

# IBM DataPower Gateway Administration

## 2-dniowe szkolenie dla administratorów

Rafał Owczarek

CSM Architect  
IBM Polska

Mikołaj Jaworski

Technical Sales  
IBM Polska



# Agenda - Dzień 1. (25 luty 2025)

Agenda - Dzień 1.:

**10:00 - 10:10: Rozpoczęcie**

- Przedstawienie agendy, celów i oczekiwań od warsztatów

**10:10 - 10:50: Wykład 1: Wprowadzenie IBM DataPower Gateway**

- Funkcjonalności i przypadki użycia IDG.
- Dostępne usługi IDG

**10:50 - 11:20: Ćwiczenie 1: Instalacja i inicjalizacja IDG.**

- Pierwsze uruchomienie i konfiguracja firmware.
- Inicjalizacja WebGUI

**11:20 - 11:30: Przerwa kawowa**

**11:30 - 11:45: Wykład 2: Zapoznanie się z interfejsem administracyjnym IDP**

- Interface do zarządzania IDG.
- Komendy CLI.

**11:45 - 12:30: Ćwiczenie 2: Interfejs administracyjny IDG**

- Zarządzanie z wykorzystaniem CLI
- Wykorzystanie REST API do zarządzania IDG.
- WebGUI IDG.

**12:30 - 13:15: Lunch**

**13:15- 13:30: Wykład 3: Zarządzanie IDG**

- Domeny aplikacyjne.
- Użytkownicy i grupy.
- Certyfikaty.

**13:30 - 14:20: Ćwiczenia 3: Zarządzanie IBM DataPower Gateway**

- Domeny aplikacyjne – zarządzanie uprawnieniami
- Tworzenie i zarządzanie użytkownikami w IDG
- Zarządzanie certyfikatami oraz konfiguracja połączeń TLS

**14:20 - 14:30: Przerwa kawowa**

**14:30 - 14:45: Wykład 4: Troubleshooting IBM DataPower Gateway**

- Raporty błędów
- Logi systemowe
- Troubleshooting

**14:45 - 15:45 Ćwiczenia 4: Narzędzia administracyjne i Troubleshooting IDG**

- Sprawdzanie właściwości i statusu bramy oraz zdefiniowanych w niej obiektów z poziomu WebGUI.
- Konfiguracja logowania (Log Targets i poziomy logowania).
- Raportowanie błędów.
- Narzędzia do przeprowadzania diagnostyki sieci (PING, Connection Test, Przechwytywanie pakietów, Probes).

**15:45 - 16:00: Zakończenie 1. dnia warsztatów.**

- Sesja pytań i odpowiedzi.

# Agenda - Dzień 2. (26 luty 2025)

Agenda - Dzień 2.:

**10:00 - 10:10: Rozpoczęcie**

- Przedstawienie agendy, celów i oczekiwań od warsztatów

**10:10 - 10:30: Wykład 5: Backup, Eksport i Import konfiguracji IDG**

- Eksport.
- Import.
- Backup

**10:30 - 11:20: Ćwiczenie 5: Tworzenie kopii zapasowych IBM DataPower Gateway.**

- Tworzenie kopii zapasowych IBM DataPower Gateway.
- Utworzenie pełnej kopii urządzenia: Secure Backup
- Utworzenie kopii wybranej konfiguracji IDG
- Przywrócenie kopii wybranej konfiguracji IDG

**11:20 - 11:30: Przerwa kawowa**

**11:30 - 11:45: Wykład 6: Zabezpieczanie usług API**

- Typy dostępnych usług w IDG.
- WS-Proxy.
- Multi-Protocol Gateway

**11:45 - 12:30: Ćwiczenie 6: Tworzenie usługi Web Service Proxy.**

- Podstawowa konfiguracja WS-Proxy.
- SLM Policy.
- AAA Policy.
- Ochrona przed atakiem SQL Injection.

**12:30 - 13:15: Lunch**

**13:15- 14:15: Ćwiczenie 7: Tworzenie usługi Multi-Protocol Gateway**

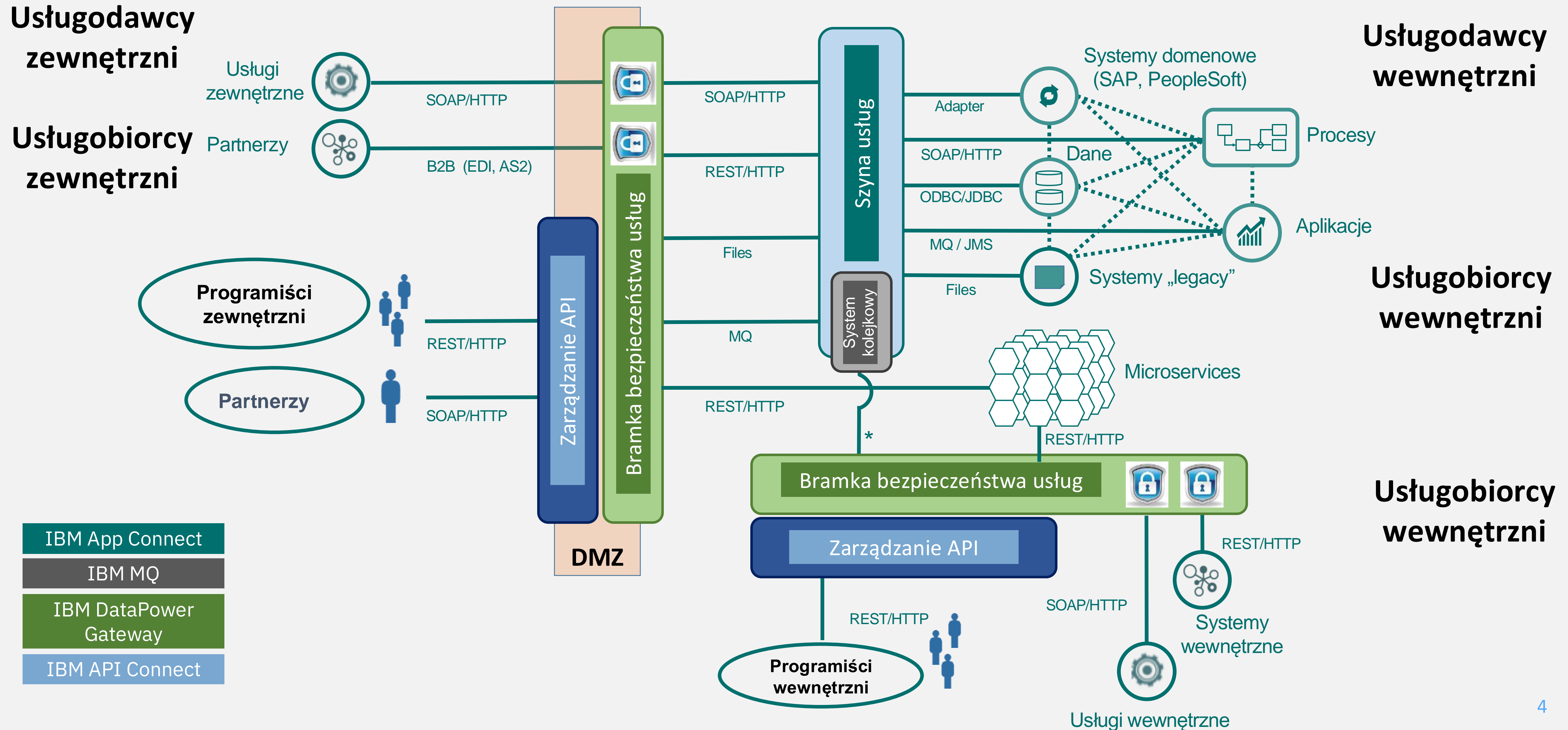
- Dynamic-backend (routing).
- Zabezpieczenia na poziomie FSH.
- Transform with XSLT style sheet.
- XML Schema Validation.
- AAA Policy.
- DataPower Gateway Script

**14:15 - 14:30: Przerwa kawowa**

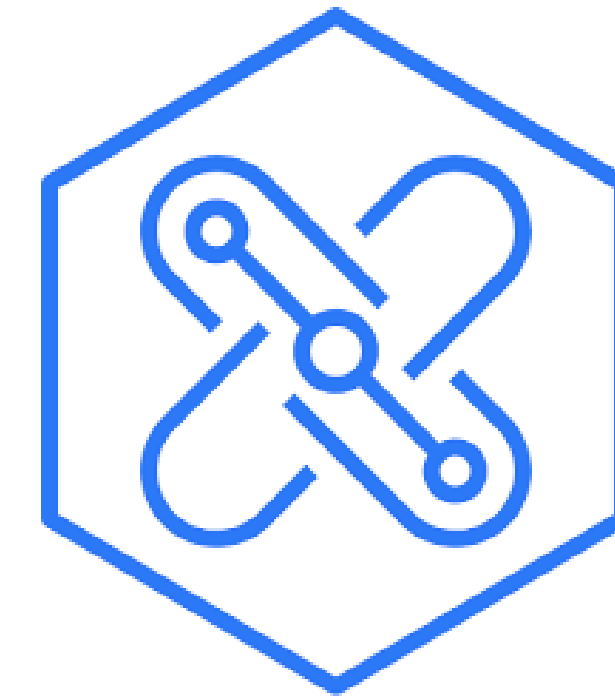
**14:30 - 15:00: Zakończenie warsztatów.**

- Sesja pytań i odpowiedzi.

# Architektura integracyjna w realizacji IBM



# IBM DataPower Gateway





# Czym jest DataPower - przez analogię ...





# DataPower Gateway – Bramka bezpieczeństwa



## OCHRONIARZ

- Strzeże wejścia do klubu.
- Decyduje, kto może wejść.
- Dbą, aby klub nie był zatłoczony.
- Integruje stałych bywalców z nowymi gośćmi.



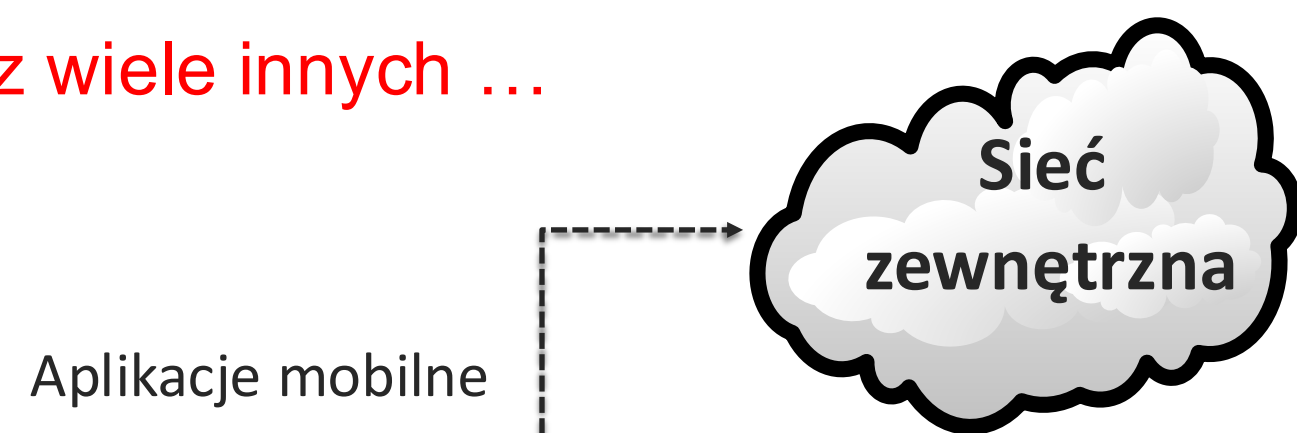
## IBM DataPower Gateway

- Zapewnia bezpieczeństwo firmy na jej granicy.
- Filtruje i analizuje ruch do usług i aplikacji.
- Rozdziela obciążenie.
- Integruje systemy i aplikacje.

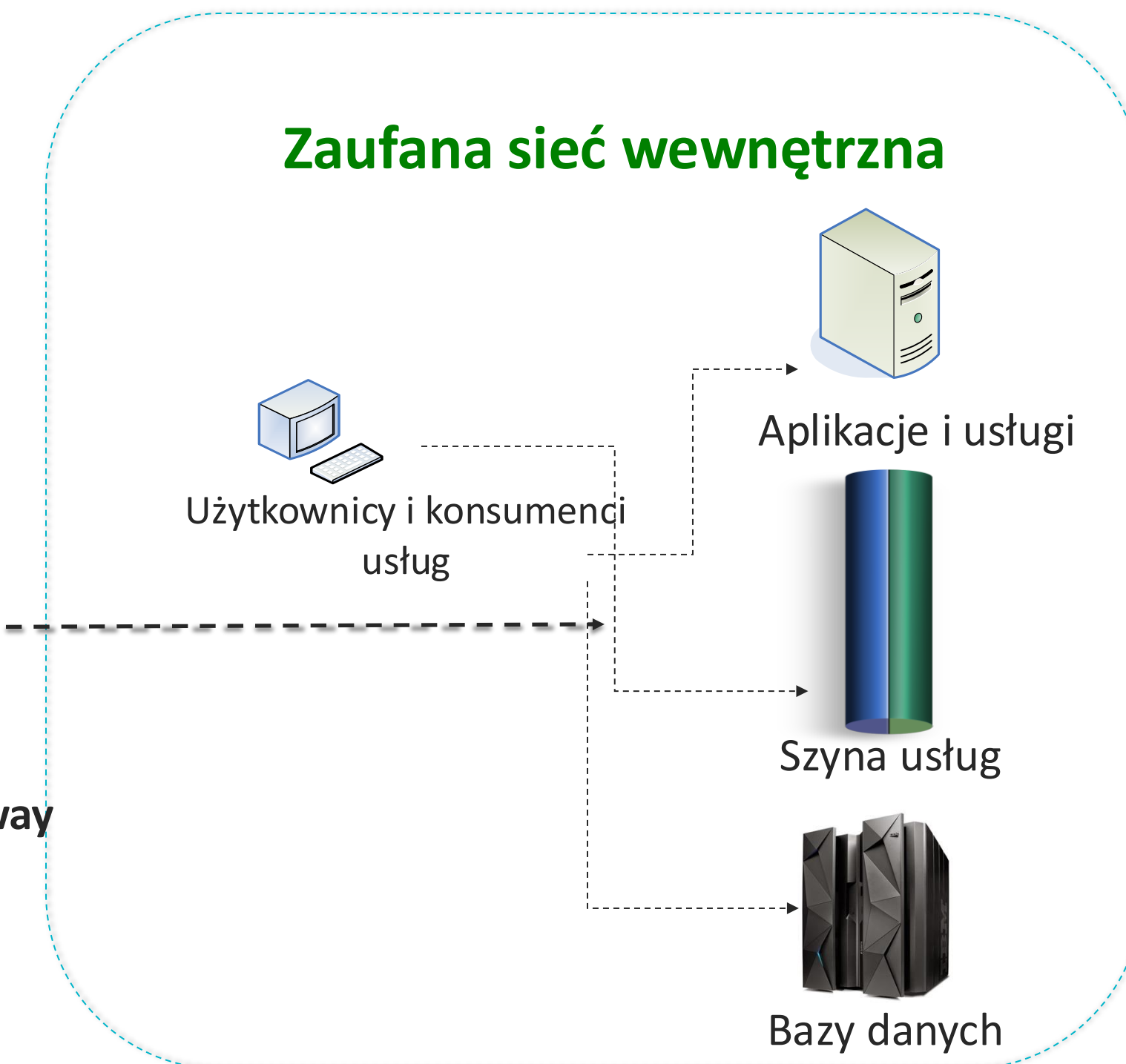
# Typowy przykład zastosowania

## Zagrożenia:

Nieautoryzowany dostęp do usług  
Próby fałszowania komunikatów  
Ataki obciążeniowe  
Wymuszenia SLA  
Podmienianie tożsamości  
Oraz wiele innych ...



- 1 Firewall na poziomie danych
- 2 Uwierzytelnianie i autoryzacja
- 3 Ochrona przed atakami
- 4 Aplikowanie polityk SLA

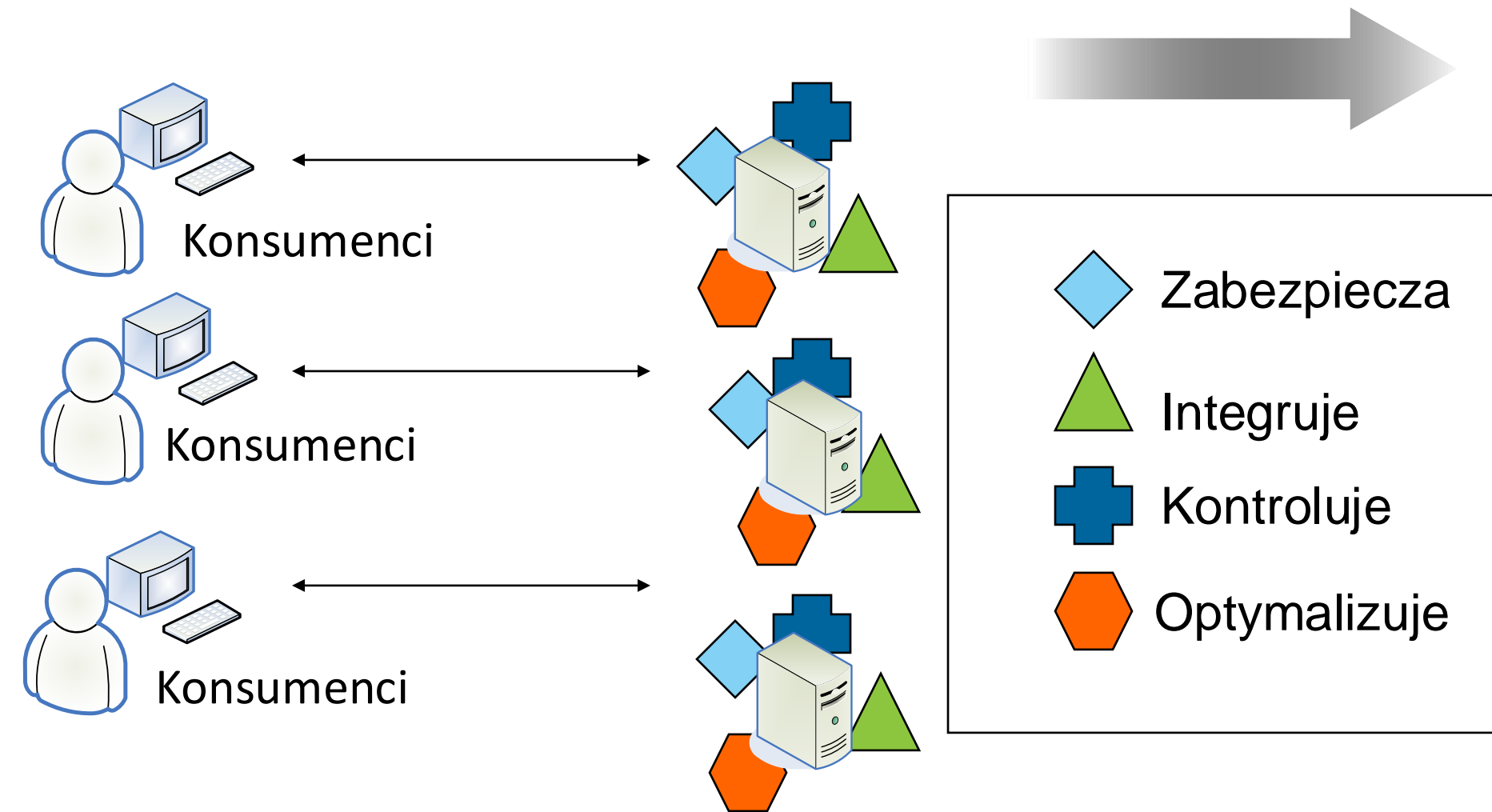


- 5 Monitorowanie i raportowanie dostępu
- 6 Dynamiczne zarządzanie obciążeniem
- 7 Konwersja protokołów i danych
- 8 Wbudowana integracja z LDAP/AD, MQ/JMS, Tibco EMS, DB ODBC, Antivirus ICAP, FTP/NFS

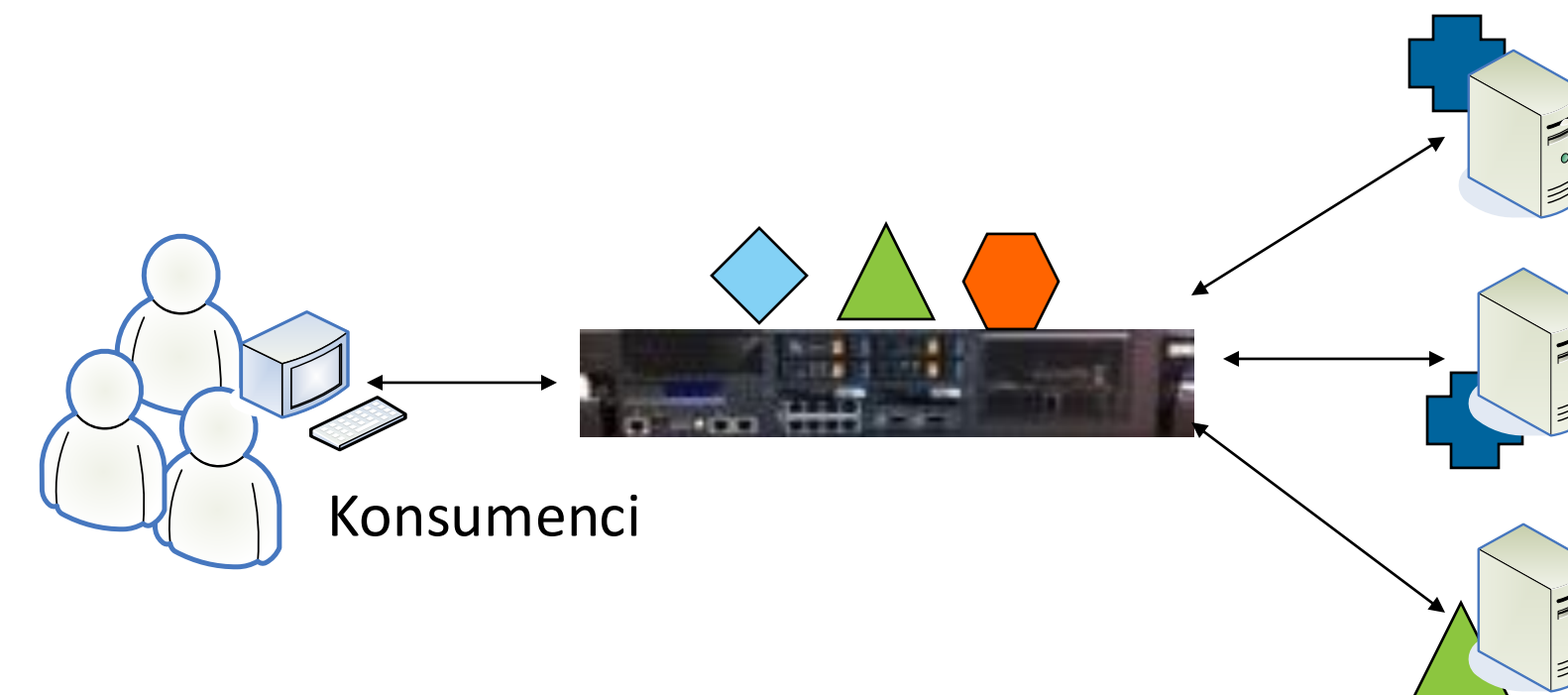


# A wewnątrz firmy?

Każdy system zabezpieczony oddzielnie



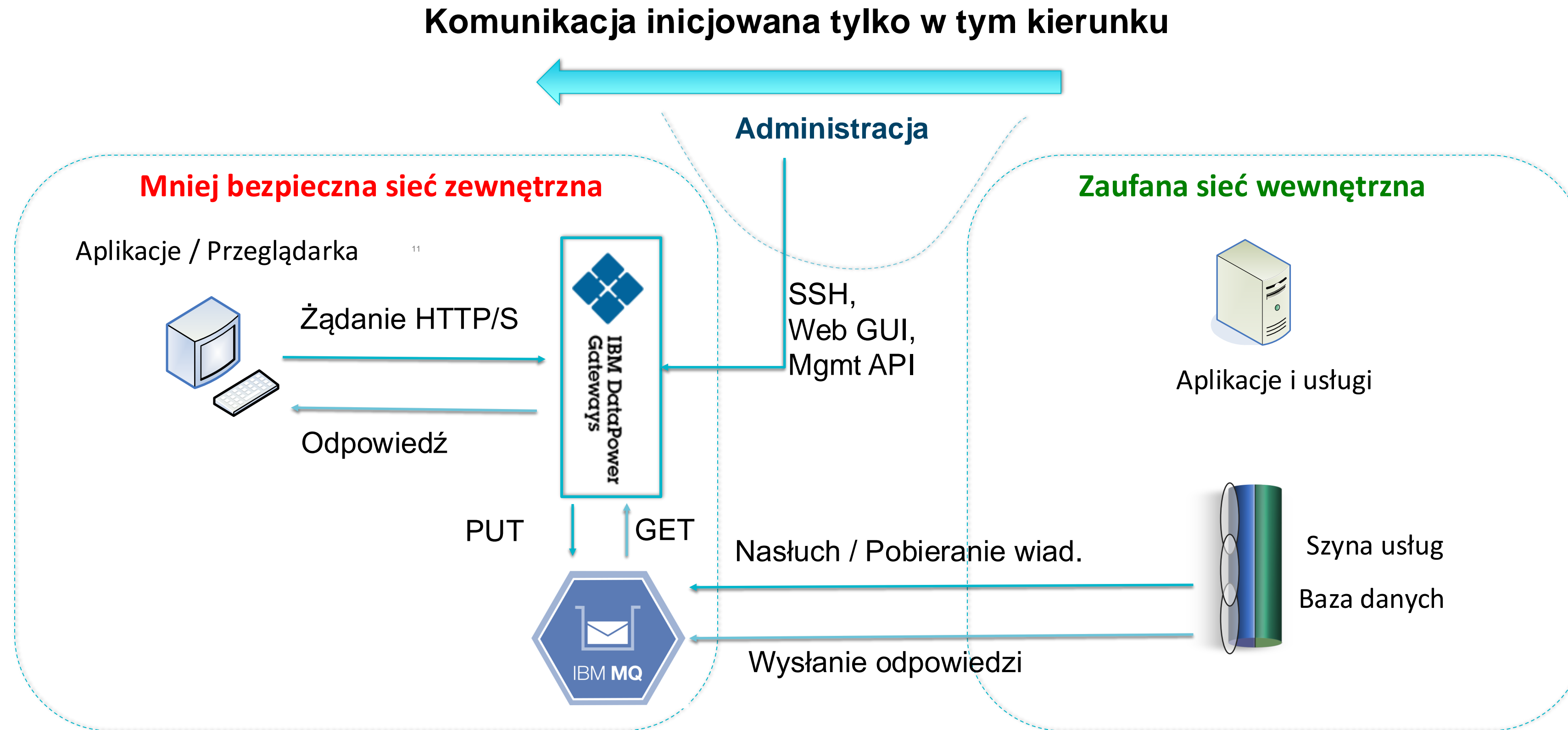
Ale można też tak:



## Upraszczając i ujednolicając konfiguracje:

- **Minimalizujemy ryzyko potencjalnego błędu**
  - \$ mniejszy koszt obsługi awarii oraz incydentów bezpieczeństwa
- **Ułatwiamy administrację i konfigurację**
  - \$ niższe nakłady na szkolenia, sprzęt, wsparcie techniczne i licencje
- **Przyśpieszamy dostęp do usług – akceleracja sprzętowa**
  - \$ mniejsza infrastruktura, mniejsze koszty utrzymania

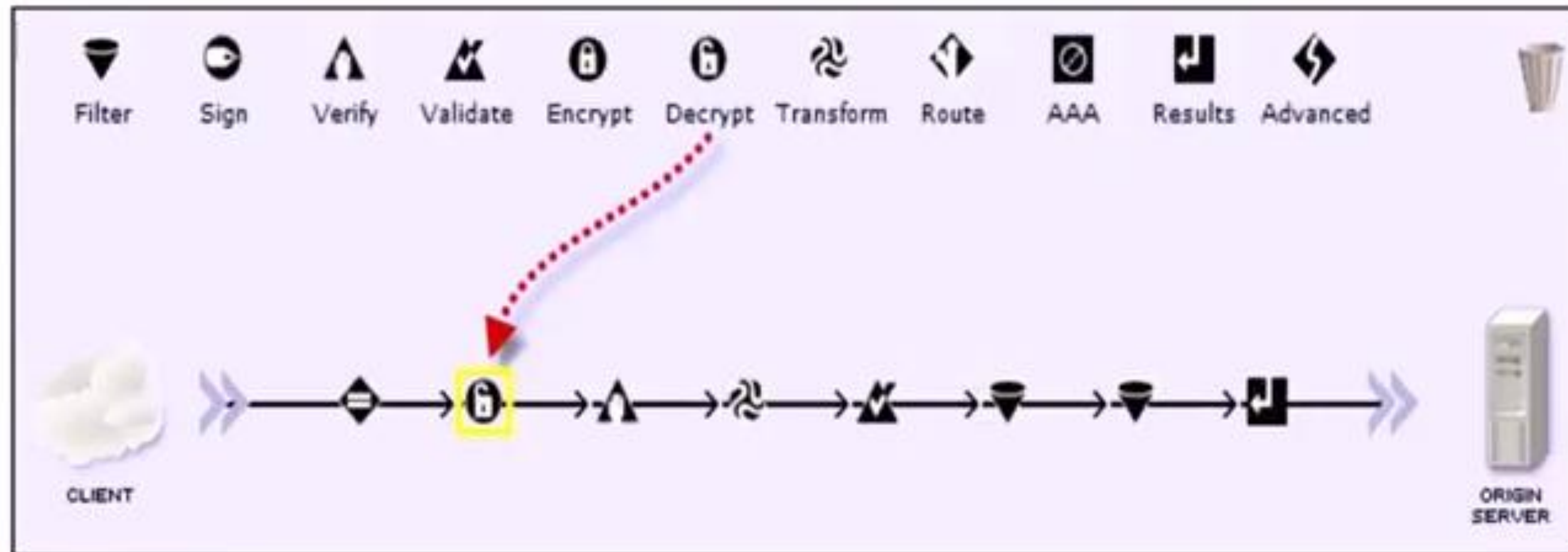
# DataPower - Separacja sieci



## DataPower Gateway zapewnia:

- Wystawienie tylko takich usług HTTP/S jakie są wymagane przez klientów
- Weryfikację komunikatu, tożsamości, podpisu cyfrowego, połączenia TLS
- Szyfrowanie/Odszyfrowanie komunikatu w zależności od potrzeb
- Transformację protokołów, komunikatów i nagłówków

# Jak to się robi?



- Uwierzytelnianie i autoryzacja użytkowników (AAA)
- Weryfikacja podpisu cyfrowego (Verify)
- Szyfrowanie i deszyfrowanie treści (Encrypt, Decrypt)
- Transformacja danych (Transform, Filter: XSLT, Gateway Script, JQuery, XPATH)
- Filtrowanie ruchu również na podstawie treści, IP, nagłówków itp.
- Dynamiczny Routing
- Monitorowanie i raportowanie
- I wiele innych ...

# Wzorce integracyjne

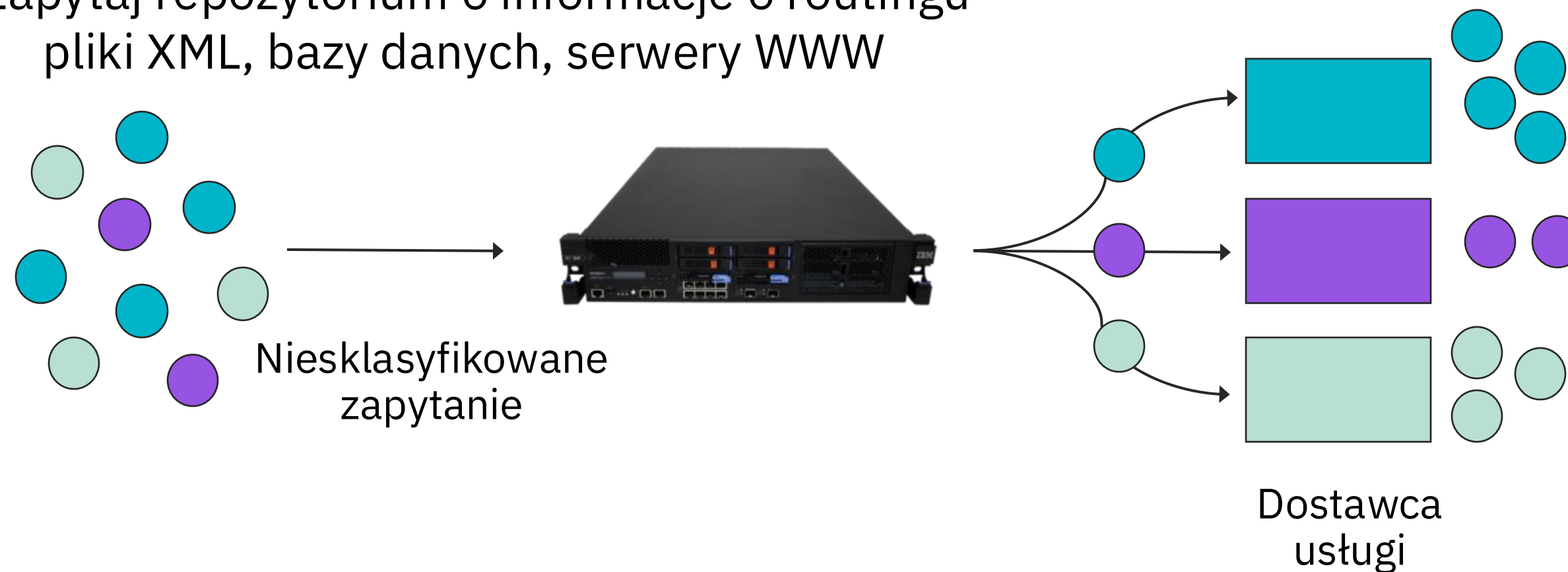
## Routing oparty na treści

Dynamicznie przekierowywuj na podstawie dowolnej treści wiadomości

- Atrybuty, takie jak źródłowy adres IP, żądany adres URL, nagłówki protokołu itp.
- Dane w wiadomości, nagłówki SOAP, XML, zawartość w formacie innym niż XML itp.

Zapytaj repozytorium o informacje o routingu

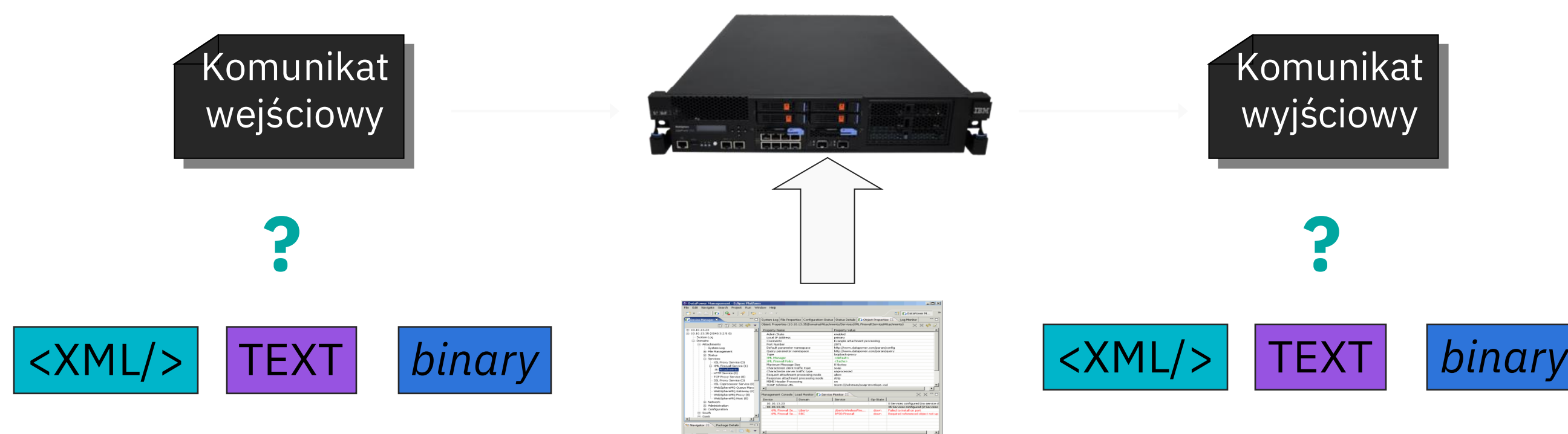
- pliki XML, bazy danych, serwery WWW



## Przekształcanie wiadomości typu „każdy do każdego”

Bardzo elastyczne przekształcanie formatu wiadomości

- Wykorzystanie dedykowanych narzędzi do mapowania danych



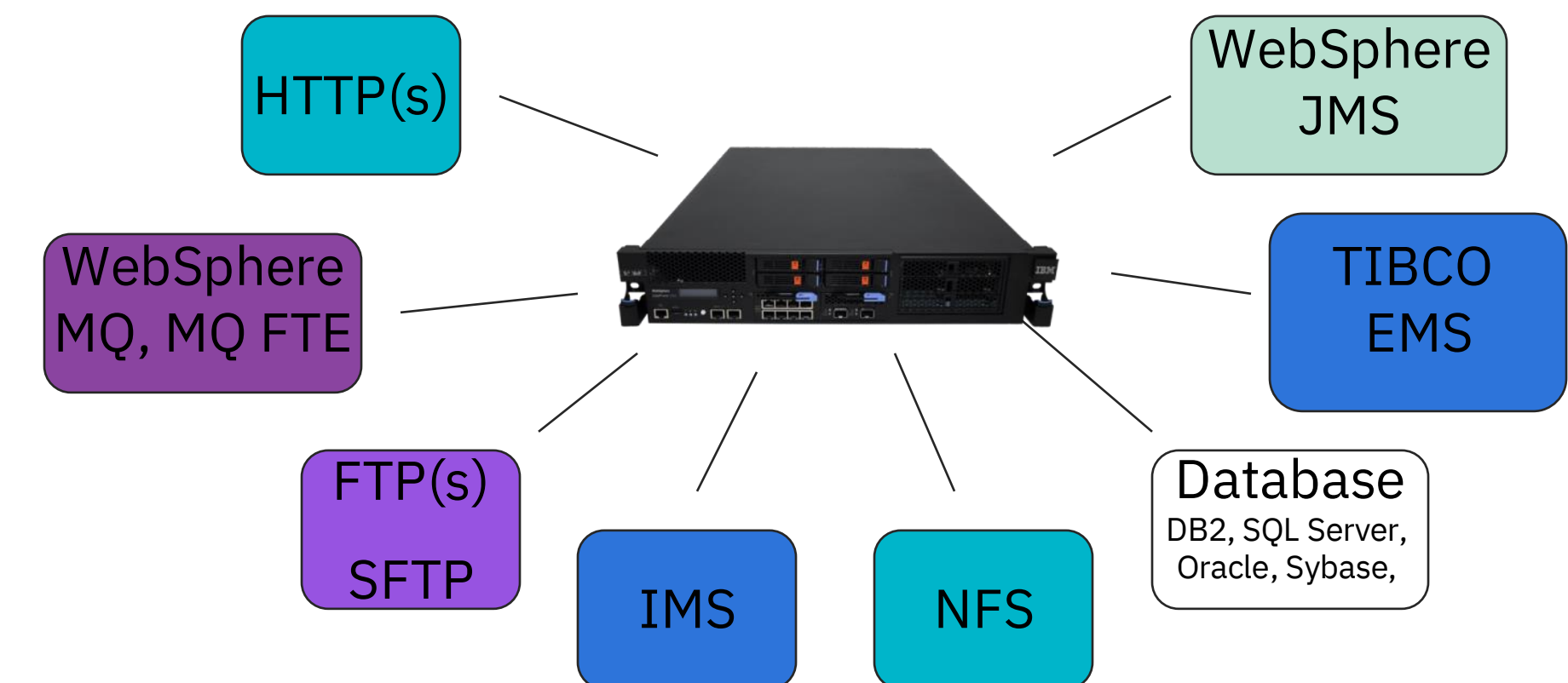
## Konwersja protokołów

Integracja różnych protokołów transportowych

- Brak zależności między przychodzącymi „front-side” i wychodzącymi „back-side”
- Przykłady: HTTP (s), WebSphere MQ, WebSphere MQ FTE, WebSphere JMS, Tibco EMS, SFTP, FTP (s), NFS, IMS, Database (DB2, Oracle, Sybase, SQL Server), Kafka, AMQP

Wsparcie wzorców komunikatów

synchronicznych, asynchronicznych, pub-sub, gwarantowane jednorazowe dostarczanie





# Bezpieczeństwo i wydajność

## SSL/TLS – Offload/terminacja

- Odciążenie systemów biznesowych

## Security Gateway

- Uwierzytelnienie i autoryzacja OAuth 2.0
- Ochrona przed zagrożeniami JSON/XML
- Walidacja JSON i transformacja do XML

## SLA

- Ograniczanie ruchu przy dużym obciążeniu

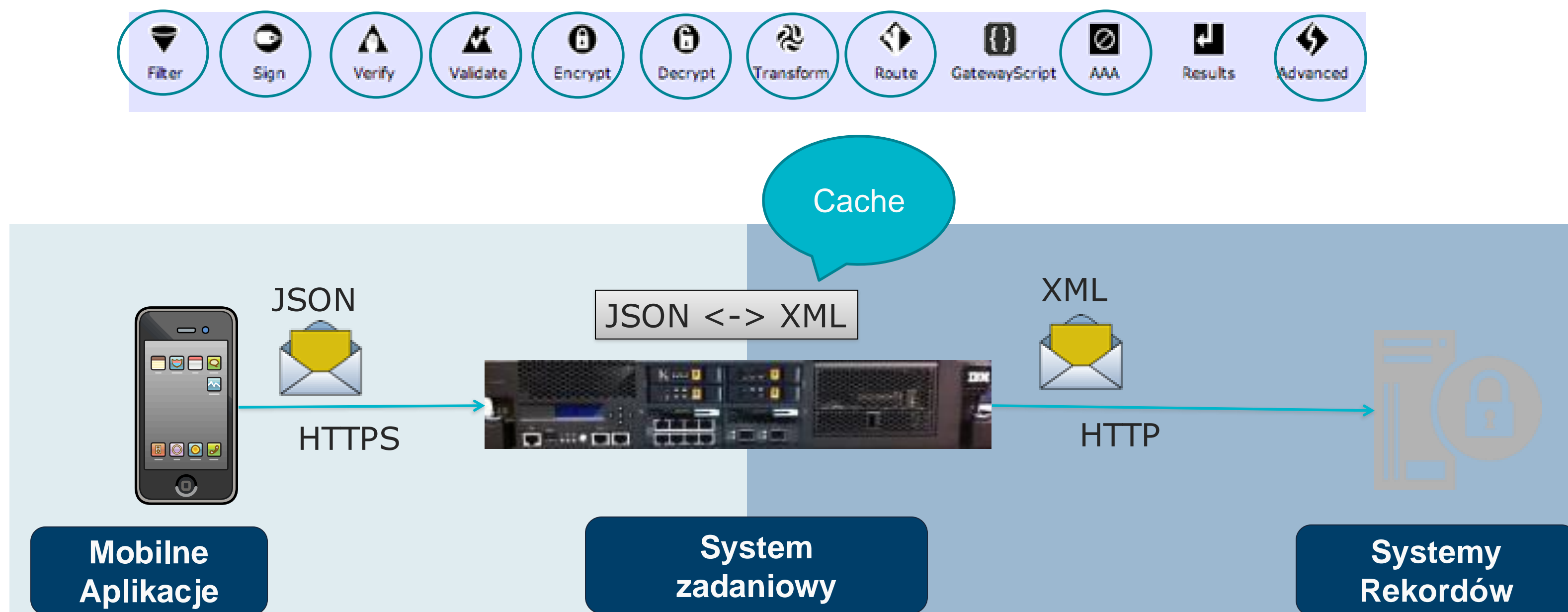
## Loadbalancing oraz routing

## Transformacja do wewnętrznego XML

- Bezpieczeństwo na poziomie pól komunikatu np.:  
nr karty kredytowej

## Przyspieszenie odpowiedzi dzięki wykorzystaniu pamięci podręcznej

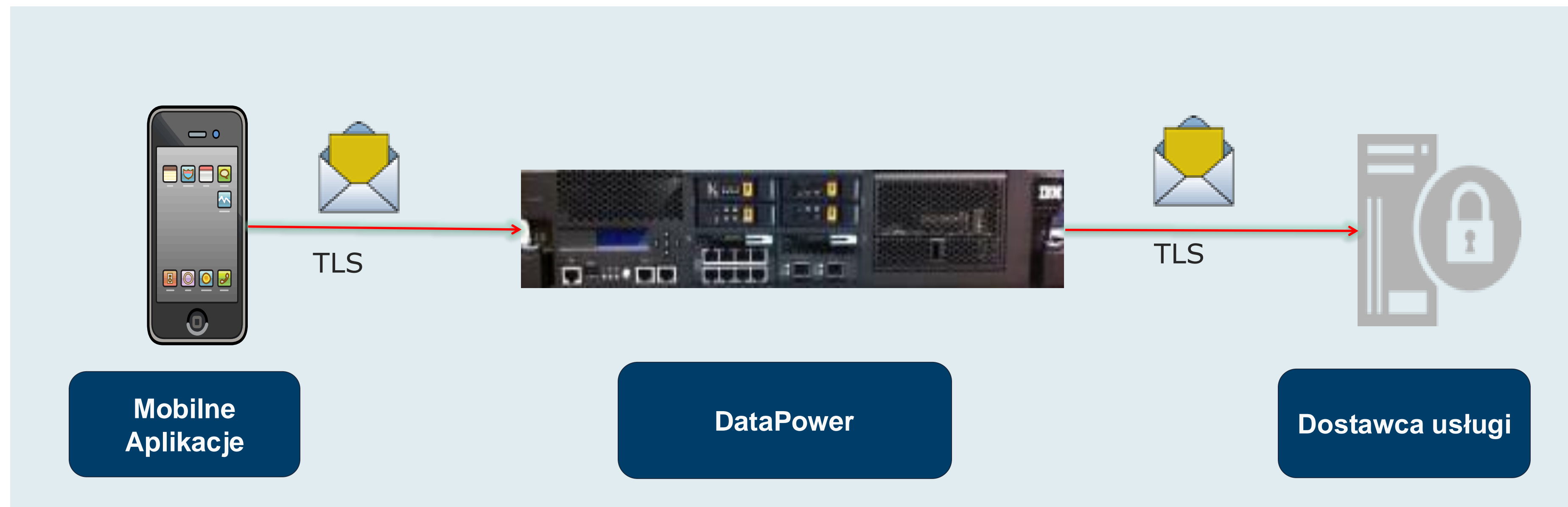
- Wbudowany cache, integracja z eXtreem Scale



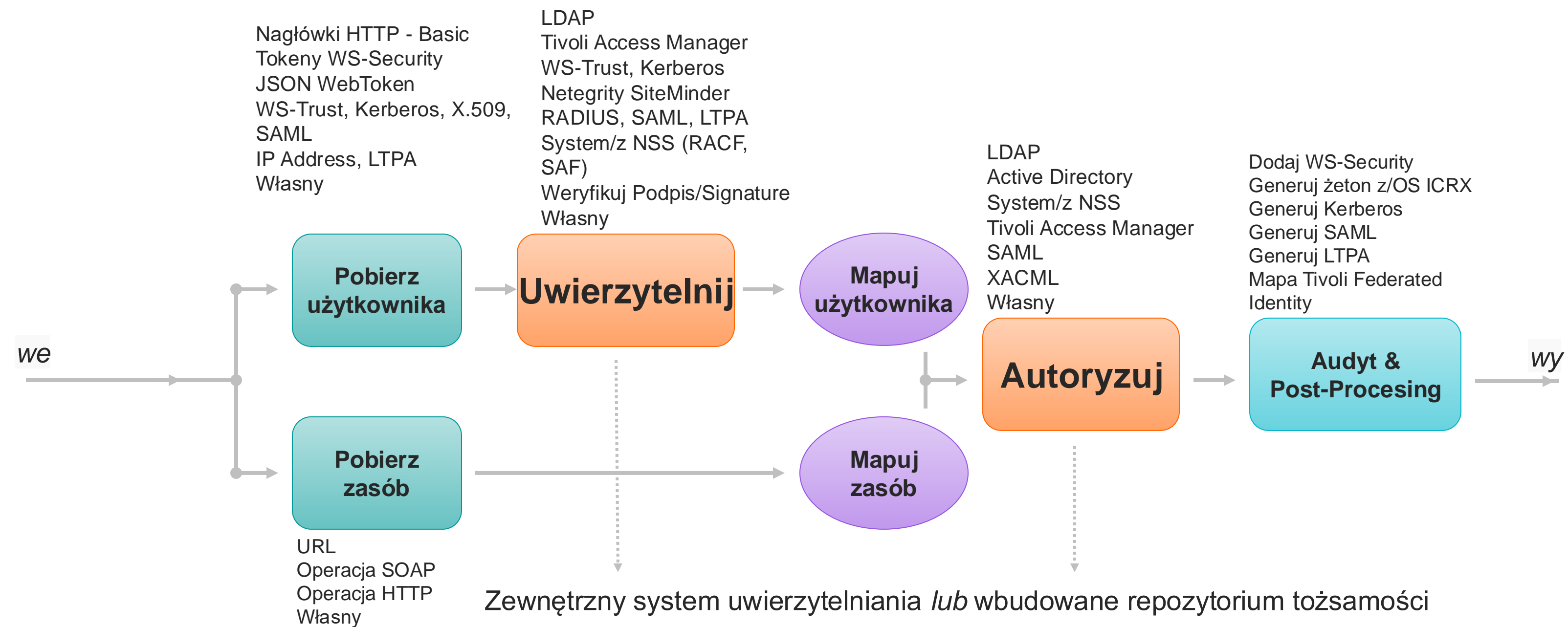
# Mocne standardy bezpieczeństwa

**Chroni najważniejsze aplikacje przed narażeniem bezpieczeństwa za pomocą TLS z użyciem Elliptic Curve Cryptography (ECC), Perfect Forward Secrecy (PFS), oraz Server Name Indication (SNI)**

- ECC zapewnia kompleksową ochronę bez obniżania wydajności, aby unikać luk w zabezpieczeniach
- PFS pomaga uniknąć narażenia bezpieczeństwa ruchu, gdy klucze kryptograficzne są zagrożone
- SNI rozszerza protokół TLS dostarczając możliwość połączenia wielu „host’ów” na tej samej maszynie



# Uwierzytelnienie, Autoryzacja, Audyt



# DataPower - Zabezpieczenia

## XML Thread Protection

- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- \* Replay Attack
- \* Message/Data Tampering
- \* XPath or SQL Injection
- \* XML Virus

## JSON Thread Protection

- Label - Value Pairs
- HTTP Headers
- Thread Protection
- \* Label, Value, Number length
- \* URL length & parameters
- \* Maximum nesting depth & doc size

## WebServices

- Webservice Security
- Digital Signature
- Encryption
- \* Schema & WSDL Validation
- \* Message transformation
- \* Dynamic backend routing

## Authentication

- LDAP/Active Directory
- Kerberos / SAML / RADIUS / LTPA / Oauth 2.0 / Connect ID
- IBM Access Manager / Netegrity SiteMinder
- Signature validation

## Authorization

- LDAP / Active Directory
- XACML
- Oauth 2.0
- IBM Access Manager



# Dostępne wersje DataPower Gateway

- **Urządzenie:** tzw. sprzętowy appliance, dedykowana i rekomendowana platforma z akceleracją sprzętową, gotowa do użycia w strefach DMZ, sprzętowy moduł szyfrujący, zabezpieczenie przed otwarciem, opcjonalny moduł HSM (certyfikacja FIPS 140-2 Level 3), olbrzymie zasoby sprzętowe (32 rdzenie, 256 GB RAM, 2 x 40GbE SFP+, 4x10GbE SFP+, 8x1GbE)
- **Wersja wirtualna:** tzw. wirtualny appliance, elastyczny model licencjonowania - PVU, wsparcie dla wielu systemów wirtualizacji (Linux, Docker, Vmware, IBM Cloud, AWS, Azure, Google Cloud)



## Fizyczne Appliance

DataPower Gateway Appliance

Wdróż urządzenie gotowe do pracy w strefie DMZ, które jest zoptymalizowane pod kątem bezpieczeństwa i wydajności, na brzegu sieci organizacji.



DataPower Gateway Virtual Edition



## Virtual Machines

DataPower Gateway for VMware

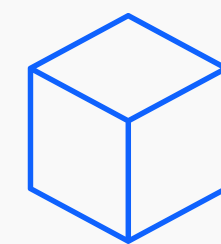
Umożliwia wdrażanie na hipewizorach VMware w chmurze, lokalnie lub w dowolnym środowisku hybrydowym.



## Linux Application

DataPower Gateway for Linux

Umożliwia wdrożenie jako aplikacji systemu Linux na hoście RHEL w chmurze lub kombinacji obu tych elementów w środowisku hybrydowym



## Containers

DataPower Gateway for Docker

Umożliwia wdrożenie jako skonteneryzowaną aplikację w dowolnych środowiskach chmurowych za pośrednictwem Kubernetes i OpenShift.

# Podstawowa funkcjonalność z możliwością rozszerzenia o moduły

## Moduł B2B

- ☐ Brama B2B DMZ
- ☐ EDIINT AS1, AS2, AS3, AS4, ebXML
- ☐ Zarządzanie profilem partnerskim
- ☐ Przeglądarka transakcji B2B
- ☐ Dowolna transformacja komunikatu
- ☐ Połączenie z bazą danych

## Moduł TIBCO EMS

- ☐ Integracja z oprogramowaniem pośrednim przesyłania komunikatów TIBCO EMS
- ☐ Obsługa kolejek i topic'ów
- ☐ Równoważenie obciążenia i odporność na błędy

## Moduł separacja na tenanty

- ☐ Włącza partycjonowanie bramy fizycznej
- ☐ Każdy tenant działa niezależnie i może uruchamiać różne poziomy firmware
- ☐ Izoluje procesor i pamięć dla każdego tenant
- ☐ Obsługiwane są dwa tenanty na bramę

## Moduł optymalizacji aplikacji

- ☐ Frontend self-balancing
- ☐ Inteligentny rozkład obciążenia
- ☐ Session affinity
- ☐ Integracja z z Sysplex Distributor

## Moduł integracji

- ☐ Dowolna transformacja komunikatu
- ☐ Połączenie z bazą danych
- ☐ Połączenia z systemem mainframe IMS

## IBM DataPower Gateway (bazowa funkcjonalność)

### Bezpieczeństwo

- Uwierzytelnianie, autoryzacja
- Translacja security token
- Wirtualizacja usług/API
- Ochrona przed zagrożeniami
- Sprawdzanie poprawności schematu komunikatów
- Filtrowanie komunikatów
- Podpis cyfrowy komunikatu
- Szyfrowanie wiadomości
- Integracja skanowania AV

### Integracja

- Konwersja protokołu transportowego
- Dowolna transformacja komunikatu
- Wzbogacanie komunikatów
- Połączenie z bazą danych
- Połączenie z komputerem mainframe
- Połączenia partnerskie B2B
- Łączność w chmurze hybrydowej
- MQ, AMQP, Kafka

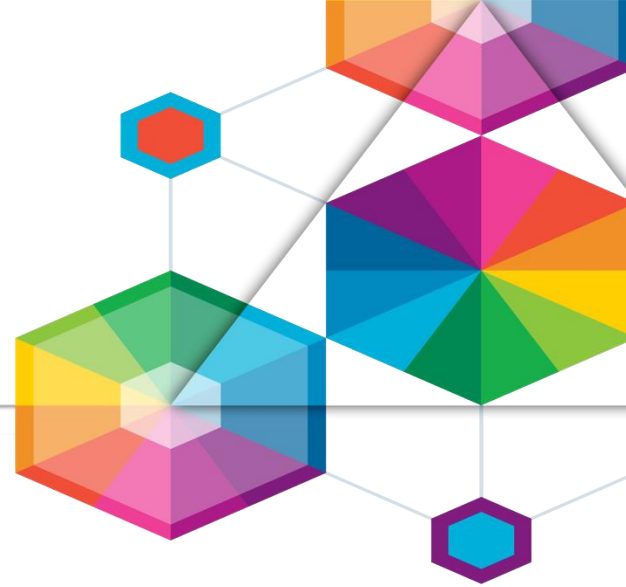
### Kontrola i zarządzanie



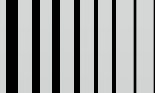

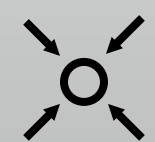
- Limit ilości i wielkości wywołań
- Routing oparty na treści
- Rozliczanie komunikatów
- Zarządzanie partnerem B2B
- Integracja w systemami zarządzania i monitorowania, w tym IBM API Connect

### Optymalizacja i odciążenie

- HTTP/2
- Odciążenie SSL/TLS
- Sprzętowa akceleracja szyfrowania
- Odciążenie JSON, XML
- Akceleracja JavaScript, JSON, XSLT, XQuery
- Lokalne buforowanie odpowiedzi
- Buforowanie rozproszone z WXS
- Równoważenie obciążenia backend

# Rola komponentu Datapower



-  **ZABEZPIECZA** Usługi SOA, Aplikacje, Komunikację B2B ...
-  **INTEGRUJE** Wewnętrzne systemy dziedzinowe z odbiorcami
-  **KONTROLUJE** Ruch i polityki SLA
-  **OPTYMALIZUJE** Wydajność w oparciu o sprzęt
-  **KONSOLIDUJE** Infrastrukturę sieciową i moduły bezpieczeństwa



**IBM DataPower Gateway - jedno miejsce do konfiguracji i zarządzania bezpieczeństwem dostępu do informacji.**



# Post-quantum cryptography

IBM DataPower enhances your ongoing security with introduction of Quantum-safe encryption



By [Matt Roberts](#) posted 11 days ago

1

Like



**IBM DataPower – Tech Preview**  
Quantum-safe encryption



