

Gdański MOPR z firewallem NG i tunelami VPN

W Miejskim Ośrodku Pomocy Rodzinie w Gdańsku wdrożone zostało centralnie zarządzane urządzenie firewallowe klasy enterprise. Między 11 oddziałami instytucji zbudowano też tunele VPN, które zapewniają bezpieczne przesyłanie siecią dokumentów urzędowych.

Stefan Kaczmarek

Miejski Ośrodek Pomocy Rodzinie (MOPR) w Gdańsku ma kilkanaście punktów obsługi rozsianych na terenie miasta, w których niezbędną pomoc mogą uzyskać rodziny znajdujące się w trudnej sytuacji materialnej, osoby starsze i niepełnosprawne. Zanim w MOPR-ze wdrożono nowe rozwiązania, ośrodek korzystał z połączeń internetowych opartych na dedykowanej dzierżawionej infrastrukturze od dwóch operatorów, jedynych mających w ofercie łącza spełniające surowe wymogi ośrodka w zakresie bezpieczeństwa przesyłanych siecią danych osobowych, informacji i dokumentów urzędowych. Wynajmowana infrastruktura, mimo że bardzo kosztowna, często ulegała awariom. Każda przerwa w działaniu łączy internetowych mocno

Cele wdrożenia NG Firewall w sieci MOPR w Gdańsku

- obniżenie kosztów utrzymania infrastruktury teleinformatycznej
- wyeliminowanie awarii sieci
- skuteczna ochrona przesyłanych danych
- centralne zarządzanie wszystkimi ośrodkami MOPR-u

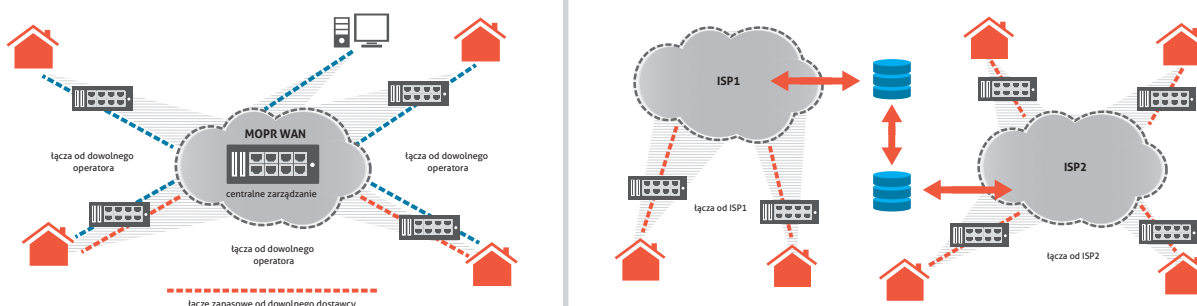
utrudniała działanie gdańskiego ośrodka, m.in. opóźniając pomoc finansową dla beneficjentów. Konieczność najmu łączy od zewnętrznych operatorów i wysokie koszty z tym związane, częste awarie dzierżawionej infrastruktury oraz brak pełnej kontroli nad siecią wymusiły poszukiwanie nowych rozwiązań.

Jako zasadnicze cele przyjęto: redukcję awarii, pełne zabezpieczenie sieci oraz obniżenie kosztów infrastruktury teleinformatycznej. Po analizie dostępnych na rynku rozwiązań zespół informatyków MOPR-u uznał, że założenia te można zrealizować, kupując centralnie zarządzane urządzenia firewallowe, między którymi zostaną zbudowane bezpieczne tunele VPN, całkowicie niezależne od dostawcy ISP (Internet Service Provider). Ośrodek ogłosił przetarg, w którym za najlepszą ofertę uznano rozwiązanie NG (Next Generation) Firewall firmy Barracuda Networks.

Sieć WAN z wielofunkcyjnym NG Firewalliem

Wdrożenie nowych urządzeń przeprowadzono w październiku 2013 r. Nie licząc przygotowań, trwało ono ok. tygodnia. Sieć rozległa WAN (Wide Area Network)

Schematy sieci przed rozbudową i po rozbudowie



Korzyści z wdrożenia NG Firewall

- możliwość rezygnacji z dróg łączy dedykowanych
- autorski protokół VPN TINA (kilkanaście odrębnych transportów w ramach jednego tunelu VPN)
- graficzna konsola do zarządzania VPN TINA
- kompresja ruchu nawet do 95%

zapewnia pracownikom MOPR-u dostęp do danych z systemów funkcjonujących w ośrodku. Część ruchu jest szyfrowana. Sieć łączy w sumie ok. 550 stanowisk rozmieszczonych w 11 lokalizacjach na terenie Gdańska. Są one podłączone do dwóch głównych lokalizacji, w których znajdują się serwerownie. Obecna sieć WAN wykorzystuje urządzenia Barracuda NG Firewall (modele od F10 do F400 w zależności od liczby stanowisk w lokalizacji). Zakupiono w sumie 12 urządzeń. Jedno z nich służy do centralnego zarządzania urządzeniami rozmieszczonymi w poszczególnych lokalizacjach.

Firewall następnej generacji

NG Firewall to rozwiązanie zapewniające funkcjonalność firewalle następnej generacji wszystkim lokalizacjom w sieci korporacyjnej. Jest centralnie zarządzany, korporacyjnym systemem ochronnym, wyposażony w wiele funkcji i modułów pozwalających na pełne zabezpieczenie komunikacji wewnątrz i na zewnątrz organizacji. Zapewnia zaawansowaną kontrolę aplikacji warstwy 7, filtrowanie WWW, ochronę przed malware, zapobieganie atakom intruzów. NG Firewall zawiera też filtr pakietów, który gwarantuje bezpieczeństwo chronionej sieci i samego rozwiązania.

Za pomocą zakupionego sprzętu możliwe stało się też zbudowanie rozległej struktury tuneli VPN (autorski protokół TINA), kształtowanie pasma (QoS) oraz uruchomienie ochrony przed włamaniami (Intrusion Prevention System) i innymi zagrożeniami (wirusy, spam). Wprowadzono też segmentację sieci i kontrolę dostępu (NAC). Istotną zaletę zakupionego

Z własną siecią WAN jesteśmy niezależni



Jacek Brauer
administrator sieci MOPR w Gdańsku

Nasza sieć WAN musi zapewnić nieprzerwaną łączność i bezpieczne przesyłanie danych między poszczególnymi lokalizacjami MOPR-u. Przed wdrożeniem NG Firewalla infrastrukturę MOPR-u stanowiły dwie osobne sieci WAN obsługiwane przez dwóch dostawców ISP. Nad tym rozwiązaniem nie mieliśmy żadnej kontroli, nie mogliśmy też wpływać na jego funkcjonowanie. Podstawową wadą poprzedniego rozwiązania było to, że awaria u jednego z dostawców ISP paraliżowała pracę całego lub

połowy ośrodka. W obecnej sytuacji awaria jednego z łączy dotyczy danej lokalizacji i nie ma wpływu na pracę pozostałych. Teraz mamy własną sieć WAN, kontrolujemy ją i nie jesteśmy uzależnieni od żadnego dostawcy ISP. Możemy nią centralnie administrować, a koszt utrzymania infrastruktury spadł o ponad 50 procent. Obsługą sieci może teraz zajmować się tylko jedna osoba, której zabiera to średnio kilkanaście minut każdego dnia. Co więcej, po trzech latach

zakup urządzeń zwróci się nam w stu procentach, a rok później otrzymamy od producenta bezpłatnie fabrycznie nowe urządzenia. Przemodelowanie infrastruktury teleinformatycznej w ośrodku pozwoliło nie tylko zwiększyć stabilność połączeń między oddziałami i obniżyć koszty, lecz także umożliwiło zaplanowanie zakupu awaryjnych łączy 3G i 4G dla lokalizacji, w których nie uda nam się uzyskać dostępu do tradycyjnych łączy od innych dostawców ISP.

rozwiązania stanowi prostota. Wśród korzyści wynikających ze scentralizowanego zarządzania regułami bezpieczeństwa treści, jakie zapewnia NG Firewall, warto wymienić także:

- spójność zabezpieczeń i egzekwowanie reguł w całej korporacji,
- kontrolę i raportowanie w czasie rzeczywistym wielu bram sieciowych,

55%

sięgają miesięczne oszczędności związane z obsługą infrastruktury teleinformatycznej unowocześnionej wdrożeniem rozwiązania typu firewall next generation.

- kompleksową historię i przywracanie konfiguracji oraz zmian reguł w całej sieci,
- scentralizowaną kontrolę: antywirusową, filtrowania sieci WWW i aktualnych informacji na temat kontroli dostępu do sieci.

Zakupione firewalle zainstalowano we wszystkich 11 oddziałach gdańskiego MOPR-u. Pendrive z kopią konfiguracji z pierwszego urządzenia dostarczano do każdego punktu, gdzie wystarczyło podłączyć go do gniazda USB urządzenia, które automatycznie zapisywało odpowiednią konfigurację i po chwili restartowało się.

IT

.....
Autor od kilkunastu lat publikuje i pracuje jako redaktor w pismach oraz serwisach internetowych poświęconych technologiom teleinformatycznym.