

MAGAZYN INFORMACYJNY FIRMY ASCOMP S.A.

SECURIUSZ

NR 9 (31)

IT SYSTEMS SECURITY

utimaco[®]
safe ware

ASCOMP
IT SYSTEMS

Współpraca ASCOMP i Utimaco

Firma ASCOMP S.A. nawiązała współpracę z firmą Utimaco Safeware, wiodącym dostawcą rozwiązań zapewniających poufność danych. Rodzina rozwiązań Utimaco umożliwia bezpieczne przechowywanie danych poprzez wykorzystanie mocnych mechanizmów kryptograficznych do szyfrowania całych dysków, katalogów lub poszczególnych plików. Podstawowym zadaniem produktów SafeGuard Easy, PriveteCrypto, PrivateDisk, LAN Crypt jest dostarczenie użytkownikowi narzędzi zapewniających, że zapisane przez niego na dysku poufne dane nie dostaną się w niepowołane ręce.

Firma Utimaco Safeware została założona w 1983 roku. Główna siedziba znajduje się we Frankfurcie. Centrum

badawczo rozwojowe znajduje się w Aachen.

Chcąc aby produkty były skuteczne w działaniu, a przy tym wygodne dla użytkownika, Utimaco utrzymuje ścisłą współpracę z partnerami: Aladdin Knowledge Systems, Citrix Systems, Microsoft, Miotec, Oberthur Card Systems, Omnickey, O2, Precise, Siemens, Setec, VoiceTrust i Xcellenet.

Wśród klientów Utimaco Safeware można wymienić takie firmy i organizacje jak: VW, Dresdner Bank, Winterthur, Bundeswehr, PricewaterhouseCoopers, Komisja Europejska, Fujitsu Siemens, UBS, ABN AMRO, Allianz, British Telecom, Ministerstwo Sprawiedliwości Holandii. □

Network Access Control (NAC)

NAC czyli sposób na kontrolę stacji przed przyznaniem jej dostępu do sieci stał się tematem bardzo na czasie. Ten trend jest szczególnie zauważalny w dużych firmach, gdzie bardzo ciężko jest zapanować nad zgodnością konfiguracji stacji roboczej z polityką bezpieczeństwa firmy. Kontrola musi się odbywać na każdym styku sieci korporacyjnej ze stacją roboczą, niezależnie od sposobu

jej podłączenia (WLAN, LAN, SSL VPN, IPSec VPN, itd.).

Choć to może temat stosunkowo świeży, są firmy, które od kilku już lat zajmują się tą tematyką. W tym numerze przedstawiamy rozwiązanie firmy Sygate Technologies, które dzięki swojej elastyczności i wielości opcji pozwala wdrożyć kontrolę stacji w praktycznie każdej sieci firmowej.



więcej na stronie 9

Aktualności firmowe Podpisane umowy:

- **Ministerstwo Infrastruktury**
- Umowa serwisowa na system bezpieczeństwa
- **Urząd Wojewódzki w Rzeszowie**
- Sprzedaż firewalle sprzętowych
- **Regionalna Izba Obrachunkowa**
- Sprzedaż firewalle lokalnych
- **Zelnar Zakład Narzędziowy**
- Przedłużenie opieki serwisowej
- **Zelmer**
- Sprzedaż oprogramowania szyfrującego
- **FFil Śnieżka**
- Rozbudowa systemu bezpieczeństwa
- **Puma Polska**
- Sprzedaż firewalle sprzętowych
- **Leroy Merlin**
- Sprzedaż firewalle sprzętowych
- **Media Express**
- Sprzedaż firewalle sprzętowych
- **Crowley Data Poland**
- Umowa o współpracy
- **Black Red White**
- Przedłużenie umowy serwisowej
- **Daab**
- Sprzedaż oprogramowania antywirusowego
- **Fakro**
- Sprzedaż szyfratorów sprzętowych
- **Enix**
- Sprzedaż firewalle sprzętowych
- **Tukaj Mapping Central Europe**
- Sprzedaż firewalle sprzętowych
- **Szpital Specjalistyczny J. Dietla**
- Sprzedaż firewalle sprzętowych
- **Huta LW**
- Dostawa systemu bezpieczeństwa
- **Multistal & Lohmann**
- Sprzedaż firewalle sprzętowych
- **Andra**
- Sprzedaż firewalle sprzętowych
- **Powiatowy Urząd Pracy Bochnia**
- Sprzedaż firewalle sprzętowych
- **Inter-Es**
- Sprzedaż firewalle sprzętowych
- **System Plus**
- Sprzedaż firewalle sprzętowych
- **New Pasja**
- Sprzedaż firewalle sprzętowych
- **JacobsGIBB Polska**
- Sprzedaż firewalle sprzętowych
- **Rzeszowski Zakład Energetyczny**
- Dostawa systemu filtrowania stron WWW
- **Calan Associates**
- Rozbudowa systemu bezpieczeństwa

□



WISŁA PANY!

Ten tytuł zaczerpnąłem nie tylko z podwórka. Mój wspaniały kolega i przyjaciel – Zbigniew Grabis zatytułował artykuł wstępny w poprzednim SECURIUSZU – „IP pany”. I oczywiście miał rację co ze zwykłą sobie swadą i zręcznością udowodnił.

Wiedząc, że mam nawiązać niniejszym artykułem do poprzedniego usiadłem sobie wygodnie w fotelu przed telewizorem aby pomyślnym wynikiem meczu Panathinaikos Ateny – Wisła Kraków – przyklepać zaplanowany wcześniej tytuł.

Niestety, życie płata niespodzianki. Statystycznie rzecz biorąc tylko co druga niespodzianka jest pomyślna. A ta była całkiem fatalna. Przypomnę, że w Krakowie Wisła wygrała 3:1 a w rewanżu przegrała 1:4, tracąc szansę na wejście do Ligi Mistrzów. Czwartą szansę pod rząd.

Już zastanawiałem się jaki nowy tytuł zaproponować, kiedy przyszło mi do głowy, jaka to wspaniała hiperbola literacka jawi się na naszych oczach pomiędzy fatalnym wynikiem Wisły a bezpieczeństwem.

„Hiperbola literacka” to jak zapamiętałem ze szkoły było pojęcie całkowicie niezrozumiałe na lekcjach języka polskiego dla uczniów, którzy choć trochę umieli matematykę. Ale będę pamiętał, że „Dżuma” Camusa – to ci dopiero hiperbola literacka była.

Wracając do Wisły i do bezpieczeństwa. Problemem Wisły było to, żeby sobie nie dać strzelić bramek. A przy najmniej nie za dużo.

Problemem bezpieczeństwa jest z grubsza rzecz biorąc – to samo. Żeby do naszej siatki (sieci) nikt nie strzelił gola.

Wiśle nie wyszło, ale NASI CZYTELNICY i nasza firma – my dalej jesteśmy w grze. Oby jak najdłużej.

A pojawia się coraz więcej technik i narzędzi aby włamać się do naszej sieci. Ale i my mamy coraz więcej narzędzi do obrony. Niedawno lekiem na wszelkie

zło miał być firewall. Potem ochrona miała być kompleksowa i lekiem był IDS (Intrusion Detection System) a teraz króluje IDP (Intrusion Detection and Prevention).

Niezwykle ciekawe zagadnienie to bezpieczeństwo w infrastrukturach mobilnych. Mamy tu do czynienia z naturalnym konfliktem – jak najbezpieczniej (czyli najbardziej skomplikowanie) – przeciwko jak najwygodniej (czyli najprościej). O tym co świat na ten temat wymyślił poświęcamy trochę miejsca w niniejszym numerze. Zachęcamy Cię drogi Czytelniku, abyś dobrze zabezpieczył swojego notebooka. Żebyś nie żałował jak Wisła po ostatnim meczu.

W niniejszym wydaniu wydaje się godne do zarekomendowania przeczytanie w pierwszej kolejności o nowych rozwiązaniach firm Sygate i WildPackets.

Firma Sygate zajmuje się kontrolą dostępu do sieci – czyli zagadnieniem mówiąc skromnie kluczowym. Przypomina mi się taki amerykański kawał rysunkowy: Zadowolony pies siedzi przed komputerem i mówi. „Každy wie, że mam na imię Tom”. „Každy wie, że mój adres IP jest taki to a taki”. „Ale nikt nie wie, że ja jestem psem”.

Drugie rozwiązanie (WildPackets) jest adresowane dla profesjonalnych administratorów dużych i wymagających sieci. Tutaj można się spełnić zawodowo. Jak się widzi takie narzędzia to w następnym wcieleniu chce się być administratorem.

Niezależnie od osobistych upodobań wydaje się, że przeczytanie wszystkiego jest godne polecenia co z głębi serca Drogim Czytelnikom podpowiadam.

Natomiast Wiśle Kraków – życzymy wytrwałości, uporu i szczęścia. Bo szczęście sprzyja lepszym. Fortes Fortuna Adiuvat.

Andrzej Szymowski
Wasz „nowy” Cenzor Naczelny.

Czy zastanawiali się Państwo, ile jest wart Wasz laptop? To jest pytanie, na które praktycznie nikt nie jest w stanie udzielić odpowiedzi. Bo jak wycenić informacje, które na nim posiadamy. Jakie konsekwencje nam grożą gdy laptop wpadnie w niepowołane ręce. Ile nas będzie kosztowała strata naszego laptopa jeżeli zapisane na nim strategia firmy, dane finansowe lub inne ważne dokumenty wpadną w ręce konkurencji. Choć nikt na tak postawione pytanie nie jest w stanie odpowiedzieć konkretnie to niemal wszyscy twierdzą, że dużo – nieporównywalnie więcej niż wart jest sam laptop.

A kradzieże się zdarzają: przypadkowe, na zamówienie, w pociągu, restauracji, hotelu. O niektórych „spektakularnych” kradzieżach, znanym osobom, politykom dowiadujemy się co jakiś czas z mediów.

Jak możemy zabezpieczyć się przed kradzieżami laptopów? Praktycznie nie możemy, ale możemy zabezpieczyć przed kradzieżą dane znajdujące się na naszym laptopie.

Metoda, dzięki której możemy to zrobić nosi nazwę Pre Boot Authentication (PBA).

Głównym zadaniem metody PBA jest uniemożliwienie osobom nieupoważnionym dostępu do danych składowanych na laptopie. Jest to zapewnione poprzez zaszyfrowanie całego dysku. Zaszyfrowane są zarówno dane jak i system operacyjny.



System działa w następujący sposób. Użytkownik włącza laptopa. Standardowo startuje BIOS, następnie system PBA pyta nas o login i hasło. Jeżeli login lub hasło są błędne, dysk pozostaje zaszyfrowany. Natomiast w przypadku poprawnego uwierzytelnienia, na podstawie wprowadzonych przez użytkownika informacji generowany jest klucz, który pozwala na rozszyfrowywanie dysku. Ze względu na wydajność i funkcjonalność



Pre Boot Authentication

system PBA nie rozszyfrowuje całego, a tylko te dane, które dotyczą systemu operacyjnego. Po uruchomieniu systemu operacyjnego każda informacja, której żąda system jest rozszyfrowywana i podawana do systemu operacyjnego. W momencie zakończenia pracy, zamknięcia systemu wszystkie dane na dysku pozostają zaszyfrowane

Jak łatwo zauważyć z punktu widzenia użytkownika pojawia się tylko dodatkowe logowanie przy uruchomieniu komputera. PBA nie wpływa na dalszą pracę użytkownika na komputerze.

Myślę, że sam mechanizm PBA jest

mnie są ważne. Zaczę od zarządzania, bo to od niego myślę, najbardziej zależy czy wdrożenie PBA zakończy się sukcesem. Pisząc zarządzanie myślę o możliwościach bezpiecznego i szybkiego wdrożenia systemu na dużą skalę, dostępnych procedurach na wypadek zapomnienia hasła (od tego



zależy ile pracowników helpdesku jest potrzebnych oraz po jakim czasie pracownik odzyska dostęp do komputera), a także w jaki sposób można monitorować system.

Kolejnym ważnym elementem jest funkcjonalność takiego rozwiązania. Czy można go zintegrować

hasła do systemu operacyjnego, domeny lub aplikacji. Technologia PBA, zabezpieczając dane przenoszone na laptopie, powinna być jak najmniej uciążliwa dla użytkowników.

Należy również zwrócić uwagę na możliwości uwierzytelniające. W standardzie przewidziane są logi i hasło. Ale może to za mało. Może trzeba dać użytkownikowi token bo tego od nas wymaga polityka bezpieczeństwa? To kolejny element, na który powinniśmy zwrócić uwagę przy wyborze systemu. W przypadku obsługi tokenów, system musi również mieć wbudowane procedury awaryjne na wypadek ich zniszczenia lub zagubienia.

Pracownicy firm stają się coraz bardziej mobilni, a ich miejsce pracy jest tam gdzie jest ich laptop a nie biurko, dlatego też rozwiązania PBA będą zdobywać coraz większą popularność. Warto jednak przed wdrożeniem takiego systemu zastanowić się nad potrzebną funkcjonalnością. W tym numerze przedstawiamy rozwiązanie PBA firmy Utimaco SafeGuard Easy. Zapraszam do lektury.

Krzysztof Tyl



pro-
sty.

Na co więc należy zwrócić uwagę wybierając system?

Jest kilka elementów, które według

przykład z systemem SSO, by użytkownicy nie musieli wprowadzać

utimaco®
s a f e w a r e

Rozwiązania SafeGuard firmy Utimaco



Ludzie z Utimaco naprawdę znają się na szyfrowaniu danych. Taki wniosek można wysnuć przeglądając portfolio produktów firmy Utimaco Safeware AG. Rozwiązania tej europejskiej firmy, której centrala mieści się we Frankfurcie umożliwiają szyfrowanie plików, dysków, katalogów. Pełna gama rozwiązań, które ze sobą mogą współpracować pozwala na budowę kompleksowego systemu bezpieczeństwa danych, zgodnie z naszą polityką bezpieczeństwa. Tym samym produkty firmy Utimaco pozwalają zabezpieczyć poufne informacje przed różnymi zagrożeniami.

Pierwszym i można powiedzieć sztandarowym produktem firmy jest SafeGuard Easy, system zabezpieczający dane przechowywane na laptopie. SafeGuard Easy jest systemem Pre-Boot Authentication, umożliwiającym szyfrowanie całej zawartości dysku twardego stacji roboczej, najczęściej laptopa. SG Easy zapewnia bezpieczne przenoszenie danych na laptopie. Ma to szczególne znaczenie w czasie podróży, gdy laptop

jest narażony na zgubienie lub kradzież. Dane przechowywane na laptopie pozostają niedostępne dla ludzi, którzy chcieliby je sprzedać lub wykorzystać. Należy oczywiście pamiętać, że dane pozostają zaszyfrowane tylko gdy stacja robocza jest wyłączona. Gdy włączymy komputer, dokonamy uwierzytelnienia, dane stają się dostępne, zarówno bezpośrednio, jak i poprzez sieć. Dlatego hasło jest kluczowe, z punktu widzenia bezpieczeństwa. By podnieść poziom bezpieczeństwa w SG Easy uwierzytelnienie hasłem można zastąpić uwierzytelnieniem poprzez eToken firmy Aladdin lub w przypadku laptopów IBM, poprzez wbudowany w nich czytnik biometryczny. SafeGuard Easy umożliwia centralne



zarządzanie oraz integracje z systemem Single Sign On.

Projektanci systemu SG Easy przewidzieli bardzo elastyczny system zarządzający, pozwalający zarówno na szybkie wdrożenie i łatwą opiekę serwisową nad systemem, ale także zdefiniowanie bezpiecznego scenariusza awaryjnego na wypadek, gdy użytkownik zgubi token lub po prostu zapomni hasła. W takim przypadku możemy zdefiniować nowe hasło (może być to również hasło jednokrotnego użycia). Wykorzystywany jest do tego bezpieczny schemat challenge-response. Użytkownik wciska klawisz F9 i na ekranie pojawia się ciąg znaków, który przez telefon może być przekazany do operatora. Operator po krótkim uwierzytelnieniu wygeneruje i przekaże nowe hasło z powrotem do użytkownika. Można również wdrożyć serwer VoiceTrust, który uwierzytelnia użytkownika na podstawie głosu a następnie obsługuje procedurę challenge-response bez konieczności włączania w nią operatora.

Ponieważ dla prawidłowego działania systemu SG Easy, a także systemu operacyjnego kluczowe znaczenie ma Master Boot Record, firma Utimaco wbudowała w swoje oprogramowania procedury awaryjne na wypadek zniszczenia MBR, np. przez wirus. SG Easy jest w stanie automatycznie wykryć takie zdarzenie, a następnie przywrócić poprawną wartość MBR.

Innym produktem firmy Utimaco jest SafeGuard PrivateCrypto, rozwiązanie służące do szyfrowania plików oraz załączników korespondencji elektronicznej email. SG PrivateCrypto integruje się z Microsoft Windows Explorer. Dzięki temu możemy w szybki i wygodny sposób szyfrować pliki, które następnie będą przesłane pocztą, nagrane na CD, lub skopiowane na dysk USB lub urządzenie PDA. Wystarczy aby użytkownik



kliknął prawym klawiszem myszy na plik, który chce zaszyfrować, a pojawi się standardowe menu z dodatkową opcją „zaszyfruj”, którą należy wybrać. Implementację takiego rozwiązania ułatwia fakt, że zaszyfrowane pliki nie wymagają instalacji oprogramowania po stronie odbiorcy takiego pliku. Plik może być zaszyfrowany z opcją „self-extracting”. Wystarczy znać hasło, którym zostało zaszyfrowane.



W rozszerzonym przez SG PrivateCrypto menu znajduje się jeszcze jedna ciekawa opcja, która umożliwia bezpieczne usuwanie plików. Usuwany plik jest nadpisany trzykrotnie losowo wygenerowanymi liczbami.

Oprócz szyfrowania plików z poziomu Explorera Windows, za pomocą SG PrivateCrypto możemy szyfrować załączniki poczty email. Funkcjonalność ta pozwala z poziomu klienta poczty zaszyfrować plik przed wysłaniem. SG PrivateCrypto integruje się z klientami pocztowymi Microsoft Outlook, Outlook Express, Netscape Messenger, Lotus Notes oraz Pocket Explorer (Windows Mobile).

Dodatkowo SG PrivateCrypto podczas szyfrowania dokonuje wydajnej kompresji danych.

Korzystając z PrivateCrypto użytkownik musi pamiętać, żeby pliki nad którymi pracuje zaszyfrować po skończonej pracy. Tylko w ten sposób pliki będą zabezpieczone przed niepożądanym dostępem. Jeżeli taki scenariusz wydaje się uciążliwy należy zainteresować się rozwiązaniem SafeGuard PrivateDisk, który umożliwia tworzenie zaszyfrowanych wirtualnych dysków. Utworzone wirtualne

dyski mogą być zamapowane do systemu operacyjnego. Po utworzeniu takiego zaszyfrowanego dysku, każdy plik, który zapiszemy na tym dysku będzie automatycznie zaszyfrowany. Proces ten jest przezroczysty dla użytkownika. Nie tylko pliki są zabezpieczone, również struktura tego dysku nie jest dostępna osobom nieupoważnionym. W momencie pracy na plikach umieszczonych na wirtualnym dysku, rozszyfrowane dane znajdują się tylko w pamięci komputera, a nie na dysku. Wirtualne dyski mogą rezydować zarówno na dyskach sieciowych, dyskach lokalnych jak i dyskietkach, CD, DVD itp. Wszystkie informacje znajdujące się na wirtualnym dysku są szyfrowane jednym kluczem.

W obrębie jednego dysku fizycznego można utworzyć kilka dysków wirtualnych szyfrowanych różnymi kluczami. PrivateDisk, podobnie jak SG Easy, umożliwia uwierzytelnienie użytkownika za pomocą tokenów Aladdin i tak jak on ma wbudowane procedury awaryjne na wypadek zgubienia hasła lub tokena. Natomiast zasadnicza różnica pomiędzy tymi produktami to fakt, że SG Easy zabezpiecza dane tylko w momencie gdy stacja jest wyłączona.

SafeGuard PrivateDisk choć oprócz wersji „domowej” dostępny jest też w wersji korporacyjnej to jednak ma pewne ograniczenia, które może rozwiązać kolejny produkt Utimaco – SafeGuard LAN Crypt.

LAN Crypt jest rozwiązaniem zapewniającym szyfrowanie plików i katalogów w systemie wieloużytkownikowym. LAN Crypt wykorzystywany jest w środowisku sieciowym, aby zapewnić pełną poufność danych, nad którymi pracują różne zespoły i departamenty. Z punktu widzenia poszczególnych użytkowników korzystających ze swoich danych przechowywanych np. na dysku sieciowym nic się nie zmienia. Jeżeli mają uprawnienia do odczytu lub zapisu na danym

dysku mogą pracować spokojnie. Dla nich system jest przezroczysty. Mechanizmy bezpieczeństwa działają w tle a ich dane są przechowywane w formie zaszyfrowanej. Dane są zabezpieczone przed włamaniem do serwera. Dodatkowo LAN Crypt umożliwia odseparowanie uprawnień administratora serwera od administratora bezpieczeństwa. Dzięki temu administrator serwera mimo, że ma uprawnienie żeby odczytać każdy plik i katalog na serwerze, nie będzie w stanie odczytać przechowywanych na serwerze informacji.

Jeżeli rozdzielenie uprawnień administratora serwera od administratora bezpieczeństwa nie jest konieczne można zintegrować LAN Crypta z ActiveDirectory, Novell eDirectory lub kontrolerem domeny.

Przezroczystość systemu dla użytkownika objawia się również tym, że wszystkie reguły współdzielenia danych na serwerze pozostają niezmienione po wdrożeniu LAN Crypta.

LAN Crypt posiada rozbudowany system zarządzania pozwalający wydajnie i przejrzysto zarządzać wszystkimi kluczami i uprawnieniami w systemie. W sieciach rozproszonych pozwala na delegację uprawnień administracyjnych według zdefiniowanej hierarchii.

W ofercie znajduje się również rozwiązanie SafeGuard PDA, które pozwala przenieść funkcjonalność PrivateCrypto oraz PrivateDisk na urządzenia PDA. SG PDA jest w pełni zgodny ze swoimi odpowiednikami na PC.

Do każdego z tych produktów można dokupić SafeGuard Advanced Security, który może rozszerzyć funkcjonalność opisanych powyżej produktów. W zależności od tego jakie moduły zostaną wybrane można dodać uwierzytelnianie z wykorzystaniem SmartCard, SSO, zaawansowane zarządzanie uprawnieniami, obsługę certyfikatów X.509, kontrolę z jakich nośników danych może korzystać użytkownik (CD, dyskietka, dysk USB).

Na pierwszy rzut oka wydaje się, że rozwiązania Utimaco są do siebie funkcjonalnie bardzo podobne i wystarczyłoby jedno z nich. Istnieją jednak zasadnicze różnice między nimi i to właśnie na nie należy zwrócić uwagę zapoznając się z rodziną rozwiązań SafeGuard. Zostały one tak zaprojektowane, żeby sprostać wymaganiom polityki bezpieczeństwa każdej firmy.

Krzysztof Tyl



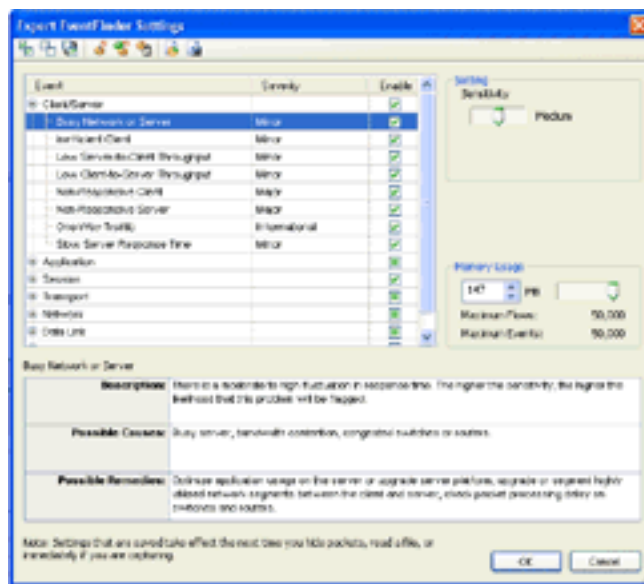
Rodzina produktów EtherPeek firmy WildPackets

W poprzednim numerze przedstawiliśmy Państwu możliwości oprogramowania AiroPeekNX, służącego do kompleksowej analizy sieci bezprzewodowych. Dzisiaj chcielibyśmy zaprezentować całą rodzinę produktów, służących analizie klasycznych sieci – pod nazwą EtherPeek. Obecnie dostępne są cztery produkty, które służą analizie sieci pod różnymi kątami. Podstawowym i najbardziej rozpowszechnionym pozostaje od lat EtherPeek NX – niezwykle skuteczny analizator protokołów. Kolejnym produktem jest EtherPeek SE – który pozwala w kompletny sposób poddać analizie sieci Ethernetowe, wspomaga debugging i poszukiwanie problemów w rozproszonej architekturze sieciowej. Produktem specjalizowanym do analizy sieci VoIP jest EtherPeek VX. Istnieje również wersja EtherPeeka przeznaczona dla komputerów z systemem Mac OS X.

EtherPeek NX to znakomita propozycja dla każdego administratora sieci, szczególnie dla administratorów sieci większych. Dzięki unikalnym możliwościom dekodowania ponad tysiąca różnych protokołów sieciowych (ich dokładna lista znajduje się na stronie http://www.wildpackets.com/support/product_support/etherpeek/decodes) może analizować działanie praktycznie

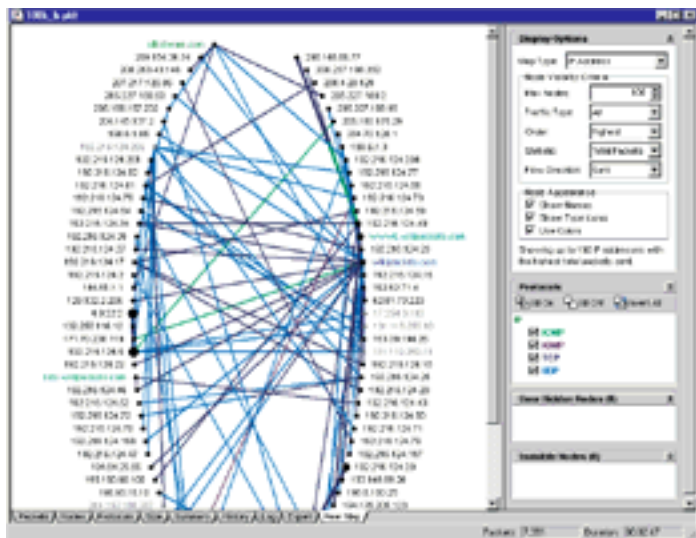
całej sieci – z uwzględnieniem nawet najbardziej specyficznych wymagań użytkowników. Z drugiej strony, dzięki wykorzystaniu specjalnych mechanizmów, możliwa jest analiza wielu segmentów sieci jednocześnie z wykorzystaniem wielu interfejsów. Daje to ogromne możliwości analizy nawet z użyciem pojedynczego stanowiska, na którym instalowany jest produkt. Sama analiza przebiega w czasie rzeczywistym, zawartość ramek większości znanych protokołów staje się podstawą do tworzenia różnorodnych raportów. Analizowane są również parametry sieciowe takie jak czas odpowiedzi p o s z c z e g ó l n y c h nodów sieci, przepustowość poszczególnych segmentów, opóźnienia. Wszystkie parametry badanej sieci dają w rezultacie możliwość generowania w czasie rzeczywistym znakomitego odwzorowania działania sieci w dostępnych raportach, analizach. Możliwe jest graficzne przedstawienie połączeń pomiędzy

specjalizowane narzędzia wspomagające bezpieczeństwo danych – raporty ukazujące potencjalne zagrożenia, luki bezpieczeństwa, nieautoryzowany dostęp do zasobów. Dzięki modułom zdalnym możliwe jest analizowanie danych zbieranych w segmentach sieci, do których samo urządzenie analizujące nie jest podłączone – dane z niewielkich modułów przesyłane są do centralnego serwera, gdzie podlegają analizie przez



EtherPeeka. Najważniejszą różnicą pomiędzy produktem EtherPeek NX a konkurencją (a także EtherPeekiem SE) jest jednak coś innego – ogromna wiedza o zachowaniach sieci, która została zaimplementowana w modułach Expert Analysis oraz Expert ProblemFinder. Moduły te umożliwiają odnajdywanie problemów sieciowych niewidocznych bez użycia specjalizowanych narzędzi – a także, co bardzo ważne – podają konkretne informacje o sposobach ich rozwiązania, prawdopodobnych przyczynach, oraz wszystkich objawach obserwowanego zjawiska. Ciekawą funkcją jest również możliwość szybkiego (jedno kliknięcie) odfiltrowania tylko interesujących nas informacji – np. o danym komputerze i jego połączeniach.

Do podstawowej funkcjonalności EtherPeeka dodano możliwości szczegółowej analizy ruchu VoIP – tworząc tym samym produkt EtherPeek VX. Umożli-



wia on dekodowanie transmisji głosowej, analizę przepływów rozmów, ich jakości, obserwowanych zakłóceń, sygnalizacji z użyciem rozmaitych protokołów (w tym SIP, H.323, MGCP, Megaco, SCCP (Skinny v3.0.3), NCS, TGCP, SIPT, C-SIP i inne). Wszystkie niepokojące zjawiska są w czasie rzeczywistym raportowane, istnieją możliwości alarmowania administratorów. Możliwe jest prowadzenie próbnych rozmów, czy analizy zapisanych sesji pod kątem wpływu opóźnień na jakość rozmów. Dla każdej firmy, która zainwestowała w technologię VoIP produkt ten oferuje znakomite możliwości kontroli wykorzystania, poprawnego działania i co za tym idzie odpowiedniego dopasowania do rzeczywistych potrzeb użytkowników istniejących rozwiązań sprzętowych.

Wszystkie produkty firmy WildPackets oferują znakomity interfejs, efektywne działanie i ogromną liczbę dostępnych raportów. Dla każdego administratora sieci, który dba o utrzymywanie jej w jak najlepszym stanie produkty te stanowią nieocenioną pomoc i podstawowe narzędzie. Z uwagi na swoją popularność i wysokie oceny specjalistów (produkt ten nagrodzono min. kilkakrotnie przyznaniem tytułu Network Magazine „Product of the Year”, czy Network Computing „Well-Connected”) EtherPeek stanowi propozycję, którą administrator powinien rozważyć przy zakupie rozwiązania wspomagającego zarządzanie siecią.

Miłosz Franaszek



eIQ networks

- nowe licencjonowanie

Nazwa producenta	Model
Astaro	ASG 110, ASG 120
Clavister	SG 30 Series
Cisco	Pix 501, 505 i 506
Cisco Routers	1700 Series, 1800 Series i 2600 Series
CyberGuard	SG300, SG530 i SG550
Fortinet	FortiGate 50, 60, FortiWifi-60 i 100
GNAT	GB-200
McAfee	WebShield e250 tylko
Microsoft ISA	Single processor edition tylko
Juniper Routers	2300 Series
Juniper/NetScreen Firewall	5GT Series
SNORT IDS	Wszystkie
ServGate	100 Series, M30 Series
SonicWALL	TZ 150, TZ170, SOHO TZ, SOHO TZW, PRO 1260
Symantec	Gateway Security 320, 360, 420, 440, 460
WatchGuard	Firebox X5, Firebox X15, SOHO 6, SOHO 6 Wireless

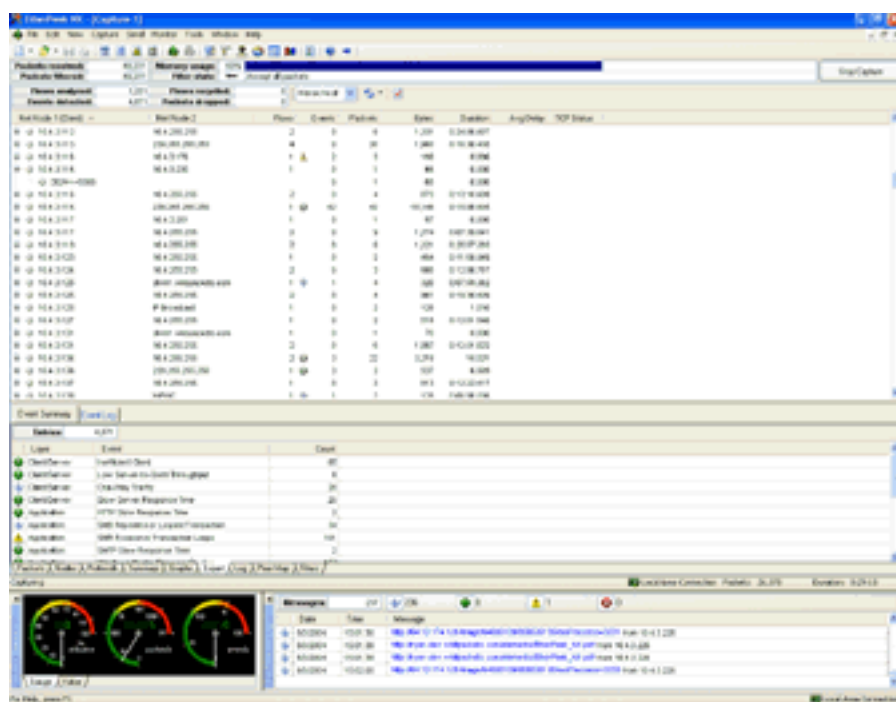
Firma eIQ networks wprowadziła do oferty zmiany w licencjonowaniu swoich głównych produktów, jakimi są Firewall Analyzer oraz Security Analyzer. Nowa

polityka firmy przewiduje sprzedaż tych produktów po cenach zależnych od ich wykorzystania. Tym sposobem wprowadzono dwa segmenty klientów, do których skierowana jest oferta eIQ networks. Pierwszy z nich to tzw. SOHO, czyli użytkownicy domowi oraz małe firmy zainteresowane analizą urządzeń, których cena nie przekracza \$1500. Produkt oferowany dla tego segmentu posiada funkcjonalność starego Firewall Analyzera – jednak w celu zaznaczenia przeznaczenia zmianie uległa jego nazwa na Network Security Analyzer for SOHO.

Kompletna lista urządzeń dla wersji SOHO znajduje się w tabelce.

Drugim segmentem są duże firmy i przedsiębiorstwa chcące poddać analizie urządzenia wyższej klasy. Dla tych klientów oferowany jest Network Security Analyzer.

Michał Putała





MailMarshal SMTP

- kompleksowe rozwiązanie antyspamowe

SPAM – czyli niechciane wiadomości to wciąż problem dużej ilości użytkowników domowych oraz dużych i małych przedsiębiorstw. Skutecznie przeszkadza w pracy, ogranicza produktywność i

produkt firmy NetIQ o nazwie MailMarshal SMTP.

MailMarshal SMTP jest oprogramowaniem antyspamowym instalowanym w środowisku Windows 2000/XP/

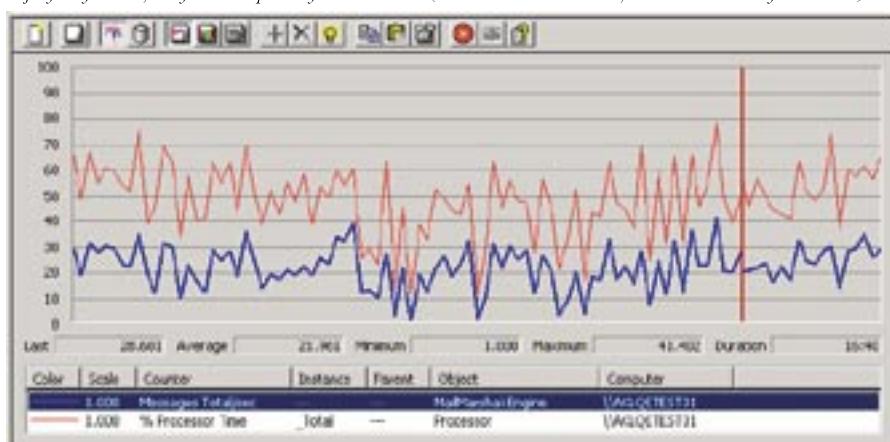
oraz włączyć obsługę active scripting w opcjach przeglądarki, gdyż bez tego nie dostaniemy się do menu instalacyjnego. Opcje menu oferują zainstalowanie programu na niezależnym serwerze lub dołączenie do istniejących serwerów, które dzielą opcje konfiguracyjne. Możliwa jest także instalacja klientów, którzy zostaną wykorzystani do zdalnej konfiguracji serwera. Zarówno historia wiadomości jak i opcje konfiguracji przechowywane są w bazie danych. MailMarshal współpracuje z Microsoft SQL Server 2000 i jest dostępny wraz z tym oprogramowaniem. W skład oprogramowania wchodzi ponadto moduł raportowania, który może być zainstalowany na wielu stacjach roboczych oraz moduł do webowego zarządzania wiadomościami skierowanymi do kwarantanny.

Podczas pracy MailMarshal dzięki zaawansowanemu silnikowi SpamCensor z dużą skutecznością chroni użytkowników przed niechcianymi wiadomościami email. Oferuje wygodne zarządzanie z wewnątrz jak i zewnątrz sieci, które odbywa się w prosty i wygodny sposób z poziomu konsoli webowej. MailMarshal SMTP umożliwia filtrowanie wiadomości na podstawie zarówno słownikowego jak i inteligentnego skanowania zawartości. Obsługuje również większość formatów kompresujących i analizuje pliki zawarte w skompresowanych archiwach. W przypadku analizy załączników bardzo przydatna jest obsługa ponad 170 różnych typów plików, która daje pewność, że spam zawarty w załączniku zostanie poprawnie zidentyfikowany i zablokowany. Ponadto MailMarshal wspiera bardzo przydatną funkcję jaką jest ESMTP – czyli blokowanie zbyt dużych wiadomości zanim dotrą do sieci. Jest to bardzo przydatne w celu zabezpieczenia sieci przed przeciążeniem. Nie trudno wyobrazić sobie sytuację gdy duże wiadomości email paraliżują ruch w sieci, doprowadzając ją do częściowego lub całkowitego zablokowania. Dzięki produktowi firmy NetIQ taka sytuacja nigdy nie będzie mieć miejsca, gdyż konfiguracja ESMTP umożliwia zadanie z góry maksymalnego rozmiaru wiadomości, powyżej którego wiadomości w ogóle nie zostaną dopuszczone do wnętrza sieci.

To wszystko czyni MailMarshal SMTP bardzo skutecznym narzędziem do walki ze spamem, którego wdrożenie zaleca się każdemu przedsiębiorstwu, firmie, której sieć jest narażona na przeciążenia i kłopoty związane z niechcianymi wiadomościami.

Michał Putała

Pojedynczy serwer, wszystkie komponenty na 1 serwerze (Dual 2.6 GHz Xeon CPU, 2 GB RAM i dwa dyski 146 GB)



Średnio 21 wiadomości / sekundę, 5GB wiadomości email przetworzonych w ciągu godziny.

zwyczajnie denerwuje. Około 60%-70% wiadomości docierających do przedsiębiorstw to spam, który bardzo często doprowadza do przeciążeń w sieci. Nie dziwi więc chęć stworzenia uniwersalnego, łatwo integrującego się z wewnętrznymi systemami pocztowymi przedsiębiorstw, oprogramowania antyspamowego. Wśród wielu pozycji na uwagę zasługuje

2003 i służącym do ochrony serwerów pocztowych SMTP takich jak Postfix, Sendmail, Lotus Domino, MS Exchange i innych. Instalacja programu nie sprawia większych problemów, jednakże należy posiadać jako domyślną przeglądarkę internetową Internet Explorer w wersji 5.0 lub nowszej, trzeba pamiętać o deaktywacji blokowania wyskakujących okienek

Serwer Dual 2.6 GHz Xeon CPU, 2 GB RAM i dwa dyski 146 GB jako MailMarshall Node. Wszystkie inne komponenty zainstalowane na innym serwerze.



Średnio 33 wiadomości / sekundę, 7GB wiadomości email przetworzonych w ciągu godziny.



Sygate Network Access Control

Kontrola dostępu do sieci nie jest tematem nowym. Mówi się o niej zarówno w kontekście silnego uwierzytelniania, bezpiecznych połączeń szyfrowanych jak i myśląc o kontroli konfiguracji stacji roboczych przed przydzieleniem im prawa dostępu do sieci korporacyjnej. Dziś skupię się na tym ostatnim zagadnieniu.

O opracowywanych standardach dotyczących tego zagadnienia, a także o nowych rozwiązaniach z tej dziedziny pisaliśmy już wielokrotnie na łamach Securiusza. Z naszych kilkuletnich doświadczeń w tej tematyce wynika, że początkowo była ona dla osób odpowiedzialnych za bezpieczeństwo sieci ciekawą koncepcją, potem nową, wchodząca technologią, a teraz jest tematem numer jeden jeżeli chodzi o bezpieczeństwo sieci. Praktycznie wszyscy liczący się producenci sprzętu sieciowego budują swoje rozwiązania lub przynajmniej ich marketingowy wizerunek z silnym naciskiem na zagadnienia dotyczące kontroli dostępu do sieci. Obecnie wszystkie nowe urządzenia sieciowe klasy „enterprise” posiadają takie mechanizmy. Największą kampanie marketingową, zwracającą uwagę na zagadnienie związane kontrola dostępu do sieci prowadzi firma Cisco. I mimo, że jej sztandarowe rozwiązanie w tej dziedzinie – NAC (Network Admission Control) jest jeszcze w fazie mocno początkowej, to myślę, że jest ona potrzebna, ponieważ buduje wśród administratorów oraz oficerów bezpieczeństwa świadomość potencjalnych zagrożeń a także zwiększa ich wiedzę o technologiach zapewniających bezpieczny dostęp do sieci. W poniższym artykule chciałbym, krótko przedstawić co kryje się angielską brzmiącą nazwą Network Access Control, następnie przedstawić rozwiązanie, które moim zdaniem jest obecnie najbardziej zaawansowanym i najbardziej uniwersal-

nym narzędziem do kontroli dostępu do sieci – Sygate Network Access Control.

Na kontrolę dostępu do sieci składa się kilka elementów, które razem tworzą schemat bezpieczeństwa, dzięki któremu dostęp do sieci uzyskają tylko stacje posiadające odpowiedni poziom bezpieczeństwa.

Wspomniany poziom bezpieczeństwa należy określić w polityce bezpieczeństwa, która jest podstawą każdego systemu bezpieczeństwa, w szczególności również systemu Network Access Control. Polityka określa wymagania dotyczące urządzeń, które mają uzyskać dostęp do sieci. To w niej administrator bądź oficer bezpieczeństwa definiuje konfigurację stacji roboczej, którą chce wymusić na wszystkich komputerach, które uzyskają dostęp do sieci korporacyjnej. W praktyce zawiera ona wymagania dotyczące oprogramowania, które musi być zainstalowane na stacji: aktualne patch'e, oprogramowanie antywirusowe z odpowiednio „świeżymi” bazami sygnatur, lokalny firewall i IPS z aktualnymi wzorcami ataków i prawidłową konfiguracją, itd. Ilość wymagań jest dowolna i zależy do twórców polityki bezpieczeństwa.

Gdy mamy już zdefiniowaną politykę, do głosu dochodzi mechanizm sprawdzający, który porównuje konfigurację stacji dołączającej się do sieci ze zdefiniowaną polityką bezpieczeństwa. Aby zapewnić pełne bezpieczeństwo sieci, sprawdzenie komputera musi być wykonane niezależnie od sposobu podłączenia stacji do sieci: LAN, WAN, WLAN, IPSec, SSL VPN.

Bazując na wynikach działania mechanizmu sprawdzającego, mechanizm kontroli dostępu przydziela każdej podłączającej się stacji odpowiedni poziom dostępu. Przykładowo, system, który jest w pełni zgodny ze zdefiniowaną polityką

bezpieczeństwa dostaje pełny dostęp, natomiast stacja niespełniająca polityki może zostać zablokowana, lub przeniesiona na poziom kwarantanny.

I to właśnie kwarantanna jest kolejnym elementem Network Access Control. Bez kwarantanny mogłoby się okazać, że cała koncepcja kontroli dostępu do sieci nie ma szans na wdrożenie, ponieważ wymaga utrzymywania ogromnych zasobów helpdesku, który aktualizowałby stacje do poziomu zgodnego z polityką bezpieczeństwa. Kwarantanna jest poziomem dostępu do tej części sieci, w którym użytkownik może dokonać aktualizacji konfiguracji stacji roboczej. Cały ten proces powinien odbywać się automatycznie, a na zakończenie powinna zostać wykonywana ponowna weryfikacja poziomu bezpieczeństwa stacji. Jeżeli proces kwarantanny przebiegł prawidłowo to stacja otrzymuje dostęp do sieci korporacyjnej.

Mamy politykę bezpieczeństwa, mechanizmy sprawdzające, przydzielające dostęp oraz kwarantanny. Można by rzec, że to już wszystko. Prawie...

Bo co prawda powyższe mechanizmy zapewniają nas, że tylko stacja zgodna z polityką uzyska dostęp do sieci korporacyjnej, to jednak potrzebujemy jeszcze mechanizm, który będzie monitorował stację, czy jej zgodność z polityką bezpieczeństwa nie zmieniła się (np. przez wyłączenie oprogramowania antywirusowego). Monitoring ma na celu ciągłą kontrolę stacji, pod kątem jej zgodności z polityką oraz ewentualne przełączenie stacji na poziom kwarantanny, w przypadku wykrycia jakichkolwiek niezgodności.

Oprócz tych elementów, system Network Access Control powinien oczywiście spełniać ogólne wymagania systemu korporacyjnego jak: skalowalność,

centralne zarządzania, niezawodność, mechanizmy ułatwiające wdrożenie w środowisku rozproszonym oraz uniwersalność zapewniająca możliwość pracy w środowisku heterogenicznym.

Opisany przeze mnie ogólny model rozwiązania typu Network Access Control został przyjęty przez instytucje zajmujące się badaniami i analizą rynku i technologii IT jak np. Gartner Group.

Przedstawiając rozwiązanie firmy Sygate Technologies – Sygate Universal Network Access Control – mógłbym napisać, że jest to produkt, który jako jedyny dostępny na rynku spełnia wszystkie założenia modelu Networks Access Control i na tym zakończyć. Jednak pozostałby niedosyt nie tylko u czytających ten artykuł, ale również u mnie, ponieważ jestem pod dużym wrażeniem tego co przygotowała firma Sygate dla bezpiecznego dostępu do sieci.

Tytułem wstępu myślę, że warto w tym miejscu wspomnieć kilka słów o firmie Sygate Technologies, która od wielu lat specjalizuje się w kontroli dostępu do zasobów. Pierwsza wersja komercyjna rozwiązania realizującego ideę Network Access Control – Sygate Secure Enterprise 2.0 została wprowadzona na rynek w 2001 roku, kiedy jeszcze inni ledwie zaczęli o tym myśleć o rozpoczęciu takich projektów. Oprócz rozwiązania klasy „enterprise” firma Sygate jest pro-

ducentem firewlla osobistego dla rynku SOHO i SMB – Personal Firewall PRO – z którym dość dużo osób kojarzy firmę Sygate.

Wróćmy jednak do głównego bohatera tego artykułu. W nazwie Sygate Universal Network Access Control (SNAC) najważniejszym słowem jest universal. SNAC jest rozwiązaniem uniwersalnym. Wykorzystuje standardowe protokoły, może być wykorzystywany z sprzętem sieciowym dowolnego producenta wykorzystującego standardowe protokoły, zabezpiecza dostęp poprzez LAN, WAN, WLAN, IPSec, SSL VPN, obsługuje rozwiązania z wykorzystaniem klienta na stacje roboczej jak rozwiązania clientless. Jak widać, jeżeli tylko infrastruktura sieciowa pozwoli to nie ma takiego schematu Network Access Control z którym SNAC by sobie nie poradził.

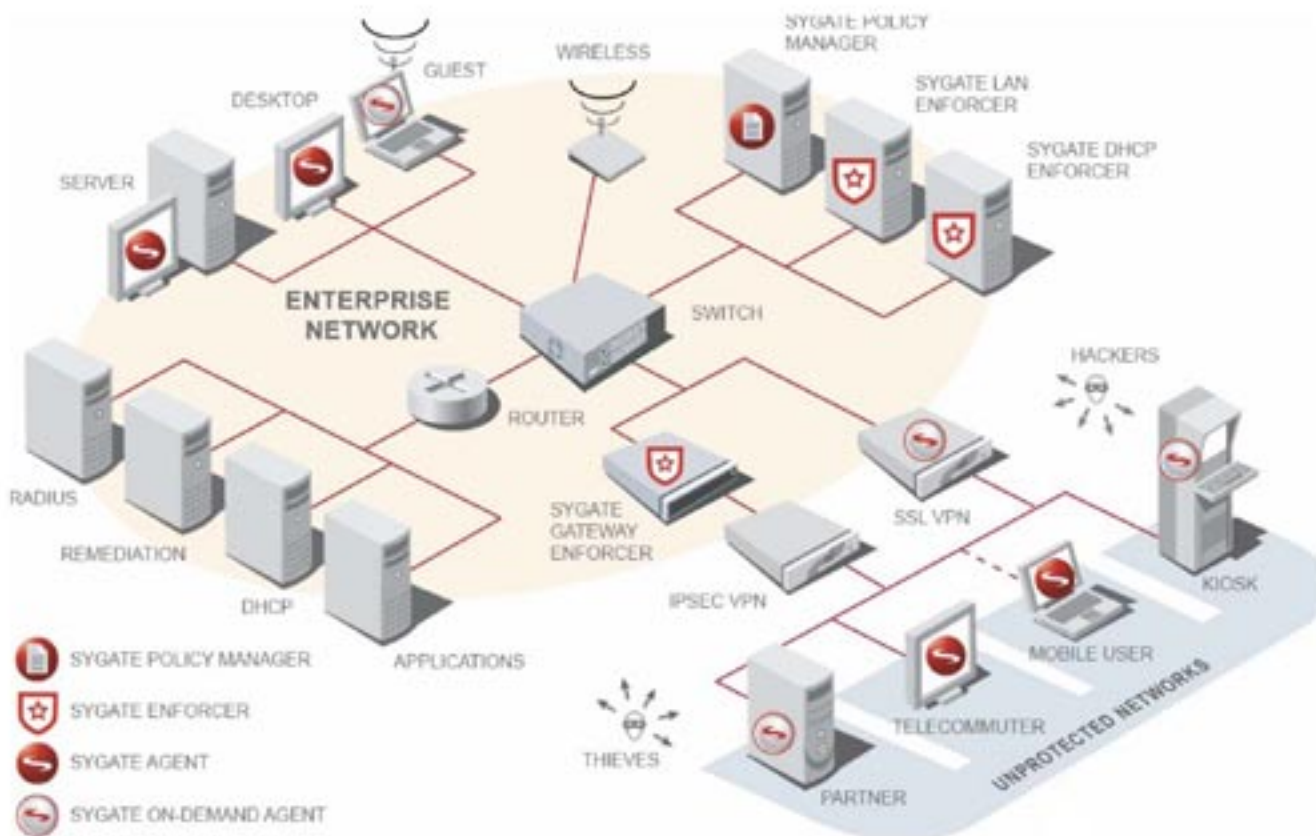
Aby wspomniana uniwersalność była możliwa Sygate Universal Network Access Control wykorzystuje sześć różnych technik:

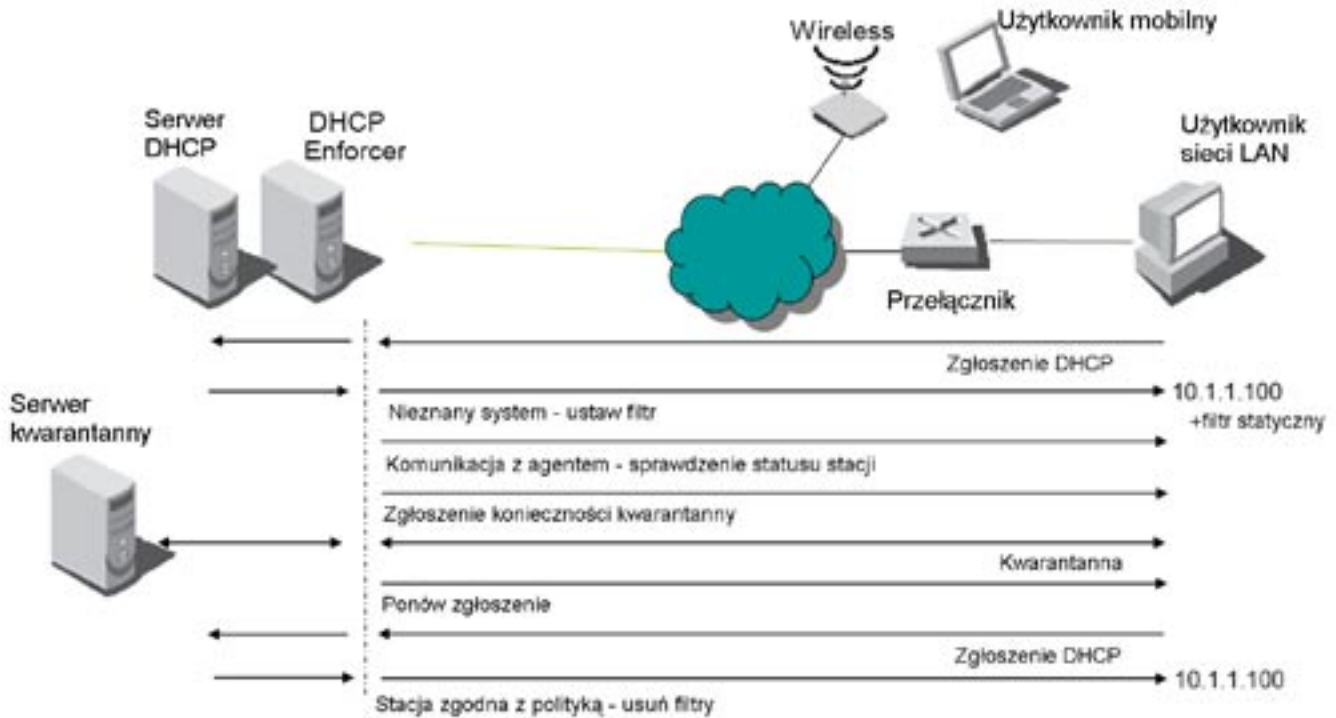
1. Integracja poprzez API
2. Sygate Gateway NAC
3. Sygate On-Demand NAC
4. Sygate 802.1x-Based NAC
5. Sygate DHCP-Based NAC
6. Cisco Network Admission Control v1

Pierwsze cztery metody były już

opisywane wielokrotnie w poprzednich numerach Securiusza. Dlatego nie będę się wdawał w szczegóły techniczne tych rozwiązań. Każdą z metod kontroli dostępu stosuje się w określonej sytuacji. Integracja poprzez API oraz Sygate Gateway NAC są wykorzystywane przy kontroli dostępu zdalnego poprzez IPSec VPN lub dial up. Gdy chcemy kontrolować dostęp przez SSL VPN najlepiej skorzystać z Sygate On-Demand NAC. Ta metoda okaże się również skuteczna w przypadku kontroli laptopów, które należą np. partnerów biznesowych i nie mają zainstalowanych agentów Sygate NAC. Sygate 802.1x-Based NAC to rozwiązanie dla sieci lokalnych. Możemy kontrolować zarówno stacje wpięte do przełączników jak i te które korzystają z połączeń bezprzewodowych WLAN. Metoda wykorzystująca standard 802.1x zapewnia maksymalne bezpieczeństwo, jednak wymaga infrastruktury zgodnej z tym standardem, i w tym miejscu może pojawić się problem. Nawet duże i nowoczesne korporacje nie są w stanie sobie pozwolić na wymianę całego niezgodnego ze standardem sprzętu w jednym momencie. Dodatkowo ta metoda wymaga bardzo szczegółowego projektu.

Aby umożliwić łatwe, a przede wszystkim nie wymagające wymiany sprzętu, wdrożenie kontroli dostępu do sieci LAN firma Sygate opracowała meto-



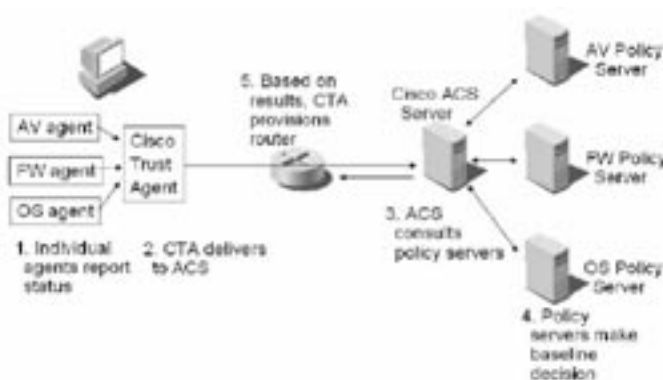


dę Sygate DHCP-Based NAC.

Podstawą tej metody jest Sygate DHCP Enforcer, który jest wpięty in-line pomiędzy serwer DHCP a sieć. Zasada działania kontroli dostępu w oparciu o tę metodę jest następująca. DHCP Enforcer przydziela użytkownikom nieroutowalne lub kwarantannowe adresy IP w przypadku gdy stacja nie ma zainstalowanego agenta lub nie jest znany status zgodności stacji z polityką SNAC. Adresy przydzielane są na dwa sposoby: albo przydzielane są adresy IP z odpowiednio zdefiniowanego adresu, a listy ACL na routerach określają gdzie może mieć dostęp stacja z adresem IP z tego przedziału, albo stacja dostaje „standardowy” adres IP, ale ze specjalną statyczną trasą routingu do serwera kwarantanny i bez domyślnej trasy routingu do sieci. Kiedy stacja ma adres IP DHCP Enforcer komunikuje się z agentem na stacji aby sprawdzić zgodność stacji z polityką SNAC. Jeżeli stacja nie jest zgodna z polityką, stacja zostaje zaktualizowana. Gdy aktualizacja zostaje zakończona agent wysyła nowe zgłoszenie do serwera DHCP. DHCP Enforcer otrzymuje zgłoszenie i dokonuje ponownego sprawdzenia stacji. Jeżeli wszystko jest w porządku, stacja otrzymuje swój właściwy adres IP zapewniający dostęp do systemu produkcyjnego.

Ponieważ DHCP Enforcer jest umieszczony pomiędzy siecią a serwerem DHCP, konieczne było przygotowanie kilku scenariuszy na wypadek dołączenia się do sieci stacji nie windowsowych oraz innych urządzeń oczekujących na adres IP od serwera DHCP. Stacje nie windowsowe można wyłączyć z procedury SNAC lub można też tworzyć listy adresów MAC. Istnieją też mechanizmy pozwalające wyłączać całe klasy specyficznych rozwiązań takich jak np. telefon IP.

Jak wspominałem we wstępie w ostatnim czasie mocno zaczęła inwestować w technologię Network Access Control firma CISCO. W 2004 roku ogłosiła swoją inicjatywę – Cisco Network Admission Control. Inicjatywa zakłada współpracę, lub można nawet rzec integrację z producentami systemów bezpieczeństwa dla stacji roboczych tj. oprogramowanie antywirusowe, lokalny firewall, itd. Zasadę działania CNAC przedstawia rysunek nr....



W obecnej wersji CNAC obsługują tylko routery Cisco oraz koncentratory VPN. Oznacza to, że wymuszanie polityki bezpieczeństwa odbywa się na routerze, a nie na najbliższym przełączniku. Podstawą zarządzania jest Cisco ACS. Podstawa jednak nie oznacza pełnej centralizacji oraz integracji. Potrzebne są do tego serwery polityk dostarczone przez producentów systemów bezpieczeństwa dla stacji roboczych. Podobnie wygląda sprawa po stronie stacji roboczej. Oprócz agenta Cisco Trust Agent na stacji muszą być plug-in'y rozwiązań bezpieczeństwa np. do kontroli polityki oprogramowania antywirusowego danego producenta.

CNAC jest rozwiązaniem, które dopiero jest budowane. Obecnie obowiązuje CNAC v1. Dlaczego w takim razie firma Sygate weszła w alians z Cisco NAC? Powód wydaje się prosty. Uniwersalność.

Inżynierowie z firmy Sygate chcą aby ich produkt był uniwersalny. By mógł pracować nie tylko w sieciach zbudowanych w oparciu o urządzenia jednego producenta, ale by każda firma posiadająca sieć budowaną przez kilka lat, opartą o urządzenia różnych producentów mogła wdrożyć technologię NAC.

Niezależnie od tego jakie metody dostępu są wykorzystywane w naszej sieci (Dial-up, IPSec VPN, SSL VPN, WLAN, LAN, itd.) oraz jaki jest producent urządzeń sieciowych i ilu ich jest, Sygate NAC umożliwia na wdrożenie technologii Network Access Control. Dla niewiernych Tomaszów proponujemy instalację demo.

Krzysztof Tyl



SSL = bezpieczeństwo ?



W ostatnich latach na wskutek rosnącej roli Internetu w rozwiązaniach biznesowych naturalnym wydaje się zapytanie o bezpieczeństwo połączeń internetowych. Przecież nikt nie zaryzykuje posiadania niezabezpieczonego dostępu internetowego do swojego konta bankowego, czy też przesyłania cennych, niezabezpieczonych danych. Odpowiedzią na rosnące ryzyko wymiany danych w otwartym świecie Internetu został opracowany przez firmę Netscape protokół SSL, którego wersja SSL 3.0 z 1996 roku jest obowiązującym standardem do dziś. Czy wobec ciągle aktualnego prawa Moore'a zgodnie z którym moc procesorów podwaja się dwukrotnie co 18 miesięcy, a co za tym idzie rosną możliwości łamania algorytmów kryptograficznych, stosowanie standardu z 1996 roku jest nadal bezpieczne?

Aby odpowiedzieć na to pytanie należy bliżej przyjrzeć się technologii firmy Netscape. SSL został stworzony z zamierzeniem spełnienia trzech warunków : uwierzytelniania, poufności oraz integralności przesyłanych danych. Jest protokołem, który w typowym modelu ISO/OSI znajduje się

między warstwami transportową i aplikacyjną. Jako dodatkowa warstwa dokonuje modyfikacji danych, które wychodzą z aplikacji i wykorzystują protokół HTTP (lub inny), zanim dotrą do warstwy transportowej.

Typowa sesja SSL składa się z kilku etapów :

1) Uzgadnianie pomiędzy hostem a serwerem takich parametrów połączenia jak najwyższa wspierana wersja SSL (najczęściej SSL 3.0 lub TLS 1.0), metoda szyfrowania niesymetrycznego (RSA, Diffie-Hellman, DSA lub Fortezza), metoda szyfrowania symetrycznego (RC2, RC4, IDEA, DES, Potrójny DES lub AES), algorytm mieszający wiadomości (MD5 lub SHA), metoda kompresji danych oraz wysyłany zostaje losowy numer, który zostanie wykorzystany później.

2) Wymiana certyfikatów, która najczęściej jest jednostronna gdyż mało użytkowników posiada swoje osobiste certyfikaty. W związku z tym to serwer na podstawie wysłanego certyfikatu jest weryfikowany przez klienta

– klient sprawdza czy dostarczony certyfikat jest podpisany przez zaufany ośrodek taki jak CA.

Dzieje się to w taki sposób:

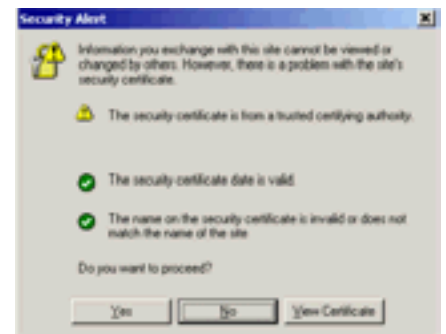
A -> B „Cześć”

B -> A „Cześć, Jestem użytkownikiem B”, dołączony CERTYFIKAT_B

A -> B „Udowodnij to”

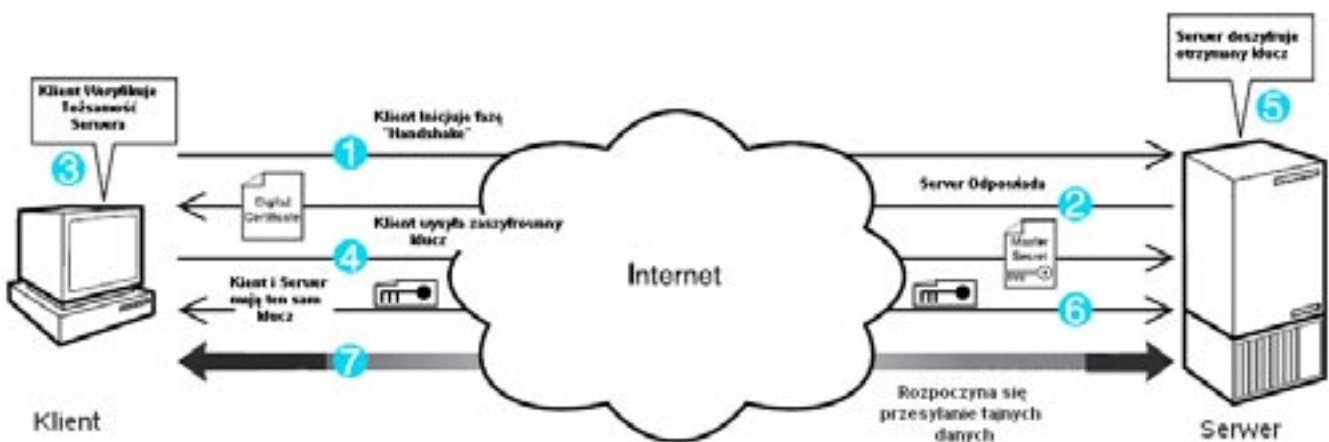
B -> A „Użytkownik A, Tu użytkownik B” – w formie jawnej oraz: „Użytkownik A, Tu użytkownik B” – przetworzone algorytmem mieszającym i zaszyfrowane przy pomocy prywatnego klucza użytkownika B

W tym momencie użytkownik A sprawdza aktualność i prawdziwość CERTYFIKATU_B (CA), a następnie dokonuje deszyfracji otrzymanej in-



formacji przy pomocy publicznego klucza użytkownika B, który zostaje udostępniony mu przez CA. Wiadomość jawną przetwarza tym samym algorytmem mieszającym co użytkownik B i porównuje ją z wynikiem deszyfracji. Jeżeli obie wynikowe wiadomości są takie same to ostatecznie potwierdza, że połączenie klienta A z serwerem B jest autentyczne i nikt nie podszywa się pod serwer B. Uwierzytelnianie w ten sposób powszechnie nazywane jest podpisem cyfrowym.

3) Wymiana klucza prywatnego



go, który zostanie zastosowany do szyfrowania przesyłanych danych za pomocą algorytmu symetrycznego.

A->B „W porządku B, oto klucz prywatny, \$private_key” – zaszyfrowane przy pomocy publicznego klucza użytkownika B.

Serwer B otrzymuje prywatny klucz zaszyfrowany za pomocą publicznego klucza B. Swoim kluczem prywatnym dokonuje deszyfracji i tym sposobem obie strony posiadają prywatny klucz, który zostanie wykorzystany do kodowania jedną z metod symetrycznych.

4) Wymiana danych pomiędzy użytkownikami A i B.

B->A „tajna wiadomość,

MAC” – zaszyfrowane kluczem \$private_key

Zastosowanie MAC (Message Authentication Code), pozwala na wyeliminowanie zagrożenia w postaci ataków typu Man In The Middle. MAC jest wynikiem przetworzenia algorytmem mieszającym wiadomości „tajna wiadomość” wraz z kluczem prywatnym, który przez cały czas pozostaje niejawnym dla osób próbujących ataku typu Man In The Middle. Przy wykorzystaniu popularnego algorytmu mieszającego MD5, powstaje 128-bitowy MAC, którego

większych przeszkód dokonać rejestracji przebiegu całego połączenia i pomimo tego, że nie będzie wiadział jakie dane są wysyłane pomiędzy użytkownikami może dokonać kryptoanalizy. W praktyce aby zabezpieczyć się przed tą możliwością stosuje się większą ilość kluczy prywatnych.

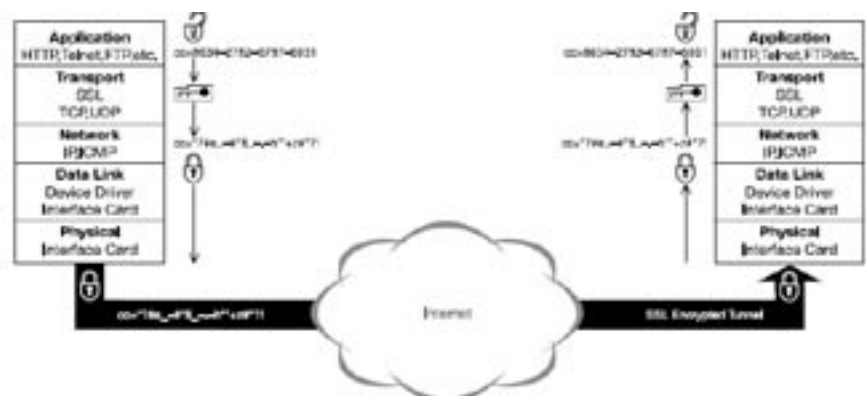
Czy w takim razie SSL pomimo swojego wieku jest nadal bezpieczny? Odpowiedź brzmi tak. Jest bezpieczny ponieważ został bardzo dokładnie zaprojektowany i sukcesywnie aż do wersji SSL 3.0 następowała eliminacja jego wad. Jego

szanse na odgadnięcie wynoszą 1 do 18,446,744,073,709,551,616 czyli jest to praktycznie niemożliwe. W momencie wykrycia nieprawidłowego MAC połączenie jest natychmiastowo zrywane.

Należy zauważyć, że atakujący techniką Man In The Middle nie może w żaden sposób włączyć się w komunikację pomiędzy użytkownikami A i B. Jednak jest w stanie bez

przemysłana konstrukcja zakłada wykorzystanie różnych algorytmów szyfrujących, co daje pewność aktualności tej technologii. Dlatego nie mają znaczenia zwiększające się stale możliwości obliczeniowe komputerów gdyż równocześnie powstają coraz to trudniejsze do złamania algorytmy kodujące. Wyścig trwa...

Michał Putała





Nowe IDP



Firma Juniper Networks wprowadziła nowe modele urządzeń z rodziny NetScreen-IDP. Urządzenia IDP 50, IDP 200, IDP 600 oraz IDP 1100 są nowymi platformami sprzętowymi opracowanymi specjalnie dla rodziny systemów Intrusion Prevention. Tym samym nowe

urządzenia będą zastępować urządzenie IDP oparte o platformę serwerową firmy Dell. Nowe urządzenia pracują na sprawdzonym na platformach Della systemie operacyjnym IDP w wersji 3.1.

IDP 50 jest wyposażony w dwa interfejsy 10/100/1000 oraz port zarządzający. IDP 200 ma wbudowanych 8 interfejsów 10/100/1000, port do zarządzania oraz port HA. Urządzenia IDP 600 oraz IDP 1100 występują w dwóch wersjach „skrętkowej” oraz światłowodowej i są wyposażone w 10 interfejsów 10/100/1000 lub 8 interfejsów 1GbE SX i 2 interfejsy 10/100/1000. Zarówno IDP 600 jak i IDP 1100 mają wbudowane porty do zarządzania i HA. Szczegóły podajemy w tabelce poniżej

Model	NetScreen-IDP 50	NetScreen-IDP 200	NetScreen-IDP 600	NetScreen-IDP 1100
Interfejsy				
Interfejsy do obsługi ruchu	2 10/100/1000	8 10/100/1000	10 10/100/1000 lub 8 FiberSX Gigabit +2 10/100/1000	10 10/100/1000 lub 8 FiberSX Gigabit +2 10/100/1000
Interf. zarządzający	1 10/100/1000	1 10/100/1000	1 10/100/1000	1 10/100/1000
Porty HA	Brak	1 10/100/1000	1 10/100/1000	1 10/100/1000
Parametry sprzętowe				
Pamięć	1 GB	1 GB	4 GB	4 GB
Liczba sesji sieciowych	10 000	70 000	220 000	500 000
Przepustowość	do 50 Mbps	do 250 Mbps	do 500 Mbps	do 1 Gbps
RAID	Nie	Nie	Tak	Tak
Redundantny zasilacz	Nie	Opcjonalny	Tak	Tak
HighAvailability				
Standalone failover	Nie	Tak	Tak	Tak
Failover firm trzecich	Nie	Tak	Tak	Tak
Load sharing	Nie	Tak	Tak	Tak
Klastrowanie	Nie	Tak	Tak	Tak
Fail-Open	Tak	Tak	Tak	Tak



NetScreen Secure Access Series



Firma Juniper Networks, wiodący dostawca urządzeń SSL VPN (33% rynku wg analizy z marca 2005), dokonała zmian w swojej rodzinie produktów Secure Access służącej do tworzenia połączeń

szyfrowanych, realizowanych z użyciem protokołu SSL (Secure Socket Layer). Dotychczasowe urządzenia RA 500, SA 1000, SA 3000, SA 5000 zostały zastąpione modelami SA 700, SA 2000, SA 4000, SA 6000. Urządzenia Secure Access skierowane są do firm, które chcą udostępnić swoim pracownikom/klientom wewnętrzne zasoby. Urządzenia Juniper Networks są bardzo wygodnym i komfortowym rozwiązaniem, gdyż korzystając ze standardowych przeglądarek internetowych nie wymagają instalacji dodatkowych klientów VPN, jak to ma miejsce w przypadku IPsec VPN.

Model	SA700	SA2000	SA4000	SA6000
Liczba jednoczesnych użytkowników	10 - 25	25 - 100	50 - 1000	100 - 2500
Opcje klastrowania	Nie	Cluster Pair	Cluster Pair	Multi Unit
Sprzętowa kompresja GZIP HTTP	Nie	Nie	Tak	Tak
Sprzętowe przyspieszenie szyfrowania SSL	Nie	Nie	Opcja	Tak
Podwójny interfejs Gigabit Ethernet	Nie	Nie	Nie	Tak
Typowe zastosowania	Dostęp dla zdalnych pracowników	Dostęp dla zdalnych pracowników i partnerów klasa Enterprise.	Dostęp dla zdalnych pracowników i partnerów klasa Enterprise.	Dostęp dla zdalnych pracowników i partnerów klasa Enterprise. Wysoka niezawodność i wydajność systemu

Rozwiązania ISG już zintegrowane



Juniper Networks wprowadziła do sprzedaży karty IDP dla ISG 2000 dzięki którym, obecna już na rynku od roku platforma ISG 2000 stała się rozwiązaniem integrującym funkcje firewalla, szyfrotora VPN oraz systemu intrusion prevention. Do ISG 2000 można włożyć maksymalnie trzy karty IDP uzyskując tym samym przepustowość 1 Gbps przy włączonym systemie IDP. Karty IDP są oparte o szybkie układy FPGA (Field Programmable Gate Arrays) oraz procesory PowerPC. Mają zaimplementowane algorytmy sprzętowego wsparcia dla dopasowywania wzorców sygnatur, wydajnego i równoległego porównywania sygnatur oraz obsługi protokołów zawierających ciągi tekstowe, tj. HTTP, SMTP, oraz POP3.

Podstawą całego rozwiązania jest system operacyjny ScreenOS, który teraz może zarządzać zarówno funkcjami firewall/VPN jak i IPS. W dużym skrócie konfiguracja wygląda następująco. Najpierw konfigurowana jest polityka firewallowa, określająca jaki ruch i między jakimi strefami jest dozwolony a jakie połączenia zabronione. Czyli tak jak w każdym urządzeniu firewall/VPN firmy Juniper Networks. Z tą tylko różnicą, że pojawiła się możliwość zaznaczenia w polityce, czy dany ruch ma być sprawdzany przez system IDP czy też tylko przez firewall. Jeżeli ruch ma być sprawdzany przez system IDP to musimy zdefiniować osobną politykę określającą pod jakim kontem ten ruch ma być sprawdzany, jakie grupy sygnatur dotyczą tego ruchu.

Oprócz nowych kart pojawił się również nowy model w rodzinie rozwiązań zintegrowanych – ISG 1000 posiadający 4 wbudowane porty 10/100/1000 oraz dwa sloty na karty z dodatkowymi interfejsami lub karty IDP. Nowe urządzenie jest w stanie obsłużyć ruch firewall/VPN do 1 Gbps. Karty IDP do ISG 1000 będą dostępne pod koniec roku.

Wirtualny świat dysku

Rosnące potrzeby aplikacji i serwerów sprawiają, iż coraz ważniejsze staje się zapewnienie odpowiednich zasobów dyskowych. Technologie popularne w zakresie składowania danych zmieniają się jednak na tyle szybko, iż inwestycje w produkty konkretnych firm starzeją się bardzo szybko – a co za tym idzie występuje konieczność ich wymiany na now-



sze i pojemniejsze. Abstrahując od kosztów tych operacji należy zwrócić uwagę na fakt, iż tego typu działania zwykle nie są możliwe do zrealizowania bez czasowej utraty choćby części funkcjonalności używanych aplikacji. Pewnego rodzaju remedium na te problemy jest wdrożenie systemu wirtualizacji zasobów. Technologia ta służy do odpowiedniego zamaskowania fizycznej strony systemów dyskowych, tak by dla użytkownika czy aplikacji nie było widocznej różnicy pomiędzy emulowanymi systemami a urządzeniami rzeczywistymi.

Więcej o plusach stosowania wirtualizacji

Tego typu rozwiązania, mimo iż były oferowane przez różnych dostawców już wcześniej, dopiero obecnie (dzięki wzrostowi mocy obliczeniowej) znajdują coraz więcej zastosowań. Wirtualizacja może odbywać się w trzech miejscach infrastruktury przechowywania danych – na serwerach korzystających z zasobów, na urządzeniach składających dane lub w przypadku sieci SAN – na urządzeniach sieciowych znajdujących

się pomiędzy zasobami a używającymi ich serwerami.

Prawdopodobnie najwcześniej rozwinięła się technologia wirtualizacji w oparciu o specjalne funkcjonalności urządzeń służących do składowania danych. W tej odmianie technologii oprogramowanie służące do emulowania zasobów jest preinstalowane na macierzy czy bibliotece taśmowej, i odpowiednio przydziela zasoby do wirtualnych dysków, czy napędów. Przykładowe urządzenia wspierające tą technologię to StorageTec VSM, emulujące działanie do 256 wirtualnych napędów taśmowych, czy macierze EMC Symmetrix, lub HP EVA, oferujące wirtualne przestrzenie dyskowe tworzone na wspólnych pulach fizycznych dysków. Zastosowanie takiej technologii ma swoje plusy – umożliwia korzystanie z zasobów sieciowych dowolnym syste-

na brak jakiegokolwiek standaryzacji w tym zakresie są to rozwiązania typowo firmowe – działają w obrębie produktów jednego producenta, jeżeli nawet posiadamy macierze różnych producentów oferujące wirtualizację, potrzebne jest administrowanie z użyciem innych narzędzi każdym z nich. Bezpieczeństwo zapewniane jest poprzez maskowanie



poszczególnych wirtualnych zasobów i musi być przeprowadzane na każdej macierzy z osobna.

Wirtualizacja na serwerze

Rzadziej stosowanym sposobem wirtualizacji jest technologia oparta o oprogramowanie instalowane bezpośrednio na serwerach korzystających z zasobów dyskowych. Pozwala ono co prawda uniezależnić się od dostawców macierzy, jednakże posiada szereg niedogodności. Mimo iż oferuje często bardzo zaawansowane funkcje (jak mirroring, path failover, czy snapshoty) to nie ma nic za darmo – aplikacje te zabierają znaczną część zasobów serwerowych, przez co zmniejszają wydajność serwerów na których rezydują. Jak każde rozwiązanie służące wirtualizacji pozwalają zwiększyć wykorzystanie fizycznych zasobów, jednak pamiętać trzeba iż w większości przypadków nie wiąże się to ze znacz-

nym obniżeniem kosztów – dlatego że licencjonowanie odbywa się per serwer – więc im więcej serwerów korzysta z tego rozwiązania tym więcej wydamy na same licencje. Pamiętać należy również o fakcie, iż w przypadku podłączenia się do zasobów dyskowych serwera nie skonfigurowanego do współpracy z tym systemem, istnieje możliwość uzyskania dostępu do przechowywanych danych – mimo iż intencją twórcą tego wirtualne dyski administratora było odseparowanie dostępnych różnym użytkownikom zasobów.

Specjalizowane urządzenia sieci SAN

Obydwa wyżej wymienione sposoby realizowania wirtualizacji mają również jedną wspólną cechę – w przypadku posiadania sieci SAN nie wymagają wprowadzania w niej żadnych istotnych zmian. Nie można tego powiedzieć o ostatniej metodzie wirtualizacji – opartej o specjalizowane urządzenia sieci SAN – a to dlatego że wybranie tej metody skutkuje uruchomieniem kolejnego urządzenia w tej sieci, lub znaczącej modyfikacji funkcjonalności istniejących już w tej sieci urządzeń. Jest to praktycznie jedyna wada tego rozwiązania w porównaniu z poprzednimi – konieczne jest zarządzanie kolejnym urządzeniem sieciowych, na nieco wyższym od standardowego poziomie. Jeśli jednak spojrzymy na zalety tego rozwiązania, okaże się iż warto zainteresować się tego typu implementacją wirtualizacji. Przede wszystkim jest to rozwiązanie niezależne zarówno od rodzaju systemów operacyjnych korzystających z zasobów, jak i od producentów systemów dyskowych, które udostępniamy. Samo urządzenie umożliwia wykonywanie zaawansowanych operacji na dyskach, analogicznie do dostępnych w przypadku rozwiązań serwerowych. Bardzo dużym plusem jest również możliwość występująca w wielu tego typu urządzeniach, połączenia sieci SAN z istniejącą infrastrukturą sieci IP. Daje nam to ogromne możliwości dostępu zdalnego do danych, niemożliwe do realizacji przy zastosowaniu sieci Fibre Channel. Co również warto podkreślić – ponieważ urządzenie przenosi cały ruch pomiędzy serwerami a dostępnymi fizycznymi nośnikami, jest w stanie zapewnić najwyższy poziom

bezpieczeństwa z wymienionych wyżej metod.

Implementacje

Wśród rozwiązań realizujących wirtualizację na poziomie sieci SAN znaleźć można kilka, które zasługują na szczególną uwagę. Wspomnieć należy przede



wszystkim o EMC Invista – produkcie, który rezyduje na klastrze dwóch serwerów zarządzających (Control Path Cluster), które komunikują się ze switchami SAN. Przełączniki te pochodzić mogą od dowolnych producentów, którzy uczestniczą w programie partnerskim EMC – m.in. Brocade, Cisco, McDATA – nowe przełączniki mogą współpracować z Invista bez zmian w budowie, do nieco

starszych dostępne są specjalne karty. Zarządzanie systemem odbywa się poprzez konsolę opartą w www, command line lub z użyciem EMC Control Center. Z uwagi na realizowaną przez wszystkie produkty EMC filozofię ILM (Information Lifecycle Management) oprogramowanie to dostarcza znakomite, automatyczne mechanizmy raportowania, i zarządzania wykorzystaniem zasobów i informacji o przechowywanych na zasobach sieciowych danych. Korzystając z macierzy różnych producentów mamy więc możliwość dynamicznego przenoszenia danych pomiędzy nośnikami o różnej szybkości i właściwościach, np. przenoszenie rzadko używanych danych na tanie i wolne nośniki dyskowe lub taśmy. Możliwe jest kopiowanie danych w tle, niewidoczne dla aplikacji z nich korzystających, co pozwala bezpiecznie i bez utraty funkcjonalności przenosić potrzebne dane na nowe i wydajniejsze macierze. Dzięki klastrowej infrastrukturze całe rozwiązanie pozwala dodatkowo zwiększyć bezpieczeństwo używanej sieci SAN.

Ciekawym rozwiązaniem, tym razem typowo sprzętowym jest Hitachi TagmaStore NSC55. Rozwiązanie to jest połączeniem switcha SAN z macierzą dyskową – pozwala łączyć systemy poprzez FibreChannel, iSCSI, IBM ESCON i FICON. Jednocześnie oferuje do 72 TB wewnętrznej pamięci dyskowej (z użyciem zewnętrznych macierzy wartość ta wzrasta do imponującej liczby 16 PB wirtualizowanej przestrzeni dyskowej), która może być dowolnie partycjonowana i zapewniać QoS dla poszczególnych korzystających z danych aplikacji. Jako zewnętrzne macierze poszerzające wewnętrzną pamięć dyskową można stosować min. macierze Sun, Hitachi, IBM, czy EMC, więc wszystkich liderów rynku. Jednocześnie wraz z urządzeniem otrzymujemy zestaw dostępnych aplikacji, pozwalających zrealizować nawet najbardziej zaawansowane funkcje na dostępnych danych.

Miłosz Franaszek

WYDAWCA: ASCOMP S.A.

ul. Walerego Sławka 3, 30-653 Kraków
Tel. (+48 12) 254 62 62
Fax (+48 12) 254 62 72
Red. Nacz.: Jakub Czajęcki
e-mail: j.czajeki@ascomp.com.pl
Dział Bezpieczeństwa: wew. 105, 120
e-mail: securiusz@ascomp.com.pl
www.ascomp.com.pl