Na prednjoj strani uređaja samo je nužna signalizacija napajanja, statusa uređaja te informacija o zauzetim *portovima* i brzini na kojoj rade

Mali, ali tehničar!

FortiGate 40F objedinjuje funkciju NG vatrozida, sigurne virtualne privatne mreže te antivirusne zaštite, na mjestima gdje to već ranije nije bilo implementirano. Tu je i SD-WAN funkcionalnost, stoga imamo rješenje za visoku sigurnost izdvojenih lokacija, lako upravljivo iz zajedničkog web-sučelja

Rajko Plečko

Fortinet je američka multinacionalna kompanija sa sjedištem u Sunnyvaleu u Kaliforniji. Nastala je prije 20 godina kad su braća Ken i Michael Xie napustili i rasprodali prethodne uspješne kompanije i odlučili se baviti mrežnom sigurnošću na svim razinama, od lokalnih mreža do Interneta. Oko misije i vizije nove kompanije, na svu sreću, nisu bili neodlučni kao oko imena koje je pri osnivanju glasilo Appligation Inc., pa je vrlo brzo promijenjeno u ApSecure te nakon kratkog vremena konačno u Fortinet, što bi povezivanjem riječi "fortified" i "networks" trebalo dati naslutiti njeno područje interesa. Prvi proizvod koji su ponudili korisnicima bio je *firewall* FortiGate, daleki predak uređaja koji testiramo.

FortiGate 40F dolazi u varijanti s Wi-Fijem i bez njega, u kućištu koje bismo mogli nazvati stolnim (iako ima mogućnost montaže na zid). Namijenjen je, osobito u varijanti s Wi-Fijem, manjem prostoru i manjem broju korisnika, gdje neće biti ugrađen u komunikacijski ormar (premda je i to opcija). Činjenica da se radi o uređaju *desktop* kategorije ne bi trebala obeshrabriti potencijalne kupce, jer će, zahvaljujući snažnom SoC-u, FortiGate 40F sve zadaće odraditi bolje od deklariranog.

OSNOVNE KARAKTERISTIKE

FortiGate 40F, iako "malen rastom", pruža sveobuhvatno rješenje kakva inače uglavnom susrećemo na većim i skupljim uređajima. Tu su najvažniji NGFW (Next Generation Firewall), SD-WAN te VPN i antivirusna zaštita.

Vatrozidovi nove generacije filtriraju mrežni promet kako bi zaštitili organizaciju od vanjskih prijetnji. Uz standardne značajke zaštitnih zidova, poput filtriranja paketa, nadzora mreže i regulacije mrežnog prometa statičnim pravilima, NGFW također posjeduju mogućnosti dublje inspekcije, koje im pružaju izvrsnu sposobnost prepoznavanja napada, zlonamjernog softvera i drugih prijetnji. Vatrozidovi sljedeće generacije pružaju organizacijama mogućnost kontrole aplikacija te detekciju i prevenciju provale zlonamjernog softvera ili osoba na lokalnu, odnosno štićenu mrežu. Kako se profil prijetnji i zlonamjernih akcija razvija zapanjujućom brzinom, tradicionalni vatrozidovi zaostaju i dovode u opasnost organizacije koje se na njih oslanjaju. NGFW se prije svega oslanja na "zajedničko znanje" sakupljeno u AI sustavima u FortiGuard Labsu, koje je dostupno pretplatnicima na određenu uslugu ili servis, kako bi im pružio proaktivnu zaštitu, uz inspekciju nekriptiranog i kriptiranog prometa, i tako im omogućio da ostanu u utrci s najnovijim prijetnjama.

Kako se primjena poslovno kritičnih aplikacija i alata baziranih u *cloudu* i dalje povećava, distribuirane organizacije s više udaljenih ureda prelaze iz širokopojasnih mreža (WAN-ovi) s prosječnim performansama na SD-WAN. SD-WAN je softverski definirana WAN mrežna arhitektura koja omogućuje digitalne inovacije. SD-WAN rješenja transformiraju sposobnosti organizacije korištenjem korporativnog WAN-a i *multi-cloud* povezivanja za postizanje boljih performansi aplikacije na WAN Edgeu u dislociranim uredima. SD-WAN pruža dinamički izbor putanja između MPLS, 4G/5G ili širokopojasne mreže te prioritizaciju prometa, osiguravajući organizacijama da brzo i lako pristupe kritičnim poslovnim aplikacijama u *cloudu*. No SD-WAN rješenje samo za sebe ne pruža ugrađenu sigurnost, što je

Fortinet FortiGate 40F

Sučelja	**1x GbE WAN/DMZ *port*, 1x GbE FortiLink *port*, 1x GbE interni *port*, 1x USB, 1x konzola (RJ45)**
Wi-Fi	**802.11a/b/g/n/ac**
Propusnost	**IPS 1 Gbps, NGFW 800 Mbps, Threat Protection 600 Mbps, IPsec VPN 4,4 Gbps, SSL VPN 490 Mbps, SSL Inspection Throughput 310 Mbps**
Dimenzije (VxŠxD)	**38 x 216 x 160 mm**
Jamstvo	**1 godina**

+ Napredne funkcionalnosti sagrađene na snažnom i modernom SoC-u, klasičan dizajn ravnih linija

– Relativno beznačajno, ali – razočaravajući izbor konektora za napajanje, što nepotrebno otežava zamjenu u slučaju kvara

Dojam Uređaj visokih performansi, namijenjen manjim i srednje velikim tvrtkama (prema našim mjerilima)

Ustupio Veracomp, www.veracompadria.com, tel. 01/5535-465, fortinet@veracompadria.com

CIJENE

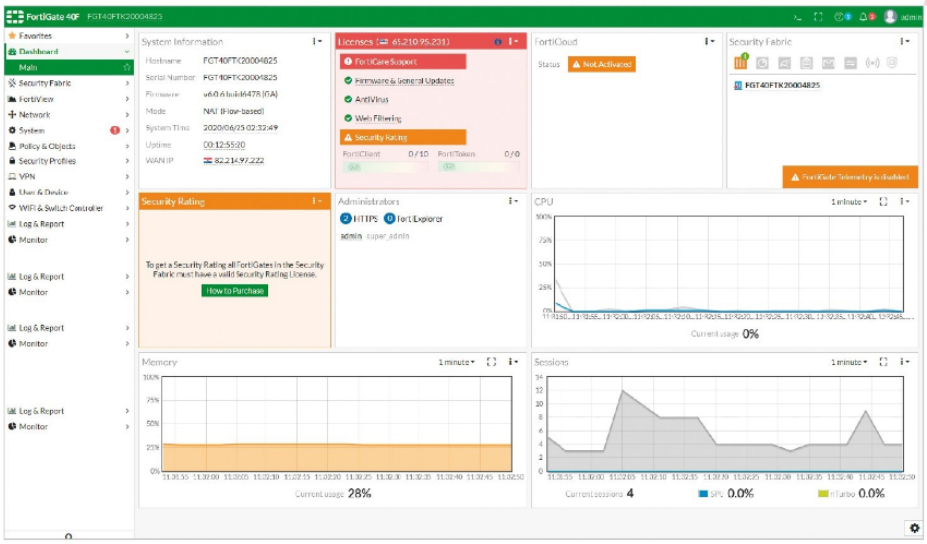
FortiGate 40F + 1 godina 24x7 podrške: 594 eura + PDV

FortiGate 40F + Advanced Threat Protection (Advanced Malware Protection, IPS i 1 godina 24x7 podrške): 718 eura + PDV

FortiGate 40F + Unified Threat Protection (Advanced Threat Protection, Web Filtering, Anti-Spam i 1 godina 24x7 podrške): 817 eura + PDV

kritično za izravan pristup Internetu. Monitoring i sigurnosna provjera mrežnog prometa na izdvojenim lokacijama postaju nevidljivi alatima na centralnoj lokaciji, pa se otvara prostor za razne *shadow IT* aplikacije koje mogu ugroziti sigurnost mreže, a bez kontrole mrežnog prometa, ugrožen je i kapacitet pristupnog *linka* prema Internetu, koji može biti zagušen YouTubeom, Netflixom i raznim drugim servisima, koji mogu vrlo brzo potrošiti ograničeni kapacitet *linka*.

Fortinet je na taj izazov odgovorio dodavanjem SD-WAN funkcionalnosti na spomenutu NGFW platformu, koja pokriva različite tipove korisnika – od malih SMB-a do velikih *enterprisea* te je upravo spajanjem tih tehnologija u jedan paket riješio problem sigurnosti na izdvojenim lokacijama. One imaju visoku razinu sigurnosti uz FortiGate NGFW te brz i lako dostupan pristup mreži, a sve to u jednom uređaju te uz upravljanje iz jednog sučelja.



Dashboard **web-sučelja s osnovnim informacijama za nadzor stanja**

INSTALACIJA I KORIŠTENJE

Uređaj se nakon priključenja na izvor napajanja i mrežu vidi na preddefiniranoj adresi i može se konfigurirati kroz web-sučelje, SSH (naredbeni redak – CLI) ili priključenim terminalom na serijskom *portu* (RJ45 sa zadnje strane uređaja), također u naredbenom retku. Za prve dvije varijante morat ćete podesiti odgovarajuću adresu na računalu s kojeg pristupate, ali je zato treća više nego jednostavna. S USB-*to*-*serial* adapterom, adapterom s DB9 na RJ45, konzolnim kabelom i *defaultnim* postavkama svima poznatog Puttyja (9600,N,8,1) do naredbenog retka došli smo za manje od minute. Jedini je problem u tome što s CLI naredbama vjerojatno niste upoznati, jer radi se o specifičnom OS-u (FortiOS) pa ćete se vjerojatno odlučiti za najkomforniju varijantu: pristup kroz web-sučelje.

Korisničkim imenom "admin" i bez inicijalne lozinke (lijepo od proizvođača što vam je uštedio nekoliko minuta kopanja i traženja po dokumentaciji), na što će vas uređaj odmah upozoriti, dolazimo do nadzornog panela (*dashboard*) s pregledom osnovnih informacija o stanju sustava, aktivnim licencama, opterećenjem CPU-a i memorije, broju aktivnih sesija te "Security Ratingom" vašeg uređaja. Koristan alat koji vas informira koliko ste dobro konfigurirali svoj FortiGate u "Security Fabric" kartici detaljno opisuje i sugerira vam kako to poboljšati.

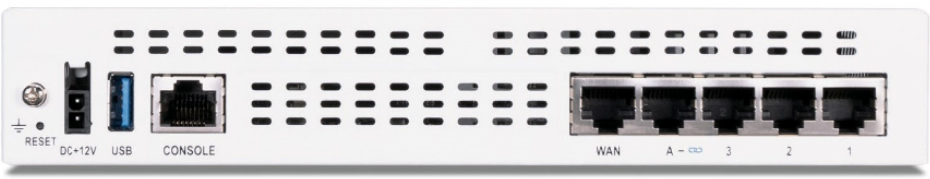
Dalje od te točke nastupa pažljivo otvaranje jednog od desetak menija, s barem još toliko ispod svakog od njih, i fino podešavanje filtera kako bismo se što više približili optimalnoj konfiguraciji. To podrazumijeva set politika koje neće previše braniti pristup stranicama koje ne predstavljaju opasnost, ili dodatno opterećenje za mrežnu infrastrukturu, ali će istodobno onemogućiti nepoželjne sadržaje, sumnjive lokacije, koje bi potencijalno mogle ugroziti sigurnost organizacije te svakako viruse i sličan maliciozni softver.

Ovdje također možemo definirati i postavke pristupa u virtualnu privatnu mrežu (VPN) oslonjenog na IPsec (200 *gateway to gateway* tunela; 250 *client to gateway* tunela) i SSL (200 VPN korisnika).

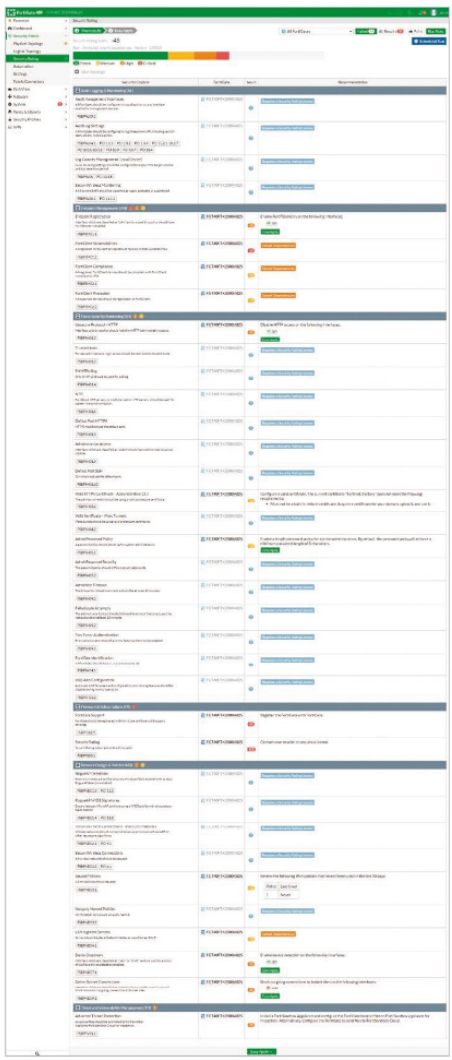
Moguće je i kreiranje SSL-VPN portala, koji će pristup pojedinim aplikacijama unutar organizacije pružiti i korisnicima bez unaprijed definiranog i podešenog klijentskog softvera, što će znati cijeniti administratori koji su se napatili sa sličnim poslom od početka pandemija, koja je tisuće ljudi natjerala na rad od kuće.

Kad jedno kreiramo sve potrebne politike i sigurnosne profile, jednostavno ćemo ih primijeniti na uređaje u mreži, i tako vrlo fino granulirati "prava i obaveze" svakog pojedinog korisnika, odnosno računala, pa nam preostaje samo redovito praćenje zapisa i izvješća kako bismo pravodobno uočili eventualni propust koji smo napravili.

Očito je da nije moguće pobrojati sve mogućnosti i podesive parametre ovog uređaja, ali to ionako nije cilj. Ako ste u opisu glavnih značajki i funkcionalnosti FortiGatea 40F prepoznali neku koja bi mogla unaprijediti sigurnost vaše organizacije, preporučujemo vam da svakako uzmete u razmatranje ovog "malog diva" i njegove mogućnosti, čija popularnost počiva na dobrim iskustvima široke korisničke baze.



Straga su svi priključci pet mrežnih, serijska konzola te USB i napajanje



Security Rating nepodešenog uređaja s mnogo prijedloga i mogućih poboljšanja