Konfiguriranje i sigurnost lokalne računalne mreže i servisa

Vrančić, Arian

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

Arian Vrančić

Konfiguriranje i sigurnost lokalne računalne mreže i servisa

Završni rad

Pula, rujan, 2023.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

Arian Vrančić

Konfiguriranje i sigurnost lokalne računalne mreže i servisa

Završni rad

JMBAG: 0303094641, redoviti student

Studijski smjer: Informatika

Kolegij: Mrežni sustavi

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: izv. prof. dr. sc. Siniša Sovilj Dalibor Fonović (sumentor)

Pula, rujan, 2023.

SADRŽAJ

1. UVOD

Lokalna računalna mreža je sustav koji povezuje mrežne uređaje koji obrađuju podatke i komunikacijske uređaje u jednu cjelinu, bilo to na razini države, grada ili zgrade.

U današnjem dobu potreba za umrežavanjem je u stalnom porastu zbog sve veće razmjene podataka između korisnika. Kako bi korisnicima uštedjeli vrijeme na razmjeni podataka izmišljeni su mnogi uređaji (računala, pisači, skeneri) koji olakšavaju svakodnevni posao, a da bi ti uređaji olakšavali razmjenu podataka potrebno ih je povezati u jednu računalnu mrežu putem koje će dijeliti podatke između korisnika.

Računalne mreže potrebno je pravilno konfigurirati, povezati i nadzirati kako bi ispravno obavljale svoje zadatke u razmjeni podataka. Cilj svake računalne mreže je pravilno upravljanje i održavanje što ju onda čini pouzdanom i sigurnom. Administrator mreže je zadužen za upravljanje i održavanje računalne mreže.

Računalne mreže korisnicima pružaju lakše povezivanje i razmjenjivanje podataka između računala u mreži. Računalima i podacima iz računalne mreže moguće je pristupiti s bilo koje lokacije koja posjeduje internetsku vezu.

Računalne mreže danas su pogođene velikim brojem napada koji prijete njihovoj sigurnosti, te sigurnosti podataka. Veliki broj neovlaštenih osoba pristupa osjetljivim podacima i širi ih dalje. Kako bi se pravilno i na vrijeme zaštitili potrebno je planirati zaštitu računalne mreže i ispitati sve njezine ranjive točke.

Ovaj rad ima cilj objasniti kako pravilno konfigurirati računalnu mrežu i osigurati njezinu sigurnost od mogućih napada. Korisnike je potrebno pravilno obučiti za rad u mreži kako bi umanjili mogućnost napada. Cilj ovog rada je objasniti korak po korak konfiguraciju, sigurnost i rad lokalne računalne mreže.

2. ANALIZIRANJE ZAHTJEVA RADA RAČUNALNE MREŽE

Računalne mreže služe za povezivanje računala i drugih uređaja kako bi se korisnicima olakšala komunikacija i razmjena podataka olakšalo u komunikaciji i razmjeni podataka. Računalne mreže čine dva ili više međusobno povezana računala koja dijele podatke povezanih računala koji dijele podatke. Kada računala mogu razmjenjivati informacije tada se smatraju povezanim.

Danas imamo mnogo mogućnosti povezivanja u mrežu, no postoje dvije osnovne: žičane i bežične veze. Žičane veze su stari klasični način povezivanja putem kabela u telefonske linije, a bežične veze su način povezivanja putem elektronskih magnetskih valova kao što je WLAN[11], 3G[2], 4G[3] itd[4].

2.1 Upravljanje i održavanje računalnih mreža

Upravljanje mrežom znači da je računalna mreža pravilno konfigurirana, povezana i pravilno nadzirana. Upravljanje mrežom u užem djelu odnosi se na upravljanje komunikacijskom mrežom, a u širem odnosi se na upravljanje krajnjih sistema koji su spojeni na mrežu i proces koji se izvode na mreži te brigu o podacima i korisnicima koji ju koriste. Administrator mreže je zadužen za upravljanje i održavanje.

Mrežna oprema koja se nalazi na nižim mrežnim modelima najčešće ne traži konfiguriranje i upravljanje, već ju je dovoljno spojiti u mrežu. Mrežnu opremu dijelimo na dva načina: aktivna mrežna oprema i pasivna mrežna oprema. Aktivnom mrežnom opremom nazivamo sve elektroničke uređaje koji primaju i šalju podatke unutar mreže, dok pasivnom mrežnom opremom zovemo žičani sustavi koji povezuju aktivnu opremu.

Računalne mreže mogu sadržavati mnogo računala i uređaja, a kako bi ih međusobno raspoznali i razlikovali koristimo se adresama, bez obzira na veličinu

[1] WLAN-Bežična lokalna mreža.

[2] 3G- Treća generacija mobilne telefonije.

[3] 4G- četvrta generacija mobilne telefonije.

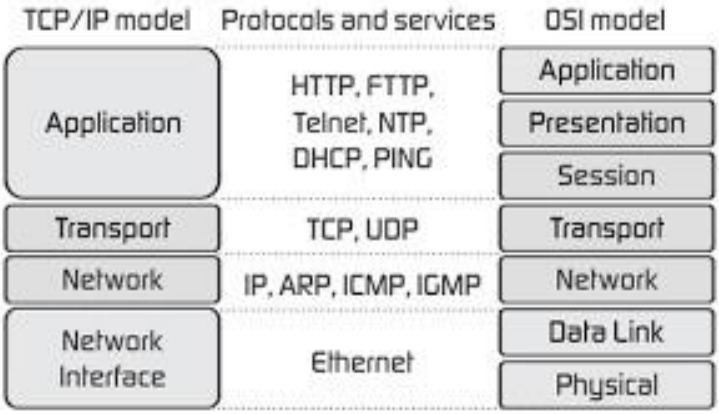
[4] Itd.- i tako dalje.

mreže. Danas računalna mreža Internet funkcionira na TCP/IP protokolu. Uređaje povezane u mreži adresiramo pomoću IP adresa i naziva.

Više razine mrežnih modela koriste korisničke programe instalirane u operacijskim sustavima za pravilno konfiguriranje i upravljanje mrežom. Računalne mreže su većinom zasnovane na modelu klijent-poslužitelj. Poslužitelj je program koji je instaliran na računalu i izvršava zadatke od strane korisnika, on je ključni dio modela klijent-poslužitelj. Prema ovome modelu zadaci koji se izvršavaju na računalu raspoređuju se na poslužitelja koji nam pruža usluge ili podatke i na korisnika koji podatke ili usluge traži. Ovakav model traži vezu između klijenta i poslužitelja.

2.2 Mrežna arhitektura interneta

Najraširenij opis arhitekture mreže je OSI model, OSI model opisuje sklopovlje, programe, software i protokole kod računalnih mreža. Većina proizvođača i stručnjaka koristi ga kod rada s mrežama. OSI model je podijeljen na sedam logičkih razina. Danas se sve više računalnih mreža okreće ka TCP/IP skupu protokola zbog jednostavno definiranih adresa uređaja u mreži. Njegov naziv ima dva najčešća korištena protokola – TCP (*engl. Transmission Control Protocol*) i IP (*engl. Internet Protocol*). TCP/IP model ima četiri razine (Slika1.).



Slika 1. Usporedba TCP/IP modela i OSI modela

Kod TCP/IP modela, podaci se prosljeđuju, kao i kod OSI modela, od više razine prema nižoj razini kad se šalje u mrežu, a kod primanja u mrežu od nižih prema višim razinama.

Najniža razina kod TCP/IP modela izvršava prve dvije razine OSI modela i zadužena je za međusobnu komunikaciju između dva uređaja u mreži. Protokoli prve razine TCP/IP modela su:

- Ethernet protokol
- SLIP (*engl. Serial Line Internet Protocol*)
- PPP (*engl. Point to Point Protocol*)

Mrežna razina kod TCP/IP modela služi za uspostavljanje logičkih veza između dva uređaja koji međusobno komuniciraju. Na mrežnoj razini IP je osnovni protokol, a uređaji se razlikuju putem 32-bitnih IP adresa koje sadrže mrežni i računalni broj. Mrežna razina je zaslužena za prijenos podataka, to jest ona prihvaća pakete sa pristupne razine i predaje ih prijenosnoj razini. Na mrežnoj razini osim IP-a imamo i ICMP (*engl. Internet Control Message Protocol*), ARP (*engl. Address Resolution Protocol*), RARP (*engl. Reverse Address Resolution Protocol*) i DHCP (*engl. Dynamic Host Configuration Protocol*).

Prijenosna razina je zadužena za prijenos paketa između dvije krajnje točke u mreži. Na prijenosnoj razini vrši se kontrola toka i kontrola pogrešaka. Mreža razina i aplikacijska razina povezane su prijenosnom razinom. Povezane su tako da mrežna razina u zaglavlju sadrži podatke kojem protokolu na prijenosnoj razini mora dati podatke, dok prijenosna razina šalje podatke točno onoj usluzi na aplikacijskoj razini kojoj su podaci bili namijenjeni. Prijenos podataka ove razine vrši se uspostavljanjem logičkog kanala ili bez uspostavljanja logičkog kanala.

Uspostava logičkog kanala donosi i osigurava slanje i isporuku podataka uz minimalne pogreške i minimalno gubljenje. Ovu metoda se koristi kod važnih podataka jer dobivamo potvrdu o pravilnoj isporuci. Prijenos podataka bez uspostave logičkog kanala koristi se kod prijenosa podataka koji podnose gubitke. Na prijenosnoj razini postoje dva značajna protokola: TCP (*engl. Transmission Control Protocol*) i UDP (*engl. User Datagram Prtotocol*).

HTTP[5] je glavni i najčešći protokol prijenosa podataka na internetu i zadužen je za komunikaciju između poslužitelja i klijenta. HTTP prvo uspostavi TCP vezu s poslužiteljem na portu i prenosi tražene podatke klijentu. SMTP (*engl. Simple Mail Transfer Protocol*) protokol koristi se kod prijenosa elektroničke pošte,

sadrži sve informacije kod slanja i primanja pošte računalu u lokalnoj mreži i prosljeđuje lokalnim programima za obradu pošte. Telnet protokol koristi se kod uspostavljanja dvosmjernog 8-bitnog kanala između dva računala u mreži. Telnet ime protokola potječe od engleskog naziva TELephone i NETwork. SSH (*engl. Secure Shell*) protokol namijenjen uspostavi sigurnog komunikacijskog kanala između dva računala. SSH protokol koristi metodu enkripcije koja omogućuje sigurnosni prijenos podataka računala u mreži.

UDP (*engl. User Datagram Protocol*) se koristi kod protokola druge skupine koji izvršavaju zadatke neovisno o aplikacijama i bez znanja korisnika, a bez kojih mreža ne može funkcionirati. DNS (*engl. Domain Name Service*) je sustav koji je hijerarhijsko raspoređen za imenovanje računala, servisa ili bilo čega spojenog na mrežu. DNS prevodi domenska imena u numeričke IP adrese koje služe za lakše pronalaženje bilo kojeg računalnog servisa u svijetu.

DHCP (*engl. Dynamic Host Configuration Protocol*) je protokol kojeg koriste mrežna računala za dodjeljivanje IP adresa i ostalih postavki u mreži. Sve postavke sam dodjeljuje, kao što su Gateway[6], subnet maska, te nije potrebno ručno unošenje tih postavki za računalnu mrežu. DHCP vodi brigu o tome da u mreži ne postoje dvije iste IP adrese i da ne dolazi do sukoba unutar mreže. VoIP (engl. Voice over Internet Protocol) je komunikacijska tehnologija kojom se preko internetske mreže prenosi zvuk. Ovaj protokol se pojavio razvojem širokopojasnog interneta i omogućuje besplatno telefoniranje putem interneta.

2.3 Organizacija lokalne mreže

Svaka lokalna mreža mora biti organizirana od samih početaka stvaranje mreže kako bi mogla nesmetano funkcionirati i isporučiti sve tražene podatke klijentu. Svaka mreža sastoji se od računala i poslužitelja. Na početku moramo napraviti plan prostorije, zgrade ili ustanove, te zatim izraditi popis koliko će nam računala i opreme za spajanje u mrežu biti potrebno. Nakon izrade detaljnog plana kreće se u opremanje i puštanje mreže u rad. Osnovni tipovi koje koristimo kod povezivanja su: zvijezda, sabirnica i prsten.

[5] HTTP- protokol za objavljivanje i prezentiranje HTML dokumenata to jest WEB stranica.
[6] Gateway- protokol za razmjenu informacija sa drugim gateway-ima na brzi i pouzdan način.

2.3.1 Spajanje računala u mrežu

Svako računalo koje se priključuje u mrežu zahtjeva konfiguraciju kako bi se povezalo u mreži. Računala prije povezivanja u mrežu moraju posjedovati mrežne kartice. Proizvođači računala najčešće ugrađuju mrežne kartice serijski u računala, ali postoje iznimke. Većina mrežnih kartica koje su serijski ugrađene u računala ne podržavaju velika opterećenja i brzine zato zahtjevniji korisnici ugrađuju mrežne kartice s jačim performansama kako bi neometano radili. Svaka mrežna kartica ima svoju MAC adresu. Kod većine mrežnih kartica sve postavke se podešavaju automatski i nije ih potrebno ručno podešavati osim ako korisnik želi izmijeniti automatske postavke.

Operacijski sustavi danas imaju već ugrađene driver-e za mrežne kartice, a ukoliko ih nema onda se dodatno instaliraju pomoću CD-a koji je priložen uz mrežnu karticu ili operacijski sustav ponudi automatsko preuzimanje i instaliranje potrebnog driver-a. Operacijski sustavi podržavaju sve protokole potrebne za rad mreže.

Korisnici koji žele samostalno podesiti postavke kao što su IP adresa, subnet maska i ostale parametre na Windows operacijskim sustavima to čine ulaskom u Control Panel[7] i ulaskom u rubriku Network. Korisnici UNIX operacijskih sustava moraju urediti par datoteka i upisati valjane parametre koji se mogu razlikovati kod svakog izdanja

UNIX-a. Računalo je povezano u mrežu kad je mrežna kartica pravilno konfigurirana, ima odgovarajuće parametre i spojena kabelom na usmjerivač.

Svako računalo koje je spojeno u mrežu mora biti evidentirano i dokumentirano. Evidencija je potrebna kako bi se imao uvid u stanje mreže, njene resurse i nedostatke kako bi se moglo planirati nadograđivanje mreže. Dokumentiranje je potrebno kod moguće promjene administratora kako bi novi administrator mogao proučiti mrežu i njen plan, kao npr. gdje se nalaze računala i koja je njihova adresa, gdje se nalaze usmjerivači itd.

Lokalna računalna mreža (*engl. Local Area Network*) povezuje računala i ostale uređaje na malim udaljenostima. LAN mreža pomaže klijentima u lakšoj

[7] Control Panel- Upravljačka ploča na Windows operativnim sustavima

komunikaciji između ostalih računala i uređaja kao što su printeri i skeneri na malim udaljenostima. LAN mreža podržava velike brzine prijenosa podataka.

WAN (*engl. Wide Area Network*) radi na većim udaljenostima od LAN mreže. WAN povezuje računala na velikim udaljenostima koji nisu spojeni u istoj mreži niti se nalaze na malim udaljenostima. WAN povezivanje se izvršava uz optičke kabele i satelite.

2.4 Konfiguracija usmjerivača

Konfiguracija usmjerivača jako je bitna kako bi mreža funkcionirala. Zato konfiguracija mora biti isplanirana i pravilno odrađena. Kada je konfiguracija pravilno odrađena mreža će ne ometano izvršavati svoje zadatke. Prilikom konfiguracije mreže potrebno je voditi i brigu o sigurnosti kako bi se spriječili napadi krađa podataka. Privatni korisnici

se najčešće odluče za automatsko dodjeljivanje postavaka. Kada se odabere automatsko dodjeljivanje postavki usmjerivač će se podesiti automatski i biti spreman za rad u mreži. Poslovni korisnici ne koriste automatsko dodjeljivanje postavki već odrede administratora mreže koji vodi brigu o sigurnosti i samoj mreži. Poslovnim korisnicima je bitno da se usmjerivači pravilno konfiguriraju kako bi smanjili opasnost od napada i krađe povjerljivih podataka.

Kod konfiguracije usmjerivača postoji par važnih stavki koje je potrebno podesiti kako bi mreža funkcionirala i bila zaštićena. Neke od važnih stavki su: filtriranje MAC adresa, sigurnost, DHCP itd.

Filtriranje MAC adresa omogućava korisniku da konfigurira popis MAC adresa za pristup usmjerivaču te pristup ograničiti na uređaje s adresama koje se nalaze na popisu. Uređaji i računala čija MAC adresa nije na popisu neće se moći povezati u mrežu. MAC adrese je jednostavno promijeniti stoga se ne treba pouzdati u taj način onemogućavanja pristupa neovlaštenim osobama mreži.

Postavkama sigurnosti kontrolira se pristup mreži određuje se razina zaštite privatnosti, a određuje se i vrsta autorizacije i enkripcije koju koristi usmjerivač.

WPA[8]2 Personal enkripcija najjača je zaštita WIFI-a i preporučuje se za sve upotrebe. Kod WPA2 Personal enkripcije potrebno je staviti i jaku lozinku koju nije lako probiti. Neki usmjerivači ne podržavaju WPA2 Personal enkripciju i kod njih je potrebno odabrati malo slabiju WPA/WPA2 enkripciju.

DHCP protokol koristi se za dodjeljivanje automatskih adresa u mreži koji služe za prepoznavanje uređaja unutar mreže. Kada svaki uređaj dobije svoju adresu onda pomoću nje komunicira s računalima na internetu. Na mreži se nalazi samo jedan DHCP poslužitelj. DHCP poslužitelj je ugrađen u usmjerivaču.

[8] WPA-engl. Wi-Fi Protected Access

3. PRIJETNJE RAČUNALNIM MREŽAMA

Korisnici povezivanjem računala u mrežu imaju mogućnost pristupa informacijama na udaljenim računalima koji se ne nalaze u lokalnoj računalnoj mreži. Većina računala nema administratora, tada je nadzor vlasnika i sigurnosti zanemarena. Umreženi sustav puno je teže zaštiti od mogućih napada od onog sustava koji nije umrežen. Cilj zaštite sustava je da se osigura njegova funkcionalnost i pouzdanost podataka. Zaštita nekad može utjecati na dostupnost i kvalitetu podataka i najčešće je dogovor s klijentom između zaštite osobnih podataka i slobode pristupa podacima.

Kada se stvara plan zašite sustava, najčešće se temelji na poznatim prijetnjama i prijedlozima rješenja problema. Zaštita čuva cijeli sustav od osoba koji su ovlašteni ili čak neovlašteni korisnici resursa u mreži. Sustav je zaštićen i od novih, nedovoljno upućenih korisnika koji također mogu ugroziti rad sustava. Kada govorimo o zaštiti sustava onda se u to ubraja mrežna oprema, poslužitelj, podaci, korisnici i radne stanice.

Model klijent-poslužitelj važna je stavka u planiranju zaštite mrežnih usluga. Korisnici traže usluge unutar mreže ili izvan nje, a poslužitelj je stalno spojen u mrežu i dostavlja klijentu traženu uslugu. Poslužitelji su glavni i prvi cilj u zaštiti mreže jer oni čuvaju podatke koje je potrebno zaštiti. Neki od ciljeva zaštite sustava su:

- promjena ili brisanje podataka,
- onemogućavanje usluga, • neovlašten pristup podacima,
- neovlašten pristup sustavu.

Projektiranje zaštite mreže može se znatno ubrzati ako se znaju načini na koje bi sustav mogao biti ugrožen.

3.1 Planiranje prijetnji

Planiranje prijetnji danas je znatno olakšano raznim tehnikama. Jedna od tehnika je i modeliranje prijetnji (*engl. Threat modeling*) koja se koristi prilikom identificiranja prijetnji, ranjivosti sustava i kod protumjera. Modeliranje olakšava pronalaženje mogućih prijetnji, definiranje ciljeva sigurnosti, ranjivosti sustava i

potrebnih protumjera u zaštiti sustava. Za najbolju zaštitu mreže prvo je potrebno poznavati i ocijeniti svaku prijetnju, te zatim poduzeti odgovarajuću mjeru.

Modeliranje prijetnji temelji se na tome da sustav ima vrijedne podatke i resurse koji su izloženi napadima i potrebno ih je zaštiti. Podaci i resursi u sustavu imaju mnogo točaka na kojima su osjetljivi i lako ih je napasti zato je potrebno imati protumjere koje će brzo odgovoriti na svaki mogući napad.

Planiranje zaštite prva je i bitna činjenica u planiranju svake mreže. Prije samih početaka stvaranja mreže i konfiguriranja potrebno je razviti sustav zaštite. Sustav zaštite vodi brigu i odgovoran je za zaštitu resursa sustava. Osobe koje rade na zaštiti sustava i planiranju prijetnji moraju biti obučeni za rad s takvim osjetljivim stvarima kao što je zaštita. U svijetu postoji mnogo tehnika u zaštiti sustava no bitno je imati protumjeru koja će spriječiti napada na sustav i njegove resurse.

3.1.1 Pristupi planiranju prijetnji

Kada se govori o pristupanju prijetnjama potrebno je prilikom planiranja razviti plan kako prijetnju procijeniti i pristupiti joj.

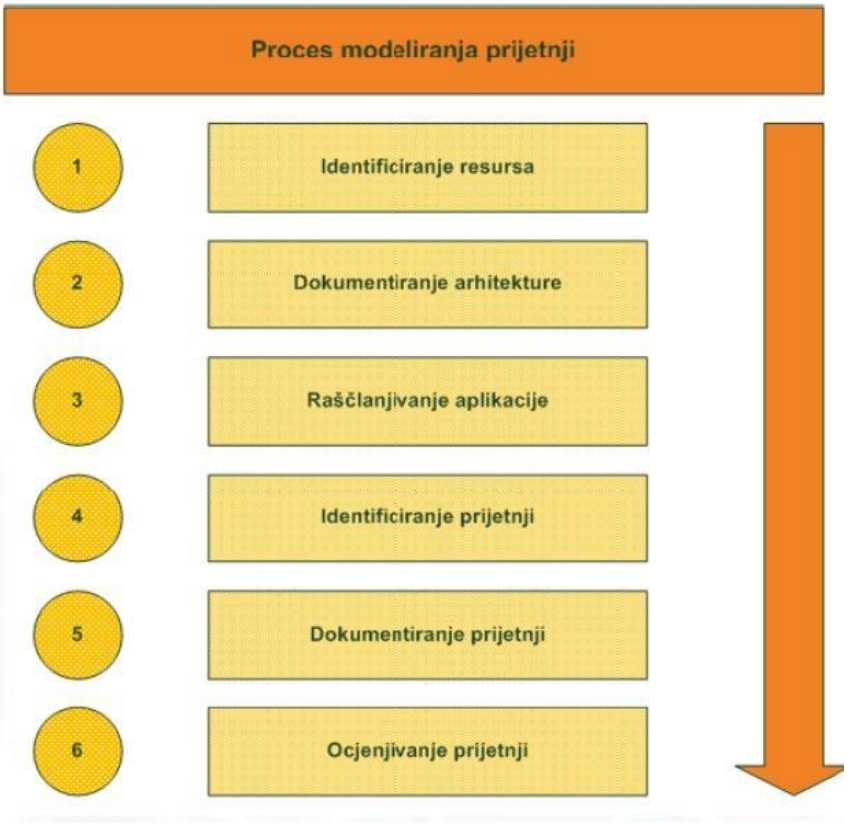
Pristupi planiranju prijetnji koje se najčešće događaju:

- pristup prema napadaču koji se odnosi na napadača i procjenu njegovih ciljeva i načina na koje bi mogao napasti sustav. Pristup kreće od one točke gdje je napadač ušao u sustav,
- pristup prema programskom rješenju koji se zove još i pristup usredotočen na sustav i dizajn. Ovaj pristup kreće od dizajniranja sustava i ide kroz model sustava u potrazi za napadima,
- pristup prema resursima kreće od resursa sustava, kao što su osjetljivi podaci,
- pristup prema obrani služi za procjenjivanje slabih točki u sustavu.

3.2 Principi planiranja prijetnji

Planiranje prijetnji nije proces kroz koji se prolazi samo jedanput prilikom stvaranja mreže. Proces planiranja prijetnji započinje u ranim počecima prilikom razvoja aplikacije i traje kroz cijeli životni vijek aplikacije. Proces planiranja prijetnji potrebno je stvarati i nadograđivati zajedno uz razvoj aplikacije jer

aplikacije je potrebno stalno nadograđivati i prilagođavati korisnicima. Proces planiranja prijetnji ima šest faza koje su prikazane na slici 2.



Izvor: CIS

Slika 2. Proces planiranja prijetnji kroz šest faza

3.2.1 Identificiranje resursa

Prvi korak u procesu planiranja prijetnji je identificiranje resursa koje treba zaštiti. Kad je riječ o resursima to je širok pojam u kojeg spadaju i povjerljivi podaci koji zahtijevaju najveću zaštitu. Povjerljivi podaci su osobni podaci, zaporke, informacije o kreditnim karticama i tako dalje.

3.2.2 Dokumentiranje arhitekture

Sljedeći korak je dokumentiranje arhitekture. Dokumentiranje arhitekture podrazumijeva dokumentiranje arhitekture aplikacije, njene funkcije i tehnologija kojim je aplikacija stvorena. Druga faza zahtijeva da se obave tri zadatka, a to

su: identificiranje funkcija aplikacije, stvaranje dijagrama arhitekture aplikacije i identificiranje tehnologija kojima je aplikacija stvorena.

3.2.3 Raščlanjivanje aplikacije

Treća faza je raščlanjivanje aplikacije u kojoj aplikaciju rastavljamo na dijelove, stvaramo sigurnosni profil koji se temelji na napadima. U ovoj fazi imamo 5 zadataka kroz koje moramo proći: identificiranje granice povjerenja, identificiranje protoka podataka, identificiranje ulaznih točaka, identificiranje privilegiranog koda i dokumentiranje sigurnosnog profila.

3.2.4 Identificiranje prijetnji

Četvrta faza je identificiranje prijetnji. Identificiranje prijetnji veoma je važno kako bi mogli zaštiti sustav od napada. Kod identificiranja prijetnji imamo dva pristupa, to je Stride i kategoriziran popis prijetnji. Stride je pristup koji radi na principu da otkriva moguće ciljeve napadača. Kategorizirani popis prijetnji pristupa uz popis prijetnji koje se često događaju u mrežnoj i aplikacijskoj kategoriji. Kod identificiranja prijetnji imamo tri zadatka: identificiranje mrežnih prijetnji, identificiranje domaćinskih prijetnji i identificiranje aplikacijskih prijetnji.

3.2.5 Dokumentiranje prijetnji

Svaku prijetnju potrebno je dokumentirati kako bi imali sve potrebne informacije o njoj.

Dokumentiranje pomaže u stvaranju i poboljšavanju plana zaštite. U dokumentiranju prijetnji spremamo atribute i mete prijetnje.

3.2.6 Ocjenjivanje prijetnji

Zadnja faza je ocjenjivanje prijetnji. Nakon što smo prošli kroz sve faze dolazimo i do ove. U ovoj fazi imamo popis prijetnji za aplikaciju koju smo promatrali. Prijetnje se ocjenjuju temeljem rizika koji nose. Dobivamo listu prijetnji i na samom vrhu svrstane su prijetnje koje donose najviše rizika i mogu napraviti velike štete. Na drugoj polovici liste nalaze se prijetnje koje ne donose velike rizike i mogu napraviti male štete. Prijetnje se ocjenjuju skalom od 1 do 3 i na

kraju se dobiva skala od 5 do 15. Pod visoke rizike spadaju rizici od 12 do 15, srednji rizik od 8 do 11 i niski rizik od 5 do 7.

3.3 Brute Force

Brute Force napad jedan je od prijetnji računalnim mrežama. Ovaj napad je jednostavan za implementaciju i veoma uspješan. Koristi se za probijanje lozinki i raznih enkripcija. Uvijek pronalazi rješenje ako postoji. Vrijeme i resursi koji su potrebni za rješavanje problema rastu s brojem mogućih kombinacija za rješenje. Kada korisnik želi probiti lozinku koristeći Brute Force napad onda korisnik zadaje listu moguće kombinacije i duljinu zaporke nakon čega započinje probijanje. Ovaj proces često dugo traje jer ima bezbroj kombinacija koje treba pokušati da bi pronašlo se rješenje. Što je lozinka ili enkripcija dulja to se vrijeme povečava.

3.4 SQL injection

SQL (*engl. Structured Query Language*) je računalni jezik koji se koristi za izradu, ažuriranje i brisanje podataka iz relacijskih baza podataka. SQL injection služi napadačima da obavljaju svoje softverske napade. SQL injection ne koristi viruse već mjenja, dodaje ili briše podatke zapisane u bazama podataka. Ova vrsta napada jedna je od nakritičnijih sigurnosnih rizika za Web aplikacije. Prilikom ovih napada najbolje je izrađivati sigurnosne kopije kako bi se zaštitili od mogućih napada i gubitka podataka.

4. ZLOĆUDNI SOFTVERI

Zloćudni softveri ili kako ih se još naziva štetnim softverima ili malwerima. Zloćudni softveri su softveri koji napadaju korisnika i čine štetu. Takvi softveri su računalni programi koji se nalaze na računalu i pokreću se u sustavu bez znanja korisnika. Takvi softveri čine štetu u sustavu tako što oštećuju programe, podatke, šire se dalje u mreži, kradu podatke itd. Vrste zloćudnih softvera su: spyware, adware, trojanski konj, crv i virusi.

4.1 Virusi

Operativni sustavi su se razvijali godinama i još uvijek se razvijaju, međutim uz njihov razvoj razvijaju se i virusi. Virus je računalni program koji zarazi računalo bez znanja i dopuštenja korisnika i smjesti se u sustav ili memoriju. Računalni virusi sami se pokreću učitavanjem zaražene datoteke na računalu. Kada korisnik otvara zaraženu datoteku ili pokreće aplikaciju, neprimjetno se pokreću i virusi. Virusi traže druge datoteke na računalu koje bi mogli zaraziti, a cilj im je slanje zaraženih datoteka na druga računala kako bi se proširili. Virusi, u počecima ne uzrokuju štete jer se šire, no u jednom trenutku uzrokuju manju ili veću štetu. Takvi zloćudni programi mogu uzrokovati razne štete, od ispisa poruke na ekranu, brisanje datoteka, generiranje velikog mrežnog prometa i uništenje računalne mreže. Prvi virus je napisao Rich Skrent 1982. godine i nije stvarao štetu već je bio stvoren kao šala. Razvojem računala i sve masovnije upotrebe dolazi do stvaranja sve većeg broja virusa. Najveći broj virus došao je s internetom, jer je tada stvorena baza korisnika i žrtava, nakon čega je krenulo stvaranje sve većeg broja virusa. Virus se prenosi raznim putevima, prenose se prenošenjem zaraženih datoteka i pokretanjem zaraženih datoteka. Virus možemo prenijeti putem DVD, USB-a, CD-a, dijeljenjem datoteka u mreži, elektroničkom poštom, putem web-a itd.

4.2 Crv

Crvi su slični virusima, međutim njima za razmnožavanje nije potreban program ili datoteka jer se šire sami. Ovaj zloćudni softver stvoren je da iskoristi nedostatke u sigurnosti kod slanja podataka i tada iskoristi mrežu da napravi

kopiju i pošalje bez znanja korisnika. Crv može blokirati cijeli promet na mreži i stvoren je da djeluje na cijelu mrežu. Najčešće napadaju mreže u tvrtkama tzv. poslovne mreže jer se takvim mrežama najviše šalju povjerljivi podaci.

Crvi su stvoreni u znanstvene svrhe i pronalazili su slobodne procesore u mreži. Danas su postali opasni softveri koji nanose štetu korisnicima. Najgori crv je mail crv koji se širi putem elektroničke pošte, on šalje zaraženi privitak svim osobama iz adresara koje pronađe na računalu. Crvi se šire još putem ostalih mrežnih protokola i u kratkom vremenu prošire se Internetom nakon čega dolaze u sustav i dopuštaju da netko s udaljenosti preuzme kontrolu. On je u početku kada stigne u sustavu jako mali, no s vremenom se širi toliko da se čak u jednoj minuti može udvostručiti. Crv izaziva zagušenje mreže i rušenje poslužitelja.

4.3 Trojanski konj

Trojanski konj je jedan od najtežih zloćudnih softvera. On zarazi računalni sustav i uzrokuje zlonamjerne aktivnosti. Trojanski konj se koristi za krađu osobnih podataka, širenje virusa i otežavanje rada na računalu tako da smanjuje performanse računala. Trojanci kada uđu u sustav sakriju se i nije ih moguće prepoznati. U njihovom pronalasku mogu pomoći samo antivirusni programi ako ga uspiju pronaći. Razvojem interneta i računala razvija se i Trojanski konji tako da danas ima opciju da se umnožava. To znači da kada ga se pronađe i obriše onda se aktivira drugi. Autor takvog virusa odlučuje o njegovoj namjeri, a uspjeh ovisi o korisnicima. Trojanski konj uvijek nanosi štetu, ali postoje rijetke iznimke kada su bezopasni. Možemo ih podijeliti u nekoliko kategorija po šteti koju uzrokuju:

- proxy trojanski konj,
- trojanski konj koji šalje podatke,
- trojanski konj koji omogućuje udaljeni pristup,
- FTP trojanski konj,
- trojanski konj koji ometa rad sigurnosnih programa,
- trojanski konj koji otvara određene Web stranice.

Primjeri što Trojanski konj izvršava:

- brisanje podataka,
- širenje virusa,
- šifriranje podataka,
- špijuniranje korisnika i slanje podataka napadaču,
- instaliranje programa kojima će se napadač priključiti na računalo,
- prikupljanje adresa elektroničke pošte kako bi slao zaraženu poštu,
- ponovno pokretanje računala,
- dopuštanje udaljenog pristupa.

Trojanski konj može biti i vremenski podešen, tada se aktivira određenog dana u određeno vrijeme. On najčešće dolazi na računalo nakon što korisnik pokrene zaraženi program. Širi se putem elektroničke pošte, CD-a, DVD-a, USB-a, Web-a i ostalih medija.

5. OSIGURANJE RAČUNALNE MREŽE

Istovremeno s razvojem računala i virusa razvijala se i zaštita podataka. Kroz povijest razvoja postoje različite metode koje su se koristile i bile manje ili više uspješne u obrani podataka. Većina metoda bila je jednostavna i lako ih se zaobilazilo čime podaci nisu bili dovoljno osigurani. Kroz razvoj tehnologije zaštite razvila se i kriptografija koja kriptira i štiti dokumente. Ona sprječava pregledavanje podataka od strane neovlaštenih osoba tako što dokument kriptira i samo ga ovlaštena osoba može otvoriti. No postoji problem da ga ovlaštena osoba loših namjera može dekriptirati, zatim spremiti i proslijediti dalje. Potrebno je ograničiti broj osoba koje mogu pregledavati zaštićene dokumente, ali uvijek postoji opasnost da jedna osoba koja ima pristup može te dokumente proslijediti i tako ih odati. Kada se takvo nešto dogodi potrebno je pronaći osobu koja je to učinila, te je potrebno da snosi posljedice za svoje postupke. Danas se u zaštiti dokumenta upotrebljavaju razne metode kao što su antivirusni programi, sigurnosni protokoli mreža, kontrole pristupa, kriptiranje i ostalo.

Kako bi zaštita bila što bolja i efikasnija potrebno je kombinirati više metoda.

5.1 Antivirusni programi

Antivirusni programi su računalni programi koji imaju zadatke da identificiraju i, eliminiraju viruse, crva, trojanskog konja i ostale maliciozne programe. Cilj antivirusnog programa je da prepozna virus i osigura sustav od njega. U slučajevima kada je računao već zaraženo tada antivirusni program identificira virus i ukloni ga s računala. Antivirusni programi pronalaze viruse pomoću znakovnih kodova jer je svaki virus računalni program. Nakon što ih je detektirao antivirusni program će učiniti sljedeće:

- probati popraviti zaraženu datoteku tako što će izbrisati virus,
- datoteku premjestiti u izolirani dio i njoj se neće moći više pristupiti i virus se neće širiti,
- izbrisati zaraženu datoteku.

Antivirusni programi se stalno razvijaju kako bi mogli pratiti razvoj virusa. To se radi tako da se baze virusa i baza njihovih kodova stalno ažurira i više puta dnevno, a to rade antivirusni programi automatski. Neki virusi pokušavaju

mijenjati svoje kodove i zato je važno osvježavanje baza kodova kako bi se spriječilo njihovo širenje.

5.2 Kriptiranje

Kriptiranje je jedan od važnih dijelova kada se govori o zaštiti dokumenata koji su pohranjeni na tvrdom disku. Ovaj lagan i jednostavan postupak štiti otkrivanje povjerljivih podataka prilikom napada na računalo ili gubitkom prijenosnog računala.

Operativni sustavi imaju već ugrađene programe koji vrše kriptiranje podataka.

Kriptiranje jasan i razumljiv tekst preoblikuje u nejasan i nerazumljiv tekst osobama kojima nije namijenjen. Osobe koje imaju pravo pristupa tom dokumentu i osobe koje smiju čitati taj dokument imaju ključ koji pretvara dokument u jasan tekst. Imamo dvije vrste kriptiranja simetričnu i asimetričnu.

5.3 IPSec protokol

IPSec (*engl. IP Security*) je proširenje IPv4 protokola, a osigurava osnovne sigurnosne aspekte mrežne komunikacije. IPSec kod IPv6 protokola dolazi kao ugrađeni dio.

IPSec se nalazi u mrežnom sloju OSI modela no moguće ga je implementirati i u drugim slojevima. IPSec osigurava tajnost i integritet.

5.4 Vatrozid

Vatrozid (engl. Firewall) je jedan od bitnijih dijelova mreže kada se govori o sigurnosti mreže. Koristi se kao sigurnosni sustav koji ima zadaću zaštititi računalnu mrežu ili uređaj od neovlaštenog pristupa i neželjenog prometa s mreže. Njegova osnovna zadaća je kontrola prometa koji ulazi ili izlazi iz mreže te odlučivati što će biti dopušteno ili blokirano prema unaprijed definiranim pravilima i postavkama sigurnosti. Filtri na razini mreže pregledavaju pakete na niskoj razini TCP/IP protokolarnog skupa i ne dopuštaju paketima da prođu kroz vatrozid osim ako se podudaraju s postavljenim skupom pravila. Nedostatak je što nepoželjne aplikacije ili zlonamjerni softveri mogu proći preko dopuštenih

priključaka, naprimjer izlazni internetski promet putem web protokola HTTP i HTTPS, priključci 80 i 443.

Djelovanje vatrozida:

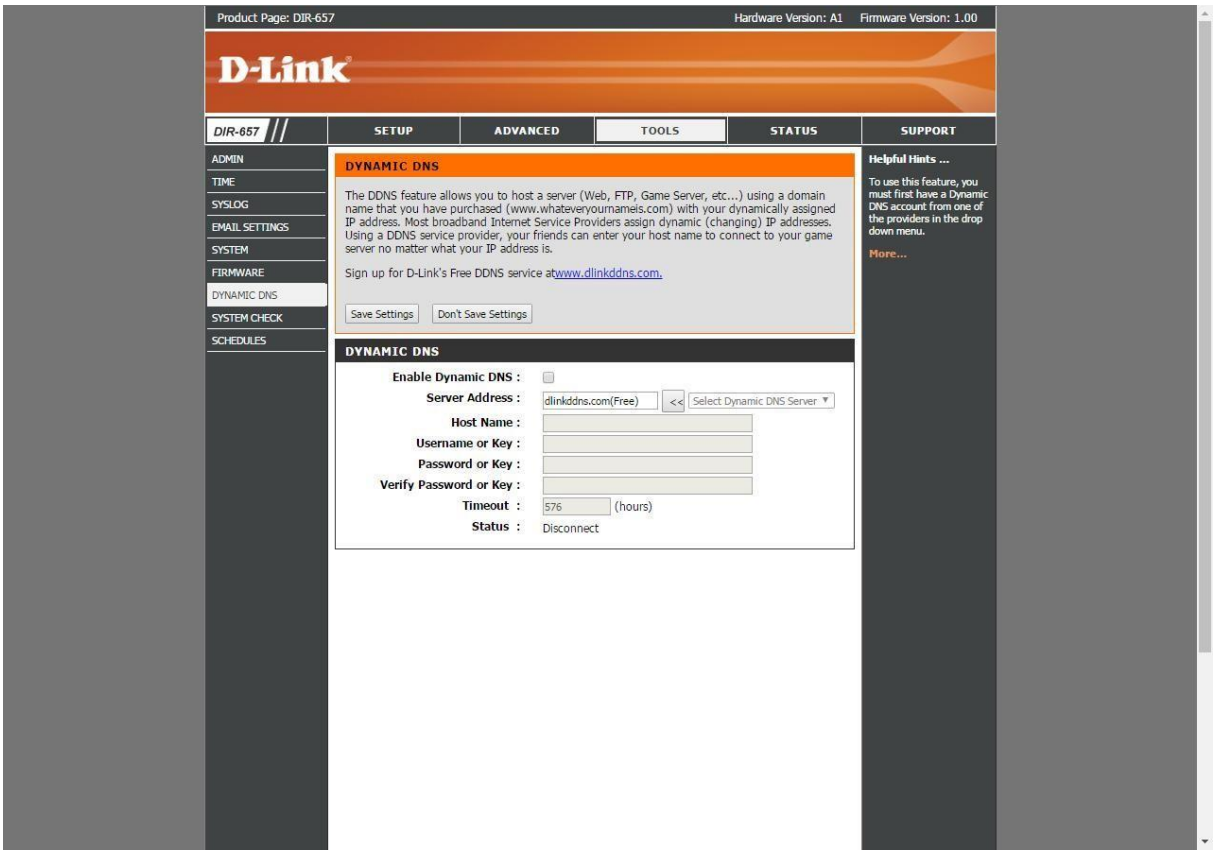
- Filtriranje prometa – analiziranje dolaznog i odlaznog prometa gdje se identificira izvor, odredište, vrsta i druge karakteristike paketa.
- Proxy usluga – pored osnovnog vatrozida dodatno filtrira promet na razini aplikacija što omogućuje još dublju inspekciju i kontrolu nad aplikacijskim slojem.
- Nadzor portova – vatrozid može nadzirati i kontrolirati otvorene mrežne portove na uređaju ili u mreži jer svaki mrežni servis koristi određeni port te vatrozid može blokirati pristup određenim portovima kako bi spriječio napad ili neovlašteni pristup.
- Analiziranje paketa – vatrozid na temelju različito postavljenih parametara analizira pakete poput IP adrese, portova, protokola itd. Kada određeni paket podataka ne odgovara postavljenim parametrima vatrozid ga može blokirati.
- Stanje promatranja – tehnika koju današnji moderni vatrozidovi je koriste za praćenje stanja aktivnih mrežnih veza što donosi bolje donošenje odluka o dopuštenjima ili blokiranju prometa.
- Logging i upozorenja – dnevnički zapisi vatrozida o njegovom radu, omogućuju administratoru mreže praćenje i analizu prometa te ono najvažnije otkrivanje pokušaja neovlaštenog pristupa i drugih sigurnosnih prijetnji. Postoji mogućnost generiranja upozorenja kako bi obavijestio administratora o potencijalnim problemima.

Vatrozid je ključan sigurnosni alat svake mreže koji pomaže administratorima održavati sigurnost kroz kontrolu prometa, sprječavanje neovlaštenih pristupa što dovodi do smanjenja mogućih prijetnji poput napada hakera, virusa i zlonamjernih softvera.

6. PRAKTIČAN RAD

Praktični rad ovog maturalnog rada sastoji se od konfiguriranja osnovnih funkcija usmjerivača. Usmjerivač potrebno je pravilno konfigurirati kako bi mreža bila zaštićena od mogućih napada. Administrator mreže je glavna osoba koja vodi brigu o radu i sigurnosti mreže zato je bitno dodijeliti administratora. Na usmjerivačima imamo mnogo opcija koje se mogu konfigurirati. Većinom na usmjerivačima koji se dobiju od pružatelja telekomunikacijskih usluga nema mnogo opcija koje se mogu podesiti jer se radi o usmjerivačima za kućnu upotrebu. U trgovinama postoji mnogo usmjerivača od niskih cijena do visokih, a ovisno o potrebama biraju se usmjerivači koji su potrebni da bi mreža nesmetano funkcionirala i izvršavala svoje zadaće.

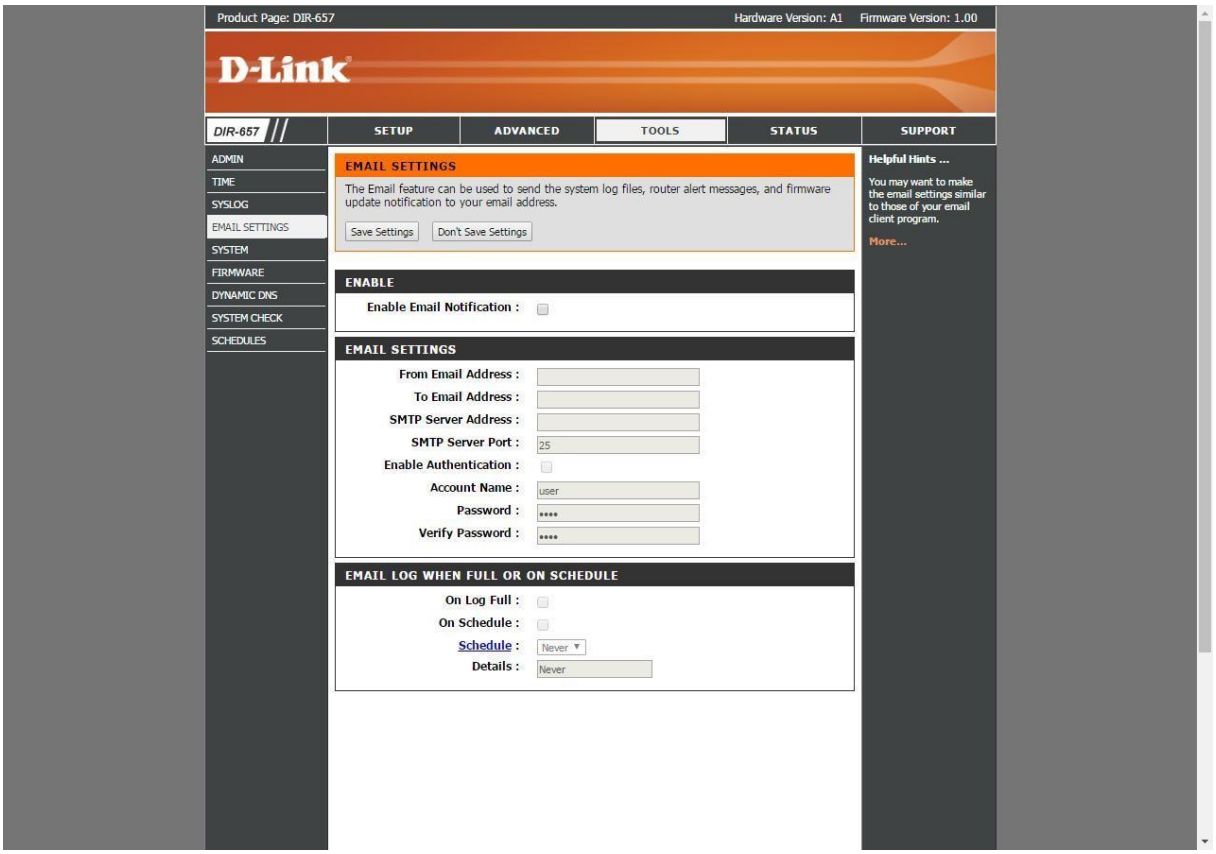
6.1 Dinamički DNS



Slika 3. Postavke dinamičkog DNS-a na usmjerivaču

Dinamički DNS (*engl. Dynamic DNS*) kod konfiguracije usmjerivača jedan je od bitnih stvari koje je potrebno konfigurirati. Kada je uključena ova opcija usmjerivač nema statičku javnu IP adresu što je važno u zaštiti mreže. Usmjerivač mijenja svoju javnu IP adresu svakih par sati ili svakih 24 sata što otežava napadačima u napadu i štiti mrežu.

6.2 Email postavke

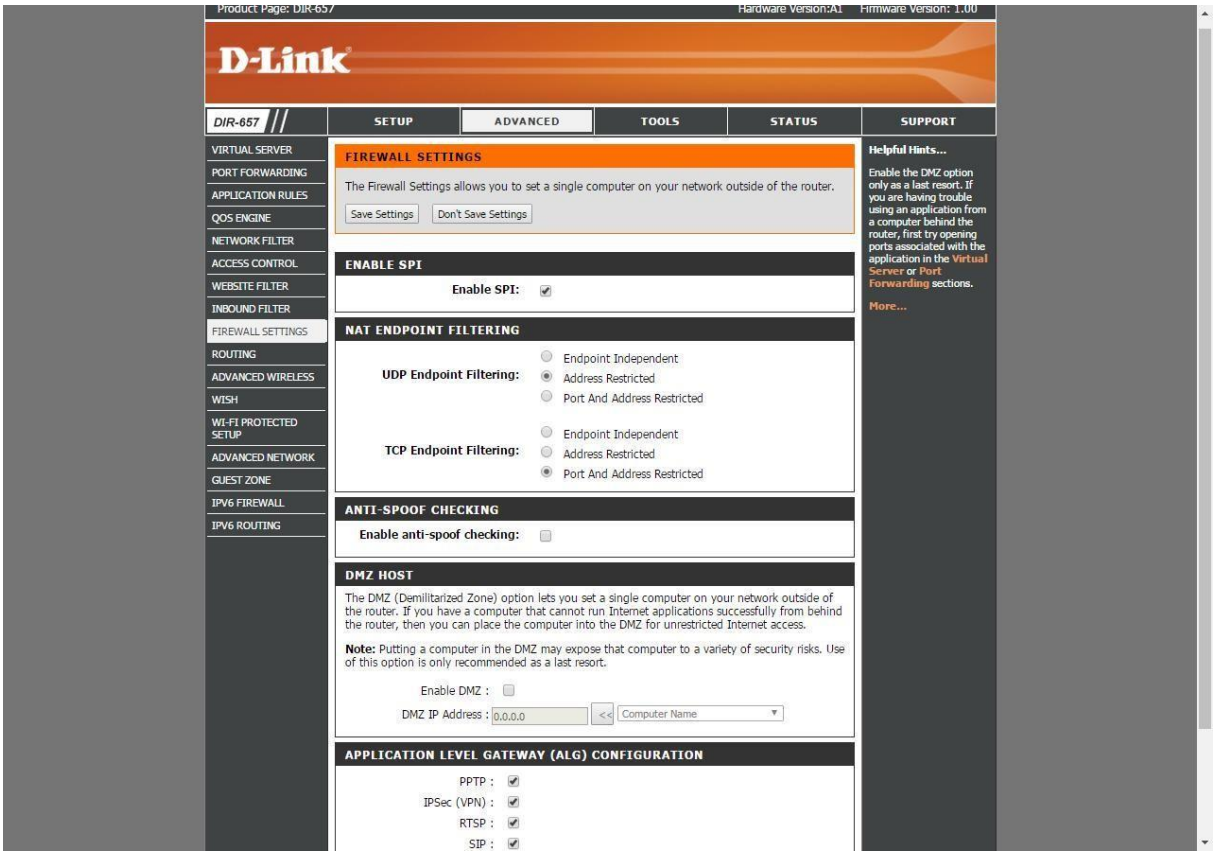


Slika 4. Email postavke na usmjerivaču

Ulaskom u email postavke odobravamo slanje informacija na email. Prije nego što usmjerivač krene slati informacije potrebno je konfigurirati email. Email se konfigurira tako što se unose podaci i informacije (lozinka, korisničko ime, SMTP server) o emailu koji će služiti kao odlazni i email na koji ćemo primati informacije. Usmjerivač će nam slati obavijesti o prijavama u sustav usmjerivača, poruke mogućih opasnosti, podsjetnike o ažuriranju zaštite itd.

6.3 Vatrozid postavke

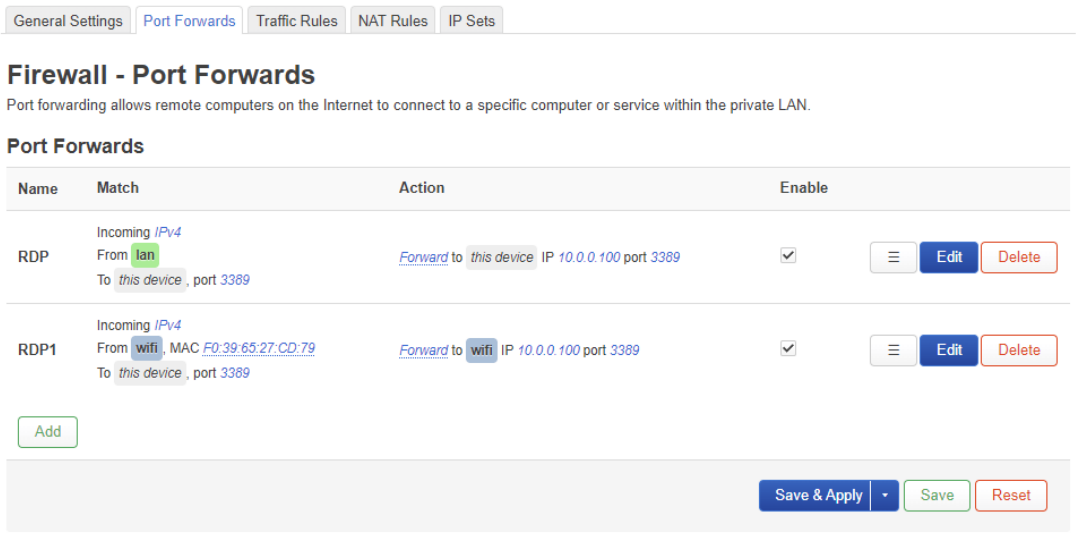
Vatrozid je zaštitni zid koji filtrira mrežni promet tako da stvara sigurnosne zone. Svaki program ili aplikacija koja želi pristupiti Internetu treba imati dopuštenje vatrozida. Vatrozid je bitna stavka u sigurnosti mreže jer filtriranjem štiti korisnike mreže od neželjenih sadržaja i mogućih izloženosti napadima.



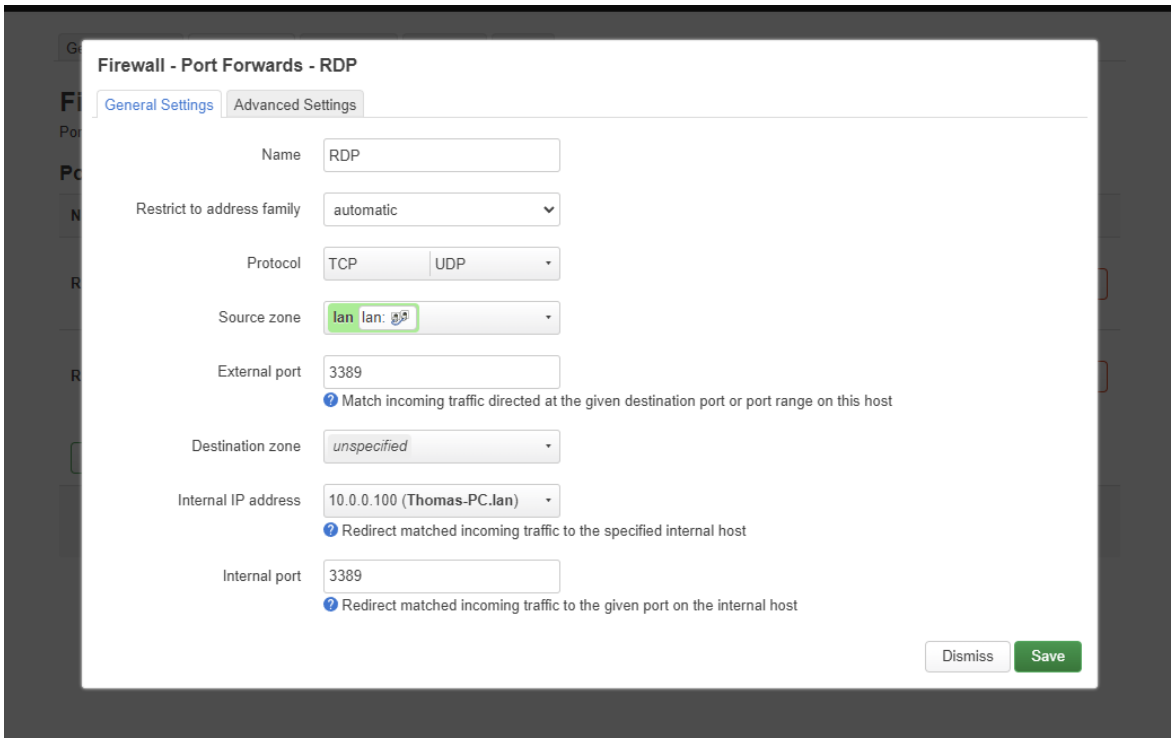
Slika 5. Uključivanje vatrozida na usmjerivaču

Unutar postavki vatrozida moguće je postaviti i takozvani port preusmjeravanja (*engl. Port forwarding*). Navedenu metodu ne posjeduju svi usmjerivači već određeni usmjerivači te uglavnom se radi o uređajima koji nisu namijenjeni za kućnu upotrebu već profesionalnu. Port forwarding je tehnologija prevođenja adrese ili broja priključka mrežnog paketa na novu odredišnu adresu. Omogućuje udaljenim računalima ili uređajima na internetu da se povežu s određenim računalom unutar LAN mreže tako da se promet usmjeren prema određenom mrežnom priključku preusmjeri s vanjske mreže na određeni uređaj unutar interne mreže. Uglavnom ga se koristi kako bi se omogućilo udaljeno pristupanje i komunikacija s računalom unutar lokalne mreže. Port forwarding se

konfigurira unutar postavki na usmjerivaču koji zatim omogućuje ovaj oblik komunikacije.

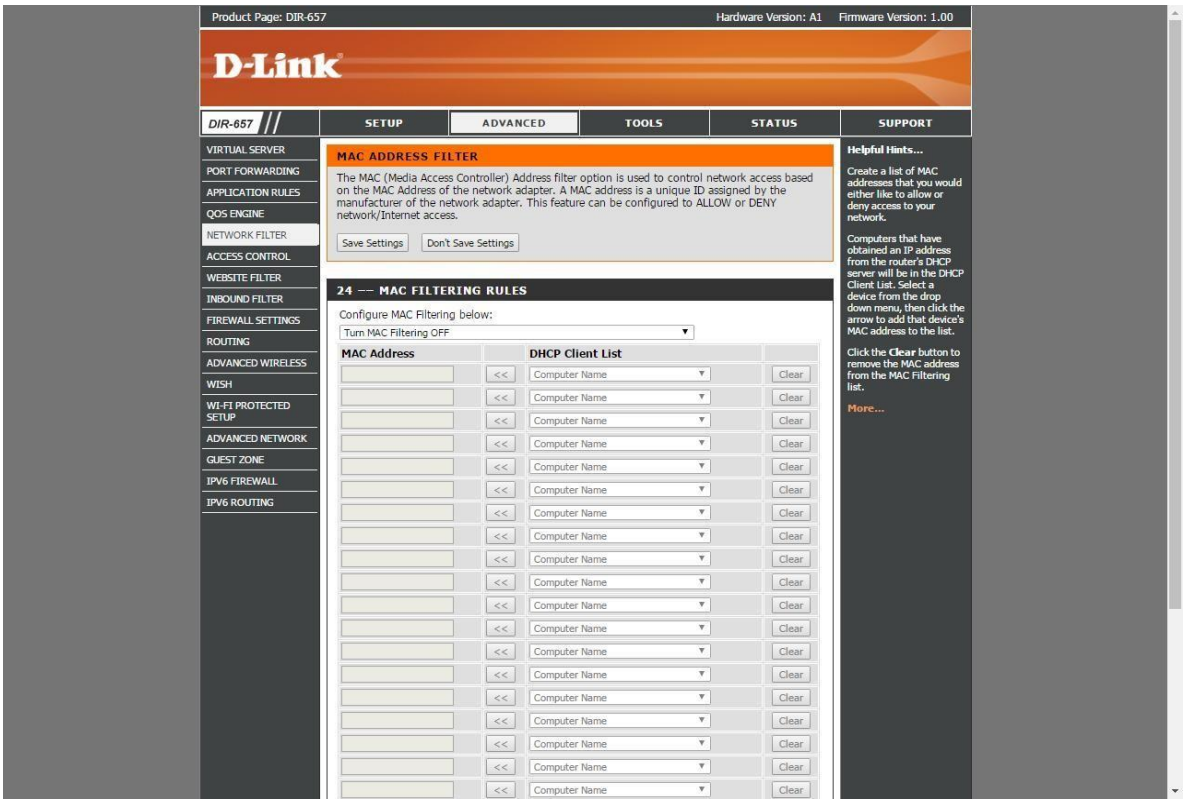


Slika 6. Port forwarding



Slika 7. Podešavanje Port forwarding

6.4 Filtriranje adresa

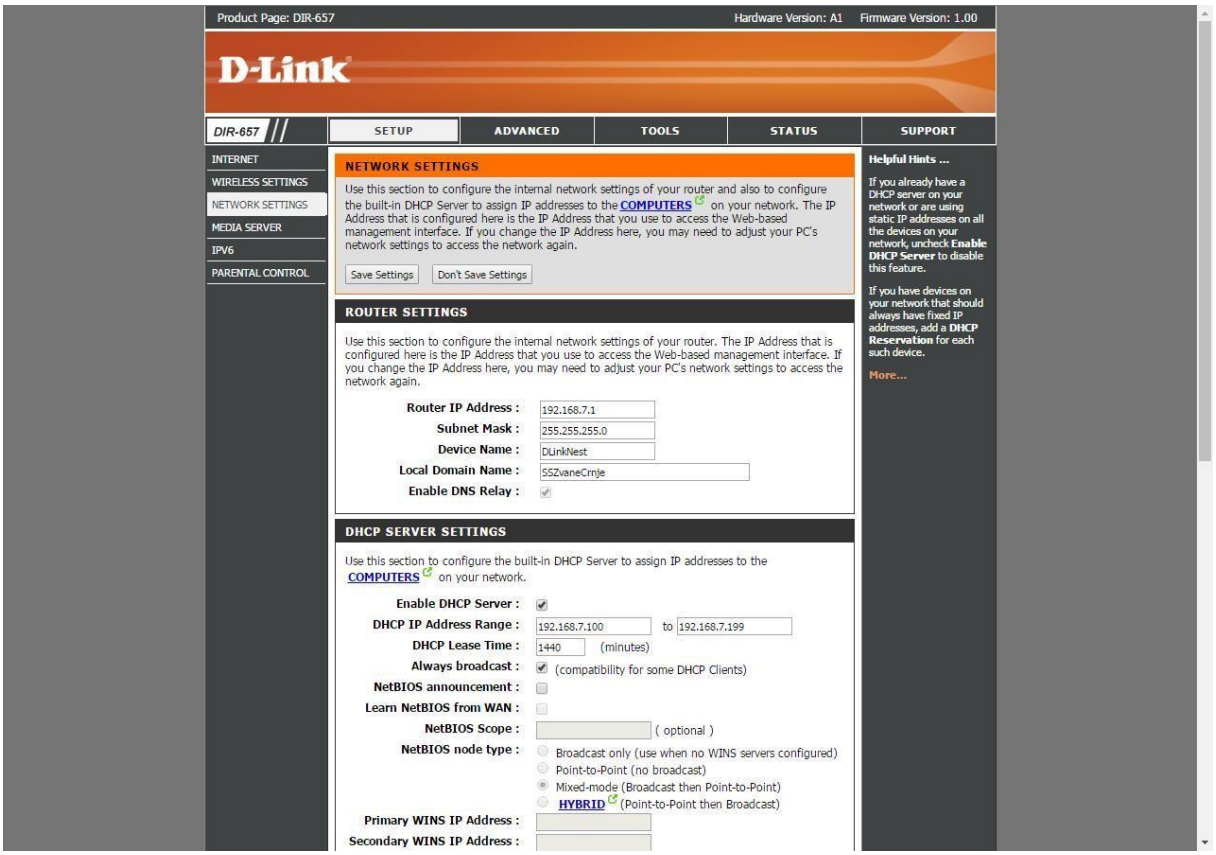


Slika 8. Filtriranje adresa

Filtriranje adresa na usmjerivaču služi administratoru kako bi mogao zabraniti pristup mreži određenom računalu. Svako računalo u mreži ima svoju MAC adresu po kojoj je prepoznatljivo. Na usmjerivaču je pohranjena tablica svih MAC adresa u mreži.

Administrator mreže kako bi računalu zabranio pristup mreži dovoljno je da unese njegovu MAC adresu na listu za filtriranje.

6.5 Postavke mreže

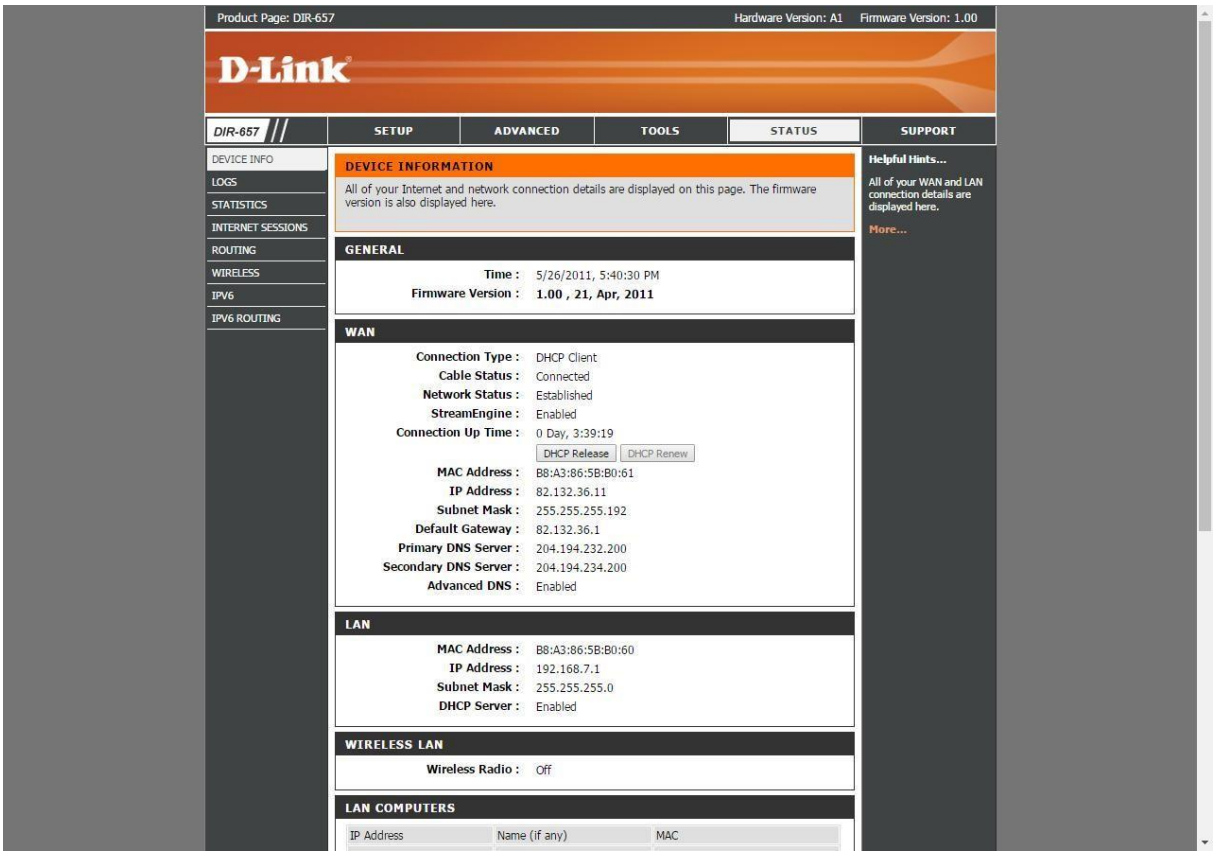


Slika 9. Postavke mreže

U postavkama mreže podešavaju se opće postavke usmjerivača. U mrežnim postavkama možemo podesiti IP adresu usmjerivača, subnet masku, ime usmjerivača i ime mreže. Pod mrežne postavke spadaju i postavke DHCP-a. Kod DHCP-a bitne postavke su da ga se može uključiti ili isključiti i raspon DHCP IP adresa.

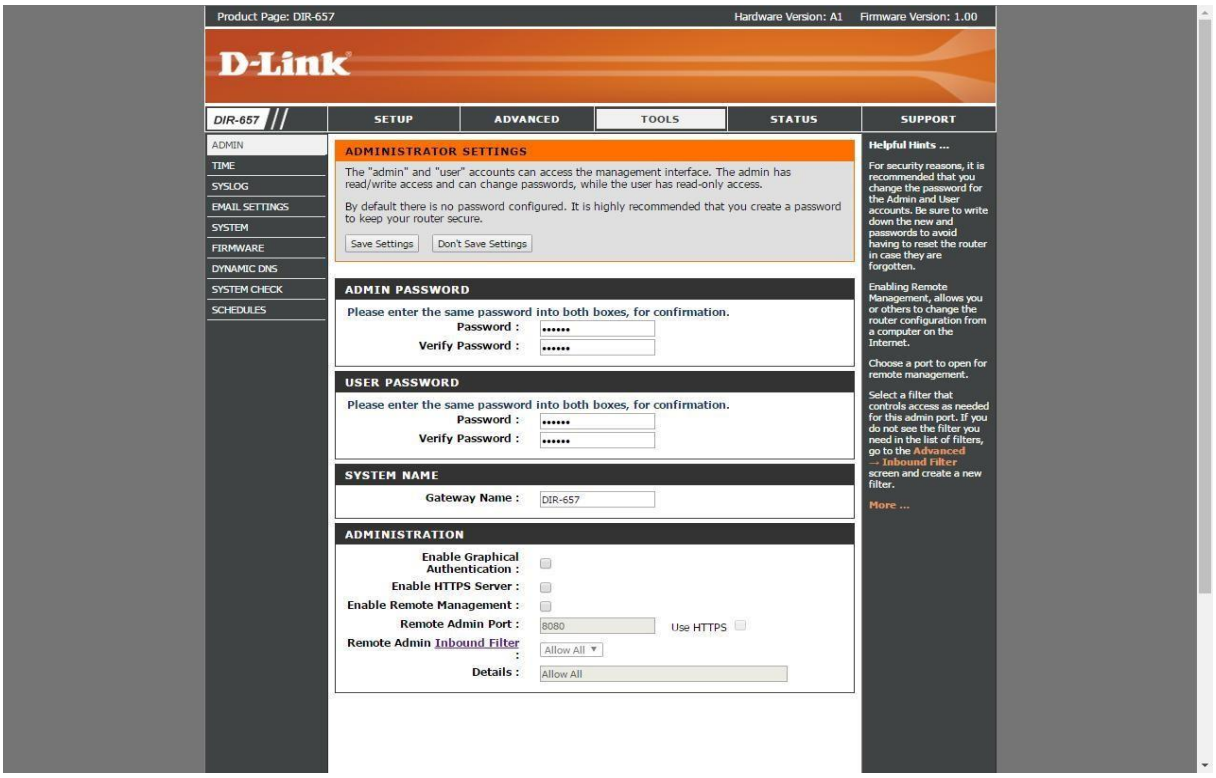
6.6 Informacije o statusu usmjerivača

U izborniku na usmjerivaču postoji opcija status. Kada se odabere ova opcija otvara se stranica sa statusom usmjerivača na kojoj su prikazane sve informacije o usmjerivaču. U ovoj opciji ne može se ništa konfigurirati već samo pregledavati.



Slika 10. Informacije o usmjerivaču

6.7 Dodijeljivanje administratora

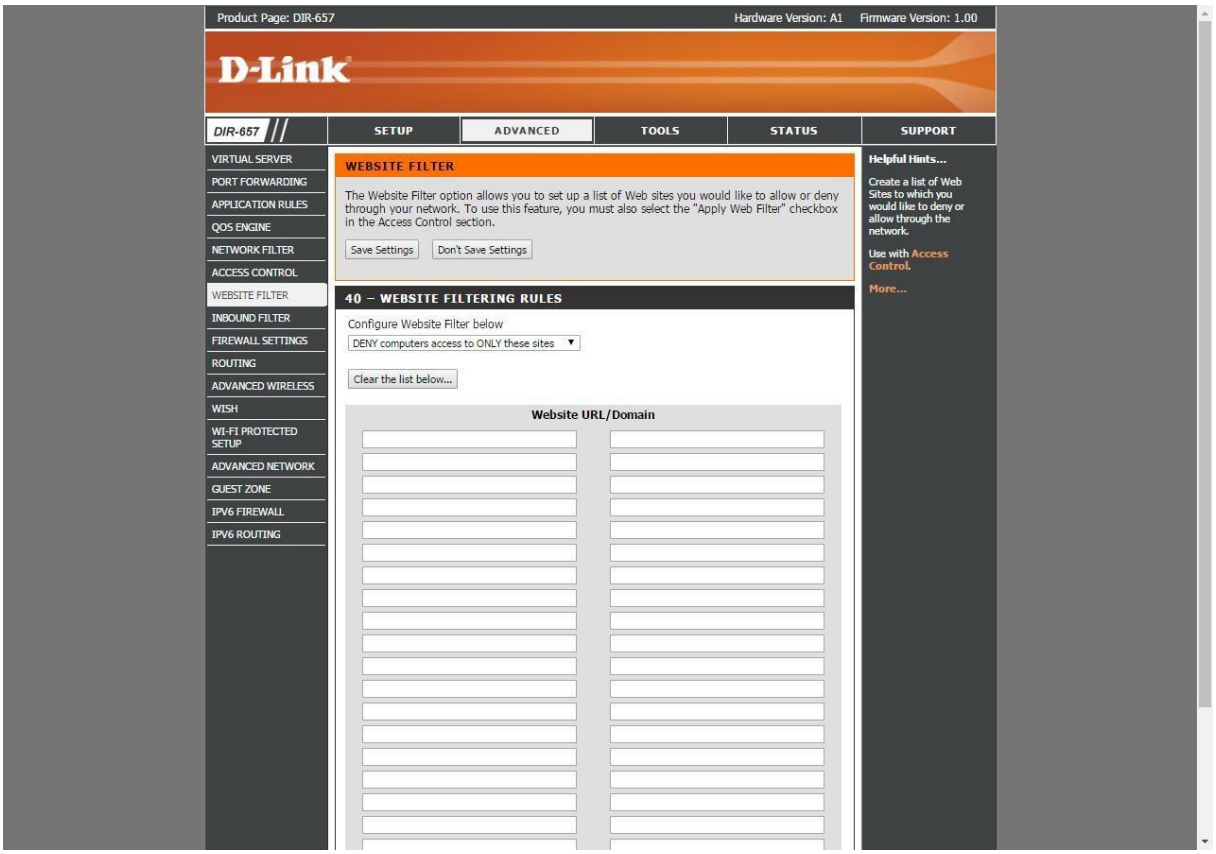


Slika 11. Dodjeljivanje administratora

Konfiguriranje usmjerivača zahtijeva i dodjeljivanje administratora mreže.

Administrator mreže dodaje se na usmjerivaču pod opcijom alati i odabirom pod opcije Admin. U ovoj opciji konfiguracije dodjeljujemo administratora, lozinku za administratora i korisnika. Administrator ima ovlasti konfiguriranja svih opcija mreže dok korisnik ima samo pravo na određene postavke ovisno o odluci administratora.

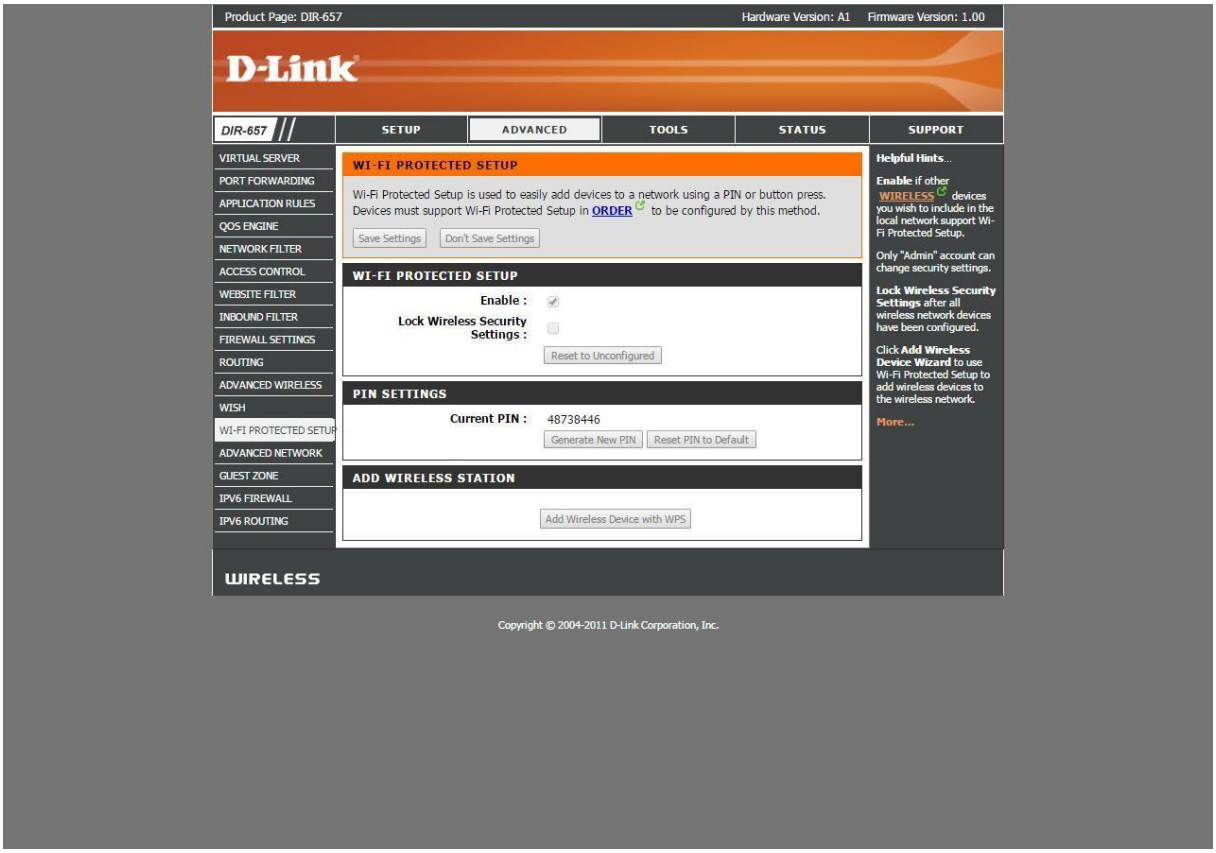
6.8 Filter WEB stranica



Slika 12. Filtriranje WEB stranica

U opciji naprednih postavaka imamo i pod opciju kojom se može zabraniti pristup određenim internetskim stranicama. Ovu opcija koristi se u velikim poduzećima, tvrtkama, ustanovama ali i kod privatnih kuća. Svako poduzeće ili ustanova imaju svoj pravila i načela po kojima posluju i u njihovim pravilima postoje i odredbe kojim sadržajima na internetu njihovi zaposlenici ne smiju pristupiti. Zato koriste opciju filtriranja internetskih stranica koja omogućuje da se na popis dodaju stranice sa neželjenim sadržajima kojim korisnici u mreži neće moći pristupiti. Ova opcija je korisna i u domovima jer se dodaju stranice s neželjenim sadržajem kako korisnici kao djeca ne bi mogla pristupiti takvim stranicama.

6.9 Podešavanje WI-FI postavki



Slika 13. WI-FI podešavanje

Pod razvojne opcije spada i pod opcija zaštita WIFI-a. Ovu opciju je važna u zaštiti mreže kada se govori o bežičnom pristupu mreži. Kada je ova metoda uključena onda prilikom spajanja na mrežu moramo unijeti PIN.

6.10 Automatsko dodjeljivanje postavki

Većina privatnih korisnika ne koristi niti jednu od mogućih opcija na usmjerivaču već dodjele postavke automatski. Automatsko dodjeljivanje postavki je osnovno i kod poslovnih korisnika ne dovoljno u zaštiti mreže zato je važno samostalno proći kroz svaku funkciju usmjerivača i podesiti mrežu kako bi bila zaštićena od napada. Opcija automatskog dodjeljivanja postavki pojavljuje nam se na prvoj stranici nakon prijave u usmjerivač i odaberemo opciju automatskog dodjeljivanja postavki. Nakon odabira usmjerivač biti će konfiguriran i spreman za rad po postavkama koje je zadao proizvođač.

Slika 14. Automatsko dodjeljivanje postavki

7. ZAKLJUČAK

Lokalna računalna mreža je sustav koji olakšava korisnicima povezivanje putem mreže. Mreža može djelovati na više različitih razina. Globalizacijom je porasla potreba

za umrežavanjem jer korisnici lakše razmjenjuju informacije putem mreže. Umrežavanje ima više prednosti u komunikaciji, jedna od bitnijih je ušteda vremena jer je u današnjici svaki trenutak vremena ispunjen obavezama.

Računalne mreže razvile su se u zadnjih godina veoma brzo. Danas se putem mreže može se prenijeti veliki broj podataka u kratkom roku, dok je to nekad bilo nezamislivo. Kako bi svaka mreža obavljala svoje zadatke potrebno ju je pravilno konfigurirati i povezati. Prije samog početka povezivanja potrebno je napraviti plan i razraditi svaki detalj u mreži. Kod izrade plana potrebno je voditi računa da mreža bude što efikasnija i što sigurnija. Bitna stavka kod izrade mreže je plan sigurnosti. Sigurnost mreže veoma je bitna u današnjem vremenu kada je prisutan sve veći broj napada na mreže i krađa podataka. Plan sigurnosti mora predvidjeti moguće napade na mrežu i moguće obrane od njih. Obzirom da se svakodnevno razvijaju nove metode krađe podataka, potrebno je taj plan stalno obnavljati s novim metodama zaštite.

Nakon izrade samog plana mreže prelazi se na spajanje računala u mrežu i konfiguriranje usmjerivača. Računala ćemo povezati u mrežu putem kabla, dok ćemo neke uređaje povezati putem bežične veze. Konfiguracija usmjerivača bitan je segment u izradi mreže. Usmjerivače je moguće podesiti s osnovnim postavkama koje u većini slučajeva sadrže samo osnovne stvari za rad mreže. Kako bi mrežu osigurali od napada i kako bi mreža bila što efikasnija, potrebno je proći kroz postavke usmjerivača i podesiti nekoliko opcija. U radu je opisano koje vrste napada postoje i koja rješenja postoje, dok u praktičnom djelu postoje osnovni koraci koje je potrebno podesiti da bi mrežu osigurali. Neki od osnovnih koraka su podešavanje lozinki, dodjeljivanje administratora, filtriranje MAC adresa itd. Od osnovnih koraka najvažniji je dodjeljivanje samog administratora mreže. Administrator mreže treba nadzirati mrežu, voditi brigu o sigurnosti i stalno ažurirati metode obrane u slučaju napada.

Računalne mreže danas su neizbježan segment u prijenosu informacija i podataka. Putem mreža prenosimo informacije s jednog računala na drugo bez obzira koliko je to računalo udaljeno od početnog. Mnogo dokumenata u današnjici sadrži osjetljive podatke. Takve dokumente, kako ne bi došli do neželjenih osoba, treba zaštiti. Danas ima mnogo slučajeva prepisivanja, krađa, kvarenja tvrdog diska i drugo. Kako bi se sve to izbjeglo potrebno je izraditi plan zaštite mreže i podataka. Razvojem novih tehnologija i kriptografije pronašli su se načini kriptiranja i zaštite podataka. Postoji nekoliko metoda zaštite podataka to su upotreba enkripcije, upotreba zaporki, ograničavanje pristupa, kriptiranje diska itd.. Antivirusni programi imaju zadaću prepoznati virus i zaštiti sustav. No nekada niti antivirusni programi nisu dovoljni u obrani mreže. Svaku mrežu potrebno je veoma dobro isplanirati i ispitati sve moguće načine napada i pronaći rješenja. Kada jednom dođe do napada potrebno je odmah postaviti protuobranu i spriječiti štetu.

8. POPIS LITERATURE

1. Stallings, W. (1984). *Local networks. ACM Computing Surveys, 16(1), 3–41.*
2. Shoch, J. F., & Hupp, J. A. (1980). Measured performance of an Ethernet local network. Communications of the ACM, 23(12), 711–721.
3. Yokota, H., Idoue, A., Hasegawa, T., & Kato, T. (2002). Link layer assisted mobile IP fast handoff method over wireless LAN networks. Proceedings of the 8th Annual International Conference on Mobile Computing and Networking - MobiCom '02.
4. Leland, W. E., Taqqu, M. S., Willinger, W., & Wilson, D. V. (1993). On the self-similar nature of Ethernet traffic. Conference Proceedings on Communications Architectures, Protocols and Applications - SIGCOMM '93.
5. Khoussainov, R., & Patel, A. (2000). LAN security: problems and solutions for Ethernet networks. Computer Standards & Interfaces, 22(3), 191–202.
6. Huynh, M., & Mohapatra, P. (2007). Metropolitan Ethernet Network: A move from LAN to MAN. Computer Networks, 51(17), 4867–4894.
7. Tenti, P., & Caldognetto, T. (2018). Optimal control of Local Area Energy Networks (E-LAN). Sustainable Energy, Grids and Networks, 14, 12–24.
8. Wei, W., Wang, B., Zhang, C., Kurose, J., & Towsley, D. (2008). Classification of access network types: Ethernet, wireless LAN, ADSL, cable modem or dialup? Computer Networks, 52(17), 3205–3217.
9. Zerfiridis, K. G., & Karatza, H. D. (2004). Brute force web search for wireless devices using mobile agents. Journal of Systems and Software, 69(1-2), 195–206.
10. Ganz, A., Park, S. ., & Ganz, Z. (2000). Security broker for multimedia wireless LANs. Computer Communications, 23(5-6), 588–594.
11. Mamat, K., & Azmat, F. (2013). Mobile Learning Application for Basic Router and Switch Configuration on Android Platform. Procedia - Social and Behavioral Sciences, 90, 235–244.
12. Schroeder, M. D., Birrell, A. D., Burrows, M., Murray, H., Needham, R. M., Rodeheffer, T. L., … Thacker, C. P. (1991). Autonet: a high-speed, self-configuring local area network using point-to-point links. IEEE Journal on Selected Areas in Communications, 9(8), 1318–1335.

13. Cho, J.-S., Yeo, S.-S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer Communications, 34(3), 391–397.
14. Hofstede, R., Jonker, M., Sperotto, A., & Pras, A. (2017). Flow-Based Web Application Brute-Force Attack and Compromise Detection. Journal of Network and Systems Management, 25(4), 735–758.
15. Knudsen, L. R., & Robshaw, M. J. B. (2011). Brute Force Attacks. The Block Cipher Companion, 95–108.
16. Najafabadi, M. M., Khoshgoftaar, T. M., Kemp, C., Seliya, N., & Zuech, R. (2014). Machine Learning for Detecting Brute Force Attacks at the Network Level. 2014 IEEE International Conference on Bioinformatics and Bioengineering.
17. Boyd, S. W., & Keromytis, A. D. (2004). SQLrand: Preventing SQL Injection Attacks. Lecture Notes in Computer Science, 292–302.
18. Shar, L. K., & Tan, H. B. K. (2013). Defeating SQL Injection. Computer, 46(3), 69–77.
19. Li, P., Salour, M., & Su, X. (2008). A survey of internet worm detection and containment. IEEE Communications Surveys & Tutorials, 10(1), 20–35.
20. Weaver, N., Ellis, D., Staniford, S., & Paxson, V. (n.d.). Worms vs. perimeters: the case for hard-LANs. Proceedings. 12th Annual IEEE Symposium on High Performance Interconnects.
21. Schechter, S. E., Jung, J., & Berger, A. W. (2004). Fast Detection of Scanning Worm Infections. Recent Advances in Intrusion Detection, 59–81.
22. Pandey, R. K., & Misra, M. (2016). Cyber security threats — Smart grid infrastructure. 2016 National Power Systems Conference (NPSC).
23. Choi, Y. B., Muller, J., Kopek, C. V., & Makarsky, J. M. (2006). Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance. International Journal of Mobile Communications, 4(3), 266.
24. Zhang, Z.-K., Cho, M. C. Y., & Shieh, S. (2015). Emerging Security Threats and Countermeasures in IoT. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security - ASIA CCS '15.

25. Skrzewski, M. (2010). Monitoring Malware Activity on the LAN Network. Communications in Computer and Information Science, 253–262.
26. O'Malley, S. W., & Peterson, L. L. (1992). A dynamic network architecture. ACM Transactions on Computer Systems, 10(2), 110–143.
27. Koponen, T., Chawla, M., Chun, B.-G., Ermolinskiy, A., Kim, K. H., Shenker, S., & Stoica, I. (2007). A data-oriented (and beyond) network architecture. Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications - SIGCOMM '07.
28. Khan, I. (2012). An introduction to computer viruses: problems and solutions. Library Hi Tech News, 29(7), 8–12.
29. Zhauniarovich, Y., Khalil, I., Yu, T., & Dacier, M. (2018). A Survey on Malicious Domains Detection through DNS Data Analysis. ACM Computing Surveys, 51(4), 1–36.
30. Arvidsson, M., Collet, F., & Hedström, P. (2021). The Trojan-horse mechanism: How networks reduce gender segregation. Science Advances, 7(16).
31. Morison, M., & Moir, J. (1998). The role of computer software in the analysis of qualitative data: efficient clerk, research assistant or Trojan horse? Journal of Advanced Nursing, 28(1), 106–116.
32. Tang, S. (2009). The Detection of Trojan Horse Based on the Data Mining. 2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery.
33. Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. IEEE Wireless Communications, 17(1), 51–58.
34. Alieyan, K., ALmomani, A., Manasrah, A., & Kadhum, M. M. (2015). A survey of botnet detection based on DNS. Neural Computing and Applications, 28(7), 1541–1558.
35. Gupta, N., Naik, V., & Sengupta, S. (2017). A firewall for Internet of Things. 2017 9th International Conference on Communication Systems and Networks (COMSNETS).
36. Razzaq, A., Hur, A., Shahbaz, S., Masood, M., & Ahmad, H. F. (2013). Critical analysis on web application firewall solutions. 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS).

37. Hu, H., Ahn, G.-J., & Kulkarni, K. (2012). Detecting and Resolving Firewall Policy Anomalies. IEEE Transactions on Dependable and Secure Computing, 9(3), 318–331.
38. Neupane, K., Haddad, R., & Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. SoutheastCon 2018.
39. Wu, Q.-X. (2012). The Research and Application of Firewall based on Netfilter. Physics Procedia, 25, 1231–1235.
40. Shukla, J. B., Singh, G., Shukla, P., & Tripathi, A. (2014). Modeling and analysis of the effects of antivirus software on an infected computer network. Applied Mathematics and Computation, 227, 11–18.
41. Pandian, A. P., Fernando, X., & Islam, S. M. S. (Eds.). (2021). Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies.
42. Dhall, H., Dhall, D., Batra, S., & Rani, P. (2012). Implementation of IPSec Protocol. 2012 Second International Conference on Advanced Computing & Communication Technologies.
43. Li, X. (2020). Application of Data Encryption Technology in Computer Network Communication Security. Journal of Physics: Conference Series, 1574, 012034.
44. Ren, J., Xu, Y., & Liu, J. (2015). Investigation of dynamics of a virus–antivirus model in complex network. Physica A: Statistical Mechanics and Its Applications, 421, 533–540.

9. PRILOZI

9.1 Popis slika

10. SAŽETAK I KLJUČNE RIJEČI (ABSTRACT AND KEYWORDS)

Kroz ovaj rad prikazali smo kako konfigurirati i zaštit lokalnu računalnu mrežu od napada. Razvojem tehnologija došlo je do razvoja metoda napada i sve većeg broja krađa podataka. Konfiguracija je prva stavka u planiranju i izradi mreže. Ovaj rad govori kako pravilno konfigurirati i isplanirati mrežu kako bi se izbjegli napadi i krađa podataka. Također, objašnjeni su mogući napadi različitim metodama i softwer-ima na mrežu, kako oni djeluju na mrežu i kako zaštiti mrežu od takvih napada. Nakon prikaza konfiguracije i zaštite mreže, naveden je praktični dio koji prikazuje kako pravilno konfigurirati usmjerivač kroz par osnovnih koraka. Primjeri u praktičnom dijelu sastoje se od par osnovnih prikaza koji prikazuju kako podesiti osnovne postavke usmjerivača kako bi zaštitili mrežu i spriječili moguću krađu podataka.

In this paper, we have demonstrated how to configure and secure a local computer network from attacks. With the advancement of technologies, there has been an increase in attack methods and data theft incidents. Configuration is the first step in network planning and development. This paper explains how to properly configure and plan a network to prevent attacks and data breaches. Additionally, various attack methods and software that can be used to compromise a network are explained, including how they affect the network and how to protect it from such attacks. After presenting network configuration and security measures, a practical section is provided that illustrates how to correctly configure a router through a few basic steps. The examples in the practical section consist of a few basic demonstrations that show how to adjust router settings to safeguard the network and prevent potential data breaches.

Ključne riječi: Lokalna računalna mreža, organizacija lokalne mreže, prijetnje lokalnoj računalnoj mreži, mrežna arhitektura, zlođudni softveri, osiguranje računalne mreže

Keywords: Local computer network, local network organization, threats to local computer network, network architecture, malicious software, network security