

System obsługi portowania numerów (Number Portability), lokalizacji abonenta dla celów połączeń alarmowych (112) oraz rejestracji i udostępniania domen ENUM

Rozwiązanie sprzętowo-programowe oferowane przez NASK zapewnia ma realizację następujących zadań w zakresie portowania numerów, obsługi numerów alarmowych (112) oraz rejestracji i udostępniania domen ENUM:

- Realizację administracyjnej procedury przeniesienia numeru przy zmianie operatora
- Realizację rozpowszechniania (rozgłaszania) informacji technicznych o przeniesionych numerach, w szczególności numerów telefonów i związanych z nimi numerów routingowych
- Obsługa metod ACQ lub metody QoR dla celów portowania numerów zgodnie z oczekiwaniami operatorów oraz dodatkowo w standardzie bazy ENUM
- Dostęp dla służb ratowniczych do centralnej bazy o lokalizacji abonentów w zakresie:
 - adresu (nazwy miejscowości, ulicy z adresem domu i mieszkania), pod którym znajduje się zakończenie sieci, udostępnione abonentowi - w przypadku stacjonarnej publicznej sieci telefonicznej
 - geograficzne umiejscowienie (według standardów ETSI) osoby wykonującej połączenie z numerem alarmowym w przypadku sieci mobilnych
 - współrzędnych geograficznych osoby wykonującej połączenie z numerem alarmowym w przypadku stacjonarnej publicznej sieci telefonicznej o ile operator posiada takie dane.
- Pełna możliwość wprowadzania i uaktualniania danych o lokalizacji abonentów przez operatorów
- Możliwość rejestracji domen ENUM przez operatorów i Abonentów oraz udostępnianie danych w systemie DNS

Metoda implementacji

System pomimo realizacji trzech rozdzielnych zdań stanowi całość, co pozwala np. podczas realizacji procedury przeniesienia numerów na korzystanie przez operatorów z istniejących danych o abonentach, a procedura przeniesienia numeru pozwoli na aktualizowanie danych niezbędnych dla służb ratowniczych.

Dzięki oparciu kwestii lokalizacji i przenośności numerów o to samo rozwiązanie (oprogramowanie i sprzęt), można zaoszczędzić na budowie trzech rozdzielnych systemów oraz instalacji oprogramowania.

Warto nadmienić że zamawiający może wybrać jedno lub więcej oferowanych funkcjonalności, zgodnie ze swoimi oczekiwaniami. Tak więc jeśli wolą zamawiającego jest wykorzystanie tylko wybranej funkcjonalności (np. portowanie numerów), NASK dostosowuje odpowiednio rozwiązania, rezygnując z modułów opartych realizujących funkcje lokalizacji dla numerów alarmowych czy bazę ENUM.

Metody dostępu do systemu (interface)

Dla obu zadań (A i B) System będzie oferował identyczne mechanizmy dostępu dla uprawnionych użytkowników (Operatorzy, Służby ratownicze):

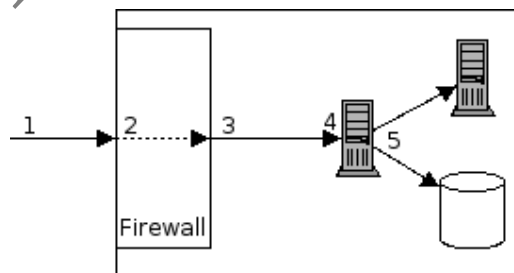
- W zakresie realizowania procedur administracyjnych przez operatorów zakłada się realizację uwierzytelnionego dostępu do obu funkcji systemu (lokalizacja i przenośność) w sposób on-line na dwa sposoby tj. przez interface WWW oraz interface oparty o XML (w celu integracji systemu z systemami back-office operatorów)- w standardzie EPP.
- W zakresie dostępu do danych technicznych związanych z numerami przeniesionymi poprzez rozgłaszanie on-line wszystkich zmian numerów przeniesionych oraz rozgłaszanie zbiorcze dokonywane raz na dobę w oknie portowania w formacie ustalonym przez jednostkę odpowiedzialną za nadzór nad operatorami telekomunikacyjnymi
- Uwierzytelniony dostęp on-line z wykorzystaniem interface XML (standard EPP) oraz WWW do systemu dla uprawnionych służb ratowniczych w celu uzyskania informacji o lokalizacji abonentów

Założenia budowy systemu

Zakłada się bezpieczne przechowywanie i udostępnianie danych, spełniając następujące wymagania:

- Skalowalność – łatwa i szybka rozbudowa systemu bez przerywania jego pracy poprzez m.in. budowę wielowarstwową, komponentową pozwalającą na rozdzielanie podstawowych funkcji systemu
- Wydajność - odporność na zwiększone (nagłe i nieprzewidziane) obciążenie systemu oraz możliwość rozbudowy w kierunku balansowania obciążenia
- Niezawodność – zapewniona ciągłość świadczenia serwisu
- Wysoki poziom dostępności systemu (high availability) poprzez zabezpieczenie w postaci redundantnego centrum zapasowego oraz odporność na awarie pojedynczych elementów rozwiązania

Uwierzytelnianie



Rysunek: uwierzytelnianie

Opis procesu autoryzacji

W pierwszej etapie połączenie przechodzi przez firewall (oznaczony numerem 2) dedykowany dla systemu. Na firewallu na podstawie jego konfiguracji oraz danych na temat połączenia, jest podejmowana decyzja czy je przyjąć czy odrzucić. W przypadku akceptacji tego połączenia, następuje jego wpuszczenie do sieci wewnętrznej (numer 3). W następnym kroku następuje negocjacja certyfikatów (oznaczona numerem 4). Na tym etapie, aby zostać przepuszczonym dalej, połączenie operatorskie, musi się przedstawić pasującym do niego certyfikatem, który został podpisany (uwierzytelniony) przez certyfikat, którym przedstawia się system. Dzięki temu:

- Weryfikujemy połączenie operatorskie jako uprawnione do przedstawienia się danym certyfikatem (musi on pasować do parametrów tego połączenia)
- Operator weryfikuje czy podłącza się do właściwego systemu (nikt się nie podszywa pod taki system, aby wykraść lub podejrzeć dane wysyłane przez operatora)
- Po przejściu powyższego kroku, wszystkie dane przesyłane przez obie strony do siebie, są szyfrowane mocnym algorytmem, uniemożliwiając tym samym wykradzenie przesyłanych danych (ataki typu "man-in-the-middle")
- W ostatnim etapie (oznaczonym numerem 5), operator połączenia autoryzuje się np. za pomocą loginu i hasła w usłudze, do której chce mieć dostęp

Strona techniczna uwierzytelniania

Firewall może być dowolnym z dostępnych: od zintegrowanego z systemem operacyjnym np. iptables systemu Linux, do dedykowanych rozwiązań oferowanych np. przez firmę Check Point. Autoryzacja połączenia operatorskiego w tym kroku, przebiega na poziomie protokołów warstwy transportowej (TCP/UDP). Parametry połączenia, które mogą być brane pod uwagę przy tym etapie autoryzacji to np. adres źródłowy i docelowy, port docelowy.

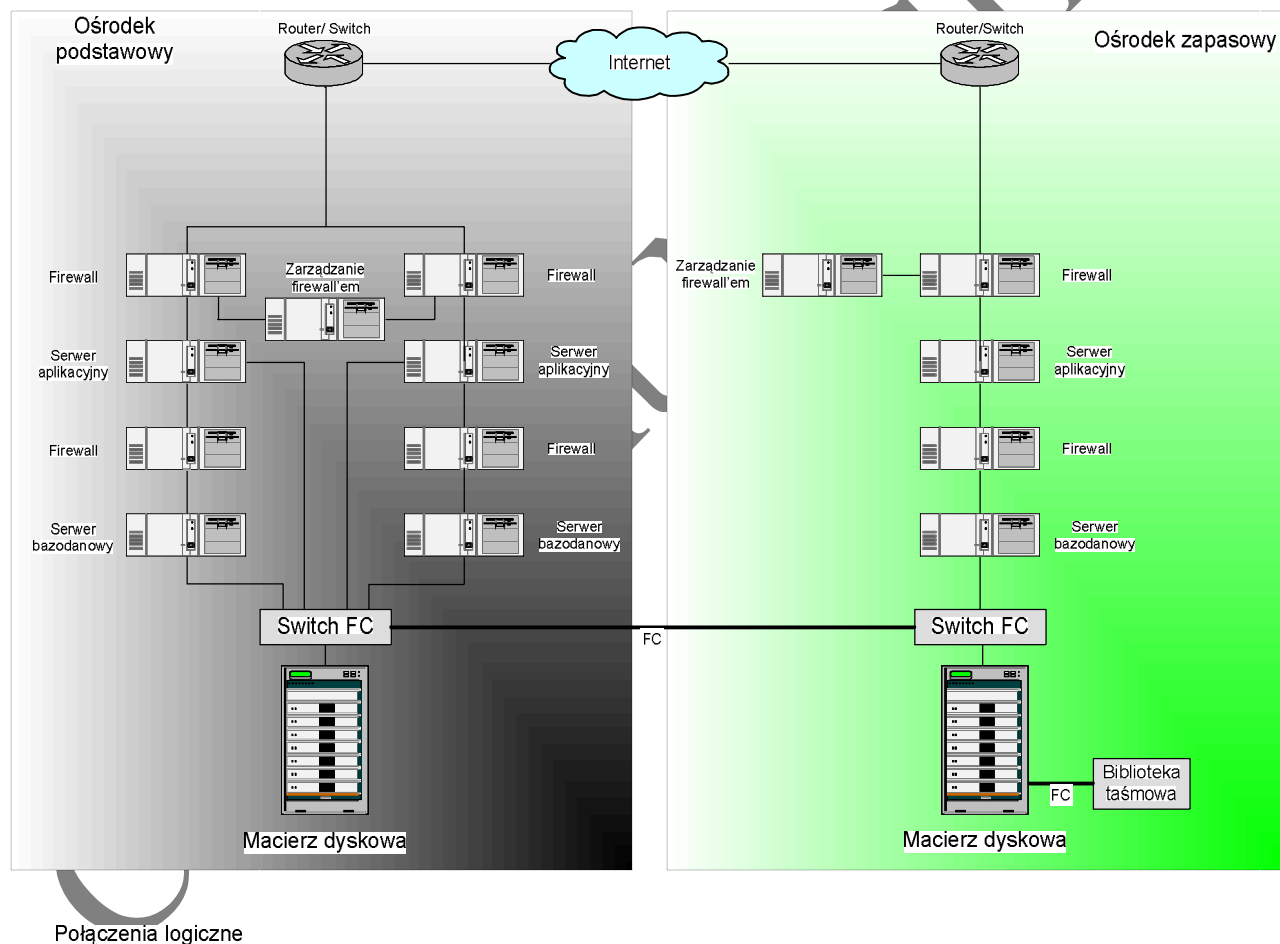
Proces certyfikacji odbywa się na poziomie protokołów wyższego poziomu np. HTTPS (bezpieczny HTTP). Po stronie systemu jest certyfikat, natomiast operator połączenia, który chciałby uzyskać dostęp do tego systemu wystawia zlecenie certyfikacji. Zlecenie dotyczy konkretnego komputera, z którego operator będzie się łączył z systemem. Aby ten operator mógł nawiązywać połączenie z tym systemem, zlecenie takie musi zostać podpisane przez certyfikat systemu i powstały w ten sposób certyfikat operatora musi mu zostać dostarczony np. przez pocztę elektroniczną. W ten sposób certyfikacja połączenia operatorskiego polega na tym, że po nawiązaniu połączenia musi się on przedstawić ważnym (certyfikaty są wystawiane na określony czas, najczęściej na jeden rok) certyfikatem, który jest podpisany przez certyfikat systemu, oraz pasującym do komputera, z którego jest nawiązywane połączenie operatorskie. Jeśli tego nie zrobi, połączenie jest zrywane. Po poprawnym przejściu etapu weryfikacji certyfikatów, obie strony negocjują algorytm szyfrowania, oraz wymieniają w sposób bezpieczny klucze szyfrujące. Od tego momentu wszystkie przesyłane dane muszą być zaszyfrowane uzgodnionym algorytmem, jeśli nie jest to możliwe połączenie jest zrywane. Do szyfrowania najczęściej wykorzystuje się obecnie, jeden z algorytmów protokołów SSLv2, SSLv3 lub TLSv1.

Ostatnim etapem autoryzacji jest zalogowanie się przez operatora do systemu. Do logowania najczęściej wykorzystuje się login i statyczne hasło, ale nic

nie stoi na przeszkodzie na wykorzystaniu tutaj bardziej zaawansowanych metod autoryzacji jak np. klucze publiczne, klucze sesyjne czy hasła jednorazowe.

Opis architektury systemu

System musi się składać się z dwóch ośrodków: podstawowego i zapasowego oraz miejsca gdzie będą przechowywane zarchiwizowane dane (musi to być fizycznie różne miejsce od ośrodka podstawowego i zapasowego). Ośrodki, podstawowy i zapasowy, powinny być oddalone od siebie o co najmniej 20 kilometrów.



Rysunek: Schemat logiczny systemu

Powyższy rysunek przedstawia przykładowe rozwiązanie, które może być zaimplementowane w celu zbudowania systemu spełniającego w/w założenia. W skład każdego ośrodka wchodzi:

1. router – aktywne urządzenie sieciowe,
2. switch IP – przełącznik sieciowy (zarządzalny),
3. serwery – urządzenia do obsługi poszczególnych serwisów,
4. switch FC – przełącznik do komunikacji z użyciem protokołu FC,

5. macierz dyskowa – bezpieczne urządzenie do przechowywania danych ,
6. biblioteka taśmowa – urządzenie do archiwizowania danych (tylko w ośrodku zapasowym).

Ruch przychodzący do systemu byłby filtrowany na serwerach firewall (odpowiednia polityka dostępu), następnie zapytania trafiałyby do serwera aplikacyjnego (logi z serwerów aplikacyjnych zapisywane będą na macierzy) i poprzez kolejny serwer firewall byłyby kierowane do serwera bazodanowego, który korzystałby z bazy danych utrzymywanej na macierzy dyskowej.

Dane w zaproponowanej architekturze systemu będą replikowane pomiędzy macierzami dyskowymi znajdującymi się w różnych ośrodkach w sposób synchroniczny z użyciem mechanizmu wewnątrz macierzowego – wykorzystując zdublowane łącza światłowodowe (dwie różne drogi). System byłby objęty odpowiednią polityką backup'u i archiwizacji danych realizowaną z użyciem biblioteki taśmowej. W przypadku awarii ośrodka podstawowego, ruch automatycznie zostanie skierowany do ośrodka zapasowego.

Skalowalność

Zaproponowana architektura systemu jest bardzo łatwo skalowalna zarówno, jeśli chodzi o rozbudowę pojedynczych urządzeń, jak i dołączanie kolejnych serwerów – wszystko to odbywać się może bez zatrzymywania działania systemu.

W przypadku rozbudowy pojedynczych urządzeń:

- Serwery aplikacyjne i bazodanowe muszą być urządzeniami przystosowanymi do rozbudowy o kolejne procesory i kolejne moduły pamięci operacyjnej.
- Switchy FC muszą być przystosowane do rozbudowy o kolejne porty obsługujące nowe serwery.
- Macierz dyskowa musi być przystosowana do rozbudowy o kolejne dyski, pamięć „cache”, kontrolery, porty – wszystko w sposób dynamiczny.
- Biblioteka taśmowa musi być przystosowana do rozbudowy o nowe napędy.

W przypadku rozbudowy o kolejne urządzenia:

Serwery firewall – dopinanie kolejnego urządzenia firewall w przypadku dopuszczenia do systemu znacznie większej ilości użytkowników oraz możliwość rozbudowy o usługi typu:

- Przełącznik zawartości (*ang. content switch*) – zapewniający skalowalność rozwiązania wyznaczoną ilością użytkowników i odwołań do serwisu. Zapewnia wydajność systemu balansując ruch użytkowników do zwielokrotnionej struktury www/aplikacja. Możliwe jest sprzężenie ww. funkcjonalności z terminowaniem tuneli SSL oraz w przypadku wzrastającej ilości tych tuneli z mechanizmem szybkiej ich obsługi (*ang. SSL accelerator*).
- IPS (*ang. Intrusion Prevention System*). Kontrola i wymuszenie poprawności przepływów danych.

- Serwer AAA (ang. authorization, authentication, accounting) – serwer zapewniający potwierdzenie tożsamości użytkowników oraz nadanie im uprawnień oraz wysyłanie danych o przebiegu sesji użytkowników do centralnego systemu logów
- Serwery aplikacyjne i bazodanowe – dołączanie do systemu kolejnego serwera, powodować będzie rozłożenie obciążenia na kolejne urządzenie.

Istnieje również możliwość dobudowania do systemu kolejnego ośrodka, który sprawi, że przetrzymywane dane będą jeszcze lepiej chronione gdyż będą replikowane w trzecie miejsce (fizycznie różne od dwóch pozostałych) oraz przypadku awarii dwóch ośrodków mamy trzeci, w którym możemy uruchomić usługę.

Wydajność

Zaproponowana architektura jest przystosowana nie tylko do obsługi standardowej (założonej) ilości zapytań, ale także do obsłużenia znacznie zwiększonego ruchu.

Wydajność systemu wynika zarówno z użytych komponentów, jakie są zainstalowane w poszczególnych urządzeniach (serwery powinny być zbudowane w oparciu o architekturę 64-bitową, systemy operacyjne powinny być dostosowane do architektury 64-bitowej itp.), ale również w architekturze połączeń pomiędzy urządzeniami.

Połączenia IP powinny być oparte o technologie GbEth, a komunikacja FC powinna mieć przepustowość min. 2 Gb/s. Zarówno serwery aplikacyjne jak i bazodanowe będą pracowały w klastrze, który pozwala na równomierne rozłożenie obciążenia pomiędzy urządzeniami tak, aby w każdym przypadku optymalnie wykorzystywać posiadaną moc przetwarzania danych. Serwery te korzystałyby z przestrzeni na macierzy przy użyciu protokołu FC (w serwerach instalowane będą karty HBA tak, aby komunikacja serwera z macierzą nie obciążała procesora serwera). Wszystkie te zabiegi są po to, aby system pracował z takim zapasem mocy, który pozwoli w sytuacjach zwiększonego obciążenia na niezauważalne dla użytkownika końcowego obsłużenie zwiększonej ilości zapytań do bazy.

Niezawodność

Podstawową cechą zaproponowanej architektury jest jej niezawodność. Wszystkie najważniejsze elementy składowe urządzeń takie jak: dyski, zasilacze, procesory muszą być redundantne, tak, aby awaria pojedynczego elementu nie zatrzymała działania całego systemu. Większość tych elementów dodatkowo można wymieniać bez potrzeby zatrzymywania pracy danego urządzenia. Dyski w serwerach powinny pracować w systemie RAID 1 - mirror (oznacza to, że awaria jednego dysku jest niezauważalna dla użytkowników)

Elementy systemu:

- **Serwery firewall** – praca w klastrze, wyłączenie (awaria) pojedynczego serwera nie zatrzymuje pracy systemu (awaria serwera zarządzania firewall -

- który jest pojedynczy- nie wpływa na działanie ani samych firewall'i ani całego systemu)
- **Serwery aplikacyjne i bazodanowe** – praca w klastrach, wyłączenie (awaria) pojedynczego serwera nie zatrzymuje pracy systemu
 - **Macierz dyskowa** – praca w systemie RAID 1 lub 5, redundantne kontrolery – generalnie najważniejsze (i najdroższe) urządzenie w systemie, ale również zapewniające najwyższe bezpieczeństwo przechowywanych danych.

Każdy serwer, który korzysta z macierzy powinien być dołączony do niej (poprzez switch FC) dwoma niezależnymi linkami (w każdym serwerze powinny być dwie karty HBA). Każdy ośrodek zapasowy powinien być dołączony do ośrodka podstawowego dwoma niezależnymi drogami światłowodowymi, oraz trzecia IP o przepustowości 1 Gb/s. Dodatkowo każdy ośrodek powinien być dołączony do dwóch różnych stacji transformatorowych, a do tego być wyposażony w UPS i agregat prądowłoczy – tak by w razie nawet potężnej awarii prądu system mógł dalej świadczyć światu swoje usługi.

Aby zapewnić również bezpieczny rozwój i upgrade oprogramowania zaleca się zbudowanie systemu developerskiego (podobnego do tego, jaki znajdowałby się w ośrodku zapasowym), który służyłby do testów nowych wersji oprogramowania, tak, aby na system produkcyjny wgrzywać tylko i wyłącznie wcześniej sprawdzone, na podobnym modelu, oprogramowanie. Na takim modelu można również z powodzeniem testować rozbudowę sprzętowa.

Czas wdrożenia

NASK zakłada że po uzgodnieniu kwestii technicznych i organizacyjnych maksymalny czas wdrożenia nie przekroczy 4 miesięcy.

Kontakt

Andrzej Bartosiewicz
Kierownik Działu Domen
NASK

tel: +48 22 380 8595
SIP: 1595@194.181.119.227
kom: +48 606 24 15 70
ENUM: 0.7.5.1.4.2.6.0.6.8.4.e164.arpa