Neprobojni zid

Iako je najmanji član obitelji SuperMassive 9000, *firewall* 9200 impresionira sirovim performansama i pukim brojem mogućnosti

Dell Networks SonicWall SuperMassive 9200

Kućište	**1U *rackmount***
Memorija	**32 GB**
Sučelja	**8x *copper* GbE, 8x SFP Gigabit, 4x SFP+, 10x GbE**
Ostali konektori	**2x USB, RJ45 konzola**
Napajanje	**2x 300 W *hot-plug***
Upravljanje	**Web *browser***

+ Brzo puštanje u rad, vrhunske performanse, *zone-based* sigurnost, napredne kontrole

− Visoka cijena, dodatno plaćanje *reportinga*, buka u radu

Dojam: Iako vrlo skup uređaj, SuperMassive 9200 pruža iznimnu sigurnost uz vrhunske performanse. Implementacija je vrlo brza i relativno jednostavna, a fokus na aplikacijske kontrole čini ga svestranijim od konkurencije

Cijena **250.369 kn** + licence*

155.228 kn godišnje

* Licence uključuju CaptureATP (sandboxing), Gateway Anti-Virus, Gateway Anti-Spyware, Application Control, Visulization and Intelligence, Intrusion Prevention System, Content Filtering Premium i 24x7 support

Ustupio Callidus grupa, www.callidus.hr, tel. 01/5590-500

Rajko Plečko

Prije nego što proučimo kako nam SonicWALL SuperMassive 9200 može pomoći, spomenimo nekoliko riječi o tvrtki koja je za njega zaslužna. SonicWall su 1991. godine, u San Joseu u Kaliforniji, pokrenula braća Sreekanth i Sudhakar Ravi, da bi se posvetili razvoju i proizvodnji sveobuhvatnih sigurnosnih rješenja za mrežnu zaštitu te siguran udaljeni pristup, i to za kompanije svih veličina. Kompanija je, najprije pod imenom Sonic System, počela s proizvodnjom Ethernet adaptera za računala Macintosh. Kasnije su se razgranali u softver za menadžment, razvoj *embedded* sustava i druge, a nakon tridesetak predstavljenih proizvoda i tehnologija prepoznali su tržišnu potrebu za sigurnosnim uređajima za male i srednje kompanije. Vrlo brzo svoj su fokus preselili na ovo novo tržište te uskoro predstavili prvi sigurnosni uređaj (*security appliance*) SonicWALL.

Zahvaljujući dobro izabranoj tržišnoj niši i kvalitetnom proizvodu, prepoznatom od velikog broja korisnika, SonicWALL je ostao "u plusu" kad govorimo o zaradi i tržišnom udjelu, čak i u posljednjih nekoliko godina, kad je cijela Silicijska dolina doživjela oscilacije i padove.

2011. godine, u sklopu akcije *rebrandinga* svojih mrežnih proizvoda, Dell je preuzeo tvrtku Force10 Networks, koja je uglavnom proizvodila *high-end* mrežnu opremu namijenjenu *data* centrima te se pozicionirala na tržištu mrežne opreme klase *enterprise*. Do tada su mrežni preklopnici, koji su se prodavali pod Dellovim brendom PowerConnect, bili proizvodi Broadcoma, Marvel Technologies grupe, Brocadea ili Junipera. Akvizicijom kompanija Force10 Networks i SonicWALL, te njihovog intelektualnog vlasništva i tehnologije, Dell se najprije riješio Brocadea i Junipera, a do 2013. godine i ostalih partnera. Tada je počeo proces konačne integracije na zajedničkom "Dell Networking OS-u" i finalnog *rebrandinga* u Dell Networking.

Redundantna napajanja i ventilatori lako se mogu promijeniti u slučaju kvara

Iako je SuperMassive 9200 najmanji član obitelji SM9000, mogućnosti su mu iznimne

MLAĐI BRAT VELIKIH MOGUĆNOSTI

Dellova serija uređaja SuperMasive dijeli se na seriju E10000 i 9000. U prvoj su dva modela, E10800 i E10400, a u drugoj četiri, i to SM9800, SM9600, SM9400, te uređaj koji smo testirali i kojim ćemo se baviti u ovom članku, SM9200. Neka vas ne zavara činjenica da se radi o uređaju s početka ljestvice, jer to što je najslabiji u obitelji nikako ne opisuje njegove apsolutne mogućnosti i kvalitetu.

Obitelj uređaja SuperMassive 9000 popunila je prazninu između najviše klase SM10000 i slabije NSA klase uređaja, tako što pružaju iste funkcionalnosti kao i "starija braća", ali u moćnom kompaktnom paketu.

Za testirani SonicWALL SuperMassive SM9200 proizvođač tvrdi da je u stanju provjeriti i propustiti 15 Gbit/s podataka, što je višestruko brže nego što nude uređaji iz niže NSA klase, čija se propusnost kreće od 750 Mbit/s za NSA 250, do 12 Gbit/s za NSA 6600. Kad govorimo o testiranju ovakvog uređaja, jasno je da ga je u našim uvjetima gotovo nemoguće podvrgnuti maksimalnim opterećenjima, jer bi to zahtijevalo testno okruženje skuplje od samog uređaja (koji nije jeftin) pa ćemo se ograničiti na podatke koje daje proizvođač i dojmove koje ostavlja grafički *interface*, odnosno na lakoću korištenja.

Next Generation Firewallovi (NGFW), u koje se SM9200 s ponosom ubraja, predstavljaju integriranu mrežnu platformu koja kombinira tradicionalne funkcionalnosti *firewalla* – primjerice, *packet filtering*, *network* i *port* translaciju adresa (NAT i PAT), *statefull packet* inspekciju te virtualne privatne mreže (VPN) – s novim i naprednim, kao što su aplikacijski *firewall*, *deep packet inspection* (DPI) te *intrusion prevention* sustavi (IPS).

Prva generacija *firewallova* (*stateless inspection*) bavila se svakim paketom posebno, provjeravajući samo zaglavlja paketa, i nije bila posebno učinkovita u svojem poslu. Druga generacija (*statefull inspection*) znala je pratiti statuse i karakteristike mrežnih konekcija te na temelju toga donijeti odluku o sudbini paketa. NGFW spada u treću generaciju, koja je otišla korak dalje i bavi se sadržajem svakog pojedinačnog paketa, uspoređujući ga s poznatim zloćudnim uzorcima kao što su virusi ili *malware*.

SM9200 izgrađen je na procesoru Octeon MIPS64 sa 24 jezgre takta 1 GHz, koji prati 8 GB memorije. *Smart* funkcije uređaja uključuju mogućnost dinamičkog dodavanja procesorskih jezgri kad se za to steknu uvjeti, odnosno kad poraste opterećenje uređaja.

Hardverska redundancija uključuje dva bloka za napajanje i module ventilatora dostupne i zamjenjive izvana. Ventilatori su vrlo bučni, što je za očekivati od uređaja visine 1U, ali kako mu mjesto gotovo sigurno biti u nekom ormaru u ionako bučnoj serverskoj sobi, to i nije osobit problem.

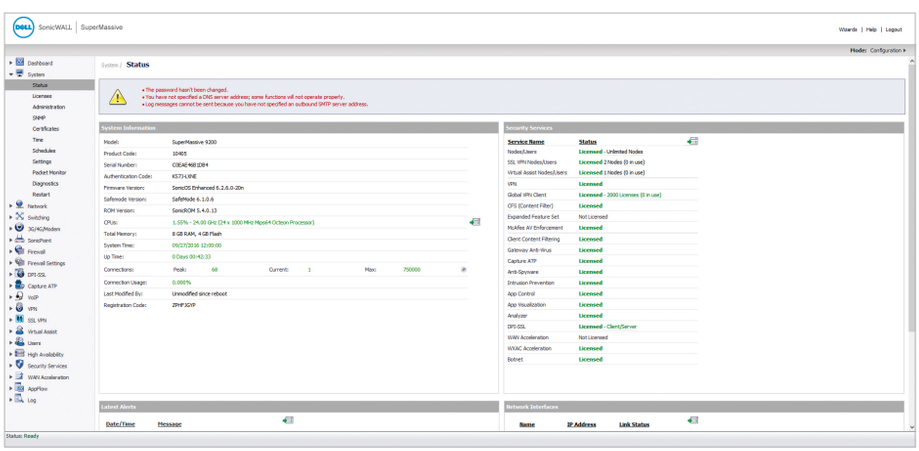
PREGRŠT FUNKCIJA

Na prednjoj strani oku ugodnog 1U kućišta nalazi se mali LCD s tipkama za navigaciju, RJ45 serijski *port* za spajanje konzole, dva USB *porta* namijenjena spajanju modema (3G/4G/analogni), nekoliko LED-ica koje daju osnovne informacije o stanju uređaja ili alarmiraju ako je u pitanju kvar, te mrežni priključci. Na raspolaganju je osam gigabitnih "bakrenih" RJ45 priključaka, osam priključnih mjesta za gigabitne SFP-ove (optičke ili bakrene) te četiri mjesta za 10-gigabitne SFP+ module.

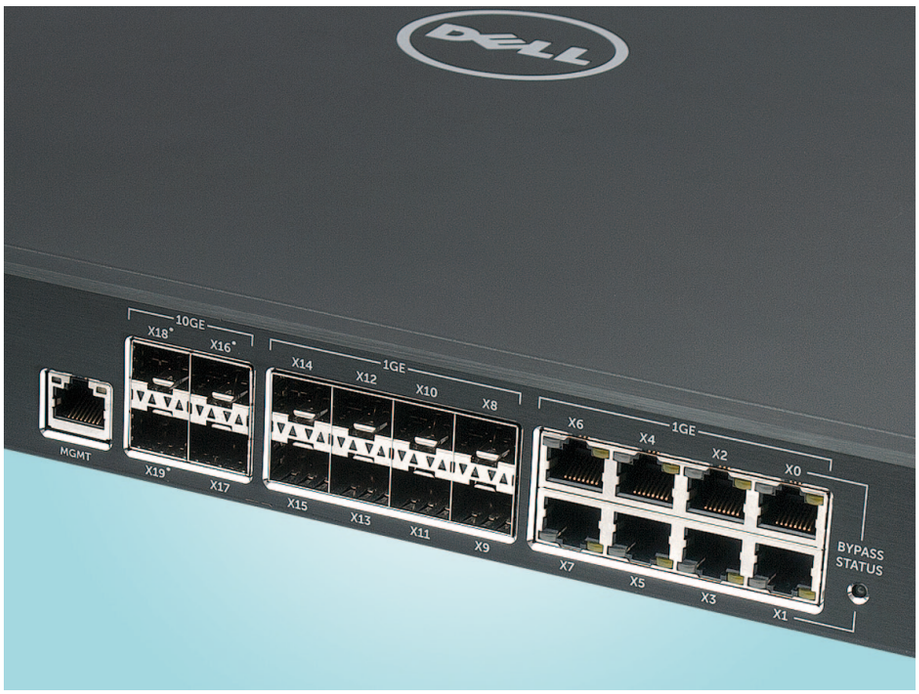
Sa stražnje strane nalaze se dva izmjenjiva i kontrolirana ventilatora te redundantna izmjenična napajanja.

Uređaj u mrežnu infrastrukturu možemo postaviti na razne načine, pa tako može koegzistirati s postojećim *gatewayom* ili biti spojen s drugim isto takvim *firewallom* u sinkronizirani par, za redundanciju i visoku dostupnost (High Availability).

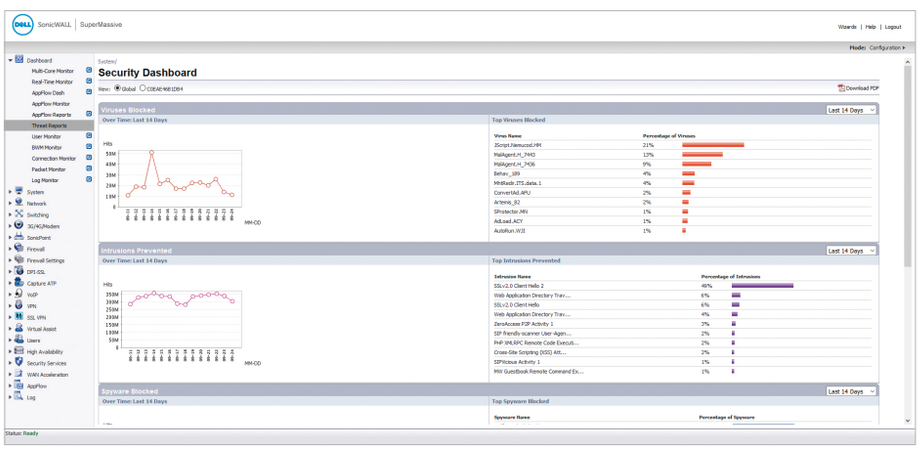
Kao što je već spomenuto, uređaj nije jeftin, ali kao olakotnu okolnost treba spomenuti da je u njegovu cijenu uključena godišnja licenca za sve sigurnosne



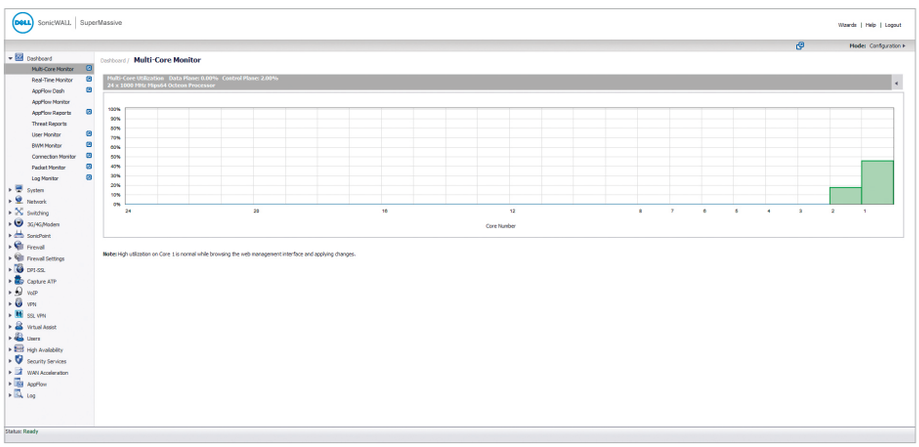
Osnovne informacije o sustavu i sigurnosnim servisima



Na raspolaganju je osam gigabitnih "bakrenih" RJ45 priključaka, osam priključnih mjesta za gigabitne SFP-ove (optičke ili bakrene) te četiri mjesta za 10-gigabitne SFP+ module



Primjer informacija sakupljenih sa SonicWall Grida o ukupnom broju otkrivenih virusa, spriječenih upada, blokiranog *spywarea* i P2P prometa. Podaci se odnose na sve aktivne uređaje u svijetu koji su informacije o svojem djelovanju uspješno poslali na Grid



Pregled rada i opterećenja CPU-a po svakoj pojedinoj jezgri

funkcije. To uključuje patentiranu metodu Reassembly-Free Deep Packet Inspection (RFDPI), dizajniranu za identifikaciju i nadzor aplikacija bez značajnog utjecaja na performanse, za koju se licenca obnavlja na godišnjoj bazi.

DUBINSKO NJUŠKANJE

Uz DPI su vezane i mnoge dubioze, jer je omogućeno njuškanje vaših kriptiranih podataka (a tu spadaju i vaše bankovne transakcije) te se stalno postavlja pitanje gdje prestaje borba protiv prijetnji i napada, a počinje apsolutni nadzor i kontrola. No, poslovica kaže: "*Guns don't kill people, people kill people*!". Ovako moćna platforma na isti se način na koji traži i eliminira prijetnje, može iskoristiti za cenzuru, traženje bilo koje ključne riječi i blokiranje pristupa određenim informacijama.

Američka kompanija Phorm pokušala je 2008. godine u Ujedinjenom Kraljevstvu pokrenuti sustav koji bi presretao i analizirao *web surfing* promet i tako dobivene informacije prodavao oglašivačima. Nakon mnogo prepirki, sve je kulminiralo dokumentom Europske komisije protiv britanske vlade, koja je sustavu dozvolila rad. Slučaj je zatvoren tek 2012. godine, kad je Velika Britanija dopunila svoje zakone sankcijama za nezakonito prisluškivanje komunikacija. Imajući sve spomenuto u vidu, važno je reći da SM9000 ima mogućnost isključivanja pojedinih web-stranica ili domena iz procesa "dubokog njuškanja".

Zatim treba spomenuti *gateway* antivirus sustav, koji blokira viruse na samom ulazu mrežu, mnogo prije nego što uopće dođu u priliku napraviti neku štetu. *Anti-malware* sustav, poput antivirusa, detektira i blokira "crve", "trojance", *rootkitove* i ostali *spyware* već na samom ulazu. Intrusion Detection & Prevention System (IDS/IPS) za detekciju i prevenciju upada štiti od brojnih vrsta mrežnih napada. Koristeći dubinsku provjeru paketa, lako blokira bilo koji poznati napad, ali isto tako i nepoznate, tražeći anomalije u mrežnom prometu. Za URL filtriranje SonicWall ima omogućen vlastiti Content Filtering Service (CFS), a opcionalno se može dodati i WebSense Enterprise *cloud* servis.

Anti-Botnet sustav na SM9200 prieči korištenje resursa štićene infrastrukture za kriminalno djelovanje prema trećoj strani, što se inače izvodi pomoću *botova*, računalnog kôda koji na razne načine može kompromitirati računalo, pa ga napadači mogu u potpunosti preuzeti i iskoristiti za DDoS napad na nama potpuno nepoznatu žrtvu

RJ45 serijski *port* koristi se za spajanje konzole, a dva USB *porta* namijenjena su spajanju modema (3G/4G/analogni)

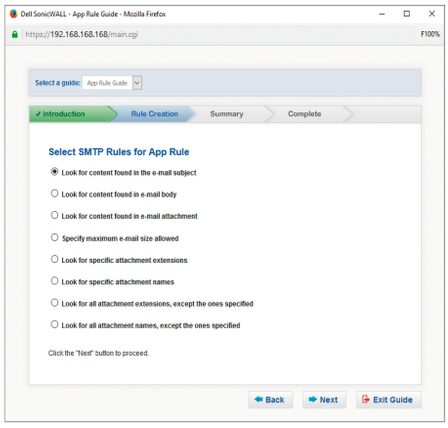
Application Control funkcionalnost pruža više razine sigurnosti za nadzor korištenja internetskih resursa, kao što su pretraživanje web-stranica, transferi datoteka i *e-mailovi*. Osim samog prometa, identificirani su i korisnici, što značajno olakšava praćenje tijekova prometa i reagiranje na anomalije.

SSL je još jedna kategorija koja čini trećinu ukupnog prometa, a protiv koje je klasični *firewall* nemoćan. Uz pomoć spomenute metode RFDPI, SonicWall pregledava enkriptirani promet tako da ga dekriptira, provjeri sadržaj, primjeni na njega predefinirani *policy*, ponovno ga kriptira i šalje na odredište bez vidljiva zastoja.

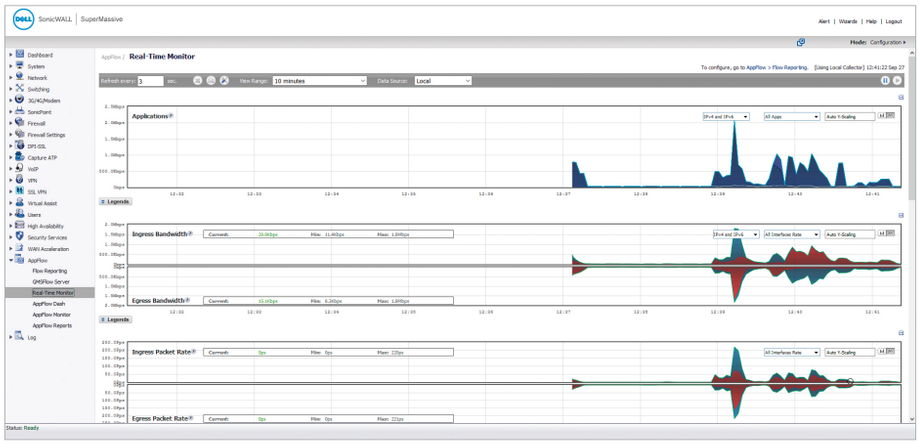
SonicWall Grid je inteligentna mreža koja kontinuirano prikuplja i analizira prijetnje sa svih aktivnih sustava te kroz globalni sustav reputacije štiti klijente od učestalih napadača i izvora prijetnji. Informacije s Grida sigurno se i anonimno distribuiraju u mrežu instaliranih uređaja, konstantno povećavajući učinkovitost cijelog spektra sigurnosnih mehanizama.

Zone sigurnosti pojednostavnjuju implementaciju sigurnosnih politika, jer se ne moraju primjenjivati na svaki pojedini *port*, nego na zone u koje, prema potrebi, uključujemo fizičke *portove* na koje želimo primijeniti određena pravila. Prilikom kreiranja zona biramo vrstu sigurnosti pa je tako preddefinirana WAN zona klasificirana kao nesigurna, i uređaj neće dopustiti da promet od nje prođe prema nekoj drugoj zoni, osim ako to nekim pravilom nije eksplicitno dopušteno.

Budući da je podržana *wizardima*, instalacija je vrlo jednostavna pa podešavanja aplikacijskog *firewalla*, VPN-ova i DMZ-ova ne predstavljaju problem. Vrlo intuitivan GUI, koji će zbog ekskluzivnosti uređaja imati prilike vidjeti tek rijetki čitatelji, odgovorit će na sva pitanja i brzo vas provesti kroz cijelu proceduru. Eto dokaza da sigurnosni *appliance* s cijenom od preko 300.000 kuna može istovremeno biti iznimno moćan i nadasve intuitivan za korištenje.



Primjer konfiguracijskog čarobnjaka za definiranje aplikacijskih pravila



Grafički prikaz rada sustava namijenjen praćenju u realnom vremenu