištenjem *google docs* i *gmail* aplikacija za poslovnu komunikaciju kao i navika korisnika da te aplikacije koristi za privatne svrhe. Smanjivanjem granica između osobnih i poslovnih aplikacija dolazi se do odrađenog stapanja između njih. *Web* aplikacije koje su orijentirane prema korisniku s ciljem da korisnik sam sudjeluje u stvaranju sadržaja a ne bude pasivni promatrač opisane su pojmom *web*2.0 aplikacija.

[7]*Gartner*: jedna on najpoznatijih svjetskih istraživačkih i savjetodavnih kompanija

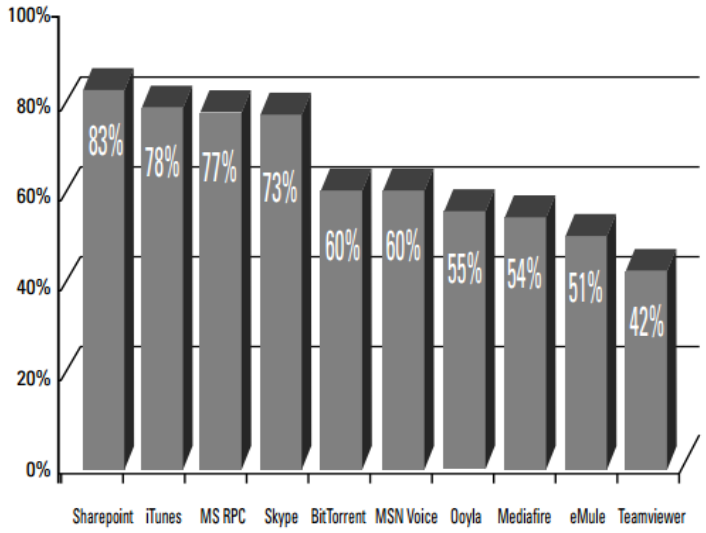
Promjene navika korisnika koji su svakodnevno počeli koristiti *web* 2.0 aplikacije dovela je do značajnog porasta samog broja takvih aplikacija kao i prometa generiranih od takvih aplikacija. Primjeri *web* 2.0 aplikacija su:

- *Microsoft SharePoint* za kolaboraciju,
- *Dropbox* kao servis za razmjenu podataka,
- *Facebook* kao društvena mreža,
- *Youtube* kao servis za objavljivanje sadržaja i promociju,
- *Skype* kao aplikacija za razmjenu poruka i ostale oblike komunikacije i
- *Wikipedia* kao stranica za razmjenu znanja.

U današnjem poslovanju sve je veća integracija *web* 2.0 aplikacija unutar samih poslovnih sustava, mnoge organizacije koriste brojne društvene mreže za razne poslovne funkcije kao npr. regrutiranje radnika, istraživanje tržišta, marketing i odnose s kupcima [7]. Također brojne organizacije dopuštaju primjenu aplikacija da bi kod djelatnika stvorili bolje okruženje za rad. Radi svega toga dolazi se do potrebe za definiranjem sigurnosne politike prema tim aplikacijama. Primjenjuju se dva različita načina definiranja sigurnosne politike o odnosu prema tim aplikacijama. Mnoge organizacije implicitno dopuštaju prolaz prometa tih aplikacija kroz vatrozide s pretpostavkom da djelatnici neće koristiti takve aplikacije na radnom mjestu za privatne svrhe. Druge organizacije imaju pristup da zabranjuju apsolutno sve takve aplikacije. Oba pristupa imaju mane, dopustiti sve aplikacije i vjerovati korisnicima jako je rizično jer je ljudski faktori najranjiviji dio informacijske sigurnosti. Zabraniti sve aplikacije nemoguće je ostvariti sa tradicionalnim vatrozidima i javlja se i problem da se pojavljuje supkultura koja uvijek teži alternativnim načinima dolaska do sadržaja tih aplikacija [8]. Niti jedan od ova dva pristupa nije idealan i oba načina donose određeni stupanj rizika. Javlja se i problem pri klasifikaciji aplikacije jer nisu sve aplikacije samo dobre ili samo loše, već su negdje između, tj. njihova klasifikacija ovisi o kontekstu i načinu primjene. Korištenje aplikacije za pohranu podataka (npr. *Dropbox*) za razmjenu dokumentacije o proizvodu je dobar način korištenja aplikacije, dok korištenje iste aplikacije za razmjenu piratskog sadržaja nije dobar način korištenja [9].

Da bi se povećala učinkovitost i pristupačnost *web* 2.0 aplikacija, mnoge aplikacije koriste specifične tehnike rada. Te tehnike mogu uključivati [6]:

- preskakanje portova (*port hopping*): portovi i protokoli se nasumično mijenjaju tijekom sesije. Slikom 4 prikazan je trend primjene tehnike preskakanja potrova.



Slika 4 Korištenje tehnike preskakivanja portova kod pojedinih aplikacija, [6]

- korištenje nestandardnih portova: brojne aplikacije otvaraju nasumične portove i ne koriste *well-known* portove[8].
- tuneliranje prometa unutar poznatog protokola kao npr. korištenje aplikacije za razmjenu poruka ili sadržaja preko porta 80.
- korištenje SSL [9] enkripcije: korištenje SSL-a za zaštitu sadržaja predstavlja pozitivnu praksu ali i veliki problem u slučaju potrebe za pregledavanjem tog sadržaja na sigurnosnim uređajima, kao i problem povećanja količine prometa .

[8] *Well-known* portovi- portovi dodijeljeni od strane *Internet Assigned Numbers Authority*, organizacije.
[9] SSL(*Secure Sockets Layer*): transportni protokol koji omogućuje sigurnu komunikacija na internetu.

3.2 Slabosti tradicionalnih sigurnosnih rješenja

Paralelnom s razvojem *web* 2.0 aplikacija i njihovom sve većom primjenom, razvijaju se i sve kompleksniji i softiciraniji napadi na informacijsko-komunikacijske sustave. Novi načini napada baziraju se na aplikacije i aplikacijski sloj. Napadači koriste tehnike koje su opisane u prethodnom odjeljku da bi dobili pristup sustavima. Također porastom broja aplikacija dolazi se i do porasta *zero-day*[10] ranjivosti. U ovome poglavlju opisati će se nedostaci klasičnih vatrozida u osiguravanju informacijsko-komunikacijskih sustava i zašto je došlo do potrebe za razvojem nove generacije vatrozida.

Tradicionalni vatrozidi druge generacije povijesno su osiguravali visok stupanj sigurnosti. Iz razloga što su ponašanja aplikacija bila dobro poznata npr. *email* se bazirao na portu 25, *web* surfanje na portu 80 itd. vrijedilo je pravilo port+protokol=aplikacija. Sukladno tom pravilu vatrozidi su mogli lako održavati visoku razinu sigurnosti. Blokiranjem određenog porta blokirala bi se i aplikacija. U današnjem svijetu događaju se promjene, internet promet zauzima sve veću količinu prometa. Problem predstavlja da se pod internet prometom nalazi veliki broj aplikacija od kojih svaka ima svoj način ponašanja i donosi određeni rizik, također sve je više prometa koji je kriptiran korištenjem SSL protokola. Tradicionalni vatrozidi kao uređaji vide sav promet koji prolazi kroz njih, problem predstavlja da su na određeni način "slijepi" tj. mogu vidjeti određene generalne stvari ali ne i detalje. Tradicionalni vatrozidi pregledavaju pakete i određuju aplikaciju temeljem broja porta te se oslanjaju na činjenicu da je određeni port dodijeljen određenom aplikacijskom protokolu (npr. TPC port 80 odgovara HTTP[11] protokolu). Također vatrozidi prve i druge generacije ne mogu detektirati i procesirati određene tehnike kao npr. tehnike preskakanja portova i tuneliranja prometa. Iz svega navedenog može se zaključiti da tradicionalni vatrozidi nemaju inteligencije da odrede koje aplikacije [6]:

- služe poslovnoj svrsi.

[10] *Zero day*ranjivost : otkrivena i napadačima poznata ranjivost za koju proizvođač nije objavio zakrpu.

[11] HTTP (*HyperText Transfer Protocol*): protokol za prijenos HTML dokumenata tj. *web* stranica. Najkorišteniji protokol na Internetu. Radi na aplikacijskom sloju OSI modela.

- služe poslovnoj svrsi ali u određenim uvjetima koriste se za nedozvoljene radnje .
- trebaju biti blokirane jer mogu predstavljati veliku prijetnji iako mogu služiti poslovnoj svrsi.

Veliki problem predstavlja nedostatak kontrole prometa koji se može blokirati ili propustiti ali ne postoji mogućnost za detaljnijom kontrolom koja bi dopuštala određene funkcionalnosti aplikacija i odgovarala bi kao idealni model za brojne *web* 2.0 aplikacije. Primjeri naprednih kontrola su propuštanje aplikacije određenoj grupi korisnika ili u određenom vremenu itd.

Da bi se poboljšali tradicionalni vatrozidi proizvođači su dodali mogućnost duboke inspekcije paketa. Ova nadogradnja donijela je više kontrole i mogućnosti vidljivosti aplikacijskog sloja. Ipak ova nadogradnja bila je samo nadodana funkcionalnost koja nije bila integrirana u sami vatrozid što je dovodilo do toga da se zaglavlje mrežnog i transportnog sloja koristilo za inicijalnu klasifikaciju paketa. Ostali su brojni problemi među kojima su najznačajniji:

- mnoge aplikacije koje ne bi trebale imati pristup mreži su imale pristup mreži.
- iz razloga da se vrši duboka inspekcija svih paketa, dolazi se do zagušenja sustava jer se pregledava i ono što se ne bi trebalo.
- oslanjanje na sadržaj mrežnog i transportnog sloja za odlučivanje dali se provodi duboka inspekcija može uzrokovati ulazak neželjenog prometa u sustav .

Uvođenjem IPS rješenja za blokiranje napada koji se fokusiraju na ranjivosti u aplikacijama i sustavima podiže se nivo sigurnosti ali i dalje postoje brojni problemi. IPS radi na način da razumije protokole i ima mogućnost detaljnije analize prometa i primjena metoda za otkrivanje napada. Većina IPS sustava koristi IP adresu i port u prvom koraku klasifikacije aplikacije. Iz razloga da *web* 2.0 aplikacije ne koriste standardne portove ili je promet tuneliran, IPS sustavi imaju problema s detekcijom takvog prometa jer ne mogu prepoznati o kojoj se točno aplikaciji radi. IPS je dizajniran na sprječavanje prijetnji metodom "nađi i ubi" što ne omogućuje kontrolu aplikacija, također IPS sustavi primjenjuju se kao dodatni uređaji uz vatrozid. IPS i IDS sustavi

rade na tehnikama koje su dobro definirane ali su relativno stare. Prema [8] nove metode napada koje IPS i IDS ne pokrivaju uključuju

- kriptirani napadi: ukoliko se prijetnja šalje unutar kriptiranog prometa IPS i IDS sustavi ne mogu otkriti takvu prijetnju. IPS i IDS sustavi ne posjeduju mogućnost dekripcije prometa.
- nemogućnost kontrole i klasifikacije sadržaja dovodi do brojnih napada koji koriste sigurne aplikacije kao prijenosno sredstvo za maliciozne programe.

Tijekom godina uz opisana sigurnosna rješenja sigurnost sustava nastojala se podići implementacijom brojnih dodatnih samostalnih sigurnosnih rješenja kao npr. *Antivirus* rješenja, *web* filtra, itd. Ovaj pristup donosi brojne probleme, dodavanjem rješenja za rješenjem povećava se kompleksnost sustava. Uz povećanu kompleksnost povećava se i cijena održavanja sustava kao i problem povećanog kašnjenje i zagušenje prometa iz razloga što promet mora prolaziti kroz više odvojenih uređaja.

3.3 Mogućnosti vatrozida nove generacije

Radi svih problema opisanih u prošlom poglavlju došlo je do potrebe za razvojem jedinstvenog sigurnosnog rješenja koji bi zadovoljio moderne sigurnosne potrebe za kontrolom i identifikacijom aplikacija. Godine 2009. *Gartner* definira pojam vatrozid nove generacije kao "popravljeni" vatrozid sa nadodanim brojnim funkcionalnostima. Vatrozid nove generacije temelji rad na klasifikaciji prometa prema identitetu aplikacije. Mogućnost identifikacije aplikacije odnosi se na *web* 2.0 aplikacije kao i povijesne aplikacije koje se koriste u poslovnim sustavima. Osnovne funkcionalne zahtjeve za efektivne vatrozide nove generacije uključuju brojne mogućnosti [6] :

- identifikacija aplikacije neovisno o portu, protokolu, tehnici rada ili korištenju SSL enkripcije.

- podrška za prioritiziranje prometa primjenom *traffic shaping i traffic policing*[12]mehanizama.
- omogućavanje bolje vidljivosti i granularne kontrole aplikacija.
- točna identifikacija korisnika i korištenje identitete korisnika kao atributa za sigurnosnu kontrolu.
- osiguravanje starovremenske zaštite sustava od brojnih prijetnji uključujući prijetnje na aplikacijskom sloju.
- integracija a ne kombiniranje tradicionalnih vatrozida sa IPS sustavima, *antivirusnim* rješenjima i *web* filtrima.
- podrška za obradom velike količine prometa reda više gigabita u sekundi bez opadanja performansi sustava.

Uz ove zahtjeve potrebna je podrška za funkcije tradicionalnih vatrozida što uključuje podršku za:

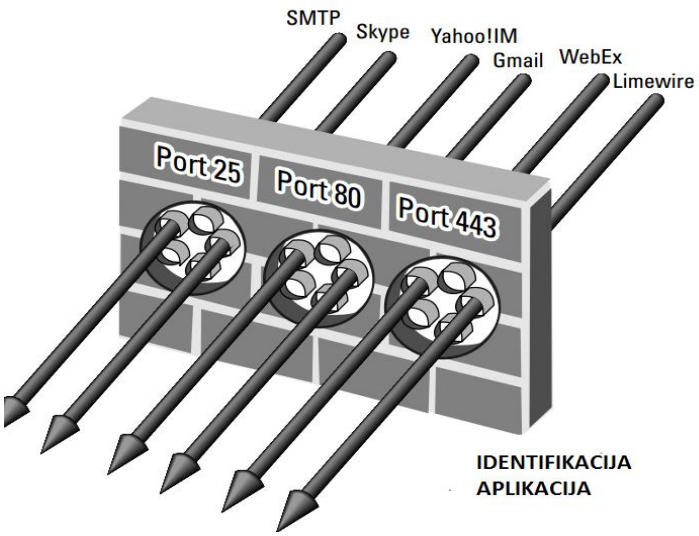
- paketno filtriranje,
- inspekciju stanja,
- NAT [13],
- duboku inspekciju paketa,
- VPN [14] i
- IPS i IDS mogućnosti.

Ključna mogućnost vatrozida nove generacije je da može sve što i tradicionalni vatrozid ali sa nadodanim naprednim mogućnostima koje uključuju nove tehnologije, visoke performanse i dodatne funkcionalnosti koje ovise o zahtjevima sustava. U nastavku rada biti će detaljnije opisane važnije komponente i funkcionalnosti vatrozida nove generacije.

[12]*traffic shaping* i *traffic policing*: najpoznatiji mehanizmi za omogućavanje ostvarivanja kvalitete usluge (QoS)
[13] NAT (*Network address translation) :* metoda za takozvanu translaciju adresa tj .prevađanje više adresa u jednu. Najkorišteniji mehanizam za pristupanje internetu korištenjem lokalnih privatnih adresa.
[14] VPN (virtual privat network): sigurnosni mehanizam koji omogućuje slanje i primanje podataka kroz javnu mrežu kao da su ti uređaji direktno spojeni na privatnu mrežu

3.3.1 Identifikacija aplikacija

Određivanje porta i protokola važan je prvi korak u identifikacije aplikacije ali je sam za sebe nedovoljan. Mogućnost robusne identifikacije i inspekcije prometa omogućuje granularnu kontrolu nad sesijom podataka koja prolazi kroz vatrozid bazirajući se na aplikacije a ne na poznavanju komunikacijskih parametara (IP adresa, port). Identifikacija aplikacija i prometa koje generiraju te aplikacije predstavlja samo srce vatrozida nove generacije.



Slika 5 Identifikacija aplikacija, [6]

Identifikacija aplikacija temelji se na višekriterijskom pristupu koji mora raditi bez obzira na port, protokol, enkripciju ili tehniku rada koja se koristi. Prema [11] tehnike koje se koriste za identifikaciju aplikacija obuhvaćaju:

- detekciju protokola i dekripciju podataka: određivanje protokola aplikacije (npr. FTP [15]) i ako se koristi SSL mogućnost dekripcije podataka radi daljnje analize. Nakon analize podataka promet se ponovo kriptira.

[15] FTP (*File Tranfer Protocol*): protokol koji služi za razmjenu podataka između 2 *hosta* na mreži.

- mogućnost analize protokola: utvrđivanje dali je detektirana aplikacija prava ili se koristi kao tunel za skrivanje stvarne aplikacije (npr. mail aplikacija može ići preko porta 80).
- aplikacijski potpisi: točno utvrđivanje aplikacije i pretraživanje prometa po definiranim obrascima tj. potpisima neovisno o tome koji se port i protokol koristi. Podržana je mogućnost otkrivanja specifičnih funkcija unutar aplikacija (npr. otkrivanje prijenosa podataka unutar razgovora)
- heuristika: za aplikacije koje se ne mogu otkriti temeljem potpisa (npr. *voip*[16], P2P[17]) mogućnost otkrivanja putem heuristike.

Pravilno otkrivanje aplikacije predstavlja prvi i ključni korak u zaštiti modernih informacijsko-komunikacijskih sustava.

3.3.2 Identifikacija korisnika

Identifikacija korisnika povezuje IP adrese sa određenim korisnikom. Postoji mogućnost da određeni korisnik ima samo jednu IP adresu ali postoji i mogućnost da korisnik ima nekoliko IP adresa ako koristi više različitih uređaja sa kojima je povezan. Identifikacija korisnika omogućuje pregled i kontrolu mrežnih aktivnosti i prometa po svakom korisniku. Integracija sa LDAP [18] direktorijima kao npr. *Microsoft Active Directory* omogućuje identifikaciju korisnika i mogućnost kontrole korisnika. Identifikacija korisnika može se provoditi na više načina kao npr. preko specijaliziranih formi za prijavu ili sa direktnom integracijom sa servisima za prijavu. Komunikacijom sa LDAP direktorijima dobivaju se važne informacije o korisniku kao npr. uloge i grupe. Uz pomoć dobivenih detalja o korisniku može se [12]:]

- nadzirati koju aplikaciji koristi, koji sadržaj prenosi i koliki promet generira korisnik na mreži.
- omogućiti identitet korisnika kao varijable unutar sigurnosne politike

[16] *Voip*- tehnika prijenosa govora korištenjem IP tehnologije
[17] P2P- arhitektura komunikacije u kojoj svi hostovi komuniciraju sa svima bez centralne jedinice za nadzor i kontolu
[18] LDAP (*Lightweight Directory Access Protocol*): protokol koji služi za pisanje i čitanje iz imeničkih servisa kao npr. *Microsoft Active Directory*

- olakšati dobivanje izvještaja o radu korisnika.

Identifikacijom korisnika omogućava se i pametna kontrola korištenja aplikacija koja može pridonijeti poboljšanju poslovanja. Npr. moguće je dopustiti marketinškom odjelu ili odjelu za odnose s javnošću korištenje društvenih mreža jer je to potrebno u njihovom poslu ali zabraniti korištenje društvenih mreža ostalim grupama ili individualcima kojima to nije potrebno za posao.

3.3.3 Identifikacija sadržaja

Identifikacija sadržaja dodaje vatrozidima nove generacije brojne funkcionalnosti i mogućnosti. Ovisno o proizvođaču i modelu ove funkcionalnosti se znatno razlikuju. Ova komponenta vatrozida sastoji se od više pod komponenti koje mogu biti:

- Prevencija prijetnji: ova komponenta sprječava crve, viruse i ostale prijetnje od ulaza u mrežu. Provjera i kontrola prometa izvodi se neovisni o aplikaciji. Ova komponenta sastoji se od nekoliko pod komponenti i funkcionalnosti kao npr.:
    - dekoder aplikacija: ukoliko se koristi poznata aplikacija, pregledava se sadržaj aplikacije i pretražuju određene prijetnje tj. potpisi. Ova metoda potvrđuje da određeni promet pripada određenom protokolu.
    - skeniranje prijetnji zasnivano na protoku: promet se skenira kada dođe prvi paket i skeniranje se odvija paket po paket. Ovom metodom ne čeka se učitavanje cijelog sadržaja za skeniranje, čime se dobiva povećanje propusnost i smanjenje latencije.
    - IPS funkcionalnosti: uz dekoder aplikacija za traženje prijetnji implementiraju se i anomalije protokola, anomalije ponašanja i heurističke metode. Implementacijom svih ovih metoda postiže se visok stupanj sigurnosti za poznate kao i nepoznate prijetnje [13].

- URL[19] filtriranje: URL filtriranje je alat koji se koristi za klasifikaciju sadržaja. Moderni vatrozidi sadrže baze podataka u kojima se nalazi veliki broj stranica sortiranih u brojne kategorije koje se mogu jednostavno filtrirati. Također radi se nadziranje *web* prometa. *Web* promet može se kontrolirati i filtrirati i uz kombinaciju sa identifikacijom korisnika. Primjenom pametne sigurnosne politike može se povećati sigurnost cijelog sustava jer postoji mogućnost filtriranja korištenja *weba* do razine korisnika. Ukoliko se zabrane *web* stranice koje su poznate po velikom broju prijetnji jednostavnom tehnikom URL filtriranja znatno se povećava sigurnost sustava [14].
- filtar datoteka i podataka: omogućena je primjena raznih sigurnosnih politika koje onemogućavaju prijenos nedozvoljenih podataka. Sposobnosti filtra uključuju mogućnost blokiranja datoteka ovisno o tipu i ekstenziji kao i mogućnost kontrole prijenosa osjetljivih podataka kao Filtar datoteka i podataka nadopunjuje identifikaciju aplikacija i za mnoge aplikacije ima mogućnost kontrole prijenosa datoteka i podataka unutar same aplikacije (npr. prijenos slike unutar programa za razmjenu poruka) [13].

Primjenom identifikacije sadržaja dobiva se mogućnost sprječavanja prijetnji, smanjenja neprimjerenog korištenja interneta kao i kontrola prijenosa osjetljivih podataka.

3.3.4 Politike kontrole prometa

Identifikacijom aplikacije, korisnika koji je koristi i sadržaja koji se prenosi predstavlja važan i prvi korak u identifikaciji prometa koji ulazi i prolazi kroz mrežu. Učenje o ponašanju aplikacije predstavlja sljedeći korak pri donošenju odluke kako se odnositi prema aplikaciji. Nakon što se dobije potpuna slika o upotrebi aplikacije, organizacija

[19] URL(*Uniform Resource Locator):* točna putanja do određenog sadržaja na internetu najčešće neke web stranice

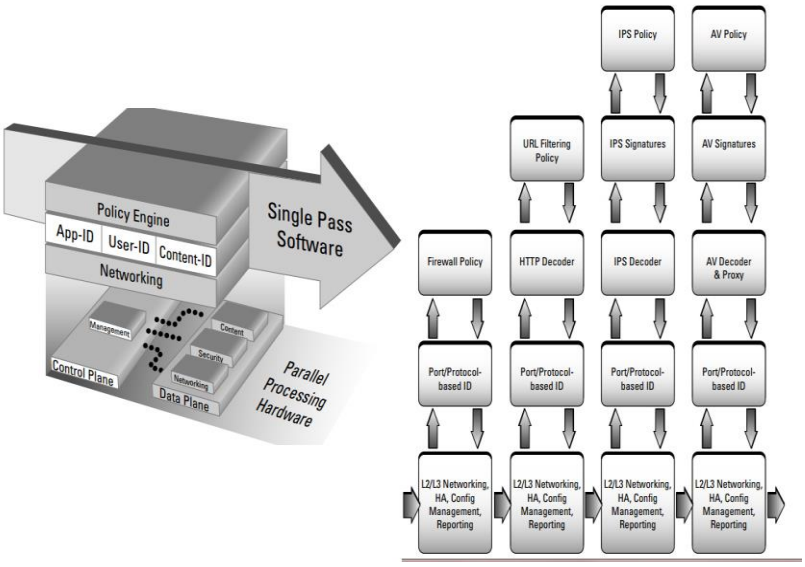
može primijeniti sigurnosnu politiku na promet koji generira određena aplikacija i koji ulazi ili izlazi iz mreže. Za razliku od tradicionalnih vatrozida koji su propuštali ili odbijali promet, vatrozidi nove generacije imaju mogućnosti granularnijeg pristupa prema prometu. Radi postojanja mogućnosti kombiniranja aplikacija, korisnika i sadržaja koji se prenosi mogu se primjenjivati napredne politike koje mogu [15]:

- propustiti ili odbiti promet,
- propustiti ali skenirati promet
- propustiti ovisno o vremenu, korisniku ili grupi korisnika,
- dekriptirati i pregledati sadržaj pa donijeti odluku,
- propustiti ali tretirati promet prema parametrima kvalitete usluge,
- dopustiti određene funkcionalnosti aplikacije,
- kombinacija prethodno navedenih.

Pravilnim odabirom i implementacijom politika zajedno s pravilnom korištenjem ostalih komponenti vatrozida ostvaruje se visok stupanj zaštite informacijsko-komunikacijskih sustava.

3.3.5 Arhitektura visokih performansi

Za razliku od tradicionalnih vatrozida koji su imali potrebe za malim performansama i hardverskim zahtjevima vatrozidi nove generacije dizajnirani su da od početka dostave visoke performanse. Iz razloga da je došlo do velikog povećanja količine i raznolikosti prometa kao i osjetljivosti brojnih aplikacija na kašnjenje i latenciju potrebno je osigurati visoke performanse. Vatrozidi nove generacije dizajnirani su tako da unutar velikog opterećenja, čak i ako su sve mogućnosti inspekcije prijetnji pokrenute simultano da održavaju normalne latencije i kašnjenja. Tradicionalni sigurnosni proizvodi dizajnirani su na način da se svaka sigurnosna funkcija obavlja samostalno. Takav način dizajna povećava kašnjenje i latenciju jer se provjera paketa ponavlja više puta. Vatrozidi nove generacije dizajnirani su da koriste arhitekturu jednostrukog prolaza (*single pass arhitecture)*. Slikom 9 prikazana je usporedba arhitekture jednostrukog prolaza i arhitekture višestrukog prolaza.



Slika 6 Prednost sustava s jednostrukim prolazom, [8]

Upotrebom arhitekture jednostrukog prolaza ostvaruju se visoke performanse sustava.

4.Arhitekture vatrozida

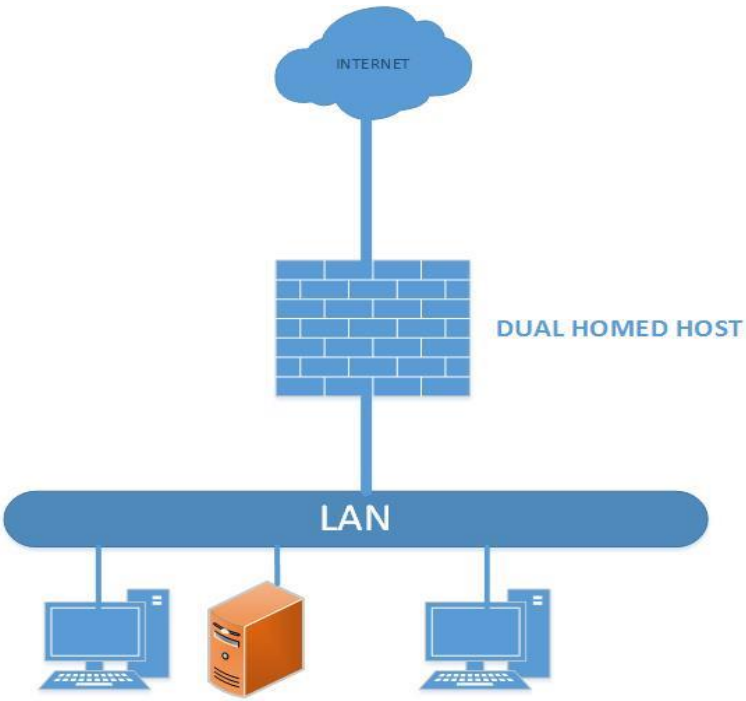
Vatrozidi mogu biti postavljeni na više mjesta u mreži. Uz pravilnu konfiguraciju vatrozida od velike važnosti je i postaviti vatrozid na pravo mjesto u mreži. Odluka o mjestu postavljanja vatrozida u mreži donosi se ovisno o potrebama. U ovome poglavlju biti će opisane osnovne arhitekture s vatrozidima tj. mjesta u mreži na koja se postavljaju vatrozidi.

4.1 *Bastion host*

Bastion *hostom* smatra se svako računalo tj. poslužitelj koji je dostupan s interneta. Radi dostupnosti s interneta bastion *host* predstavlja visoko izloženi uređaj koji će najvjerojatnije biti meta napadačima. Bastion *host* postavlja se što bliže nesigurnoj vanjskoj mreži kao npr. internetu. Mnogi različiti poslužitelji smatraju se bastion *hostom* kao npr. *web* ili *mail* poslužitelji [5].

4.2 *Dual homed* arhitektura

Dual homed predstavlja uređaj koji ima 2 mrežna sučelja. Jedno sučelje prihvaća promet sa vanjske mreže a na drugo sučelje priključuje se unutarnja mreža. *Dual homed* vatrozid može služiti kao usmjernik prometa. Ova arhitektura radi na principu jedne točke ulaza u mrežu što se može vidjeti iz slike 9. Sav promet u mrežu ulazi kroz jedno sučelje i tada se vrši potrebna kontrola prometa. Kod primjene ove arhitekture *hostovi* iz unutarnje mreže mogu komunicirati sa vatrozidom kao i *hostovi* iz vanjske mreže ali je direktna veza između vanjske i unutarnje mreže onemogućena čime se dobiva visoka razina kontrole. Prednost ovakve arhitekture je samo jedan ulaz u mrežu čime se dobiva velika kontrola. Nedostatak ovakve arhitekture je veliko opterećenje performansi vatrozida kao i problem jedinstvene točke ispada, jer u slučaju ispada vatrozida napadač dobiva direktan pristup unutarnjoj mreži [5] .

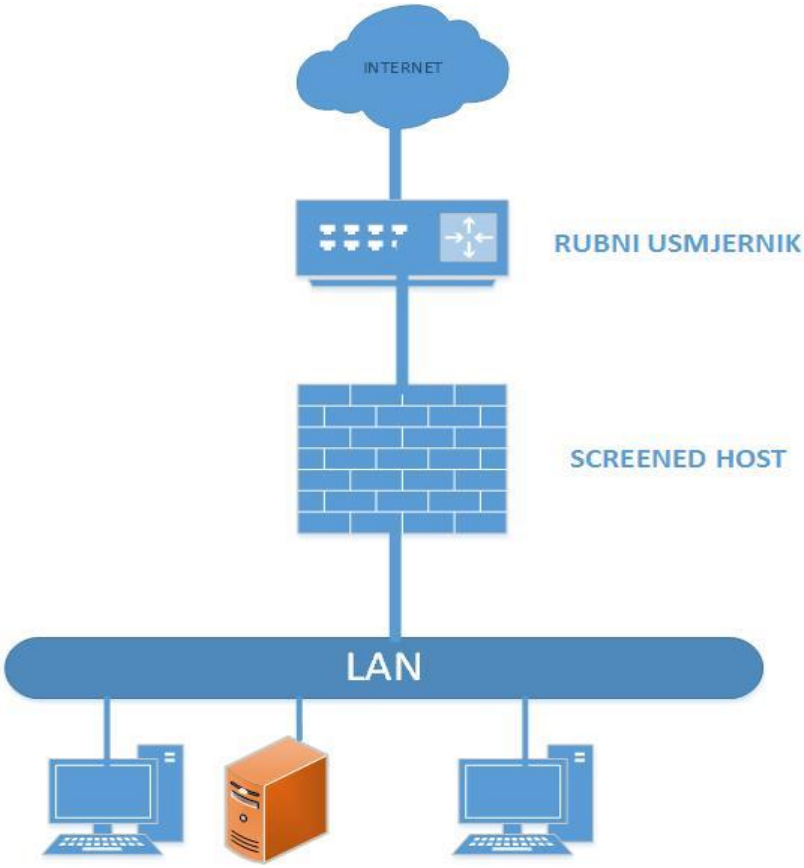


Slika 7 *Dual homed* arhitektura

Izvor: [16]

4.3 *Screened host* arhitektura

Screened host predstavlja vrstu vatrozida koji se nalazi između rubnog usmjernika tj. usmjernika koji se nalazi na ulazu u mrežu i unutarnje mreže. Promet koji dolazi sa interneta prvo se paketski filtrira na rubnom usmjerniku a nakon toga promet se prosljeđuje vatrozidu koji vrši dodatnu kontrolu prometa. Nakon kontrole promet se prosljeđuje unutarnjoj mreži. *Screened host* tj. vatrozid predstavlja jedini uređaj koji prima promet sa usmjernika i sav promet između interneta i vanjske mreže uvijek prolazi kroz vatrozid. Ovaj model predstavlja osnovnu arhitekturu višeslojne zaštite mreže tzv. *defense in depth* modela iz razloga da ako se dogodi ispad vatrozida veliki dio prometa filtrirati će se na rubnom usmjerniku [5].

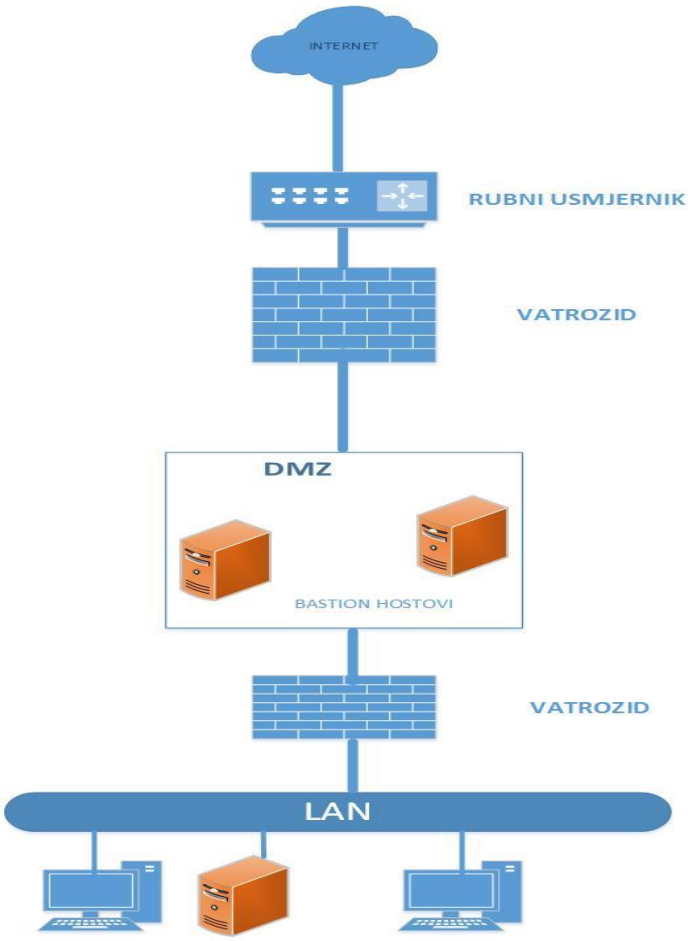


Slika 8 Screened host arhitektura

Izvor: [5]

4.4 *Screened subnet* arhitektura

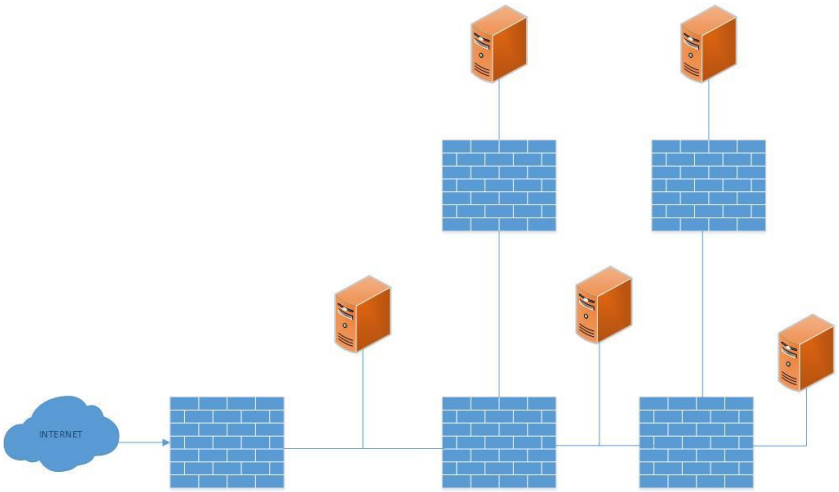
Screened subnet arhitektura predstavlja nadogradnju *screened host* arhitekture na način da se dodaje još jedan sigurnosni sloj u *screened host* arhitekturu. Arhitektura se temelji na korištenju tzv. demilitazirane zone i upotrebe 2 vatrozida. Demilitazirana zona nalazi se između 2 vatrozida tj. vatrozida koji se nalazi na ulazu u mrežu i kontrolira pristup demilitaziranoj zoni i vatrozida koji filtrira promet namijenjen unutarnjoj mreži. U demilitaziranu zonu smještaju se bastion *hostovi* tj. serveri i računa za koje postoji potreba pristupa i sa interneta i sa unutarnje mreže [5].



Slika 9 *Screened subnet* arhitektura

Izvor: [5]

Ova arhitektura predstavlja pravi primjer višeslojne zaštite jer da bi napadač dobio pristup unutarnjoj mreži mora probiti 3 uređaja a ne samo jedan. Također postoje kompleksnije izvedbe ove arhitekture u kojima se koriste više različitih demilitariziranih zona kao i više vatrozida među kojima se i upotrebljavaju *proxy* vatrozida za kontrolu pristupa određenoj aplikaciji kao što je prikazano slikom 12 [17].



Slika 10 Arhitektura sa višestrukim vatrozidima

Prednost ovakve arhitekture predstavlja visok stupanj sigurnosti a glavni nedostatak visok stupanj kompleksnosti za konfiguriranje i nadzor.

5. Implementacija vatrozida nove generacije

Zaštita informacijsko komunikacijskog sustava svodi se na zaštitu od neovlaštenog pristupa sustavu, a samim time na zaštitu od neovlaštenog pristupa podacima koji se unutar takvog sustava pohranjuju, obrađuju i prenose. Kako bi se umanjila vjerojatnost da prijetnja utječe na rad informacijskog sustava ili da se umanji nastala šteta kad prijetnja iskoristi ranjivost, uvode se sigurnosne kontrole [18]. Postoje brojni proizvođači i brojne verzije vatrozida nove generacije. Radi pravilnog odabira vatrozida nove generacije koji će se implementirati nužno je pravilno definirati zahtjeve prema potrebe organizacije. U ovome poglavlju biti će opisane sigurnosne kontrole koje se moraju uzeti u obzir prilikom odabira i implementacije vatrozida nove generacije. Također opisati će se koncept segmentacije mreže na sigurnosne zone.

5.1 Kontrola zaposlenika

Većina organizacija ima definiranu politiku korištenja aplikacija koja propisuje koje su aplikacije odobrene i dopuštene za instalaciju i korištenje, a koje su zabranjene. Svaki zaposlenik organizacije trebao bi razumjeti i pridržavati se sadržaja definirane kontrole. Prilikom izrade kontrole zaposlenika trebaju se definirati sljedeće stavke:

- način informiranja korisnika o dozvoljenim i zabranjenim aplikacijama,
- tehnike i načine izmjena i nadopunjavanja liste zabranjenih i dozvoljenih aplikacija, kao i način informiranja korisnika o promjeni liste,
- definiranje povreda politike,
- definiranje kazne za povredu politike,

Pravilno dokumentirana kontrola zaposlenika predstavlja ključni dio za pravilnu konfiguraciju i implementaciju vatrozida nove generacije [6].

5.2 Kontrola radne površine

Uz pravilno definiranje kontrole zaposlenika, kontrola radne površine predstavlja ključni dio osiguravanja sigurnosti sustava. Kontrolom radne površine korisnicima se ograničavaju mogućnosti instalacije novih aplikacija kao i izmjene instaliranih aplikacija. Prilikom definiranja kontrole radne površine trebaju se definirati sljedeći stavke [6]:

- pravila korištenja i instalacije aplikacija koje se nalaze na USB diskovima,
- pravila korištenja i instalacije i aplikacija koji se nalaze unutar *email* poruka,
- pravila korištenja i instalacije aplikacija preuzetih sa interneta,
- opseg korisničkih prava tj. definiranje što sve može napraviti određeni korisnik na računalu,
- prava korištenja administratorskih prava tj. definiranje tko sve ima pravo pristupa i korištenja administratorskih računa.

Kombinacijom kontrola radne površine i kontrola zaposlenika definirane su kontrole ljudskog faktora informacijske sigurnosti.

5.3 Mrežne kontrole

Mrežnom kontrolom definiraju se načini zaštite računalne mreže kao i mehanizmi za kontrolu pristupa i prijenosa informacija kroz mrežu. Prilikom definiranja mrežne kontrole trebaju se definirati sljedeći stavke:

- pravila za filtriranje paketa,
- popisi dozvoljenih i zabranjenih IP adresa,
- popisi dozvoljenih i zabranjenih portova,
- pravila za korištenje i implementaciju IPS sustava,
- pravila za korištenje i implementaciju IDS sustava i
- pravila za implementaciju *proxy* rješenja.

Pravilnom mrežnom kontrolom postiže se visok stupanj sigurnosti prijenosa informacija kroz mrežu.

5.4 Definiranje korisničkih zahtjeva za uvođenje vatrozida nove generacije

Pravilnim definiranjem sigurnosnih politika znatno se olakšava proces definiranja zahtjeva za vatrozidima nove generacija. Vatrozid nove generacije mora imati mogućnost da izvršava i provodi sve zadane sigurnosne kontrole. Ukoliko organizacija želi biti usklađena sa određenim standardom vezanim uz zaštitu podataka kao npr. sa PCI DSS standardom[20] tada postoje predefinirani zahtjevi vezani za vatrozide nove generacije. Ti zahtjevi kombiniraju se sa ostalim zahtjevima zadanim od organizacije prilikom definiranja zahtjeva za uvođenjem vatrozida nove generacije. Prilikom definiranja zahtjeva definiraju se potrebe i mogućnosti za svaku komponentu vatrozida nove generacije. Komponente koje se uzimaju u obzir prilikom kreiranja zahtjeva su: identifikacija aplikacija, kontrola aplikacija, sustav za prevenciju prijetnji, mogućnosti upravljanja uređajem, mrežne mogućnosti, hardverske performanse.

Identifikacija aplikacija: potrebno je definirati razinu preciznosti identifikacije aplikacija i mehanizam koji će se koristiti za identifikaciju aplikacija. Parametri koji se uzimaju u obzir prilikom kreiranja zahtjeva su: [19]

- dali se identifikacija bazira na IPS ili DPI tehnologiji,
- performanse i preciznost uređaja prilikom identifikacije aplikacija,
- mogućnost rukovanja s nepoznatim aplikacijama,
- jeli moguće kreiranje vlastitih potpisa aplikacija,
- način i mogućnosti identifikacije, inspekcije i kontrole kriptiranog prometa,
- veličina baze podataka poznatih aplikacija,
- dali postoji mogućnost dodavanja vlastitih aplikacija u bazu i
- dali postoji mogućnost URL filtriranja.

[20] PCI DSS (*Payment Card Industry Data Security Standard):* jedinstveni industrijski standard koji osigurava sigurnost podataka prilikom korištenja kartičnog poslovanja.

Politika kontrole aplikacija: potrebno je definirati proces i parametre za politiku kontrole aplikacija. Parametri koji se uzimaju u obzir prilikom kreiranja zahtjeva su [19]:

- dali se politika može primjenjivati na sve aplikacije ili samo na neke,
- dali postoji mogućnost primjene politike samo za određenog korisnika ili grupu,
- dali postoji mogućnost primjene kontrola na korisnike koji se udaljeno spajaju na sustav,
- dali postoji mogućnost kontrole portova za sve aplikacije u bazi,
- dali postoji mogućnost primjene tradicionalnih pristupnih lista,
- dali postoji mogućnost informiranja korisnika o kršenju politike

Sustav za prevenciju prijetnji: potrebno je definirati sve potrebne značajke IPS i *antivirus* sustava. Parametri koji se uzimaju u obzir prilikom kreiranja zahtjeva su [19]:

- lista prijetnji koje se mogu otkrivati i blokirati,
- lista datoteka koje se mogu blokirati,
- dali je podržano filtriranje podataka i
- dali postoji mogućnost skeniranja kriptiranog prometa

Mogućnosti upravljanja: definiraju se mogućnosti za upravljanje i konfiguraciju vatrozida kao i nadzor prometa. Parametri koji se uzimaju u obzir prilikom kreiranja zahtjeva su [6]:

- dali postoji grafičko sučelje za upravljanje
- dali postoji jedinstveno sučelje za kreiranje politika kontrole ili je potrebno kreirati politiku za svaku komponentu sustava zasebno,
- dali postoji i koje su mogućnosti nadziranja prometa,
- mogućnosti vizualizacije prometa i kreiranja izvješća i
- dali postoji mogućnost centraliziranog upravljanja više uređaja.

Mrežne mogućnosti: potrebno je definirati mogućnosti integracije mrežnih funkcionalnosti (usmjeravanje, preklapanje itd.). Parametri koji se uzimaju u obzir prilikom kreiranja zahtjeva su:

- dali postoji mogućnost usmjeravanja i preklapanja prometa,
- dali je podržano VLAN označavanje prometa,
- dali su podržani dinamički protokoli za usmjeravanje (npr. OSPF, BGP, RIP),
- dali je podržana mogućnost konfiguracije i primjene DHCP servera,
- dali je podržan IPSec VPN,
- dali je podržan SSL VPN i
- dali postoji mogućnost implementacije sustava visoke dostupnosti

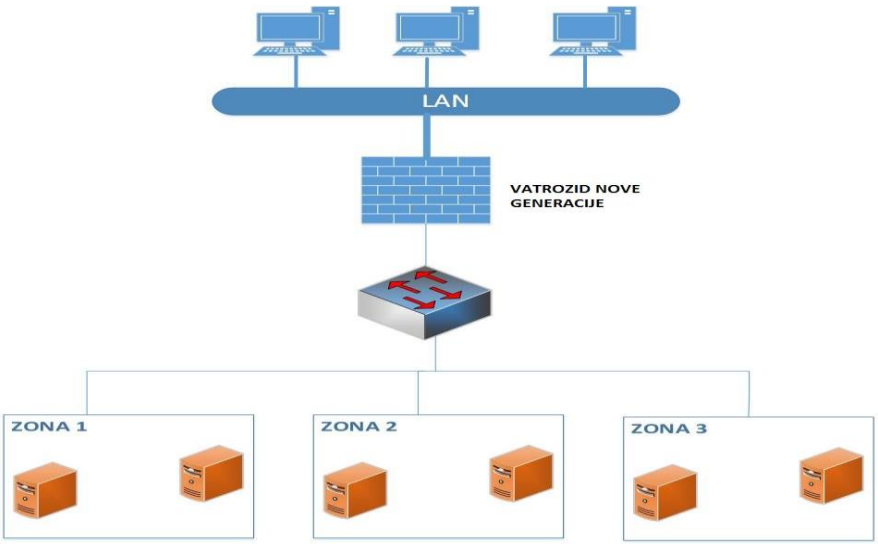
Hardverske performanse: definiraju se potrebni hardverski resursi koji će osigurati zadovoljavajuću razinu performansi sustava. Parametri koji se uzimaju u obzir prilikom kreiranja zahtjeva su:

- brzina procesora,
- broj jezgri procesora,
- arhitektura procesora,
- količina memorije ,
- brzina memorije,
- vrsta memorije,
- propusnost portova,
- broj portova i
- dali postoji mogućnost nadogradnje hardverskih komponenti

Nakon definiranja korisničkih potreba za svaku komponenti kreira se zahtjev. Nakon kreiranja zahtjeva odabire se i implementira proizvod koji najbolje odgovara kreiranom zahtjevu.

5.5 Segmentacija mreže i sigurnosne zone

Postavljanje vatrozida nove generacije na pravilnu lokaciju unutar sustava predstavlja ključni čimbenik u dizajniranju sustava. Dizajn sustava u kojima se implementiraju vatrozidi nove generacije temelji se na konceptu segmentacije. Postoji mnogo načina za segmentaciju mreža. Vatrozidi nove generacije koriste jedinstvenu kombinaciju hardverskih i softverskih mogućnosti segmentacije da bi omogućili organizaciji da izolira ključne dijelove mreže. Vatrozidi nove generacije koriste koncept sigurnosnih zona za segmentaciju mreže i izolaciju ključnih dijelova informacijsko-komunikacijskih sustava. Sigurnosna zona predstavlja logički spremnik za fizičko sučelje, VLAN[21], skup IP adresa ili kombinaciju navedenih. Sučelja kojima se pridjeljuje određena sigurnosna zona mogu biti konfigurirana u *Layer* 2, *Layer* 3 ili mješovitom modu. Sučelja koja rade u *Layer* 2 modu klasificiraju promet prema MAC[22] adresi ili dodijeljenoj VLAN oznaci. *Layer* 3 sučelja klasificiraju promet prema IP adresi. Sučelja u mješovitom modu koriste kombinaciju *Layer* 2 i *Layer* 3 moda.



Slika 11 Koncept segmentacije mreže i primjene sigurnosnih zona

[21] VLAN (*virtual* LAN): izvedba lokalne mreže u kojoj se jedna lokalna mreža dijeli na više odvojenih cjelina
[22] MAC: jedinstvena adresa mrežnog sučelja. Nalazi se na 2 sloju OSI modela.

6. Mogućnosti primjene vatrozida nove generacije

U ovome poglavlju biti će prikazane mogućnosti primjene vatrozida nove generacije u osiguravanju informacijsko-komunikacijskih sustava. Opisati će se i prikazati konfiguracija i testiranje nekih funkcionalnosti *Palo Alto* Pa-500 i *Fortigate* D60 vatrozida unutar laboratorijskog okruženja.

6.1 Prikaz mogućnosti i testiranje Palo Alto Pa-500 vatrozida nove generacije

U ovome poglavlju biti će prikazane osnovne funkcionalnosti *Palo Alto* vatrozida. Opisati će se i prikazati konfiguracija i testiranje nekih funkcionalnosti *Palo Alto* Pa-500 vatrozida unutar laboratorijskog okruženja.

6.1.1 Palo Alto tehnologije

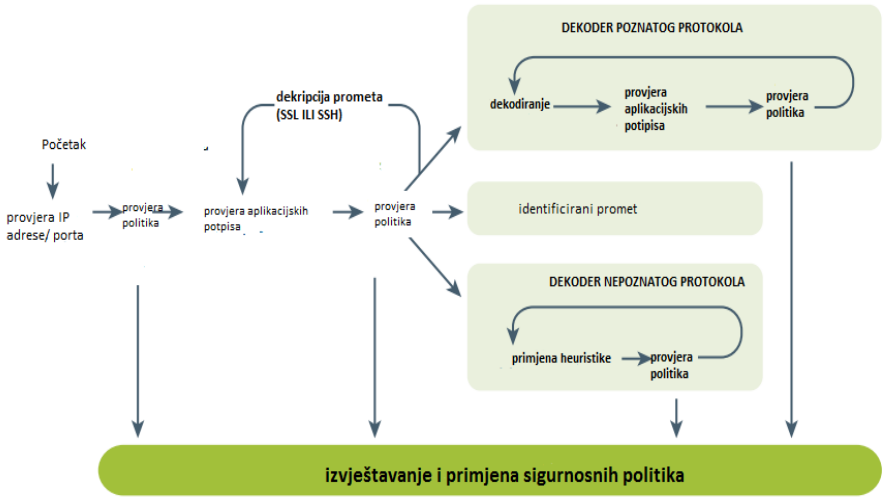
Palo Alto kompanija osnovao je 2005 godine Nik Zuk bivši zaposleni brojnih firmi za sigurnosna rješenja i glavni programer prvog IPS sustava. Od svoga nastanka, tvrtka se koncentrirala na razvoj vatrozida nove generacije jer je smatrala kako je pojam vatrozida općenito zastario te kako u posljednjih 15 godina nije bilo značajnijeg napretka na tom području. Stoga je tvrtka unijela mnoštvo inovacija u razvoj hardverskih vatrozida poput patentirane tehnologije APP-ID™ [15]. *Palo Alto* vatrozide pokreče PAN-OS operacijski sustav a svoj rad temelje na 3 tehnologije:

- *App*-ID™,
- *User*-ID i
- *Content*-ID.

6.1.1.1 App-ID

App-ID tehnologija predstavlja okosnicu svakog *Palo Alto* vatrozida i omogućuje prepoznavanje i kontrolu prometa više od 950 različitih aplikacija. Klasifikacija aplikacija koristi više mehanizama za prepoznavanje i kontrolu aplikacija. Mehanizmi koji se koriste za prepoznavanje aplikacija su: [20]

- potpisi aplikacija: aplikacijski potpisi koriste se za traženje jedinstvenih karakteristika aplikacije i osobine komunikacije aplikacija. Potpisi također otkrivaju dali aplikacija koristi standardni port za komunikaciju ili neki drugi.
- TLS/SSL i SSH dekripcija: ako *App*-ID otkrije da se koristi TLS/SSL enkripcija podataka i ako je uključena politika dekriptiranja prometa, tada se taj promet dekriptira i prosljeđuje drugim mehanizmima za identifikaciju aplikacija.
- dekodiranje aplikacijskog protokola: ako je potrebno, koriste se dekoderi koji otkrivaju koristi li se neki protokol isključivo za svoj transport ili se koristi za prijenos druge vrste prometa.
- heuristika: u nekim slučajevima aplikacija se ne može otkriti primjenom svih navedenih metoda. U tim slučajevima primjenjuje se dodatna heuristika ili analiza ponašanja aplikacije.



Slika 12 App-ID

Izvor: [22]

Identifikacija aplikacije predstavlja prvi korak u učenju o ponašanju prometa. Učenje o tome što aplikacija radi, koje portove koristi i na koje tehnologije se oslanja predstavlja sljedeći korak. Nakon što se dobije cjelokupni uvid u aplikaciju i način na koji radi primjenjuju se sigurnosne politike. Sigurnosne politike mogu biti [23]:

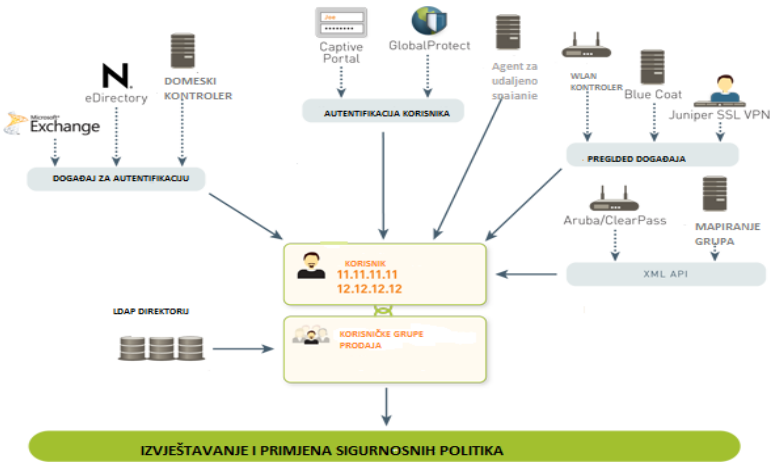
- dozvola ili zabrana prometa,
- dozvola ali uz skeniranje u potrazi za prijetnjama,
- dozvola ovisno o rasporedu, korisnicima ili grupama,
- dekripcija i analiza,
- dozvola i primjena QoS politike i
- dopuštanje samo određenih funkcionalnosti aplikacija.

Pravilnom konfiguracijom sigurnosnih politika može se ostvariti apsolutna kontrola nad radom aplikacije u određenom informacijsko-komunikacijskom sustavu.

6.1.1.2 User-ID

User-ID predstavlja komponentu vatrozida koja nadzire korisnike i primjenjuje sigurnosne politike. Korištenjem *User*-ID-a omogućena je integracija vatrozida sa različitim imeničkim servisima. Moguće je za svakog korisnika ili grupu korisnika definirati određenu sigurnosnu politiku. *User*-ID agent predstavlja aplikaciju koju je potrebno instalirati na računala u domeni ukoliko se želi raditi identifikacija korisnika. Za ostvarivanje svoje funkcionalnosti *User*-ID agent koristi sljedeće tehnike

- nadgledanje prijave na domenu (*Loging Monitoring*)-ovakvo nadgledanje vrši se kako bi se uspostavila korelacija između korištenih IP adresa i korisnika, odnosno grupa.
- povlačenje informacija s radnih stanica(*End Station Polling*)-svako aktivno računalo se ispituje kako bi se provjerila njegova IP adresa, što je nužno u slučaju kretanja korisnika bez ponovne autentifikacije na domenu.
- *Captive porta*l- služi za pridruživanje IP adresa korisnicima putem *web* sučelja. Koristi se u slučaju kada računala nisu dio domene [12].

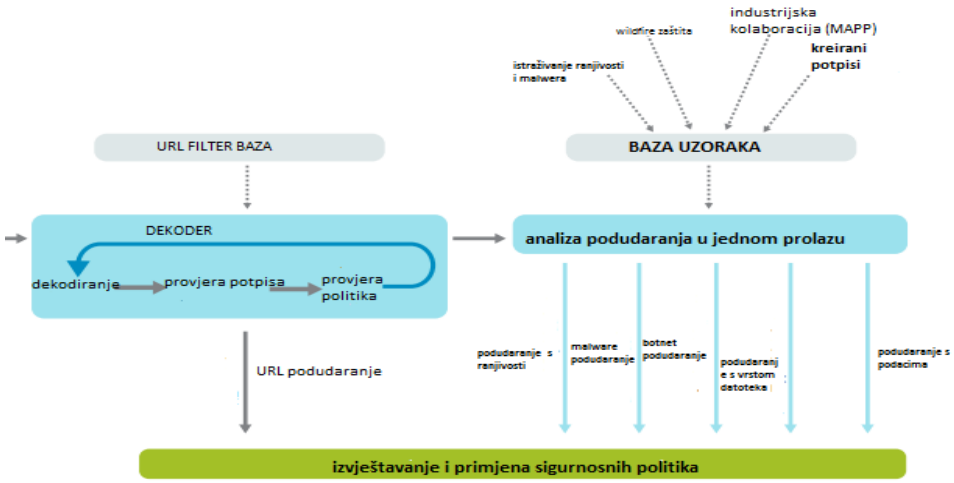


Slika 13 *User*-ID

Izvor: [12]

6.1.1.3 Content-ID

Content-ID tehnologija bazira se paralelnoj obradi sadržaja prometa. U jednom prolazu sadržaj se skenira na više različitih prijetnji. *Content*-ID tehnologija sastoji se od 3 komponente. Prva komponenta obrađuje sadržaj prometa. Druga komponenta otkriva sve maliciozne prijetnje (virusi, crvi itd.) kao i pokušaje iskorištavanja ranjivosti pojedinih aplikacija. Treća komponenta služi za filtriranje URL-ova [13].



Slika 14 *Content*-ID

Izvor: 13

6.1.2 *Palo Alto* PA-500

Palo Alto PA-500 predstavlja vatrozid nove generacije koji je namijenjen malim tvrtkama ili pojedinim odjelima velikih organizacija. Uređaj ima ugrađen PAN-OS operacijski sustav i podržava *App*-ID, *Content*-ID i *User*-ID tehnologije.

Slika 15 Palo Alto PA-500, [16]

Prema [21] *Palo Alto* posjeduje sljedeće specifikacije uređaja:

- propusna moć: 250 Mbps
- propusna moć komponente za prevenciju prijetnji: 100Mbps
- propusna moć IPSec VPN komponente: 50Mbps
- maksimalni broj novih sesija po sekundi: 7500
- maksimalni broj sesija: 64000
- maksimalni broj SSL sesija: 1000
- maksimalni broj sigurnosnih zona: 20
- maksimalni broj sigurnosni politika:1000
- maksimalni broj virtualni usmjernika: 3

Uređaj posjeduje sljedeća sučelja:

- 8 RJ45 sučelja (brzina 1Gbps)
- RJ45 konzolni port za upravljanje uređajem
- RJ45 (brzina 1Gbps) port za upravljanje uređajem

Uređaj posjeduje sljedeće hardverske specifikacije:

- kapacitet diska: 160GB

- Ulazni napon: 180W
- prosječna/maksimalna potrošnja električne energije: 45W/75W
- MTBF: 10.16 godina
- dimenzije: 1U" standardni *rack* (1.75*17*17 inča)

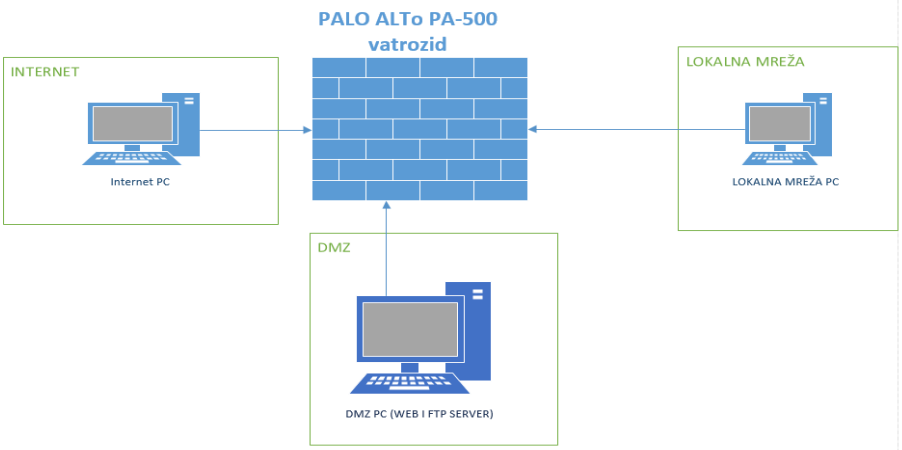
6.1.3 Opis testnog okruženja

Testiranje mogućnosti uređaja izvedeno je u laboratorijskom okruženju. Za testiranje su korištena tri računala s instaliranim *windows* 7 operacijskim sustavom i vatrozid nove generacije *Palo Alto* PA-500. Na vatrozid su direktno priključena tri računala i definirane tri različite mreže. Računala koja su spojena na vatrozid simuliraju:

- računalo koje se nalazi u lokalnoj mreži određene kompanije,
- računalo koje pristupa resursima mreže s interneta i
- server koji se nalazi u DMZ-u.

Na računalo koje je postavljeno u DMZ instaliran je *XAMPP. XAMPP* je vrlo jednostavna platforma s kojom se instalira *Apache*, *MySQL*, *PHP*, *FileZilla* i mnoge druge aplikacije. U laboratorijskom okruženju korištenom za izradu diplomskog rada računalo u DMZ-u simulirati će *web*[23] i FTP server[24] koji bi se nalazio u demilitariziranoj zoni kompanije. *XAMPP* je podešen na računalu u DMZ-u na način da je na njemu pokrenut *FileZilla*[25] i *Apache*[26] servis. Unutar *apache*-a postavljen je juss2 folder koji će simulirati *web* stranicu kompanije.

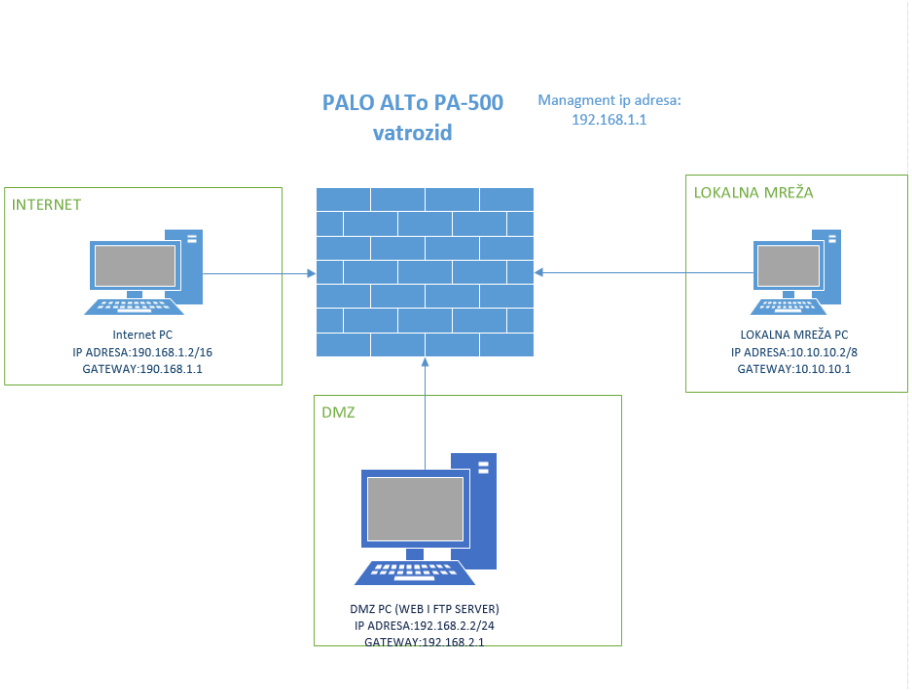
[23] *web* server: server na kojemu se nalaze *web* stranice .
[24] FTP server: server koji omogućuje spremanje i dohvaćanje podataka korištenjem FTP protokola
[25] Najpoznatija i najkorištenija FTP platforma. Sastoji se od *FilleZilla* servera i *FileZilla* klijenta
[26] *Apache*: najpoznatiji i najkorišteniji *web* server na internetu



Slika 16 Osnovna shema laboratorijskog okruženja

6.1.4 Konfiguracijsko Sučelje *Palo Alto* PA-500 vatrozida

Za testiranje funkcionalnosti vatrozida priključena su tri računala na vatrozid i konfigurirane su im mrežne postavke prikazane slikom 17.



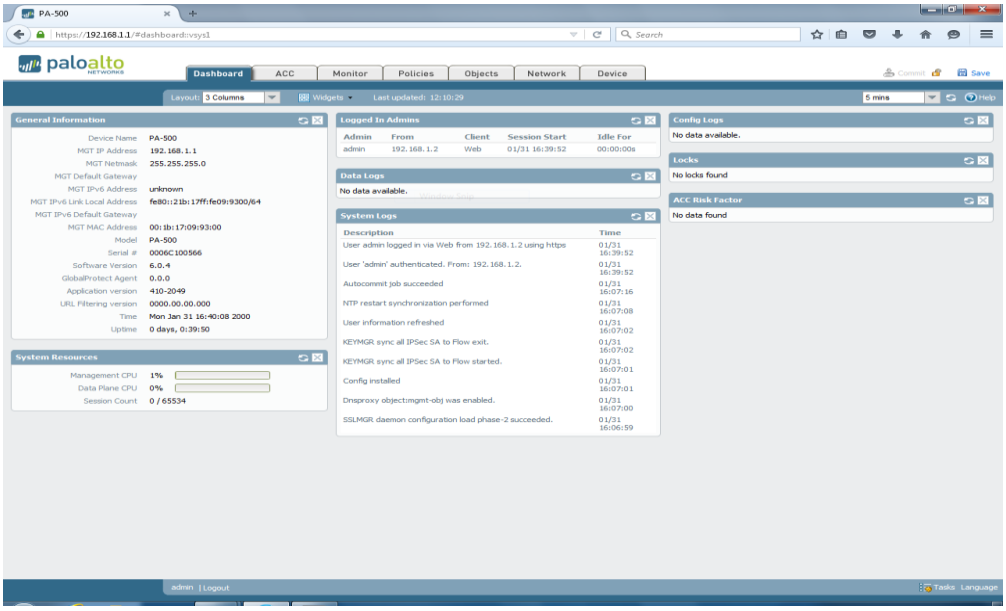
Slika 17 Shema labosa s navedenim IP postavkama

Nakon spajanja računala na vatrozid i njegovog pokretanja pristupa se konfiguraciji vatrozida. Pristup i konfiguracija vatrozida mogu se izvršavati uz pomoć grafičkog sučelja i uz pomoć komandne linije. Konfiguracija pomoću grafičkog sučelja ostvaruje se tako da se u *web* preglednik unosi IP adresa *management* porta koja odgovara adresi 192.168.1.1. Uvjet za konfiguraciju je da je računalo sa kojega se konfigurira vatrozid priključeno na *management* port vatrozida. Nakon pristupanja adresi pojaviti će se stranica za prijavu na vatrozid. Prijavu na vatrozid moguće je ostvariti i konzolnim putem ali taj način nije korišten i opisan u ovome radu.

Uspješnom prijavom otvara se PAN-OS sučelje za konfiguraciju vatrozida.

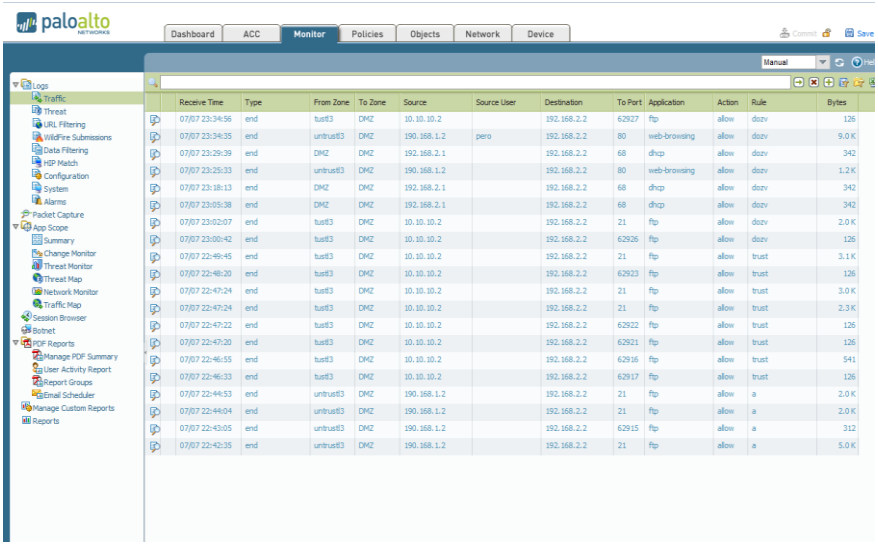
Glavna traka izbornika se nalazi na vrhu i u njoj se nalaze sljedeće opcije:

- *Dashboard*: početni prikaz kada se prijavi u vatrozid. Služi za nadzor i prikaz osnovnih funkcionalnosti uređaja. Izgled *dashboard*-a prikazan je slikom 19.
- ACC(*Application Command Center*): sadrži interaktivni grafički pregled korisnika, aplikacija, prijetnji i URL-ova.



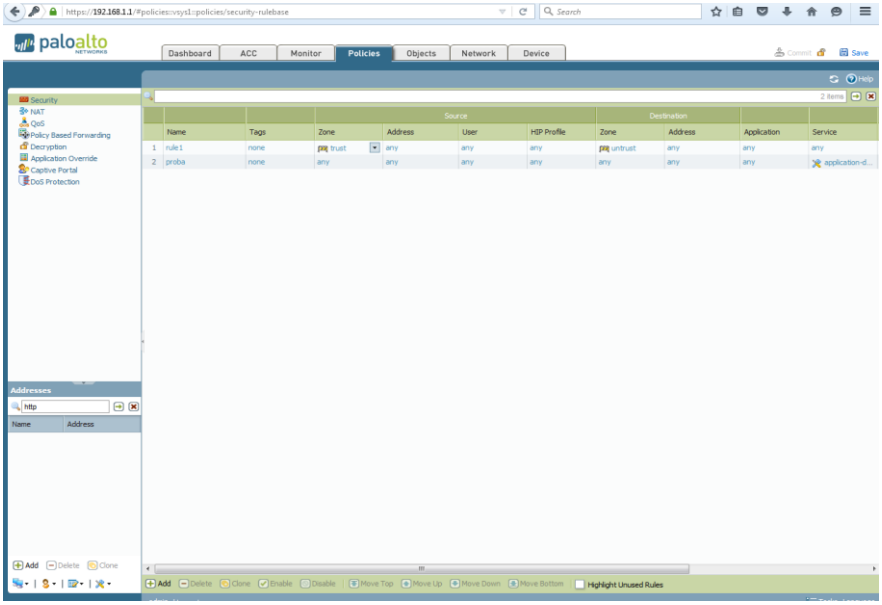
Slika 18 *Palo Alto* početni zaslon

- *Monitor*: sadrži log datoteke koje prikupljaju sve radnje vatrozida. Služi za nadzor rada vatrozida i izradu izvješća.



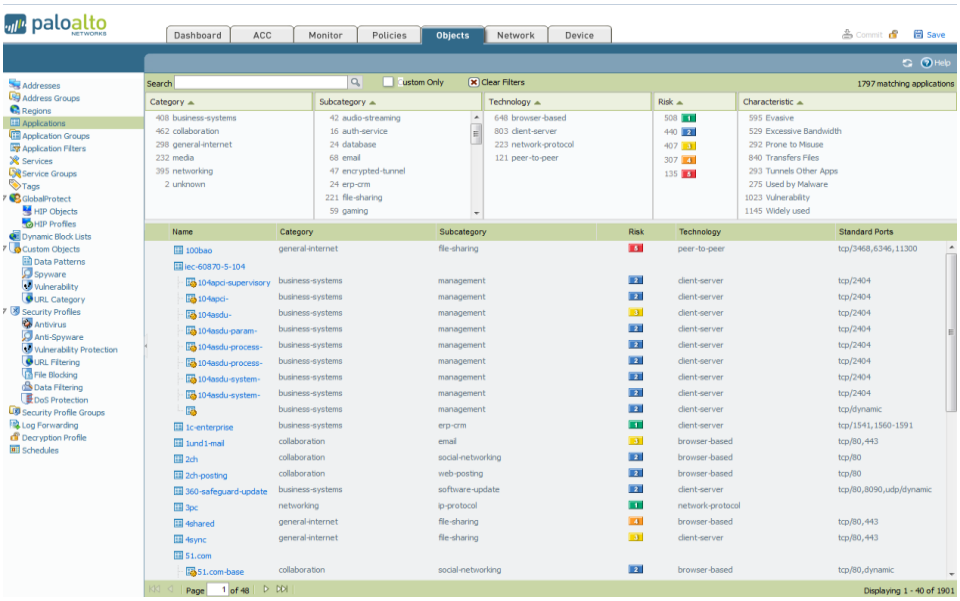
Slika 19 *Palo Alto Monitor* kategorija

- *Policies*: sadrži sve konfigurirane sigurnosne politike. Služi za kreiranje, uređivanje, brisanje i primjenjivanje svih politika vezanih uz aplikacije, korisnike i sadržaj.



Slika *20 Palo Alto* Policies kategorija

- *Objects*: služi za pregled kreiranih sigurnosnih objekata kao i za kreiranje vlastitih sigurnosnih objekata.

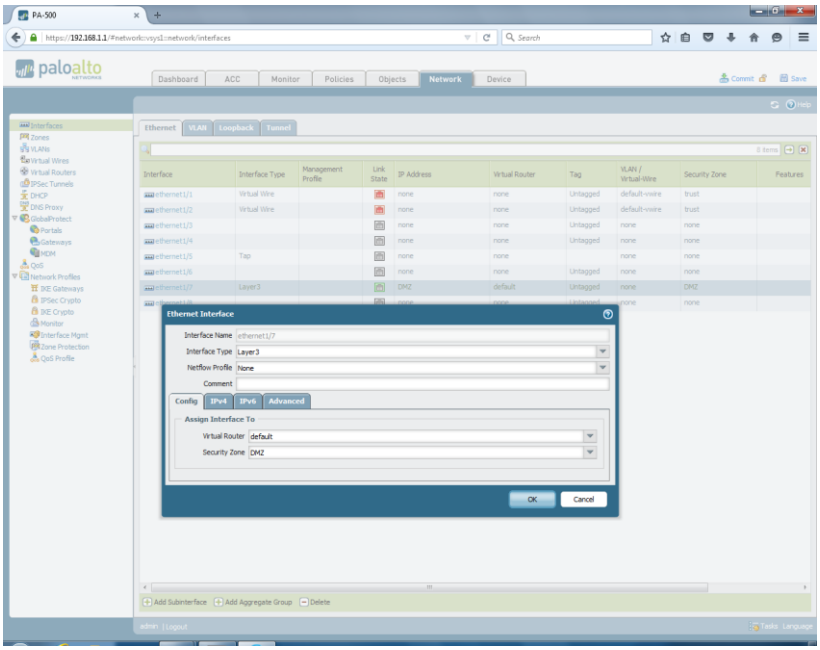


Slika 21 *Objects* kategorija

- *Network*: služi za pregled i konfiguraciju svih mrežnih postavki i mogućnosti uređaja.
- *Device*: služi za konfiguraciju postavki samog uređaja kao npr. naziv uređaja ili IP adresa *Managment* sučelja.

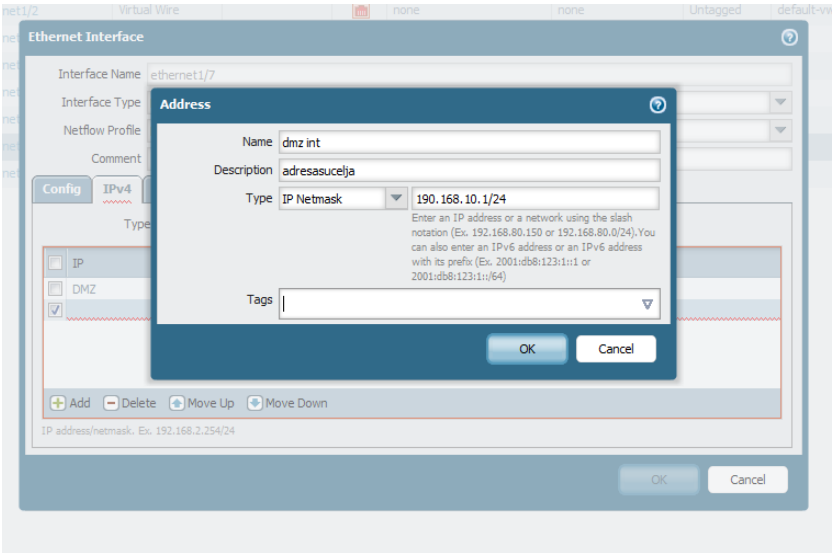
6.1.5 Konfiguracija sučelja i mrežnih postavki

Nakon pokretanja vatrozida potrebno je konfigurirati adrese sučelja na koja su priključena računala. Osnovna konfiguracija sučelja prikazana je slikom 25.



Slika 22 Osnovna konfiguracija sučelja

Nakon osnovne konfiguracije potrebno je pridodati sučelju IP adresu ako se radi o *Layer* 3 sučelju ili VLAN oznaku ako se radi o *Layer* 2 sučelju. Dodavanje statičke IP adrese na sučelje prikazana je slikom 26.

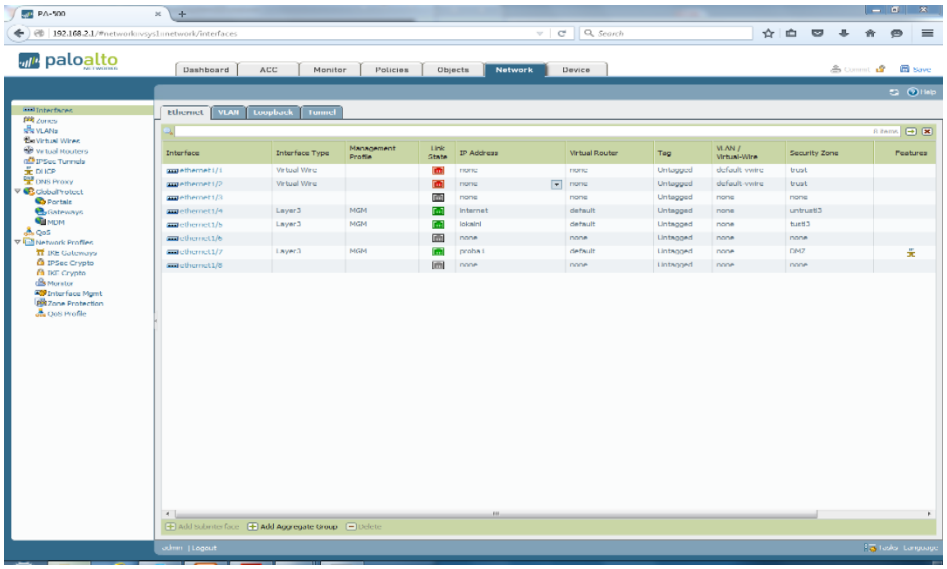


Slika 23 Konfiguracija statičke IP adrese sučelja

Za potrebe izrade rada konfigurirana su 3 sučelja. Dodijeljena su im imena Internet, lokalni i proba1 i postavljene su im sljedeće IP adrese:

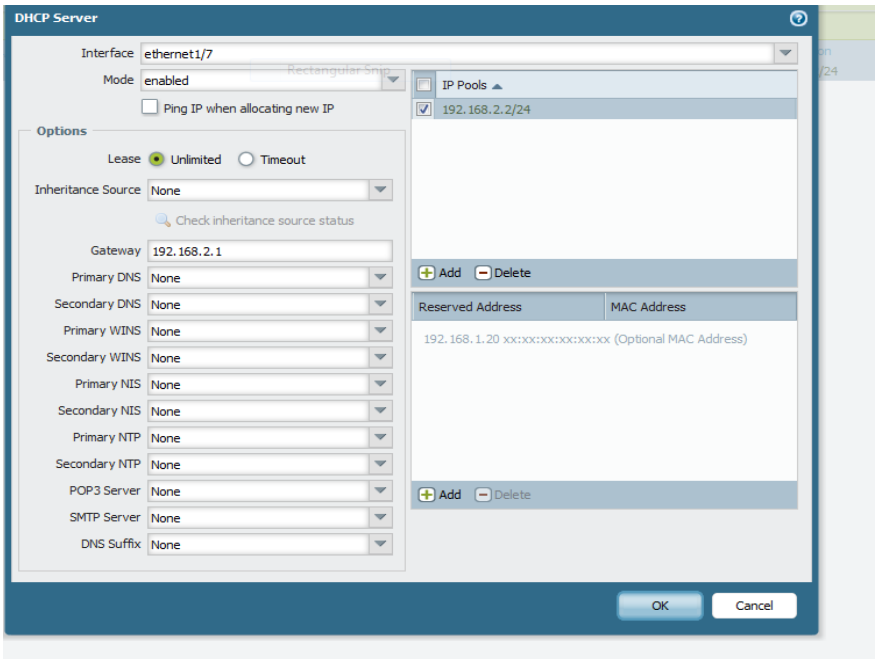
- Internet sučelje: 190.168.1.1
- Lokalni: 192.168.2.1
- Proba1:10.10.10.1

Konfigurirana sučelja na vatrozidu prikazana su slikom 2.



Slika 24 Konfigurirana sučelja na vatrozidu

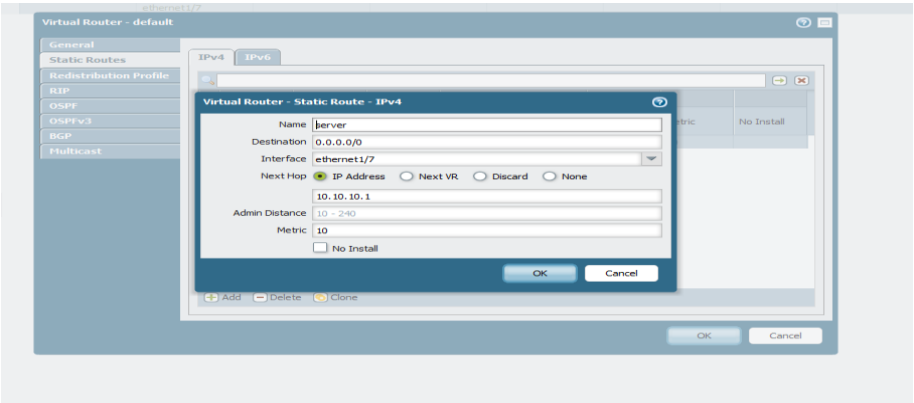
Unutar laboratorija za potrebe prikaza mrežnih mogućnosti vatrozida konfigurirani su DHCP server i virtualni usmjernik. DHCP server služi za automatsko dodjeljivanje IP adresa i ostalih mrežnih postavki unutar određene mreže. Konfiguracija DHCP servera prikazana je slikom 28.



Slika 25 Konfiguracija DHCP servera

Na *Palo Alto* PA-500 vatrozidu mogu se konfigurirati virtualni usmjernici. Vatrozid podržava konfiguraciju tri virtualna usmjernika, a od protokola za usmjeravanje podržane su statičke rute i OSPF, RIP i BGP protokoli za usmjeravanje.

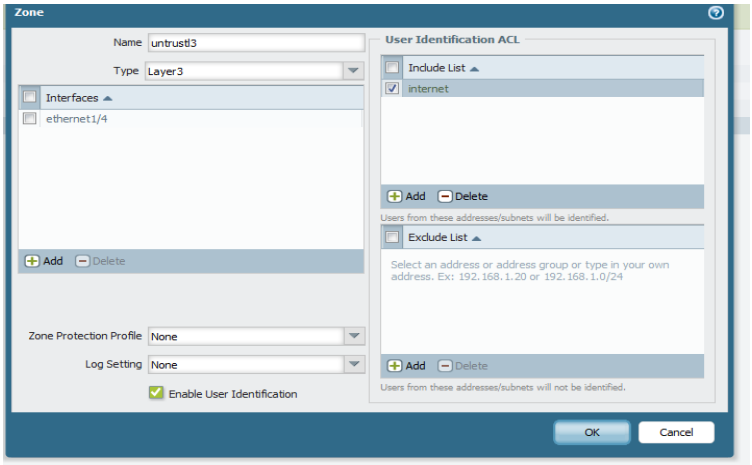
Slikom 30. prikazan je postupak dodavanja nove statičke rute na virtualnom usmjerniku.



Slika 26 Dodavanje nove statičke rute

6.1.6 Konfiguracija zona i osnovnih politika

Za definiranje logičkih cjelina *Palo Alto* koristi sigurnosne zone. Sigurnosna zona predstavlja logičku izoliranu sigurnosnu cjelinu koja se nakon izrade pridodaje mrežnim sučeljima. Prilikom izrade nove zone konfiguriraju se naziv zone, vrsta zone i sučelja koja pokriva kreirana zona. Slikom 31 prikazan je postupak dodavanja zona.



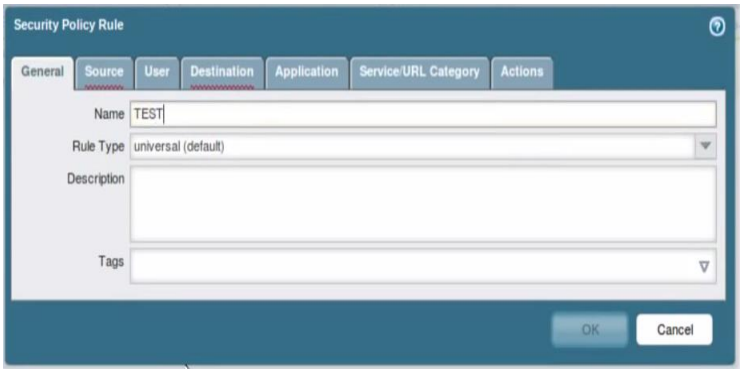
Slika 27 Dodavanje zone

Za potrebe izrade rada kreirane se 3 zone: DMZ, Trustl3, Untrustl3. Kreirane zone prikazane su slikom 32.

Slika 28 Kreirane zone

Nakon kreiranja zona mogu se kreirati sigurnosne politike. Svaka politika može dopuštati ili zabranjivati promet koji odgovara određenim uvjetima (aplikacija, korisnik itd.). Slikom 33 prikazana je izrada sigurnosne politike. Prilikom izrade politike konfiguriraju naziv i vrsta politike (*Rule Type*). Vrste politike mogu biti:

- *Universal*: standardna postavljena vrsta, kreirane sigurnosne politike primjenjuju se na sav poslani promet između definiranih zona kao i na promet koji se šalje unutar definiranih zona.
- *Intrazone*: sigurnosne politike primjenjuju se na sav promet koji se šalje unutar određene zone.
- *Interzone*: sigurnosne politike primjenjuju se na sav promet koji se šalje između zona ali se ne primjenjuju na promet unutar zona.

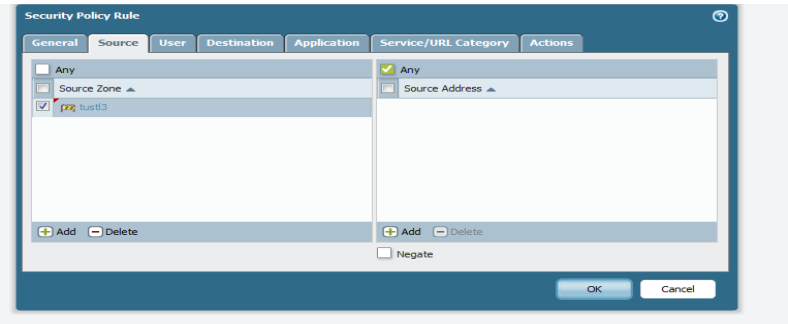


Slika 29 Kreiranje sigurnosne politike

Nakon konfiguriranja osnovnih postavki zone određuju se

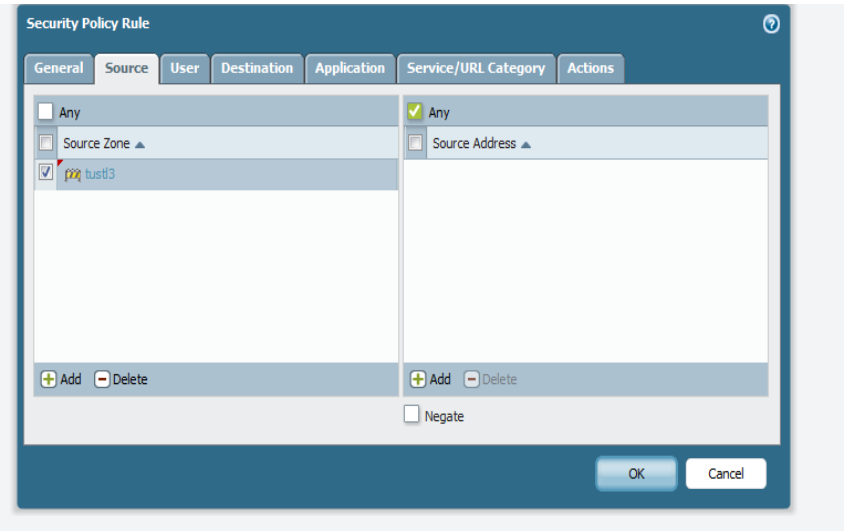
- izvorišne zone tj. zone iz kojih se upućuje promet koji se kontrolira (*Source* kartica)
- odredišne zone tj. zone na koje se upućuje promet (*Destination* kartica)
- korisnici za koje se sigurnosna politika odnosi (*User* kartica)
- aplikacije za koje se sigurnosna politika odnosi (*Application* kartica)
- servisi i skupine web stranica na koje se politika odnosi (*Service/URL Category* kartica)
- akcije koje će vatrozid raditi tj. dali će dopuštati ili odbijati promet koji zadovolji definirane uvjete (*Actions* kartica)

Slika 30 prikazana je konfiguracija izvorišnih zona na koje se politika primjenjuje.



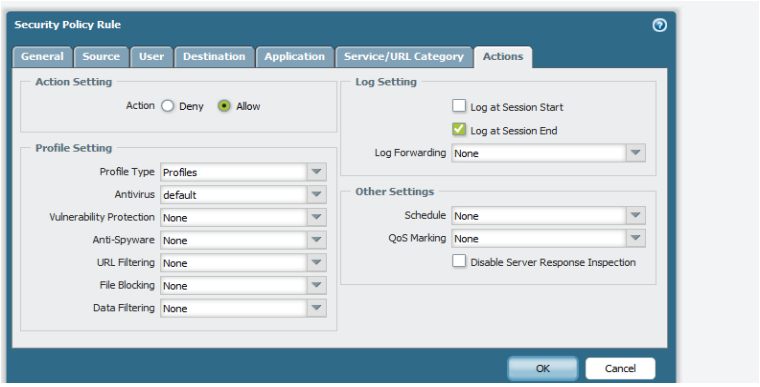
Slika 30 Konfiguracija izvorišnih zona

Slikom 31 prikazana je konfiguracija odredišnih zona.



Slika 31 Konfiguracija odredišnih zona

Slikom 32 prikazana je konfiguracija akcija koje se odnose na definirane parametre.



Slika 32 Konfiguracija akcija

Za potrebe izrade rada kreirane su sljedeće sigurnosne politike:

- dozvoljen sav promet koji se šalje iz zone trustl3 prema untrustl3 i DMZ zoni.
- dozvoljen sav promet koji se šalje iz zone untrustl3 prema DMZ zoni.
- zabranjen sav promet koji se šalje iz zone untrustl3 prema trustl3 zoni.

Nakon kreiranja politika provodi se testiranje kreiranih politika. Testiranje se provodi na način da se upućuje *ping*[27] iz računala koja se nalaze u jednoj zoni prema računalima koja se nalaze u drugim zonama.

Iz slike 33 može se zaključiti da sigurnosna politika koja kontrolira sav promet koji se upućuje između zona trustl3 i zona untrustl3 i DMZ uspješno konfigurirana. Može se primijetiti da je promet koji se upućuje iz zone DMZ prema zonama trustl3 i untrustl3 bio dopušten.

[27]*Ping*- Administrativni alat koji se koristi za provjeru dostupnosti *hostova* u računalnim mrežama koje se temelje na IP protokolu.

```
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\0246033286>ping 190.168.1.2

Pinging 190.168.1.2 with 32 bytes of data:
Reply from 190.168.1.2: bytes=32 time=1ms TTL=127
Reply from 190.168.1.2: bytes=32 time<1ms TTL=127
Reply from 190.168.1.2: bytes=32 time<1ms TTL=127
Reply from 190.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 190.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Slika 33 Testiranje politike prijenosa prometa između zone trustl3i ostalih zona

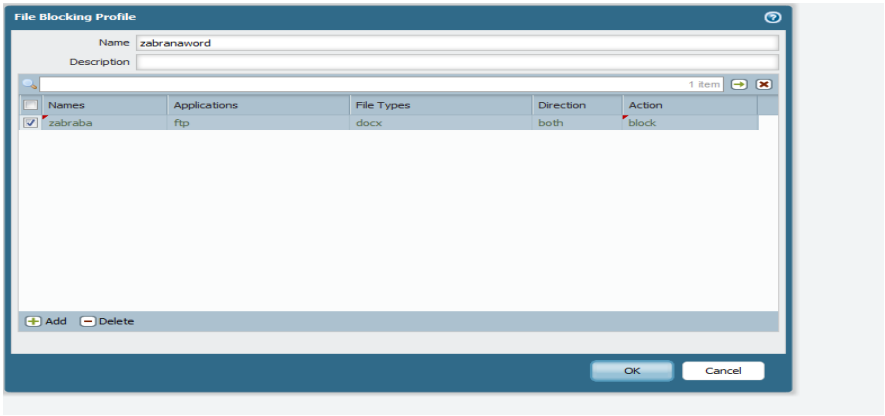
Iz slike 34 može se zaključiti da sigurnosna politika koja kontrolira sav promet koji se upućuje između zona untrustl3 i zona DMZ i trustl3 bila uspješno konfigurirana. Može se primijetiti da je promet koji se upućuje iz zone untrustl3 prema zoni DMZ dopušten, a promet koji se upućuje iz zone untrustl3 prema zoni trustl3 nije bio dopušten tj. vatrozid je blokirao taj promet.

```
Ping statistics for 192.168.2.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\0246033286>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.10.10.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Slika 34 Testiranje politike prijenosa prometa između zone untrustl3 i ostalih zona

6.1.7 Blokiranje sadržaja

Palo Alto vatrozidi imaju mogućnost blokiranja različitih vrsta sadržaja. Moguće je blokirati određenu vrstu datoteka za određenu aplikaciju. Politika za blokiranje sadržaja kreira se na način da se prvo kreira sigurnosni profil za blokiranje sadržaja. Unutar profila dodaju se objekti. Za svaki objekt konfigurira se za koju će aplikaciju blokirati koju vrstu sadržaja. Slikom 35 prikazana je konfiguracija profila koji će blokirati prijenos svih dokumenata sa ekstenzijom *.docx*[28] kada se prenose putem FTP aplikacija[29]. Kreirani profil koristiti će se za potrebe testiranja mogućnosti za potrebe izrade diplomskog rada.



Slika 35 Sigurnosni profil za blokiranje sadržaja

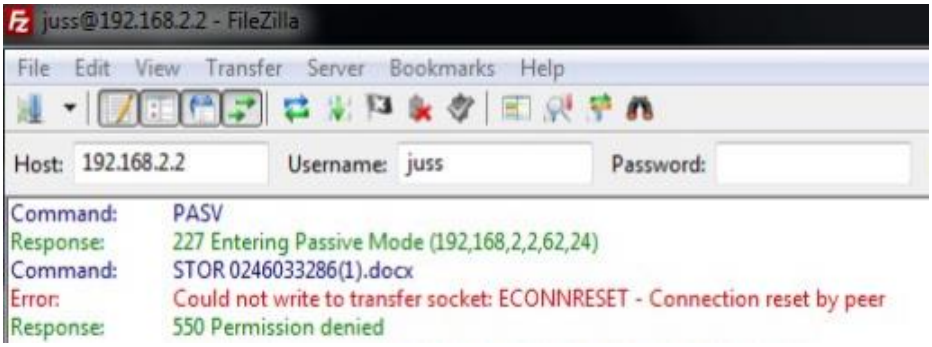
Kreirani sigurnosnog profila može se primjenjivati na više različitih sigurnosnih politika. Profil se primjenjuje na način da se unutar sigurnosne politike unutar kartice *actions*, unutar *file blocking* opcije izabere željeni profil.

Slikom 36 može se vidjeti da se dokument sa ekstenzijom *docx*. ne može prenijeti putem FTP protokola. Iz slike 36 može se zaključiti da se sigurnosna politika kreirana za potrebe izrade diplomskog rada uspješno primijenjena.

---

[28] *.docx* predstavlja format za spremanje tekstualnih dokumenata

[29] FTP aplikacije predstavlja automatski kreirani sigurnosni objekt unutar vatrozida koji se odnosi na sve aplikacije koje prenose podatke kroz mrežu putem FTP protokola



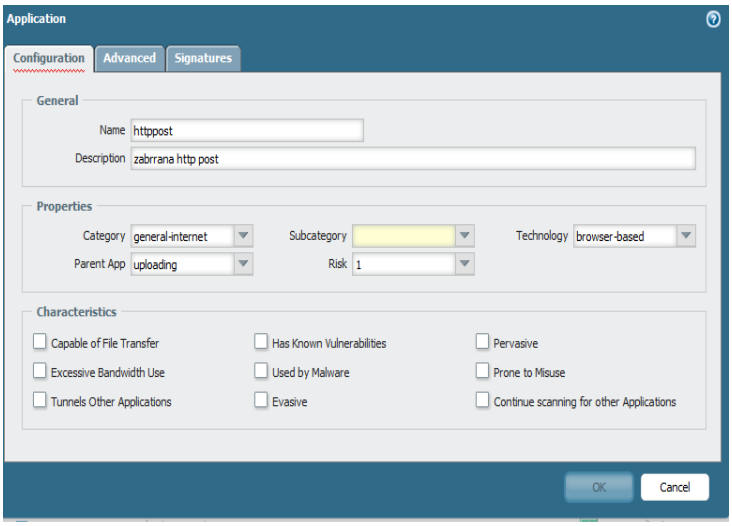
Slika 36 Blokiranje docx dokumenta

6.1.8 Kreiranje aplikacijskog potpisa

Palo Alto vatrozidi posjeduju mogućnost kreiranja aplikacijskih potpisa. Aplikacijski potpisi predstavljaju definirani obrazac ponašanja određene aplikacije te se koriste kada se želi dopustiti neka aplikacija ali se želi blokirati određena funkcionalnosti ili opcija te aplikacije. Kreiranjem i primjenom aplikacijskih potpisa postiže se veća granularnost i kontrola nad aplikacijama.

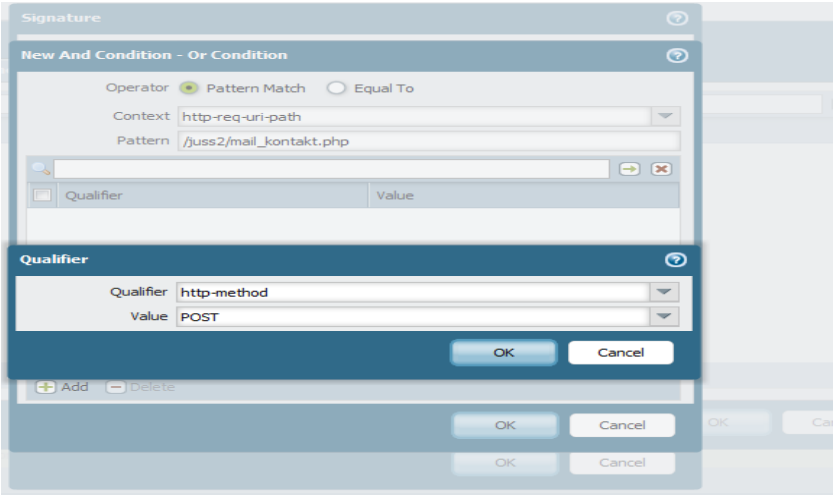
Prvi korak prije kreiranja aplikacijskog potpisa predstavlja analiza rada aplikacije za koju se želi napraviti potpis. Analiza se može raditi na više načina, kao npr. primjenom programskog alata *Wireshark* koji služi za snimanje i analizu mrežnog prometa.

Nakon analize prometa kreira se aplikacijski potpis. Za potrebe izrade diplomskog rada kreiran je aplikacijski potpis koji će blokirati *Http Post* metodu slanja podataka. Konfiguracija aplikacije na koju će se odnositi potpis prikazana je slikom 42.



Slika 37 Definiranje aplikacije

Slikom 43 prikazani su detalji konfiguracije potpisa koji blokira *Http post* metodu.

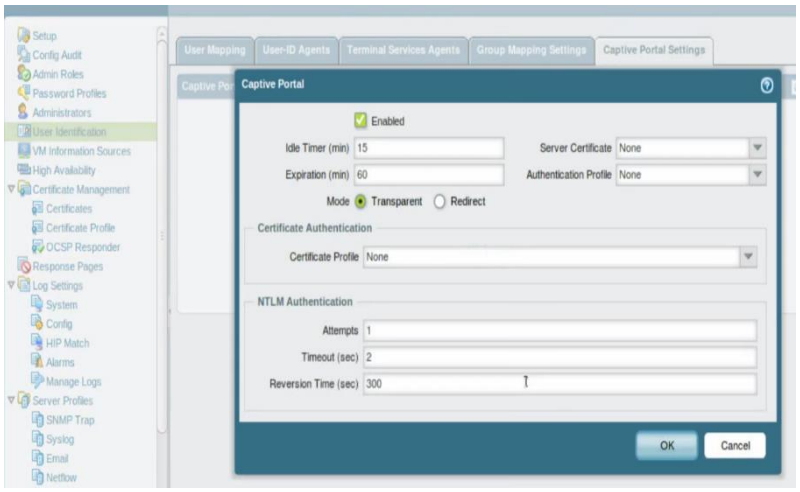


Slika 38 Aplikacijski potpis

6.1.9 Identifikacija korisnika

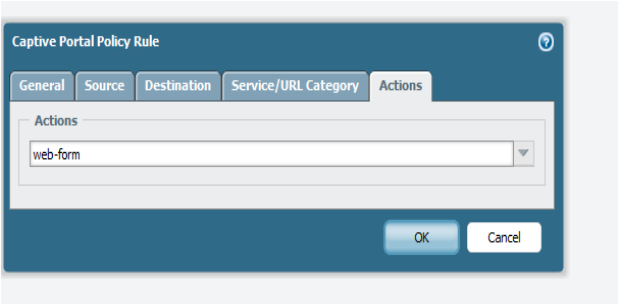
Palo Alto vatrozidi podržavaju brojne načine identifikacije korisnika. Najkorišteniji način u praksi je integracija s određenim imeničkim servisom. Iz razloga

da unutar laboratorija u kojemu se radilo testiranje za potrebe izrade rada ne postoji instalirani i konfigurirani imenički servis opisati će se način identifikacije korisnika pomoću *captive portala*. *Palo Alto* vatrozidi imaju internu bazu korisnika koji se mogu autentificirati za pristup resursima u mreži. Slikom 44 prikazano je omogućavanje *captive portala* za autentifikaciju korisnika.



Slika 39 omogućavanje *captive poratala* za autentifikaciju korisnika

Nakon omogućavanja *captive portala* kreira se sigurnosna politika koja će obavljati identifikaciju korisnika. Slikom 45 prikazana je konfiguracija *captive portala*. U ovome primjeru odabran je način autentifikacije pomoću forme.



Slika 40 Odabir načina autentifikacije

6.1.10 Ostale mogućnosti *Palo Alto* PA-500 vatrozida

Palo Alto PA-500 posjeduje brojne mogućnost čija konfiguracija nije prikazana ovim radom. Jedan od najmoćnijih alata *Palo Alto* vatrozida jesu njegove značajke za sprječavanje prijetnji (*Threat Prevention Features*). Značajke za sprječavanje prijetnji sastoje se od:

- *antivirus, anti-spyware* i alata za zaštitu ranjivosti sustava (*vulnerability protection*),
- URL filtra.

Konfiguraciju značajki za sprječavanje prijetnji nije se moglo opisati iz razloga što je za omogućavanje ovih značajki potrebna dodatna licenca. Uređaj na kojemu se provodilo testiranje nije posjedovao licencu.

Za koristiti URL filtar nije potrebna licenca, ali ako se želi koristiti *Palo Alto* baza stranica potrebno je kupiti pretplatu na nju. Od ostalih funkcionalnosti valja istaknuti:

- *data leak prevention*: mogućnost nadzora nad različitim *mail* i *web* protokolima. Moguće je pretraživati i filtrirati promet po određenim definiranim stringovima.
- dekripcija prometa kriptiranog SSL/TLS i SSH enkripcijom.
- omogućavanje VPN konekcije korištenjem *IPsec* i SSL VPN mehanizma.
- DoS protekcija: vatrozid ima mogućnost otkrivanja i sprječavanja DoS napada prema različitim kriterijima.
- konfiguracija visoke dostupnosti povezivanjem 2 ili više.
- *Wildfire*: sustav analize i obrade prijetnji u oblaku.

6.2. Prikaz mogućnosti i testiranje *Fortigate* 60D vatrozida nove generacije

U ovome poglavlju biti će prikazane osnovne funkcionalnosti *Fortigate* 60D vatrozida. Opisati će se i prikazati konfiguracija i testiranje nekih funkcionalnosti *Fortigate* 60D vatrozida unutar laboratorijskog okruženja.

6.2.1 *Fortinet* servisi

Fortinet predstavlja jednog od glavnih proizvođača i pružatelja rješenja za mrežnu sigurnost. *Fortinet* je razvio i patentirao platformu *Fortigate* za pružanje sigurnosne zaštite na svim razinama. *Fortigate* sustavi mogu se koristiti u svim okolinama od podatkovnih centara do malih ureda. *Fortigate* platformu pokreče *FortiOS* operacijski sustav koji u sebi sadrži brojne sigurnosne tehnologije. Način rada sigurnosnih tehnologija neće biti opisan u ovome radu iz razloga što sama kompanija ne otkriva dokumentaciju koja bi opisivala način rada sigurnosnih tehnologija. Uz korištenje hardvera i operacijskog sustava važan segment *Fortinet* proizvoda predstavljaju *Fortiguard* servisi. *Fortiguard* servisi predstavljaju globalnu distribuiranu mrežu koja svakodnevno pruža ažuriranja za *Fortinet* proizvode. Iza mreže stoji skupina sigurnosnih stručnjaka koja svakodnevno prati promjene i kreira ažuriranja za *Fortinet* proizvode [23].

Najznačajniji *Fortiguard* servisi su:

- *Fortiguard Antivirus* servis: pruža zaštitu od virusa, *spyware*-a i ostalih prijetnji. Koristi napredne mehanizme i alate za otkrivanje i sprječavanje napada.
- *Fortiguard Application control*: omogućuje vidljivost i kontrolu velikog broja aplikacija. Uz pomoć ovoga servisa mogu se lako kreirati sigurnosne politike vezane uz aplikacije ili skupine aplikacija.

- *Web Application*: ovaj servis koristi veliku bazu poznatih ranjivosti, uzoraka podataka i specijalnih heurističkih algoritama za osiguravanje sigurnosti *web* aplikacija.
- *Web Filtering*: ovaj servis sadrži bazu podataka stranica. Uz pomoć servisa osigurava se zaštita sustava i omogućuje blokiranje pristupa na određene *web* stranice ili skupine stranica.
- *Antispam*: ovaj servis omogućava zaštitu mail sustava na način da omogućava otkrivanje i blokiranje *spam* poruka.

6.2.2 *Fortigate* D60 vatrozid nove generacije

Fortigate D60 predstavlja vatrozid nove generacije koji je namijenjen malim tvrtkama i manjim mrežama. Uređaj ima ugrađen FortiOS operacijski sustav i podržava sve *Fortiguard* servise.

Slika 41 *Fortigate* D60 vatrozid [24]

Prema [24 uređaj posjeduje sljedeće specifikacije:

- propusna moć: 250Mbps
- propusna moć komponente za prevenciju prijetnji: 340Mbps
- propusna moć komponenta za kontrolu aplikacija: 550Mbps
- Maksimalni broj SSL-VPN korisnika: 100
- maksimalni broj novih sesija po sekundi: 30000
- maksimalni broj sesija: 1.3 milijuna
- maksimalni broj sigurnosni politika: 5000

- maksimalni broj virtualni usmjernika: 10

Uređaj posjeduje sljedeća sučelja:

- 7 RJ45 (1Gb) internih sučelja
- 2 RJ45(1Gb) WAN sučelja
- RJ45 (1Gb) DMZ sučelje
- RJ45 (1Gb) konzolni port za upravljanje uređajem
- RJ45 (1Gb) port za upravljanje uređajem
- USB sučelje za konfiguraciju i upravljanje uređajem
- 802.11 a/b/g/n/ac sučelje (samo FORTIWIFI 60E model)

Uređaj posjeduje sljedeće hardverske specifikacije:

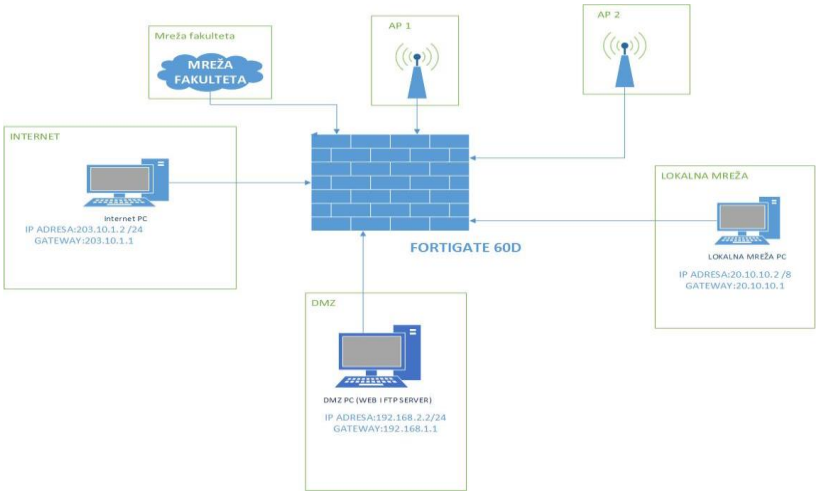
- kapacitet diska: 120GB
- Ulazni napon: 110-240V AC, 50-60Hz
- prosječna/maksimalna potrošnja električne energije: 11.7W/14W
- težina: 0.9 kg
- dimenzije: 1.5*8.5*6.3 inča

6.2.3 Opis testnog okruženja

Testiranje mogućnosti uređaja izvedeno je u laboratorijskom okruženju. Za testiranje su korištena tri računala s instaliranim *windows* 7 operacijskim sustavom i vatrozid nove generacije *Fortigate* D60. Korišteni vatrozid unutar testnog okruženja koristi se za potrebe fakulteta te je na njegovo WAN sučelje priključena mreža fakulteta. Također na vatrozidu su definirane i priključene dvije pristupne točke (*acess point*). Na vatrozid su dodatno priključena tri računala na interna sučelja i definirane tri različite mreže. Računala koja su spojena na vatrozid simuliraju:

- računalo koje se nalazi u lokalnoj mreži određene kompanije.
- računalo koje pristupa resursima mreže s interneta.
- server koji se nalazi u DMZ-u.

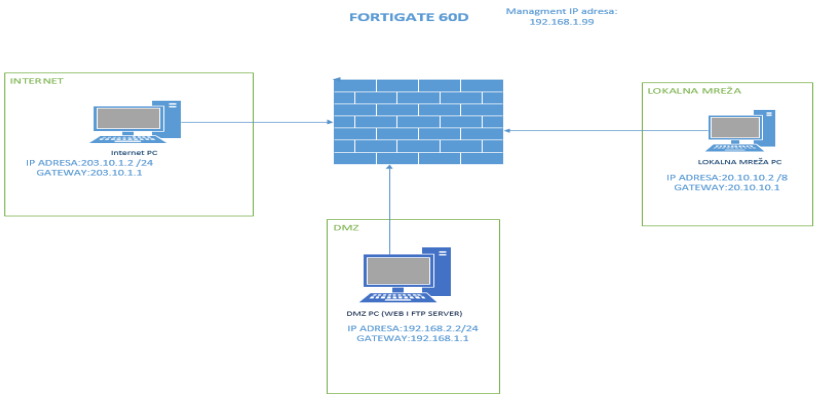
U laboratorijskom okruženju korištenim za izradu diplomskog rada računalo u DMZ-u simulirati će *web* i FTP server koji bi se nalazio u demilitariziranoj zoni kompanije. *XAMPP* je podešen na računalu u DMZ-u na način da je na njemu pokrenut *FileZilla* i *Apache* servis. Unutar *apache*-a postavljen je juss2 folder koji će simulirati *web* stranicu kompanije.



Slika 42 Osnovna shema laboratorijskog okruženja

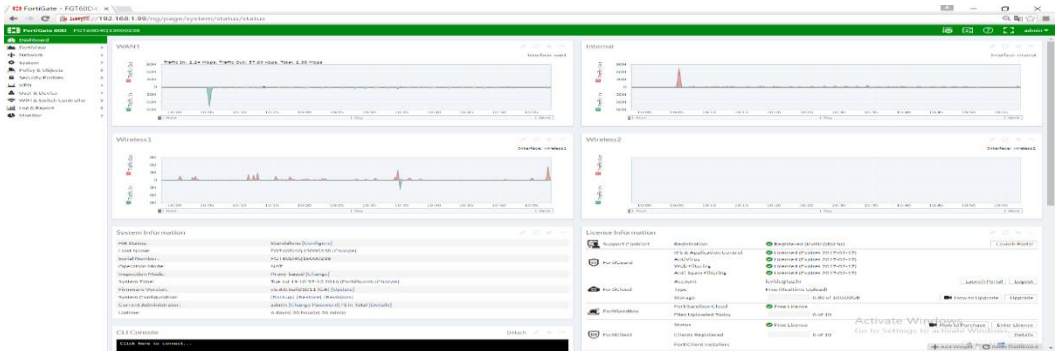
6.2.4 Konfiguracijsko sučelje *Fortigate* D60 vatrozida

Za testiranje funkcionalnosti vatrozida priključena su tri računala na vatrozid i konfigurirane su im mrežne postavke prikazane slikom 54.



Slika 43 Dodijeljene IP adrese računalima u mreži

Nakon spajanja računala na vatrozid pristupa se konfiguraciji vatrozida. Pristup i konfiguracija vatrozida mogu se izvršavati uz pomoć grafičkog sučelja, komandne linije i *FortiExplorer* programa. Konfiguracija pomoću grafičkog sučelja ostvaruje se tako da se u *web* preglednik unosi IP adresa management porta koja odgovara adresi 192.168.1.99. Uvjet za konfiguraciju je da je računalo sa kojega se konfigurira vatrozid priključeno na *managment* port vatrozida. Nakon pristupanja adresi pojaviti će se stranica za prijavu. Prijavu na vatrozid moguće je ostvariti i konzolnim putem ali taj način nije korišten i opisan u ovome radu. Nakon prijave na vatrozid moguća je konfiguracija vatrozida.



Slika 44 Početni prozor nakon prijave na vatrozid

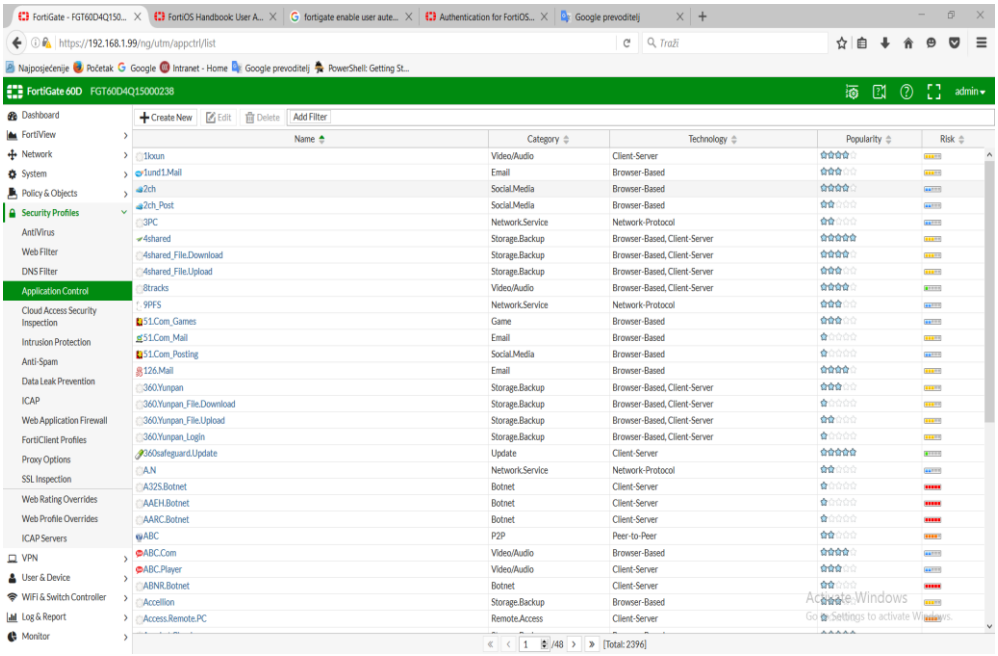
,

Uspješnom prijavom otvara se FortiOS sučelje za konfiguraciju vatrozida.

Glavna traka izbornika se nalazi na lijevoj stran i u njoj se nalaze sljedeće opcije:

- *Dashboard*: početni prikaz kada se prijavi u vatrozid. Služi za nadzor i prikaz osnovnih funkcionalnosti i licenci uređaja.
- *FortiVieW*: sučelje za grafički prikaz i analizu *log* datoteke kao i analizu svog prometa u mreži. Služi za nadzor rada vatrozida i izradu izvješća.
- *Network*: služi za pregled i konfiguraciju svih mrežnih postavki i mogućnosti uređaja.

- *System*: služi za konfiguraciju postavki uređaja.
- *Policy & Objects:* sadrži sve konfigurirane sigurnosne politike. Služi za kreiranje, uređivanje, brisanje i primjenjivanje svih politika vezanih uz aplikacije, korisnike i sadržaj.
- *Security Profiles:* sadrži funkcije za kreiranje, uređivanje i brisanje sigurnosnih profila.



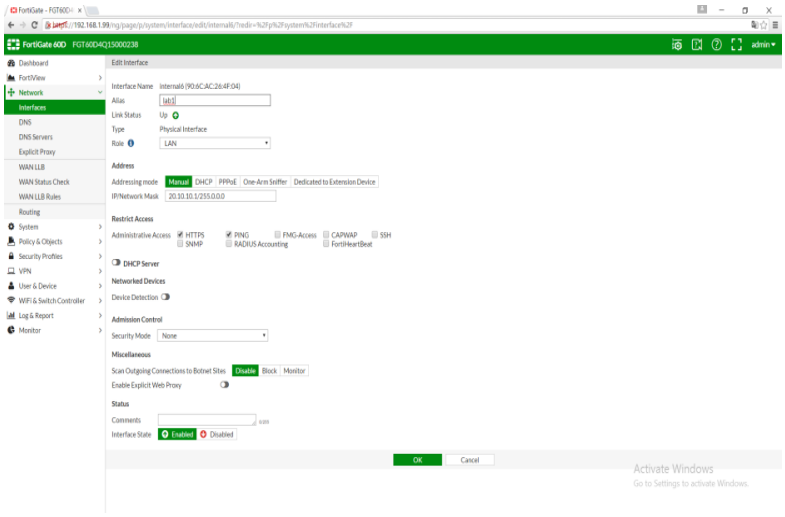
Slika 45 *Security Profiles*

- VPN: sadrži postavke za konfiguraciju postavki za omogućavanje spajanja korisnika korištenjem VPN tehnologije
- *User & Deviaces*: sadrži postavke za kreiranje korisnika i konfiguracije različitih načina autentifikacije (RADIUS, LADP itd)
- *Wifi & Switch* control: sadrži opcije za konfiguraciju pristupnih točaka
- *Log & Report*: sadrži opcije za konfiguraciju nadziranja tj. podešava se što će sve nadzirazi i kada.
- *Monitor*: opcija za nadzor I kontrolu nad svim senzorima uređaja.

6.2.5 Konfiguracija mrežnih sučelja i DHCP servera

Nakon priključivanja računala na sučelja potrebno je konfigurirati adrese sučelja na koja su priključena računala. Unutar konfiguracije sučelja određuju se vrsta, ime i IP adresa sučelja kao i mogućnost administrativnog pristupa sučelju. IP adresa unosi se u obliku IP adresa/*subnet* maska.

Slikom 46 prikazan je postupak kreiranja novog sučelja.



Slika 46 Dodavanje novog sučelja

Za potrebe izrade diplomsko rada konfigurirana su 3 sučelja, dodijeljena su im imena internetlab, labdmz i lab1loci. Na sučeljima su konfigurirane sljedeće IP adrese:

- internetlab sučelje: 203.10.1.1
- labdmz: 192.168.2.1
- lab1loc: 20.10.10.1

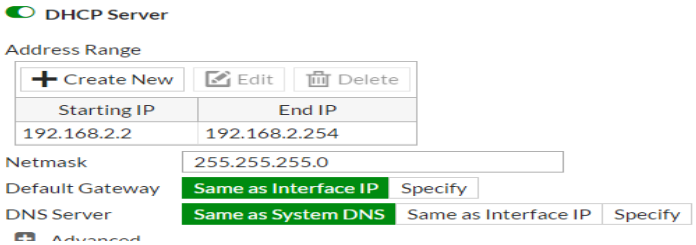
Konfigurirana sučelja na vatrozidu prikazana su slikom 47.[30]

[30] Slikom su prikazana samo sučelja koja su kreirana za potrebe testiranja vatrozida unutar laboratorijskog okruženja. Iz sigurnosnih razloga nisu prikazana sva konfigurirana sučelja na vatrozidu.

	internal4 (internetlab)		203.10.1.1 255.255.255.0	Physical		2
	internal5 (labdmz)		192.168.2.1 255.255.255.0	Physical	PING HTTPS SSH	3
	internal6 (lab1loc)		20.10.10.1 255.0.0.0	Physical	PING HTTPS	2

Slika 47 Konfigurirana sučelja na vatrozidu

Fortigate D60 posjeduje mogućnost konfiguracije DHCP servera na određenom sučelju. Slikom 48 prikazan je postupak konfiguracije DHCP servera.



Slika 48 Konfiguracija DHCP servera na sučelju

6.2.5 Konfiguracija sigurnosnih politika

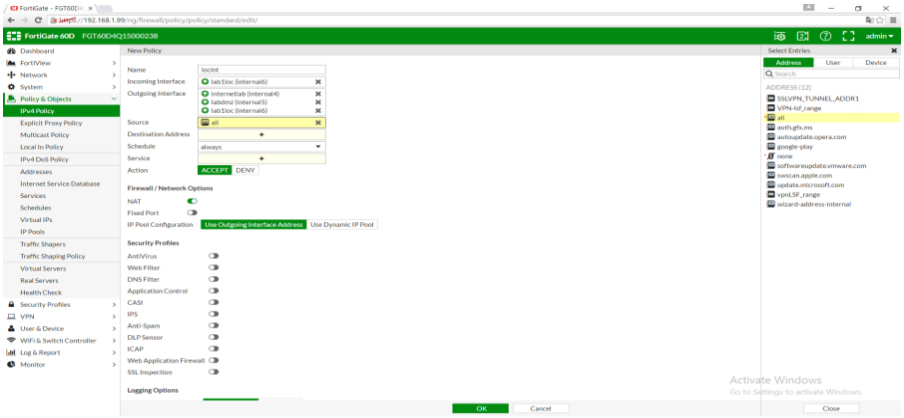
Fortigate vatrozid dozvoljava kreiranje različitih vrsta sigurnosnih politika. Kod *Fortigate* vatrozidi ne postoji opcija kreiranja sigurnosnih zona, nego se prilikom kreiranja sigurnosne politike sva izvorišna sučelja i sva odredišna sučelja smatraju sigurnosnom zonom za tu politiku. Unutar sigurnosne politike konfiguriraju se izvorišna sučelja, izvorišne adrese, odredišna sučelja, odredišne adrese i sigurnosni profili. Zatim se konfigurira akcija tj. dali se za paketi koji zadovolje uvjete politike prihvaćaju ili odbacuju.

Za potrebe testiranja kreirana su sljedeće sigurnosne politike:

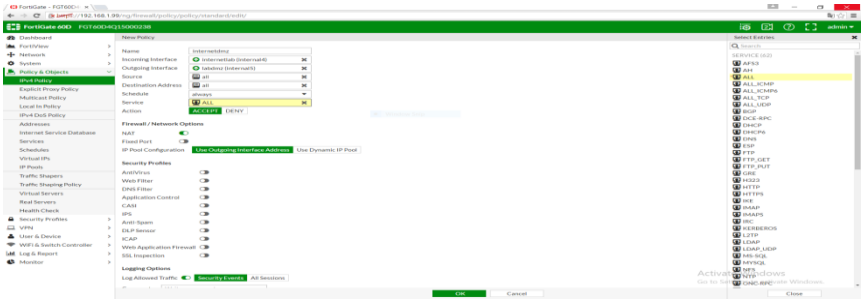
- dozvoljen sav promet koji se šalje iz zone lab1loc prema ostalim zonama.

- dozvoljen sav promet koji se šalje iz zone labdmz prema ostalim zonama.
- Dozvoljen sav promet koji se šalje iz zone internetlab prema labdmz zoni.
- Dozvoljen sav promet koji se šalje iz zone internetlab prema lab1loc zoni.

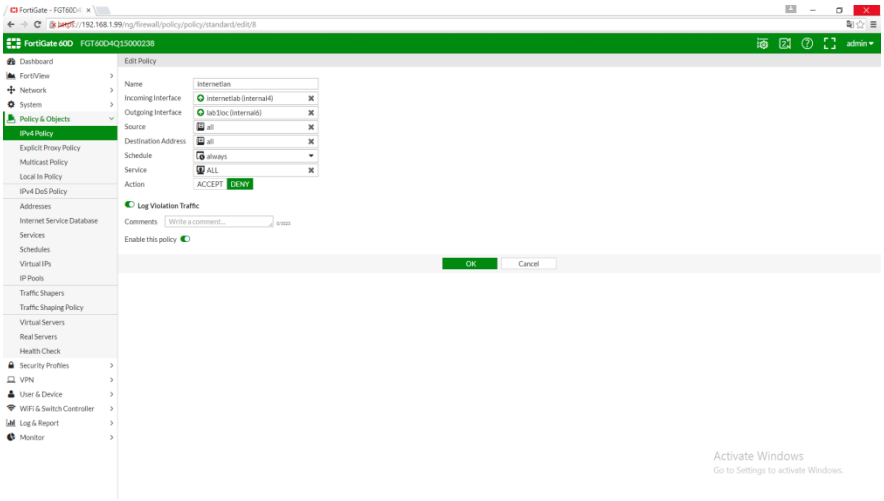
Slikama 49,50 i 51 prikazane su konfiguracije sigurnosnih politika.



Slika 49 Konfiguracija sigurnosne politike dozvole prometa iz zone lab1loc prema ostalim zonama



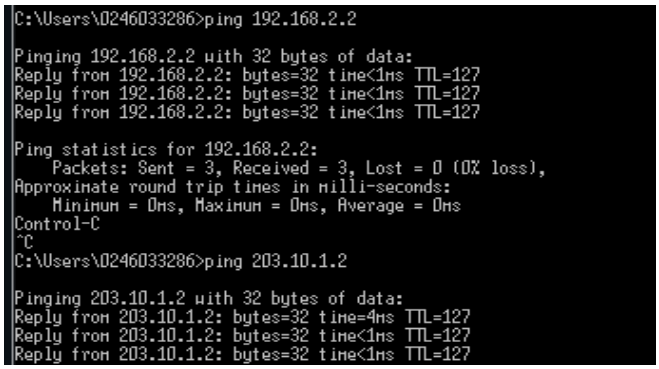
Slika 50 Konfiguracija sigurnosne politike dozvole prometa iz zone internetlab prema labdmz zoni



Slika 51 Konfiguracija sigurnosne politike zabrane prometa iz zone internetlab prema lab1loc zoni

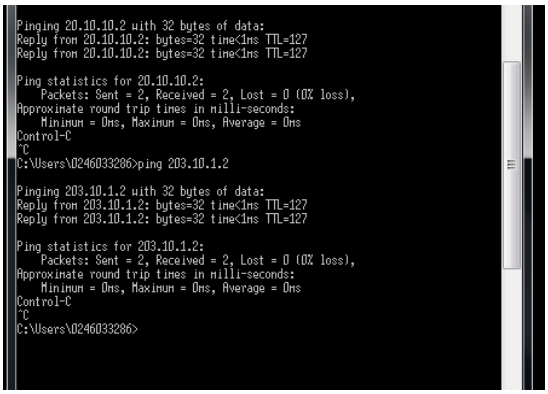
Nakon konfiguracije politika provodi se testiranje sigurnosnih politika. Testiranje se provodi na način da upućuje *ping* iz računala koja se nalaze u jednoj zoni prema računalima koja se nalaze u drugim zonama.

Iz slike 52 može se zaključiti da je sigurnosna politika koja kontrolira sav promet koji se upućuje između zona lab1loc i ostalih zona bila uspješna provedena.



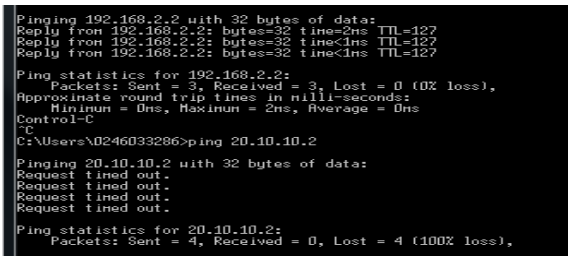
Slika 52 Kontrola sigurnosne politike

Iz slike 53 može se zaključiti da sigurnosna politika koja kontrolira sav promet koji se upućuje između zona labdmz i ostalih zona bila uspješna provedena.



Slika 53 Kontrola sigurnosne politike 2

Iz slike 54 može se zaključiti da sigurnosna politika koja kontrolira promet između internetlab i ostalih zona bila uspješna. Može se primijetiti da promet upućen iz zone internetlab i zone labdmz uspješno prolazi, a promet upućen iz zone internetlab prema lab1loc zoni ne prolazi.



Slika 54 Kontrola sigurnosne politike 3

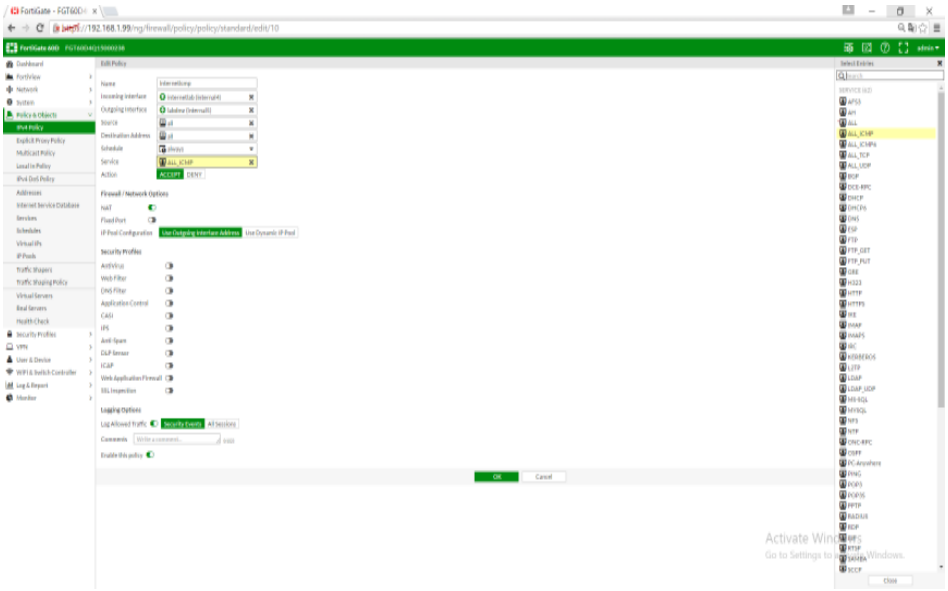
6.2.6 Konfiguracija blokiranja servisa

Fortigate vatrozidi posjeduju mogućnost blokiranja servisa. Mogu se definirati vlastiti servisi a postoje i predefinirane liste kreiranih servisa.

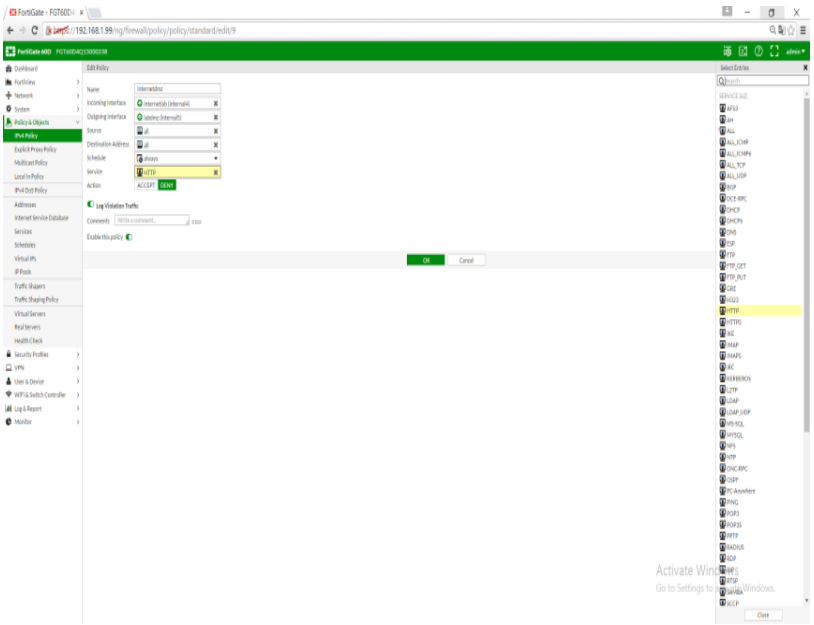
Unutar laboratorija kreirane su dvije sigurnosne politike koje:

- dopuštaju sav ICMP promet između internetlab i labdmz zona i
- blokiraju sve HTTP zahtjeve između internetlab i labdmz zona

Slikama 55 i 56 prikazana je konfiguracija sigurnosnih politika za blokiranje i dopuštanje servisa.

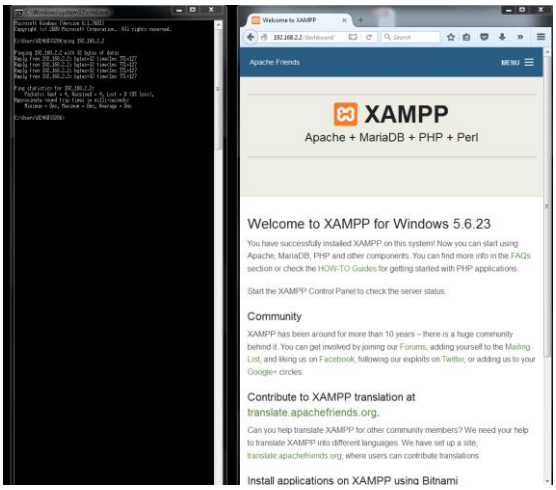


Slika 55 Sigurnosna politika za dopuštanje ICMP servisa



Slika 56 Sigurnosna politika za blokiranje HTTP servisa

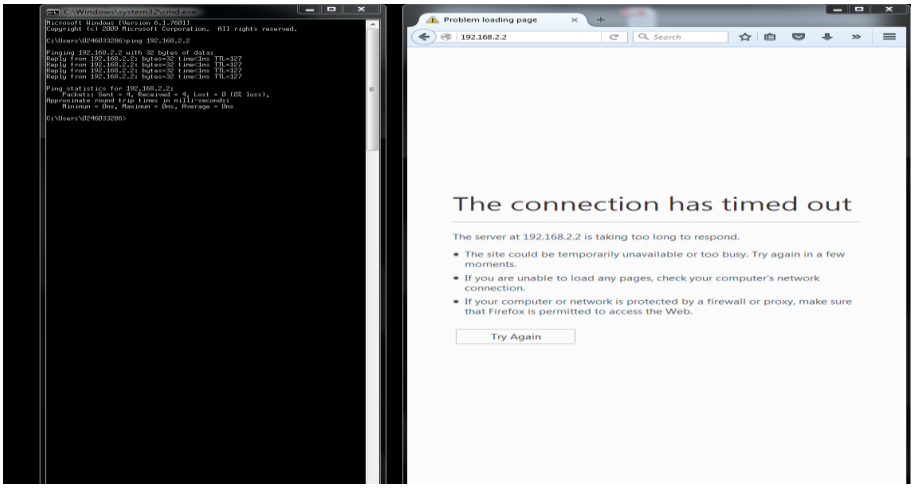
Nakon kreiranja sigurnosnih politika za blokiranje servisa provodi se testiranje politika. Slikom 57 prikazan je rad sustava prije primjene sigurnosni politika za blokiranje i dopuštane servisa.



Slika 57 Rad sustava prije primjene sigurnosnih politika

Slikom 58 prikazan je rad sustava nakon primjene sigurnosnih politika.

Iz slike 58 može se vidjeti da je pristup *web* serveru tj. upućivanje HTTP zahtjeva onemogućeno dok se ICMP komunikacija normalno odvija.

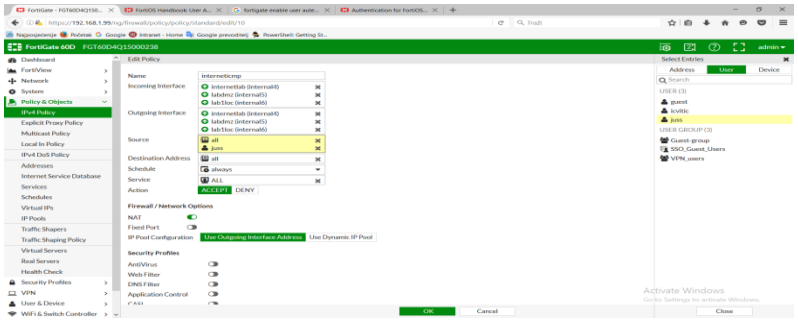


Slika 58 Rad sustava nakon primjena sigurnosnih politika

6.2.7 Identifikacija korisnika

Fortigate vatrozidi podržavaju brojne mehanizme identifikacije korisnika. Da bi se omogućila identifikacija korisnika potrebno je prilikom kreiranja sigurnosne politike navesti korisnike ili grupe korisnika za koje će se provoditi autentifikacija i identifikacija.

Slikom 59 prikazana je konfiguracija autentifikacije korisnika.



Slika 59 Konfiguracija identifikacije korisnika

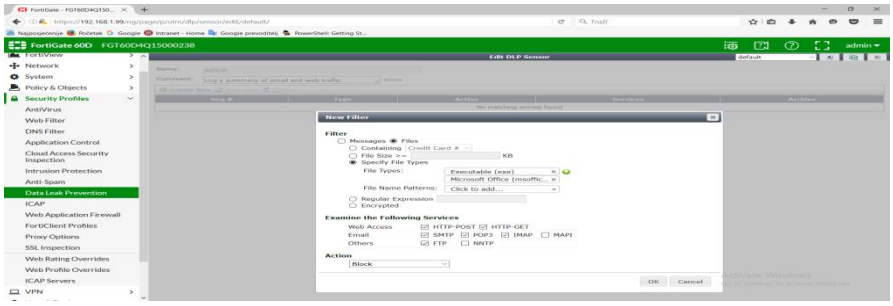
6.2.8 Konfiguracija ostalih opcija vatrozida

U ovome poglavlju prikazati će neke od mogućnosti *Fortigate* vatrozida i njihova konfiguracija. Iz razloga da je za prikaz mogućnosti vatrozida korišteno testno okruženje unutar kojeg računala priključena na vatrozid nemaju mogućnost izlaska na Internet, neke opcije nije moguće testirati već će se prikazati postupak konfiguracije bez testiranja.

6.2.8.1 Konfiguracija blokiranja datoteka

Blokiranje datoteka konfigurira se na način da se kreira novi filtar koji opisuje željene postavke za blokiranje. Također moguće je pretraživati i filtrirati poruke ukoliko sadrže u sebi osjetljive informacije poput brojeva kreditnih kartica.

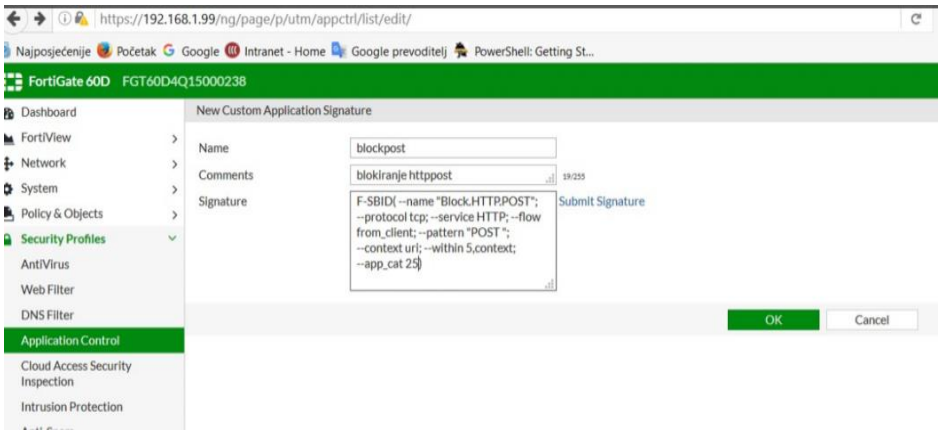
Slikom 60 prikazana je konfiguracija novog filtra za blokiranje sadržaja.



Slika 60 Konfiguracija filtra za blokiranje sadržaja

6.2.8.2 Konfiguracija aplikacijskog potpisa

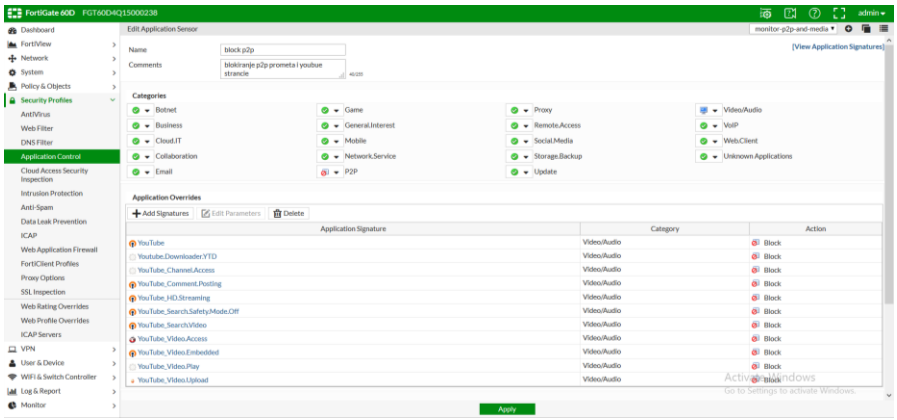
Unutar vatrozida postoji mogućnost za stvaranje vlastitog aplikacijskog potpisa. Aplikacijski potpisa stvara se na način da se potpis unosi u definiranom tekstualnom obliku gdje se navode opcije potpisa. Slikom 61 prikazana je konfiguracija aplikacijskog potpisa



Slika 61 Konfiguracija aplikacijskog potpisa

6.2.8.3 Konfiguracija blokiranja aplikacija

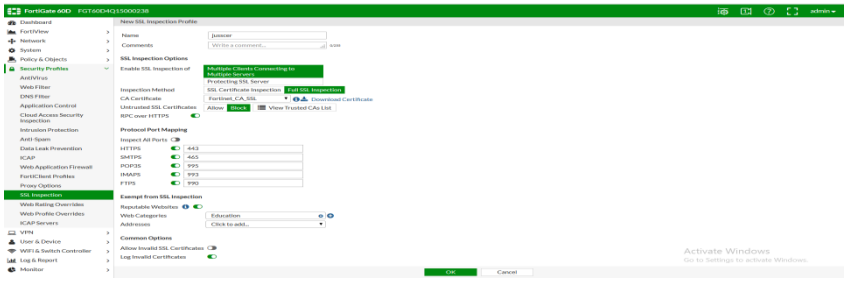
Fortigate vatrozid sadrži u sebi bazu poznatih aplikacija. Postoji opcija za kreiranje senzora koji bi blokirao samo određene aplikacije ili skupine aplikacija. Slikom 62 prikazan je postupak kreiranja senzora za blokiranje aplikacije i skupine aplikacija.



Slika 62 Senzor za blokiranje aplikacija

6.2.8.4 SSL inspekcija

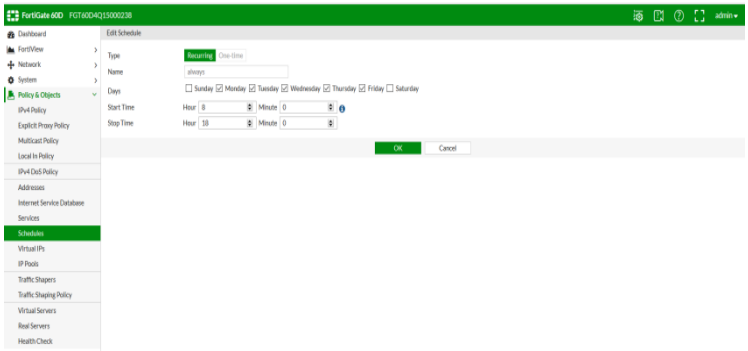
Fortigate vatrozid posjeduje opciju dekripcije i kontrole kriptiranog prometa. Slikom 63 prikazana je konfiguracija SSL dekripcije prometa.



Slika 63 Konfiguracija SSL dekripcije prometa

6.2.8.5 Konfiguracija rasporeda obavljanja

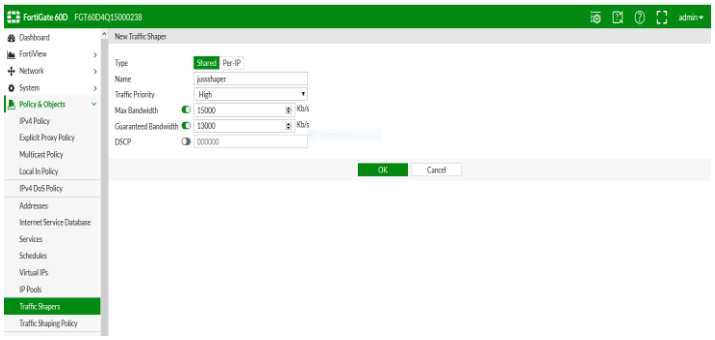
Fortigate vatrozidi posjeduje mogućnost korištenja određene sigurnosne politike samo u određenom vremenu. Slikom 64 prikazana je konfiguracija rasporeda za obavljanje sigurnosnih politika.



Slika 64 Konfiguracija rasporeda obavljanja

6.2.8.6 Konfiguracija QoS parametara

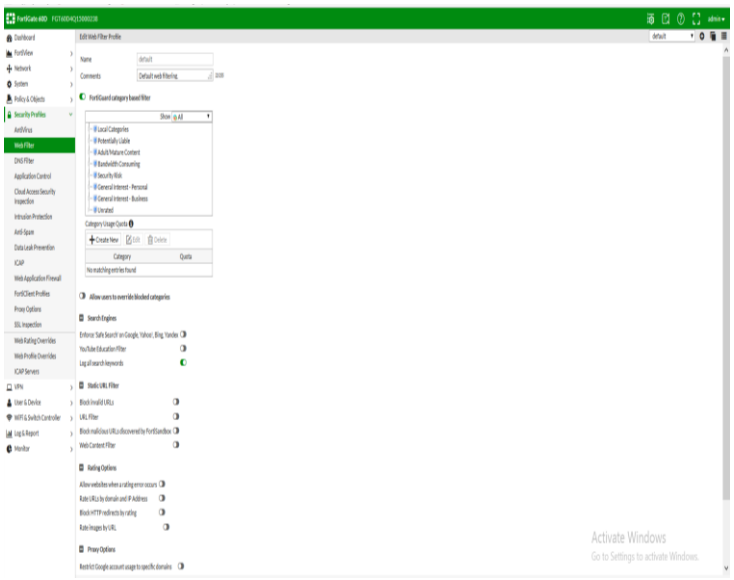
Postoji mogućnost konfiguracije i omogućavanja QoS parametara. Slikom 65 prikazana je konfiguracija QoS parametara.



Slika 65 Konfiguracija QoS parametar

.2.8.7 Konfiguracija *web* filtra

Fortigate vatrozid posjeduje veliku bazu *web* stranica sortiranih prema raznim kategorijama. Slikom 66 prikazana je konfiguracija *web* filtra.



Slika 66 Konfiguracija web filtra

6.2.8.8 Ostale opcije

Fortigate vatrozid posjeduje brojne mogućnosti čija konfiguracija nije prikazana. Najvažnije mogućnosti koje nisu prikazane su:

- mogućnost korištenja vatrozida kao usmjernika,
- mogućnost konfiguracije i omogućavanja VPN konekcija,
- *Antivirus* opcija,
- *Mail Filter,*
- *Web Application* vatrozid,
- DNS zaštita,
- IPS komponenta i
- *AntiDDos* funkcija (mogućnost ograničavanja dolaznog prometa).

8. Zaključak

U današnjem vremenu ne postoji mogućnost obavljanja normalnog poslovanja bez razvijene neke vrste informacijsko-komunikacijskog sustava. Ključni aspekt zaštite pristupa informacijskim sustavima predstavlja dobro konfiguriran i podešen vatrozid. Tradicionalni vatrozidi identificirali su aplikacije na način de je vrijedilo pravilo IP adresa+port=aplikacija. Tradicionalni mehanizmi zaštite dobro su obavljali svoj posao sve do pojave *web* 2.0 aplikacija. Pojavom i širenjem primjene *web* 2.0 aplikacija dolazi se do promjene načina ponašanja korisnika, također paralelno s razvojem i širenjem weba pojavljuje se sve veći broj tehnika napada kao i pokušaja napada. Iz razloga da tradicionalni vatrozidi nemaju mogućnosti osigurati dovoljnu razinu zaštite informacijsko-komunikacijskih sustava razvijaju se napredniji mehanizmi zaštite u obliku vatrozida nove generacije. Vatrozidi nove generacije imaju sve mogućnosti kao i tradicionalni vatrozidi ali donose brojna unaprjeđenja u rad i integraciju više različitih sigurnosnih riješena u jedan uređaj. Rad vatrozida nove generacije temelji se na tri komponente: identifikaciji aplikacija, identifikaciji korisnika i identifikaciji sadržaja. Kombiniranjem te tri komponente dobivaju se mogućnosti kreiranja naprednih sigurnosnih politika i kontrola. Postoje brojni proizvođači i brojne mogućnosti vatrozida nove generacije a izbor ovisi o potrebama korisnika.

Unutar rada opisano je testiranje i prikaz mogućnosti dva modela vatrozida: *Palo Alto* PA-500 i *Fortigate* D60. Postoje neke razlike u opcijama među ta dva modela ali je glavnina opcija i mogućnosti jednaka. Testiranje uređaja provedeno je u laboratorijskom i kontroliranom okruženju. Prilikom testiranja nisu uočeni nikakvi problemi u radu s uređajima. Treba istaknuti jednostavnost konfiguriranja vatrozida putem *web* sučelja. Iz provedenog testiranja vatrozida nove generacije može se zaključiti da se pravilnim izborom, implementacijom i konfiguracijom vatrozida nove generacije može postići visok stupanj sigurnosti informacijsko-komunikacijskog sustava.

Zahvale

Zahvaljujem se svojem mentoru izv. prof. dr. sc. Draganu Perakoviću za pomoć pri izradi ovog rada.

Posebno bih se zahvalio asistentima dr. sc. Siniši Husnjaku i mag. ing. traff. Ivanu Cvitiću na mnoštvu razumijevanja, savjetima i pomoći u laboratoriju pri izradi praktičnog dijela ovog rada.

Također, zahvaljujem se studentu Fakulteta prometnih znanosti Leu Tišljariću na pomoći pri tehničkoj izvedbi rada.

Na kraju, zahvaljujem se svojim roditeljima Snježani i Darku Juss na podršci tijekom cijelog trajanja svog studija.

Popis literature

[1] Northcutt, S., Zeltser, L., Winters, S., Kent, K., W., Ritchey, W.: Inside Network Perimeter Security (2nd Edition),Sams Publishing; Indianapolis, 2005.

[2] Harris, S.: CISSP All-in-One Exam Guide, McGraw-Hill Education; New York, 2012.

[3] Žonja, S.: STATEFUL INSPECTION FIREWALL, seminarski rad, Fakultet elektrotehnike i računrastva, Zagreb, 2005.

[4] Pleše, Ž.: Intrusion Prevention System (IPS) i Intrusion Detection System (IDS), sistemac.srce.hr, Zagreb, 2009.

[5] Frahim, J.,Santos, O.,Ossipov, A.: Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services, 3rd Edition ,Cisco Press, Indianapolis ,201

[6] Miller, L. Next-Generation Firewalls For Dummies, Wiley Publishing, Hoboken, 2011.

[7] The impact of Web 2.0 on enterprise applications, CIO, 2007, dostupno na: https://www.adobe.com/financial/pdfs/cio_mag_executive.pdf

[8] Tehnički izvještaj: Academic Freedom or Application Chaos?, Palo Alto, Santa Clara, 2009.

[9] Lohr, S. : Enterprise 2.0: A Computer Security Nightmare?, 2008, dostupno na: http://bits.blogs.nytimes.com/2008/04/14/enterprise-20-a-computer-security-nightmare/?_r=0

[10] Nazief, H: M., Sabastian, T. A.: Development of University of Indonesia next generation firewall prototype and access control with deep packet inspection, Advanced Computer Science and Information Systems (ICACSIS), 2014 International Conference, 2015.

[11] Tehnička brošura: APPLICATION-BASED POLICIES, Palo Alto, Santa Clara, 2012

[12] Tehnička brošura: USER-ID, Palo Alto, Santa Clara, 2015.

[13] Tehnička brošura :CONTENT-ID, Palo Alto, Santa Clara, 2015.

[14] Tehnička brošura: WHAT IS URL FILTERING, Palo Alto, Santa Clara, 2016.

[15] Nacionalni CERT, Palo Alto Networks Next generation Firewall, LSS-PUBDOC-2010-12-010 dostupno na: http://www.cert.hr/sites/default/files/NCERT-LAB-PUBDOC-2011-04-002.pdf

[16] Zwicky, E. D., Cooper, S., Chapman, B. D.: Building Internet Firewalls, Second Edition, Sebastopol, O'Reilly Media, 2000.

[17] The Ultra-Secure Network Architecture , RSM, dostupno na: http://rsmus.com/what-we-do/services/risk-advisory/the-ultra-secure-network-architecture.html (pristupljeno kolovoz 2016.)

[18] Peraković, D., Cvitić, I.: Sigurnost i zaštita informacijsko komunikacijskog sustava, skripta, Zagreb 2015

[19] Operativni priručnik: FIREWALL BUYERS GUIDE, Palo Alto, Santa Clara,

[20] Tehnička brošura: APP-ID, Palo Alto, Santa Clara, 2015.

[21] URL:http://www.paloguard.com/Firewall-PA-500.asp (pristupljeno svibanj 2015)

[22] Nacionalni CERT, Fortigate 60D, NCERT-LAB-PUBDOC-2014-07-001_1 dostupno na: http://www.cert.hr/node/2364

[23] URL:https://www.fortinet.com/solutions.html (pristupljeno svibanj 2016.)

[24] Operativni priručnik: FortiGate/FortiWiFi 60D Series, Sunyvale, 2016.

Popis kratica

ACC-*Application Command Center*

DHCP- *Dynamic Host Configuration Protocol*

DNS- *Domain Name System*

DoS- *Denial Of Service*

FTP- *File Transfer Protocol*

HTTP- *Hypertext Transfer Protocol*

IDS- *Intrusion Detectiony System*

IPS-*Intruson Prevention System*

IT- *Information Technology*

OSI- *Open Systems Interconnection*

QoS- *Quality of Service*

SSL-*Secure Sockets Layer*

TCP- *Transmission Control Protocol*

TLS- *Transport Layer Security*

UDP- *User Datagram Protocol*

URL- *Uniform Resource Locator*

Popis slika

Slika 1 Primjer rada paketnog filtra 4
Slika 2 Primjer tablice stanja, [1] 5
Slika 3 IPS i IDS postavljanje u mreži 8
Slika 4 Korištenje tehnike preskakivanja portova kod pojedinih aplikacija, [6] 12
Slika 5 Identifikacija aplikacija, [6] 17
Slika 6 Prednost sustava s jednostrukim prolazom, [8] 22
Slika 7 *Dual homed* arhitektura 24
Slika 8 Screened host arhitektura 25
Slika 9 *Screened subnet* arhitektura 26
Slika 10 Arhitektura sa višestrukim vatrozidima 27
Slika 11 Koncept segmentacije mreže i primjene sigurnosnih zona 33
Slika 12 App-ID 35
Slika 13 *User*-ID 37
Slika 14 *Content*-ID 37
Slika 15 Palo Alto PA-500, [16] 38
Slika 16 Osnovna shema laboratorijskog okruženja 40
Slika 17 Shema labosa s navedenim IP postavkama 40
Slika 18 *Palo Alto* početni zaslon 41
Slika 19 *Palo Alto Monitor* kategorija 42
Slika *20 Palo Alto* Policies kategorija 42
Slika 21 *Objects* kategorija 43
Slika 22 Osnovna konfiguracija sučelja 44
Slika 23 Konfiguracija statičke IP adrese sučelja 44
Slika 24 Konfigurirana sučelja na vatrozidu 45
Slika 25 Konfiguracija DHCP servera 46
Slika 26 Dodavanje nove statičke rute 46
Slika 27 Dodavanje zone 47
Slika 28 Kreirane zone 47
Slika 29 Kreiranje sigurnosne politike 48
Slika 30 Konfiguracija izvorišnih zona 49
Slika 31 Konfiguracija odredišnih zona 49

Slika 32 Konfiguracija akcija 50
Slika 33 Testiranje politike prijenosa prometa između zone trustl3i ostalih zona..... 51
Slika 34 Testiranje politike prijenosa prometa između zone untrustl3 i ostalih zona. 51
Slika 35 Sigurnosni profil za blokiranje sadržaja 52
Slika 36 Blokiranje docx dokumenta 53
Slika 37 Definiranje aplikacije 54
Slika 38 Aplikacijski potpis 54
Slika 39 omogućavanje *captive poratala* za autentifikaciju korisnika 55
Slika 40 Odabir načina autentifikacije 55
Slika 41 *Fortigate* D60 vatrozid [24] 58
Slika 42 Osnovna shema laboratorijskog okruženja 60
Slika 43 Dodijeljene IP adrese računalima u mreži 60
Slika 44 Početni prozor nakon prijave na vatrozid 61
Slika 45 *Security Profiles* 62
Slika 46 Dodavanje novog sučelja 63
Slika 47 Konfigurirana sučelja na vatrozidu 64
Slika 48 Konfiguracija DHCP servera na sučelju 64
Slika 49 Konfiguracija sigurnosne politike dozvole prometa iz zone lab1loc prema ostalim zonama 65
Slika 50 Konfiguracija sigurnosne politike dozvole prometa iz zone internetlab prema labdmz zoni 65
Slika 51 Konfiguracija sigurnosne politike zabrane prometa iz zone internetlab prema lab1loc zoni 66
Slika 52 Kontrola sigurnosne politike 66
Slika 53 Kontrola sigurnosne politike 2 67
Slika 54 Kontrola sigurnosne politike 3 67
Slika 55 Sigurnosna politika za dopuštanje ICMP servisa 68
Slika 56 Sigurnosna politika za blokiranje HTTP servisa 68
Slika 57 Rad sustava prije primjene sigurnosnih politika 69
Slika 58 Rad sustava nakon primjena sigurnosnih politika 69
Slika 59 Konfiguracija identifikacije korisnika 70
Slika 60 Konfiguracija filtra za blokiranje sadržaja 71
Slika 61 Konfiguracija aplikacijskog potpisa 71
Slika 62 Senzor za blokiranje aplikacija 72

Slika 63 Konfiguracija SSL dekripcije prometa 72
Slika 64 Konfiguracija rasporeda obavljanja 73
Slika 65 Konfiguracija QoS parametar 73
Slika 66 Konfiguracija web filtra 74