

nr 1/2011

Securariusz

IT Systems Security

Junos Pulse - dla Twojego telefonu

Ethernet jest dobry na wszystko, czyli Fibre Channel Over Ethernet

Rewolucja w pamięciach masowych - IBM Storwize V7000



ASCOMP
IT INTEGRATOR

IBM Storwize

INNOWACYJNA FUNKCJONALNOŚĆ KLASY ENTERPRISE W CENIE KLASY ŚREDNIEJ



SPIS TREŚCI

4. Drodzy Czytelnicy...
5. Nowoczesne zarządzanie infrastrukturą IT – IBM Systems Director 6.2
6. Porównanie systemów UTM z najnowszymi urządzeniami NGF
8. JUNOS PULSE – dla twojego telefonu
10. Nowoczesne rozwiązania komunikacyjne na przykładzie platformy VoipSwitch
13. Rewolucja w pamięciach masowych IBM Storwize V7000
16. Ethernet jest dobry na wszystko, czyli Fibre Channel over Ethernet
18. Nowa koncepcja zarządzania siecią – JUNOS SPACE
20. Wirtualizacja zasobów
22. Wirtualizacja środowiska serwerowego
24. Sieć od zera, czyli integracja rozwiązań Juniper Networks i Meru Networks
26. System dyskowy EntryLevel IBM DS 3500
26. Seria serwerów Enterprise IBM eX5
26. JUNOS 10.4
27. Zestawy promocyjne JUNIPER MX80
27. VIRTUAL CHASSIS dla przełączników EX 8200
27. Poszerzamy rodzinę SRX
27. Juniper Enterprise Guest Access
8. JUNOS PULSE – DLA TWOJEGO TELEFONU
¶ Niezależnie od tego, czy dany wachlarz rozwiązań pochodzi od jednego producenta, czy też od kilku, firmy zmagają się z problemem zarządzania, wdrażania i utrzymywania oddzielnego klienta programowego właściwego dla każdego produktu. ¶
13. REWOLUCJA W PAMIĘCIACH MASOWYCH - IBM STORWIZE V7000
¶ Macierz StorWize V7000, swoją budową i funkcjonalnością jest w stanie skutecznie powalczyć z rosnącymi problemami na rynku pamięci masowych. ¶
16. ETHERNET JEST DOBRY NA WSZYSTKO, CZYLI FIBRE CHANNEL OVER ETHERNET
¶ Okazało się, że Ethernet, pomimo wszystkich swoich ograniczeń (braku gwarancji dostarczenia danych, zmiennego opóźnienia), z powodzeniem może służyć do transmisji głosu. Dlatego też podjęte zostały kroki, by w ramach ethernetowych enkapsulować ruch Fibre Channel. ¶



autor: Przemysław Sternadel
e-mail: p.sternadel@ascomp.eu

NAJDŁUŻSZY KARNAWAŁ

Andrzej Szymowski/ Prezes Zarządu ASCOMP S.A.

Drodzy, Kochani i Wierni Czytelnicy. W tym roku mamy najdłuższy chyba w historii nowożytny karnawał. Święta Wielkiej Nocy wypadają 24 kwietnia, a w następną po nich niedzielę – 1 maja – zaplanowana jest beatyfikacja Jana Pawła II. I tak się stanie, że w najbardziej lewackie święto zostanie wyniesiony na ołtarze człowiek, który zdecydowanie przyczynił się do upadku komunizmu. I to będzie SuperChichot historii. Albo druga część karnawału.

Ale wróćmy do normalnego karnawału. To czas radości, szalonej zabawy, wytwornych balów nie tylko wiedeńsko-krakowskich, czas gorących rytmów i tancerek brazylijskich. Cieszymy się i my. Po bardzo intensywnym roku 2010 należy się nam wszystkim zabawa w rytm szalonej samby.

Kiedyś arcymity Naczelnik Wydziału Informatyki Dużego Miasta powiedział mi tak: „za to Panu płacimy, żebyś puścił Pan wodze wyobraźni”. No to wyznaczmy sobie kierunek i ... „puszczajmy”.

Załóżmy, że przyjdzie taki dzień, kiedy każdy w Polsce ma podłączony światłowód do domu i astronomiczną prędkość dostępu. I co? ... No właśnie – i co?

Po pierwsze – najpewniej wszyscy dalej na coś narzekają (taka przypadłość i tradycja narodowa, że nawet wygrana w totka jest nieszczęściem, bo trzeba pieniądze na coś wydać...)

Po drugie – tylko mniejszość korzysta z tego elektronicznego raj. I teraz, jako urodzony optymista, włączam radosne proroctwo...

Mam telewizję IP. Zamiast oglądać dziennik telewizyjny oglądam tylko dobre wiadomości, oglądam tylko ulubiony sport, oglądam tylko to, co mnie interesuje (to nie jest odkrywca) i tylko wtedy, kiedy mam czas i ochotę. Google przechowują dla mnie wszystkie programy telewizyjne, które kiedykolwiek wyemitowano i podają mi je (za darmo), jak na tacy.

W tym miejscu odstąpię Wam trochę mojej prywatności. Ponieważ karnawał jest nierozłączny

z gorącymi tańcami... to i ja tańczę brazylijską sambę. Taką najbardziej „czadową”. Pełną stońca, chili i kawy. Tak jest i dzisiaj, za sprawą artykułu o IBM Storwize V7000. Jestem pewien, że wszyscy, którzy mają do czynienia z macierzami, czekali na takie ułatwienia i możliwości. Amerykanie wtedy mówią, że produkt jest „hot” albo nawet „sexy”. To dla Ciebie, Kochany Czytelniku, z absolutną rekomendacją do przeczytania minimum dwa razy. Pozostałe teksty też szczerze polecam.

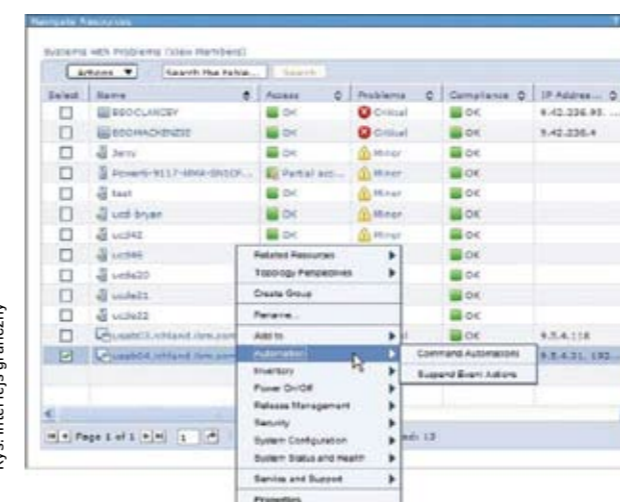
Internet i technologia mi jednak nie wystarczą. Mam takie marzenie, aby co roku jeździć na dwa tygodnie do Rio... na najbardziej słoneczny karnawał świata, bo... lekarz mi zalecił zwiększyć aktywność fizyczną. Chcę jechać do Rio i mam nadzieję spotkać tam Ciebie, mój Kochany Czytelniku. Ocenisz sam moją czadową sambę.

Wasz Cenzor Naczelnik
Andrzej Szymowski

NOWOCZESNE ZARZĄDZANIE INFRASTRUKTURĄ IT IBM SYSTEMS DIRECTOR 6.2

W dobie szybko rosnących środowisk informatycznych szczególne znaczenie ma odpowiedni wybór oprogramowania do zarządzania. W dzisiejszym artykule chciałbym przybliżyć rozwiązanie, które służy do zarządzania środowiskiem serwowym różnych producentów oraz jego monitorowania.

Przede wszystkim ważne jest to, że oprogramowanie jest darmowe. Dostajemy je wraz z zakupem każdego serwera IBM (x86, IBM POWER). Płatne są natomiast dodatkowe wtyczki, o których więcej w tym artykule. Jak już wspomniałem, Systems Director może monitorować i zarządzać serwerami IBM (zaszyty agent) oraz serwerami innych producentów



Rys. Interfejs graficzny

(wymagana instalacja agenta w systemie operacyjnym). Zarządzanie opiera się w całości na przeglądarce WWW, co sprawia, że dostęp jak i sam interfejs jest bardzo prosty i intuicyjny.

Główną funkcją jest identyfikowanie obiektów za pomocą przeszukiwania wskazanej puli adresacji IP. Każdy adres, z którym aplikacja się skomunikuje, zostanie wciągnięty na listę urządzeń i – o ile będzie to możliwe – zostaną wyświetlone szczegółowe informacje na jego temat. Po wykryciu obiektów w naszym środowisku możemy zacząć nimi administrować. Jedną z ważniejszych cech dla administratorów infrastruktury jest monitorowanie obiektów. Statusy mogą być zbierane zarówno z maszyn fizycznych, jak i wirtualnych. Jest kilka sposobów monitorowania obiektów. Jednym z nich jest określenie wskaźników i przypięcie ich do danego urządzenia. Wyniki monitoringu mogą znaleźć się w czytelnej tabeli lub zostać zaprezentowane w formie graficznej – na wykresie. Jeśli zdecydujemy się zainstalować w systemie operacyjnym agenta Systems Director, uzyskamy

bardziej szczegółowe dane. I tak na przykład administrator będzie mógł monitorować procesy systemowe, nadawać im priorytety, czy chociażby zatrzymywać i uruchamiać dany proces. Dzięki takiej funkcjonalności mamy możliwość nie tylko wczesnego wykrywania awarii, ale również określania trendów wykorzystania zasobów i tworzenia szczegółowych raportów z danego okresu.

Director może również automatyzować określone zadania. W takim wypadku korzystamy z predefiniowanych ustawień lub określamy własne. Załóżmy, że administrator chciałby zostać powiadomiony drogą mailową, jeśli wykorzystanie pamięci RAM przekroczy 80% na danym serwerze. Nic trudnego! Z menu Automation za pomocą kreatora definiujemy interesujące nas zadanie, określamy ramy czasowe oraz osoby, które mają być powiadamiane w razie wystąpienia tych szczególnych warunków.

Zakup wtyczki o nazwie Active Energy Manager pozwala na zarządzanie energią elektryczną w naszym środowisku serwowym. Oprócz standardowego monitoringu i możliwości tworzenia raportów na temat zużycia energii możemy tworzyć zadania, które obniżą koszty związane z utrzymaniem infrastruktury. Do tego celu służy zadanie ograniczające pobór energii w godzinach, kiedy aplikacje nie są wykorzystywane, co pozwala zmniejszyć realne koszty utrzymania sprzętu.

Kolejną dodatkową wtyczką do prezentowanego oprogramowania jest IBM BladeCenter Open Fabric Manager. Pozwala ona zdefiniować zadanie, które umożliwi automatyczne uruchomienie systemu operacyjnego na dodatkowym serwerze kasetowym w wypadku awarii serwera podstawowego. Co ciekawe, możemy określić jeden taki serwer dla wielu klatek BladeCenter.

Interesującym dodatkiem jest też darmowa wtyczka, IBM Service and Support Manager, pozwalająca na raportowanie o błędach bezpośrednio do pomocy technicznej IBM. Do producenta wysyłane są tylko statusy (z wykorzystaniem protokołu HTTPS), które mają związek ze sprzętem czy systemem operacyjnym. Nie ma więc obaw, że poufne dane klienta dostaną się w niepowołane ręce.

W artykule zostały przedstawione tylko podstawowe zalety oprogramowania IBM Systems Director 6.2. Dodając kolejne wtyczki do zarządzania macierzami dyskowymi czy środowiskiem wirtualnym, w prosty sposób możemy zwiększyć jego funkcjonalność. ■

PORÓWNANIE SYSTEMÓW UTM Z NAJNOWSZYMI URZĄDZENIAMI NGF



autor: Michał Putała
e-mail: m.putala@ascomp.eu

Jeśli przyjrzymy się materiałom poszczególnych producentów, najczęściej znajdziemy tam informację o przepustowości tylko i wyłącznie dla inspekcji firewall. W praktyce okazuje się, że przy włączonych pozostałych modułach z zaimplementowanymi regułami skanowania wydajność ta spada nawet kilkudziesięciokrotnie!



Szukając informacji o rozwiązaniach bezpieczeństwa sieciowego, bardzo często można spotkać się z dwoma terminami: UTM oraz od niedawna NGF. Co tak właściwie te dwa skróty oznaczają? Jakie mają znaczenie dla klientów? Czym się kierować przy wyborze odpowiedniego rozwiązania? W artykule postaram się przedstawić główne różnice pomiędzy poszczególnymi systemami oraz odpowiedzieć na te i na inne pytania, które mogą się pojawić w procesie doboru optymalnego rozwiązania.

Cofnijmy się do początku XXI wieku, kiedy to systemy UTM na dobre zagościły na rynku i spotykały się z coraz większym zainteresowaniem ze strony klientów. W tym czasie każdy czołowy producent rozwiązań bezpieczeństwa posiadał w swojej ofercie dedykowane rozwiązania sprzętowe do realizowania funkcji firewalla pełnostanowego służącego do separacji sieci w środowisku klienta. Do najczęściej wykorzystywanej funkcji tych systemów należała oczywiście separacja sieci LAN od Internetu, i to właśnie w tej drugiej sieci pojawił się problem, z którym zwykłe firewalle nie były w stanie się uporać. Mowa tutaj o wysypie wirusów, robaków czy ataków w warstwie aplikacyjnej, które musiały w jakiś sposób zostać zaadresowane. Istniejące systemy dedykowanej ochrony IPS czy Gateway AV były poza zasięgiem finansowym większości klientów, stąd bardzo szybko pojawił się pomysł zunifikowania wielu funkcji bezpieczeństwa w istniejących rozwiązaniach firewall.

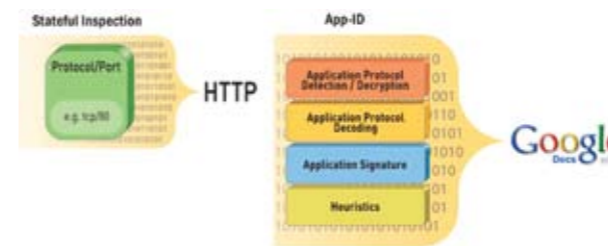
Nowo powstałe urządzenia zostały nazwane systemami UTM (Unified Threat Management) i obok funkcjonalności firewall zyskały spore możliwości skanowania ruchu silnikiem antywirusowym, wykrywania ataków IPS czy filtrowania stron internetowych. Wszystko to realizowane na pojedynczym urządzeniu, zarządzane w jednym miejscu ze spójnego interfejsu i po bardzo atrakcyjnej cenie.

Wobec tych zalet nie dziwi wielka popularność tego typu urządzeń – ale czy faktycznie pozbawione są wad? Aby odpowiedzieć na to pytanie, należy zagłębić się w warstwę samego systemu operacyjnego pracującego na tych urządzeniach. Niezależnie od producenta, niegdyś dedykowane systemy realizujące pojedynczą funkcjonalność firewall/VPN (wraz z NAT-em i QoS) zostały wzbogacone o dodatkowe moduły inspekcji odpowiedzialne za przetwarzanie ruchu w warstwie aplikacyjnej i wymieniające pomiędzy sobą informacje. Takie podejście, wynikające z zaszłości historycznych, powoduje wydłużenie drogi każdego pakietu trafiającego na urządzenie i przesyłanie go pomiędzy poszczególnymi modułami inspekcji, co oczywiście odbija się na wydajności tych rozwiązań. Sytuację częściowo ratują dedykowane układy sprzętowe do realizacji poszczególnych funkcji. Jednak jeśli przyjrzymy się materiałom poszczególnych producentów, najczęściej znajdziemy tam informację o przepustowości tylko i wyłącznie dla inspekcji firewall. W praktyce okazuje się, że przy włączonych pozostałych modułach z zaimplementowanymi regułami skanowania wydajność ta spada nawet kilkudziesięciokrotnie! Tak duża degradacja wydajności determinuje wykorzystanie systemów UTM jedynie w miejscach brzegowych dostępu do Internetu, gdzie nie jest oczekiwana zbyt duża wydajność. W większości przypadków urządzenia te nie poradzą sobie z pełnym skanowaniem ruchu w sieciach wewnętrznych.

Co w takim razie z urządzeniami NGF? Czyżby miały się okazać urządzeniami UTM pozbawionymi powyższych wad wydajnościowych? Niestety odpowiedź na to pytanie nie jest tak prosta. Wszystko zależy od poszczególnych implementacji systemu NGF przez danego producenta. Ale po kolei...

U podstaw powstania platformy NGF (Next Generation Firewall) leżało przekonanie o tym, że filtracja adresów IP i portów to znacznie za mało z uwagi na specyficzny ruch wielu niebezpiecznych aplikacji, które potrafią się tunelować w zawsze otwartych portach 80 i 443 na firewallu. W firmie PaloAlto zrodził się zatem pomysł, aby na firewallu zaimplementować możliwość rozpoznawania aplikacji i filtrowania ruchu właśnie na tym poziomie, niezależnie od portu czy serwisu, a nie na sieciowym, jak to się odbywało dotychczas. Oznaczało to konieczność uruchomienia jeszcze jednej dodatkowej funkcji. Pamiętając o problemach wydajnościowych platform UTM, producenci pierwszego historycznie urządzenia NGF zaprojektowali system operacyjny wraz z pojedynczym modułem inspekcji (dla funkcji AV, IPS, AntySpyware, URL Filtering, Data Filtering) ze zunifikowaną bazą dla zagrożeń AV, IPS i AntySpyware. Takie podejście zapobiegło wydłużonej drodze przejścia pakietu przez urządzenie i jednocześnie zminimalizowało degradację wydajnościową. Dodatkowo na firewallu poszczególne funkcje zostały przypisane dedykowanym układom sprzętowym, począwszy od specjalizowanych procesorów sieciowych, a skończywszy na programowalnych układach

Rys. Stateful vs. Application firewall.



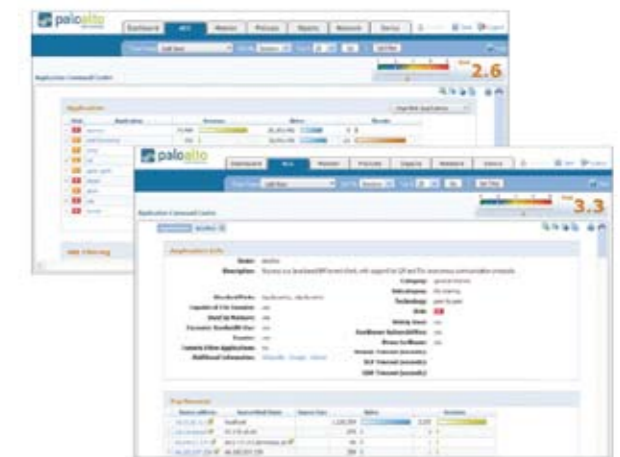
FPGA odpytujących pojedynczą bazę sygnatur (dokładny opis technologii znajduje się w „Securiuszu” nr 17).

Dzięki temu system NGF od 2007 roku realizuje proces wykrywania i filtrowania aplikacji z niespotykaną dotąd wydajnością aż do 10 Gbps (w planach na rok 2011 znajduje się model o przepustowości 20 Gbps). Przy włączonych pozostałych funkcjach wydajność systemu spada około dwukrotnie.

Niestety takie podejście w implementacji systemów NGF nie stało się standardem i wielu producentów postanowiło wykorzystać starą rodzinę rozwiązań UTM do realizacji zwiększonego zakresu funkcji. Pomijając problemy wydajnościowe tego rodzaju platform, należy podkreślić kilka głównych różnic pomiędzy takimi urządzeniami a prawdziwymi systemami NGF. Przede wszystkim urządzenia te w dalszym ciągu pozostają firewallami pełnostanowymi, gdzie regułę FW tworzy się per serwis/numer portu. Dopiero dodatkowy moduł, uruchomiony na bazie modułu IPS (jego uruchomienie wiąże się ze znaczną degradacją wydajności), pozwala na wyszukiwanie aplikacji w ruchu przepuszczonym przez firewalla. Polityka w takim systemie pozwala nam na wybranie aplikacji, które mają zostać zablokowane dopiero po zdefiniowaniu aplikacji dozwolonych. W prawdziwym systemie NGF oprócz takiego podejścia (dość niewygodnego

z uwagi na złożoność reguł) możliwe jest zdefiniowanie ruchu dozwolonego i zablokowanie ruchu pozostałego (zgodnie z zasadą Least Privilege). Dodatkowo często brakuje zaawansowanych funkcji kontroli aplikacji, takich jak kontrola pasma przydzielonego dla konkretnej aplikacji czy kontrola jej poszczególnych funkcji (np. Facebook chat, gry itd.) Poza tym w systemach UTM albo nie ma funkcjonalność deszyfracji ruchu SSL, albo jest ona niepełna i nie pozwala na zablokowanie aplikacji bądź ataków client-side tunelowanych w zaszyfowanym protokole SSL. Do pozostałych różnic funkcjonalnych należą możliwości wizualizacji ruchu aplikacyjnego na pojedynczej platformie NGF. W przypadku urządzeń udających systemy NGF możliwości tego typu są mocno ograniczone i nie są w stanie uwidocznic administratorom obecności szkodliwych aplikacji w ich sieci.

Podsumowując: rozwiązania NGF oferują znacznie większą funkcjonalność od urządzeń UTM z zachowaniem bardzo wysokiej wydajności. Jednak należy uważać w doborze rozwiązania NGF, aby nie natknąć się na urządzenie UTM, które jedynie w warstwie marketingowej przypomina swoimi założeniami systemy Next Generation Firewall. ■



Rys. Application Command Center w firewallu PaloAlto

Kluczowe funkcjonalności systemu NGF na przykładzie urządzenia firmy PaloAlto:

- Podstawowe funkcje: firewall poziomu aplikacji, IPS, AV, AntySpyware, URL Filtering, Data Filtering.
- Możliwości jednoznacznej identyfikacji aplikacji niezależnie od użytego portu, protokołu, technik ukrywania czy szyfrowania SSL.
- Wysoki poziom szczegółowości w definiowaniu polityk opartych na aplikacjach i ich funkcjach.
- Identyfikacja tożsamości użytkownika i wykorzystanie jej jako atrybutu w politykach bezpieczeństwa.
- Ochrona w czasie rzeczywistym przed szeroką gamą zagrożeń w warstwie aplikacyjnej.
- Bardzo rozbudowane logowanie i raportowanie wykorzystanych aplikacji oraz wykrytych incydentów.
- Wielogigabitowa przepustowość systemu w trybie in-line.

JUNOS PULSE – DLA TWOJEGO TELEFONU

autor: Michał Putała
e-mail: m.putala@ascomp.eu



Rys. Telefon z systemem Android.

Liczba użytkowników mobilnych korzystających z całej gamy dostępnych urządzeń przenośnych stale rośnie. Firmy chcące udostępnić swoje zasoby wewnętrzne stanęły więc przed sporym wyzwaniem polegającym na pogodzeniu interesów użytkowników z dotychczas wdrożonym bądź planowanym poziomem bezpieczeństwa. Aby zapewnić szybki i bezpieczny dostęp do swoich zasobów korporacyjnych z dowolnego miejsca, wiele firm rozważa bądź wdraża rozwiązania SSL VPN zdalnego dostępu, kontrolę dostępu do sieci (NAC), akcelerację łącz WAN oraz zabezpieczenie stacji końcowych. Niezależnie od tego, czy dany wachlarz rozwiązań pochodzi od jednego producenta, czy też od kilku, firmy zmagają się z problemem zarządzania, wdrażania i utrzymywania oddzielnego klienta programowego właściwego dla każdego produktu. Wszystko to prowadzić może do wyższych kosztów samej obsługi oraz zwiększa ryzyko implementacji projektu w warunkach rzeczywistych, np. wskutek niepoprawnej współpracy poszczególnych

komponentów bądź zbyt dużych wymagań sprzętowych stawianych poszczególnym urządzeniom mobilnym.

„ Niezależnie od tego, czy dany wachlarz rozwiązań pochodzi od jednego producenta, czy też od kilku, firmy zmagają się z problemem zarządzania, wdrażania i utrzymywania oddzielnego klienta programowego właściwego dla każdego produktu. ”

Aby sprostać tym wymaganiom, firma Juniper Networks opracowała wielozadaniowego agenta Junos Pulse przeznaczonego na platformy mobilne. Agent zapewnia przede wszystkim połączeniowość z zasobami korporacyjnymi, akcelerację połączenia oraz bezpieczeństwo przy jednoczesnym maksymalnym uproszczeniu obsługi z poziomu użytkownika. Korzystając z agenta, wystarczy go uruchomić, wpisać dane potrzebne do uwierzytelnienia i cała reszta zostanie automatycznie zrealizowana przez Junos Pulse, który jest jedynym agentem potrzebnym do wdrożenia! Prawda, że proste ?



Rys. Funkcje ochrony Junos Pulse.

W zależności od lokalizacji użytkownika (ustalanej na podstawie np. skonfigurowanego lokalnie serwera DNS) zestawiana jest lokalna bądź zdalna sesja. Podczas dostępu zdalnego Pulse, rozpoznając lokalizację, prosi użytkownika o podanie swoich danych do logowania (hasło, certyfikat) i przekazuje je do odpowiedniego urządzenia Juniper Secure Access SSL/VPN. Kiedy ten sam użytkownik znajdzie

się wewnątrz sieci korporacyjnej, jego zdalna sesja jest przezroczyście przeniesiona do urządzenia Infranet Controller UAC. Jeżeli do zestawienia nowego połączenia wymagane jest jakieś inne oprogramowanie czy dodatek, Pulse także i w tym momencie wyłącza użytkownika, pobierając i instalując potrzebny komponent.

Junos Pulse jest agentem dedykowanym dla kilku rozwiązań bezpieczeństwa firmy Juniper Networks: koncentratorów SSL/VPN, systemu NAC (UAC), Sprzętowego FW JUNOS (dla funkcji Dynamic VPN) oraz rozwiązań akceleracji łącz WAN. Funkcjonalnie odpowiada dedykowanym agentom dostarczonym standardowo w ramach wymienionych rozwiązań bezpieczeństwa i optymalizacji sieciowej. Dodatkowo platforma Pulse pozwala na wykorzystywanie oprogramowania firm trzecich skanujących stacje klienckie różnymi technologiami bezpieczeństwa, np. modułów antyspyware i antymalware firmy WebRoot. ■

Wybrane funkcje:

Proaktywna ochrona przed kodem malware	Ochrona wiadomości e-mail, SMS-ów, MMS-ów, bezpośrednio pobieranych danych, transmisji bluetooth i infrared.
Personal Firewall	Filtrowanie i blokowanie ruchu TCP/IP z pełną kontrolą mechanizmu alarmowania i blokowania.
AntySpam	Biała i czarna lista adresów oraz numerów telefonów (np. automatyczne odrzucanie rozmów z niechcianych numerów). Możliwość kasowania lub umieszczenia spamu w zadanym folderze.
Ochrona po kradzieży urządzenia	Zdalny backup i odtworzenie danych na nowym urządzeniu, zdalne śledzenie pozycji GPS, blokowanie urządzenia, kasowanie danych firmowych, alarmowanie o zmianie karty SIM i automatyczne reagowanie.
Kontrola i monitoring aplikacji	Administracyjny podgląd zainstalowanego oprogramowania, czarna lista aplikacji, monitorowanie zawartości SMS, MMS, e-mail, dziennika rozmów i kontaktów, podgląd zdjęć.
Zarządzanie	Dostępne jako SaaS (Software as a Service) w postaci konsoli zarządzającej udostępnionej przez SSL w data center firmy Juniper Networks.

„ Podczas dostępu zdalnego Pulse, rozpoznając lokalizację, prosi użytkownika o podanie swoich danych do logowania (hasło, certyfikat) i przekazuje je do odpowiedniego urządzenia. ”

Smartphones Supported with Junos Pulse Mobile Security Suite

JUNOS PULSE MOBILE SECURITY FEATURE	APPLE/iPHONE IOS 4.1 (EXACT RELEASE VERSION IS TO BE DETERMINED)	GOOGLE ANDROID 2.2, 2.1.2	WINDOWS MOBILE 6.0, 6.1, 6.5	NOKIA/SYMBIAN/S60/S90/S95	BLACKBERRY 4.1 AND BEYOND
VPN to the SA Series SSL VPN Appliances	✓	✓	✓	✓	Web Access only
Antivirus	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓
Antispam	✓	✓	✓	✓	✓
Monitor and Control	✓	✓	✓	✓	✓
Backup and Restore	✓	✓	✓	✓	✓
Loss and Theft Protection	✓	✓	✓	✓	✓

NOWOCZESNE ROZWIĄZANIA KOMUNIKACYJNE NA PRZYKŁADZIE PLATFORMY VoipSwitch



autor: Ewa Śniechowska
e-mail: e.sniechowska@ascomp.eu

Ostatnie lata upłynęły pod znakiem ogromnego rozwoju i popularyzacji systemów komunikacyjnych, w tym telefonicznych, wykorzystujących sieć jako medium transmisyjne. Dzięki łatwości implementacji, dużej elastyczności oraz szeregowi nowych możliwości, oferowanych przez systemy typu IP PBX oraz VoIP, zastępują one tradycyjne systemy telefoniczne oraz PBX. Co więcej, dotychczasowe ograniczenia do konieczności stosowania telefonów stacjonarnych zostały zniesione dzięki zastosowaniu Voice over WLAN, który wykorzystując do transmisji głosu sieć bezprzewodową, daje użytkownikom mobilnym dostęp do korzyści płynących z VoIP. Do kompletnych rozwiązań dostępnych na rynku należy platforma VoipSwitch posiadająca wszystkie elementy wymagane do tego, aby skutecznie wdrożyć pełny zakres usług VoIP.

Platforma VoipSwitch

W rozwiązaniu VoipSwitch uwzględnione zostały wszystkie kluczowe elementy niezbędne do wdrożenia kompletnego systemu Voice over IP. Architektura systemu składa się z części software'owej oraz serwerów, na których zainstalowana jest platforma.

Główny element platformy stanowi softswitch – centralne urządzenie w sieci telekomunikacyjnej, które łączy rozmowy z jednej linii telefonicznej do drugiej, w całości przy pomocy oprogramowania zainstalowanego w systemie komputerowym. Softswitch łączy w sobie funkcje następujących elementów architektury VoIP: SIP Registrar, SIP Proxy, przełącznik H.323, H.323 gatekeeper, bramka SMS. Softswitch zapewnia wsparcie dla protokołów SIP oraz H.323, z uwzględnieniem dwukierunkowej translacji adresów NAT dla obydwu protokołów. Wspierane są również wewnętrzne wirtualne prefiksy, co pozwala tworzyć odrębne plany wybierania dla różnych grup użytkowników. Zapewniona jest również pełna kompatybilność ze standardowymi urządzeniami VoIP, takimi jak bramy, przełączniki, ATA czy też terminale.

Platforma VoipSwitch zapewnia elastyczne metody zmian konfiguracji transmisji danych – możliwe są zarówno zmiany wybranych numerów, import i eksport kont użytkowników oraz planów wybierania z i do programu Excel lub pliku TXT. W systemie zaimplementowany jest również zaawansowany algorytm dbający o to, aby ruch VoIP w sieci rozmieszczany był równomiernie, przy uwzględnieniu nadanych priorytetów, co zapewnia podział obciążenia. Wprowadzono również możliwość nagrywania rozmów jako usługi wewnętrznej lub pracującej na dedykowanym hostie z lustrzanym portem Ethernet na przełączniku sieciowym.

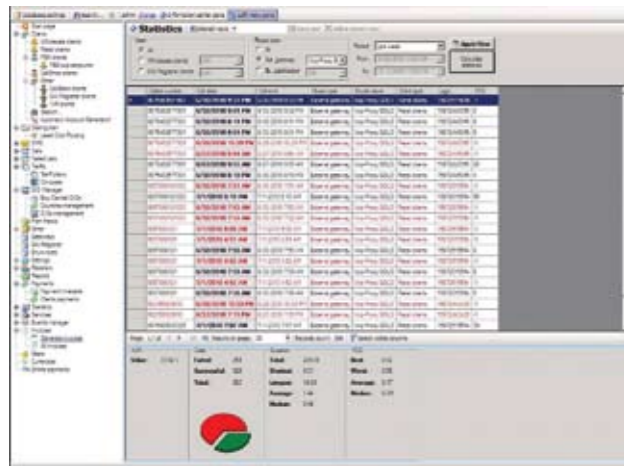
Zarządzanie oraz system billingowy

VoipSwitch umożliwia zarządzanie, blokowanie oraz ustalanie limitów zarówno dla poszczególnych użytkowników, jak i dla całych grup kont. Generowane są sprawozdania z płatności, faktury oraz szczegółowe raporty historii połączeń, dostępne poprzez interfejs WWW lub przesyłane w formacie PDF za pomocą poczty elektronicznej. Umożliwia to bieżącą kontrolę kosztów. Wszystkie informacje o kontaktach oraz dane rozliczeniowe przechowywane są w bazie danych SQL.

System billingowy jest w pełni zintegrowany z silnikiem softswitch w jednej aplikacji, co czyni system wyjątkowo skutecznym, ponieważ wykorzystuje on wewnętrzne procedury rozliczeń bez konieczności łączenia się z systemami zewnętrznymi. Ponadto takie podejście umożliwia zarządzanie całością systemu poprzez jeden interfejs graficzny – VoipSwitch Manager (VSM).

Platforma VoipSwitch posiada wszystkie elementy wymagane do tego, aby skutecznie wdrożyć pełny zakres usług VoIP.





Dialery

Aby umożliwić użytkownikom wygodne korzystanie z systemu, wraz z platformą oferowane są zarówno dialery przeznaczone do instalacji na komputerach, jak i dialery na telefony komórkowe. Dialery typu PC2Phone są kompatybilne z systemami operacyjnymi Microsoft Windows XP, Vista, 7 oraz z systemami serwerowymi. Wspierają najważniejsze kodeki VoIP, w tym G729, G711 i G723.1. Występują w trzech wersjach: Siplink, Vippie! Standard, Vippie! Extended. Oferują takie funkcjonalności jak historia połączeń wraz z ostatnio wybranymi numerami, nagrywanie rozmów, oczekiwanie na połączenia i ich przekazywanie, książka adresowa z możliwością synchronizacji z programem Microsoft Outlook. Możliwe są również: wysyłanie wiadomości SMS, rozmowy tekstowe poprzez komunikator (Instant Messaging) oraz wykonywanie połączeń konferencyjnych. Z kolei Vippie Mobile to dialery dające użytkownikom telefonów komórkowych możliwość wykonywania połączeń przy wykorzystaniu VoIP, co w znaczący sposób wpływa na obniżenie kosztów prowadzonych rozmów. Aplikacja typu softphone jest dostępna dla telefonów iPhone i BlackBerry, oraz modeli z systemami operacyjnymi Google Android, Windows Mobile i Symbian.

VoipSwitch jako centrala IP PBX

IP PBX jest rozwiązaniem przeznaczonym dla szerokiego zakresu odbiorców: od osób prowadzących własną działalność gospodarczą, poprzez niewielkie firmy z kilkoma pracownikami, do przedsiębiorstw posiadających zdalne oddziały oraz zaawansowaną strukturę organizacyjną. Każda centrala IP PBX daje możliwość swobodnego wybierania numerów wewnętrznych, które ważne są jedynie wśród rozszerzeń SIP danej firmy.

Wszelkie koszty połączeń wykonywanych przez użytkowników są rozliczane w ramach głównego konta firmy (konto IP PBX).

System Voice over WLAN



Do pełnego wykorzystania funkcjonalności platformy VoipSwitch potrzebna jest sieć bezprzewodowa o architekturze zoptymalizowanej pod kątem aplikacji głosowych, jaką gwarantują rozwiązania Meru Networks.

Dzięki technologii Virtual Cell punkty dostępowe mogą pracować na jednym kanale, co zapewnia natychmiastowe przełączanie pomiędzy nimi. Proces roamingu jest ciągły i niezauważalny dla użytkownika prowadzącego rozmowę, nie ma zagrożenia zawieszenia lub zerwania połączenia. Programowane równoważenie obciążenia pomiędzy punktami dostępowymi wraz z technologią Air Traffic Control, zapewniającą Quality of Service poprzez kontrolę i sterowanie ruchem oraz danymi, gwarantują niezwykle wysoką jakość prowadzonych rozmów. ■



Rys. Przykładowy dialer umożliwiający użytkownikom telefonów komórkowych korzystanie z telefonii VoIP



REWOLUCJA W PAMIĘCIACH MASOWYCH IBM STORWIZE V7000

autor: Przemysław Sternadel
e-mail: p.sternadel@ascomp.eu

Dzisiaj...

Coraz większa złożoność pamięci masowych i gwałtownie rosnąca ilość danych jest dziś poważnym wyzwaniem dla organizacji i osób zarządzających tymi urządzeniami. Dotychczasowe metody zarządzania nimi nie są już wystarczająco skuteczne. Ze względu na ograniczoną dostępność zasobów – zarówno fizycznych pamięci masowych, jak i zasobów kadrowych – organizacje i działy informatyczne muszą jak najszybciej podejmować działania zmierzające do optymalizacji i uproszczenia infrastruktury. Firmy stają także przed szeregiem innych problemów, takich jak zarządzanie urządzeniami pochodzącymi od różnych producentów i ich integracja, niska użycie istniejących zasobów dyskowych czy długie (nie)planowane przestoje pracy urządzenia.

Lepsze jutro...

Na rynku macierzy dyskowych pojawił się nowy gracz, który aspiruje do bycia liderem na rynku midrange. Mowa tutaj o macierzy StorWize V7000, która swoją budową i funkcjonalnością jest w stanie skutecznie powalczyć z rosnącymi problemami na rynku pamięci masowych. Czy „lepsze jutro” już nadeszło i tylko czeka, aż otworzymy mu drzwi? Przekonajmy się.

Hardware

Urządzenie wyposażone jest w dwa kontrolery typu Active/Active. Każdy z nich został wyposażony w 8 GB pamięci cache, 4 porty Fibre Channel 8 Gb/s, 2 porty iSCSI 1 Gb/s. Aby zapewnić komunikację z dodatkowymi półkami dyskowymi, pojedynczy kontroler wyposażono w dwa porty SAS 6 Gb/s. Oczywiście urządzenie posiada również redundantne złącza ethernetowe służące do zarządzania. Producent

sprzętu zostawił otwartą furtkę, jeśli chodzi o rozwiązania przyszłościowe. W każdym z kontrolerów jest dedykowane miejsce na interfejsy, które mają szansę zaistnieć w przyszłości (iSCSI 10 Gb/s?). Storwize obsługuje dyski SAS, NearLine SAS oraz dyski typu SSD komunikujące się z kontrolerami przez porty SAS o przepustowości 6 Gb/s. Możemy używać zarówno dysków 2,5", jak i 3,5". Macierz skaluje się do 240 dysków przy użyciu dedykowanych półek dyskowych. Lecz to nie koniec jej możliwości...

W celu podniesienia wydajności i bezpieczeństwa macierz standardowo zapewnia możliwość tworzenia grup RAID czy dysków typu Global HotSpare. Jednak niekonwencjonalność Storwize'a zauważymy dopiero wtedy, gdy przyjrzymy się jego oprogramowaniu.



Rys. StorWizeV7000

Diabeł tkwi w szczegółach

Być może niektórzy z Was znają rozwijane już od kilku lat rozwiązanie firmy IBM o nazwie SAN Volume Controller (SVC). Przeznaczeniem tego urządzenia jest wirtualizacja środowisk macierzy dyskowych. Po krótko działa ono w następujący sposób: do sieci SAN wpinamy sklastrowane SVC. Z zewnętrznych macierzy dyskowych (różnych, praktycznie dowolnych producentów) wystawiamy LUN-y do SVC. Dopiero z tego urządzenia wystawiane są zasoby do serwe-

rów, oczywiście uprzednio je modyfikując. Funkcjonalność ta została przeniesiona do macierzy Storwize V7000. Brzmiało ciekawie ?

W macierzy Storwize został zaimplementowany ten sam software co we wspomnianym powyżej urządzeniu, więc nie ma obaw o niestabilne i zbyt świeże rozwiązanie. Oprócz standardowego działania – wystawienia zasobów ze Storwize'a do serwerów – możemy również wystawić zasoby z innych macierzy do Storwize'a. Urządzenie zobaczy wtedy pulę dyskową, na które będzie mogło wprowadzić swoje funkcjonalności, zwirtualizować je i wystawić dalej do serwerów.

Teraz nieco szczegółów. W cenie urządzenia dostajemy licencję na wirtualizację wewnętrzną (czyli dotyczącą macierzy Storwize oraz dedykowanych pól dyskowych do niej podłączonych). W skład tej licencji wchodzi takie funkcjonalności jak FlashCopy, VolumeCopy, ThinProvisioning czy EasyTier (o którym więcej w dalszej części artykułu). Gdybyśmy chcieli podłączyć do Storwize zewnętrzną macierz dyskową, musimy wykupić licencję na zewnętrzną wirtualizację. Dostajemy wtedy te same funkcje co w przypadku samego Storwize'a i przykrywamy nimi funkcjonalności macierzy podłączanych. Daje nam to szerokie możliwości konfiguracyjne i sprawia, że nawet w najmniejszych i najprostszyc macierzach dyskowych zyskujemy funkcje z rynku macierzy HighEnd.

Wolałbym się tutaj nie rozpisywać na temat funkcji typu FlashCopy czy ThinProvisioning, ponieważ są one dość powszechnie znane i wysoko cenione wśród użytkowników. Jednak na liście pozostałych funkcjonalności znajduje się bardzo ciekawe i tajemniczo brzmiące hasło EasyTier,

o którym chciałbym opowiedzieć więcej. Na rynku macierzy zewnętrznych coraz bardziej popularne stają się dyski SSD. Niestety bardzo często zdarza się, że po zakupie nie jesteśmy w stanie optymalnie ich wykorzystać ze względu na ich specyficzną charakterystykę. EasyTier w czasie rzeczywistym monitoruje operacje wejścia/wyjścia na wolumenach logicznych i przesuwa najbardziej obciążone bloki danych na dyski SSD. EasyTier to również system „inteligentny”, który potrafi uczyć się środowiska. Dzięki takiemu użyciu dysków SSD możemy być pewni, że zostaną one wykorzystane w najlepszy możliwy sposób.

Urządzenie nie zostało pozbawione możliwości replikacji zdalnej (synchronicznej, asynchronicznej) z innymi macierzami Storwize. W przyszłości zapowiadana jest również możliwość replikacji z urządzeniami SVC.

Zarządzanie

Przechodzimy do części równie ważnej, a mianowicie do zarządzania macierzą StorWize. Do dyspozycji dostajemy interfejs web GUI oraz linię komend. Ciekawą zaletą jest również możliwość debugowania błędów oraz wstępnej konfiguracji poprzez klucz USB. Interfejs graficzny jest bardzo nowoczesny, ale nie umniejsza to jego funkcjonalności. Bardzo szybko jesteśmy w stanie odnaleźć interesujące nas rzeczy: tworzenie zasobów, funkcje wirtualizacyjne czy logi systemowe. IBM przeprowadził sondę, w której brali udział administratorzy systemów macierzowych różnych producentów. Posadzono ich przed interfejsem Storwize'a i poproszono o wykonanie kilku zadań. W skali od 1–10 (gdzie 1 = nieskomplikowany, 10 = bardzo skomplikowany) administratorzy ocenili system na 1,8.

Jeżeli posiadamy więcej niż jedną macierz i podłączymy je do StorWize'a, zyskujemy niewątpliwą zaletę w postaci zarządzania całością z jednego bardzo przejrzystego i funkcjonalnego interfejsu.

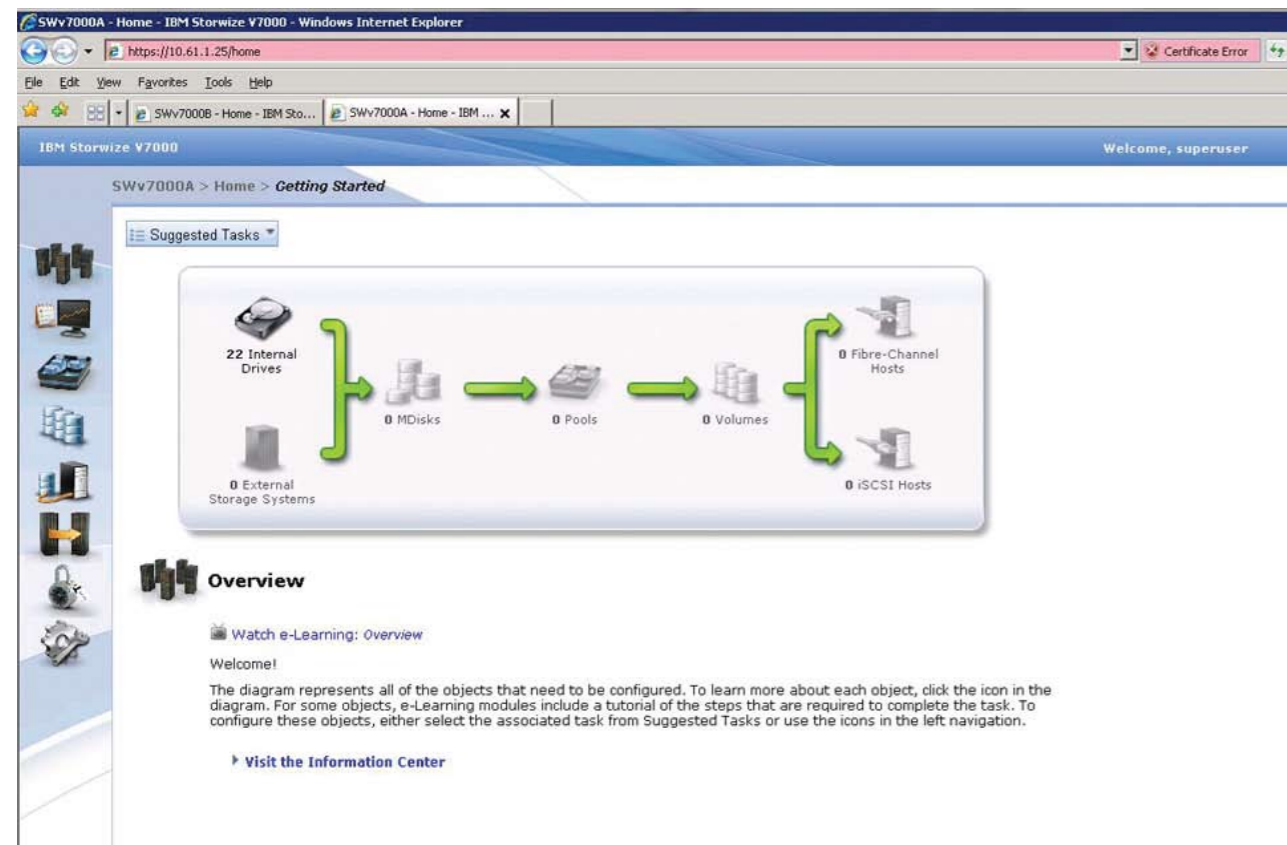
Zastosowanie

Aby przybliżyć zastosowanie dla opisywanego urządzenia, przedstawię jeden z wielu możliwych scenariuszy. Zrozumienie ułatwi krótki schemat przygotowany specjalnie pod konkretne założenie.

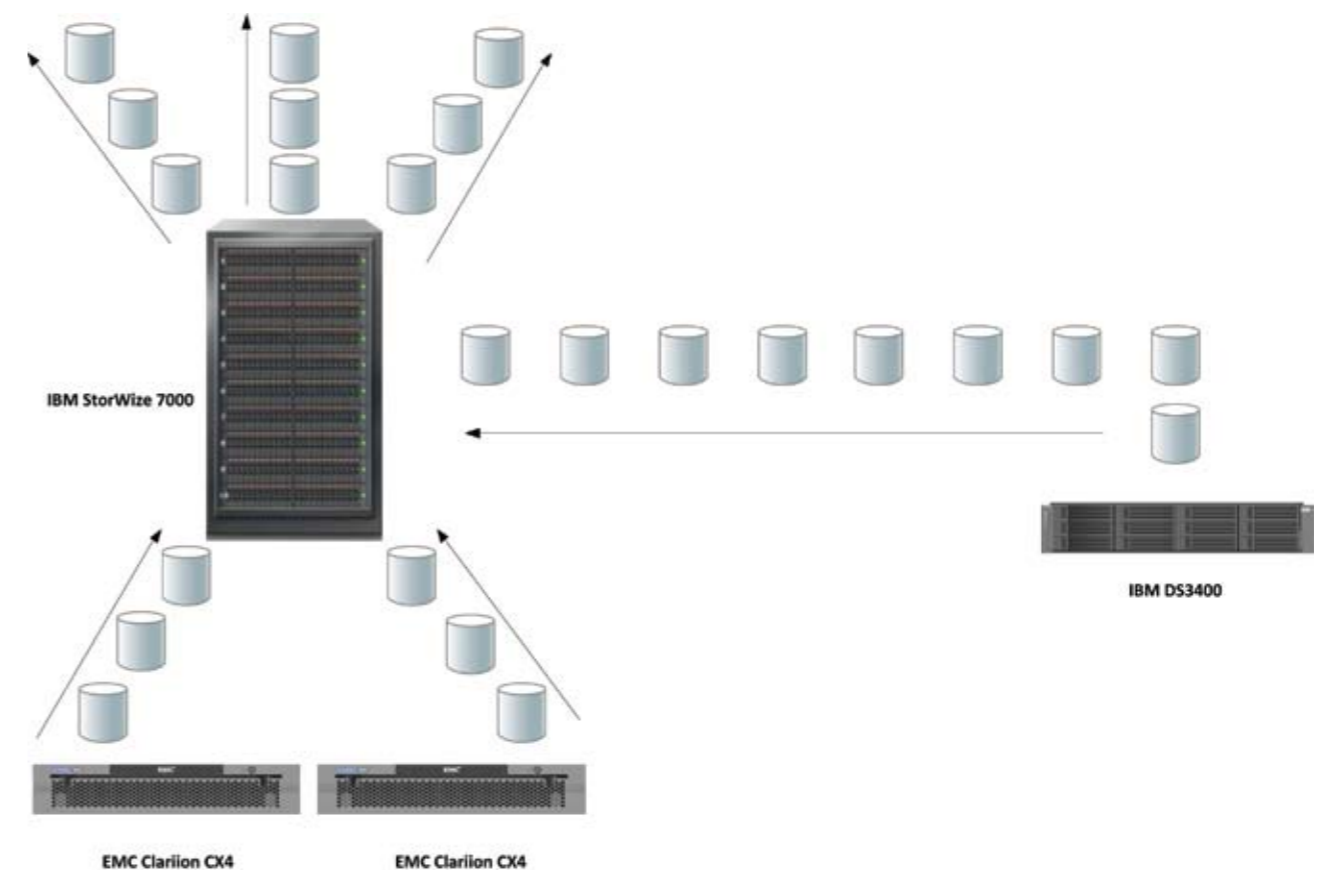
Klient X posiada dwie serwerownie. W serwerowni podstawowej pracują dwie macierze Clariion CX4 firmy EMC, a w zapasowej jedna macierz IBM DS3400. W obydwu lokalizacjach istnieje już infrastruktura SAN oparta na protokole Fibre Channel. Klient X ma potrzebę zakupu kolejnej, znacznie wydajniejszej macierzy dyskowej pod dedykowane aplikacje. Środowisko klienta robi się coraz mniej przejrzyste i zaczyna sprawiać duże kłopoty w administracji. Utylizacja zasobów i monitorowanie środowiska znacząco odbiega od ideału.

Dla klienta X idealnym rozwiązaniem będzie zakup macierzy Storwize z kilkoma dyskami SSD, zwirtualizowanie środowiska i zarządzanie całością z jednego poziomu. Pierwszym krokiem po zakupie nowej macierzy będzie migracja danych z istniejących macierzy na nowe urządzenie. Administrator taką czynność może wykonać w locie, bez przestoju dla aplikacji. Kolejną przygotujemy istniejące macierze do nowych ról. Na macierzach Clariion proponujemy rozrzuć operacje wejścia/wyjścia, co da nam wysoką wydajność dla określonych aplikacji. Macierz IBM DS3400 proponujemy przeznaczyć na kopie wolumenów oraz kopie migawkowe. Dyski wewnątrz macierzy Storwize przeznaczymy dla reszty aplikacji i usług. Zainstalowane dyski SSD pomogą w rozładowaniu ruchu w środowisku w krytycznych momentach.

Wprowadzenie ThinProvisioningu pozwoli na lepszą użycie zasobów na wszystkich urządzeniach, a centralne zarządzanie i monitorowanie umożliwi szybką reakcję w razie potrzeby.■



Rys. Zarządzanie – interfejs graficzny.

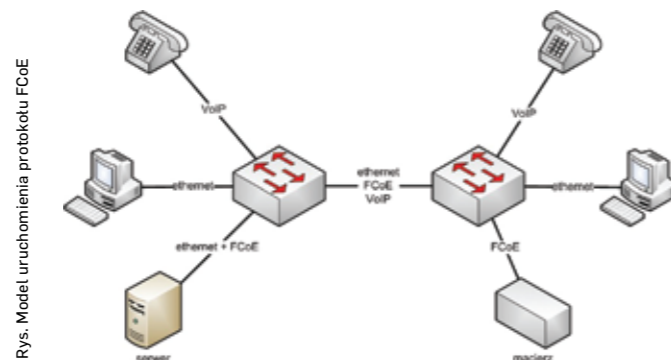


Rys. Przykład zastosowania.

ETHERNET JEST DOBRY NA WSZYSTKO, CZYLI FIBRE CHANNEL OVER ETHERNET

autor: Bartłomiej Kilanowicz
e-mail: b.kilanowicz@ascomp.eu

Z pewnością można powiedzieć, że każda większa firma posiada sieć lokalną opartą na Ethernetie, korzysta z telefonów oraz centralnie składowe dane. Klasyczne podejście zakłada budowę oddzielnych sieci służących do realizacji każdego z tych zadań: sieci LAN, sieci telefonicznej oraz sieci SAN. Jednak rozwiązanie to jest bardzo drogie, dlatego też podejmowane są próby łączenia ze sobą tych funkcji.



Okazało się, że Ethernet, pomimo wszystkich swoich ograniczeń (braku gwarancji dostarczenia danych, zmiennego opóźnienia), z powodzeniem może służyć do transmisji głosu. Dlatego też podjęte zostały kroki, by w ramach ethernetowych enkapsulować ruch Fibre Channel.

Pierwszym krokiem do pełnej integracji była telefonia Voice over IP. Na jej przykładzie okazało się, że Ethernet, pomimo wszystkich swoich ograniczeń (braku gwarancji dostarczenia danych, zmiennego opóźnienia), z powodzeniem może służyć do transmisji głosu. Dlatego też podjęte zostały kroki, by w ramach ethernetowych enkapsulować ruch Fibre Channel. Stało się to możliwe również ze względu na popularyzację 10-gigabitowego Ethernetu – w ten sposób zniknął problem niewystarczającej przepustowości. W tym celu producenci zorganizowali grupę roboczą Data Center Bridging opracowującą m.in. standard Converged Enhanced Ethernet. Efektem prac jest FCoE (Fibre Channel over Ethernet), który opisuje metodę łączenia obydwu protokołów oraz zawiera zalecenia, w jaki sposób radzić sobie ze wspomnianymi powyżej ograniczeniami Ethernetu.

JAK TO DZIAŁA?

Pierwszym zagadnieniem wymagającym opisanego jest enkapsulacja danych. Przyjęto, że ruch FCoE nie będzie mógł być rutowany, przewidziano jedynie możliwość jego przesyłania w obrębie pojedynczej domeny rozgłoszeniowej. Z jednej strony spowodowało to zmniejszenie zasięgu transmisji, z drugiej jednak ograniczyło stopień komplikacji protokołu oraz wyeliminowało narzut wprowadzany przez nagłówki IP. Ponieważ sieci NAS nie są zazwyczaj rozległe, lecz przesyłamy w nich ruch w obrębie Data Center, wspomniana wyżej wada nie jest uciążliwa. Dzięki temu Ethernet dla FCoE wygląda zupełnie klasycznie. Zawiera adresy źródłowe i docelowe, pole określające VLAN i priorytety oraz pole Ethertype o wartości 0x8914, które jednoznacznie określa protokół kolejnej warstwy jako Fibre Channel. W polu danych przenoszone są dane Fibre Channel. Jak widać, nie ma w tak sformatowanej ramce niczego niezwykłego i teoretycznie radzą sobie z nią wszystkie przetaczniki ethernetowe. Za kwestie mapowania adresów MAC na adresy WWN używane w Fibre Channel odpowiedzialne są karty sieciowe wbudowane w serwery i macierze. Z oczywistych względów nie mogą być to standardowe karty sieciowe, lecz adaptery CNA (Converged Network Adapters) integrujące funkcje adaptera FC oraz ethernetowej karty sieciowej.

A CO ZE SPRZĘTEM?

Jak widać, sam protokół nie został nadmiernie skomplikowany, co ułatwia kwestię integracji sprzętu różnych producentów. Z drugiej jednak strony, korzystając z pro-

tokółu Fibre Channel, nie można pozwolić sobie na utratę części strumienia danych czy na ich zmienne opóźnienie. Przenosi to odpowiedzialność za powodzenie transmisji na poszczególne przetaczniki ethernetowe i zaimplementowane na nich mechanizmy QoS. Rozwiązanie takie by było możliwe, ponieważ stosowane obecnie mechanizmy kontroli jakości transmisji działają na zasadzie hop-by-hop.

Kolejnym zagadnieniem jest odpowiednie znakowanie a następnie priorytetyzacja ruchu FCoE. Jednak nie usuwa ona wszystkich problemów. Dlatego powstał szereg standardów opracowanych przez wspomnianą wcześniej grupę DCB. Jednym z nich jest na przykład znany już ze zwykłego Ethernetu mechanizm PAUSE. Polega on na tym, że odbiorca, w momencie gdy nie ma możliwości przyjęcia dalszej części transmisji, wysyła do nadajnika wiadomość PAUSE, po której ten zaprzestaje nadawania. Wiadomość może zostać przesłana kolejno przez wszystkie urządzenia pośredniczące, aż do momentu osiągnięcia serwera lub macierzy źródłowej. Oczywiście mechanizm ten nie miałby sensu w przypadku przesyłania tym samym linkiem ruchu FC, LAN i VoIP, ponieważ zablokowałby całą transmisję. Dlatego też mechanizm ten został zmodyfikowany o możliwość dodania do wiadomości PAUSE informacji o klasie ruchu, której ona dotyczy. W ten sposób można zatrzymać tylko transmisję FCoE. Jak łatwo zauważyć, integracja Ethernetu i protokołu Fibre Channel jest zadaniem wymagającym przede wszystkim odpowiedniego sprzętu. W tym celu producenci opracowują

nowe urządzenia, wspierające standardy DCB. Przykładem takiego przetacznika może być Juniper EX4500.

PO CO TO WSZYSTKO?

Integracja sieci używanych przez firmy niesie ze sobą szereg zalet. Największymi są oszczędności okablowania oraz brak konieczności zakupu dodatkowych adapterów sieciowych. Nie mniej znacząca jest poprawa przejrzystości sieci i możliwość elastycznego wykorzystania posiadanych zasobów. W prosty sposób przekłada się to na ograniczenie kosztów zakupu i utrzymania sieci. ■



Rys. Juniper EX4500 wspierający protokół FCoE



NOWA KONCEPCJA ZARZĄDZANIA SIECIĄ – JUNOS SPACE

autor: Bartłomiej Kilanowicz
e-mail: b.kilanowicz@ascomp.eu

” Ciężko wyobrazić sobie zarządzanie dużą siecią bez użycia centralnego systemu zarządzania. Obecnie każdy liczący się producent sprzętu udostępnia swoim klientom platformę służącą do tych celów. Jednak jakiegokolwiek rozwiązanie byśmy wybrali, zawsze będziemy zarządzać siecią na zasadzie urządzenie-po-urządzeniu. ”

Ciężko wyobrazić sobie zarządzanie dużą siecią bez użycia centralnego systemu zarządzania. Obecnie każdy liczący się producent sprzętu udostępnia swoim klientom platformę służącą do tych celów. Istnieją również duże rozwiązania pozwalające na kontrolę nad urządzeniami wielu producentów, tj. HP Open View czy IBM Tivoli. Jednak jakiegokolwiek rozwiązanie byśmy wybrali, zawsze będziemy zarządzać siecią na zasadzie urządzenie-po-urządzeniu. Sytuację tę można zobrazować na przykładzie korzystania z domowego zestawu multimedialnego, składającego się z telewizora, dekodera i zestawu audio. Chcąc np. oglądać telewizję, musimy włączyć telewizor i przetączyć wejście na dekodery, włączyć zestaw audio i jego przetączyć również na sygnał z dekodera, a na koniec włączyć dekodery i wybrać żądany kanał. Jeśli korzystamy z oddzielnych pilotów, można to porównać do braku centralnego systemu zarządzania siecią. Bardziej użyteczny będzie pilot wielofunkcyjny, lecz również korzystając z niego, będziemy musieli przetączyć się na kolejne urządzenia i tak naprawdę wykonywać dokładnie tę samą sekwencję czynności. Tak działają klasyczne systemy zarządzania siecią.

Lecz wyobraźmy sobie sytuację, że na pilocie możemy nacisnąć po prostu klawisz „Chcę oglądać telewizję”, a on już sam wykona odpowiednie działania. Nam pozostanie tylko wybrać kanał... W domu za takim rozwiązaniem przemawia głównie wygoda, w firmie zalety są dużo bardziej wymierne. Ułatwione jest zarządzanie skomplikowaną infrastrukturą, dzięki czemu zostaje nam więcej czasu na planowanie usprawnień, których wdrażanie również jest ułatwione. Wszystko to pozwala na lepsze wykorzystanie kwalifikacji administratorów, ponieważ ściąga z nich obowiązek wykonywania żmudnych, powtarzających się czynności, co z kolei w prosty sposób przekłada się na oszczędności dla firmy. Wyobraźmy sobie konieczność udostępnienia nowej usługi dla klientów naszej firmy. W prostym wariantcie jedynymi parametrami, jakie musimy podać, są zewnętrzny adres IP i numer portu, pod jakim ma być dostępna usługa, oraz adres IP i numer portu serwera, na którym będzie ona hostowana. Nasz idealny system zarządzania sam odpowiednio skonfiguruje translację adresów oraz dostosuje polityki firewalli na ścieżce danych. W ten właśnie sposób działa Junos Space, nowy system zarządzania urządzeniami Juniper Networks. Junos Space jest otwartą platformą, do której samemu można dodawać kolejne elementy. W ten właśnie sposób

można zrealizować scenariusz nakreślony w poprzednim akapicie. Oprócz zapewnienia otwartości systemu producent udostępnia szereg opracowanych przez siebie narzędzi, z których najważniejsze dla sieci korporacyjnych są:

- Ethernet Design – zarządzanie przełącznikami LAN,
- Security Design – tworzenie i uruchamianie polityki bezpieczeństwa,
- Virtual Control – zarządzanie przełącznikami wirtualnymi będącymi częścią środowisk wirtualnych vSphere.

ETHERNET DESIGN

Moduł ten ułatwia konfigurację sieci LAN w zakresie przyłączania nowych użytkowników, urządzeń i serwerów do sieci, a także łączenie ze sobą infrastruktury sieciowej.



Rys. Konsola zarządzająca

Konfiguracja portu przełącznika obejmuje zazwyczaj włączenie szeregu mechanizmów. Są to m.in. określanie maksymalnej liczby adresów MAC na porcie, inspekcja ARP i DHCP Snooping, ustawienia CoS, STP i VLAN-ów. Oczywiście parametry te będą się różnić w zależności od tego, czy port będzie wykorzystany przez komputer PC, PC i telefon VoIP, serwer, Access Point, czy też inny przełącznik. Zazwyczaj, ustawiając te opcje, żmudnie „przeklikujemy się” przez wszystkie parametry lub kopiujemy określone fragmenty pliku konfiguracyjnego, zmieniając w nim odpowiednie wartości Junos Space umożliwia dużo wygodniejsze rozwiązanie oparte na profilach. Każdy profil (np. PC, PC+Tel, AP, serwer) zawiera zestaw ustawień, które następnie wystarczy „przypiąć” do wybranego interfejsu. Pozwala to na bardzo proste rekonfiguracje sieci, np. w wypadku zmiany biurka przez użytkownika.

Kolejnym często spotykanym problemem jest zapewnienie spójności konfiguracji VLAN-ów w obrębie całej sieci. Również w tym aspekcie można łatwo utworzyć szablony, które oprócz samych ustawień VLAN-ów, mogą zawierać również reguły filtracji ruchu w warstwach wyższych. Można np. ograniczyć komunikację pomiędzy użytkownikami w VLAN-ie do określonych numerów portów lub zablokować możliwość nawiązywania połączeń z wybranymi adresami IP. Filtry te mogą być następnie przypisane do każdego fizycznego portu w danym VLAN-ie.

SECURITY DESIGN

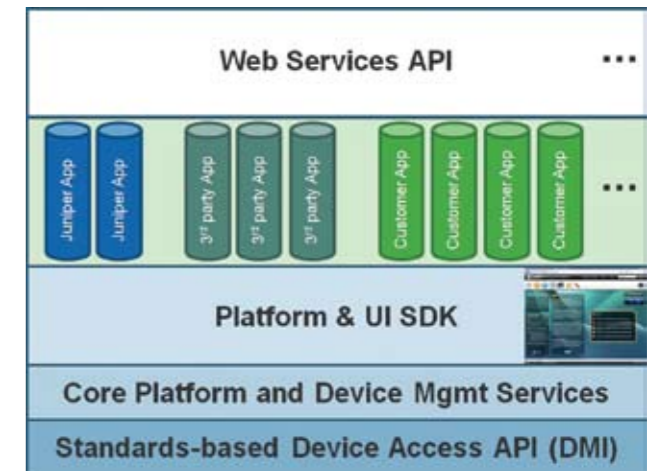
Moduł ten odpowiedzialny jest za zarządzanie infrastrukturą bezpieczeństwa, a w szczególności za przełożenie korporacyjnej polityki bezpieczeństwa na język sprzętu (w szczególności firewalli). Z jego pomocą w prosty sposób skonfigurujemy spójne i skuteczne reguły firewallingu w obrębie całości naszej infrastruktury (łącznie z lokalizacjami zdalnymi), a także zapewnimy bezpieczną komunikację pomiędzy oddziałami przez IPsec VPN.

Security Design również wykorzystuje konfigurację przez użytkownika szablonów, dlatego też uruchamianie kolejnych usług wymaga pojedynczych kliknięć myszką.

VIRTUAL CONTROL

Obecnie coraz ważniejszą częścią sieci stają się serwery wirtualne. Technologia jest bez wątpienia przyszłościowa, jednak wiąże się z nią pewne zagadnienia, które bardzo często są pomijane. Myśląc o wirtualnych serwerach, często zapominamy o pracujących w ich obrębie wirtualnych przełącznikach. Z jednej strony jest to część środowiska wirtualnego i z tego względu powinna podlegać adminis-

tratorowi serwerów. Z drugiej natomiast – jest to element realizujący dokładnie te same zadania co przełącznik fizyczny, czyli powinien podlegać administratorowi sieci, który będzie w stanie lepiej określić jego konfigurację.



Rys. Struktura oprogramowania Junos Space

Jak dotąd brakowało skutecznego narzędzia pozwalającego na wspólne zarządzanie infrastrukturą fizyczną i wirtualną. Dzięki interfejsowi API do vCenter dostarczanego przez VMware możliwe jest zintegrowanie tego narzędzia z Junos Space. Zyskujemy tym samym możliwość wykorzystania szablonów konfiguracji również dla infrastruktury wirtualnej.

PLATFORMA

Junos Space dostępny jest w formie dedykowanego urządzenia (appliance), lub też maszyny wirtualnej dla środowisk VMware. Zarządzanie infrastrukturą odbywa się z poziomu przeglądarki WWW, bez konieczności instalacji dodatkowego oprogramowania klienckiego. ■

ASCOMP



WIRTUALIZACJA ZASOBÓW

autor: Ewa Śniechowska
e-mail: e.sniechowska@ascomp.eu

Wirtualizacja sieci jest technologią, która umożliwia tworzenie logicznie odizolowanych segmentów sieci we współdzielonej fizycznej infrastrukturze. W kontekście architektury nowoczesnej sieci wirtualizację należy rozważać zarówno jako współdzielenie zasobów sieciowych (VLAN) i sprzętowych (wirtualne routery) oraz jako agregację (LACP).

VLAN

Wirtualna sieć lokalna (Virtual Local Area Network) to sieć wydzielona logicznie w ramach większej sieci fizycznej. Do tworzenia VLAN-ów wykorzystuje się przełączniki sieciowe umożliwiające podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych poprzez separację ruchu pomiędzy określonymi grupami portów. Sieć VLAN stanowi logiczną domenę rozgłoszeniową, która może obejmować wiele fizycznych segmentów sieci LAN. Komunikacja między VLAN-ami jest możliwa przy użyciu urządzeń warstwy wyższej, takich jak routery oraz przełączniki warstwy trzeciej. Sieci VLAN grupują użytkowników w zależności od pełnionych przez nich funkcji bądź też przynależności do danych grup, niezależnie od fizycznego położenia.

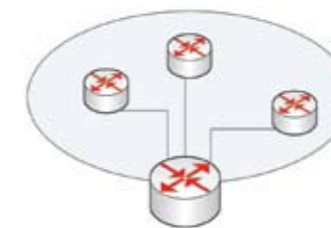
Do korzyści z zastosowania sieci VLAN należy między innymi łatwość dodawania i zmian stacji roboczych do sieci, co pozwala szybciej dostosować ją do zmian w organizacji. Zaletą jest również uproszczone wprowadzanie zmian w konfiguracji sieci, a przede wszystkim łatwość w nadzorowaniu ruchu, ograniczenie ruchu rozgłoszeniowego, a co za tym idzie, zwiększenie wydajności i bezpieczeństwa sieci.

Wirtualizacja routerów

Wirtualizacja routera polega na logicznym podziale maszyny fizycznej na routery wirtualne. Do każdego z nich przypisane są między innymi bufor pamięci, przestrzeń adresowa, tablica routingu oraz porty. Każdy router może być konfigurowany, monitorowany oraz zarządzany w sposób niezależny – co więcej, dostęp i prawa administracji do poszczególnych routerów również przydzielane są niezależnie. Zwiększenie ruchu płynącego przez jeden z wirtualnych routerów pozostaje bez wpływu na pozostałe dzięki izolacji ścieżek poszczególnych routerów wirtualnych, którymi przesyłane są pakiety, co czyni całość systemu niezwykle stabilną.

Grupa routerów wirtualnych w ramach jednej maszyny fizycznej jest

w stanie udźwignąć zadania realizowane dotychczas przez kilka mniejszych urządzeń.



Rys. Koncepcja routerów wirtualnych

Wirtualne routery w Juniper Networks

W nomenklaturze przyjętej przez Juniper Networks wyróżniamy routery wirtualne (virtual routers) i logiczne (logical routers). Virtual routers są jedynie instancjami routującymi o oddzielnych tablicach routingu – na jednej platformie można ich zaimplementować od 500 do 6500. Logical routers to routery wirtualne w tradycyjnym rozumieniu, powstałe w wyniku logicznego podziału maszyny na segmenty. Począwszy od wersji 9.3 oprogramowania JUNOS, nazwa logical router została zmieniona na logical system. Wszystkie komendy konfiguracyjne i polecenia, komunikaty o błędach itp. zawierające ciąg logical-router lub też logical-routers zostały odpowiednio zamienione na logical-system bądź też logical-systems. Na routerach wirtualnych możliwa jest implementacja takich protokołów, jak OSPF, IS-IS, RIP, w tym RIPng, BGP, RSVP, LDP, wspierane jest IPv4 jak i IPv6, jak również podstawowe funkcjonalności MPLS. Do routera logicznego można przypisać większość typów interfejsów, w tym interfejsy typu SONET, Ethernet, ATM i ATM2.

Wirtualizacja bramy domyślnej

Dzięki wirtualizacji routerów prostsze i mniej kosztowne staje się wprowadzenie zvirtualizowanej bramy domyślnej. VRRP (Virtual Router Redundancy Protocol) jest protokołem zapewniającym zwiększenie dostępności bramy domyślnej dla danej podsieci. Większa niezawodność jest osiągnięta dzięki temu, że zamiast pojedynczego routera jako brama domyślna rozgłaszany jest wirtualny router, za którym kryją się działające razem router główny i zapa-

sowy. Skonfigurowane są one w ten sposób, że tylko jeden z nich pełni funkcje bramy, przy czym drugi jest gotowy, by go zastąpić w razie awarii.

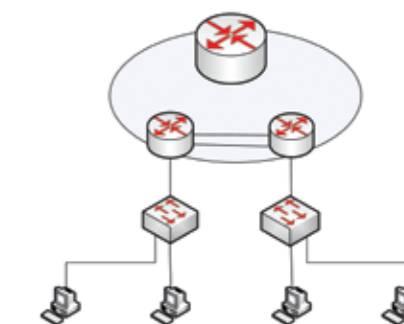
Agregacja łączy

Kolejnym zagadnieniem z dziedziny wirtualizacji sieci jest agregacja łączy. LACP (Link Aggregation Control Protocol) zapewnia metody kontroli wielu fizycznych portów połączonych ze sobą, tworzących w ten sposób jeden kanał logiczny. LACP pozwala urządzeniom sieciowym na automatyczną negocjację grupowania łączy. Zasada działania oparta jest o wysyłanie ramek (LACPDU) do wszystkich łączy, gdzie uruchomiony jest protokół, w celu automatycznego tworzenia kanałów. Tryb ten może być również stosowany jako sposób kontrolowania przypadkowych pętli.

Agregacja łączy jest prostą metodą na stworzenie sieci szkieletowej o wysokiej przepustowości, dającej możliwość transferu o wiele większej ilości danych, niż oferuje to pojedynczy port. Rzeczywiste korzyści z zastosowania agregacji zależą od sposobów równoważenia obciążenia na danym urządzeniu. Agregacja pozwala również na stopniowe zwiększanie przepustowości sieci szkieletowej wraz z rosnącym zapotrzebowaniem na pasmo, bez konieczności wymiany czy zakupu nowego sprzętu.

Kluczowy jest również fakt, że poprzez agregację uzyskujemy nadmiarowość, która zapewnia niezawodność połączenia w przypadku awarii pojedynczych łączy.

Wykorzystanie opisanych powyżej możliwości, jakie daje nam wirtualizacja zasobów sieciowych, pozwala zbudować sieć o nowoczesnej i wysoce niezawodnej architekturze. ■



Rys. Schemat sieci z wykorzystaniem wirtualnej bramy domyślnej

WIRTUALIZACJA ŚRODOWISKA SERWEROWEGO

autor: Przemysław Sternadel
e-mail: p.sternadel@ascomp.eu

Spotkanie z klientem

Klientem była w tym wypadku jedna z większych polskich uczelni. Na spotkaniu technicznym dowiedzieliśmy się, że klient ma problem z utrzymaniem środowiska serwerowego. W jego infrastrukturze od kilku lat w szybkim tempie przybywało dużo aplikacji czego wynikiem były częste zakupy serwerów różnych producentów. Taka sytuacja doprowadziła w końcu do wielkich trudności z zarządzaniem środowiskiem fizycznym (kończąca się gwarancja w różnych okresach czasu, skomplikowane zarządzanie...), a także z administracją systemami i aplikacjami (przede wszystkim problemy wydajnościowe). Naszym zadaniem było znalezienie „złotego środka”, który „wyleczy” klienta z omawianych problemów. Pierwszym krokiem było uzyskanie szczegółowych informacji na temat aktualnie posiadanego sprzętu serwerowego oraz infrastruktury LAN/SAN. Ważnym elementem było dokładne doprecyzowanie wersji systemów operacyjnych oraz aplikacji, które na nich pracują. Klient dysponował danymi na temat obciążenia serwerów (pamięci, procesora, sieci, operacji dyskowych), które zgodził się udostępnić w celach projektowych. Jak się później okazało zbiór takich danych był bardzo pomocny w tworzeniu koncepcji.

Stan zastany

Po dwóch dniach tworzenia dokumentacji ze stanu zastanego otrzymaliśmy informacje, które wystarczyły do stworzenia koncepcji:

- 43 serwery fizyczne różnych producentów mające od 3 do 7 lat, produkcyjne oraz testowe;
- Pełna specyfikacja wyżej wymienionych serwerów;
- Jedna macierz dyskowa podłączona do 5 serwerów za pomocą protokołu iSCSI;
- Jedna macierz dyskowa podłączona do 2 serwerów za pomocą interfejsu SAS;
- Brak infrastruktury SAN opartej na protokole Fibre Channel;
- Infrastruktura LAN/WAN modernizowana 6 miesięcy temu, spełniająca wysokie standardy;
- Średnia utylizacja podstawowych zasobów (pamięć, procesor, dysk, sieć) z ostatniego miesiąca na każdym serwerze – dane dostarczone przez klienta.

Nadchodzi pomoc - koncepcja i konfiguracja urządzeń.

Zdecydowaliśmy, że proponujemy klientowi rozwiązanie, które opiera się na serwerach jednego producenta oraz platformę wirtualizacyjną, na którą w przyszłości zostaną przeniesione aktualne systemy wraz z aplikacjami.

Pomimo iż klient początkowo zakładał użycie serwerów typu rack, zaproponowaliśmy koncepcję wykorzystującą serwe-

ry kasetowe firmy IBM. Wcześniejsza kalkulacja kosztów wykazała, że w przypadku zakupu 14 serwerów kasetowych wraz z obudową może on zaoszczędzić ponad 20% kosztów (zakupu, użytkowania) w stosunku do serwerów typu rack 19". Oczywiście zwróciliśmy też uwagę na ilość potrzebnego miejsca do zainstalowania sprzętu w szafach przemysłowych – ponad dwukrotnie mniej miejsca w przypadku serwerów kasetowych. Do wszystkiego doszły koszty gniazd oraz kabli, których jest kilkakrotnie mniej w zaproponowanym przez nas rozwiązaniu. Ogółem zaproponowana przez nas koncepcja była niemal o 30% tańsza od zakładanej początkowo przez klienta, przy założeniu, że sprzęt użytkowany będzie w okresie przynajmniej 5 lat.



Z przeprowadzonej dokumentacji stanu zastanego wynikało, że do wirtualizacji nadaje się 40 z 43 serwerów fizycznych. Pozostałe trzy serwery pozostały bez zmian w konfiguracji i pełnią dotychczasowe role. Zaproponowaliśmy rozwiązanie oparte o serwery kasetowe BladeCenter H z 14 serwerami HS22V oraz oprogramowanie do wirtualizacji VMware vSphere 4.1. Klatka obsługująca serwery została wyposażona w redundantne przetworniki Fibre Channel 8 Gb/s, 4 przetworniki Ethernet 1/10 Gb/s, redundantne zasilanie oraz zarządzanie całością. Każdy serwer wyposażono w dwa procesory Intel Xeon X5650 oraz 64 GB pamięci RAM. Dodatkowo w każdym serwerze zainstalowano 4 porty Ethernet 1 Gb/s oraz 2 porty FC 8 Gb/s. W serwerach nie przewidziano dysków, a jedynie klucz USB, na którym znalazł się Hypervisor ESXi.

Jako platformę wirtualizacyjną zaproponowaliśmy vSphere 4.1 Enterprise w wersji embedded w postaci klucza USB. Środowisko produkcyjne zostało oddzielone od środowiska testowego. Na 10 pierwszych serwerach zostały umieszczone 32 systemy produkcyjne, a na 4 ostatnich

umieszczono 8 systemów testowych. Całość działa w dwóch niezależnych klastrach wysokiej dostępności oraz jest zarządzana z poziomu aplikacji vCenter Server. Ze względu na charakterystykę utylizacji zasobów (duże obciążenie w godzinach od 8:00 do 18:00) zaproponowaliśmy wdrożenie funkcji Distributed Resources Scheduler oraz Distributed Power Management (automatyczna migracja maszyn wirtualnych w obrębie klastra oraz wyłączenie wolnych serwerów fizycznych w okresie zmniejszonej utylizacji zasobów), co pozwoliło zaoszczędzić kolejne wydatki na energię elektryczną. Do całości rozwiązania została podłączona macierz dyskowa IBM StorWise V7000 po protokole Fibre Channel. W macierzy zainstalowano 45 dysków SAS 300 GB i 3 dyski SSD 300 GB. Całość zasobów została wystawiona do serwerów fizycznych.

Wdrożenie i przeszkolenie personelu

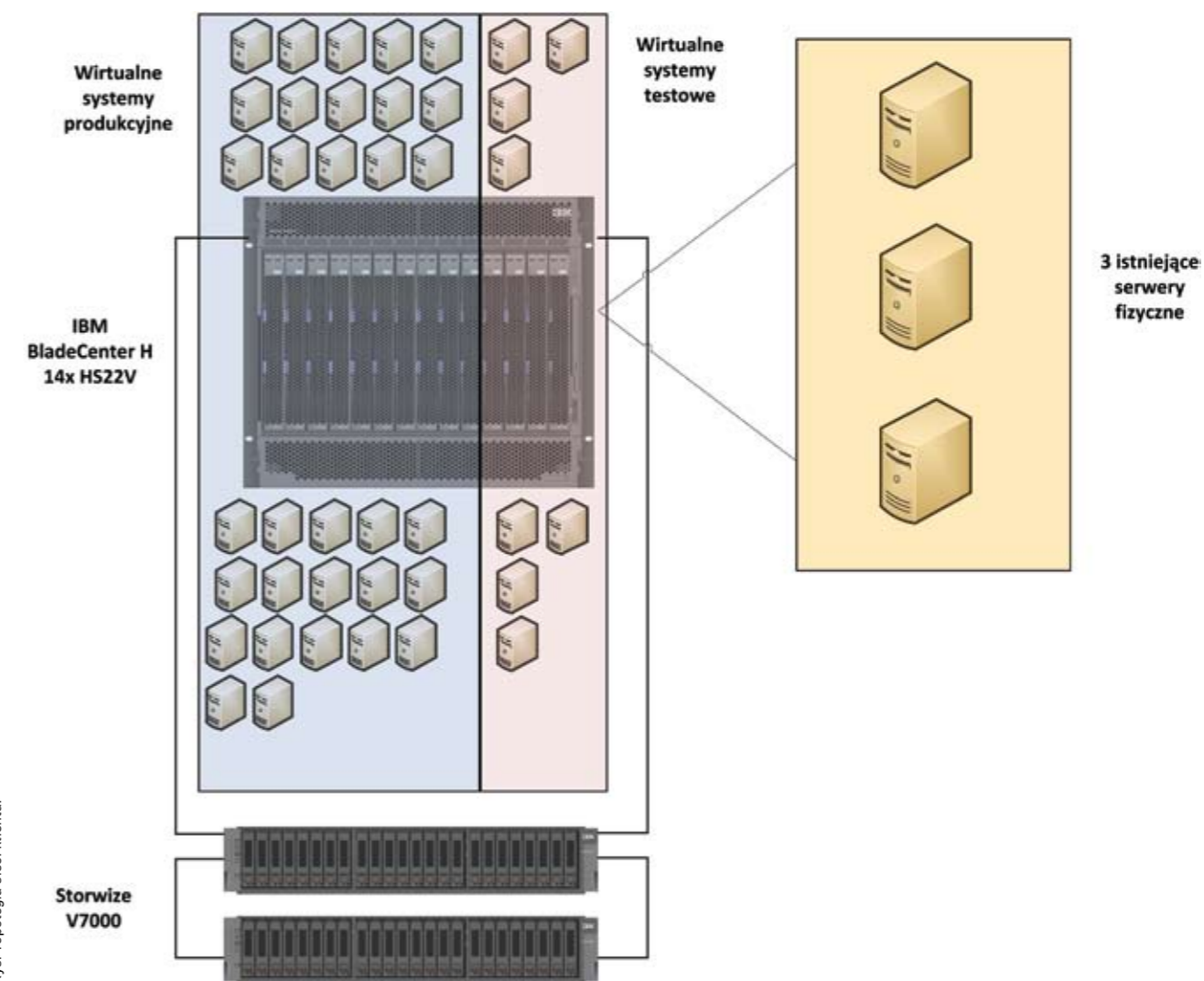
Ostatnim etapem było przeprowadzenie wdrożenia oraz przeszkolenie dedykowanego personelu. Dzięki wybranemu rozwiązaniu oraz doświadczeniu inżynierów wdrożeniowych fizyczna instalacja serwerów oraz macierzy dyskowej przebiegła w bardzo szybkim tempie. Następnymi krokami było

odpowiednie połączenie urządzeń ze sobą oraz konfiguracja logiczna (konfiguracja macierzy, środowiska wirtualnego). Tak przygotowane środowisko było wstępem do sukcesywnej migracji systemów na infrastrukturę wirtualną przez klienta. Ostatnim krokiem było przeszkolenie kadry administracyjnej z wdrożonego środowiska oraz wirtualizacja 3 systemów testowych. Wdrożenie wraz z przeszkoleniem zajęło 8 dni roboczych.

Wdrożone środowisko zostało dobrane z nadmiarowością ze względu na przyszłe plany wdrożeniowe kolejnych systemów przez klienta. Kolejnymi krokami będą implementacja systemu replikacji środowiska wirtualnego do odległej serwerowni oraz tworzenie środowiska wirtualnych PC wykorzystującego rozwiązanie firmy VMware.

Zysk dla klienta:

Dzięki wybranemu rozwiązaniu klient zyskał szereg nowych możliwości oraz wysokie oszczędności w użytkowaniu i zarządzaniu infrastrukturą serwerową, począwszy od wprowadzenia bardzo wysokiej dostępności dla aplikacji poprzez ułatwienie zarządzania oraz monitorowania systemów serwerowych, a kończąc na bardzo niskich kosztach utrzymania wdrożonych urządzeń. ■



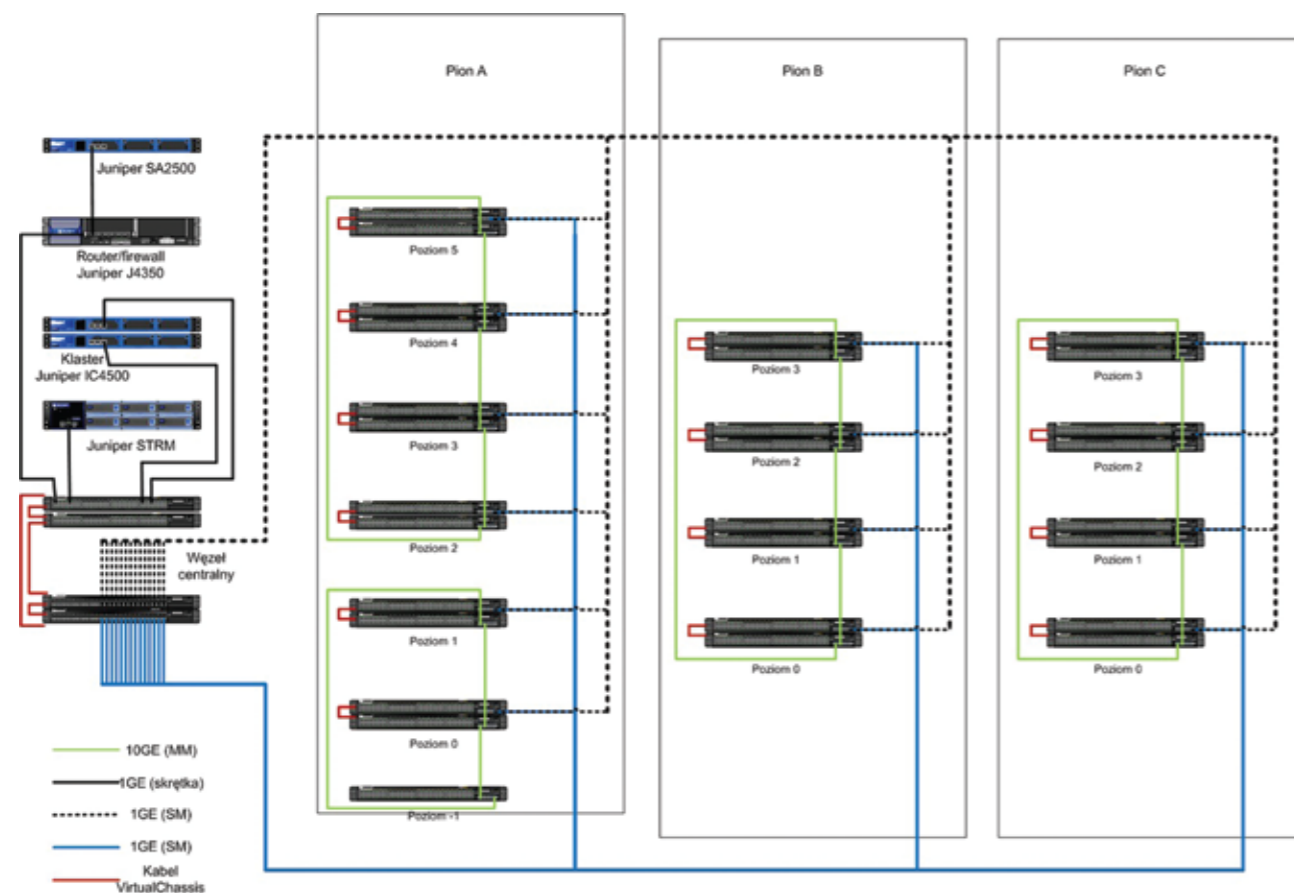
Rys. Topologia sieci klienta.

SIEĆ OD ZERA, CZYLI INTEGRACJA ROZWIĄZAŃ JUNIPER NETWORKS I MERU NETWORKS

autor: Bartłomiej Kilanowicz
e-mail: b.kilanowicz@ascomp.eu

Klient, instytucja publiczna zatrudniająca ponad 500 pracowników zaplanowała całkowitą wymianę infrastruktury sieci LAN. Założenia obejmowały budowę węzła szkieletowego i warstwy dostępowej oraz sieci bezprzewodowej zintegrowanych z systemem kontroli dostępu. Zaproponowaliśmy zintegrowane rozwiązania Juniper Networks połączone z siecią bezprzewodową Meru Networks.

PROPOZYCJA ROZWIĄZANIA



Rys. Topologia sieci klienta.

PRZEŁĄCZNIKI

Szkielet sieci oparto na dwóch 24-portowych przełącznikach światłowodowych i dwóch 24-portowych przełącznikach wyposażonych w interfejsy RJ-45. Wszystkie są różnymi wariantami modelu Juniper EX4200. Zostały one połączone w jeden przełącznik logiczny przy użyciu dedykowanych portów, co zapewniło przepustowość na poziomie przełączników modułarnych przy dużo mniejszym zapotrzebowaniu na energię i miejsce w szafie. Stos ten jest odpowiedzialny za połączenie z warstwą dostępową, węzłem dostępu do Internetu i sieci zewnętrznych oraz serwerów (w tym z kontrolerami dostępu i systemem korelacji zdarzeń). Przełączniki dostępowe Juniper EX4200 zostały podzielone na przełączniki wirtualne według schematu przedstawionego na rysunku, tj. w pionie A – dwa stosy, a pionach B i C – po je-

dnym stosie. Na każde piętro przypadają 2 przełączniki wyposażone w 48 portów z pełną obsługą PoE oraz modułami uplinkowymi na wkładki SFP+ (obsługa zarówno połączeń 1-, jak i 10-gigabitowych). Przełączniki w obrębie jednego piętra zostały połączone za pomocą dedykowanych portów, natomiast piętra w obrębie grupy połączone za pomocą łączy światłowodowych krótkiego zasięgu o przepustowości 10Gbit/s. Rozwiązanie takie ułatwia zarządzanie siecią, ponieważ cała grupa widoczna jest jako jeden duży przełącznik, a także zwiększa jej przepustowość, jako że ruch pomiędzy użytkownikami w obrębie stosu jest przelazany lokalnie, bez udziału szkieletu sieci. Dodatkową korzyścią jest wzrost niezawodności sieci, ponieważ nawet w przypadku uszkodzenia światłowodu pomiędzy danym

piętro a szkieletem sieci, ruch może zostać przestany przez inne przełączniki w stosie.

Każde piętro jest połączone ze szkieletem sieci dwoma interfejsami o przepustowości 1Gbit/s. Dla zwiększenia niezawodności sieci połączenia te realizowane są za pośrednictwem oddzielnych magistral światłowodowych. Dzięki użyciu funkcji Link Aggregation (wg standardu 802.3ad) możliwe jest połączenie do ośmiu portów w jedno łącze logiczne. Porty wchodzące w skład takiego interfejsu mogą należeć do różnych przełączników w obrębie jednego stosu. Funkcja ta pozwala na równoczesne wykorzystanie wszystkich połączeń fizycznych pomiędzy stosem a szkieletem sieci, tak więc przepustowość pomiędzy warstwami sieci wynosi 8Gbit/s. Link Aggregation pozwala na ciągłe działanie połączenia nawet w przypadku awarii łączy. Oznacza to, że w razie uszkodzenia światłowodu połączenie będzie utrzymane, lecz będzie dysponowało mniejszą przepustowością. W razie uszkodzenia światłowodu wyeliminowanie konieczności zbudowania nowego drzewa Spanning Tree pozwala w rezultacie uniknąć przestoju sieci.

SIEĆ BEZPRZEWODOWA

Ze względu na liczbę klientów, rozległość instalacji i warunki propagacyjne optymalnym rozwiązaniem był system bezprzewodowy Meru Networks. Działa on na pojedynczym kanale, dzięki czemu nie występują w nim problemy związane z planowaniem rozmieszczenia poszczególnych kanałów. Tym samym umożliwia również budowę trzech niezależnych sieci radiowych pracujących na różnych zakresach częstotliwości. Kolejną zaletą jest bardzo szybkie przełączanie

wędrujących użytkowników bezprzewodowych pomiędzy punktami dostępowymi. System bezprzewodowy Meru Networks w pełni integruje się z pozostałymi elementami zaproponowanego klientowi rozwiązania, w tym z systemem kontroli dostępu Juniper Unified Access Control.

SYSTEM KONTROLI DOSTĘPU

Zadaniem systemu Juniper Unified Access Control jest uwierzytelnianie użytkowników i wymuszenie przestrzegania polityki bezpieczeństwa przedsiębiorstwa. W sieci klienta został zastosowany w celu sprawdzania tożsamości użytkowników oraz wymuszenia stosowania przez nich aktualnego systemu operacyjnego i antywirusowego oraz firewalla. Użytkownik, który spełnia wymagania polityki bezpieczeństwa, otrzymuje dostęp do właściwego dla swojej funkcji VLAN-u, a także odpowiedni filtr określający dozwolony profil ruchu w warstwach L3-L4. Filtry te stosowane są na portach brzegowych przełączników dostępowych, a więc już w miejscu styku użytkownika z siecią. Użytkownicy, którzy nie spełniają określonych warunków, są kierowani do VLAN-u kwarantanny, który umożliwia pobranie aktualizacji, lecz nie pozwala na dostęp do kluczowych zasobów sieciowych.

CO ZYSKAŁ KLIENT?

Dzięki wdrożonemu rozwiązaniu klient uzyskał wydajną i bezpieczną infrastrukturę dostępową do sieci. Zintegrowane zostały infrastruktura przewodowa i bezprzewodowa oraz zbudowany został centralny punkt sterujący dostępem do niej. W znaczący sposób zwiększyło się bezpieczeństwo sieci i gromadzonych w niej danych. ■



System dyskowy EntryLevel IBM DS 3500

W 2010 roku pojawiła się nowa macierz dyskowa, która ma szansę zaistnieć w wielu małych i średnich firmach. Urządzenie to charakteryzuje się bardzo przystępną ceną za funkcje, które oferuje. Modułowa konstrukcja pozwala dostosować rozwiązanie do naszych potrzeb – porty klientki: SAS 6 Gb/s, FC 8 Gb/s lub iSCSI 1 Gb/s. Urządzenie wyposażono w dwa kontrolery Active/Active z maksymalnie 4 GB pamięci podręcznej. W obudowie można zainstalować dyski 2,5" (do 24 sztuk) lub 3,5" (do 12 sztuk). W obu przypadkach są to szybkie dyski SAS oraz wolniejsze dyski o większej pojemności Near-line SAS. Za pomocą dodatkowych półek dyskowych możemy zwiększyć maksymalną liczbę dysków do 96. Oczywiście naszą macierz możemy

wyposażać w takie funkcje jak tworzenie kopii migawkowych oraz kopii całościowych wolumenów logicznych. W tej klasie macierzy do rzadkości należy możliwość replikacji zdalnej wolumenów na inne macierze dyskowe IBM posiadające tę funkcję.



Seria serwerów Enterprise IBM eX5

W zeszłym roku oprócz pojawienia się kilku nowinek technologicznych w urządzeniach firmy IBM mieliśmy również premierę całej serii serwerów przeznaczonych z naciskiem na rynek dużych firm. Mowa tutaj o trzech serwerach stelażowych (x3690 X5, x3850 X5 x3950 X5) oraz jednym serwerze kasetowym (HX5). Każdy z nich charakteryzuje się wysoką skalowalnością wertykalną (rozszerzenie komponentów wewnątrz pojedynczego serwera), a niektóre – także horyzontalną (dodanie kolejnego serwera działającego w klastrze wydajnościowym). W razie awarii jednego z nodów w klastrze system operacyjny zostanie podniesiony na sprawnym serwerze. Do każdego urządzenia dodatkowym elementem może być rozszerzenie MAX5, które zwiększa maksymalną ilość pamięci RAM do niewyobrażalnych wartości. Wysoka skalowalność (szczególnie pamięci RAM)

tych urządzeń sprawia, że idealnie nadają się one jako platforma pod wirtualizację.



JUNOS 10.4

Wraz z najnowszą wersją systemu operacyjnego JUNOS 10.4 Juniper Networks wprowadza szereg nowych funkcjonalności. Na przełącznikach serii EX wprowadzona została możliwość konfiguracji PVLAN (private VLAN) oraz kontroli sztormów multicastowych. Dla przełączników EX8200 jest już dostępna technologia Virtual Chassis pozwalająca na łączenie wielu fizycznych przełączników w jeden przełącznik logiczny. Z kolei na przełącznikach EX4500 istnieje możliwość zastosowania FIP snooping (zapobiegającego atakom typu man-in-the-middle, kiedy urządzenie używane jest jako przełącznik FCoE) oraz PFC (dającego możliwość sterowania ruchem w zależności od jego klasy).

Dla routerów serii MX oraz M120 i M320 wprowadzona została nowa generacja silników routingu, o lepszej wydajności, pamięci i niezawodności, wraz z aktualizacją do 64-bitowego systemu operacyjnego JUNOS. Przed-

stawiono również JSF (Junos OS Services Framework), mający pozwalać na ujednoczenie usług w ramach systemu. Zaimplementowane zostały również nowe funkcje równoważenia obciążenia w przypadku zagregowanych łącz ethernetowych.

JUNOS 10.4 pozwala na dodatkowe wsparcie dla IPv6 na urządzeniach serii SRX, takie jak NAT, NAT-PT, zaawansowane opcje kontroli przepływu, filtrowanie pakietów, serwer DHCPv6 i wiele innych. Aktualizacja wersji systemu operacyjnego na urządzeniach serii SRX będzie odtąd możliwa także za pomocą dysku USB.

Zestawy promocyjne JUNIPER MX80

Juniper proponuje zestawy promocyjne routera MX80 przeznaczonego dla operatorów telekomunikacyjnych oraz dużych przedsiębiorstw. Posiadają one redundantne zasilanie, licencje zapewniające pełną obsługę BGP oraz licencyjnie określone liczby dostępnych portów. Możliwe jest późniejsze odblokowywanie portów poprzez zakup kluczy licencyjnych. Dostępne są następujące warianty:

- dostępnych 20 portów 1000BASE-X, zablokowane 4 porty 10GBASE-X i slot MIC,
- dostępnych 20 portów 1000BASE-X i slot MIC (do obsadzenia wybraną kartą), zablokowane 4 porty 10GBASE-X,

- dostępnych 20 portów 1000BASE-X, slot MIC i 2 porty 10GBASE-X, zablokowane 2 porty 10GBASE-X.
- Zestawy dostępne są w atrakcyjnych cenach.



VIRTUAL CHASSIS dla przełączników EX8200

Juniper udostępnił znaną z linii EX4200 funkcjonalność Virtual Chassis dla przełączników szkieletowych EX8200. Jest ona realizowana przez zewnętrzny moduł XRE200 pełniący rolę zewnętrznego silnika rutującego. Virtual Chassis pozwala na połączenie dwóch urządzeń fizycznych w jedno logiczne, dzięki czemu sieć zyskuje na wydajności oraz na odporności na awarie. Istotne jest również uproszczenie zarządzania, jako że konfiguracji wymaga tylko jedno urządzenie logiczne zamiast dwóch fizycznych. Zastosowanie takiej architektury umożliwia też wyeliminowanie protokołów z rodziny STP, dzięki czemu zmniejsza się czas powrotu sieci do pełnej funkcjonalności po awarii. Obecnie możliwe

jest budowanie przełączników logicznych z maksymalnie dwóch urządzeń EX8200. W kolejnych etapach planowane jest rozszerzenie tej liczby do czterech, a następnie ośmiu przełączników.



Poszerzamy rodzinę SRX

Firma Juniper Networks wprowadziła dwa kolejne modele do swojej już niemałej rodziny rozwiązań SRX. Urządzenie SRX 220, dedykowane do brzożu sieci, oferuje przepustowość na poziomie maksymalnym do 950 Mb/s i wyposażone jest w osiem interfejsów miedzianych w standardzie Gigabit Ethernet. Standardowo urządzenie można doposażyć w dodatkowe interfejsy WAN (T1/E1, ADSL, G.SHDSL, VDSL2, SFP, Serial, DOCSIS 3.0 Cable Modem). Dodatkowo firma Juniper postanowiła wypełnić lukę pomiędzy dostępnymi urządzeniami SRX 650 i SRX 3400, wprowadzając w pełni modułarne rozwiązanie SRX 1400 oferujące maksymalną przepustowość na poziomie 10 Gb/s. Tym samym zwiększyła

się liczba urządzeń, jakie możemy z powodzeniem stosować zarówno na styku sieci z Internetem, jak i w miejscach separujących szybkie sieci LAN.



Juniper Enterprise Guest Access

W ofercie firmy Juniper Networks pojawiło się nowe rozwiązanie klasy NAC przeznaczone do separacji użytkowników gości w sieciach LAN i WLAN od sieciowych zasobów korporacyjnych. Juniper Enterprise Guest Access bazuje na dobrze znanym rozwiązaniu UAC firmy Juniper Networks, z tą różnicą, że w jednym urządzeniu zostały zintegrowane funkcje PDP oraz PEP. Typowo urządzenie EGA umiesz-

czamy pomiędzy siecią guest a siecią korporacyjną w trybie in-line bridge pozwalającym na wymuszenie wcześniej skonfigurowanych polityk. EGA oferuje uruchomienie portalu obsługowego pozwalającego na generowanie nazw użytkowników oraz co świetnie predysponuje system do zastosowań w salkach konferencyjnych, hotelach czy publicznych sieciach WiFi.

I System kontroli dostępu do sieci – UAC Juniper Networks

- Chcesz zabezpieczyć swoją sieć przed nieautoryzowanymi użytkownikami?
- Masz problem z komputerami rozsiewającymi wirusy z powodu nieaktualnego oprogramowania?
- Chcesz się dowiedzieć jak poprawić bezpieczeństwo swojej sieci nie rezygnując z posiadanej infrastruktury?

Zapraszamy Cię na warsztaty dotyczące systemu kontroli dostępu użytkowników i urządzeń do sieci Juniper Unified Access Control. UAC pozwala na łączenie się z siecią jedynie użytkowników o pewnej tożsamości, dodatkowo sprawdzając stan stacji końcowej. Tym samym można zezwolić na dostęp do sieci tylko komputerom z aktualnym systemem operacyjnym, chronionym systemem antywirusowym i firewallem. Punktem wymuszenia polityki bezpieczeństwa mogą być praktycznie dowolne przełączniki, punkty dostępowe Wi-Fi, a także firewalle Juniper Networks.

- **31 styczeń 2011 (Kraków)**
- **1 luty 2011 (Kraków)**
- **3 luty 2011 (Kraków)**

I Wirtualizacja urządzeń pamięci masowych w oparciu o IBM StorWize V7000

- Chcesz poznać najnowsze trendy związane z urządzeniami pamięci masowych?
- Masz problem z wydajnością i miejscem na używanych systemach dyskowych?
- Chcesz uprościć zarządzanie siecią Storage Area Network?

Jeśli tak, to zapraszamy Cię na warsztaty dotyczące pamięci masowych – IBM Storwize V7000. Urządzenie oprócz „standardowych” funkcji macierzy dyskowych umożliwia wirtualizację zasobów dyskowych pochodzących z innych źródeł. Dzięki wirtualizacji możemy znacznie uprościć zarządzanie środowiskiem SAN, a także wprowadzić wiele uproszczeń wdrażając zaimplementowane funkcjonalności.

- **2 marzec 2011 (Kraków)**

I Platforma serwerowa i wirtualizacja systemów operacyjnych - IBM BladeCenter oraz VMware vSphere4

- Chcesz zmodernizować swoją infrastrukturę serwerową?
- Masz problem z wydajnością swoich systemów operacyjnych i aplikacji?
- Chcesz się dowiedzieć jak sprawnie zarządzać środowiskiem serwerowym oraz w jaki sposób zmniejszyć koszty użytkowania urządzeń?

Zapraszamy Cię na warsztaty dotyczące systemów serwerowych IBM BladeCenter oraz platformy wirtualizacyjnej VMware vSphere 4. Serwery kasetowe firmy IBM umożliwiają szeroki dobór rozwiązań zapewniając przy tym bardzo wysoką dostępność. Urządzenia te charakteryzują się ponadto niskimi kosztami utrzymania oraz ułatwionym zarządzaniem. Oprogramowanie vSphere 4 pozwala na wirtualizację środowiska serwerowego, co umożliwia instalację wielu systemów operacyjnych na jednym serwerze fizycznym. Jednocześnie wprowadza szereg funkcji, które zwiększają bezpieczeństwo i dostępność aplikacji.

- **22 marzec 2011 (Kraków)**
- **24 marzec 2011 (Warszawa)**
- **30 marzec 2011 (Rzeszów)**