Požarni zidovi SonicWALL PRO

..Požarni zid je prepreka, ki zunanjim nevarnostim preprečuje dostop do lokalnega omrežja in računalnikov v njem..

Danesa®
VARUJEMO PRIHODNOST

Požarni zidovi SonicWALL PRO predstavljajo na področju internetne varnosti pravo umetniško delo. Naprave so se z lahkoto uvrstile na listo najboljših "ubijalcev hekerjev", saj so uspešno preživele več kot 20.000 različnih napadov. Med napadi so bili izvajani: DoS, SymLink, Buffer Overflow, Cross site scripting, SQL injection, Directory Traversal, avtentifikacijske napake, test odpornosti enkripcije (3DES, AES), test napačne konfiguracije in odpornosti na znane pomanjkljivosti požarnih zidov.

To so samo nekateri izmed načinov, s pomočjo katerih lahko napadalec pridobi zunanji dostop do spletnega vmesnika običajnega požarnega zidu. V primeru SonicWALL so tovrstne skrbi popolnoma odveč, saj se SonicWALL PRO požarni zidovi proti tovrstnim nevarnostim borijo z implementacijo IDS (intrusion detection sistem), IPS (intrusion prevention sistem) in protivirusnim pregledom mrežnega prometa ter DPI (deep packet inspection) funkcionalnostjo.

SonicWALL naprave se lahko konfigurirajo iz lokalnega omrežja, dodana pa jim je tudi možnost varnega VPN dostopa. Sposobnejšim hekerjem seveda takšne omejitve ne predstavljajo težav, saj poznajo napadalci nešteto načinov za pridobitev neavtoriziranega dostopa v lokalno omrežje od zunaj. Takšen dostop je npr. mogoč z odpiranjem posredovanja vrat terminalnih servisov ali VNC, povezovanjem s pomočjo nepravilno konfiguriranih brezžičnih mostov, namestitvijo trojanskega konja itd. Tovrstni dodatki so nato hekerjem v pomoč pri pridobivanju informacij in izvedbi kasnejšega napada, ki pogosto vključuje tudi človeške napake in malomarnost zaposlenih.

SonicWALL uspešno zazna tudi tovrstno taktiko napadalcev, imenovano "reverse shell" oz. "call home".

Običajni požarni zidovi na tem področju pogosto pokleknejo, saj se jim zdi promet, ki ga inicializira škodljiva skripta, popolnoma regularen in ga zato spustijo v omrežje. V takšnih primerih se nahajamo samo še korak od katastrofe in kompromitacije vašega omrežja.

SonicWALL namestitveni čarovnik nas v nekaj korakih popelje skozi vnose podatkov. Požarni zid ima vgrajeno NAT (network address translation) in DHCP funkcionalnost, katere uporabo vam vsekakor priporočamo, saj nudi poleg ostalih prednosti tudi zaščitne ukrepe pred internetnimi napadi. Uporabniški vmesnik požarnega zidu je pregleden, njegovo upravljanje pa nadvse enostavno. Ravno preprostost uporabe je adut, ki nas je med testiranjem SonicWALL požarnih zidov prijetno presenetila.

SonicWALL ima neverjetno enostavne možnosti konfiguracije, pri čemer lahko na primer z enim samim klikom onemogočimo javno oddajanje NetBIOS-a ali omogočimo t.i. "Stealth mode", ki bo hekerjem napravo naredil praktično "nevidno". Nevidnost požarnega zidu deluje samo v kontekstu, ko napadalec napravo skenira v agresivnem načinu (10 povezav na sekundo). V kolikor bo napadalec vztrajen in bo napravo preverjal v razumnih intervalih ter z uporabo naprednejših metod, bo vseeno pridobil informacije o njenih dejavnostih, pri čemer SonicWALL omogoča tudi namestitev tako imenovanih "Honey pot" sistemov za zavajanje in spremljanje napadalcev. Verjemite, da so tovrstne pasti za hekerje prava nočna mora.

Protivirusni pregled je še ena v vrsti implementiranih zmožnosti požarnih zidov SonicWALL, vendar pa naj v podjetju kljub temu ne predstavlja edino točko obrambe.

Dejstvo, ki govori temu v prid, je, da se lahko virusi v omrežja prenašajo tudi s pomočjo disket, CD-jev, USB pomnilnikov in prenosnih računalnikov. V kratkem se pričakuje tudi uvedba anti-Spyware aplikacije, s čimer bo SonicWALL postal na področju požarnih zidov eden prvih borcev proti tovrstnim varnostnim nadlogam.

Največja prednost SonicWALL požarnih zidov pred tekmeci pa je prav gotovo dejstvo, da v tem trenutku za te naprave ni javno znanih varnostnih pomanjkljivosti. To je v tem segmentu varnostnih naprav prava redkost. Vsi dobro poznani in večji proizvajalci požarnih zidov so namreč zaradi kritične mase, ki jo na trgu dosegajo, redne tarče hekerskih napadov in razkritja slabosti posameznih naprav. (P.R.)

SONICWALL

Danesa, informatika, svetovanje in posredništvo d.o.o.
Legatova 2, p.p. 4555
1001 Ljubljana

tel: +386 1 242 9000
fax: +386 1 242 9010
www.danesa.com
e-mail: info@danesa.com