

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 odrazení 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.

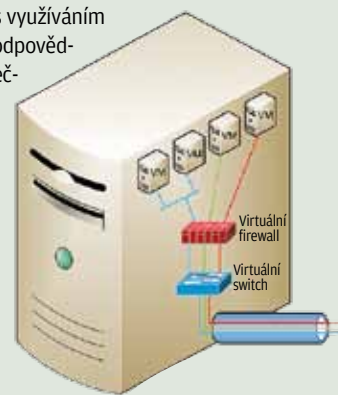
Na obrázku je znázorněn provoz několika virtuálních počítačů na jednom fyzickém stroji. Každý z nich může mít odlišnou úroveň důvěryhodnosti nebo klasifikace dat, s nimiž pracuje. Pro oddělení komunikace jednotlivých virtuálních strojů a zajištění jejich bezpečnosti je proto potřeba zajistit stavovou 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 pracovnějších 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 síťářů, 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



Partnerský příspěvek

Osobní strážce internetu Filtr webového provozu Kernun Clear Web

Devadesát procent. Přesně tolik z internetového provozu typické organizace představuje webová komunikace. A pokud budeme souhlasit s tvrzením, že internet znamená jeden z nejrizikovějších faktorů pro naši bezpečnost (a asi není důvod s ním nesouhlasit), pak je nabíledni, že ošetření tohoto provozu musíme dát odpovídající důraz.

Bezkonkurenční znalost terénu

Dvě až čtyři procenta webového obsahu představují riziko (pro zajímavost: mezi placenými odkazy je to šest až deset procent!). Průměrný web je díky absenci nejnovějších záplat nebo špatně zvoleným programátorským postupům nebezpečný svému okolí až devět měsíců v roce! O nárůstu internetových podvodů (podle některých statistik meziročně o 8 tisíc procent) ani nemluvě.

Se všemi těmito výzvami si přitom dokáže poradit Kernun Clear Web: řešení pro filtrování webového provozu. Jeho hlavní předností je skutečnost, že se zaměřuje na prostředí „českého internetu“. To pochopitelně není technický pojem, ale je zapotřebí si uvědomit, že čeští uživatelé navštěvují jiné stránky než například Američané (jimž je většina řešení „sítá na míru“) a že mají

jiné profily chování. Argument „je jen jeden internet“ je sice pravdivý, ale v daném případě neobstojí. Svědčí o tom i to, že Kernun Clear Web má v českém prostředí úspěšnost převyšující 98 procent – konkurenční produkty ze zahraničí se typicky pohybují mezi šedesáti a sedmdesáti procenty.

Filtr pro dvacet tisíc uživatelů

Důležitost filtrování webového provozu si uvědomilo i Ministerstvo práce a sociálních věcí ČR, které zaměstnává téměř 20 tisíc osob s přístupem na internet: a to v mnoha lokalitách a s rozličnými právy nebo bezpečnostními režimy. Ministerstvo donedávna používalo pro správu sítě a filtrování webů řešení, které bylo závislé na spolupráci několika webových proxy. Tento systém se ovšem nedal jednoduše aktualizovat, udržovat v chodu – a o nějaké centralizaci nebylo možné ani uvažovat.

Kromě vytvoření přehledné a bezpečné počítačové sítě bylo zároveň potřeba vyřešit další dva navazující problémy. Za prvé provést transparentní opatření, aby zaměstnanci využívali internet co nejefektivněji a zároveň sít zbytečně nezátěžovali. Za druhé zvýšit efektivitu práce.



Tzn. zamezit tomu, aby zaměstnanci ministerstva využívali svou pracovní dobu k nepracovním aktivitám. Ze všech nabízených řešení si nakonec ministerstvo vybralo právě řešení Kernun Clear Web. Ostatně o jeho možnostech se můžete přesvědčit sami na stránkách www.kernun.cz/demo.

Testováno na lidech

Pokud bychom měli nechat promluvit suchou řeč statistik, pak z měřitelných parametrů po nasazení řešení Kernun Clear Web poklesl počet virových nákaz na klientských stanicích ministerstva o plnou třetinu (což je ohromný úspěch vzhledem k tomu, že Kernun není primárně antivirovým systémem) a využívání internetu pro soukromé potřeby kleslo o 69 procent. A to nemluvíme o nepřímých efektech: produktivité práce, lepším využití hardwaru apod. Kernun Clear Web zkrátka ukázal, že se na něj lze při filtrování webového provozu sto procentně spolehnout. Více informací lze také najít v případové studii MPSV ČR na stránkách www.kernun.cz.

