v některých případech nemusí být dostatečně popisná. Lze využít autentizace přes LDAP/AD/ /RADIUS a řadu dalších.

Soubor nástrojů doplňují analytické funkce umožňující intuitivní zobrazení konfliktů, pravidel a korelací aplikačních aktivit v reálném čase podle identity uživatele, umístění (geolokace) či úrovně oprávnění. Pomocí nástroje Firewall Reporter, který centrálně monitoruje provoz a generuje korelovaná upozornění a hlášení, lze vytvářet a měnit proudy dat do informací přímo použitelných pro účely auditu.

Zdarma je také možné využít reporting využití webového provozu McAfee Web Reporter. Druhý zmiňovaný využívá výstupy SmartFilteru. Tato komponenta na firewallu nám umožňuje regulovat využití webového provozu, a to na základě 90 kategorií obsahujících desítky milionů kategorizovaných stránek, tak příslušnosti do skupin nebo denní doby.

Zařízení se pyšní certifikací Common Criteria EAL4+ pro aplikační kontroly a filtruje šifrovaný provoz do hloubky – dešifruje zabezpečené protokoly (jako HTTPS, SSH, SCP a SFTP), uplatní antivirovou ochranu, IPS a aplikační filtraci a poté provoz opět šifruje a odesílá na cílový server. Systém dále neumožňuje oklamání firewallu tunelováním jiných protokolů, poskytuje plnohodnotné skrytí vnitřní sítě (network cloaking) a disponuje virtuální technologií „black hole“ pro odražení útoků. ■

Virtualizace firewallů

V počítačovém odvětví se stále zřetelněji prosazuje trend přesunout stavové firewally v rámci IT prostředí blíže k serverům.

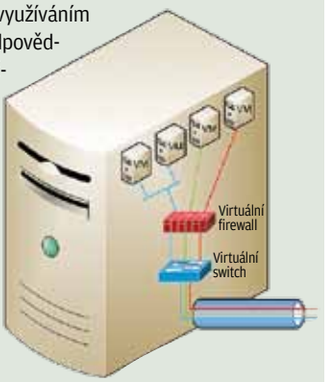
Díky virtualizaci a konsolidaci serverů můžeme provozovat na jednom fyzickém serveru několik virtuálních serverů s rozdílnými úrovněmi důvěryhodnosti. Základní (core) firewally a firewally na perimetru už nejsou těmto serverům dostatečně blízko. Firewall blízko fyzického serveru může lépe zabezpečit každý virtuální server a umožňuje serverům komunikaci s dalšími servery odlišných úrovní důvěryhodnosti pouze přes stavový firewall. Takový firewall provozovaný na vrstvě hypervizoru či serverové virtualizace zabraňuje nežádoucí komunikaci mezi servery.

Na obrázku je znázorněn provoz několika virtuálních počítačů na jednom fyzickém stroji. Každý z nich může mít odlišnou úroveň důvěryhodnosti nebo klasifikace dat, s nimiž pracuje. Pro oddělení komunikace jednotlivých virtuálních strojů a zajištění jejich bezpečnosti je proto potřeba zajistit stavovou filtraci paketů v rámci virtuálního prostředí. Taková filtrace na dané architektonické úrovni může být někdy vyžadována i pro účely zajištění souladu s legislativou.

Současným trendem je posun směrem k hostovaným firewallům. Stále více organizací se poohlíží po využití propracovanějších firewallů na úrovni hypervizoru. V současnosti už tyto typy virtualizovaných produktů nabízí celá řada dodavatelů jako Cisco, Juniper, Check Point, Fortinet či Sophos (dříve Astaro).

Další otázkou, která v mnoha organizacích přichází na přetřes v souvislosti s využíváním virtuálního firewallu, je, kdo má tento virtualizovaný firewall spravovat. Bude odpovědnost za konfiguraci a správu virtuálního firewallu ležet na bedrech síťařů, bezpečnostního týmu nebo systémových administrátorů? Otázka je ještě naléhavější v případech, kdy do virtualizační vrstvy se přesunují celá zařízení pro UTM.

Navíc se dá předpokládat, že se do této vrstvy přesunou i virtualizované verze nástrojů SLB (Server Load Balancer) pro vyrovnávání zátěže serverů a systémů ADC (Application Delivery Controller) pro řízení aplikačních zdrojů. Tradiční fyzické hranice se tak budou stírat stále více a místo dříve využívaných centralizovaných firewallů se budou ve stále větší míře nasazovat firewally distribuované.



Virtualizace firewallu v rámci virtuálního výpočetního prostředí