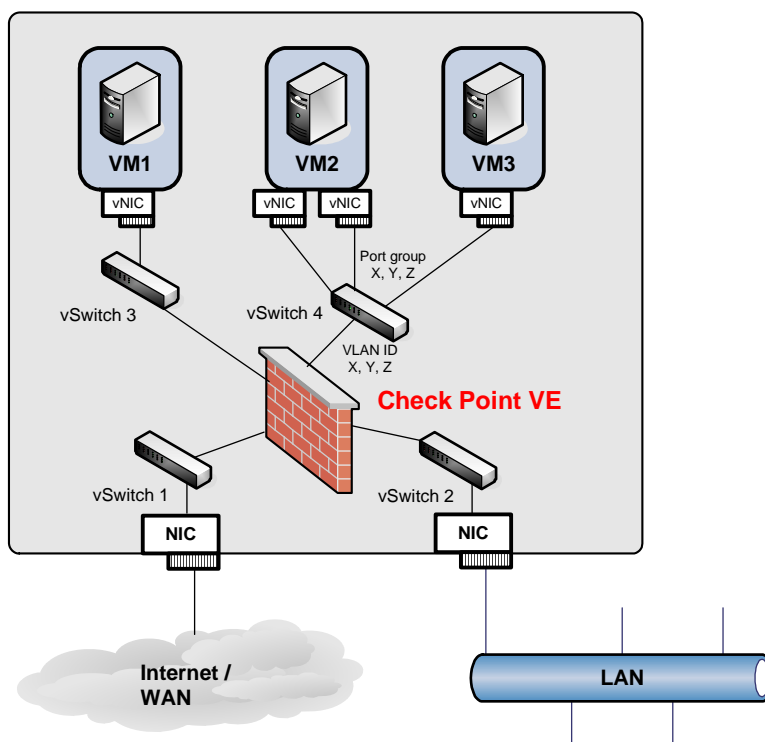


Check Point VPN-1 Virtual Edition

- optymalna ochrona środowiska wirtualnego

Wirtualizacja środowiska serwerowego stanowi efektywną metodę optymalizacji rosnących kosztów utrzymania i rozwoju systemów informatycznych (m.in. niższe koszty sprzętu serwerowego i urządzeń sieciowych, mniejsze wymagania na miejsce w serwerowni, zasilanie, klimatyzację, itd.). Należy jednak pamiętać, że środowiska wirtualne jak VMware posiadają analogiczne zagrożenia jak środowiska fizyczne (m.in. ataki intruzów, złośliwy kod, DoS) i wymagają wdrożenia adekwatnych środków bezpieczeństwa.

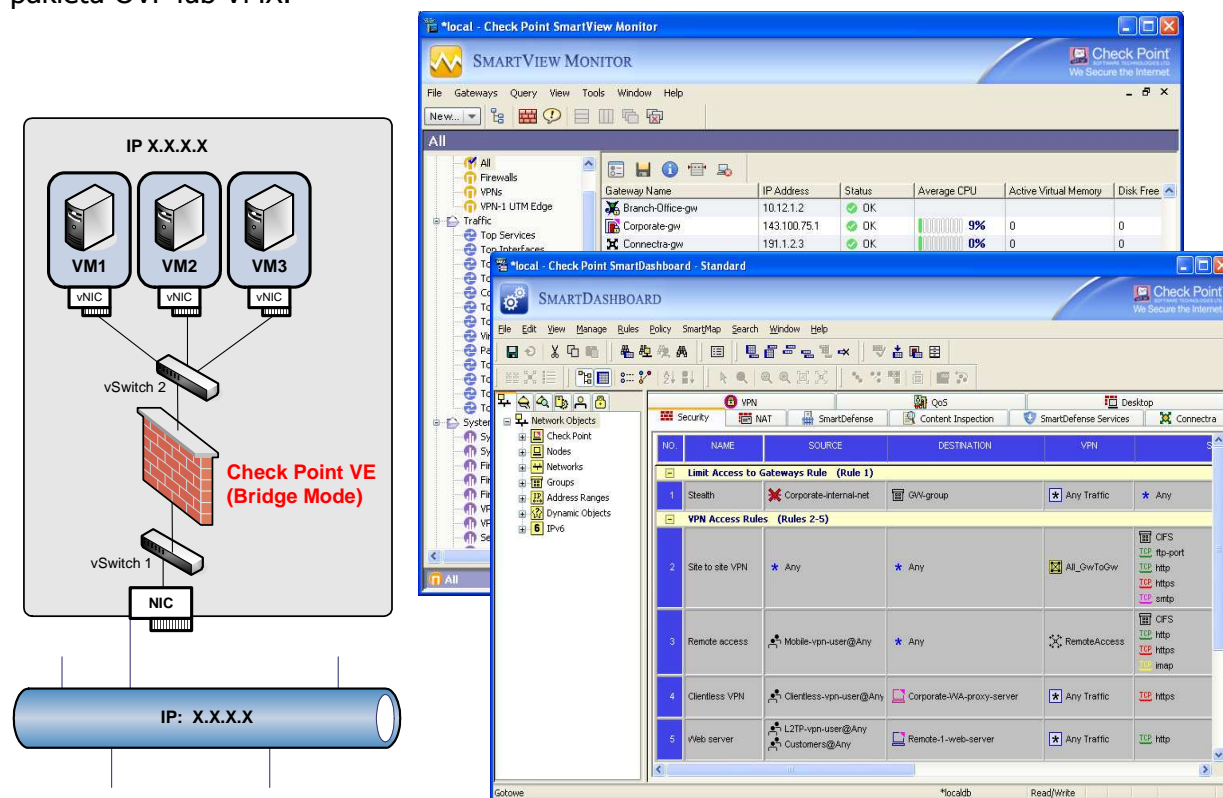
Zabezpieczenia środowiska VMWare (m.in. izolacja VM i vSwitch) nie ograniczają możliwości wykonywania ataków na/z maszyn wirtualnych VM. Występują zagrożenia analogiczne jak dla środowiska fizycznego, a także zagrożenia specyficzne dla VMware (np. ataki na Service Console i Hypervisor). Mając do dyspozycji konwencjonalne zabezpieczenia (m.in. firewall, IPS, WAF) trudno jest w środowisku wirtualnym wdrożyć właściwe środki bezpieczeństwa. Wymagane jest przekierowanie ruchu z VM do urządzeń zabezpieczeń, gdzie będzie odbywała się kontrola komunikacji. Zastosowanie zewnętrznych urządzeń jest niezgodne z „filozofią” środowiska wirtualnego, generuje wysokie koszty wdrożenia i utrzymania zabezpieczeń, a także ogranicza swobodę rozwoju wirtualnego środowiska IT. Każdorazowa zmiana w środowisku VMWare wymaga wykonania analizy zagrożeń, weryfikacji możliwości oraz wprowadzenia odpowiedniej modyfikacji zabezpieczeń.



Zabezpieczenia VE stanowią integralny element środowiska wirtualnego

Check Point VPN-1 Virtual Edition (VE) to kompletny system zabezpieczeń dedykowany do zastosowań wewnątrz środowiska VMware. VE w środowisku VMware działa jak maszyna wirtualna VM z specjalizowanym systemem operacyjnym Check Point SecurePlatform.

Rozwiązanie jest certyfikowane na serwery VMware ESX 3.0.2, 3.5 i ESXi 3.5 (vSphere wkrótce). Uruchomienie zabezpieczeń VE wymaga niewielkich nakładów i nie wymaga użycia dodatkowych urządzeń. Moduł zabezpieczeń VE jest uruchamiany z prekonfigurowanego pakietu OVF lub VMX.



Zabezpieczenia VE zapewniają kompletną ochronę zasobów IT w środowisku wirtualnym

Check Point VPN-1 VE zapewnia stały poziom bezpieczeństwa bez względu na zmiany wirtualnego środowiska (Failure, VMotion, DRS, itp.). Chroni maszyny VM oraz Service Console (każdy pakiet z sieci jest poddawany inspekcji). Zastosowanie VE sprawia, że moduł Hypervisor jest mniej zagrożony atakiem z sieci. Wirtualne przełączniki vSwitch i Hypervisor nie posiadają adresów IP i nie nasłuchują na żadnych portach, co znacznie utrudnia wykonywanie ataków z zewnątrz na te komponenty. VE kontroluje całość ruchu sieciowego z/do środowiska wirtualnego. Zastosowany w VE mechanizm VMsafe umożliwia ochronę maszyn VM w sytuacji, gdy podłączone są do tego samego vSwitch. Wsparcie dla VMotion (także dla Storage) zapewnia elastyczność i ochronę przed awariami. Inspekcja na poziomie Hypervisor zapewnia wysoką wydajność pracy zabezpieczeń VE.

Rozwiązanie bezpieczeństwa VE zostało opracowane dla środowiska wirtualnego na bazie sprawdzonej technologii zabezpieczeń Check Point VPN-1/FireWall-1. VE oferuje komplet funkcji ochrony przed zagrożeniami z sieci (m.in. firewall, intrusion prevention, antivirus, antispayware, Web application firewall, IPSec i SSL VPN). Moduł ClusterXL zapewnia ochronę przed awariami zabezpieczeń i podwyższenie wydajności (load sharing). Moduły zabezpieczeń VE mogą być zarządzane z centralnego systemu zarządzania SmartCenter. Także moduł SmartCenter może zostać uruchomiony jako maszyna wirtualna.

Więcej informacji dostępnych na stronie producenta oraz polskiego dystrybutora:

<http://www.checkpoint.pl>