UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matej Bertoncelj

Varen dostop do internetnih storitev z uporabo požarne pregrade naslednje generacije

DIPLOMSKO DELO
NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Ljubljana, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matej Bertoncelj

Varen dostop do internetnih storitev z uporabo požarne pregrade naslednje generacije

DIPLOMSKO DELO
NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

MENTOR: prof. dr. Miha Mraz

Ljubljana, 2016

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge: Varen dostop do internetnih storitev z uporabo požarne pregrade naslednje generacije

Kandidat naj v svojem delu predstavi različne tehnološke pristope za realizacijo mrežnih požarnih pregrad. Pri tem naj različne tehnologije razvrsti glede na njihove zmožnosti in izpostavi najmodernejši pristop. Slednjega naj uporabi pri vzpostavitvi rešitve varnega dostopa do interneta za namišljenega naročnika - podjetje s širokim spektrom informacijskih dejavnosti.

Zahvala: Zahvaljujem se svoji ženi, ki je več let potrpežljivo poslušala »Sej bom.« in v času nastanjanja diplomskega dela požrtvovalno skrbela za dom, družino in bodoči naraščaj.

Kazalo

Povzetek

Naslov: Varen dostop do internetnih storitev z uporabo požarne pregrade naslednje generacije

Dobra praksa varovanja informacijske infrastrukture narekuje večplastni pristop. V večini primerov prvo obrambno vrsto predstavlja mrežna požarna pregrada. Diplomska naloga obravnava različne tipe mrežnih požarnih pregrad ter prednosti in slabosti različnih tehnoloških pristopov. Čedalje bolj sofisticirane grožnje so vzpodbudile razvoj naprednih sistemov za zaščito ter njihovo integracijo v sodobne požarne pregrade. Tako je podrobneje predstavljena požarna pregrada naslednje generacije in njene najpomembnejše funkcionalnosti.

Ker pri varovanju računalniških omrežij največjo ranljivost predstavlja uporabnik s končnimi napravami, je na primeru hipotetičnega naročnika predstavljen koncept uporabe požarne pregrade naslednje generacije. Glede na zahteve naročnika je podana analiza prometa in aplikacij. Analiza služi kot izhodišče za pripravo načrta rešitve in izvedbo varnega dostopa uporabnikov do interneta. Cilj diplomskega dela je predstaviti uporabnika in aplikacijo kot gradnika za izdelavo politike dostopov.

Ključne besede: varovanje informacijske infrastrukture, vrste požarnih pregrad, požarna pregrada naslednje generacije, prepoznava aplikacij

Abstract

Title: Securing user internet access using the next generation firewall

Good practice in information infrastructure security requires a multifaceted approach. In the majority of cases, the firewall represents the first line of defence. The thesis discusses diverse types of firewalls, as well as advantages and disadvantages of diverse technological approaches. Increasingly more sophisticated threats have promoted the development of advanced security systems together with their integration into present day firewalls. A detailed description of a next generation firewall and its most important functions is, therefore, given.

When securing computer networks the user himself with his devices represents the biggest threat to its vulnerability. An example of a hypothetical client, therefore, introduces the concept of the next generation firewall use. In reference to the needs of the client, the traffic and application analysis is introduced. The analysis serves as a basis for both implementation plan and the execution of a secure user internet access. The main goal of the thesis is to present the user and the application as the cornerstones of access policy.

Keywords: information infrastructure security, firewall types, next generation firewall, application recognition

Poglavje 1 Uvod

Ideja po ločevanju in gradnji zidov je stara tisoče let. Dobro poznan primer je kitajski zid, zgrajen za zaščito pred plemeni s severa. Vladarji v Evropi so gradili gradove z obzidji in jarki, s katerimi so se varovali pred vpadi sovražnikov in plenilskih skupin.

Besedna zveza "požarni zid" izhaja iz gradbeništva. To je namenska pregrada, narejena iz opeke, kovine ali drugega negorljivega materiala, ki omejuje širjenje požara iz ene sobe ali stavbe v drugo [1]. Požarno pregrado je moč zaslediti tudi v strojništvu [2]. Pri parnih lokomotivah se je uporabljala za ločevanje kurišča (kotla) in prostora s premogom.

Diplomska naloga obravnava požarno pregrado v modernejši izvedbi in sicer v informacijski tehnologiji (IT). V svetu IT požarne pregrade sicer nimajo opravka z ognjem ali pirotehniko, a služijo podobnemu namenu. Tovrstne požarne pregrade lahko zaščitijo tako individualne računalnike kot tudi omrežja korporacij, vendar jih moramo razumeti, da bi jih lahko uporabljali pravilno.

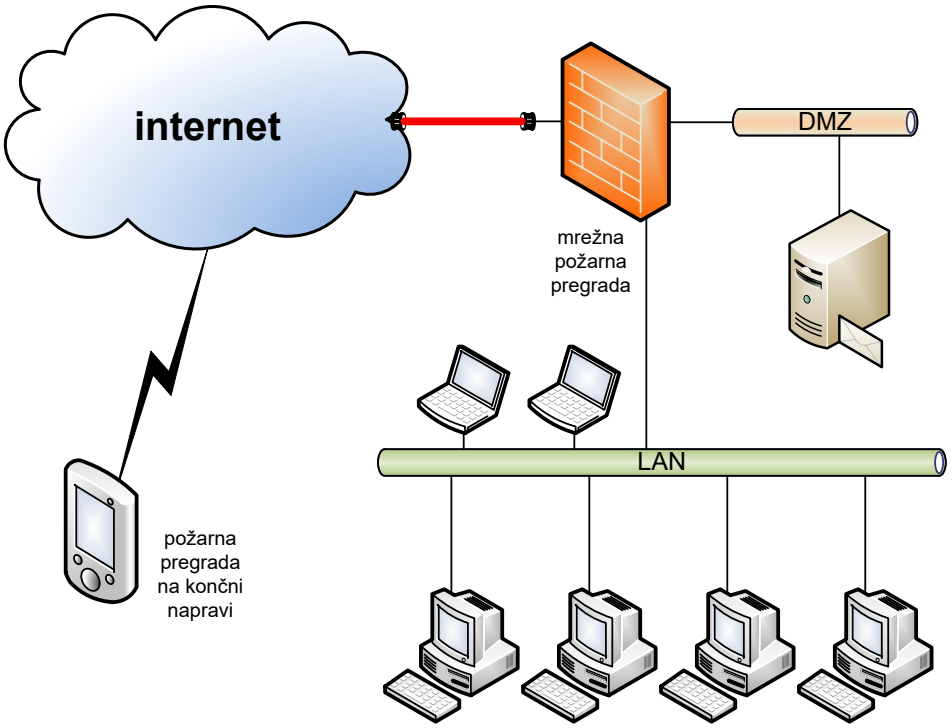
1.1 Namen požarne pregrade

Požarna pregrada je primarna metoda varovanja omreženih računalnikov pred vsiljivci. Omejuje izmenjavo podatkov na komunikacijski poti. Izvedena je lahko kot strojna ali kot programska oprema. Predstavlja osnovni način zagotavljanja bodisi varnega dostopa do interneta, bodisi varovanja velikih korporativnih omrežij.

1.2 Vrste požarnih pregrad

Najpogostejša vrsta požarne pregrade je realizirana kot programska oprema za zaščito končnih naprav kot so osebni računalniki, delovne postaje, pametni telefoni, strežniki (glej sliko 1). Nekatere so integrirane v operacijske sisteme, druge pa nastopajo kot samostojni programski produkti ali tudi kot modul programskih paketov za zaščito končnih naprav (integracija s protivirusnimi programi, programi za izdelovanje varnostnih kopij, odjemalci oddaljenega dostopa, itd).

Druga vrsta požarne pregrade, ki jo obravnava diplomska naloga, je mrežna požarna pregrada. Realizirana je lahko kot namenska strojna naprava (glej sliko 1), kot programska oprema, ki se izvaja na generičnem strežniku ali kot naprava v virtualiziranem sistemu. Običajno deluje na meji med mrežnimi segmenti. Na virtualni poti preko pregrade preverja mrežni promet in ga glede na določena pravila in ostale kriterije lahko prepušča ali zavrže.



Slika 1: Primer požarne pregrade na končni napravi in mrežne požarne pregrade.

V drugem poglavju pričujočega dela so predstavljene osnove mrežnih požarnih pregrad. Podani so vzroki za nastanek in potrebe po mrežni požarni pregradi. Skozi prizmo referenčnega modela so predstavljeni različni tehnološki pristopi, razvoj in funkcionalnosti sodobne požarne pregrade. V tretjem poglavju pričujočega dela je na primeru hipotetičnega naročnika predstavljena problematika zaščite omrežja in v četrtem poglavju njegova rešitev. Ta je predstavljena kot vzorčni koncept uporabe požarne pregrade naslednje generacije in njenih funkcionalnosti.

Poglavje 2 Mrežne požarne pregrade

V prvem delu pričujočega poglavja so predstavljene osnovne smernice delovanja, razlogi in potrebe za razvoj mrežnih požarnih pregrad. Da bi razumeli njihovo delovanje, so s pomočjo referenčnega modela podrobno razdelani različni tehnološki pristopi in njihove lastnosti. Podana sta tudi kronološki pregled in vpliv na razvoj tehnoloških pristopov. V zadnjem delu so predstavljene najpomembnejše funkcije sodobnih mrežnih požarnih pregrad ter podroben opis njihovega delovanja.

2.1 Uvod

Mrežna požarna pregrada je skupek strojne in programske opreme, ki kontrolira prometne tokove med mrežnimi segmenti. Ti so kategorizirani v varnostne cone od najmanj varovanih javnih omrežij (kot je internet) do najbolj varovanih omrežij, kjer se nahajajo najobčutljivejši podatki [3]. Ne glede na izvedbo deluje mrežna požarna pregrada kot kontroliran prehod, preko katerega mora prehajati ves mrežni promet. Na tem prehodu se po administratorjevih navodilih izvaja manipulacija s prometom. Najpogosteje uporabljena funkcionalnost je filtriranje prometa, pri čemer poznamo dva osnovna koncepta filtriranja:

- dovoljeno je vse, kar ni prepovedano in
- prepovedano je vse, kar ni dovoljeno.

Zelo pogosto sta oba koncepta uporabljena pri enostavnih postavitvah mrežnih požarnih pregrad. Kot primer navedimo mrežno požarno pregrado za domačo rabo, kjer je uporabnikom dovoljen ves promet, ki gre v smeri iz domačega omrežja proti internetu (odhodni promet) in prepovedan ves promet, ki gre iz smeri interneta proti domačemu omrežju (dohodni promet).

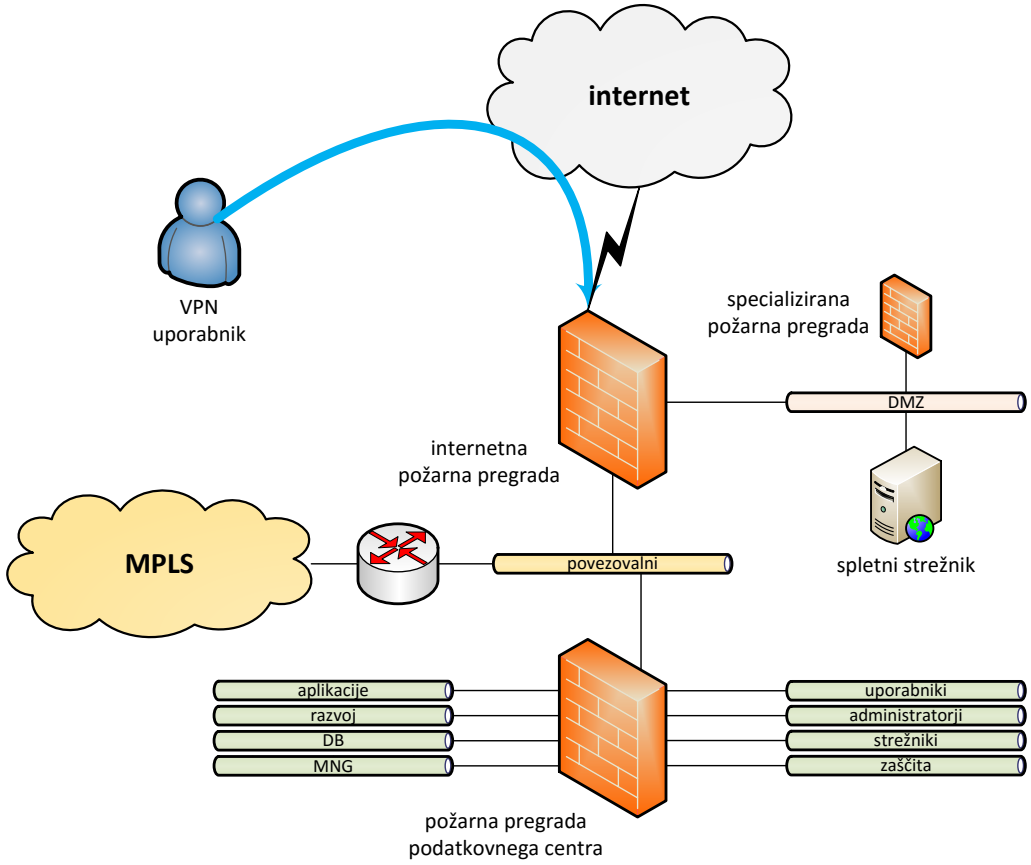
Zadeva je veliko manj preprosta pri resnejših postavitvah. Administrator po določilih, ki jih narekuje varnostna politika, nastavi mrežno požarno pregrado tako, da izvaja željeno politiko filtriranja. Primer takšne politike bi bil lahko sledeč:

- omogočen je dostop iz interneta do korporativnih poštnih strežnikov;
- do podatkov o plačah je dovoljen dostop le avtoriziranemu vodstvenemu kadru;

- med delovnim časom je prepovedan dostop do multimedijskih portalov z zabavnimi vsebinami.

V profesionalni rabi se mrežne požarne pregrade glede na postavitev delijo na (glej sliko 2):

- internetne požarne pregrade: te varujejo mejo med javnim in varovanim omrežjem;
- notranje požarne pregrade ali požarne pregrade podatkovnega centra: te so implementirane z namenom, da ločujejo varnostno najobčutljivejše podatke pred morebitnimi zlorabami znotraj varovanega omrežja;
- specializirane požarne pregrade: te so namenjene zaščiti točno določenih servisov.



Slika 2: Primer internetne, specializirane in požarne pregrade podatkovnega centra.

2.2 Osnovne smernice delovanja požarnih pregrad

Večina programske kode (programov) vsebuje hrošče. Večji programi imajo več hroščev (običajno še več, kot bi jim pripisali glede na velikost). Večina omreženih računalnikov ima večje število programov, od tega verjetno kakšnega večjega. Zatorej je omrežene računalnike

smotrno vsaj deloma izolirati od ostalih omrežij. Iz tega sledi tudi to, da naj imajo požarne pregrade (izpostavljeni računalniki) čim manj programov, ti pa naj bodo čim manjši. Sama konfiguracija požarne pregrade naj bo minimalistična. Mrežna požarna pregrada igra pomembno vlogo pri varovanju podatkov, ker zmanjšuje možnosti zlorabe varnostnih pomanjkljivosti [4]. Mrežna požarna pregrada je skupek elementov, umeščenih med dve ali več omrežij, s sledečimi lastnostmi:

- ves promet med dvema ali več omrežji mora prehajati skozi požarno pregrado;
- prehaja lahko samo tisti promet, katerega mrežni administrator specificira s politiko filtriranja;
- naprava sama je imuna na penetracijo.

2.3 Mrežne požarne pregrade v praksi

Prakso narekujejo različni parametri od dejanske potrebe uporabnikov, administratorjev, vsiljevanja varnostnih politik, do nenazadnje bolj ali manj dodelanih idej izdelovalcev opreme. Varnost informacijske tehnologije je predmet večmilijonskega, visoko konkurenčnega posla, kar v praksi pripelje do modificiranih alinej osnovnih smernic delovanja. Te so sledeče:

- to, da promet prehaja kontrolirano skozi napravo, ni dovolj; pomembno je tudi razumevanje vsebine prometa;
- politike filtriranja so zelo pogosto polne nedokumentiranih zapisov, vsebujejo zastarane ali neuporabljene definicije dostopov in so tako ali drugače v nasprotju z dobrimi praksami; vzrokov je običajno več, vse od slabe organizacijske strukture v podjetju, nedefiniranih postopkov uvajanja sprememb, pa vse do nezadostnega znanja ali celo malomarnosti administratorjev; politika filtriranja je prepogosto prilagojena željam uporabnikov namesto dobro premišljeni varnostni politiki;
- zaradi konkurenčnosti proizvajalci tekmujejo, kako v svoje naprave vgraditi čim večje število funkcionalnosti; finančna in časovna stiska pri razvoju v veliki meri doprineseta, da je sistemska programska oprema polna hroščev, ki nemalokrat močno povečujejo število varnostnih pomanjkljivosti; primera slednjih sta sledeča:
  - več let trajajoča varnostna pomanjkljivost mrežne požarne pregrade proizvajalca *Juniper*: ta je omogočala prisluškovanje tunelom prometnih tokov, ki so zavarovani s tehnologijo navideznih privatnih omrežij (ang. *virtual private network* – VPN) [5];

- varnostna pomanjkljivost, ki je omogočala izvedbo napada ohromitve storitve (ang. *denial of service* – DoS), na požarnih pregradah proizvajalca *Cisco* [6].

2.4 Razlogi za razvoj mrežnih požarnih pregrad

Internet je relativno mlad izum. Pionir interneta je bila manjša in zaprta skupina raziskovalcev in sodelavcev *Advanced Research Projects Agency Network* (ARPANET) projekta [7]. V času razvoja je bil izziv vzpostaviti in ohraniti povezljivost med računalniki. Ravno zaradi sodelovanja in usklajevanja številnih parametrov so se med pionirji interneta spletala mnoga profesionalna prijateljstva. Internet je nastal kot posledica raziskovanja in sodelovanja [8]. Začetki uporabe so tako potekali v duhu izmenjave informacij, akademskih znanj, oddaljenega dostopa, itd. Postopoma se je vključevalo vedno več udeležencev. Zaupanje v omrežje je leta 1988 resno omajal črv *Morris* [9]. Pred tem je bil fokus predvsem poenostaviti administracijo ter povečati zanesljivost računalnikov in omrežij, s katerimi so bili povezani. Po črvu *Morris* je bilo tovrstnih incidentov vedno več, kar je usmerilo pozornost tudi k varovanju omrežij. Sčasoma je postalo jasno, da je na internetu mnogo nezaupanja vrednih ali celo nevarnih uporabnikov.

2.5 Potrebe po mrežni požarni pregradi

Ko povezujemo omrežja, torej ne moremo zaupati komurkoli. Različna omrežja predstavljajo različne stopnje tveganja oz. različne stopnje zaupanja. Požarne pregrade lahko razmejujejo cone z različnimi stopnjami zaupanja iz številnih razlogov. Najpogostejši so:

- varnostne luknje v operacijskih sistemih,
- preprečevanje dostopa do informacij,
- preprečevanje odtekanja zaupnih podatkov,
- vsiljevanje varnostne politike,
- revidiranje informacijskih sistemov.

2.5.1.1 Varnostne luknje v operacijskih sistemih

Kritične varnostne pomanjkljivosti se pojavljajo tako rekoč v vseh modernih operacijskih sistemih. Primera takih pomanjkljivosti sta sledeča:

- kritična varnostna ranljivost proizvajalca *Apple* v operacijskem sistemu *OS X* in operacijskem sistemu mobilnih naprav *iOS*; ta ranljivost napadalcu omogoča, da zaobide *Applov* varnostni sistem, ki skrbi za integriteto sistema, in omogoča oddaljeno izvajanje škodljive kode [10];

- kritična varnostna pomanjkljivost imenovana *Stagefrihgt* v mobilnem operacijskem sistemu *Google Android*; ta varnostna pomanjkljivost je zaradi razdrobljenega sistema posodabljanja verjetno še bolj kritična kot prva. Tudi ta omogoča oddaljeno izvajanje škodljive kode [11].

Tako kot moderni, so imeli tudi starejši operacijski sistemi kritične varnostne pomanjkljivosti. Kot primer je moč navesti sledeče:

- *Microsoft Windows 95* in *Windows 98* sta imela po privzetih nastavitvah vklopljeno skupno rabo datotek, kar so s pridom izkoriščali številni virusi [1];

- Starejša *Linux* distribucija *Red Hat* je s privzeto instalacijo omogočila kar tri oddaljene napade.

2.5.1.2 Preprečevanje dostopa do informacij

Ko govorimo o preprečevanju dostopa do informacij, lahko kot zanimivost omenimo uporabo nacionalnih požarnih pregrad določenih držav. Te požarne pregrade so (bile) prvenstveno namenjene omejevanju aktivnosti državljanov. V kasnejših fazah te požarne pregrade zamenjujejo rezultate spletnih iskalnikov in s tem omejujejo dostop do informacij v obliki cenzure.

2.5.1.3 Preprečevanje odtekanja zaupnih podatkov

Preprečevanje odtekanja podatkov lahko pomeni preprečitev kraje intelektualne lastnine, lahko pa tudi preprečitev odtekanja pomembnih poslovnih podatkov.

2.5.1.4 Vsiljevanje varnostne politike

Mrežna požarna pregrada je orodje, ki na mrežnem nivoju omogoča izvajanje varnostne politike. Ta določa rabo spletnih in lokalnih virov informacijske tehnologije.

2.5.1.5 Revidiranje informacijskih sistemov

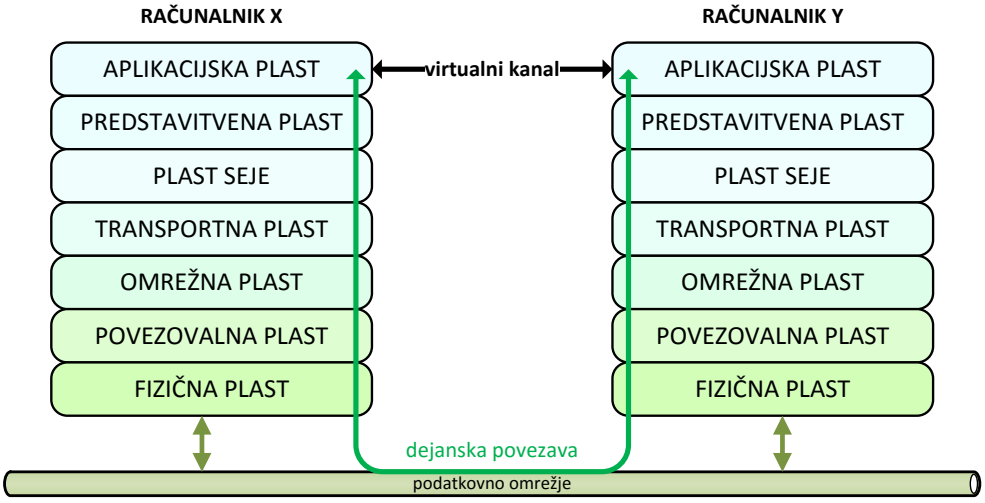
V primeru varnostnega incidenta se lahko na požarni pregradi izvede forenzična analiza sledi. Analiza sledi se lahko uporablja tudi za spremljanje porabe virov, na primer rabe interneta v privatne namene med delovnim časom.

2.6 Model ISO/OSI in TCP/IP

Kljub temu, da modela ISO/OSI in TCP/IP nista osrednja tema tega diplomskega dela, sta ključnega pomena za razumevanje pristopov in tehnologij mrežnih požarnih pregrad.

2.6.1 ISO/OSI

Model OSI (*Open Systems Interconnection*) je konceptualni model mednarodne organizacije za standardizacijo (ang. *International Organization for Standardization* – ISO). Gre za hierarhični model, ki standardizira in razdeli funkcije komunikacijskega sistema v eno izmed sedmih abstraktnih plasti. Podobne komunikacijske funkcije združuje v logične plasti [12]. Nižje ležeča plast streže višje ležeči plasti. Na isti plasti sta dve instanci s protokolom medsebojno povezani v virtualni kanal (glej sliko 3).



Slika 3: Sedemplastni OSI model.

2.6.1.1 Aplikacijska plast

Sedma – aplikacijska plast zagotavlja komunikacijsko podporo aplikaciji oziroma njeni komunikacijski komponenti [13]. Tipične funkcije aplikacijske plasti so sledeče:

- identifikacija komunikacijskega partnerja: za aplikacijo, ki želi prenos podatkov, aplikacijska plast določi identiteto in dosegljivost aplikacije komunikacijskega partnerja;
- zagotavljanje mrežnih zmožnosti: aplikacijska plast določi ustreznost mrežnih zmožnosti komunikacijskega partnerja;

- sinhronizacija komunikacije: aplikacijska plast zagotavlja sodelovanje pri medaplikativni komunikaciji.

2.6.1.2 Predstavitvena plast

Šesta – predstavitvena plast skrbi za pravi izbor sintakse in po potrebi njene pretvorbe. Zagotavlja neodvisno prezentacijo podatkov (kodne tehnike, vrste spremenljivk, sintakse) tako, da vrši prevajanje med aplikacijo in mrežnimi formati. Skrbi za šifriranje in kompresijo podatkov brez izgube.

2.6.1.3 Plast seje

Peta po vrsti je plast seje. Ta nadzoruje (vzpostavlja, kontrolira, zaključuje) dialog med lokalno in oddaljeno aplikacijo. Določa interakcijo (enosmerno, dvosmerno, izmenično dvosmerno), sinhronizacijo (določanje točk, od katerih se, ob morebitni napaki, ponovi del dialoga) in poroča o napakah.

2.6.1.4 Transportna plast

Četrta – transportna plast logično povezuje dva komunikacijska partnerja. Ponuja funkcionalna in postopkovna sredstva za prenos podatkovnih sekvenc različnih dolžin in pri tem zagotavlja kvaliteto storitve. Definiranih je pet nivojev povezovalno orientiranih transportnih protokolov (TP), od TP0 do TP4, pri čemer slednji zagotavlja največ funkcij (za manj zanesljiva omrežja – kot je internet), oziroma TP0, ki zagotavlja zgolj osnovne funkcionalnosti, namenjene za brezizgubne povezave. Najpomembnejši funkciji transportne plasti sta ugotavljanje in odprava napak ter kontrola pretoka in zaporedja podatkov.

2.6.1.5 Omrežna plast

Tretja – omrežna plast skrbi za prenos podatkov med enim ali več medsebojno povezanimi omrežji. Zagotavlja fragmentacijo, multipleksiranje, usmerjanje in določanje poti podatkom.

2.6.1.6 Podatkovno-povezovalna plast

Druga plast zagotavlja povezavo med dvema neposredno povezanima sistemoma, zagotavlja identifikacijo in delno odpravo napak ter definira protokol za vzpostavitev in zaključitev povezave med dvema fizično povezanima napravama. Istočasno zagotavlja kontrolo nad pretokom podatkov.

2.6.1.7 Fizična plast

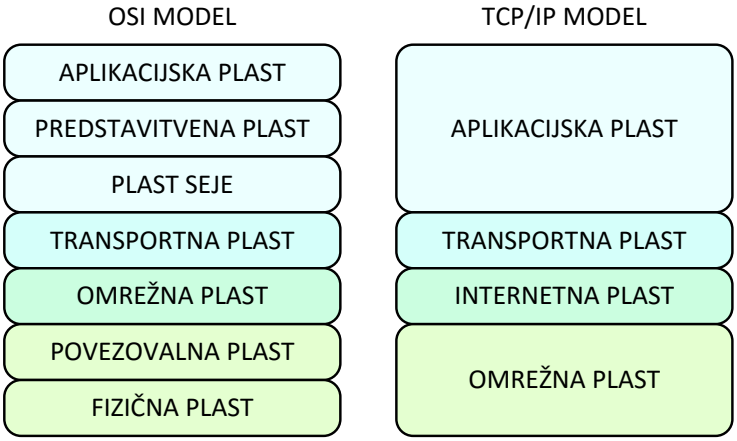
Glavne funkcije fizične plasti so deljene na tiste, ki so odvisne, in tiste, ki so neodvisne od prenosnega medija. Odvisne funkcije določajo vrste in oblike signalov, postavitve kontaktov,

napetostnih nivojev in ostalih fizičnih lastnosti priključenih medijev. Neodvisne funkcije definirajo kodiranje, sinhronizacijo in postopke povezovanja.

2.6.2 Primerjava modela OSI in modela TCP/IP

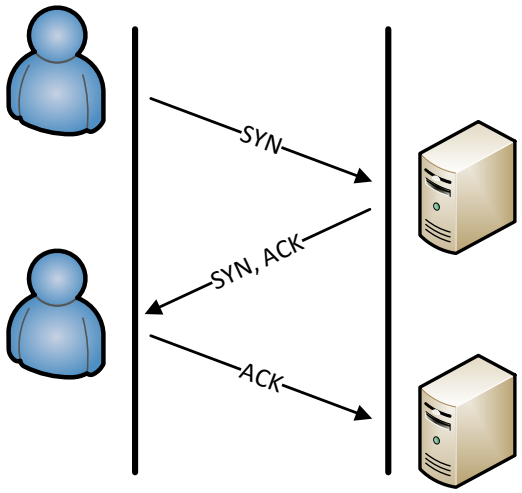
TCP/IP je v praksi uveljavljen standard, za razliko od modela OSI, ki je le konceptualen. Ime je dobil po dveh najpogosteje uporabljenih protokolih TCP (*Transmission Control Protocol*) in IP (*Internet Protocol*) [14].

TCP/IP je štiri plastni model. Sestavljajo ga aplikacijska, transportna, internetna in omrežna plast. Četrta – aplikacijska plast modela TCP/IP je soležna aplikacijski plasti, predstavitveni plasti in plasti seje modela OSI (glej sliko 4).



Slika 4: Relacija med modelom OSI in modelom TCP/IP.

Model TCP/IP ne predvideva, kaj se zgodi v aplikacijski plasti. Če komunikacijska komponenta aplikacije potrebuje kaj več kot zagotavlja model TCP/IP, je to potrebno realizirati v aplikaciji sami. Pri tretji – transportni plasti modela TCP/IP je pomembno poudariti, da poleg funkcij transportne plasti vključuje tudi funkcijo plasti seje modela OSI – elegantno zaključevanje (ang. *graceful end*) [15]. Protokol TCP pred pričetkom prenosa uporablja trismerno rokovanje (ang. *three-way handshake*), pri čemer stran, ki želi vzpostaviti povezavo, pošlje začetno sporočilo z zastavico *SYN*, druga stran odgovori s *SYN ACK*, in spet prva z *ACK* (glej sliko 5).



Slika 5: Trismerno rokovanje protokola TCP.

Poleg povezovalno usmerjenega protokola TCP vključuje funkcija transportne plasti tudi nepovezovalno usmerjen UDP (*User Datagram Protocol*). Ta za razliko od protokola TCP pred pričetkom prenosa ne uporablja trismernega rokovanja, saj sta prioriteti hitrost in enostavnost pomembnejši od zanesljivosti. Druga – internetna plast temelji na nepovezovalno usmerjenem protokolu IP. V nasprotju z modelom ISO ne predvideva povezovalno usmerjenega protokola na tej plasti. Prva – mrežna plast modela TCP/IP je soležna podatkovno-povezovalni in fizični plasti modela OSI. Mrežna plast modela TCP/IP je najbolj ohlapna, saj je odvisna od mrežnega vmesnika in omrežja samega. Model OSI je zaradi svoje granularnosti in natančne specifikacije referenčni model in zaradi tega primeren za opisovanje mrežnih funkcij.

2.7 Tehnološki pristopi mrežnih požarnih pregrad

Tehnološki pristopi mrežnih požarnih pregrad so pogojeni predvsem z obdobjem, v katerem so bili razviti. To je povezano z zmogljivostjo računalniške opreme in mrežnih povezav, evolucijsko stopnjo interneta in groženj ter posledično s potrebami po mrežnih požarnih pregradah [8].

Pri arhitekturi mrežnih požarnih pregrad velja pravilo, da ima mrežna požarna pregrada, višje kot gremo po modelu OSI, več informacij, s katerimi lahko operira in s tem zagotavlja višjo stopnjo varnosti. Posledično pa z obdelavo podatkov na višjih nivojih modela OSI požarna pregrada porabi več strojnih virov (ciklov centralno procesne enote, pomnilnika, itd.) [3].

Na tem mestu je potrebno omeniti, da imajo nekatera poimenovanja tehnoloških pristopov izrazito močno marketinško komponento. Ker pa v veliki večini nimamo dostopa do izvorne kode mrežne požarne pregrade, težko z gotovostjo določimo tehnološki pristop. Po

podrobnejšem pregledu mrežne požarne pregrade in pripadajoče dokumentacije se običajno izkaže, da se za inovativnimi marketinškimi imeni pogosto ne skriva revolucionarna ali nova tehnologija [8]. Marsikatera komercialna poimenovanja mrežnih požarnih pregrad ne sovpadajo z dejansko uporabljenimi tehnološkimi pristopi.

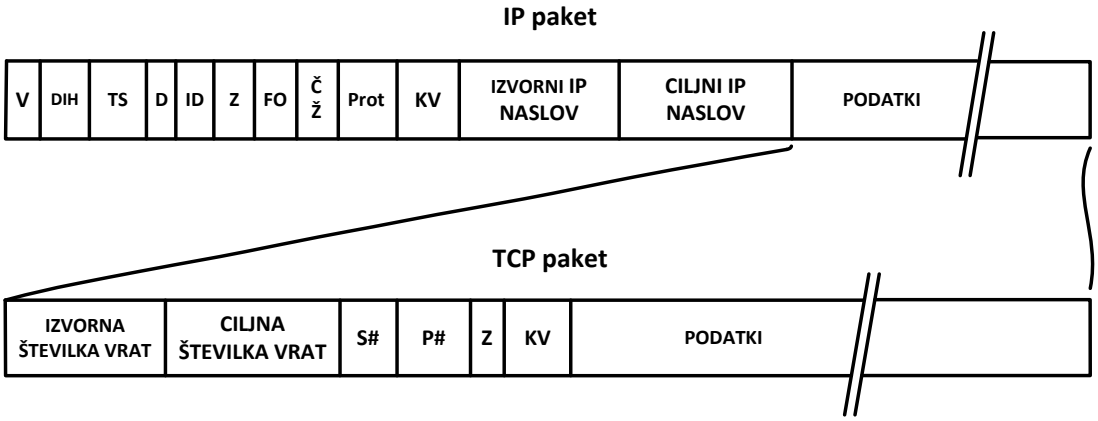
Kljub temu, da so mrežne požarne pregrade navadno hibridi tehnoloških pristopov, jih razvrščamo po njihovih prevladujočih lastnostih. Te lastnosti so sledeče:

- filter paketov,
- filter paketov z upoštevanjem vseh stanj,
- požarna pregrada kot posrednik paketov,
- aplikacijski prehod,
- stanovitna kontrola,
- temeljito pregledovanje paketov,
- večnamenska mrežna požarna pregrada,
- mrežna požarna pregrada naslednje generacije,
- specializirana mrežna požarna pregrada.

2.7.1 Filter paketov

Filter paketov (ang. *packet filter*) je enostavna mrežna naprava. Običajno gre za usmerjevalnik s funkcijo filtriranja paketov (ang. *packet filtering*). Za svoje delovanje uporablja sledeče informacije iz glave paketa IP in paketa TCP ali UDP (glej sliko 6) [16]:

- izvorni naslov IP,
- ciljni naslov IP,
- uporabljeni protokol,
- izvorno številko vrat in
- ciljno številko vrat.



Slika 6: Glava paketa IP in TCP.

Filter paketov za vsak paket preveri, ali zanj obstaja pravilo v politiki filtriranja. Glede na to paketu dovoli prehod ali ga zavrže. Če v politiki filtriranja ne najde zapisa, velja privzeto pravilo – kar v veliki večini implementacij pomeni, »prepovej vse« [3]. Kljub temu, da uporablja informacije iz glave TCP ali glave UDP, je samo delovanje omejeno na omrežno plast modela OSI. Glavne značilnosti paketnih filtrov so sledeče:

- za nizko ceno omogočajo osnovno nalogo filtriranja;
- filtriranje paketov je učinkovito in omogoča majhne zakasnitve, še posebej, če je strojno pospešeno;
- omejenost rabe, saj je potrebno eksplicitno omogočiti vsak promet in tako je s filtri težko zajeti vse dele aplikacij;
- politika filtriranja mora slediti spremembam naslovov v omrežju;
- potrebno je eksplicitno omogočiti povratni promet;
- posledično je mogoče dostopati do klientov na varovani strani omrežja.

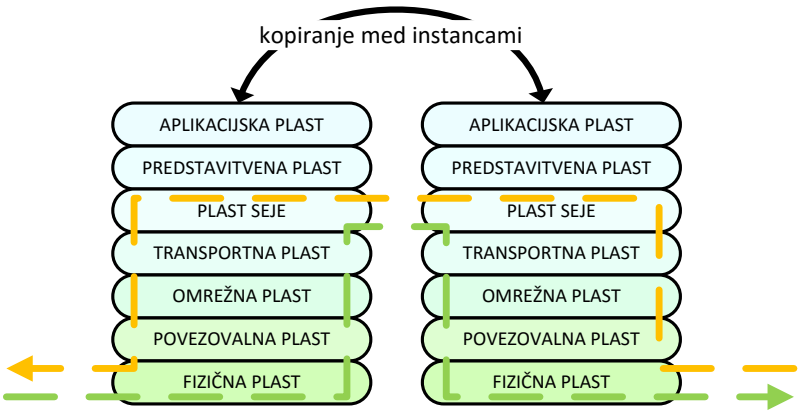
2.7.2 Filter paketov z upoštevanjem vseh stanj

Filter paketov z upoštevanjem vseh stanj (ang. *stateful packet filter*) je pravzaprav nadgradnja navadnega filtra paketov, saj deluje na transportni plasti modela OSI. Ta poleg »*packet filtering*« tehnike filtriranja paketov spremlja stanje povezave. Požarna pregrada sledi iniciatorju povezave, trismernemu rokovanju in številkam sekvence ter podatke zapiše v pomnilnik. S tako dobljeno dinamično tabelo vzpostavljenih sej TCP in navideznih povezav UDP omogoča veliko učinkovitejše procesiranje paketov. Z vidika porabe resursov je

preprosteje ugotoviti, ali določen paket pripada že obstoječi povezavi, kot ga primerjati s številnimi zapisi v politiki filtriranja. »*Stateful packet filter*« s tabelo stanj omogoča dinamično prepuščanje povratnega prometa, ki je del (navidezne) povezave. Na tak način omogoča mnogo bolj učinkovito izgradnjo politike dostopov, predvsem pa bolje ščiti naprave na varovani strani omrežja. Mrežna požarna pregrada iz pomnilnika sprosti zapis stanja, ko prestreže zastavico za končanje povezave (*FIN*) ali po časovnem izteku [17]. Slednjega uporablja nepovezovalno usmerjeni protokol UDP. V posebnih primerih mora aplikacija skrbeti za sporočila o vzpostavljeni povezavi (ang. *keepalive*). »*Stateful packet filter*« je performančno zelo učinkovit in zato takšne mrežne požarne pregrade dosegajo visoke propustnosti.

2.7.3 Mrežna požarna pregrada kot posrednik paketov

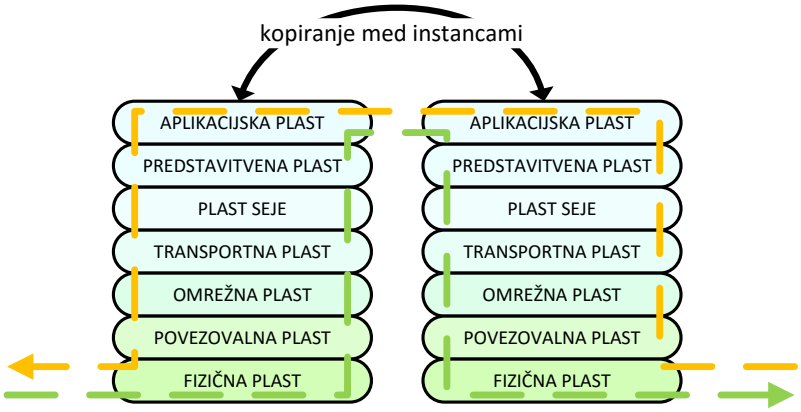
Mrežna požarna pregrada kot posrednik paketov (ang. c*ircuit relay*) za namene filtriranja uporablja informacije iz TCP, UDP in glave paketa IP. Deluje na plasti seje modela OSI. Za razliko od filtra paketov ne dopušča direktne komunikacije med komunikacijskima entitetama. Za vsako povezavo vzpostavi dve instanci (glej sliko 7). V primeru seje TCP, ko izvor pošlje zahtevo po komunikaciji, »*circuit relay*« preveri politiko filtriranja in če je komunikacija dovoljena, ustvari drugo povezavo proti cilju. S ciljem izvede trismerno rokovanje in če je leto uspešno, dokonča trismerno rokovanje še z izvorom. Med povezavo z izvorom in povezavo s ciljem vzpostavi navidezno komunikacijsko cev (ang. *pipe*) [16]. Podobno kot »*stateful packet filter*« se »*circuit relay*« zaveda stanja povezav. Dodatno pa, ravno zaradi posredovanja med instancami, izvaja prevajanje mrežnih naslovov (ang. *network address translation* – NAT). Ker mora vsak paket navidezno preko dveh instanc, predstavlja tudi nekoliko večje breme za strojno opremo.



Slika 7: Navidezna pot skozi »*circuit relay*«.

2.7.4 Aplikacijski prehod

Aplikacijski prehod (ang. *application gateway*) je mrežna požarna pregrada in je pravzaprav skupek več različnih aplikacijskih proksijev (ang. *proxy* – posrednik, ki prestreza zahteve klienta in jih posreduje strežniku). Aplikacijski prehod deluje podobno kot »*circuit relay*«. Torej za vsako povezavo ustvari dve instanci (glej sliko 8). Bistvena razlika pa je, da to počne na aplikacijski plasti modela OSI. To pomeni, da pregleduje tudi podatkovni del paketa in da razume vsebino.



Slika 8: Navidezna pot skozi aplikacijski prehod.

Prav funkcija posrednika omogoča višjo stopnjo zaščite, saj lahko izloči nepravilnosti na vseh plasteh modela OSI [16]. Bistvena je možnost filtriranja na podlagi aplikativnih podatkov, kot so ukazi znotraj seje SMTP ali naslovov URL (*Uniform Resource Locator)* znotraj protokola HTTP (*Hyper Text Transfer Protocol*). Aplikacijski prehod lahko filtrira tudi na podlagi podatkov iz glav paketov TCP, UDP in IP. Če je določen promet dovoljen, ga aplikacijski proksi skopira v drugo instanco in pošlje prejemniku.

Če želimo pregledovati podatke na sedmi plasti modela OSI, potrebujemo aplikacijski proksi za vsak protokol. To je bistvena slabost take požarne pregrade. Sam razvoj proksija je zahteven proces, poleg tega pa mora razvoj proksija slediti razvoju protokola [8]. Posledično je protokolov bistveno več kot aplikacijskih proksijev, zato v praksi ni požarne pregrade, ki bi lahko filtrirala celoten mrežni promet in bi delovala izključno na temelju aplikacijskih proksijev. Aplikacijski prehod za protokole, za katere nima specifičnega aplikacijskega proksija, uporablja tehnologijo »*circuit relay*«.

Pomembno je tudi dejstvo, da so proksi funkcionalnosti s stališča porabe strojnih virov zelo potratne in pogosto predstavljajo opazno povečanje latence.

2.7.5 Stanovitna kontrola

Stanovitna kontrola (ang. *stateful inspection*) označuje tehnologijo, ki temelji na osnovi »*stateful packet filter*«, »*inspection*« pa označuje funkcijo pregledovanja vsebine. »*Stateful inspection*« mrežna požarna pregrada na svojevrsten način združuje funkcije sledečih treh različnih tehnoloških pristopov [16] in sicer:

- »*stateful packet filter*«,
- »*circuit relay*« in
- aplikacijskega prehoda.

"Stateful inspection« požarna pregrada podobno kot »*circuit relay«* preprečuje nepravilnosti pri trismernem rokovanju s to razliko, da »*stateful inspection«* požarna pregrada to funkcionalnost izvede znotraj ene same povezave [18]. »*Stateful inspection«* požarna pregrada lahko filtrira promet tudi na podlagi podatkov aplikacijske plasti modela OSI. Podobno kot aplikacijski prehod, lahko to funkcionalnost nudi le za podprte protokole. Nasprotno z aplikacijskim prehodom ne uporablja aplikativnih proksijev, pač pa se zanaša na posebne algoritme, da interpretirajo podatke. Ti algoritmi primerjajo znane vzorce (podpise oz. odtise aplikacij) s podatkovnim tokom. Prepoznava aplikativnih podatkov omogoča dinamično prilagajanje politike filtriranja. Primer takšnega prilagajanja bi bil sledeč: uporabnik na notranji strani internetne požarne pregrade sproži povezavo proti javnemu strežniku FTP. Požarna pregrada nato sledi seji FTP in prestreže podatek, na katerih vratih TCP naj odjemalec posluša za podatkovni del povezave. Požarna pregrada za ta strežnik FTP dinamično odpre podatkovni promet proti odjemalcu [19]. Taka kombinacija različnih tehnoloških pristopov ima sledeče prednosti:

- dinamično prilagajanje in omogočanje pregledne politike filtriranja;
- vsak paket gre samo enkrat skozi sklad TCP/IP;
- podpira model strežnik-odjemalec;
- primerjanje vzorcev je z vidika porabe strojnih virov bolj učinkovito kot aplikacijski proksiji;
- taka požarna pregrada lahko filtrira ves promet.

2.7.6 Temeljito pregledovanje paketov

Temeljito pregledovanje paketov (ang. *deep packet inspection* – DPI) označuje tehnologijo, ki nadgrajuje »*stateful inspection«* s sistemi za odkrivanje vdorov (ang. *intrusion detection system* – IDS). Tako omogoča razširjeno pregledovanje prometa na aplikacijski plasti modela OSI. Požarne pregrade DPI razširjajo »*stateful inspection«* filtriranje ne le z uporabo t. i. podpisov IDS, ampak tudi z uporabo hevristike, statistične analize oziroma z uporabo odkrivanja anomalij. Rezultati skeniranja se nato uporabijo v procesu filtriranja. Na ta način pridobijo podatke o stanju povezave na aplikacijski ravni. Tudi odkrivanje škodljive kode temelji na tehnologiji podpisov IDS. V njih se skrivajo odtisi ali vzorci napadov ali druge zlonamerne kode [20]. Poleg varnostnih funkcij omogoča tehnologija »*deep packet inspection«* še druge funkcije, kot so zagotavljanje kvalitete storitev (ang. *quality of service* – QoS) in identifikacijo aplikacije.

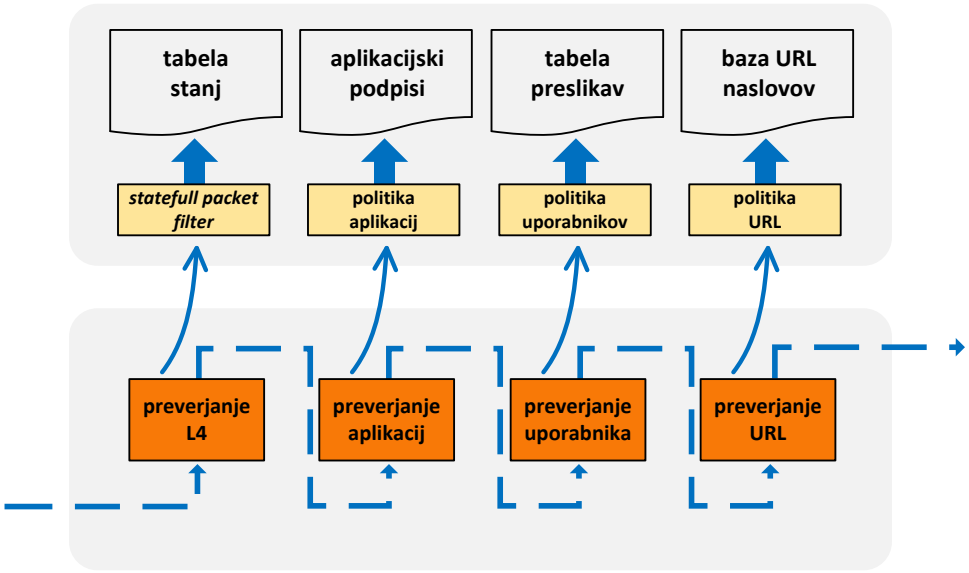
2.7.7 Večnamenska požarna pregrada

Večnamenska požarna pregrada (ang. *unified threat management* – UTM) združuje več varnostno usmerjenih funkcij v eni sami napravi. Deluje na aplikacijski plasti modela OSI. Požarna pregrada UTM je nadgradnja požarne pregrade DPI, saj se proti kombinaciji različnih nevarnosti spopada z naborom varnostno usmerjenih funkcij, kot so »*stateful packet filter«*, sistem za preprečevanje vdorov (ang. *intrusion prevention system* – IPS), spletni proksi, protivirusni sistem, sistem za preprečevanje neželene pošte, itd. Požarna pregrada UTM v primerjavi z neintegriranimi sistemi omogoča sledeče funkcije [21]:

- zmanjšuje kompleksnost upravljanja;
- ponuja enoten uporabniški grafični vmesnik;
- omogoča krajše čase implementacij vseh varnostno usmerjenih funkcij;
- privzeto omogoča kompatibilnost samih funkcionalnosti;
- omogoča poenostavljeno nadgrajevanje sistemske programske opreme.

Vse te funkcije zmanjšujejo vektor napada (ang. *vector of attack*) in povečujejo stopnjo varnosti. Po drugi strani pa zbuja skrb ravno dejstvo, da en sam proizvajalec zagotavlja tako širok nabor varnostno usmerjenih funkcij. Poleg tega ima večnamenska požarna pregrada še sledeče pomanjkljivosti:

- različne varnostne funkcije pogosto niso integrirane, npr. protivirusni sistem se ne zaveda sistema za preprečevanje vdorov;
- različne varnostno usmerjene funkcije so povezane zaporedno; posledično prihaja do bistvenega poslabšanja prepustnosti in povečanja latence (glej sliko 9);
- ena varnostna pomanjkljivost lahko kompromitira celotno napravo [22];
- da bi dosegli optimalen rezultat, je potreben kompromis med nivojem pregledovanja in propustnostjo sistema.



Slika 9: Zaporedno procesiranje prometa.

Zavoljo dodatnega zmanjšanja kompleksnosti vključujejo večnamenske požarne pregrade še številne druge funkcionalnosti, kot so razširjena podpora dinamičnim usmerjevalnim protokolom, dešifriranje prometa, prepoznava aplikacij, centralizirano poročanje in hramba dnevniških zapisov. Ob integraciji z aktivnim imenikom omogočajo filtriranje prometa tudi na podlagi uporabnika oz. uporabniške skupine, vendar je ta funkcionalnost navadno omejena le na nekatere varnostno usmerjene funkcije (spletni proksi).

2.7.8 Požarna pregrada naslednje generacije

Požarna pregrada naslednje generacije (ang. *next generation firewall* – NGFW) je odgovor na sodobne grožnje. Požarna pregrada naslednje generacije je nadgradnja večnamenske požarne pregrade. Pri tem pa ne gre za število varnostno usmerjenih funkcionalnosti, temveč za

medsebojno delovanje le-teh. Glavna prednost požarne pregrade naslednje generacije je, da so različne varnostno usmerjene funkcije popolnoma integrirane med seboj [23].

Nasprotno od večnamenske požarne pregrade, kjer je prepoznava aplikacije, uporabnika ali vsebine funkcionalni dodatek, je pri požarni pregradi naslednje generacije ravno to bistveno. Na primer pri večnamenski požarni pregradi, »*stateful packet filter*« funkcija dovoli uporabniški promet na vratih TCP 80 proti internetu. Ta promet se nato posreduje funkcionalnosti IPS, ki ugotovi, da gre za multimedijsko aplikacijo. Ponovno posreduje promet funkcionalnosti, ki preveri identiteto uporabnika. Naslednja funkcionalnost preveri kategorijo naslova URL in odloči, da ta ni dovoljena, zato filtrira promet. Požarna pregrada naslednje generacije v nasprotju s tem multiplicira promet in z vzporednim procesiranjem določi atribute, ki jih nato uporabi v procesu filtriranja. Na tak način bistveno zmanjša latenco procesiranja paketov.

Tako delovanje požarne pregrade je še posebej pomembno, ker današnje aplikacije uporabljajo različne tehnike, s katerimi si zagotavljajo povezljivost. Te tehnike so na primer uporaba pogosto odprtih vrat 53 (DNS), 80 (HTTP), 443 (HTTPS) ali spreminjanje vrat (ang. *port hopping*). Požarna pregrada naslednje generacije uporablja aplikacijske dekoderje, da neodvisno od uporabljenih transportnih vrat določi aplikacijo. Pomembno je tudi prepoznavanje mikro aplikacij oziroma različnih delov aplikacije. Ta granularnost omogoča, da na primer znotraj spletne aplikacije *Gmail* posamično filtriramo spletni klepet ali nalaganje priponk, dovolimo pa pregledovanje elektronske pošte. S pomočjo kategorizacije lahko filtriramo vse (mikro) aplikacije, ki imajo skupno lastnost, kot je na primer ta, da omogočajo prenašanje datotek.

Delovanje orientirano na aplikacijo in visoka stopnja integracije omogočata tudi veliko boljšo izrabo ne varnostno orientiranih funkcionalnosti, kot so pogojno usmerjanje, izraba pasovne širine ali zagotavljanje kvalitete storitev.

Požarna pregrada naslednje generacije poleg hevristike in statistične analize uporablja različne podpise za odkrivanje. Le-ti so sledeči:

- podpisi aplikacij ali mikro aplikacij,
- podpisi zaupnih informacij (korporativnih skrivnosti, osebnih podatkov, podatkov strank),
- podpisi sistemov poveljevanja in kontrole (ang. *command and control*),
- podpisi varnostnih ranljivosti,

- podpisi vohunskega programja,
- podpisi trojanskih konjev,
- podpisi virusov in druge škodljive kode.

Kljub številnim prednostim imajo požarne pregrade naslednje generacije določene slabosti. Te so sledeče:

- paralelno procesiranje zahteva specifične strojne vire;
- če želimo promet pregledati z vzorci, moramo določen del prometa spustiti skozi požarno pregrado;
- aplikacijski dekoderji morajo neprestano slediti spremembam aplikacij;
- visoka cena požarnih pregrad.

V kombinaciji s primerno mrežno topologijo, dešifriranjem SSL in prilagodljivimi aplikativnimi podpisi omogoča požarna pregrada naslednje generacije transparenten pregled nad mrežnim prometom.

2.7.9 Specializirana požarna pregrada

Specializirana požarna pregrada deluje na aplikacijski plasti modela OSI in skrbi za zaščito specifičnih storitev. Tipično gre za varnostno utrjevanje proti internetu objavljenih storitev. V primerjavi z aplikacijskim prehodom delujejo specializirane požarne pregrade s proksijem, namenjenim za točno določen protokol in tip podatkov [24]. Te požarne pregrade delujejo po principu »vse kar ni eksplicitno dovoljeno, je prepovedano«. Na primer, požarna pregrada za zaščito spletne storitve (ang. *web application filter* – WAF) za vsako formo dopušča le vnaprej določen vzorec podatkov. Specializirana požarna pregrada striktno sledi zahtevam protokola.

2.8 Kronološki pregled mrežnih požarnih pregrad

Za boljše razumevanje razvoja je v nadaljevanju naveden kronološki pregled razvoja mrežnih požarnih pregrad.

2.8.1 Obdobje od 1987 do 1994

To obdobje predstavlja prvi raziskovalni val na področju varovanja računalniških omrežji. Predhodniki požarnih pregrad so bili usmerjevalniki – prve naprave, ki so ločevale različna

omrežja. Namenjeni so (bili) tako za povezovanje različnih omrežij, kot za razdeljevanje večjih omrežij na podomrežja. V začetku niso opravljali varnostnih funkcij, temveč so služili za zmanjševanje problemov, tako da so »glasnim« aplikacijam omejili prelivanje na celotno omrežje [7]. Na nek način so reševali problem različnih administrativnih domen, kjer so lokalni administratorji samovoljno uvajali različne, ne redko tudi problematične aplikacije [1]. Ti usmerjevalniki so z implementacijo omejevanja paketov postali filtri paketov. Leta 1989 je Jeffrey Mogul zasnoval prvo generacijo požarnih pregrad (filter paketov) imenovano *Screend* [24]. Leta 1991 je Marcus Ranum izumil požarno pregrado – aplikacijski prehod, ki temelji na uporabi aplikativnih proksijev. Le-ta je bila kot prva komercialna izvedenka požarne pregrade tržena pod imenom *DEC SEAL* [1]. Šlo je za hibrid, saj se je uporabila kombinacija aplikativnih proksijev in filtriranja paketov. Istega leta sta Steve Bellovin in Bill Cheswick iz *AT&T* izumila »*circut relay«* napravo imenovano »*Raptor Eagle«*. Ker je temeljila na proksiju TCP, je bilo takšno požarno pregrado lažje integrirati v omrežje, kot požarno pregrado *DEC SEAL*.

Leta 1993 Marcus Ranum in Frederick Avolio izdata množico pripravljenih rutin za izdelavo različnih aplikacijskih proksijev imenovano »*Trusted Information Systems«* (TIS). S tem se je razvoj razdelil med požarne pregrade, ki temeljijo na »*stateful packet filtering«* tehnologiji in na tiste, ki temeljijo na aplikacijskih proksijih.

Leta 1994 podjetje Check Point na tržišče postavi požarno pregrado z imenom Firewall-1. Gre za »*stateful inspection«* požarno pregrado, ki je poleg filtra paketov prva, ki je za uporabnika transparentna. Novost je tudi administracija z uporabo grafičnega uporabniškega vmesnika (ang. *graphical user interface* – GUI). Tudi zaradi bistveno večjih zmogljivosti predstavlja alternativo aplikacijskemu prehodu [24].

2.8.2 Obdobje od 1995 do 2004

V obdobju od 1995 do 2004 se požarnim pregradam dodajajo mnoge druge funkcionalnosti, kot so VPN (požarna pregrada *Interlock* podjetja *ANS*), zagotavljanje kvalitete storitve, filtriranje URL, sistemi odkrivanja in preprečevanja vdorov ter funkcionalnost protivirusne zaščite.

Večina požarnih pregrad so hibridi med »*stateful packet filter«* ali »*stateful inspection«* in aplikacijskim prehodom. Večina proizvajalcev sledi trendu, ki ga je postavilo podjetje *Check Point*. Alternativo predstavljajo požarne pregrade, ki temeljijo na aplikacijskih prehodih.

V poznih devetdesetih se pojavijo specializirane požarne pregrade, kot so produkti za zaščito specifičnih storitev. Leta 1997 se pojavi *rWeb* in leta 1999 se pojavi *AppShield*.

V požarne pregrade se implementira vse več funkcionalnosti in s prodajnega področja se začnejo pojavljati marketinško naravnana poimenovanja, kot so npr. DPI in UTM. Tehnologija DPI se razvije kot posledica vse večjega števila varnostnih groženj ter napadov na aplikacijski plasti. Leta 2003 podjetje *Internet Security Systems* predstavi prvo požarno pregrado DPI – *Proventia*. V istem letu sledita s svojimi rešitvami še podjetji *Symantec* in *Cisco*. Tehnologija DPI postavi osnovo za razvoj požarnih pregrad UTM in kasneje NGFW. Podjetje Gartner, ki se ukvarja z analizo trga, začne leta 2003 omenjati požarno pregrado naslednje generacije. Leta 2004 podjetje *IDC* predstavi prvo večnamensko požarno pregrado. Naprave UTM lahko z uporabo spletnega proksija filtrirajo promet glede na uporabnika. Več proizvajalcev integrira sisteme za preprečevanje vdorov v svoje požarne pregrade DPI in UTM. Med drugimi to storita tudi podjetji *Snort* in *Squid.*

2.8.3 Obdobje od 2005 do 2016

Po razcvetu številnih naprav UTM se pokažejo predvsem performančne slabosti in številne omejitve pri pregledovanju prometa na aplikativni plasti. S pomočjo konzorcija *Web Application Security Consortium* se leta 2006 definira požarna pregrada WAF in s tem se poveča njena prisotnost na tržišču. Leta 2008 podjetje *Palo Alto Networks* objavi prvo različico požarne pregrade naslednje generacije. Ta rešuje številne performančne težave požarnih pregrad UTM, dodaja integracijo funkcionalnosti, granularnejšo kontrolo in vpogled v mrežni promet. Prvič je mogoča manipulacija prometa glede na uporabnika, vrsto podatkov ali aplikacije. V letu 2009 tudi *Gartner* definira termin »požarna pregrada naslednje generacije« [23]. V letu 2012 se na tržišču požarnih pregrad naslednje generacije pojavijo tudi drugi proizvajalci, kot so *SonicWALL, Fortinet* in *Check Point*. Leta 2013 podjetje *Cisco* kupi *Sourcefire,* proizvajalca naprav IPS, z namenom, da vstopi na tržišče požarnih pregrad naslednje generacije s produktom *Firepower*. Integracija je še v teku. Vse bolj je prisotna tudi specializirana požarna pregrada v izvedenki požarna pregrada podatkovne baze (ang. *Database Firewall* – DBF). Gartner v letu 2016 prepozna podjetje *Palo Alto Networks* tudi kot vodilno na področju požarnih pregrad naslednje generacije. Številni proizvajalci tržijo svoje požarne pregrade UTM kot požarne pregrade naslednje generacije.

2.9 Funkcionalnosti sodobnih požarnih pregrad

Glavna funkcionalnost sodobnih požarnih pregrad je filtriranje prometa, ki pa še zdaleč ni edina. Tekom razvoja so proizvajalci v svoje produkte vgradili številne funkcionalnosti. Kljub različnim pristopom pa se je izkazalo, da nihče ne želi zaostajati za konkurenco, zato lahko danes zaznamo zelo podoben nabor funkcionalnosti pri vsakemu izmed njih.

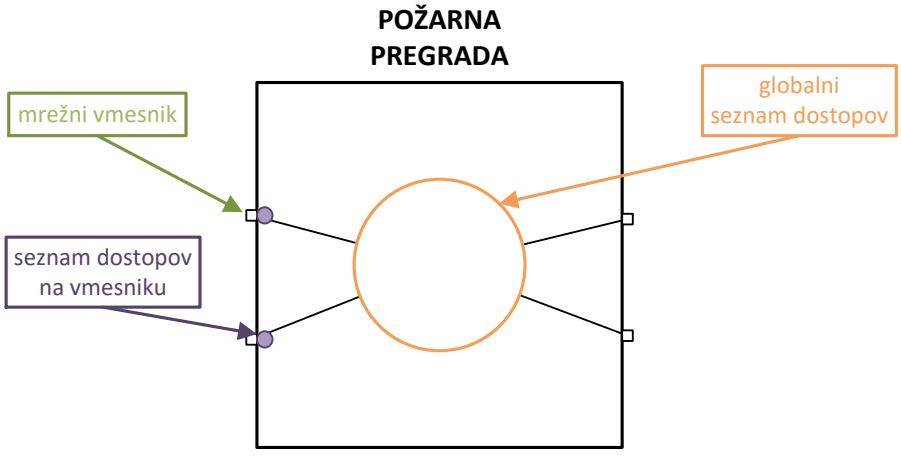
2.9.1 Filtriranje prometa

Požarna pregrada v primeru klasičnega filtriranja uporablja naslednje podatke:

- izvorni naslov IP,
- ciljni naslov IP,
- vrsto protokola,
- izvorno številko vrat (v primeru protokola TCP ali UDP),
- ciljno številko vrat (v primeru protokola TCP ali UDP).

Tipični ukazi pravil so »dovoli« ali »zavrzi«. Z njimi administrator opiše podatkovne povezave in sestavi seznam oziroma politiko dostopov. Običajno velja, da požarna pregrada filtrira promet tako, da zgoraj naštete parametre prometa primerja s prvim zapisom s seznama dostopov. V primeru, da ne najde ujemanja, nadaljuje s primerjanjem drugega zapisa in tako naprej vse do konca seznama dostopov. Ko se promet »ujame« v zapis, se zanj izvede preddefinirana akcija. Če promet ni opisan v seznamu dostopov, velja privzeto pravilo »zavrzi«.

Pri požarnih pregradah se srečujemo z različnimi implementacijami politike dostopov. Pri nekaterih so seznami dostopov pripeti na vmesnike požarne pregrade. Druge implementacije uporabljajo globalni seznam dostopov (glej sliko 10). Posledično tak seznam dostopa dobi, poleg zgoraj naštetih, dva nova podatka in sicer izvorni mrežni vmesnik in ciljni mrežni vmesnik.



Slika 10: Dva tipa seznamov dostopa.

Moderne implementacije uporabljajo varnostne cone, ki vsebujejo enega ali več različnih (fizičnih, logičnih ali navideznih) vmesnikov. To omogoča večjo fleksibilnost pri izbiri mrežne topologije, olajša administracijo in poveča preglednost konfiguracije. V tem primeru se seznamu dostopa dodata še podatka o izvorni varnostni coni in o ciljni varnostni coni.

2.9.1.1 Filtriranje uporabnikov oz. skupin

Administratorji se pogosto soočajo s težavo, da je uporabniškim napravam s protokolom DHCP (*Dynamic Host Configuration Protocol)* večinoma dodeljen dinamični naslov IP. Če želimo politiko filtriranja prilagoditi glede na uporabnika, je ena izmed rešitev uporaba statičnih rezervacij in s tem predvidljivega dodeljevanja naslovov IP. Ta rešitev se pogosto izkaže za nezadostno, saj se je v zadnjih letih močno povečalo število brezžičnih in mobilnih naprav. Zaradi nekonstantnosti inventarja in kompleksnega upravljanja so proizvajalci požarnih pregrad izbrali drugačno rešitev. Večina korporacij namreč v svoji informacijski infrastrukturi uporablja centralni imenik uporabnikov. Tega požarna pregrada uporabi kot zunanji vir informacij, s katerim omogoča preslikavo med uporabnikom (uporabniškim računom) in naslovi IP, ki jih uporablja. Če centralni imenik uporabnikov omogoča združevanje v skupine, jih lahko, podobno kot uporabnika, namesto naslova IP, uporabimo v politiki filtriranja. Seznam dostopa dobi nov podatek o uporabniškem računu ali uporabniški skupini.

2.9.1.2 Filtriranje aplikacij

Sodobne požarne pregrade z aplikacijskimi dekoderji določijo tip oziroma del aplikacije, ki ga pogosto imenujemo mikro aplikacija. Proizvajalci združujejo aplikacije v skupine, ki imajo s stališča varovanja omrežja podobno lastnost, na primer aplikacije, ki omogočajo oddaljeno administracijo ali aplikacije, ki so zadolžene za posodobitve programske opreme [25]. Proizvajalec požarne pregrade mora zagotavljati ustreznost in posodobitve aplikacijskih podpisov. V primeru, da v omrežju obstaja aplikacija, za katero proizvajalec nima podpisa, mora požarna pregrada imeti možnost, da podpis administrator ustvari sam. Seznam dostopa dobi nov podatek o aplikaciji oziroma skupini aplikacij.

2.9.1.3 Filtriranje URL

Funkcionalnost filtriranja URL deluje tako, da požarna pregrada prestreza zahteve protokola HTTP. Pridobljeni naslov URL primerja s podatkovno bazo, kjer se nahaja tudi podatek o kategoriji URL. Odvisno od proizvajalca ima požarna pregrada različno število preddefiniranih kategorij URL. Najpogostejše so novice, finance, erotične vsebine, orožje, multimedija, socialna omrežja itd. Korporativne politike tipično definirajo primerne in neprimerne vsebine. Seznam dostopa dobi nov podatek o naslovu URL ali o skupini URL.

2.9.2 Prevajanje mrežnih naslovov

Prevajanje mrežnih naslovov rešuje več problemov. Le ti so sledeči:

- skrivanje naslovov notranjih segmentov,
- zagotavljanje povezljivosti, kljub prekrivanju naslovov IP,
- reševanje problemov z usmerjanjem,
- omogočanje delovanja interneta kljub pomanjkanju naslovov IPv4.

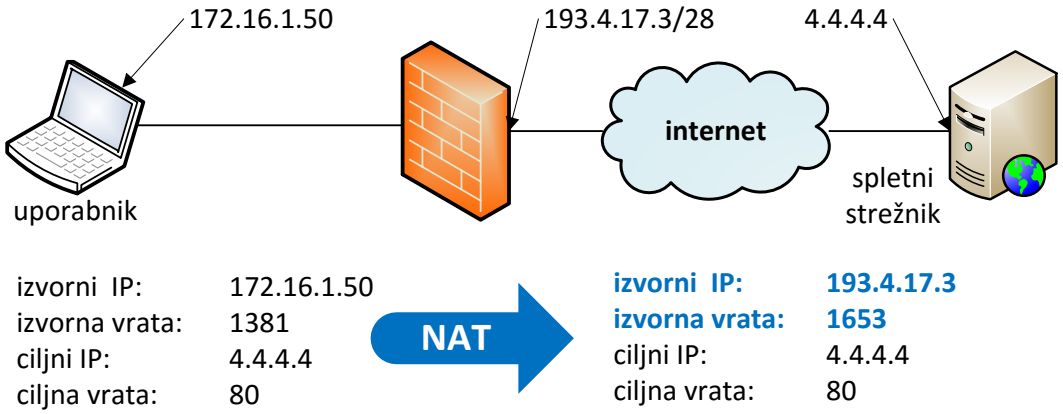
Funkcionalnost NAT omogoča zamenjavo katerega koli od sledečih podatkov:

- izvorni naslov IP,
- ciljni naslov IP,
- izvorno številko vrat,
- ciljno številko vrat.

Implementacija NAT je zelo odvisna od posebnosti posamičnega omrežja (topologije, usmerjanja, števila VPN povezav itd.). Najpogosteje se uporabljata sledeči dve različici implementacij:

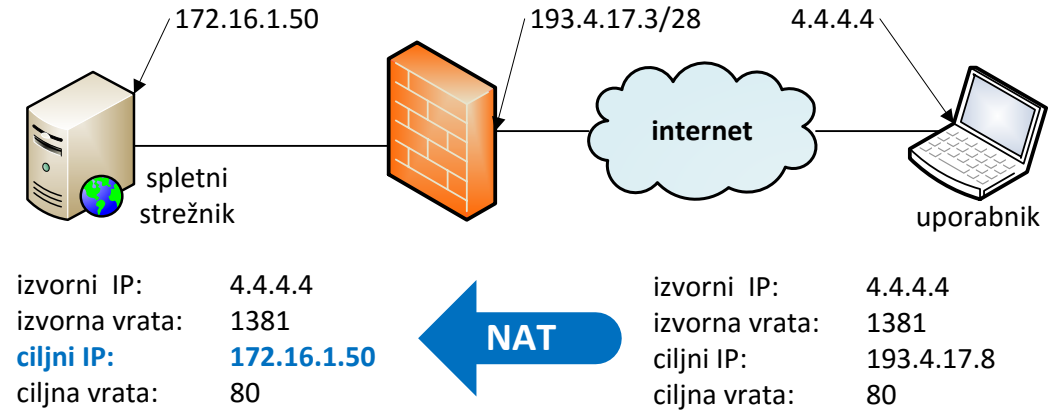
- NAT izvornega naslova, pri čemer se množica naslovov prevede v enega. V notranjih mrežnih segmentih se praviloma uporablja privatne naslove IP iz treh območji [26]:
  - 10.0.0.0 - 10.255.255.255,
  - 172.16.0.0 - 172.31.255.255,
  - 192.168.0.0 - 192.168.255.255.

  Ko želi odjemalec iz notranjega omrežja dostopati do vira na internetu, izvede požarna pregrada prevod njegovega izvornega naslova IP (in izvorne številke vrat v primeru protokola TCP ali UDP) v enega od javnih naslovov IP (in naključne številke vrat) (glej sliko 11). Požarna pregrada vsak prevod zapiše v pomnilnik in ga v obratni smeri uporabi pri povratnem prometu.



Slika 11: NAT izvornega naslova.

- NAT ciljnega naslova se uporablja v primeru, ko imamo v enem izmed notranjih mrežnih segmentov storitev, ki jo želimo objaviti v javnemu omrežju. Požarna pregrada prejme odjemalčevo zahtevo po storitvi in prevede ciljni javni IP naslov v pravega privatnega (glej sliko 12). Shranjeni prevod v obratni smeri uporabi pri povratnem prometu.



Slika 12: NAT ciljnega naslova.

2.9.3 Usmerjanje

Požarne pregrade v korporativnih omrežjih pogosto nastopajo kot naprave z vlogo na tretji plasti modela OSI. Požarna pregrada tipično zmore usmerjati promet med lokalno povezanimi mrežnimi segmenti. V primeru ne-lokalnih mrežnih segmentov mora mrežni administrator ročno vpisati naslednjo napravo, preko katere je določeno omrežje dosegljivo. Usmerjanju po principu ročno vpisanih poti pravimo tudi statično usmerjanje.

Dinamične protokole navadno uporabljamo v večjih omrežjih, saj se le-ta pogosto spreminjajo. Razlogi so različni - od načrtovanih sprememb do okvare mrežnih elementov. Dinamični usmerjevalni protokoli omogočajo samodejne reakcije na spremembe mrežne topologije, kar pripomore k večji zanesljivosti. Delujejo tako, da z napravami, ki so udeležene v proces, izmenjujejo informacije o dosegljivosti mrežnih segmentov. Sodobne požarne pregrade poznajo naslednje usmerjevalne protokole:

- *Routing Information Protocol* (RIP),
- *Open Shortest Path First* (OSPF),
- *Border Gateway Protocol* (BGP).

2.9.4 Navidezna privatna omrežja

Ena izmed pogosto uporabljenih funkcionalnosti požarnih pregrad je tehnologija navideznih privatnih omrežij. Ta omogoča povezovanje različnih delov omrežja preko omrežij, ki jim ne zaupamo (javna omrežja – internet).

Klub temu, da obstaja večje število protokolov VPN, se večinoma uporabljajo tisti, ki s šifriranjem zagotavljajo varen prenos podatkov. Če je tako zavarovan tunel VPN na prenosni poti prestrežen, je vsebina neberljiva. Najpogostejša primera uporabe navideznega privatnega omrežja sta povezava oddaljenih lokacij in oddaljeni dostop.

2.9.4.1 Povezava oddaljenih lokacij

Tipični primer je izpostava z informacijsko infrastrukturo, ki se nahaja na centralni lokaciji. Na obeh lokacijah je potrebna naprava, ki ima podporo funkcionalnosti VPN. Industrijski standard je *IPSec*. Za overjanje se najpogosteje uporablja vnaprej dogovorjen šifrirni ključ. Če vsi parametri ustrezajo, se med lokacijama vzpostavi šifriran tunel. V kombinaciji z usmerjanjem je za odjemalca uporaba storitev transparentna.

2.9.4.2 Oddaljeni dostop

Ta dostop se najpogosteje uporablja za oddaljeno delo ali oddaljeno administracijo. Podobno kot pri povezavi oddaljenih lokacij gre tudi pri oddaljenem dostopu za vzpostavitev tunela VPN, s to razliko, da v tem primeru na odjemalčevi strani ni fizične požarne pregrade, temveč je povezava realizirana z uporabo odjemalca VPN. Pri oddaljenem dostopu je v porastu uporaba šifrirne tehnologije SSL. Za overjanje se uporabljajo različni mehanizmi. Ti so sledeči:

- uporabniško ime in geslo,

- overjanje z uporabo generatorja naključnih gesel,
- biometrični podatki,
- overjanje s certifikati.

Ko gre za korporativne prenosnike, se vse pogosteje uporablja pristop, pri katerem se povezava VPN vzpostavi avtomatično vsakič, ko je uporabnik izven službenega omrežja. Na tak način se zagotavlja varen dostop do spleta.

2.9.5 Zaščita pred zlonamerno kodo

Za zaščito pred zlonamerno kodo se pretežno uporabljajo tehnike izposojene iz tehnologije IPS (iskanje vzorcev). Za razliko od predhodnikov iščejo sodobne požarne pregrade vse znane oblike zlonamerne kode (črve, viruse, trojanske konje, izrabo ranljivosti, promet kontrolnih centrov, preplavljanje medpomnilnika, itd.). V politiki zaščite pred zlonamerno kodo se glede na stopnjo grožnje določi primerno reakcijo. Ta proces od administratorja zahteva precejšnjo pozornost, saj vedno obstaja možnost lažno pozitivnih dogodkov. V nasprotnem primeru požarna pregrada prekine povezavo, ko odkrije katero izmed oblik zlonamerne kode.

2.9.6 Nadzorovano okolje za preizkus programja

Nadzorovano okolje za preizkus programja (ang. *sandbox*) služi za odkrivanje zlonamerne kode, za katero v danem trenutku še ni podpisa. Znano je, da proizvajalci protivirusne programske opreme od trenutka prve indikacije potrebujejo več dni, da izdelajo podpis [27]. V okolju »*sandbox*« se simulira zagon programja in opazuje morebitno delovanje, ki je tipično za škodljivo kodo.

Funkcionalnost je v večini tesno povezana s storitvijo, ki jo nudi proizvajalec. Ko požarna pregrada zazna datoteko, izračuna njeno zgoščeno vrednost (ang. *hash*) in to vrednost primerja z lokalno bazo zgoščenih vrednosti. Tu dobi podatek o morebitni škodljivosti. Če »*hash*« vrednosti ni v lokalni bazi, pošlje celotno datoteko v proizvajalčev »*sandbox*« v analizo. Vrnjene vrednosti so lahko sledeče:

- datoteka je benigna ali
- datoteka je maligna.

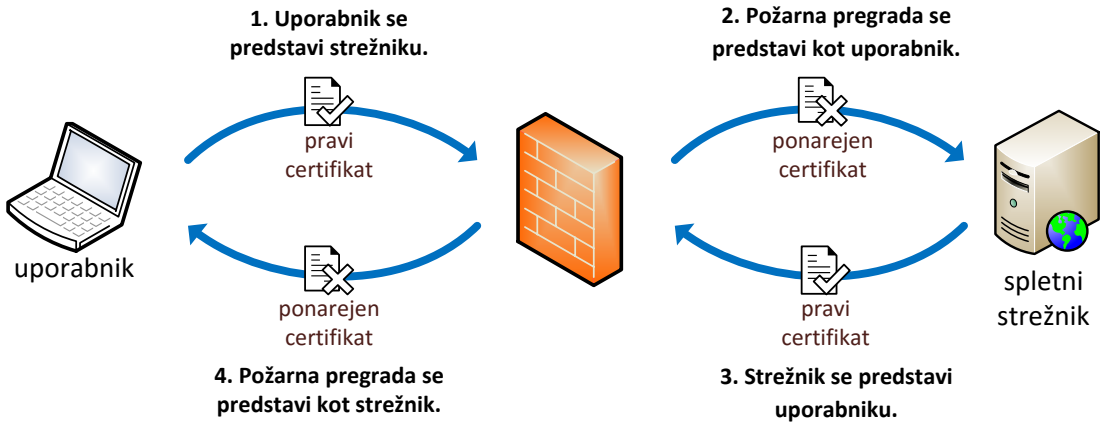
Pridobljena vrednost se zabeleži v dnevniškem zapisu požarne pregrade. Po potrebi se sproži postopek obveščanja. Pogosto imajo finančne institucije z varnostno politiko prepovedano

pošiljanje datotek izven lastnega omrežja. Proizvajalci mrežnih požarnih pregrad ta problem naslavljajo z namenskimi sistemi, ki omogočajo lokalno okolje »*sandbox*«.

2.9.7 Dešifriranje SSL

Požarna pregrada lahko izvaja napredne oblike filtriranja samo s prometom, ki ga lahko interpretira. Ne more filtrirati na podlagi vsebine, če je promet zaščiten s šifriranjem. To izrabljajo tudi pisci zlonamerne programske kode. Ena od napovedi za konec leta 2016 predvideva, da bo s tehnologijo SSL ali tehnologijo TLS (Transport Layer Security) zaščitenega kar 70% prometa [28].

Sodobna požarna pregrada dešifrira zaščiten promet z uporabo proksija SSL. Glede na politiko dešifriranja SSL prestreže požarna pregrada odjemalčevo zahtevo, ponaredi certifikat in se mu predstavi kot ciljni strežnik. Podobno se strežniku predstavi s ponarejenim certifikatom odjemalca (glej sliko 13). Da bi odjemalec zaupal ponarejenemu certifikatu strežnika, mu je potrebno naložiti korenski certifikat, ki ga za ponarejanje uporablja požarna pregrada.



Slika 13: Štiri faze dešifriranja SSL.

V primerih, ko tudi strežnik preverja identiteto odjemalca (spletno bančništvo, dostop do portalov sodstva ali drugih državnih organov), tak način dešifriranja SSL ne deluje. V takem primeru je potrebno definirati izjeme, za katere se dešifriranje SSL ne izvaja.

Poglavje 3 Predstavitev problema

Pričujoče poglavje na primeru hipotetičnega naročnika rešitve opisuje problem varnega in učinkovitega dostopa do interneta za uporabnike. V prvem podpoglavju je opisan hipotetični naročnik, njegove zahteve in cilji. Drugo podpoglavje analizira promet oziroma aplikacije in jih obravnava z vidikov varnosti in porabe pasovne širine. V tretjem podpoglavju je povzetek zahtev, ki vključuje analizo prometa in aplikacij.

3.1 Opis hipotetičnega naročnika

Hipotetični naročnik (v nadaljevanju Naročnik) želi svojim uporabnikom omogočiti dostop do interneta. Posebno skrb namenja zaščiti delovnih postaj, ki naj bodo varovane s sodobnimi funkcijami požarne pregrade naslednje generacije. Pri tem skuša doseči sledeče cilje:

- preprečevanje uporabe ne varnih aplikacij;
- pregledovanje prometa, šifriranega s tehnologijo SSL;
- zaščito pred zlonamerno kodo.

Poleg tega se Naročnik želi zavarovati pred (ne)namernim odtekanjem intelektualne lastnine. Skrb predstavljajo številne storitve v oblaku, ki so namenjene izmenjavi datotek (*Dropbox*, *Box*, *Google Drive*, *WeTransfer* itd.). Za interno bazo uporabnikov se uporablja aktivni imenik. Uporabniki s specifičnimi potrebami so v strukturi aktivnega imenika včlanjeni v različne organizacijske enote. Te so sledeče:

- *razvoj,*
- *IT,*
- *trženje*.

Če uporabnik nima specifičnih potreb, je včlanjen v krovno skupino *vsi uporabniki*. Z vidika upravljanja požarne pregrade in preglednosti politik Naročnik želi, da se filtriranje mrežnega prometa izvaja na podlagi aplikacij in na podlagi uporabnika, oziroma članstva v skupini

aktivnega imenika. Želja Naročnika je tudi, da je rešitev za uporabnika kar se da transparentna. Z vidika učinkovitosti naj se omejuje poraba pasovne širine aplikacijam, ki prenašajo vizualne medijske vsebine. Te aplikacije naj za prenos podatkov ne uporabijo več kot 20 Mb/s.

Cilj je doseči rešitev, ki bo uporabnikom omogočala varen dostop do zunanjih storitev z upoštevanjem vseh želja Naročnika in upoštevanjem analize prometa. Doseči je potrebno kompromis med varovanjem omrežja in dostopnostjo spletnih virov.

3.2 Analiza prometa oziroma aplikacij

Za izvedbo rešitve je zelo pomembna analiza prometa. Potrebno je identificirati nezaželene, potencialno škodljive aplikacije in aplikacije, potrebne za opravljanje dela. Upoštevati je potrebno tudi, da imajo različne skupine uporabnikov tudi različne potrebe. Da bi se določilo politiko filtriranja, je najprej potrebno poiskati presek med zahtevami Naročnika, skupinami uporabnikov ter naborom aplikacij, ki so podprte s strani proizvajalca mrežne požarne pregrade – v našem primeru *Palo Alto Networks*. Proizvajalec podpira dobrih 2200 aplikacij. Te po različnih ključih deli v skupine s skupnimi lastnostmi. Delitev na kategorije in podkategorije je sledeča:

- poslovni sistemi:
  - storitve overjanja,
  - podatkovne baze,
  - načrtovanje virov podjetja in upravljanje odnosov s strankami,
  - splošno poslovno,
  - upravljanje,
  - trženje,
  - pisarniški programi,
  - razvoj programske opreme,
  - posodabljanje programske opreme,
  - zaščita podatkovne shrambe;
- sodelovanje:
  - spletna pošta,
  - takojšnje sporočanje,
  - spletno konferiranje,
  - poslovno mreženje,

  - socialno mreženje,
  - avdio in video komunikacija,
  - spletno objavljanje;

- splošno internet:

  - izmenjava datotek,
  - spletni pripomočki;

- multimedija:

  - pretakanje zvoka,
  - igranje,
  - slike in video;

- povezovanje:

  - šifriran tunel,
  - infrastruktura,
  - protokoli IP,
  - proksi,
  - oddaljen dostop,
  - usmerjanje.

Proizvajalec deli aplikacije še po stopnji rizika (od 1 do 5), po tehnologiji (brskalnik, odjemalec-strežnik, mrežni protokol, odjemalec-odjemalec) in po posebnih karakteristikah aplikacij. Te so sledeče:

- aplikacije se izmikajo,
- visoka poraba pasovne širine,
- možnost zlorabe,
- programska oprema kot storitev,
- aplikacije prenašajo datoteke,
- aplikacije prenašajo druge aplikacije,

- aplikacije uporablja škodljiva koda,
- aplikacije so varnostno pomanjkljive,
- aplikacije so v široki rabi.

Aplikacije je mogoče združevati v dinamične skupine. To pomeni, da so v skupini aplikacije, ki jim pripada določena lastnost ali celo kombinacija lastnosti. Primer takšne skupine bi vseboval aplikacije, ki so v podkategoriji *igranje* in imajo stopnjo rizika večjo ali enako štiri. Dinamične skupine aplikacij se lahko uporabi tudi v politiki filtriranja. Dobra stran takega pristopa je, da ko proizvajalec doda novo aplikacijo (igro) z enako stopnjo rizika, se tudi ta samodejno upošteva v politiki filtriranja.

Z vidika varnosti in skladno z zahtevami Naročnika so identificirane skupine aplikacij, ki predstavljajo največje tveganje. Razen izjem (te so večinoma vezane na uporabniško skupino) naj bo uporaba sledečih podskupin aplikacij onemogočena:

- Podkategorija aplikacij *šifriran tunel*. Če želi požarna pregrada izvajati varnostne funkcionalnosti (filtriranje aplikacij, pregledovanje za škodljivo kodo) mora imeti vpogled v vsebino podatkov. To ni mogoče, če je promet šifriran. Najpogosteje uporabljene aplikacije v tej podkategoriji so sledeče:
  - *hola-unblocker*,
  - *ipsec*,
  - *tunnelbear*,
  - *ssl*,
  - *hamachi*.

  Aplikacije, ki so v tej podkategoriji in naj bodo dovoljene:

  - *ssl* – za skupino *vsi uporabniki*,
  - *cisco VPN*, *ipsec*, *openVPN* – za skupino *razvijalci,*
  - *ssh* – za skupino *IT.*

- Podkategorija aplikacij *izmenjava datotek*. Te predstavljajo grožnjo odtekanja intelektualne lastnine. Najpogosteje uporabljene aplikacije v tej podkategoriji so:
  - *bittorrent*,
  - *dropbox*,
  - *google-cloud-storage*,

- *ms-onedrive*,
- *rapidshare*,
- *yousendit*.

Aplikacije, ki so v tej podkategoriji in naj bodo dovoljene:

- *bittorrent*, *bittorrent-sync* – za skupino *IT*,
- *facebook-file-sharing* – za skupino *trženje*.

- Podkategorija aplikacij *proksi*. Uporaba proksija za Naročnika predstavlja grožnjo skrivanja identitete ali enkapsulacije drugih protokolov. Najpogosteje uporabljene aplikacije v tej podkategoriji so:

  - *avoidr*,
  - *bypass*,
  - *freegate*,
  - *http-proxy*,
  - *http-tunnel*.

- Podkategorija aplikacij *oddaljen dostop*. Te lahko omogočijo nenadzorovan dostop do uporabniških delovnih postaj. Najpogosteje uporabljene aplikacije v tej podkategoriji so:

  - *gotomypc*,
  - *logmein*,
  - *ms-rdp*,
  - *pcanywhere*,
  - *teamviewer*,
  - *vnc*.

  Aplikacije, ki so v tej podkategoriji in naj bodo dovoljene:

  - *ms-rdp*, *rlogin*, *vnc* – za skupini *razvijalci* in *IT*,
  - *telnet* – za skupino *IT*.

Aplikacije ostalih kategorij in podkategorij naj bodo dovoljene.

Z vidika učinkovitosti naj se omejuje poraba pasovne širine aplikacijam, ki so v podkategoriji *slike in video* in hkrati s karakteristiko *visoka poraba pasovne širine*. Najpogosteje uporabljene aplikacije, ki ustrezajo temu izboru, so sledeče:

- *facebook-video*,
- *google-picasa*,
- *google-video*,
- *http-video*,
- *netflix*,
- *popcorn-time*,
- *vimeo*,
- *youtube*.

3.3 Končne zahteve hipotetičnega naročnika

S pomočjo analize prometa in aplikacij je izveden presek med zahtevami Naročnika in podprtimi aplikacijami s strani proizvajalca mrežnih požarnih pregrad (glej tabelo 1). Aplikacije, ki niso eksplicitno definirane, naj bodo dovoljene.

eksplicitno dovoljene aplikacije	
skupina uporabnikov	aplikacija ali skupina(e) aplikacij
vsi uporabniki	*ssl*
trženje	*facebook-file-sharing*
razvoj	*ciscovpn*
	ipsec
	open-vpn
	ms-rdp
	rlogin
	vnc
IT	*ssh*
	bittorrent
	bittorrent-sync
	ms-rdp
	rlogin
	vnc
	telnet

eksplicitno prepovedane aplikacije	
vsi uporabniki	*šifriran tunel*
	izmenjava datotek
	proksi
	oddaljen dostop
aplikacije omejene s pasovno širino	
vsi uporabniki	*slike in video, visoka poraba pasovne širine*

Tabela 1: Uporaba aplikacij glede na skupino uporabnikov.

Naročnik poleg tega zahteva uporabo sledečih funkcionalnosti:

- filtriranje na podlagi aplikacij;
- filtriranje na podlagi članstva v skupini aktivnega imenika;
- dešifriranje uporabniškega prometa zaščitenega z SSL;
- uporaba storitve DHCP v uporabniškem segmentu;
- zaščita pred zlonamerno kodo;
- omejevanje pasovne širine.

Poglavje 4 Uporaba tehnologije NGFW za varen dostop uporabnikov do interneta

Pričujoče poglavje predstavlja primer rešitve za problematiko opisano v prejšnjem poglavju. Kljub temu, da je v rešitvi integriranih več gradnikov, je poudarek na mrežni požarni pregradi. Prvo podpoglavje definira načrt rešitve. V njemu so opisani koraki, ki so potrebni za izvedbo rešitve. Drugo podpoglavje opisuje učinkovito rešitev varnega dostopa do interneta. Ta je izvedena kot potrditev vzorčnega koncepta in uporablja vse elemente prave postavitve. Uporabljena je požarna pregrada naslednje generacije, model *PA-3020*, vodilnega proizvajalca *Palo Alto Networks*. Zadnje podpoglavje na kratko povzema rešitev problematike.

4.1 Načrt rešitve

Definirati je potrebno osnovne gradnike in razumeti njihove vloge. Prvi korak je definicija mrežne topologije. Glede na stopnjo ogroženosti je potrebna segmentacija omrežja na različne varnostne cone. Posamični varnostni coni je potrebno dodeliti mrežni vmesnik. Mrežnim vmesnikom je potrebno določiti naslov IP, profil upravljanja, virtualni usmerjevalnik in varnostno cono. Profil upravljanja določi storitve, ki jih požarna pregrada nudi na mrežnem vmesniku. Na vmesniku, ki je najbližje uporabnikom, je potrebno nastaviti storitev DHCP. Potrebno je določiti virtualni usmerjevalnik in pripadajoče statične usmerjevalne poti. Nastaviti je potrebno prevajanje izvornih naslovov. S politiko NAT se omogoči, da se izvorni, privatni naslovi IP dinamično prevajajo v javni naslov.

V drugem koraku je potrebno izvesti identifikacijo uporabnikov. Za delovanje le-te je potrebno omogočiti povezavo s sledečima zalednima storitvama:

- povezavo z aktivnim imenikom: tu je potrebno s seznama vseh skupin uporabnikov določiti tiste, ki so relevantne za uporabo v politikah požarne pregrade;
- povezavo z identifikacijskim agentom.

Tretji korak je nastavitev dešifriranja SSL. Potrebno je ustvariti certifikat s funkcijo CA (*certificate authority*). Temu je potrebno določiti vlogo v procesu dešifriranja SSL. Potrebno je

definirati skupino naslovov URL, za katero se dešifriranje ne bo izvajalo. Nato se ustvari politiko dešifriranja SSL, pri čemer je potrebno paziti na vrstni red pravil.

V četrtem koraku je potrebno ustvariti statične skupine, s katerimi se definira eksplicitno dovoljene aplikacije. Podobno je potrebno ustvariti dinamični skupini, s katerimi se zajame eksplicitno prepovedane aplikacije in aplikacije, za katere bomo izvajali omejitev pasovne širine. Slednje se izvede v treh korakih:

- s politiko QoS se klasificira mrežni promet;
- v profilu QoS se določi zgornjo vrednost porabe pasovne širine;
- profil QoS se namesti na zunanji in notranji mrežni vmesnik.

S politiko dostopov se določi promet, ki prehaja skozi mrežno požarno pregrado, pri čemer je potrebno paziti na vrstni red. Pravila je potrebno razvrstiti od bolj podrobnih proti manj podrobnim. Na začetku se definirana izjeme, nato prepovedane aplikacije in na koncu pravilo, ki dovoljuje vse aplikacije, ki niso eksplicitno določene.

V zadnjem koraku je potrebno nastaviti zaščito pred zlonamerno kodo. Glede na stopnjo varnostne grožnje in uporabljen protokol prenosa je potrebno definirati protivirusni profil in ustrezno obrambno akcijo. Podobno je potrebno definirati obrambne akcije in varnostna profila za preprečevanje vohunskega programja in za zaščito pred ranljivostmi. Te tri varnostne profile je potrebno združiti v skupino varnostnih profilov in jo aktivirati v politiki dostopov.

4.2 Izvedba rešitve

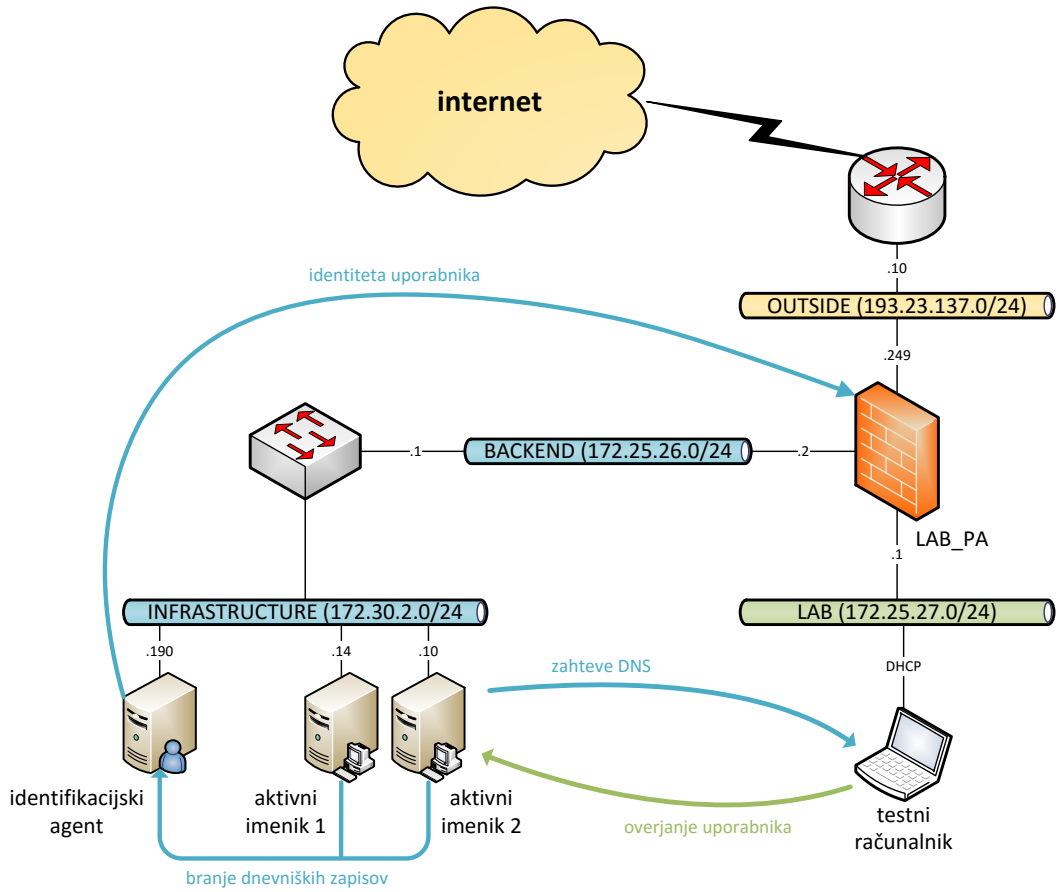
Konceptualna rešitev prikazuje uporabo in integracijo mrežne požarne pregrade z infrastrukturnimi gradniki informacijskega sistema. Izvedba rešitve upošteva vse zahteve in pričakovanja Naročnika in potrjuje delovanje vzorčnega koncepta. Osnovni gradniki rešitve so:

- požarna pregrada *LAB_PA*,
- strežnika *aktivni imenik 1* in *aktivni imenik 2*,
- *identifikacijski agent*,
- *testni računalnik*.

Kljub temu, da je gradnikov več, je opis rešitve osredotočen na mrežno požarno pregrado.

4.2.1 Mrežna topologija

Požarna pregrada logično razdeljuje omrežje na več varnostnih con, ki sovpadajo s segmentacijo omrežja (glej sliko 14). V coni *LAB* je uporabniško omrežje. V coni *BACKEND* je povezovalno omrežje, ki povezuje mrežni segment *INFRASTRUCTURE* in uporabniški segment. Cona *OUTSIDE* je namenjena dostopu do interneta.



Slika 14: Logična shema.

4.2.2 Mrežni vmesniki

Mrežni vmesniki imajo določen naslov IP, profil upravljanja, virtualni usmerjevalnik in varnostno cono (glej sliko 15).

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone	Features
ethernet1/1	Layer3	LAB_MP_OUTSIDE		193.23.137.249/24	LAB_VR1	OUTSIDE	
ethernet1/2	Layer3	LAB_MP		172.25.27.1/24	LAB_VR1	LAB	
ethernet1/3	Layer3	LAB_MP		172.25.26.2/24	LAB_VR1	BACKEND	

Slika 15: Mrežni vmesniki in pripadajoči atributi.

4.2.3 Profil upravljanja mrežnega vmesnika

Definirana sta profila upravljanja, ki omogočata storitve na mrežnem vmesniku (glej sliko 16).

Name	Ping	User-ID
LAB_MP_OUTSIDE	☑	☐
LAB_MP	☑	☑

Slika 16: Dovoljene storitve na fizičnih vmesnikih.

4.2.4 Storitev dinamičnega dodeljevanja naslovov IP

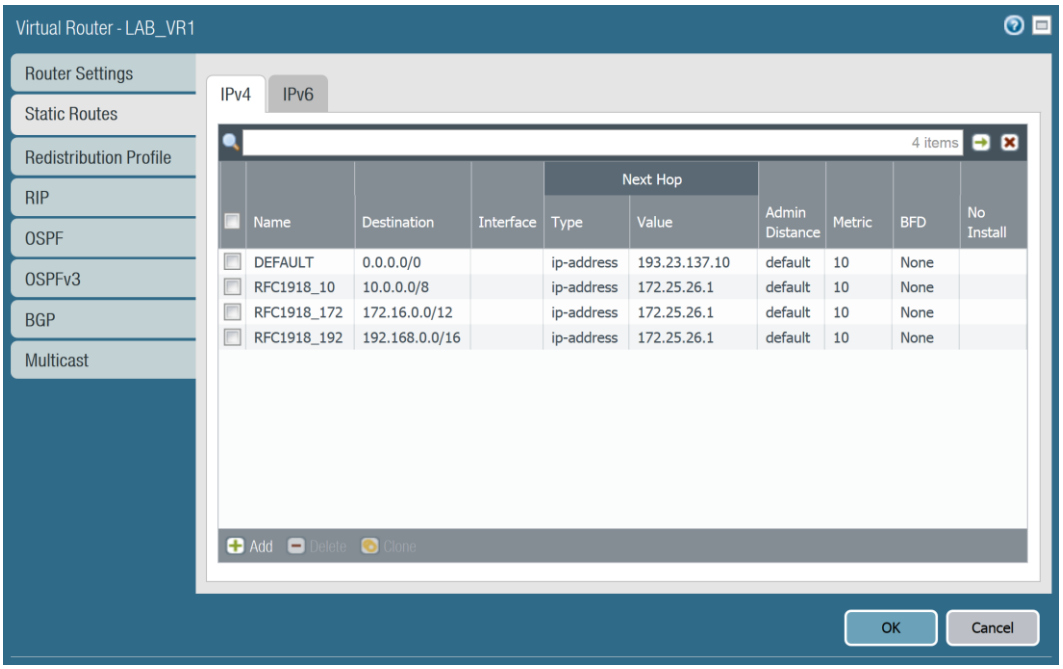
Storitev DHCP dodeljuje naslove IP v coni *LAB* (glej sliko 17).

Interface	Options	IP Pools
ethernet1/2	Lease: Unlimited DNS: 172.30.2.14,172.30.2.10 Gateway: 172.25.27.1	View Allocation 172.25.27.20-172.25.27.200

Slika 17: Nastavitve storitve DHCP.

4.2.5 Usmerjanje

Požarna pregrada je izvedena v usmerjevalnem načinu. Virtualni usmerjevalnik *VR1* je nastavljen s statičnimi usmerjevalnimi potmi in skrbi za usmerjanje med mrežnimi segmenti (glej sliko 18).



Slika 18: Statične usmerjevalne poti virtualnega usmerjevalnika *VR1*.

4.2.6 Prevajanje mrežnih naslovov

Nastavljeno je prevajanje izvornih naslovov, katerih izvor je cona *LAB* in cilj cona *OUTSIDE*. Notranji privatni naslovi se dinamično prevajajo v javni naslov IP (glej sliko 19).

	Name	Original Packet					Translated Packet
		Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation
1	NAT_INTERNET	LAB	OUTSIDE	any	any	any	dynamic-ip-and-port 193.23.137.249

Slika 19: Nastavitve politike NAT.

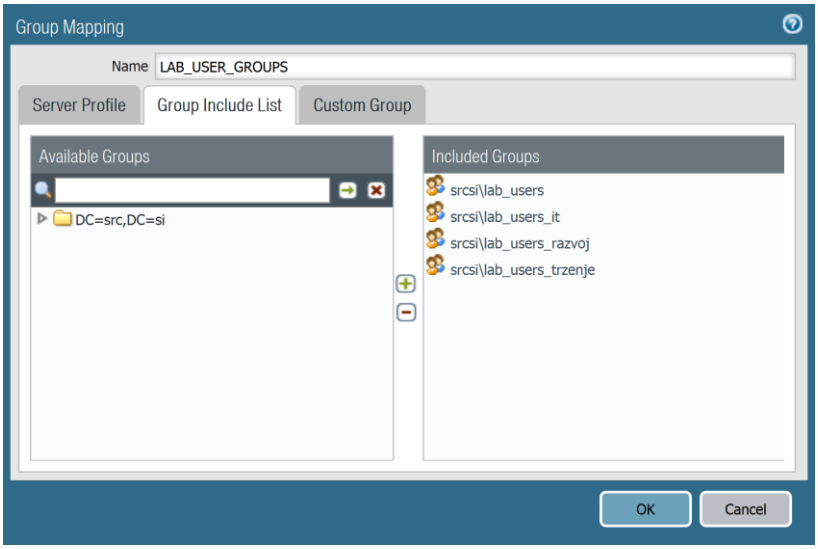
4.2.7 Identifikacija uporabnikov

Identifikacija uporabnikov zahteva integracijo z zalednimi storitvami. Prva od dveh je povezava z obema aktivnima imenikoma z uporabo protokola LDAP (*Lightweight Directory Access Protocol*) (glej sliko 20).

Name	Servers	Others
LAB_LDAP	Name: DC1 LDAP Server: 172.30.2.14 Port: 389 Name: DC2 LDAP Server: 172.30.2.10 Port: 389	Type: active-directory Base: DC=src,DC=si Bind DN: CN=SVC Palo Alto,OU=SRCSI-Services,DC=src,DC=si

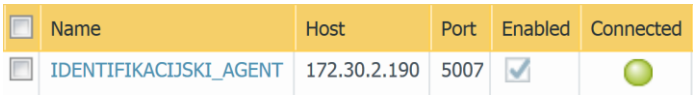
Slika 20: Nastavitve profila LDAP.

S profilom LDAP požarna pregrada dostopa do strukture uporabniških skupin in uporabniških računov v aktivnem imeniku. Določene so aktivne skupine uporabnikov (glej sliko 21).



Slika 21: Izbor aktivnih skupin uporabnikov.

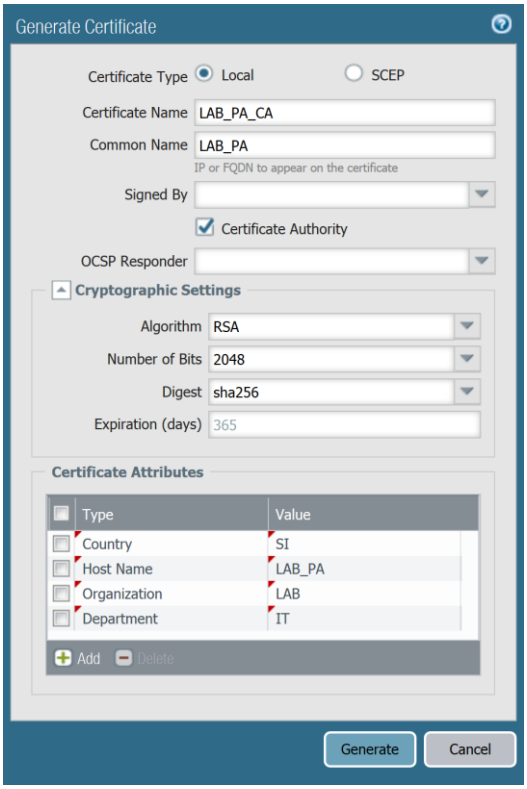
Drugi del identifikacije uporabnikov je integracija z *identifikacijskim agentom* (glej sliko 22). Ko se uporabnik prijavi v delovno postajo, se ta overi tudi na enemu od aktivnih imenikov. Ta dogodek se, skupaj z naslovom IP, zapiše v dnevniški zapis. *Identifikacijski agent* periodično bere te zapise in vzdržuje tabelo preslikav naslovov IP in uporabniških računov. Na požarni pregradi se nastavi povezava požarne pregrade z *identifikacijskim agentom*.



Slika 22: Povezava z *identifikacijskim agentom*.

4.2.8 Dešifriranje SSL

Za potrebe funkcionalnosti dešifriranja SSL je ustvarjen certifikat s funkcijo CA (glej sliko 23). Ta je potrebna za nadaljnje ustvarjanje ponarejenih certifikatov.



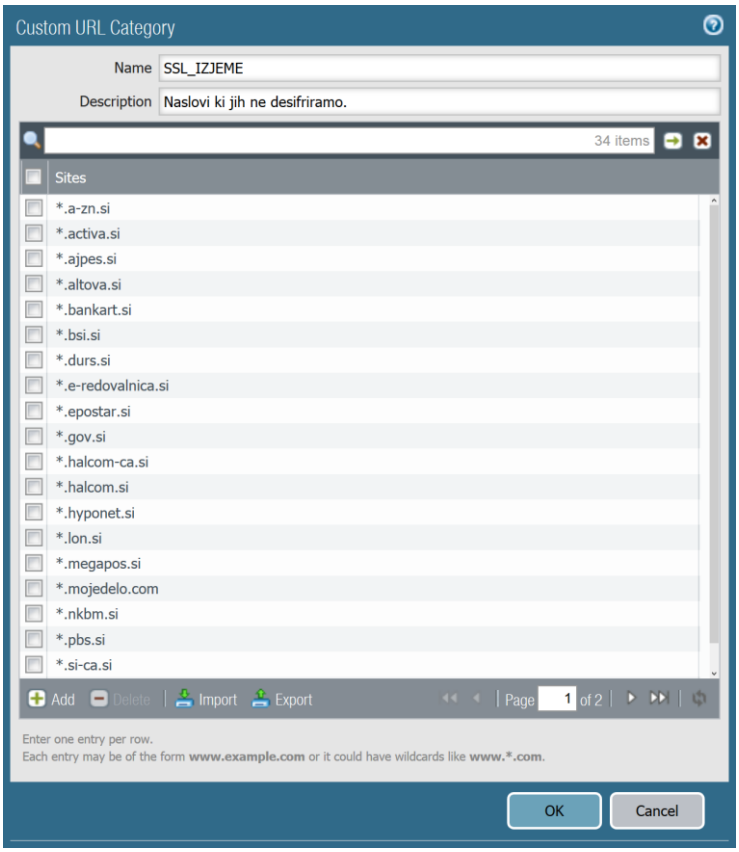
Slika 23: Parametri ustvarjenega certifikata CA.

Na novo narejenemu certifikatu se določi vloga v procesu dešifriranja SSL (glej sliko 24).

Name	Subject	Issuer	CA	Key	Expires	Algorithm	Usage
LAB_PA_CA	C = SI, O = LAB, OU = IT, CN = LAB_PA	C = SI, O = LAB, OU = IT, CN = LAB_PA	☑	☑	Jul 14 16:29:22 2017 GMT	RSA	Forward Trust Certificate Forward Untrust Certificate

Slika 24: Nastavitve certifikata.

Za vzpostavitev hierarhije zaupanja se na testnem računalniku ta certifikat namesti v lokalno bazo digitalnih podpisov CA. Ker dešifriranje SSL ne deluje v primeru, ko se z digitalnim potrdilom overja tudi odjemalec, je potrebno definirati izjeme (glej sliko 25).



Slika 25: Definicija izjem SSL.

Politika določa promet, ki gre v proces dešifriranja SSL. Potrebno je paziti na vrstni red, ker se politika izvaja od prvega zapisa proti zadnjemu (glej sliko 26).

		Source			Destination			
	Name	Zone	Address	User	Zone	Address	URL Category	Action
1	SSL_IZJEME	LAB	any	srcsi\lab_users	OUTSIDE	any	SSL_IZJEME	no-decrypt
2	SSL_DESIFRIRANJE	LAB	any	srcsi\lab_users	OUTSIDE	any	any	decrypt

Slika 26: Politika dešifriranja SSL.

4.2.9 Skupine aplikacij

Skladno z zahtevami ter analizo prometa so definirane statične skupine aplikacij (glej sliko 27).

Name	Applications
IZJEME_USERS	ssl
IZJEME_TRZENJE	facebook-file-sharing
IZJEME_RAZVOJ	ciscovpn
	ipsec
	open-vpn
	ms-rdp
	rlogin
	vnc
IZJEME_IT	ssh
	bittorrent
	bittorrent-sync
	ms-rdp
	rlogin
	vnc
	telnet

Slika 27: Definicija izjem.

Definirani sta dinamični skupini aplikacij, ki pripadata določenim podskupinam ali posebnim karakteristikam (glej sliko 28).

Name	Subcategory	Characteristic
BANDWIDTH_CONTROL	photo-video	Excessive Bandwidth
PREPOVEDANE_APLIKACIJE	encrypted-tunnel	
	file-sharing	
	proxy	
	remote-access	

Slika 28: Definicija dinamičnih skupin aplikacij.

4.2.10 Omejevanje porabe pasovne širine

Omejevanje porabe pasovne širine je izvedeno v treh korakih. V prvem se s politiko QoS klasificira mrežni promet (glej sliko 29).

		Source			Destination				
	Name	Zone	Address	User	Zone	Address	Application	Service	Class
1	LAB_QOS_POLICY	any	any	srcsi\lab_users	any	any	BANDWIDTH_CONTROL	any	3

Slika 29: Klasifikacija mrežnega prometa.

Tako klasificiran promet se uporabi v profilu QoS, kjer se mu določi zgornjo vrednost porabe pasovne širine (glej sliko 30).

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
LAB_QOS_PROFIL			
class3	0.000	20.000	medium

Slika 30: Profil QoS.

Porabo pasovne širine je mogoče omejevati le na odhodnem mrežnem vmesniku. Ker želimo omejitev v obe smeri, je potrebno profil QoS namestiti na zunanji in notranji mrežni vmesnik (glej sliko 31).

Name	Profile
ethernet1/1	
Tunneled Traffic	LAB_QOS_PROFIL
Clear Text Traffic	LAB_QOS_PROFIL
ethernet1/2	
Tunneled Traffic	LAB_QOS_PROFIL
Clear Text Traffic	LAB_QOS_PROFIL

Slika 31: Aplikacija profila QoS na mrežni vmesnik.

4.2.11 Politika dostopov

Politika dostopov določa promet, ki prehaja skozi mrežno požarno pregrado. Potrebno je paziti na vrstni red, ker se politika izvaja od prvega zapisa proti zadnjemu. Pravila morajo biti razvrščena od bolj podrobnih proti manj podrobnim. Na začetku so definirane izjeme, nato prepovedane aplikacije in na koncu pravilo, ki dovoljuje vse aplikacije ki niso eksplicitno določene (glej sliko 32).

		Source			Destination				
	Name	Zone	Address	User	Zone	Address	Application	Action	Profile
1	VSI_SSL	LAB	any	srcsi\lab_users	OUTSIDE	any	IZJEME_USERS	Allow	
2	TRZENJE	LAB	any	srcsi\lab_users_trzenje	OUTSIDE	any	IZJEME_TRZENJE	Allow	
3	RAZVOJ	LAB	any	srcsi\lab_users_razvoj	OUTSIDE	any	IZJEME_RAZVOJ	Allow	
4	IT	LAB	any	srcsi\lab_users_it	OUTSIDE	any	IZJEME_IT	Allow	
5	NEVARNE_APLIKACIJE	LAB	any	srcsi\lab_users	OUTSIDE	any	PREPOVEDANE_APLIKACIJE	Deny	none
6	OSTALE_APLIKACIJE	LAB	any	srcsi\lab_users	OUTSIDE	any	any	Allow	

Slika 32: Politika dostopov.

4.2.12 Zaščita pred zlonamerno kodo

Zaščita pred zlonamerno kodo je izvedena v dveh delih. V prvem so definirani trije profili za zaščito pred zlonamerno kodo. Ti so sledeči:

- protivirusna zaščita,
- zaščita pred vohunskimi programi in
- zaščita pred ranljivostmi.

Požarna pregrada ima vgrajene protivirusne dekodirnike, ki delujejo znotraj transportnih protokolov. Glede na stopnjo varnostne grožnje in uporabljen protokol prenosa je definirana obrambna akcija (glej sliko 33).

Name	Decoders		
	Name	Action	WildFire Action
LAB_AV_PROFILE	http	default (reset-both)	default (reset-both)
	smtp	default (alert)	default (alert)
	imap	default (alert)	default (alert)
	pop3	default (alert)	default (alert)
	ftp	default (reset-both)	default (reset-both)
	smb	default (reset-both)	default (reset-both)

Slika 33: Profil protivirusne zaščite.

Podobno se profilu za preprečevanje vohunskega programja glede na stopnjo nevarnosti specificira obrambne akcije (glej sliko 34).

Name	Rule Name	Threat Name	Severity	Action
LAB_AS_PROFILE	simple-critical	any	critical	reset-both
	simple-high	any	high	reset-both
	simple-medium	any	medium	reset-both
	simple-informational	any	informational	default
	simple-low	any	low	default

Slika 34: Profil za preprečevanje vohunskega programja.

Definiran je profil za zaščito pred ranljivostmi. Glede na vir ranljivosti in stopnjo ogroženosti je definirana obrambna akcija (glej sliko 35).

Name	Rule Name	Threat Name	Host Type	Severity	Action
LAB_VP_PROFILE	simple-client-critical	any	client	critical	reset-both
	simple-client-high	any	client	high	reset-both
	simple-client-medium	any	client	medium	reset-both
	simple-client-informational	any	client	informational	default
	simple-client-low	any	client	low	default
	simple-server-critical	any	server	critical	reset-both
	simple-server-high	any	server	high	reset-both

Slika 35: Profil zaščite proti zlorabi ranljivosti.

V drugem delu so doslej definirani varnostni profili združeni v skupino varnostnih profilov (glej sliko 36).

Name	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile
SGP_OUTSIDE	LAB_AV_PROFILE	LAB_AS_PROFILE	LAB_VP_PROFILE

Slika 36: Skupina varnostnih profilov.

Skupina varnostnih profilov je uporabljena v politiki filtriranja, in sicer le v pravilih, ki dovoljujejo mrežni promet (glej sliko 32).

4.3 Povzetek rešitve

Z vidika varnosti so v predlagani rešitvi implementirane vse zahtevane funkcionalnosti, kot sledi:

- filtriranje na podlagi aplikacij;
- filtriranje na podlagi članstva v skupini aktivnega imenika;
- dešifriranje uporabniškega prometa zaščitenega z SSL;
- preprečevanje uporabe ne varnih aplikacij;
- zaščita pred zlonamerno kodo.

Poleg tega so izvedene tudi ne varnostno orientirane funkcionalnosti. Te so sledeče:

- uporaba storitve DHCP v uporabniškem segmentu;

- preprečevanje odtekanja intelektualne lastnine.

Z vidika učinkovitosti je implementirano omejevanje porabe pasovne širine. Politika omejevanja je vezana na dinamično skupino aplikacij, ki prenašajo vizualne medijske vsebine.

Rešitev zaobjame vse zahteve in želje Naročnika ter potrjuje koncept uporabe požarne pregrade naslednje generacije za varen dostop uporabnikov do internetnih storitev.

Poglavje 5 Zaključek

Z današnjo tehnologijo je mogoče ustrezno zaščititi tako uporabniški dostop kot celotno infrastrukturo IT. Zelo pomembno je razumevanje različnih tehnoloških pristopov mrežnih požarnih pregrad, da bi lahko določili, kateri je primeren za specifično okolje. Eden od doseženih ciljev diplomske naloge je pregled nad različnimi vrstami požarnih pregrad ter predstavitev njihovih prednosti in slabosti. Drugi doseženi cilj diplomske naloge je na dovolj kompleksnem primeru prikazati koncept uporabe požarne pregrade naslednje generacije za zaščito dostopa uporabnikov do interneta.

Implementacija požarne pregrade naslednje generacije je kompleksna, saj je za optimalno delovanje potrebna integracija z drugimi deli informacijskega sistema. Dodatno se poveča zahtevnost ob menjavi požarne pregrade prejšnjih generacij, ker so prometni tokovi navadno opisani s številkami vrat protokolov TCP in UDP. Za optimalno izrabo požarne pregrade naslednje generacije je potrebno prometne tokove opisati z aplikacijami.

Sodobnim požarnim pregradam predstavljajo poseben problem aplikacije, ki z lastninskimi ali drugimi šifrirnimi mehanizmi onemogočajo vpogled v promet. Na tem področju se pojavlja dilema med zasebnostjo in varovanjem korporativnih omrežij.

Naloga proizvajalcev sodobnih požarnih pregrad je, da ažurno obnavljajo in izdelujejo podpise, ki omogočajo učinkovito prepoznavanje tako aplikacij kot škodljive kode. Ker gre za zahteven proces obratnega inženiringa, se proizvajalci vse pogosteje dogovarjajo o sodelovanju. V prihodnosti lahko pričakujemo, da bodo proizvajalci večnamenskih požarnih pregrad konvergirali k vse večji integraciji varnostno usmerjenih funkcionalnosti, proizvajalci požarnih pregrad naslednje generacije pa k večjemu številu le-teh. Ena izmed njih bo zagotovo integracija s sistemi za zaščito končnih naprav. Poleg dodatne zaščite bo tak pristop lahko zaobšel problem lastniške ali druge tehnike šifriranja.

Literatura

[1] K. Ingham in S. Forrest, „A History and Survey of Network Firewalls,“ 2002. [Elektronski]. Dostopno na: http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf, [Poskus dostopa .12 .6 2016].

[2] TechTerms, „Firewall Definition,“ [Elektronski]. Dostopno na: http://techterms.com/definition/firewall, [Poskus dostopa 18. 4. 2016].

[3] D. Thakur, „Types of Firewall Architectures,“ Technology Motivation, [Elektronski]. Dostopno na: http://ecomputernotes.com/computernetworkingnotes/security/types-of-firewall-architectures, [Poskus dostopa 11. 6. 2016].

[4] W. Cheswick in S. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Reading (Massachusetts) [etc.] : Addison-Wesley, 1995, cop. 1994, 1995, p. 306.

[5] K. Zetter, „Discovery Around Juniper Backdoor Raises More Questions About the Company,“ Wired, 8. 1. 2016. [Elektronski]. Dostopno na: https://www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/, [Poskus dostopa 11. 6. 2016].

[6] D. Barksdale, J. Gruskovnjak in A. Wheeler, „Execute My Packet,“ Exodus Intelligence, 10. 2. 2016. [Elektronski]. Dostopno na: https://blog.exodusintel.com/2016/02/10/firewall-hacking/, [Poskus dostopa 11. 6. 2016].

[7] F. Avolio, „Firewalls and Internet Security, the Second Hundred (Internet) Years, “ *The Internet Protocol Journal,* Izv. 2, št. 2, junij 1999.

[8] T. Darmohray, „Firewalls and Fairy Tales,“ *;LOGIN:,* Izv. 30, št. 1, 2. 2005.

[9] C. Schmidt in T. Darby, julij 2001. [Elektronski]. Dostopno na: http://www.snowplow.org/tom/worm/worm.html, [Poskus dostopa 18. 4. 2016].

[10] S. Khandelwal, „Mac OS X Zero-Day Exploit Can Bypass Apple's Latest Protection Feature,“ The Hacker News, 24. 3. 2016. [Elektronski]. Dostopno na: http://thehackernews.com/2016/03/system-integrity-protection.html, [Poskus dostopa 12. 6. 2016].

[11] M. Burgess, „Millions of Android devices vulnerable to new Stagefright exploit,“ Wired, 16. 3. 2016. [Elektronski]. Dostopno na: http://www.wired.co.uk/article/stagefright-android-real-world-hack, [Poskus dostopa 12. 6. 2016].

[12] Ž. Cucej, 4. 2008. [Elektronski]. Dostopno na: http://www.sparc.uni-mb.si/Fileji/TK_modeli-1.pdf, [Poskus dostopa 10. 2010].

[13] Wikipedia, „OSI model,“ 2016. [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/OSI_model, [Poskus dostopa 8. 5. 2016].

[14] J. Burke, „What is the difference between OSI model and TCP/IP other than the number of layers?,“ TechTarget, 10. 2014. [Elektronski]. Dostopno na: http://searchnetworking.techtarget.com/answer/What-is-the-difference-between-OSI-model-and-TCP-IP-other-than-the-number-of-layers, [Poskus dostopa 31. 5. 2016].

[15] T. Jajish, „How TCP terminate connection gracefully, TCP Connection Termination, TCP FIN Flag,“ OmniSecu.com, [Elektronski]. Dostopno na: http://www.omnisecu.com/tcpip/tcp-connection-termination.php, [Poskus dostopa 13. 6. 2016].

[16] L. Boyer, „Great Walls of Fire,“ Novell, 1. 1. 1997. [Elektronski]. Dostopno na: https://support.novell.com/techcenter/articles/nc1997_01a.html, [Poskus dostopa 18. 6. 2016].

[17] Wikipedia, „Stateful firewall,“ 2016. [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/Stateful_firewall, [Poskus dostopa 19. 6. 2016].

[18] Cisco, „CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1,“ 22. 8. 2014. [Elektronski]. Dostopno na:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/conns_connlimits.html#pgfId-1080734, [Poskus dostopa 25. 6. 2016].

[19] Cisco, „ASA 8.3 and Later: Enable FTP/TFTP Services Configuration Example," 19. 7. 2011. [Elektronski]. Dostopno na: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113110-asa-enable-ftp-00.html, [Poskus dostopa 26. 6. 2016].

[20] T. Dr. Porter, „The Perils of Deep Packet Inspection," SecurityFocus.com, 11. 1. 2005. [Elektronski]. Dostopno na: http://www.symantec.com/connect/articles/perils-deep-packet-inspection, [Poskus dostopa 15. 5. 2016].

[21] Wikipedia, „Unified threat management," 29. 2. 2016. [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/Unified_threat_management, [Poskus dostopa 29. 6. 2016].

[22] D. Pauli, „Researcher pokes holes through Fortinet UTM," SC Magazine, 20. 9. 2012. [Elektronski]. Dostopno na: http://www.itnews.com.au/news/researcher-pokes-holes-through-fortinet-utm-316308, [Poskus dostopa 29. 6. 2016].

[23] Palo Alto Networks, „Next-Generation Firewall Defined By Gartner," 16. 10. 2009. [Elektronski]. Dostopno na: http://researchcenter.paloaltonetworks.com/2009/10/next-generation-firewall-defined-by-gartner/, [Poskus dostopa 2. 7. 2016].

[24] Firewalls.com, „History and Evolution of Firewalls," 2012. [Elektronski]. Dostopno na: http://www.firewalls.com/resources/firewall-history-1.html, [Poskus dostopa 29. 4. 2012].

[25] Palo Alto Networks, „Application Research Center," [Elektronski]. Dostopno na: https://applipedia.paloaltonetworks.com/, [Poskus dostopa 3. 7. 2016].

[26] Network Working Group, „Address Allocation for Private Internets," 2. 1996. [Elektronski]. Dostopno na: https://tools.ietf.org/html/rfc1918, [Poskus dostopa 3. 7. 2016].

[27] I. Barker, „Antivirus tools miss almost 70 percent of malware within the first hour," 12. 2. 2015. [Elektronski]. Dostopno na: http://betanews.com/2015/02/12/antivirus-tools-miss-almost-70-percent-of-malware-within-the-first-hour/, [Poskus dostopa 5. 7. 2016].

[28] Sandvine Incorporated, „Global Internet Phenomena Spotlight - Encrypted Internet Traffic,“ 30. 4. 2015. [Elektronski]. Dostopno na: https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf, [Poskus dostopa 5. 7. 2016].