

# IBM DataPower Gateway

## Usługi DP oraz zabezpieczenia

Mikołaj Jaworski  
Partner Technical Specialist @ IBM



# Typy usług dostępne na Datapower

- XML Firewall
  - zabezpieczenie ruchu XML (XML Encryption, Signatures + AAA)
  - Offload (odciążenie) aplikacji biznesowych w zakresie przetwarzania XML
- Web Services Proxy (WS-Proxy)
  - Wirtualizacja i zabezpieczenie usług bazujących na SOAP/XML
  - Wsparcie standardów WS-\* oraz XML Enc/Sign + AAA
- Web Application Firewall (WAF)
  - Zabezpieczenie i odciążenie przetwarzania dla aplikacji webowych (AAA, walidacje, mitygowanie zagrożeń)
- Multi-protocol Gateway (MPG)
  - Odbiór komunikatów jednym z wielu protokołów i wysyłka do systemów docelowych dowolnym wspieranym protokołem



**XML Firewall**



**Web Service Proxy**



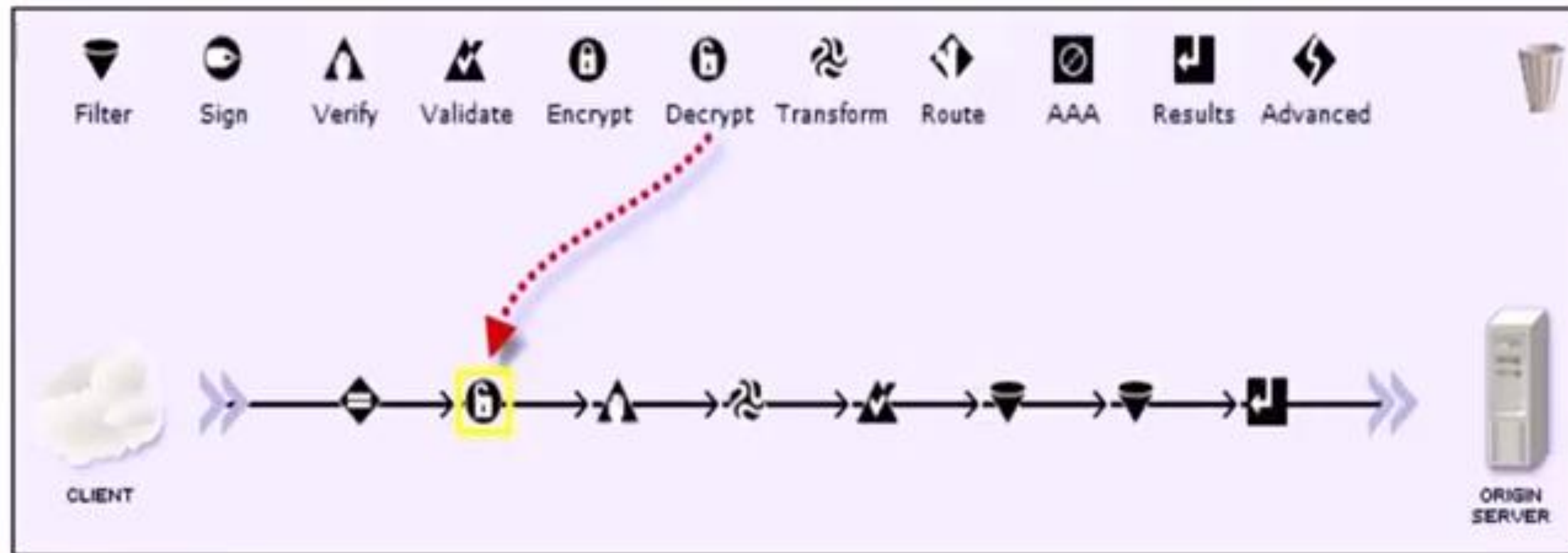
**Web Application Firewall**



**Multi-Protocol Gateway**



# Datapower – logika przetwarzania komunikatów



- Uwierzytelnianie i autoryzacja użytkowników (AAA)
- Weryfikacja danych
- Szyfrowanie i deszyfrowanie treści
- Transformacja danych
- Definiowanie podpisu cyfrowego
- Filtrowanie ruchu również na podstawie treści, numeru pesel bądź IP
- Monitorowanie i raportowanie

# Web Service Proxy (WS-Proxy)

to komponent oprogramowania pośredniego, który istnieje pomiędzy klientem, a usługą internetową.



**Web Service Proxy**

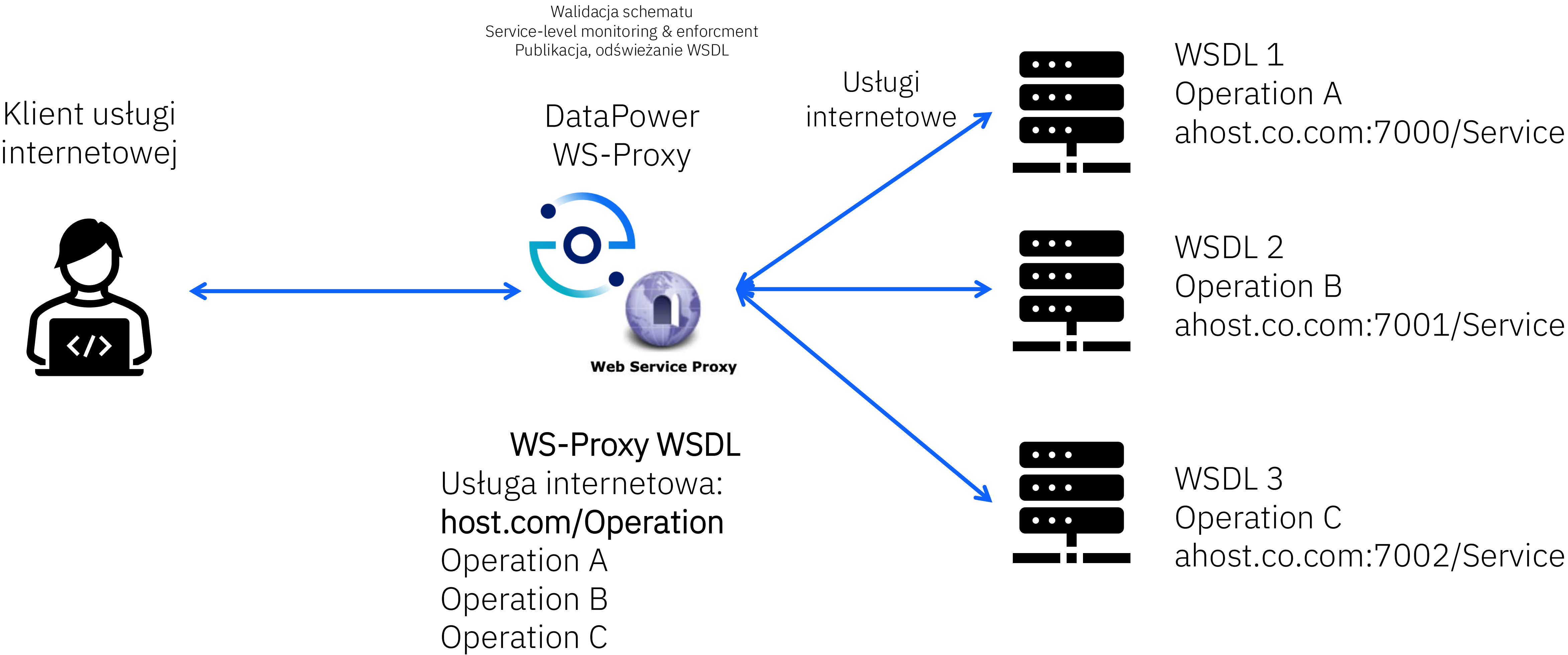
Funkcje WS-Proxy:

- Oddziela klienta usługi od rzeczywistej usługi internetowej.
- Ukrywa adres końcowy usługi internetowej przed klientem.
- Zapewnia elastyczność zmiany adresu back-end'u bez wpływu na kod klienta.
- Może wirtualizować wiele usług internetowych w jedną usługę internetową wystawioną klientowi.
- Zabezpiecza, weryfikuje i wykonuje transformacje zapytania lub odpowiedzi, aby odciążyć usługi back-end'owe.

DataPower umożliwia utworzenie Web Service Proxy w celu przyspieszenia i pośredniczenia w komunikacji pomiędzy klientem, a usługą internetową:

- Reguły powiązane z różnymi częściami interfejsu WSDL.
- Obsługuje wiele dokumentów WSDL.
- Szczegółowa kontrola polityki dla poszczególnych usług.
- Wbudowane funkcje monitorowania poziomu usług (SLM).
- XML Threat Protection.

# Wirtualizacja usług internetowych



# Korzyści Web Service Proxy



## **Web Service Proxy**

1. Wirtualizacja usługi poprzez proste załadowanie dokumentu WSDL
  - Klienci łączą się teraz bezpośrednio z WS-Proxy, a nie z usługą back-end
2. Tworzy politykę przetwarzania z regułami i działaniami na szczegółowym poziomie
  - Reguły na poziomie serwera proxy, usługi, portu lub operacji mogą przetwarzać komunikaty zapytań i odpowiedzi
3. Automatyczna weryfikacja schematu zapytania, odpowiedzi i komunikatów o błędach.
4. Wirtualizacja usług może odbywać się w czasie rzeczywistym
  - WS-Proxy może automatycznie aktualizować WSDL proxy po aktualizacji bazowego WSDL
  - Integruje się z rejestrem i repozytorium usług WebSphere oraz rejestrami UDDI
5. Potrafi egzekwować zasady i monitorować wydajność usług

# Scenariusz

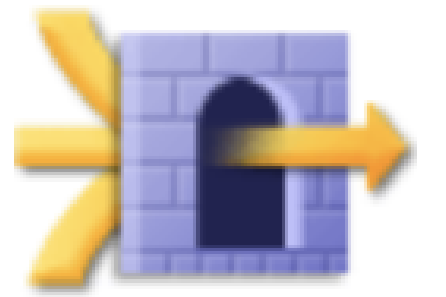
## WS-Proxy

1. Podstawowa konfiguracja usługi WS-Proxy
2. SLM Policy
3. AAA Policy
4. Ochrona przed atakiem SQL Injection



# Multi-Protocol Gateway (MPGW)

łączy zapytania klientów wysyłane przez jeden lub więcej protokołów transportowych z usługą back-end'ową korzystającą z tego samego lub innego protokołu.



**Multi-Protocol  
Gateway**

Oprócz ochrony przed zagrożeniami i możliwości przetwarzania wieloetapowego, MPGW może przetwarzać żądania między różnymi protokołami. Obsługiwane protokoły to HTTP, HTTPS, WebSphere MQ, WebSphere JMS, IMSTM, FTP, NFS, SFTP i TIBCO EMS.

MPGW odbiera przychodzące zapytania, przetwarza je zgodnie z politykami przetwarzania i przekazuje zapytanie do usługi back-end. MPGW przetwarza następnie odpowiedź w podobny sposób, stosując odpowiednie reguły, jeśli została skonfigurowana.

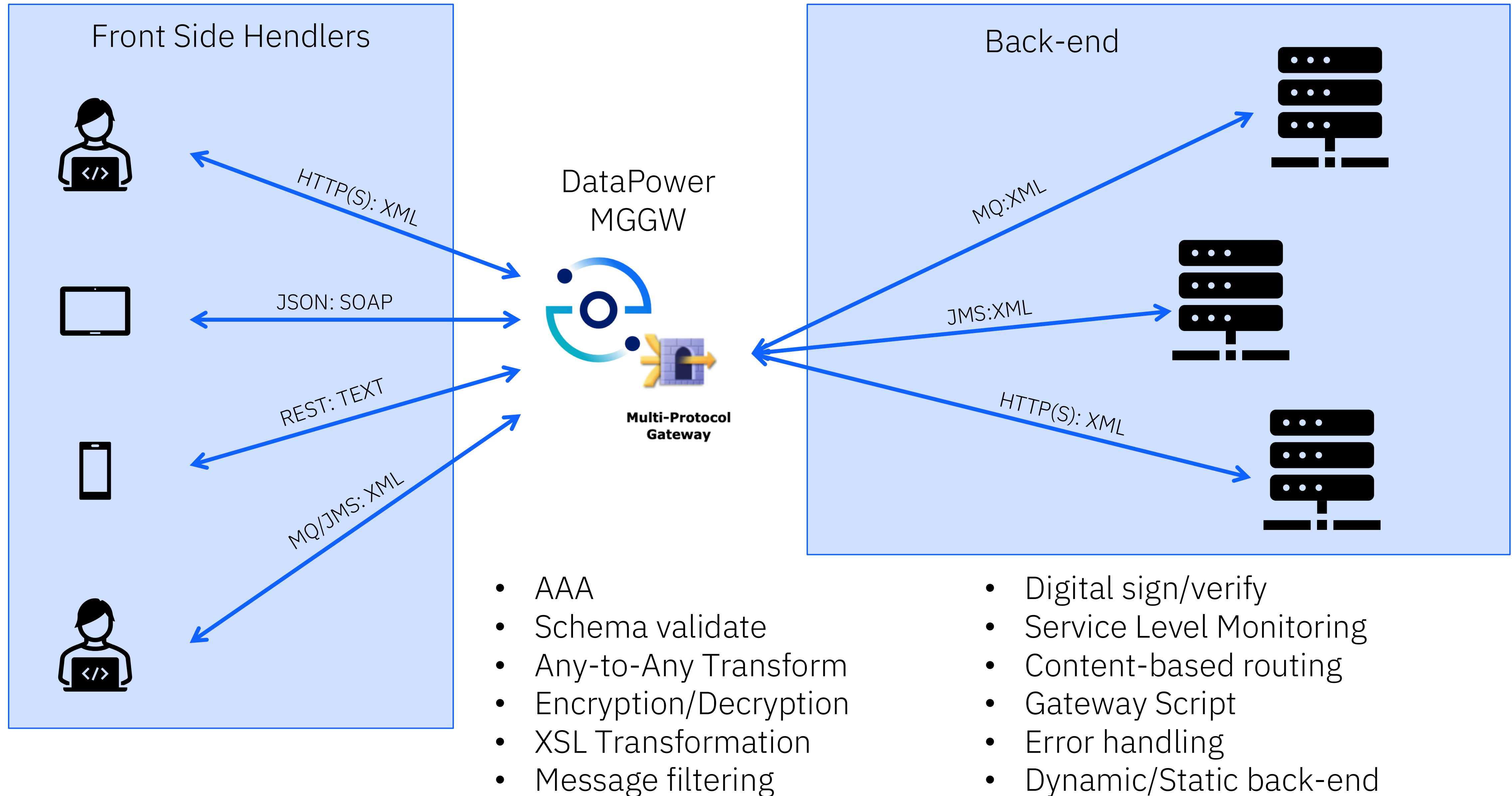
MPGW wykorzystuje Front Side Handlers do zarządzania połączeniem z klientami. Możliwość skonfigurowania wielu FSH umożliwia MPGW odbieranie zapytań z różnych protokołów.

Wszystkie dostępne protokoły, na których MPGW może odbierać przychodzące zapytania, mogą być również używane po stronie serwera w celu przekazywania zapytań do miejsca przeznaczenia. Protokół po stronie klienta nie musi być zgodny z protokołem po stronie serwera.

Usługa MPGW oferuje wiele takich samych usług i możliwości, jak usługa WS-Proxy. W odróżnieniu od WS-Proxy, usługa MPGW nie może wykorzystywać WSDL do określenia konfiguracji.



# Koncepcyjna architektura MPGW



# Scenariusz

## MPGW

1. Podstawowa konfiguracja usługi WS-Proxy
2. Dynamic-backend (routing).
3. Zabezpieczenia na poziomie FSH.
4. Transform with XSLT style sheet.
5. XML Schema Validation.
6. AAA Policy.
7. DataPower Gateway Script.

