

Koncept varovanja virtualnega okolja

Z vse pogostejšo uporabo virtualizacije strežnikov so podjetja elegantno rešila najmanj dva problema. V prvi vrsti so se zmanjšale investicije v potrebno strojno opremo, zmanjšali pa so se tudi operativni stroški porabe energije, potrebnega prostora za strežnike in s tem povezani posredni stroški (klimatske naprave, najemnine za prostore itd.). Prav tako je virtualizacija strežnikov in njihovih aplikacij prinesla rešitev za zagotavljanje visoke zanesljivosti ter z različnimi mehanizmi svojim uporabnikom omogočila neprekinjeno in kontinuirano poslovanje.

Virtualizacija je poleg pozitivnih posledic zmanjševanja stroškov prinesla tudi nekaj kompromisov, predvsem na račun varnosti. Gre za opuščeno segmentacijo strežnikov in aplikacij, pomanjkanje kontrole dostopa do virtualnih entitet in pomanjkanje ali odsotnosti kontrole prometa med samimi aplikacijami na virtualnih entitetah. V virtualnem okolju torej skoraj nimamo mehanizmov, ki bi kontrolirali ali zgolj nadzorovali in spremljali, katera aplikacija dela ali kliče druge aplikacije (npr. aplikacijski strežnik → strežnik z bazo), po katerih portih poteka promet znotraj virtualnih entitet in ali je ta promet legitimen. Prav tako se opaža pomanjkanje mehanizmov kontrole dostopa, saj se lahko uporabnik oziroma administrator, ko se enkrat prijavi na virtualni strežnik, prosto »sprehaja« in dostopa do vseh virtualnih entitet in aplikacij, ki so na tem strežniku.

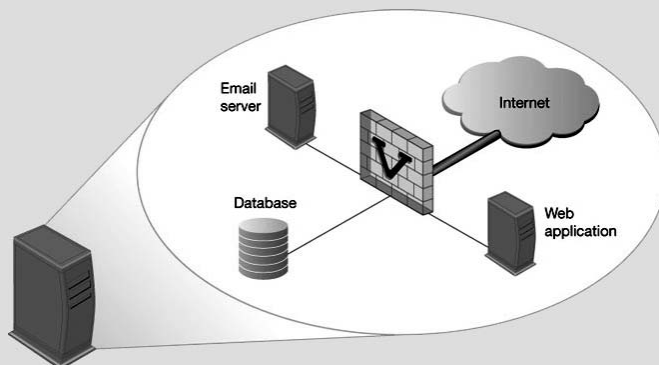
Problem varovanja virtualnega okolja je na podlagi prepoznanih pomanjkljivosti potreboval primerno rešitev. Vodilni proizvajalec Check Point Software Technologies je tako v letu 2008 predstavil nov koncept varovanja virtualnega okolja. Gartner uvršča Check Point-ove rešitve v pozicijo vodilnih na trgu in ga ob enem prepoznava kot vizionarja na področju požarnih pregrad naslednje generacije.

ZAŠČITA VIRTUALNIH STREŽNIKOV

Check Point VPN-1 VE (Virtual Edition) ščiti virtualne sisteme z enako vrhunsko tehnologijo kot je zagotovljena na mrežnem nivoju. Rešitev omogoča medsebojno izolacijo virtualnih entitet na virtualiziranem strežniku in zaščito pred zunanjimi nevarnostmi. Nad temi sistemi bdi centralni management, ki omogoča enostavno in učinkovito upravljanje, kot smo ga vajeni pri vseh Check Point produktih. Prednosti Check Point VPN-1 VE:

- Zaščita aplikacij v virtualnem okolju z vrhunsko tehnologijo
- Zaščita pred zunanjimi in notranjimi nevarnostmi ter nedovoljenimi aktivnostmi
- Poenostavitev zagotavljanja varnosti v virtualiziranih okoljih
- Enotno upravljanje fizičnih in virtualnih okolij

VPN-1 za VMware se lahko vpelje na samem VMware ESX ali ESXi strežniku za zaščito vseh virtualnih entitet, kot so npr. baze podatkov, Web strežniki, strežniki za e-pošto idr. Po tem scenariju je vsaka virtualna entiteta nameščena na ločenem virtualnem mrežnem segmentu. VPN-1 VE, ki se med njimi nahaja, pa te entitete med seboj varnostno ločuje oziroma nadzira in upravlja komunikacijo med njimi. Log o dogajanju o vseh komunikacijah se hrani na centralnem managementu.



Slika1: Prikaz logične umestitve VPN-1 VE požarne pregrade v virtualnem okolju

Check Point VPN-1 VE pregleduje ves promet med virtualnimi entitetami. To omogoča sledeče funkcionalnosti:

ZAŠČITA PRED ZLORABAMI NA APLIKACIJSKEM NIVOJU – VPN-1 VE zagotavlja integrirano zaščito pred napadi na aplikacijskem nivoju s SmartDefense tehnologijo. Če se nek virtualni strežnik ali druga virtualna entiteta kompromitira, VPN-1 VE še vedno lahko ščiti ostale virtualne sisteme pred zlonamernim prometom.

KONTROLA DOSTOPA – VPN-1 VE vsebuje produkt Firewall-1, ki ga odlikuje močna kontrola dostopa. Na ta način lahko povrnemo tradicionalno kontrolo dostopa do strežnikov ter njihovo segmentacijo tudi v virtualiziranem okolju.

ZAŠČITA VIRTUALNIH STREŽNIKOV – Uporaba VPN-1 VE omogoča izolacijo virtualnih strežnikov med seboj, kar preprečuje napadalca ali neavtoriziranemu uporabniku, da bi se prosto »sprehajal« z enega virtualnega strežnika na drugega.

VARNA KOMUNIKACIJA MED VIRTUALNIH STREŽNIKI – VPN-1 VE omogoča enkripcijo prometa med samimi virtualnimi strežniki in med virtualnim strežnikom in uporabnikom (IPSec ali SSL tunel). Lahko se omogoči varen dostop oddaljenih uporabnikov tudi samo do samo določene aplikacije na določeni virtualni entiteti.

SEGMENTACIJA STREŽNIKOV IN APLIKACIJ – Z uporabo VPN-1 VE se strežniki ali aplikacije lahko ločijo v različne segmente. Na ta način lahko zagotovimo ustreznost revizorskim zahtevam, ne da bi bili prikrajšani za ugodnosti virtualiziranega okolja. Rešitev je idealna za organizacijo gostujočih aplikacij na istem strežniku, ki so v upravljanju različnih uporabnikov oziroma lastnikov.

KONTROLA IN NADZOR PREKO PREGLEDOVANJA VSEBIN – VPN-1 VE se lahko vpelje kot UTM (Unified Threat Management) rešitev, vključno z antivirusno rešitvijo in zaščito pred malware zlorabami. Varovanje lahko zagotavlja tudi na nivoju pregledovanja vsebin prometa.

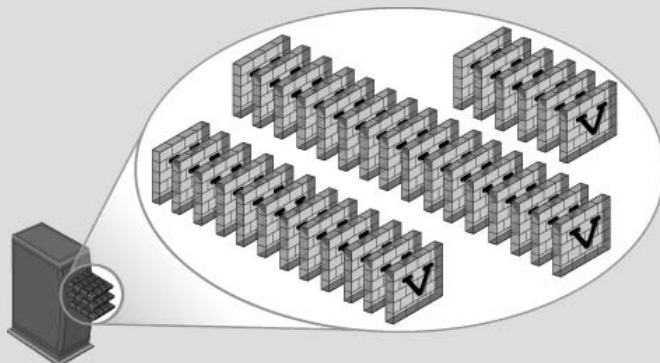
CERTIFICIRANA ZDRUŽLJIVOST – Zdržljivost VPN-1 VE je certificirana s strani VMware-a za VMware ESX in ESXi Server. To zagotavlja zaupanje v varovanje poslovno kritičnih aplikacij v virtualiziranem okolju.

PREDKONFIGURIRANO OKOLJE – VPN-1 VE je dobavljiv kot pred-konfiguriran sistem z ustreznimi nastavitvami, kot so npr. alociranje spomina, definiranje vmesnikov itd. Vsi parametri se lahko kasneje poljubno nastavijo.

MANJŠE POTREBE PO KONFIGURACIJI MREŽE – Ker se VPN-1 VE nahaja v samem ESX Serverju, ščiti vse virtualne entitete, ne da bi bilo potrebno namestiti kompleksnih VLAN ali segmentacijskih nastavitvev.

VIRTUALIZACIJA POŽARNIH PREGRAD

Druga rešitev na temo virtualizacije ponudnika Check Point je virtualizacija požarnih pregrad. Check Point-ov produkt VPN-1 Power VSX je več-opravljalna izvedbena platforma, namenjena večjim virtualnim okoljem. Z VPN-1 VSX lahko administratorji implementirajo virtualne fizične topologije, ki imajo centralne in oddaljene DMZ cone. VSX platforma omogoča implementacijo do 250 popolnoma neodvisnih varnostnih sistemov (požarnih pregrad) na samostojni ali redundantni (clutser) strojni platformi. Na ta način dobimo na fizično enem strežniku več virtualnih firewall-ov oziroma Security Gateway-ev. To pomeni direktno zmanjšanje stroškov za strojno opremo, prihranek pri prostoru in porabi energije ter lažje obvladovanje stroškov.



Slika2: Na eni strojni platformi se lahko nahaja do 250 virtualnih varnostnih prehodov (požarnih pregrad).

Pri virtualizaciji požarne nadgradnje je možno vpeljati več različnih scenarijev implementacije:

KONSOLIDACIJA DATA CENTRA – Kljub konsolidaciji Data centrov ostaja potreba po segmentaciji različnih aplikacij ali poslovnih enot. VPN-1 Power VSX omogoča učinkovito segmentacijo in implementacijo večjega števila varnostnih con oziroma Security Gateway-ev na fizično eni strojni platformi (strežniku).

NAPREDNA SEGMENTACIJA OMREŽJA – S VPN-1 Power VSX se lahko kreira do 250 Security Gateway-ev za segmentacijo dohodnega in odhodnega prometa med poslovnimi enotami ali internimi oddelki in entitetami, kot so npr. oddelki podjetja, uporabniki po nadstropjih, več podjetij v isti stavbi ... Te požarne pregrade so logično umeščene na mestih, kjer želimo izvajati kontrolo in nadzor, medtem ko so fizično nameščene na eni strojni platformi (strežniku), ki se nahaja v IT-centru.

VIRTUALIZACIJA SECURE PLATFORM OS – SecurePlatform operacijski sistem zagotavlja varnost poslovno kritičnim aplikacijam.

Virtualizacija požarnih pregrad ima ekonomske, investicijske in TCO prednosti:

ZMANJŠANJE INVESTICIJE V HARDWARE – VPN-1 Power VSX omogoča s konsolidacijo varnostnih sistemov na eni strojni platformi tudi izvedbo virtualnih firewall-ov, stikal, usmerjevalnikov ...

HITRA VPELJAVA NOVIH SERVISOV – S povečanjem potreb VPN-1 VSX omogoča hitro vpeljavo novih storitev, pri čemer ni potrebno pristajati na varnostne kompromise. Segmentacija je že definirana in ni potrebe po dodatnih investicijah v novo strojno opremo.

KAKO DO VARNOSTI IN CHECK POINT-A V SLOVENIJI

Check Point-ove varnostne rešitve so vodilne tovrstne rešitve na trgu in predstavljajo smernice razvoja tudi za ostale ponudnike. Načine in smernice razvoja varovanja virtualnega okolja v Sloveniji pa postavlja S&T Slovenija. Ta ponuja nabor varnostnih rešitev, ki jih razvija S&T-jeva samostojna skupina varnostnih strokovnjakov, hkrati pa je na slovenskem trgu S&T Slovenija edini Check Point partner s statusom za nudenje podpore. V sodelovanju s podjetjem Check Point S&T Slovenija predstavlja zanesljivega partnerja na področju varovanja virtualnega okolja, svojim uporabnikom pa poleg uporabe Check Point izobraževalnega centra ter neposrednega dostopa do Check Point podpore nudi tudi uporabnikovim specifičnim potrebam in željam prilagojene varnostne rešitve.



S&T Slovenija d.d.
Leskoškova cesta 6
1000 Ljubljana
www.snt.si