

Network and Security Manager 2008

Revoluce v managementu sítě v Enterprise prostředí

Noční můra administrátorů je vyřešena. Juniper uvedl produkt, který slučuje funkce managementu bezpečnostních systémů i aktivních síťových prvků, čímž v konečném důsledku významně šetří provozní náklady a velmi zefektivňuje práci celého IT oddělení.



"Hey, now that we've switched to Juniper, we should have plenty of spare time to learn how to fly!"

V čem je problém?

Na dnešní podnikové sítě jsou kladeny obrovské nároky z pohledu stability, výkonu i zabezpečení. Ve svém důsledku to znamená zajistit vysokou dostupnost infrastruktury, monitorovat její funkce a mít k dispozici nástroj, kterým by administrátor mohl ihned reagovat na změny, a to z pohledu zabezpečení: stanovením restrikcí a politik, povolení provozu schválených protokolů a aplikací, správy VPN tunelů, ale i síťové problematiky: VLAN, QoS, dynamického směrování.

Takové požadavky vedou k instalaci mnoha systémů, přičemž každý disponuje svým sofistikovaným ovládáním. V konečném důsledku to znamená implementovat celou

řadu různých dohledových serverů, instalovat mnoho softwarových programů, knihoven ale i nástaveb a nástrojů, které umožní správu systémů jako celku.

Celkový výsledek však stále pokulhává

Nelze totiž zajistit, aby konfigurace systémů nebyly ve vzájemném rozporu, je velmi finančně nákladné a komplikované stále udržovat systémy aktualizované, vzájemně provázané a události korelované, o vysoké dostupnosti (clusterovaných) řešení nemluvě.

Řešení má Juniper

Juniper uvedl produkt, v zásadě se jedná o komplexní systémové řešení, které umožní centralizovanou správu síťových i bezpeč-

nostních systémů včetně možnosti jejich konfigurace. **Network and Security Manager 2008 (NSM)** v sobě integruje přednosti a výhody managementu jednotlivých prvků, systémů sběru dat, korelace logů a reportovacích nástrojů. Podporovány jsou následující produktové řady Juniper Networks:

- Firewally (SSG, ISG, NS serie)
- IPS systémy (IDP serie)
- SSL VPN brány (SA serie)
- NAC/UAC systémy (IC serie)
- Switche (EX serie)
- Routery (J-serie)

NSM disponuje nástroji pro delegaci a určení správce či skupin správců, které mohou prvky nastavovat či pouze na ně dohlížet. Nabízí se tak separace úloh dle funkce zodpovědnosti administrátorů.

- **Sítový specialista** může mít na starosti funkce směrování, VLAN, QoS
- **Bezpečnostní administrátor** spravuje a stanovuje bezpečnostní politiky, stanovuje podmínky autentikace a autorizace přístupu k aplikačním serverům a informacím, omezuje a monitoruje komunikaci, aby čelil hrozbám zvnějšku ale i zevnitř.
- **Dispečeri** mohou mít práva pouze pro nezbytnou údržbu svěřených systému a jejich monitoring.

Může existovat celá řada tzv. rolí, které přesně definují práva uživatele NSM systému, je podporováno i hierarchické členění správy.

V čem je síla takového řešení?

Integrace správy firewallů, Intrusion and Prevention systémů (IPS) spolu se systémy pro ověření přístupu Network Admission Control (NAC) v jednom management řešení má v konečném důsledku obrovský význam. Lze dědit podmínky a určovat restriktce v rámci jednoho nástroje. Nastavení IPS se tak může promítnout do podmínek NAC, preference VoIP nebo webové aplikace díky QoS v přepínači v závislosti na typu zařízení či uživatele a jeho následné přidělení do VLAN, a to v závislosti na příslušnosti ve skupině třeba v Active Directory.

Možnosti systému jsou skutečně obrovské, záleží na potřebách společnosti. A dále - administrátoři jsou díky podpoře firewallů

a VPN schopni velmi pružně stanovovat podmínky nejen v LAN, ale i v distribuovaném Enterprise prostředí.

NSM systém je navržen hierarchicky, takže jej lze rozčlenit do regionálních serverů a následně korelovaná data z regionálních center zasílat do centrálního serveru k vyhodnocení. Třívrstvá architektura zvyšuje rychlost a flexibilitu správy. Technologie vychází ze známé platformy NetScreen-Security Manageru.

Součástí systému je nadále modul NetScreen statistical Report server, který archivuje a statisticky vyhodnocuje informace zasílané z aktivních prvků. Toto je důležité pro stanovení a následné zabezpečení sítě. Inventory management napomáhá efektivně řešit správu firmware, záplat a update všech systémů.

Přednosti technologie

- Značné snížení pořizovacích nákladů (hardware, licence, ale také školení), které díky unifikaci a široké podpoře systémů zefektivňuje práci celého IT oddělení společnosti.
- Značná úspora provozních nákladů díky časovým úsporám na stanovení příčiny problémů a jeho řešení. Ovládání systémů různých výrobců, sjednocení politik a odladění systémů je časově velmi náročné, v případě implementace nových aplikací a systémů se investice dále protahuje a finančně prodražuje.
- Rychlejší analýza, identifikace problému (ať již bezpečnostního incidentu či komunikačního charakteru) a řešení problému vede k rychlejšímu znovu zprovoznění provozovaných aplikací, což snižuje provozní ztráty.
- Celkové zvýšení úrovně komplexního zabezpečení serverů, aplikací i uživatelů, a to díky integračnímu charakteru managementu; v případě stanovení rizik je zajištěna jejich efektivní eliminace.
- Integrace více bezpečnostních technologií v rámci NSM vede ke sníženému riziku chybného či rozporného nastavení jednotlivých systémů a zrychluje implementaci a odladění sítě.
- Intuitivní grafické prostředí pro správu systémů prostřednictvím web prohlížeče

nevyžaduje instalaci a údržbu nastavbových software.

- Možnosti kustomizace hierarchicky řešeného managementu s ohledem na svěřené role umožňuje detailní delegaci práv pro správu definované skupiny prvků; NSM tak vyhoví potřebám každé společnosti.
- Vysoká spolehlivost a stabilita řešení díky podpoře HA designu pro maximální dostupnost (s plně automatizovanou synchronizací).
- Statistical report server umožňuje zobrazit řadu reportů ve čtyřech oblastech pokrývajících kompletní provoz skrze VPN zařízení a lze nastavit filtry pro různá zařízení sítě, skupinu zařízení nebo dle uvážení.

Otázkou tak není „jestli uvažovat o řešení a proč,“ ale kdy? Rozhodně ano v případě, že...

- Řešíte komplexně otázku bezpečnosti IT, s výhledem a zárukou otevřeně, na standardech ověřené platformě.
- Hodláte snížit celkové provozní náklady na bezpečnost a zabezpečení IT.
- Zamýšlíte implementaci NAC řešení, a to vzhledem k investicím i postupně.
- Konsolidujete systémy a v rámci redesignu sítě hodláte zajistit návaznost a integritu celého řešení.
- Zvažujete instalaci nové networking platformy z důvodu podpory bezpečnostních funkcí, anebo bezproblémového chodu nových služeb, VoIP.
- Požadujete z důvodu dostupnosti a stability přepínání na L3 nebo přechod k MPLS.
- Kapacitně chcete přejít na 10GE s přímou podporou bezpečnosti.
- Chcete být připraveni na váš růst či případné akvizice dalších společností.

Důvodů může být celá řada, rádi s vámi zkonzultujeme ty vaše.

Více informací naleznete na www.juniper.net