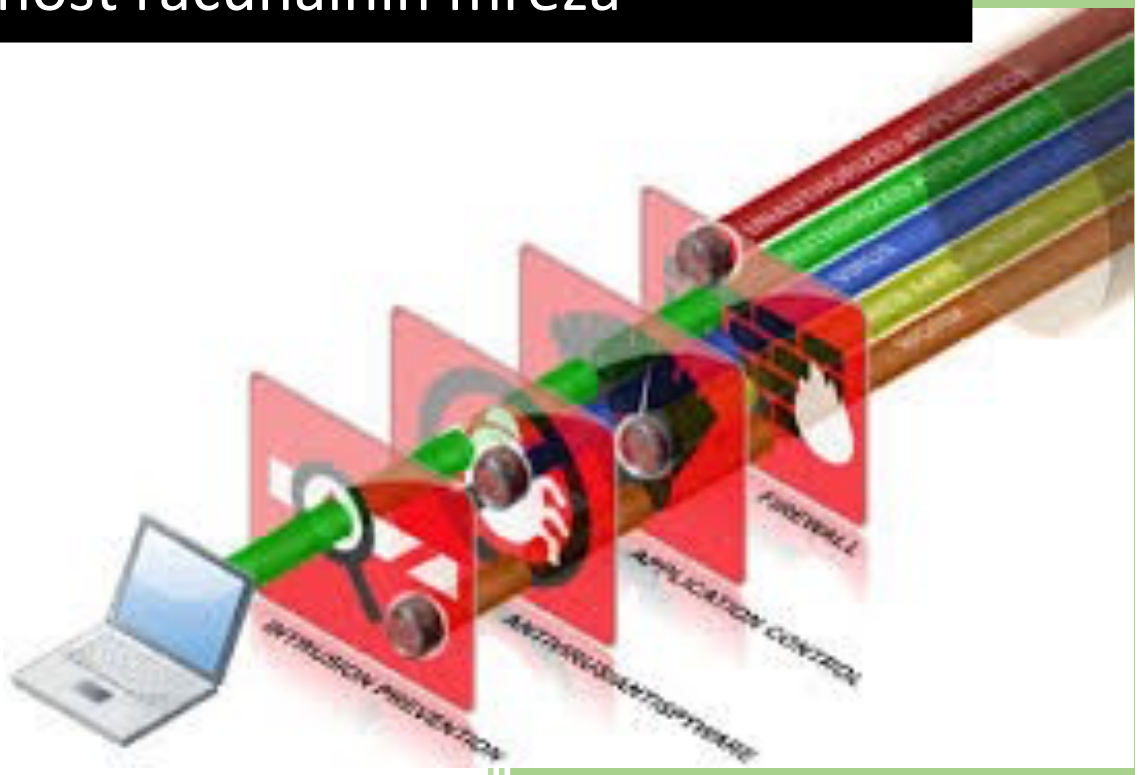
2025

Vatrozidi nove generacije – projekt Sigurnost računalnih mreža



Marin Krešić

Sveučilište Algebra

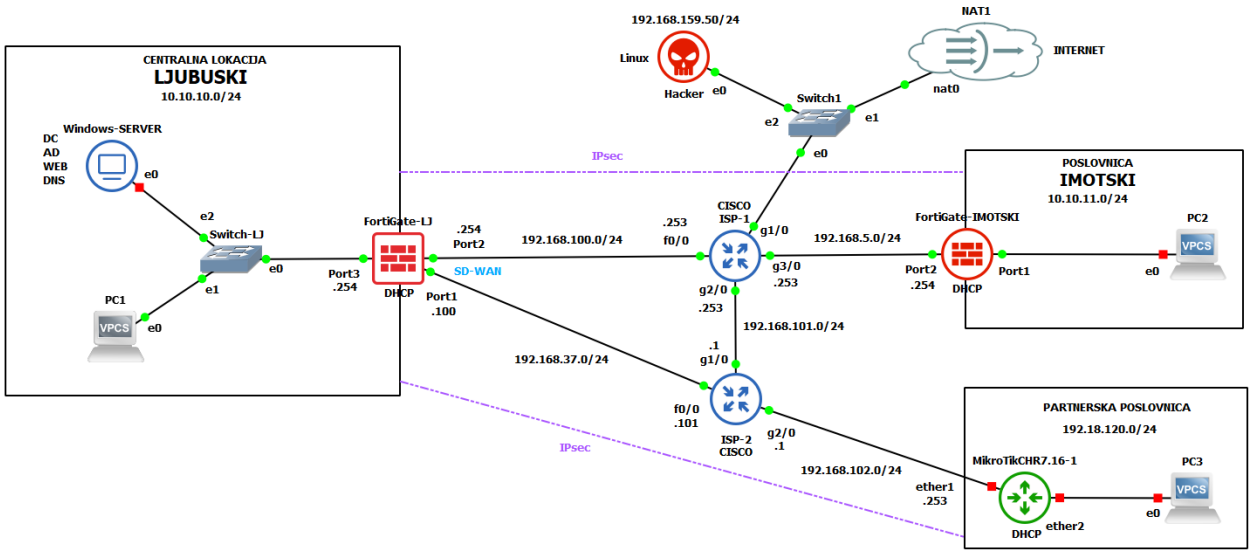
12/23/2025

Sadržaj

1. Uvod

Vatrozidi predstavljaju temeljnu komponentu sigurnosne arhitekture svih suvremenih računalnih mreža. Njihova primarna funkcija je kontrola i filtriranje mrežnog prometa između pouzdanih i nepouzdanih mrežnih segmenata, zaštita od neautoriziranih pristupa te prevencija prodora zlonamjernog softvera i napada. U današnjem digitalnom okruženju gdje preko 90% internetskog prometa koristi SSL/TLS enkripciju, a sofisticirane prijetnje poput ransomware napada, DDoS napada i zero-day exploita postaju sve češće, tradicionalni vatrozidi više nisu dovoljni za adekvatnu zaštitu organizacija.

Vatrozidi nove generacije (NGFW – Next Generation Firewall) poput Fortinet FortiGate platforme, nude napredne sigurnosne funkcije koje nadilaze osnovnu kontrolu pristupa na temelju IP adresa i portova. NGFW rješenja integriraju dubinsku inspekciju paketa (DPI), identifikaciju i kontrolu aplikacija neovisno o korištenim portovima, inspekciju enkripciranog SSL/TLS prometa, sustave za prevenciju napada (IPS), antivirusnu zaštitu, web filtriranje te mogućnost primjene sigurnosnih politika bazirano na korisničkom identitetu.



Slika 1 – Topologija mreže

Kroz projekt će biti prikazana implementacija usmjeravanja prometa s redundancijom, SD-WAN mehanizama za optimizaciju korištenja internet linkova, IPsec Site-to-Site VPN tunela za sigurnu komunikaciju između lokacija, Fortinet Single Sign-On integracije s Active Directory infrastrukturom, te sveobuhvatnih UTM (Unified Threat Management) sigurnosnih profila koji obuhvaćaju SSL/TLS inspekciju, web filtriranje, kontrolu aplikacija, antivirusnu zaštitu i IPS sustave za prevenciju napada. Opisane sigurnosne funkcionalnosti biti će konfigurirane i testirane kako bi se demonstrirala njihova praktična primjena u zaštiti mrežnih resursa HercMerc firme od suvremenih sigurnosnih prijetnji.

Napomena: Hacker Linux VM je u nekim koracima bio korišten i kao korisnički PC zbog manjka resursa na host računalu.

2. Usmjeravanje prometa

Usmjeravanje prometa u računalnim mrežama određuje optimalni put kojim mrežni paketi putuju od izvora do odredišta kroz kompleksne mrežne topologije. Usmjernici (routeri) koriste tablice usmjeravanja koje sadrže informacije o odredišnim mrežama, sljedećem skoku (next hop), mrežnom sučelju za proslijeđivanje paketa te metrikama koje određuju prioritet pojedine rute. Na FortiGate vatrozidima nove generacije, usmjeravanje nije samo mehanizam za proslijeđivanje paketa, već integrirana komponenta sigurnosne arhitekture koja omogućava primjenu različitih sigurnosnih politika ovisno o smjeru i izvoru prometa.

Administrativna distanca (AD) predstavlja ključni koncept u procesu odabira optimalne rute kada postoji više putova prema istoj odredišnoj mreži. AD je numerička vrijednost u rasponu od 0 do 255 koja označava razinu pouzdanosti izvora informacija o usmjeravanju - niža AD vrijednost ukazuje na veću pouzdanost. Primjerice, direktno povezane rute imaju AD vrijednost 0 (najviši prioritet), statičke rute obično imaju AD 10, OSPF protokol koristi AD 110, dok RIP protokol ima AD 120. Kada usmjernik posjeduje više ruta prema istoj destinaciji, automatski odabira rutu s najnižom administrativnom distancom, čime se omogućava implementacija redundantnih veza (failover) gdje se backup ruta aktivira tek nakon ispada primarne veze.

Na FortiGate vatrozidu centralne lokacije u Ljubuškom implementirano je redundantno usmjeravanje s automatskim failover mehanizmom kako bi se osigurala kontinuirana povezanost s Internetom čak i u slučaju ispada primarnog linka. Konfigurirane su dvije statičke default rute (0.0.0.0/0) s različitim administrativnim distancama.

Primarna ruta usmjerava promet prema gateway adresi 192.168.100.253 kroz sučelje WAN-primarni (port2) s administrativnom distancom postavljenom na vrijednost 10, što označava preferiranu rutu za sav odlazni internetski promet.

Backup ruta usmjerava promet prema gateway adresi 192.168.37.101 kroz sučelje WAN-backup (port1) s administrativnom distancom 20, što ju čini sekundarnom rutom koja ostaje neaktivna dok je primarna ruta dostupna.

Funkcionalnost osnovnog usmjeravanja verificirana je testiranjem odlazne povezanosti s klijentskog računala PC1 koje je dinamički dobilo IP adresu iz DHCP servisa FortiGate-LJ vatrozida. Izvršena je ping naredba prema javnoj Google DNS adresi 8.8.8.8, što je rezultiralo uspješnim ICMP Echo Reply odgovorima prikazanim na Slici 2, potvrđujući ispravnu konfiguraciju NAT mehanizma i sigurnosnih pravila za odlazni promet.

```
PC1> dhcp
DORA IP 10.10.10.1/24 GW 10.10.10.254

PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=93.206 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=78.422 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=185.130 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=140.550 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=93.483 ms

PC1>
```

Slika 2 – Ping test s PC1 prema Internetu

Traceroute naredba pokazala je da paketi iz PC1 najprije prolaze kroz FortiGate-LJ, a zatim kroz usmjernik ISP-1 na adresi 192.168.100.253 preko port2 sučelja, što je vidljivo na Slici 3.

```
CLI Console (1)
FORTI-LJ # execute traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe
 1  192.168.100.253  4.257 ms  15.396 ms  15.580 ms
 2  192.168.159.2  30.427 ms  30.620 ms  30.501 ms
 3  * * *
 4  * * *
```

Slika 3 – Traceroute preko primarne rute (port2)

Zbog niže administrativne distance, FortiGate u normalnim uvjetima koristi isključivo primarnu rutu, dok backup ruta ostaje neaktivna dok ne dođe do prekida primarne veze. Fortigate-IMOTSKI je konfiguriran istim putem samo bez backup linka.

Kako bi se testirao failover mehanizam, simuliran je ispad primarne veze privremenim isključenjem port2 sučelja. FortiGate je automatski detektirao ispad i aktivirao backup rutu preko port1 sučelja. Traceroute test nakon aktivacije backup rute pokazao je prolazak prometa kroz alternativni gateway 192.168.37.101 (Slika 4), čime je potvrđena ispravnost redundantnog rješenja.

```
CLI Console (1)
FORTI-LJ # execute traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe
 1  192.168.37.101  10.911 ms  15.195 ms  15.478 ms
 2  192.168.101.253  46.005 ms  45.502 ms  46.242 ms
 3  192.168.159.2  61.252 ms  61.950 ms  61.394 ms
 4  *
```

Slika 4 – Traceroute preko backup rute (port1) nakon simulacije ispada

Implementirano rješenje usmjeravanja osigurava visoku dostupnost pristupa javnoj mreži, što je bitno za poslovanje u situacijama kada dolazi do ispada primarnog Internet linka.

3. Sigurnosna pravila i NAT mehanizam

Sigurnosna pravila su važna komponenta FortiGate vatrozida koja definira način obrade i propuštanja mrežnog prometa između različitih mrežnih segmenata. Svrha sigurnosnih pravila je omogućiti kontrolu pristupa resursima na temelju definirane sigurnosne politike organizacije, specificirajući pritom koje vrste prometa su dozvoljene, blokirane ili inspicirane dodatnim sigurnosnim profilima.

NAT (Network Address Translation) mehanizam omogućava transformaciju IP adresa u mrežnim paketima tijekom prolaska kroz vatrozid.

Za potrebe ovog projekta konfigurirano je šest sigurnosnih pravila. Pravila su organizirana po funkcionalnosti i smjeru prometa, omogućavajući detaljnu kontrolu mrežne komunikacije između različitih lokacija i prema vanjskim resursima. Prvo pravilo "LAN-internet" regulira odlazni internetski promet iz centralne lokacije LJUBUSKI gdje je omogućen Source NAT mehanizam i primijenjeni su svi UTM sigurnosni profili (AntiVirus-LJ, LAN-LJ Web Filter, netflix-block Application Control, TLS-inspection SSL profil). Drugo pravilo "WAN-LAN" omogućava pristup vanjskih korisnika prema internoj LJUBUSKI mreži s primijenjenim IPS-zastita profilom za detekciju i prevenciju napada izvana, također s omogućenim NAT mehanizmom. Sljedeća četiri pravila (vpn_LJ-IM_local_0, vpn_LJ-IM_remote_0, vpn_MikrotikVPN_local_0, vpn_MikrotikVPN_remote_0) omogućavaju Site-to-Site VPN komunikaciju između centralne lokacije LJUBUSKI i poslovnice IMOTSKI te partnerske lokacije s MikroTik uređajem. VPN pravila koriste "no-inspection" SSL profil jer je promet unutar IPsec tunela već enkriptiran i ne zahtijeva dodatnu inspekciju.

Ključna značajka ovog pravila je primjena kompletnog sigurnosnog profila (Security Profiles) koji omogućava Unified Threat Management (UTM) inspekciju odlaznog prometa. Na pravilo "LAN-internet" primijenjeni su sljedeći sigurnosni profili prikazani na Slici 5: *AntiVirus-LJ* profil za detekciju i blokiranje malware prijetnji, *LAN-LJ* Web Filter profil za kontrolu pristupa web kategorijama (blokiranje Social Networking), *netflix-block* Application Control profil za blokiranje specifičnih aplikacija poput Netflix streaming servisa, te *TLS-inspection* SSL Inspection profil za dekriptiranje i inspekciju HTTPS prometa.

Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles
Uncategorized 6											
vpn_LJ-IM_local_0	LAN (port3)	LJ-IM	LJ-IM_local	LJ-IM_remote	always	ALL	ACCEPT		Disabled	Standard	SSL no-inspection
vpn_LJ-IM_remote_0	LJ-IM	LAN (port3)	LJ-IM_remote	LJ-IM_local	always	ALL	ACCEPT		Disabled	Standard	SSL no-inspection
vpn_MikrotikVPN_local_0	LAN (port3)	MikrotikVPN	MikrotikVPN_local	MikrotikVPN_remote	always	ALL	ACCEPT		Disabled	Standard	SSL no-inspection
vpn_MikrotikVPN_remote_0	MikrotikVPN	LAN (port3)	MikrotikVPN_remote	MikrotikVPN_local	always	ALL	ACCEPT		Disabled	Standard	SSL no-inspection
LAN-internet	LAN (port3)	virtual-wan-link	LAN-LJ	all	always	ALL	ACCEPT		NAT	Standard	AV AntiVirus-LJ WEB LAN-LJ APP netflix-block +2
WAN-LAN	virtual-wan-link	LAN (port3)	all	all	always	ALL	ACCEPT		NAT	Standard	IPS IPS-zastita SSL certificate-inspecti
Implicit 1											
Implicit Deny	any	any	all	all	always	ALL	DENY				

Slika 5 – FortiGateLJ sigurnosna pravila

4. Fortinet mehanizam jedinstvene prijave

Fortinet Single Sign-On (FSSO) predstavlja napredni mehanizam autentikacije koji omogućava transparentnu identifikaciju korisnika na vatrozidu bez potrebe za ponovnim unosom vjerodajnica prilikom pristupa mrežnim resursima. FSSO rješenje omogućava FortiGate vatrozidu da koristi postojeću Active Directory infrastrukturu organizacije za automatsko mapiranje IP adresa s autenticiranim korisničkim računima, čime se omogućava primjena sigurnosnih politika na razini pojedinačnih korisnika ili Active Directory grupa umjesto isključivo na temelju IP adresa.

FSSO arhitektura sastoji se od tri ključna elementa. Prvi element je *FSSO Collector Agent* - softver koji se instalira na Windows Domain Controller ili poseban Windows Server s pristupom Active Directory okruženju. Collector Agent prati Windows Security Event logove i prikuplja informacije o korisničkim prijavama i odjavama, mapira IP adrese sa svakog PC-a s korisničkim imenima koji su s te adrese autenticirani, te komunicira s FortiGate vatrozidom slanjem ažuriranih user-IP mapiranja.

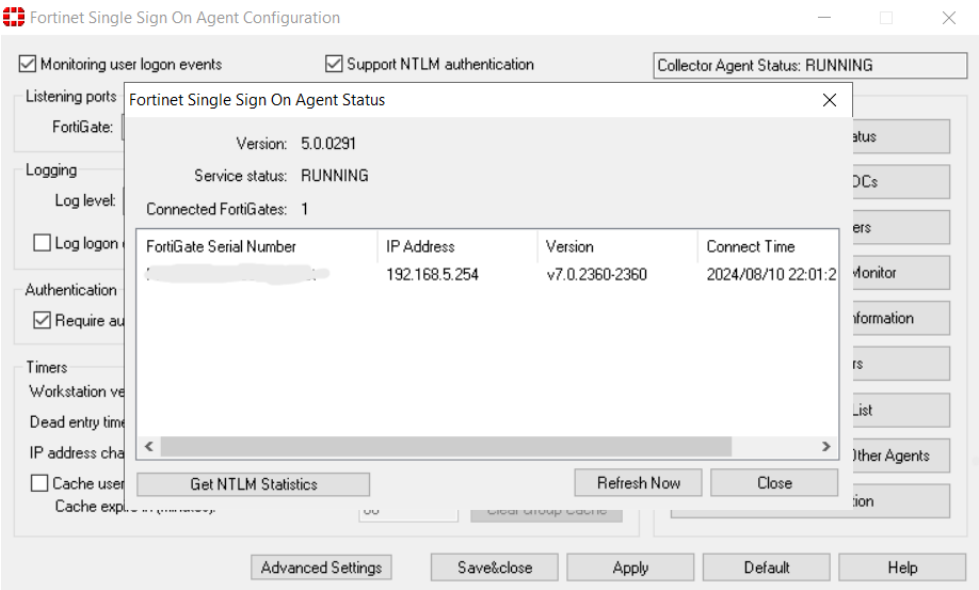
Drugi element je *FortiGate External Connector*: konfiguracija na FortiGate vatrozidu koja uspostavlja sigurnu vezu s FSSO agentom i prima podatke o aktivnim korisničkim sesijama.

Treći element su *User Groups*: grupe kreirane na FortiGate vatrozidu koje referenciraju Active Directory grupe ili organizacijske jedinice (OUs) i koriste se u sigurnosnim pravilima za definiranje pristupnih politika prema korisničkim ulogama.

FSSO eliminira potrebu za eksplicitnom autentikacijom korisnika na vatrozidu što poboljšava korisničko iskustvo. Nakon što se korisnik prijavi na Windows domenu, sav njegov mrežni promet automatski se povezuje s njegovim identitetom bez dodatnih akcija. Centralizirano upravljanje pristupnim pravima moguće je kroz postojeću Active Directory infrastrukturu. Administratori mogu koristiti AD grupe za definiranje sigurnosnih politika umjesto održavanja zasebnih korisničkih baza na vatrozidu.

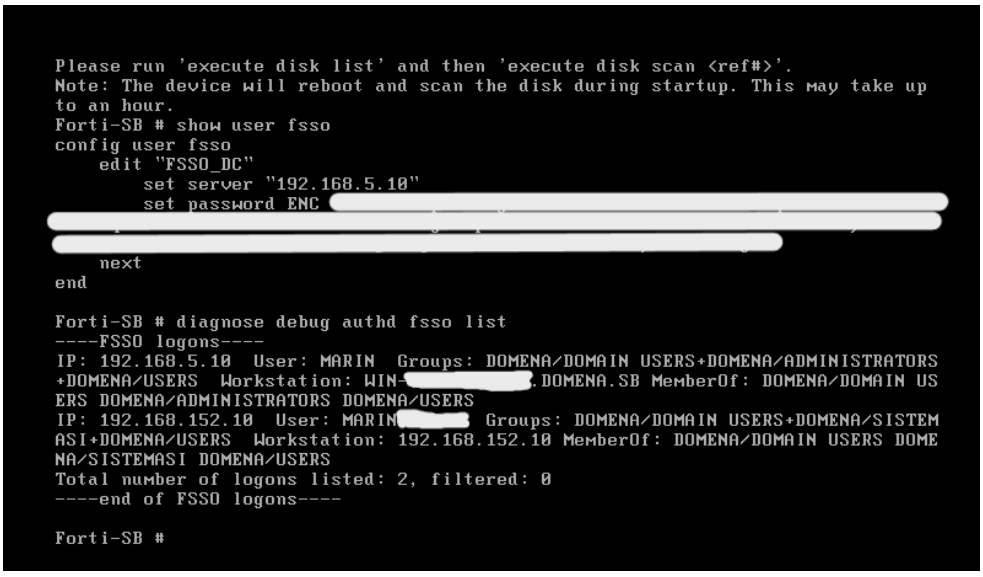
Detaljno logiranje i izvještavanje po korisnicima omogućava preciznu analizu mrežnih aktivnosti i brzu identifikaciju bezbijednosnih incidenata kroz jasnu povezanost između mrežnog prometa i specifičnih korisničkih računa. Dodatno, FSSO omogućava implementaciju prilagođenih sigurnosnih profila prema korisničkim ulogama - različiti odjeli ili grupe mogu imati različite razine pristupa internetskim resursima, aplikacijama ili web kategorijama.

Za potrebe ovog projekta implementirano je FSSO rješenje koje integrira FortiGate vatrozid lokacije LJUBŠKI s Windows Server Active Directory okruženjem domena DOMENA.SB (*Široki Brijeg, kasnije promijenjen u Ljubuški*). Fortinet Single Sign-On Agent je instaliran na Windows Server Domain Controller.



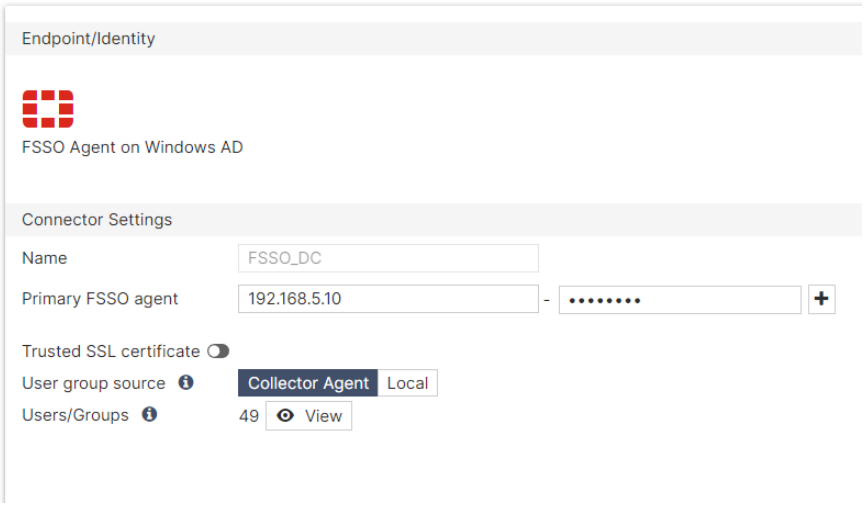
Slika 6 – FSSO Agent status s povezanim FortiGate vatrozidom

Na Slici 6. prikazan je status Fortinet Single Sign-On Agenta koji pokazuje uspješnu konekciju s FortiGate vatrozidom. FSSO Agent verzije 5.0.0291 ima servisni status *RUNNING*, što potvrđuje aktivan rad Collector Agent servisa.



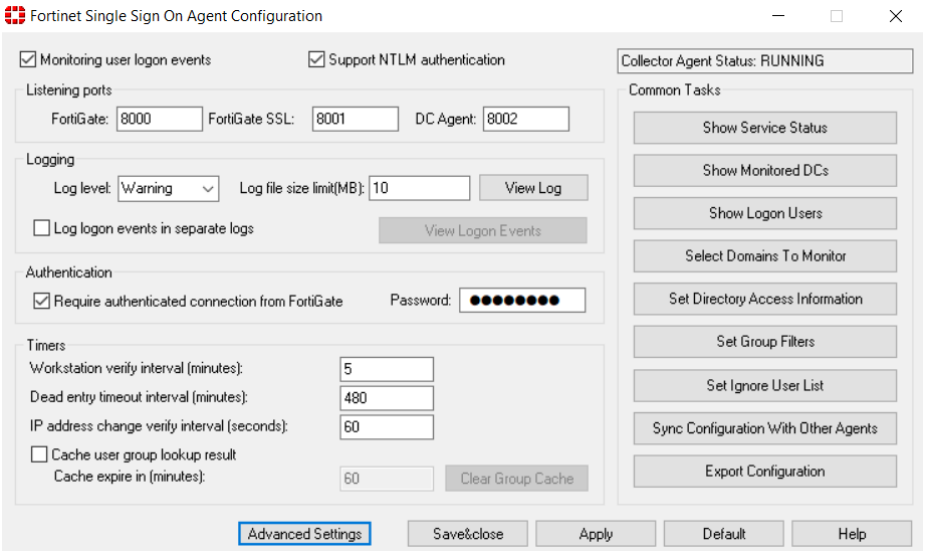
Slika 7 – CLI output FSSO agent konfiguracije i logirane korisničke sesije

Slika 2. prikazuje FortiGate CLI output naredbi za konfiguraciju i verifikaciju FSSO funkcionalnosti. Konfiguracija FSSO connectora definirana je kroz config user fsso sekciju gdje je kreiran "FSSO_DC" connector s parametrima - server IP adresa 192.168.5.10 (Primary FSSO agent), lozinka za autentikaciju te korištenje Collector Agent tipa. Output naredbe diagnose debug authd fsso list prikazuje trenutno aktivne korisničke sesije evidentirane kroz FSSO mehanizam.



Slika 8 – FortiGate External Connector konfiguracija za FSSO Agent

Na Slici 8. prikazana je konfiguracija FSSO External Connectora na FortiGate vatrozidu. U sekciji Security Fabric > External Connectors kreiran je connector tipa "FSSO Agent on Windows AD" s nazivom "FSSO_DC". Connector Settings definiraju primarni FSSO agent s pripadajućom lozinkom za autentikaciju. User group source postavljen je na "Collector Agent" što označava da se korisničke grupe prikupljaju direktno s FSSO agenta, a "Local" opcija označava da se koriste lokalno definirane grupe.



Slika 9 – FSSO Agent listening portovi i autentikacijske postavke

Implementacija FSSO mehanizma omogućava FortiGate vatrozidu primjenu sigurnosnih pravila baziranih na Active Directory grupama, čime se postiže centralizirano upravljanje pristupnim politikama kroz postojeću domensku infrastrukturu organizacije. Korisnici automatski nasljeđuju pristupna prava prema svojim AD grupama bez potrebe za dodatnom konfiguracijom na vatrozidu.

5. Softversko upravljanje odlaznim prometom

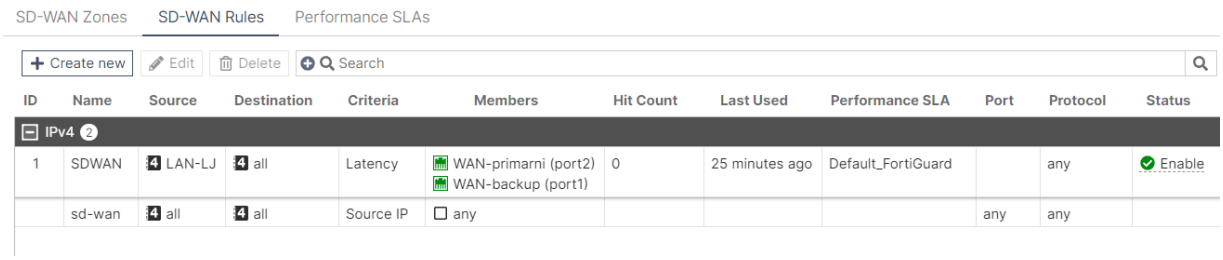
SD-WAN (Software-Defined Wide Area Network) je tehnologija upravljanja mrežnim prometom koja omogućava pametno usmjeravanje na temelju stvarnih performansi linkova i definiranih prioriteta. Za razliku od statičkog usmjeravanja koje koristi fiksne metrike poput administrativne distance, SD-WAN donosi dinamičko odlučivanje prema parametrima kao što su latencija, jitter, gubitak paketa i raspoloživost linka.

Prednosti implementacije SD-WAN rješenja su povećana dostupnost povezanosti kroz automatski failover, optimizacija performansi aplikacija usmjeravanjem prema najkvalitetnijem linku te smanjenje troškova korištenjem više jeftinijih Internet linkova umjesto skupih MPLS veza.

U sklopu mreže kompanije HercMerc implementirano je SD-WAN rješenje na FortiGate-LJ vatrozidu kako bi se optimizirao odlazni promet prema Internetu i osigurala visoka dostupnost u slučaju ispada jednog od linkova. Kreirana je SD-WAN zona pod nazivom "SDWAN" koja objedinjuje dva izlazna linka: WAN-primarni (port2) i WAN-backup (port1).

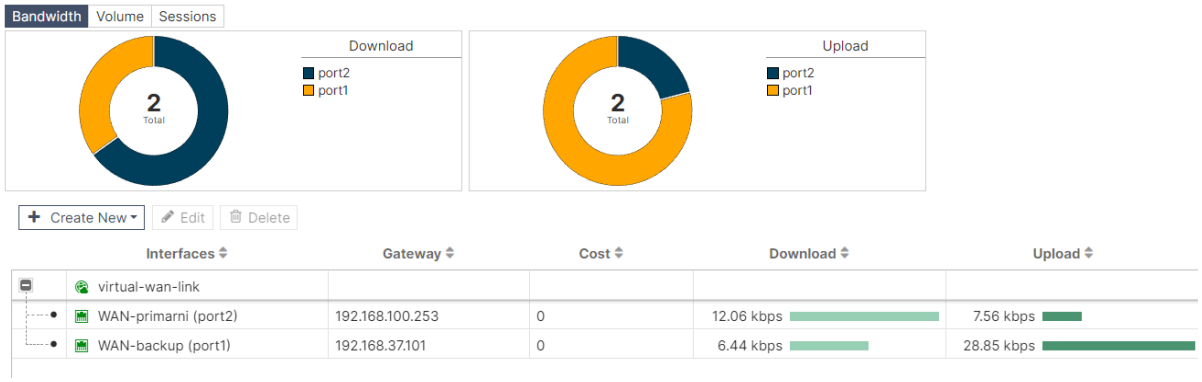
Za ovu SD-WAN zonu definirano je pravilo koje postavlja izvor prometa na LAN-LJ zonu, destinaciju na sve adrese (all), a kao kriterij odabira linka koristi se latencija. Ova konfiguracija osigurava da će FortiGate u svakom trenutku koristiti link s nižim kašnjenjem, čime se optimiziraju performanse za aplikacije koje koriste korisnici iz centralne lokacije.

Za mjerenje kvalitete linkova korišten je ugrađeni FortiGuard servis kao target za monitoring performansi (Default_FortiGuard) i proizvoljni dodatni test na Google DNS (8.8.8.8).



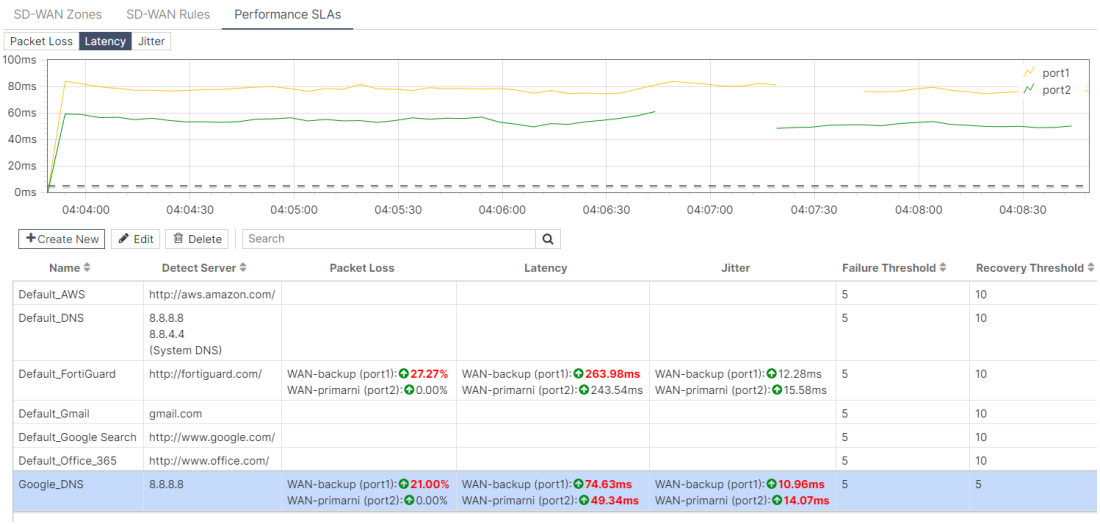
Slika 10 – SD-WAN pravilo s kriterijima odabira linka i definiranim članovima zone

Funkcionalnost SD-WAN rješenja verificirana je analizom distribucije prometa između linkova te praćenjem performansi oba linka kroz vremenski period. Slika 11 prikazuje grafičke prikaze uporabe linkova u SD-WAN zoni, gdje se jasno vidi da promet dinamički koristi oba linka ovisno o njihovim trenutnim performansama.



Slika 11 – Grafički prikazi uporabe linkova (bandwidth) u SD-WAN zoni

Slika 12 prikazuje detaljan prikaz performansi Default_FortiGuard targeta kroz oba linka, gdje su vidljive metrike latencije, jittera i dostupnosti. Na temelju ovih mjerenja FortiGate donosi odluke o usmjeravanju prometa prema linku s boljim performansama.



Slika 12 – Grafički prikaz performansi Default_FortiGuard targeta kroz oba linka

Implementirano SD-WAN rješenje na FortiGate-LJ vatrozidu osigurava pametno upravljanje odlaznim prometom kompanije HercMerc, automatsku redistribuciju prometa u slučaju degradacije performansi jednog linka te povećanu otpornost na ispade kroz seamless failover mehanizam.

6. Virtualne privatne mreže između lokacija

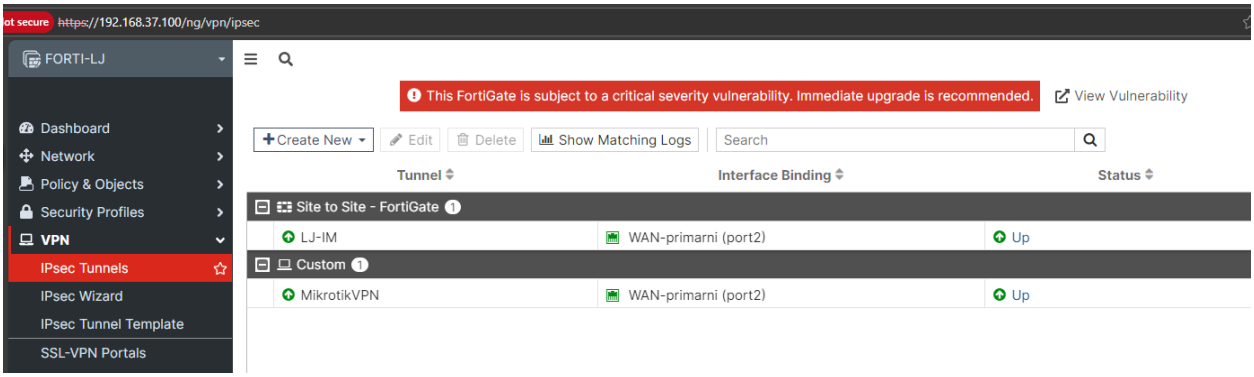
Virtualne privatne mreže između lokacija (Site-to-Site VPN) omogućavaju sigurnu komunikaciju između geografski udaljenih lokacija organizacije preko javne mreže Internet. U ovom projektu implementiran je IPsec Site-to-Site VPN tunel između partnerske lokacije (MikroTik usmjernik sa LAN mrežom 192.168.120.0/24) i centralne lokacije (FortigateLJ sa LAN mrežom 10.10.10.0/24, kasnije u projektu 20.20.20.0/24).

IPsec (Internet Protocol Security) predstavlja skup protokola za kriptografsku zaštitu IP komunikacije koji pruža povjerljivost enkripcijom podataka, integritet korištenjem hash algoritama i autentikaciju komunikacijskih strana. Uspostava IPsec tunela odvija se kroz dvije faze pregovaranja - IKE Phase 1 i Phase 2.

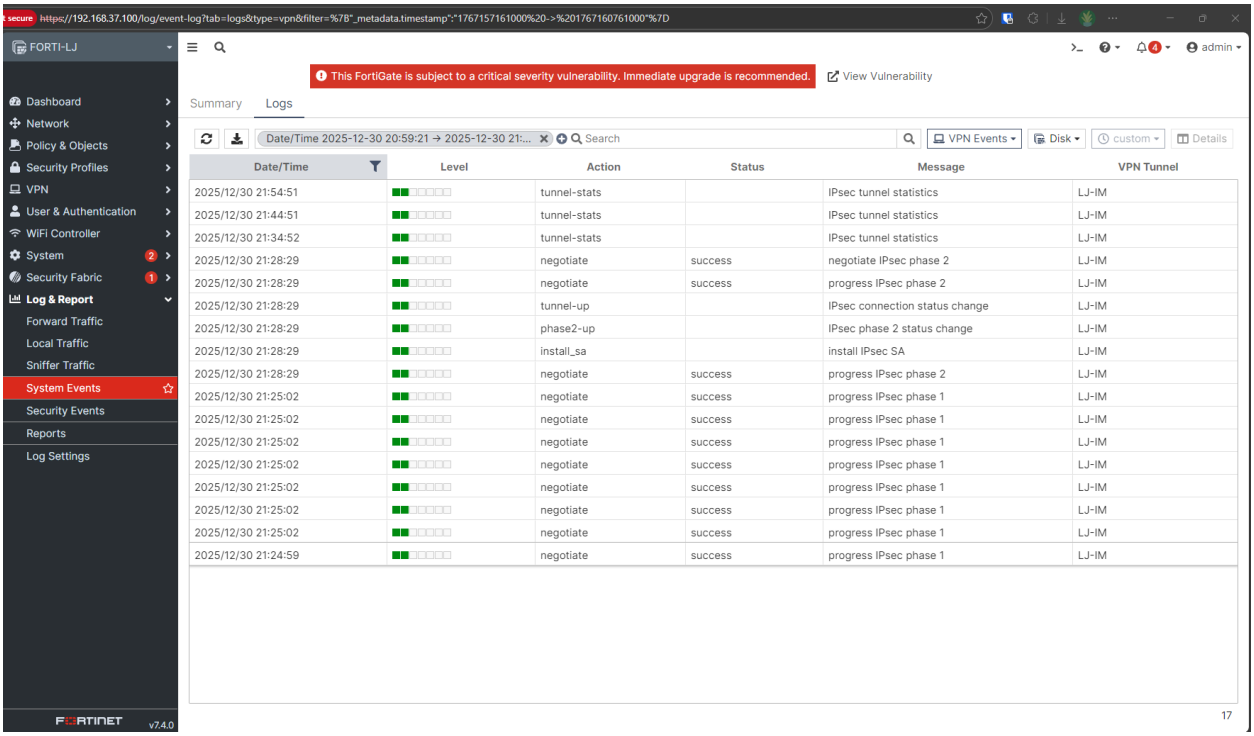
IKE Phase 1 uspostavlja siguran kontrolni kanal između VPN gateway uređaja. U našoj implementaciji koristimo IKEv2 protokol, AES-256 enkripciju, SHA-256 hash algoritam i Diffie-Hellman Group 14 (modp2048). Autentikacija se provodi Pre-Shared Key metodom.

IKE Phase 2 uspostavlja IPsec Security Associations za enkripciju korisničkog prometa. Koristi ESP sa AES-256-CBC enkripcijom i SHA-256-HMAC autentikacijom, te Perfect Forward Secrecy (PFS) sa DH Group 14. IPsec policy definira da će promet između subneta 192.168.120.0/24 i 20.20.20.0/24 biti enkriptiran kroz tunel između WAN adresa 192.168.102.253 (MikroTik) i 192.168.100.254 (FortigateLJ).

Konfiguracija MikroTik usmjernika obuhvaća definiranje IPsec Proposal sa encryption algoritmom AES-256-CBC, authentication algoritmom SHA-256 i PFS group modp2048. IPsec Peer definira remote gateway adresu 192.168.100.254 i specificira IKEv2 protokol. Kritičan element je NAT bypass konfiguracija - dva pravila postavljena na vrhu firewall NAT chain-a izuzimaju IPsec promet iz NAT procesa, omogućavajući da paketi zadrže originalne IP adrese prije enkripcije.

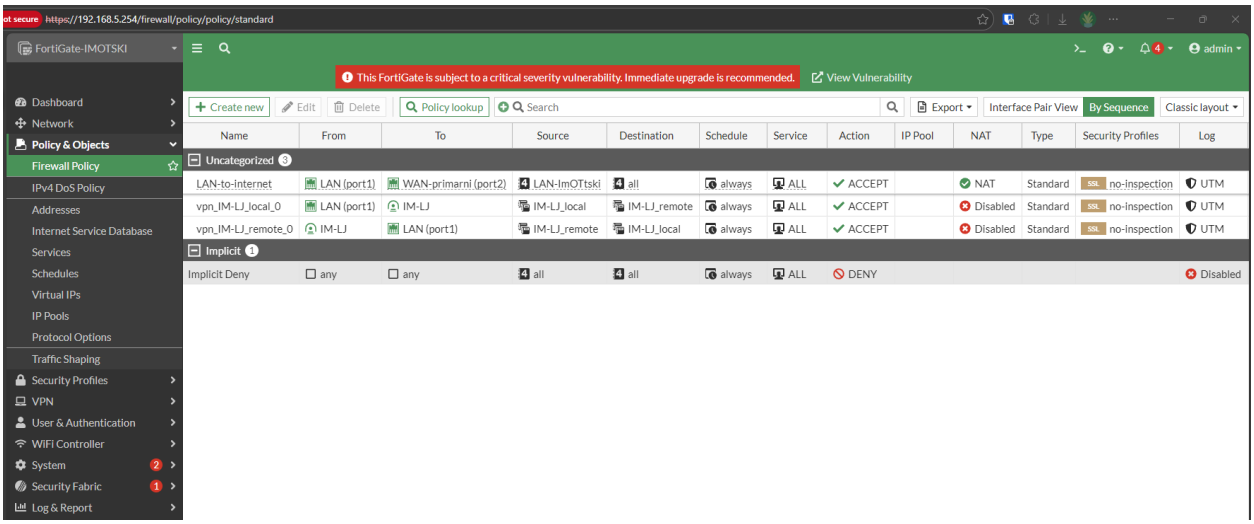


Slika 13 – Status IPsec tunela na FortigateLJ - tunel "MikrotikVPN" aktivan sa statusom UP



Slika 14 – FortigateLJ System Events logovi prikazuju uspješnu IKE Phase 1 i Phase 2 uspostavu

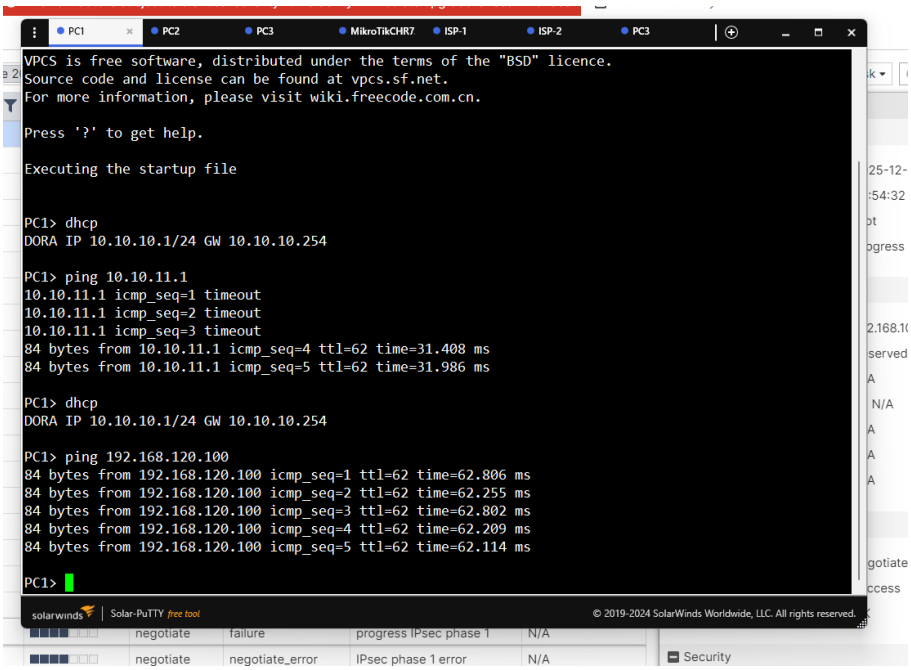
Funkcionalnost tunela verificirana je na više načina. FortigateLJ logovi pokazuju redovne "progress IPsec phase 1" i "progress IPsec phase 2" događaje sa statusom "success", te "tunnel-up" i "phase2-up" poruke koje potvrđuju aktivnost tunela.



Slika 15 – FortiGate-IMOTSKI Firewall policy – automatski dodani vpn local i remote

Firewall policy pravila kreirana su između "LAN" i "LJ-IM" (IPsec interface) dozvoljavajući sav promet između lokalnog subneta 10.10.10.0/24 i remote subneta 192.168.120.0/24 kroz tunel.

End-to-end connectivity test proveden je sa PC1 klijentskog računala (10.10.10.1) korištenjem ping naredbe prema PC3 računalu (192.168.120.100). Uspješan ping sa 84 bytes paketa i približno 62ms latencije potvrđuje funkcionalnost IPsec tunela.



Slika 16 – Uspješan ping sa PC1 (10.10.10.1) prema PC3 (192.168.120.100) kroz IPsec tunel

Tijekom implementacije IPsec tunela bilo je potrebno dodatno prilagoditi NAT i routing kako bi komunikacija između PC1 i PC3 funkcionirala u oba smjera. Umjesto da se promet jednostavno prepusti postojećoj masquerade konfiguraciji, MikroTik NAT pravila bilo je potrebno nadopuniti tako da ne mijenjaju source IP adresu prometa namijenjenog IPsec tunelu. Konkretno, na vrh NAT chain-a dodana su NAT bypass pravila koja izuzimaju sav promet između subneta 10.10.10.0/24 i 192.168.120.0/24 iz NAT procesa, čime se omogućuje da IPsec policy ispravno prepozna i enkriptira originalne IP adrese.

Ovaj dodatni korak jasno pokazuje koliko su redoslijed firewall/NAT pravila i simetričan routing važni elementi kod Site-to-Site VPN implementacija između različitih vendorskih platformi. Umjesto da se problem promatra kao pogreška konfiguracije, može se smatrati sastavnim dijelom finog ugađanja VPN rješenja, gdje je potrebno uskladiti način rada NAT-a, IPsec politika i ruta na oba kraja tunela kako bi se osigurala potpuno transparentna dvosmjerna komunikacija.

7. Analiza SSL/TLS prometa

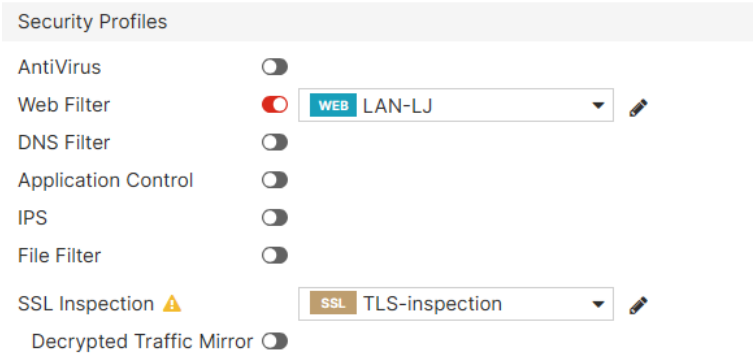
SSL/TLS inspekcija predstavlja ključnu sigurnosnu funkcionalnost modernih vatrozida nove generacije koja omogućava dubinsku analizu šifriranog mrežnog prometa. U današnjem digitalnom okruženju gdje preko 90% internetskog prometa koristi HTTPS protokol sa SSL/TLS enkripcijom, tradicionalni vatrozidi postaju neučinkoviti jer ne mogu analizirati šifrirani sadržaj.

SSL/TLS inspekcija funkcionira na principu kontroliranog Man-in-the-Middle (MITM) pristupa, gdje vatrozid djeluje kao posrednik između klijenta i poslužitelja. FortiGate podržava dva načina inspekcije šifriranog prometa.

Prva metoda je *Certificate Inspection* koja analizira samo zaglavlja paketa i SSL certifikat bez dekriptiranja sadržaja gdje vatrozid provjerava valjanost certifikata, izdavača i datum isteka, ali ne može vidjeti enkriptirani payload.

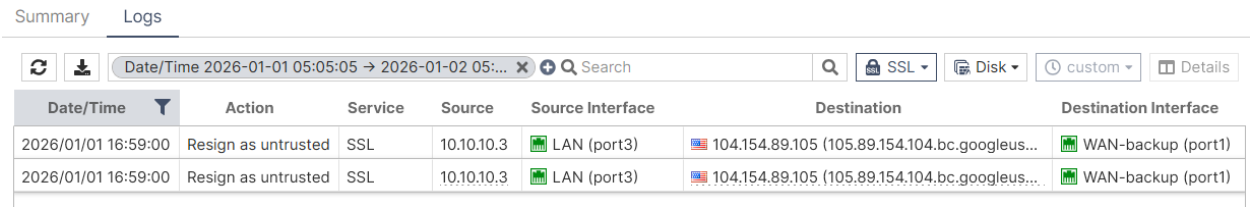
Druga metoda je *Deep Inspection* (potpuna inspekcija) koja omogućava kompletnu dubinsku analizu enkriptiranog sadržaja. Kod potpune inspekcije, FortiGate uspostavlja SSL sesiju s vanjskim poslužiteljem, prima originalni certifikat i verificira njegovu autentičnost, zatim dinamički generira zamjenski certifikat potpisan vlastitim CA certifikatom, te taj zamjenski certifikat predstavlja klijentu. Na taj način vatrozid može dekriptirati promet pomoću vlastitog privatnog ključa, provesti ga kroz sve sigurnosne profile, te ponovno enkriptirati prije slanja prema klijentu.

Za potrebe ovog projekta konfiguriran je SSL inspekcijski profil koji koristi metodu potpune inspekcije (*Full Deep Inspection*). Profil je postavljen za analizu odlaznog internetskog prometa gdje se više klijenata iz lokalne mreže povezuje na više vanjskih poslužitelja. Unutar profila odabran je Fortinet_CA_SSL certifikat koji vatrozid koristi za potpisivanje svih dinamički generiranih certifikata tijekom HTTPS sesija. SSL inspekcijski profil primijenjen je u sigurnosno pravilo koje regulira odlazni promet iz lokalne mreže 10.10.10.0/24 prema NAT1 cloud-u, s konfiguriranim praćenjem SSL anomalija kako bi se evidentirali pokušaji pristupa stranicama s nevažećim ili isteklim certifikatima.



Slika 17 – FortiGate-LJ Security Profiles

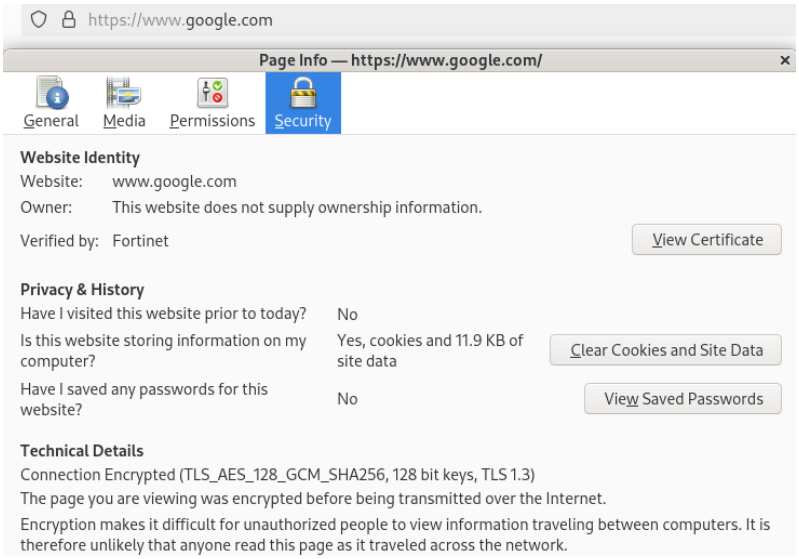
Nakon konfiguracije SSL inspekcijskog profila, Fortinet_CA_SSL root certifikat izvezen je i instaliran u Firefox web preglednik na klijentskom računalu Windows-SERVER. Instalacija CA certifikata ključna je kako bi klijent prihvatio zamjenske certifikate koje dinamički generira vatrozid, a da pritom ne prikazuje sigurnosna upozorenja.



Slika 18 – FortiGate logovi SSL inspekcije s prikazom resign akcije

Funkcionalnost SSL inspekcije potvrđena je kroz FortiGate log zapise prikazane na Slici 18. U logovima je vidljiva akcija „Resign as trusted“ za SSL servis, što označava da je FortiGate presreo SSL certifikat vanjskog poslužitelja, ocijenio ga kao nevaljan ili nepouzdan, te ga zamijenio vlastitim certifikatom.

Zapisi prikazuju izvornu adresu 10.10.10.3 s LAN sučelja (port3) koja pristupa destinaciji 104.154.89.105 (bc.googleusercontent.com) preko WAN-backup sučelja (port1). Datum i vrijeme logova (2026/01/01 16:59:00) potvrđuju kontinuiranu inspekciju SSL prometa u realnom vremenu.



Slika 19 – Detalji SSL/TLS certifikata prilikom pristupa google.com s aktivnom SSL inspekcijom

Na Slici 19. prikazan je dokaz uspješno konfigurirane SSL inspekcije prilikom pristupa google.com web stranici. U Security tabu Firefox preglednika vidljivo je da je certifikat verificiran od strane *Fortinet* CA autoriteta umjesto standardnog Google Trust Services certifikata. Ovo potvrđuje da FortiGate presreće HTTPS promet, dekriptira ga, analizira sadržaj kroz konfigurirane sigurnosne profile, te predstavlja vlastiti certifikat klijentu.

8. Kontrola web prometa

Kontrola web prometa predstavlja temeljnu sigurnosnu funkcionalnost vatrozida nove generacije koja omogućava nadzor i regulaciju pristupa internetskim sadržajima na temelju definiranih politika. Organizacije koriste web filtriranje kako bi smanjile izloženost sigurnosnim prijetnjama poput malware distribucije, phishing napada i zlonamjernih web stranica, te istovremeno povećale produktivnost zaposlenika ograničavanjem pristupa neprikladnom sadržaju tijekom radnog vremena. Benefiti ovog mehanizma uključuju zaštitu od web-based napada, kontrolu propusnosti mreže, usklađenost s regulatornim zahtjevima te optimizaciju korištenja internetskih resursa.

FortiGate vatrozidi podržavaju dva primarna mehanizma web filtriranja - FortiGuard dinamičko kategorizirano filtriranje i statičko URL filtriranje. FortiGuard web filtriranje koristi cloud-based bazu podataka koja sadrži preko milijardu kategoriziranih web stranica raspodijeljenih u 85+ kategorija.

Ovaj mehanizam funkcionira tako da FortiGate presreće HTTP/HTTPS zahtjev korisnika, izvlači URL ili IP adresu destinacije, šalje upit FortiGuard serverima za provjeru kategorije, te na temelju povratne informacije primjenjuje konfiguriranu akciju (allow, block, monitor, warning). Prednost FortiGuard filtriranja je automatsko ažuriranje baze podataka i dinamička kategorizacija novih web stranica, dok je nedostatak ovisnost o cloud povezivosti i potencijalna latencija pri upitima.

Statičko URL filtriranje omogućava administratorima ručno definiranje specifičnih URL uzoraka s regex izrazima i primjenu akcija (Block, Exempt, Monitor) neovisno o FortiGuard kategorizaciji. Ova metoda koristi se za precizno blokiranje ili dozvoljavanje određenih domena ili dijelova web stranica koje nisu adekvatno pokrivene kategorijama. Prednost statičkog filtriranja je potpuna kontrola i neovisnost o vanjskim servisima, dok je nedostatak potreba za ručnim održavanjem popisa i nemogućnost skaliranja na velike količine URL adresa.

Za potrebe ovog projekta konfigurirano je web filtriranje koje blokira pristup društvenim mrežama (Social Networking kategorija) za sve korisnike iz mreže 10.10.10.0/24. Kreiran je web filter profil unutar Security Profiles gdje je FortiGuard kategorija broj 37 (Social Networking) postavljena na akciju *Block*. Profil je primijenjen u sigurnosno pravilo koje regulira odlazni internetski promet prema NAT1 cloud-u.

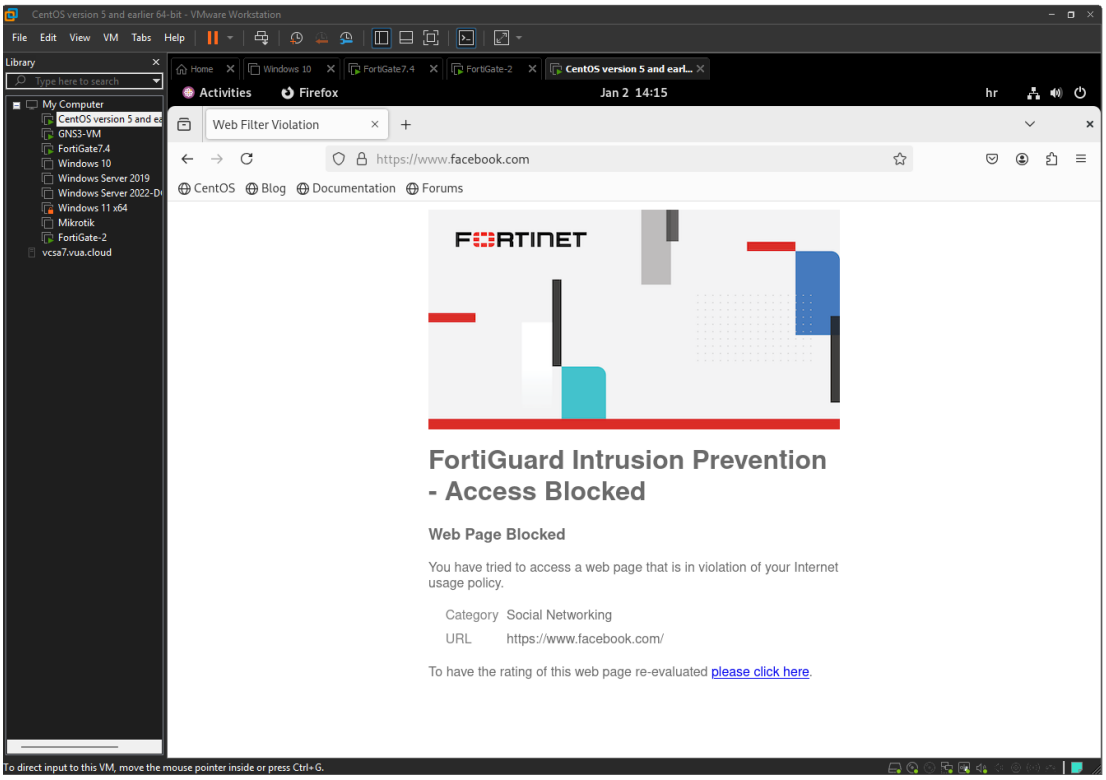
Summary | Logs

Search | Web Filter | Disk | 24 hours | Details

Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
2026/01/02 05:08:43		10.10.10.3	Blocked	https://www.facebook.com/	Social Networking		516 B / 61 B
2026/01/01 17:05:29		10.10.10.3	Blocked	http://instagram.com/favicon.ico	Social Networking		349 B / 0 B
2026/01/01 17:05:28		10.10.10.3	Blocked	http://instagram.com/	Social Networking		379 B / 0 B
2026/01/01 16:58:45		10.10.10.3	Blocked	https://www.facebook.com/favicon.ico	Social Networking		5.16 kB / 7.92 kB
2026/01/01 16:58:45		10.10.10.3	Blocked	https://www.facebook.com/	Social Networking		4.72 kB / 7.64 kB

Slika 20 – FortiGate logovi blokiranja pristupa društvenim mrežama

Funkcionalnost web filtriranja potvrđena je kroz FortiGate log zapise prikazane na Slici 20. U logovima je vidljivo kontinuirano blokiranje pristupa različitim društvenim mrežama - Instagram (instagram.com/favicon.ico) i Facebook (facebook.com/favicon.ico i facebook.com). Zapisi prikazuju izvornu adresu 10.10.10.3 s LAN sučelja koja pokušava pristupiti blokiranom sadržaju kategorizirane kao *Social Networking*. Svi zahtjevi označeni su akcijom *Blocked* s detaljnim prikazom URL-a, kategorije i količine poslanih/primljenih podataka (Sent/Received).



Slika 21 – FortiGuard Intrusion Prevention blokada pristupa Facebooku

Na Slici 21. prikazan je prikaz s korisničke strane prilikom pokušaja pristupa facebook.com web stranici. FortiGate prikazuje replacement message s naslovom "*FortiGuard Intrusion Prevention - Access Blocked*" i informacijom "*Web Page Blocked - You have tried to access a web page that is in violation of your Internet usage policy*". U detaljima je navedena kategorija *Social Networking* i puni URL https://www.facebook.com/ koji je blokiran. Ovaj vizualni prikaz potvrđuje da web filter ispravno funkcionira i obavještava korisnike o razlogu blokiranja pristupa, čime se povećava transparentnost sigurnosne politike organizacije.

9. Kontrola prometa aplikacija

Kontrola aplikacija predstavlja naprednu sigurnosnu funkcionalnost vatrozida nove generacije koja omogućava identifikaciju, praćenje i regulaciju mrežnog prometa na razini aplikacijskog sloja (Layer 7 OSI modela) neovisno o korištenim portovima ili protokolima. Za razliku od tradicionalnih vatrozida koji kontroliraju promet isključivo na temelju IP adresa i TCP/UDP portova, Application Control koristi tehniku Deep Packet Inspection (DPI) za analizu payload dijela paketa i prepoznavanje specifičnih aplikacija prema njihovim karakterističnim digitalnim potpisima.

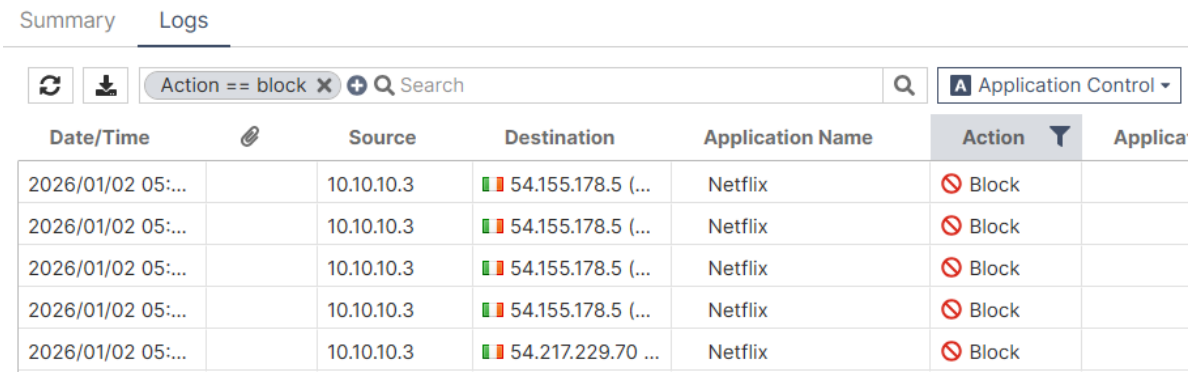
Svrha ovog mehanizma je omogućiti preciznu kontrolu nad upotrebom pojedinih aplikacija unutar organizacije, blokirati neželjene servise koji zaobilaze standardne portove, te spriječiti propuštanje povjerljivih podataka kroz neautorizirane aplikacijske kanale.

Bitna razlika između web filtriranja i aplikacijske kontrole ogleda se u razini analize i obuhvatu kontrole prometa. Web filtriranje funkcionira isključivo na HTTP/HTTPS protokolima i fokusira se na kategorizaciju i blokiranje web stranica prema URL adresama ili FortiGuard kategorijama, analizirajući pritom HTTP request/response zaglavlja. S druge strane, Application Control djeluje na svim protokolima i može identificirati specifične aplikacije bez obzira koriste li web (HTTP/HTTPS), custom protokole ili enkapsuliraju promet u standardne portove kako bi zaobišle vatrozid.

Primjerice, web filtriranje može blokirati pristup youtube.com domeni, ali ne može spriječiti YouTube video streaming kroz mobilnu aplikaciju koja koristi različite tehnike tuneliranja. Application Control prepoznaje i sam YouTube promet na temelju aplikacijskih signatura (Netflix_Video.Play, Skype.Voice, BitTorrent, itd.) neovisno o korištenoj metodi prijenosa.

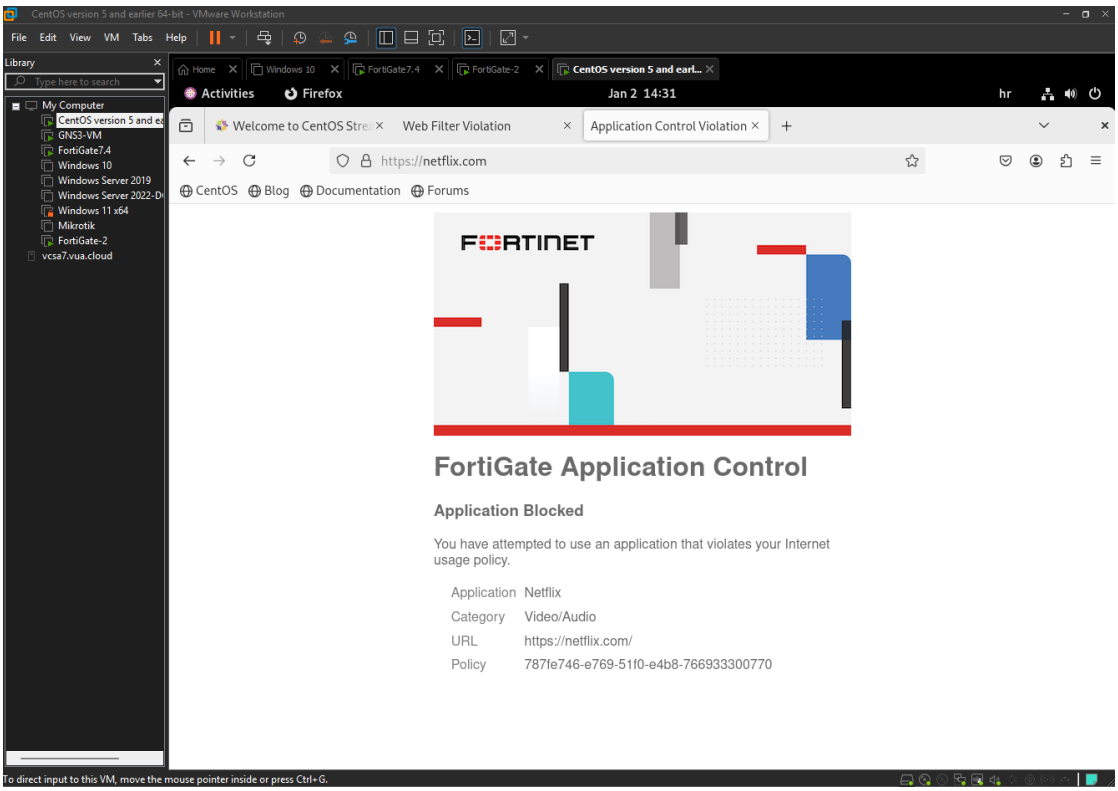
Za potrebe ovog projekta konfiguriran je Application Control profil koji blokira pristup Netflix streaming servisu. Unutar Security Profiles kreiran je Application Control profil s override pravilom (Application and Filter Overrides) koje definira blokiranje svih Netflix aplikacijskih signatura. Override pravilo postavljeno je s prioritetom 1 i akcijom *Block* za sve navedene aplikacije kategorije Video/Audio.

Profil je primijenjen u sigurnosno pravilo koje regulira odlazni internetski promet iz mreže 10.10.10.0/24 prema vanjskim destinacijama.



Slika 22 – FortiGate logovi blokiranja Netflix aplikacijskog prometa

Funkcionalnost Application Control mehanizma potvrđena je kroz FortiGate log zapise prikazane na Slici 22. U logovima je vidljivo kontinuirano blokiranje pokušaja pristupa Netflix servisu s izvorne adrese 10.10.10.3 prema različitim Netflix poslužiteljima (54.155.178.5, 54.217.229.70). Svi zapisi označeni su akcijom *Block* s jasno identificiranom aplikacijom "Netflix" u Application Name polju. Vremenski zapisi (2026/01/02 05:...) potvrđuju kontinuiranu inspekciju i blokiranje aplikacijskog prometa u realnom vremenu.



Slika 23 – FortiGate Application Control blokada pristupa Netflixu

Na Slici 23. je prikaz s korisničke strane prilikom pokušaja pristupa netflix.com web stranici. Ovaj vizualni dokaz potvrđuje da Application Control uspješno funkcionira i transparentno obavještava korisnike o razlogu blokiranja, čime se osigurava jasna komunikacija sigurnosne politike organizacije.

10. Antivirusna kontrola prometa

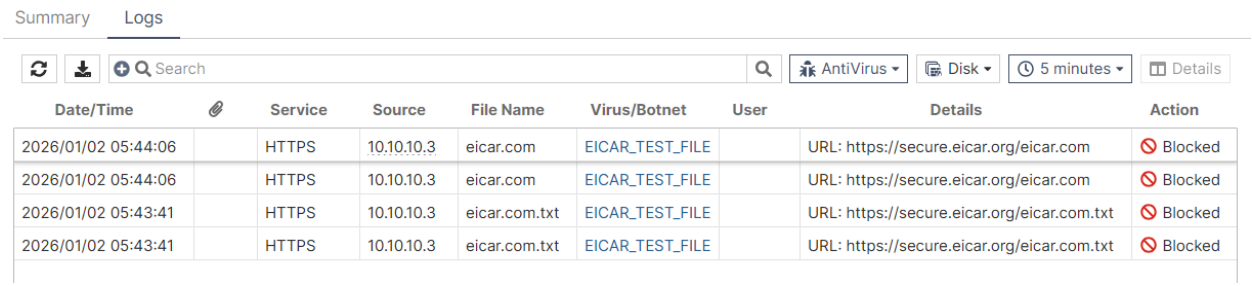
Antivirusna kontrola prometa predstavlja važnu sigurnosnu funkcionalnost NGFW koja omogućava detekciju i blokiranje malicioznog softvera u stvarnom vremenu tijekom prolaska kroz mrežnu infrastrukturu. Važnost ovog mehanizma očituje se u zaštiti krajnjih korisnika od malware infekcija, ransomware napada, trojanaca i drugih vrsta zlonamjernog koda prije nego takav sadržaj stigne do klijentskih računala. Vatrozid koristi tehniku *inline scanning* gdje analizira sadržaj datoteka koje prolaze kroz njega, uspoređuje ih s ažuriranom bazom virusnih signatura (FortiGuard Antivirus Database), te primjenjuje definiranu akciju kada detektira prijetnju.

Unatoč svojoj važnosti, antivirusna kontrola posjeduje određena ograničenja koja utječu na njenu učinkovitost. Primarno ograničenje je nemogućnost inspekcije šifriranog prometa bez prethodne implementacije SSL/TLS inspekcije. Kada je promet enkriptiran, antivirus mehanizam ne može vidjeti payload dio paketa i samim time ne može detektirati malware. Dodatno ograničenje predstavlja ovisnost o bazi virusnih signatura, što znači da antivirus ne može detektirati zero-day prijetnje ili potpuno nove varijante malwarea dok njihove signature nisu dodane u bazu podataka.

Također, dubinska inspekcija datoteka uzrokuje dodatno opterećenje CPU resursa i uvodi latenciju u mrežni promet, što može utjecati na performanse mreže kod velikog volumena prometa ili velikih datoteka. Konačno, sofisticirani malware može koristiti tehnike obfuscacije, polimorfizma ili enkapsulacije koje otežavaju detekciju signature-based antivirusnim sustavima.

Za potrebe ovog projekta konfiguriran je antivirusni profil pod nazivom "AntiVirus-LJ" koji omogućava inspekciju HTTP i HTTPS prometa. Profil je postavljen s opcijom *Include mobile malware protection* kako bi se proširila detekcija i na prijetnje namijenjene mobilnim platformama. Antivirusni profil primijenjen je u sigurnosno pravilo koje regulira odlazni internetski promet iz mreže 10.10.10.0/24 prema vanjskim destinacijama.

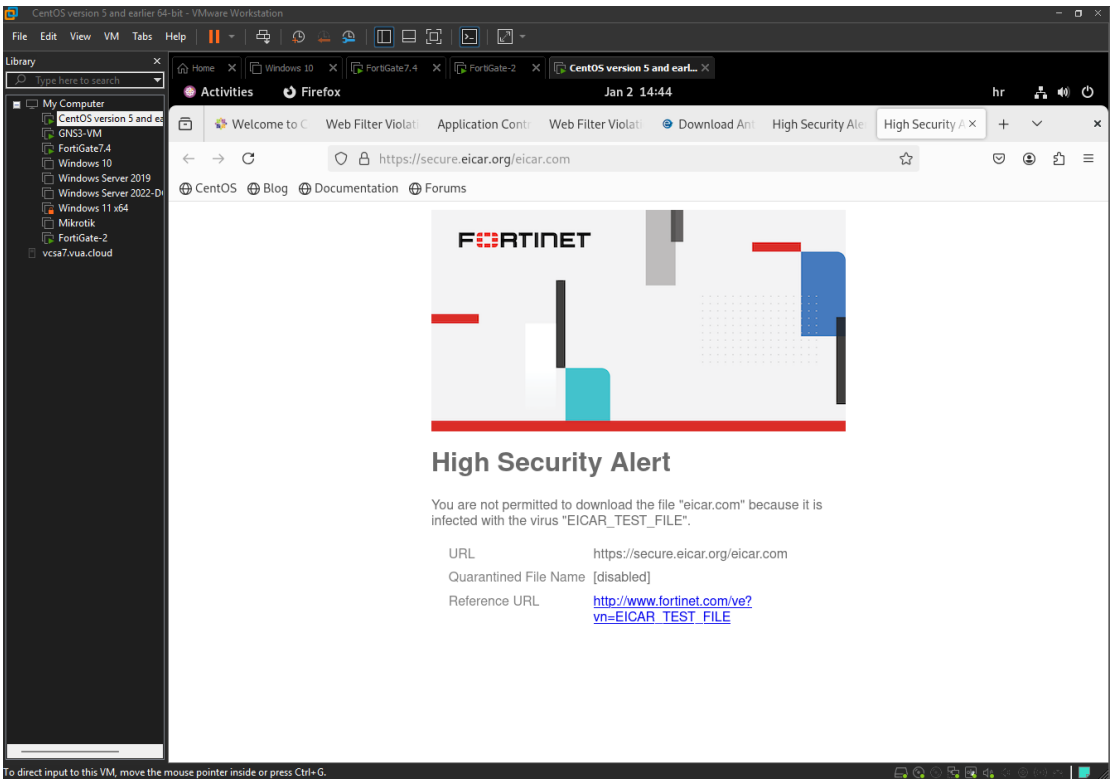
Funkcionalnost antivirusne kontrole testirana je korištenjem EICAR standardne test datoteke. EICAR (European Institute for Computer Antivirus Research) test file je bezopasna datoteka koju svi antivirusni sustavi prepoznaju kao malware isključivo u svrhu testiranja funkcionalnosti antivirusnih mehanizama. Test je proveden pokušajem downloada EICAR datoteka s secure.eicar.org web stranice preko HTTPS protokola.



Slika 24 – FortiGate logovi detekcije i blokiranja EICAR test datoteka

Na Slici 24. prikazani su FortiGate log zapisi s filterom AntiVirus gdje je vidljiva uspješna detekcija EICAR test datoteka. U logovima su evidentirani pokušaji downloada s izvorne adrese 10.10.10.3 prema secure.eicar.org serveru preko HTTPS protokola. File Name polje prikazuje nazive detektiranih datoteka (eicar.com i eicar.com.txt), dok je Virus/Botnet polje jasno označilo prijetnju kao "EICAR_TEST_FILE".

Svi zapisi imaju akciju *Blocked* što potvrđuje da FortiGate uspješno presreće i blokira maliciozne datoteke prije nego stignu do klijentskog računala. Vremenski zapisi (2026/01/02 05:43-05:44) i detalji URL-a potvrđuju kontinuiranu antivirusnu inspekciju u realnom vremenu.



Slika 25 – FortiGate High Security Alert blokada downloada EICAR datoteke

Na Slici 25. prikazan je prikaz s korisničke strane prilikom pokušaja downloada EICAR test datoteke. FortiGate prikazuje replacement message s naslovom "*High Security Alert*" i jasnom porukom "*You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE"*". U detaljima je navedena URL adresa https://secure.eicar.org/eicar.com, oznaka da je Quarantined File Name onemogućen (disabled), te referentni link na FortiGuard bazu podataka za dodatne informacije o detektiranoj prijetnji.

Ovaj vizualni dokaz potvrđuje da antivirusni mehanizam transparentno obavještava korisnike o detektiranom malwareu i razlogu blokiranja, čime se sprječava slučajno preuzimanje zaraženih datoteka i povećava sigurnosna svijest zaposlenika.

11. Sustav prevencije napada i zaraza malicioznim softverom

Sustav prevencije napada (IPS - Intrusion Prevention System) predstavlja ključnu sigurnosnu komponentu vatrozida nove generacije koja aktivno štiti mrežnu infrastrukturu od poznatih i nepoznatih prijetnji. Za razliku od pasivnih sustava detekcije (IDS), IPS sustav djeluje u realnom vremenu analizirajući svaki paket koji prolazi kroz vatrozid te ima mogućnost blokiranja zlonamjernog prometa prije nego dospije do krajnjih sustava unutar mreže.

Moderna IPS rješenja koriste kombinaciju tehnika prepoznavanja prijetnji uključujući analizu potpisa napada (signature-based detection), heurističku analizu ponašanja prometa te algoritme za detekciju zero-day napada koji iskorištavaju do tada nepoznate ranjivosti.

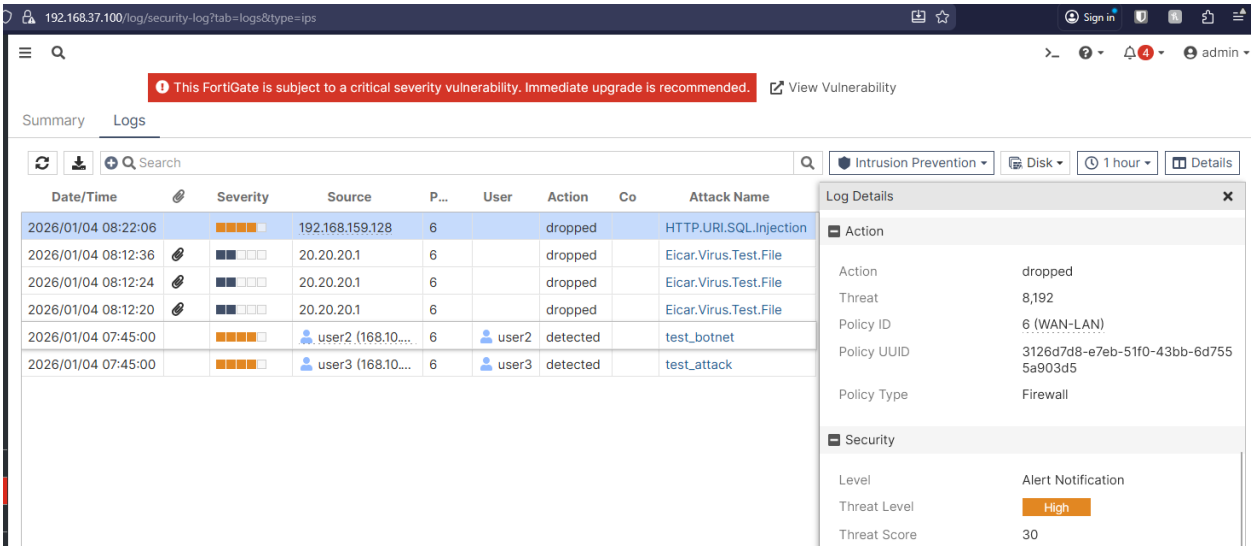
Anomalije predstavljaju odstupanja od normalnog ponašanja mrežnog prometa koje mogu ukazivati na potencijalni napad ili zloupotrebu mrežnih resursa. Primjeri anomalija uključuju TCP SYN flooding napade gdje napadač šalje prekomjerni broj TCP SYN paketa kako bi iscrpio resurse ciljnog sustava, prekomjerni ICMP promet, neobične obrasce fragmentiranih paketa ili abnormalno velike količine prometa iz jednog izvora

Prvim korakom potrebno je konfigurirati IPS senzore koji definiraju koje vrste napada će biti detektirane i blokirane, uključujući odabir potpisa napada prema težini prijetnje, verziji operacijskog sustava i ciljane aplikacije.

Drugim korakom konfigurirani sigurnosni profili primjenjuju se na odgovarajuća sigurnosna pravila koja određuju na koji promet, iz kojih izvora i prema kojim odredištima će se primjenjivati IPS inspekcija.

U projektnom zadatku uspostavljena je IPS zaštita koja demonstrira mogućnosti detekcije i prevencije različitih vrsta napada iz javne mreže. Za testiranje sustava korištena je Linux mašina s IP adresom 192.168.159.128 iz koje su pokrenuti exploit napadi prema internoj infrastrukturi (Windows-SERVER 20.20.20.1, prijašnje 10.10.10.0/24 mreža). Exploit napad proveden je pokušajem SQL injection-a preko HTTP protokola koja cilja kompromitiranje web aplikacija unutar organizacije.

Kao što je vidljivo na Slici 1, FortiGate sustav uspješno je detektirao HTTP.URI.SQL.Injection napad te je aktivirao zaštitnu akciju koja je blokirala zlonamjerni promet. Log zapis prikazuje datum i vrijeme napada, izvornu IP adresu napadača (192.168.159.128), protokol koji se koristio (protokol 6 - TCP), te provedenu akciju (dropped) što potvrđuje da napad nije dospio do ciljanog sustava.

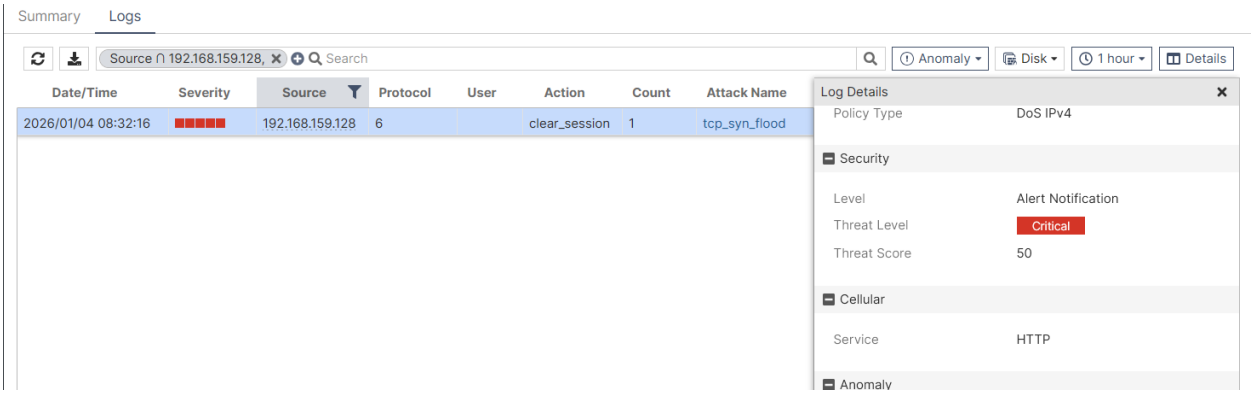


Slika 26 – Prikaz IPS logova s detektiranim HTTP.URI.SQL.Injection exploit napadom

U detaljima log zapisa prikazanog na Slici 26 vidljivo je da je prijetnja klasificirana kao visoka (Threat Level: High). Sigurnosno pravilo koje je primijenilo IPS inspekciju označeno je kao Policy ID 6 (WAN-LAN), što ukazuje da je zaštita aktivirana na prometu koji dolazi iz javne mreže prema lokalnoj mreži.

Dodatno je testirana i zaštita od mrežnih anomalija simulacijom TCP SYN flood napada koji predstavlja jedan od najčešćih DoS (Denial of Service) napada. Kao što prikazuje Slika 27, vatrozid je prepoznao anomaliju kroz potpis tcp_syn_flood te je detektirao pokušaj iscrpljivanja resursa slanjem velikog broja TCP SYN paketa bez dovršavanja three-way handshake procesa.

FortiGate sustav je primijenio clear_session akciju kako bi automatski prekinuo sve zlonamjerne sesije i zaštitio resurse unutar mreže. Prijetnja je klasificirana kao kritična (Threat Level: Critical) s rezultatom prijetnje 50 bodova, što predstavlja najviši stupanj opasnosti i zahtijeva trenutnu intervenciju. Log zapis prikazuje da je napad pokrenut u 08:32:16 sati, također iz izvora 192.168.159.128, koristeći HTTP servis kao vektor napada.



Slika 27 – Detekcija TCP SYN flood anomalije u IPS logovima s kritičnom razinom prijetnje

Dodatni segment testiranja obuhvatio je i antivirusnu komponentu IPS sustava koristeći EICAR test virus datoteke koje služe za sigurno testiranje antivirusnih mehanizama bez stvarnog rizika za sustave.

Implementirano IPS rješenje na FortiGate vatrozidu demonstrira sveobuhvatnu zaštitu koja pokriva različite vektore napada uključujući exploite aplikacijskih ranjivosti, mrežne anomalije DoS/DDoS tipa, detekciju botnet aktivnosti te integriranu antivirusnu zaštitu. Sustav djeluje transparentno u realnom vremenu analizirajući svaki paket koji prolazi kroz vatrozid, što osigurava visok stupanj sigurnosti bez značajnog utjecaja na performanse mreže.

Kontinuirano ažuriranje potpisa napada putem FortiGuard servisa osigurava da sustav ostaje zaštićen od najnovijih prijetnji, dok detaljno logiranje svih sigurnosnih događaja omogućava analizu napada i prilagodbu sigurnosnih politika prema potrebama organizacije.

Zaključak

Projektni zadatak pokazuje da je na primjeru kompanije HercMerc uspješno implementiran cjelovit sigurnosni sustav temeljen na FortiGate vatrozidu nove generacije i pratećoj mrežnoj infrastrukturi.

Kroz topologiju s dvije glavne lokacije i partnerskom poslovnicom demonstrirano je kako se kombinacijom usmjeravanja, SD-WAN mehanizama i IPsec Site-to-Site VPN tunela može postići pouzdana, redundantna i sigurna povezanost između svih dijelova organizacije. Time su ispunjeni ključni funkcionalni zahtjevi: visoka dostupnost pristupa Internetu, sigurna komunikacija između lokacija te granularna kontrola prometa na više slojeva OSI modela.

Implementacijom sigurnosnih pravila, NAT mehanizama i FSSO rješenja postignuta je fina kontrola pristupa resursima koja se temelji na kombinaciji mrežnih parametara i korisničkog identiteta. Web filtriranje, kontrola aplikacija i antivirusni profil pokazuju da FortiGate može učinkovito filtrirati nepoželjan web sadržaj, blokirati specifične aplikacije poput Netflixa te spriječiti preuzimanje malicioznih datoteka, što je verificirano kroz logove i korisničke poruke o blokiranju pristupa. Uz to, aktivna SSL/TLS inspekcija omogućila je da se i šifrirani promet analizira i zaštiti, čime je uklonjena velika slijepa točka tradicionalnih sigurnosnih rješenja.

Dodatnu vrijednost projekta čini demonstracija sustava prevencije napada (IPS) koji je uspješno detektirao i blokirao različite vrste prijetnji, uključujući HTTP.URI.SQL.Injection exploit, TCP SYN flood anomaliju te prijenose EICAR test datoteka. Time je prikazano kako se u praksi kombiniraju signature detekcija, analiza anomalija i integrirana antivirusna zaštita za zaštitu interne mreže od napada iz javne mreže i kompromitiranih internih sustava. Kroz rješavanje problema asimetričnog routinga i NAT bypass konfiguracije na MikroTik usmjerniku dodatno je naglašena važnost razumijevanja interakcije između routing tablica, NAT pravila i IPsec politika u heterogenim okruženjima.

Sveukupno, projekt potvrđuje da pravilno dizajnirana i konfigurirana NGFW arhitektura može značajno podići razinu sigurnosti organizacije, uz zadržavanje visoke dostupnosti i performansi mrežnih servisa.

Literatura

- *Fortinet, "FortiGate Administration Guide," Fortinet Inc., 2024. [Online]. Dostupno na: https://docs.fortinet.comimage.jpg*
- *Fortinet, "IPsec VPN Configuration Guide," Fortinet Inc., 2024. [Online]. Dostupno na: https://docs.fortinet.comScreenshot-2026-01-04-173317.jpg*
- *Fortinet, "Fortinet Single Sign-On (FSSO) Solution Guide," Fortinet Inc., 2024. [Online]. Dostupno na: https://docs.fortinet.com*
- *Fortinet, "SD-WAN Deployment Guide," Fortinet Inc., 2024. [Online]. Dostupno na: https://docs.fortinet.com*
- *MikroTik, "RouterOS IPsec Configuration Manual," MikroTik, 2024. [Online]. Dostupno na: https://help.mikrotik.com*
- *W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2020.ppl-ai-file-upload.s3.amazonaws*
- *E. Maiwald, Network Security: A Beginner's Guide, 3rd ed. McGraw-Hill Education, 2014.*
- *EICAR, "EICAR Anti-Virus Test File," European Institute for Computer Antivirus Research, 2024. [Online]. Dostupno na: https://www.eicar.org*
- *GNS3, "GNS3 Documentation," GNS3 Technologies, 2024. [Online]. Dostupno na: https://docs.gns3.com*

Popis slika

Popis kratica

1. ***AD*** *- Active Directory*
2. ***AES*** *- Advanced Encryption Standard*
3. ***CA*** *- Certificate Authority*
4. ***CBC*** *- Cipher Block Chaining*
5. ***CLI*** *- Command Line Interface*
6. ***DC*** *- Domain Controller*
7. ***DHCP*** *- Dynamic Host Configuration Protocol*
8. ***DH*** *- Diffie-Hellman*
9. ***DNS*** *- Domain Name System*
10. ***DoS*** *- Denial of Service*
11. ***DPI*** *- Deep Packet Inspection*
12. ***EICAR*** *- European Institute for Computer Antivirus Research*
13. ***ESP*** *- Encapsulating Security Payload*
14. ***FSSO*** *- Fortinet Single Sign-On*
15. ***HMAC*** *- Hash-based Message Authentication Code*
16. ***HR*** *- Human Resources (Ljudski resursi)*
17. ***HTTP*** *- Hypertext Transfer Protocol*
18. ***HTTPS*** *- Hypertext Transfer Protocol Secure*
19. ***ICMP*** *- Internet Control Message Protocol*
20. ***IDS*** *- Intrusion Detection System*
21. ***IKE*** *- Internet Key Exchange*
22. ***IMAP*** *- Internet Message Access Protocol*
23. ***IP*** *- Internet Protocol*
24. ***IPS*** *- Intrusion Prevention System*
25. ***IPsec*** *- Internet Protocol Security*
26. ***MITM*** *- Man-in-the-Middle*
27. ***MPLS*** *- Multiprotocol Label Switching*
28. ***NAT*** *- Network Address Translation*
29. ***NGFW*** *- Next Generation Firewall*
30. ***NTLM*** *- NT LAN Manager*
31. ***OSI*** *- Open Systems Interconnection*
32. ***OU*** *- Organizational Unit*
33. ***PFS*** *- Perfect Forward Secrecy*
34. ***POP3*** *- Post Office Protocol version 3*
35. ***SA*** *- Security Association*
36. ***SD-WAN*** *- Software-Defined Wide Area Network*
37. ***SHA*** *- Secure Hash Algorithm*
38. ***SMTP*** *- Simple Mail Transfer Protocol*
39. ***SSL*** *- Secure Sockets Layer*
40. ***TCP*** *- Transmission Control Protocol*
41. ***UDP*** *- User Datagram Protocol*
42. ***URL*** *- Uniform Resource Locator*
43. ***UTM*** *- Unified Threat Management*
44. ***VM*** *- Virtual Machine*
45. ***VPN*** *- Virtual Private Network*
46. ***WAN*** *- Wide Area Network*