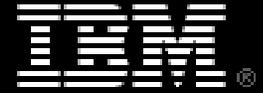


IBM Security Forum
Soluções para um ambiente seguro

WebSphere DataPower SOA Appliance
Garantindo flexibilidade, integração, segurança e governança

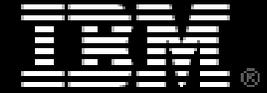
WebSphere. software

Abel Roberth Junior
Product Manager DataPower Brasil
aroberth@br.ibm.com



Agenda

- Desafios
- Tendência de Mercado
- Visão IBM
- O que é Datapower?
- Casos de Uso
- Demonstração



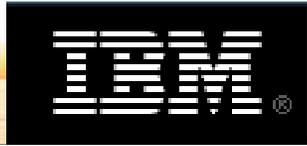
Desafios de IT



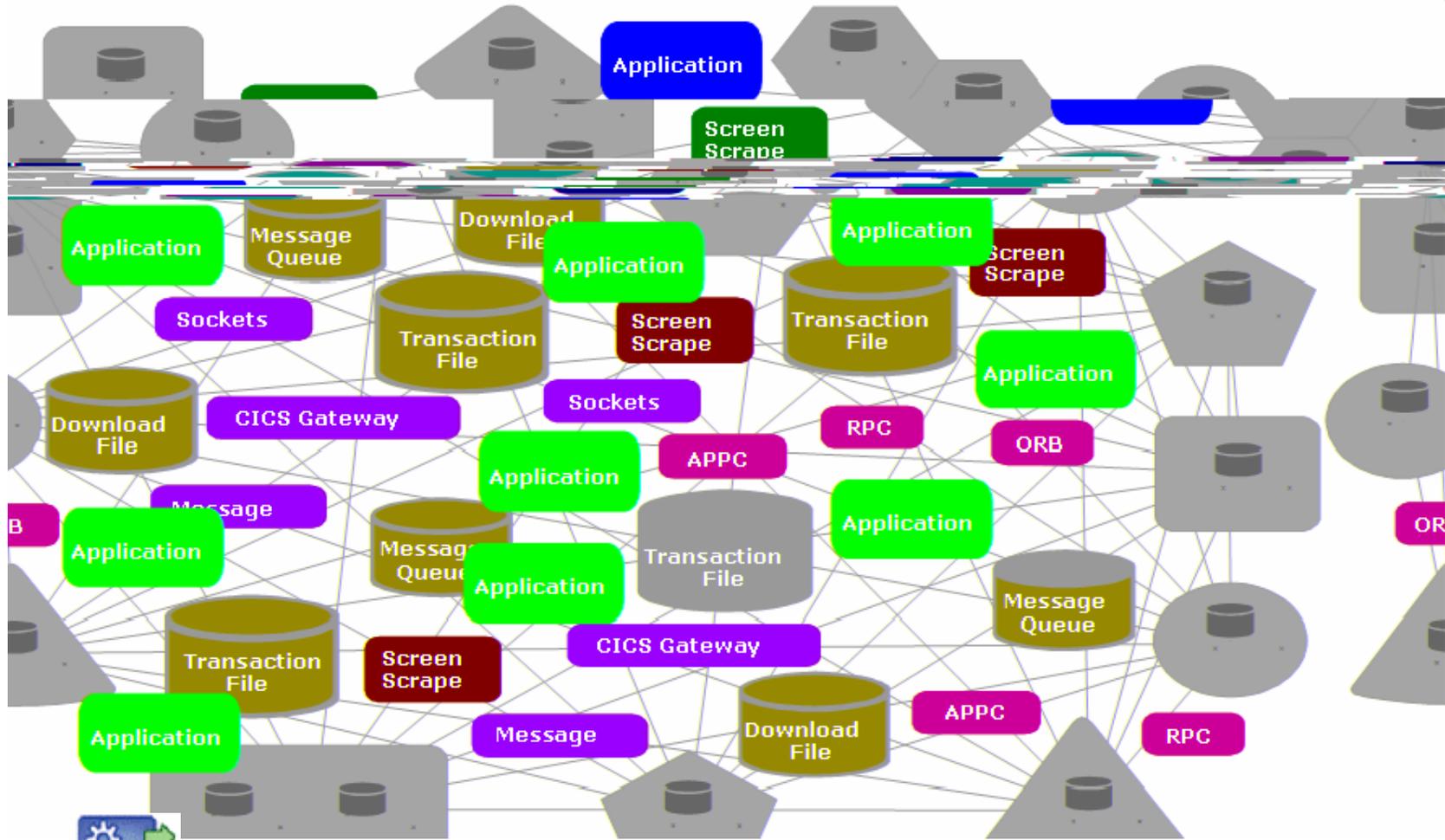
- **Flexibilidade**
 - Adaptação a mudanças.
 - Fusões, parcerias e mudanças de cenário.

- **Governança**
 - Segurança de acesso à informação.
 - Rastreabilidade.
 - Gestão de informação não-estruturada.

- **Alta Performance**



IT: Realidade Cruel...



**Várias aplicações
Tecnologias diferentes**

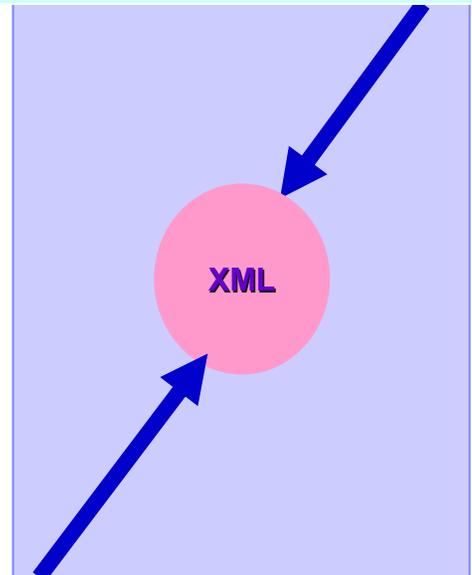


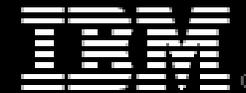


...Qual é a visão do mercado?

Visão do Mercado

- **Aplicativos que permitam ter mais eficiência através da reutilização de serviços.**
- **Aplicativos desenvolvidos em XML para formar a base principal de serviços, mas com isso trazem novos desafios:**
 - ▶ **Escalabilidade**
 - ▶ **Segurança**
 - ▶ **Integração.**
- **As empresas querem mudar para os padrões baseados em XML...mas podem ter desempenho afetado.**
- **As empresas precisam implantar segurança nas aplicações baseadas em XML, mas...aplicar segurança em todas as aplicações requer muito custo e tempo.**
- **As empresas precisam integrar seus novos serviços web com os sistemas legados...mas isto cria a necessidade de um esforço muito grande de integração.**





Solução IBM: XML-aware Network Appliances

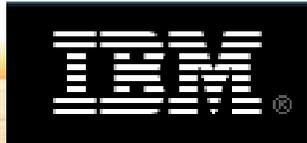
- Resolver performance e escalabilidade de aplicações
- Arquitetura voltada para processos “SOA”
- Offload e combina funções tradicionais de software dentro da arquitetura de appliance:
 - Segurança e transformação de XML
 - Gerenciamento de Web Services
 - Integração com Aplicativos Legados e outros protocolos
 - Recursos de multi tarefas



WebSphere DataPower Appliances

RESULTADOS:

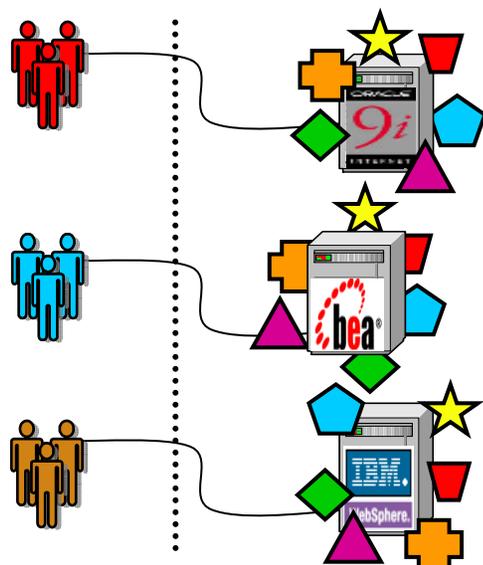
- Maior segurança nas integração
- Redução de latência, maior throughput
- Redução significativa de infraestrutura
- Retorno do investimento da arquitetura em < 1 ano
 - ▶ Redução de custo com manutenção no desenvolvimento das aplicações.
 - ▶ Redução do tempo de implantação de novas regras de integração.



Simplificar, Integrar e Centralizar melhor o core business...

- Centralize - Route, transform, and help secure multiple applications without code changes
- Secure multiple applications without code changes
- Dramatically reduce cost and complexity
- Enable new business with unmatched performance

Before SOA Appliances

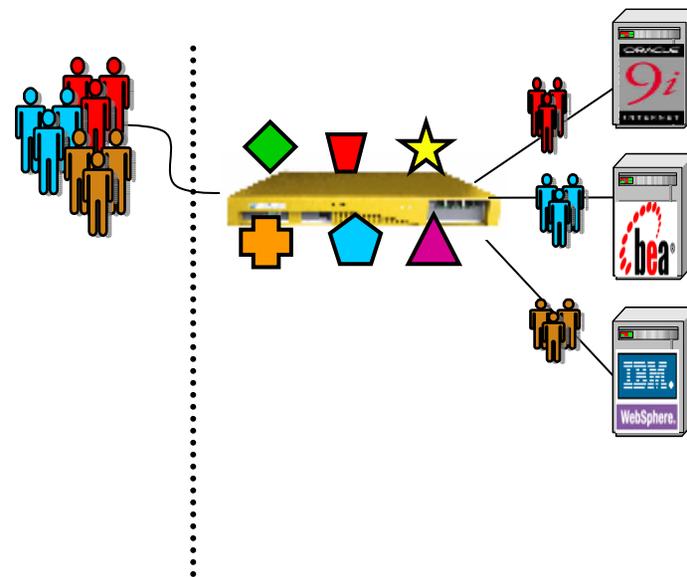


Update application servers individually

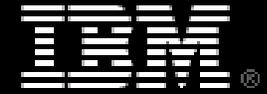
A legend box with a yellow background lists the following symbols and their corresponding functions:

- ▲ Firewall filter
- ⊕ Secure auditing
- ⬠ Routing policy
- ◆ New XML standard
- ★ Access control update
- ▼ Change purchase order schema

After SOA Appliances



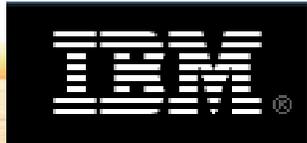
Secure all applications instantly
No changes to applications



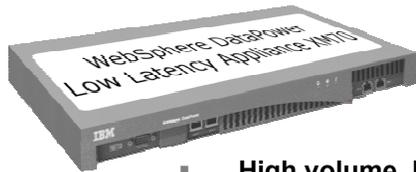
Quais os Benefícios em utilizar um Appliance?

- Reduzir complexidade nas integração com legado e o crescimento de Infraestrutura de servidores.
- Administração centralizada.
- Aumentar a performance em até 70x com até 50% na redução de custo.
- Validação de documentos XML e outros arquivos, com controle de acesso as aplicações via SAML, XACML, WS-Security, LDAP, SSO
- Encriptação e assinatura digital interoperável com WS-Security.
- Complementar as funcionalidades “ESB” na velocidade de Hardware.
- Transformação de XML, binário e mensagens de arquivo.
- Unir múltiplos protocolos de transporte síncronos e assíncronos.
- Roteamento de mensagens baseadas no conteúdo, protocolo de rede ou outro metadado.
- Suporte para Cobol, mensagens ATM, EDI/EDIFACT, ASN.1, IIP0 CORBA, ISO 8583, CICS e MQ.





WebSphere DataPower SOA Appliance Product Line



XM70

- High volume, low latency messaging
- Enhanced QoS and performance
- Simplified, configuration-driven approach to LLM
- Publish/subscribe messaging
- High Availability



XB60

- B2B Messaging (AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Simplified management and configuration



XA35

- XML Pasing, Transformation
- XML Schema Validation
- Extensible Stylesheet Language Transformation (XSLT)
- XML Path Language (XPath) Content Based Routing



XI50

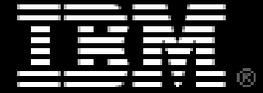
- Hardware ESB
- "Any-to-Any" Transformation at wire-speed
- Bridges multiple protocols (HTTP, MQ, FTP, etc)
- Integrated message-level security
- Message Enrichment, Message Augmentation



XS40

- Enhanced Security Capabilities
- Centralized Policy Enforcement
- Fine-grained authorization
- Rich authentication





Padrões Suportados

▪ OASIS:

- Web Services Security (WSS) TC - Rich Salz
- Web Services Distributed Management (WSDM) – Brian Del Vecchio
- Security Services (SAML) – Rich Salz
- XACML - Rich Salz
- Reliable Exchange, Web Services Transactions – Rich Salz
- XSLT/XPATH Conformance - Jeff Kenton
- Digital Signature Services - Rich Salz
- ebXML Messaging TC - Rich Salz



▪ WS-I:

- Basic Security Profile Working Group - Rich Salz, Bret Hartman
- MC Committee - Kevin Anderson
- SOAP with Attachments Working Group - Rich Salz



▪ W3C:

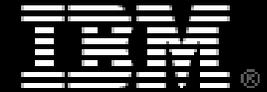
- XML Protocol WG for SOAP - Rich Salz
- XML Binary – Rich Salz
- WS Addressing – Rich Salz
- XML Key Management Services (XKMS) WG - Rich Salz
- XML Encryption WG - Rich Salz
- XML-DSig WG - Rich Salz

▪ OMG (Object Management Group):

- CORBA Security specification - Bret Hartman

▪ ACORD

- Joint Architecture Group [Framework][Security]- Bret Hartman



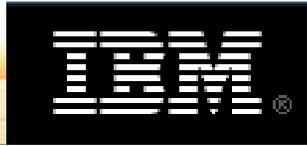
Lista Parcial de Proteção Contra Ataques XML

- XML Entity Expansion and Recursion Attacks
- XML Document Size Attacks
- XML Document Width Attacks
- XML Document Depth Attacks
- XML Wellformedness-based Parser Attacks
- Jumbo Payloads
- Recursive Elements
- MegaTags – aka Jumbo Tag Names
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Message Tampering
- Data Tempering
- Message Snooping
- XPath Injection
- SQL injection
- WSDL Enumeration
- Routing Detour
- Schema Poisoning
- Malicious Morphing
- Malicious Include – also called XML External Entity (XXE) Attack
- Memory Space Breach
- XML Encapsulation
- XML Virus
- Falsified Message
- Replay Attack



Referencias Mundiais



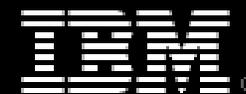


Clientes América Latina



reinventando / los seguros

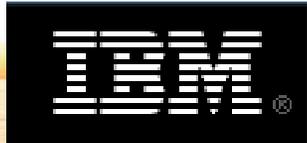




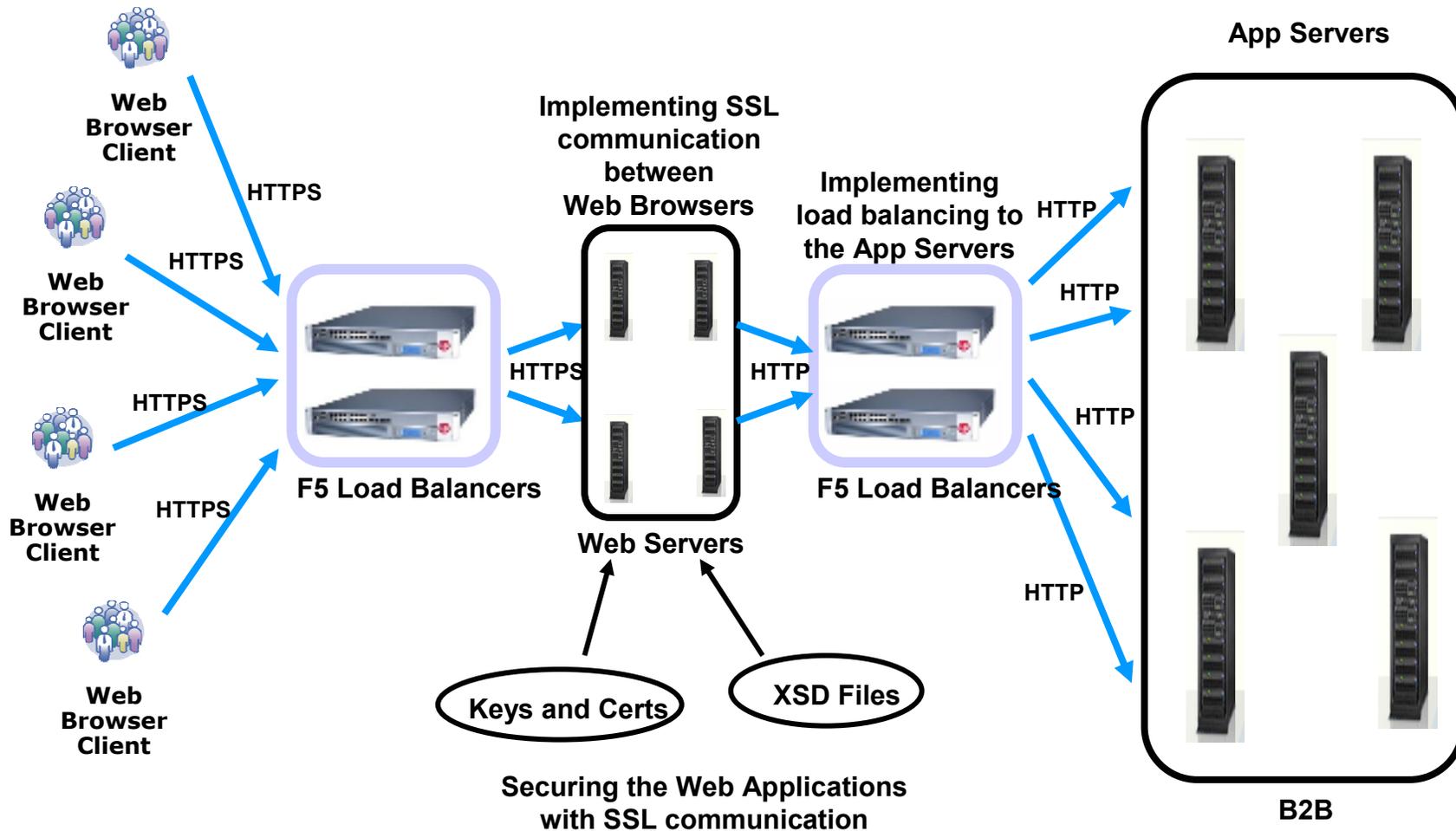
IBM Security Forum
Soluções para um ambiente seguro

Caso de Uso

WebSphere® software

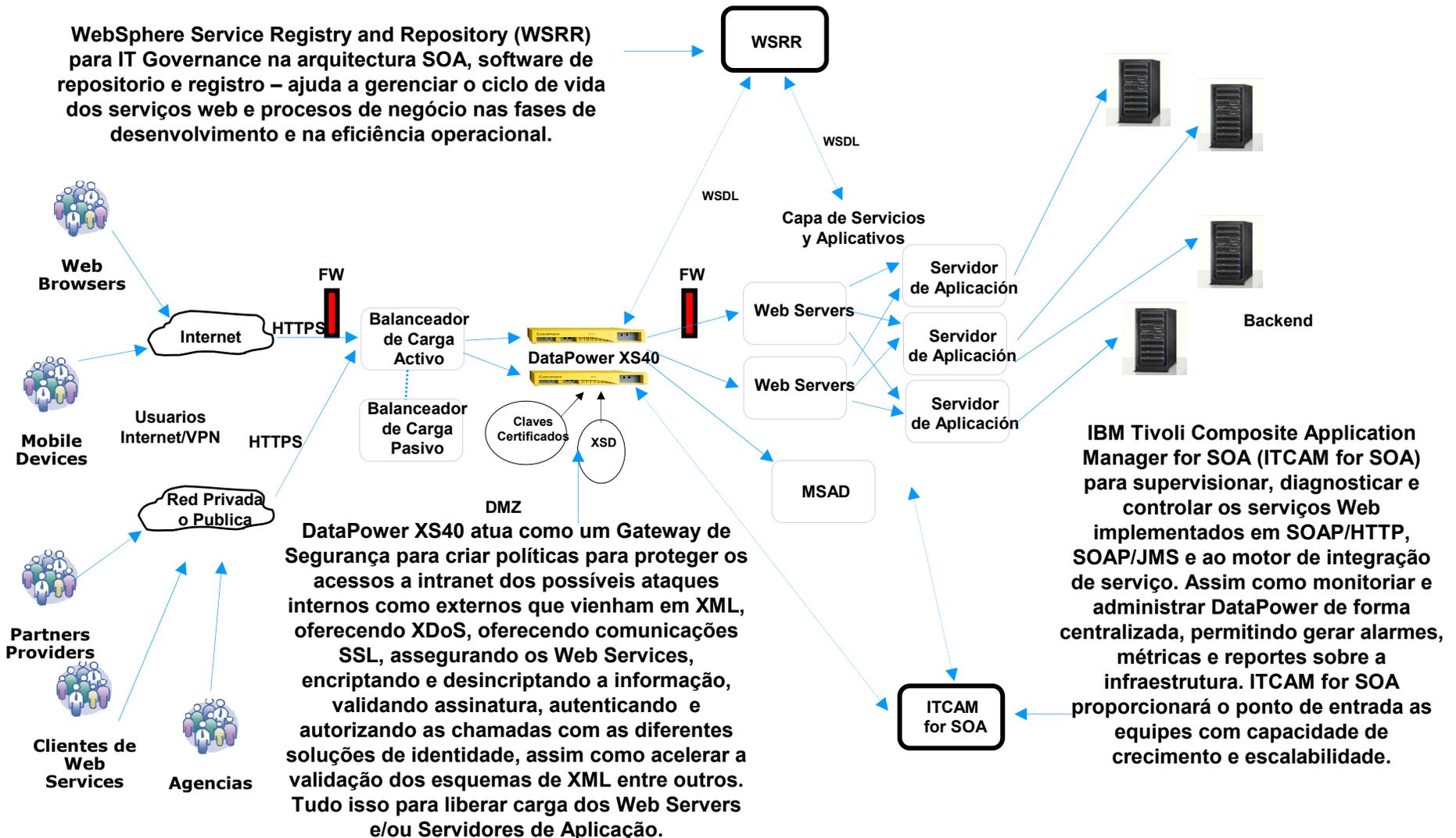


Situação encontrada - Gateway de segurança e Load Balance para App. Server



Ambiente Implantado - Governança

WebSphere Service Registry and Repository (WSRR) para IT Governance na arquitetura SOA, software de repositório e registro – ajuda a gerenciar o ciclo de vida dos serviços web e processos de negócio nas fases de desenvolvimento e na eficiência operacional.





Healthcare Insurance

Infra-estrutura SOA– Reuso, Integração e Segurança

Desafios:

- Construir infra-estrutura SOA com segurança.
- Necessidade de diferentes níveis de segurança interno/externo nos serviços web tanto para cliente quanto para parceiro.

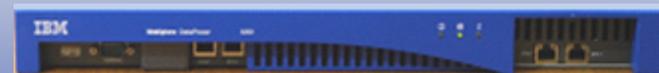
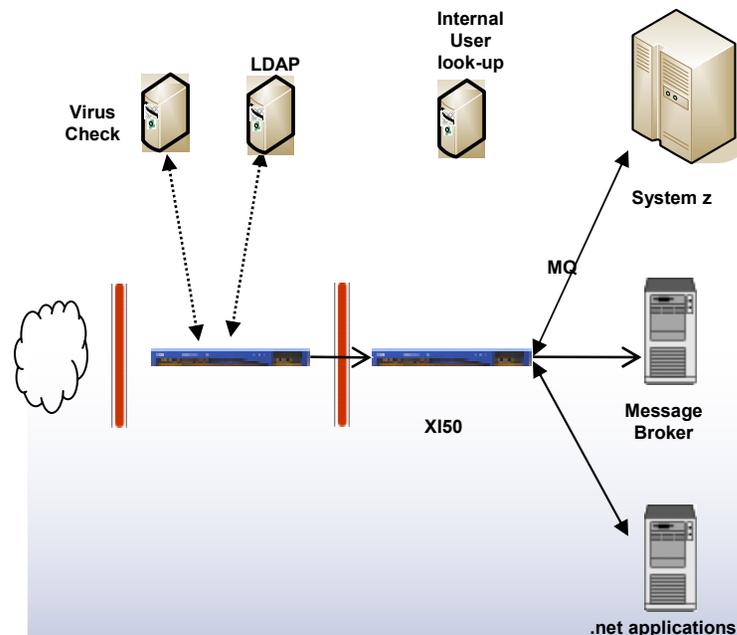
Solução:

Implementação de 10 WebSphere DataPower Integration Appliance XI50

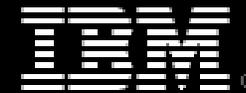
- 8 XI50s - Produção
- 4 XI50s – Site Backup
- 1 XI50s – Desenvolvimento e Teste
- DataPower estendeu o ESB existente Message Broker ESB atuando como gateway para receber transformações com segurança, mensagens encriptadas, assinatura digital e protocolo (HTTPS-para-MQ)

Benefícios:

- Centralização das políticas de acesso.
- Validação de Schema, verificação de ataques XML (vírus)
- Gerenciamento do SLA
- Aceleração nas transformação XML



- WebSphere DataPower Integration Appliance XI50
 - WebSphere Message Broker



Intuit Inc.

Simplifique, Ajuda na Segurança, & Aceleração SOA

Desafios:

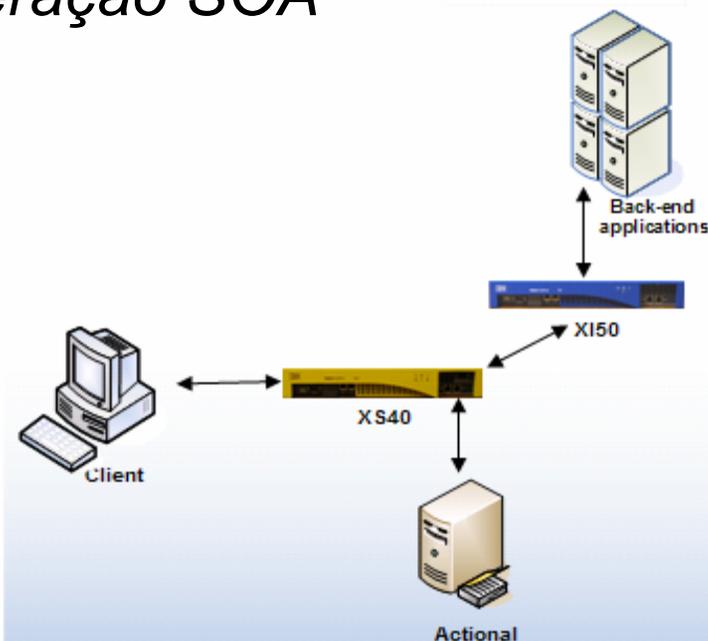
- Implementar uma infra-estrutura com maior escalabilidade para suportar transações online com mais segurança e gerenciamento do ambiente de IT.

Solução:

- Implementar WebSphere DataPower Integration Appliance XI50 e WebSphere DataPower XML Security Gateway XS40
- O XI50 como integrador das chamadas externas aliviando a carga ao TIBCO EMS. A solução quebrava as chamdas e redirecionava aos Web services apropriados.
- O XS40 implantado na DMZ garantindo que todos os acesso sejam validos no ambiente da corporaçã, oferecendo uma gama de serviços de segurança aos serviços web da companhia.

Benefícios:

- Maior segurança ao alto volume de autorização de cartão de crédito.
- Mais rápido na implementação das regras com menor custo.
- Solução avalida como, menor risco, menor custo do que outras abordagens tradicional de software.



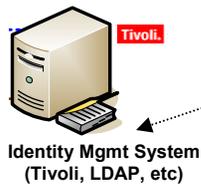
- WebSphere DataPower Integration Appliance XI50
- WebSphere DataPower XML Security Gateway XS40



Cenário

1. External Party makes Web Service request
(Web Services = HTTP with XML Payload)

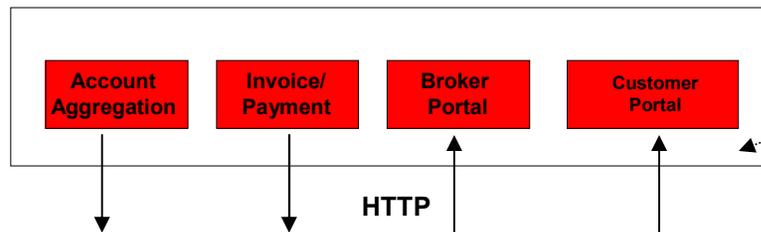
- 2. Verifica assinatura
- 3. Descripta & Valida
- 4. Acessa o sistema IDM
- 5. Autentica & autoriza



- 6. Inserir token na chamada (e.g. SAML, Kerberos)
- 7. Envia chamada para integrar ao legado

- 8. Transforma XML
- 9. Switch protocol (e.g. HTTP to MQ)
- 10. Routea baseado no conteúdo

Request Message



Web Services Interfaces



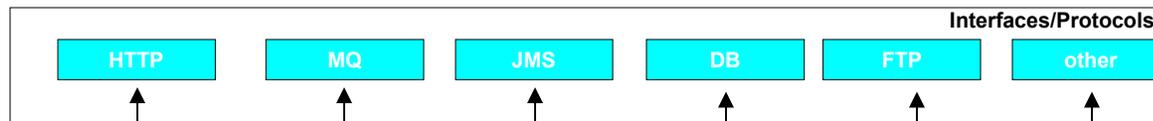
- 17. Envia resposta de retorno
- 16. Encrypta & Assina
- 15. Filtra a resposta



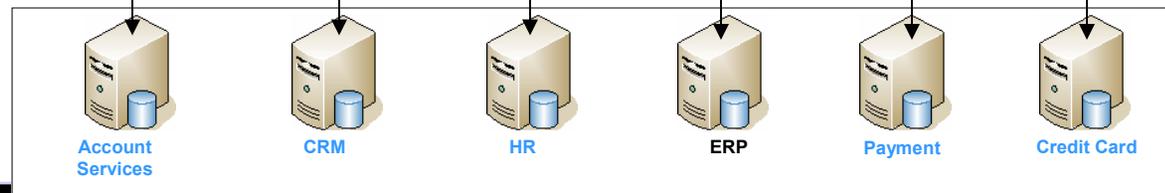
Security Layer
Integration Layer

- 14. Envia para security layer
- 13. Transforma a resposta
- 12. Troca o protocolo
- 11. Agrega as respostas

MQ, JMS, FTP, HTTP, etc.

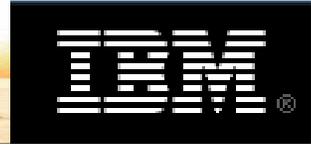


Response Message



FI Owned Systems
External Systems





Regional Manufacturing Company

Segurança de Web Service e ESB Leve na para SOA

Desafios:

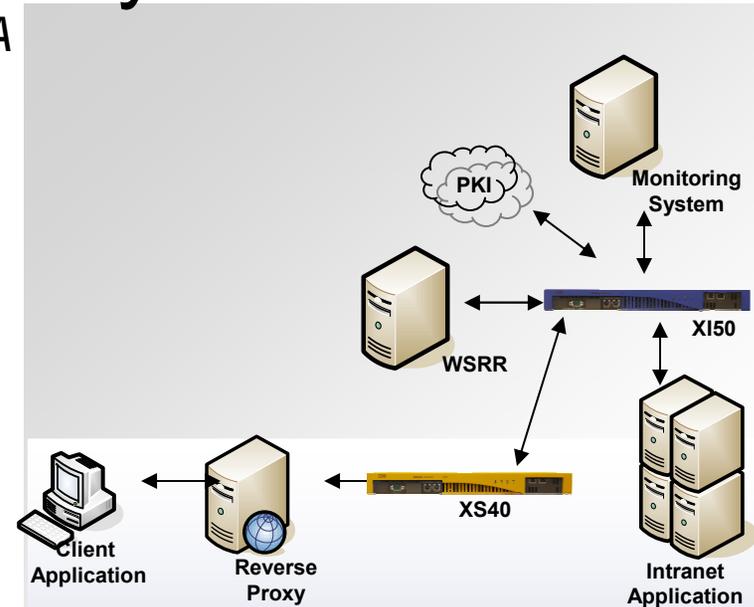
- Implementar Web services baseados em SOA
- Capacidade de fornecer lista de problemas conhecidos por cada produto fabricado.

Solução:

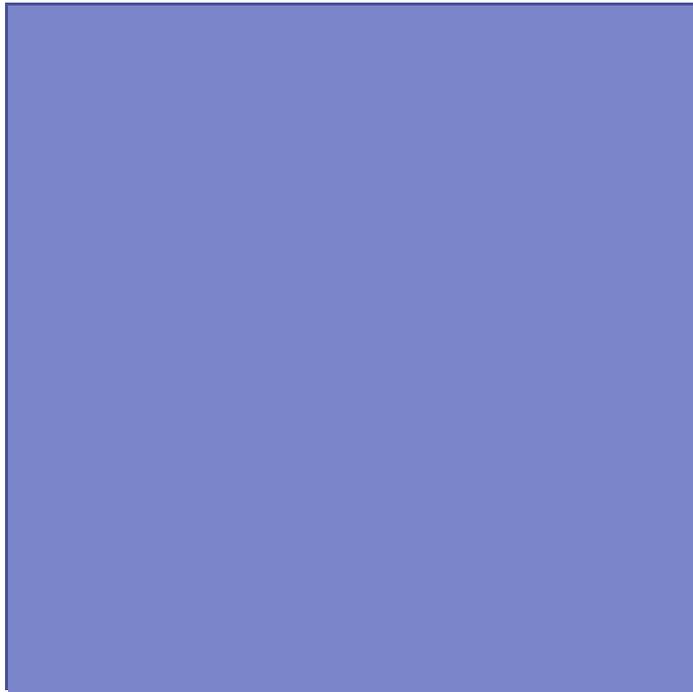
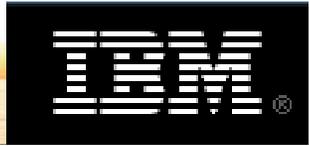
- Implementar WebSphere DataPower Integration Appliance XI50 como um ESB
- Implementar WebSphere DataPower XML Security Gateway XS40 como um proxy para verificar assinatura digital, autenticação e autorização do Web services do cliente
- Planejar integração entre DataPower & WSRR

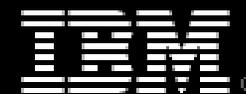
Benefícios:

- Dezenas de serviços implementados no 01 ano e 2x mais no segundo ano.
- Log files & SNMP alerts to 3rd party Monitoring System



- WebSphere DataPower Integration Appliance XI50
- WebSphere DataPower XML Security Gateway XS40
- WebSphere Service Registry & Repository
- WebSphere Application Server & System z

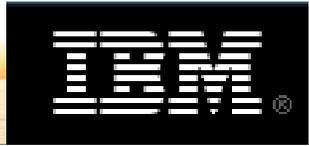




IBM Security Forum
Soluções para um ambiente seguro

Demonstração de Caso de Uso

WebSphere. software

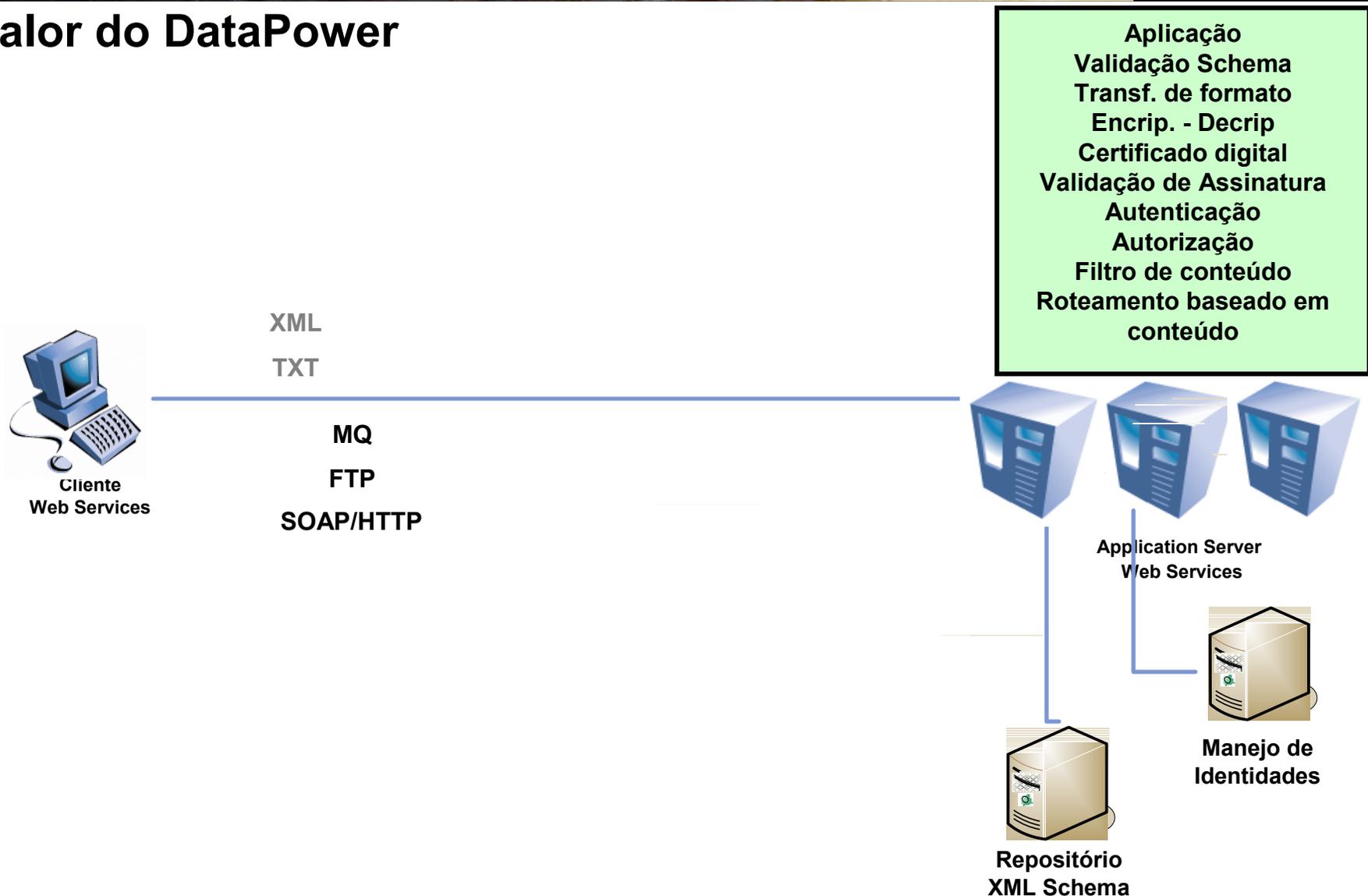


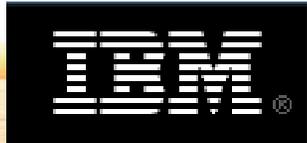
Demonstração





O Valor do DataPower

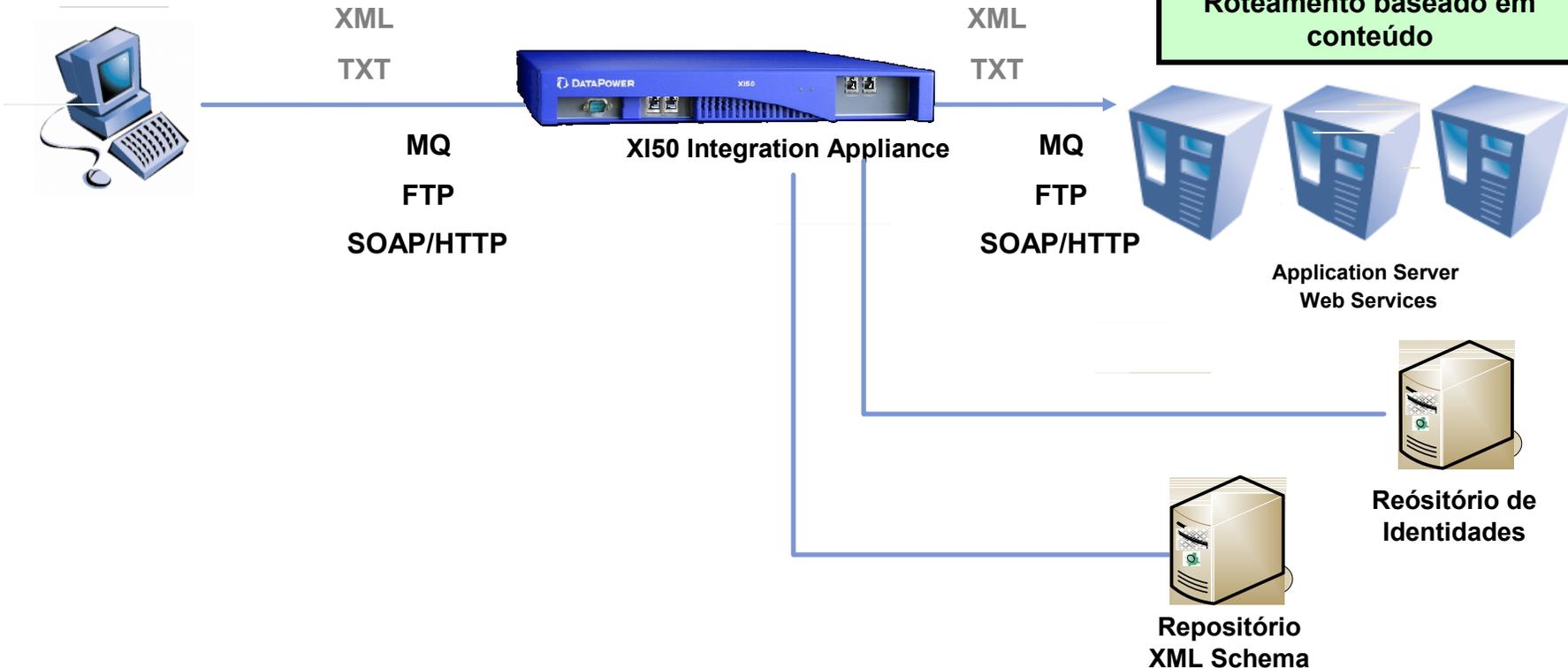


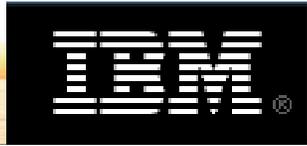


O Valor do DataPower

Appliance

- Aplicação
- Validação Schema
- Transf. de formato
- Encryp. - Decrip
- Certificado digital
- Validação de Assinatura
- Autenticação
- Autorização
- Filtro de conteúdo
- Roteamento baseado em conteúdo





Trugarez

Breton

Merci

French

Dziękuję

Polish

ﻻ ﺷﻜﺮ ﻻ ﻛﻮﻥ

Arabic

고맙습니다

Korean

תודה רבה

Hebrew

धन्यवाद

Hindi

多謝

Traditional Chinese

Tack så mycket

Swedish

Thank You

English

Obrigado

Brazilian Portuguese

Tak

Danish

Grazie

Italian

Dankon

Esperanto

谢谢

Chinese Simplified

Danke

German

Dank u

Dutch

ขอบคุณ

Thai

ధన్యం

Telugu

Dekujeme Vam

Czech

Abel Roberth Junior *rt*
aroberth@br.ibm.com