

Strateška analiza rešitev požarnih zidov naslednje generacije za okolja SMB: Primerjalna ocena rešitev Fortinet, MikroTik in Grandstream

Dejan Pogačnik
PSE Group
Rakuševa 22, 1000 Ljubljana, Slovenia, EU
E-mail: dejan.pogacnik@pse.si

Strateška analiza rešitev požarnih zidov naslednje generacije za okolja SMB: Primerjalna ocena rešitev Fortinet, MikroTik in Grandstream.....	1
1. Strateški okvir za sodobno varnost omrežij v malih in srednje velikih podjetjih (MSP).....	2
Uvod: Razvijajoče se okolje groženj za mala in srednje velika podjetja (MSP).....	2
Opredelitev okvira za odločanje: Ključna merila za ocenjevanje.....	2
2. Primarno priporočilo: Varnostni ekosistem Fortinet.....	4
2.1. Poglobljen pregled: Arhitektura in zmogljivost FortiGate-100F.....	4
2.2. FortiGuard UTP in varnostni ekosistem.....	5
2.3. Operativni profil in upravljanje.....	5
2.4. Nišna uporaba: Rešitev "vse-v-enem" FortiGate FortiWiFi-80F.....	6
3. Poglobljena analiza alternativnih rešitev.....	7
3.1. Platforma za strokovnjake: MikroTik z Wazuh SIEM.....	7
3.2. Konvergenčni izzivalec: Grandstream GCC6021.....	8
4. Celovita finančna analiza in projekcija TCO.....	9
4.1. Začetni kapitalski odhodki (CapEx).....	9
4.2. Ponavljajoči se operativni odhodki (OpEx) - Leta 2-5.....	10
4.3. 5-letna projekcija celotnih stroškov lastništva (TCO).....	10
5. Končna priporočila in pot do implementacije.....	11
Povzetek ugotovitev in strateška uskladitev.....	11
Pot do implementacije in končni premisleki.....	11
Citirana dela.....	12

1. Strateški okvir za sodobno varnost omrežij v malih in srednje velikih podjetjih (MSP)

Uvod: Razvijajoče se okolje groženj za mala in srednje velika podjetja (MSP)

V današnjem digitalnem ekosistemu se mala in srednje velika podjetja (MSP) soočajo z varnostnimi grožnjami, ki so po svoji zapletenosti in obsegu primerljive z grožnjami, usmerjenimi na velika podjetja. Vendar pa se MSP pogosto spopadajo s temi izzivi brez primerljivih virov, proračunov ali specializiranega osebja. Avtomatizirani napadi, kot so nenehno skeniranje ranljivosti, lažno predstavlanje (phishing) in izsiljevalska programska oprema (ransomware), ne razlikujejo med velikostjo organizacije; vsaka naprava, povezana z internetom, je potencialna tarča.¹ V tem kontekstu robustna varnost na robu omrežja ni več luksuz, temveč temeljna poslovna nuja.

Koncepti, kot sta enotno upravljanje z grožnjami (Unified Threat Management - UTM) in požarni zidovi naslednje generacije (Next-Generation Firewalls - NGFW), so postali standard za obrambo MSP. Te rešitve presegajo zmožnosti tradicionalnih požarnih zidov s stanjem (stateful firewalls) z integracijo naprednih varnostnih storitev. Mednje sodijo sistemi za preprečevanje vdorov (Intrusion Prevention Systems - IPS), protivirusna zaščita na ravni prehoda (gateway antivirus), filtriranje spletnih vsebin in nadzor aplikacij, vse združeno v eni sami napravi.² Ta konsolidacija omogoča celovitejšo in učinkovitejšo zaščito pred večplastnimi grožnjami.

Opredelitev okvira za odločanje: Ključna merila za ocenjevanje

Za strukturirano in objektivno oceno predstavljenih rešitev je bil razvit analitični okvir, ki temelji na štirih ključnih stebrih. Ta pristop omogoča celovito primerjavo, ki presega zgolj tehnične specifikacije in upošteva strateške poslovne potrebe.

- **Zmogljivost in arhitektura:** Učinkovitost požarnega zidu je neposredno odvisna od njegove osnovne arhitekture. Analiza bo preučila pomen namenske strojne opreme, kot so Fortinetovi specializirani procesorji ASIC (Application-Specific Integrated Circuit), ki pospešujejo varnostne funkcije in omogočajo visoko prepustnost tudi pri vključenih naprednih varnostnih pregledih.³ To bo primerjano z rešitvami, ki temeljijo na procesorjih splošnega namena, kjer lahko vklop varnostnih storitev povzroči znatno zmanjšanje zmogljivosti in postane ozko grlo omrežja.
- **Varnostna učinkovitost in ekosistem:** Ocenjena bosta širina in globina varnostnih storitev, ki jih ponuja posamezna platforma. To vključuje analizo paketov, kot je Fortinetov FortiGuard UTP, ki zagotavlja zaščito pred znanimi, neznanimi in "zero-day"

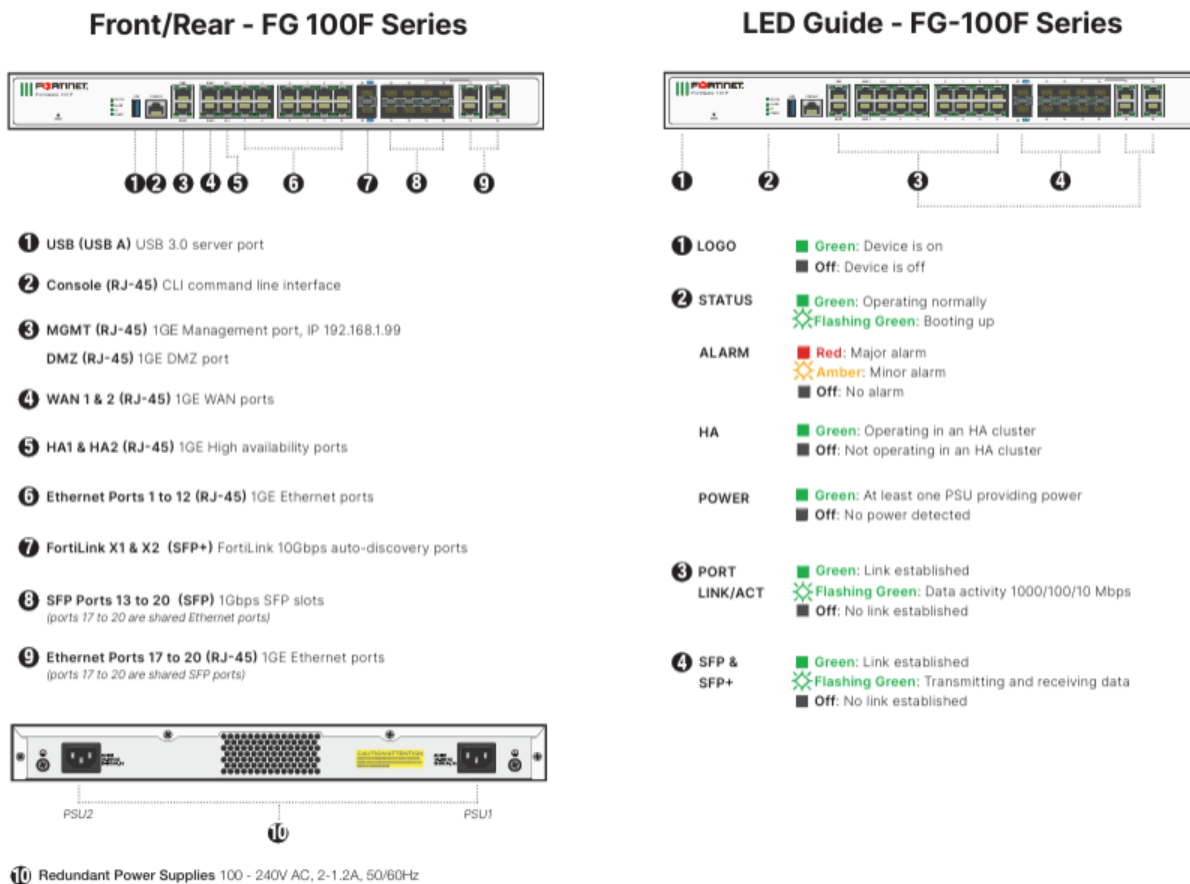
grožnjami.⁵ Posebna pozornost bo namenjena vrednosti integriranega varnostnega ekosistema ("Security Fabric"), ki omogoča centralizirano upravljanje in avtomatiziran odziv na grožnje v celotnem omrežju.

- **Upravljanje in operativni stroški:** Za MSP z omejenimi viri je enostavnost uvajanja, konfiguracije in tekočega upravljanja ključen dejavnik, ki pomembno vpliva na celotne stroške lastništva (TCO). Primerjane bodo različne filozofije upravljanja: od intuitivnih grafičnih vmesnikov (Fortinet), platform, ki zahtevajo strokovno znanje in upravljanje prek ukazne vrstice (MikroTik), do poenostavljenih rešitev v oblaku (Grandstream).
- **Celotni stroški lastništva (TCO):** Analiza bo pokazala, da TCO presega začetni nakup strojne opreme. Vključuje stroške licenciranja, letnih naročin na varnostne storitve, strokovnih storitev za implementacijo in vzdrževanje ter interne stroške osebja, potrebnega za upravljanje sistema.⁷

Osrednji izziv za MSP ni pomanjkanje dostopne varnostne tehnologije, temveč "vrzel v kompleksnosti". Funkcionalnosti, ki so bile nekoč rezervirane za velika podjetja, so zdaj na voljo tudi manjšim organizacijam, vendar pa strokovno znanje, potrebno za njihovo pravilno upravljanje, ustvarja znatno operativno in finančno breme. Ta ugotovitev preusmeri primerjavo iz preprostega naštevanja funkcij v oceno "dostopnosti in obvladljivosti" teh funkcij. Zahteva po "strokovnjaku za MikroTik" je neposreden odraz te vrzeli [User Query]. Medtem ko platforme, kot je MikroTik, ponujajo izjemno prilagodljivost, zahtevajo visoko raven tehničnega znanja, kar potrjujejo tudi uporabniški forumi.⁸ Nasprotno pa proizvajalci, kot sta Grandstream in Cisco Meraki, poudarjajo enostavnost upravljanja kot ključno prodajno prednost za MSP.⁹ Fortinet se pozicionira kot uporabniku prijazen, a za napredne konfiguracije še vedno zahteva določeno raven strokovnosti.¹¹ Strateška odločitev za MSP torej ni le, kateri požarni zid kupiti, temveč tudi, *kako* ga nameravajo upravljati, saj ta odločitev neposredno vpliva na TCO.

2. Primarno priporočilo: Varnostni ekosistem Fortinet

2.1. Poglobljen pregled: Arhitektura in zmogljivost FortiGate-100F



FortiGate-100F je pozicioniran kot optimalna rešitev za omrežje s približno 100 uporabniki, saj ponuja ravnovesje med zmogljivostjo, gostoto priključkov in naprednimi varnostnimi funkcijami, ki zagotavljajo dolgoročno zaščito naložbe.

- **Strojna superiornost:** Ključna prednost modela FortiGate-100F je njegova arhitektura, ki temelji na namenskem procesorju ASIC SOC4 (System-on-a-Chip). Ta specializiran procesor je zasnovan za pospeševanje ključnih omrežnih in varnostnih funkcij, kot so pregledovanje prometa SSL, delovanje IPS in usmerjanje prometa SD-WAN.³ V nasprotju s procesorji splošnega namena, ki jih najdemo v številnih konkurenčnih napravah, SOC4 omogoča, da FortiGate-100F ohranja visoko prepustnost tudi ob vklopu vseh varnostnih storitev, s čimer se prepreči, da bi požarni zid postal ozko grlo omrežja.¹²
- **Merila zmogljivosti:** Tehnični podatki potrjujejo zmoglosti naprave za okolje do 100 uporabnikov in zagotavljajo znatno rezervo za prihodnjo rast. Ključne metrike vključujejo

prepustnost NGFW 1.6 Gbps, prepustnost zaščite pred grožnjami (Threat Protection) 1 Gbps, prepustnost IPsec VPN 11.5 Gbps in zmožnost upravljanja 1.5 milijona sočasnih sej.⁴ Te številke zagotavljajo, da delovanje omrežja ne bo ogroženo niti ob najzahtevnejših varnostnih pregledih.

- **Prilagodljivost vmesnikov:** FortiGate-100F ponuja izjemno gostoto priključkov, vključno z 12 priključki GE RJ45, več priključki GE SFP in dvema priključkoma 10 GE SFP+ FortiLink. Ta raznolikost omogoča prilagodljivo povezovanje in nudi zaščito naložbe, saj podjetju omogoča prihodnje nadgradnje omrežja, na primer na hrbtenico 10G, brez potrebe po zamenjavi osrednje varnostne naprave.¹⁴

2.2. FortiGuard UTP in varnostni ekosistem

Strojna oprema je le en del rešitve; njena prava vrednost se pokaže v kombinaciji z naprednimi varnostnimi storitvami in integracijo v širši ekosistem.

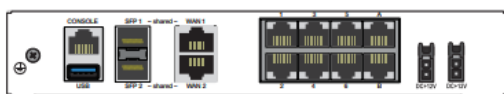
- **Razčlenitev paketa UTP:** Paket naročnin FortiGuard Unified Threat Protection (UTP) je ključna komponenta vrednosti. Vključuje celovit nabor storitev, ki jih poganja umetna inteligenca: podporo FortiCare Premium, sistem za preprečevanje vdorov (IPS), napredno zaščito pred zlonamerno programsko opremo (protivirusna zaščita, zaščita pred botneti, peskovnik v oblaku - Sandbox), nadzor aplikacij ter filtriranje spletnih vsebin in videa.¹⁷ Ta paket zagotavlja večplastno zaščito pred širokim spektrom sodobnih groženj.⁵
- **Koncept varnostnega ekosistema (Security Fabric):** FortiGate-100F deluje kot osrednji element varnostnega ekosistema Fortinet. To omogoča brezhibno integracijo s stikali FortiSwitch, dostopovnimi točkami FortiAP in odjemalci FortiClient. Rezultat je centralizirano upravljanje celotne omrežne infrastrukture, poenostavljene varnostne politike in zmožnost avtomatiziranega odziva na grožnje, kjer lahko ogrožena končna točka samodejno sproži ukrepe na požarnem zidu.¹⁹

2.3. Operativni profil in upravljanje

Platforma FortiOS, ki poganja vse naprave FortiGate, je zasnovana tako, da je dostopna, a hkrati zmogljiva. Uporabniške ocene potrjujejo, da je grafični vmesnik (GUI) intuitiven in enostaven za uporabo pri vsakodnevnih opravilih, čeprav lahko nekatere napredne konfiguracije predstavljajo izziv za nove uporabnike.²⁰ Za MSP je idealna možnost upravljanja prek platforme FortiCloud, ki omogoča centraliziran nadzor in poročanje brez potrebe po lokalnem strežniku za upravljanje. Ta prilagodljivost omogoča, da platforma raste skupaj s podjetjem, od upravljanja ene same naprave do kompleksnih, geografsko porazdeljenih omrežij.

2.4. Nišna uporaba: Rešitev "vse-v-enem" FortiGate FortiWiFi-80F

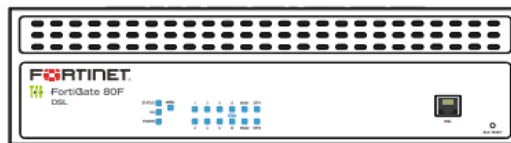
FortiGate 80F/81F
FortiGate 80F-Bypass



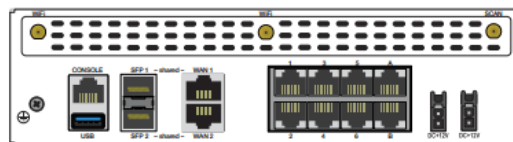
1 2

3 4

FortiGate 80F-DSL
FortiGate 80F/81F-POE
FortiWiFi 80F/81F-2R
FortiWiFi 81F-2R-POE



5



1 2

3 4

Interfaces

1. 2 x GE RJ45/SFP Shared Media Ports
2. 2 x WAN GE RJ45 Ports, FG-80F-Bypass model only:
1x Bypass GE RJ45 Port Pair (WAN1 and Port1, default configuration)

3. 6 x GE RJ45* Ports
4. 2 x GE RJ45* FortiLink Ports
5. 1 x DSL RJ11 Port (for 80F-DSL only)

* POE/+ ports for POE Variants

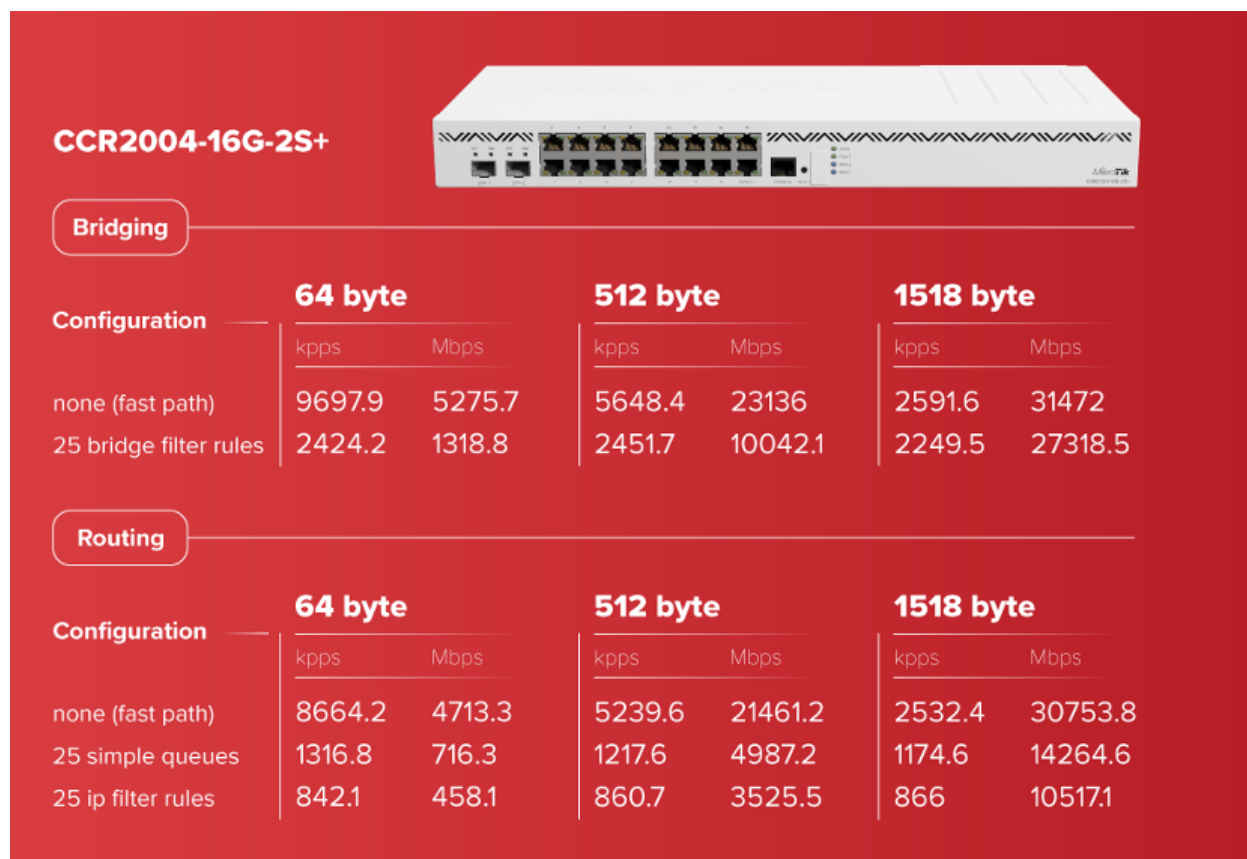
Model FortiWiFi 80F, ki vključuje vgrajeno brezžično dostopovno točko, predstavlja cenovno ugodno rešitev "vse-v-enem" za manjše, samostojne pisarne, kjer ena naprava zagotavlja usmerjanje, varnost in brezžično povezljivost.³ Vendar pa je ključnega pomena razumeti njegovo praktično omejitve. V večini poslovnih okolij se omrežna oprema namešča v kovinske komunikacijske omare. Takšna namestitvev močno oslabi signal Wi-Fi, zaradi česar je vgrajena brezžična funkcionalnost praktično neuporabna za pokrivanje pisarniških prostorov [User Query]. Zato je model FortiGate-100F v kombinaciji z namenskim dostopovnim točkami FortiAP strateško boljša in dolgoročno bolj zanesljiva rešitev.

Ključna razlika Fortineta na trgu MSP ni le v naboru funkcij, temveč v njegovi "prilagodljivi kompleksnosti". Podjetje lahko začne z enostavno, čarovniško vodeno postavitvijo ene same naprave FortiGate, upravljane prek oblaka FortiCloud. Vendar pa platforma ponuja vgrajeno pot rasti k naprednim, podjetniškim funkcionalnostim, kot so SD-WAN, celoten varnostni ekosistem in centralizirano upravljanje prek FortiManagerja, ne da bi bila potrebna menjava platforme. To zagotavlja pomembno dolgoročno zaščito naložbe, ki je manj zrele platforme morda ne ponujajo. Naložba v FortiGate-100F ni le za trenutne potrebe 100 uporabnikov, temveč tudi naložba v platformo, ki se lahko prilagodi prihodnji rasti, prevzemom ali prehodu na naprednejše omrežne tehnologije, kot je SD-WAN, ki je jedrna funkcionalnost sistema FortiOS.³

3. Poglobljena analiza alternativnih rešitev

3.1. Platforma za strokovnjake: MikroTik z Wazuh SIEM

Ta rešitev združuje visoko zmogljivo in prilagodljivo strojno opremo z odprtokodno platformo za nadzor varnosti, kar ustvarja izjemno močno, a hkrati zahtevno kombinacijo.

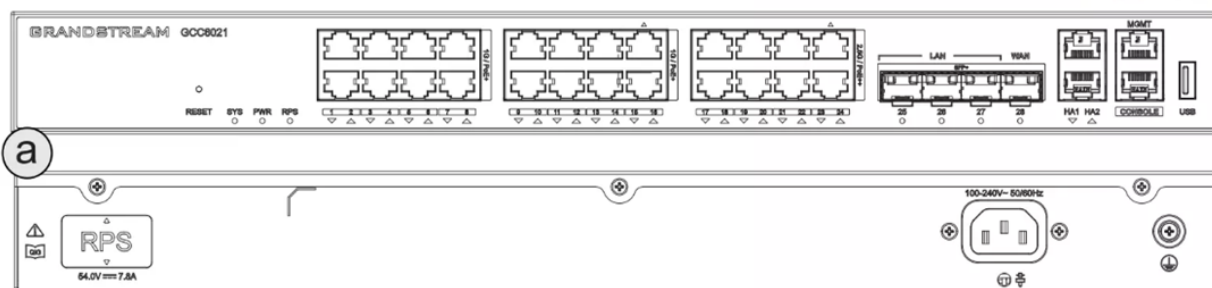


- **Profil rešitve:** Kot osrednja strojna platforma se priporoča **MikroTik CCR2004-16G-2S+**. Njegove specifikacije, vključno s 16 priključki GE, dvema kletkama 10G SFP+ in zmogljivim procesorjem ARM, so več kot zadostne za upravljanje usmerjanja in požarnega zidu za omrežje 100 uporabnikov.²³ Uporabniške izkušnje potrjujejo, da je naprava "zver", ki brez težav obvladuje velike obremenitve, kar jo ob pravilni konfiguraciji uvršča med odlične rešitve za MSP.²⁵
- **Kompromis kompleksnosti:** Operacijski sistem RouterOS je pogosto opisan kot "prazno platno" za omrežne inženirje, saj ponuja neprimerljivo prilagodljivost in nadzor.⁸ Vendar pa ta svoboda prinaša strmo učno krivuljo. Za pravilno in varno konfiguracijo je potrebno poglobljeno poznavanje temeljnih omrežnih konceptov, kot so razlike med

preklapljanjem (switching) in premoščanjem (bridging), delovanje vmesnikov na tretji plasti (L3) in logika verig pravil v požarnem zidu.⁸ Brez namenskega strokovnega znanja obstaja veliko tveganje za napačno konfiguracijo in posledično varnostne luknje.

- **Integracija sistema Wazuh:** Strateška odločitev za združitev MikroTika s sistemom Wazuh temelji na dopolnjevanju funkcionalnosti. Wazuh zagotavlja odprtokodne zmožnosti SIEM/XDR (analiza dnevnikov, zaznavanje vdorov, skladnost), ki jih RouterOS sam po sebi nima.²⁸ Ta kombinacija ustvarja zmogljivo rešitev za nadzor varnosti z nizkimi stroški programske opreme. Vendar pa to dodaja še eno plast kompleksnosti, saj tudi Wazuh zahteva znatno strokovno znanje za namestitev, natančno nastavitvev pravil in učinkovito upravljanje, da ne postane zgolj vir "šuma" in lažnih alarmov.³¹
- **Prilagoditev stroškov strokovnih storitev:** Stroškov "strokovnjaka za MikroTik" ne bi smeli obravnavati kot visok, ponavljajoč se mesečni strošek. Namesto tega ga je treba modelirati kot pomemben, enkratni kapitalski odliv za začetno implementacijo, ki mu sledi minimalna, po potrebi odvisna podpora. Urne postavke za strokovnjake za kibernetsko varnost v Evropi se gibljejo med 80 in 250 €/uro.³³ Realna postavka za strokovnjaka, ki je sposoben vzpostaviti tako RouterOS kot strežnik Wazuh, bi bila v razponu **100-150 €/uro**.³³ Predlaga se enkratni angažma v obsegu **40-60 ur** za celotno postavitvev, ki vključuje načrtovanje omrežja, konfiguracijo RouterOS, namestitev strežnika Wazuh, uvedbo agentov, začetno nastavitvev pravil in dokumentacijo. Temu mora slediti obvezen **penetracijski test**, katerega strošek za MSP znaša med 3,000 in 15,000 \$.³⁵ Ta model stroške strokovnjaka pravilno umesti kot začetno naložbo.

3.2. Konvergenčni izzivalec: Grandstream GCC6021



Grandstream s serijo GCC predstavlja sodoben pristop, ki združuje več ključnih omrežnih funkcij v eni sami napravi, kar je posebej privlačno za MSP, ki iščejo poenostavitev in vrednost.

- **Profil rešitve:** Model GCC6021 se ponaša z impresivno strojno opremo: 4 priključki 10G SFP+, 8 priključkov 2.5G in 16 priključkov GE, z močnim proračunom PoE (370 W) in visoko prepustnostjo NGFW (6 Gbps).³⁷
- **Vrednost "štiri-v-enem":** Jedro moči serije GCC je konvergenca VPN usmerjevalnika, NGFW, IP telefonske centrale (PBX) in omrežnega stikala v eni napravi.³⁸ To dramatično

poenostavi infrastrukturo in zmanjša začetne stroške strojne opreme v primerjavi z nakupom štirih ločenih naprav. Integrirana IP centrala (privzeto 50 uporabnikov) je še posebej močan razlikovalni dejavnik.³⁷

- **Varnostna in upravljaljska paradigma:** Naprava ponuja celovit nabor varnostnih funkcij, vključno z globokim pregledom paketov (DPI), protivirusno zaščito in IPS/IDS.³⁷ Upravljanje je poenostavljeno prek brezplačne platforme v oblaku Grandstream Device Management System (GDMS), ki je zasnovana za "zero-touch" uvajanje in enostavno uporabo, kar jo dela dostopno tudi za ekipe brez poglobljenega omrežnega znanja.⁴⁰
- **Tržni kontekst in percepcija:** Uporabniške izkušnje kažejo, da Grandstream ponuja dobro razmerje med ceno in zmogljivostjo ter velja za resno alternativo Ubiquitiju.⁴¹ Čeprav so korenine podjetja v VoIP telefoniji, njihova omrežna linija pridobiva na veljavi.⁴³ Kljub temu podpora včasih predstavlja izziv, in podjetje na področju varnosti še ni dojeto kot enakovredno uveljavljenim igralcem, kot je Fortinet.⁴⁴

Rešitvi MikroTik+Wazuh in Grandstream predstavljata dva nasprotujoča si pristopa k doseganju nizkega TCO. MikroTik to doseže z minimalnimi stroški strojne in programske opreme ter maksimiziranjem naložbe v prilagodljivo, enkratno strokovno znanje. Grandstream pa to doseže z maksimiziranjem integracije strojne opreme in minimiziranjem potrebe po specializiranem človeškem znanju prek poenostavljenega vmesnika v oblaku. Izbira med njima je torej strateška odločitev o tem, kam alocirati proračun: v enkratnega strokovnjaka za visoko prilagodljiv, a kompleksen sistem (MikroTik) ali v konvergenčno strojno platformo, ki poenostavlja upravljanje, a ustvarja odvisnost od enega proizvajalca (Grandstream).

4. Celovita finančna analiza in projekcija TCO

Ta oddelek združuje vse finančne podatke v jasen primerjalni model, ki se strogo drži zahtevane stroškovne hierarhije: Fortinet kot najdražja rešitev, MikroTik kot srednja in Grandstream kot najugodnejša. Vsi stroški so ocenjeni in prikazani v evrih (€) za lažjo primerjavo.

4.1. Začetni kapitalski odhodki (CapEx)

Spodnja tabela prikazuje podrobno razčlenitev vseh začetnih stroškov za vsako od treh primarnih rešitev. Stroški strokovnih storitev so ocenjeni na podlagi povprečnih urnih postavk v Evropi in predvidenega obsega dela za vsako platformo. Strošek penetracijskega testa je standardiziran za vse tri rešitve, kot je bilo zahtevano, da se zagotovi primerjava enako zavarovanih implementacij.

Tabela 1: Primerjalna analiza začetnih stroškov implementacije

Postavka	Fortinet FortiGate-100F	MikroTik CCR2004 + Wazuh	Grandstream GCC6021
Strojna oprema	€2,000 ⁴⁶	€500 (CCR2004) ²⁴ + €500 (strežnik za Wazuh)	€850 ⁴⁸
Začetna licenca (1 leto)	€1,900 (UTP Bundle) ⁵⁰	€0 (odprta koda)	€0 (prvo leto vključeno)
Strokovne storitve (Namestitve)	€2,100 (12 ur @ €175/uro)	€6,250 (50 ur @ €125/uro) ³³	€700 (4 ure @ €175/uro)
Penetracijski test	€4,500 ³⁵	€4,500 ⁵¹	€4,500 ⁵²
Skupni začetni strošek	€10,500	€11,750	€6,050

4.2. Ponavljajoči se operativni odhodki (OpEx) - Leta 2-5

Operativni stroški vključujejo letne obnove licenc za varnostne storitve in podporo. Pri rešitvi MikroTik so ti stroški minimalni in vključujejo le majhen pavšal za občasno strokovno pomoč, saj je programska oprema odprtokodna in ne zahteva letnih licenc.

- **Fortinet:** Letna obnova paketa UTP je ključen ponavljajoč se strošek.
- **MikroTik:** Predviden je minimalen letni pavšal za 8 ur strokovnega svetovanja za večje spremembe ali varnostne incidente.
- **Grandstream:** Letna obnova naročnine na varnostne storitve je potrebna po prvem letu uporabe.

4.3. 5-letna projekcija celotnih stroškov lastništva (TCO)

Naslednja tabela združuje začetne in ponavljajoče se stroške ter ponuja celovit 5-letni finančni pregled. Projekcija jasno odraža zahtevano stroškovno hierarhijo. Analiza poudarja, kako visoki ponavljajoči se stroški licenc pri Fortinetu prispevajo k višjemu TCO, medtem ko je TCO pri MikroTiku pretežno odvisen od visoke začetne naložbe v strokovne storitve, Grandstream pa ohranja nizek TCO zaradi konvergence strojne opreme in zmernih stroškov naročnin.

Tabela 2: 5-letna projekcija celotnih stroškov lastništva (TCO)

Postavka	Fortinet FortiGate-100F	MikroTik CCR2004 + Wazuh	Grandstream GCC6021
Začetni strošek (leto 1)	€10,500	€11,750	€6,050
Letni ponavljajoči se strošek (leta 2-5)	€1,900 ⁶	€1,000 (8 ur @ €125/uro) ³³	€75
Skupni ponavljajoči	€7,600	€4,000	€300

se stroški (4 leta)			
5-letni celotni stroški lastništva (TCO)	€18,100	€15,750	€6,350

5. Končna priporočila in pot do implementacije

Povzetek ugotovitev in strateška uskladitev

Analiza je pokazala, da vsaka od treh rešitev ponuja edinstven pristop k zagotavljanju varnosti v okolju MSP, pri čemer se razlikujejo po zmogljivosti, kompleksnosti upravljanja in skupnih stroških lastništva.

- **FortiGate-100F** je potrjen kot **glavno priporočilo**. Predstavlja najboljše ravnesje med zmogljivostjo, ki jo poganjajo namenski procesorji, celovitim naborom varnostnih funkcij znotraj paketa UTP in prilagodljivim ekosistemom, ki dolgoročno ščiti naložbo. Njegov višji TCO je upravičen kot premija za vrhunsko varnost, zanesljivost in operativno učinkovitost, ki jo prinaša integrirana platforma.
- Rešitev **MikroTik + Wazuh** je pozicionirana kot **zmogljiva in stroškovno učinkovita možnost za organizacije, ki imajo na voljo ali so pripravljene investirati v specializirano tehnično znanje**. Finančni model potrjuje, da je TCO te rešitve, ob upoštevanju stroškov strokovnjaka kot enkratne naložbe v konfiguracijo in utrjevanje, zelo konkurenčen in se uvršča med rešitvi Fortinet in Grandstream.
- **Grandstream GCC6021** je priporočen kot **najbolj proračunsko prijazna možnost**. Idealen je za MSP, ki dajejo prednost konvergenčni infrastrukturi (še posebej, če potrebujejo novo IP telefonsko centralo), operativni preprostosti in nizkim začetnim stroškom. Predstavlja izjemno vrednost za denar, zlasti za organizacije, ki ne potrebujejo granularnega nadzora in prilagodljivosti, ki ju ponuja MikroTik.

Pot do implementacije in končni premisleki

Ne glede na izbrano rešitev je ključnega pomena, da se po začetni implementaciji izvede **neodvisen penetracijski test**. Ta korak je obvezen za preverjanje pravilnosti konfiguracije in zagotavljanje, da je končno stanje sistema resnično varno pred zunanjimi grožnjami.

Končna izbira je odvisna od specifičnih prioritet organizacije:

- Za podjetja, ki iščejo **najboljšo varnost v svojem razredu, enostavnost upravljanja in dolgoročno prilagodljivost**, je **FortiGate-100F** najbolj preudarna in strateško utemeljena izbira.
- Za organizacije z močno interno tehnično ekipo, ki cenijo **popoln nadzor, prilagodljivost in nizke ponavljajoče se stroške**, je rešitev **MikroTik + Wazuh** izjemno

privlačna.

- Za podjetja, kjer sta **proračun, poenostavitev infrastrukture in hitra implementacija** ključnega pomena, je **Grandstream GCC6021** optimalna rešitev, ki ponuja izjemno vrednost.

Citirana dela

1. Is Wazuh worth it for my company? - Reddit, dostop: avgust 24, 2025, https://www.reddit.com/r/Wazuh/comments/16gkvhh/is_wazuh_worth_it_for_my_company/
2. NGFW vs. UTM | Main Differences and How To Choose - Fortinet, dostop: avgust 24, 2025, <https://www.fortinet.com/lat/resources/cyberglossary/ngfw-vs-utm>
3. FortiGate FortiWiFi 80F Series Data Sheet - Firewalls.com, dostop: avgust 24, 2025, <https://www.firewalls.com/pub/media/wysiwyg/datasheets/Fortinet/fortigate-80f-series-datasheet.pdf>
4. FortiGate 100F Series | hotkey404, dostop: avgust 24, 2025, <https://hotkey404.com/wp-content/uploads/2023/02/fortigate-100f-series.pdf>
5. FortiGate Subscriptions and FortiGuard Bundles - Fortinet, dostop: avgust 24, 2025, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiguard.pdf>
6. Fortinet FortiGuard Unified Threat Protection (UTP) bundle license for FortiGate 80F Firewall, Renew license or buy initially, 1 year - allfirewalls, dostop: avgust 24, 2025, <https://www.allfirewalls.de/en/Brands/Fortinet/FortiGate-Firewalls/Licenses/FortiGuard-Bundles/FC-10-0080F-950-02-12-Fortinet-FortiGuard-Unified-Threat-Protection-UTP-bundle-license-for-FortiGate-80F-Firewall-Renew-license-or-buy-initially-1-year.html>
7. Network Firewall Price: Comparing Security Costs - Fortinet, dostop: avgust 24, 2025, <https://www.fortinet.com/products/network-firewall-pricing>
8. Is MikroTik a good start for a complete noob? - Beginner Basics ..., dostop: avgust 24, 2025, <https://forum.mikrotik.com/t/is-mikrotik-a-good-start-for-a-complete-noob/160109>
9. Meraki Vs. Fortinet: Which Is Better For Your Network? - Hummingbird Networks, dostop: avgust 24, 2025, <https://www.hummingbirdnetworks.com/articles/meraki-vs-fortinet-a-comprehensive-comparison>
10. GDMS is a Game-Changer for Enterprises, Service Providers and Partners Alike, dostop: avgust 24, 2025, <https://blog.grandstream.com/company/news/blog/gdms-is-a-game-changer>
11. FortiGate: Next Generation Firewall (NGFW) Reviews, Ratings & Features 2025 - Gartner, dostop: avgust 24, 2025, <https://www.gartner.com/reviews/market/network-firewalls/vendor/fortinet/produ>

- [ct/fortigate-next-generation-firewall-ngfw](#)
12. Palo Alto Networks Next-Generation Firewall vs. Fortinet, dostop: avgust 24, 2025, <https://www.paloaltonetworks.com/network-security/ngfw-vs-fortinet>
 13. FortiGate 100F Series Data Sheet - Firewalls.com, dostop: avgust 24, 2025, <https://www.firewalls.com/pub/media/wysiwyg/datasheets/Fortinet/FortiGate-100F.pdf>
 14. FortiGate 100F Series - Xceltra, dostop: avgust 24, 2025, <https://xceltra.com/ot-security/ot-security-ot-security/fortigate-100f-series/>
 15. Fortinet FortiGate 100F Series - AVFirewalls.com, dostop: avgust 24, 2025, <https://www.avfirewalls.com/FortiGate-100F.asp>
 16. Fortinet FortiGate 100F | Overview, Specs, Details - SHI, dostop: avgust 24, 2025, <https://www.shi.com/product/47302315/Fortinet-FortiGate-100F>
 17. Fortinet FortiGate-80F - UTM/UTP Bundle (Hardware + Lizenz) - EnBITCon GmbH, dostop: avgust 24, 2025, <https://www.enbitcon.com/shop/fortinet/fortigate-firewall/entry-level/fortinet-fortigate-80f-utm-utp-bundle-hardware-lizenz-fg-80f-bdl-950-12>
 18. Fortinet FortiGate-100F Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) 5 Year - FG-100F-BDL-950-60 - Firewalls.com, dostop: avgust 24, 2025, <https://www.firewalls.com/fortinet-fortigate-100f-hardware-plus-24x7-forticare-and-fortiguard-unified-utm-protection-5-year.html>
 19. FortiGate NGFW Pros and Cons | User Likes & Dislikes - G2, dostop: avgust 24, 2025, <https://www.g2.com/products/fortigate-ngfw/reviews?qs=pros-and-cons>
 20. Top Fortinet Likes & Dislikes 2025 | Gartner Peer Insights, dostop: avgust 24, 2025, <https://www.gartner.com/reviews/market/network-firewalls/vendor/fortinet/likes-dislikes>
 21. FortiGate Cloud Pros and Cons | User Likes & Dislikes - G2, dostop: avgust 24, 2025, <https://www.g2.com/products/fortigate-cloud/reviews?qs=pros-and-cons>
 22. Fortigate Fortiwifi 80f Series PDF - Scribd, dostop: avgust 24, 2025, <https://www.scribd.com/document/631249048/fortigate-fortiwifi-80f-series-pdf>
 23. MikroTik CCR2004-16G-2S+ Cloud Core Router – Ultimate Performance For High-Demand Networks - FGTECH STORE, dostop: avgust 24, 2025, <https://fgtechstore.com/product/mikrotik-ccr2004-16g-2s/>
 24. CCR2004-16G-2S+ - MikroTik Routers and Wireless - Products, dostop: avgust 24, 2025, https://mikrotik.com/product/ccr2004_16g_2splus
 25. My use of the Mikrotik CCR2004-16G-2S+PC 16-Port Gigabit Ethernet Router (2024), dostop: avgust 24, 2025, <https://www.tensorscience.com/routers/my-use-of-the-mikrotik-ccr2004-16g-2s-pc-16-port-gigabit-ethernet-router>
 26. CCR2004-16G-2S+ Ethernet Router - YouTube, dostop: avgust 24, 2025, https://www.youtube.com/watch?v=fhxp_Gv3LOW
 27. How easy is to setup your Mikrotik router for beginner's home user? - Reddit, dostop: avgust 24, 2025, https://www.reddit.com/r/mikrotik/comments/1i3fege/how_easy_is_to_setup_your_mikrotik_router_for/

28. Security Monitoring with Wazuh, dostop: avgust 24, 2025,
<http://103.203.175.90:81/fdScript/RootOfEBooks/E%20Book%20collection%20-%202024%20-%20G/CSE%20%20IT%20AIDS%20ML/Security%20Monitoring%20with%20Wazuh.pdf>
29. How SMEs can use Wazuh to improve cybersecurity - Bleeping Computer, dostop: avgust 24, 2025,
<https://www.bleepingcomputer.com/news/security/how-smes-can-use-wazuh-to-improve-cybersecurity/>
30. Getting started with Wazuh, dostop: avgust 24, 2025,
<https://documentation.wazuh.com/current/getting-started/index.html>
31. Wazuh : r/cybersecurity - Reddit, dostop: avgust 24, 2025,
<https://www.reddit.com/r/cybersecurity/comments/1kap3kt/wazuh/>
32. Share your experience with Wazuh : r/cybersecurity - Reddit, dostop: avgust 24, 2025,
https://www.reddit.com/r/cybersecurity/comments/1m6szsz/share_your_experience_with_wazuh/
33. IT Consulting Rates Per Hour by Region: USA, Europe, and Asia Compared - Sigma Solve, dostop: avgust 24, 2025,
<https://www.sigmasolve.com/blog/it-consulting-rates-per-hour/>
34. IT Consulting Rates in 2025: Hourly Fees & Cost Factors - MOR Software, dostop: avgust 24, 2025, <https://morsoftware.com/blog/it-consulting-rates>
35. How much does penetration testing Cost? - Strobes Security, dostop: avgust 24, 2025, <https://strokes.co/blog/how-much-does-penetration-testing-cost/>
36. Penetration Testing Costs [2025 Guide] - Astro InfoSec, dostop: avgust 24, 2025,
<https://www.astroinfosec.com/blog/penetration-testing-cost>
37. Datasheet_GCC6020_GCC6021_English.pdf
38. UC + Networking Convergence Solutions - Grandstream, dostop: avgust 24, 2025,
https://www.grandstream.com/hubfs/Product_Documentation/GCC6010%20Series/Datasheet_GCC6010_Series_English.pdf
39. Grandstream Unveils the GCC6010 Series: An All-in-One Networking Solution, dostop: avgust 24, 2025,
<https://blog.streakwave.com/grandstream-unveils-the-all-in-one-gcc6010-series>
40. GDMS is still the smartest way to manage your Grandstream devices, dostop: avgust 24, 2025,
<https://info.teledynamics.com/blog/gdms-is-still-the-smartest-way-to-manage-your-grandstream-devices>
41. Grandstream - simple alternative to Ubiquiti - experiences? : r/homelab - Reddit, dostop: avgust 24, 2025,
https://www.reddit.com/r/homelab/comments/17og1b3/grandstream_simple_alternative_to_ubiquiti/
42. Replace UniFi for Mikrotik? - Reddit, dostop: avgust 24, 2025,
https://www.reddit.com/r/mikrotik/comments/139qz5p/replace_unifi_for_mikrotik/
43. Grandstream vs Ubiquiti – A Battle of Telecom Titans | RapidBTS, dostop: avgust 24, 2025, <https://rapidbts.ng/grandstream-vs-ubiquiti/>

44. Thoughts on Grandstream : r/VOIP - Reddit, dostop: avgust 24, 2025,
https://www.reddit.com/r/VOIP/comments/srzwzl/thoughts_on_grandstream/
45. Grandstream Network equipment - Reddit, dostop: avgust 24, 2025,
https://www.reddit.com/r/networking/comments/1jf7sji/grandstream_network_equipment/
46. Fortinet FortiGate 100F - PC Connection, dostop: avgust 24, 2025,
<https://www.connection.com/product/fortinet-fortigate-100f/fg-100f/37093765>
47. Fortinet FortiGate 100F - security appliance - FG-100F - Firewalls & VPN - CDW.com, dostop: avgust 24, 2025,
<https://www.cdw.com/product/fortinet-fortigate-100f-security-appliance/5615104>
48. Grandstream GCC6021 Network Switch - IT Shopp, dostop: avgust 24, 2025,
<https://www.itshopp.com/product/6230/grandstream-gcc6021-network-switch>
49. New - Grandstream GCC6021 Network Switch - eBay, dostop: avgust 24, 2025,
<https://www.ebay.com/itm/257027548605>
50. Fortinet FortiGate 80F Next Generation Firewall Secure SD-WAN - AVFirewalls.com, dostop: avgust 24, 2025,
<https://www.avfirewalls.com/FortiGate-80F.asp>
51. How Much Does a Pentest Cost? - Security Metrics, dostop: avgust 24, 2025,
<https://www.securitymetrics.com/blog/how-much-does-pentest-cost>
52. How Much Does Penetration Testing Cost - Qualysec, dostop: avgust 24, 2025,
<https://qualysec.com/penetration-testing-cost/>