

Network and Security Manager 2008.2

centrální management - nové možnosti

Společnost Juniper Networks uvedla již před nějakým časem produkt Network and Security Manager 2008.1, který byl přelomový z pohledu podpory správy bezpečnostních a síťových produktů Juniper Networks. Nová verze 2008.2 tohoto produktu jde ještě dále a nabízí mnoho vylepšení a funkcí, o kterých bych rád mluvil v následujícím článku.



Je spousta důležitých věcí, které by měl dobrý dohledový systém poskytovat. Kromě samotného nastavení zařízení by určitě neměl chybět modul bezpečnosti, log manažer a neměla by chybět také rozsáhlá reportovací schopnost. Protože, získat informace včas, nám dává výhodu před útočníky a jinými potenciálními hrozbami.

Pokud mají být informace co nejpřesnější, je potřeba zapojit do reportingu co možná největší počet jak síťových, tak bezpečnostních prvků. Je jistě výhodou, že Juniper NSM pokrývá celou síťovou infrastrukturu. Ve verzi 2008.2 tudíž můžete počítat s těmito Juniper produkty:

- Firewall (SSG, ISG, NS řada založená na ScreenOS)
- Firewall (SRX řada založená na JUNOSe)
- Detektor průniku (IDP řada)
- SSL VPN brány (Secure Access řada)
- Network Access Control (Infranet Controller řada)
- Přepínače (EX, MX řada)
- Routery (J, M řada)

Každý z výše uvedených produktů má svůj neocenitelný význam v budování bezpečné sítě. Na to, aby se daly využít jejich propa-

cované schopnosti, je nutno se s nimi naučit spolupracovat co nejtěsněji. Do této verze byla přidána tato vylepšení:

Rozsáhlá správa verzí konfiguračních souborů zařízení

Tato volba umožňuje automaticky při importu smazat nejstarší verzi konfigurace v NSM a vy sami si také můžete počet předchozích verzí konfigurací nastavit. Přednastavená hodnota je 25 posledních verzí konfigurace. Toto je možno nastavit pro každou řadu prvků. U prvků s operačním systémem JUNOS je možno nastavit automatický import konfigurace v momentě, když napíšete příkaz Commit. Výhodou je možnost porovnávání verzí mezi sebou, kde pomocí jednoduchých filtrů vidíte jen části konfigurace, které byly změněny.

Komunikace se zařízením

Nyní je možno přidat všechna výše uvedená zařízení prostřednictvím uživatelského panelu bez nutnosti nejdříve iniciovat spojení ze zařízení samotného. NSM tak dokáže naimportovat i boxy, které mají dynamickou IP adresu.

Jelikož si NSM se zařízením vytvoří bezpečný tunel založený na SSP protokolu, dokáže tak i sledovat změny konfigurací na zařízení. V případě, že administrátor cokoliv změní například z Web konsoly, NSM upozorní správce hlášením „Device changed“. Toto se

děje dynamicky i v opačném směru, kde pro změnu upozorní správce na změnu NSM konfigurace hlášením „NSM changed“. Ideální je stav konfigurace „In sync“, kde víte, že máte jak konfiguraci v zařízení, tak konfiguraci v NSM naprosto shodné.

Komplexní ochrana před bezpečnostními hrozbami (UTM)

NSM integruje veškeré UTM funkce poskytované firewall prvky. Nyní se nainportují také profily vytvořené na zařízeních samotných a tyto profily je následně možno použít při vytváření globálních bezpečnostních pravidel v NSM.

- Antivirus Kaspersky
(Kompletní vlastnosti AV a Express AV)
- Antispam Symantec
(Kompletní správa Brightmail)
- URL filter SurfControl, WebSense
(Kompletní správa Black a White listů včetně obsahu)
- Content filtering
(Nastavení signatur)

Hledání zařízení v síti (Network discovery and mapping)

K tomuto úkolu je v NSM připraven tzv. Topology Manager, který dokáže pasivně vysledovat, kde se nachází jaké zařízení na síti a s kým si to zařízení povídá. Tuto funkci poskytují přepínače a routery založené na JUNOS operačním systému, ale také IDP, které detekují provoz, jenž přechází přes jejich porty v transparentním režimu. Topology Manager dokáže celou síťovou infrastrukturu zobrazit v grafické podobě a to pro každou doménu zvlášť. Jeho výhodou je také zobrazení koncových zařízení jako jsou počítače, tiskárny apod. včetně napojení na v NSM importované přepínače. Všechna zařízení si lze velmi jednoduše pojmenovat a přidat do adresní knihy NSM, kde je možno s nimi dále pracovat například v bezpečnostních politikách firewallů.

Pojmenování statických cest u ScreenOS zařízení, zde se nabízí možnost přidat kompletní komentář ke každé statické cestě.

Restart zařízení z centrálního managementu
NSM nabízel do této chvíle hromadný restart

pouze prvků založených na ScreeOS nebo IDP zařízení. Od verze 2008.2 je tak možno restartovat i boxy s operačním systémem JUNOS. Velmi snadno tak lze restartovat stovky zařízení najednou např. po hromadné změně operačních systémů zařízení.

Sledování provozu dle provozovaných aplikací

Už dlouhou dobu se volalo po tom, aby bylo možno sledovat výměnu informací mezi uživateli sítě rozdělenou do jednotlivých aplikací. V této nové verzi NSM je připraveno několik zásadních vylepšení pro takovéto monitorování.

Application Policy Enforcement pravidla (APE)

Na základě aplikačních signatur je schopno každé IDP/ISG poznat o jakou aplikaci se jedná a uplatnit na takovýto provoz představené pravidlo. Toto pravidlo může vyvolat akci v případě, kdy se například z jedné adresy přenesou po P2P síti větší objem dat, než je přípustné. Takto lze provoz buď úplně zakázat, omezit jej šířkou pásma, nebo dát provozu v rámci pravidel nejnižší prioritu.

Koordinovaná konfigurace UAC zařízení a EX přepínačů

Každý centrální prvek, řídicí bezpečnou komunikaci na úrovni LAN musí spolupracovat s 802.1x přepínači a access pointy. Jen takto, pomocí radius knihoven, lze efektivně řídit přístup koncových stanic do sítě přiřazením do patřičné VLAN apod. Většinou se tak děje dle příslušnosti skupiny přístupových prvků k nějaké lokalitě např. „kanceláře Praha“. Tuto skupinu včetně nadřazeného UAC zařízení lze velmi jednoduše prostřednictvím NSM spravovat. Vždy vidíte, který port přístupového bodu je napojen na jakou roli v UAC a kdo je právě připojen včetně jeho přihlašovacího jména. Toto schéma lze velmi jednoduše aplikovat i na zařízení bez možnosti správy jako jsou tiskárny, IP kamery apod. V případě, že budete využívat ve své struktuře zařízení IDP, můžete toto napojit na UAC prvek a díky vzájemné komunikaci mezi těmito technologiemi pak například vysledovat kdo používá jaké aplikace, a které soubory si navzájem uživatelé sítě vyměnili.

Vylepšení správy aplikace vzorů konfigurací na EX- přepínačích

Díky možnosti vytvářet vzory, ať už sami nebo z nainportovaných konfigurací, je možno tyto vzory následně aplikovat na jednotlivé přepínače v síti. Tím můžete docílit jednotnosti v nastavení VLAN, access listů na portech apod. Díky tzv. Delta konfiguraci máte možnost porovnávat právě běžící konfiguraci na zařízení s tou, kterou do zařízení hodláte nahrát z NSM. Tak máte možnost se rozhodnout, které nastavení je pro vás důležitější.

Správa zařízení v konfiguraci HA (vysoká dostupnost)

Nyní je možno spravovat zařízení v tzv. clusteru Active/Passive nebo Active/Active z prostředí NSM také pro platformy založené na JUNOS operačním systému jako jsou SRX firewally.

Konfigurační skupiny

Skupiny prvků s operačním systémem JUNOS lze od této chvíle provozovat v tzv. konfiguračních skupinách. Výhodou je jednotné a hromadné nastavení funkcí pro SRX, EX, MX, M a J řadu. Tato funkce dovoluje replikaci parametrů všech nastavení v rámci JUNOS operačního systému.

Správa logů

Log manager je od verze 2008.2 vybaven dalšími předdefinovanými filtry pro získání podrobných informací z jednotlivých importovaných platform a jejich následný reporting.

Výše jsem uvedl jen několik základních důležitých vylepšení z rozsáhlé skupiny připravené v Network and Security Manageru 2008.2. Tento produkt se tak stává velmi silným nástrojem pro správu kompletního síťového a bezpečnostního portfolia Juniper Networks a my na něj můžeme být právem hrdí.

Více informací naleznete na www.juniper.net