Analiza sigurnosnih zaštitnih stijena

Šavora, Nikola

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:605966

Rights / Prava: Attribution-NonCommercial 3.0 Unported/Imenovanje-Nekomercijalno 3.0

Download date / Datum preuzimanja: **2024-05-13**

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Nikola Šavora

ANALIZA SIGURNOSNIH ZAŠTITNIH STIJENA

ZAVRŠNI RAD

Varaždin, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Nikola Šavora

Matični broj: 44734/16 - I

Studij: Primjena informacijske tehnologije u poslovanju

ANALIZA SIGURNOSNIH ZAŠTITNIH STIJENA

ZAVRŠNI RAD

Mentor/Mentorica:

Izv.prof.dr.sc. Magdalenić Ivan

Varaždin, siječanj 2022.

Nikola Šavora

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Tema rada „Analiza sigurnosnih zaštitnih stijena" upućuje na rad s programima koji služe za zaštitu i sprječavanje zlonamjernih napada koji se mogu desiti na računalu, tabletu, mobitelu ili ostalim sličnim uređajima. Ovaj rad je većim djelom praktičan. Objašnjava razlike između različitih antivirusnih programa i koje su njihove mogućnosti u sprječavanju napada na računalo.

Prije početka prikazivanja praktičnog djela, opisuje se općenito o zaštitnim stijenama. Zatim se prelazi na opisivanje karakteristika koje ima Windows Defender – blokiranje portova, blokiranje aplikacija. Nakon Windows Defender programa opisuje se Bitdefender antivirusni program gdje se opisuje blokiranje portova i aplikacija, opisuje se i stavka definiranja zabrane odlaska na određena web mjesta za određene korisnike. Kao i kod Bitdefender programa, na kraju se opisuje Kaspersky Total Security program koji ima slične karakteristike kao Bitdefender, a najveća razlika je u radu računala nakon njihove instalacije.

Sadržaj

1. Uvod

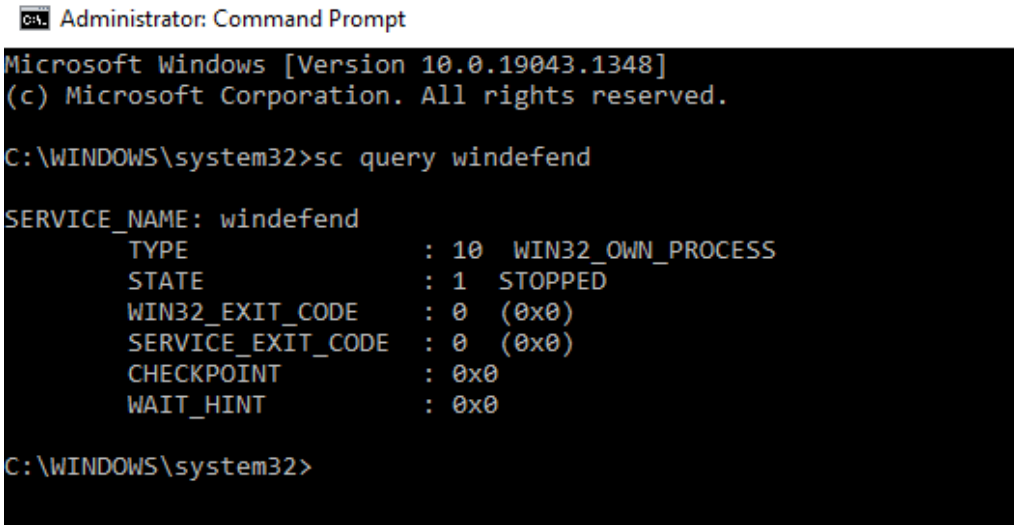
Kako se računalna tehnologija razvijala od samih početaka, od prvog računala, prvih prijenosa podataka putem interneta pa do današnjih društvenih mreža i kupovine putem interneta, tako su se razvijali i napadi na korisnička računala. Postoje razne vrste napada, virusi koji prikupljaju korisničke podatke, oštećuju programe i samo računalo korisnika… Da bi se otkrila ili spriječila prijetnja za računalo, razvojem računala i napada razvijala se i tehnologija zaštitnih stijena. Kao i kod ostalih aplikacija za računala i ovdje je slučaj da programi koji se plaćaju nude više karakteristika i mogućnosti od onih koji su besplatni. U ovom slučaju je Windows Defender besplatan pa ima manje mogućnosti od Bitdefender i Kaspersky Total Security programa.

2. Zaštitne stijene

Zaštitne stijene se danas najviše koriste za zaštitu tvrtki od virusa i napada s vanjske mreže. Paketi koji dolaze na računalo i odlaze s računala korisnika moraju proći prepreku, a ta prepreka su zaštitne stijene. Paketi se provjeravaju po odredišnoj i izvornoj IP adresi, izvornom portu, odredišnom portu i tipu protokola. Ako nešto nije u redu s bilo kojim od tih dijelova u paketu, paketi se ne dostavljaju korisniku. Zaštitne stijene su konfigurirane pravilima. Konfiguracijom se procjenjuje koji paketi su sumnjivi ili zaraženi, a koji paketi su u redu i mogu do korisnika. Putem zaštitnih stijena može se pratiti sav promet kroz mrežu i mogu se zapisivati i analizirati sve prijetnje koje se nalaze u paketima. Kod definiranja tih pravila nailazi se na tri glavna problema – konzistentnost, potpunost i kompaktnost. Pod konzistentnost se smatra da je teško postaviti poredak pravila kod primanja i slanja paketa. Nakon toga, problem nastaje prilikom potpunog pregledavanja svih vrsta prometa prema vanjskoj mreži i od vanjske mreže. Na kraju je kompaktnost za koju vrijedi da je problem smanjiti broj pravila, npr. neka pravila se mogu zanemariti pa nisu potrebna, a neka pravila se mogu kombinirati u jedno pravilo. (Alex X. Liu, 2011.)

3. Windows Defender Firewall

Windows Defender Firewall je program koji služi za zaštitu od raznih napada, kao što su virusi, malware-i, spyware i ostale slične prijetnje. On se automatski instalira kad se instalira Windows operativni sustav (Windows 7 na novije). Kad korisnik želi instalirati neki program na računalu koji sadrži malware ili kad aplikacija želi promijeniti neka svojstva ili postavke na operativnom sustavu Windows Defender automatski blokira i sugerira da se postavke na operativnom sustavu žele promijeniti. Slika niže prikazuje naredbeni redak gdje se vidi da u ovom slučaju Windows Defender nije aktivan (STATE = STOPPED), da je sustav aktivan u retku STATE bi pisalo RUNNING. Informacije o stanju programa se dobiju pokretanjem Naredbenog retka kao administrator i upisuje se komanda „sc query windefend“(Palemer, 2018).



Slika 1: Win Defender - status

4. Microsoft Defender Firewall – Postavke

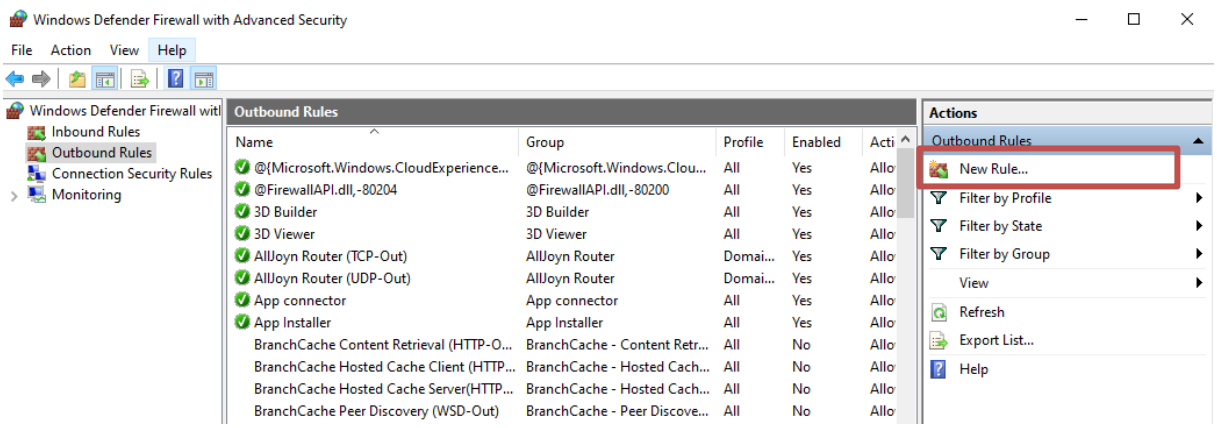
4.1. Port 443

Praktični dio o Microsoft Windows Firewall-u se bazira na blokiranju porta 443 i blokiranju aplikacije Microsoft Edge . Port 443 je port na kojem se pokreću sve stranice koje počinju sa „https://“.

Da bi se postavila jedna od tih dviju mogućnosti mora se ući u izbornik Napredne postavke (eng. Advanced settings). Zatim nam se otvara prozor sa Ulaznim i Izlaznim pravilima (eng. Inbound rules, Outbound rules).

Slika 2: Win Defender - postavke

U dijelu „Outbound rules“ definira se novo pravilo (eng. New rule)

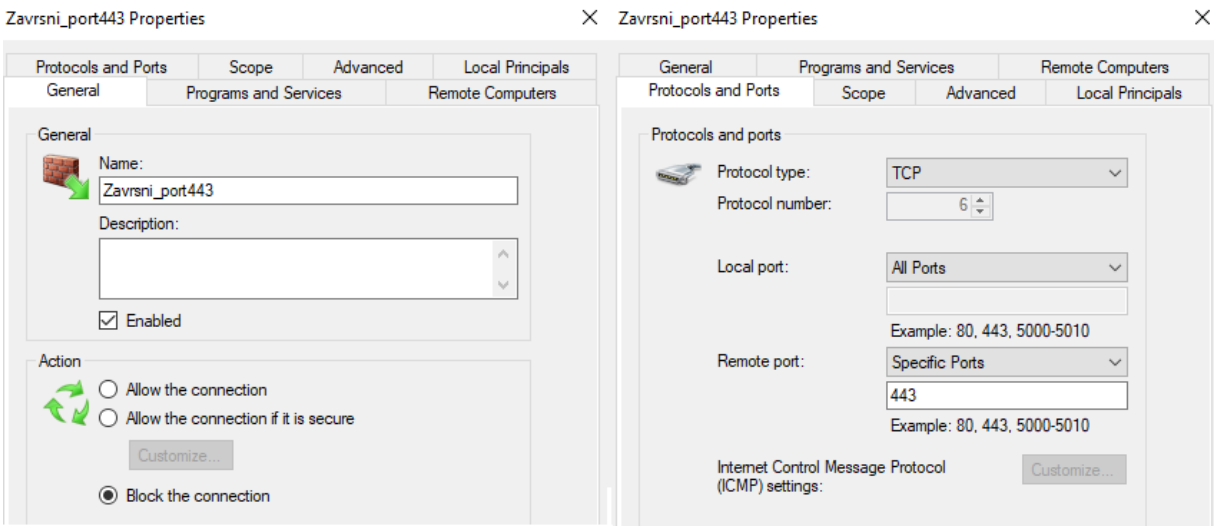


Slika 3: Win Defender - novo pravilo

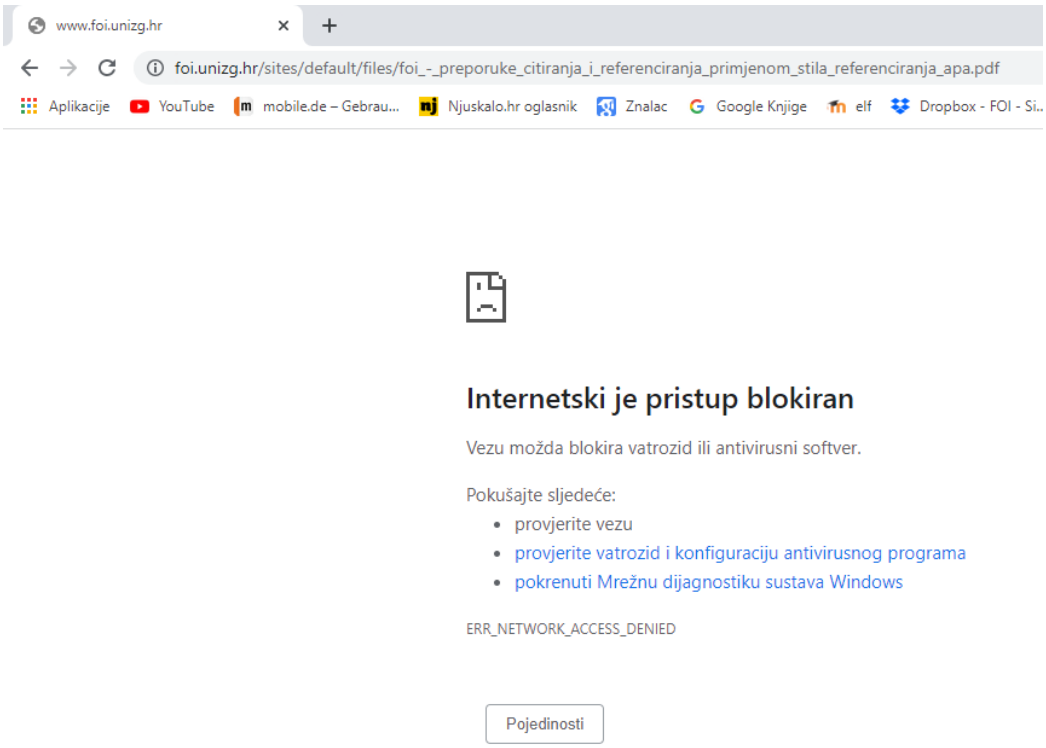
Stvaranjem pravila za blokiranje porta 443 potrebno je definirati par stavki na karticama „General“ i „Protocols and Ports“. Na kartici „ General“ u tekstualno polje pod labelom

„Name“ definiramo naziv novog pravila, u ovom slučaju je to ime „Zavrsni_port443“. Nakon toga se stavi kvačica kod oznake „Enabled“ da se uključi to pravilo. U dijelu sa akcijama (eng. Action) odabiremo 3. gumb da bi se blokirala konekcija (eng. Block the connection). U tome dijelu se može još i staviti neki opis da bi se detaljnije opisalo pravilo koje je tu definirano, zbog budućih korisnika. Nakon toga se prelazi na drugu karticu - „Protocols and Ports“.

Kartica „Protocols and Ports“ sadrži sljedeće stavke koje se definiraju da bi se zaključao port: tip protokola i lokalni port ili udaljeni port (eng. Protocol type, Local port, Remote port). U ovom slučaju se bira TCP tip protokola, a mogu se još birati UDP, IPv6, ICMPv4… Od portova se kod udaljenog porta, između svih portova, specifičnih portova i IPHTTPS (eng. All ports, Specific ports), bira Specifični port (eng. Specific ports). Nakon toga se omogući tekstualno polje u koje se mogu upisati portovi koje želimo blokirati, u ovom slučaju je to port 443. Klikom na „Apply“ se pravilo aktivira.



Slika 4: Win Defender - novo pravilo - port 443

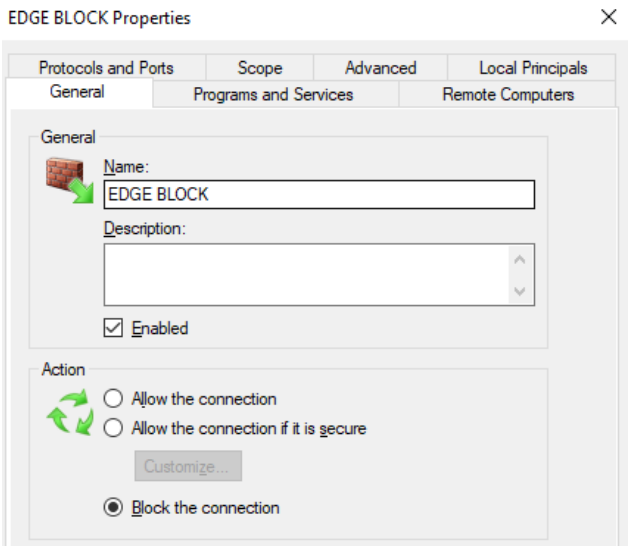


Slika 5: Win Defender - novo pravilo - port443

4.2. Windows Defender Firewall – Microsoft Edge

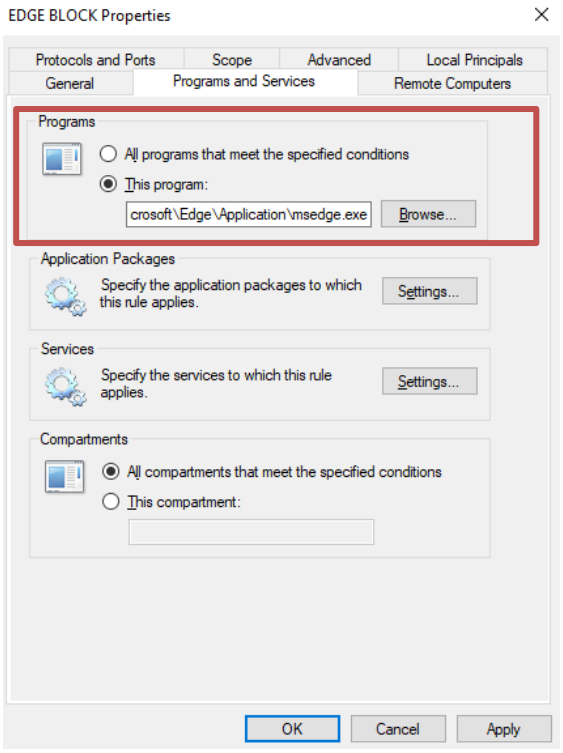
Sljedeće pravilo koje se definira je: blokiranje Microsoft Edge-a. Prvi dio je identičan kao i kod blokiranja porta 443, iz tog razloga će se postupak blokiranja porta prikazati od koraka gdje se ulazi u stvaranje novog pravila u Izlaznim pravilima (eng. Outbound Rules).

Otvaranjem novog pravila se prikazuje kartica s postavkama. Postavke se definiraju na dvije kartice: „General“ i „Programs and Services“. U kartici „General“ se definira isto kao i kod blokiranja porta 443. Unese se naziv pravila, u ovom slučaju je to „EDGE BLOCK“, stavi se kvačica na „Enabled“ i u dijelu za akciju se stavi oznaka na „Block the connection“.

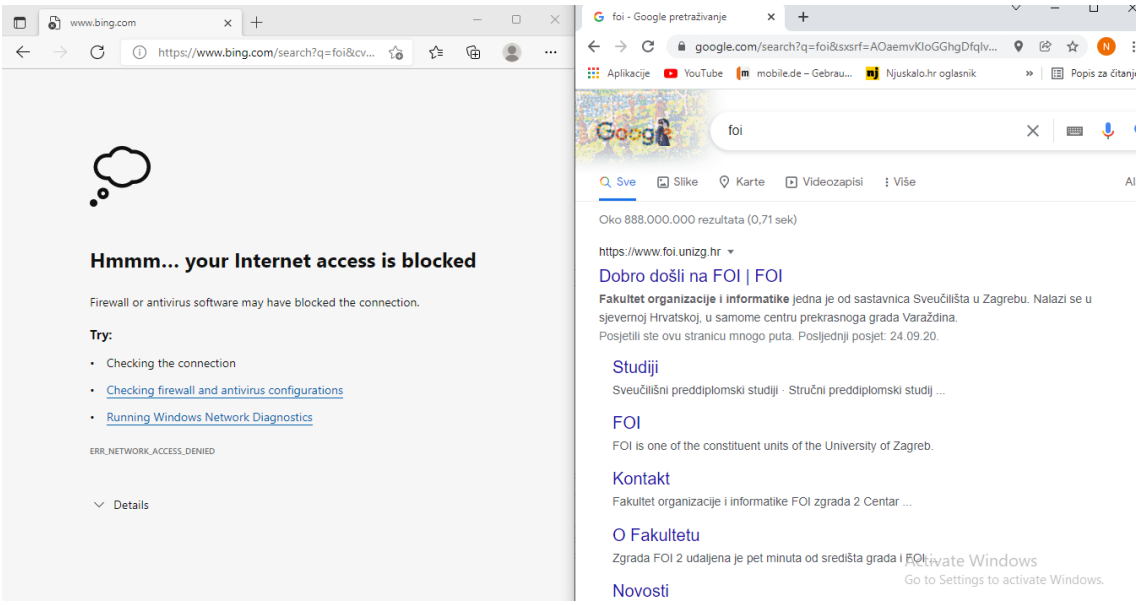


Slika 6: Win Defender - blokiranje Edge

Nakon toga se prelazi na karticu „Programs and Services“. Na tom dijelu se odabire program koji se želi blokirati da se povezuje sa mrežom. U ovom slučaju je to Microsoft Edge, pa se u dijelu „Programs“ odabere „This program:“ i upiše se poveznica do mjesta gdje je instaliran sam program na disku - C:\\Program Files (x86)\Microsoft\Edge\Application\ msedge.exe. Zatim klik na „Apply“ i pravilo je definirano i pokrenuto.



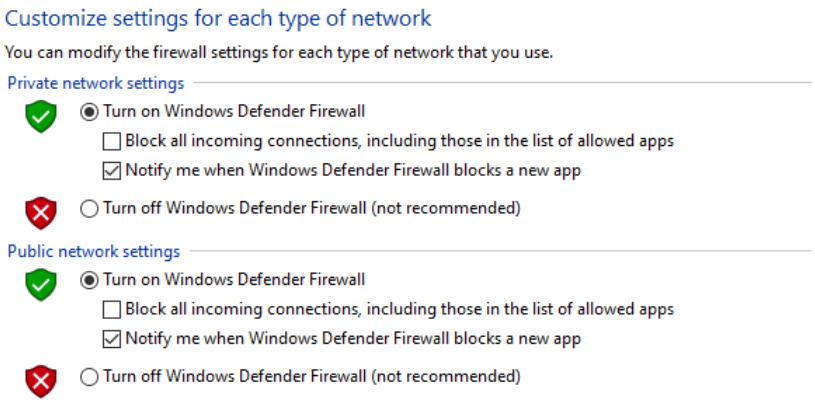
Slika 7: Win Defender - blokiranje Edge 2



Slika 8: Win Defender - Edge - Chrome

4.3. Windows Defender Firewall – lokalna i vanjska mreža

Windows Defender Firewall je moguće isključiti ovisno o mreži. Zaštitne stijena se može isključiti unutar lokalne mreže, a može se isključiti i na vanjskoj mreži. Ukoliko je program uključen za lokalnu mrežu, vanjsku mrežu ili obje mreže, može se birati između dvije opcije. Prva opcija je da se blokiraju sva povezivanja na sve aplikacije, čak i one aplikacije koje su na listi za dopuštenja. Druga opcija je da se šalje obavijest kada „Firewall“ blokira neku aplikaciju. Te dvije opcije mogu istovremeno biti uključene.



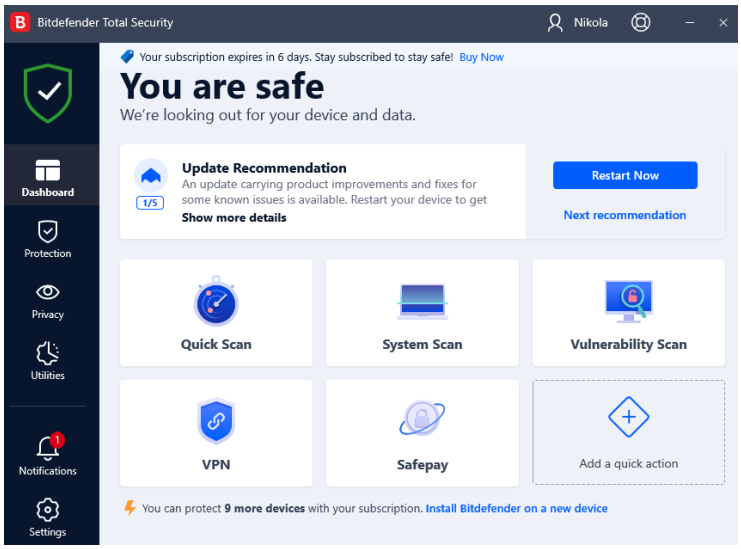
Slika 9: Win Defender - lokalna i vanjska mreža

5. Bitdefender

Bitdefender je antivirusni program koji je među boljim programima za zaštitu od virusa i napada na računala. Sama tvrtka Bitdefender se osamostalila 2007. godine kad se odvojila od Softwin tvrtke koja je nastala 1990-ih kao start-up za zaštitu od računalnih virusa u Rumunjskoj (Bitdefender, 2021).

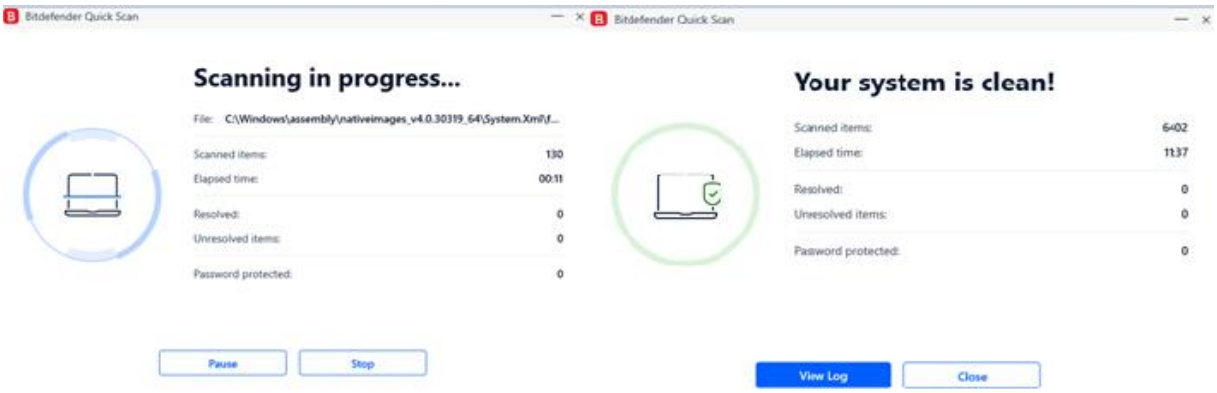
5.1. Bitdefender – Dashboard

Program Bitdefender na početnoj strani nudi korisniku da si sam posloži 5 stavki koje najčešće koristi i koje su mu najpotrebnije kod korištenja antivirusnih programa. Dolje na slici se nalazi mojih 5 stavki koje su odabrane za prikaz na početnoj strani programa.



Slika 10: Bitdefender - početna

Prva stavka je „Quick scan“ koja omogućuje korisniku da pokrene brzo skeniranje kroz sve datoteke i aplikacije koje se nalaze na računalu korisnika. Ukoliko je računalo „čisto“ i bez virusa i prijetnji program nakon skeniranja izbaci obavijest o stanju računala. U mom slučaju je brzo skeniranje trajalo 11 minuta i 37 sekundi i prikazuje se da je računalo čisto.



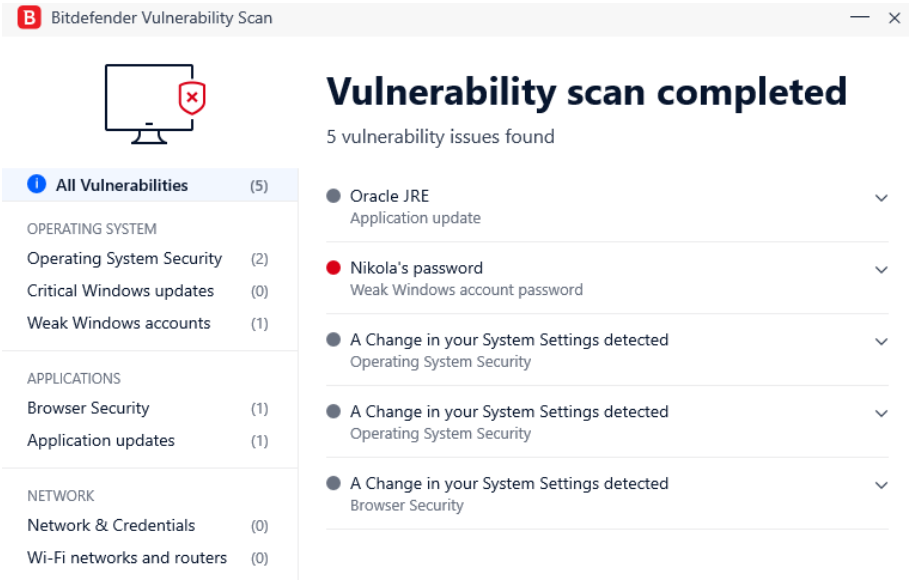
Slika 11: Bitdefender - Quick scan

Sljedeća stavka na početnoj strani je „System scan“ koja radi slično kao i „Quick scan“, ali kroz datoteke i aplikacije prolazi puno detaljnije i temeljitije nego brzo skeniranje (eng. Quick Scan). Treća stavka je „Vulnerability scan“ koja na računalu korisnika traži slabosti. Kod skeniranja se slabosti traže na tri područja.

Prvo su slabosti na operativnom sustavu. U mojem slučaju slabosti na operativnom sustavu su automatska prijava na računalo, automatsko pokretanje „driver-a“ nakon priključenja memorijske kartice ili USB memorije i slaba lozinka na Windows računu.

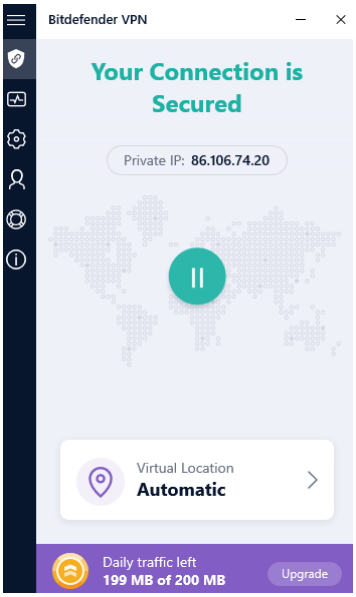
Drugi dio su slabosti aplikacija. Na skeniranju je uočena jedna slabost sa sigurnosnom zonom. Microsoft Edge dopušta svim korisnicima da pokreću sve web stranice, čak i one sumnjive. Druga slabost je stara vezija aplikacije Oracle JRE. Bitdefender nakon pronalaska stare verzije nekog programa preporučuje da se program ažurira na noviju verziju.

Treći dio skeniranja su slabosti mreže kod kojih nije bilo pronađeno nikakvih slabosti i i kod mreže je sve u redu.



Slika 12: Bitdefender - Vulnerability scan

Četvrta stavka na početnoj strani Bitdefender-a je VPN koji nam omogućuje kompletnu anonimnost prilikom pretraživanja interneta. Lokacija VPN-a se može birati između pedeset država, ali to je omogućeno na „Premium“ verziji.

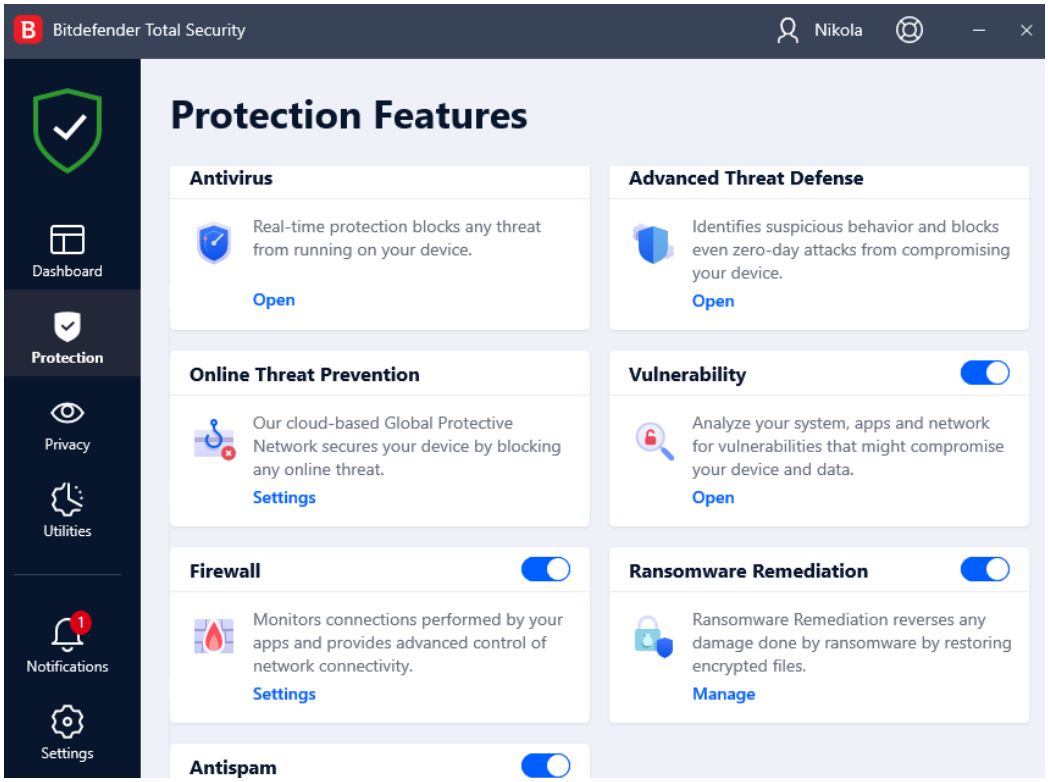


Slika 13: Bitdefender - VPN

Zadnja stavka na početnoj stranici Bitdefender-a je „Safepay“ koja pruža dodatnu sigurnost kod plaćanja prilikom Internet kupovine. Kod internet kupovine se daju osobni podaci i broj kartice pa je dobro imati dodatnu zaštitu prilikom davanja tih podataka.

5.2. Bitdefender – Protection

U Bitdefender-u pod dijelom „Protection“ se nalaze sljedeće stavke: Antivirus, Advanced Threat Defense, Online Threat Prevention, Vulnerability, Firewall, Ransomware Remediation i Antispam. Neke stavke su objašnjene u „Dashboard“ dijelu tako da će se ovdje opisivati ostali dijelovi zaštite.



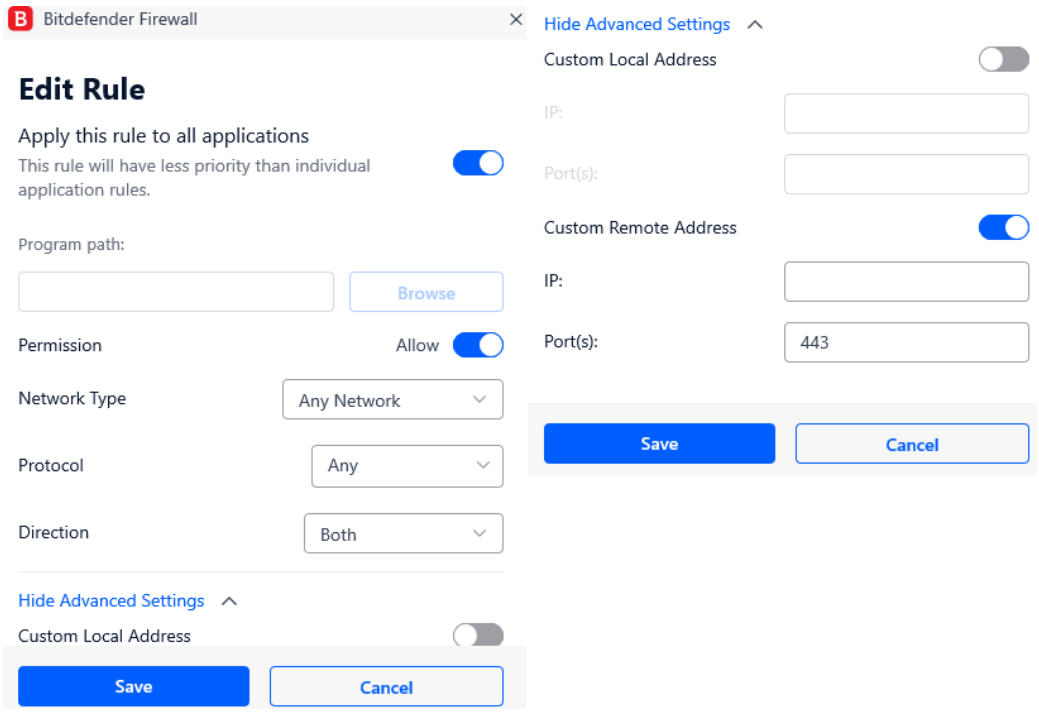
Slika 14: Bitdefender - Protection

- Antivirus - unutra se nalaze „Quick scan“ i „System scan“ dodatno se mogu postaviti napredne postavke što je sve potrebno skenirati (mogu se stavljati neke iznimke za određene aplikacije)
- Advanced Threat Defense – prikazuje je li bilo kakvih prijetnji zadnjih 90 dana.
- Online Threat Prevention – služi za postavke kod zaštite internetske veze. Provjerava se svaka web stranica i ono što se skida. Isto tako ima opciju provjere je li web stranica zlonamjerna u vezi novčanih prevara. Može se podesiti i skeniranje dolaznih i odlaznih mailova.
- Ransomware Protection – „čisti“ datoteke koje su oštećene od strane „Ransomwer-a“.
- Antispam – ima mogućnost blokiranja određenih e-mail adresa, kao što su adrese sa čudnim znakovima.

5.3. Bitdefender – Firewall

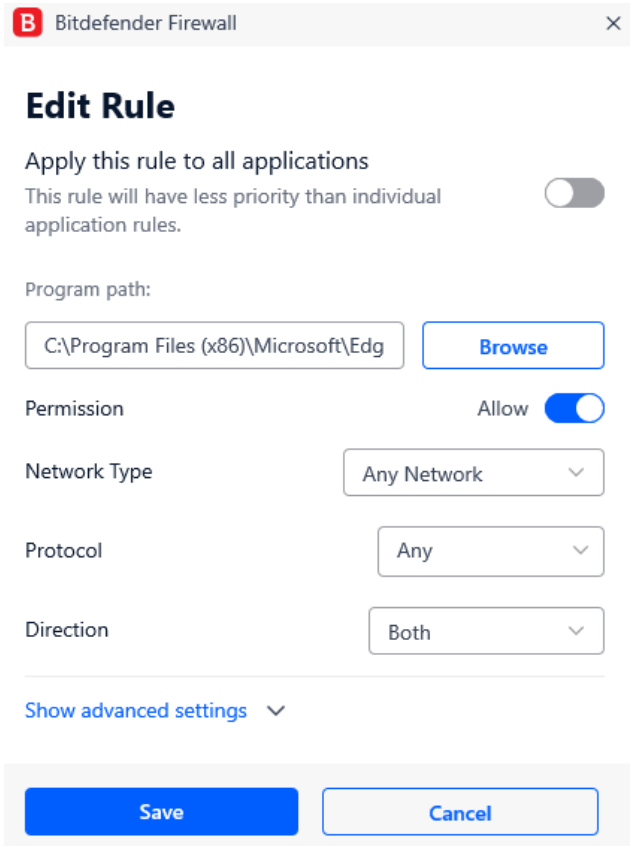
Zaštitna stijena se u Bitdefender-u nalazi u dijelu za zaštitu (eng. Protection). Taj dio će se opisivati opširnije nego ostali dijelovi radi usporedbe sa Windows Defender Firewall-om.

Kod zaštitnih stijena se mogu definirati pravila slično kao i kod Windows Defender Firewall-a, samo je u Bitdefender programu taj dio bolje prilagođen korisniku. Stvaranjem novog pravila može se birati želi li se pravilo primijeniti na sve aplikacije ili samo određenu aplikaciju. Da bi se postupak prenio na sve aplikacije uključuje se „Apply this rule to all applications“. Zatim se „Premission“ mijenja iz „Allow“ u „Deny“ i može se birati vrsta mreže, protokol i hoće li to biti pravilo za ulazni ili izlazni smjer podataka, ili oboje. Sljedeći korak su napredne postavke (eng. Show advanced settings) - tu se definira port ili IP adresa koji se žele blokirati.

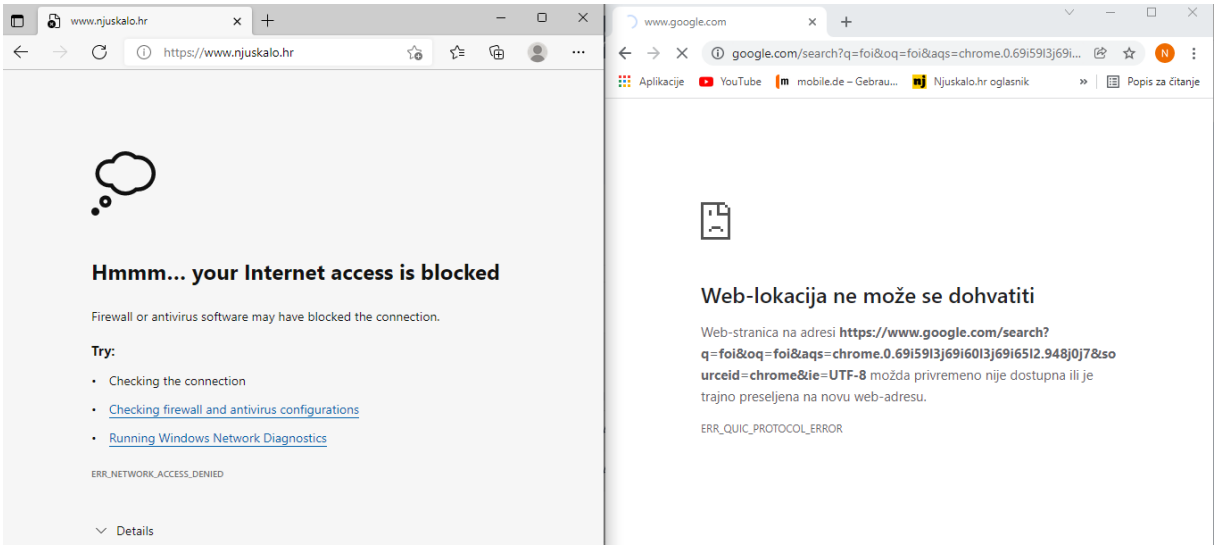


Slika 15: Bitdefender - port 443

Kod definiranja pravila na određenoj aplikaciji „Apply this rule to all applications“ makne se i stavi se poveznica mjesta gdje je instalirana aplikacija koja će se blokirati. Blokira se Microsoft Edge pa se stavi poveznica na mjesto gdje je Edge instaliran i „Permission“ se promijeni iz „Allow“ u „Block“.



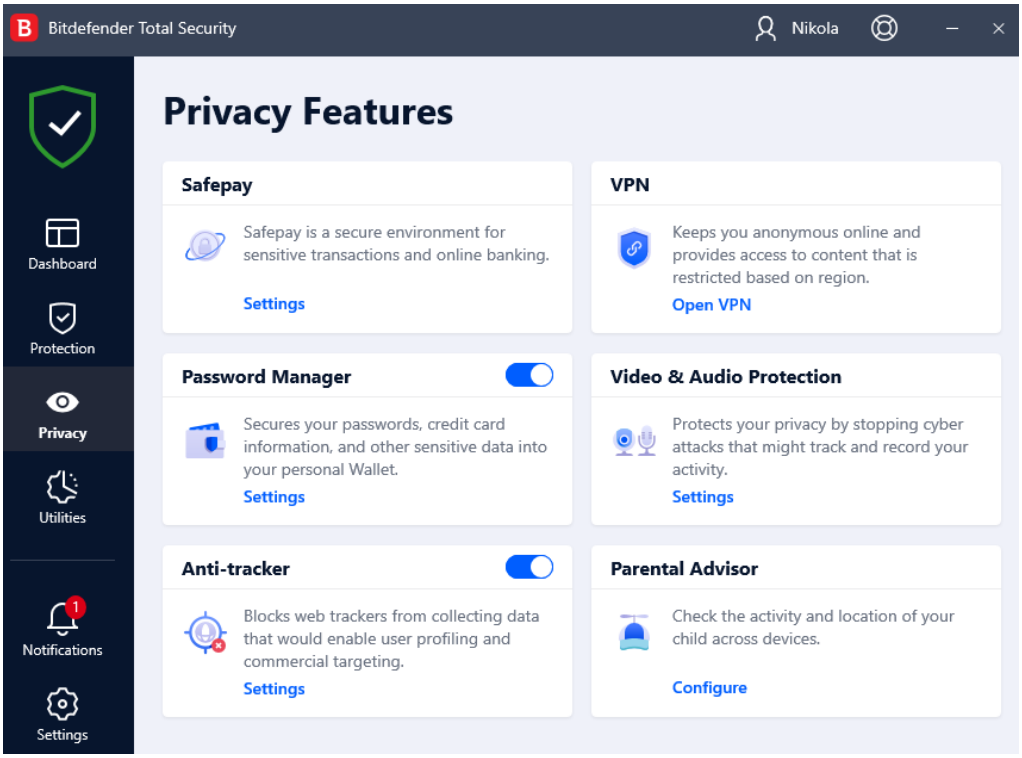
Slika 16: Bitdefender - pravila



Slika 17: Bitdefender - blokiranje Edge i Port 443

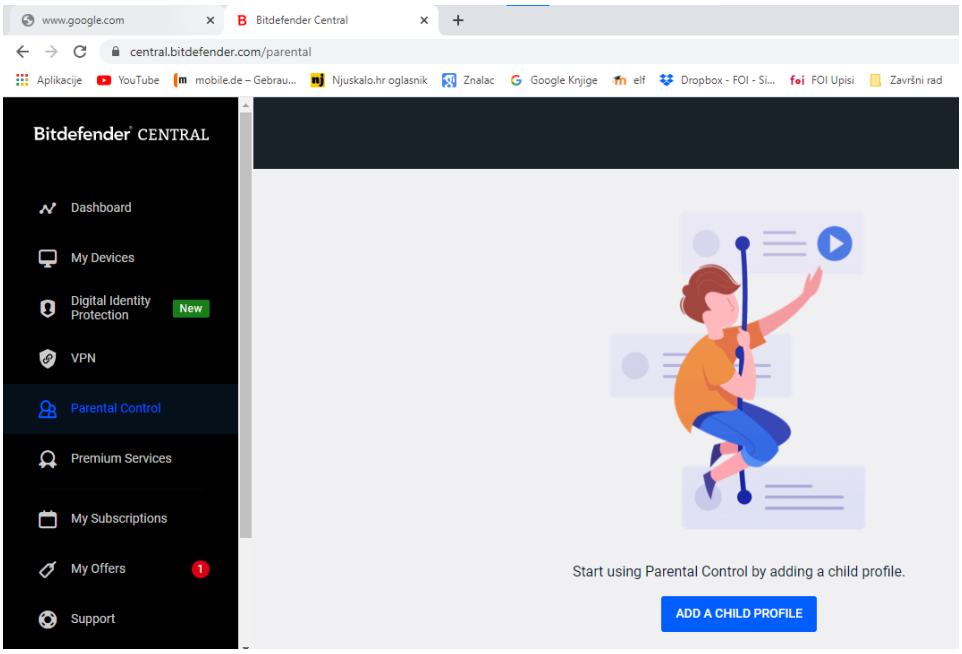
5.4. Bitdefender – Privacy

U dijelu za privatnost se nalaze „Safepay“ i VPN koji su objašnjeni na dijelu početne stranice Bitdefender-a. Ostali dijelovi u „Privacy“ dijelu su „Password Manager“ koji služi za pohranu lozinki i ostalih tajnih informacija. Zatim ima i „Video & Audio Protection“ koji sprječava napade i ne dopušta da se vide aktivnosti korisnika računala. Na taj način se može spriječiti praćenje na web mjestima, taj dio se zove „Anti-tracker“. Na kraju je „Parental Advisor“ koji ima zanimljive značajke pa će se njega malo bolje opisati.



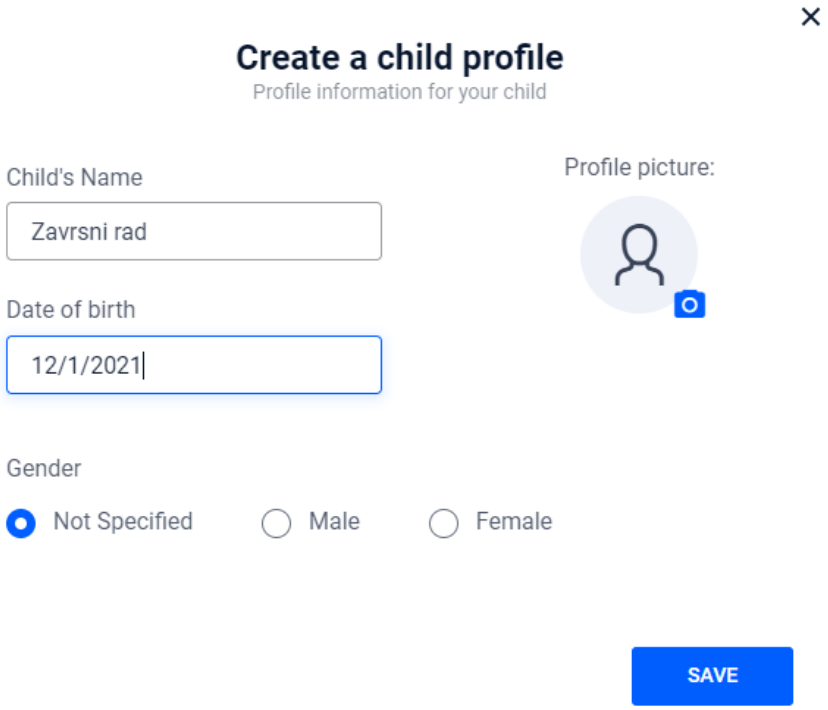
Slika 18: Bitdefender - Privacy

Pokretanjem „Parental Advisor“ ikone Bitdefender se pokreće u web pregledniku i omogućuje da se napravi određeni profil za pojedinca sa određenim dopuštenjima.



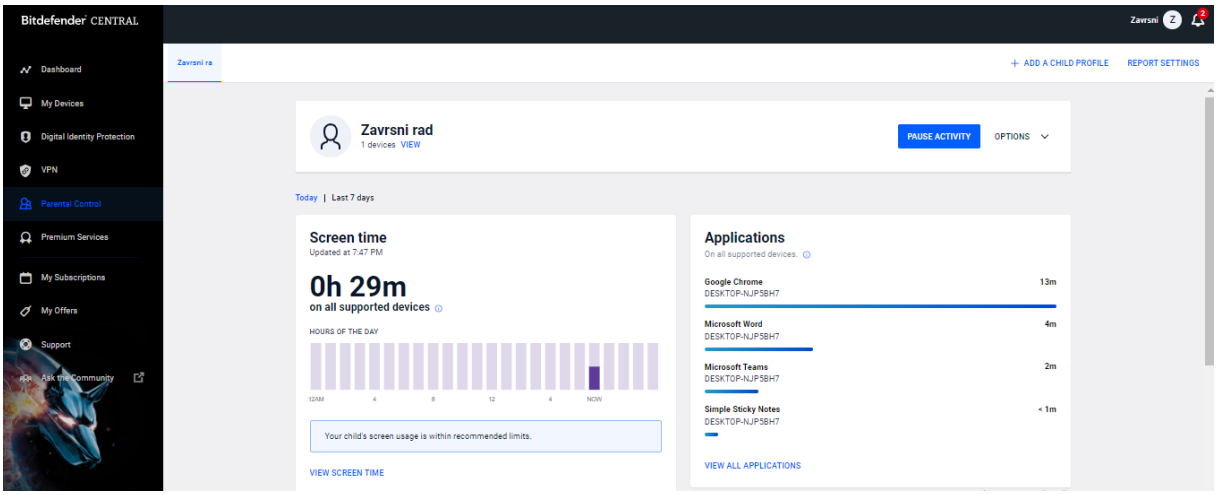
Slika 19: Bitdefender - Parental Advisor

Klikne se na „Add a child profile“ i upiše se ime korisnika, datum rođenja i spol.



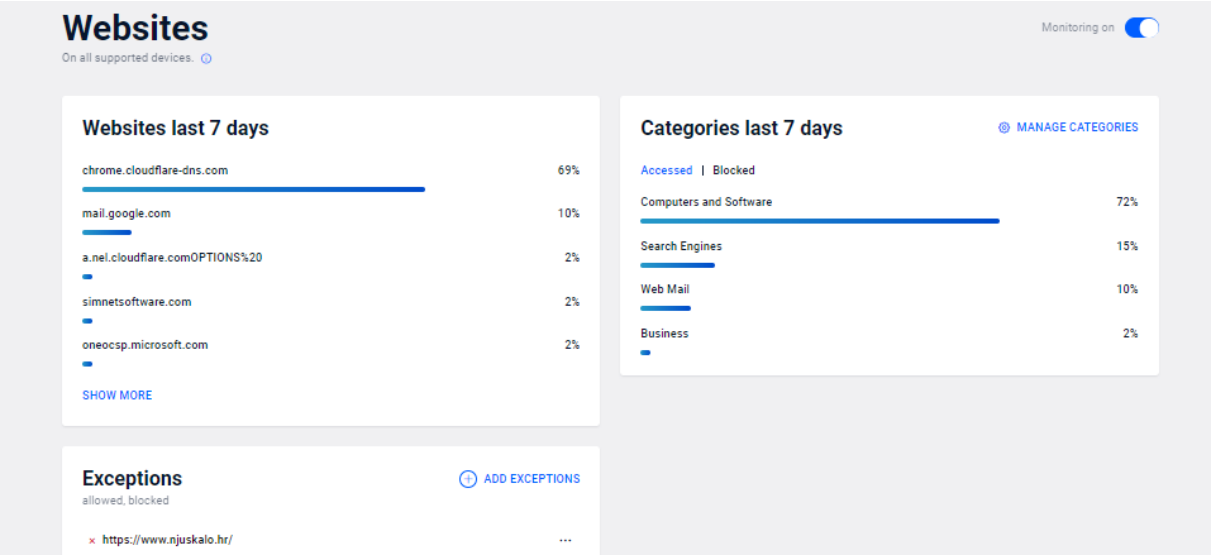
Slika 20: Bitdefender - Child profile

Taj dio je namijenjen roditeljima da djeci ograniče kretanje internetom i za praćenje provedenih sati na internetu tijekom dana. Na početnom ekranu nekog profila se vide informacije o vremenu provedenom na računalu. Evidencija je po danima u tjednu i može se vidjeti zadnjih 30 dana provedenih na računalu. Nakon toga je područje za aplikacije. Moguće je vidjeti vrijeme provedeno na određenim aplikacijama koje korisnik koristi. Sljedeće područje su web mjesta kroz koje se korisnik kreće i tu postoji mogućnost zabrane pristupa određenim web mjestima. Taj dio je pobliže opisan u nastavku rada. „Parental Advisor“ ima još mogućnost otkrivanja lokacije korisnika ako je u postavka uređaja na kojem je instalirana aplikacija aktivirana lokacija. Ako je Bitdefender instaliran na mobilnom uređaju korisnika mogu se vidjeti i novi kontakti koji se dodaju.



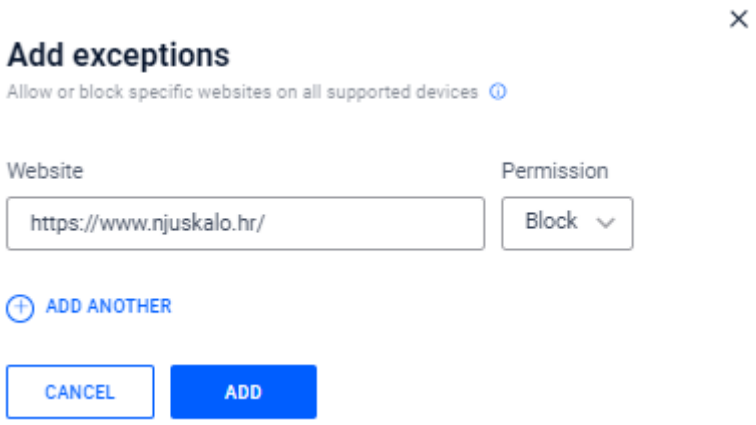
Slika 21: Bitdefender - Parental control

Da bi se postavila zabrana na neko web mjesto potrebno je promijeniti postavke u „Websites activitiy“. U ovom primjeru se uzima web mjesto njuškalo.hr na koje se stavlja zabrana pregleda.



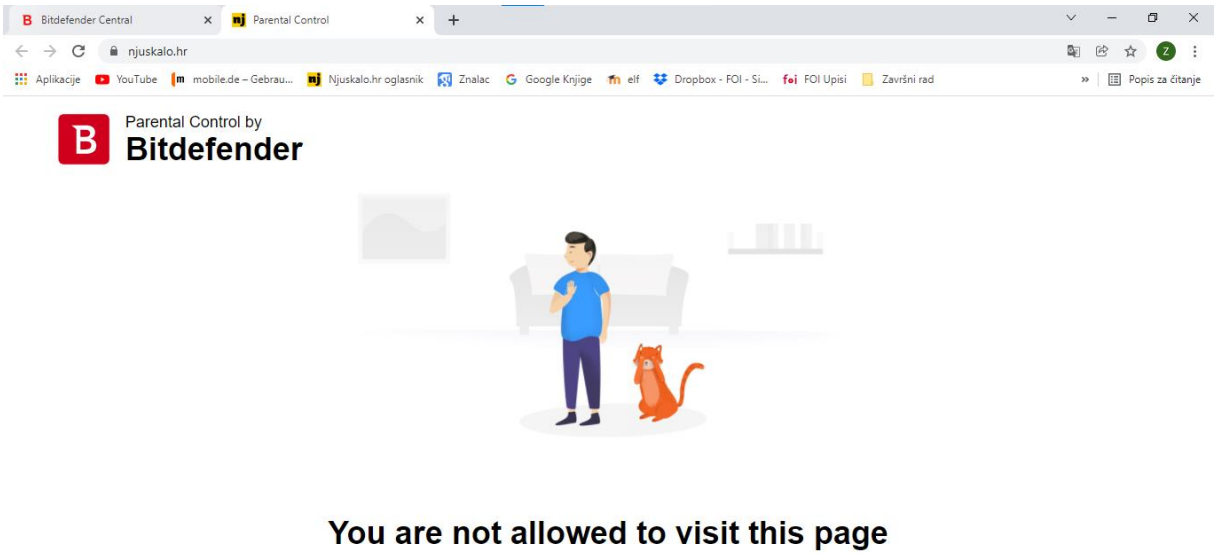
Slika 22: Bitdefender - Websites activity

U donjem dijelu stranice se nalaze „Iznimke“ u kojima definiramo želimo li neko web mjesto zabraniti ili dopustiti pristup. Klikom na „Add Exceptions“ se otvara prozor gdje se upisuje URL web mjesta i odabire karakteristika „Allow“ ili „Block“ kojom se odlučuje želi li se aplikacija blokirati za korisnika ili želi li se dopustiti pristup aplikaciji.



Slika 23: Bitdefender - Iznimke

Nakon definiranja iznimke u „Parental Control“, odlaskom na web mjesto, njuškalo.hr, prikazuje se zabrana ulaska na to web mjesto.



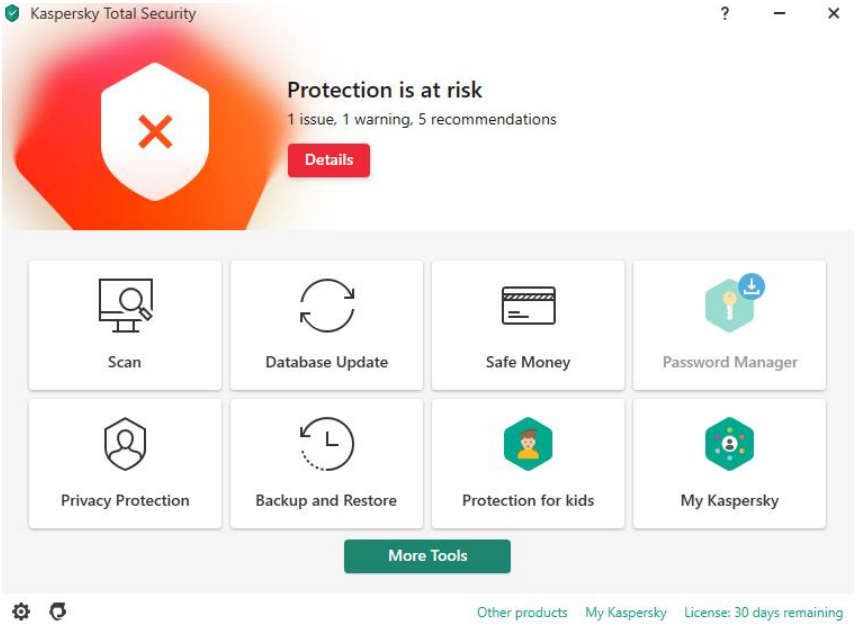
Slika 24: Bitdefender - blokiranje web mjesta

6. Kaspersky – Total Security

Kaspersky je globalna tvrtka koja je osnovana 1997. godine. Pruža poslovnim korisnicima, javnim službama i korisnicima kod kuće rješenja i servise za zaštitu od zlućudnih napada na korisnički sistem i mreže. (https://www.kaspersky.com/about)

U ovom dijelu rada se opisuje Kaspersky – Total Security antivirusni program. Također se uspoređuje s ostala 2 programa – Windows Defender i Bitdefender. Postavke koje se uspoređuju su blokiranje porta 443, blokiranje aplikacije (Microsoft Edge) i blokiranje Web mjesta (Njuškalo.hr)

Na prvoj stranici Kaspersky antivirusnog programa se nalazi 8 mogućnosti koje su najčešće korištene od strane korisnika. Te stavke se ne definiraju za svakog korisnika posebno, nego je tako definirano u programu. U usporedbi sa Bitdefender-om koji nije prikazao nikakav rizik za računalo, Kaspersky je pronašao jedan problem, jedno upozorenje i 5 preporuka.



Slika 25: Kaspresky - Početna

Klikom na „Scan“ prikažu nam se mogućnosti skeniranja računala na viruse i prijetnje. Prvi u izborniku je „Quick scan“ koji omogućuje brzo skeniranje kroz sistem i provjerava mjesta gdje se najčešće sakrivaju malware-i. Ako pronađe bilo kakvu prijetnju obavijesti korisnika i preporuča „Full scan“ koji je sljedeći na listi u izborniku skeniranja. Odabirom na „Full scan“ skeniranje računala provjerava se cijelo računalo. Postoji mogućnost da će se kod skeniranja znatno usporiti sistem i skeniranja traje dosta dugo. Nakon skeniranja računala računalo se može automatski ugasiti, staviti u „sleep mode“, može se i staviti da bude u „hibernation mode“, da se restarta ili da se ostavi upaljeno.

Sljedeća mogućnost je „Selective scan“ koja omogućuje korisniku da odabere mape ili aplikacije koje želi skenirati. Zatim je mogućnost skeniranja vanjskih jedinica kao što su prijenosni tvrdi diskovi ili USB diskovi. Ako ništa nije priključeno neće se niti prikazati mogućnost „Removable drives scan“. Od ostalih mogućnosti skeniranja tu su još i „Vulnerability scan“, „Scan from context menu“ i „Background scan“.

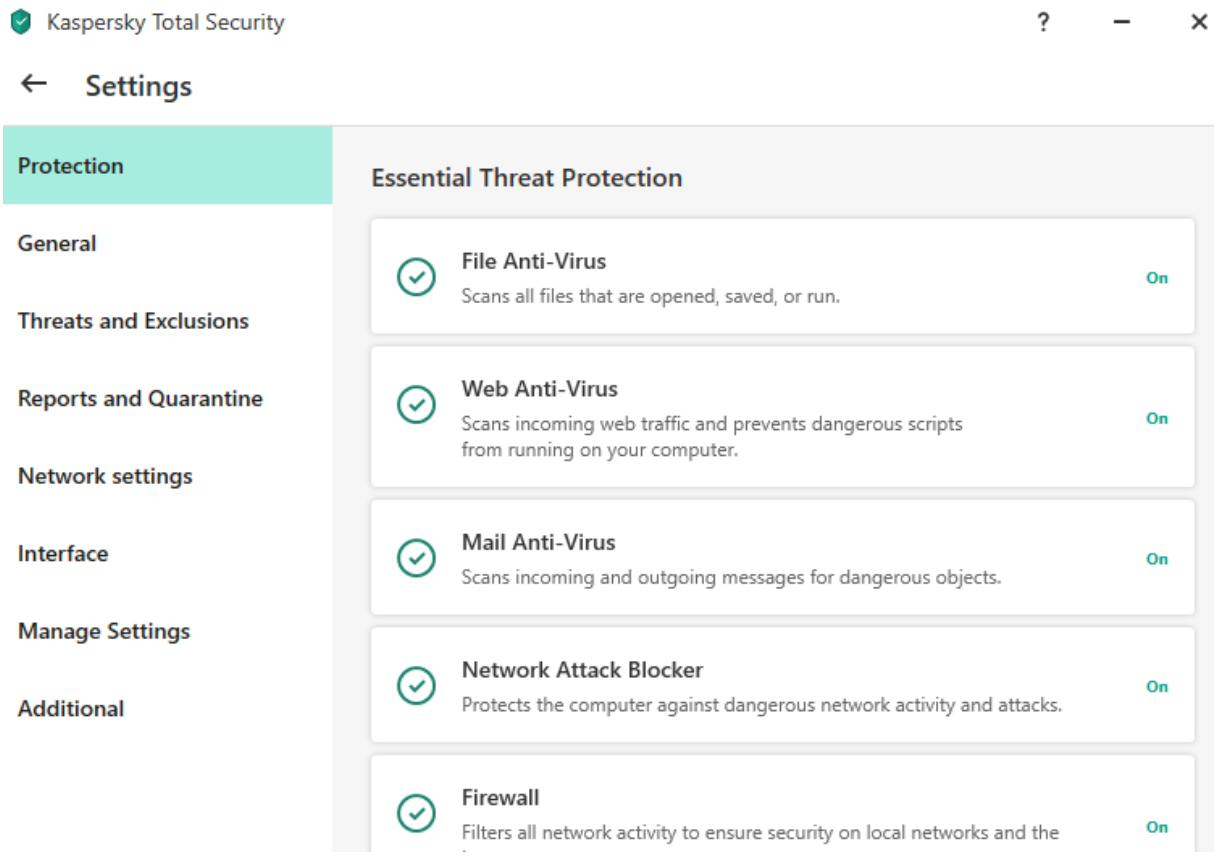
„Database Update“ omogućuje korisniku da ažurira cijeli antivirusni program ako je došlo do kakve nadogradnje na programu. Nakon toga u izborniku se nalazi „Safe money“ gdje program prvo provjera je li siguran web preglednik gdje se unose podaci za obavljanje kupnje putem interneta, a zatim obavlja i ostale provjere i javlja korisniku je li sigurno plaćanje putem provjerenog web mjesta. Ostale mogućnosti u izborniku su „Password Manager“ koja je zadužena za upravljanje lozinkama, „Privacy Protection“ omogućuje korisniku sigurno

korištenje web kamere i sigurnu pretragu web stranica bez prikupljanja podataka o korisniku. „Backup and Restore“ daje mogućnost korisniku da pohrani važne podatke u slučaju kvara računala. „Protection for kids“ će se detaljnije opisati u radu, a služi za ograničavanje pristupa aplikacija određenim korisnicima. Zadnja mogućnost je „My Kaspersky“ gdje si korisnik sam prilagođava i dodaje mogućnosti koje ima program.

U usporedbi sa Bitdefender-om, početna stranica Bitdefender ima mogućnost mijenjanja ikona na početnom zaslonu, dok su kod Kaspersky programa ikone fiksne i korisnik si ih ne može prilagoditi. Iz tog se razloga kroz Bitdefender može lakše kretati, ako si to korisnik dobro pripremi.

Klikom u glavnom izborniku na „More Tools“ otvaraju se i ostale mogućnosti Kaspersky Total Security programa i nalaze se ostali dijelovi programa: “Security“, „My Network“, „Manage applications“, „Dana Protection“, „Clean and optimize“.

6.1. Kaspersky – postavke



Slika 26: Kaspersky - Settings

Protection – Unutra se nalaze razne mogućnosti skeniranja na viruse, kao što su skeniranje svih datoteka i aplikacija, skeniranje mail-ova, zaštita od internetskih napada, uključivanje i isključivanje „Firewall-a“, kontroliranje pristupa aplikacijama…

General – upravljanje osnovnim postavkama programa, poput automatskog uključivanja programa nakon što se uključi računalo, prekid skeniranja kad prijenosno računalo radi na bateriji, prekid skeniranja računala kad je na računalu pokrenuta video igra…

Threats and Exclusions – u ovom dijelu se određuje kojim aplikacijama korisnik „vjeruje“ i definira programu da nije potrebno skeniranje tih aplikacija.

Reports and Quarantine – odabire se na koji rok program pohranjuje podatke o skeniranju sistema i koja je veličina tih podataka.

Network settings – odabire se vrsta skeniranja na web-u. Definiraju se web mjesta kojima korisnik vjeruje.

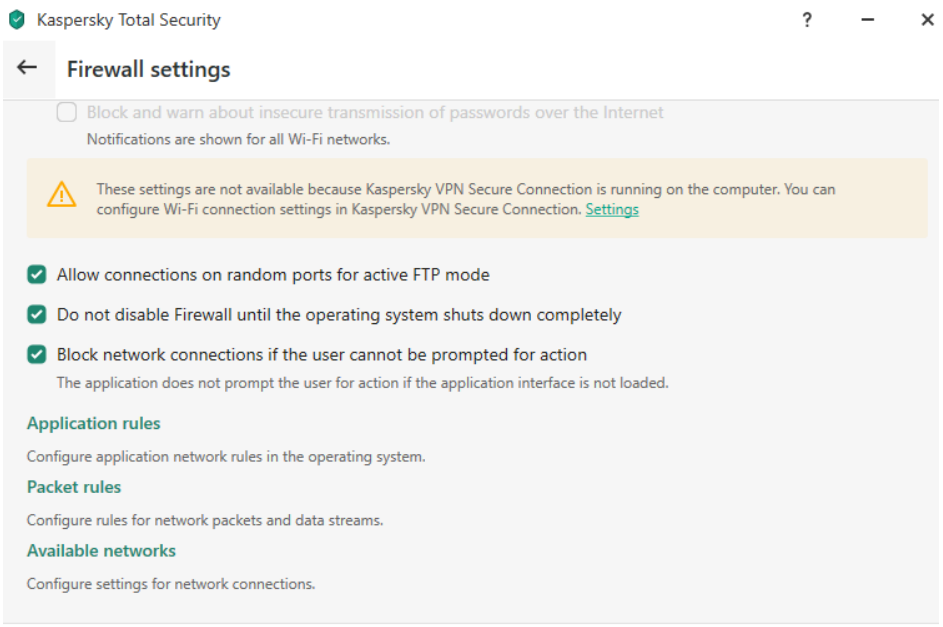
Interface – definira se izgled i ponašanje korisničko sučelja. Može se promijeniti izgled ikone aplikacije, bira se jezik aplikacije. Korisnik može birati želi li dobivati obavijesti od programa.

Manage settings – postavke (ograničeno kretanje po aplikacijama i web mjestima) koje napravi korisnik na jednom računalu mogu se prebaciti na ostala računala pa je to primjereno za tvrtke koja uzimaju određena dopuštenja djelatnicima za kretanje po web-u.

Additional – dodatne postavke za sigurnosnu tipkovnicu.

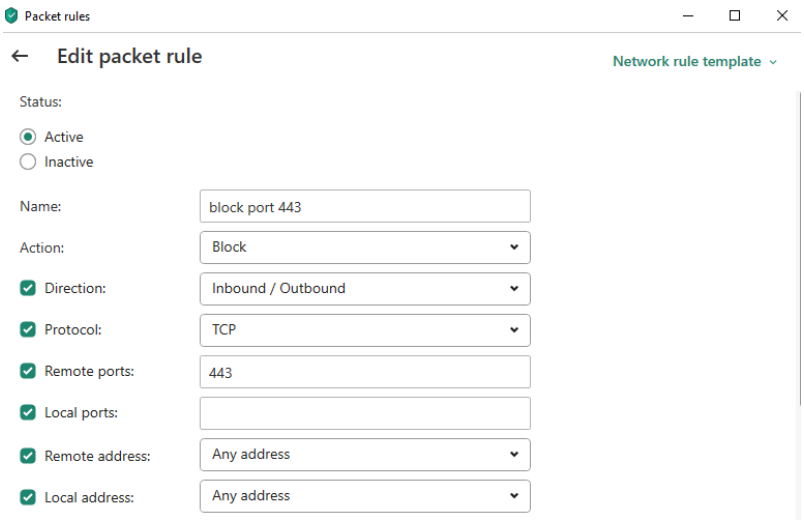
6.2. Kaspersky – blokiranje porta 443

Blokiranje porta kod Kaspersky Total Security programa se nalazi u postavkama programa, u „Protection“ dijelu. Klikom na „Firewall“ otvara se prozor sa postavkama zaštitne stijene. Zatim je potrebno otvoriti u aplikaciji prozor – „Packet rules“.



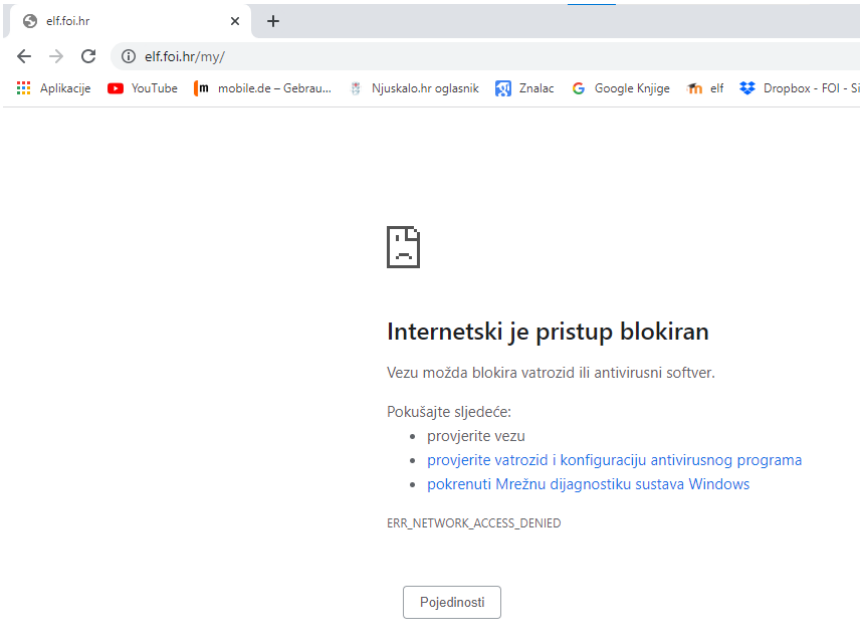
Slika 27: Kaspersky - port 443

Otvara se prozor sa raznim vrstama paketa koji se šalju i koje je moguće blokirati ili dati dopuštenje za slanje. Klikom na „Add“ dodaje se novo pravilo koje je nazvano „block port 443“. Nakon naziva pravila definira se dopuštenje, „Allow“ ili „Block“. U ovom slučaju se odabere „Block“, ostavi se pravilo da bude za dolazne i odlazne pakete. Zatim se bira protokol koji se postavlja na TCP i u „Remote ports“ se dodaje broj porta koji se blokira – 443.



Slika 28: Kaspersky - port 443 - Packet rules

Blokiranje web mjesta koja počinju sa „https:\\“ radi na sva 3 programa koja su se testirala, ali kod Kaspersky programa korisniku je najteže pronaći gdje se blokiraju portovi.

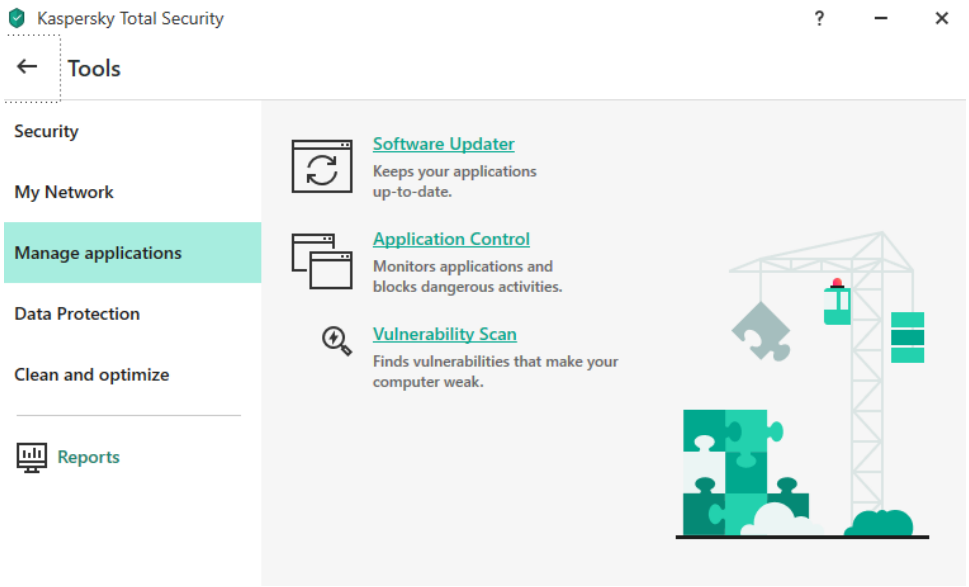


Slika 29: Kaspersky - port 443 - elf.foi

6.3. Kaspersky – blokiranje Edge

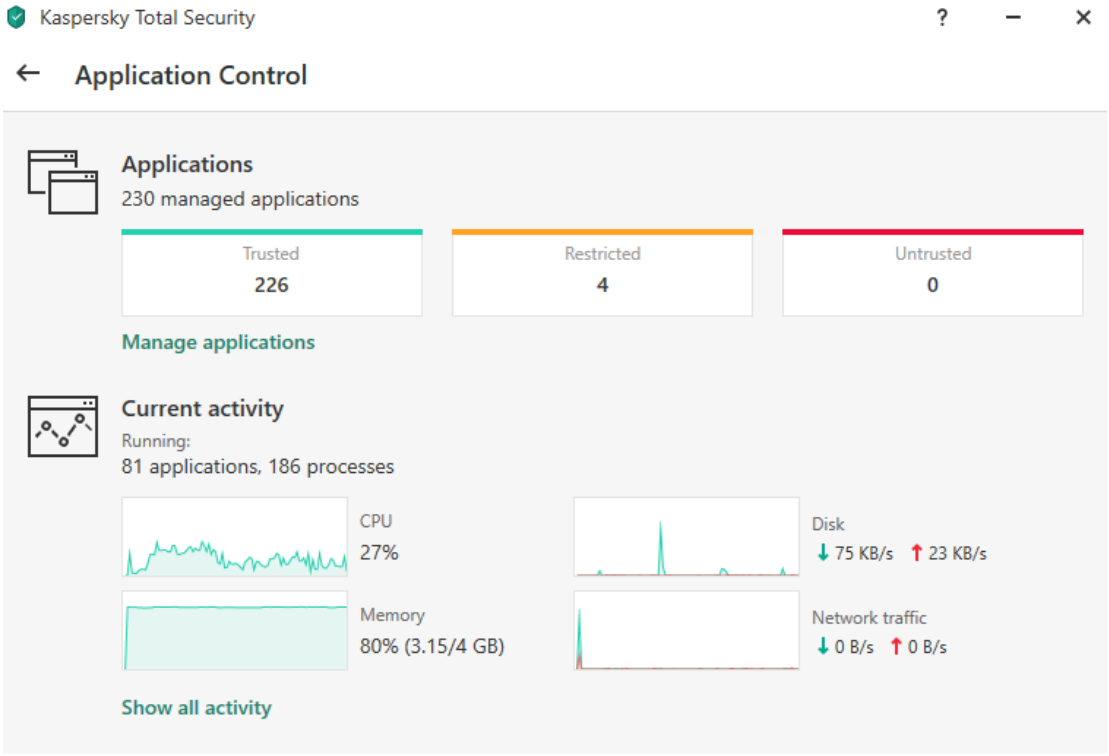
Blokiranje aplikacija, od svih testriranih programa, najlaške je na Kaspersky Total Security programu jer Kaspersky nudi mogućnost odabira blokiranja programa bez da se pronalazi mjesto instalacije programa, Kaspersky ga sam pronađe i daje mogućnost blokiranja.

U glavnom sučelju programa kad se klikne na „More Tools“ i nakon toga se ode u „Manage applications“ od 3 odabira koja se nude odabire se „Application Control“.



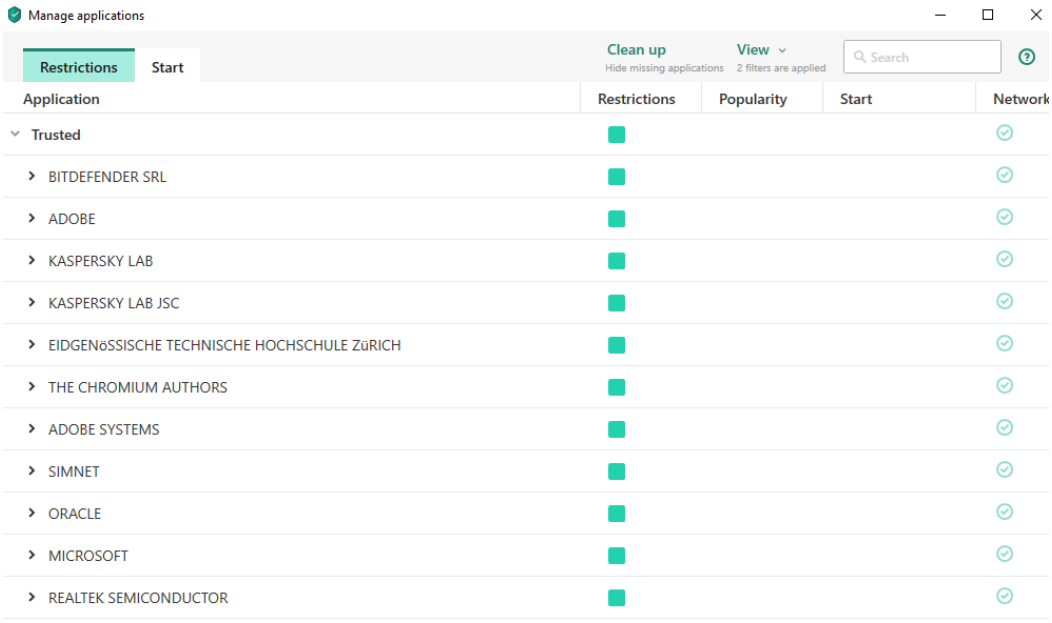
Slika 30: Kaspersky - blokiranje Edge

Otvara se prozor koji pokazuje koliko aplikacija se „vjeruje“, koliko ih nema pristup i koliko aplikacija se „ne vjeruje“. Ispod se nalaze grafovi aktivnosti procesora, memorije, diska i interneta.



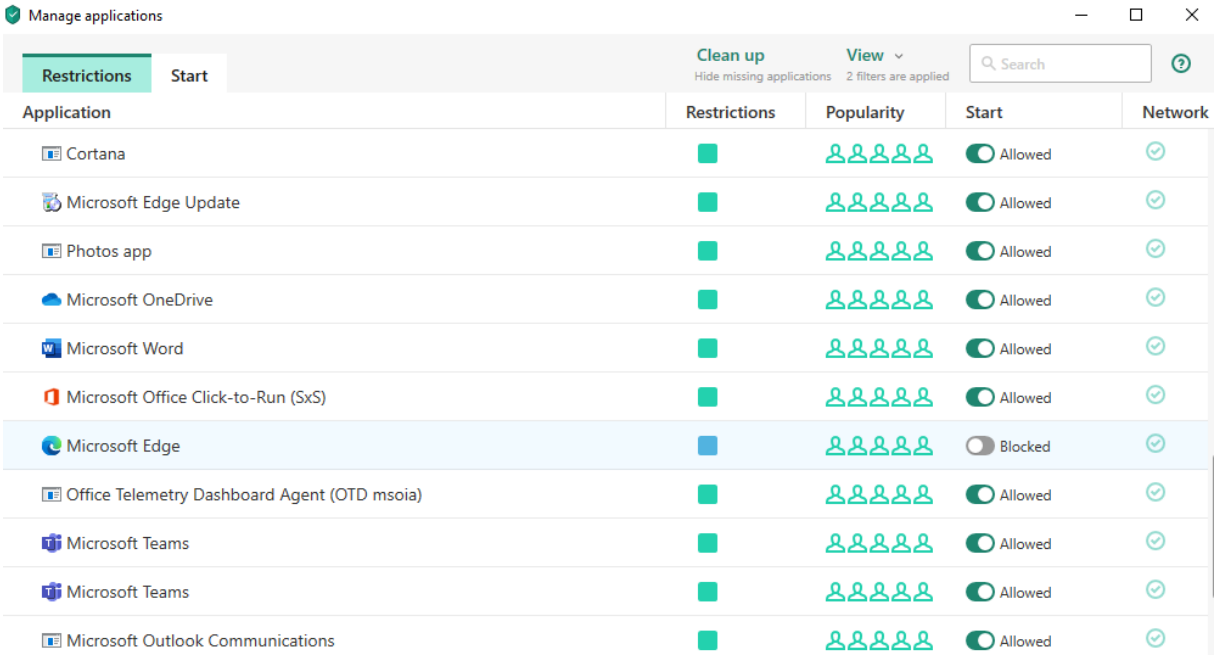
Slika 31: Kaspersky - Application Control - Edge

Klikom na „Manage applications“ se vidi detaljniji pregled svih aplikacija koje korisnik koristi na računalu.



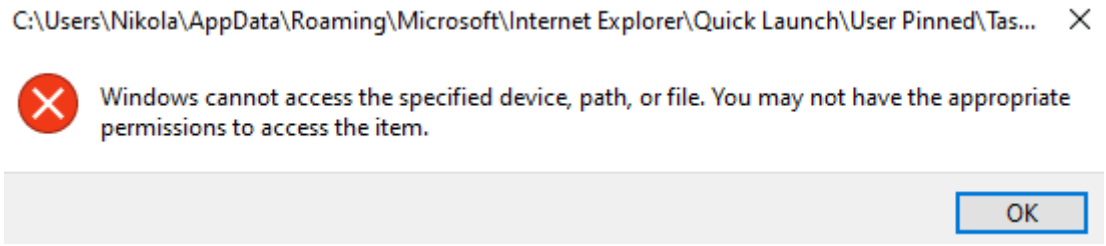
Slika 32: Kaspersky - Application Control - Edge 2

Da bi se pronašla aplikacija koju korisnik želi blokirati potrebno je znati proizvođača aplikacije. U ovom slučaju je to Microsoft. Proširi se Microsoft dio i prikažu se sve aplikacije na računalo korisnika, tvrtke Microsoft. Kad se pronađe program Edge, samo se promijeni status iz „Allowed“ u „Blocked“.



Slika 33: Kaspersky - Application Control - Edge 3

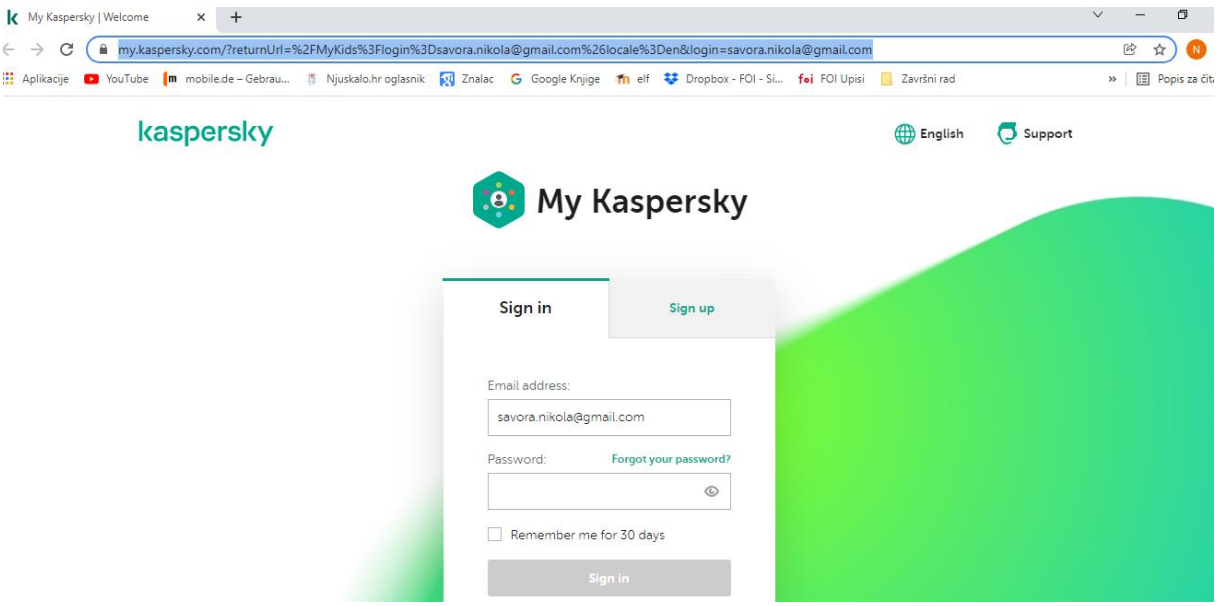
Kaspersky uspješno blokira otvaranje Microsoft Edge programa, razlika u odnosu na Bitdefender i Microsoft Defender je ta da Kaspersky ne dopušta niti otvaranje prozora, nego izbaci grešku kod otvaranja.



Slika 34: Kaspersky - Application Control - Edge 4

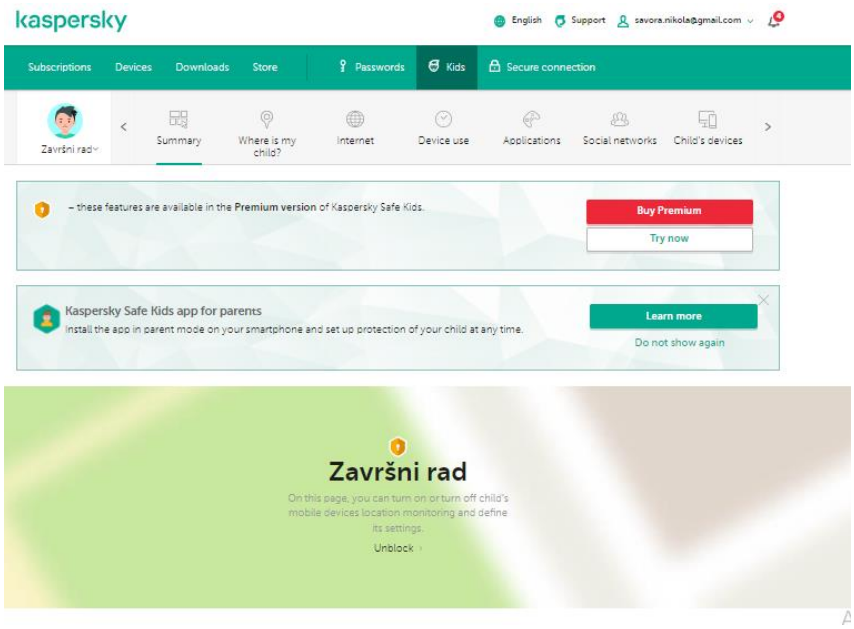
6.4. Kaspersky – Safe Kids

Dodatna mogućnost koju nude Kaspersky i Bitdefender, a kod Microsoft Defender programa ih nema, je zaštita za djecu. Kaspersky isto otvara aplikaciju u pregledniku, ali prije toga je potrebno instalirati dodatak za aplikaciju „Safe Kids“.

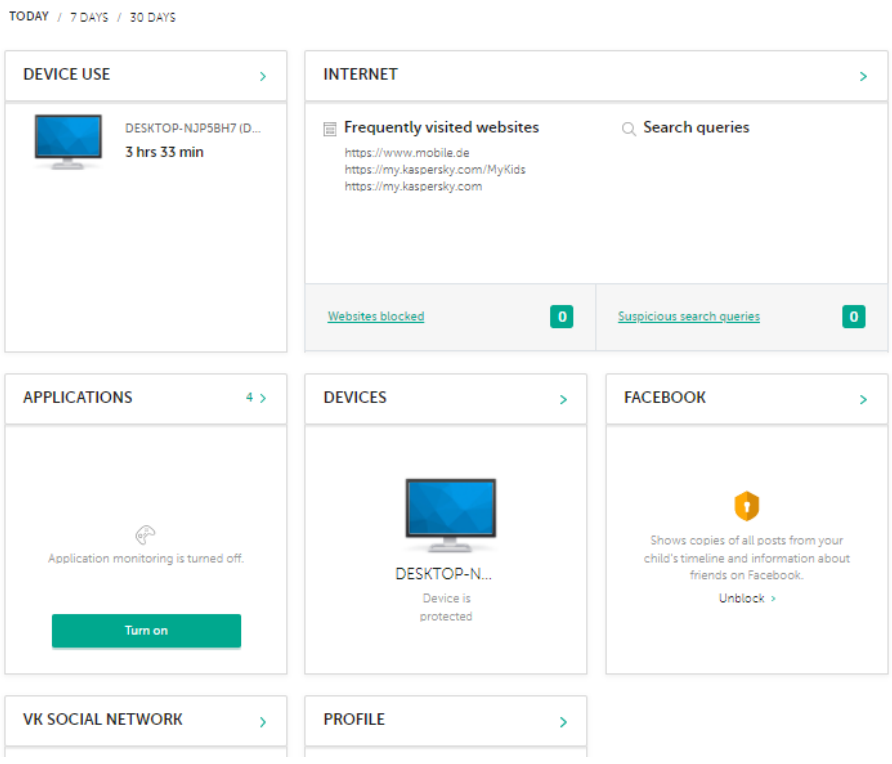


Slika 35: Kaspersky - Safe Kids

Mogućnost mijenjanja postavki određenog profila djeteta se dobiva prijavom u „My Kaspersky“ koji se otvara klikom na dodatak „Safe kids“. Sučelje koje se otvara je slično onome od Bitdefender programa. Može se vidjeti lokacija djeteta, kojim web mjestima se najčešće koristi, na kojim uređajima je „Safe Kids“ instaliran…



Slika 36: Kaspersky - Safe Kids 2



Slika 37: Kaspersky - Safe Kids 3

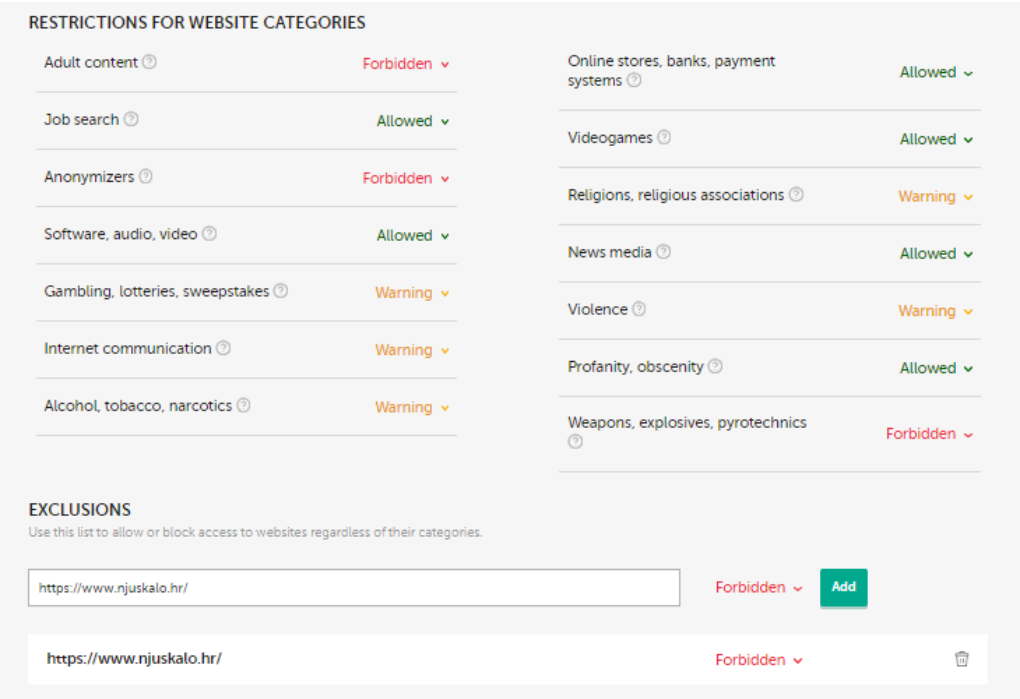
U dijelu za Internet na početnom sučelju klikne se na „Website blocked“. Otvara se nova stranica gdje se u dijelu sa postavkama (eng. Settings) mogu vidjeti razne vrste sadržaja koji se nalaze na internetu i na svaki sadržaj se može staviti jedan od triju statusa:

1. Allowed – korisnik ima dopuštenje za odlazak na stranice sa tim sadržajem

2. Warning – odlaskom na web mjesto sa sadržajem koji ima status „Warning“ šalje se obavijest roditelju gdje roditelj može potvrditi ulazak na to web mjesto ili odbiti ga.

3. Forbidden – korisniku su zabranjena web mjesta sa tim sadržajem

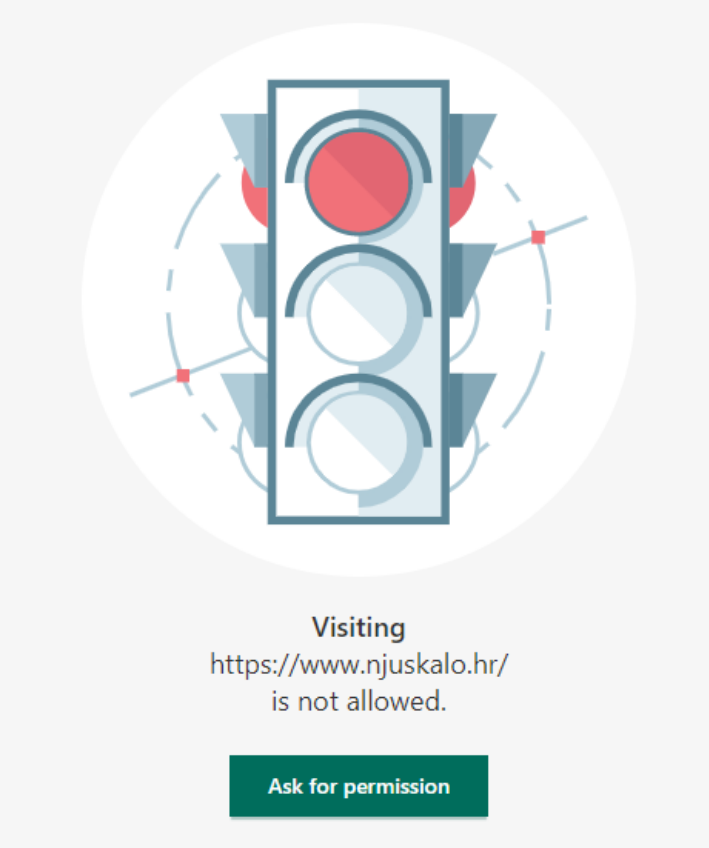
Niže se nalazi mjesto sa iznimkama (eng.Exclusions), tu se dodaju web stranice koje imaju sadržaj koji je dopušten, ali roditelj ih ipak želi blokirati. Mogu se dodati web stranice koje imaju status sadržaja „Forbidden“, ali im roditelj želi dati pristup.



Slika 38: Kaspersky - Safe Kids 4

U prostor za pisanje se dodaje URL web stranice na koju se želi dati pristup ili zabrana. U ovom slučaju je to zabrana na Njuškalo.hr. Klikne se na „Add“ i dodijeljena je zabrana na web stranicu Njuskalo.hr.

Dolje se nalazi slika koju preglednik izbaci kad se želi posjetiti stranica koju je administrator zabranio.



Slika 39: Kaspersky - Safe Kids 5

7. Zaključak

Usporedbom programa ustanovljena je velika razlika između Windows Defender programa koji je besplatan na Windows operativnom sustavu i Kaspersky i Bitdefender programa koji se plaćaju, ali u ovom slučaju su korištene probne verzije od 30 dana. Kaspersky i Bitdefender su prilagođeni korisniku i imaju više mogućnosti. Osim sitnih razlika u mogućnostima i prilagodljivosti korisniku, najznačajnija razlika između Kaspersky i Bitdefender programa je ta da je nakon instalacije Kaspersky Total Security računalo počelo sporije raditi i dugo otvarati aplikacije. Ako se želi zabraniti pristup određenim korisnicima na neka web mjesta preporučio bih i Kaspersky i Bitdefender program, a ako pak je korisniku bitno da mu je računalo zaštićeno i bez virusa preporučio bih da se pazi kojim web mjestima i aplikacijama se korisnik koristi. Na kraju sam korisnik snosi krivnju za dobivanje virusa i štetnih programa zbog svoje nepažnje i ne kontrolirane kretnje na internetu.

8. Popis literature

- Michael Palmer (2018), Hands-On Microsoft Windows Server 2016
- https://www.bitdefender.com/company/
- Alex X. Liu (2011), Firewall Design and Analysis

9. Popis slika