IBM WebSphere DataPower XML Security Gateway XS40

Umsetzung von Richtlinien und sichere Services, Anwendungen und Daten mithilfe anpassbarer, erweiterbarer und automatisierter Funktionen für Servicetransparenz und Steuerung

Highlights

- Besseres Systemmanagement durch intelligente Funktionen für den Lastausgleich und dynamische Kontrolle von Service-Leveln
- Einhaltung gesetzlicher Bestimmungen durch zuverlässige Funktionen für Datenschutz und Prüfungen
- Eingrenzung von Risiken durch Sicherheitsfunktionen auf DMZ-Niveau für geschäftskritische Anwendungen, Services und Daten
- Stärkeres Vertrauen in vorhandene Services durch äußerst sichere Hardware für die Steuerung bei Laufzeit und die Umsetzung von Richtlinien
- Steuerung des Zugriffs auf Anwendungen, Services und Daten basierend auf anpassbaren Rollen und Berechtigungen

Das heutige dynamische Geschäftsumfeld bedeutet für Unternehmen, noch intelligenter arbeiten zu müssen, um wettbewerbsfähig zu bleiben und auf Veränderungen bei den Kunden und deren Anforderungen schnell reagieren zu können. Um diese Ziele zu erreichen, müssen Unternehmen kostenintensive Redundanzen vermeiden, die erneute Verwendung vorhandener Services fördern und sicherstellen, dass diese Services sicher, zuverlässig und qualitativ hochwertig sind. Die IBM WebSphere DataPower SOA Appliances bieten anpassbare, erweiterbare und automatisierte Funktionen für transparente Services und Governancelösungen, mit denen Unternehmen in der Lage sind, Services, Anwendungen und Daten besser zu verwalten, verlässlicher zu gestalten und zu schützen. Durch die Konsolidierung ihrer SOA-spezifischen (Service-Oriented Architecture) Sicherheits- und Governancefunktionen auf einem zentralen, speziell hierfür vorgesehenen System können Unternehmen neue Services schnell auf dem Markt einführen, Risiken im Zusammenhang mit Geschäftsanwendungen verringern, die Produktivität der Mitarbeiter steigern, Wartungskosten reduzieren und gleichzeitig die Rendite für ihre Ressourcen steigern.

Warum wird ein System für Servicetransparenz, Governance und Sicherheit benötigt?

Aufgrund der immer größeren Zahl an SOA-Anwendungen, die über externe Entitäten angebotene Services verwenden, ist es von entscheidender Bedeutung, dass Unternehmen sichere SOA-Services zur Verfügung stellen, die erweiterbar und kosteneffizient sind, ohne Leistungseinbußen hinnehmen zu müssen. Der mehrfach ausgezeichnete IBM WebSphere DataPower XML Security Gateway XS40 (siehe Abbildung 1) ist eine vollständige, speziell konzipierte Hardwareplattform zur Bereitstellung einfach zu verwaltender SOA-Lösungen, die größere Sicherheit und mehr Erweiterungsmöglichkeiten bieten.

Bei diesem Produkt handelt es sich um eine äußerst sichere SOA-Appliance mit einer hochentwickelten Softwareebene zur Verringerung von XML-Risiken und zur Umsetzung von Sicherheitsrichtlinien für XML-Nachrichten und Web-Services-Transaktionen. Sie wird allen Anforderungen für eine schnelle und zuverlässige XML-Verarbeitung auf einem benutzerfreundlichen System gerecht, auf dem nachgelagerte, unterschiedliche Nachrichtenformate in XML umgewandelt und Sicherheits- und Servicerichtlinien auf Nachrichtenebene angewendet werden. WebSphere DataPower XML Security Gateway XS40 trägt zur Optimierung Ihrer SOA-Implementierung in einer Umgebung mit hohem Sicherheitsniveau bei und erfordert nur ein Mindestmaß an Konfiguration, Anpassung und Verwaltung. Über diese Einheit werden SOA-Übertragungen durch die Implementierung von Funktionen zum Schutz vor XML-Risiken und für die Sicherheit von Web-Services sowie durch die Integration in Sicherheitssoftware und Software für das Identitätsmanagement (z. B. IBM Tivoli Software) abgeschirmt.

Abbildung 1 – WebSphere DataPower XML Security Gateway XS40.

WebSphere DataPower XML Security Gateway XS40 ist eine 1U-Netzwerkeinheit für die Rackmontage (1,75 Zoll), die speziell für Rackgehäuse nach Branchenstandard konzipiert wurde. Der Anschluss an das Netzwerk erfolgt über Ethernet. Die Einheit ist nahezu manipulationssicher und kann nicht herausgenommen und in anderen Servern verwendet werden. Der geschäftliche Nutzen für Ihr Unternehmen erhöht sich somit, ohne dass Sie Änderungen an der Netzwerk- oder Anwendungssoftware vornehmen müssen. Somit sind für die Installation oder die Verwaltung der Einheit keine proprietären Schemas, Codierungen oder Anwendungsprogrammierschnittstellen (APIs) erforderlich. Aufgrund seiner Vielseitigkeit und einfachen Inbetriebnahme ist der Gerätetyp des WebSphere DataPower XML Security Gateway XS40 eine zentrale Komponente einer ausfallsicheren Infrastruktur. Er richtet sich an viele Zielgruppen, die an einer erfolgreichen SOA-Implementierung interessiert sind, beispielsweise an Unternehmensarchitekten, im Bereich der Netzverwaltung, des Sicherheitsmanagements oder des Identitätsmanagements tätige Personen sowie Web-Service-Entwickler.

Besseres Systemmanagement durch intelligente Funktionen für den Lastausgleich

In den verteilten Anwendungsumgebungen von heute, die in immer stärkerem Maß mit Netzwerken zwischen Unternehmen und deren Kunden, Geschäftspartnern und Lieferanten verknüpft sind, hängt der geschäftliche Erfolg von stets aktuellen Rückmeldungen zu den Ressourcen und deren Verwaltung ab. Eingehende Netzwerkübertragungen müssen den am besten geeigneten und verfügbaren Ressourcen zugeordnet werden. Die Option zur Anwendungsoptimierung (Application Optimization, AO) der IBM WebSphere DataPower Appliance wurde speziell im Hinblick auf die Bereitstellung dynamischer und intelligenter Funktionen für den Lastausgleich in den anspruchsvollsten Systemumgebungen im heutigen Geschäftsumfeld konzipiert. Dadurch können die Effizienz gesteigert und kritische Ausfälle auf ein Minimum reduziert werden. Durch die gleichmäßige Verteilung von Workloads über mehrere Geräte hinweg und auf speziell ausgewählten Servern, sorgt die Option zur Anwendungsoptimierung für längere Betriebszeiten, eine für den Benutzer transparente, größere Reaktionsfähigkeit und eine bessere Ressourcenauslastung (siehe Abbildung 2).

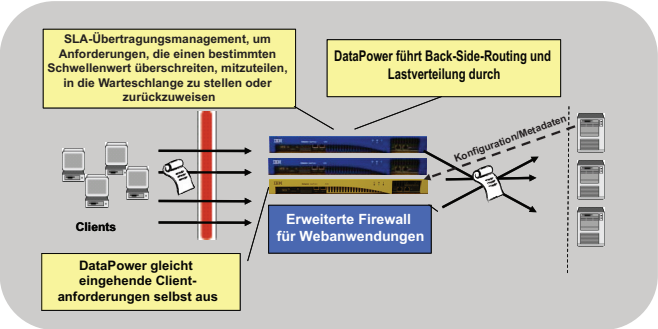

Abbildung 2 – Option zur Anwendungsoptimierung umfasst Funktionen für den Selbstausgleich auf unterschiedlichen Systemen und intelligente Funktionen zur Lastverteilung auf nachgelagerte Systemumgebungen.

XS40 unterstützt Konfigurationen mit Web Services Distributed Management (WSDM), Universal Description, Discovery, and Integration (UDDI), Web Services Description Language (WSDL), Dynamic Discovery und Service Level Management (SLM). Dadurch bietet das Gerät ein natives Framework für das Web-Service-Management, um verteilte Web-Service-Endpunkte und Proxys in heterogenen SOA-Umgebungen effizient verwalten zu können. XS40 bietet darüber hinaus SLM-Alerts, Protokollierungsfunktionen und „Pull-and-Enforce"-Richtlinien, die eine umfassende Integration mit Managementsystemen und einheitlichen Dashboards anderer Anbieter ermöglichen. Hierzu gehören auch die Unterstützung und Umsetzung von Governance-Frameworks und -Richtlinien. In Kombination mit den Leistungsmerkmalen zur Anwendungsoptimierung bieten die Features des XS40 für Nachrichtenrouting, Service Level Management (SLM), Inhaltsprüfung und Sicherheit neue Möglichkeiten, um komplexe Strukturen in der IT-Umgebung zu vereinfachen und dabei Serviceleistungen zu verbessern.

Einhaltung gesetzlicher Bestimmungen durch zuverlässige Funktionen für Datenschutz und Prüfungen

Über das leistungsfähige Authentication, Authorization, and Auditing (AAA) Framework des XS40 kann die Einheit zahlreiche unterschiedliche Methoden für das Extrahieren von Benutzerkennwörtern, Sicherheitstoken und anderen Identitätsinformationen von eingehenden Anforderungen verwenden. Die Authentifizierungs- und Autorisierungsschritte erfolgen ebenfalls vollständig modular und können entweder auf integrierten oder nicht integrierten Repositorys basieren. Die Verarbeitung von Audits und Abrechnungen ist in vollem Umfang erweiterbar. Dank dieses erstklassigen Frameworks lässt sich der XS40 in eine Vielzahl von Lösungen für das Identitätsmanagement integrieren. Der Kunde hat so die Möglichkeit, proprietäre, unternehmensinterne SSO-Systeme (Single Sign-On) in die Sicherheitsarchitektur für Web-Services zu integrieren. XS40 nutzt wahlweise Informationen gemeinsam auf der Basis von Verschlüsselung und Entschlüsselung sowie Unterzeichnung und Prüfung vollständiger Nachrichten oder einzelner XML-Felder. Diese differenzierten und bedingten Sicherheitsrichtlinien können auf nahezu allen Variablen basieren, z. B. Inhalte, IP-Adresse, Hostname und andere benutzerdefinierte Filter. Sie gehören zu den vielen zuverlässigen Merkmalen des XS40 für Datenschutz, Umsetzung von Richtlinien und Prüfung, durch die Unternehmen auf der ganzen Welt in der Lage sind, branchenspezifische und/oder gesetzliche Bestimmungen wie Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS) und den Health Insurance Portability and Accountability Act (HIPAA) einzuhalten.

Eingrenzung von Risiken durch Sicherheitsfunktionen auf DMZ-Niveau für geschäftskritische Anwendungen

Der WebSphere DataPower XML Security Gateway XS40 ist eine Hardwareeinheit mit hochentwickelter Zugriffskontrolle für XML und Web-Services, ohne dass hierfür komplexe Konfigurationen oder Codeanpassungen erforderlich sind. Er bietet die höheren Stufen von Sicherheitszertifizierungen, die beispielsweise für Finanzdienstleister und Regierungsbehörden erforderlich sind. Zu diesen Zertifizierungen gehören Public Key Infrastructure (PKI), Federal Information Processing Standard (FIPS) 140-2, Hardware Security Module (HSM), General Services Administration (GSA), eAuthentication, Homeland Security Presidential Directive (HSPD)-12 und Common Criteria Evaluation Assurance Level (EAL) 4+. Die Kombination aus hoher Hardwarebeschleunigungsleistung und vereinfachter Inbetriebnahme und Verwaltung ermöglicht die Vereinfachung komplexer Strukturen und die Reduzierung von Kosten für den Schutz geschäftskritischer Services, Anwendungen und Daten. Da weniger SOA-spezifische Programmierkenntnisse erforderlich sind, können die Vorteile von SOA schneller und ohne Sicherheitsrisiken auf dem Markt eingeführt werden.

Stärkeres Vertrauen in vorhandene Services durch die Umsetzung von Richtlinien bei Laufzeit

Aufgrund der bisher unübertroffenen Leistungsmerkmale des XS40 können Unternehmen Sicherheits- und Governance-funktionen auf einer einzigen Drop-in-Einheit zentralisieren und dadurch die laufenden Wartungskosten reduzieren (siehe Abbildung 3). Einfache Proxyfunktionen für Firewall und Web-Services können über eine Web-GUI konfiguriert und innerhalb weniger Minuten ausgeführt werden. Dank der Leistungsfähigkeit von XSLT (Extensible Stylesheet Language Transformation) lassen sich mit dieser Einheit darüber hinaus zukunftsorientierte Sicherheits- und Routingregeln erstellen. WebSphere DataPower XML Security Gateway XS40 ist ein ausgezeichnetes Hilfsmittel zur Umsetzung und Ausführung von Richtlinien im Hinblick auf den Schutz von Anwendungen der nächsten Generation. Unternehmen können auf dieser Grundlage den Zugriff auf Anwendungen, Services und Daten mithilfe anpassbarer Rollen und Berechtigungen steuern. XS40 lässt sich in erstklassige Policy Manager und Service-Registrys integrieren und unterstützt Standards wie WS-Security, WS-SecurityPolicy, WS-ReliableMessaging und WS-Policy. Die Einheit kann lokal oder remote verwaltet werden und unterstützt SNMP (Simple Network Management Protocol), scriptbasierte Konfigurationen und Remoteprotokollierungen für die nahtlose Integration in führende Management-Software.

Abbildung 3 – WebSphere DataPower XML Security Gateway XS40 zentralisiert und vereinfacht das Management von Web-Services und SOA-Governance.

Drop-in-, auf Standards basierende Sicherheits- und Governancefunktionen für Web 2.0-Anwendungen

Bei modernen Webanwendungen werden neben statischen Seiten und Formularen immer mehr Interaktionen unterstützt, die mit nativen Desktopprogrammen wie E-Mail-Clients, Straßenkartensoftware und CRM-Systemen konkurrieren. Kunden und Partner aus allen Branchen fordern dasselbe hohe Maß an Interaktion und Datenzugriff für ihre Informations-bestände. Leider befinden sich kritische Geschäftsdaten sehr häufig in traditionellen Anwendungen, die für diese Art von Nutzung nicht ausgelegt sind, und sind somit praktisch gesperrt. Durch die native Unterstützung von JavaScript™ Object Notation (JSON) und REpresentational State Transfer (REST) lassen sich mithilfe des IBM WebSphere DataPower XML Security Gateway XS40 Web 2.0-Anwendungen mit eher formalen Unternehmensstandards wie WS-* verknüpfen. Dadurch können Unternehmen verstärkt in neuen Bereichen wie Social Networking, Cloud Computing und Software as a Service (SaaS) tätig werden.

Middlewaregeräte vom Middlewarespezialisten

Die IBM WebSphere DataPower SOA-Geräte bestechen durch ihre Kombination aus langjähriger Erfahrung eines Branchenführers und gewachsenem Know-how für SOA-Middleware einhergehend mit den verbraucherfreundlichen, dedizierten Geräten, die vereinfachte Integration, überlegene Leistung und erhöhte Sicherheit für SOA-Implementierungen in sich vereinen. Diese hochspezialisierten Geräte, die sorgfältig konzipiert wurden, um alle Phasen des SOA-Lebenszyklus und der Implementierung zu verbessern, stellen eine Vielzahl von wichtigen SOA-Funktionen in einem spezialisierten Gerät zur Verfügung, das sich durch einfache Bedienung, Implementierung, Verwaltung und Servicebereitstellung auszeichnet.

IBM WebSphere DataPower XML Security Gateway XS40 auf einen Blick

XML:

- XPath
- XSLT
- XML Schema

Optimierung:

- Komprimierung
- Mehrstufige Datenflussverarbeitung und Mediation
- Wirespeed-XML- und XPath-Verarbeitung; XSLT
- Servicequalität (QoS) und Servicepriorisierung

Enterprise Messaging und Integration:

- HTTP, Secure HTTP (HTTPS)
- Routing (XPath, WS-Routing und XML)
- Nachrichtenprotokollierung

Datensicherheit:

- Datenprüfung (XML Schema, Web Services Description Language [WSDL] und SOAP-Filterung)
- XML-Verschlüsselung und digitale Signatur
- WS-Security
- WS-SecureConversation
- XML-Sicherheit auf Feld- und Nachrichtenebene
- Integration von Internet Content Adaptation Protocol (ICAP) (Antivirus)

Umsetzung der Sicherheitsrichtlinien für XML- und Web-Services:

- Authentifizierung von Web-Service-Nachrichten mithilfe von WS-Security und Security Assertion Markup Language (SAML), Version 1.0, 1.1 und 2.0
- XACML (Extensible Access Control Markup Language)
- Autorisierung für XML-Nachrichten
- Unterstützung für Kerberos, RADIUS, Lightweight Directory Access Protocol (LDAP), Microsoft® Active Directory und SAML-Abfragen
- Fähigkeit zur Verarbeitung von Liberty Alliance ID-FF-, WS-Trust- und WS-Federation-Nachrichten bei Konfiguration mit Tivoli Federated Identity Manager oder einem ähnlichen Policy Manager
- Federal Information Processing Standard (FIPS) 140-2 Hardware Security Module (HSM) als Systemerweiterung
- Einbindung von Sicherheitstokens bei Konfiguration mit Tivoli Federated Identity Manager oder einem ähnlichen Policy Manager

IBM WebSphere DataPower XML Security Gateway XS40 auf einen Blick

Web-Services:

- SOAP 1.1 und 1.2
- WSDL (Web Services Description Language)
- WS-SecurityPolicy
- WS-Policy Framework
- Integration von Registrierungssoftware (UDDI V2/V3, UDDI V3 Subscription, IBM WebSphere Service Registry and Repository)
- WS-Trust
- WS-ReliableMessaging
- WS-I Basic Profile
- WS-I Basic Security Profile
- WSDM
- WS-Management
- Unterstützung für JavaScript Object Notation (JSON) und REpresentational State Transfer-Anwendungen (REST)

System- und Servicesicherheit:

- Servicevirtualisierung
- XML- und SOAP-Firewall
- XDoS-Schutz

Management:

- Web-GUI
- Befehlszeilenschnittstelle (Command Line Interface, CLI)
- Simple Network Management Protocol (SNMP)
- SOAP-Managementschnittstelle
- IDE-Einbindung (Integrated Development Environment) unter Eclipse und Altova XML Spy
- Service-Level-Management (zum Konfigurieren, Umsetzen und Überwachen der Servicequalität)
- Protokollierung, Drilldown und Alertausgabe (on-box, off-box oder zentralisiert)
- Einheitenpartitionierung und rollenabhängiges Management

Transport Layer Security (TLS):

- SSL und HTTPS, hardwarebeschleunigt

Zuverlässigkeit:

- Virtual Router Redundancy Protocol (VRRP)
- Ein einziges Firmware-Image

Zusatzfunktionen:

- Anwendungsoptimierung
- Integration von Tivoli Access Manager
- Gespiegelte RAID-1-Plattenlaufwerke

Weitere Informationen

Wenn Sie mehr über IBM WebSphere DataPower SOA-Geräte erfahren möchten, wenden Sie sich an den zuständigen IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/software/integration/datapower

Die Global WebSphere Community finden Sie unter der folgenden Adresse:

www.websphere.org

IBM Deutschland GmbH
IBM Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

WSD14015-DEDE-01