Univerza v Ljubljani

Fakulteta za elektrotehniko

Matej Repovž

Požarni zidovi naslednje generacije

Diplomsko delo

Mentor: prof. dr. Andrej Kos

Ljubljana, 2016

Zahvala

Za pomoč in mentorstvo pri diplomskem delu se posebej zahvaljujem prof. dr. Andreju Kosu, saj me je s predlogi in komentarji usmerjal pri pisanju naloge. Velika zahvala gre tudi mag. Romanu Kotniku za pomoč pri izvedbi laboratorijskih testov in njegova pojasnila, ki so pripomogla k mojemu boljšemu razumevanju teme.

Vsebina

Seznam slik

Seznam uporabljenih simbolov

APT	advanced persistent threat	napredno trajno ogrožanje
BYOD	bring your own device	prinesi svojo napravo
C&C	command and control	vodenje in nadzor
DLP	data loss prevention	sistem za preprečevanje izgube podatkov
DNS	Domain name system	Sistem domenskih imen
DoS	Denial of service	Zavračanje storitev
FSAE	Fortinet server authentication extension	Fortinet-ovo razširjeno preverjanje pristnosti strežnikov
FTP	File transfer protocol	Protokol za prenos datotek
Gbit/s	Gigabit per second	Gigabit na sekundo
HTTP	Hypertext transfer protocol	Komunikacijski protokol
HTTPS	Hypertext transfer protocol secure	Zavarovana različica komunikacijskega protokola
ICSA	International Computer Security Association	Mednarodno združenje za računalniško varnost
IP	Internet protocol	Komunikacijski protokol
IPS	Intrusion prevention system	Sistem za preprečevanje vdorov
IPsec	Internet protocol security	Zaščita omrežnega protokola
ISO	International Organization for Standardization	Mednarodna organizacija za standardizacijo
KB	Kilobyte	Kilobajt
LAN	Local area network	Lokalno omrežje
LDAP	Lightweight directory access protocol	Internetni protokol za dostop do imenikov
MB	Megabyte	Megabajt
Mbit/s	Megabit per second	Megabit na sekundo
NAT	Network address translation	Prevajanje omrežnega naslova

NGIPS	Next generation intrusion prevention system	Sistem za preprečevanje vdorov naslednje generacije
NSS	Network and system security	Omrežna in sistemska varnost
N/A	Not available	Ni na voljo
OSI	Open system interconnection model	Referenčni model za oblikovanje protokolov
PDF	Portable document format	Prenosni format datoteke
POP3	Post office protocol version 3	Vrsta protokola
P2P	Peer-to-peer	Vrsta omrežne arhitekture
QoS	Quality of service	Kakovost storitev
SMTP	Simple mail transfer protocol	Internetni protokol za prenos elektronske pošte
SSL	Secure socket layer	Kriptografski protokol
SYN	Synchronization	Sinhronizacija
TCP	Transmission control protocol	Komunikacijski protokol
UDP	User datagram protocol	Nepovezavni protokol transportnega sloja
URL	Uniform resource locator	Naslov spletnega vira
VPN	Virtual private network	Navidezno zasebno omrežje
WAN	Wide Area Network	Javno omrežje
XMPP	Extensible messaging and presence protocol	Komunikacijski protokol

Povzetek

Požarni zidovi so pomemben člen pri zagotavljanju varnosti v času, ko si življenja brez interneta enostavno ne znamo predstavljati. So naprave, ki nadzorujejo omrežni promet med notranjim lokalnim in zunanjim javnim omrežjem. Poznamo programske različice požarnih zidov in strojne različice oziroma samostojne naprave. Diplomsko delo je osredotočeno predvsem na strojne različice požarnih zidov. Prve različice požarnih zidov so se pojavile konec osemdesetih let prejšnjega stoletja in zadoščale za takratne potrebe v internetni tehnologiji. Vendar sta neverjetni razvoj informacijskih tehnologij in storitev, prav tako pa tudi pojav zlonamernih programov in vdorov povzročila, da prvotne različice niso bile več učinkovite za zagotavljanje visoke ravni varnosti. Postopno so se začeli pojavljati nove različice požarnih zidov in novi načini pregledovanja omrežnega prometa, ki so ustrezali takratnim zahtevam. Poleg požarnih zidov se je na trgu pojavila vrsta dodatnih orodij, ki so v povezavi s požarnimi zidovi učinkovito pregledovala omrežni promet. Orodja so bila kakovostna, vendar so zahtevala dodatni strošek zaradi nakupa novih naprav in licenc, potrebna so bila dodatna izobraževanja, potreben je bil prostor za namestitev naprave itd. Potrebe po visoki zaščiti omrežja in prilagoditev novim načinom uporabe omrežnih storitev so pripeljale do razvoja požarnih zidov naslednje generacije. To so zmogljive naprave, ki s pomočjo naprednih orodij zagotavljajo varnost lokalnih omrežij, nadzor nad aplikacijami in pregled nad uporabniki omrežja. Bistvo požarnih zidov naslednje generacije je, da združujejo dobre lastnosti prejšnjih različic, vsebujejo napredna orodja, prav tako pa vključujejo novejše pristope za odkrivanje zlonamernih programskih kod in napadov. Poleg zagotavljanja varnosti in nadzora morajo biti požarni zidovi naslednjih generacij pregledni za uporabo, saj tako administratorjem omrežij zagotovijo čim enostavnejše rokovanje z napravo. V zadnjih letih pa so se na trgu pojavile zmogljive naprave, ki naj bi kot dodatek k požarnim zidovom zagotavljale visoko stopnjo varnosti. To so t. i. Sandbox naprave, katere z naprednimi načini pregledovanja iščejo zlonamerne vsebine in napade. Rezultat diplomskega dela so v teoretičnem delu razloženo splošno delovanje požarnih zidov, ter v drugem delu z laboratorijskimi testi prikazani praktični preizkusi na napravah.

Ključne besede: požarni zidovi naslednje generacije, evolucija požarnih zidov, Sandbox.

Abstract

Firewalls are an important element in ensuring computer security in times when we simply cannot imagine living without the Internet. These applications and devices control network traffic between the internal local and external public networks. Software and hardware firewall solutions are available or, as the case may be, independent devices. The bachelor's thesis focuses primarily on the hardware firewall solutions. The first firewall solutions occurred at the end of the 1980's and were sufficient for the needs of Internet technologies of the time. However, the incredible development of information technologies and services, but especially the occurrence of malicious software and hacking attacks, made those forms of firewalls inefficient as regards providing high levels of security. Gradually, new forms of firewalls began to spring up, as well as new ways of monitoring network traffic to meet the requirements of the time. In addition to firewalls, a number of additional tools occurred on the market which, together with firewalls, enabled efficient monitoring of network traffic. The tools were of good quality, but the additional cost of purchasing new devices and licences was a problem for many. Moreover, additional training was required for their use, additional space for installing the devices and so on. The needs for high quality network protection and adjustment to new forms of network services have brought on the development of next-generation firewalls. These are high capacity devices which, in combination with advanced tools, ensure security of local networks, monitoring of applications, as well as monitoring of network users. The essence of the next-generation firewalls is that not only do they combine the good characteristics of previous versions and contain advanced tools, but also that they use novel approaches to discovering malicious software codes and hacking attacks. In addition to ensuring security and monitoring, the next-generation firewalls also provide transparent use in order to simplify the management of these devices for network administrators as much as possible. In the last few years, a capable device came to the market which would, as an addition to next-generation firewalls, ensure a high level of security. These are the so-called Sandbox devices, which employ advanced levels of searching to discover malicious contents and attacks. The first part of the bachelor's thesis explains the general operation of firewalls by using theory, whilst the second part uses laboratory work to demonstrate the practical tests on devices.

Key words: Next-generation firewall, evolution of firewall, Sandbox.

1 Uvod

V času, ko si težko predstavljamo življenje brez spletnih storitev in dostopa do svetovnega spleta, je varna uporaba te tehnologije velik izziv podjetjem in ustanovam. Pri tem so mišljeni predvsem zaščita lokalnih omrežij, varovanje ključnih informacij, zaščita uporabnikov oziroma njihovih naprav in pa nadzor nad neverjetno količino omrežnega prometa. Požarni zidovi naslednjih generacij ponujajo vrsto naprednih možnosti za zagotavljanje varnega lokalnega omrežja. Vendar se je ob pripravi na diplomsko delo postavilo vprašanje: zakaj je bila potrebna naslednja generacija požarnih zidov? Kaj je manjkalo prejšnjim različicam, da je prišlo do razvoja naslednjih generacij požarnih zidov? Da bi dobro razumeli namen požarnih zidov nove generacije, moramo poznati, kako so se ti razvijali, prav tako pa moramo poznati, kateri novi trendi so se pojavili pri uporabi spletnega omrežja in storitev.

Razvoj požarnih zidov je potekal vzporedno z razvojem napadov in zlorab na lokalna omrežja podjetij in ustanov. Naprednejši, ko so postajali napadi, bolj so razvijalci varnostne opreme razvijali nove načine zaščite lokalnih omrežij in nadzora prometa. Velik izziv sta predstavljala tudi porast uporabe aplikacij in mobilnost dostopa do spletnega omrežja preko različnih prenosnih naprav. Aplikacije so cenovno ugodne in so na napravah, kot je mobilni telefon zelo priročne za uporabo. Tako so skrbniki omrežij želeli večji nadzor nad aplikacijami, večji nadzor nad uporabniki in visoko raven varnosti v omrežjih. Prav to so bili ključni razlogi za pojav požarnih zidov naslednje generacije. V letu 2009 so prišle na trg prve različice požarnih zidov naslednje generacije, podjetje Gartner pa je postavilo prvo definicijo, kaj pravzaprav je požarni zid naslednje generacije in katerim standardom mora ustrezati. Požarni zidovi naslednjih generacij delujejo s pomočjo različnih naprednih orodij, katerih namen je zaščititi lokalna omrežja in uporabnike pred različnimi vrstami napadov in zlorab. Orodja morajo biti učinkovita in pregledna za uporabo, poleg tega pa morajo administratorjem omrežij ponuditi vrsto možnih nastavitev, da jih lahko nastavijo za potrebe določenega omrežja. Laboratorijski testi v diplomski nalogi se nanašajo na požarni zid naslednje generacije ponudnika Fortinet, pri katerem me je zanimalo prav to: kako delujejo napredna orodja za varnost in ali so učinkovita. Diplomsko delo vključuje še opis in preizkus naprave Sandbox, ki jo kot dodatno orodje k osnovni različici požarnega zidu priporočajo priznana podjetja in inštituti za varnost v informacijski tehnologiji. Pri napravi Sandbox nas je zanimalo, kakšna orodja vsebuje, ali so ta učinkovita in kako naprava deluje v povezavi z

napravo FortiGate. Skupaj smo izvedli pet laboratorijskih testov, in sicer štiri testi na napravi FortiGate in enega na napravi Sandbox.

1.1 Nameni in cilji

Namen diplomskega dela je v teoretičnem delu raziskati, zakaj je prišlo do razvoja požarnih zidov naslednje generacije in z laboratorijskimi testi prikazati delovanje orodij za varnost, ki jih vsebuje požarni zid naslednje generacije. Cilji diplomskega dela so:

- V teoretičnem delu raziskati in obrazložiti, kako so se požarni zidovi razvijali vse do zadnje različice-požarnih zidov naslednje generacije, ter zakaj so ti nujno potrebni za visoko raven varnosti v omrežjih,
- praktično prikazati delovanje požarnih zidov naslednje generacije in pojasniti delovanje nekaterih naprednih orodij, ki jih vsebuje požarni zid naslednje generacije,
- prikazati zadnji trend na področju varnosti, in sicer napravo Sandbox, ki v povezavi s požarnim zidom varuje omrežje pred varnostnimi grožnjami.

1.2 Metode dela

Za izdelavo diplomske naloge smo v prvi fazi izbrali različno strokovno slovensko in tujo literaturo o opisani temi. Sledili so pregled literature in priprava testov na napravah FortiGate in FortiSandbox. Ko so bile postavljene smernice, je sledila izdelava dispozicije. Diplomsko delo je ločeno na dva dela, in sicer na začetni teoretični del, kjer smo s pomočjo deskriptivne metode analizirali spletne vire, knjige, priročnike in članke. Teoretični del nam je predstavil jasno sliko o izbrani temi. Sledili so laboratorijski testi na napravah, pri katerih smo z eksperimentalno metodo testirali postavljene cilje. Izvedba testov diplomskega dela je potekala na Fakulteti za elektrotehniko, kjer jih je bilo možno izvesti na primerni opremi. Po opravljenih testih na napravah so sledile analiza rezultatov in sklepne ugotovitve diplomskega dela.

2 Problemi varnosti

V današnjem svetu si je nemogoče predstavljati, da bi človeštvo lahko delovalo brez tehnologije in spletnih povezav. Ta tehnologija pa odpira nove možnosti zlorab, ki so prav tako doživele razcvet, zato je danes v podjetjih in ustanovah prednostna naloga zaščititi omrežje in računalniške sisteme. Za omrežne napade je odgovorna nova generacija napadalcev, ki so tehnično podkovani in za napad ne potrebujejo nobenega stika z žrtvijo. Ne da bi izdali svojo identiteto, z oddaljene lokacije preko internetnega omrežja napadejo vsakogar, ki je povezan v svetovni splet, prenesejo podatke, jih spreminjajo ali uničijo in lahko povzročijo ogromno nepopravljivo škodo. Po storjenem napadu pa velik izziv predstavlja identiteta napadalca, ki jo je zelo težko odkriti, še težje pa dokazati in napadalca obsoditi za napad. Tarče so predvsem podjetja, državne ustanove, pomembne osebnosti, spletne strani itd.

Statistike napadov so v omrežnem svetu nepredstavljivo velike. Poročilo organizacije Symantec Corporation navaja, da je bilo v letu 2013 blokiranih kar 568.700 omrežno osnovanih napadov na dan. Kot napreduje obramba pred napadi, se posledično razvijajo tudi načini napadov in ti so vedno zahtevnejši. Samo v letu 2013 je bilo zaznanih 6.787 novih vrst ranljivosti [1].

Vzrokov za nezanesljivo varnost je več, med večjimi pa so [2]:

- **Tehnološke slabosti**
  Vsaka tehnologija ima svoje pomanjkljivosti, ki so zanimive za napadalce in jih uporabljajo za zlorabo oziroma napad. Da se temu izognemo, se proizvajalci trudijo popraviti programsko opremo, uporabniki pa jo morajo obvezno nadgrajevati.

- **Slabosti v varnostni politiki**
  Tu sta težavi predvsem pomanjkljivi varnostni predpisi in njihovo nespoštovanje. Ponekod sta prizadevanje za varnost in ukrepanje ob zlorabi neorganizirani. Prav tako v nekaterih podjetjih ne izvajajo stalnega nadzora nad varnostjo in ne skrbijo nad njeno stalno nadgradnjo. Problem zagotavljanja varnosti lahko predstavljajo tudi zaposleni, ki niso dobro seznanjeni z varnostno politiko in lahko nevede škodujejo varnostni politiki

podjetja. Tu morata biti postavljena jasen dogovor in spoštovanje varnostne politike, da zmanjšamo tveganje na področju varnosti. Prav tako pa je pomembno stalno izobraževanje skrbnikov omrežij in zaposlenih, ki skrbijo za varnost omrežij, saj se to področje nenehno razvija in spreminja.

- **Slabosti v nastavitvah sistemov**
  Veliko omrežnih naprav se uporablja s privzetimi nastavitvami in to lahko privede do resnih posledic, saj privzete nastavitve seveda poznajo tudi napadalci. Tu je treba poskrbeti za dobra in varna gesla ter jih na določeno obdobje tudi menjati. Narediti je treba seznam nadzora dostopa do omrežja in blokirati nezaželenega. Če je mogoče, je treba imeti šifriran promet (brezžični dostop) itd.

2.1 Pomen varnosti in zaščite

Glede na vrsto zlonamernih napadov in groženj sta zaščita podatkov in zaščita pred nezaželenimi posegi v naše lokalno omrežje prav gotovo večni izziv skrbnikom omrežij. Glede na to, da poznamo različne vrste napadov, se tudi načini zaščite pred njimi razlikujejo. Vsem pa je skupno, da jih poskušamo preventivno preprečiti ter da ob samem napadu ukrepamo hitro in pravilno. J.E Canavan je to opisal z izrazom »varnostni trikotnik« in ga definiral kot [3]: »Tri veje varnostnega trikotnika so preventiva, odkrivanje in ukrep, ter sestavljajo osnovo za omrežno varnost. Varnostni trikotnik bi moral biti temelj varnostne politike vsakega podjetja in ukrep, ki bi ga podjetje razvijalo.«

Slika 1: Varnostni trikotnik

2.2 Vrste napadov

O napadu na napravo ali omrežje govorimo, ko neznana oseba ali skupina oseb skuša iz oddaljenega dostopa onemogočiti normalno delovanje te naprave ali pa pride do kraje občutljivih informacij. Poznamo veliko vrst napadov, ki jih razvrščamo po načinu, kako je napad izveden in s kakšnim namenom. Če govorimo o zaščiti omrežja in naprav, je zelo pomembno, da poznamo različne vrste napadov. Pojavljajo se vedno novi načini zlorab, ki jim moramo slediti, da ob zlorabi prepoznamo tip napada in da znamo ustrezno ukrepati.

2.2.1 Pasivni napadi

Pri pasivnih napadih napadalec samo spremlja informacije in nadzoruje omrežje oziroma prenosni kanal. Glavni namen takega napada je pridobiti informacije za nadaljnjo zlorabo, med samim napadom pa ne pride do spreminjanja nastavitev in informacij [4].

Poznamo dve vrsti pasivnih napadov:

- prisluškovanje in
- analizo prometa.

2.2.2 Aktivni napadi

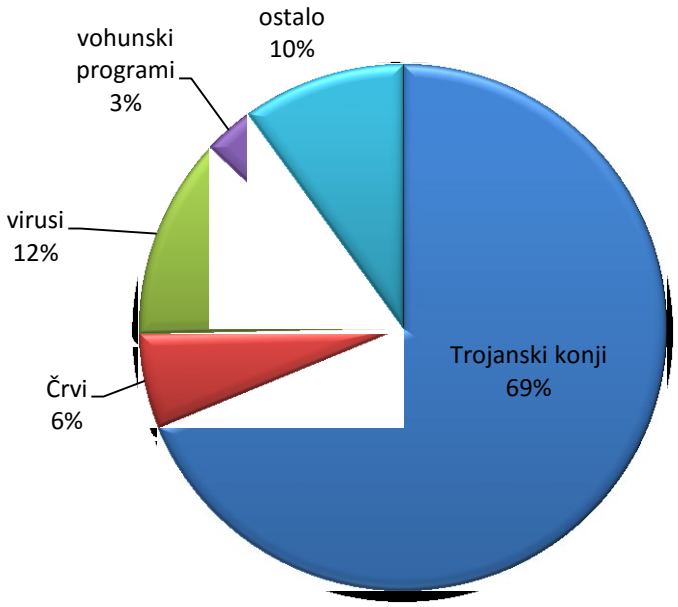
Napadalec je v tem primeru neposredno umeščen v povezavo in poizkuša vplivati na sistem in spremeniti njegovo delovanje.

Poznamo več vrst aktivnih napadov, med katere spadajo:

- kraja identitete ali maškarada (angl. masquerade),
- sprememba sporočila,
- zavračanje storitev (DoS),
- napredno trajno ogrožanje (APT),

2.3 Zlonamerni programi

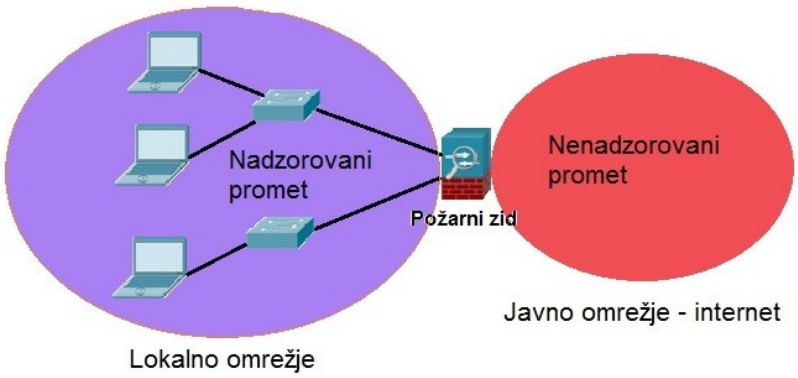
Zlonamerni programi so še ena od nevarnosti, ki ji moramo posvetiti pozornost, saj so neverjetno razširjeni po svetovnem omrežju. Zlonamerni program je programska koda, ki škoduje okuženemu računalniškemu sistemu ali omrežju, prav tako pa se lahko razširi še na druge sisteme. Zavira lahko normalno delovanje ali pa je orodje za nadaljnji vdor v sistem. Razlikujemo jih glede na to, katere gostiteljske datoteke uporabljajo za svoje širjenje, kako se naložijo v gostiteljev sistem in kako nanj vplivajo. Med pogostejše načine zlonamernega programiranja uvrščamo slepa vrata, logične bombe, trojanske konje in viruse. Prav tako pa poznamo tudi zlonamerne programe, ki za svoje širjenje ne potrebujejo gostiteljske datoteke in so se zmožni širiti sami. Mednje spadajo črvi in tako imenovani zombiji [2].



Slika 2: Pogostost zlonamernih napadov v letu 2014 [5, str. 8]

3 Požarni zidovi

Nedvomno je velik izziv v svetu omrežne varnosti zagotoviti varen dostop do podatkov, varne transakcije, varnost in zasebnost naših podatkov itd. Vsakokrat, ko se povežemo na svetovni splet tvegamo stvari, kot so podatki in informacije v našem lokalnem omrežju, sredstva oziroma oprema (računalniki in druge omrežne naprave) in ugled. Ena od osnovnih vrst zaščit v sodobnem internetnem omrežju so požarni zidovi. Izraz požarni zid izhaja iz ovir, ki so ognjevzdržne in preprečujejo širitev požara iz enega dela hiše na ostale lokacije, torej nevarni del (požar) ločijo od varnega dela hiše. Podobno pa je v omrežnem okolju. Požarni zid v svetu računalništva predstavlja napravo, ki ločuje potencialno nevarno zunanje omrežje od lokalnega omrežja, vendar pa mora biti tako napredna, da z določenimi pravili omeji vhodni in izhodni omrežni promet ter zagotavlja varnost pred nezaželenim in nevarnim omrežnim prometom [6]. Požarni zid lahko nastopa kot programska ali kot strojna oprema.



Slika 3: Lokacija požarnih zidov v omrežju

3.1 Programski požarni zidovi

Programski požarni zidovi so vrsta požarnih zidov, ki so programsko nameščeni na posameznem računalniku. Njihova naloga je nadzirati vsak vhod, preko katerega poteka omrežni promet na računalniku. Programski požarni zidovi imajo tako seznam vseh aplikacij, ki imajo dostop do omrežja, in izvajajo nadzor na vhodih, preko katerih poteka komunikacija. Če požarni zid odkrije nevaren promet, ga blokira in opozori uporabnika o neavtoriziranem prometu. So dokaj enostavni za uporabo in skoraj obvezna programska oprema na osebnih računalnikih [7]. Prednosti programskih požarnih zidov so:

- **Cena**: so cenovno ugodni in cenejši kot fizični oziroma strojni požarni zidovi.
- **Kompleksnost**: enostavni za uporabo in primerni tudi za ljudi, ki imajo splošno znanje o računalnikih.
- **Fleksibilnost**: hitro in enostavno lahko spreminjamo nastavitve požarnega zidu, ter ga prilagajamo svojim potrebam.
- **Personalizacija**: požarni zid samodejno opazuje aktivne aplikacije na računalniku in na tej podlagi samodejno spremeni nastavitve filtriranja podatkov.
- **Izhodno filtriranje**: je učinkovito, ker je požarni zid na sami napravi, ki ustvarja omrežni promet in je najbližje sistemu, kolikor je to mogoče.

Slaba stran programskih požarnih zidov naj bi bila ranljivost na fizični ravni ISO/OSI-referenčnega modela[1]. Ves omrežni promet iz zunanjega omrežja pride na računalnik, preden ga požarni zid temeljito pregleda. Učinkovitejši je pri filtriranju izhodnega prometa, tako da je celoten neavtoriziran promet nemudoma blokiran. Programski požarni zidovi so občutljivi na DoS napade, saj ti obremenijo požarni zid, s tem pa tudi računalnik, na katerem je nameščen. Še ena pomanjkljivost požarnih zidov je, da varujejo samo računalnik, na katerem so nameščeni, ne pa ostalih naprav v lokalnem omrežju [8]. Pozorni moramo biti pa tudi uporabniki, da pomotoma ne izključimo zaščite oziroma filtriranja zaradi delovanja določene aplikacije. Vsak uporabnik mora poskrbeti, da se redno opravljajo posodobitve požarnega zidu na osebnem računalniku. Ob osveščenem uporabniku in

[1] ISO/OSI-referenčni model: model za razvoj in oblikovanje komunikacijskih protokolov osnovan s strani mednarodne organizacije za standardizacijo.

posodobljeni različici je programski požarni zid razmeroma močno orodje za zaščito osebnih računalnikov.

3.2 Strojni požarni zidovi

Strojni požarni zidovi so samostojne naprave, umeščene med zunanjim omrežjem (WAN) in lokalnim omrežjem (LAN), in tako fizično ločujejo omrežja. Naprava pregleduje vhodni in izhodni omrežni promet in na podlagi vnaprej določenih pravil lahko pregledan paket spustijo v omrežje ali pa ga zavrnejo. Prednosti strojnih požarnih zidov so [9]:

- niso odvisni od operacijskih sistemov (npr. Microsoft Windows, Linux), tako da jih njihove pomanjkljivosti ne omejujejo,
- zmogljivost in hitrost delovanja sta njihovi največji prednosti pred programskimi različicami,
- so razširljivi (brez težav lahko dodajamo nove naprave v omrežje),
- primerni za večja omrežja, kjer imamo veliko omrežne komunikacije.

Seveda imajo strojni požarni zidovi tudi svoje slabosti. Na primer, če naprava iz nekega razloga preneha delovati, se vhodni in izhodni omrežni promet ustavi za celotno lokalno omrežje (v smeri omrežja WAN). So zahtevnejši za namestitev, konfiguracijo in vzdrževanje, tako da mora z napravo upravljati usposobljena oseba. Poleg tega sta tudi ceni naprave in vzdrževanja primerno višji, kot pri programskih požarnih zidovih. Strojni in programski požarni zidovi imajo vsak svoje prednosti in slabosti. Za katero različico se odločimo, je seveda predmet varnostne politike v podjetju oziroma organizaciji.

4 Evolucija in razvoj požarnih zidov

Kako je sploh prišlo do razvoja požarnih zidov naslednje generacije? Da bi si odgovorili na to vprašanje, si bomo najprej pogledali razvoj požarnih zidov skozi zgodovino. Varovanje informacij in zaščita pred vdori sta se razvijali vzporedno z razvojem zlonamernih programskih kod in napadov. Poleg tega so nove tehnologije ter novi načini uporabe internetnih tehnologij in storitev zahtevali od razvijalcev varnostnih sistemov boljši in učinkovitejši pregled nad stanjem in varnostjo omrežja. Odkar so v poznih osemdesetih letih prejšnjega stoletja na trg prišle prve različice požarnih zidov, jih glede na njihove značilnosti in zmogljivosti razvrščamo na tri generacije in pa zadnjo četrto generacijo – naslednjo generacijo požarnih zidov.

4.1 Prva generacija požarnih zidov: paketno filtriranje

Ta metoda je bila ena od prvih relativno preprostih in cenejših oblik požarnih zidov. Poznana je kot statično paketno filtriranje in deluje na omrežnem sloju. Pri paketnem filtriranju se pregleda vsak paket, ki pride v omrežje oziroma ga zapusti. Požarni zid pregledan paket spusti ali zavrne po pravilih, ki jih določi administrator omrežja. Požarni zid pregleduje paket po naslednjih kriterijih [10]:

- kdo je poslal paket in komu je namenjen (izvorni in ciljni IP-naslov),
- izvorna in ciljna vrata (angl. port),
- uporabljen protokol za prenos prometa.

Zgoraj našteto se izvaja pri pregledovanju glave paketa, in sicer na tretji in četrti ravni ISO/OSI-modela. Kot primer lahko vzamemo elektronsko pošto. Če želimo uspešno pošiljanje in prejemanje omrežnih paketov preko SMTP-strežnika, nastavimo na požarnem zidu, da prepusti promet paketov s TCP-izvornimi in ciljnimi vrati 25 (prav ta so namenjena za SMTP-promet) in IP-naslov strežnika za elektronsko pošto (bodisi kot izvor ali cilj). Po takih nastavitvah lahko pričakujemo, da bo požarni zid blokiral ves ostali promet. Vendar pa so požarni zidovi, ki delujejo na podlagi takega preverjanja paketov, dokaj enostavni za napade in zlorabe. Mogoča je predvsem IP-prevara (angl. IP Spoofing), kjer napadalec pošilja sporočila s takim IP-naslovom, kot ga ima zanesljiv oziroma varen gostitelj, ter se tako zakrije z IP-naslovom in pride skozi požarni zid [11].

4.2 Druga generacija požarnih zidov: stanovitna kontrola

Zgrajeni so na konceptu požarnih zidov prve generacije, le da požarni zidovi s stanovitno kontrolo spremljajo še stanje omrežnih povezav in preverjajo vsebino omrežnih paketov. Če paket ustreza vsem zahtevam požarnega zidu za njegovo prepustnost, požarni zid spusti paket, prav tako pa shrani pomembne značilnosti povezav in paketov v posebno tabelo stanj (angl. State tabel). Požarni zidovi s stanovitno kontrolo pregledajo prvi paket v seji vse do aplikacijske ravni, pri vseh naslednjih paketih iste komunikacijske seje pa se ne pregleda vsebina, ampak se izvede pregled samo na tretji in četrti ravni ISO/OSI-modela, torej se pregledata IP-naslov in TCP/UDP-številka vrat. Da se tabela stanj ne zapolni, se po končani komunikaciji v določenem času vnos v tabeli stanj izbriše. Ta način pregledovanja povečuje zmogljivost požarnih zidov s stanovitno kontrolo [12].

Prav tako pa so s takim načinom delovanja prišle nove možnosti za zlorabe. Primer napada je tako neke vrste DoS-napad[2]. Napadalec pošlje vrsto SYN-paketov za prijavo nove komunikacijske seje,da bi nasičil tabelo požarnega zidu in s tem onemogočil vzpostavitev oziroma komunikacijo ostalih sej. Angleški Izraz za ta napad se imenuje »SYN flood attack« [13].

4.3 Tretja generacija požarnih zidov: aplikacijski požarni zidovi

Ob razvoju požarnih zidov so tudi napadi in zlorabe postajali vse naprednejše in se razvijali na višjih ravneh ISO/OSI-modela, kar je bilo za obstoječe požarne zidove praktično nevidno. Juniper networks na primer navaja spletno osnovane napade, ki se izvajajo preko rezerviranih vrat, npr. vrat 80 (HTTP-promet) ali pa vrat 443 (HTTPS-promet). Obstoječi požarni zidovi niso bili zmožni pregledovati različne aplikacije, katerih promet poteka prav preko teh vrat. To so lahko varne ali pa nevarne aplikacije, s pomočjo katerih skušajo napadalci vdreti v sistem in mu škodovati [10].

Tako se je razvila tretja generacija požarnih zidov, tako imenovani aplikacijski požarni zidovi. Ti niso pregledovali paketov samo na osnovi vhodnih in izhodnih vrat, temveč so pregledali pakete vse do aplikacijske ravni ISO/OSI-modela. Večina

[2] DoS napad (angl. denial-of-service attack): Vrsta napada, kjer napadalec oziroma skupina napadalcev napade napravo ali omrežje tako, da zapolni njene zmogljivosti, in tako ni zmožna normalno delovati.

aplikacijskih požarnih zidov vsebuje tudi posebna programska orodja, na primer »proxy« storitve.

»Proxy« storitve so posebne aplikacije oziroma strežniški programi, ki delujejo kot posrednik med uporabnikom in drugimi strežniki, ter zagotavljajo določeno mero varnosti in anonimnosti. Ko omrežna komunikacija poteka preko »proxy« strežnika, lahko ta glede na pravila, ki jih je postavil skrbnik omrežja, dovoli ali pa zavrne omrežni promet. Zaradi njihove pomembnosti v tretji generaciji požarnih zidov jih nekateri viri imenujejo kar »proxy firewalls« oziroma »proxy« osnovani požarni zidovi [14].

4.4 Porast aplikacij in ideja o prenovi požarnih zidov

Način življenja, kot ga poznamo danes, se je zelo spremenil, še posebej na področju tehnologije in njenih zmožnosti. Zmogljive naprave, kot so pametni telefoni, tablice in prenosni računalniki, nas preko vrsto aplikacij povežejo v svet socialnih omrežij (primer Facebook, Twitter), ponujajo vrsto storitev, ki jih lahko opravljamo kjerkoli in kadarkoli. Aplikacije so enostavne za namestitev, enostavne za uporabo in tako blizu ljudem, ki jih uporabljajo. Dobra pokritost internetnega omrežja pa omogoča, da lahko mobilno uporabljamo aplikacije kjerkoli in kadarkoli. Poleg uporabnikov pa je tudi politika podjetji naravnana k uporabi aplikacij, saj lahko svoje storitve bolj približajo strankam. V podjetjih je posledično nastal problem z nadzorom notranjega prometa, saj je vedno pogostejši trend BYOD omogočil, da se zaposleni preko svojih osebnih naprav povežejo v službeno omrežje za poslovne ali zasebne namene [15]. Drugi znani trend, ki se je razširil in je zelo podoben BYOD, pa je t. i. konsumerizacija. Prvi jo je opredelil Gartner in jo opisal kot povezovanje tehnologije in aplikacij z osebnim življenjem ter poenostavitvijo slednjega [16].

Cilj aplikacij je, da delujejo tekoče in hitro. Za njihovo večjo zmožnost delovanja, so se uveljavili načini, ki zaobidejo tradicionalne požarne zidove. Načini so naslednji [17]:

- preskakovanje vrat (angl. Port hopping), kjer se naključno izbirajo različna vrata za komunikacijo,
- uporaba nestandardnih vrat, kjer komunikacija poteka preko vrat, rezerviranih za drugo vrsto komunikacije. Primer za to je aplikacija Google

talk, pri kateri gre promet skozi vrata 80 (HTTP), namesto skozi vrata 5222 (XMPP),

- tuneliranje, kjer P2P-program kot je recimo BitTorrent, poteka s pomočjo HTTP protokola oziroma ga uporabi za prikrivanje,
- zakrivanje s pomočjo SSL-enkripcije, kjer se zakrije aplikacijski omrežni promet.

Podjetje za spletno varnost Palo Alto je v letu 2014 v raziskavi »Application usage and risk report« objavilo, da je kar 34% od analiziranih 2076 aplikacij uporabljalo SSL-enkripcijo. Poleg SSL-enkripcije aplikacije zelo pogosto uporabljajo tudi druge zgoraj opisane tehnike. Tu pa se postavljajo vprašanja glede varnosti in možnosti vdorov preko aplikacij. Problem zgoraj opisanih tehnik je, da obidejo požarne zidove, in tako tvegamo možnost zlonamernega vdora. Posledično so vdori preko aplikacij postali vse bolj razširjeni. Palo Alto je objavilo še zanimive podatke, kjer navajajo problem aplikacij, z izmenjavo datotek (na primer elektronska pošta, socialna omrežja, Dropbox itd.). Ta vrsta aplikacij predstavlja kar 27 % vseh aplikacij, kar jih poznamo, in se je preko njih je bilo izvedenih 32 % vseh napadov [18].

Požarni zidovi prvih in drugih generacij niso več sledili novim tehnikam, ki so uporabljale aplikacije v omrežju in so tako zaobšle požarne zidove. S tem, da so pregledali samo izvorni in ciljni IP naslov, ter informacije o TCP/UDP-vratih, niso zagotavljali varnosti lokalnih omrežij in niso kljubovali bolj naprednejšim vrstam napadov in zlorab. Organizacije so zahtevale popolno zaščito za svoje občutljive podatke. Nujno je bilo treba vzpostaviti nadzor nad aplikacijami in pregledovati aplikacijski promet, poleg tega sta bila potrebna po nadzor uporabnikov in celoviti pregled, kdo in katero aplikacijo uporablja v omrežju. Veliko težav je bilo rešenih že s pojavom aplikacijskih požarnih zidov, ki so pregledovali omrežne pakete vse do aplikacijske ravni OSI-modela, ter z dodatno razvitimi napravami, ki so pripomogle k boljši zaščiti omrežja. Vendar pa nadgradnja obstoječih požarnih zidov z dodatnimi orodji za pregled in varnost ni zagotavljala preglednega in centraliziranega sistema, ampak vedno bolj zapleten sistem zaščite. Z nadgradnjami so se povečevali stroški, predvsem zaradi dragih naprav, dodatne porabe elektrike in nakupa dodatnih licenc.

5 Požarni zidovi naslednje generacije

Podjetje Gartner je v letu 2003 med prvimi začelo razvijati idejo o naslednji generaciji požarnih zidov, leto pozneje pa so objavili že prve publikacije na to temo. V letu 2009 je prav tako podjetje Gartner realiziralo prvo različico požarnega zidu naslednje generacije. Greg Young in John Pescatore iz podjetja Gartner pa sta definirala, kaj spada pod pojem požarni zidovi naslednje generacije. Definicija se glasi nekako tako [19]: »Požarni zidovi naslednje generacije so požarni zidovi z globokim pregledovanjem omrežnih paketov ter presegajo pregledovanje samo na ravni vrat in protokola. Zmožni so pregledovati pakete na aplikacijski ravni OSI-modela, ter zmožni preprečevati vdore.«

Požarni zidovi naslednje generacije so torej samostojne naprave, katerih glavna namena sta celovita zaščita med lokalnim omrežjem in zunanjim omrežjem, ter nadzor prometa po lokalnem omrežju. Bistvo naslednje generacije je, da ima vse zmožnosti prejšnjih različic požarnih zidov, poleg tega pa združujejo še nove tehnologije pregledovanja paketov ter zagotavljanja nadzora nad aplikacijami in uporabniki.

Vodilna podjetja, ki se ukvarjajo z omrežno varnostjo (Cisco, Fortinet, Palo Alto, McAfee, Watchguard, Check Point itd.) so začela razvijati požarne zidove v smeri naslednjih generacij in tako so prihajali prvi produkti na trg. Požarni zidovi različnih proizvajalcev se malo razlikujejo, vsi pa imajo enak koncept naslednje generacije požarnih zidov, kot ga je definiralo podjetje Gartner. Zasnovani so tako, da se držijo smernic [20]:

- zagotavljanja osnovnih funkcij prejšnjih različic požarnih zidov,
- nadzora nad aplikacijami,
- identifikaciji uporabnika in ne samo IP-naslova,
- nadzora vsebine omrežnih paketov,
- pregleda in nadzora nad delovanjem naprave,
- visoki zmogljivosti in zanesljivosti naprav.

5.1 Zagotavljanje osnovnih funkcij požarnih zidov

Pri požarnih zidovih naslednje generacije je pomembno, da še vedno zagotavljajo osnovne funkcije požarnih zidov, poleg tega pa so ob kombinaciji naprednih orodij, ki jih bomo opisali v nadaljevanju, kakovostna zaščita lokalnih omrežij. Te osnovne funkcije so [21]:

- **Stanovitna kontrola**

  Požarni zid spremlja izvorni in ciljni IP-naslov ter vrsto protokola. Prav tako pa spremlja stanje povezave in zbira podatke v tabeli stanj. Princip delovanja je isti kot pri požarnih zidovih s stanovitno kontrolo.

- **Prevajanje omrežnega naslova**

  Prevajanje omrežnega naslova (NAT) je metoda, ki lokalne IP-naslove prevaja v globale IP-naslove in obratno. V lokalnem omrežju naprave komunicirajo z lokalnimi naslovi in ti veljajo samo znotraj lokalnega omrežja. Vsaka komunikacija navzven pa s pomočjo NAT dobi svoj globalni IP-naslov. To je potrebno zaradi omejenega števila IP-naslovov, predvsem IPv4 naslovnega prostora.

- **Podpiranje navideznih zasebnih omrežij**

  Navidezno zasebno omrežje (VPN) je način povezave, kjer se preko javnega omrežja vzpostavi varna in kodirana povezava v lokalno omrežje. Uporabnik lahko preko mobilne naprave ali stacionarnega računalnika dostopa v lokalno službeno omrežje, ter uporabi varnost, pravice in politiko službenega omrežja. Požarni zidovi naslednje generacije tako podpirajo uporabo VPN in omogočajo uporabo standardne IPsec VPN in tudi SSL VPN [22].

5.2 Nadzor nad aplikacijami

Ena od glavnih zahtev požarnih zidov naslednje generacije je nedvomno nadzor nad aplikacijami. Požarni zidovi pregledujejo in nadzorujejo ves promet, ne glede na vrsto protokola, izhodnih vrat ali uporabe tehnik, ki zaobidejo tradicionalne požarne zidove. Skrbnik omrežja ima tako nadzor nad posameznimi aplikacijami, ter lahko glede na varnostno politiko podjetja določene blokira ali pa omogoča normalno prepustnost omrežnega prometa.

Tehnike nadzora so naslednje [20]:

- **Detekcija protokola in dešifriranje**
  Ugotovi se, katera vrsta protokola je uporabljena (na primer FTP, HTTPS, POP3). Če aplikacija uporablja IPSec ali SSL, se dešifrira promet, nato se analizira in po sami analizi ponovno šifrira.
- **Dekodiranje protokola in odkrivanje njegove verodostojnosti**
  Mnoge aplikacije pogosto uporabljajo tehniko tuneliranja, kjer se določen protokol inkapsulira v drug protokol, običajno v HTTP-protokol. HTTP-protokol v tem primeru deluje kot ovojni kanal, znotraj katerega se skriva dejanski protokol aplikacije. Zato je potrebno pregledovanje ali je identificiran protokol »pravi« ali pa je s pomočjo tuneliranja uporabljen za prikrivanje pravega aplikacijskega prometa.
- **Pregled podpisa aplikacije**
  Ko se aplikacijski omrežni promet dekodira, je mogoče aplikacijo identificirati na podlagi unikatnega podpisa (vsaka aplikacija ima svoj značilni podpis). Na primer Fortinet-ova baza (FortiGuard Application Control Database) vsebuje več kot 1400 znanih podpisov različnih spletno osnovanih aplikacij in se stalno osvežuje, saj na trg prihajajo nove in nove aplikacije [23].
- **Spremljanje aplikacij in poročanje**
  Orodje za spremljanje aplikacij analizira promet preko požarnega zidu in prikaže trend aplikacij. To je skrbnikom omrežij v veliko pomoč, saj ti spremljajo promet aplikacij, ki gredo čez požarni zid, katere aplikacije uporabniki najpogosteje uporabljajo, katere so najpogosteje blokirane itd. Na podlagi teh informacij pa lahko administrator oziroma podjetje sestavi primerno strategijo o uporabi aplikacij in varnostno politiko v podjetju.

5.3 Identifikacija uporabnika

Požarni zidovi naslednje generacije identificirajo uporabnika tako, da povežejo njegov IP-naslov z njegovo identiteto, s tem pa dobi skrbnik omrežja dober pregled nad tem, kdo vstopa v omrežje in s katero aplikacijo. Tako lahko enemu ali skupini uporabnikov omogočimo uporabo določenih aplikacij, ali pa zavrnemo dostop. Dostop lahko omejimo tudi ob določenih urah ali dnevih. Identifikacija uporabnikov pa je zelo pomembna tudi pri dokazovanju odgovornosti, saj skrbnik omrežja v primeru kakršnihkoli incidentov, zlorab ali napak ve, kdo je odgovoren za to. Za pridobitev informacij o uporabnikih, požarni zid deluje v povezavi z LDAP imeniki[3].

Fortinet pa ponuja tudi zanimivo orodje za identificiranje uporabnikov, in sicer FSAE. Ta nadzoruje prijavo uporabnikov in zbira uporabniška imena, IP-naslove in podatke iz npr. Microsoft Active Directory (informacije o pripadnosti določeni skupini). Ko uporabnik želi dostopati do internetnega omrežja, požarni zid preveri, ali ima uporabnik pravico do dostopa do določene spletne strani do uporabe določene aplikacije ali pa je ti skupini dostop omejen [24].

5.4 Nadzor vsebine omrežnih paketov

Požarni zidovi naslednje generacije so pregledovanje vsebine paketov pripeljali popolnoma na novo raven in pregled opravljajo kakovostneje, kot so to opravljale prejšnje različice požarnih zidov. Tu gre za vrsto naprednih orodij, ki v realnem času pregledujejo vsebino podatkov omrežnih paketov, temeljito pregledajo glede virusov in črvov, ter pregledajo in filtrirajo URL-naslove.

[3] Imenik LDAP je baza podatkov o uporabnikih in skupinah ter deluje s pomočjo protokola LDAP (Lightweight Directory Access Protocol)

Slika 4: Nadzor vsebine omrežnih paketov [26, str. 2]

5.4.1 Integrirani sistem za preprečevanje vdorov

Sistem za preprečevanje vdorov oziroma IPS je eno od orodij, ki s pomočjo nadzora omrežnega prometa in analize išče sledi in podpise, ki jih lahko poveže z znanimi grožnjami. IPS ščiti uporabnike omrežja in lahko zazna črve, vohunske programe, omrežne viruse in tako imenovane napredne napade ATP. Njegova prednost je, da je zelo hiter in odziven. Takoj ko zazna potencialno nevarnost, se odzove z določenim ukrepom, ki ga je postavil skrbnik omrežja oziroma razvijalci IPS-sistemov. Ta ukrep je alarm, ki ga IPS sproži ob morebitni nevarnosti, nato pa IPS blokira potencialno škodljivi promet določenega izvornega IP-naslova [25].

IPS deluje s pomočjo treh detekcijskih metod:

- **Detekcija, osnovana na podpisih**
  S to metodo IPS-sistem spremlja omrežni promet in išče znane podpise, ki jih je mogoče povezati z znanimi grožnjami. Podatki o tem, kateri podpis pripada kateri grožnji, so shranjeni v bazi podpisov in ta se mora obvezno posodabljati.
- **Detekcija osnovana na statističnih anomalijah**
  Sistem določi normalno aktivnost omrežnega prometa in tej na podlagi išče odstopanja oziroma nenadne obremenitve omrežja. To bi lahko pomenilo sum napada na omrežje, ni pa nujno, da gre za napad.
- **Detekcija stanovitne analize protokola**
  Deluje zelo podobno kot metoda, osnovana na detekciji podpisov, vendar ta metoda zagotavlja temeljitejšo analizo protokola omrežnega prometa.

IPS-sistemi so bili prvotno razviti kot samostojne naprave in dodatki k požarnim zidovom prejšnjih generacij. Požarni zidovi naslednjih generacij pa vsebujejo integrirani IPS-sistem ter s tem zagotavljajo centraliziran in učinkovitejši

način obrambe pred napadi. Zelo pomembno je, da skrbniki omrežji stalno nadgrajujejo IPS, saj tako širijo zbirko znanih podpisov in novih pravil s razvijalcev [10]. Podjetje Cisco je celo razvilo sistem za preprečevanje vdorov naslednje generacije (NGIPS), ki ponuja visoko zmogljivo in napredno zaščito pred omrežnimi napadi.

5.4.2 URL-filtriranje

S pomočjo URL-filtriranja lahko skrbnik omrežja nadzira dostop notranjih uporabnikov do spletnih strani. Skrbnik dovoli, ali zavrne dostop do določenih spletnih strani ali kategorij spletnih strani. Podatki o dostopu do spletnih strani uporabnikov se beležijo, tako da ima skrbnik celovit pregled, kdo je želel dostopati do katere spletne strani, ter ali mu je URL-naslov blokiralo ali ne [26]. S takim orodjem se v podjetju lahko izognemo obisku potencialno nevarnih spletnih strani, prav tako pa tudi strani, ki so nepotrebne za poslovanje podjetja (npr. socialna omrežja, spletne igre, pornografija itd.).

5.4.3 Protivirusna zaščita

Računalniški virus je programska koda, ki zavira normalno delovanje našega računalnika, omrežja ali katere druge naprave. Po sistemu se je sposoben širiti brez vednosti uporabnika in tako »okuži« druge sisteme, ter zavira njihovo normalno delovanje. Da se temu izognemo, potrebujemo protivirusni program, ki išče sledi oziroma tipične podpise virusov v omrežju in jih nato odstrani. Podpis virusa je algoritem ali numerična vrednost, ki točno identificira določen virus. Protivirusni programi morajo biti obvezno posodobljeni, saj se le tako posodobi baza znanih podpisov virusov v protivirusnem programu in le tako lahko pričakujemo višjo in kakovostnejšo zaščito. Poleg tega pa so protivirusne aplikacije sposobne zaznati in odstraniti še druge znane oblike zlonamernih programskih kod, kot so: trojanski konji, črvi itd. [3]. Čeprav že IPS-sistemi zagotavljajo določeno mero zaščite, je protivirusna zaščita priporočljiv in integriran sistem, ki deluje v povezavi z IPS in tako zagotavlja višjo stopnjo zaščite.

5.4.4 Sistem za preprečevanje izgube podatkov

Za razliko od ostalih sistemov, ki so osredotočeni na vhodni promet in napade na notranje lokalno omrežje, je sistem za preprečevanje izgube podatkov oziroma DLP namenjen zaščiti občutljivih podatkov, namenjenih iz lokalnega omrežja. DLP pregleduje vsebino omrežnih paketov in glede pravila, ki jih postavi skrbnik, označi zaupne informacije (npr. številke kreditnih kartic, osebne podatke zaposlenih, informacije o financah, programske kode itd.) in blokira izhodni promet s tako vsebino. Prav tako pa je mogoče omejiti tudi vrsto in velikost datotek, ki se prenašajo preko elektronske pošte ali kako drugače.

Podjetje Gartner je v svojem poročilu v letu 2008 objavilo raziskavo, da je:

- 1:400 sporočil vsebuje občutljive podatke,
- 1:50 omrežnih datotek je napačno oziroma ne bi smele biti izpostavljene,
- 4:5 podjetij izgubi občutljive podatke na prenosnih računalnikih.
- 1:2 podjetji izgubi občutljive podatke preko USB-ključev.

Poleg DLP-sistema je zelo pomembna ozaveščenost zaposlenih glede varovanja informacij, saj se prav preko zaposlenih izgubi največ informacij. Podjetje mora opredeliti, katere informacije so občutljive ter kdo ima dostop do njih, poleg tega pa mora imeti postavljeno strogo varnostno politiko o varovanju podatkov. Kadar je ta postavljena, lahko skupaj z DLP-sistemom zagotavljamo relativno dobro varovanje podatkov [27].

5.5 Pregled in nadzor nad delovanjem naprave

Identifikacija aplikacij, kdo jih uporablja ter za kaj se uporabljajo, je nedvomno velik napredek pri nadzoru omrežja. Poleg tega požarni zidovi naslednje generacije stalno beležijo poročila, na podlagi katerih skrbnik omrežja analizira promet, raziskuje in po potrebi spreminja varnostno politiko in orodja za zaščito.

Poročila se zaradi preglednosti beležijo po posameznih kategorijah oziroma orodjih za varnost. Prav tako pa si lahko skrbnik omrežja po svoji želji prilagodi, katere informacije oziroma poročila mu požarni zid prikazuje, ali se bodo poročila pošiljala na spletno pošto itd. Pri ponudniku Fortinet so razvili zanimivo orodje za analizo poročil in sicer Fortianalyzer, kamor se samodejno pošiljajo poročila, ki jih lahko temeljito in pregledno analiziramo. Poleg pregleda poročil, lahko skrbnik omrežja nadzira obremenjenost naprave, predvsem obremenjenost procesorja in

delavnega pomnilnika. Zelo pomemben je tudi pregleden operacijski sistem na požarnih zidovih, saj tako omogoča lažje in hitrejše upravljanje.

5.6 Visoko zmogljiva in zanesljiva naprava

Kakovostna orodja za zaščito, nadzor vsebine in druge prednosti požarnih zidov naslednje generacije so brez pomena, če nimamo dovolj zmogljive naprave. Zato je še kako pomembno, da podjetje izbere primerno zmogljivo napravo, ki bo kakovostno in v realnem času opravljala svoje naloge v omrežju. Glede na vrsto različnih ponudnikov in neodvisnih laboratorijskih testov lahko na podlagi testov izberemo kakovostno napravo. Požarni zidovi naslednjih generacij morajo zagotavljati [20]:

- **Prepustnost**
  Požarni zidovi morajo zagotavljati visoko prepustnost omrežnega prometa, saj se za nakup take zaščite odločajo velika podjetja in organizacije, ki imajo ogromne količine omrežnega prometa. Prepustnost je med požarnimi zidovi različna, pri čemer gre za vrednosti več sto Mbit/s do več Gbit/s
- **Kakovost storitev**
  Kakovost storitev ali QoS predstavlja vrsto pravil, s pomočjo katerih se postavijo prioritete omrežnemu prometu ter zagotovita minimalna in maksimalna pasovna širina glede na prioriteto. Tako ima pomembnejši promet višjo prioriteto od manj pomembnega.
- **Stabilnost in zanesljivost**
  Požarni zidovi imajo bistveno vlogo za kakovostno delovanje omrežja in za njegovo varnost, zato morajo biti sposobni delovati stalno, brez izpadov. Ob izpadu mora naprava imeti pripravljen preklop v nadomestni način (angl. Failover). Zelo priporočljive pa so tudi vzporedne komponente (na primer napajanje naprave), ter več povezovalna (angl. Multi-link) tehnologija, ki zagotavlja visoko razpoložljivost s pomočjo alternativnih omrežnih povezav [14].
- **Prilagodljivost**
  Požarni zidovi morajo biti omrežno prilagodljivi, kar pomeni, da morajo delovati v vsakem omrežju, kjer so vgrajeni.

- **Razširljivost**

  Razširljivost požarnih zidov pomeni, da jih je mogoče nadgraditi ali jim dodati nove zmožnosti. Nekateri požarni zidovi (npr. FortiGate) imajo pa tudi podporo za vzpostavitev navideznih domen. Tako lahko na eni fizični napravi vpeljemo več navideznih požarnih zidov in vsakega po svoje prilagodimo potrebam v omrežju.

5.7 Prednosti požarnih zidov naslednje generacije

Požarni zidovi naslednje generacije vsebujejo vrsto prednosti pred prejšnjimi različicami, med katere spadajo:

- **Pregled in nadzor**

  S pomočjo vrste že opisanih orodij ima skrbnik požarnega zidu naslednje generacije dober pregled nad aplikacijami, vsebino omrežnih paketov in uporabniki. Dober pregled nad dogajanjem v omrežju pa prinese tudi zagotavljanje višje stopnje varnosti, saj skrbnik omrežja vidi možne kritične točke, kje bi se dalo povečati raven varnosti, katere aplikacije so kritične itd. Ob morebitnih zlorabah pa lahko zaradi zmožnosti identifikacije uporabnika najde krivca za nespoštovanje pravil.
- **Visoka raven varnosti**

  Požarni zidovi naslednje generacije vsebujejo naprednejša orodja za zagotavljanje varnosti in temeljitejši pregled, kot so to izvajale prejšnje različice. Velika prednost naslednje generacije je predvsem, da se lahko zoperstavi novim trendom, predvsem neverjetnemu porastu uporabe aplikacij.
- **Centraliziran sistem**

  Požarni zidovi naslednje generacije združujejo vrsto mehanizmov oziroma orodij, ki so bila pri prejšnjih različicah dodana kot posamezne naprave k obstoječemu požarnemu zidu. Centraliziran sistem pa predstavlja enostavnejše upravljanje in kakovostnejše medsebojno sodelovanje med varnostnimi mehanizmi[21].
- **Ekonomičnost**

  Ker požarni zidovi naslednjih generacij združujejo več orodij za zagotavljanje varnosti omrežja v eni napravi, se posledično zmanjšajo stroški za

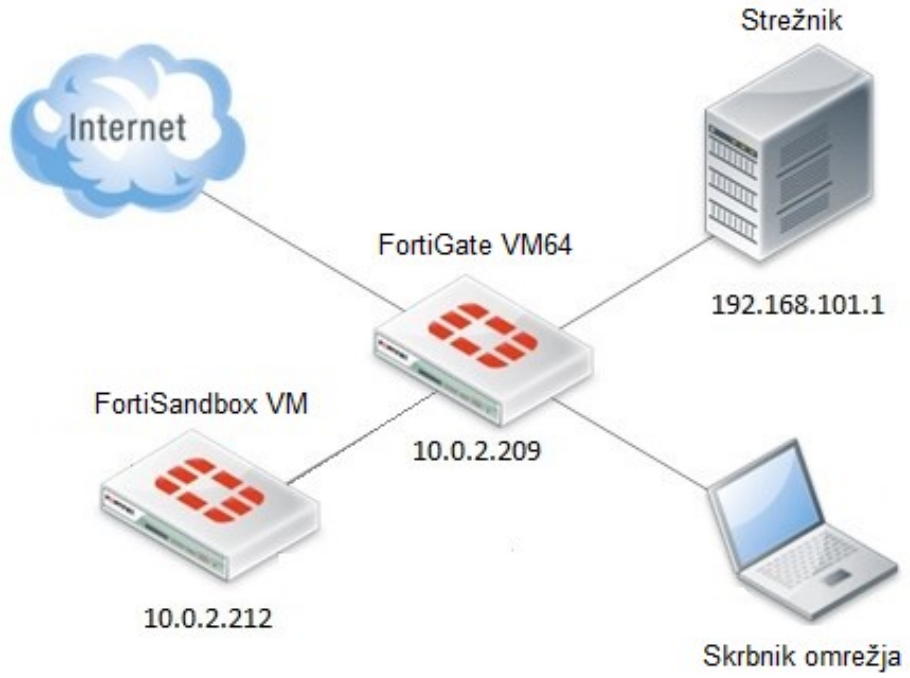
vzdrževanje, licence in porabo elektrike. Prav tako pa potrebujemo manj prostora za namestitev naprave.

6 Laboratorijski testi požarnega zidu naslednje generacije

Pri praktičnem delu smo testirali nekatera orodja požarnega zidu naslednje generacije. Glavni namen testov je bil prikazati učinkovitost orodij, njihovo enostavnost uporabe in možnosti, ki jih ponujajo. Vsak test je vseboval nastavitev požarnega zidu oziroma orodja znotraj požarnega zidu, temu pa je sledil praktični preizkus. Pri tem je bila v veliko pomoč spletna literatura proizvajalca Fortinet (Fortigate cookbook in FortiSandbox – Administration Guide). Vsi testi so potekali na naslednjih napravah:

- FortiGate VM64 proizvajalca Fortinet,
- FortiSandbox VM proizvajalca Fortinet,
- navidezni strežnik,
- prenosni računalnik.

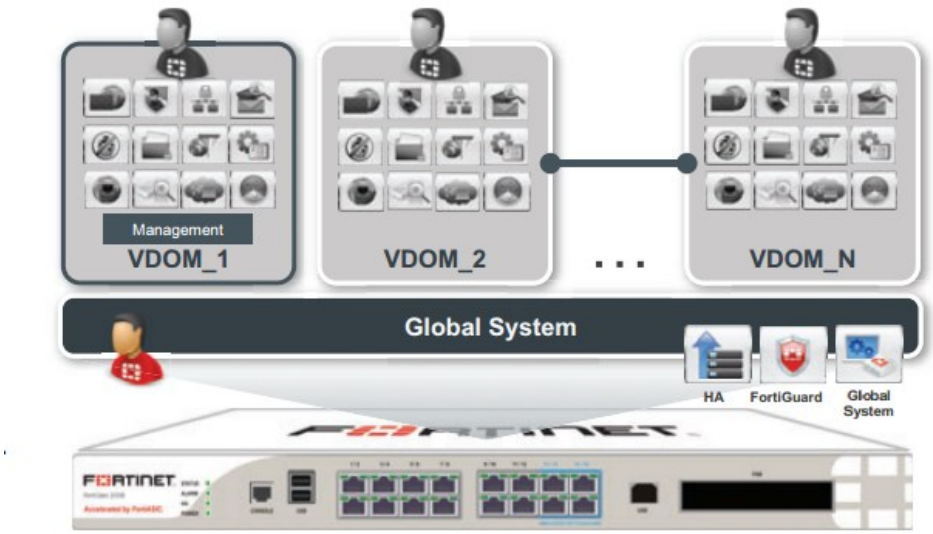
Za simulacijo testov je bil uporabljen navidezni strežnik, s katerega se je preko požarnega zidu dostopalo do internetnega omrežja, nastavitev FortiGate in FortiSandbox naprave pa je potekala iz osebnega računalnika. Strežnik je deloval s pomočjo operacijskega sistema Linux Ubuntu. Topologija vezave elementov je bila naslednja:



Slika 5: Topologija vezave elementov

Za oddaljen dostop do navideznega strežnika smo uporabili program VNC viewer. Da je povezava delovala, je bilo treba na uporabnikovem računalniku dodati statično pot (angl. Static route). Na operacijskem sistemu Windows je sintaksa naslednja: route add 192.168.0.0 mask 255.255.0.0 10.0.2.209. Do naprav FortiGate in FortiSandbox smo dostopali preko IP-naslova in sicer je bila naprava FortiGate dosegljiva preko lokalnega IP-naslova 10.0.2.209, naprava FortiSandbox pa preko lokalnega IP-naslova 10.0.2.212.

Ko smo enkrat povezani na napravo, imata tako FortiGate kot tudi FortiSandbox pregledni meni za upravljanje in nastavitve. Izbiramo lahko med globalnimi nastavitvami naprave, lahko pa izberemo nastavitve posamezne domene na napravi. Na napravi je možno ustvariti več navideznih domen in vsaki navidezni domeni priredimo svoja pravila delovanja. S pomočjo navideznih domen dosežemo enako, kot bi imeli več naprav FortiGate. To je ena od praktičnih rešitev, s pomočjo katere privarčujemo s prostorom, energijo in denarjem. Za izvedbo laboratorijskih testov je zadostovala ena sama domena.



Slika 6: Navidezne domene [27, str. 1]

Pred začetkom laboratorijskih testov smo preverili osnovne nastavitve naprave. Tu je bilo potrebno za osnovno povezljivost preveriti nastavitve vhodov v napravo, in sicer:

- Vrata »port1 (management)« z IP-naslovom 10.0.2.209 in masko 255.255.0.0 so bila namenjena neposrednemu dostopu do naprave, prav tako pa je preko vrat »port1« potekal omrežni promet v lokalno in naprej v javno omrežje.
- Vrata »port2 (inside)« z IP-naslovom 192.168.101.1 in masko 255.255.255.0 so bila potrebna za povezavo s strežnikom, preko katerega smo izvajali teste.

Pri osnovnih nastavitvah naprave lahko pregledamo še splošne informacije o napravi, sistemu, licencah, porabo pomnilnika, procesorja itd. Ko preverimo in po potrebi nastavimo splošne nastavitve naprave, lahko začnemo nastavljati orodja za varnost. Vsa orodja se nahajajo pod zavihkom »security profiles«, kjer izberemo želeno orodje in ga priredimo svojim potrebam (slika 7).

Slika 7: Glavni meni za nastavitev naprave

Po nastavitvi izbranega orodja nastavimo politiko izvrševanja. Izbiramo lahko med vrsto možnosti, med katere spadajo:

- vhodni in izhodni vmesnik (angl. interface),
- izvorni ali ciljni IP-naslov,
- podomrežje (npr. 192.168.100.0),
- aplikacija (npr. Citrix, Dropbox),

- uporabnik ali skupina uporabnikov,
- vrsta naprave (mobilna naprava, omrežna naprava),
- vrsta naprave glede na operacijski sistem ali druge lastnosti (npr. android, Linux, igralna konzola itd),
- čas izvajanja (med tednom, konec tedna, določen dan ali določena ura).

Ko nastavljamo politiko izvrševanja, izberemo, ali bo določeno orodje za varnost opravljalo svojo nalogo iz javnega v notranje omrežje (z vrat »port1« na vrata »port2«) ali v obratni smeri (z vrat »port2« na vrata »port1«).

Pri vseh laboratorijskih testih sta opisani in slikovno prikazani nastavitev orodij in nastavitev politike izvrševanja, sledi pa testiranje. Vsak test smo najprej izvedeli z izključenim orodjem, nato pa smo ga vključili, test ponovil in rezultate komentirali na koncu vsake laboratorijske vaje. V diplomskem delu so slikovno predstavljeni le rezultati po uporabljenem orodju, saj so prav ti ključni za predstavitev učinkovitega delovanja posameznega orodja.

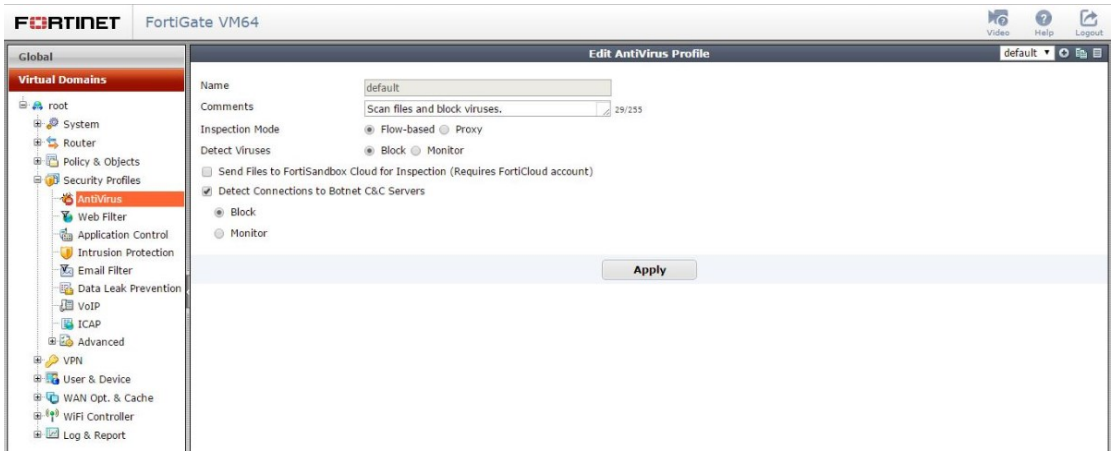
6.1 Seznam laboratorijskih testov

Na napravah smo izvedeli naslednje laboratorijske teste:

- **Protivirusna zaščita**
  Preverili smo zmožnosti, ki jih ponuja orodje za protivirusno zaščito, in jih testirali na praktičnem primeru.
- **Filtriranje URL-naslovov**
  Preverili smo delovanje URL-filtriranja in z uporabo orodje omejili dostop do določenih URL-naslovov.
- **Nadzor nad aplikacijami**
  Raziskali in na praktičnih primerih smo testirali napredno orodje za nadzor aplikacij.
- **Orodje za varovanje podatkov**
  Preverili smo orodje za varovanje podatkov, katerega namen je, nadzor omrežnega prometa in varovanje podatkov.
- **FortiSandbox**
  Preverili smo delovanje dodatne napredne naprave k požarnemu zidu naslednje generacije in izvedli praktični preizkus.

6.2 Prvi laboratorijski test: protivirusna zaščita

Protivirusna zaščita pregleduje in varuje lokalno omrežje pred morebitnimi virusi oziroma drugimi zlonamernimi programi. Pod zavihkom »Antivirus« nastavimo osnovne konfiguracije orodja (slika 8). Za začetek si izberemo ime nastavitev in dodamo komentarje (v tem primeru so to nastavitve »Default« in obrazložitev »Scan files and block viruses«). Nato izberemo, ali naj protivirusni program izvaja t. i. pregledovanje »Flow-based« ali t. i. »Proxy-based«. »Proxy-based« metoda pregledovanja deluje tako, da se vsebina paketov shranjuje, in ko je celotna informacija prenesena, se izvede pregled nad vsebino. To je ena od varnejših metod, vendar ta tudi razmeroma močno obremeni procesor naprave. Pri tej metodi imamo še na voljo izbrati vrsto protokola, ki ga želimo, da ga protivirusni program pregleda. »Flow-based« metoda deluje malo drugače. Ta izvaja pregledovanje nad vsebino posameznih paketov, ko ti prehajajo skozi napravo FortiGate. Naslednja nastavitev je ukrep, ali FortiGate najdeno zlonamerno vsebino blokira ali samo nadzoruje in naredi poročilo skrbniku omrežja. Kadar je z napravo FortiGate povezan še FortiSandbox (v tej vaji smo testirali brez naprave FortiSandbox), lahko nastavimo, da FortiGate pošilja podatke v dodatni pregled na FortiSandbox. Na koncu pa lahko še izberemo nadzor ali blokado »botnet C&C servers« napadov[4]. FortiGate jih je sposoben zaznati in blokirati ali pa samo nadzirati.

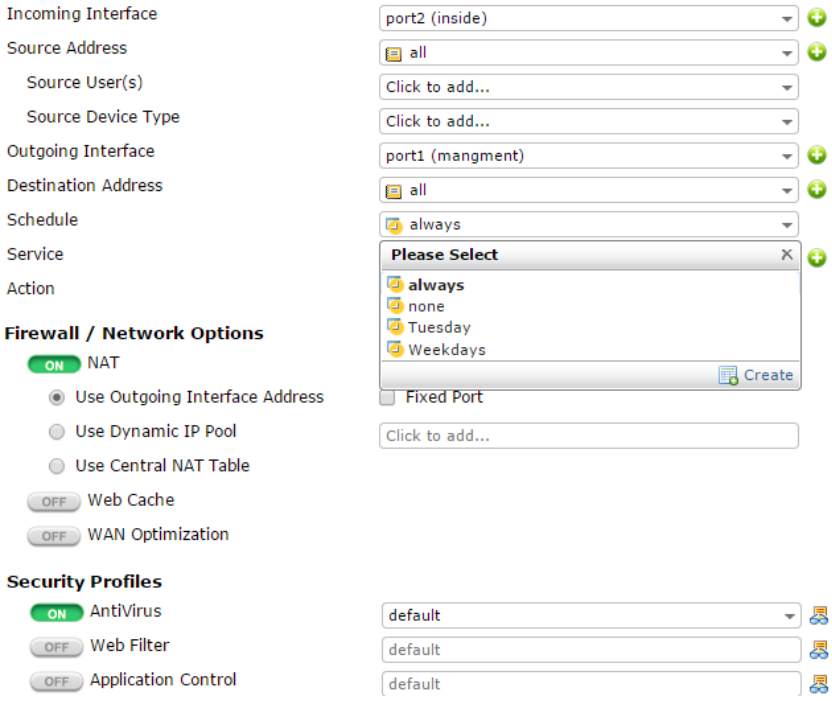


Slika 8: Nastavitve za protivirusno pregledovanje

Ko so postavljena pravila za protivirusno pregledovaje, nastavimo še politiko izvajanja. Tu smo izbrali izvajanje v smeri z javnega v lokalno omrežje ter izbrali

[4] Botnet C&C servers napadi: vrsta napadov, kjer se s pomočjo skupine računalnikov izvaja DoS napad na napravo

politiko izvajanja za vse IP-naslove katerikoli čas. V varnostnem profilu smo nato aktivirali protivirusno pregledovanje in izbrali svoje nastavite (ime nastavitev default).



Slika 9: Nastavitev politike izvajanja

Orodje smo testirali tako, da smo s spletne strani www.eicar.org poskušali prenesti na strežnik sumljivo datoteko oziroma lažni virus, ki je namenjen testiranju protivirusne zaščite. Ob prenosu se je takoj pokazalo opozorilo, da je datoteka okužena in je ni mogoče prenesti (slika 10). Naredili smo še en test, in sicer ds »proxy« načinom pregledovanja. Tokrat smo poskušali prenesti lažni virus s spletne strani http://malware.wicar.org, vendar je protivirusno pregledovanje na napravi FortiGate ponovno zaznalo sumljivi dokument in blokiralo prenos (slika 11).

Slika 10: Prenos okužene datoteke (flow-based način)

Slika 11: Prenos okužene datoteke (proxy nastavitve)

6.3 Drugi laboratorijski test: filtriranje URL-naslovov

Namen laboratorijskega testa je bil testirati omejitve dostopa vseh ali pa samo določenih uporabnikov do določenih spletnih naslovov. Gre za preprosto orodje na napravi FortiGate, s pomočjo katerega lahko zagotavljamo nadzor nad uporabniki znotraj lokalnega omrežja. V zavihku »web filter« se odpre vrsta možnih nastavitev za omrežno filtriranje. Najprej nastavimo način pregledovanja. Tu lahko izbiramo med »Proxy-based« in »Flow-based« načinom pregledovanja. »Proxy-based« način zbira in analizira spletne vsebine, ki prehajajo skozi požarni zid, medtem ko »Flow-based« uporablja FortiOS IPS-orodje za filtriranje vsebine omrežnih paketov. Za izvedbo testa smo nastavili »proxy-based« nastavitve izvajanja.

Pri testu smo testirali statično URL-filtriranje, kjer lahko ročno ustvarimo filter za točno določen URL-naslov. Na napravi smo ustvarili filter za nadzor vseh različic strani Facebook, in sicer tako, da pred URL-naslov dodamo simbol »*«. Paziti moramo, da izberemo pravilni tip vnosa (v testu smo izbrali tip vnosa Wildcard), ker

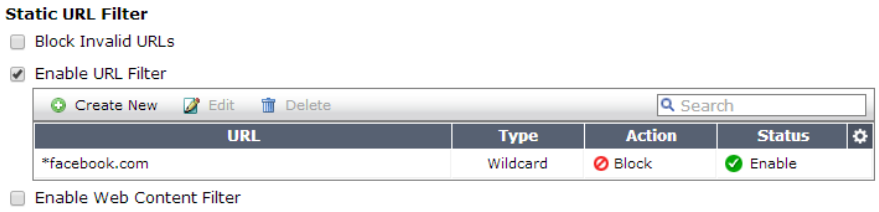
ima simbol »*« različen pomen, pri različnih tipih vnosa. Tip vnosa »Simple« tega simbola ne zazna, pri tipu vnosa »Regular expression« pa bi zvezdica pomenila podvajanje znaka, za katerim stoji (Facebook* bi tako predstavljal Facebookk).

Slika 12: Nastavitev URL-filtra

Ko definiramo URL-naslove, označimo še ukrep, ki ga bo filter sprožil. Tako lahko izbiramo med:

- **Omogoči (angl. Allow)**
  Uporabnikom omogočimo dostop do spletne strani.
- **Blokiraj (angl. Block)**
  Uporabnikom blokiramo dostop do spletne strani.
- **Obidi dodatni varnostni pregled (angl. Exempt)**
  Uporabnikom dovolimo dostop do spletnih strani, poleg tega pa omrežni promet z vnesenega URL-naslova obide dodatni varnostni pregled, ko se odpirajo nove povezave na naslednjem URL-naslovu. Če bi na primer dodali URL www.facebook.com bi bila povezava varnostno pregledana, če pa za tem odpremo povezavo www.facebook.com/page1, pa se varnostni pregled spusti oziroma obide. Fortinet odsvetuje uporabo tega, če nismo prepričani, da je spletna stran popolnoma varna.
- **Spremljaj (angl. Monitor)**
  Uporabnikom omogočimo dostop do spletne strani, vendar se vsak dostop beleži v poročilu za nadaljnjo analizo.

Pri izvedbi testa smo torej blokirali dostop do vseh različic spletne strani Facebook (nastavitve so na sliki 12) in po nastavitvah se pokaže pregledno okno naših nastavitev za statično URL-filtriranje (slika 13).

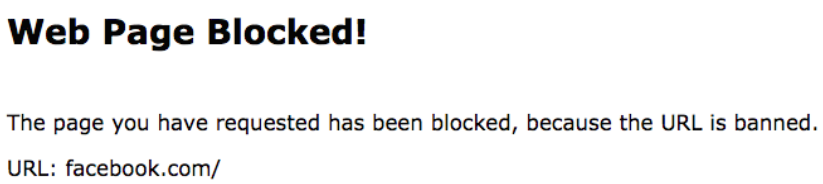


Slika 13: Nastavitev statičnega URL-filtriranja

Ko smo pod zavihkom »web filter« nastavili nastavitve, shranimo nastavitve pod določenim imenom (v našem primeru so to »default« nastavitve). Nato nastavimo še politiko izvrševanja URL-filtra, in sicer pod zavihkom »policy and object«. Tako smo nastavili izvajanje URL-filtra za vse uporabnike ob vsakem času. Na koncu aktiviramo URL-filtriranje in izberemo nastavitve, ki smo jih shranili pod imenom »default«.

Slika 14: Nastavitev varnostnega profila

Po nastavljenih nastavitvah smo izvedli test tako, da smo s strežnika poskušali dostopati do spletne strani www.facebook.com. Najprej se je prikazalo sporočilo o nezanesljivi povezavi, če pa smo dodali izjemo in šli preko opozorilnega okna, se je za tem pojavilo opozorilo naprave FortiGate, da je spletna stran blokirana zaradi politike o dostopu do URL-naslovov (slika 15).

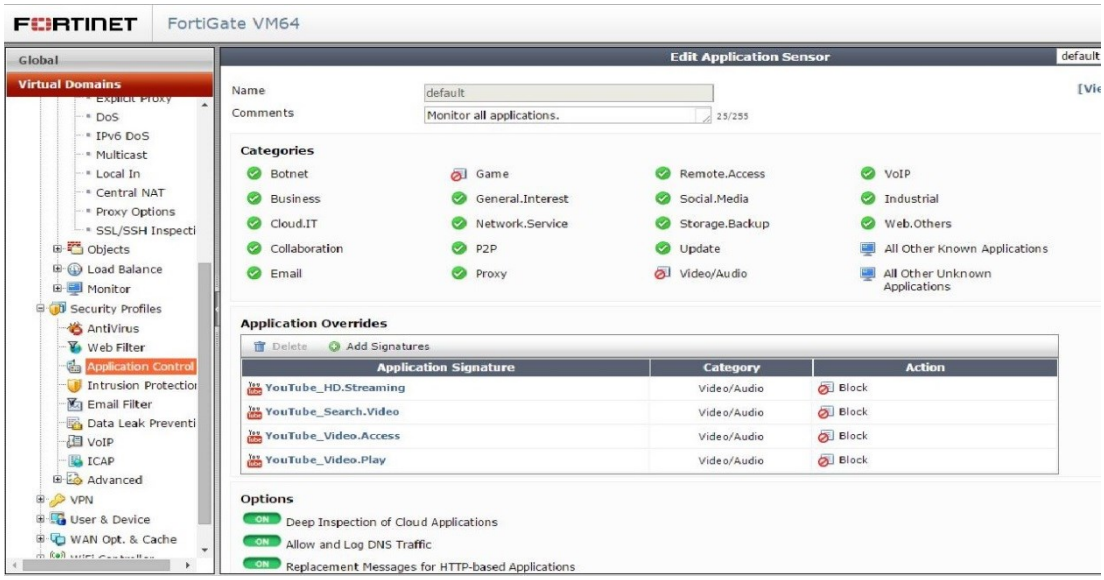


Slika 15: Opozorilo o blokiranem URL-naslovu

6.4 Tretji laboratorijski test: nadzor nad aplikacijami

Funkcija nadzora nad aplikacijami je na napravi FortiGate zelo zanimiva in ponuja ogromno različnih možnosti za varnost in nadzor. Ta s pomočjo dekodiranja protokola in z obsežno bazo znanih podpisov aplikacij analizira promet in identificira aplikacije. Namen testa je bilo testiranje nadzora nad aplikacijami, ter omejiti dostop s strežnika do določene kategorije aplikacij oziroma storitev.

Pod zavihkom »application control« se prikaže meni, kjer nastavimo orodje za nadzor aplikacij (slika 16). Ponovno lahko izbiramo ime nastavitev, v našem primeru smo jo shranil kot »default« nastavitve, ter jim dodali komentar.



Slika 16: Nadzor nad aplikacijami

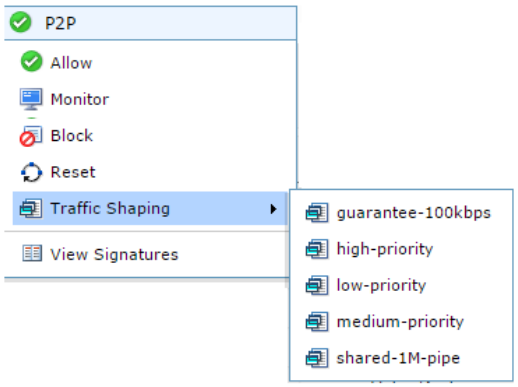
Naslednja zelo uporabna funkcija orodja je razvrstitev podpisov aplikacij po kategorijah. Za vsako kategorijo lahko pogledamo zbrane podpise, ročno lahko vnašamo ali odstranjujemo določene podpise, prav tako pa se tabela znanih podpisov osvežuje z rednimi posodobitvami naprave. Za eno ali več podanih kategorij lahko poljubno priredimo pravila, med katera spadajo:

- **dostop aplikacije,**
- **blokiranje aplikacije,**
- **nadzor aplikacije,**
- **ponastavitev,**

  Ta operacija sproži ponastavitev seje oziroma povezave.

- **omejitev pasovne širine.**
  Določeni kategoriji ali več kategorijam lahko omejimo hitrost prenosa tako, da jim dodelimo prioriteto, vsaka prioriteta ima pa pripadajočo največjo pasovno širino.

Omejitev pasovne širine določeni kategoriji aplikacij (angl. Traffic shaping) ponuja možnost, da lahko posamezni kategoriji aplikacij oziroma storitvam dodelimo prioriteto, ki ji pripada določena pasovna širina. Skrbnik omrežja lahko pomembnejšim aplikacijam dodeli višjo prioriteto in s tem večjo pasovno širino kot drugemu omrežnemu prometu. Na napravi FortiGate najprej pogledamo, kako so nastavljene prioritete in njim pripadajoče pasovne širine. Te lahko po potrebi nastavljamo sami, tako da jim določimo ime, prioriteto, največjo pasovno širino in zagotovljeno pasovno širino. Ko so prioritete določene, so vidne v izbirnem meniju pri vsaki kategoriji (slika 17).



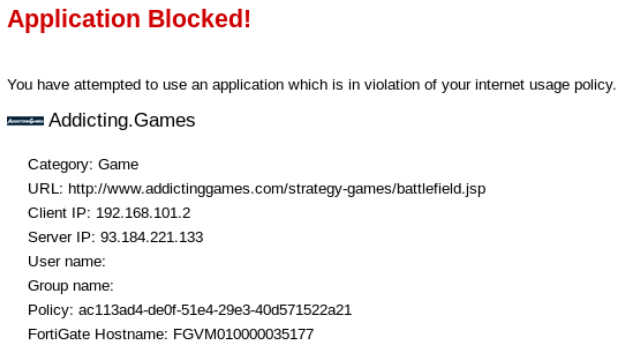
Slika 17: Primer nastavitev prioritet

Omejitev pasovne širine smo poskusno testirali s prenosom datoteke preko FTP-protokola, kateremu smo določili nizko prioriteto in s tem posledično tudi omejili pasovno širino na 50 KB. Politika izvajanja je bila nastavljena za vse uporabnike ob vsakem času. Pri prenosu poskusne datoteke z URL-naslova speedtest.ftp.otenet.gr na strežnik je bil po nastavljeni omejitvi prenos bistveno počasnejši kot pred nastavitvijo. Ker podatki o hitrosti prenosa niso bili vidni, je to samo naše opažanje in ne verodostojna meritev oziroma rezultat.

Nato smo izvedeli test, ki je temeljil na poskusu blokiranja kategorije iger ter kategorije video/avdio, v katero spada Youtube. Tako nastavimo za kategorijo »game« in kategorijo »video/audio« ukrep blokiranja. Pred kategorijama je tudi vidno, da je nastavljena operacija blokiranja (slika 16). Ko nastavimo ukrep za izbrani kategoriji, izberemo še politiko izvrševanja. Tokrat smo politiko dostopa omejili na določenega uporabnika. Uporabnika moramo na napravi ustvariti ter mu dodeliti ime in geslo. Za izvedbo testa smo ustvarili uporabnika z imenom John. Poleg uporabnika pa smo pod politiko izvajanja operacije nastavili še izvorni naslov. Tega je treba predhodno še nastaviti, kjer mu dodelimo ime (v tem primeru Server101) in IP-naslov strežnika.

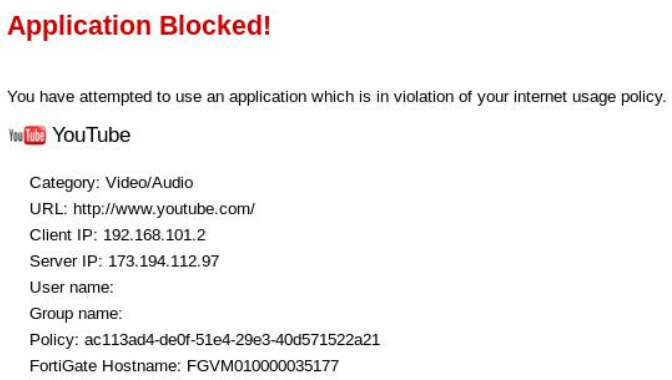
Slika 18: Nastavitev politike izvajanja

Ko so nastavitve za blokiranje aplikacij pravilno nastavljene in je politika pravilno postavljena, testiramo dostop s strežnika do spletnih naslovov oziroma aplikacij. Testirali smo dostop do spletne strani www.addictinggames.com, ki je namenjena igranju iger. Najprej se je pojavilo opozorilno okno za identifikacijo uporabnika, kjer smo vpisali uporabniško ime in geslo, ki smo ju definirali na napravi FortiGate. Za tem pa naprava FortiGate blokiral uporabniku Johnu dostop do spletne strani ter izpisalo obvestilo o zavrnjenem dostopu.



Slika 19: Opozorilno okno o zavrnjenem dostopu

Sledil je še test dostopa do spletne strani www.youtube.com, kjer se je prav tako najprej pojavilo okno za vpis uporabniškega imena in gesla, zatem pa opozorilo o zavrnjenem dostopu.

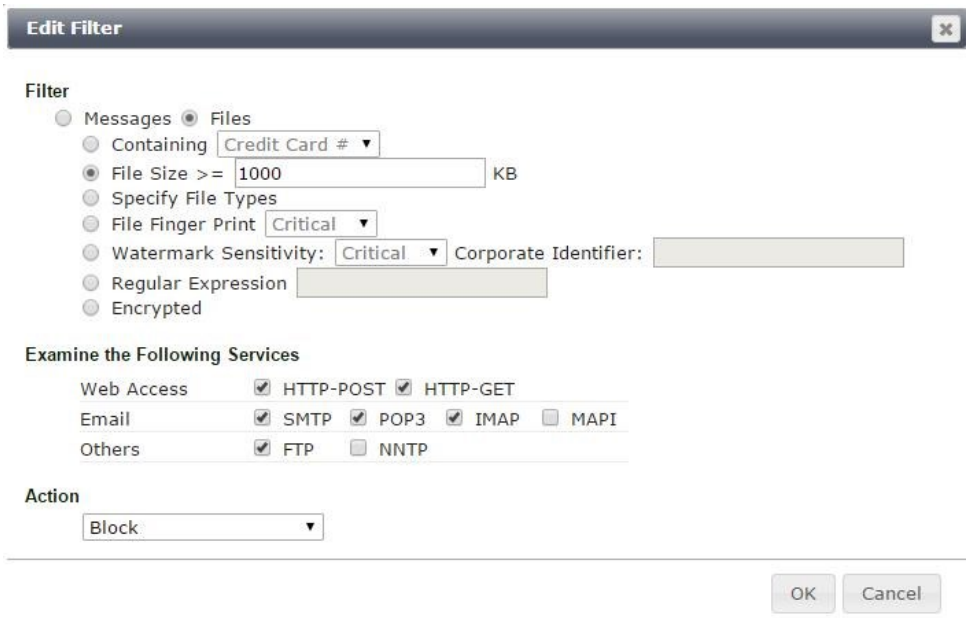


Slika 20: Opozorilno okno o zavrnjenem dostopu

Test orodja za nadzor aplikacij je bil uspešno izveden. Zmožnost zaznave aplikacij predstavlja prednost pred nadzorom URL-naslovov predvsem zato, ker lahko omejimo dostop določeni kategoriji. Če želimo v podjetju omejiti dostop do vseh video vsebin, je to orodje zelo praktično za ta namen. Pri testu smo uspešno testirali tudi nadzor dostopa določenega uporabnika. V praksi to pomeni, da lahko iz določenega podomrežja ali iste naprave, ki jo uporablja več uporabnikov, postavimo različno politiko različnim uporabnikom.

6.5 Četrti laboratorijski test: orodje za varovanje podatkov

Namen četrtega laboratorijskega testa je raziskati možnosti, ki jih ponuja sistem za varovanje oziroma omejevanje podatkov oziroma DLP. Fortinet-ovo orodje deluje z naprednimi tehnikami nadzora in tako zazna neavtorizirano komunikacijo ali pošiljanje podatkov iz omrežja in vanj. Za delovanje orodja moramo najprej nastaviti DLP-filter glede na potrebe laboratorijskega testa.



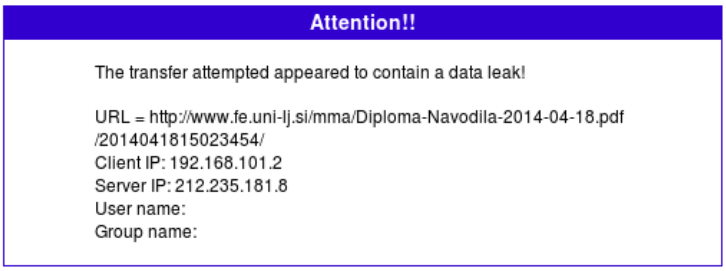
Slika 21: Nastavitev DLP-filtra

Tu lahko izbiramo med vrsto možnosti, med katera na primer spadajo:

- **številke kreditnih kartic,**
- **velikost datotek,**
- **vrsta datotek,**
- **prstni odtis dokumenta,**
  Vsaka digitalna datoteka ima svoj unikatni »prstni odtis« (angl. finger print). S pomočjo tega orodja lahko kategoriziramo (pomembne, manj pomembne) prstne odtise datotek. Ko jih FortiGate enkrat prepozna, jim lahko sledi po lokalnem omrežju ali pa omeji izhod iz omrežja [29].
- **vodni žig dokumenta,**
  Podobno kot prstni odtis tudi vodni žig (angl. Watermark) označi dokument, vendar s to razliko, da lahko isti vodni žig označi več različnih dokumentov (torej ni unikaten za vsak dokument posebej)[29].
- **filter za šifrirana sporočila,**
- **iskanje vzorcev oziroma besednih zaporedij,**
- **šifriran promet.**

Za optimalno delovanje požarnega zidu lahko označimo, na kateri protokol omrežnega prometa naj bo požarni zid posebej pozoren in na katerega ne. Na koncu definiramo še ukrep, za katerega želimo, da ga izvede požarni zid.

Pri laboratorijskem testu smo najprej testirali onemogočen prenos datotek PDF. Tako pod vrsto datotek izberemo obliko PDF, ostale nastavitve so prikazane na sliki 21. Politiko izvajanja smo omejili na vse uporabnike, ob vsakem času, izvajanje orodja pa vključili v smeri iz javnega v zasebno omrežje. Nato smo pokušali na strežnik prenesti datoteko PDF iz URL-naslova www.fe.uni-lj.si/mma/Diploma-Navodila-2014-04-18.pdf/20140418150234524/. Prenos datoteke je takoj blokiralo, ter prikazalo opozorilno okno o zavrnitvi prenosa.



Slika 22: Opozorilno okno o zavrnitvi prenosa

Sledil je še en test, in sicer smo testirali omejitev prenosa datotek glede na velikost datotek. Tu smo omejili prenos datotek na velikost 1000KB, kar pomeni, da orodje blokira vse prenose datotek, večjih od 1000 KB, manjšim od 1000 KB pa omogoči prenos na strežnik. Za testiranje orodja smo na URL-naslovu http://speedtest.ftp.otcnet.gr/ poskušali prenesti različne velikosti datotek preko FTP protokola. Testiranje je vključevalo prenos datotek z velikostjo 100KB, 1MB, 10MB in 100 MB. Datoteka z velikostjo 100KB se je uspešno prenesla, ostalim datotekam pa je bil prenos onemogočen (slika 23).

Slika 23: Opozorilno obvestilo ob testu prenosa datoteke

Čeprav je orodje za varovanje podatkov v splošnem namenjeno nadzoru podatkov iz lokalnega omrežja v javno, smo zaradi lažje izvedbe testov naredil to v obratni smeri, torej smo nadzorovali prenos podatkov iz javnega v lokalno omrežje.

Orodje je v praksi zelo uporabno, saj je odtekanje občutljivih informacij v podjetjih in ustanovah velik problem, ki lahko povzroči nepopravljivo škodo.

6.6 Peti laboratorijski test: FortiSandbox

Namen petega laboratorijskega testa je bilo testiranje naprave FortiSandbox, ki jo Fortinet ponuja kot dodatek k napravi FortiGate. Je naprava, ki jo znane institucije za varnost (NSS labs, ICSA labs) opisujejo kot kakovostno ter jo priporočajo za kakovostno zaščito lokalnih omrežij. Osnovni princip skupnega delovanja naprav FortiGate in FortiSandbox je, da lahko opravljamo zahtevnejše in naprednejše preglede na napravi FortiSandbox ter tako preprečujemo napredne napade APT, posledično pa tudi razbremenimo napravo FortiGate.

Laboratorijski test smo opravljali na napravi FortiSandboxVM, ki je bila v lokalnem omrežju dosegljiva na IP-naslovu 10.0.2.212. Ko se povežemo na napravo, imamo tako kot pri napravi FortiGate na levi strani pregledni meni za nastavitve. Če posplošimo, lahko načine zaščite oziroma pregledovanja razdelimo v tri večje kategorije:

- **Detekcija na osnovi datotek**
  Na napravi FortiGate lahko nastavimo, da na napravo FortiSandbox pošilja vse ali pa samo sumljive datoteke na dodatni pregled. FortiSandbox nato naredi podroben pregled in naredi poročilo pregledanih datotek. Rezultate oziroma poročilo pregledanih datotek jasno prikaže čiste datoteke, zlonamerne datoteke in sumljive datoteke.
- **Omrežna detekcija**
  Omrežna detekcija (angl. Network detection) daje pregled nad omrežnimi aktivnostmi. Omrežni paketi se pregledujejo s pomočjo IPS-orodja.

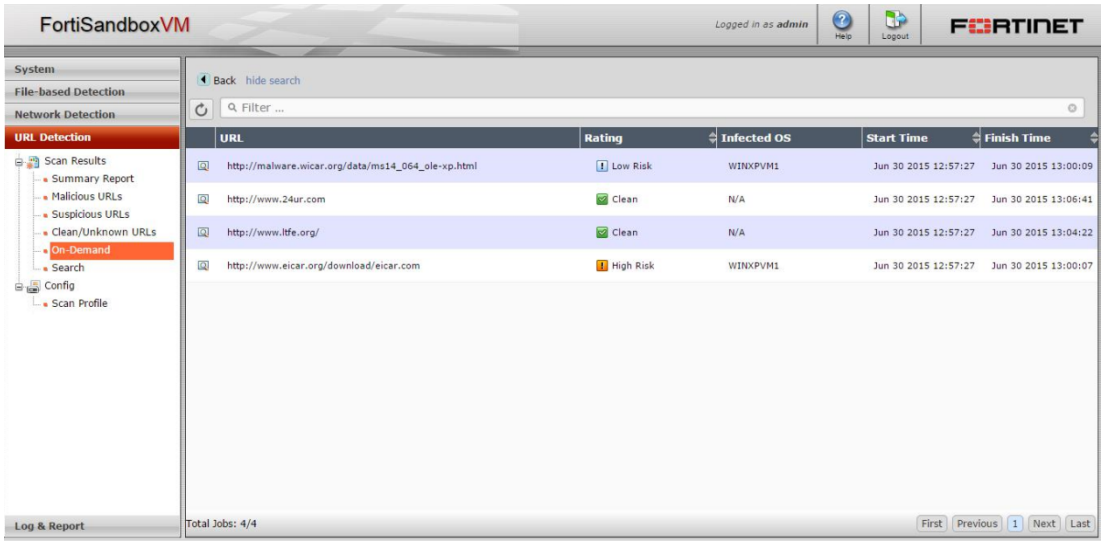
- **URL-detekcija**
  Naprava FortiGate lahko FortiSandbox napravi pošlje: vse URL-naslove, sumljive URL-naslove, prav tako pa lahko na zahtevo (angl. on-demand) vnesemo URL-naslov, ki naj ga FortiSandbox temeljito preišče in poroča, ali je pregledan URL-naslov varen, ali pa obstaja tveganje za dostop.

Naprava stalno beleži poročila o rezultatih pregledovanja po posameznih kategorijah. Tako lahko pod vsako kategorijo pregledamo poročila in na njihovi podlagi naredimo analizo. Prav tako pa se beležijo še splošna poročila za celotno napravo, ki zajemajo vse tri kategorije skupaj. Tako ima skrbnik omrežja res jasno sliko, kaj se dogaja na napravi.

V prvem delu vaje smo testirali URL-detekcijo, in sicer tako, da je naprava FortiSandbox na našo zahtevo preverila določene URL-naslove. Pod zavihkom »URL Detection« izberemo način preverjanja »On-Demand«, kjer ročno vnesemo naslove, ki jih želimo preveriti. Za test smo preverili varnost štirih URL-naslovov:

- http://malware.wicar.org/data/ms14-064_ole-xp.html
- http://www.24ur.com
- http://ltfe.org
- http://www.eicar.org/download/eicar.com

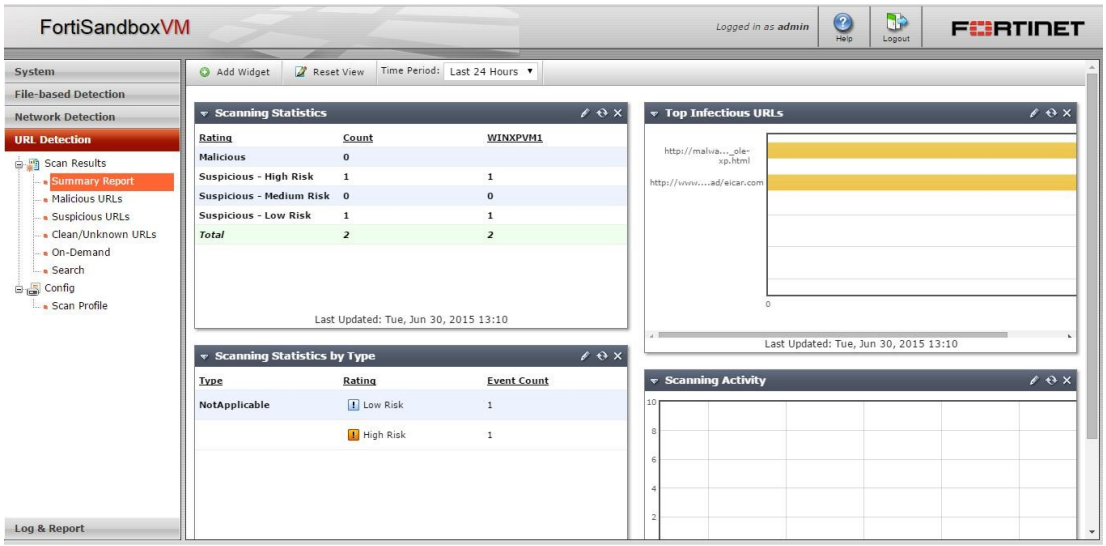
FortiSandbox nato preveri URL-naslove in prikaže rezultate (slika 24). V rezultatih se pregledno prikažejo naslov, status (varen, nizka stopnja tveganja, srednja stopnja tveganja, visoka stopnja tveganja, zlonamerno, neznano ali pa »N/A), verzija operacijskega sistema FortiSandboxVM (podatek, katera verzija OS je bila uporabljena za odkrivanje URL-naslovov) ter začetni in končni čas preverjanja stopnje tveganja.



Slika 24: Prikaz rezultatov za URL-detekcijo

Če pregledamo rezultate preverjanja, je FortiSandbox dva URL-naslova označil kot varna oziroma »Clean«, medtem ko je enega označil kot manj tveganega (angl. Low Risk), enega pa kot bolj tveganega (angl. High Risk). Za preverjanje uporabljena verzija operacijskega sistema FortiSandbox, se prikaže samo za URL naslov z določeno stopnjo tveganja. V našem primeru je verzija OS Microsoft Windows XP Service Pack 3 (32-bit). Prav tako pa je iz rezultatov razvidno, da je FortiSandbox razmeroma hitro izvedel preverjanje URL-naslovov (preverjanje je trajalo med tremi in devetimi minutami).

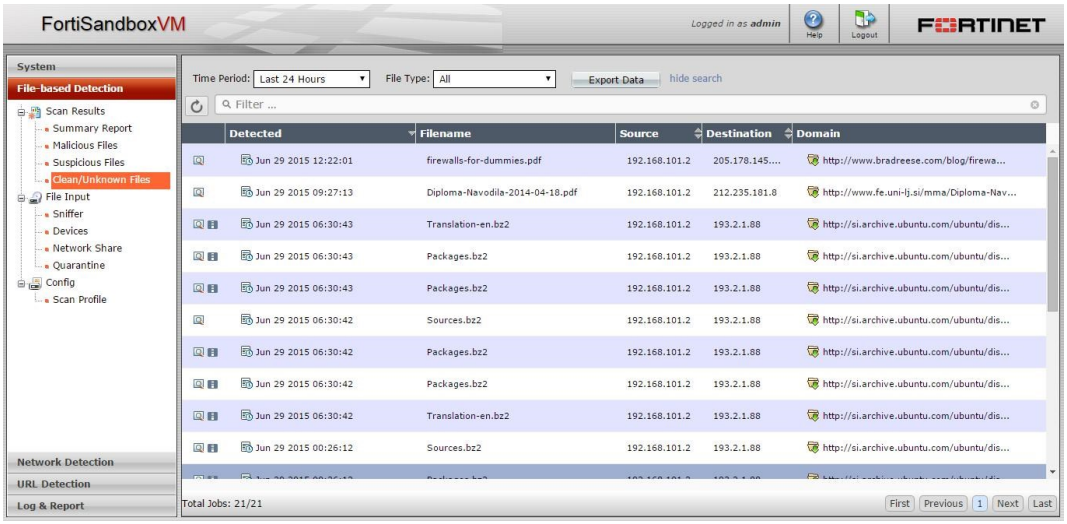
Po pregledu lahko pogledamo še skupno poročilo za URL-detekcijo, na podlagi katere lahko analiziramo uporabo orodja URL-detekcije (slika 25). Izberemo lahko časovno obdobje, iz katerega želimo podatke (zadnjih 24 ur, zadnjih sedem dni ali zadnje dva tedna), beležimo statistiko po stopnjah tveganja (na primer, koliko visoko tveganih URL naslovov je odkril FortiSandbox), beležimo najpogosteje izbrane URL-naslove itd.



Slika 25: Poročilo stanja po izvedbi URL-detekcije

Z možnostjo »Add Widget« lahko po potrebi dodajamo prikaz poljubnih analiz, prav tako pa lahko z možnostjo »reset« ponastavimo beleženje. Orodje za prikaz beleženja je zelo prilagodljivo in daje skrbniku omrežja dober pregled nad preteklim dogajanjem v omrežju.

V drugem delu laboratorijskega testa pa smo testirali delovanje detekcije datotek. Na napravi FortiGate smo nastavili, da vse prenesene datoteke pošilja na dodatno preverjanje na napravo FortiSandbox. Nato smo na strežnik prenesli dve datoteki, in sicer »Firewalls-for-dummies.pdf« in »Diploma-Navodila-2014-04-18.pdf«. Po končanem prenosu smo rezultat preverili na napravi FortiSandbox pod zavihkom »File-based detection«, kjer je viden prenos datotek. Obe preneseni datoteki sta varni, zato ju FortiSandbox prikaže v »clean/Unknown Files«.



Slika 26: Pregled detekcije datotek

Pregled detekcije datotek smo nastavili, da prikaže prenose zadnjih 24 ur in vse vrste prenesenih datotek. Prav tako imamo podane podrobnejše informacije o posameznem prenosu, kot so datum in ura, ime datoteke, izvorni in ciljni IP naslov, ter domena. Po uspešnem prenosu dveh datotek, ki sta bili pregledani in »čisti«, smo testno poskušali prenesti še okuženo datoteko s spletne strani www.eicar.org. Prenos je onemogočil že FortiGate, kajti orodje za protivirusno pregledovanje je zaznalo zlonamerno vsebino. Poročilo o prenesenem prometu v tem primeru ni bilo vidno na FortiSandboxu, po naši domnevi zaradi blokade o prenosu na napravi FortiGate.

6.7 Povzetek laboratorijskih testov

V tabeli so prikazani izvedeni testi ter rezultati in ugotovitve.

Izveden test	Uspešno/neuspešno opravljen	Ugotovitve in komentarji
Protivirusna zaščita	Uspešno opravljen	Orodje deluje učinkovito in v realnem času, prav tako je pregledno za uporabo.
Filtriranje URL naslovov	Uspešno opravljen	Blokiranje URL-naslovov je delovalo učinkovito, prav tako pa je enostavno za uporabo.
Nadzor nad aplikacijami	Uspešno opravljen	Orodje za nadzor nad aplikacijami ponuja res veliko možnosti, ter rešuje prav problem nadzora nad aplikacijami.
Orodje za varovanje podatkov	Uspešno opravljen	Napredno orodje se je izkazalo učinkovito za nadzor nad pretokom informacij ter je blokiralo prenos določenega tipa in velikosti datoteke.
FortiSandbox	Uspešno opravljen	Uspešno je bil opravljen test pregledovanja na zahtevo URL naslovov in detekcije datotek.

Tabela 1: Povzetek laboratorijskih testov

7 Zaključek

V teoretičnem delu diplomske naloge smo analizirali in predstavili, zakaj potrebujemo zaščito, kot je požarni zid, in kako so se ti z leti razvijali. Ta vidik se nam zdi zelo pomemben za samo razumevanje požarnih zidov naslednje generacije, saj so ti kljub novim orodjem in novim tehnologijam preverjanja rezultat dobrih lastnosti prejšnjih različic požarnih zidov. Razvoj in trend uporabe spleta in aplikacij sta povzročila, da so požarni zidovi naslednje generacije nujno potrebni, saj so prejšnje različice postale neučinkovite za zagotavljanje visoke ravni varnosti. Pri izvajanju praktičnega dela diplomske naloge ni bilo večjih težav, saj je naprava pregledna za nastavitev in upravljanje. V veliko pomoč sta bili tudi dobro napisana literatura in podpora na spletni strani http://www.fortinet.com. Orodja za izvajanje nadzora in zaščite so pri vseh testih delovala, kar smo tudi dodali kot rezultat na koncu laboratorijskih testov. Problem pa je bil testirati nekatera izmed zanimivih naprednih orodij, predvsem na napravi FortiSandbox. Ponudniki teh naprav poudarjajo, da je naprava učinkovita za zaščito pred naprednimi napadi, vendar z našim znanjem o omrežjih tega ni bilo mogoče testirati. Prav tako smo imeli težavo testirati prenos okužene datoteke, ki bi bila napravi FortiGate sumljiva, FortiSandbox pa bi potrdil okuženo datoteko. Ob poskusu prenosa okuženih datotek je FortiGate blokiral prenos, tako da preko njega ni prišla nobena okužena datoteka na FortiSandbox. V analizi smo na napravi Sandbox videli samo uspešne prenose »čistih« datotek. Ima pa FortiSandbox pregled nad omrežnim prometom, saj piše poročila za posamezna orodja, prav tako pa omogoča pregled splošnega poročila. Orodja na napravah delujejo v realnem času, kar je točno tako, kot mora biti pri požarnih zidovih naslednje generacije. Samo pregledovanje na zahtevo na napravi FortiSandbox potrebuje določen čas za celovit pregled, vendar se tudi ta izvede sorazmerno hitro.

Čeprav sta FortiGate in FortiSandbox zmogljivi napravi, se nam postavlja vprašanje: ali je to dolgoročna rešitev? Ne vemo, kakšni trendi in tehnologije se bodo pojavljali v naslednjih desetletjih. Zelo verjetno je, da se bodo pojavljala dodatna zmogljiva orodja oziroma naprave, ki bodo sposobna ščititi omrežje, s tem pa bomo verjetno dobili vedno bolj decentraliziran sistem varnosti, kot je že bil v preteklosti.

Kljub razvoju naprav in orodij za zagotavljanje varnosti mora biti velik poudarek predvsem na izobraženosti zaposlenih in seznanitvi z varnostno politiko posameznega podjetja ali ustanove. Kot je že iz podatkov v diplomskem delu razvidno, je za velik odstotek ranljivosti odgovoren prav človek in ne naprava.

Literatura

[1] Symantec corporation, »Internet security Threat Report 2014«. Dosegljivo: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. [Dostopano 10.10.2015]

[2] M. Soriano, »Information and Network Security«. Dosegljivo: http://techpedia.eu/modules/improvet/download/C2EN/Information_and_network_security.pdf [Dostopano 2.9.2015]

[3] J.E. Canavan, »Fundamentals of Network Security«. Dosegljivo: http://www.askcypert.org/sites/default/files/Canavan_J.E._Fundamentals_of_network_security_(2001)(en)(218s).pdf [Dostopano 14.9.2015]

[4] W. Stallings, »Network Security Essentials: Applications and Standards«, 4th edition. New York: Person Education Inc, 2011.

[5] Panda Security, »PandaLabs annual report 2014«. Dosegljivo: http://www.pandasecurity.com/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF2-en.pdf [Dostopano 2.3.2016]

[6] D. Chapman, S. Cooper, E. Zwicky, »Building internet firewalls«, 2nd edition, O'Reily Media, 2000.

[7] R. Panchal, »Firewalls: Hardware vs Software«. Dosegljivo: http://www4.ncsu.edu/~kksivara/sfwr4c03/projects/4c03projects/RPanchal-Project.pdf [Dostopano 25.10.2015]

[8] N. Krawetz, »Introduction to network security«, Charles River Media, Boston, 2007.

[9] Decipher information system, »Firewalls – overview and best practices«. Dosegljivo: http://www.decipherinfosys.com/Firewall.pdf [Dostopano 2.9.2015]

[10] J. Thompson-Melanson, »Learn about Firewall Evolution from Packet Filter to Next Generation«. Dosegljivo: http://www.juniper.net/techpubs/en_US/learnabout/LA_FIrewallEvolution.pdf [Dostopano1.12.2015]

[11] D. Smith, »Understand the evolution of firewalls«. Dosegljivo: http://www.techrepublic.com/article/understand-the-evolution-of-firewalls/ [Dostopano1.12.2015]

[12] Pearson Education, »Stateful Firewalls«. Dosegljivo: https://www.pearsonhighered.com/samplechapter/0672327376.pdf [Dostopano 2.12.2015]

[13] A. Ginter, »13 Ways through a Firewall«. Dosegljivo: https://files.sans.org/summit/scada13/PDFs/13%20Ways%20through%20a%20Firewall%20-%20Andrew%20Ginter,%20Waterfall%20Security%20Solutions.pdf [Dostopano 2.12.2015]

[14] R Shimonski, D. Shinder, T. Shinder, »Best damn firewall period book«, Syngress Publishing Inc, Rockland, 2003.

[15] Gartner, Inc., »Gartner says bring your own device is an applications strategy, not just purchasing policy«. Dosegljivo: http://www.gartner.com/newsroom/id/2629518 [Dostopano 5.1.2016]

[16] Gartner, Inc., »Consumerization«. Dosegljivo: http://www.gartner.com/it-glossary/consumerization/ [Dostopano 5.1.2016]

[17] L.C. Miller, »Cybersecurity survival guide, principles and best practices«. Dosegljivo: https://live.paloaltonetworks.com/twzvq79624/attachments/twzvq79624/AcademyTKB/3/1/Cybersecurity-Survival-Guide.pdf [Dostopano 22.12.2015]

[18] Palo Alto Networks, »The application usage and threat report 2014, 11th edition« Dosegljivo: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/Application_Usage_Threat_Report_2014.pdf [Dostopano 10.1.2016]

[19] Gartner, Inc., »Next-Generation Firewall«. Dosegljivo: http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws/ [Dostopano 5.1.2016]

[20] L. C. Miller, »Next-Generation firewalls for dummies«. Wiley Publishing Inc., Indianapolis, 2011.

[21] J. Hufferd, »Next-Generation Firewall Myth, Legend & Reality«. Dosegljivo: http://sfbay.issa.org/comm/presentations/2011/feb.pdf [Dostopano 10.10.2015]

[22] Mcafee, »NGFW reference guide for firewall/VPN Role 5.7«. Dosegljivo: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25140/en_US/McAfee_NGFW_Reference_Guide_for_Firewall_VPN_Role_v5-7.pdf [Dostopano 10.12.2016]

[23] Fortinet, »Next-generation firewall: Fact and Fiction«. Dosegljivo: https://www.techdata.com/fortinet/files/FORTINETFAQ-Next%20Generation%20Firewalls%20Fact%20and%20Fiction_120811.pdf [Dostopano 10.10.2015]

[24] Fortinet, »Fortinet server Authentication Extension – FSAE«. Dosegljivo: http://www.fortigate.cz/upload-sys/stranky/file/47/fsae-ds.pdf [Dostopano 3.2.2016]

[25] S. Piper, »Intrusion Prevention System for dummies«. Wiley Publishing Inc., Indinapolis, 2011.

[26] Palo Alto networks, »Next-generation Firewall feature overview«. Dosegljivo: http://www.adines.fr/pdfs/paloalto/Firewall_Feature_Overview.pdf [Dostopano 11.10.2015]

[27] P. Kanagasingham, »Data Loss Prevention«. Dosegljivo: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883 [Dostopano 15.2.2016]

[28] Fortinet, »Virtual Domains«. Dosegljivo: http://www.fortinet.es/images/datasheets/FortiOS/inside-fortios-vdoms-50.pdf [Dostopano 3.3.2015]

[29] Fortinet, »The Fortigate cookbook«. Dosegljivo: http://docs.fortinet.com/uploaded/files/359/fortigate-cookbook-507-expanded.pdf [Dostopano 7.7.2015]

[30] Fortinet, »FortiSandbox – Administration Guide, version 2.0.1«. Dosegljivo: http://docs.fortinet.com/uploaded/files/2353/FortSandbox%202.0.1%20Administration%20Guide.pdf [Dostopano 7.7.2015]