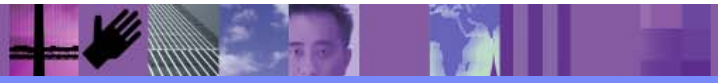
Soluciones de seguridad de implantación inmediata

WebSphere software

Alex Gabarró
WS Sales Specialist
agabarro@es.ibm.com

Agenda

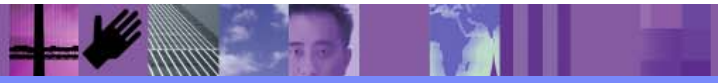
- **Problema de negocio**
- **Solución Propuesta por IBM**
- **Ventajas diferenciadoras de la propuesta de IBM**
- **Recuperación de la inversión – Ahorro de costes.**
- **Casos de éxito**



Problema de Negocio: Retos asociados al XML y a los Web Services

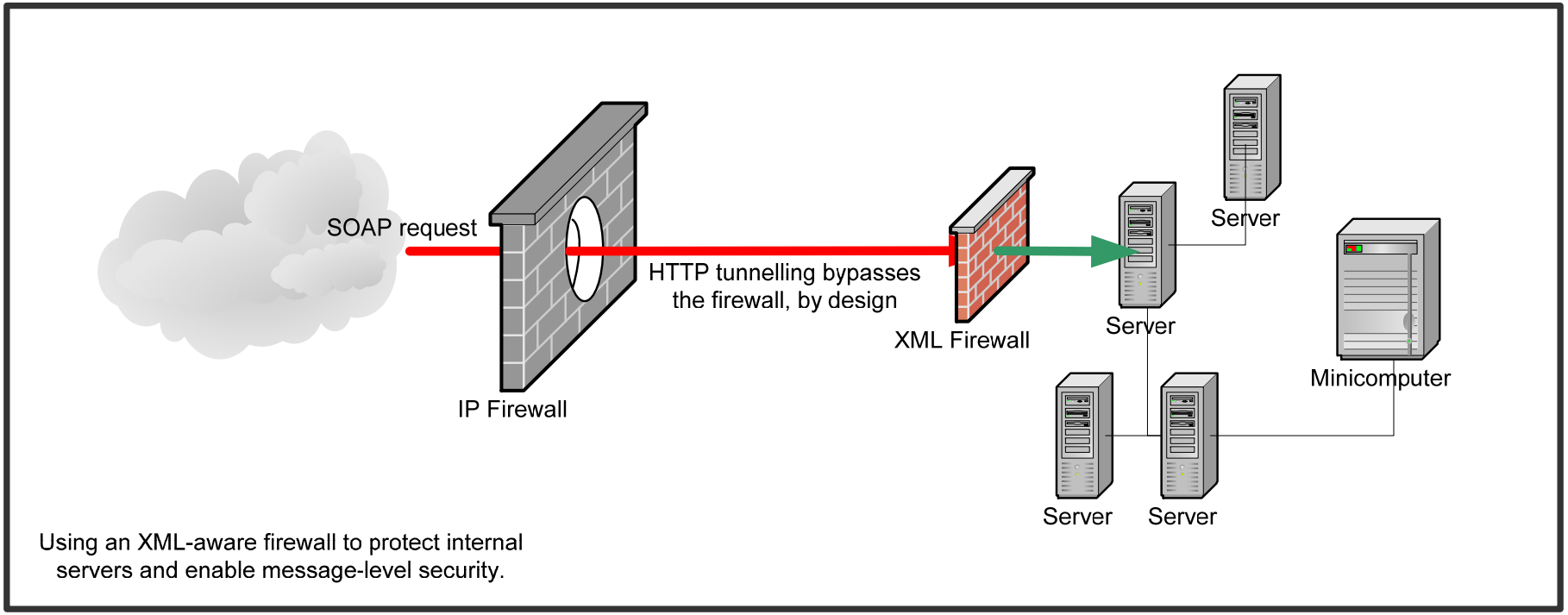
- TENDENCIA: La **comunicación entre aplicaciones tanto internas como externas** se va a realizar utilizando **Web Services.**
  - Conjunto de protocolos y estándares abiertos que facilitan la comunicación entre aplicaciones. Utiliza HTTP como protocolo de transporte y XML como lenguaje

- Este sistema de comunicación puede resultar caro y complejo



Seguridad: La gran preocupación

- La utilización de Web Services expone los back-ends a los distintos usuarios
- Los dispositivos tradicionales de seguridad no protegen contra Ataques XML/SOAP
- Asegurar las comunicaciones antes de que el mensaje se introduzca en la red interna



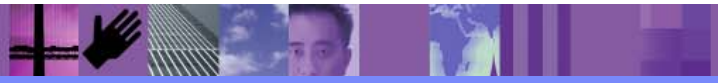
Using an XML-aware firewall to protect internal servers and enable message-level security.

Lista de 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

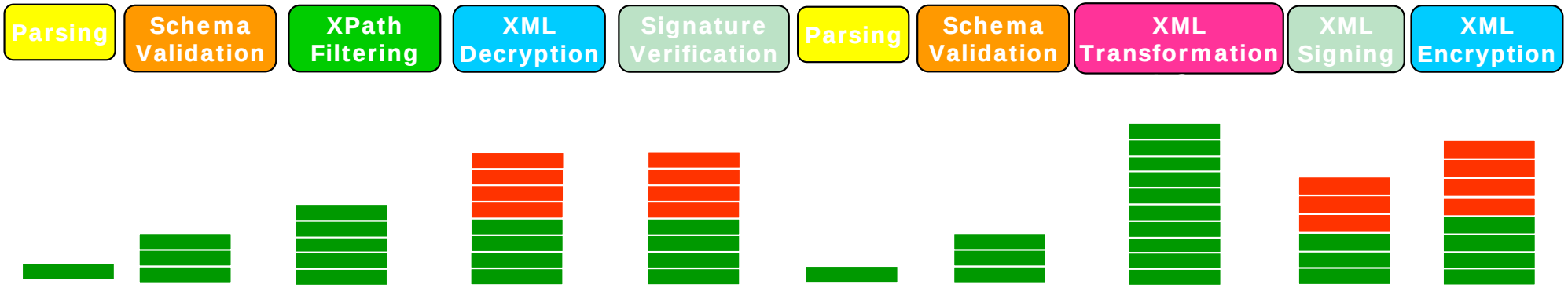
¿Qué entendemos por seguridad en el mundo de los WS?

- **Firewall XML**
  - Protección contra ataques XML
  - Filtro por cualquier parámetro: dato, metadato, puerto, IP, url, etc.
- **Validación de Datos** – Aceptación o Rechazo de tráfico XML entrante/saliente
  - Mensajes bien formados
  - Mensajes que cumplen el esquema XML/WSDL esperado
- **Control de Acceso**
  - Autentificación: ¿quién está intentando acceder?
  - Autorización: ¿tiene permiso?
  - Auditoría: ¿puedo registrarlo?
- **Virtualización de servicios** – Ocultación del back end
- **Gestión de ficheros adjuntos** – Integración con antivirus
- **Confidencialidad**
  - Encriptación del canal de comunicación: SSL, HTTPS
  - Encriptación de la información
- **Comprobación de la integridad de la información-** Firma digital
- **Monitorización y niveles de servicio**



Retos asociados al XML y a los Web Services
Escalabilidad y Rendimiento

Pasos del procesamiento XML



- Todas las funciones de seguridad requieren un procesamiento intensivo
- Obligación de implementar todos los servicios sin comprometer a la empresa
- Necesidad de poder escalar la solución al aumentar el número de peticiones y el número de servicios

La solución de IBM: WebSphere DataPower

- **ASEGURA** los entornos SOA, Web 2.0, B2B y Cloud
- **SIMPLIFICA** la infraestructura de conectividad
- **ACELERA** el tiempo de conseguir valor
- **GOBIERNA** la arquitectura que tengamos

Dispositivos DataPower proveen un **bajo coste de arranque**

Ayudando a las compañías a incrementar **ROI** y **reducir TCO**

Con un especializado y dedicado dispositivo, que combina el rendimiento superior y la seguridad más robusta

DataPower ajusta las necesidades de conetividad

XB60

- Mensajería B2B (AS1/AS2/AS3)
- Gestión de perfiles de socios comerciales
- Visor de transacciones
- Alto rendimiento B2B

XM70

- Volumenes extremos, latencia en micro segundos
- Calidad de servicio mejorada y rendimiento
- Configuración dirigida a LLM
- Puenteo de protocolos de mensajería

XS40

- Seguridad de Web Services
- Política de gestión centralizada
- Autenticación muy amplia
- Autorización muy granuralizada

XI50

XI50B

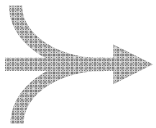
- Hardware ESB
- Conversión “Any-to-any” a alta velocidad
- Puenteo de protocolos amplio
- Ruteo dinámico e inteligente distribución de carga

¿Porqué usar un dispositivo para seguridad?

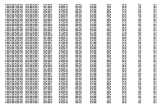
- Construido a propósito, plataforma ajustada **segura**
- Provee los más altos niveles de certificación de **Seguridad**
  - **FIPS 140-2 Level 3**
  - **Common Criteria EAL4**
- Ejecuta el más alto **rendimiento** con múltiples niveles de aceleración HW
- Multiples funciones incorporadas en un **único dispositivo**
  - **Gestión de Nivel de Servicio**
  - **Ruteo dinámico y distribución de carga dinámic**
  - **Seguridad completa**
  - **Políticas robustas**
  - **Transporte y transformación de mensajes**
- **Simplificado** modelo de mantenimiento
  - **Despliegue sencillo.**
  - **Dispositivo configurable.**
  - **Securización de tráfico en minutos**
  - **Proceso de actualización sencillo, basado en F**
  - **Se integra con los sistemas existentes**

Dispositivos WebSphere DataPower

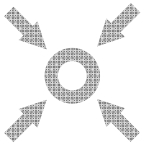
SEGURIDAD



SIMPLIFY



ACCELERATE



GOVERN

Cómo lograr una seguridad sin precedentes con hardware y firmware

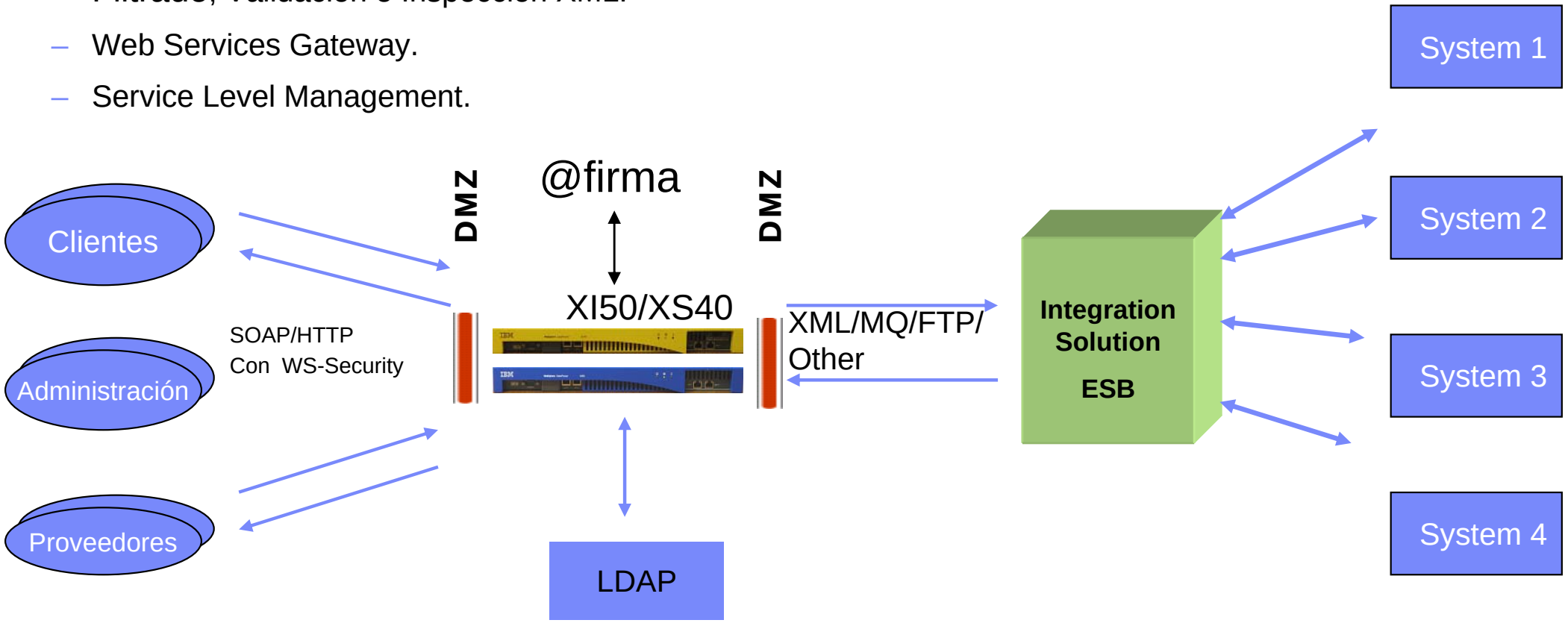
- **Hardware** específico proporciona seguridad física
  - Sellado, caja con protección antiapertura
  - Sin puertos USB, unidades externas, etc.
  - Configuración “cerrada” por defecto
  - Log de auditoría

Certificaciones de terceros
- *Common Criteria EAL4*
- *FIPS 140-2 Level 3 (with optional HSM)*
- *Drummond Group AS2*

- Los DataPowers usan un **firmware** securizado
  - Firmado y cifrado por IBM
  - Se actualiza en minutos
  - Optimizado, sistema operativo DPOS embebido
  - Sin software arbitrario ni Java

Seguridad: Firewall de WS

- Protección contra ataques XML.
- WS-Security, AAA Framework basada en cualquier elemento del mensaje y a velocidad de cable.
- Descarga del procesamiento XML.
- Filtrado, Validación e Inspección XML.
- Web Services Gateway.
- Service Level Management.



Protección de datos con criptografía y contra ataques XML

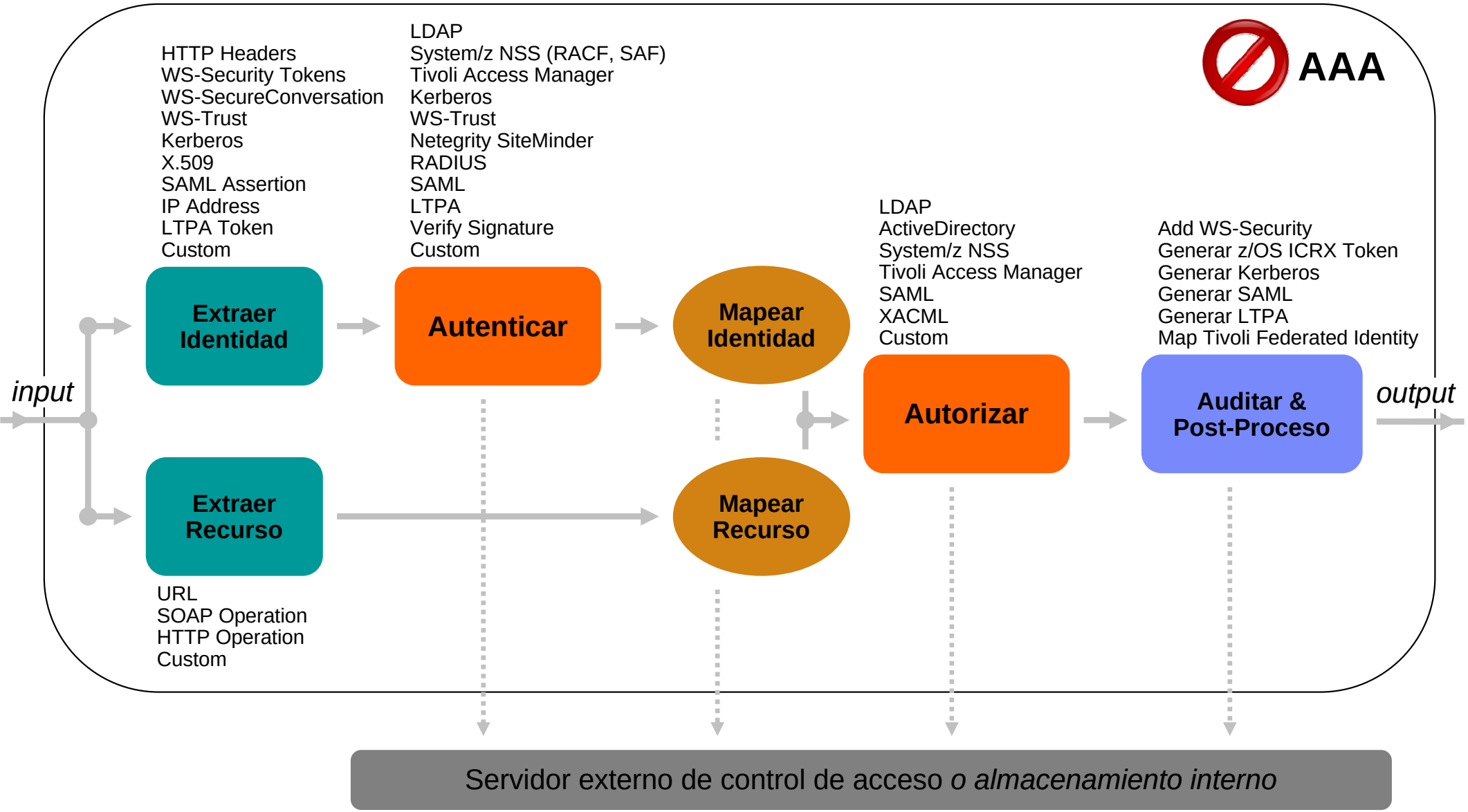
- Uso de DataPower para resolver la **conformidad PCI**
- Firmado, verificación, cifrado y descifrado sencillo de cualquier contenido
- Cifrado XML y firma digital **configurable**
  - Nivel de mensaje
  - Nivel de campo
  - Cabeceras

Algunos ataques XML

- Entity Expansion/Recursion Attacks
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Replay Attack
- Message/Data Tampering
- Message Snooping
- XPath or SQL Injection
- XML Encapsulation
- XML Virus
- …many others

The (XML) threat is out there… de Bill Hines
ibm.com/developerWorks

Flexibilidad de políticas AAA (Autenticación, Autorización, Auditoría)



Asegurando la nube

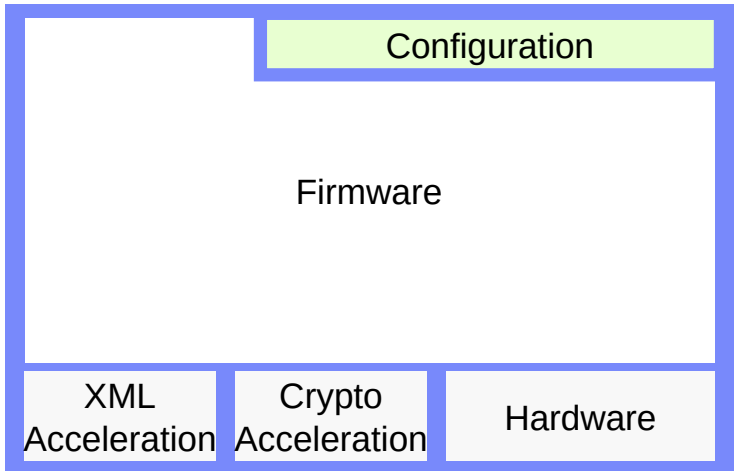
- **No todas las interacciones son Web Services…**
  - *Multiples protocolos*
  - *Formatos de datos opacos*
- **…pero Web Services provee base para la correcta seguridad**
  - *Basada en IP, interacción por programación, ataques hasta Layer 7*
  - *Listas blancas y negras de protección*
  - *PCI DSS es también un buen framework para protecciín*
- **Dispositivos WebSphere DataPower estan construidos para proteger el perímetro de la empresa**
  - *Framework extensible AAA*
  - *Firewall de aplicaciones Web “Built-in”*
  - *Listo para trabajar en la DMZ*

WebSphere DataPower Appliances…

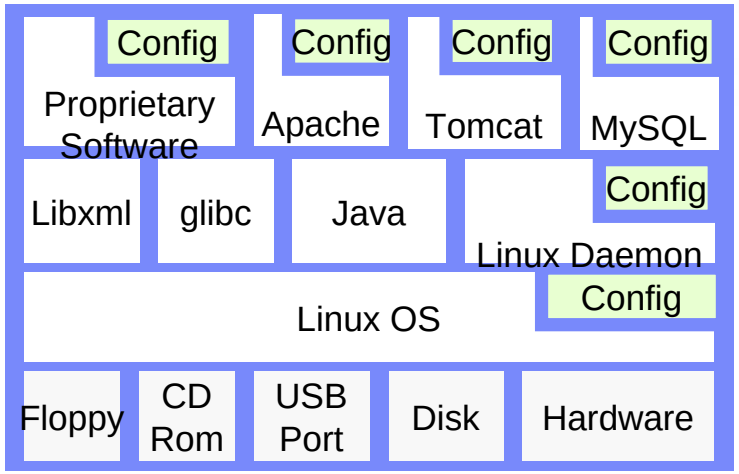
Simplificación de Infraestructura

Ventajas de un Appliance vs. Servidor de Propósito General

DataPower Network Appliance



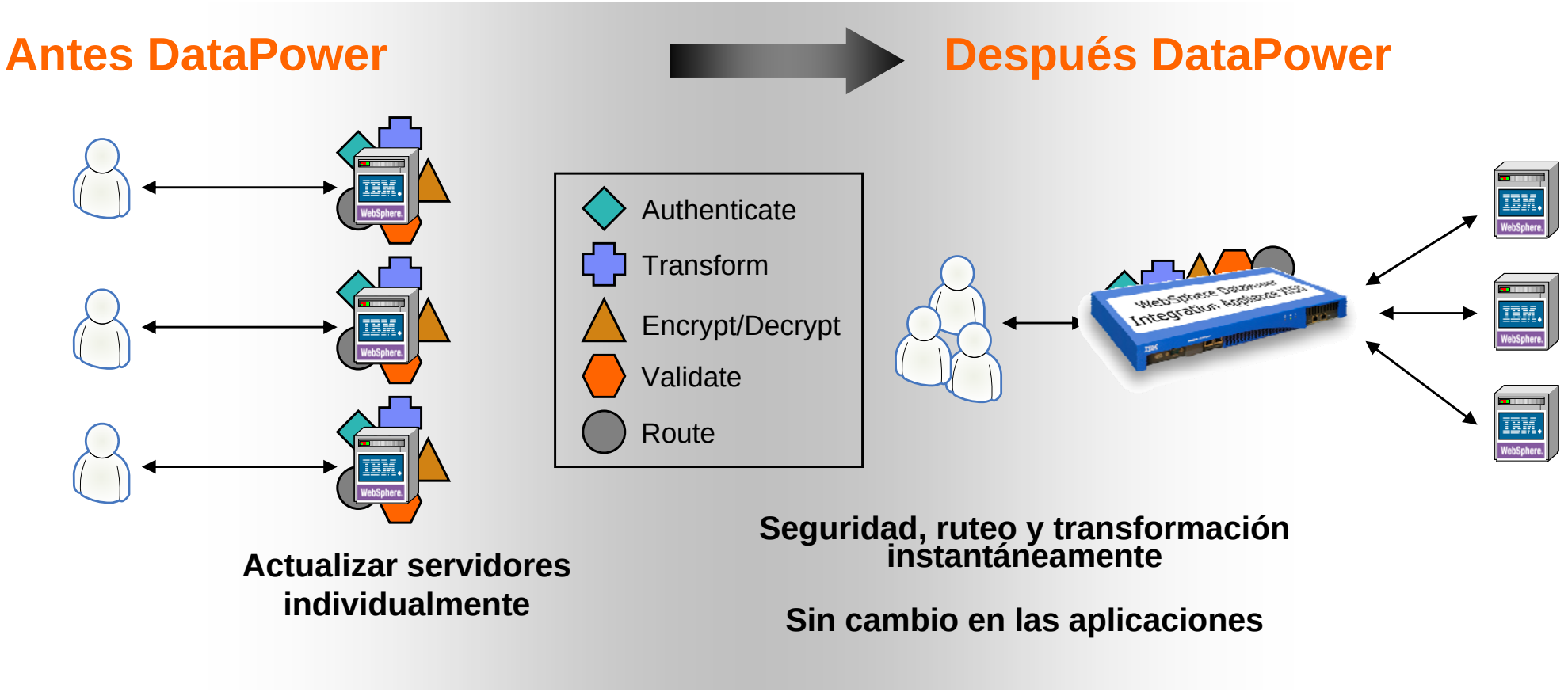
Server Appliance



- Hardware optimizado y precintado para reducir riesgos (sin USB, CDROM, discos)
- No tiene sistema operativo: sólo firmware. Soporte de estándares por firmware
- Vulnerabilidades de seguridad minimizadas (pocos componentes de terceros)
- Almacenamiento en hardware de las claves de encriptación
- Log de auditoria protegidos
- Sin necesidad de codificar, **sólo configurar:** reducción de tiempos de implementación

Usar appliances para simplificar y centralizar funciones críticas

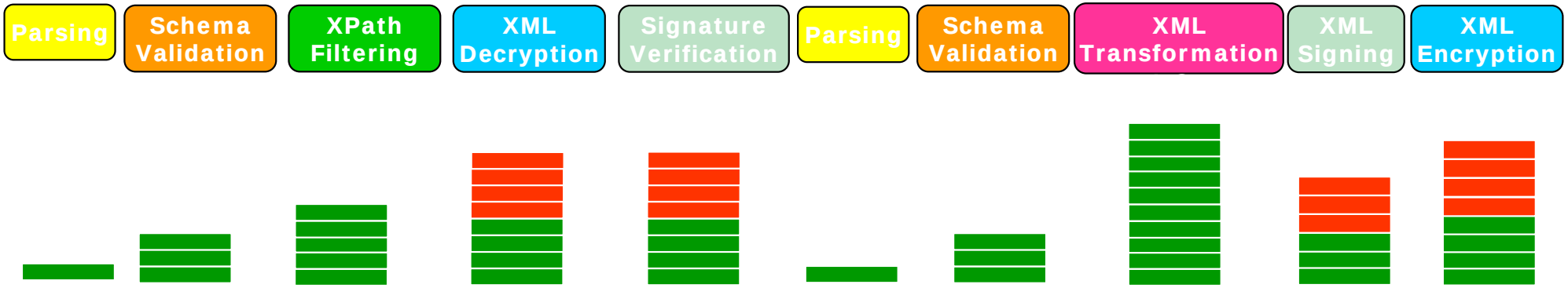
- Ruteo, transformación y seguridad de múltiples aplicaciones sin cambio de código
- Coste y complejidad bajos
- Posibilita nuevos negocios debido al elevado rendimiento



WebSphere DataPower Appliances…

Rendimiento XML y Web Services
Escalabilidad y Rendimiento

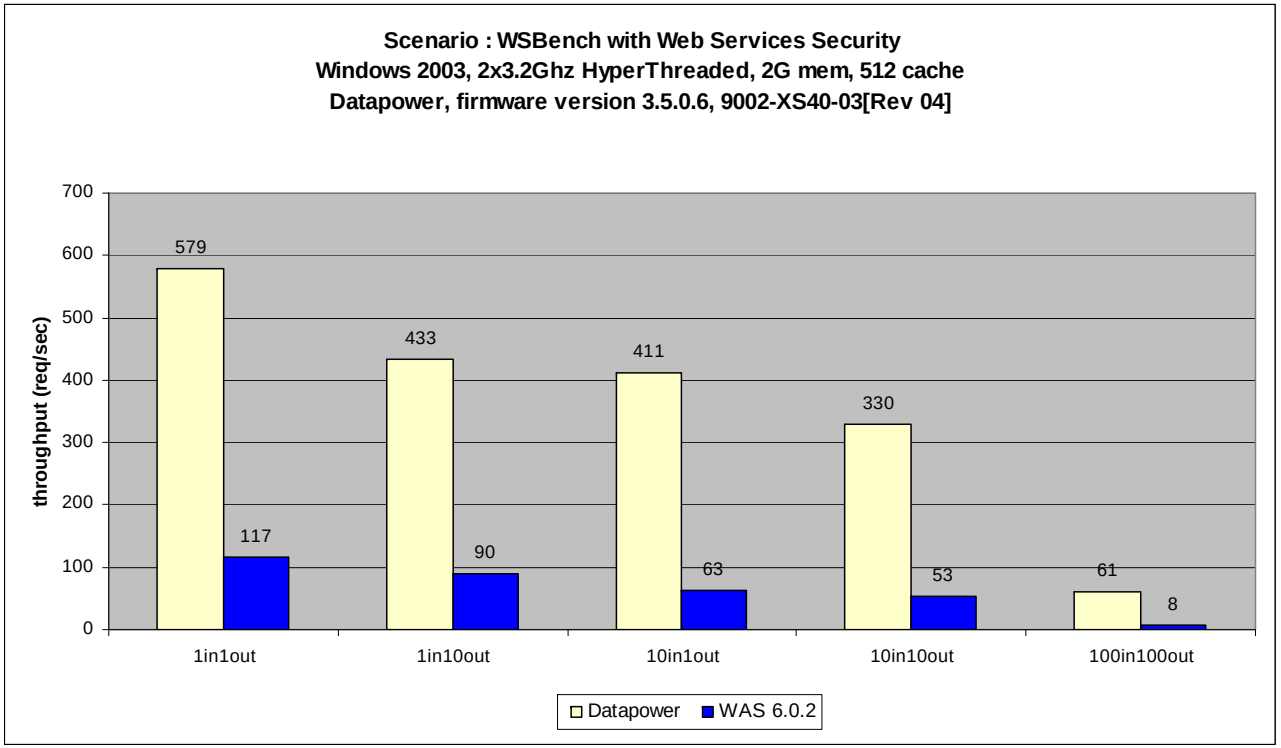
Pasos del procesamiento XML



- Todas las funciones de seguridad requieren un procesamiento intensivo
- Obligación de implementar todos los servicios sin comprometer a la empresa
- Necesidad de poder escalar la solución al aumentar el número de peticiones y el número de servicios

Reducción de HW y SW preciso

Comparativa de rendimiento: DP vs. Software



- Web Services Security
  - Para mantener el mismo nivel de rendimiento al implementar Web Services Security, se puede añadir a la arquitectura:
    - 1 DataPower XS40 or XI50 o
    - *De 5 a 8* servidores xSeries x335 (2x3.2GHz (hyper threaded), 2GB RAM, 512 cache)
  - Estos números dependen del tamaño de la carga de trabajo (workload size).

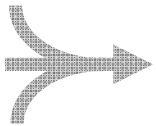
Comparativa en producción con ESB: Cliente de Finanzas

Antes – 24 con planeado crecimiento hasta 48 servidores (HP DL-380, DL-385)

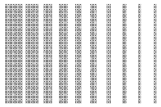
Después – 10 appliances (IBM DataPower XI50)

WebSphere DataPower Appliances…

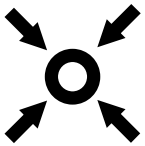
SECURE



SIMPLIFY



ACCELERATE



GOBIERNO

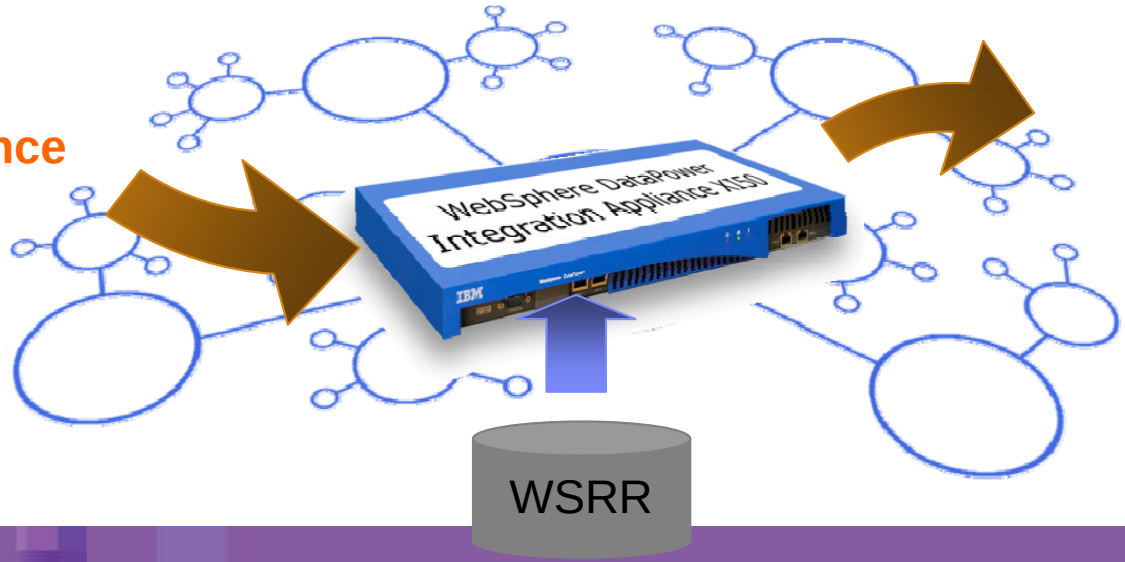
Gestión centralizada de servicios expuestos en DataPower

- **Uso WebSphere Service Registry & Repository (WSRR) para almacenar, publicar, y gobernar los web services**

- **Automaticamente expose los services en DataPower via subscripción WSRR**
  - **Incluye directrices WS-Policy y via WS-PolicyAttachment**
  - **Usar WSDLs por específico número de versión**

- **Dinamicamente saca información de ruteo desde el WSRR**

- **Solición completa para SOA Governance**
  - **WSRR para gestión de políticas de ciclo de vida de web services**



Uso de estándares para aplicar políticas en DataPower

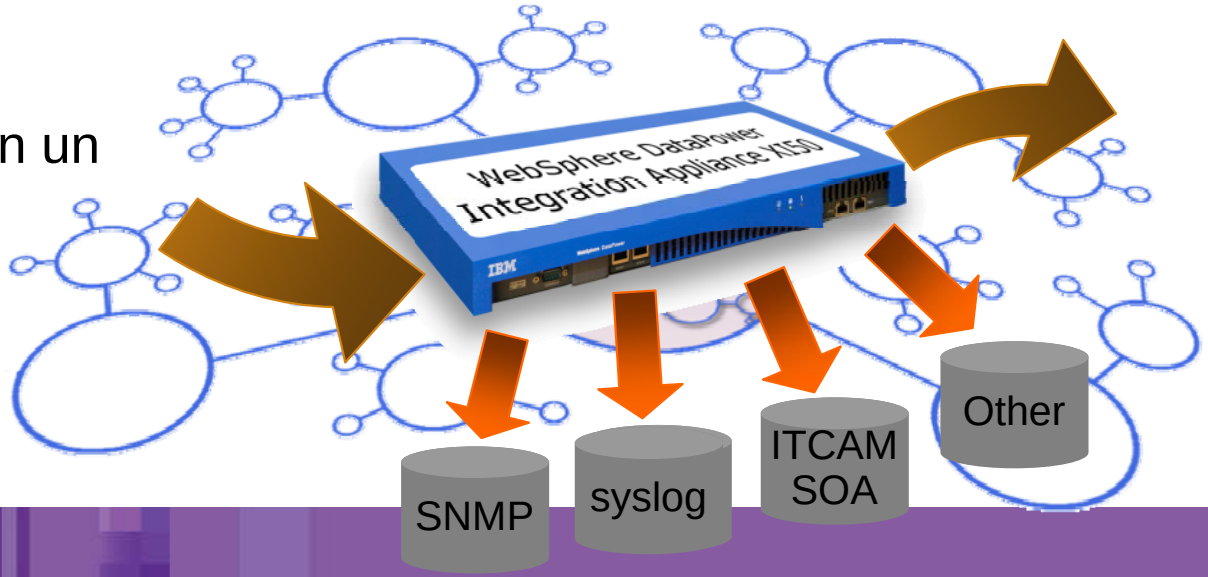
- Uso de **WS-SecurityPolicy** para definir requerimientos de seguridad de los web services
  - DataPower consume y aplica sentencias de WS-SecurityPolicy de forma nativa
    - Identity Tokens
    - Encrypted Elements
    - Signed Elements

- Uso de **XACML** para definir políticas de acceso y autorización a los web services
  - DataPower consume y aplica políticas XACML de forma nativa
    - Autorización basada en recursos

- Uso de **Tivoli Security Policy Manager (TSPM)** para definir las políticas WS-Security y XACML
  - PAP: Policy Authoring Point
  - PDP: Policy Decision Point
  - PEP: Policy Enforcement Point

Use herramientas nuevas o existentes para monitorizar el tráfico

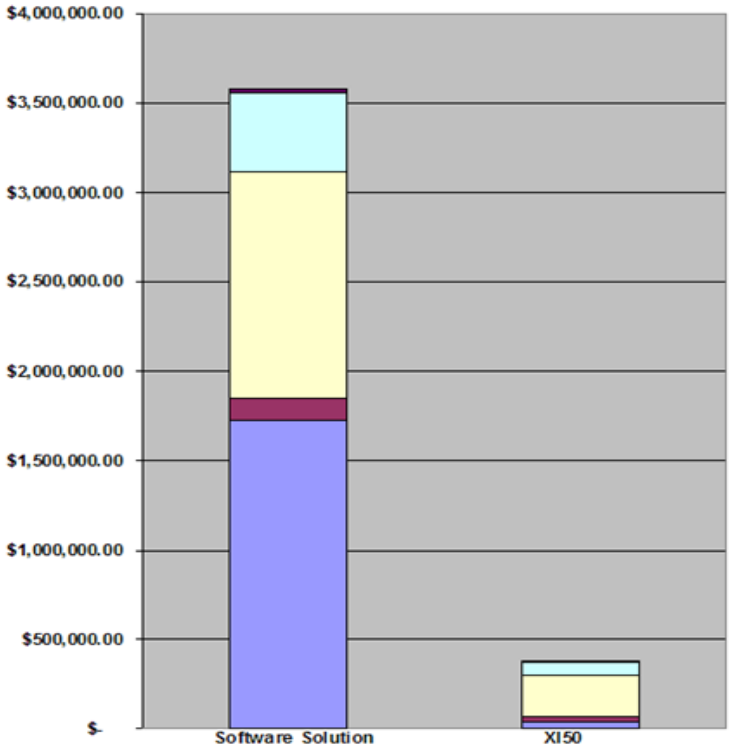
- Fácil integración con su **infraestructura de monitorización existente**
  - Información sobre estado del dispositivo por SNMP
  - Información detallada sobre transactiones via syslog
- Integración con herramientas de monitorización SOA avanzadas para un análisis más completo
  - **IBM Tivoli Composite Application Manager (ITCAM) for SOA**
- Cree soluciones de log y auditoría avanzada para cumplir los requerimientos de sus aplicaciones
  - Log síncrono o asíncrono
- Adáptelo a su monitorización con un flexible motor de suscripción
  - Envío a **múltiples destinos**
  - Envío en **múltiples formatos**



Recuperación de la inversión – Ahorro de costes.

- Reducción del tiempo de implementación y desarrollo
- Reducción de Servidores y Licencias de sw
- Reducción Costes Mantenimiento y Operación.

TCO: DataPower Appliance vs. Software Based Solution
Top 10 *Financial Services Company in North America*



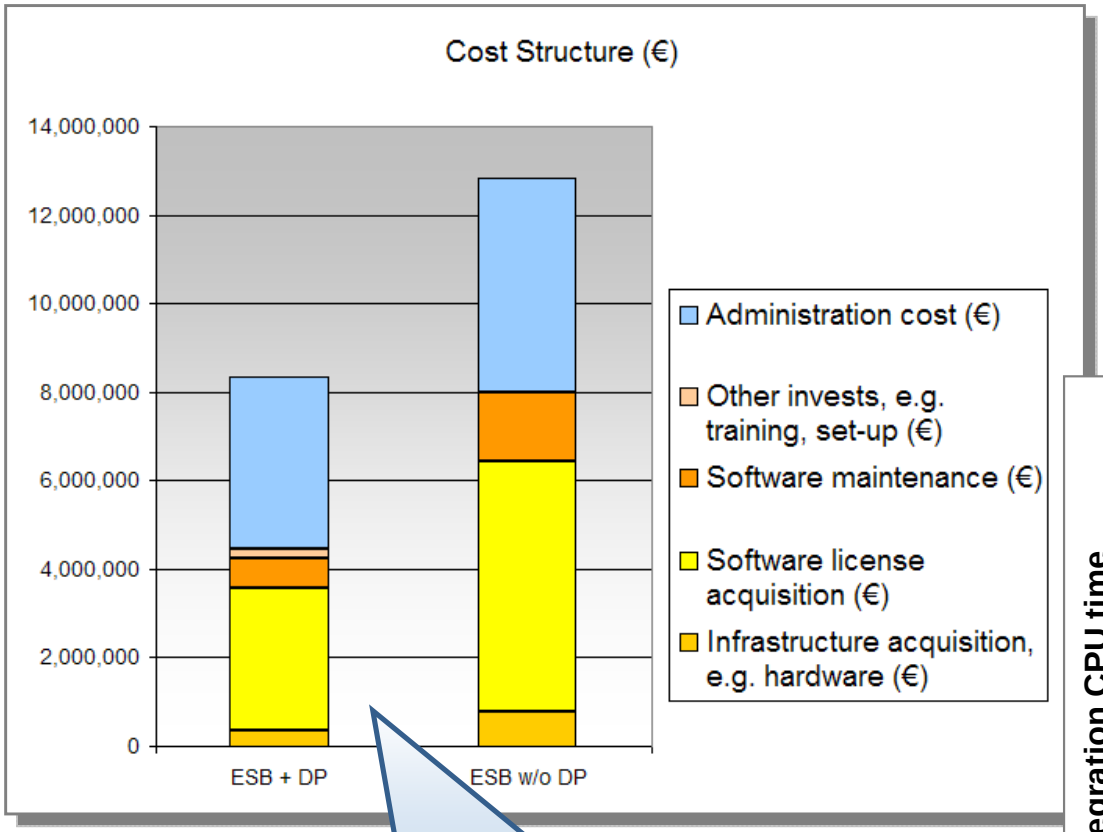
- Study compared expanding an existing software based solution vs. starting fresh with DataPower appliances
- Three primary drivers:
  1) Reduce maintenance burden associated with software based solution.
  2) Reduce overall yearly costs.
  3) Increase throughput and scale solution to meet growth in business.

Cumulative Cost of Ownership over 3 years

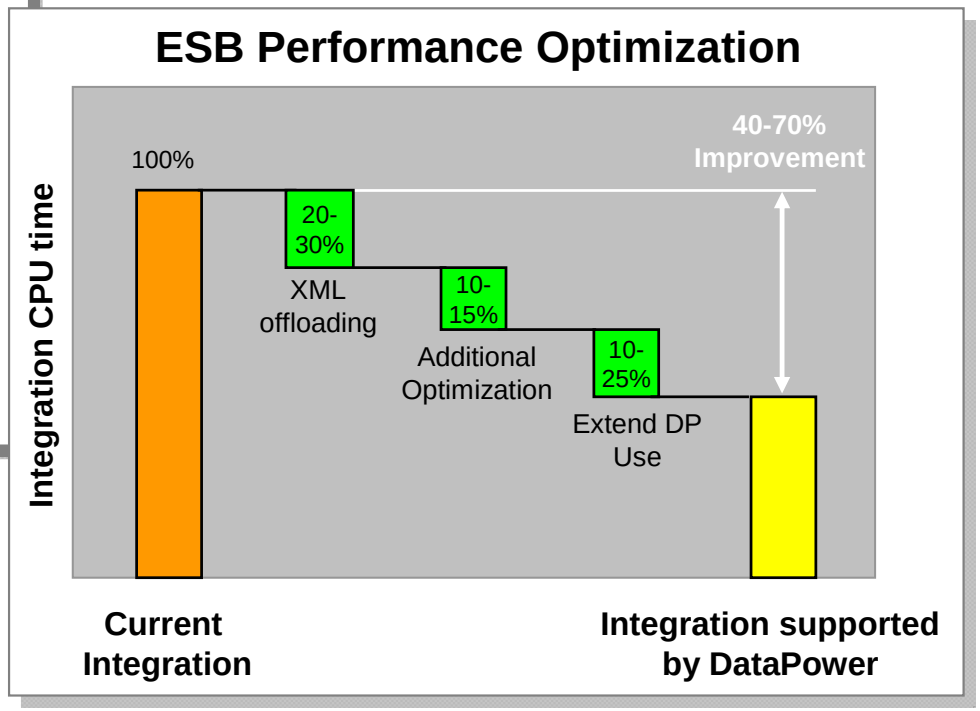
	Software	Appliance
Infrastructure Operating Costs	$1,728,000	$38,400
Application Development/Maintenance	$118,800	$30,096
Capital Costs	$1,268,640	$231,000
Product Maintenance	$435,456	$78,000
Installation & Deployment	$28,800	$2,000
Total	**$3,579,696**	**$379,496**

Note: above figures obtained from cost accounting dept, not IT

Estudio de Valor de Negocio: Cliente de Distribución



La funcionalidad de DataPower ayuda en la optimización de la infraestructura ESB para integración y seguridad



Costes de Hardware, software, mantenimiento y administración son reducidos, el despliegue se acelera.

Proveedor de Servicio de Distribución

SOA provee más agilidad, flexibilida y adaptabilidad

Reto

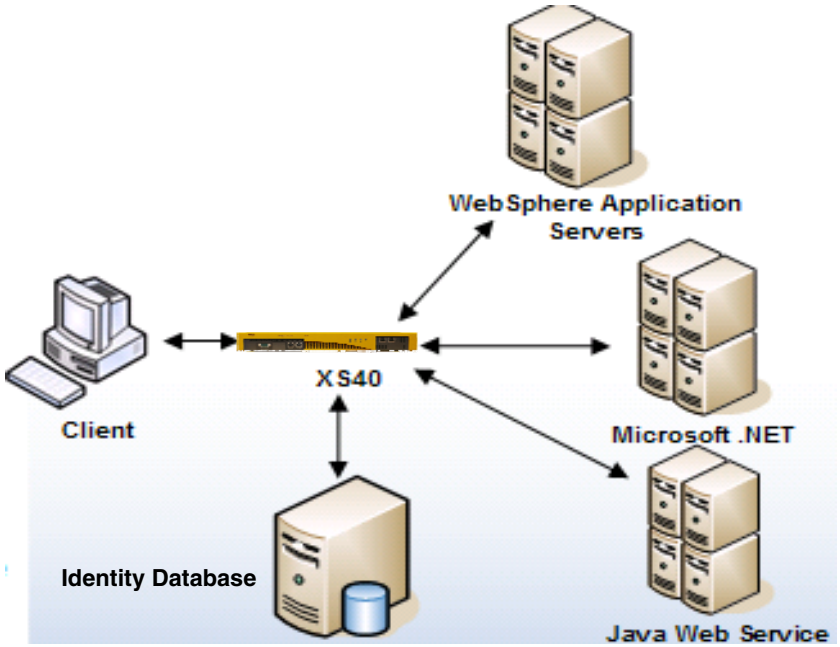
- **Asegurar consistentemente y asegurar el despliegue de servicios on-line a proveedores que pueden ser compartidos, integrados y flexibles**
- **Infraestructura de Web services necesarios para asegurar altos volúmenes seguros diarios e información sensible**

Solución

- **Poner WebSphere DataPower XML Security Gateway XS40 para formar el backbone**
- **Usando ruteo basado en el contenido, robusta política de seguridad y encriptado, XS40 asegura el flujo eficiente de datos confidenciales**
- **Entorno integrado y heterogéneo**

Beneficios

- **Plataforma SOA segura y con estándares y reuso dácil de Web services**
- **Acortar sustancialmente la entrada de nuevos WS en el mercado**

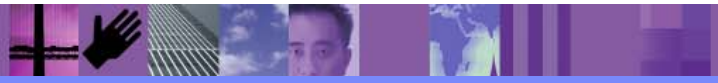


- **WebSphere DataPower XML Security Gateway XS40**
- **WebSphere Application Server**

Registro Único de Seguros de Vida

Ley 20/2005: “Los contratos de seguro, cuyos datos han de figurar en el Registro, serán los relativos a los seguros de vida con cobertura de fallecimiento y a los seguros de accidentes en los que se cubra la contingencia de la muerte del asegurado, ya se trate de pólizas individuales o colectivas.”

- Entrada en vigor: Mayo 2.007
- Ámbito de aplicación: todas las Aseguradoras
- Gestión: Ministerio de Justicia (Registro General de Actos de Última Voluntad de la Dirección General de los Registros y del Notariado)
- Forma de envío de datos: el Ministerio publica un Servicio Web y las aseguradoras tienen que mandar los datos en un fichero XML con un formato predefinido.
- Periodicidad del envío: Semanalmente se tienen que mandar las altas, bajas y modificaciones desde el último envío válido.



Registro Único de Seguros de Vida

- AS/400 genera un fichero de Copybooks de Cobol.
- Mediante FTP, el DataPower adquiere el fichero.
- En el DataPower se transforma de Cobol al formato XML definido por el Ministerio.
- Se valida para comprobar que el fichero cumple con las especificaciones requeridas.
- El fichero se firma y se encripta.
- Se envía mediante HTTP al Web Service del Ministerio.

Referencias:

WebSphere DataPower Appliances…

SECURE

SIMPLIFY

ACCELERATE

GOVERN

www.ibm.com/software/integration/datapower

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Thank You
English

Gràcies

شكرا
Arabic

Merci
French

Obrigado
Brazilian Portuguese

Grazie
Italian

多谢
Simplified Chinese

Danke
German