

Univerza v Ljubljani

Fakulteta za elektrotehniko

LOVRO STRMČNIK

OPTIMIZACIJA DELOVANJA KORPORATIVNEGA OMREŽJA

Diplomsko delo visokošolskega strokovnega študija

Mentor: doc. dr. Marko Meža

Ljubljana, 2016

Zahvala

Za pomoč in podporo pri izdelavi diplomskega dela se zahvaljujem mentorju doc. dr. Marku Meži. Za pomoč in podporo se zahvaljujem tudi sodelavcem, še posebej Urošu Parazajdi, v podjetju, kjer sem zaposlen. Zahvaljujem se tudi staršem, ženi Andreji in vsem bližnjim za podporo ter spodbujanje med študijem, kot tudi avtorju predloge diplomskega dela, višjemu pred. dr. Janezu Zaletelju.

Kazalo vsebine

1	Uvod.....	5
2	Korporativno računalniško omrežje	9
2.1	Nabor storitev in potreb	13
2.2	Problematika omrežja	15
3	Načrtovanje robnega strežnika	19
3.1	Smernice načrtovanja.....	19
3.2	Kriteriji izbire ustreznega strežnika	22
3.3	Kriteriji izbire programske opreme.....	23
4	Predlagana arhitektura robnega strežnika.....	29
4.1	Strojna oprema (specifikacija, karakteristike)	29
4.2	Programska oprema	30
4.2.1	Nabor orodij in dodatnih funkcionalnosti.....	38
4.3	Druge predvidene možnosti	40
5	Priprava in implementacija robnega strežnika	47
5.1	Namestitev in priprava.....	47
5.2	Implementacija v omrežje.....	66
6	Testiranja in rezultati	69
6.1	Metodologija testiranja	69
6.2	Preizkus delovanja	70
6.3	Rezultati in primerjava.....	72
7	Zaključek.....	85
	Literatura	89

Seznam slik

Slika 1: Shema korporativnega omrežja.....	9
Slika 2: Drevesna topologija v računalniških omrežjih [2]	11
Slika 3: Optični pretvornik Allied Telesyn AT-MC102XL [3].....	12
Slika 4: <i>pfSense</i> pregledna plošča (začetni zaslon WebGUI).....	31
Slika 5: <i>pfSense</i> – načini izhodnega NAT	34
Slika 6: <i>pfSense</i> – privzete nastavitve DHCP-strežnika za omrežje 172.16.0.0.....	36
Slika 7: Rezultat oblikovanja prometa pri omejevanju pasovne širine [17].....	39
Slika 8: Uporabniški vmesnik TMG.....	40
Slika 9: TMG 2010 napaka skripta programa pri zagonu [22].....	41
Slika 10: Diagram poteka ustvarjanja »netipičnega« pravila v požarnem zidu TMG 2010.....	42
Slika 11: OPNSense uporabniški vmesnik – pregledna plošča (začetni zaslon GUI) [27]	45
Slika 12: <i>pfSense</i> – začetni zaslon namestitve v konzoli.....	48
Slika 13: <i>pfSense</i> – prepoznane mrežne kartice, njihove oznake in strojni naslovi MAC	49
Slika 14: <i>pfSense</i> – uspešno konfigurirano zunanje WAN- in notranje LAN-omrežje.....	51
Slika 15: <i>pfSense</i> – konfiguracija WAN-omrežja preko WebGUI.....	53
Slika 16: <i>pfSense</i> – konfiguracija LAN-omrežja preko WebGUI	54
Slika 17: <i>pfSense</i> – pregledna plošča uspešno vzpostavljenega robnega strežnika z osnovnimi konfiguracijami	54
Slika 18: <i>pfSense</i> – vzpostavljen DHCP-strežnik in definirani razponi IP-naslovov.....	55
Slika 19: <i>pfSense</i> – definiranih šest navideznih (zunanjih) IP-naslovov	57
Slika 20: <i>pfSense</i> – konfiguracija NAT-preslikave za podomrežje 172.16.1.0/24.....	58
Slika 21: <i>pfSense</i> – pregled nad vsemi definiranimi podomrežji in izhodnimi NAT- preslikavami	59
Slika 22: <i>pfSense</i> – konfiguracija 1 : 1 NAT za poštni strežnik	60
Slika 23: <i>pfSense</i> – pregled nad nekaj konfiguriranimi 1 : 1 NAT-preslikavami.....	61
Slika 24: <i>pfSense</i> – definiranje vzdevka (vrat) za poštni strežnik KURIR.....	62
Slika 25: <i>pfSense</i> – pregled nad konfiguriranimi vzdevki (vrati).....	63
Slika 26: <i>pfSense</i> – pregled nad konfiguriranimi vzdevki (IP-naslovi).....	63
Slika 27: <i>pfSense</i> – pregled nad definiranimi izhodnimi pravili iz omrežja LAN	64
Slika 28: <i>pfSense</i> – definirano vhodno pravilo za potrebe poštne strežnika.....	65

Slika 29: Stanje sistemskih sredstev prejšnjega robnega strežnika v času višjih zakasnitev...	74
Slika 30: Deset lokalnih naprav z največ prometa, zajetim v 4,59 sekundah v času višjih zakasnitev (Meritev zakasnitev 1)	75
Slika 31: Izmerjena hitrost internetne povezave v času večjih zakasnitev (Meritev zakasnitev 1).....	76
Slika 32: <i>pfSense</i> – število prejetih in poslanih paketov v času enourne meritve.....	77
Slika 33: <i>pfSense</i> – rezultati meritve podatkovnega prometa in hitrosti prenosa v času enourne meritve	78
Slika 34: <i>pfSense</i> – hitrost pretoka podatkov v času enourne meritve.....	79
Slika 35: <i>pfSense</i> – minimalne, maksimalne in povprečje zakasnitev v času enourne meritve	80
Slika 36: <i>pfSense</i> – stanje obremenjenosti procesorja v času enourne meritve	81
Slika 37: <i>pfSense</i> – stanje porabe pomnilnika v času enourne meritve	81
Slika 38: Izmerjena hitrost internetne povezave po implementaciji robnega strežnika izven delovnega časa	82

Seznam grafov in tabel

Graf 1: Ciscova VNI-napoved rasti globalnega IP-prometa do leta 2019 [1]	5
Graf 2: Primerjava količin paketov, podatkovnega prometa in hitrosti pretoka	83
Graf 3: Primerjava minimalnih, maksimalnih in povprečnih zakasnitev	83
Graf 4: Primerjava povprečnih in maksimalnih obremenitev procesorja	84
Tabela 1: Seznam že vgrajenih poglobitnih funkcionalnosti / značilnosti <i>pfSense</i> [15]	33
Tabela 2: Statistični povzetek šestih različnih meritev zakasnitev	73
Tabela 3: Rezultati meritve podatkovnega prometa v času višjih zakasnitev (Meritev zakasnitev 1) in ocenjene količine	76

Slovar uporabljenih kratic in izrazov

Kratica / Izraz	Angleški prevod	Slovenski prevod
1 : 1 NAT	1 : 1 NAT	način prevajanja omrežnih naslovov 1 : 1 NAT
10 K RPM	10.000 revolutions per minute	10.000 vrtljajev na minuto
48-port switch	48-port switch	48-vratno stikalo
4-Core	4-Core	4 jedrni
AD	Active Directory	aktivni imenik
Add a new alias	Add a new alias	Dodaj nov vzdevek
Add new mapping	Add new mapping	Dodaj novo preslikavo
Add new rule	Add new rule	Dodaj novo pravilo
additional pools	additional pools	dodatni nabor (razpon) naslovov
address pool	address pool	nabor (razpon) naslovov
aliases	aliases	vzdevki
alternative monitor ip	Alternative monitor IP	alternativni spremljajoči IP-naslov
appliance	appliance	namenska naprava
application server	application server	aplikacijski strežnik
array	array	polje
auto-detection	auto-detection	samodejna prepoznavna
automatic outbound NAT	automatic outbound Network Address Translation	samodejni izhodni način prevajanja omrežnih naslovov
available range	available range	razpoložljiv razpon
backup	backup	varnostna kopija
bandwidth	bandwidth	pasovna širina
blacklist	blacklist	črna lista
bottleneck	bottleneck	ozko grlo
cache	cache	predpomnilnik
central hub	central hub	glavno dostopovno vozlišče
cloud	cloud	oblak
com port	com port	komunikacijska vrata
command channel	command channel	ukazni kanal
console	console	konzola (upravljalnik)
core router	core router	notranji usmerjevalnik
CPU	Central Processing Unit	centralna procesna enota
dashboard	dashboard	pregledna plošča
data link layer	data link layer	sloj podatkovne povezave
dead end	dead end	slepa ulica
description	description	opis
destination	destination	cilj
destination port range	destination port range	ciljni razpon vrat
DHCP	Dynamic Host Configuration Protocol	protokol za dinamično konfiguriranje gostiteljev
diagnostics	diagnostics	diagnostika

DNS	Domain Name System	sistem domenskih imen
DNS Forwarder	DNS Forwarder	posrednik domenskih imen
DNS rebind check	Domain Name System rebind check	vnovično preverjanje povezave
domain	domain	domena
domain controller	domain controller	domenski krmilnik
domain network	domain network	domensko omrežje
download	download	prenašanje
downtime	downtime	prekinjeno delovanje
DPI	Deep Packet Inspection	podrobno pregledovanje paketov
edge server	edge server	robni strežnik
embedded system	embedded system	vgradni sistem
EB	Exabyte	eksabajt (10^{18} bajtov = 1 milijon terabajtov)
external DNS Server	external Domain Name Server	zunanj DNS-strežnik
firewall	firewall	požarni zid (požarna pregrada)
floating licence server	floating licence server	strežnik s plavajočo licenco
fork	fork	vejitev
FTP	File Transfer Protocol	protokol za prenos datotek
full installation	full installation	polna inštalacija
general configuration	general configuration	splošna konfiguracija
GUI	Graphical User Interface	grafični uporabniški vmesnik
halt system	halt system	zaustavitev sistema
hardware firewall appliances	hardware firewall appliances	strojne namenske naprave s požarnimi zidovi
high ports	high ports	visoka vrata
hostname	hostname	ime gostitelja
HT	Hyper-Threading	večnitenje
HTTP	Hypertext Transfer Protocol	protokol za prenos hiperteksta
HTTPS	Hypertext Transport Protocol Secure Sockets	varni protokol za prenos hiperteksta
hybrid outbound NAT	hybrid outbound Network Address Translation	hibridni izhodni način prevajanja omrežnih naslovov
I/O	Input/Output	vhodi/izhodi
ICMP	Internet Control Message Protocol	internetni protokol za pošiljanje kontrolnih sporočil
IDS	Intrusion Detection System	sistem zaznavanja vdorov
IMAP	Internet Message Access Protocol	internetni protokol za dostop do e-pošte
IMAP over SSL	IMAP over SSL	internetni protokol za varen dostop do e-pošte preko SSL
inbound	inbound	vhodni -a -o
inbound traffic	inbound traffic	vhodni promet
interfaces	interfaces	vmesnik
internal DNS	internal Domain Name System	notranji sistem domenskih imen

internal DNS Server	internal Domain Name Server	notranji DNS-strežnik
interrupt	interrupt	prekinitev
IP alias	IP alias	IP vzdevek
IPS	Intrusion Prevention System	sistem preprečevanja vdorov
kernel	kernel	jedro operacijskega sistema
corporate network	corporate network	korporativno omrežje
LAN	Local Area Network	lokalno omrežje
latency	latency	zakasnitev
layer-2 switch	layer-2 switch	stikalo drugega sloja
layer-3 switch	layer-3 switch	stikalo tretjega sloja
lease	lease	najem
Live CD	Live CD	zagonski CD-medij
logical drive	logical drive	logični disk
MAC	Media Access Control	naslov MAC (naslov strojne opreme)
MAC spoofing	Mac spoofing	podvajanje naslova MAC
mail server	mail server	poštni strežnik
malware inspection	malware inspection	pregledovanje škodljive programske opreme
managed switch	managed switch	upravljano stikalo
management console	management console	upravljalna konzola
manual outbound nat	manual outbound network address translation	ročni izhodni način prevajanja omrežnih naslovov
mirroring disk	mirroring disk	zrcaljenje diska
multithread	multithread	večnitne
NAS	Network Attached Storage	omrežno diskovno polje
NAT	Network Address Translation	prevajanje omrežnega naslova
NAT reflection	Network Address Translation reflection	zrcaljenje NAT
network layer	network layer	omrežni sloj
NIC	Network Interface Card	mrežna kartica
open source software	open source software	odprtokodna programska oprema
outbound	outbound	izhodni -a -o
outbound NAT	outbound Network Address Translation	izhodni način prevajanja omrežnih naslovov
outbound traffic	outbound traffic	izhodni promet
P2P	Peer-to-Peer	omrežje vsak z vsakim
packet sniffing	packet sniffing	prisluškovanje (vohlanje) paketov
password	password	geslo
PDC	Primary Domain Controller	glavni domenski krmilnik
peaks	peaks	vrhovi
physical layer	physical layer	fizični sloj
POP3	Post Office Protocol	protokol za sprejemanje pošte POP3

port range	port range	obseg vrat
ports	ports	vrata
proxy	proxy	posrednik (proksi)
queue	queue	čakalna vrsta
Quick/Easy	Quick/Easy	hitro/enostavno
rackmount	rackmount	rezina
RAID	Redundant Array of Independent Disks	redundantno diskovno polje
RAID Controller	Redundant Array of Independent Disks Controller	krmilnik za redundantno diskovno polje
RAM	Random Access Memory	bralno-pisalni pomnilnik
range	range	razpon
RDP	Remote Desktop Protocol	protokol oddaljenega namizja
RDS	Remote Desktop Services	storitve oddaljenega namizja
RRAS	Routing and Remote Access Service	storitev usmerjanje prometa in oddaljenega dostopa
screenshot	screenshot	posnetek zaslona
script error	script error	napaka skripta
SFTP	Secure File Transfer Protocol	varni protokol za prenos datotek
site-to-site	site-to-site	lokacija z lokacijo
SMTP	Simple Mail Transfer Protocol	preprosti protokol za prenos pošte
SMTP over SSL	Simple Mail Transfer Protocol over SSL	preprosti protokol za prenos pošte preko SSL
software firewall	software firewall	programski požarni zid
source	source	vir
SSH	Secure Shell	varna lupina
SSL	Secure Socket Layer	sloj varnih vtičnic
state table	state table	tabela stanj
stateful firewall	stateful firewall	požarna pregrada z upoštevanjem vseh stanj (stanovitni požarni zid)
stateful packet inspection	stateful packet inspection	stanovitna kontrola paketov
subnet	subnet	podomrežje
tagged port	tagged port	označena vrata
task manager	task manager	upravitelj opravil
TC	Telecommunications Closet	telekomunikacijska omara
TCP	Transmission Control Protocol	protokol za krmiljenje prenosa
throughput	throughput	pretok
TMG	Forefront Threat Management Gateway	Forefront Threat Management Gateway
TOE	TCP/IP Offload Engine	razbremenitev procesiranja TCP/IP-sklada
traffic shaping	traffic shaping	Oblikovanje prometa
translation	translation	prevajanje

tree network topology	tree network topology	drevesna topologija omrežja
UDP	User Datagram Protocol	protokol uporabniškega datagrama
untagged port	untagged port	neoznačena vrata
uplink	uplink	povezava navzgor
upload	upload	nalaganje
UPS	Uninterruptible Power Supply	brezprekinitveno napajanje
upstream gateway	upstream gateway	prehod povratnega toka
URL	Uniform Resource Locator	enotni naslov vira
URL filtering	Uniform Resource Locator filtering	filtriranje enotnega naslova vira
username	username	uporabniško ime
utilization	utilization	izkoriščenost
UTP	Unshielded Twisted Pair	neoklopljena sukana parica
VGA	VGA	analogni standardni prikaz slike na monitorju
virtual IP	virtual IP	navidezen IP-naslov
VLAN	Virtual Local Area Network	navidezno lokalno omrežje
VPN	Virtual Private Network	navidezno zasebno omrežje
WAN	Wide Area Network	prostrano omrežje
web caching server	web caching server	spletni strežnik s predpomnjenjem
web framework	web framework	spletno ogrodje
web proxy cache	web proxy cache	spletni posrednik s predpomnilnikom
web server	web server	spletni strežnik
WebGUI	Web Graphical User Interface	spletni grafični uporabniški vmesnik
webmail	webmail	spletna pošta
wizard	wizard	čarovnik
ZB	Zettabyte	zetabajt (10^{21} bajtov = 1000 eksabajtov)

Pri prevodih sem si pomagal z naslednjimi spletnimi slovarji: <http://islovar.org/>,
<http://slovar.ltfe.org>, <http://dis-slovarcek.ijs.si/>,
<http://www.termania.net/slovarji/122/racunalniski-slovarcek/>

Povzetek

V pričujočem diplomskem delu sem predstavil srednje veliko korporativno računalniško omrežje in problematiko njegove upočasnjenosti, ki je ovirala vsakodnevno delo v podjetju. Analiza prejšnjega stanja je pokazala, da je bil vzrok za pogosto daljše zakasnitve in slabo izkoriščenost internetne povezave preobremenjen robni strežnik. Za uspešno rešitev sem moral premišljeno načrtovati, pripraviti in v omrežje implementirati ustrezen robni strežnik. Pri tem sem s predstavljenimi postopki uspešno odpravil vse težave, omrežje ustrezno optimiziral in hkrati predlagal tudi smernice za dodatne izboljšave v prihodnosti. Primerjava stanja pred posegom in po njem je pokazala, da robni strežnik sedaj omogoča vsaj 10-krat hitrejši pretok in količino podatkovnega prometa s skoraj nespremenjeno porabo sistemskih sredstev, ki je bila pred tem glavni razlog vseh težav. Tako je izkoristek razpoložljive internetne povezave, ki je bil pred optimizacijo manj kot 10-odstoten, sedaj skoraj 100-odstoten. Stabilno delovanje omrežja se kaže tudi s tem, da se je kljub veliko večji obremenitvi omrežja povprečje zakasnitev zmanjšalo za skoraj 30-krat.

KLJUČNE BESEDE: WAN, LAN, robni strežnik, storitve, dostop, zakasnitve, podatkovni promet, pretok, ping, paketi, IP-naslov, protokoli in vrata, DNS, DHCP, NAT, varnost, požarni zid

Abstract

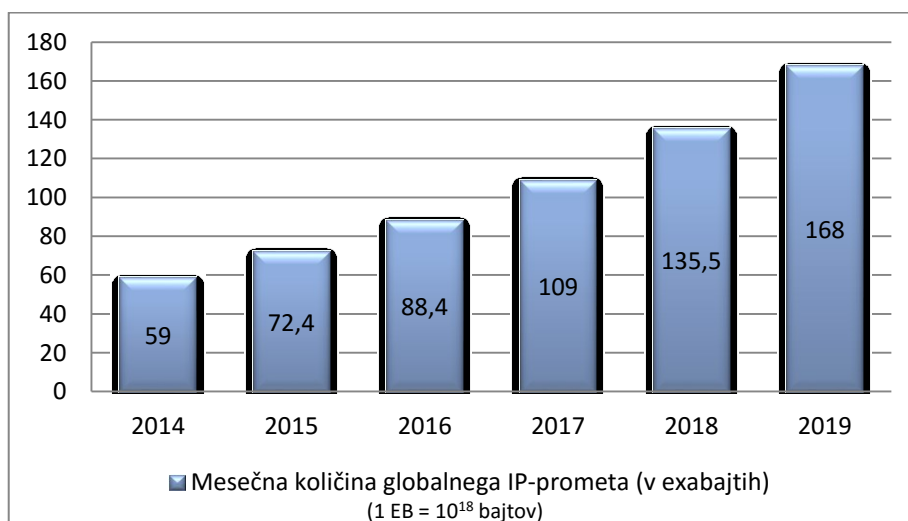
In this thesis I have presented medium sized corporate network and issues with its slow performance which obstructed company everyday work. Previous state analysis showed that the reason for high latencys and poor network utilization was an overloaded edge server. Successful solution required a thoughtful design, prepararation and implementation of appropriate edge server. With featured procedures I have successfully solved all problems and properly optimized the network. At the same time I suggested further improvement guidelines in the future. State comparison before and after showed that the edge server now allows at least 10-times higher troughput speed and amount of data traffic with almost constant consumption of system resources, that previously caused all main problems. Network utilization is now almost at 100 percent, compared to less then 10 percent in previous state. Stable network performance is also reflected by a 30-times lower average latency despite of much larger network load.

KEYWORDS: WAN, LAN, edge server, services, access, latency, data traffic, throughput, ping, packets, IP address, protocols and ports, DNS, DHCP, NAT, security, firewall

1 Uvod

Razvoj računalniških tehnologij je v zadnjih letih tako napredoval, da omogoča uporabnikom interneta uporabo večjega števila internetnih storitev hkrati (brskanje po svetovnem spletu, prenašanje vsebin, pregledovanje e-pošte, ogled multimedijskih vsebin visokih ločljivosti, video klici in video konference, družbena omrežja, delo v oblaku (ang. *cloud*), navidezna zasebna omrežja VPN (ang. *VPN – Virtual Private Network*), prenosi preko protokola FTP (ang. *FTP – File Transfer Protocol*), promet p2p (ang. *p2p – Peer-to-Peer*) itd.). Sleherni uporabnik interneta si želi storitve uporabljati zanesljivo in hitro, zato je pomembna tako varnost komunikacije kot hitrost samega dostopa do interneta.

Zaradi stremjenja k vedno višjim hitrostim in zagotavljanja vedno bolj kakovostnih storitev se to drastično odraža tudi pri celotni količini globalnega (svetovnega) IP-prometa, ki skozi leta strmo narašča. Kot pravi Ciscov vizualni (splošni) indeks mreženja VNI (ang. *VNI - Visual Networking Index*) [1], se je globalni IP-promet med letoma 2009 in 2014 petkratno povečal, zato napovedujejo, da se bo do leta 2019 povečal še za trikrat. Tako bo do konca leta 2016 globalni IP-promet prvič presegel letni prag tako imenovanega zetabajta ZB (ang. *ZB – Zettabyte*), kjer je 1 ZB enak 1000 eksabajtom EB (ang. *EB – Exabyte*) oziroma 10^{21} bajtom in bi naj do leta 2019 le-ta dosegel letno 2 zetabajta [1] oziroma 168 eksabajtov mesečno. Za lažjo predstavo je podan tudi prvi graf – Graf 1, ki prikazuje rast globalnega IP-prometa med letoma 2014 in 2019, glede na eksabajt mesečno, kjer je 1 eksabajt (10^{18} bajtov) enak 1 milijonu terabajtov.



Graf 1: Ciscova VNI-napoved rasti globalnega IP-prometa do leta 2019 [1]

Uporaba raznovrstnih storitev povzroča velike količine prenesenih in poslanih podatkov, ki pa jih je treba varno in ustrezno krmiliti (usmerjati), še posebej v korporativnih omrežjih. Ta zelo pomembna naloga je ena izmed glavnih t. i. robnega strežnika (ang. *edge server*), ki služi kot prehodna naprava (posrednik, tudi glavni prehod) med notranjim lokalnim omrežjem LAN (ang. *LAN – Local Area Network*) in prostranim omrežjem WAN (ang. *WAN – Wide Area Network*), kakršen je internet. V omrežju je lahko izveden kot fizična strojna, programska oprema ali skupek obeh. V korporativnih omrežjih (ang. *corporate networks*) naprava, ki notranjemu omrežju predstavlja glavni prehod in usmerja promet med omrežji, pogosto deluje tudi kot požarni zid (ang. *firewall*) ter skrbi za nadzor vstopnega in izstopnega prometa. To pomeni, da vstopa v notranje (lokalno) omrežje le promet, ki je temu omrežju namenjen, in izstopa le tisti, ki je namenjen zunanjemu svetu. Torej skrbi za nadzor in usmerjanje celotnega prihodnega in odhodnega podatkovnega prometa.

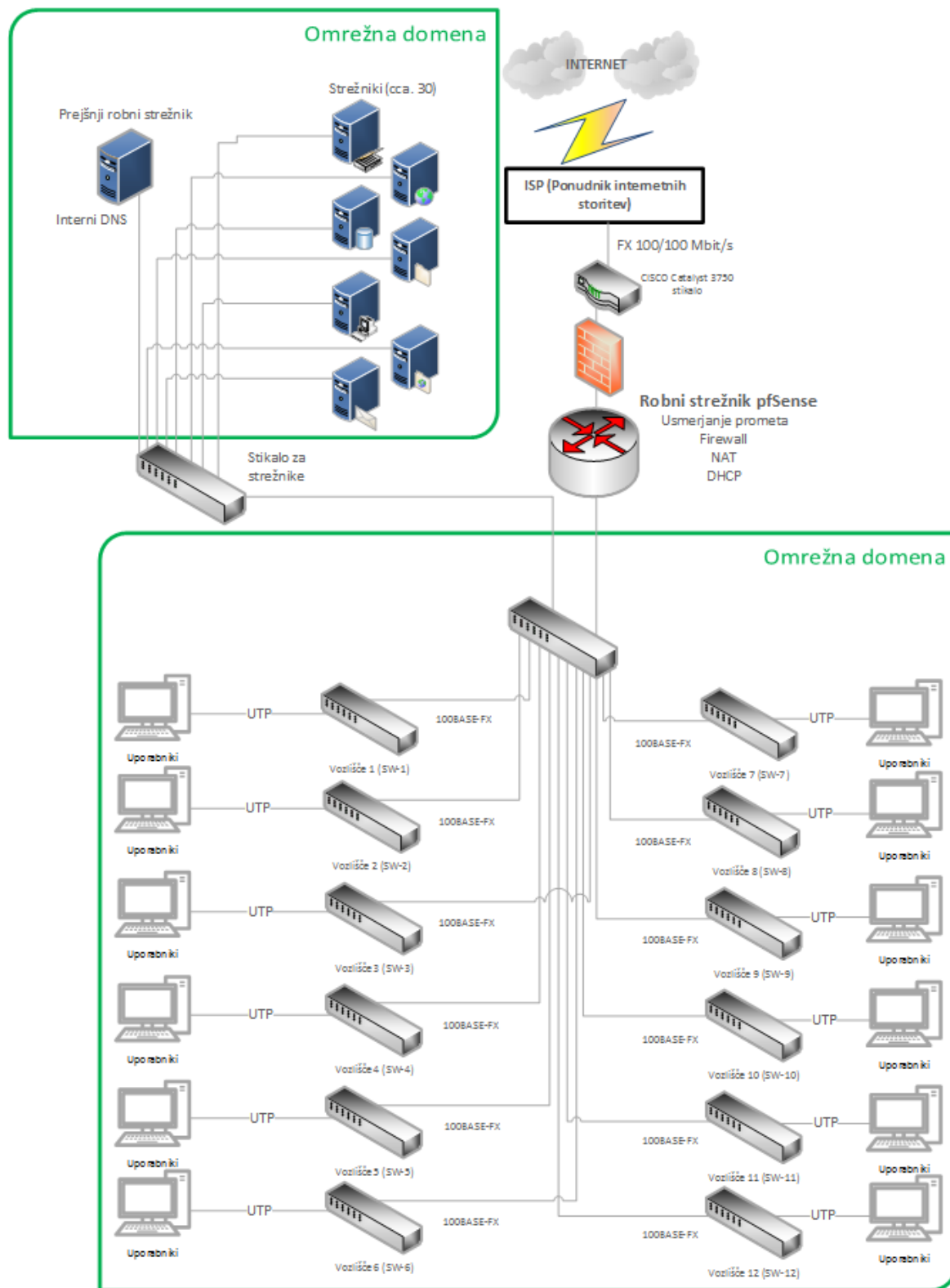
V srednje velikem korporativnem omrežju, ki ga bom natančneje predstavil v tem diplomskem delu, je med drugim tudi napredek tehnologij botroval k temu, da stanje tega omrežja ni več zadoščalo vsem zahtevam in potrebam. Že začetni vpogled v to problematiko je pokazal, da razlog upočasnitosti tega omrežja in skoraj vsakodnevnih visokih zakasnitev predstavlja starejši robni strežnik. Zaradi njegove dotrajane strojne opreme ter nabora različnih funkcij in vlog, ki jih je moral hkrati opravljati, je postalo omrežje in vsakodnevno delo v podjetju zelo ovirano. Pri tem je bila tudi razpoložljiva 100/100 Mbit/s internetna povezava slabo izkoriščena.

Namen tega diplomskega dela je analizirati in razrešiti problematiko upočasnitosti tega omrežja in tako zagotoviti višji izkoristek internetne povezave. Zaradi omenjenih težav, vedno večjih zahtev in potreb po višjih hitrosti ter zanesljivem delovanju omrežja bom v tem diplomskem delu predstavil, kako sem načrtoval in implementiral predlagani robni strežnik. Pri tem bom natančno opisal vse postopke, ki so pripeljali do uspešne rešitve. Pred končno predlagano rešitvijo bom preizkusil in omenil tudi druge predvidene rešitve. Glede na ugotovitve pa bom omenil tudi njihove omejitve in slabosti. Cilj je sistematsko načrtovanje robnega strežnika, njegove ustrezne priprave in konfiguracije ter dejanske implementacije v omrežje. Pri celotnem projektu sem sledil splošno zastavljenim smernicam takšnega načrtovanja. Ključnega pomena je tudi hitra in uspešna vzpostavitev robnega strežnika v obstoječe omrežje, če je mogoče brez prekinjenega delovanja (ang. *downtime*). Za to je

potrebna predpriprava strežnika, vzpostavitev in preizkus vseh funkcij in potreb, ki jih omrežje zahteva. Priprava robnega strežnika se mora izvajati ločeno (vzporedno) z obstoječim omrežjem, da lahko omrežje podjetja deluje nemoteno. Za ta namen bom uporabil prosta vrata (vtičnice) glavnega stikala ponudnika internetnih storitev, ki je locirano v tem korporativnem omrežju.

Prikazal bom rezultate raznih merjenj in testiranj, vedenje in delovanje obeh robnih strežnikov z raznimi tabelami, posnetki zaslona in diagrami ter na koncu naredil tudi primerjavo. Iz teh bo vidna učinkovitost implementirane rešitve in bistveno izboljšano delovanje tega omrežja. V zaključku pa bom glede na rezultate in primerjavo podal še dodatne ugotovitve ter mnenja. Ker je bila prioriteta hitra in učinkovita rešitev omenjene problematike, sem na podlagi tega in trenutnih zahtev omrežja vzpostavil tokrat le osnovne funkcionalnosti in vloge robnega strežnika, ki pa zadoščajo vsem potrebam tega omrežja. Na kratko pa bom omenil tudi druge funkcionalnosti, ki jih ponuja izbrana rešitev in njeni dodatki za še boljšo optimizacijo omrežja in poostreno varnost. Te bom krajše opisal v naboru dodatnih funkcionalnosti in v zaključku predvidel njihovo uporabo v temu omrežju pri naslednjih večjih projektih in posegih v omrežje. Na podlagi teh bo vidna tudi nadaljnja vizija (smernice) oziroma smer razvoja tega informacijskega sistema.

2 Korporativno računalniško omrežje



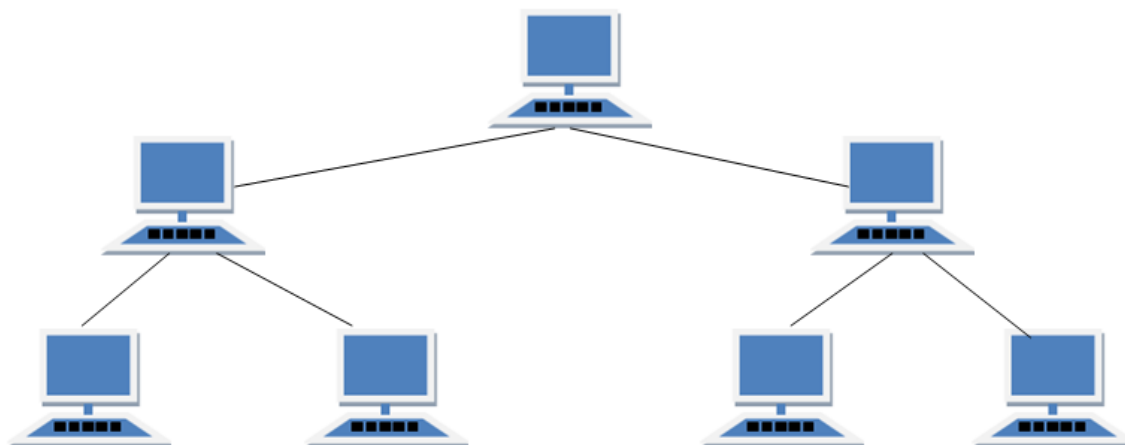
Slika 1: Shema korporativnega omrežja (Vir: Dejanski popis stanja in povezav komunikacijske opreme; vpogled v strežniško sobo, pregled optičnih pretvornikov in vseh vozlišč v omrežju)

Slika 1 prikazuje shemo korporativnega računalniškega omrežja v trenutnem stanju oziroma »posnetek« tega omrežja po uspešni implementaciji robnega strežnika. Shemo omrežja sem narisal sam na podlagi pripravljenega osnutka, ki sem ga ustvaril glede na dejanski popis stanja in povezav komunikacijske opreme tega omrežja. Pri tem sem si pomagal z vpogledom v strežniško sobo, pregledom optičnih pretvornikov in vseh vozlišč v omrežju. Pri kakih nejasnostih sem se lahko posvetoval tudi z vodjo IT-oddelka tega omrežja.

Omrežje, ki ga predstavljam, je domensko (ang. *domain network*), ki ga lahko nadzorujejo in urejajo le skrbniki (administratorji) tega omrežja. Domenski način delovanja omrežja jim omogoča popoln nadzor nad vsemi uporabniškimi računi in pravicami, ki so jim dodeljene. Da je to izvedljivo, imajo tukaj pomembno vlogo tudi t. i. »notranji« strežniki. Sem med drugimi sodi domenski krmilnik (ang. *domain controller*) z aktivnim imenikom AD (ang. *AD – Active Directory*), ki vsebuje celotno bazo uporabniških računov. Na podlagi njihovih informacij (veljavnost, pravice dostopov) dovoljuje oziroma zavrača zahteve uporabnikov pri prijavi v domeno ali pa recimo pri dostopu in uporabi omrežnih sredstev. Poleg njega je v omrežju tudi interni DNS-strežnik (ang. *internal DNS – internal Domain Name System*), ki omogoča pretvorbo imen med napravami znotraj omrežja kot tudi pretvorbo zunanjih imen, če to zahtevajo notranji uporabniki. Vloga internega DNS-strežnika je bila pred implementacijo dodeljena kot dodatna vloga robnega strežnika. Ta pa je sedaj kot edina po implementaciji ostala prejšnjemu robnem strežniku, kateremu sem moral ustrezno spremeniti konfiguracijo, da se sedaj v omrežju predstavlja zgolj kot interni DNS-strežnik. Za ta namen sem ga v shemi (Slika 1) za to tudi izpostavil in ga posebej poimenoval kot »Prejšnji robni strežnik, Interni DNS«. Če bi hotel na shemi uprizoriti prejšnje stanje oziroma izgled omrežja pred implementacijo, bi moral le prejšnji robni strežnik umestiti nazaj na njegovo mesto, kjer je sedaj »Robni strežnik pfSense« in tega iz sheme odstraniti.

Podjetje je že v začetku priklopa na internet od ponudnika internetnih storitev prejelo C-razred naslovov zunanjih IP-števil, kar znaša 254 razpoložljivih javnih IP-naslovov. Celotnih javnih naslovov razreda C se dandanes ne dodeljuje več, zaradi pomanjkanja naslovov IPv4. Na podlagi tega in glede na število naprav v omrežju je treba skrbno določiti in izbrati tiste naprave, ki res potrebujejo lasten enolični javni naslov.

Topologija celotnega omrežja podjetja je bila že v začetku nastanka zasnovana na podlagi drevesne topologije (ang. *tree network topology*) [2] kot prikazuje naslednja slika (Slika 2). To se tudi še dandanes upošteva tako pri širjenju notranjega omrežja kot pri raznih poseganjih, menjavi ali nadgradnji omrežne opreme.



Slika 2: Drevesna topologija v računalniških omrežjih [2]

Definicija drevesne topologije (po www.islovar.org) predstavlja topologijo omrežja, kjer je vozlišče povezano samo z enim nadrejenim ter enim ali več podrejenimi vozlišči. Takšna topologija je primerna za veliko omrežje, katerega posledično ni težko upravljati, saj je dodajanje novih naprav, stikal in vozlišč preprosto. Pri okvarah ali težavah je tudi lažje locirati mesto napake v takšni hierarhični razporeditvi. V primeru okvare glavnega dostopovnega vozlišča (ang. *central hub*) oziroma glavnega stikala to ohromi celotno omrežje, kar pa je tudi njena glavna slabost.

Omrežje podjetja je sestavljeno iz dvanajstih vozlišč, ki jih predstavljajo ločene telekomunikacijske omare (ang. *TC – Telecommunications Closet*). V omarah je v rezinah (ang. *rackmount*) nameščenih dvanajst 48-vratnih omrežnih stikal (ang. *48-port switch*) tipa drugega sloja t. i. sloja podatkovne povezave (ang. *data link layer*) in omogočajo priključitev vsega skupaj 576 naprav. Omenjen tip stikal deluje na sloju podatkovne povezave, posledično prav tako podatkovni promet med napravami v omrežju. Omrežne naprave so z mrežnimi kablji UTP (ang. *UTP – Unshielded Twisted Pair*) povezane na stikala in se identificirajo na podlagi njihovega strojnega naslova (ang. *MAC address*), kar omogoča prvi, t. i. fizični sloj (ang. *physical layer*). Stikala si sprotno ustvarjajo tabele teh naslovov, ki jih nato uporabljajo

za učinkovito posredovanje paketov znotraj omrežja. Ker se takšnih stikal tretji sloj t. i. omrežni sloj (ang. *network layer*) ne tiče veljajo za izredno hitra in učinkovita, saj se ne potrebujejo ukvarjati še z usmerjanjem paketov. Stikala drugega sloja (ang. *layer-2 switch*) pogosto imenujemo tudi upravljana stikala, kar je že iz imena razvidno, da jih je mogoče tudi upravljati oziroma nastavljeni (npr. vzpostavitev VLAN).

V tem omrežju trenutno konfiguracij VLAN še ni, in sicer zaradi zelo pogostih zahtev oziroma želj uporabnikov po deljenju datotek in tiskalnikov neposredno med njihovimi računalniki (tako med tistimi znotraj istih stikal kot tudi med tistimi iz različnih vozlišč in stikal). Optimalna konfiguracija VLAN zaradi omenjenih potreb v obstoječem omrežju tudi zaradi fizičnih karakteristik obstoječih stikal ne bi bila mogoča, saj bi bilo za to treba ustrezno usmerjati promet VLAN. V omrežju podjetja so namreč v vozliščih vsa stikala, kot sem že omenil, tipa drugega sloja, ki pa ne omogočajo usmerjanja prometa VLAN, kot to omogoča višji tip stikal, npr. stikala tretjega sloja (ang. *layer-3 switch*). Za to bi v omrežju potrebovali dodatni notranji usmerjevalnik (ang. *core router*), ki bi usmerjal promet naprav med VLAN-i tudi znotraj istega stikala, ali pa bi morali zamenjati vsa stikala s tipom tretjega sloja. Ker vzpostavitev konfiguracij VLAN tokrat ni bila prioriteta, sem slednje pustil za naslednji večji projekt dodatne optimizacije notranjega omrežja.

Vozlišča so preko optičnih povezav povezana v centralni strežniški prostor, kjer so strežniki, glavna stikala in tudi robni strežnik, ki je prek stikala ponudnika internetnih storitev povezan v internet. Na stikalih vozlišč so aktivne povezave navzgor (ang. *uplink*) vzpostavljene s pomočjo samostojnih 100M-bitnih optičnih pretvornikov tipa *Allied Telesyn AT-MC102XL (100TX to 100FX (SC))* kar medsebojno povezuje vse naprave tega omrežja. Ta model prikazuje spodnja slika (Slika 3).



Slika 3: Optični pretvornik Allied Telesyn AT-MC102XL [3]

Vsa komunikacijska oprema je v strežniškem prostoru in v omarah vozlišč povezana na brezprekinitveno napajanje, saj je ta ključna za delovanje omrežja.

2.1 Nabor storitev in potreb

V omrežju je skupaj 43 strežnikov, od tega 16 virtualnih različnih tipov in operacijskih sistemov (Microsoft Server 2000, 2003, 2008 R2 in 2012 R2, Ubuntu Server, XenServer, CentOS ...), ki nudijo notranjim in zunanjim uporabnikom raznovrstne storitve.

Kratko bom opisal storitve in funkcionalnosti, ki jih omogočajo strežniki in naprave, ki morajo biti za različne namene dostopni tudi odzunaj. Te strežnike in naprave bom v nadaljevanju imenoval kot »zunanji strežniki« oziroma »zunanje«. Vse storitve in funkcionalnosti tega omrežja omogoča prav robni strežnik, od katerega je odvisno tudi pravilno in optimalno delovanje vsake izmed njih.

Storitev spremljanja elektronske pošte:

- Med pomembnejšimi storitvami je spremljanje (pošiljanje in prejemanje) elektronske pošte, kar je postalo v tem času postalo del vsakdana. Preko poštnega strežnika tega podjetja se pošilja in prejema vedno večje količine podatkov, ki so v nekaterih primerih ključni za nemoteno delo. Za to je treba tudi tukaj poskrbeti za ustrezno hitrost in varnost teh prenosov. E-poštne storitve lahko zaposleni uporabljajo od kjerkoli, tudi preko mobilnih naprav, kot so prenosniki, pametni telefoni ter tablice z nameščenimi in ustrezno konfiguriranimi e-poštnimi odjemalci. Na voljo pa je tudi storitev spletne pošte (ang. *webmail*), ki omogoča dostop do uporabnikovega poštnega nabiralnika preprosto preko spletne strani.

Storitev spletnih strani in spletnih aplikacij:

- V podjetju deluje več spletišč, ki so množično in redno obiskovana. Gostujoče so na spletnih strežnikih podjetja, ki se z njimi predstavlja tudi zunanjemu svetu. Zaposlenim omogočajo objavo raznovrstnih vsebin, dogodkov, novic, projektov itd. ter vsakodnevno delo v različnih spletnih aplikacijah.

Storitev oddaljenega namizja (ang. *RDS – Remote Desktop Services*):

- Gre za storitve, ki uporabnikom omogočajo delo preko oddaljenega namizja. Dostop do strežnikov, ki nudijo te storitve, je zagotovljen tako znotraj internega omrežja kot tudi od zunaj, za potrebe dela od drugod.

Storitev shranjevanja in arhiviranja podatkov:

- V omrežju so te storitve realizirane s pomočjo omrežnih diskovnih polj NAS (ang. *NAS – Network Attached Storage*) oziroma krajše: NAS-naprav. Te se v podjetju uporabljajo za shranjevanje podatkov, arhivov in tekočih projektov, pri katerih sodeluje in gradi bazo podatkov več uporabnikov hkrati. Nekatere so dostopne zgolj interno, druge pa tudi od zunaj.

Storitev za nalaganje in prenos datotek:

- V podjetju jih potrebujejo za preprosto in hitro izmenjavo datotek in podatkov, kar omogočajo t. i. FTP-strežniki. Podatke si izmenjujejo z zunanjimi sodelavci in strankami, uporabljajo pa jih tudi uredniki spletnih strani za prenos datotek v podatkovne baze spletnih strežnikov, kot so npr. članki, ki jih pošljejo uporabniki na FTP-strežnik.

Storitev gostovanja plavajočih licenc:

- Le-te omogoča strežnik s plavajočimi licencami (ang. *floating licence server*), ki gostuje licence določenih programov, ključnih za delo v podjetju, in s tem omogoča njihovo uporabo tudi od druge.

Storitev pretvorbe imen:

- V omrežju sta tudi dva zunanja DNS-strežnika (ang. *external DNS server*) primarni in sekundarni, ki zagotavljata pretvorbo imen za domene, ki jih uporablja podjetje. Zaradi večjega števila zgoraj omenjenih strežniških storitev je uporaba le-teh praktična in zagotavlja fleksibilnost in neodvisnost pri zamenjavah ali selitvah strežnikov oziroma storitev.

Storitev brezžičnega dostopa do interneta:

- V sodobnem času skoraj vsak uporabnik že uporablja pametni telefon in brezžično internetno povezavo, nekateri izmed njih pa poleg stacionarnih delovnih postaj uporabljajo tudi prenosne računalnike za delo v službi, za kar uporabljajo večinoma brezžično povezavo. Brezžični dostop do spleta v vseh zgradbah in prostorih podjetja, omogoča 20 brezžičnih usmerjevalnikov. Za potrebe zaposlenih so večinoma konfigurirani kot »brezžične dostopne točke«, tako da je mogoče brezžično dostopati poleg spleta tudi do notranjih omrežnih sredstev. Ker pa so v podjetju občasno tudi gosti, so za ta namen nekateri konfigurirani tudi kot brezžični usmerjevalniki in je tako njihov promet ločen (izoliran) od notranjega omrežja podjetja.

2.2 Problematika omrežja

Zaradi v uvodu omenjenih velikih količin prenesenih in poslanih podatkov v korporativnem omrežju oziroma lokalnem omrežju podjetja s 350 zaposlenimi, s katerim sodelujem in kjer bom implementiral boljšo rešitev, so se na obstoječem robnem strežniku vedno pogosteje začeli pojavljati problemi. Le-ti so začeli ovirati celoten omrežni promet in s tem tudi delo v podjetju. Trenutno stanje omrežja in zmogljivost robnega strežnika omogočata slabo izkoriščenost 100/100 Mbit/s internetne povezave in s tem povzročata upočasnenost tega omrežja.

Sklepam, da so težave nastale tudi zaradi dotrajane in zastarele strojne opreme strežnika (zastarela centralna procesna enota (ang. *CPU – Central Processing Unit*) – v nadaljevanju procesor, zastarel in počasen pomnilnik (ang. *RAM – Random Access Memory*), zastarele mrežne kartice (ang. *NIC – Network Interface Card*)) ter starejšega operacijskega sistema – Microsoft Windows Server 2000, ki je že vrsto let brez podpore posodobitev.

Ena izmed mojih hipotez, zakaj je delovanje omrežja tako problematično, je tudi ta, da obstoječi robni strežnik glede na svoje zmogljivosti opravlja preveč pglavitnih funkcij in vlog hkrati.

Funkcije in vloge, ki jih opravlja trenutni robni strežnik:

- storitev usmerjanja prometa in oddaljenega dostopa (ang. *RRAS – Routing and Remote Access Service*);
- požarni zid – Program *Visnetic* –, pri katerem je prišlo do prevzema podjetja in je nov lastnik ukinil nadaljnji razvoj in podporo te programske požarne zaščite;
- mehanizem prevajanja omrežnih naslovov NAT (ang. *NAT – Network Address Translation*);
- notranji sistem domenskih imen oziroma interni DNS, ki je integriran z aktivnim imenikom AD na drugem strežniku.

V omrežju podjetja so se začele dnevno pojavljati daljše zakasnitve (ang. *latency*) ter včasih tudi začasna odpoved delovanja omrežja. V tem času je bila vsa komunikacija v omrežju in izven njega onemogočena. Za ponovno vzpostavitev dostopa do prostranega omrežja interneta je bilo treba znova zagnati robni strežnik. Procesor robnega strežnika je pri malo večji obremenitvi omrežja dosegal največje zmogljivosti (dlje časa konstantno 100-% obremenjen), zaradi česar je posledično zelo upadla hitrost interneta. Hkrati pa so za dlje časa narasle zakasnitve omrežja (pogosto nad 1000 milisekund) in so se znižale šele takrat, ko se je stanje robnega strežnika umirilo. Ob takih preobremenjenosti je bilo zaradi zelo počasne odzivnosti operacijskega sistema tudi upravljanje strežnika izredno oteženo. Vse skupaj sem dlje časa preverjal in analiziral s pošiljanjem in prejemanjem paketov na IP-naslov Arnesovega strežnika (193.2.1.87) z orodjem *ping* ter spletno aplikacijo za preverjanje hitrosti internetne povezave, dostopno na spletnem naslovu <http://www.speedtest.net>. Aplikacija posreduje kot rezultat precej realne podatke o hitrosti internetnega prenosa (ang. *download*) kot tudi hitrosti nalaganja (ang. *upload*) in zakasnitev ob času preverjanja.

Med drugim sem večkrat spremljal tudi vhodni in izhodni promet ter ga analiziral. Strežnik preprosto ni zmozel procesirati vseh zahtevkov, ki sta jih pri obremenitvah zahtevali obe omrežni kartici. Vpogled v stanje uporabe sistemskih sredstev v operacijskega sistema Windows Server 2000 je preprosto mogoč kar prek upravitelja opravil (ang. *task manager*), kjer je očitno razbrati problematiko tudi delovanja samega jedra operacijskega sistema (ang. *kernel*), ki posreduje dostope do sistemskih sredstev. Kar pomeni, da ni zmozel več

učinkovito in pravočasno deliti sredstev strojne opreme vsem aplikacijam in procesom. Iz tega je razvidno, da tudi sama strojna oprema fizično ni več zadoščala vsem potrebam tega omrežja.

Karakteristike prejšnjega robnega strežnika:

Procesor: AMD Athlon™ XP 2200+ (1-jedrni, L1 Cache = 64KBytes, L2 Cache = 256KBytes)

Sistemski pomnilnik: velikosti 512 MB, tipa DDR in hitrosti 400 MHz

Omrežne kartice: dve omrežni kartici – ena za notranje LAN-omrežje ter druga za povezavo v internet (zunanje WAN-omrežje)

Notranja – Realtek RTL8139/810x Family Fast Ethernet NIC (10/100 Mbit/s)

Zunanja – Realtek RTL8139/810x Family Fast Ethernet NIC (10/100 Mbit/s)

Operacijski sistem: Microsoft Windows 2000 SP4 (32-bitni)

V omrežju se pojavlja tudi problematika napačnega razreševanja notranjih domenskih naslovov (DNS-vpisov). Pri iskanju DNS-vpisa določene naprave se tako domensko ime naprave kot njen IP-naslov pogosto nista ujemala oziroma je prikazani IP-naslov kazal na drugo napačno napravo ali obratno. Zaradi tega je bilo kdaj kako težavo na omrežju težko identificirati in locirati. Povzročitelje je bilo treba vedno še enkrat preverjati na strežniku za dinamično konfiguriranje gostiteljev DHCP (ang. *DHCP – Dynamic Host Configuration Protocol*), kjer pa je bil seznam vpisov oziroma seznam notranjih domenskih imen naprav z ustreznimi IP-naslovi pravilen. Ker je tudi omenjeni DHCP-strežnik že zastarel in kot še edini v omrežju (poleg robnega) z operacijskim sistemom Microsoft Windows Server 2000, je smiselno ob tej reševanju te problematike poiskati hkrati tudi ustrezno rešitev za to.

Na podlagi vseh dejstev, rezultatov, daljšega opazovanja delovanja omrežja in robnega strežnika ter analiz pri testiranjih prometa je jasno razvidno, da je glavni razlog za omenjene težave prav robni strežnik.

3 Načrtovanje robnega strežnika

Glavno omejitev pri izbiri oziroma nakupu robnega strežnika so predstavljala omejena denarna sredstva, zato je bilo treba poiskati najboljšo rešitev glede na ceno, zmogljivost in ustreznost, ob tem pa zagotoviti, da bo tako strojna oprema strežnika kot programska zadoščala vsem trenutnim in prihodnjim potrebam omrežja.

3.1 Smernice načrtovanja

Pri načrtovanju tega omrežja oziroma pri načrtovanju robnega strežnika sem sledil osmim zastavljenim splošnim smernicam oziroma t. i. osnovnim pravilom načrtovanja.

Določene smernice sem zastavil na podlagi priporočil o nespremenljivih zakonih pri načrtovanju omrežja (ang. *Immutable Laws of Network Design*) [4] ter ostale na podlagi osebnih izkušenj, ki sem jih pridobil v zadnjih šestih letih kot vzdrževalec IT-infrastrukture in sistemski administrator.

Zastavljene splošne smernice:

- Vedi, ne ugibaj

Za omrežja lahko rečemo, da so podedovana, saj se jih v njihovem obstoju dotakne marsikateri omrežni administrator in jih spreminja glede na trenutne potrebe, bodisi pri reševanju težav, iskanju rešitev ali zgolj pri testiranju. [4] Pred dejansko implementacijo je treba podrobno pregledati obstoječe omrežje, vozlišča, optične pretvornike, stikala, brezžične usmerjevalnike, in sicer tako njihovo fizično stanje kot konfiguracijo. Ustvariti je treba natančno in pregledno shemo za lažjo predstavo celotnega omrežja, s pomočjo katere se preprosto in hitro vidijo povezave in fizične lokacije. Pred resnim posegom v omrežje vedno preverimo in se prepričamo o posledicah takšnega posega.

- Varnostno kopiranje

Vedno poskrbimo za posnetek sistema oziroma varnostno kopijo (ang. *backup*) vsakega strežnika v omrežju, ki ga bomo spreminjali. Uspešnega delovanja nove implementacije in s tem delovanja celotnega omrežja ni nikoli mogoče popolnoma predvideti. Nekatere težave so hitro in preprosto rešljive, lahko pa pride do kritične situacije, katere reševanje bi povzročilo

daljši izpad delovanja omrežja. V takšnih primerih je treba poskrbeti za možnost povrnitve celotnega sistema v prejšnje stanje. Ker je včasih to nemogoče, so za to ključnega pomena varnostne kopije.

- Vzpostavi testno okolje

Nikoli ne preizkušajte pomembnih stvari, ki zadevajo celotno omrežje, kot je npr. usmerjanje prometa, dodeljevanje naslovov, globalnih požarnih pravil itd., v obstoječem omrežju. Vzpostaviti je treba vzporedno testno okolje za preverjanje in testiranje, ki naj bo ločeno od obstoječega omrežja. V testnem okolju poskušamo vzpostaviti stanje, ki bo čim bolj podobno obstoječemu omrežju, in preizkušamo zadeve, ki so v obstoječem ključnega pomena. V testnih okoljih se velikokrat pojavijo napake in nepredvideni zapleti in imamo zagotovljen čas za njihovo odpravo ali optimizacijo.

Glavni smisel testnega okolja je, da se v njem odpravi kolikor se le da zapletov, težav in se v naprej ustrezno pripravi implementirano rešitev, tako da je čas okrnjenega delovanja ali nedelovanja omrežja po dejanski implementaciji čim krajši.

- Dokumentiraj, beleži

Vedno zabeležimo vsa trenutna stanja – tako osnovne kot napredne nastavitve, funkcije in povezave naprav pred posegom v omrežje. Zabeležimo vsak korak in spremembo v konfiguraciji sistemov, da lahko na podlagi tega hitro najdemo vzrok napake ter ugotoviš kako in na kakšen način povrniti stanje. Včasih je tudi kaka najmanjša malenkost v teh dokumentih bistvenega pomena in je ključna pri odkrivanju kakšne napake, lahko pa je ta sprememba tudi vzrok za izboljšano delovanje omrežja ali določene storitve.

- Preizkusi več rešitev, ne samo eno

Prva rešitev ni vedno nujno najboljša, čeprav se na prvi pogled zdi kot celovita in optimalna. Zato je treba preizkusiti in imeti na razpolago vedno več rešitev, ki jih lahko primerjamo ter poiščemo njihove prednosti in slabosti ter se na podlagi tega odločimo za najboljšo oziroma najustreznejšo.

- Preprosto, pregledno omrežje

V testnih omrežjih je mogoče preizkušati poljubne konfiguracije, česar v realnih oz. delujočih omrežjih ne moremo. Tukaj je dobro slediti stavku »Obdrži preprostost in enostavnost« (ang. *keep it simple and straightforward*) [5].

Pri posegih v omrežja velja pravilo, da ne komplicirajmo preveč, saj bi s tem gradili še bolj kompleksno in nepregledno omrežje; stremeti moramo k temu, da so stvari preproste, pregledne in logične.

- Odločitev vzpostavitve navideznih lokalnih omrežij na upravljanih stikalih

Pri odločitvi konfiguracije navideznih lokalnih omrežij (ang. *VLAN – Virtual Local Area Network*) se moramo izogibati konfliktnim in neusklajenim situacijam. V omrežjih so pogost pojav napačno konfigurirana omrežja VLAN na upravljanih stikalih (ang. *managed switch*), kot npr. napačno označena vrata na stikalu (ang. *tagged port*), ki bi sicer morala biti neoznačena (ang. *untagged port*), ali pa VLAN slepe ulice (ang. *dead end*) v neoznačenih VLAN-ih. [4].

Odločitev za tako obsežen poseg v omrežje mora biti tehtno premišljena na podlagi obstoječe komunikacijske opreme (vrsta, tip stikal ...) in tudi na podlagi zahtev uporabnikov in ostalih naprav v danem omrežju.

- Električno napajanje je pomembno

Prepričaj se, da so vsi ključni sistemi za optimalno delovanja celotnega omrežja priključeni v brezprekinitveno napajanje (ang. *UPS – Uninterruptible Power Supply*). Pri izbiri in nakupu novih strežnikov bodimo pozorni na to, da vključujejo možnost uporabe dveh napajalnikov, pri čemer drugi služi kot redundantni, če je prvi okvarjen. Redno je treba preverjati, da naprave UPS in njihovi akumulatorji (baterije) delujejo optimalno, da niso polno obremenjeni in imajo na razpolago dodatno rezervo. Priporočen je redni servis s strani podjetja za naprave UPS vsaj enkrat mesečno. Ob kakršnihkoli nenadnih napakah, odpovedi katerega od akumulatorjev ali preobremenitvah pa se mora sprožiti zvočni alarm z obvestilom o napaki na zaslonu naprave UPS in takrat je treba takoj ukrepati.

3.2 Kriteriji izbire ustreznega strežnika

Na podlagi zgoraj omenjenih omejitev in potreb, spremljanja podatkovnega prometa ter starega robnega strežnika, sem določil priporočene strojne karakteristike, ki jih bo treba upoštevati pri nakupu.

- Strežnik oblike rezine za vgradnjo v telekomunikacijsko omaro
- Procesor (CPU): *Intel Xeon* z vsaj štirimi jedri (ang. *4-core*) z minimalno velikostjo predpomnilnika 8 MB (ang. *cache*) s tehnologijo večnitenja HT (ang. *HT – Hyper-threading*)
- Sistemski pomnilnik (RAM): vsaj 8 GB DDR3 (z dodatnimi prostimi razširitvenimi režami – z možnostjo nadgradnje)
- Mrežne kartice (NIC): 4 (lahko tudi 2) hitrosti *Gigabit (GbE)* – z lastnostjo razbremenitve procesiranja celotnega TCP/IP sklada (ang. *TOE – TCP/IP Offload Engine*)
- Vključevati mora krmilnik za redundantno diskovno polje (ang. *RAID controller*).
- Vključevati mora vsaj dva zmogljiva in hitra trda diska, npr. tipa SAS s hitrostjo vrtiljajev vsaj 10000/min (ang. *10 K RPM – 10.000 revolutions per minute*) in zmogljivosti vsaj 300 GB.
- Vsaj dva vgrajena ločena električna napajalnika (eden kot redundantni)

Večnitenje predstavlja možnost obdelave več procesov hkrati, kakor jo tudi opisuje njena definicija (po www.islovar.org). Ta tehnologija uporablja razpoložljiva sredstva procesorja učinkoviteje, saj omogoča še dodatno na vsakem jedru procesorja izvajanje več niti naenkrat [6]. Ker večnitne (ang. *multithread*) operacije omogočajo oziroma izkoriščajo tudi trenutne različice *pfSense* [7], bo to pomenilo še hitrejšo procesiranje vseh zahtevkov in boljše delovanje.

Hitrost lokalnih omrežij *Ethernet* je narasla iz začetnih 10 Mbit/s na 10 Gbit/s, kar pomeni da se je hitrost komunikacij povečala hitreje kot hitrost računalniških in strežniških procesorjev. To pa povzroča t. i. ozko grlo (ang. *bottleneck*) za vhode in izhode I/O (ang. *Input/Output*)

[8], ki jih generirajo vhodno izhodne naprave (npr. mrežne kartice). V našem primeru so vhodi vsi podatki in povezave, ki jih robni strežnik prejema preko mrežnih kartic, in izhodi vsi tisti, ki jih oddaja naprej. Procesorji težka sledijo vsej masi podatkov, ki se prenašajo po hitrih omrežjih, saj so v osnovi zasnovani za računanje [8]. Lahko se zgodi, da so hitrosti pretoka podatkov v omrežju višje, kot jih premore preleteti procesor, in je zato pretok procesiran počasneje. Za to pa je bila razvita tehnologija razbremenitve procesiranja TCP/IP-sklada, ki rešuje ta problem.

3.3 Kriteriji izbire programske opreme

Z implementirano rešitvijo je potrebno zadostiti vsem storitvam in potrebam tega omrežja, predvsem pa tudi zagotoviti, da programska oprema robnega strežnika omogoča vnos vseh ažurnih pravil prejšnjega požarnega zidu ter da le ta deluje ustrezno in učinkovito. Pri iskanju ustrezne rešitve sem za to postavil tudi nekakšno hierarhijo zahtev uporabnikov. Pri tem pa upošteval tudi potrebe strežnikov in ostalih naprav, da bo njihovo delovanje po implementaciji robnega strežnika optimalno.

Zahteve uporabnikov:

- Direktor: Omogočiti dostop do službenega računalnika in notranjih omrežnih diskov iz oddaljenih lokacij. Oddaljena pomoč – IT-administracija do njegovega računalnika iz oddaljenih lokacij tudi ob vikendih in praznikih.
- Računovodstvo: Omogočiti dostop do službenih računalnikov in računovodskih strežnikov iz oddaljenih lokacij. Omogočiti, da v primerih uporabe prenosnega računalnika, s katerim se uporabnik povezuje preko oddaljenega namizja na svojo delovno postajo lokalno v omrežju in od zunaj, ni treba vedno znova spreminjati zunanjšega IP-naslova gostitelja (delovne postaje) v notranjega. Torej, da se lahko iz notranjega omrežja dostopa do naprave tudi prek zunanjšega IP-naslova.
- IT administracija: Omogočiti dostop do službenih računalnikov, računalnika direktorja iz oddaljenih lokacij. Dostop mora biti urejen tudi do robnega strežnika (lahko tudi posredno preko drugega strežnika s storitvami oddaljenega namizja) in do ostalih pomembnejših strežnikov, kot so npr. (poštni, strežnik z aktivnim imenikom,

računovodski ...) le iz točno določenih statičnih zunanjih IP-naslovov. Za potrebe oddaljene administracije ostalih odprtokodnih strežnikov (*Ubuntu server* ...) omogočiti dostop tudi preko varne lupine SSH (ang. *SSH – Secure Shell*).

- Organizacijske enote: Poskrbeti za posamezne potrebe enot in zaposlenih kot na primer zunanji dostop do strežnikov za prenos datotek – prek standardnega protokola FTP in varnega SFTP (ang. *SFTP – Secure File Transfer Protocol*), NAS-naprav ter strežnikov s storitvami oddaljenega namizja. Zagotoviti tudi zunanji dostop do strežnika s plavajočimi licencami le določenim zaposlenim (z restriktivnimi pravili požarnega zidu) za uporabo programov, ki te zahtevajo. Zagotoviti zunanji dostop do strežnika s plavajočimi licencami tudi oddaljenim enotam (pisarnam).

Zahteve strežnikov:

- Poštni strežnik: Je eden izmed tistih, ki redno in najpogosteje (poleg robnega) komunicira z zunanjim svetom in katerega je treba posledično tudi dodatno ustrezno zaščititi. Ščitijo ga požarni zid robnega strežnika in ustrezna pravila, ki morajo biti skrbno premišljena in točno določena. Do poštnega strežnika je treba zagotoviti zunanji dostop od kjerkoli, dodatno nevarnost pa predstavlja tudi dejstvo, da do njega lahko dostopajo uporabniki tudi prek mobilnih naprav. S konfiguracijami e-poštnih programov na teh napravah obstaja povečano tveganje za nedovoljene poskuse pridobitev tako uporabniških kot strežniških prijavnih podatkov (uporabniško ime, geslo). Še posebej zaradi možnosti brezžičnih povezav teh naprav na odprta in nezavarovana omrežja, kot so npr. spletne kavarne. Ker so takšna omrežja prosto dostopna, promet preko njih nešifriran, lahko spletni kriminalci te podatke prestrežejo na način prisluškovanja (ang. *packet sniffing*) in se tako dokopljejo do pomembnih informacij. Zaradi omenjenega mora biti na takšnih napravah ustrezna in varna konfiguracija e-poštnih odjemalcev, da je podatkovni promet vsaj med njimi in poštnim strežnikom šifriran. Vzpostavitev šifrirane povezave med takšnima napravama mora seveda omogočati predhodno tudi poštni strežnik, robni strežnik pa mora dovoljevati to vrsto prometa skozi požarni zid. Za interno (notranjo) komunikacijo v omrežju med klienti in poštnim strežnikom ni nujno uporabljati šifrirane povezave, saj ves takšen promet ostane znotraj omrežja. Zaradi tega znotraj omrežja uporabljamo zgolj standardni e-poštni protokoli za dostop in prejemanje e-

pošte preko POP3 (ang. *POP3 – Post Office Protocol*) in IMAP (ang. *IMAP – Internet Message Access Protocol*) ter za pošiljanje SMTP (ang. *SMTP – Simple Mail Transfer Protocol*). Šifriranje zunanje podatkovne komunikacije pa je na obstoječem poštnem strežniku zagotovljeno s pomočjo protokola SSL (ang. *SSL – Secure Socket Layer*). Ker protokol šifriranja povezave SSL deluje tudi v uporabi z ostalimi protokoli, ga v našem primeru uporablja tudi IMAP-protokol na strežniku in se tako imenuje tudi IMAP preko SSL (ang. *IMAP over SSL*) [9]. V omrežju deluje tudi strežnik za spletno pošto, ki je prav tako tesno povezan s poštnim. Ker je pri vpisu uporabnika v svoj račun (preko spletne pošte) potreben le vnos uporabniškega imena in gesla, je tudi ta promet šifriran s protokolom IMAP preko SSL.

Za ustrezno konfiguracijo pravil požarnega zidu za namen poštnega strežnika je treba poznati vrata (ang. *ports*), ki jih uporabljajo zgoraj omenjeni protokoli, in dovoliti komunikacijo le prek teh. Za nešifrirano pošiljanje pošte *SMTP* uporablja vrata 25, za prejemanje POP3 vrata 110 in za IMAP vrata 143. Za šifrirano pošiljanje SMTP preko SSL vrata 465, za varen dostop IMAP preko SSL vrata 993. Za potrebe distribucijskega seznama oziroma t. i. »mailing liste« potrebuje še dovoljeno komunikacijo prek vrat 8080.

Na požarnem zidu robnega strežnika pa je treba tudi zagotoviti, da lahko standardna vrata 25 za pošiljanje uporabljajo zgolj poštni strežnik podjetja ter Arnesovi strežniki za odhajajočo pošto, vsem ostalim pa se ta promet blokira. To pa zaradi morebitnih zlonamernih in škodljivih programov, ki bi se lahko namestili na računalnike klientov ali strežnike za namen smetenja oziroma pošiljanja neželene elektronske pošte v različne namene (oglaševanje, širjenje okužb itd.).

- Spletni in aplikacijski strežniki: Spletni strežniki (ang. *web server*) in aplikacijski strežniki (ang. *application server*) uporabljajo za svoje delovanje najbolj razširjena protokola HTTP (ang. *Hypertext Transfer Protocol*) s standardnimi vrati 80 in HTTPS (ang. *Hypertext Transfer Protocol Secure*) z vrati 443. Da bodo spletišča gostujoča na spletnih strežnikih podjetja ter spletne aplikacije dostopne od koderkoli, bo treba na požarnem zidu ustrezno definirati pravila in odpreti omenjena vrata TCP 80 in 443. Tudi za njihov obstoj in hitrost nalaganja, ko je to zahtevano s strani obiskovalca spletne strani, je v veliki meri odgovoren robni strežnik. Določeni aplikacijski in

strežniki s podatkovnimi bazami pa zahtevajo, da se v požarnem zidu do njih dovoljuje tudi komunikacijo preko drugih vrat. Tako eden izmed strežnikov z SQL podatkovno bazo (SQL strežnik #1) zahteva komunikacijo preko vrat 8080 in 1433.

- Strežniki s storitvami oddaljenega namizja: Uporabljajo znan protokol oddaljenega namizja (ang. *RDP – Remote Desktop Protocol*), ki uporablja standardna vrata TCP (ang. *TCP – Transmission Control Protocol*) 3389. Zato je treba na požarnem zidu dovoliti vhodni promet preko vrat TCP 3389. Zaradi uporabe ter storitev iz različnih nestatičnih IP-naslovov je treba dovoliti promet od koderkoli.
- NAS naprave: V omrežju jih je 23 in do nekaterih mora biti dovoljen tudi zunanji dostop. Za ta namen je za podatkovne prenose omogočena povezava prek varnega protokola za prenos datotek SFTP, ki v osnovi uporablja vrata TCP 22. Ker so pa omenjena vrata pogost poskus vdorov v informacijske sisteme, je le-ta smiselno spremeniti v višjo nestandardno naključno številko vrat (če naprava to omogoča), kar še dodatno izboljša varnost. Z ustreznimi pravili požarnega zidu je tako za določene naprave potrebno urediti zunanje dostope preko vrat TCP 22 od koder koli.
- FTP strežniki: Ker komunikacija med klienti in standardnimi FTP-strežniki ni zaščitena oziroma šifrirana, sodijo ti med bolj »ranljive«. Anonimne prijave na teh strežnikih so onemogočene, saj bi se lahko v nasprotnem primeru prijavil kdorkoli, ki lahko pridobi informacije o programski opremi FTP-strežnika, poišče morebitne varnostne luknje v sistemu in ga zlorabi. V omrežju deluje nekaj strežnikov obeh vrst – tako aktivni kot pasivni, oboji pa uporabljajo za ukazni kanal (ang. *command channel*) standardna vrata TCP 21. Glavna razlika aktivnim in pasivnim načinom delovanja je v tem, da se pri aktivnem v osnovi uporablja za podatkovni kanal standardna vrata TCP 20, pri pasivnem pa se le-ta naključno izberejo. Zaradi naključne izbire vrat velja pasivni način za manj varnega, saj za delovanje zahtevajo večji razpon vrat (ang. *port range*), ki jih mora pravilo požarnega zidu dovoljevati, drugače se podatkovni kanal ne more vzpostaviti. Za to je smiselno nastaviti le določen obseg vrat na FTP-strežniku in dovoliti le ta. Treba bo definirati ustrezno pravilo požarnega zidu, ki bo omogočalo zunanji dostop (od koderkoli) preko vrat TCP 20 in TCP 21, vendar le za zunanja števila visokih vrat (ang. *high ports*) 1024-65535.

- Strežnik s plavajočimi licencami: Zahteva, da so na požarnem zidu odprta določena vrata TCP (1246, 3955) in razpon vrat TCP (27000:27010), ki se pri komunikacijah med uporabniki, ki licenco zahtevajo, ter strežnikom naključno določajo. Zaradi dodatne varnosti mora biti zunanji dostop do tega strežnika omejen le iz specifičnih zunanjih IP-naslovov, kar mora zagotavljati ustrezno (restriktivno) pravilo požarnega zidu.
- Zunanja DNS-strežnika: Poleg vloge pretvorbe imen za domene, ki jih uporablja podjetje, sta pomembna tudi zaradi varnosti omrežja. Na ta način fizično ločimo notranji DNS-strežnik, ki vsebuje informacije aktivnega imenika. Pri delovanju uporabljata protokola TCP in UDP (ang. *UDP – User Datagram Protocol*) in komunicirata z zunanjim omrežjem preko vrat 53. Požarni zid robnega strežnika mora za njuno ustrezno delovanje dovoljevati komunikacijo (TCP in UDP preko vrat 53) z poljubnimi napravami zunaj omrežja.

Vsi zgoraj naštetih strežniki, omrežne naprave in določeni računalniki morajo imeti konfigurirane statične notranje IP-naslove. Da bi bili dostopni od zunaj, pa potrebujejo tudi svoje enolične zunanje IP-naslove, za to je potrebna ustrezna individualna konfiguracija načina prevajanja naslovov z uporabo 1 : 1 NAT za vsakega izmed njih. Zaradi velikega števila in raznovrstnosti strežnikov in njihovih zahtev je treba na robnem strežniku premišljeno in skrbno konfigurirati pravila požarnega zidu. Od tega bo namreč odvisno njihovo pravilno delovanje in predvsem tudi varnost, ki jo nudi robni strežnik. Pri vseh dostopih, kjer je pri oddaljenih lokacijah možna uporaba statičnih zunanjih IP-naslovov, je smiselno s pravilom požarnega zidu restriktivno omejiti dostope le s teh naslovov.

4 Predlagana arhitektura robnega strežnika

V tem poglavju bo opisana tako strojna kot programska oprema predlaganega robnega strežnika. Podrobneje bo opisana programska oprema, njene vloge in funkcije, ki jih bo strežnik opravljal. Omenil bom tudi dodatne funkcionalnosti, ki bi jih bilo smiselno dodatno implementirati v prihodnosti.

4.1 Strojna oprema (specifikacija, karakteristike)

Spodaj je podana strojna oprema predlaganega in kupljenega strežnika, na katerem bo nameščena izbrana programska oprema. Strežnik je bil cenovno ugoden in v vseh pogledih zadošča zastavljenim kriterijem oziroma priporočenim karakteristikam.

Izbran je bila strežnik (rezina) znamke HP ProLiant model DL360 G7 s karakteristikami:

Procesor: *1x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz* (4-jedrni, 8-jedrni z *HyperThreading*), z 12 MB predpomnilnika (možnost nadgradnje – osnovna plošča omogoča dva procesorja)

Pomnilnik: *12 GB DDR 3 PC3 10600 (1066 MHz) (3 × 4 GB)* (maksimalno 384 GB)

Mrežne kartice: *HP NC382i Dual Port Multifunction Gigabit Server Adapter* (fizično 4 × 1GbE priključki)

Optične enote: *1 × DVD-RW*

Krmilnik: *HP Smart Array P410i/512MB* (krmilnik za redundantno diskovno polje)

Trdi diski: *2 × SAS 2,5" 300GB 10.000 RPM* (možnost nadgradnje še dodatnih dveh)

Napajanje: *2 × 460W CS Gold Hot Plug* (1 kupljen dodatno – redundantni)

Priključki: *1 × serijski vmesnik (ang. serial), 1 × video VGA (ATI ES1000), 1 × iLO 3 remote RJ-45, 1 × management port, 4 × USB 2.0* (2 zadaj, 1 spredaj, 1 notranji)

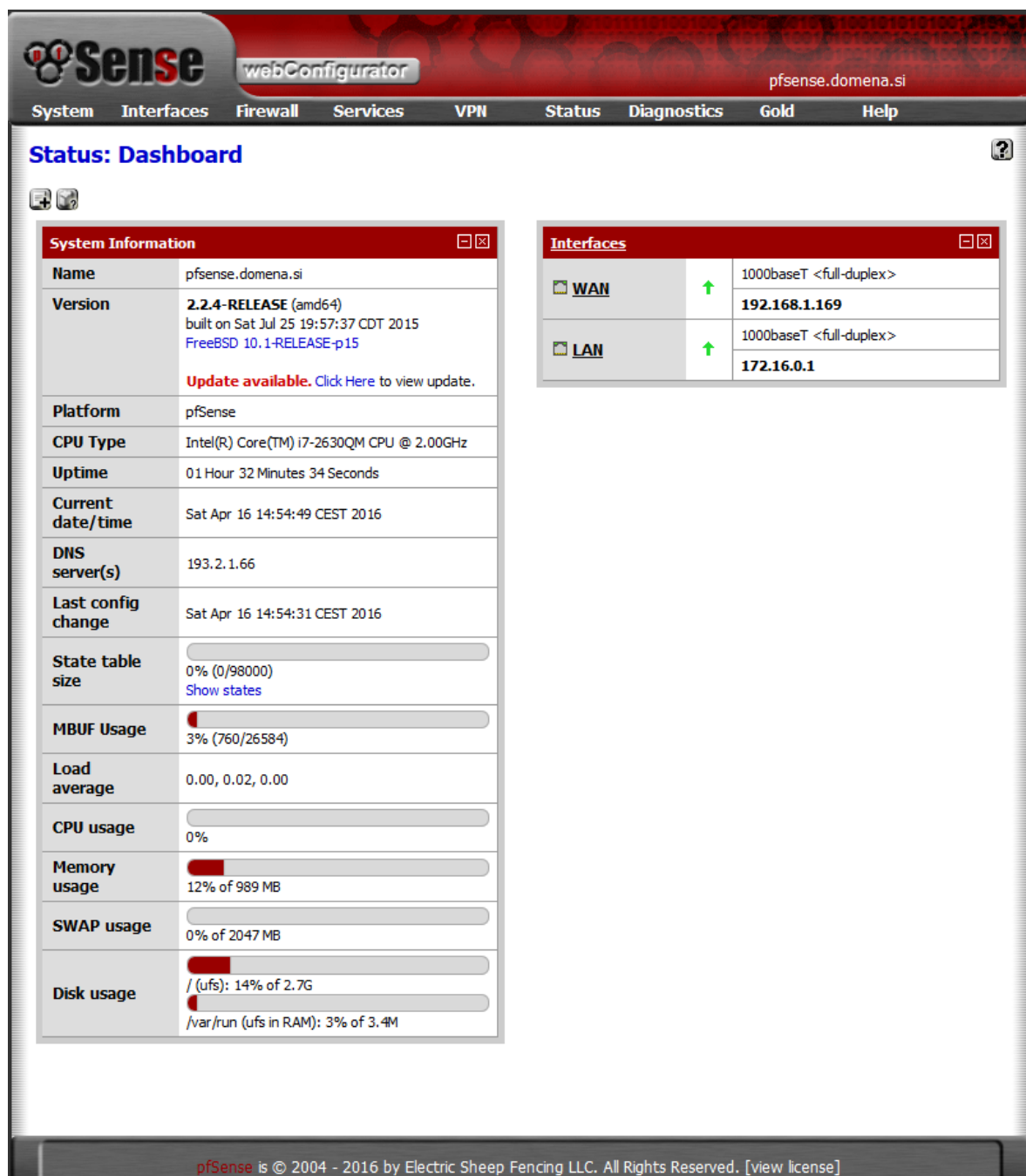
4.2 Programska oprema

V paketu skupaj s strežnikom je bil priložen tudi DVD-medij *HP SmartStart*, ki omogoča enostavno in hitro začetno postavitve strežnika. Če bi nameščal Microsoftov operacijski sistem, je s tem medijem možna tudi predpriprava strežnika, saj samodejno namesti vse potrebne gonilnike, glede na verzijo in arhitekturo operacijskega sistema. Zaradi odprtokodnega operacijskega sistema *FreeBSD* pa sem *HP SmartStart* uporabil zgolj za vzpostavitev logičnih diskov oziroma redundantnega diskovnega polja *RAID*.

Programska oprema, ki sem jo predlagal kot končno rešitev, se imenuje *pfSense*. Je odprtokodna programska oprema distribucije odprtokodnega operacijskega sistema *FreeBSD* in je posebej prilagojena za uporabo kot usmerjevalnik in požarni zid [10].

S projektom *pfSense* sta se leta 2004 začela ukvarjati začetna ustanovitelja Chris Buechler in Scott Ullrich, sčasoma pa sta pridobila več novih članov. Sama ideja in korenine te programske opreme izhajajo iz projekta *m0n0wall*, pri kateremu je v preteklosti sodeloval tudi Chris. Slednji je bil ukinjen januarja 2015 in se od *pfSense* najbolj razlikuje v tem, da ga ni mogoče namestiti na trdi disk, saj deluje kot vgradni sistem (ang. *embedded system*) in se v celoti pri zagonu zažene iz systemskega pomnilnika RAM [11].

Začetna namestitvev operacijskega sistema in programske opreme *pfSense* poteka preko upravljalnika (terminala) oziroma konzole kasneje pa tudi preko spletnega grafičnega uporabniškega vmesnika *WebGUI* (ang. *WebGUI – Web Graphical User Interface*). *WebGUI* predstavlja spletna stran, ki jo gostuje ta strežnik in je dostopna na IP-naslovu, ki ga dodeli administrator po inicializaciji mrežnih kartic. To pa olajša nadaljnjo konfiguracijo sistema, saj ukazov ni treba ročno vpisovati preko konzole. Po dodelitvi imena gostitelja (ang. *hostname*), v tem primeru imena strežnika ter vpisa domene (ang. *domain*), je dostop do *WebGUI* kasneje lahko mogoč tudi preko preglednejšega polnega imena (npr. *pfsense.domena.si*) namesto IP številke. Slika 4 prikazuje omenjen *WebGUI* in začetno stran *pfSense*, t. i. pregledno ploščo (ang. *dashboard*), kjer je prikazana večina pomembnih informacij.



Slika 4: *pfSense* pregledna plošča (začetni zaslon WebGUI) (Vir: Posnetek zaslona – *pfSense* 2.2.4 na VirtualBox (Status | Dashboard))

PfSense beleži stanja in spremembe vseh sistemskih konfiguracij ter omogoča enostavno povrnitev zadnjih nekaj sprememb, če je to potrebno. Omogoča tudi preprosto ročno varnostno kopiranje vseh uporabniških nastavitev v datoteko v formatu .XML, ki jo *pfSense* ponudi za prenos in shranitev na lokalni trdi disk računalnika. O tem, ali se arhivirajo tudi vsi podatkovni podatki, ki jih *pfSense* beleži in prikazuje v obliki grafov, se odloči administrator.

S pomočjo te datoteke, ki vsebuje celotno konfiguracijo *pfSense*, se lahko ponovno vzpostavi enako stanje sistema v primeru, da se ta popolnoma sesuje. Uporabljena datoteka (arhivska kopija konfiguracije) mora biti seveda ažurna, da je stanje novo vzpostavljenega sistema ustrezno. Vse, kar je treba storiti, je namestitev enake različice programske opreme *pfSense* ter v konzolnem vmesniku uvoziti, npr. preko USB ključka, datoteko z ustrezno konfiguracijo. Če se pri ponovni inštalaciji dodeli nastavitve mrežni kartici za LAN, je povrnitev iz datoteke s konfiguracijo mogoča tudi preko spletnega vmesnika.

PfSense predstavlja požarno pregrado z upoštevanjem vseh stanj in se zato imenuje tudi kot stanovitni požarni zid (ang. *stateful firewall*), saj deluje na način stanovitne kontrole paketov (ang. *stateful packet inspection*). Z drugimi besedami lahko to opišemo tudi kot dinamično paketno filtriranje. Takšni požarni zidovi ne gledajo le na pravila, ki jih je vnesel administrator in se ne odločajo le na podlagi vrat in protokolov paketov, temveč pri odločitvi dovoljevanja ali zavračanja paketov upoštevajo tudi njihovo zgodovino, ki jo hranijo v svojih tabelah stanja (ang. *state table*). V tabele si lahko zapisujejo več podrobnosti za vsako povezavo in vključujejo poleg podatkov o IP-naslovih, protokolih in uporabljenih vratih tudi stanja teh omrežnih povezav. Tako pri prejetju vsakega paketa najprej v tabeli preverijo njihove morebitne prejšnje povezave, ali če je bila zahteva za ta paket zahtevana s strani notranje naprave [12]. Paketi so prepuščeni pravilom požarnega zidu, če nič od zgornjega ni najdeno in so dovoljeni le v primeru, če obstaja specifično pravilo, ki ta promet dovoljuje. V našem primeru tabela stanj omogoča največ 1.224.000 vpisov. Tabele stanj so dinamične, se samodejno spreminjajo in sproti odstranjujejo vse neaktivne povezave, če nekaj časa ni prometa, ki jih je ustvaril. S tem pa se preprečuje, da bi se prekomerno napolnile (postale prevelike), kar bi upočasnilo delovanje požarnega zidu.

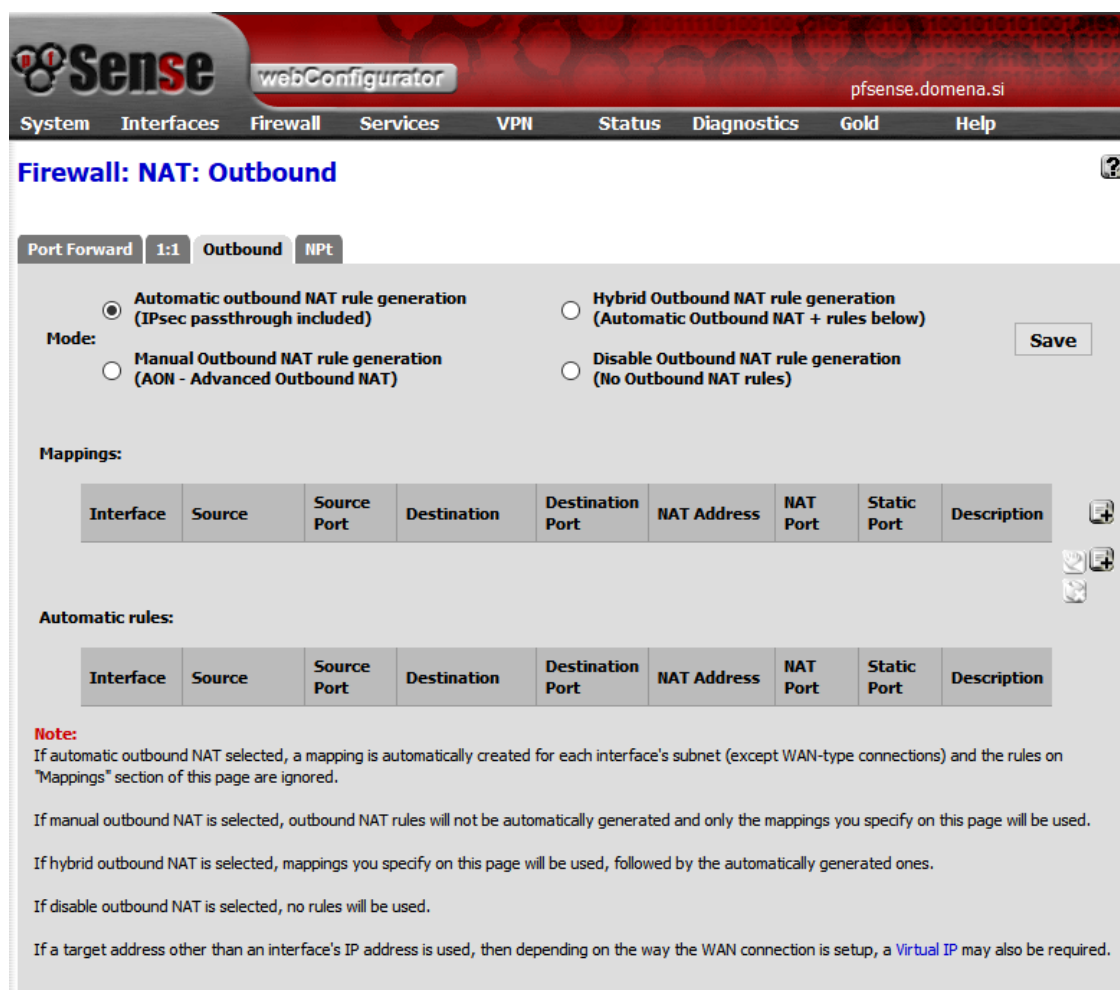
Pravila požarnega zidu *pfSense* so privzeto nastavljena tako, da dovoljujejo ves promet iz notranjega LAN-omrežja, ne pa tudi v omrežje. V omrežje se dovoljuje le tisti promet, ki ga administrator dovoli z definiranimi pravili in so procesirana od zgoraj navzdol [13]. Vnos pravil požarnega zidu je možen ločeno na obeh »segmentih« oziroma vmesnikih (ang. *interfaces*), torej za zunanje WAN- in notranje LAN-omrežje. Omogoča pa tudi t. i. plavajoča pravila (ang. *floating rules*), s pomočjo katerih se ustvarjajo naprednejša pravila, ki se lahko uveljavljajo na več »segmentih« hkrati. Za potrebe tega omrežja plavajočih pravil tokrat ne bo treba konfigurirati.

Omenjena programska oprema vsebuje številne vgrajene funkcionalnosti poleg ostalih, ki se lahko naknadno namestijo kot dodatni programski paketi. S pomočjo vseh razpoložljivih funkcionalnosti, ki jih lahko nudi *pfSense*, se lahko le-ta kosa tudi z dragimi komercialnimi požarnimi zidovi [14]. Omogoča tudi filtriranje in oblikovanje prometa sedmega, t. i. aplikacijskega sloja, kar omogoča način podrobnega pregledovanja paketov (ang. *DPI – Deep Packet Inspection*). Spodnja tabela (Tabela 1) prikazuje seznam [15] nekaj že vgrajenih funkcionalnosti in med drugimi tudi vse pglavitne funkcionalnosti, ki so pomembne za izvedbo naše rešitve.

Osnovne (vgrajene) funkcionalnosti / značilnosti	
Firewall (Stateful)	požarna pregrada z upoštevanjem vseh stanj
Web Based Graphical Interface	spletni grafični vmesnik
State Table	tabela stanj
NAT (Port Forwards, 1:1 NAT, Outbound NAT)	podpora več tipov prevajanja omrežnih naslovov
Redundancy / High Availability	redundanca / visoka razpoložljivost
Multi-WAN	zmožnost uporabe več WAN-omrežij
Server Load Balancing	strežniška delitev obremenitev
VPN (IPSec, OpenVPN, L2TP)	podpora več tipov navideznih zasebnih omrežij
PPPoE Server	podpora vzpostavitve PPPoE povezav
Reporting and Monitoring	poročanje in spremljanje
Dynamic DNS	dinamični DNS
DNS Forwarder / Resolver	DNS posrednik / razreševalnik
Captive Portal	prestrezni portal
DHCP Server and DHCP Relay (IPv4 and IPv6)	strežnik za dinamično konfiguriranje gostiteljev
IPv4 and IPv6 support	podpora za IPv4 in IPv6
Wireless Access Point	brežžična dostopna točka
Wireless Client Support	podpora za brezžične odjemalce
Inbound Load Balancing	vhodna delitev obremenitev
Utilities(ping, traceroute, port tests)	več pripomočkov (orodij)
RRD Graphs (Historical information)	grafi in historične informacije
Real-time interface traffic graphs	grafi prometa v realnem času
Command line shell access (via console or SSH)	dostop do ukazne vrstice preko konzole ali SSH
Wake on LAN	zbuditev LAN
Packet capture / sniffer	zajemanje paketov / vohljač
Backup and restore firewall configuration	arhiv in obnova konfiguracij požarnega zidu
Edit files via the web GUI	urejanje datotek preko WebGUI
Can be run in many virtualization environments	Lahko ga uporabljamo v virtualnih okoljih
Proxy Server (using packages)	proksi (posredniški) strežnik – z uporabo dodatkov
...	...

Tabela 1: Seznam že vgrajenih pglavitnih funkcionalnosti / značilnosti *pfSense* [15]

Funkcije, ki jih implementirani robni strežnik trenutno opravlja, so bile izbrane glede na potrebe tega omrežja. Poleg požarnega zidu, katerega delovanje sem že opisal zgoraj, je bilo treba na robnem strežniku vzpostaviti tudi mehanizem prevajanja omrežnih naslovov NAT, ki predstavlja pomemben del požarne zaščite. Le-ta omogoča usmerjevalniku (robnemu strežniku), da deluje kot posrednik med notranjim omrežjem LAN in zunanjim omrežjem internet. Za dostop do interneta se tako potrebuje le en zunanji IP-naslov, za katerim so »skrite« vse notranje naprave oziroma celotno notranje omrežje, s tem pa se poveča tudi varnost tega omrežja. Ta možnost oziroma omejitev uporabe zunanjih IP-naslovov pa je seveda bistvena za delovanje tako velikega omrežja, saj je število prostih enoličnih zunanjih IP-naslovov premajhno in zelo omejeno. V izbrani programski opremi se ta tip prevajanja omrežnih naslovov imenuje izhodni NAT (ang. *outbound NAT*), ki pa je lahko izveden na več načinov kot samodejni, hibridni in ročni NAT, kot je razvidno na naslednji sliki (Slika 5).



Slika 5: pfSense – načini izhodnega NAT (Vir: Posnetek zaslona – pfSense 2.2.4 na VirtualBox (Firewall | NAT | Outbound))

V spodnjem delu slike so pod opombo na kratko definirani omenjeni načini izhodnega tipa NAT. Samodejni izhodni NAT (ang. *automatic outbound NAT*), kot pove že ime samo, samodejno ustvari preslikave (ang. *mappings*) naslovov za vsako podomrežje in ignorira spodnje vpisane preslikave. Hibridni izhodni NAT (ang. *hybrid outbound NAT*) ustvari preslikave samodejno, ob tem pa tudi upošteva spodaj vpisane preslikave. Ročni izhodni NAT (ang. *manual outbound NAT*) pa uporablja izključno le ročno vpisane (specificirane) preslikave. Za dano omrežje morata delovati dva tipa prevajanja naslovov, in sicer omenjeni izhodni NAT ter tudi 1 : 1 NAT. Le-ta pa omogoča, da lahko določene (izbrane) naprave znotraj omrežja, dostopajo izven omrežja preko svojih lastnih enoličnih javnih IP-naslovov. Tudi pri temu tipu pretvorbe naslovov robni strežnik (usmerjevalnik, požarni zid) deluje kot posrednik, ki omejuje dostope (protokolov in vrat) in nadzira povezave v obe smeri. Da je delovanje tipa 1 : 1 NAT sploh izvedljivo, je treba predhodno ustrezno definirati t. i. navidezni IP-naslov (ang. *virtual IP*) in pri tem izbrati ustrezen tip, v primeru tega omrežja IP-vzdevek (ang. *IP alias*). Ta navidezni IP-naslov (vzdevek) mora biti enak zunanjemu IP-naslovu naprave, ki zahteva takšno konfiguracijo oziroma svoj enolični zunanji naslov. Tudi za delovanje ročnega izhodnega NAT je treba prej definirati zunanji IP-naslov (z navideznim), s katerim se bodo notranje naprave predstavljale izven omrežja (v internetu).

Robnemu strežniku je bilo treba dodati tudi novo vlogo, in sicer funkcionalnost dinamičnega dodeljevanja IP-naslovov DHCP, ki jo je doslej opravljal starejši strežnik. Ta odločitev je smotrna, saj strežnika ta vloga praktično dodatno ne obremenjuje. Kar DHCP-strežnik nudi, je to, da napravam, ki nimajo vnesenih statičnih omrežnih nastavitev in ki le-te zahtevajo, dodeli prost IP-naslov ter jim posreduje preostale informacije omrežnih nastavitev. IP-naslov, dodeljen tem napravam, oziroma naslov, ki ga naprave najamejo (ang. *lease*), imajo čas trajanja in se po določenem času neaktivnosti odstranijo s seznama najemov. Ta način delovanja je smiseln, saj se takrat, ko naprava dlje časa ni priključena v omrežju, njen dodeljen IP-naslov sprosti in je na voljo preostalim (npr. novo priključenim napravam). Naprava, ki je bila nekaj časa neaktivna, po ponovni priključitvi v omrežje zaprosi oziroma skuša podaljšati pred tem dodeljen IP-naslov. Tega DHCP-strežnik preveri v svojem naboru IP-naslovov (ang. *address pool*) in (če je prost), ji ga ponovno dodeli (podaljša najem tega naslova). Pri notranjem omrežju 172.16.0.0 s 16-bitno masko, je razpoložljivi razpon IP-naslovov (ang. *available range*), ki jih DHCP-strežnik lahko dodeljuje, med 172.16.0.1 ter 172.16.255.254, kar omogoča dodelitev vsega skupaj 65534 naslovov. V *pfSense*

konfiguraciji DHCP-strežnika je mogoče definirati en osnovni razpon (ang. *range*) kot tudi dodatne razpone naslovov (ang. *additional pools*). Ker je uporaba vseh razpoložljivih naslovov za to omrežje nesmiselna, se lahko z omejitvijo osnovnega razpona ta nabor naslovov ustrezno zmanjša. Omrežje potrebuje vsega skupaj okoli cca. 700 razpoložljivih notranjih naslovov. Zato je smiselno osnovni razpon omejiti z vnosom razpona (172.16.1.0–172.16.3.254), ki omogoča dodeljevanje 762 različnih IP-naslovov, ter po potrebi definirati še dodatne razpone. Z nastavitvijo tudi dodatnih razponov naslovov pa je mogoče definirati bolj specifične »omejene« razpone naslovov izven razpona definiranega v osnovnem. Tem je mogoče (če se to želi) med drugim dodeliti drugačne čase najemov oziroma rezervacij IP-naslovov, kot so definirani v osnovnem razponu. Naslednja slika (Slika 6) prikazuje privzete nastavitve *pfSense* DHCP-strežnika za notranje omrežje 172.16.0.0 s 16-bitno omrežno masko, razpoložljivi razpon IP-naslovov ter privzete in maksimalne čase najemov.

Services: DHCP server

WAN LAN

☒ **Enable DHCP server on LAN interface**

☐ **Deny unknown clients**
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet 172.16.0.0
Subnet mask 255.255.0.0
Available range 172.16.0.1 - 172.16.255.254
Range [] to []

Additional Pools If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description

WINS servers []

DNS servers []
 []
 []
 []

NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.

Gateway []
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network. Type "none" for no gateway assignment.

Domain name []
The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.

Domain search list []
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator

Default lease time [] seconds
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum lease time [] seconds
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Slika 6: *pfSense* – privzete nastavitve DHCP-strežnika za omrežje 172.16.0.0 (Vir: Posnetek zaslona – *pfSense* 2.2.4 na VirtualBox (Services | DHCP server))

Za rešitev razreševanja (pretvorbe) tako zunanjih kot notranjih (domenskih) imen je treba na robnem strežniku uporabiti funkcionalnost, ki bi temu omrežju najboljše ustrezala. Kot ta je bila uporabljena vloga posrednika domenskih imen (ang. *DNS Forwarder*), ki omogoča preprosto posredovanje zahtev notranjih klientov za pretvorbe imen. V primeru tega omrežja jih mora posredovati internemu DNS-strežniku, za ustrezno pretvorbo tako zunanjih kot tudi notranjih imen med klienti in strežniki. Ta je v tem omrežju nujen in tudi tesno povezan s strežnikom, ki v omrežju deluje kot glavni domenski krmilnik (ang. *PDC – Primary Domain Controller*). Vloga internega DNS-strežnika je bila že od nekdaj dodeljena prejšnjemu robnemu strežniku in je ta predstavljal primarni DNS-strežnik vsem napravam v omrežju (statičnim in dinamičnim). Na podlagi testiranja prejšnjega robnega strežnika sem ugotovil, da se stanje obremenjenosti bistveno izboljša, če se na njem zaustavijo vloge požarnega zidu, prevajanja omrežnih naslovov in usmerjanja prometa. Tako je povprečna obremenitev procesorja padla za več kot 80 odstotkov oziroma se je gibala med 0–15 odstotki. Od tukaj pa sem dobil idejo, da bi začasno (do nakupa novega strežnika za to vlogo) v omrežju tega obdržali in bi služil le kot interni DNS-strežnik, kar se je izkazala kot hitra in ustrezna rešitev.

Z uporabo te funkcionalnosti sem privarčeval tudi čas, ki bi bil potreben za spremembo omrežnih konfiguracij, če te ne bi uporabil. Spremeniti bi tako moral konfiguracijo (vpisati novi IP-naslov DNS-strežnika) vsem napravam s statičnimi notranjimi omrežnimi nastavitvami, ki pa jih ni malo. Spremenitev teh nastavitvev bi bila potrebna, ker je prejšnji robni strežnik (z IP-naslovom 172.16.0.1) predstavljal tako glavni prehod kot tudi primarni DNS-strežnik. Sedaj pa zgolj kot interni DNS-strežnik uporablja IP-naslov 172.16.0.2, zdajšnjemu robnemu strežniku (kot glavnemu prehodu) pa je bil seveda dodeljen njegov prejšnji naslov 172.16.0.1. Tako lahko naprave naprej nemoteno in nespremenjeno delujejo in uporabljajo omrežne nastavitve enako kot pred posegom v omrežje. Interni DNS-strežnik tako še vedno prejme in odgovori na zahtevo pretvorbe imena, ki jo je zahteval notranji klient preko posrednika (robni strežnik).

4.2.1 Nabor orodij in dodatnih funkcionalnosti

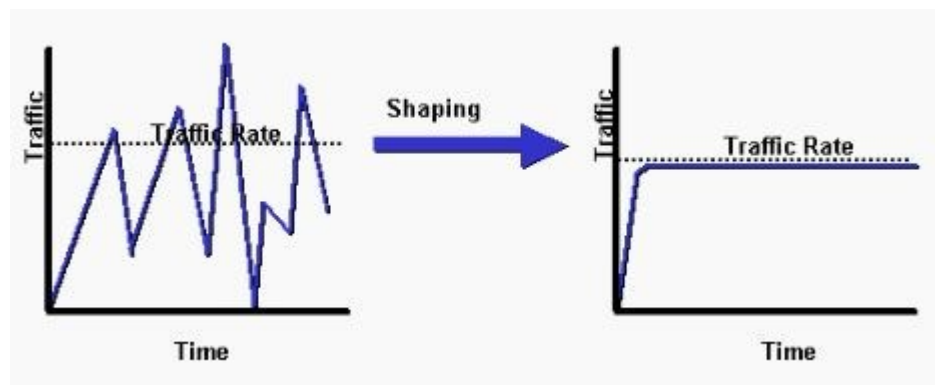
Ker je preostalih dodatnih orodij oziroma programskih paketov ogromno (okoli 73) [15], bi izpostavil le pomembnejše, in sicer tiste, ki bi jih bilo še smotrno uporabiti in namestiti (implementirati) v prihodnosti. Tukaj jih bom le naštel, kratko opisal [15] in definiriral namen njihove uporabe, v zaključku tega diplomskega dela pa predvidel njihovo dejansko uporabo.

- *Snort* – S programskim paketom *snort* je mogoče vzpostaviti sistema za zaznavanje IDS (ang. *IDS – Intrusion Detection System*) in preprečevanje vdorov IPS (ang. *IPS – Intrusion Prevention System*). Oba analizirata celotno vsebino paketov – tako glavo paketov kot tudi vsebino – in iščeta kakršnokoli nenavadno aktivnost ali nepravilnost. Sistem preprečevanja IPS za razliko od sistema zaznavanja IDS vdorov pri takšnih zaznambah paket zavrne, IDS ga pa zgolj zazna in zapiše v dnevnik.
- *HAVP* – Paket *HAVP antivirus* omogoča protivirusno zaščito pri spletnem brskanju in deluje kot HTTP protivirusni proksi (posrednik). Ker je s tem spletna protivirusna zaščita vgrajena na samem vhodu v omrežje oziroma na glavnem prehodu, skozi katerega gre ves promet, ta dodatno ščiti vse notranje kliente in naprave pred virusi.
- *Squid* – Paket *squid* omogoča, da robni strežnik postane tudi spletni posrednik s predpomnilnikom (ang. *web proxy cache*). Ob tem se lahko dodatno namesti še *squidGuard*, ki omogoča tudi URL-filtriranje (ang. *URL filtering*) spletnega posrednika. Tako se prvič obiskane spletne strani in različne prenesene vsebine shranjujejo na lokalni trdi disk posrednika. Kasneje pa so na voljo tudi ostalim in tudi bistveno hitreje, saj so lahko dostopne lokalno in jih ni treba ponovno v celoti prenašati preko interneta. S tem se lahko razbremenijo uporabo internetne povezave in posledično dodatno optimizira delovanje celotnega omrežja.

pfSense vsebuje tudi veliko že vgrajenih (dodatnih) funkcionalnosti, ki pa v privzetih nastavitvah ne delujejo, zato se mora administrator sistema odločiti, ali jih bo konfiguriral ali ne. Zopet bi izpostavil in le tiste, ki bi jih bilo v prihodnosti smiselno vključiti:

- Funkcionalnost oblikovanja prometa (ang. *Traffic shaping*), drugače imenovano tudi kot oblikovanje paketov [16], predstavlja kontrolo nad podatkovnim prometom računalniškega omrežja. Takšno upravljanje omrežnega prometa deluje na način

povečanja ali zmanjšanja razpoložljive pasovne širine določenim vrstam paketov glede na pravila oziroma profil prometa, v katerega spadajo. Želene profile prometa mora administrator znotraj nastavitev te funkcionalnosti primerno definirati glede na to, kakšne vrste prometa (paketov) so za dano omrežje bolj prioritete kot ostale. S pomočjo oblikovanja prometa in t. i. čakalnimi vrstami (ang. *queue*) paketov se lahko delovanje omrežja še dodatno optimizira (Slika 7) kot tudi izboljša zakasnitve v omrežju.



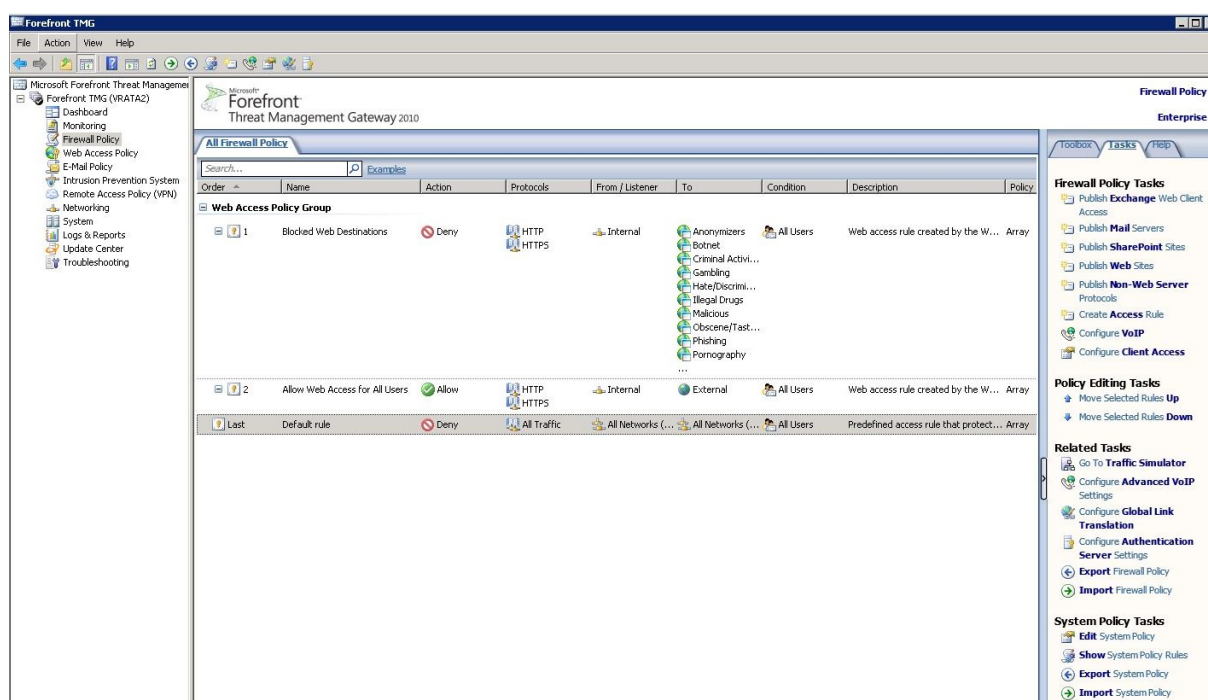
Slika 7: Rezultat oblikovanja prometa pri omejevanju pasovne širine [17]

- Vzpostavitev navideznega zasebnega omrežja VPN. VPN predstavlja storitev, ki omogoča varno in zanesljivo povezavo preko »javnega« omrežja, kot je internet [18]. Pri tem se ustvarijo in uporabljajo »virtualne« povezave, ki so skozi internet usmerjane od zasebnega (notranjega) omrežja podjetja do oddaljenih lokacij ali dislociranih uporabnikov [19]. VPN-omrežja so potrebna oziroma zaželena predvsem v podjetjih, ki imajo omenjene oddaljene pisarne in zaposlene. Tako lahko od drugod do korporativnega omrežja dostopajo varno (preko šifrirane povezave) in se povezujejo z načinom oddaljenega dostopa VPN. Za povezovanje oddaljenih lokacij med seboj pa je tukaj drugi način VPN-povezovanja, imenovan lokacija z lokacijo (ang. *site-to-site*) [19], kjer obe lokaciji potrebujeta za takšno delovanje le lokalno povezavo do istega javnega omrežja. Programska oprema *pfSense* omogoča vzpostavitev VPN preko naslednjih protokolov, ki omogočajo šifriranje te povezave IPsec, OpenVPN, L2TP in PPTP. Pred odločitvijo za uporabo in vzpostavitev ustrezne tehnologije VPN bo treba v prihodnje (do naslednjega večjega projekta) natančno preučiti, kakšna konfiguracija bi za dano omrežje najbolj ustrezala.

4.3 Druge predvidene možnosti

Za rešitev v uvodu omenjenih problematik sem opisal več ostalih možnih predvidenih rešitev. Na podlagi njihovega delovanja, slabosti in prednosti sem se na koncu odločil za najboljšo oziroma najustreznejšo, ki sem jo ravnokar predstavil. Preverjal sem delovanja in funkcionalnosti izbranih vzporedno (ločeno) z obstoječim omrežjem, tako da je bilo delovanje omrežja podjetja nemoteno. Moj namen je bil vzpostaviti podobno stanje z robnim strežnikom, ki bi zadoščal vsem kriterijem obstoječega omrežja. Torej ustrezno konfigurirati požarni zid, vzpostaviti NAT in dodelovanje IP-naslovov.

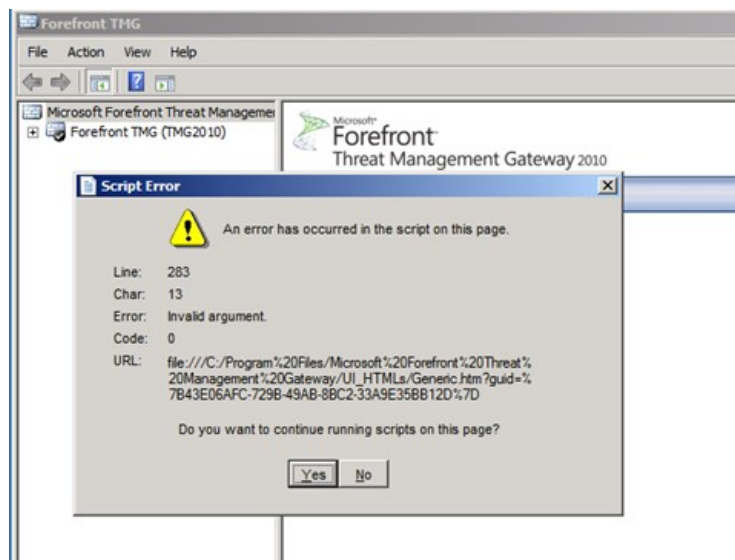
Kot prvo sem preizkušal znano Microsoftovo programsko rešitev napredne požarne pregrade *Forefront Threat Management Gateway 2010* ali krajše TMG 2010 na strežniku z operacijskim sistemom Microsoft Server 2008 R2. Spodnja slika (Slika 8) prikazuje uporabniški vmesnik TMG 2010 po uspešni namestitvi s privzetimi nastavitvami požarnega zidu in vključeno funkcionalnostjo filtriranja URL-naslovov (ang. *Uniform Resource Locator*).



Slika 8: Uporabniški vmesnik TMG (Vir: Posnetek zasлона – uporabniški vmesnik TMG 2010 s privzetimi nastavitvami – Microsoft Server 2008 R2)

Deluje lahko kot usmerjevalnik, požarni zid in vključuje tudi prevajanje naslovov NAT, kar so bistvene lastnosti, ki jih obstoječe omrežje potrebuje za ustrezno delovanje. TMG 2010 predstavlja večplastno požarno zaščito za podjetja s številnimi funkcionalnostmi [20]. Predstavlja tudi omrežni protivirusni program, ki deluje na podlagi pregledovanja in preprečevanja škodljive programske opreme (ang. *malware inspection*), pregledovanja HTTPS prometa in filtriranja URL naslovov [20]. Lahko je tudi konfiguriran kot VPN strežnik, spletni proksi (ang. *proxy*) in spletni strežnik s predpomnjenjem (ang. *web caching server*). Omogoča tudi sistema za zaznavanje IDS in preprečevanje vdorov IPS. TMG, pred tem znan tudi kot ISA Server, predstavlja za omrežje napredno zaščito za celoten vstopni in izstopni promet.

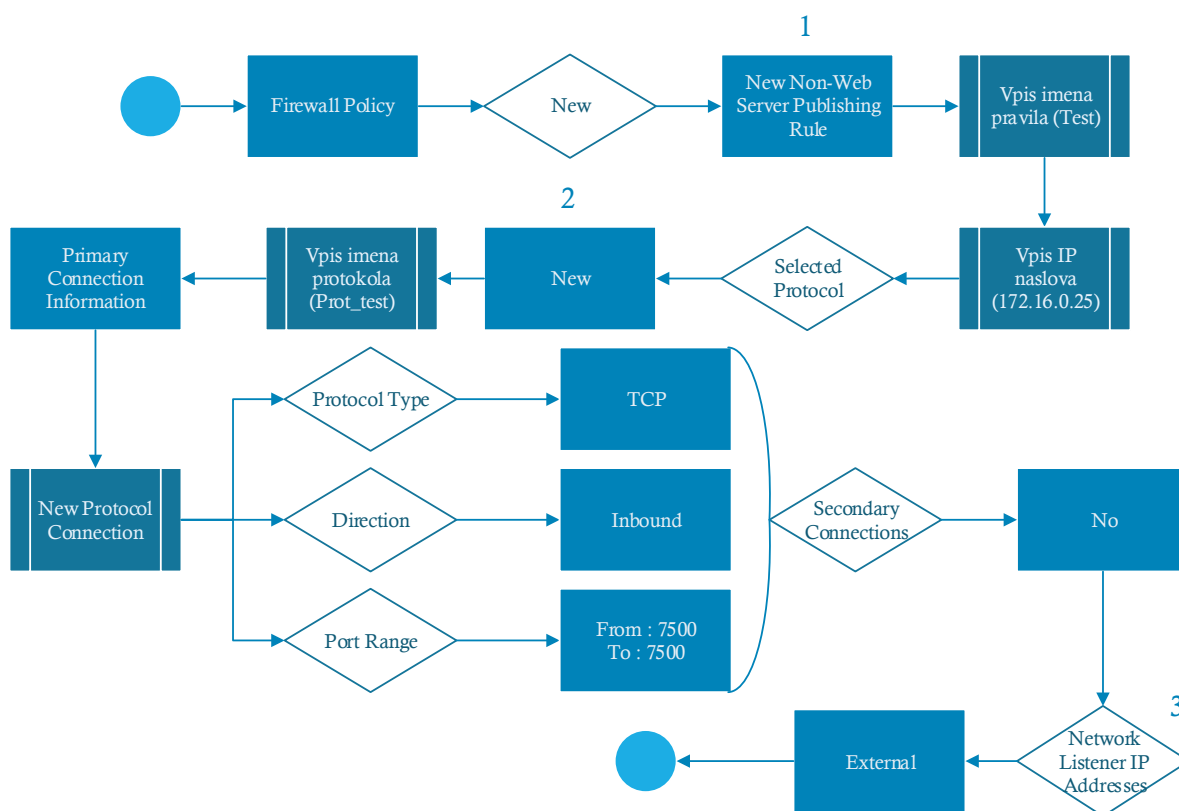
Ker sem to izbiro testiral skoraj dva tedna, sem kljub zgoraj omenjenim dobrim lastnostim naletel na več slabosti. Kot prvo slabost TMG izpostavljam dejstvo, da bodo varnostne posodobitve in podaljšana podpora le do leta 2020 [21], kar je dokaj kratko obdobje za takšno rešitev, ki bi morala biti dolgoročna. Nato sem že v samem pričetku naletel na prvo težavo, in sicer na nedelovanje upravljalne konzole (ang. *management console*) z napako skripta programa (ang. *script error*) kot prikazuje spodnja slika (Slika 9).



Slika 9: TMG 2010 napaka skripta programa pri zagonu [22]

S pomočjo spletnega foruma TMG [23] sem ugotovil, da sta si upravljalna konzola TMG in privzeto nameščen spletni brskalnik Internet Explorer 9 v nekaterih sistemih konfliktna. Rešitvi za odpravo te napake, ki so jih podali ostali uporabniki TMG, sta bili dve, in sicer:

ali popolnoma odstraniti privzeti Microsoftov spletni brskalnik ali pa ročno spremeniti vsebino konfiguracije v datoteki *TabsHandler.htc* programa TMG 2010 z odstranitvijo nekaj vrstic kode. Glede na to, da je preteklo že slabih šest let od prijave te napake na forum podjetja, ki naj bi te odpravljali s samodejnimi popravki, ta napaka še vedno obstaja. Tudi uporabniški vmesnik je bil slabo optimiziran in precej neodziven saj je vsaka sprememba konfiguracije trajala skoraj minuto, da je obveljala. Že pri ustvarjanju najpreprostejših pravil požarnega zidu (npr. odpreti določena vrata od koder koli do specifične notranje naprave) naletimo na dolg in kompleksen postopek. Kot primer lahko pogledamo spodnji diagram (Slika 10), ki prikazuje zamuden postopek ustvarjanja pravila požarnega zidu, ki dovoljuje katerikoli zunanji promet TCP preko številke vrat 7500 do specifične notranje naprave za požarnim zidom TMG 2010. Pri ostalih rešitvah, ki sem jih preizkusil (*OPNSense*, *pfSense*), je takšno pravilo mogoče preprosto in elegantno ustvariti znotraj enega samega okna, pri TMG 2010 pa je za ta primer okoli deset novih pojavnih oken.



Slika 10: Diagram poteka ustvarjanja »netipičnega« pravila v požarnem zidu TMG 2010 (Vir: TMG 2010 – ustvarjanje pravila za nespletni strežniški protokol)

Kot prikazuje zgornji diagram poteka ustvarjanja tega pravila, je bilo najprej (»1«) treba ustvariti novo pravilo za nespletni strežniški protokol, mu nadeti ime ter vpisati notranji IP-naslov, na katerega bo dovoljen takšen promet. Nato (»2«) je bilo treba ustvariti nov protokol, ga poimenovati in mu definirati parametre povezave (tip, smer ter razpon vrat) ter na koncu obkljukati, da dovoljuje promet od koderkoli.

Prav tako je bilo treba za vzpostavitev načina prevajanja omrežnih naslovov, ki preslika določen notranji IP-naslov na določenega zunanjega 1 : 1 NAT, vsak zunanji IP-naslov, ki bo uporabljan, prej ločeno dodati znotraj naprednih nastavitev zunanje omrežne kartice. To je bil edini način, da je bila uporaba več statičnih zunanjih naslovov mogoča. Kar se je izkazalo, da tudi, če bi bila naprava, ki ji je bil dodeljen eden izmed teh statičnih zunanjih IP-naslovov ugasnjena, bi bil ta IP-naslov še vedno aktiven. Pri preverjanju z orodjem *ping* oziroma pri pošiljanju nadzornih paketov ICMP (ang. *ICMP – Internet Control Message Protocol*) na katerikoli zunanji IP-naslov (ki je bil dodeljen drugemu strežniku), je nanje odgovarjal vedno robni strežnik (TMG 2010). Rezultat je bil enak tudi, če je bil ciljni strežnik s tem IP-naslovom ugasnjen. Zaradi preveč kompleksne programske opreme TMG 2010 in vseh omenjenih zapletov in težav sem to opustil in začel z iskanjem boljše rešitve.

Med drugim je bila poslana tudi poizvedba s podatkom o številu zaposlenih v podjetju na zastopništvo podjetja Sophos, ki se ukvarja z IT-varnostjo in varovanjem podatkov za podjetja [24]. V odgovoru smo prejeli možnost izbire zgolj programske opreme (*UTM SW 500 FullGuard*) in tudi (strojne) namenske naprave (ang. *appliance*) z vključeno programsko opremo (*UTM SG330 Total Protect*). Če bi se odločili za nakup in enoletno vezavo omenjene programske opreme, ki je namenjena do 500 uporabnikom, bi morali za to plačati več kot 8.000 evrov. Za namensko napravo skupaj s programsko opremo (enoletna vezava) pa bi moralo podjetje za to vsako leto odšteti preko 10.000 evrov. Obe izbiri sta zelo presegali za to namenjena denarna sredstva, zato je bilo treba najti primerno in cenejšo rešitev.

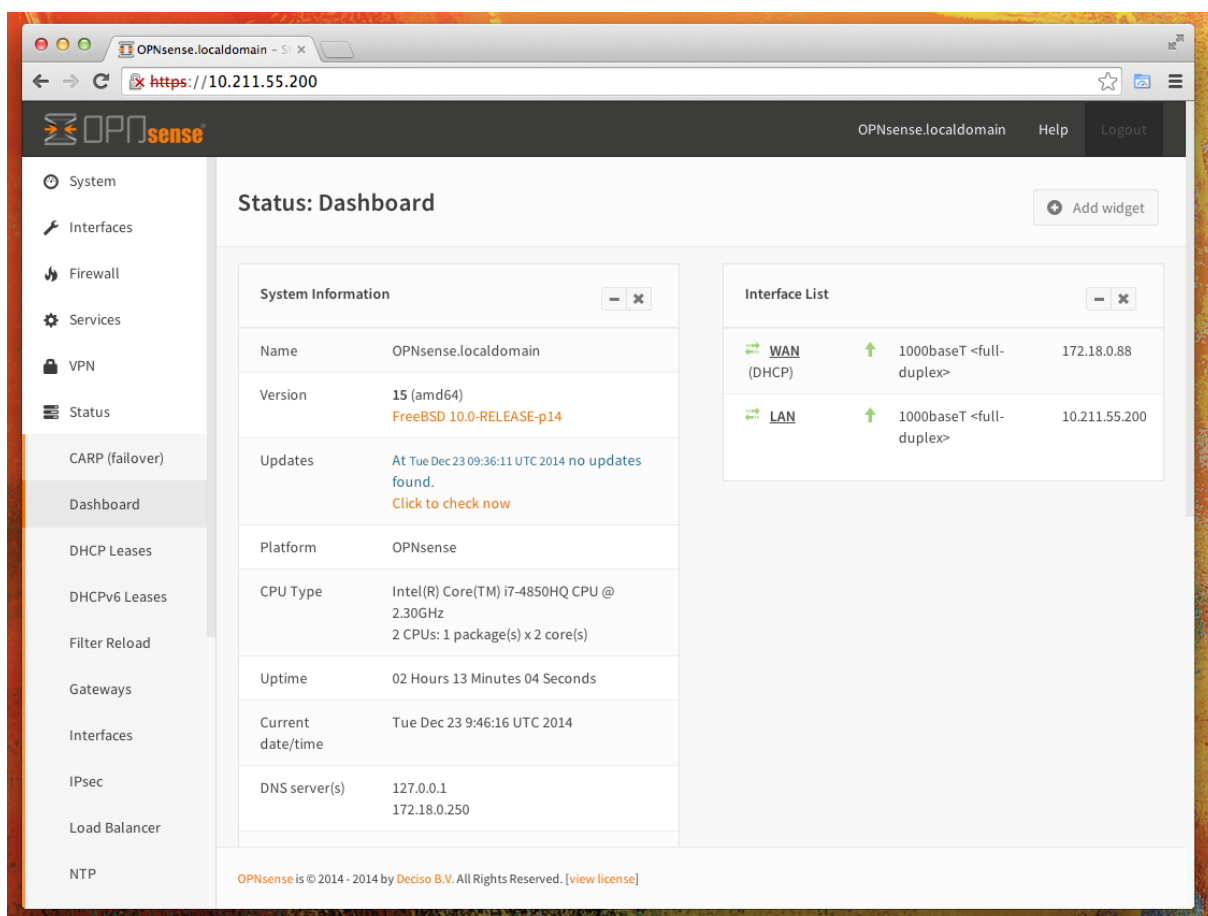
Ostale namenske naprave s požarnimi zidovi (ang. *hardware firewall appliances*) oziroma strojni požarni zidovi kot npr. ZyWall, SonicWall, Cyberoam itd. bi glede na njihovo funkcionalnost in dobro preverjena delovanja zadoščale potrebam tega omrežja. Vendar se zaradi števila uporabnikov oziroma števila omrežnih naprav, ki potrebujejo dodatno zaščito (strežniki, stacionarni in prenosni računalniki) cene tudi teh gibljejo nad 5.000 evrov.

Na podlagi pregledovanja, preverjanja in preizkusa različnih rešitev, ki bi bile za dano dokaj kompleksno omrežje ustrezne, upoštevajoč tudi stroškovne omejitve, sem prišel do spoznanja, da bi bilo smotrno razmišljati tudi v smeri odprtokodnih rešitev.

Kot pravi definicija odprte kode (po www.islovar.org), je to politika zasnove, razvoja in razširjanja programja, pri kateri je dostopna izvorna koda, ki se jo sme spreminjati in razširjati. Za odprtokodno programsko opremo (ang. *open source software*) velja, da je njihova izvorna koda prosto dostopna in jo lahko uporablja vsakdo. Uporablja se lahko v namene raziskovanja, spreminjanja in razširjanja delovanja. Vendar tudi za odprtokodne programe veljajo pravila, ki jih definirajo licence in jih je treba spoštovati [25]. Vse licence imajo osnovna skupna pravila, ki so definirana [25] tudi na COKS (center odprte kode Slovenije):

1. Odprtokodno programsko opremo je mogoče svobodno redistribuirati. Lahko jo redistribuirati kdorkoli brezplačno ali za plačilo.
2. Izvorna programska koda je dostopna uporabniku. Licenca mora dovoljevati distribucijo v prevedeni kakor tudi v izvorni obliki.
3. Licenca mora dovoljevati spremembe osnovne kode in izvedene oblike nove kode.
4. Kljub temu da mora biti izvorna koda dostopna, lahko izvorni avtorji zahtevajo, da se morebitne spremembe jasno ločijo od originalne kode in tako ohranijo ločnico med prvotno in modificirano kodo (npr. v obliki popravkov ali različnih verzij).
5. Licenca ne sme omejevati katerekoli osebe ali skupine.
6. Licenca ne sme biti omejevalna glede na področje dela, v okviru katerega se programska koda uporablja.
7. Distribucija licenc mora biti enakovredna za vse uporabnike, brez dodatnih omejitev.
8. Licenca za isto programsko kodo se ne sme razlikovati, če se jo uporablja v kombinaciji z drugo programsko opremo.
9. Licenca ne sme omejevati uporabe druge programske opreme.
10. Licenca mora biti tehnološko nevtralna.

Kot prvo odprtokodno programsko rešitev sem preizkusil programsko opremo *OPNsense*, ki je distribucija prav tako odprtokodnega operacijskega sistema *FreeBSD*. Pri testiranju se je leta izkazala za odlično rešitev, saj omogoča in vsebuje vse značilnosti, ki jih dano omrežje zahteva. Po temeljitnem raziskovanju spleta in spletnih forumov sem naletel na nekatere pomanjkljivosti v primerjavi s kasneje izbrano rešitvijo *pfSense*. Poleg tega, da je *OPNsense* nastal z vejitvijo kode (ang. *fork*) *pfSense-a* [26], je pri njem tudi precej slabša in okrnjena dokumentacija, slaba podpora uporabnikom ter zelo majhna skupnost uporabnikov. Vejitev kode se je zgodila zaradi prerekanj med razvijalci in predvsem zaradi nesporazuma glede drugačnega ter sodobnejšega videza grafičnega uporabniškega vmesnika (ang. *GUI – Graphical User Interface*). Slednje pa predstavlja edino »prednost« *OPNsensa*, in sicer novejši in navidezno lepši grafični uporabniški vmesnik (Slika 11) v drugem spletnem ogrodju (ang. *web framework*), ki pa seveda za dejansko učinkovitost in uporabnost sploh ni poglobljen. Zaradi omenjenih pomanjkljivosti sem tudi to opustil in kot končno rešitev predlagal in uporabil odprtokodno programsko opremo *pfSense*.



Slika 11: OPNsense uporabniški vmesnik – pregledna plošča (začetni zaslon GUI) [27]

5 Priprava in implementacija robnega strežnika

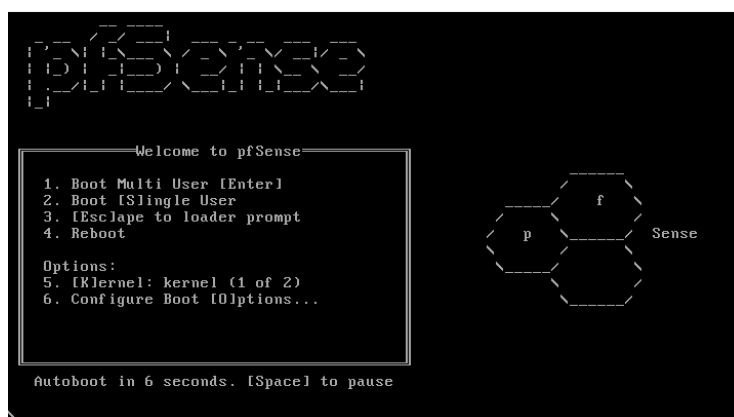
V tem poglavju bodo natančno podani vsi postopki namestitve in priprave robnega strežnika s priloženimi slikami, ki so bile narajene s fotoaparatom ter s posnetki zaslona (ang. *screenshot*). Postopke namestitve in konfiguracije robnega strežnika bom opisal po korakih, ki so bili potrebni za njegovo pripravo, zraven pa priložil tudi nekaj bistvenih slik za boljšo predstavo. Določene posnetke zaslona, ki jih med postopkom namestitve nisem uspel ustvariti ali pa so bile zajete slike neustrezne (slabše kvalitete), sem ustvaril ponovno s pomočjo programa *VirtualBox*. V programu sem za to namestil enako različico operacijskega sistema in programske opreme *pfSense* (2.2.4), kot je bila pri uporabljeni pri dejanski namestitvi. Slike, zajete iz virtualnega sistema, so bolj informativne narave, vse ostale in pomembnejše pa so bile zajete v dejanskem (realnem) sistemu oziroma na strežniku HP ProLiant DL360 G7. Na koncu poglavja pa bom podal tudi vse korake, ki so pripeljali do uspešne implementacije robnega strežnika v omrežje.

5.1 Namestitev in priprava

Namestitev operacijskega sistema in napredna konfiguracija programske opreme ni vplivala na delovanje obstoječega omrežja, saj sem to izvajal ločeno od omrežja. Kot prvo sem začel ustvarjanjem polja diskov, logičnih diskov ter izbral način redundantnega diskovnega polja s priloženim medijem *HP SmartStart*. Pripravil sem zagonski medij, ki sem ga ustvaril s pridobljeno inštalacijsko datoteko programske opreme *pfSense* in začel nameščati operacijski sistem na strežnik preko konzole s pomočjo optičnega pogona in priključenega monitorja ter tipkovnice. Po uspešni namestitvi operacijskega sistema in pravilni prepoznavi mrežnih kartic sem začel z njihovo dodelitvijo glede na uporabo in definiral omrežne nastavitve za zunanje WAN- ter notranje LAN-omrežje. Preko dodeljenega IP-naslova notranjega omrežja in grafičnega uporabniškega vmesnika sem s spletnim brskalnikom s pomočjo čarovnika opravil osnovne nastavitve robnega strežnika. V nadaljevanju sem z naprednejšimi konfiguracijami vzpostavil vlogo DHCP-strežnika in definiral razpone IP-naslovov in vse potrebne zunanje IP-naslove omrežja preko t. i. navideznih naslovov. Vzpostavil sem delovanje obeh tipov prevajanj omrežnih naslovov (izhodni, 1 : 1 NAT) in ustrezno definiral vse preslikave naslovov, ki jih zahtevajo notranje naprave in strežniki. Nato sem uporabil in ustvaril še t. i. vzdevke, s pomočjo katerih sem si v zadnjem koraku olajšal ustvarjanja pravil požarnega

zidu, ki so tako izhodna kot vhodna, in kot primere podrobnejših konfiguracij za boljšo predstavo natančneje podal le pravila in posnetke zaslona, ki zadevajo poštni strežnik tega omrežja.

1. S priloženim medijem *HP SmartStart* sem najprej ustvaril polje (ang. *array*) dveh fizičnih diskov (2×300 GB *SAS*), kar je v velikosti pomenilo 558,7 GB razpoložljivega prostega prostora. Nato sem iz obeh ustvaril logični disk (ang. *logical drive*) in izbral način redundantnega diskovnega polja *RAID 1*, ki omogoča t. i. zrcaljenje diska (ang. *mirroring disk*), tako da je enaka kopija vseh podatkov na obeh.
2. Preko spletne strani programske opreme *pfSense* sem pridobil inštalacijsko datoteko (*Live CD with Installer*) z izbrano 64-bitno arhitekturo operacijskega sistema za polno inštalacijo sistema na trdi disk (ang. *full installation*), ki omogoča namestitve tudi dodatnih paketov. Iz te datoteke (z datotečnim sistemom ISO 9660) sem pripravil zagonski medij (ang. *Live CD*) s pomočjo programa za peko CD, DVD medijev.
3. Pripravljen zagonski medij sem vstavil optično enoto strežnika, kateremu sem priključil tudi monitor in tipkovnico za lažjo inštalacijo in konfiguracijo. Ta način namestitve je izvedljiv z uporabo konzole in analognega standardnega prikaza slike VGA (ang. *VGA – Video Graphics Array*). Obstaja tudi t. i. serijski tip konzole za inštalacijo preko komunikacijskih vrat (ang. *com port*), če priklop in uporaba zgornjih perifერიj ni izvedljiva. Strežnik sem vklopil, za zagon izbral CD-enoto in prišel do začetnega zaslona namestitve (Slika 12) ter počakal, da se inštalacija sistema samodejno nadaljuje.



Slika 12: *pfSense* – začetni zaslon namestitve v konzoli (Vir: Posnetek zaslona – *pfSense* 2.2.4 na VirtualBox (konzola))

Po končanem samodejnem pregledovanju strojne opreme (komponent) strežnika sem s tipko »I« začel nameščati operacijski sistem, kjer sem izbral hiter in preprost (ang. *Quick/Easy*) način namestitve. Ko se je namestitev zaključila, sem odstranil medij iz optičnega pogona ter ponovno zagnal strežnik, tokrat iz trdega diska. Kot prikazuje slika (Slika 13), je operacijski sistem pravilno prepoznal štiri mrežne kartice, ki jih je označil z oznakami (*bce1*, *bce2*, *bce3* in *bce4*) in ponudil kot možnost tudi vzpostavitev in uporabo VLAN, česar pa nisem nastavljal. Poleg celotnega imena mrežnih kartic je prikazal tudi njihove naslove MAC.

```
(C) continues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 1

Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.

Valid interfaces are:

bce0  e8:39:35:a6:bf:44  (up) HP NC382i DP Multifunction Gigabit Server Adap
r (C0)
bce1  e8:39:35:a6:bf:46  (up) HP NC382i DP Multifunction Gigabit Server Adap
r (C0)
bce2  e8:39:35:a6:bf:30  (up) HP NC382i DP Multifunction Gigabit Server Adap
r (C0)
bce3  e8:39:35:a6:bf:32  (up) HP NC382i DP Multifunction Gigabit Server Adap
r (C0)

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? █
```

Slika 13: *pfSense* – prepoznane mrežne kartice, njihove oznake in strojni naslovi MAC (Vir: Zajem slike zaslona s fotoaparatom – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (konzola))

4. V naslednjem koraku je sledila dodelitev omrežij t. i. vmesnikov in posledično tudi mrežnih kartic glede na to, za kaj bodo uporabljene. Definirati je treba, katera mrežna kartica bo predstavljala zunanje WAN- in katera notranje LAN-omrežje. Možna sta dva načina dodelitve, in sicer ročni in samodejni (ang. *auto-detection*) način. Pri ročnem načinu administrator vnese (vtipka) ustrezno oznako mrežne kartice, glede na

to kaj predstavlja (zunanje ali notranje omrežje), v primeru tega strežnika eno izmed prej naštetih (*bce0*, *bce1*, *bce2* ali *bce3*). Za samodejni način prepoznave, ki se izbere z vnosom ukaza »a«, pa morajo biti vsi mrežni kabli UTP za razliko od ročnega načina predhodno izključeni. Mrežni kabel se priključi takrat, ko se pojavi obvestilo za priključitev kabla, ki bo predstavljal definirano omrežje. Sam sem postopek dodelitve izvedel s samodejnim načinom. Najprej sem definiral zunanje omrežje WAN in mrežno kartico, ki ga bo predstavljala. Mrežni kabel za zunanje omrežje sem za tako priključil v vrata »4« na strežniku, ki jih predstavlja mrežna kartica z oznako *bce3*. Za notranje omrežje LAN sem postopek ponovil in tako mrežna kartica z oznako *bce1* in vrati »2« na strežniku predstavlja le-to. Za vzpostavitev notranjega omrežja, dokončne namestitve in konfiguracije strežnika sem uporabil 8-vratno gigabitno omrežno stikalo. Ostalih dveh mrežnih kartic z oznakami *OPT1* in *OPT2* kot izbirnih (neobveznih) tokrat nisem dodeljeval ali uporabil. Nato je bilo treba definirati še ustrezne omrežne nastavitve zunanjega in notranjega omrežja.

Zaradi varovanja poslovnih skrivnosti tega podjetja bom moral zunanje IP-naslove tega omrežja in druge zaupne podatke prekriti. Zato jih bom v prihodnje in do konca tega diplomskega dela primerno označeval z oznakami (npr. {IP1}, {IP2}, {IP3} itd.). Sem sodita tudi imeni gostitelja (robnega strežnika) in domene podjetja, ki jih bom v besedilu in slikah označil kot {I} in {D.si}. Oznake le-teh pa se bodo ujemale tudi z oznakami vseh zajetih slik, tako da bodo stvari jasno razvidne in logične.

Za WAN-omrežje sem tako nastavil prost zunanji IP-naslov {IP1} in ustrezno omrežno masko 255.255.255.0 oziroma v bitnem zapisu /24. Kot naslednje je treba definirati prehod povratnega toka (ang. *upstream gateway*). Tega predstavlja IP-naslov {IP2} stikala ponudnika internetnih storitev, ki je povezan z njihovim hrbteničnim vozliščem. V času priprave in napredne konfiguracije robnega strežnika sem uporabljal kar Arnesov DNS-strežnik, in sicer 193.2.1.66, ki sem ga nato spremenil v naslov, s katerim se predstavlja zdajšnji interni DNS-strežnik podjetja (172.16.0.2). Po uspešni konfiguraciji WAN-omrežja preko internetnega protokola IPv4, *pfSense* omogoča oziroma ponuja tudi konfiguracijo preko IPv6, ki pa v tem omrežju še ni implementiran.

V konzoli je tako preostala le še konfiguracija notranjega omrežja LAN. Omrežne nastavitve za notranje omrežje sem nastavljal enake, kot so bile definirane na prejšnjem robnem strežniku. Torej vpisal IP-naslov 172.16.0.1, ki napravam znotraj omrežja predstavlja glavni prehod in primarni DNS-strežnik, ter za omrežno masko vpisal številko 16, ki predstavlja 16-bitno masko (/16) oziroma 255.255.0.0.

Spodnja slika (Slika 14) prikazuje uspešno konfigurirano zunanje WAN- in notranje LAN-omrežje z ustreznimi oznakami (*bce3* in *bce1*) dodeljenih mrežnih kartic, IP-naslovi ter omrežnimi maskami.

```
*** Welcome to pfSense 2.2.6-RELEASE-pfSense (amd64) on zid ***

WAN (wan)      -> bce3      -> v4: IP1 /24
LAN (lan)      -> bce1      -> v4: 172.16.0.1/16
OPT1 (opt1)    -> bce2      ->
OPT2 (opt2)    -> bce0      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Slika 14: *pfSense* – uspešno konfigurirano zunanje WAN- in notranje LAN-omrežje (Vir: Zajem slike zaslona s fotoaparatom – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (konzola))

- Preko dodeljenega notranjega IP-naslova (172.16.0.1) je s spletnim brskalnikom (Internet Explorer, Mozilla Firefox, Google Chrome itd.) sedaj mogoče dostopati do *WebGUI*, ki omogoča preglednejšo osnovno in napredno konfiguracijo programske opreme *pfSense*. Takoj po prijavi oziroma vnosu privzetega uporabniškega imena (ang. *username*) »admin« in gesla (ang. *password*) »pfsense«, se požene čarovnik (ang. *wizard*), ki vodi skozi začetno (osnovno) konfiguracijo *pfSense*. Uporaba čarovnika ni nujna in ga je mogoče zapreti s klikom na logotip *pfSense* v zgornjem

delu okna ter opraviti tudi začetno (osnovno) konfiguracijo ročno. Sam sem nekatere osnovne nastavitve opravil prek čarovnika, kar bom tudi opisal in podal nekaj bistvenih slik (posnetkov zaslona). V čarovniku je bilo treba najprej vnesti osnovne parametre robnega strežnika, kot so ime gostitelja, ime domene in primarni DNS-strežnik. Strežniku sem tako dodelil ime {I} in vpisal domeno podjetja {D.si} ter v času priprave in konfiguracije kot primarni DNS-strežnik uporabil Arnesov (193.2.1.66). Robni strežnik bo tako na podlagi te konfiguracije na voljo kasneje tudi preko svojega polnega domenskega imena {I}.{D.si}.

V naslednjem pojavnem oknu sem kot strežnik za sinhronizacijo časa vpisal (ntp1.arnes.si) ter izbral časovni pas (Europe/Ljubljana). Za tem se pojavi okno za konfiguracijo zunanjega WAN-omrežja; če to ni bilo urejeno že predhodno v konzoli, je to lahko izvedljivo tudi sedaj. Tukaj je mogoče nastaviti tudi drugačne načine WAN-konfiguracij oziroma različne načine priklopa v internet (DHCP, PPPoE, PPTP), kar pa je odvisno od ponudnika internetnih storitev. Med drugim je pod splošno konfiguracijo (ang. *general configuration*) mogoče vpisati tudi naslov mrežne kartice MAC, kar služi za t. i. prevaro oziroma podvajanje naslova MAC (ang. *MAC spoofing*). Nekateri ponudniki namreč zahtevajo, da se za omrežje WAN uporablja izključno ena določena mrežna kartica (s specifičnim naslovom MAC), slednje pa omogoča enostaven »trik«, kako to zaobiti.

V našem primeru okno konfiguracije WAN-omrežja (Slika 15) služi zgolj za pregled pravilne konfiguracije, ki sem jo definiral že v konzoli. Po preverbi pravilnih nastavitvev (izbran statični način WAN-omrežja, pravilen zunanji IP-naslov {IP1} robnega strežnika ter pravilen IP-naslov {IP2} prehoda povratnega toka) sem lahko nadaljeval naprej.

On this screen we will configure the Wide Area Network information.

Configure WAN Interface

SelectedType: Static ▾

General configuration

MAC Address: 
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU: 
Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS: 
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address:  **IP1** / 24 ▾

Upstream Gateway:  **IP2**

DHCP client configuration

DHCP Hostname: 
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

PPPoE Username: 

PPPoE Password: 

PPPoE Service name: 
Hint: this field can usually be left empty

Slika 15: *pfSense* – konfiguracija WAN-omrežja preko WebGUI (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (WebGUI čarovnik))

Kot zadnja osnovna konfiguracija preko vodiča oziroma čarovnika se pojavi okno, kjer se preveri tudi nastavitve notranjega omrežja LAN (Slika 16) in po potrebi tudi to spremeni. Poleg spremembe omrežne maske in statičnega notranjega IP-naslova je mogoče spremeniti tudi način dodelitve IP-naslova oziroma vklop DHCP-strežnika (z vpisom »dhcp« namesto IP-naslova), če je to potrebno. Ker so bile nastavitve tudi tukaj pravilne, sem lahko preprosto nadaljeval do naslednjega koraka.

On this screen we will configure the Local Area Network information.

Configure LAN Interface

LAN IP Address:	172.16.0.1 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask:	16

Slika 16: *pfSense* – konfiguracija LAN-omrežja preko WebGUI (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (WebGUI-čarovnik))

Naslednja slika (Slika 17) prikazuje pregledno ploščo *pfSense* in uspešno vzpostavljen robni strežnik z zgornjimi osnovnimi konfiguracijami, ki so bile definirane preko konzole in čarovnika.

System Information

Name	I.D.si
Version	2.2.4-RELEASE (amd64) built on Sat Jul 25 19:57:37 CDT 2015 FreeBSD 10.1-RELEASE-p15 You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz Current: 1500 MHz, Max: 2400 MHz 8 CPUs: 1 package(s) x 4 core(s) x 2 SMT threads
Uptime	00 Hour 16 Minutes 38 Seconds
Current date/time	Sat Sep 26 21:14:21 CEST 2015
DNS server(s)	193.2.1.66
Last config change	Sat Sep 26 21:11:10 CEST 2015
State table size	0% (226/1224000) Show states
MBUF Usage	25% (6596/26584)
Temperature	8.3°C
Load average	0.00, 0.02, 0.08
CPU usage	0%
Memory usage	2% of 12243 MB
SWAP usage	0% of 32767 MB
Disk usage	/ (ufs): 0% of 240G /var/run (ufs in RAM): 3% of 3.4M

Interfaces

WAN	100baseTX <full-duplex> ↑ IP1
LAN	1000baseT <full-duplex> ↑ 172.16.0.1

Slika 17: *pfSense* – pregledna plošča uspešno vzpostavljenega robnega strežnika z osnovnimi konfiguracijami (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | Dashboard))

6. Sledila je podrobnejša ročna (napredna) konfiguracija robnega strežnika. Začel sem z vzpostavitev vloge DHCP-strežnika za LAN-omrežje preko menija *Services* in iz spustnega seznama *DHCP Server* izbral *LAN*. Najprej sem moral omogočiti (obkljukati) DHCP-strežnik na LAN-omrežju (*Enable DHCP server on LAN interface*) in definirati osnovni razpon IP-naslovov, ki jih bo dodeljeval strežnik. Tako sem vpisal osnovni razpon (*Range*: 172.16.1.0–172.16.3.254), nastavitve shranil in nato definiral še dodatni razpon naslovov (*Additional Pools*: 172.16.204.0–172.16.206.254), ki sem ga poimenoval »Pool 2«. Dodatni razpon sem definiral predvsem zaradi zanesljivosti dovolj velikega števila razpoložljivih notranjih naslovov in daljšega časa najema. Poleg tega sem obema razponoma spremenil tudi privzet čas najema IP-naslovov na vrednost (*Default lease time*: 1296000 sekund), kar predstavlja 15 dni, ter maksimalni čas najema na vrednost (*Maximum lease time*: 2592000 sekund), kar predstavlja 30 dni. To so bile vse potrebne nastavitve za ustrezen začetek delovanja DHCP-strežnika, kot jih prikazuje tudi spodnja slika (Slika 18).

Services: DHCP server

WAN LAN

☒ **Enable DHCP server on LAN interface**

☐ **Deny unknown clients**
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet 172.16.0.0

Subnet mask 255.255.0.0

Available range 172.16.0.1 - 172.16.255.254

Range 172.16.1.0 to 172.16.3.254

Additional Pools
If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description
172.16.204.0	172.16.206.254	Pool #2

WINS servers

DNS servers

Note: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.

Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network. Type "none" for no gateway assignment.

Domain name l.d.si

The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.

Domain search list

The DHCP server can optionally provide a domain search list. Use the semicolon character as separator

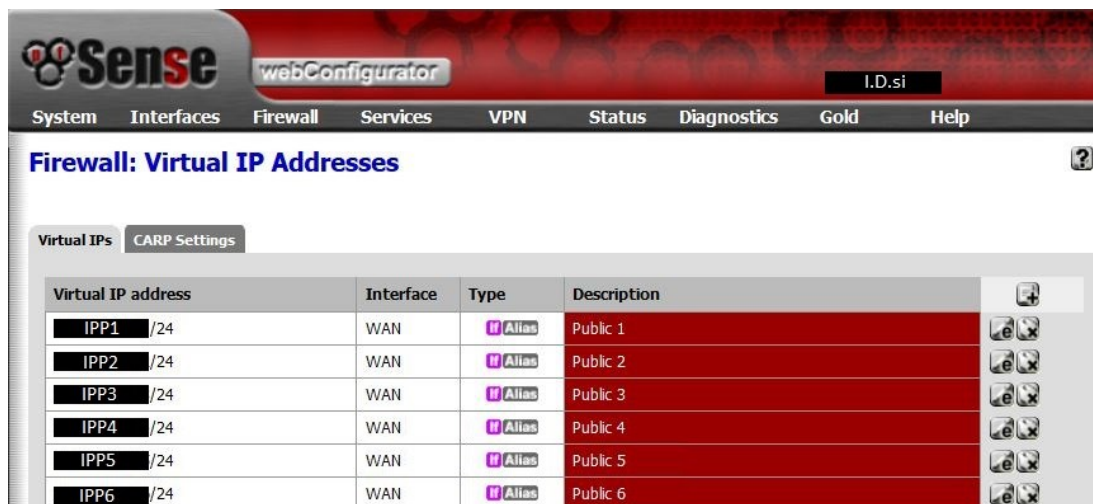
Default lease time 1296000 seconds
This is used for clients that do not ask for a specific expiration time.
The default is 7200 seconds.

Maximum lease time 2592000 seconds
This is the maximum lease time for clients that ask for a specific expiration time.
The default is 86400 seconds.

Slika 18: *pfSense* – vzpostavljen DHCP-strežnik in definirani razponi IP-naslovov (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Services | DHCP server))

7. V naslednjem koraku sem definiriral najprej zunanje IP-naslove (navidezne IP-naslove), ki jih bodo uporabljali klienti, glede na njihov dinamično dodeljen notranji IP-naslov oziroma glede na to, v kateri razpon naslovov spada njihov naslov. Lahko bi sicer za osnovni in dodatni razpon naslovov definirali le dva zunanja IP-naslova, vendar sem jih zaradi boljše preglednosti definirali šest. To pa zato, ker je na voljo še dosti prostih zunanjih IP-naslovov in predvsem zaradi lažjega lociranja potencialno problematične notranje naprave. V preteklosti se je namreč že zgodilo, da je ponudnik internetnih storitev poslal opozorilo (obvestilo), da so zaznali problem (npr. širjenje oglasnih sporočil) na IP-naslovu (npr. {IPP1}). Če bi zgolj eden IP-naslov {IPP1} predstavljal zunanji naslov vseh notranjih naprav, ki imajo dinamično dodeljen notranji IP-naslov, bi bilo iskanje »težavne naprave« veliko bolj oteženo. Za delovanje tega (uporabe različnih zunanjih IP-naslovov) in dostopa do interneta je treba kasneje še ustrezno urediti NAT-preslikave, kar bom opisal v nadaljevanju.

Tako sem preko menija *Firewall* in iz spustnega seznama *Virtual IPs* ter po kliku na gumb za kreiranje novega navideznega IP-naslova izbral tip (*IP Alias*), vpisal zunanji IP-naslov {IPP1}, izbral ustrezno 24-bitno masko (/24) in ga opisal (*Description: Public 1*). IP-naslov {IPP1} oziroma *Public 1* bo v nadaljevanju predstavljal zunanji IP-naslov vseh klientov, ki jim je bil dodeljen IP-naslov iz razpona naslovov (172.16.1.0–172.16.1.254). Kot sem že omenil, bo to delovalo šele po ustrezni konfiguraciji NAT-preslikav. Enako sem naredil tudi za ostale razpone naslovov (172.16.2.0–172.16.2.254, 172.16.3.0–172.16.3.254, 172.16.204.0–172.16.204.254, 172.16.205.0–172.16.205.254, 172.16.206.0–172.16.206.254), tako da sem definirali še preostalih pet zunanjih IP-naslovov {IPP2}, {IPP3}, {IPP4}, {IPP5} in {IPP6} ter jih primerno označil kot *Public 2*, *Public 3*, *Public 4*, *Public 5* in *Public 6*, kot je razvidno s spodnje slike (Slika 19).



Slika 19: pfSense – definiranih šest navideznih (zunanjih) IP-naslovov (Vir: Posnetek zaslona – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | Virtual IP Addresses))

Nato sem naredil enako (definiral zunanje IP-naslove) tudi za vse ostale naprave v omrežju, ki pa imajo statično definirane notranje IP-naslove in potrebujejo svoj enolični zunanji IP-naslov. Teh je v omrežju 68 in če bi želel prikazati posnetek zaslona, bi moral prekriati tako njihove zunanje IP-naslove kot tudi njihove opise, zato tukaj tega ni smiselno prikazovati.

8. V tem koraku je tako sledila konfiguracija NAT. Kot sem v tem delu že omenil, morata v omrežju delovati dva tipa (izhodni in 1 : 1 NAT). Najprej sem vzpostavil izhodni NAT preko menija *Firewall* kjer sem iz spustnega seznama *NAT* izbral tip *Outbound*. V razdelku izhodnega NAT sem nato izbral (napredni) ročni način izhodnega NAT (*Mode: Manual Outbound NAT rule generation*) ter spodaj posamično definiral ustrezne NAT-preslikave. Izbran ročni način in definirane preslikave omogočajo, da se lahko različnim razponom naslovov dodeli različne zunanje IP-naslove, ki pa sem jih že definiral zgoraj (7. korak). NAT-preslikave sem ustvaril s pomočjo gumba »Dodaj novo preslikavo« (ang. *Add new mapping*) in ustvaril posamezne preslikave. Tako sem definiral prvo NAT-preslikavo z nastavitvami: (Interface: WAN), (Protocol: any), (Source – Type : Network; Address: 172.16.1.0/24), (Destination: any), (Translation – Address: {IPP1} (Public 1)), (Description: LAN to WAN Public 1). To konfiguracijo prikazuje spodnja slika (Slika 20).

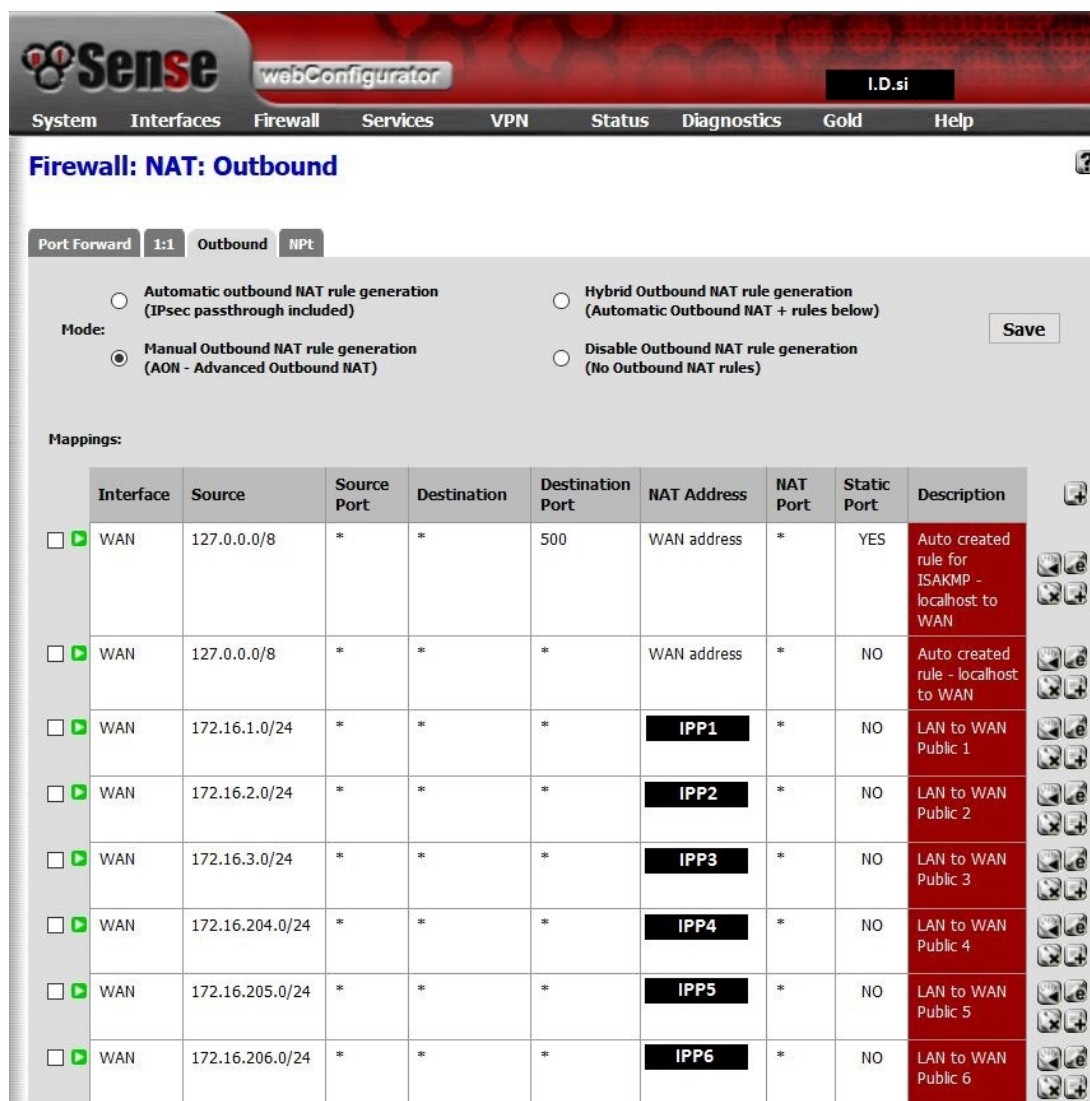
Firewall: NAT: Outbound: Edit



Edit Advanced Outbound NAT entry	
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
Do not NAT	☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. Hint: in most cases, you won't use this option.
Interface	WAN ▾ Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	any ▾ Choose which protocol this rule should match. Hint: in most cases, you should specify <i>any</i> here.
Source	Type: Network ▾ Address: 172.16.1.0 / 24 ▾ Enter the source network for the outbound NAT mapping. Source port: (leave blank for any)
Destination	☐ not Use this option to invert the sense of the match. Type: any ▾ Address: / 24 ▾ Enter the destination network for the outbound NAT mapping. Destination port: (leave blank for any)
Translation	Address: IPP1 (Public 1) ▾ Packets matching this rule will be mapped to the IP address given here. If you want this rule to apply to another IP address rather than the IP address of the interface chosen above, select it here (you will need to define Virtual IP addresses on the interface first). Port: Enter the source port for the outbound NAT mapping. Static-port: ☐
No XMLRPC Sync	☐ Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
Description	LAN to WAN Public 1 You may enter a description here for your reference (not parsed).

Slika 20: *pfSense* – konfiguracija NAT-preslikave za podomrežje 172.16.1.0/24 (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | NAT | Outbound | Edit))

Definirano podomrežje 172.16.1.0 s 24-bitno omrežno masko predstavlja razpon naslovov 172.16.1.0–172.16.1.254, ki mu bo dodeljen zunanji IP-naslov {IPP1}. Ker sem tega definiral že v 7. koraku, sem ga lahko enostavno izbral iz spustnega menija nastavitve prevajanja (ang. *translation*). Enako sem storil za preostala podomrežja oziroma preostale razpone naslovov, kar pregledno ponazarja naslednja slika (Slika 21).



Slika 21: pfSense – pregled nad vsemi definiranimi podomrežji in izhodnimi NAT-preslikavami (Vir: Posnetek zaslona – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | NAT | Outbound))

Z zgornjo specifično konfiguracijo NAT-preslikav sem povečal varnost celotnega omrežja kot tudi samega robnega strežnika. Uporabniki in naprave z dinamično dodeljenimi IP-naslovi bodo tako izven omrežja uporabljali drugačne, točno določene zunanje IP-naslove, ki pa so drugačni od IP-naslova robnega strežnika {IP1}. Vsem ostalim napravam v omrežju, ki imajo definirane statične omrežne nastavitve izven razpona naslovov, pa bo dostop do interneta onemogočen. Sem sodijo npr. omrežni tiskalniki, notranje NAS-naprave, določeni notranji strežniki in stikala, ki ne potrebujejo komunikacije izven omrežja in je tudi pravilno, da ta ni mogoča oz. dovoljena. Slednje se lahko sicer enostavno razreši (dovoli), tako da se ustvari še en

zunanji IP-naslov, ustrezno definira dodatno izhodno NAT-preslikavo za celotno omrežje 172.16.0.0/16 in nato to umesti na konec seznama NAT-preslikav.

V skupino naprav s statičnimi notranjimi nastavitvami spadajo tudi vsi »zunanji« strežniki oziroma ostale omrežne naprave, ki pa potrebujejo, kot sem že omenil svoje lastne (enolične) zunanje IP-naslove. Te naprave so že od nekdaj zaradi boljše preglednosti in ločevanja od ostalih konfigurirane tako, da imajo definirane statične IP-naslove med 172.16.0.1 in 172.16.0.254, kjer IP-naslov 172.16.0.1 predstavlja notranji IP-naslov robnega strežnika.

9. Zato je v tem koraku za ta namen (ostalih »zunanjih« naprav) treba vzpostaviti in konfigurirati še tip 1 : 1 NAT preko menija *Firewall* in iz spustnega seznama *NAT* izbrati tip 1 : 1. S pomočjo gumba »Dodaj novo preslikavo« sem tako definiral ustrezne preslikave za vseh 68 naprav in jim dodelil njihove unikatne specifične zunanje IP-naslove, ki sem jih z navideznimi IP-naslovi definiral že v 7. koraku. Kot primer (Slika 22) bi predstavil, kako sem konfiguriral 1 : 1 NAT za poštni strežnik (KURIR), ki ima notranji IP-naslov 172.16.0.35 in zunanji {IP35}.

Firewall: NAT: 1:1: Edit

Edit NAT 1:1 entry	
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
External subnet IP	IP35 Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address. Hint: this is generally an address owned by the router itself on the selected interface.
Internal IP	☐ not Use this option to invert the sense of the match. Type: Single host Address: 172.16.0.35 / 31
Destination	☐ not Use this option to invert the sense of the match. Type: any Address: / 31 The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually 'any'.
Description	KURIR You may enter a description here for your reference (not parsed).
NAT reflection	use system default
Save Cancel	

Slika 22: *pfSense* – konfiguracija 1 : 1 NAT za poštni strežnik (Vir: Posnetek zaslona – *pfSense 2.2.4* na strežniku HP ProLiant DL360 G7 (Firewall | NAT | 1 : 1 | Edit))

Torej vse, kar je potrebno za vzpostavitev 1 : 1 NAT, je izbrati omrežje WAN (*Interface: WAN*), v polje (*External subnet IP*) vnesti ustrezen zunanji IP-naslov (za primer poštnega strežnika {IP35}) ter v polju za notranji IP-naslov izbrati tip enega gostitelja (*Internal IP – Type: Single host*) in vnesti ustrezen notranji IP-naslov (za zgornji primer 172.16.0.35). Pri tem je smiselno pod opis (ang. *description*) za boljšo preglednost vnesti še ime naprave (npr. KURIR). Naslednja slika (Slika 23) predstavlja pregled nad konfiguriranimi 1 : 1 NAT-preslikavami nekaj prvo vnesenih naprav (11 od 68).

Firewall: NAT: 1:1

Port Forward 1:1 Outbound NPT					
	Interface	External IP	Internal IP	Destination IP	Description
☐	WAN	IP10	172.16.0.10	*	
☐	WAN	IP11	172.16.0.11	*	
☐	WAN	IP12	172.16.0.12	*	
☐	WAN	IP14	172.16.0.14	*	
☐	WAN	IP16	172.16.0.16	*	
☐	WAN	IP17	172.16.0.17	*	
☐	WAN	IP18	172.16.0.18	*	
☐	WAN	IP19	172.16.0.19	*	
☐	WAN	IP21	172.16.0.21	*	
☐	WAN	IP22	172.16.0.22	*	
☐	WAN	IP24	172.16.0.24	*	

Slika 23: *pfSense* – pregled nad nekaj konfiguriranimi 1 : 1 NAT-preslikavami (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | NAT | 1:1))

- Preostala je le še konfiguracija in definiranje pravil požarnega zidu ter pred tem še definiranje t. i. vzdevkov (ang. *aliases*), ki bodo v prihodnosti bistveno olajšali morebitne spremembe pravil požarnega zidu. Uporaba vzdevkov, ki jih je mogoče

definirati v programski opremi *pfSense* preko menija (*Firewall* → *Aliases*) omogoča boljše upravljanje z IP-naslovi, vrati kot tudi URL-naslovi. Posebej so uporabni za zmanjšanje števila požarnih pravil, saj se z njimi lahko npr. IP-naslove gostiteljev in vrata pregledno združi in ustrezno poimenuje. Primerni so tudi v primerih, če je treba kdaj spremeniti pravila požarnega zidu, če bi se spremenil IP-naslov določenega gostitelja ali vrata. Pri uporabi vzdevkov ni treba na novo ustvarjati (ali urejati) posamično vseh pravil, ki zahtevajo spremembo, temveč se lahko spremembe preprosto uredijo z enim korakom znotraj tega vzdevka. Kot primer (Slika 24) bom prikazal, kako sem definiral vzdevek poštnega strežnika (KURIR) in s tem preprosto združil vsa vrata, ki jih uporablja. S pomočjo gumba »Dodaj nov vzdevek« (ang. *Add a new alias*) sem preko menija *Firewall* in iz spustnega seznama *Aliases* izbral *Ports*, nato vpisal ime vzdevka, podal opis, izbral tip (Type: Port(s)) ter vpisal vsa potrebna vrata, ki jih potrebuje za komunikacijo v omrežju in izven njega.

Firewall: Aliases: Edit

Alias Edit

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
You may enter a description here for your reference (not parsed).

Type

Port(s)
Enter as many ports as you wish. Port ranges can be expressed by separating with a colon.

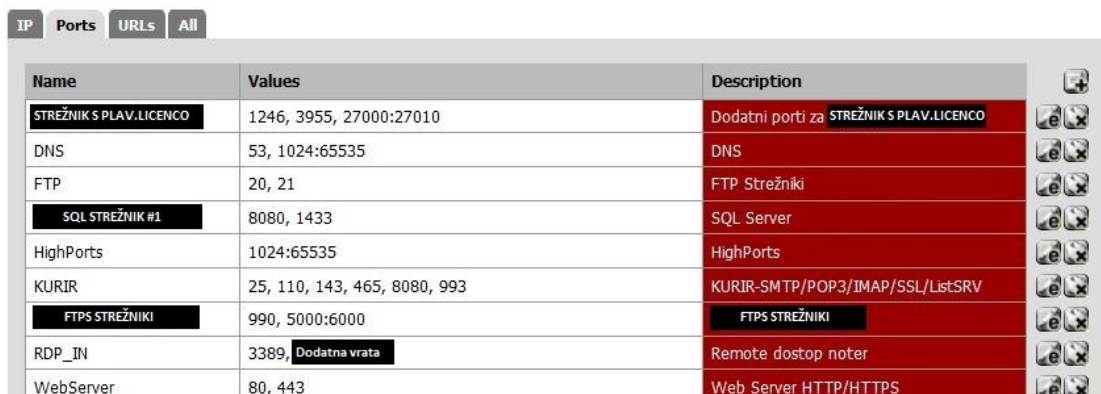
Port	Description
25	SMTP
110	POP3
143	IMAP
465	SMTP over SSL
8080	ListSRV
993	IMAP over SSL

Slika 24: *pfSense* – definiranje vzdevka (vrat) za poštne strežnik KURIR (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | Aliases | Edit))

Pred nadaljnjo konfiguracijo vzdevkov in požarnih pravil sem na podlagi popisa vseh obstoječih (ažurnih) pravil prejšnjega požarnega zidu premišljeno zasnoval, kako najboljše izkoristiti uporabo vzdevkov in s tem tudi nekoliko zmanjšati število in

olajšati kreiranje pravil požarnega zidu. Spodnji sliki (Slika 25 in Slika 26) tako prikazujeta pregled nad definiranimi vzdevki za vrata in IP-naslove različnih strežnikov in storitev.

Firewall: Aliases



The screenshot shows the 'Ports' tab of the 'Firewall: Aliases' configuration page. It displays a table of defined port aliases. The 'Name' column lists aliases like 'STREŽNIK S PLAV.LICENCO', 'DNS', 'FTP', 'SQL STREŽNIK #1', 'HighPorts', 'KURIR', 'FTPS STREŽNIKI', 'RDP_IN', and 'WebServer'. The 'Values' column shows the corresponding port ranges. The 'Description' column provides a brief explanation for each alias. Action icons (edit, delete, add) are visible on the right of each row.

Name	Values	Description
STREŽNIK S PLAV.LICENCO	1246, 3955, 27000:27010	Dodatni porti za STREŽNIK S PLAV.LICENCO
DNS	53, 1024:65535	DNS
FTP	20, 21	FTP Strežniki
SQL STREŽNIK #1	8080, 1433	SQL Server
HighPorts	1024:65535	HighPorts
KURIR	25, 110, 143, 465, 8080, 993	KURIR-SMTP/POP3/IMAP/SSL/ListSRV
FTPS STREŽNIKI	990, 5000:6000	FTPS STREŽNIKI
RDP_IN	3389, Dodatna vrata	Remote dostop noter
WebServer	80, 443	Web Server HTTP/HTTPS

Slika 25: *pfSense* – pregled nad konfiguriranimi vzdevki (vrati) (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | Aliases – Ports))

Firewall: Aliases



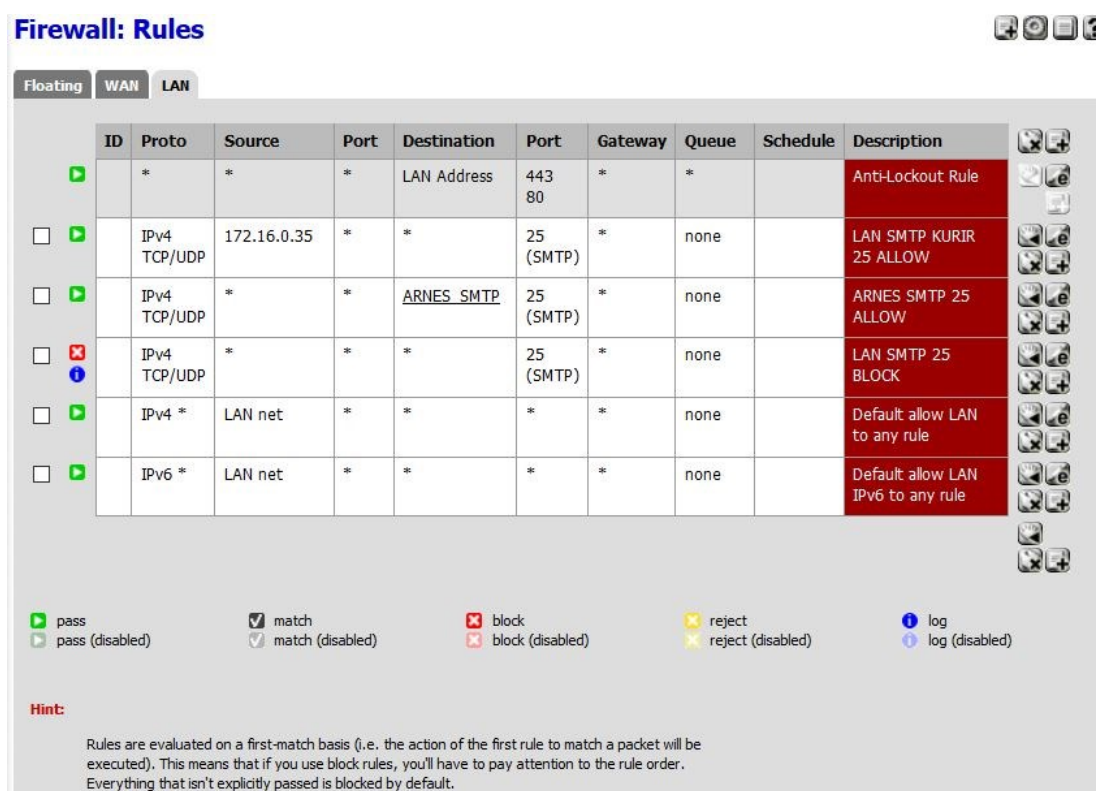
The screenshot shows the 'IP' tab of the 'Firewall: Aliases' configuration page. It displays a table of defined IP address aliases. The 'Name' column lists aliases like 'ZUNANJI UPORABNIKI - DOSTOP DO STREŽNIKA S PLAVAJOČO LICENCO', 'ARNES SMTP', 'DNS Servers', 'IT za računovodstvo', and 'ODDALJENE ENOTE (LOKACIJE)'. The 'Values' column shows the corresponding IP ranges. The 'Description' column provides a brief explanation for each alias. Action icons (edit, delete, add) are visible on the right of each row.

Name	Values	Description
ZUNANJI UPORABNIKI - DOSTOP DO STREŽNIKA S PLAVAJOČO LICENCO	[Redacted IP ranges]	Dovoljen dostop do STREŽNIKA S PLAV.LICENCO
ARNES SMTP	193.2.1.74, 193.2.1.75	ARNES Mail Servers
DNS Servers	172.16.0.19, 172.16.0.22	DNS Strežniki
IT za računovodstvo	[Redacted IP ranges]	Zunanji izvajalci (IT računovodstvo)
ODDALJENE ENOTE (LOKACIJE)	[Redacted IP ranges]	ODDALJENE ENOTE (LOKACIJE)

Slika 26: *pfSense* – pregled nad konfiguriranimi vzdevki (IP-naslovi) (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | Aliases – IP))

- Kot zadnje je preostala konfiguracija pravil požarnega zidu preko menija *Firewall* in iz spustnega seznama *Rules*. Kot sem že omenil, privzete nastavitve požarnega zidu prepuščajo ves izhodni promet (ang. *outbound traffic*) iz notranjega LAN-omrežja brez omejitev (blokad). Zato sem moral na »LAN-segmentu« definirati potrebna izhodna (ang. *outbound*) pravila, ki vsem napravam, razen poštnemu strežniku podjetja in Arnes strežnikoma za odhajajočo pošto (z IP-naslovoma 193.2.1.74 in

193.2.1.75), blokirajo izhodni promet preko vrat TCP/UDP 25. Kot je razvidno z zgornje slike (Slika 26), sem za namen dveh Arnesovih SMTP strežnikov predhodno ustvaril vzdevek (ARNES SMTP), ki sem ga uporabil pri ustvarjanju izhodnega pravila »ARNES SMTP 25 ALLOW«, kot prikazuje naslednja slika (Slika 27). Pred tem sem na enak način kreiral »podobno« pravilo tudi za poštni strežnik podjetja s pomočjo gumba »Dodaj novo pravilo« (ang. *Add new rule*) preko menija *Firewall* in iz spustnega seznama *Rules*, kjer sem izbral *LAN*. Pravilo poštnega strežnika (z notranjim IP-naslovom 172.16.0.35) predstavlja prvo vpisano pravilo z opisom »LAN SMTP KURIR 25 ALLOW«. Ker se pravila požarnega zidu procesirajo od zgoraj navzdol, sem moral za to pod njiju ustvariti pravilo, ki pa blokira izhodni promet preko vrat 25 vsem ostalim napravam v omrežju, neodvisno od vira (ang. *source*) ali cilja (ang. *destination*) prometa.



Slika 27: *pfSense* – pregled nad definiranimi izhodnimi pravili iz omrežja LAN (Vir: Posnetek zaslona – *pfSense* 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | Rules – LAN))

Razlika med definiranim pravilom poštnega strežnika (KURIR) in Arnesovih strežnikov za odhajajočo pošto je le v tem, da mora biti prvi (KURIR) kot notranji

strežnik podjetja definiran v pravilih »LAN-segmenta« kot vir, zunanja strežnika Arnes pa kot cilj.

Ves vhodni promet (ang. *inbound traffic*) v notranje omrežje pa je privzeto blokiran oziroma dovoljen le tisti, ki ima aktivne omrežne povezave, in tisti, ki je dovoljen s ustreznimi požarnimi pravili. Ta t. i. vhodna (ang. *inbound*) pravila do notranjega omrežja je bilo potrebno ustvariti na »WAN-segmentu«, kjer sem z ustreznimi pravili zadostil vsem zahtevam (potrebam) tega omrežja. Kljub uporabi vzdevkov je število pravil požarnega zidu, ki jih zahteva to omrežje, dokaj veliko, zato bi bil njihov prikaz z enim posnetkom zaslona nemogoč in tudi nesmiseln, saj bi moral večino informacij prekriti. Zato bom prikazal le, kako sem izkoristil uporabnost vzdevka za poštni strežnik KURIR (Slika 24) in z enim pravilom definiral »vhodno« pravilo požarnega zidu za potrebe poštnega strežnika (Slika 28), tokrat na »WAN-segmentu«.

Firewall: Rules: Edit

Edit Firewall rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 Select the Internet Protocol version this rule applies to
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	☐ not Use this option to invert the sense of the match. Type: any Address: [redacted] / 127 Advanced - Show source port range
Destination	☐ not Use this option to invert the sense of the match. Type: Single host or alias Address: 172.16.0.35 / 31
Destination port range	from: (other) KURIR to: (other) KURIR Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port
Log	☐ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	KURIR You may enter a description here for your reference.

Slika 28: pfSense – definirano vhodno pravilo za potrebe poštnega strežnika (Vir: Posnetek zaslona – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Firewall | Rules | Edit))

Preko menija *Firewall* in spustnega seznama *Rules* sem izbral *WAN* ter po kliku na gumb »Dodaj novo pravilo« definiral zgornje vhodno pravilo, ki dovoljuje TCP-promet od koder koli (*Source: Any*) do poštnega strežnika (172.16.0.35) preko točno določenih vrat (25, 110, 143, 465, 8080 in 993), ki pa so definirana z vzdevkom »KURIR« (Slika 24). Tako sem v t. i. ciljni razpon vrat (ang. *destination port range*) vpisal le začetne črke vzdevka »KURIR«, izbral ustrezen vzdevek iz seznama vzdevkov, podal opis in shranil (vnesel) pravilo. Na »enak način«, vendar z drugačnimi parametri in vzdevki pa sem s požarnim zidom *pfSense* lahko brez zapletov definiral tudi vsa preostala pravila, ki jih zahtevajo naprave in uporabniki tega omrežja.

5.2 Implementacija v omrežje

Za dodatno varnost samega robnega strežnika in posledično seveda celotnega omrežja podjetja sem pred njegovo implementacijo v obstoječe omrežje onemogočil dostop (preko *WebGUI*) do robnega strežnika od zunaj, tako da je dostopen le preko lokalnega omrežja. Ta odločitev je bila sprejeta predvsem zaradi prevelikega tveganja poskusov informacijskih vdorov in zloma gesla (ang. *brute force*) robnega strežnika. To sem storil z ustrezno definicijo pravila požarnega zidu, tako da sem blokiral promet preko protokola TCP na vratih 80 (HTTP) ter 443 (HTTPS)) zgolj za robni strežnik. Poleg *WebGUI* robnega strežnika to vrsto prometa »uporabljajo« namreč tudi ostali strežniki v podjetju (npr. spletni, aplikacijski itd.), zato mora biti ta vrsta prometa za te strežnike in storitve dovoljena.

Med konfiguriranjem nastavitvev in pred dejansko implementacijo robnega strežnika sem ugotovil, da popolnoma brez prekinitve delovanja omrežja žal ne bo šlo, saj je bilo treba spremeniti tudi nastavitve in vloge obstoječega (prejšnjega) robnega strežnika, ki je ključen za delovanje omrežja. Po tehtnem razmisleku sem ocenil, da bo prekinitev omrežja trajala največ 10 minut, zato sem po pogovoru z vodjo IT-oddelka dogovoril, da se bo spremembe in dejanska implementacija uredile v večernih urah s prejšnjim obvestilom vsem zaposlenim.

1. Podrobni pregled: Ponovno sem pregledal vse nastavitve pripravljenega robnega strežnika in preveril, da vzpostavljene storitve in dodeljene vloge ustrezno delujejo. Njihovo delovanje sem preveril v pregledu izvajanih in zaustavljenih storitev, kar je

dostopno preko zavihka »Status« in na spustnem meniju z imenom »Storitve« (*Status: Services*).

2. Dokončna konfiguracija robnega strežnika: Vnesel sem še zadnje spremembe, da lahko po priključitvi robnega strežnika v podjetje vse steče brez večjih zapletov. Tako sem spremenil IP-naslov 193.2.1.66 Arnesovega DNS-strežnika v notranji IP-naslov 172.16.0.2, ki bo po implementaciji dodeljen (spremenjen) internemu DNS-strežniku (prejšnjemu robnemu strežnik), nato pa vključil funkcionalnost (vlogo) DNS-posrednika (*DNS Forwarder*), ki je bila v nalogi že predstavljena. Tako bo robni strežnik po implementaciji zahteve pretvorbo imen pošiljal (posredoval) internemu DNS-strežniku oziroma na IP-naslov 172.16.0.2.
3. Zaustavitev robnega strežnika: Strežnik sem zaustavitev na način, ki vse storitve in procese ustrezno zaključi in pravilno zaustavi (ugasne) strežnik. To sem storil preko *WebGUI* s pomočjo funkcije zaustavitve sistema (ang. *halt system*) preko zavihka diagnostika (ang. *diagnostics*) in strežnik ustrezno ugasnil.
4. Fizični izklop, pregled komunikacijske omare, priprava vseh kablov in periferij: Iz strežnika sem izklopil vse priključne kable, jih prestavil v komunikacijsko omaro strežniške sobe, kjer sem jih ustrezno (brez prepletanja) napeljal in označil. Električna (napajalna) kabla sem tako vključil v ustrezni vtičnici UPS, mrežna kabla pa v stikalo ponudnika internetnih storitev in notranje stikalo omrežja. Začasno sem priključil tudi tipkovnico in monitor za potrebe spremljanja inicializacije sistema.
5. Montaža robnega strežnika v rezino komunikacijske omare: Najprej sem v komunikacijsko omaro varno montiral vodila (nosilce) strežnika in jih s priloženimi vijaki dobro pričvrstil ter nato previdno vstavil strežnik.
6. Priključitev kablov in vklop robnega strežnika: V strežnik sem priključil oba električna kabla ter začasno le en mrežni kabel, ki je na drugi strani priključen v stikalo ponudnika internetnih storitev (zunanje WAN-omrežje). Strežnik sem vklopil in počakal, da se ustrezno zažene in ponovno pravilno zazna mrežno povezavo, tokrat le za WAN.

7. Varnostna kopija prejšnjega robnega strežnika: Ustvaril sem varnostno kopijo celotnega operacijskega sistema oziroma posnetek sistema in jo varno hranil na zunanji trdi disk, predvsem zaradi morebitnih nepredvidenih večjih nadaljnjih zapletov, ki bi zahtevali povrnitev prejšnjega stanja.
8. Odstranitev vlog in storitev, sprememba nastavitev ter ponovni zagon prejšnjega robnega strežnika: Na prejšnjem strežniku sem moral zaustaviti in odstraniti vlogo prevajanja omrežnih naslovov NAT ter storitev usmerjanja prometa in oddaljenega dostopa RRAS. To pa je že pomenilo začetek prekinitve delovanja obstoječega omrežja. Moral sem ukiniti tudi vlogo požarnega zidu in popolnoma odstraniti programsko požarno zaščito *Visnetic*, zato je strežniku ostala zgolj vloga internega DNS-strežnika. Nato sem spremenil še omrežne nastavitve notranje mrežne kartice oziroma IP-naslov za notranje LAN-omrežje iz IP-naslova 172.16.0.1 na IP-naslov 172.16.0.2. IP-naslov 172.16.0.1, kot sem že omenil, sem moral spremeniti zaradi tega, ker ta služi notranjemu omrežju še vedno kot glavni prehod. Ta je vpisan na veliko napravah v celotnem omrežju, ki imajo ročno nastavljene statične IP-naslove (vsi strežniki, omrežni tiskalniki, NAS-naprave itd.). Ker zunanje mrežne kartice strežnik ne bo več potreboval, sem jo onemogočil in odstranil mrežni kabel iz stikala in strežnika. Strežnik sem tako lahko ponovno zagnal za ustrezno uveljavitev vseh sprememb.
9. Priključitev in implementacija robnega strežnika: Po ustreznem ponovnem zagonu prejšnjega robnega strežnika sem zdajšnjega priključil še v notranje (glavno) stikalo omrežja in ga tako implementiral v dano korporativno omrežje.

6 Testiranja in rezultati

Meritve pred implementacijo in po njej so bile izvedene pod podobnimi pogoji. V obeh primerih sem meritve opravljal v jutranjem delovnem času med 8. in 10. uro običajnega delavnika.

6.1 Metodologija testiranja

V omrežju sem **pred implementacijo** uporabljal različne metode za testiranje in spremljanje delovanja omrežja in prejšnjega robnega strežnika. Tako sem večkrat dlje časa in ob različnih urah ter z različnimi časovnimi intervali **meril zakasnitve omrežja** s pomočjo orodja *ping*. Pošiljal in prejemal sem t. i. nadzorne (kontrolne) pakete preko notranjega računalnika na Arnesov strežnik (193.2.1.87) z ukazom »*ping 193.2.1.87 -t*« in meril čas potovanja teh nadzornih sporočil oziroma t. i. paketov ICMP. Z rezultati sem tako pridobil statistični povzetek oziroma informacije o minimalnem, maksimalnem in povprečnem času prenosa teh paketov od računalnika do Arnesovega strežnika in nazaj (ang. *RTT – Round Trip Time*), ki jih bom kasneje primerjal z rezultati meritev po implementaciji. Rezultate zakasnitev pred implementacijo bom zato podal zgolj v tabeli. Podal bom predvsem rezultate merjenih zakasnitev v času slabšega delovanja omrežja oziroma v času višjih zakasnitev.

V tem času pa sem **spremljal** tudi **takratni podatkovni promet** z nameščenim programom *Iris Traffic Analyzer*. Tako sem pridobil informacije o vrsti in količini podatkovnega prometa in informacijo o napravah, ki so takrat v omrežju povzročale največ prometa. Količino zajetih paketov sem moral omejiti največ na število 2000, da ne bi spremljanje prometa vplivalo na še slabše delovanje obstoječega omrežja. Z zajetim prometom pa sem pridobil poleg količine podatkovnega prometa tudi informacije o času, ki je pretekel za zajetje teh paketov. Na podlagi tega časa sem lahko izračunal in ocenil približke za lažjo primerjavo količine podatkovnega prometa z rezultati po implementaciji. Med drugim sem lahko tako izračunal (ocenil) tudi takratno **hitrost pretoka** (ang. *throughput*) podatkov, ki so se prenesli skozi robni strežnik v časovni enoti. Kot sem že omenil, sem ob takšnih obremenitvah dlje časa spremljal zakasnitve, medtem zajel podatkovni promet, hkrati pa sem **spremljal** tudi **porabo sistemskih sredstev na robnem strežniku** prek upravitelja opravil. Predstavil bom tudi te rezultate in tudi posnetke zaslona z izmerjenimi hitrostmi internetne povezave, ki sem jo

izmeril prek posebne spletne strani na naslovu <http://www.speedtest.net/>. Na podlagi tega in ostalih informacij (rezultatov) se bo videla tudi slaba izkoriščenost internetne povezave in dejstvo, da je ozko grlo res predstavljal prejšnji robni strežnik.

Rezultate vseh meritev v **omrežju po implementaciji** robnega strežnika pa bom pregledneje podal slikovno, in sicer s posnetki zaslona grafov, ki jih že vključuje uporabljena programska oprema *pfSense*. Ima namreč že privzeto vgrajeno funkcionalnost beleženja in **spremljanja** delovanja samega strežnika (**porabe posameznih sistemskih sredstev**) kot tudi **celotnega omrežja** (**število paketov, promet, pretok ...**) od pričetka delovanja (priključitve). Te historične informacije prikazuje v obliki grafov preko menija *Status* in spustnega seznama *RRD Graphs*, ki vključujejo vse poglavitne informacije. Med drugim tako prikazuje tudi prej omenjene minimalne, maksimalne in povprečje **zakasnitev omrežja** preko menija *Status*, kjer se iz spustnega seznama izbere *Quality*, zaradi katerih jih ni treba dodatno (ročno) meriti. Za realen prikaz podatkov oziroma rezultatov zakasnitev sem moral preko menija *System* in iz spustnega seznama *Gateways* izbrati *Edit gateway* ter vnesti alternativni »spremljajoč« IP-naslov (ang. *alternative monitor IP*) za pravilen izračun zakasnitev omrežja. Ta mora biti enak kot v testih pred implementacijo, torej 193.2.1.87. Prav tako pa bom tudi tukaj ponovno izmeril hitrost internetne povezave preko zgoraj omenjene spletne strani, kjer se bo iz rezultata videla izkoriščenost internetne povezave po implementaciji robnega strežnika.

Predvsem me je primerjalno zanimalo, izkoristek internetne povezave in koliko več podatkovnega prometa lahko v enakem časovnem intervalu »preteče« preko implementiranega robnega strežnika z minimalnimi spremembami porabe sistemskih sredstev, seveda pa tudi primerjava povprečnih hitrosti pretoka in koliko manjše so zakasnitve v omrežju po implementaciji kljub nekajkrat večji hitrosti pretoka in dosti večji količini celotnega podatkovnega prometa.

6.2 Preizkus delovanja

Za uspešnost implementirane rešitve sem moral preveriti delovanje notranjega omrežja, storitev in bistvenih stvari, ki jih potrebuje omrežje za nemoteno delovanje. Kot prvo sem preizkusil **pošiljanje in prejemanje testnih paketov** (z ukazom »ping«) na Arnesov strežnik 193.2.1.87 preko enega izmed notranjih računalnikov. Računalnik je pakete uspešno pošiljal in prejemal. Nato sem preveril **delovanje svetovnega spleta** (www, oz. protokola HTTP in

HTTPS), **izhodnega NAT** in **DHCP strežnika**, tako da sem preizkusil delovanje spleta preko računalnika s dinamično dodeljenim IP-naslovom. Poleg uspešnega testa je bil pravilen tudi **zunanji IP-naslov**, glede na razpon IP-naslovov (podomrežje), iz katerega je bil računalniku dodeljen notranji IP-naslov. To sem lahko hitro preveril preko spletne strani (<http://whatismyipaddress.com/>). Prav tako pa je bil uspešen tudi test ustreznega delovanja tipa **1 : 1 NAT**, ki je strežnikom in ostalim napravam dodelil pravilne lastne (enolične) zunanje IP-naslove. Na podlagi teh testov pa sem hkrati lahko videl, da tudi **vloga DNS-posrednika** (*DNS Forwarder*) in **interni DNS-strežnik** ustrezno delujeta pri pretvorbi oziroma **ustrezni razrešitvi** obiskanih zunanjih spletnih strani.

Kljub takojšnjem brezhibnem delovanju zgoraj omenjenih bistvenih stvari pa sem ugotovil, da dokončna implementacija ne bo potekala popolnoma brez težav. Nastala je namreč težava s prikazovanjem oziroma razreševanjem »internih« spletnih strani, ko sem jih skušal obiskati znotraj omrežja (od zunaj so bile te normalno dostopne). Namesto da bi se spletne strani, gostujoče na strežnikih v tem omrežju, ki imajo svoje enolične zunanje IP-naslove ustrezno odprle, se je vsaka takšna zahteva pri »internem« dostopu preusmerila na naslov robnega strežnika (*WebGUI*). Po iskanju na spletu sem takoj našel rešitev [28] na omenjeno težavo, ki se v programski opremi *pfSense* imenuje kot možnost »zrcaljenja« NAT (ang. *NAT reflection*), ki pa je s privzetimi nastavitvami izključena. To sem moral za potrebe tega omrežja vključiti in tako so tudi interne spletne strani pri dostopu iz notranjega omrežja ponovno dosegljive. Naletel pa sem tudi na problem razreševanja zopet zgolj notranjih domenskih imen z ukazom *nslookup*, ki pretvarja numerične IP-naslove v besedne (domenske) in obratno. V zdajšnjem stanju (stanju po implementaciji) klient poda zahtevo za pretvorbo zunanjega ali notranjega imena oziroma IP-naslova preko robnega strežnika internemu DNS-strežniku. Namesto da bi robni strežnik posredoval zahtevo naprej internemu DNS-strežniku, je že predhodno klientu odgovoril in odvrnil zahtevo z napako »*** No internal type for both IPv4 and IPv6 Addresses (A+AAAA) records available«. Tudi to težavo sem hitro odpravil preko menija *System*, kjer sem iz spustnega seznama *Advanced* izbral *Admin Access* in onemogočil t. i. vnovično preverjanje povezave DNS (ang. *DNS rebind check*). Ta možnost je s privzetimi nastavitvami vključena, da dodatno varuje interni domenski strežnik pred zunanjimi poizkusi razrešitve notranjih domenskih imen. Za primer tega omrežja oziroma zaradi hkratne uporabe različnih zunanjih IP-naslovov mora biti ta možnost onemogočena.

Uspešno pa sem preizkusil tudi **delovanje elektronske pošte** (pošiljanje in prejemanje) preko poštnega klienta na mobilnem telefonu in preko spletne pošte. Preizkus zunanjega dostopa do **oddaljenega namizja, NAS-naprav, FTP- in SFTP-strežnikov** je bil prav tako uspešen, kot tudi delovanje vseh preostalih storitev. Kot se je v nadaljevanju izkazalo, so bila ustrezno definirana in pravilno delujoča tudi vsa ostala pravila požarnega zidu.

6.3 Rezultati in primerjava

Implementirana rešitev (robni strežnik) in omrežje delujeta stabilno in učinkovito kar dokazujejo v tem poglavju predstavljene meritve in rezultati. V nadaljevanju tega poglavja bom podal vsa ključna merjenja in rezultate, ki sem jih spremljal in opravljal v omrežju pred in po implementaciji. **Najprej bom predstavil in prikazal rezultate prejšnjega stanja, nato še rezultate po implementaciji** robnega strežnika v omrežje in na koncu naredil še primerjavo. Rezultate (število paketov, količino prometa, zakasnitve, stanje robnega strežnika, internetna hitrost, itd.), ki jih bom podal iz prejšnjega stanja ponazarjajo meritve v času slabšega delovanja omrežja in daljših zakasnitev. Za boljšo primerjavo očitnega izboljšanja delovanja pa bom podal rezultate meritev novega stanja ob tistem času, kadar je bilo omrežje in razpoložljiva pasovna širina (ang. *bandwidth*) še bistveno bolj obremenjena kot v času meritev pred implementacijo. So pa bili pogoji, kot sem že omenil, podobni kot v času meritev prejšnjega stanja, torej običajen delavnik v jutranjem delovnem času. Na podlagi teh rezultatov se bo jasno videla učinkovitost izbranega robnega strežnika, programske opreme *pfSense* in uspešnost implementirane rešitve.

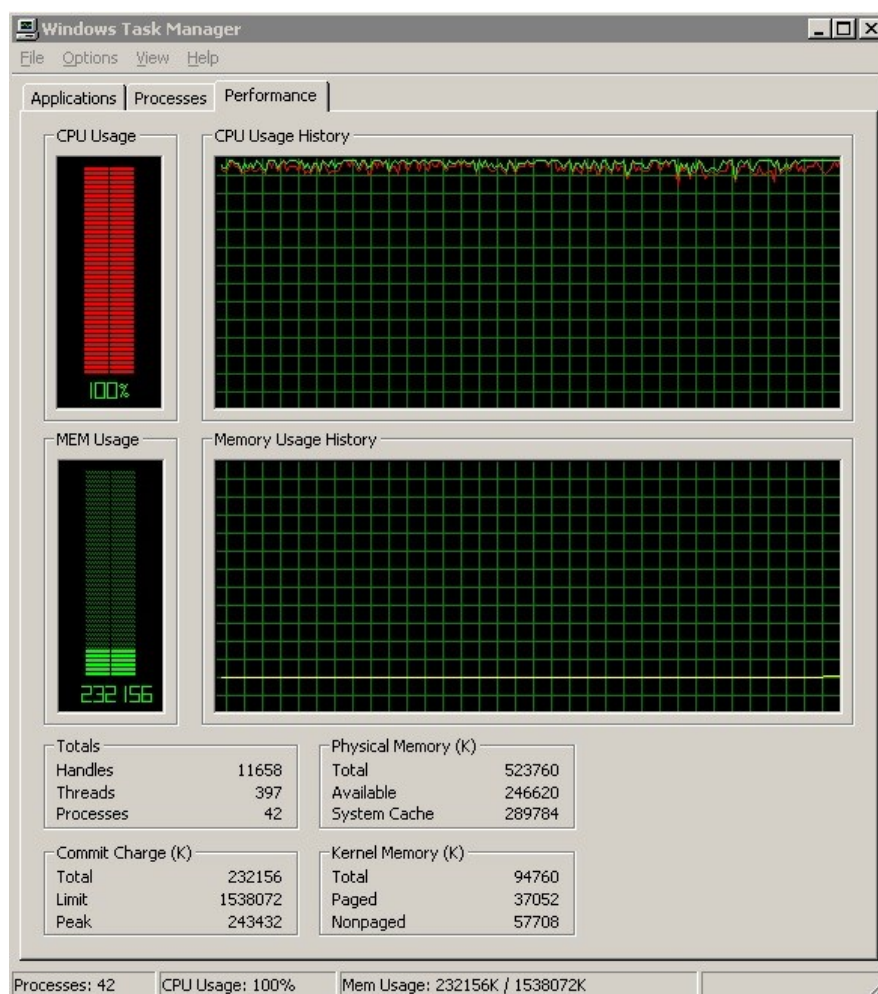
Spodnji rezultati meritev v tabeli (Tabela 2) prikazujejo statistični povzetek šestih različnih meritev zakasnitev v stanju pred implementacijo robnega strežnika. Meritve sem opravljal ob različnih časih in dnevih ter z različnimi časovnimi intervali. Povzetki meritev prikazujejo število poslanih in prejetih paketov, število in delež paketnih izgub, minimalne, maksimalne ter povprečje zakasnitev pri pošiljanju in prejemanju nadzornih paketov na IP-naslov 193.2.1.87. Ti rezultati služijo za očitni prikaz dlje časa trajajočih in ponavljajočih se višjih zakasnitev v omrežju, na podlagi katerih se lahko že sedaj razbere slabše delovanje tega omrežja. To je razvidno iz vseh rezultatov merjenj, predvsem pa iz rezultata najdaljše meritve drugega primera (Meritve zakasnitev 2), kjer je bilo poslanih kar 161.849 paketov. Iz tega podatka lahko, glede na to da računalnik pošlje po en paket vsako sekundo, približno ocenimo

pretečen čas celotnega merjenja, kar je malo manj kot dva dni (45 ur). Torej so zakasnitve v tem času dosegale maksimum 2478 ms in bile v povprečju visoke 110 ms. Pri tem igra pomembno vlogo tudi to, da je bila ta meritev izvajana brez prekinitev tudi čez noč, ko je omrežje bistveno manj obremenjeno ali pa sploh ne in je končno povprečje zakasnitev bilo vseeno zelo visoko.

Meritev zakasnitev 1 (trajanje cca. 15 minut)	Meritev zakasnitev 4 (trajanje cca. 114 minut)
... Odgovor od 193.2.1.87: bajtov=32 čas=586ms TTL=55 Odgovor od 193.2.1.87: bajtov=32 čas=558ms TTL=55 Statistika preverjanja dosegljivosti za 193.2.1.87: Paketov: Poslanih = 884, Prejetih = 881, Izgubljenih = 3 (0% izguba), Povprečni čas v milisekundah: Minimum = 118ms, Maksimum = 1102ms, Povprečje = 552ms	... Odgovor od 193.2.1.87: bajtov=32 čas=61ms TTL=55 Odgovor od 193.2.1.87: bajtov=32 čas=1ms TTL=55 Statistika preverjanja dosegljivosti za 193.2.1.87: Paketov: Poslanih = 6851, Prejetih = 6832, Izgubljenih = 19 (0% izguba), Povprečni čas v milisekundah: Minimum = 1ms, Maksimum = 1088ms, Povprečje = 267ms
Meritev zakasnitev 2 (trajanje cca. 45 ur)	Meritev zakasnitev 5 (trajanje cca. 43 minut)
... Odgovor od 193.2.1.87: bajtov=32 čas=56ms TTL=56 Odgovor od 193.2.1.87: bajtov=32 čas=1ms TTL=56 Statistika preverjanja dosegljivosti za 193.2.1.87: Paketov: Poslanih = 161849, Prejetih = 161453, Izgubljenih = 396 (0% izguba), Povprečni čas v milisekundah: Minimum = 1ms, Maksimum = 2478ms, Povprečje = 110ms	... Odgovor od 193.2.1.87: bajtov=32 čas=836ms TTL=55 Odgovor od 193.2.1.87: bajtov=32 čas=911ms TTL=55 Statistika preverjanja dosegljivosti za 193.2.1.87: Paketov: Poslanih = 2592, Prejetih = 2089, Izgubljenih = 503 (19% izguba), Povprečni čas v milisekundah: Minimum = 1ms, Maksimum = 1287ms, Povprečje = 520ms
Meritev zakasnitev 3 (trajanje cca. 6 ur)	Meritev zakasnitev 6 (trajanje cca. 4 ure)
... Odgovor od 193.2.1.87: bajtov=32 čas=1ms TTL=56 Odgovor od 193.2.1.87: bajtov=32 čas=1ms TTL=56 Statistika preverjanja dosegljivosti za 193.2.1.87: Paketov: Poslanih = 20875, Prejetih = 20660, Izgubljenih = 215 (1% izguba), Povprečni čas v milisekundah: Minimum = 1ms, Maksimum = 3598ms, Povprečje = 180ms	... Odgovor od 193.2.1.87: bajtov=32 čas=1ms TTL=56 Odgovor od 193.2.1.87: bajtov=32 čas=1ms TTL=56 Statistika preverjanja dosegljivosti za 193.2.1.87: Paketov: Poslanih = 14864, Prejetih = 14819, Izgubljenih = 45 (0% izguba), Povprečni čas v milisekundah: Minimum = 1ms, Maksimum = 1267ms, Povprečje = 211ms

Tabela 2: Statistični povzetek šestih različnih meritev zakasnitev (Vir: Meritev zakasnitev pred implementacijo z ukazom »ping 193.2.1.87 -t«)

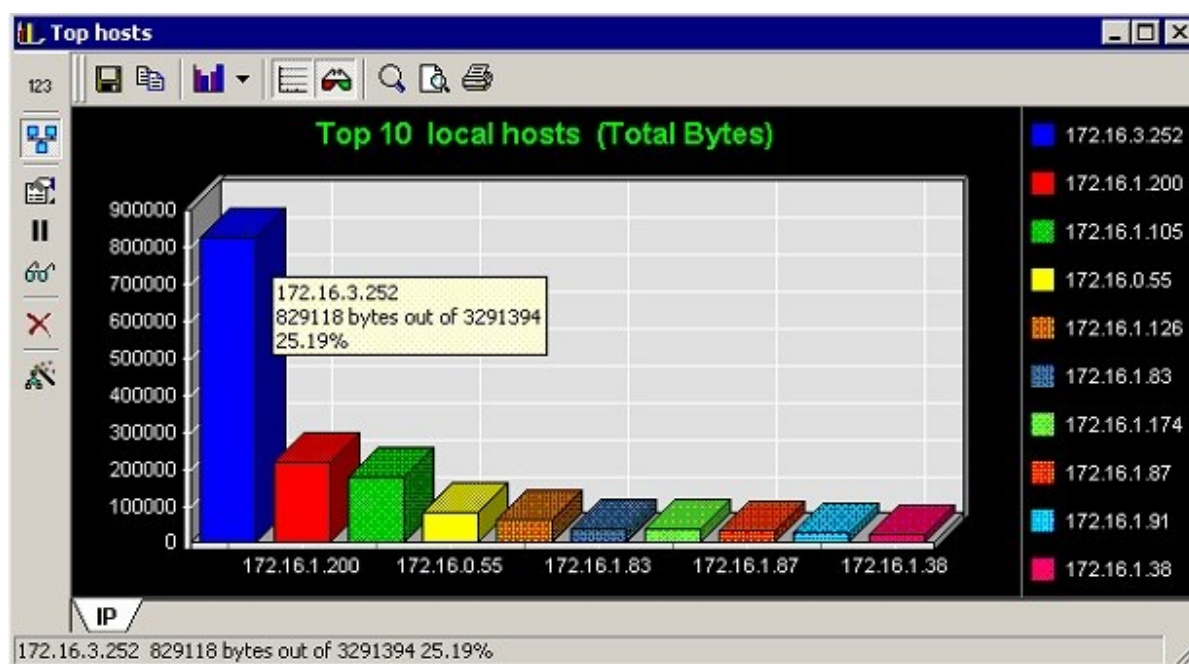
Meritev zakasnitev 1 iz tabele (Tabela 2) predstavlja rezultat zakasnitev, kjer sem medtem dokumentiral tudi zajet podatkovni promet, stanje strežnika in izmeril razpoložljivo hitrost internetne povezave. Meritve sem opravljal približno 15 minut, kar se lahko približno izračuna (oceni) tudi na podlagi števila 884 poslanih paketov, če je vsak paket poslan vsako sekundo. Zakasnitve v tem času merjenja tako niso upadle pod 118 ms, dosegale maksimum 1102 ms in so bile v povprečju visoke kar 552 ms. Stanje sistemskih sredstev robnega strežnika, ki sem ga spremljal približno 10 minut med merjenjem teh zakasnitev preko upravitelja opravil pa prikazuje naslednja slika (Slika 29).



Slika 29: Stanje sistemskih sredstev prejšnjega robnega strežnika v času višjih zakasnitev (Vir: Posnetek zaslona na prejšnjem robnem strežniku (Upravitelj opravil))

Slika 29 prikazuje konstantno, skoraj maksimalno obremenitev procesorja (ang. *CPU usage*), ki jo prikazuje zelena krivulja ter tudi samega jedra operacijskega sistema *kernel* (rdeča krivulja), ki posreduje dostope do sistemskih sredstev. To nakazuje na dejstvo, da je bil razlog

teh višjih zakasnitev res preobremenjen robni strežnik, ki ni zmožgal več učinkovito in pravočasno deliti sredstev strojne opreme vsem procesom. V tem času je bilo tudi upravljanje strežnika zaradi njegove neodzivnosti zelo oteženo. Ker sem medtem zajel in analiziral takratni vhodni in izhodni podatkovni promet, bom s sliko (Slika 30) med drugim podal tudi bistven podatek, in sicer skupno količino (velikost) podatkovnega prometa.



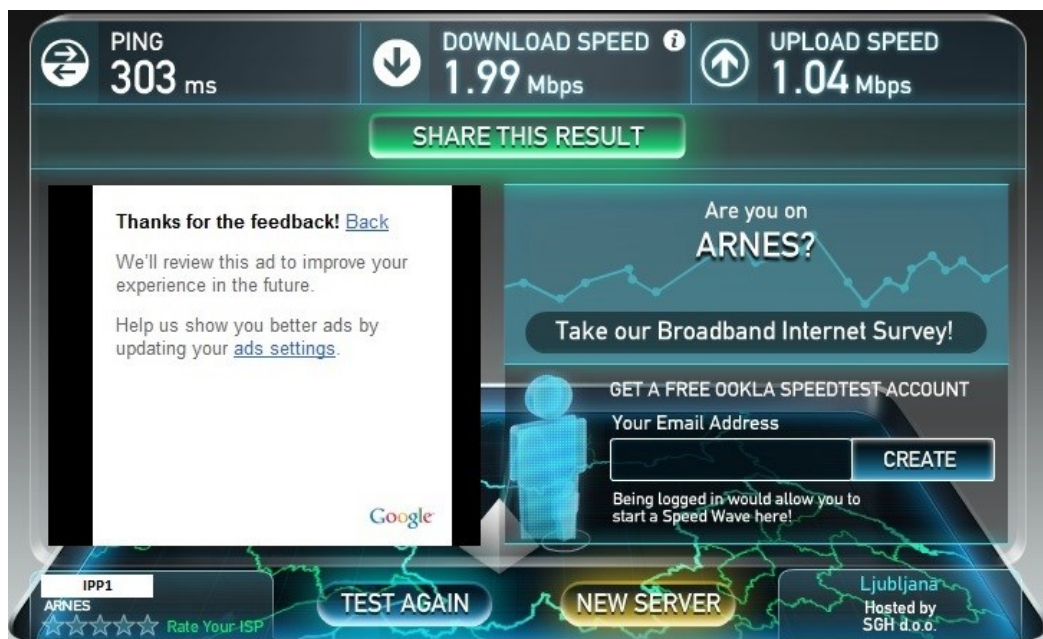
Slika 30: Deset lokalnih naprav z največ prometa, zajetim v 4,59 sekundah v času višjih zakasnitev (Meritev zakasnitev 1) (Vir: Posnetek zaslona na prejšnjem robnem strežniku (Iris Traffic Analyzer))

Slika 30 prikazuje lestvico desetih lokalnih naprav, ki so v času omenjenih meritev (pred implementacijo) povzročale največ prometa glede na celotni podatkovni promet, zajet v 4,59 sekundah, ki je v tem času skupaj znašal 3.291.394 bajtov oziroma 3,29 MB. V programu *Iris Traffic Analyzer* je mogoče izračunati pretečen čas, ki je bil potreben za zajetje teh paketov, saj do milisekunde natančno zabeleži čas vsakega zajetega paketa. Na podlagi tega časa (4,59 sekund) sem lahko približno izračunal (ocenil), kolikšna bi bila takrat (v takratnem stanju omrežja) količina paketov v pretečeni eni minuti in kolikšna bi bila skupna velikost podatkovnega prometa v eni minuti. Prav tako sem za boljšo primerjavo izračunal in ocenil tudi, kolikšne bi bile vrednosti pri pretečeni eni uri zajemanja prometa. Rezultate, ocenjene količine in izračunane približke bom podal v spodnji tabeli (Tabela 3). Ocenjene količine v tej tabeli, so pripravljene tudi z namenom lažje primerjave s podatkovnim prometom po implementaciji, ki ga bom podal kasneje v nadaljevanju tega poglavja.

	Rezultati meritve	Izračun približkov	Izračun približkov
Čas trajanja meritve:	4,59 sekund	1 minuta	1 ura
Število zajetih paketov:	2000	26.140	1.568.400 (≈ 1,57 milijonov)
Količina zajetega podatkovnega prometa:	3.291.394 bajtov (≈ 3,29 MB)	≈ 43.018.520 bajtov (≈ 43,02 MB)	≈ 2581.111.200 bajtov (≈ 2,58 GB)
Povprečna hitrost pretoka (v Mbit/s):	≈ 5,73 Mbit/s	≈ 5,73 Mbit/s	≈ 5,73 Mbit/s
Povprečje zakasnitev:	552 ms	552 ms	≈ 552 ms
Obremenitev procesorja:	100 %	100 %	≈ 100 %

Tabela 3: Rezultati meritve podatkovnega prometa v času višjih zakasnitev (Meritev zakasnitev 1) in ocenjene količine (Vir: Zajeti paketi preko Iris Traffic Analyzer na prejšnjem robnem strežniku)

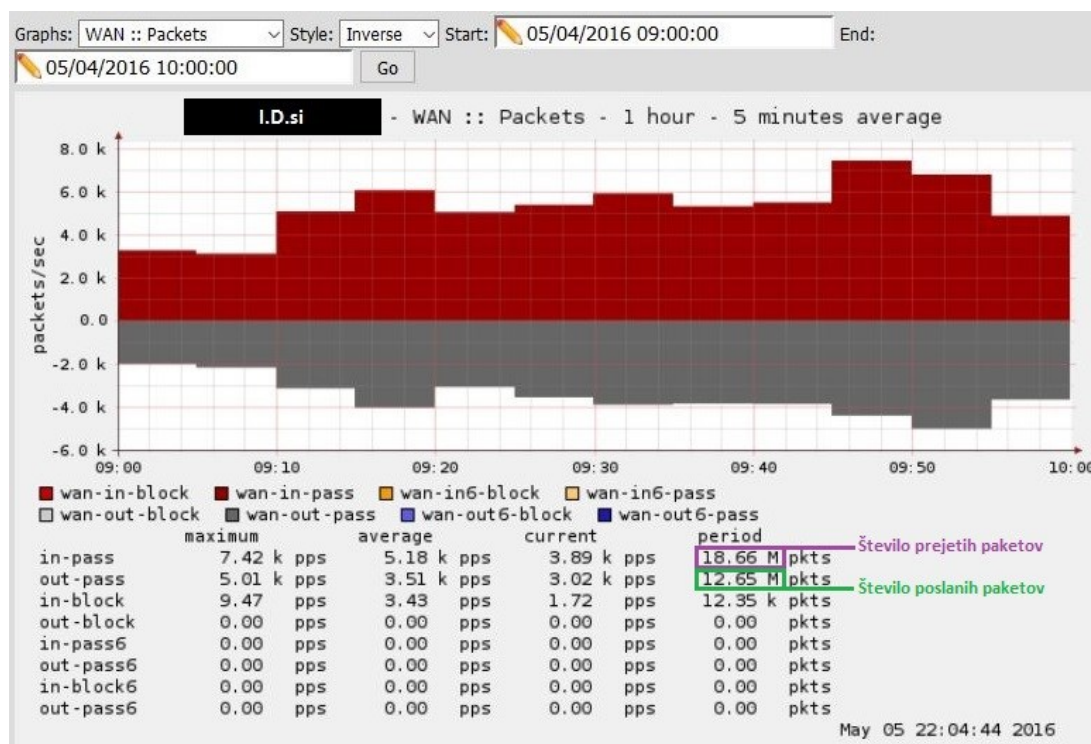
Na podlagi trajanja meritve (4,59 sekund) in količine podatkovnega prometa (3,29 MB) sem lahko približno izračunal tudi takratno (povprečno) hitrost pretoka, ki je znašala komaj 5,73 Mbit/s od razpoložljive 100/100 Mbit/s internetne povezave. Ocenjene količine, ki jih bom uporabil za primerjavo z rezultati po implementaciji, sem v zgornji tabeli označil krepko. Izmeril pa sem tudi hitrost internetne povezave v času teh višjih zakasnitev preko spletne strani (<http://www.speedtest.net/>), katere rezultat prikazuje Slika 31.



Slika 31: Izmerjena hitrost internetne povezave v času večjih zakasnitev (Meritev zakasnitev 1) (Vir: <http://www.speedtest.net/>)

Hitrost internetne povezave (v smeri proti uporabniku in proti internetu) v omrežju pred implementacijo v času višjih zakasnitev (Meritev zakasnitev 1) sem izmeril takoj po končanem zajemu (meritvi) podatkovnega prometa, in sicer na računalniku z zunanjim IP-naslovom {IPP1}. Na podlagi vseh zgoraj podanih rezultatov meritev in stanj se lahko vidi zelo slaba izkoriščenost razpoložljive 100/100 Mbit/s internetne povezave, ki je bila v času preobremenjenosti robnega strežnika manj kot 10 %. Preobremenjenost robnega strežnika je tako vplivala na višje zakasnitve in posledično na upočasnenost celotnega notranjega omrežja.

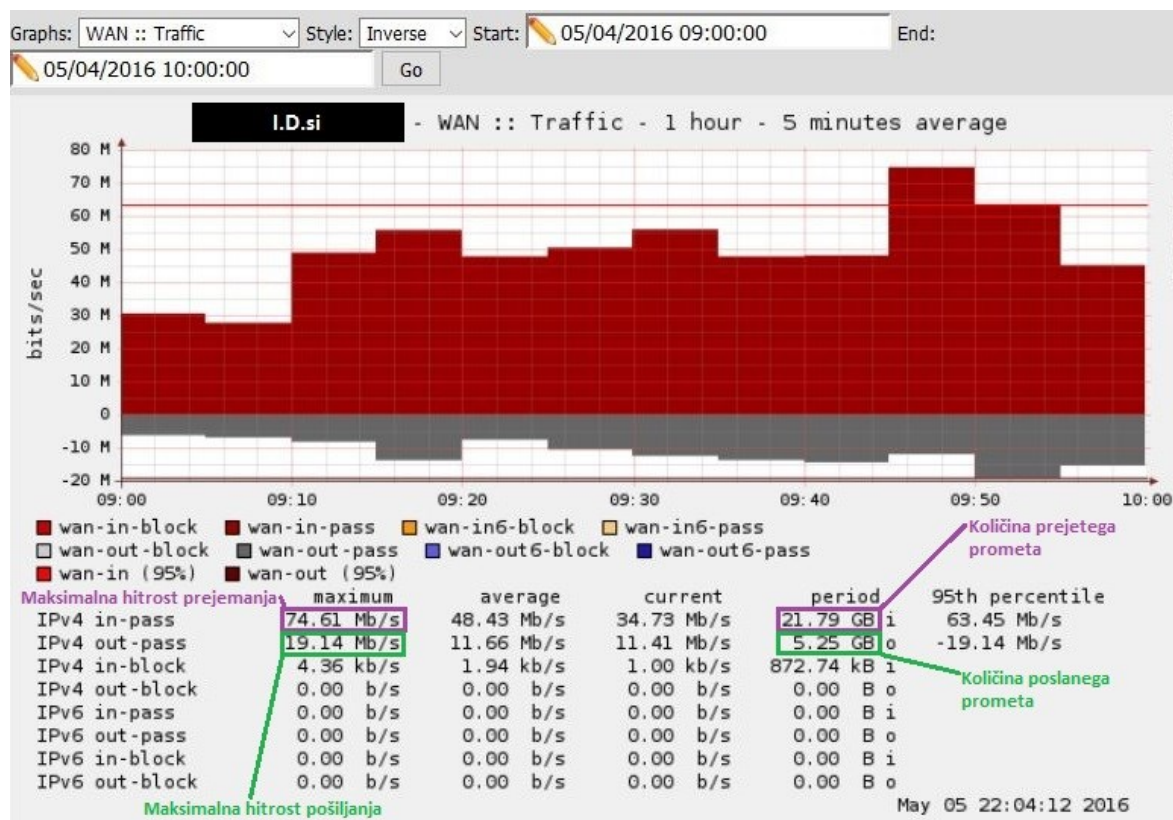
Sedaj pa bom podal tudi rezultate novega stanja oziroma stanja po implementaciji robnega strežnika v omrežje. Meritve, ki jih predstavljajo naslednji rezultati (v obliki grafov), sem pridobil preko že omenjenih historičnih informacij, kjer sem omejil čas meritve na ena uro za boljšo primerjavo z rezultati pred implementacijo. Čas enourne meritve, kot je razvidno tudi iz grafov, je bil v času normalnega delovnega dne med 09:00 in 10:00 uro zjutraj, kakor tudi pri meritvah pred implementacijo. Slika 32 spodaj med drugim prikazuje število 18,66 milijonov prejetih paketov, označenih kot »in-pass«, in število 12,65 milijonov poslanih paketov z oznako (»out-pass«) v času enourne meritve med 9. in 10. uro zjutraj.



Slika 32: pfSense – število prejetih in poslanih paketov v času enourne meritve (Vir: Posnetek zaslona grafa – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | RRD Graphs | Packets))

Skupno število vseh zajetih paketov (razen blokiranih z oznako (»in-block«)) v času pretečene ure je torej znašalo 31,31 milijonov.

Slika 33 prikazuje hitrost prenosa in natančne podatke o prejetem in poslanem podatkovnem prometu. Iz rezultatov je mogoče razbrati količino prejetega prometa z oznako (»IPv4 in-pass«), ki je znašala 21,79 GB, in količino poslanega prometa z oznako (»IPv4 out-pass«), ki je znašal 5,25 GB.

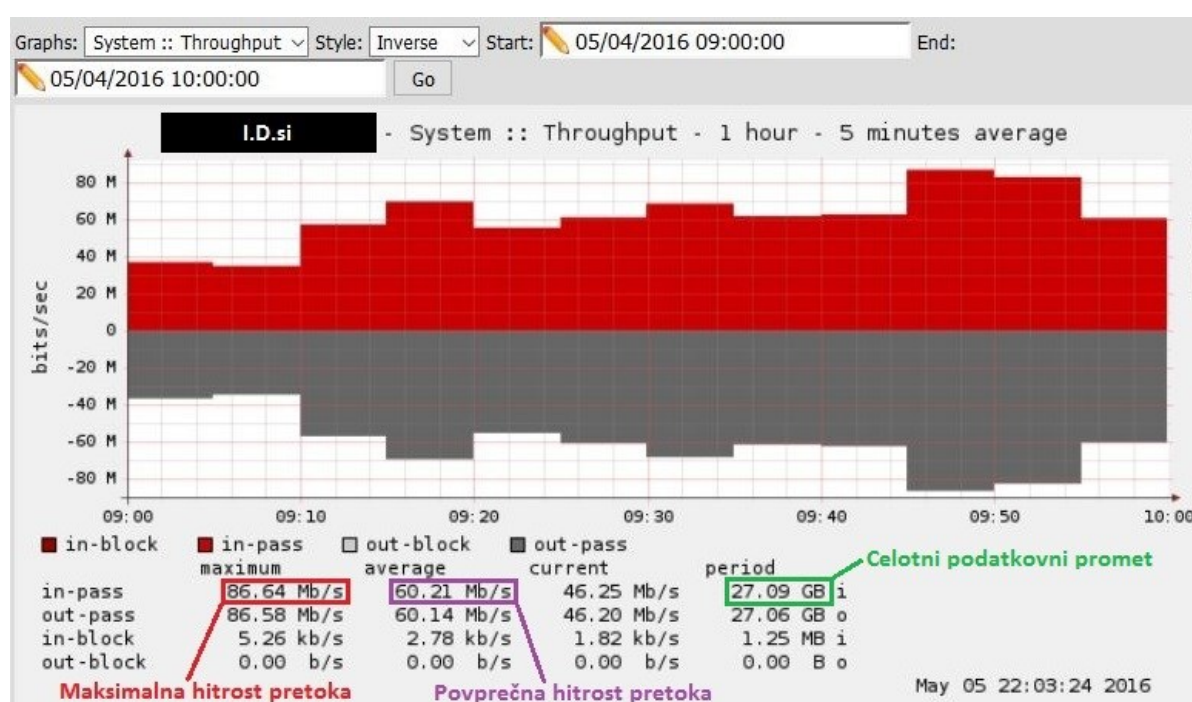


Slika 33: pfSense – rezultati meritve podatkovnega prometa in hitrosti prenosa v času enourne meritve (Vir: Posnetek zaslona grafa – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | RRD Graphs | WAN :: Traffic))

Poleg podatkovnega prometa pa zgornja slika (Slika 33) prikazuje tudi podatke o maksimalni hitrosti, s katero je bil ta promet prenesen (74,61 Mbit/s), in s kolikšno najvišjo poslan (19,14 Mbit/s). Te hitrosti in tudi hitrosti pretoka so sicer odvisne od več spremenljivk, med drugim tudi od trenutnega stanja zasedenosti zunanjih (tujih) strežnikov, od koder so uporabniki v tem času prejeli in pošiljali podatke. Realne (dejanske) hitrosti prenosa in pošiljanja podatkov (v smeri proti uporabniku in proti internetu) bom prikazal na koncu tega poglavja s testom hitrosti internetne povezave preko <http://www.speedtest.net/>.

Naslednja slika (Slika 34) pa prikazuje informacije o celotnem pretoku podatkov. Poleg količine skupnega podatkovnega prometa (prejetega in poslanega) med pomembnejšimi informacijami vsebuje podatek tudi o maksimalni in povprečni hitrosti pretoka podatkov. Slednjo bom na koncu tega poglavja lahko uporabil za primerjavo s povprečno hitrostjo pretoka prejšnjega stanja. Ta (omrežni) pretok si lahko predstavljamo kot merilo za hitrost, s katero so zajeti podatki dejansko (v povprečju) prešli preko robnega strežnika.

Celotni podatkovni promet, ki je bil prenesen preko robnega strežnika v časovnem intervalu ene ure, je torej znašal 27.09 GB.



Slika 34: pfSense – hitrost pretoka podatkov v času enourne meritve (Vir: Posnetek zaslona grafa – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | RRD Graphs | System :: Throughput))

Maksimalna hitrost pretoka v času tega merjenja je torej znašala 86,64 Mbit/s in je v povprečju bila 60,21 Mbit/s. V primeru, če bi čas meritve še dodatno omejil, npr. na interval med 09:45 in 09:50, kjer so bile hitrosti najvišje, bi bila tudi povprečna hitrost pretoka v teh petih minutah zelo blizu največji takratni hitrosti pretoka.

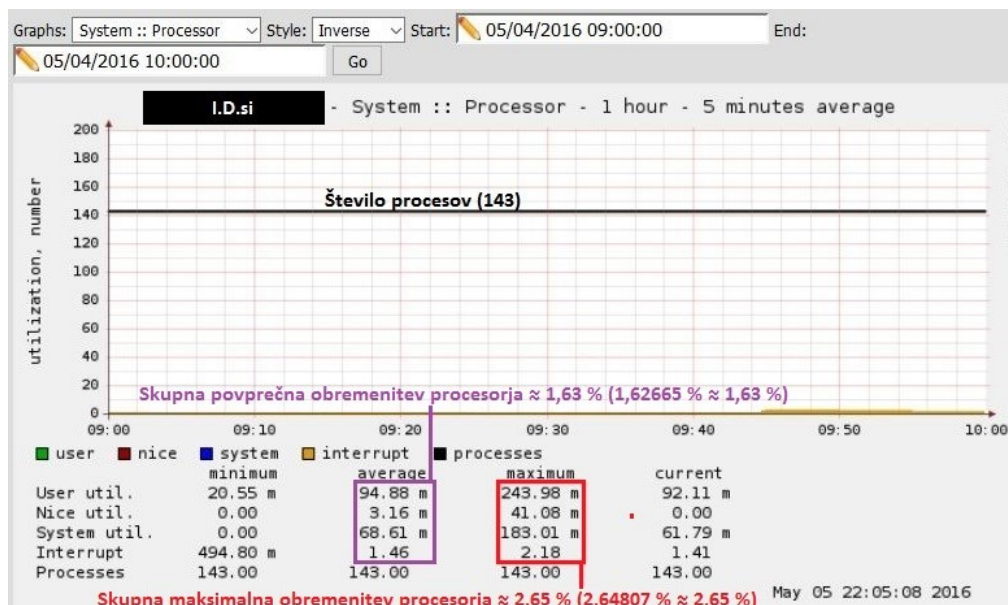
Na naslednji sliki (Slika 35) lahko vidimo rezultat minimalnih, maksimalnih in povprečnih zakasnitev v času te meritve, ki sem jih na sliki tudi označil oziroma poudaril. Minimalne zakasnitve so znašale 2,90 ms, maksimalne 127,01 ms in povprečne 18,58 ms.



Slika 35: pfSense – minimalne, maksimalne in povprečje zakasnitve v času enourne meritve (Vir: Posnetek zaslona grafa – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | RRD Graphs | WANGW :: Quality))

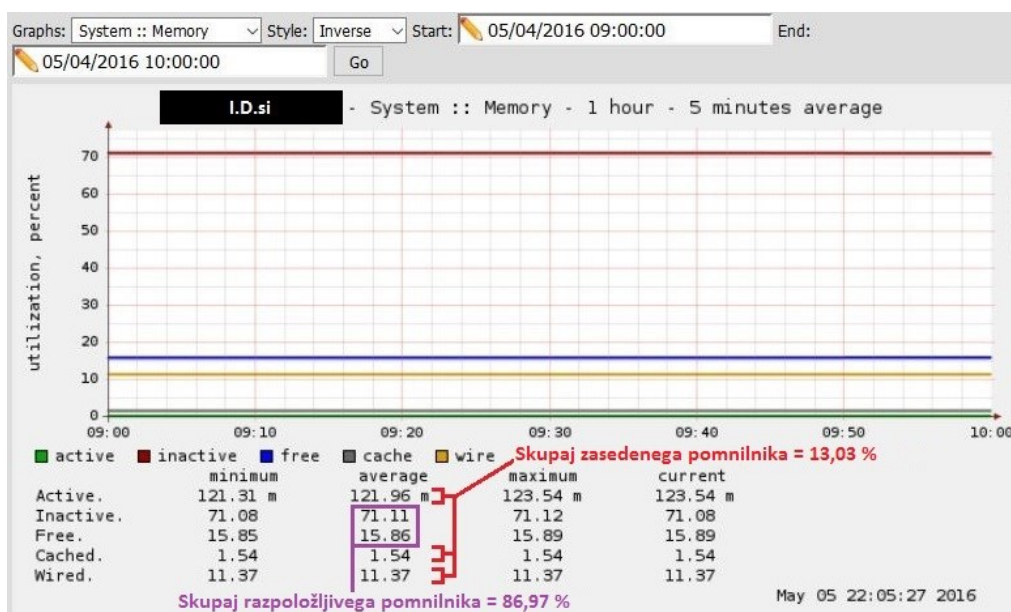
Če pogledamo čas oziroma interval med 09:45 in 09:50 na vseh štirih zgornjih priloženih slikah (grafih), lahko vidimo, da so bile takrat vse količine (število paketov, hitrost prenosa, hitrost pretoka in zakasnitve) največje, kar je logično.

Podal bom tudi sliki pregleda porabe sistemskih sredstev robnega strežnika v tem časovnem okviru, kjer naslednji dve sliki (36 in 37) prikazujeta: Slika 36 prikazuje pregled nad stanjem procesorja, Slika 37 pa pregled nad stanjem sistema pomnilnika. Iz teh rezultatov je očitno razbrati, da je tudi ob dokaj obremenjenem omrežju stanje porabe sistemskih sredstev robnega strežnika ostaja optimalno in zelo malo spremenljivo. Graf stanja obremenitve procesorja (Slika 36) prikazuje število vseh procesov in odstotek izkoriščenosti (ang. *utilization*) sredstev procesorja ločeno glede na to, koliko ga je v tem časovnem intervalu obremenjeval uporabnik, sistem in drugi programi. Pri tem je izkoristek uporabnika označen kot (»*User util.*«), izkoristek sistema kot (»*System util.*«), izkoristek programa *nice* kot (»*Nice util.*«) in izkoristek prekinitvev kot (»*Interrupt*«). Program *nice* v operacijskem sistemu FreeBSD predstavlja podobno funkcijo kot že omenjeni kernel v sistemu Windows. Odstotek obremenitve procesorja, ki so ga porabile t. i. prekinitve (ang. *interrupt*), pa večinoma predstavljajo zahteve vhodno-izhodnih naprav (npr. mrežni kartici).



Slika 36: pfSense – stanje obremenjenosti procesorja v času enourne meritve (Vir: Posnetek zaslona grafa – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | RRD Graphs | System :: Processor))

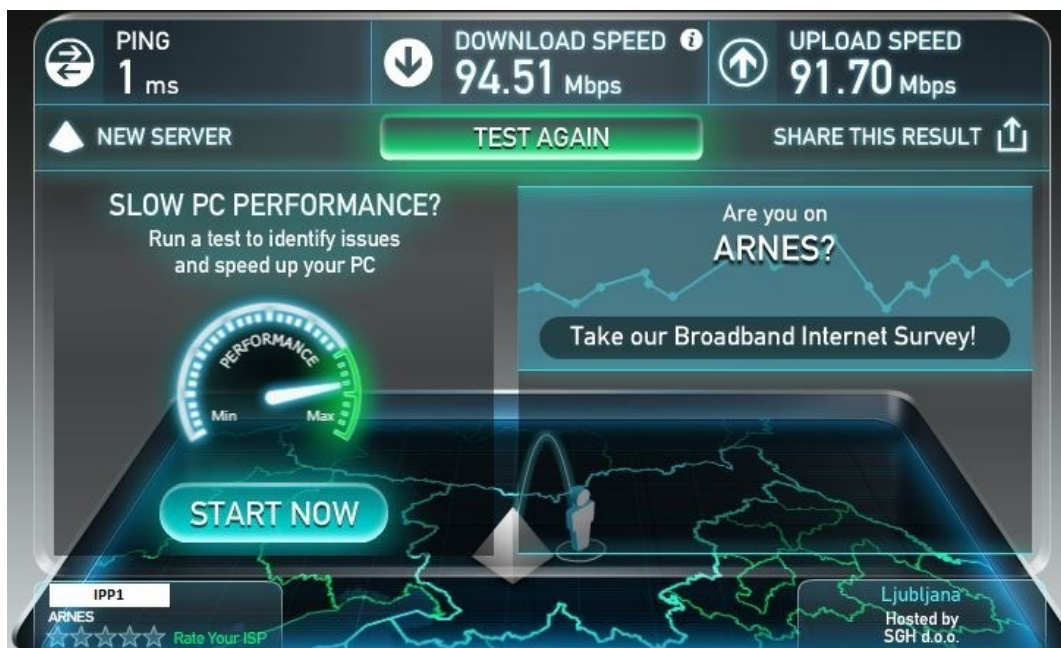
Skupna povprečna obremenitev procesorja se izračuna iz seštevka vseh povprečnih vrednosti (odstotkov) obremenitev s strani uporabnika, sistema, programa *nice* in prekinitiv. V tem času je bil procesor obremenjen povprečno 1,63-%, maksimalna obremenitev pa ni presegala 2,65 %.



Slika 37: pfSense – stanje porabe pomnilnika v času enourne meritve (Vir: Posnetek zaslona grafa – pfSense 2.2.4 na strežniku HP ProLiant DL360 G7 (Status | RRD Graphs | System :: Memory))

Iz zgornje slike (Slika 37) se vidi skoraj konstantna in nespremenjena poraba sistemskega pomnilnika, ki je bil skupaj v povprečju in tudi maksimalno zaseden zgolj 13,03-%. Ta rezultat (meritev) podajam zgolj informativno za prikaz tudi optimalne (konstantne) porabe pomnilnika, ki pa za primerjavo v nadaljevanju ni bistven.

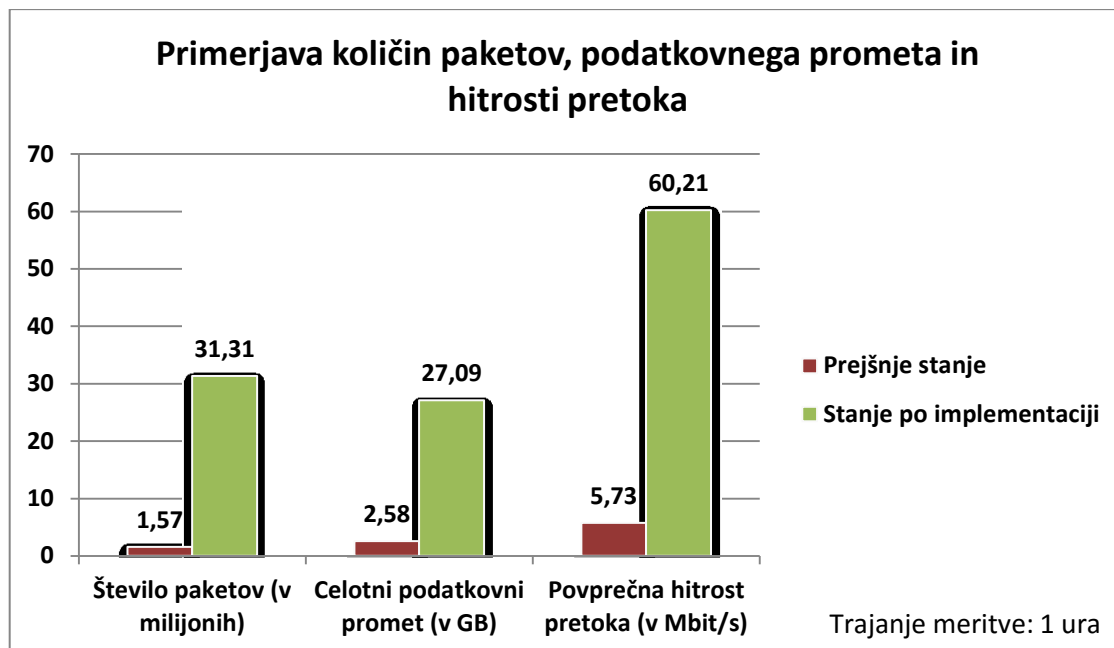
Pred primerjavo rezultatov pa za konec podajam tudi rezultat (Slika 38) izmerjene hitrosti internetne povezave po implementaciji, ki sem jo prav tako opravil preko spletne strani <http://www.speedtest.net/>. Pri tem moram opomniti tudi na to, da dano omrežje ni nikoli popolnoma neobremenjeno, saj so strežniki in nekateri računalniki neprestano vklopljeni in omrežno aktivni. Čeprav sem meritev, ki jo predstavlja slika (Slika 38), opravil izven delovnega časa, je rezultat nekoliko nižji, kot bi sicer lahko bil pri popolnoma »prostem« in nezasedenem omrežju.



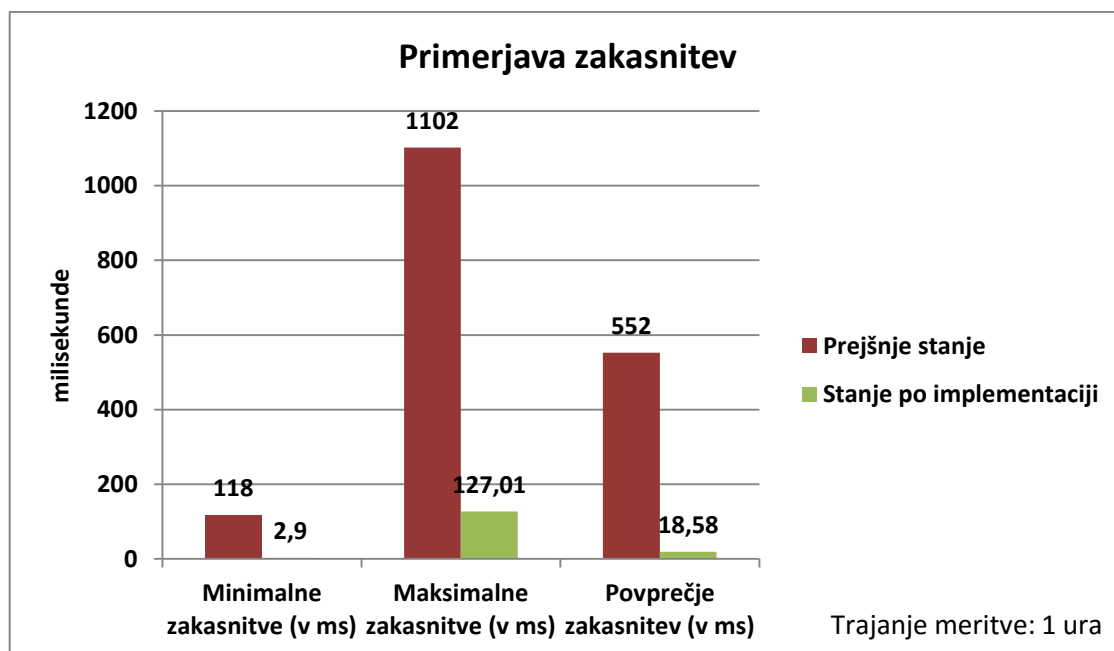
Slika 38: Izmerjena hitrost internetne povezave po implementaciji robnega strežnika izven delovnega časa (Vir: <http://www.speedtest.net/>)

Glede na rezultat zgornje meritve (hitrost 94,51 Mbit/s proti uporabniku in hitrost 91,70 proti internetu) in glede na dejstvo, da z internetom neprekinjeno komunicirajo hkrati še ostale omrežne naprave, lahko potrdim, da je izkoriščenost razpoložljive 100/100 Mbit/s internetne povezave po implementaciji sedaj skoraj 100-odstotna.

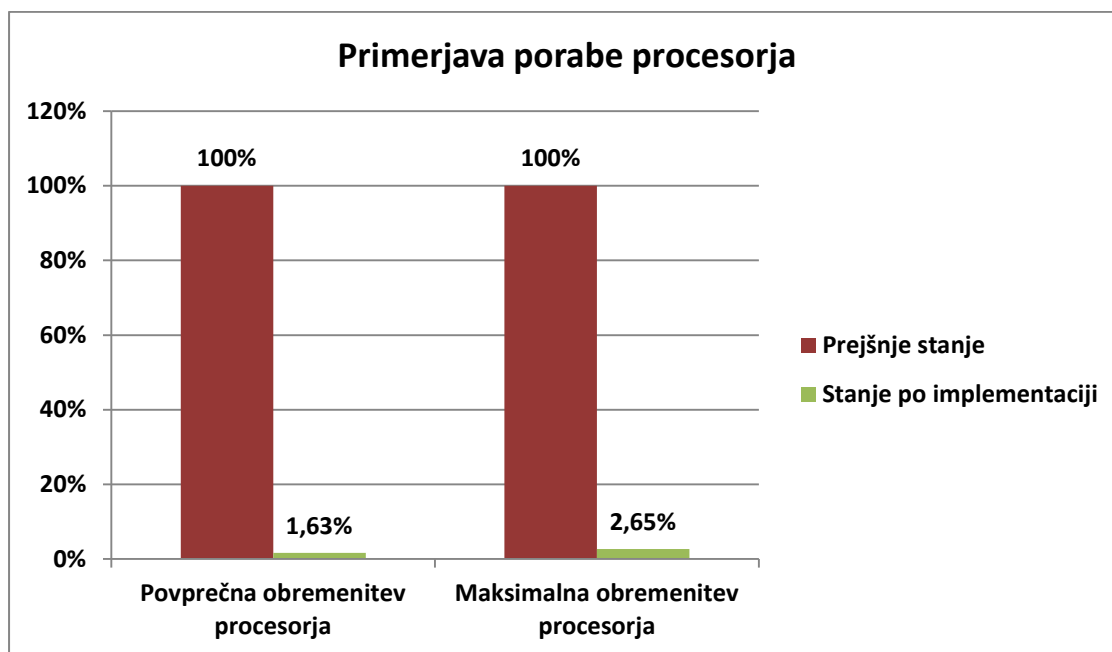
Za zaključek tega poglavja in boljši pregled nad rezultati pa spodaj prilagam tudi nekaj grafov, ki prikazujejo primerjavo rezultatov prejšnjega stanja in stanja po implementaciji robnega strežnika in s tem optimizirano delovanje tega korporativnega omrežja.



Graf 2: Primerjava količin paketov, podatkovnega prometa in hitrosti pretoka (Vir: Meritve in rezultati prejšnjega stanja in stanja po implementaciji robnega strežnika v časovnem intervalu ene ure)



Graf 3: Primerjava minimalnih, maksimalnih in povprečnih zakasnitev (Vir: Meritve in rezultati prejšnjega stanja in stanja po implementaciji robnega strežnika v časovnem intervalu ene ure)



Graf 4: Primerjava povprečnih in maksimalnih obremenitev procesorja (Vir: Meritve in rezultati prejšnjega stanja in stanja po implementaciji robnega strežnika v časovnem intervalu ene ure)

Iz primerjave rezultatov na grafu (Graf 2) lahko razberemo, da je pri skoraj 20-krat večjem številu poslanih in prejetih paketov ter 10-krat večjemu skupnemu podatkovnemu prometu, povprečna hitrost pretoka po implementaciji robnega strežnika 10-krat večja.

Graf 3 služi za primerjavo zakasnitev, kjer so minimalne zakasnitve po implementaciji 40-krat manjše, maksimalne skoraj 9-krat manjše, povprečne zakasnitve pa skoraj 30-krat manjše, kot so bile v prejšnjem stanju v času trajanja meritve (Meritve zakasnitev 1).

Zadnji graf (Graf 4) pa prikazuje primerjavo obremenjenosti procesorja, ki je bila v prejšnjem stanju v času višjih zakasnitev (Meritve zakasnitev 1) konstantno skoraj 100-%, po implementaciji pa povprečno samo 1,63-% in maksimalno zgolj 2,65-%, kljub dosti večji količini paketov in skupnega podatkovnega prometa.

7 Zaključek

Implementirana rešitev se je izkazala za uspešno in učinkovito. Rešil sem več problemov tega omrežja in ga tudi ustrezno optimiziral, ob tem pa sem poskrbel tudi za smernice dodatnih izboljšav, storitev in vlog v prihodnosti (več o tem v nadaljevanju). Med najpomembnejšimi izboljšavami je seveda stabilno in optimalno delovanje implementiranega robnega strežnika in učinkovito delovanje vseh uporabljenih značilnosti programske opreme *pfSense*. Stanje sistemskih sredstev robnega strežnika je tako skoraj nespremenljivo tudi pri večji obremenitvi omrežja. To je posledično precej izboljšalo izkoriščenost internetne povezave, ki je sedaj skoraj 100-odstotna, in tudi delovanje internetnih storitev ter s tem delovanje celotnega korporativnega omrežja, o čemer pričajo vsi podani rezultati testiranj. Uporabljeni predlog odprtokodne programske opreme *pfSense* na robnem strežniku za namen usmerjanja prometa, požarne zaščite, dodeljevanje IP-naslovov in posredovanje domenskih imen je bil za dano omrežje ustrezen. Z ustreznim načrtovanjem, pravilno konfiguracijo, premišljeno definiranimi pravili požarnega zidu in uspešno implementacijo je bilo zadoščeno vsem kriterijem, ki jih to omrežje zahteva. Odpravil pa sem tudi težavo napačnega razreševanja notranjih domenskih imen, tako da sem vlogo DHCP-strežnika z nekaj dodatnimi nastavitvami in popravki dodelil robnemu strežniku. S tem sem notranje omrežje še dodatno optimiziral, ker sem lahko posledično iz omrežja popolnoma odstranil problematičen starejši strežnik, ki je opravljal zgolj to nalogo pred tem. Prav tako je bila z implementirano rešitvijo odpravljena glavna težava zelo pogostih visokih zakasnitev, ki pa so sedaj nekoliko višje zgolj občasno ob večjih obremenitvah pasovne širine. Tako imenovani »vrhunci« oziroma vrhovi (ang. *peaks*) obremenitev razpoložljive pasovne širine so v omrežjih tipičen, a ne preveč zaskrbljujoč pojav.

Prioriteta tega diplomskega dela je bila čim prej rešiti upočasnenost tega omrežja, povečanje izkoristka internetne povezave, hitrosti delovanja internetnih storitev in s tem optimiziranje omrežja. Za to sem moral skrbno načrtovati predlagani robni strežnik, spoznati njegovo arhitekturo, ga ustrezno pripraviti in implementirati v omrežje podjetja ter hkrati poskrbeti za varnost omrežja in vseh omrežnih naprav. Implementirani robni strežnik, dodeljene vloge in uporabljene funkcionalnosti zadoščajo vsem potrebam, ki jih danes zahteva to omrežje. Kljub temu pa bo v prihodnje treba implementirati tudi nekatere dodatne funkcionalnosti, ki jih ponuja izbrana rešitev *pfSense* in ki sem jih že omenil v poglavju nabora orodij in dodatnih

funkcionalnosti. Z njimi bo mogoče še dodatno »nadgraditi« implementirani robni strežnik, poskrbeti za poostreno varnost komunikacije in podatkovnega prometa in za še boljše optimizacijo omrežja. Pri tem so uporabljene in dodatne značilnosti zaradi odprte kode na voljo zastonj, v primerjavi z ostalimi komercialnimi požarnimi zidovi, ki so pogosto za te namene cenovno zelo dragi. Tako bi lahko zgoraj omenjene vrhove obremenitev pasovne širine in posledično občasno nekoliko povišane zakasnitve odpravil ali pa jih še dodatno zmanjšal z uporabo funkcionalnosti oblikovanja prometa in ustrezno definiranimi profili prometa. S tem bi na robnem strežniku lahko v celoti omejil oziroma zmanjšal razpoložljivo pasovno širino določenim vrstam prometa oziroma paketom. Tako bi lahko zmanjšal hitrosti prenosov – recimo FTP-prenosom, prenosom posodobitev Microsoft Windows itd., kjer maksimalna hitrost in minimalni čas prenosa nista bistvenega pomena. Z ustreznimi profili pa bi definiral tudi prioritetni promet. Tega bi tako lahko definiral za e-poštne povezave in protokole, ki se pri tem uporabljajo (POP3, IMAP, SMTP), in za spletno brskanje (HTTP- in HTTPS-promet) ter promet oddaljenega namizja (TCP 3389), pri katerih sta čas in hitrost bistvenega pomena. V omrežju podjetja bo treba v prihodnosti uporabiti tudi že omenjeno funkcionalnost programske opreme *pfSense*, ki bo omogočala uporabo navideznih zasebnih omrežij in varen dostop do korporativnega omrežja ter internih omrežnih sredstev od drugje. Trenutno je dostop oddaljenim organizacijskim enotam in zaposlenim omogočen prek povezav z oddaljenim namizjem, ki pa predvsem zaradi nešifriranega prometa ni najboljša rešitev. Smiselno bi bilo robnemu strežniku dodeliti vlogo spletnega posrednika s predpomnilnikom z omenjenim dodatnim paketom *squid*. Takšen posrednik bi bil v tem korporativnem omrežju ustrezen predvsem zaradi večjega števila uporabnikov, ki dnevno obiskujejo tudi iste spletne strani ali pa prenašajo iste vsebine. S tem bi omrežje še dodatno optimiziral, saj zaposleni na enakih področjih (enotah) pogosto dostopajo in uporabljajo iste informacije. Prav tako bi s tem »olajšal« oziroma razbremenil internetno povezavo tudi pri enakih prenosih raznoraznih sistemskih (Windows, Linux itd.) in programskih posodobitev (protivirusni programi in definicije, Adobe, Java itd.). Te bi recimo kot prvi prenesel eden od uporabnikov oziroma računalnikov, za vse ostale pa bi bile te posodobitve na voljo lokalno preko posredniškega strežnika (robnega strežnika). Ob tem pa je mogoče namestiti in uporabiti tudi *squidGuard*, s pomočjo katerega je mogoče enostavno spletno filtriranje in blokiranje spletnih strani. V t. i. črno listo (ang. *blacklist*) bi lahko tako vnesel naslove raznoraznih spletnih strani, za katere interni pravilnik prepoveduje uporabo. Pri vsem tem pa

bi bila smiselna uporaba tudi protivirusnega paketa *HAVP-antivirus*, s pomočjo katerega bi robni strežnik lahko deloval tudi kot spletni protivirusni posrednik. Čeprav imajo vsi računalniki v omrežju nameščene protivirusne programe, bi bilo ustrezno imeti dodatno protivirusno zaščito tudi na samem vhodu v omrežje. Prav tako pa bi bilo v prihodnje smotno razmišljati v smeri še dodatne poostrene varnosti in dodati tudi funkcionalnost zaznavanja in preprečevanja vdorov.

Literatura

- [1] Cisco VNI, „The Zettabyte Era—Trends and Analysis,“ 2015. [Elektronski]. Dosegljivo: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html. [Dostopano: 7. 5. 2016].
- [2] Studytonight, „Types of Network Topology,“ [Elektronski]. Dosegljivo: <http://www.studytonight.com/computer-networks/network-topology-types>. [Dostopano: 19. 3. 2016].
- [3] Allied Telesyn, „AT-MC102XL,“ Avgust 2010. [Elektronski]. Dosegljivo: <https://www.alliedtelesis.com/products/mc102xl>. [Dostopano: 12. 4. 2016].
- [4] Jennifer Jabbusch, „9 Immutable Laws of Network Design,“ 9 17 2013. [Elektronski]. Dosegljivo: <http://www.networkcomputing.com/networking/9-immutable-laws-network-design/1981576846>. [Dostopano: 9. 3. 2016].
- [5] Techopedia, „Keep It Simple Stupid Principle (KISS Principle),“ [Elektronski]. Dosegljivo: <https://www.techopedia.com/definition/20262/keep-it-simple-stupid-principle-kiss-principle>. [Dostopano: 14. 3. 2016].
- [6] Intel Corporation, „Intel® Hyper-Threading Technology,“ [Elektronski]. Dosegljivo: <http://www.intel.com/content/www/us/en/architecture-and-technology/hyper-threading/hyper-threading-technology.html>. [Dostopano: 28. 3. 2016].
- [7] pfSense, „Does pfSense support SMP (multi-processor and/or core) systems,“ [Elektronski]. Dosegljivo: https://doc.pfsense.org/index.php/Does_pfSense_support_SMP_%28multi-processor_and/or_core%29_systems. [Dostopano: 28. 3. 2016].
- [8] Margaret Rouse, „TCP/IP offload engine (TOE),“ 10 2008. [Elektronski]. Dosegljivo: <http://searchnetworking.techtarget.com/definition/TCP-IP-offload-engine>. [Dostopano: 29. 3. 2016].
- [9] G.S. Jackson, „OPPOSINGVIEWS,“ [Elektronski]. Dosegljivo: <http://science.opposingviews.com/imap-vs-imap-ssl-3203.html>. [Dostopano: 21. 3. 2016].
- [10] pfSense, „pfSense Overview,“ [Elektronski]. Dosegljivo: <https://www.pfsense.org/about-pfsense/>. [Dostopano: 2. 4. 2016].
- [11] m0n0wall, „m0n0wall,“ [Elektronski]. Dosegljivo: <http://m0n0.ch/wall/index.php>. [Dostopano: 2. 4. 2016].

- [12] Palo Alto Networks, „What is a firewall?,“ [Elektronski]. Dosegljivo: <https://www.paloaltonetworks.com/documentation/glossary/what-is-a-firewall>. [Dostopano: 3. 4. 2016].
- [13] pfSense, „Firewall Rule Basics,“ [Elektronski]. Dosegljivo: https://doc.pfsense.org/index.php/Firewall_Rule_Basics. [Dostopano: 3. 4. 2016].
- [14] pfSense, „Getting Started With pfSense Software,“ [Elektronski]. Dosegljivo: <https://www.pfsense.org/getting-started/>. [Dostopano: 3. 4. 2016].
- [15] pfSense, „Features List,“ [Elektronski]. Dosegljivo: https://doc.pfsense.org/index.php/Features_List. [Dostopano: 3. 4. 2016].
- [16] Wikipedia, „Traffic Shaping,“ [Elektronski]. Dosegljivo: https://en.wikipedia.org/wiki/Traffic_shaping. [Dostopano: 18. 4. 2016].
- [17] Cisco, „Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting,“ [Elektronski]. Dosegljivo: <http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html>. [Dostopano: 18. 4. 2016].
- [18] Andrew Mason, „Overview of VPNs and VPN Technologies,“ Januar 2002. [Elektronski]. Dosegljivo: <http://www.ciscopress.com/articles/article.asp?p=24833>. [Dostopano: 18. 4. 2016].
- [19] Cisco, „How Virtual Private Networks Work,“ Oktober 2008. [Elektronski]. Dosegljivo: <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>. [Dostopano: 19. 4. 2016].
- [20] Marc Grote, „Microsoft Forefront TMG and UAG – A feature comparison,“ 1 11 2011. [Elektronski]. Dosegljivo: <http://www.isaserver.org/articles-tutorials/configuration-general/Microsoft-Forefront-TMG-UAG-feature-comparison.html>. [Dostopano: 25. 3. 2016].
- [21] Microsoft, „Microsoft Support Lifecycle,“ [Elektronski]. Dosegljivo: <https://support.microsoft.com/en-us/lifecycle?C2=12300>. [Dostopano: 25. 3. 2015].
- [22] Jaapwesselius, „TMG 2010 Console fails on startup,“ September 2012. [Elektronski]. Dosegljivo: <http://jaapwesselius.com/2012/09/09/tmg-2010-console-fails-on-startup/>. [Dostopano: 25. 3. 2016].
- [23] Microsoft, „TMG Management Console Script Error,“ 8 4 2011. [Elektronski]. Dosegljivo: <https://social.technet.microsoft.com/Forums/forefront/en-US/94e2884e-ce02-4d7d-ad53-98e1862d692a/tmg-management-console-script-error?forum=Forefrontedgegeneral>. [Dostopano: 25. 3. 2016].
- [24] Sophos, „Sophos,“ [Elektronski]. Dosegljivo: <http://sophos.si/>. [Dostopano: 26. 3. 2016].

- [25] COKS, „Vse o Odprti kodi - COKS - Center odprte kode Slovenije,“ 11 2011. [Elektronski]. Dosegljivo: http://www.coks.si/index.php5/Vse_o_Odprti_kodi. [Dostopano: 27. 3. 2016].
- [26] OPNsense, „About OPNsense,“ [Elektronski]. Dosegljivo: <https://opnsense.org/about/about-opnsense/>. [Dostopano: 27. 3. 2016].
- [27] OPNsense, „OPNsense Dashboard,“ [Elektronski]. Dosegljivo: <https://opnsense.org/wp-content/uploads/2014/12/Dashboard.png>. [Dostopano: 13. 4. 2016].
- [28] Robin Gill, „public ip resolves externally but not internally,“ Februar 2012. [Elektronski]. Dosegljivo: <http://serverfault.com/questions/361564/public-ip-resolves-externally-but-not-internally>. [Dostopano: 27. 4. 2016].