CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

FortiGate 60D

NCERT-LAB-PUBDOC-2014-07-001

Nacionalni CERT

Sadržaj

Ovaj dokument je vlasništvo Nacionalnog CERT–a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obvezno navođenje izvora podataka. Zabranjena je bilo kakva distribucija dokumenta u elektroničkom (web stranice i dr.) ili papirnatom obliku. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet–a, a sve sukladno zakonskim odredbama Republike Hrvatske.

1 Uvod

U sklopu ovog dokumenta testiran je vatrozid nove generacije, FortiGate 60D. Uređaj je dio ponude poznatog proizvođača uređaja za mrežnu sigurnost – Fortineta. Po svojim mogućnostima namijenjen je manjim korisnicima te u sebi objedinjava sve što je potrebno za zaštitu krajnjih korisnika (antivirus, VPN, IPS, web filter…). U prvom dijelu dokumenta nalazi se detaljan opis vatrozida, njegove specifikacije i mogućnosti, dok se u drugom dijelu dokumenta nalazi opis i rezultati testiranja njegovih najvažnijih komponenti.

1.1 Fortinet

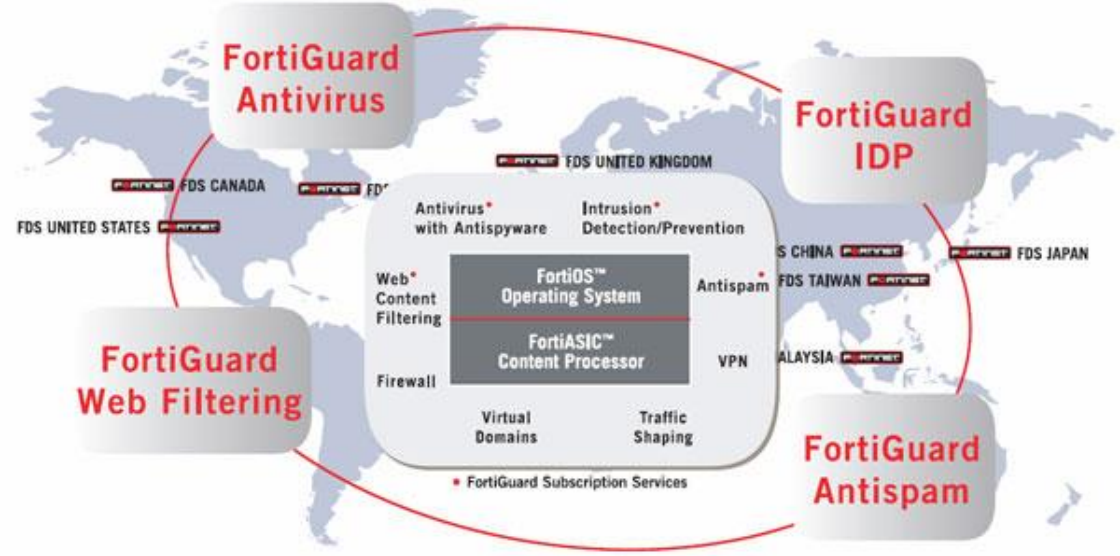
Fortinet je jedan od glavnih pružatelja rješenja za mrežnu sigurnost. Njihova FortiGate mrežna sigurnosna platforma pruža sigurnosnu zaštitu za sve razine, bilo da se radi o malim uredima, velikim ISP-ovima ili podatkovnim centrima. Cijelu FortiGate platformu uređaja pokreće FortiOS operacijski sustav koji uključuje velik raspon sigurnosnih tehnologija. Uz operacijski sustav i hardverske performanse pojedinih uređaja važnu okosnicu cijele Fortinet linije uređaja čine FortiGuard servisi.
FortiGuard servisi temelje se na sigurnoj globalnoj distribucijskoj mreži koja pruža stvarna vremenska ažuriranja za svoje Fortinet proizvode. Iza njih se krije globalni istraživački centar koji se sastoji od računalno-sigurnosnih stručnjaka koji održavaju i prate sve bitne promjene. Riječ je o sljedećim servisima:

- **FortiGuard antivirus/antispyware servis** - Pruža potpuno automatizirani sustav ažuriranja za zaštitu od novootkrivenih prijetnji. Sastoji se od naprednih mehanizama za otkrivanje zlonamjernih programa kako bi spriječio nove prijetnje Vašoj mreži, tj. vrijednom sadržaju i aplikacijama koje se nalaze u njoj. Zahvaljujući globalnoj distribucijskoj mreži koja funkcionira na velikim brzinama omogućuje brz i pouzdan pristup kritičnim ažuriranjima.

- **FortiGuard Intrusion prevention servis** - Korisnicima pruža zaštitu protiv skrivenih zlonamjernih i sumnjivih mrežnih prijetnji. Koristi prilagodljivu bazu s poznatim prijetnjama koja omogućuje Fortigate uređajima zaustavljanje napada koji bi zavarali i zaobišli konvencionalne vatrozide. Pruža mogućnost otkrivanja anomalija, odnosno detekcije odstupanja od normalnog mrežnog prometa s ciljem prepoznavanja prijetnji koje još nisu poznate i za koje ne postoje sigurnosni potpisi.

- **FortiGuard Web Content Filtering servis** - Omogućuje nadgledanje i filtriranje web aktivnosti korisnika. Uvelike olakšava rad administratorima u vidu lagane konfiguracije pristupa sadržajima na Internetu radi poštivanja raznoraznih državnih regulativa i sigurnosnih politika. Sa svojih 75 kategorija blokiranja omogućuje efikasno blokiranje zlonamjernog ili zabranjenog sadržaja.

- **FortiGuard Antispam servis** - Fortinetov globalni istraživački tim razvija i održava listu pošiljatelja neželjene elektroničke pošte i sadržaja takvih poruka. Napredna detekcija neželjene elektroničke pošte pruža bolju zaštitu od standardnih lista.



Slika 1. Prikaz FortiGuard servisa i raspodjele distribucijske mreže

FortiGate uređaji se mogu podijeliti na tri velike skupine:

- **High End** proizvodi koji obuhvaćaju FortiGate 5000 i FortiGate 3000 serije koje su namijenjene najzahtjevnijim korisnicima.

- **Mid range** proizvodi koji obuhvaćaju FortiGate 800C, 600C, 300C i 200D uređaje i namijenjeni su srednje velikim poduzećima i ustanovama.

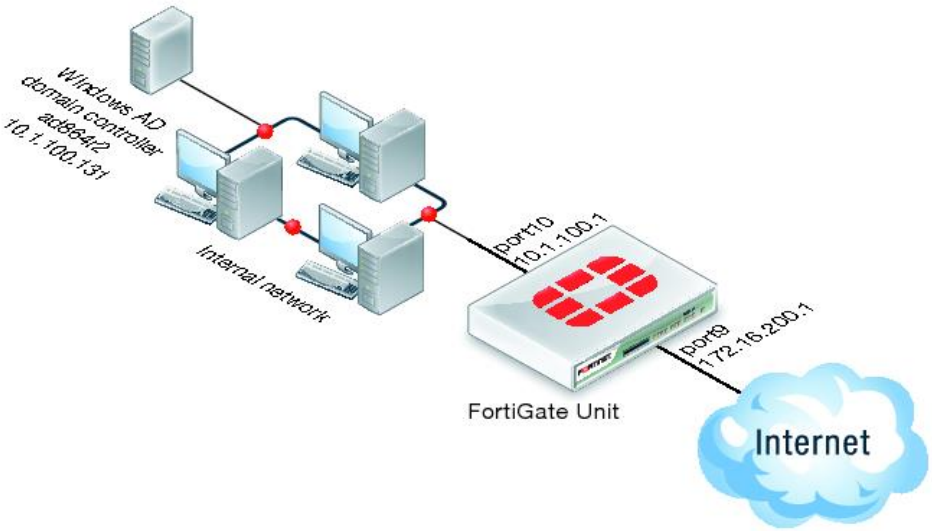
- **Entry level** proizvodi koji obuhvaćaju FortiGate 20, 30, 40, 60, 80, 90 i 100 serije i služe kao UTM (engl. *Unified Threat Management*) rješenja za manje korisnike.

2 FortiGate 60D

FortiGate 60D vatrozid namijenjen je malim tvrtkama, CPE-ovima (engl. *Customer premises equipment*) i malim mrežama. Nudi rješenje protiv sigurnosnih prijetnji, uključujući vatrozid, kontrolu prometa na aplikacijskoj razini, IPS, VPN, web filtriranje itd. Fortiguard sigurnosni servisi pružaju zaštitu protiv raznolikih prijetnji koja se ažuriraju na dnevnoj bazi.
Zanimljiva mogućnost je svakako i USB sučelje koje omogućava korištenje kompatibilnih 3G/4G USB modema, pružajući tako dodatnu WAN vezu koja može poslužiti kao redundantni link.

Slika 2. Prednja strana uređaja[1]

Glavna značajka uređaja je prepoznavanje prometa na aplikacijskom sloju. Umjesto klasičnog filtriranja prometa po portovima, vatrozid prepoznaje aplikacije i ima mogućnost filtriranja i primjenjivanja određenih pravila za pojedine aplikacije poput Skype-a, torrent klijenta i dr.
Sljedeća odlika koja ga ubraja u novu generaciju je mogućnost autentikacije korisnika putem Active Directory servisa. Nema više potrebe za starim načinom autentikacije temeljem IP adresa. Vatrozid se povezuje s poslužiteljem i cijeli se proces autentikacije prenosi na njega.



Slika 3. Autentikacija putem AD servisa[2]

[1] http://www.macmaster.se/webbshop/fortigate-60d/
[2] http://docs-egacy.fortinet.com/cb/html/index.html#page/FOS_Cookbook/Authentication/FSSO-IBP.html

Jedna od ugrađenih funkcija u obrani mreže od napada izvana je IPS funkcija. Uz predefinirane potpise, uređaj nudi mogućnost kreiranja vlastitih potpisa, što je jedna od velikih prednosti za zahtjevnije korisnike.

Vatrozid u sebi sadrži FortiASIC mrežni procesor. Zapravo se radi o RISC procesoru koji je integriran s FortiASIC akceleracijskom logikom i drugim komponentama.
Novi način obrade paketa donosi propusnost vatrozida od 1.5 Gbps te mogućnost spajanja 500 client-to-site IP Sec i 200 site-to-site IP Sec tunela.
Uz IPsec način tuneliranja, vatrozid podržava i SSL uz maksimalnu propusnost od 30Mbps.

Uređaj ima ugrađene u sebi mnoge funkcionalnosti. Neke od njih koje su vrlo korisne, a nismo testirali su:

- **SSO autentikacija** – uz uobičajene metode autentikacije Fortigate podržava SSO autentikaciju putem Windows AD poslužitelja. Ako su korisnici već prijavljeni u Windows AD mreži mogu izravno pristupati resursima bez ponovnog upisivanja pristupnih podataka. Za Linux korisnike koji nisu na domeni moguće je podesiti captive portal.

- **Data leak prevention** koristi napredne tehnike prepoznavanja uzoraka i korisnika kako bi spriječio neovlašten prijenos važnih i osjetljivih podataka kroz mrežu. Moguće je nadgledati različite web i mail protokole. Pruža mogućnost filtriranja sadržaja po određenim stringovima, a kako bi automatizirao i olakšao posao administratorima pruža mogućnost korištenja regularnih izraza. Osim filtriranja po sadržaju omogućava i prepoznavanje vrste dokumenta. Tako je na primjer moguće skenirati mrežni promet u potrazi za osjetljivim osobnim podacima ili jednostavno zabraniti prijenos svih Word dokumenta. Ako se ustanovi pokušaj prijenosa osjetljivog sadržaja, moguće je zaustaviti prijenos, generirati obavijest ili proslijediti sadržaj primatelju, ovisno o sigurnosnom pravilu i konfiguraciji.

- **Mail filter** sprječava širenje neželjenih poruka elektroniške pošte mrežom. Povezuje se s FortiGuard servisom te blokira poznate pošiljatelje spam poruka. Također je moguće definirati vlastite obrasce i spriječiti slanje mailova s određenim nizom znakova u sebi ili pak mail poruke koje dolaze s točno određenih IP adresa.

- **Virtualne domene** (engl. *Virtual Domain* - VDOM) omogućuju podjelu jednog fizičkog uređaja na više virtualnih. Svaka virtualna domena pruža kompletno odvojene funkcije (vatrozid, preusmjeravanje, VPN, UTM i ostalo), što omogućuje segmentaciju prometa i dodatno podiže sigurnost.

- **Podrška za protokole usmjeravanja -** osim mogućnosti upisivanja statičnih ruta, FortiGate 60D ima podršku za dinamičke protokole usmjeravanja (RIP, OSPF, BGP, IS-IS). Uz podršku za IPv4 uređaj ima podršku i za IPv6 . Tako je na njemu moguće pokrenuti protokole RIP next generation, BGP4+, OSPFv3 i Integrated IS-IS. Ukoliko se na vatrozidu nalazi više virtualnih domena, svaka od njih posjeduje vlastitu tablicu usmjeravanja, sa zasebnim rutama do odredišnih mreža.

- **Snimanje mrežnog prometa** - vatrozid ima mogućnost snimanja mrežnih paketa na svim mrežnim sučeljima uz korištenje naprednih filtera. Moguće je i uključiti automatsko snimanje paketa za svaki napad koji je prepoznao IPS što omogućuje naknadnu detaljniju analizu napada.

- **AntiDDoS funkcija** - na vatrozidu je moguće postaviti ograničenja za dolazni promet i na taj način spriječiti DDoS napad. Postoji više parametara koje je moguće namještati, a najbitniji je definiranje gornje granice za prihvat novih nedovršenih TCP konekcija.

- **Web cache** - pruža mogućnost spremanja popularnih stranica kako bi se poboljšale mrežne performanse.

- **Geografski bazirane adrese** - pruža mogućnost bilježenja, blokiranja ili filtriranja dolaznog i/ili odlaznog prometa prema državi gdje je određena IP adresa locirana.

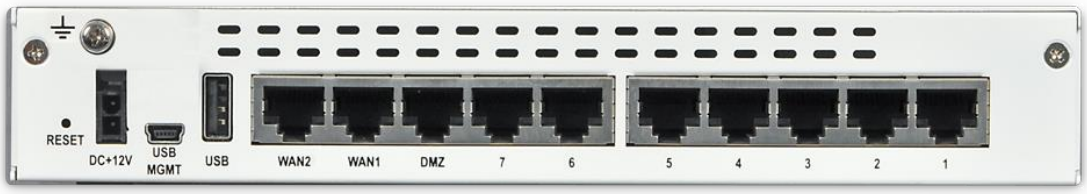
Slika 4. „System on a Chip“ tehnologija[3]

[3] http://www.avfirewalls.com/FortiGate-40C.asp

2.1 Specifikacija

Cijela stražnja strana predviđena je za sučelja. Vatrozid posjeduje sljedeća sučelja:

- 2 Gb WAN sučelja
- 7 Gb preklopničkih sučelja
- 1 Gb DMZ sučelje
- 1 USB sučelje
- 1 USB menadžment sučelje



Slika 5. Stražnja strana uređaja[4]

Performanse:

- Propusnost vatrozida (1518/512/64 byte UDP paketi): 1.5/1.5/1.5 Gbps
- Latencija vatrozida: 4µs
- Propusnost vatrozida (paketi po sekundi): 2.2 Mbps
- Maksimalni broj istovremenih konekcija: 500 000
- Maksimalni broj novih konekcija: 4 000
- IP Sec VPN propusnost: 1 Gbps
- SSL-VPN propusnost: 30 Mbps
- IPS propusnost: 200 Mbps
- Antivirusna propusnost : Proxy bazirana - 35 Mbps, Flow bazirana - 50 Mbps

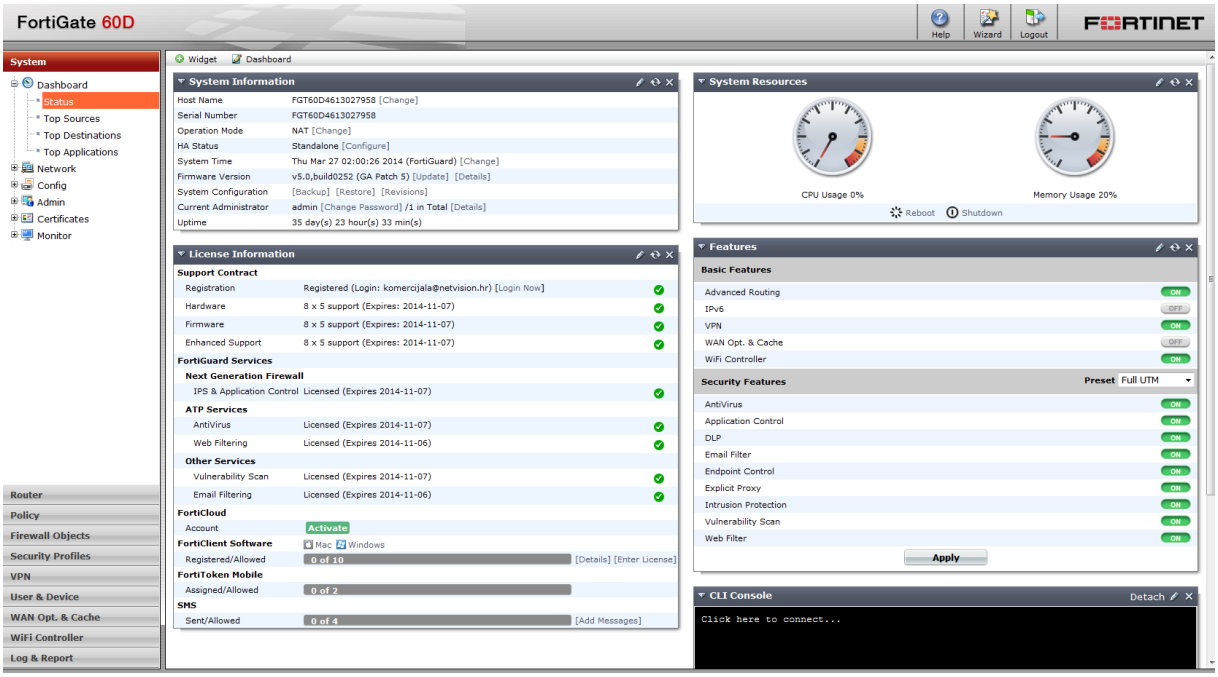
Uređaj je malih dimenzija (38x216x148 mm), te teži samo 0.9 kg. Prosječna potrošnja energije je 11.7W, a maksimalna 14W.
Kad je riječ o redundanciji, uređaj se može pohvaliti s tri načina rada: aktivni/aktivni, aktivni/pasivni i klasterirani.

2.2 Administrativna sučelja

Konfiguraciju uređaja moguće je obaviti na tri različita načina: preko web sučelja, preko komandno linijskog sučelja i pomoću FortiExplorer programa.

Web sučelje pruža brz pristup većini konfiguracijskih postavki. U sklopu njega moguće je dobiti širok opseg izvještaja te vidjeti trenutno stanje prometa i događaja koji se odvijaju.

[4] http://www.macmaster.se/webbshop/fortigate-60d/

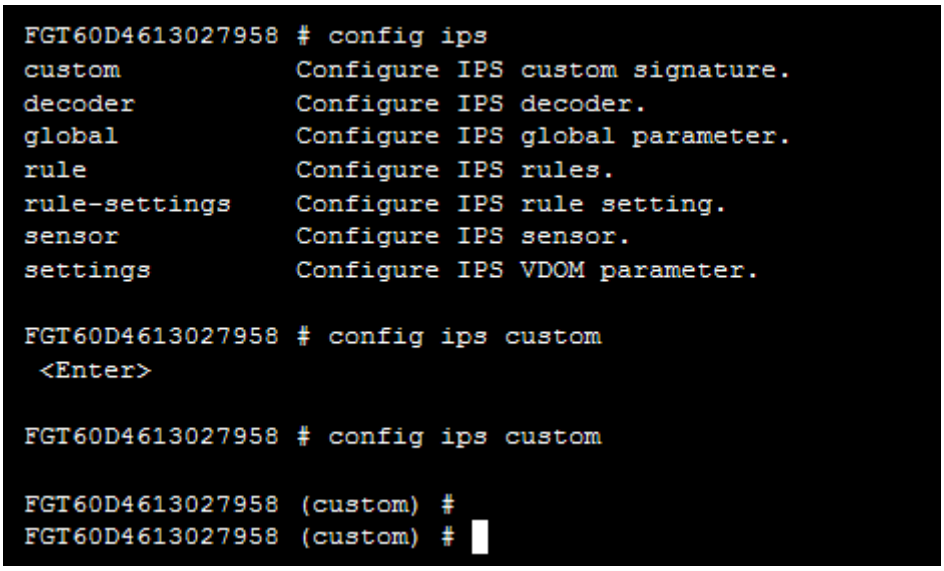


Slika 6. Web sučelje

Web sučelju pristupa se korištenjem HTTP ili HTTPS protokola putem bilo kojeg preglednika. Promjene u konfiguraciji napravljene preko web sučelja odmah se primjenjuju, stoga nije potrebno ponovno pokretanje uređaja.
Za pristup web sučelju dovoljno je spojiti računalo u jedan od 7 preklopničkih sučelja te u preglednik upisati predefiniranu adresu uređaja – 192.168.1.99. DHCP servis je automatski pokrenut te računalo dobiva IP adresu. U prozoru za prijavu u polju Username potrebno je upisati „admin“, a polje Password ostaviti praznim. Dobiva se početni prozor sučelja koji je isti za sve uređaje s FortiOS 5.0 verzijom operacijskog sustava.

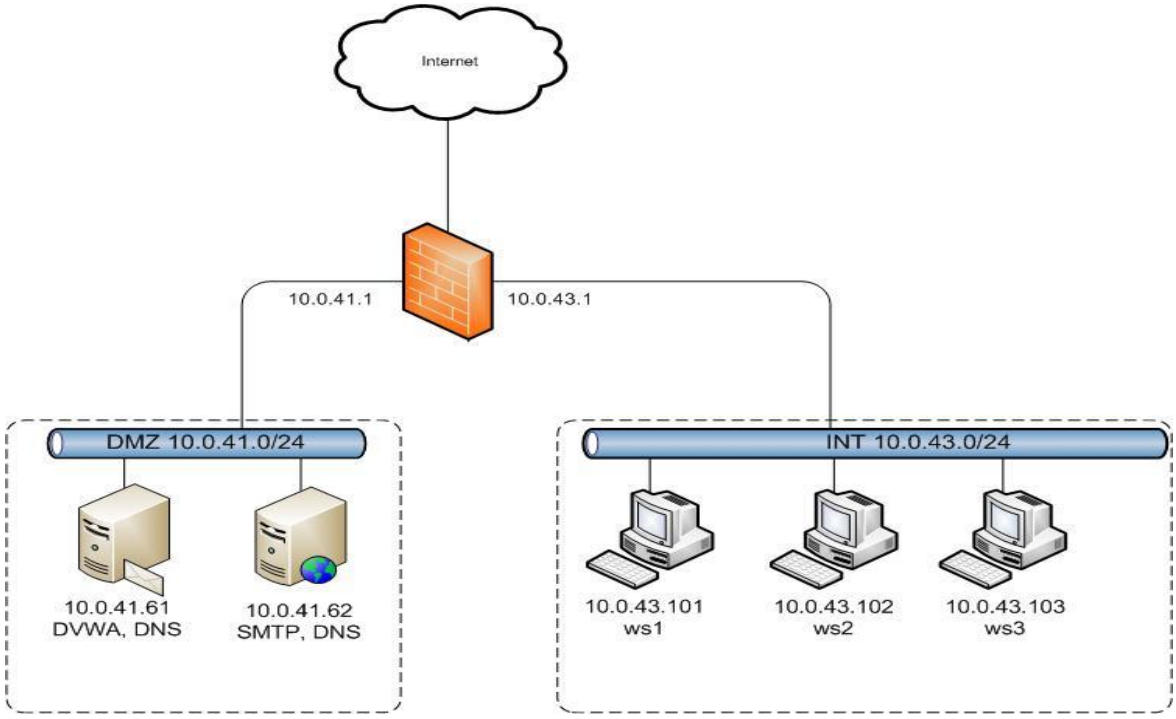
FortiExplorer program pruža korisniku prilagodljivo sučelje za konfiguraciju vatrozida preko standardne USB veze. Nakon instalacije u programu je moguće registrirati vatrozid, provjeriti verziju softvera i po potrebi ga ažurirati ili pokrenuti FortiExplorer čarobnjak za brzo podešavanje postavki uređaja.

Komandno linijsko sučelje pruža mogućnost komandno linijske konfiguracije uređaja. Preko njega je moguće mijenjati sve postavke vatrozida koristeći naredbu *config*. Neke od glavnih naredbi su još *get* - za pregled konfiguracije i dobivanje statusnih informacija, *execute* - za trenutno izvršavanje naredbi, uključujući postavljanje datuma i vremena, vraćanje konfiguracije, testiranje mrežne konekcije i slično, te *diagnose* za napredno nadgledanje i rješavanje problema.



Slika 7. Konfiguriranje putem komadno linijskog sučelja

3 Testiranje vatrozida



Slika 8. Topologija mreže korištene za testiranje vatrozida

Na slici 8 vidljiva je podjela na dvije mreže: DMZ mreža s adresom 10.0.41.0/24 i INT mreža s adresom 10.0.43.0/24. U DMZ mreži smješteni su web i mail poslužitelji. Oba služe kao DNS serveri za testnu lab.cert.hr domenu. Druga mreža je privatna INT mreža u kojoj se nalaze krajnji korisnici. Sastoji se od tri radne stanice.
Sva računala i poslužitelji prikazani u simuliranoj mreži u stvarnosti su virtualna računala. Virtualizacija je realizirana na VMWare ESXi platformi.

Kako bi korisnici s Interneta mogli pristupiti web i mail poslužitelju potrebno je obaviti translaciju privatnih adresa u javne. Na slici 9 vidljiva je tablica sa svim translacijama.

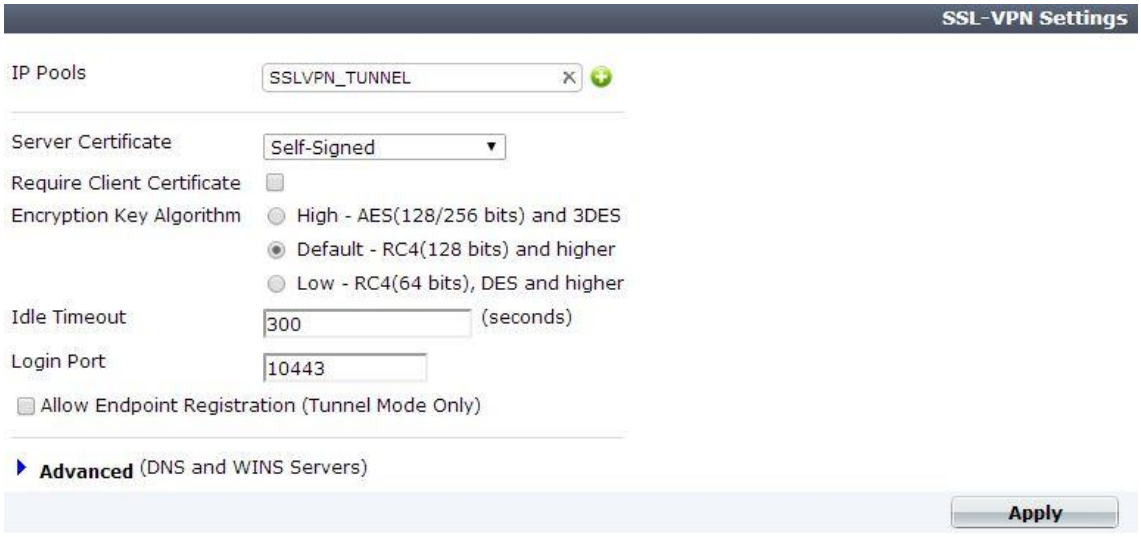
Name	External IP Address/Range	External Service Port	Mapped IP Address/Range	Map to Port
TEST_HTTP	wan1/10.0.14.102	80/tcp	10.0.41.61	80/tcp
TEST_SMTP	wan1/10.0.14.103	25/tcp	10.0.41.62	25/tcp
TEST_DNS1	wan1/10.0.14.102	53/udp	10.0.41.61	53/udp
TEST_DNS2	wan1/10.0.14.103	53/udp	10.0.41.62	53/udp

Slika 9. Popis translacija IP adresa

Pretpostavljeno pravilo vatrozida je blokiranje cijelog prometa. Kako bi se omogućila komunikacija potrebno je dodati pravila s kojima je moguće definirati tko, kad, i prema kome želi komunicirati.

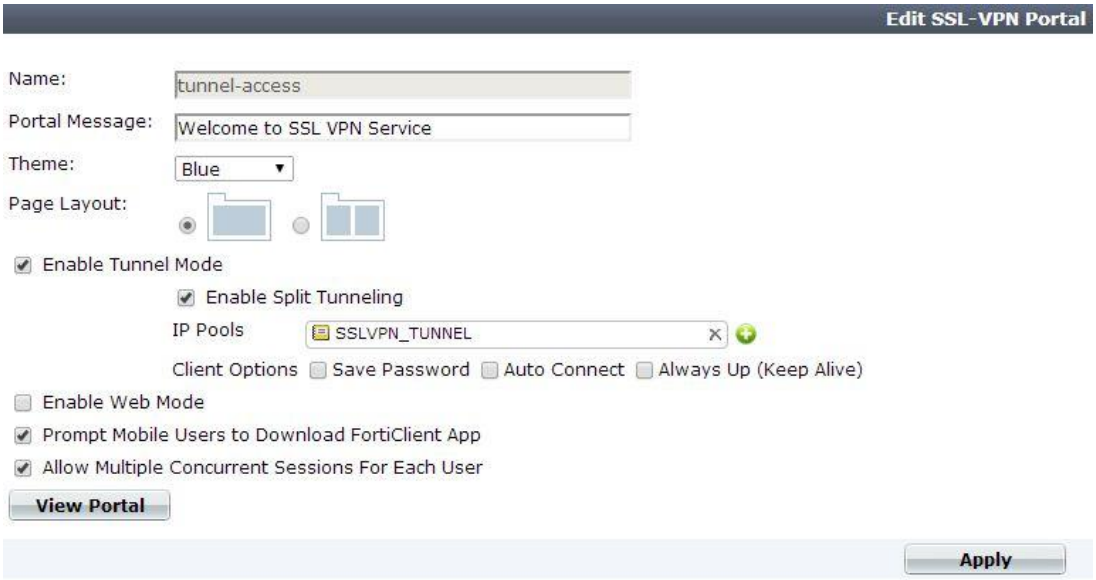
3.1 Testiranje VPN-a

U ovom poglavlju testiran je SSL VPN, točnije spajanje klijenata na SSL VPN poslužitelj i pristup lokalnim mrežama iza vatrozida. Konfiguracija je jednostavna i sve se konfigurira kroz web sučelje.



Slika 10. Podešavanje VPN tunela

Kroz VPN portale moguće je definirati način na koji udaljeni korisnici pristupaju poslužiteljima. Postoje dva načina, web način rada, tj. pristup servisima putem web preglednika ili tunelski način rada koji omogućuje direktan pristup sa korisničkih računala. U testiranju je korišten tunelski način rada sa „split tunneling" funkcijom. Ona definira da se na korisničkim računalima nakon spajanja na mrežu kreira virtualno mrežno sučelje i rute prema mrežama unutar VPN-a. U slučaju kad korisnik pristupa svim ostalim sadržajima na Internetu, promet ne prolazi preko VPN servera i na taj način se štedi propusnost. Nedostatak tog pristupa je taj da se zaobilazi sigurnost definirana na VPN serveru.



Slika 11. Detaljno podešavanje VPN tunela

Fortinet nudi više klijenata koji omogućuju spajanje. Najjednostavniji je FortiClient SSL VPN koji dolazi s vatrozidom i može se preuzeti kroz web sučelje SSL VPN-a. S web stranica moguće je preuzeti FortiClient koji uz SSL VPN nudi i niz drugih usluga kao što su Antivirus, WebFiltering, IPsec VPN itd.
Nakon konfiguracije portala, bilo je potrebno kreirati i pravilo za SSL VPN u kojemu je moguće precizno definirati način na koji pojedini korisnici ili grupe mogu pristupati resursima putem VPN-a.

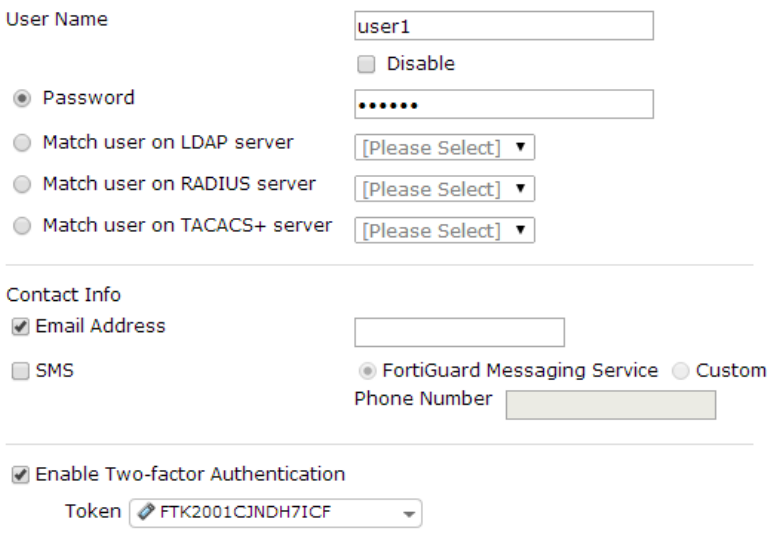
3.2 Testiranje tokena

Udaljeni pristup mrežnim resursima (VPN i web stranice) najčešće je zaštićen samo s korisničkim imenom i lozinkom, što nije uvijek najsretnije rješenje kad se radi o važnim podacima. Zbog toga se uz lozinku, kao dodatna razina zaštite, često koriste digitalni klijentski certifikati i rjeđe tokeni.
FortiToken je moguće koristiti za autentikaciju kod pristupa virtualnim mrežama, za bežični Captive portal ili kod prijave na FortiGate administratorsko sučelje.

Postoje tri vrste Fortigate tokena:

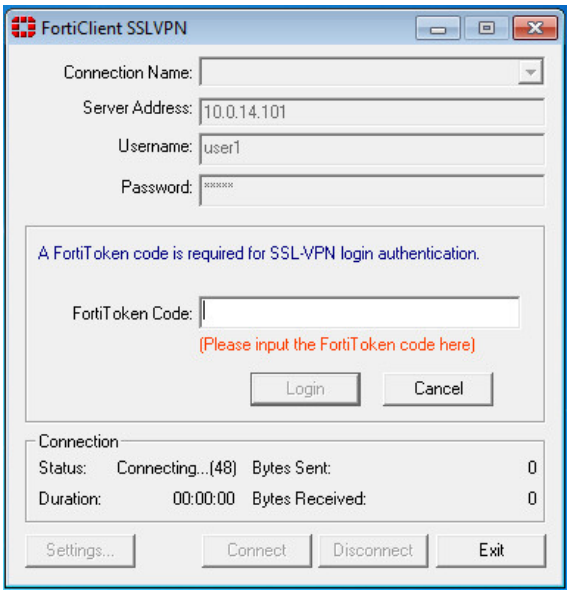
- **FortiToken-300** - USB token za X.509 PKI certifikate koji se osim za autentikaciju može koristiti i za potpisivanje/šifriranje elektroničke pošte, PDF dokumenata i drugih oblika datoteka. Zbog nemogućnosti direktnog pristupa, sigurniji su privatni ključevi generirani i smješteni na tokenu, nego oni smješteni na disku. Za korištenje ovog tokena potreban je poseban softver FortiToken Manager kojim se podešava sigurnosni pin i upravlja certifikatima.
- **FortiToken-200/200CD** - Token koji generira TOTP jednostruku lozinku s određenim vremenskim trajanjem. Koristi se isključivo za autentikaciju, a glavna mu je prednost što ne zahtjeva nikakav dodatni softver.
- **FortiToken Mobile** - Token koji ima istu funkcionalnost kao i hardverski OTP token, samo što ne dolazi kao dodatni hardver već kao aplikacija za mobilne uređaje.

Fortigate token je potrebno sinkronizirati s kontrolerom na vatrozidu i zato ga je moguće koristiti samo s jednim vatrozidom. Ukoliko se isti token želi koristiti za autentikaciju na više vatrozida potreban je FortiAuthenticator, sustav centralne autentikacije za više Fortigate uređaja.
U testiranju su korišteni tokeni za dvostruku autentikaciju prilikom spajanja na virtualnu mrežu. Aktivacija OTP tokena vrši se kroz web sučelje unošenjem aktivaciju serijskog broja smještenog na poleđini samog tokena. Dodatno je u postavkama korisnika potrebno omogućiti korištenje dvostruke autentikacije te mu pridružiti aktivirani OTP token.



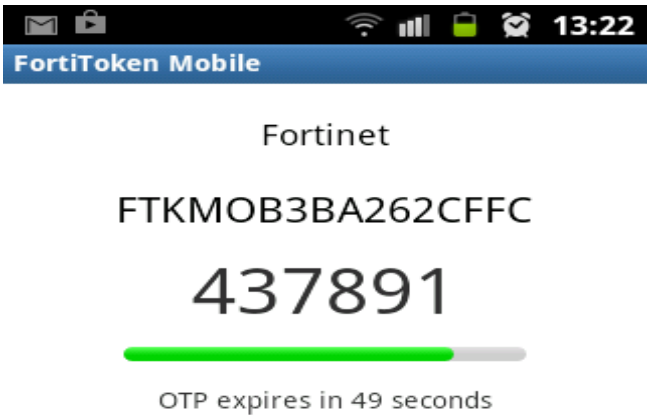
Slika 12. Podešavanje dvostruke autentikacije za korisnika

Kod sljedećeg spajanja korisnika u virtualnu mrežu SSL VPN klijentom ili kroz web portal pojavit će se polje za unos jednokratne lozinke.



Slika 13. Prijava na mrežu uz korištenje tokena

Za korištenje mobilnog tokena potrebno je preuzeti aplikaciju s Google Play repozitorija i instalirati je na mobilni uređaj s Android operacijskim sustavom.
Kao i kod korištenja običnog tokena u postavkama korisnika potrebno je omogućiti korištenje dvostruke autentikacije te korisniku pridružiti OTP token. Slijedi postupak slanja aktivacijskog koda elektroničkom porukom.
Nakon primitka poruke korisnik upisuje aktivacijski kod u Fortigate mobilnu aplikaciju ili očitava QR kod koji također dolazi s porukom.



Slika 14. FortiToken mobilna aplikacija

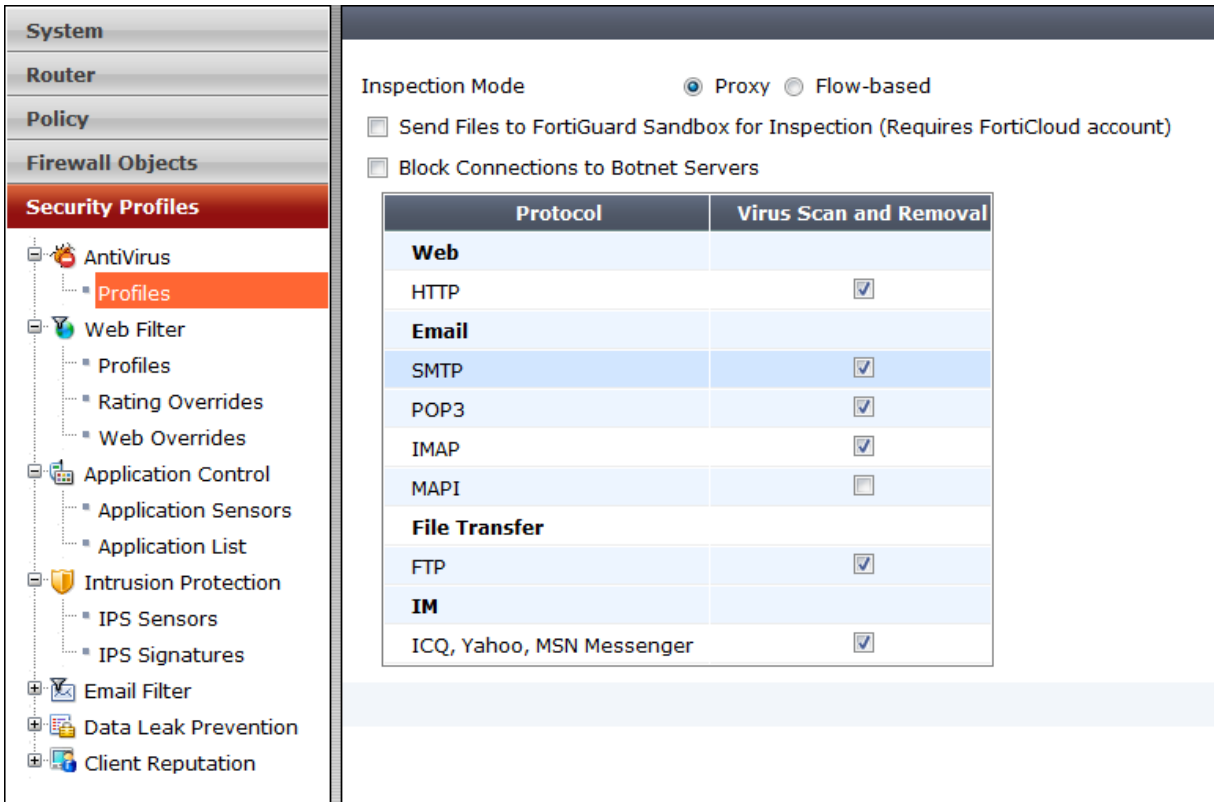
USB token služi za siguran smještaj digitalnih certifikata koje možemo koristiti za dvostruku autentikaciju prilikom spajanja u virtualnu mrežu. Princip je isti kao i kod klasičnog korištenja certifikata. Za korištenje USB tokena korisnik mora instalirati FortiToken Manager aplikaciju na računalo. FortiToken Manager omogućuje pristup certifikatima te njihov uvoz i izvoz. Podržani su sljedeći formati certifikata: P12, PFX, P7B, CRT i CER. Postoji i FortiToken Manager For Admin koji je sličan FortiToken Manageru, no još sadrži i administracijske opcije koje omogućuju deblokadu i inicijalizaciju tokena te izmjenu administratorske lozinke. Prilikom spajanja korisnika pojavit će se prozor u koji je potrebno unijeti korisnički pin tokena.

3.3 Testiranje antivirusa

Konfiguracija antivirusa na vatrozidu je krajnje jednostavna. Potrebna su dva koraka. Prvi je odabir načina pretraživanja i protokoli koji će se skenirati. Izabran je proxy način rada. On radi na principu da rekonstruira preuzete datoteke, ukoliko ima potrebu dekompresira ih, provjerava ih u potrazi za zlonamjernim sadržajima i tek potom šalje korisniku. Drugi korak je konfiguracija pravila čiji ćemo promet skenirati u potrazi za zlonamjernim programima.

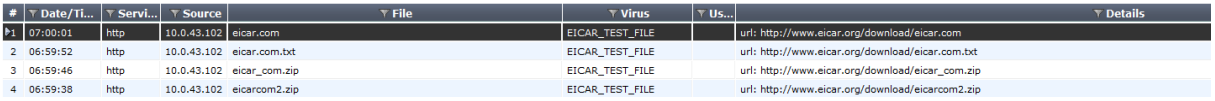
Slika 15. Dodavanje pravila za skeniranje prometa

Na slici 16 vidljiv je popis protokola koje Fortigate Antivirus skener podržava.



Slika 16. Konfiguriranje antivirusa

Testiranje antivirusa je uvijek delikatan posao te bi za pravo testiranje i usporedbu s drugim produktima mogli napraviti dokument za sebe.
Testiranje je ograničeno na prepoznavanje EICAR-e testne datoteke. EICAR (European Institute for Computer Antivirus Research) jedan je od poznatijih instituta koji su specijalizirani za otkrivanje i prevenciju zlonamjernih programa. U svrhu testiranja antivirusnih programa stvorili su datoteku koja je sigurna i može se distribuirati, ali na koju će antivirusni programi i uređaji reagirati kao na pravi virus. Vatrozid je prepoznao i reagirao u sva četiri slučaja kad smo pokušali pokrenuti testnu datoteku (kao HTML, kao tekstualnu datoteku, kao ZIP i kao dvostruki ZIP).



#	Date/Ti...	Servi...	Source	File	Virus	Us...	Details
1	07:00:01	http	10.0.43.102	eicar.com	EICAR_TEST_FILE		url: http://www.eicar.org/download/eicar.com
2	06:59:52	http	10.0.43.102	eicar.com.txt	EICAR_TEST_FILE		url: http://www.eicar.org/download/eicar.com.txt
3	06:59:46	http	10.0.43.102	eicar_com.zip	EICAR_TEST_FILE		url: http://www.eicar.org/download/eicar_com.zip
4	06:59:38	http	10.0.43.102	eicarcom2.zip	EICAR_TEST_FILE		url: http://www.eicar.org/download/eicarcom2.zip

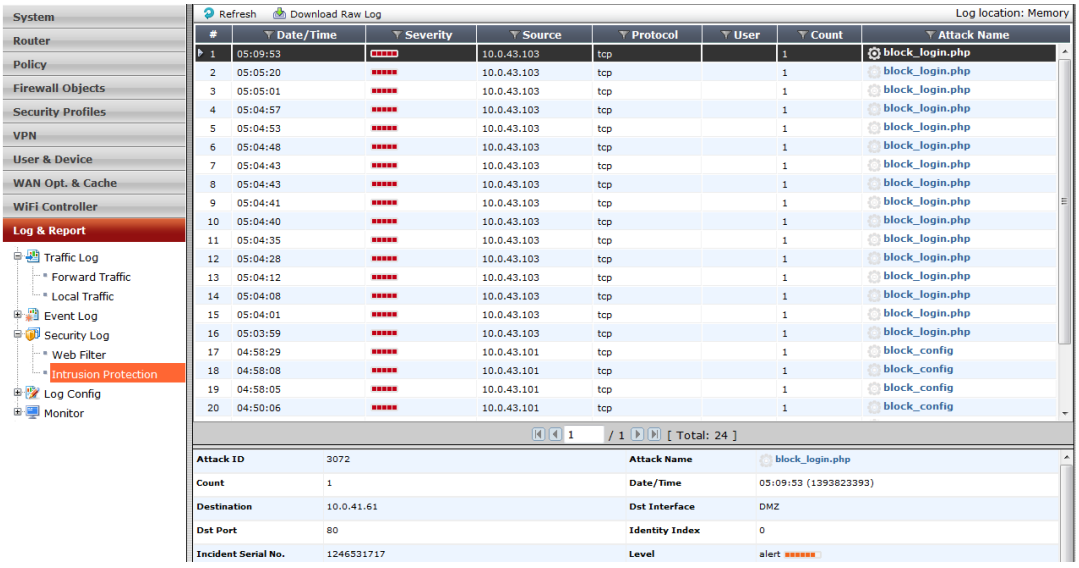
Slika 17. Prikaz loga za antivirus komponentu vatrozida

Prilikom pokušaja otvaranja stranice sa zlonamjernim sadržajem u pregledniku se otvara stranica s upozorenjem da je vatrozid blokirao pristup stranici (slika 18). U sklopu upozorenja se nalazi poveznica na Fortinetovu stranicu s detaljima o blokiranom zlonamjernom sadržaju.

Slika 18. Blokiranje pristupa zlonamjernoj datoteci

3.4 Testiranje IPS komponente vatrozida

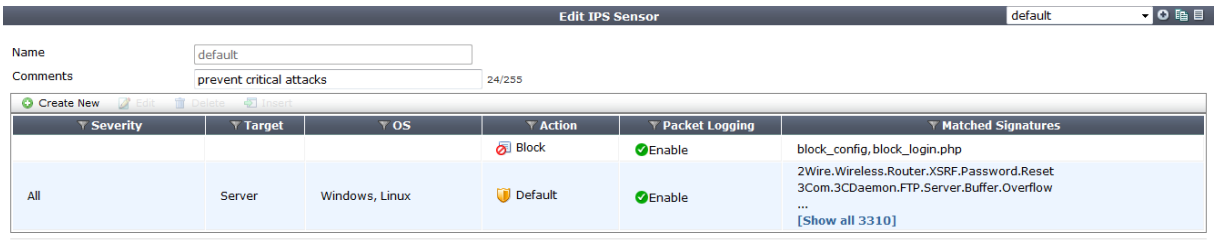
Za testiranje IPS komponente vatrozida korišten je VWAD (Vulnerable web applications directory). To je sveobuhvatan registar poznatih ranjivih web aplikacija.
Na web aplikaciju izvršen je SQL injection napad, jedan od zasigurno najpoznatijih napada u ovoj domeni. Napad je izvršen korištenjem SqlMap alata koji automatizira proces detektiranja i iskorištava ranjivost umetanjem koda. IPS je uspješno detektirao i spriječio napad.
Prednost FortiGate 60D vatrozida je mogućnost definiranja vlastitog potpisa koji pretražuje mrežni promet u potrazi za obrascem koji mu zadamo. Tako su uz testiranje predefiniranih potpisa testirana dva vlastita potpisa, čija se akcija blokiranja prometa otkida u slučaju pokušaja dohvata login.php skripte ili bilo koje druge datoteke u „config“ folderu.



Slika 19. Prikaz loga za IPS komponentu vatrozida

Zamjerka u kreiranju vlastitih potpisa je ta da sve funkcije nisu dostupne iz web sučelja. Tako je na primjer za promjenu akcije potpisa potrebno istu konfigurirati u komandno-linijskom sučelju.

Na slici 20 vidljive su postavke za predefinirani IPS senzor koji je korišten za detekciju napada. U gornjem desnom uglu moguće je dodati novi senzor i prilagoditi ga za neki drugi promet, odnosno neko drugo pravilo.



Slika 20. Postavke IPS senzora

3.5 Testiranje filtriranja prometa

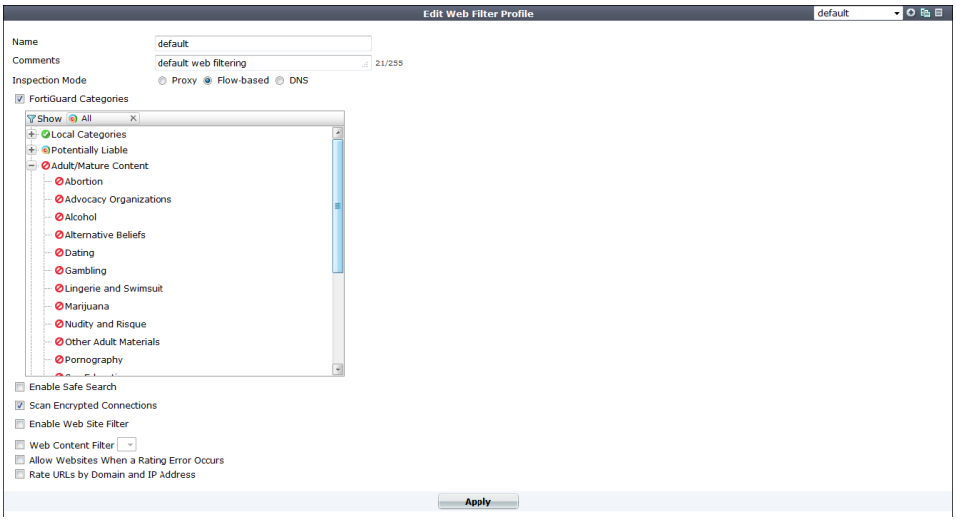
Fortigate sustav za filtriranje web prometa sastoji se od tri glavna dijela: Web Content Filter, URL Filter i FortiGuard Web Filtering servisa koji interaktivno funkcioniraju kako bi pružili maksimalnu kontrolu nad sadržajima koje korisnici posjećuju.

Postoje tri načina rada web filtera:

- **Proxy način rada** - cijeli promet se sprema na vatrozid. Tek nakon što vatrozid primi sve podatke vezane za određenu sesiju, donosi odluku o propuštanju ili blokiranju sadržaja. Prednost je manje krivih odluka (false negative i false pozitive), a mana nešto sporiji rad.
- **Flow-based način rada** - promet se analizira u trenutku dohvata, odnosno prilikom prolaska sadržaja kroz uređaj.
- **DNS način rada** - najmanje zahtjevna metoda. Nakon što korisnik zatraži neku web stranicu, njegov preglednik šalje DNS upit kako bi doznao IP adresu na koju će poslati HTTP zahtjev. Vatrozid presreće DNS upit i prosljeđuje ga na FortiGuard DNS poslužitelj gdje se radi analiza temeljem IP adrese, domenskog imena i ranga stranice kojoj korisnik želi pristupiti.

3.5.1 Filtriranje kategorija web prometa

Konfiguriranje filtriranja web prometa je trivijalno isto kao i u slučaju konfiguriranja antivirusa. Jedino što je potrebno, je odabrati jedan od tri moguća načina rada i izabrati sadržaje koji će biti blokirani.



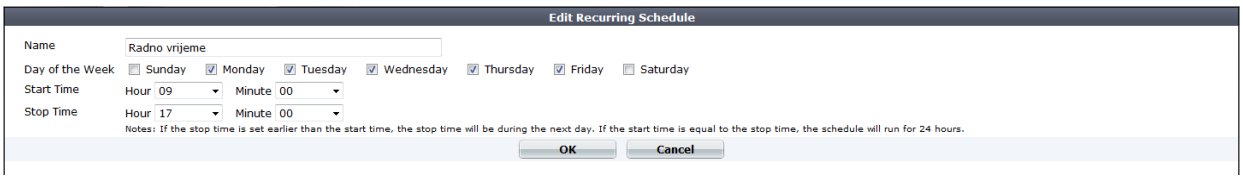
Slika 21. Konfiguriranje web filtera

Kad korisnik pokuša pristupiti stranici koja se nalazi u kategoriji kojoj je pristup zabranjen umjesto sadržaja tražene stranice dobije se obavijest o blokiranju dotične stranice (slika 22).

Slika 22. Blokiranje pristupa online kockanju

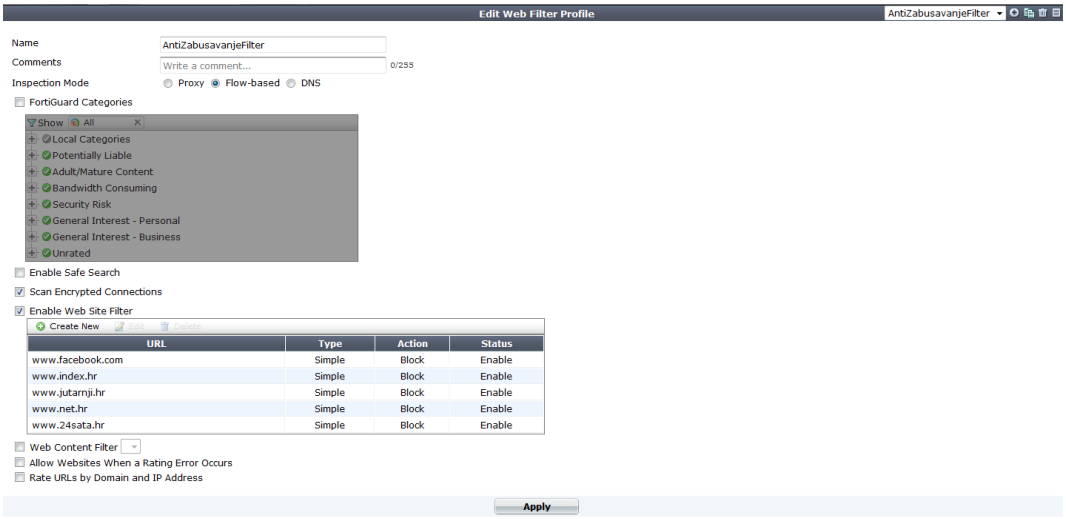
3.5.2 Filtriranje web stranica

Uz definiranje zabrane pristupa cijelim kategorijama nekog sadržaja moguće je blokirati pristup pojedinim stranicama. Uz to je moguće definirati vremenske intervale kada će pristup pojedinim stranicama biti blokiran. Ove dvije funkcionalnosti idealne su za povećavanje produktivnosti na radnom mjestu.



Slika 23. Definiranje vremenskih intervala

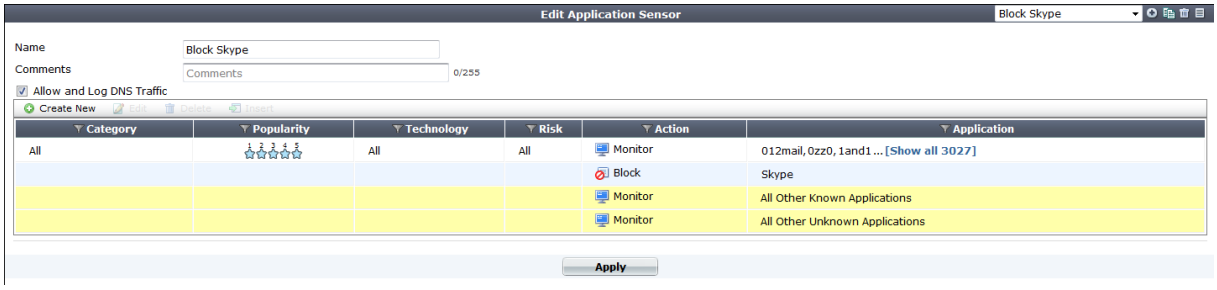
Na slici 23 vidljiva je konfiguracija vremenskog intervala u kojem će biti zabranjen pristup web stranicama. Popis web stranica kojima je zabranjen pristup i općenita konfiguracija web filtera za pristup tim stranicama vidljiv je na slici 24. Uz ova dva koraka potrebno je dodati pravilo za promet na kojem će se primijeniti ova ograničenja.



Slika 24. Konfiguriranje zabrane pristupa određenim stranicama

3.5.3 Filtriranje aplikacija

FortiGate 60D je vatrozid nove generacije i ima mogućnost filtiriranja aplikacija, odnosno njihovog prometa. Detektira aplikacije, baze podataka, IM/P2P promet, promet raznih protokola za prijenos datoteka i ostalo. Pritom se ne oslanja na portove nego na potpise koji se osvježavaju putem FortiGuard distribucijske mreže.
Za testiranje je odabrana aplikacija Skype. Konfiguracija je kranje jednostavna i sastoji se od dva koraka. Prvo je potrebno dodati aplikacijski senzor i dodati akciju blokiranja za Skype potpis (slika 25).



Slika 25. Konfiguracija aplikacijskog senzora

Drugi korak je definiranje pravila za promet nad kojim će se blokirati Skype.

Slika 26. Pravilo za blokiranje Skype-a

4 Zaključak

FortiGate 60D je uređaj koji će radi svoje pristupačne cijene i velikih mogućnosti naći svoj udio u svijetu računalne sigurnosti. Nakon testiranja i upoznavanja s njegovim mogućnostima kao glavne prednosti mogu se navesti pregledno web sučelje za konfiguraciju većine njegovih postavki te pojednostavljeno licenciranje (nema potrebe za kupnjom dodatnih licenci).
Dvije stvari koje želimo istaknuti su da je FortiGate WEB sučelje vrlo obuhvatno, ali unatoč tome neke naredbe je ipak potrebno provesti kroz komandno-linijsko sučelje, što zahtjeva da korisnik istraži potrebne naredba. Druga stvar je to da uređaj ima ograničen dnevnički zapis kroz koji nije moguće grupirati sve aktivnosti nekog korisnika, ali da je za to predviđen uređaj FortiAnalyzer koji služi za centralno praćenje i detaljno izvještavanje aktivnosti na svim nadziranim FortiGate uređajima. Uređaj je idealan za male korisnike premda se u njemu nalaze skoro sve funkcionalnosti potrebne za održavanje sigurnosti krajnjih korisnika i uređaja.