Simplifying Integration with IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise

Integration challenges

DataPower XI50z value proposition

Architecture patterns and case study

Alex Louwe Kooijmans
Bill Hines
Karan Punwani
Barry Silliman
Pradeep Thomas
Nigel Williams

Redpaper

ibm.com/redbooks

International Technical Support Organization

Simplifying Integration with IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise

September 2011

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (September 2011)

This edition applies to IBM zEnterprise System.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
BladeCenter®
CICS®
DataPower®
DB2 Connect™
DB2®
developerWorks®
Distributed Relational Database Architecture™
DRDA®
GDPS®
IBM®
IMS™
OMEGAMON®
Parallel Sysplex®
POWER7™
PowerVM™
PR/SM™
RACF®
Redbooks®
Redpaper™
Redpapers™
Redbooks (logo) ®
Smarter Banking™
System z10®
System z®
Tivoli®
WebSphere®
z/OS®
z/VM®
z10™
zSeries®

The following terms are trademarks of other companies:

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redpaper™ publication illustrates how the IBM WebSphere® DataPower® Integration Appliance XI50 for zEnterprise provides a secure, fast, cost-effective, easy-to-manage, all-in-one enterprise application integration solution. On top of all the benefits that the DataPower XI50 and XI52 already provide, incorporating the DataPower XI50z in zEnterprise also provides a number of additional benefits:

- Exploitation of the high-speed intraensemble data network (IEDN) connecting the zEnterprise Blade Extension (zBX) with the zEnterprise central processor complex (CPC), either a zEnterprise 196 (z196) or zEnterprise 114 (z114)
- Secure incorporation of the DataPower XI50z appliance into a virtual local area network (VLAN) on the zBX
- Unified management of the DataPower XI50z, along with other blades and optimizers using a common management tool
- A centralized computing model, resulting in more efficient use of floor space, lower energy costs, and a lower total cost of ownership (TCO)

The DataPower XI50z provides a variety of powerful integration scenarios specifically for older mainframe applications, making it a natural choice to include the appliance in your centralized zEnterprise server.

This publication is intended for potential and actual users of the DataPower XI50z.

The team who wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Poughkeepsie Center.

Alex Louwe Kooijmans is a project leader with ITSO in Poughkeepsie, NY, and specializes in service-oriented architecture (SOA) technology and solutions using IBM System z®. He also specializes in application modernization and transformation on IBM z/OS®, both from an architectural and tooling perspective. Previously, he worked as a Client IT Architect in the financial services sector with IBM in the Netherlands, advising financial services companies about IT issues, such as software, hardware and on-demand strategies. Alex has also worked at the Technical Marketing Competence Center for IBM zSeries® and Linux in Boeblingen, Germany, providing support to customers starting up with Java and WebSphere on System z.

From 1997 to 2000, Alex completed a previous assignment with the ITSO, managing various IBM Redbooks® projects and delivering workshops around the world in the area of WebSphere, Java, and e-business technology using System z. Prior to 1997, Alex held a variety of positions in application design and development, product support, and project management, mostly in relation to the IBM mainframe. Alex has 23 years of IT experience and has been the lead author of many IBM Redbooks and Redpapers™.

Bill Hines is an Executive IT Specialist and World-Wide Tech Sales Leader for DataPower, working out of Hershey, PA. He has many years of DataPower experience in both customer engagements and developing and delivering internal DataPower training to the IBM consulting, engineering, support, QA, and technical sales teams. He also has WebSphere Application Server experience dating back to 1998. He is the lead author of *IBM WebSphere DataPower SOA Appliance Handbook*, co-author of *IBM WebSphere: Deployment and Advanced Configuration,* and author of many articles published in *WebSphere Technical Journal* and *developerWorks*.

Karan Punwani is an Executive Consultant with IBM Software Group Services, based In the USA. He has more than 20 years of experience in technologies related to IBM middleware and e-business. Currently, he is focused on leading complex cross-brand SOA projects for clients in the Finance and Healthcare industries specializing in SOA strategy, SOA and Cloud appliances, Virtualization technologies, and SOA security. Karan holds a Master of Science degree in Computer Science from the Worcester Polytechnic Institute in Massachusetts.

Barry Silliman is a Senior IT Specialist and is a DataPower XI50z subject matter expert on the zEnterprise Focus Team in the IBM Advanced Technical Skills organization in Gaithersburg, Maryland, USA. He has 27 years of experience in the IT industry, 25 with IBM, and has held a broad range of systems administration and application development roles over the years, ranging from IBM CICS® systems programming to Assembly Language programming on System 390 to C development on OS/2.

Pradeep Thomas is a Senior IT Specialist with the IBM Software Group, based in the USA. He has more than 20 years of experience in enterprise application integration technologies, of which 15 years have been dedicated to IBM middleware and e-business solutions. He has expertise in implementing and delivering Enterprise Application Integration and SOA solutions using WebSphere DataPower and WebSphere Message Broker. Over the years, he has had extensive experience in delivering SOA-based integration solutions to clients in the Finance and Healthcare industries.

Nigel Williams is a Certified IT Specialist working in the IBM Design Centre, Montpellier, France. He specializes in enterprise application integration, security and SOA. He is the author of many papers and IBM Redbook publications, and he speaks frequently on CICS and WebSphere topics.

Thanks to the following people for their contributions to this project:

Suzanne Battenfeld
Program Director, System z Marketing

Peter Brabec
System z Software WebSphere Brand Leader and DataPower Ambassador for Eastern Europe, Middle East, and Africa

Bill Carey
Systems and Technology Group, z/OS Technical Strategy/Design for XML

Martin Dvorsky
IBM Technical Director, Worldwide System z Workload Team

Penny Hill
System z Software Marketing Manager

Alan Kittel
IBM Competitive Project Office

Olivier Manet
Systems and Technology Group, IBM Design Center, Montpellier, France

Jeffrey Miller
IBM Competitive Project Office

David Rhoderick
IBM Competitive Project Office

Alain Roessle
Systems and Technology Group, IBM Design Center, Montpellier, France

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Obtain more about the residency program, browse the residency index, and apply online at the following address:

`http://ibm.com/redbooks/residencies.html`

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online review Redbooks form found at the following address:

  `http://www.redbooks.ibm.com/`

- Send your comments in an email to:

  `http://www.redbooks.ibm.com/`

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://ibm.com/support

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

The agility and competitiveness of an enterprise greatly depends on the ability to integrate IT applications. Correlation between separate business events in separate business units, maybe even in separate geographical regions, is key to survive. Various studies, including the IBM CIO Study, have indicated that integration and themes depending on integration, such as business process management, have a high focus. Therefore, integration has to become smarter and faster and stay in control of the risk, complexity, and cost that go with it.

Designing and implementing an effective integration architecture and infrastructure is perhaps one of the biggest challenges in IT because it affects many separate IT departments, cultures and technologies. Following proper design principles and architectural thinking are nowhere as critical as in the integration area. To make sure you do not “forget” anything and to ensure that your integration architecture is “future-proof,” it is strongly recommended to start using service-oriented architecture (SOA) as a roadmap for integration if you have not already done so. One of the key aspects of SOA is a loosely-coupled integration layer called the “Enterprise Service Bus.” Most companies have adopted these concepts and understand their value in integrating their business applications.

Increasingly, these business applications span heterogeneous platforms, appliances, and devices, and this wide range of resources creates real issues for IT shops trying to create a flexible integration infrastructure. The ability to manage resources for these heterogeneous applications as one logical entity is essential. The IBM zEnterprise System technology (zEnterprise) combines scalable computing power with a new architecture that is able to manage heterogeneous workloads from a single point of control.

The key attributes of an integration architecture are flexibility, performance, manageability, security and cost-effectiveness. It is exactly these core attributes where the IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise provides unprecedented value. The IBM DataPower XI50z is a complete integration solution packaged as an appliance, meaning there is no software or middleware installation, configuration and maintenance. The appliance is hosted and integrated securely inside the IBM zEnterprise BladeCenter® Extension (zBX), and managed by the zEnterprise Unified Resource Manager, a unique cross-platform management tool.

1.1 IBM DataPower XI50z at a glance

The IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise provides a secure, fast, cost-effective, easy-to-manage, all-in-one enterprise application integration solution. The newest IBM zEnterprise has over 50,000 times more processing capability than the IBM 1401. Combining the DataPower XI50 and zEnterprise presents many advantages:

- Simplifies your infrastructure by managing all your resources, including multiple blades, with System z Unified Resource Manager.
- Increases response speed for system-critical appliances.
- Enhances your Cloud Computing model with a single hardware end-to-end infrastructure and integration of both distributed and System z applications.
- Reuses all System z assets without retraining resources.
- Provides high scalability, mission-critical design, and value.
- Monitors heterogeneous applications across your entire network with end-to-end SOA integration.
- Exploits the high speed intra-ensemble data network (IEDN) connecting the zEnterprise Blade Extension (zBX) with the z196.

The DataPower XI50z provides a variety of powerful integration scenarios specifically for older mainframe applications, making it a natural choice to include the appliance in your centralized zEnterprise server. The appliance is hosted and integrated securely inside the IBM zEnterprise BladeCenter Extension (zBX), and managed by the zEnterprise Unified Resource Manager, a unique cross-platform management tool.

1.2 Integration challenges

The integration of people and enterprises around the globe is transforming the way the world works today, driving wholesale change in systems and processes for everything from the way we create, buy, and sell products, to how we move people, goods, and services (in fact, how we fundamentally work and live). Change on such a massive scale presents tremendous IT transformation and integration challenges for organizations.

The IT industry responds with Enterprise Application Integration (EAI) projects, which often struggle to keep up with constantly changing requirements. The keys to success are a flexible integration architecture based on a standard set of integration technologies, and a flexible IT infrastructure which enables speedy deployment of applications and cost-effective monitoring of business processes.

In this section, we identify the four major integration objectives that we believe must be fulfilled to improve the success rate of EAI projects:

- Improving business agility
- Minimizing risks
- Managing IT infrastructure complexity
- Reducing IT costs

1.2.1 Improving business agility

Agility is measured by each company's own expectations and business outcomes rather than by external benchmarks. Agility is about internal readiness to respond to change, along with finding new and innovative ways of doing business.

The IBM Business Agility Study[1] surveyed companies in the financial, insurance, and health care industries, investigating business leadership, strategies, technologies, and how agility impacts business transformation. The study revealed that agility can be a powerful tool for cutting through the complexities and challenges currently dominating the IT landscape.

Today a CIO faces any of the following challenges:

- Responding quickly to changing customer demand or market opportunities, ahead of the competition
- Adding new channels (for example, mobile computing) to a multi-channel architecture
- Lacking a centralized structure and governance processes for organizing, managing, and monitoring IT systems
- Adapting IT systems as a result of mergers and acquisitions
- Responding to rapidly changing IBM Business Partner relationships
- Integrating systems that do not use standards-based messages or protocols
- Maximizing the reuse of existing assets, especially well-proven mainframe core systems
- Keeping up with evolving IT standards, such as web services specifications
- Adjusting to a constantly changing regulatory environment

In any enterprise, keeping up with and embracing change requires flexibility in the deployment of new business processes and a flexible underlying IT infrastructure. Progress in any part of a business can be bottlenecked by slow movement in a supporting area. For example, as new market opportunities arise, a company wants to move quickly to address both new and existing resources to make the most of the opportunity. However, any new investment might be wasted if either the existing infrastructure needs to be bypassed or duplicated, or changes to that infrastructure take too long or cost too much for it to be an effective part of the new market solution.

In Chapter 3, “Improving business agility” on page 19 we lay out general approaches to addressing business agility, and then we review ways in which the IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise (from now on, referred to as DataPower XI50z) can be part of the solution.

1.2.2 Minimizing risks

Whereas business agility is key to innovation and gaining market share, this cannot be done at the cost of customer confidentiality and data integrity. Measures taken to minimize risk are an important ingredient to any viable IT strategy. When our countermeasures are insufficient and are surmounted by either intentional or unintentional events, the cost to a business can be staggering.

[1] *Cutting Through Complexity with Business Agility,* an IBM study

Consequences of risk

One of the greatest fears of any IT executive or professional is a production outage because the losses to the business in transactional revenues are typically measured by the second. When this type of event occurs, the goodwill lost and frustration experienced by our partners and clients can last well beyond the event itself, causing further damage in terms of revenue and reputation. This is the stuff of nightmares, and in our role as IT professionals we live in daily fear of that phone call from the operations staff or customer that something has gone awry.

Priority of risk management

Not surprisingly, in a recent study done by IBM[2], the majority of CEOs and CIOs identified risk management as an IT focus that will help their organizations' strategy over the next five years. The peace of mind that goes along with confidence in our countermeasures is rewarding. Getting there, however, is not an easy path. Another goal listed ahead of risk management in the same study, was to reduce costs and complexity. The challenge then becomes to manage the varied and complex types of problems that can cause outages and stay within budget without introducing unmanageable complexity.

Risk management as strategy

One of the most difficult aspects of implementing strong risk management countermeasures is to anticipate where problems can occur. A typical IT infrastructure encompasses many complex topologies. There are physical, technical, geographic, and process layers to all of our systems, and all have varied types and degrees of risk associated with them. Common problems often come to mind when anticipating areas of risk, such as being hacked, broken deployment of system and application upgrades, equipment failure, natural disasters, failure to comply with regulatory requirements, and improper handling or loss of sensitive information. Proper risk management cannot be bought in a product but must have a comprehensive vision, execution, and process that includes not only good products, but skilled architects, implementers, and facilitators. You can never completely eliminate risk but can only take measures to minimize it.

In Chapter 4, “Managing risk” on page 35, we lay out general approaches to addressing these risk challenges and then review ways in which the DataPower XI50z can be part of the solution.

[2] *The Essential CIO, Insights from the Global Chief Information Officer Study*, found at
`http://www-935.ibm.com/services/c-suite/cio/study.htm`

1.2.3 Managing IT infrastructure complexity

The IT infrastructure of the typical modern enterprise has evolved to include a diverse mix of hardware platforms, operating systems, middleware, and applications to support its user community. For example, Figure 1-1 shows an example IT infrastructure that is fairly typical for a modern enterprise. The highlighted path shows the route a single transaction might take.

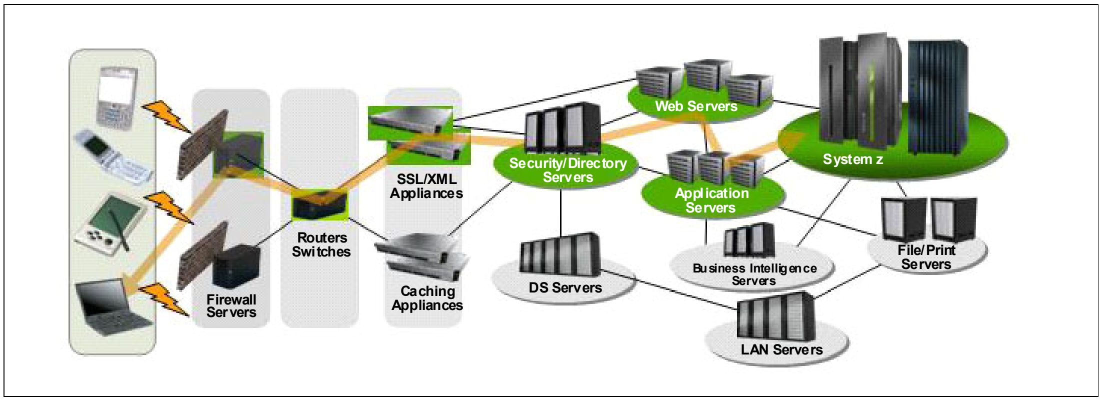

Figure 1-1 Typical hybrid infrastructure

Such a diverse mix might have come about for a variety of reasons. The widespread acceptance of the distributed computing paradigm is an obvious cause. Merger and acquisition activity might require disparate systems to be interconnected. Regardless of cause, for most organizations a complex infrastructure is a fact of life and in most cases the tendency is for complexity to increase.

Managing these diverse and increasingly complex applications, workloads, and systems can be a challenging and costly task. Often, each part of the infrastructure has its own management and monitoring tools and methodologies, each requiring specialized skills, increasing labor costs. Server sprawl contributes to increased environmental costs for floor space, power, and cooling. Distributed systems have traditionally run at a lower average processor utilization than is the norm for mainframe systems. Because software charges for distributed systems are often based on the number of processors licensed rather than their utilization, this causes increased software costs.

Complex heterogeneous environments might pose additional security challenges. Each component and each interconnection among components in the infrastructure, must be secured appropriately. An ever-increasing number of servers and network links provide an ever-increasing number of possible targets for the hacker.

Solutions that minimize IT infrastructure complexity are attractive to IT managers due to the opportunities to reduce the costs and risks associated with this complexity.

In Chapter 5, “Managing IT infrastructure complexity” on page 47, we lay out general approaches to reducing complexity and then review ways in which the zEnterprise and, in particular, the DataPower XI50z can be part of the solution.

1.2.4 Reducing IT costs

As we have seen, the IT industry is challenged with improving business flexibility and minimizing risk, but at the same time, CIOs are expected to hold to constant or decreasing budgets. Across the industry there is a deep desire to eliminate expense wherever possible. Simply put, CIOs aspire to do more with less. According to another study done by IBM[3], 14 percent of their time is dedicated to removing costs from the technology environment.

Figure 1-2 shows the trend in IT costs since 1995 with a breakdown across the four main expenditure areas: hardware, software, people, and other costs.

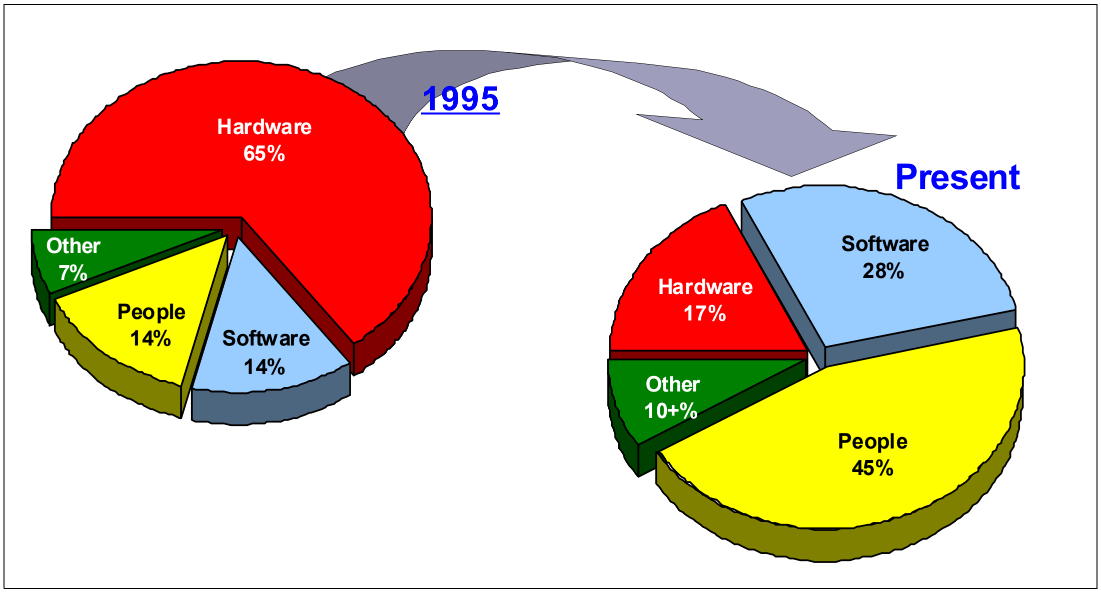

Figure 1-2 Evolution of IT costs

The underlying data used to create Figure 1-2 is based on a number of IBM Scorpion studies. It shows that over the past 15 years or so, the cost dynamics of supporting corporate IT infrastructures have changed significantly. In particular, we see that hardware costs have decreased to a third of what they were in the past; however, people costs have tripled, and software costs have doubled.

> **Note:** The *Scorpion* methodology is an approach for analyzing and optimizing corporate IT systems and infrastructures that balances the best techniques of server and storage infrastructure technical analysis with financial analysis, capital budgeting principles, and new technology solutions.

[3] *The New Voice of the CIO: Insights from the Global Chief Information Officer Study* (CIO Study 2009), page 24

To control people and software costs, CIOs commonly view a central technology organization as the future. Centralized infrastructures and processes enable shared services optimization that, in turn, provides economies of scale. Organizations also recognize that standardization is another key to cutting costs. Automation, where it makes sense, also helps lower costs within the enterprise.

Specialized systems such as optimizers and appliances can play a role in reducing IT costs in the following ways:

- Offloading the processor-intensive part of a workload, freeing up the general processors for other work
- Simplifying the integration tasks that are required when building multi-platform solutions, enabling EAI projects to be implemented more quickly and with fewer IT staff

In Chapter 6, “Reducing IT costs” on page 53, we lay out general approaches to reducing costs and then review ways in which the DataPower XI50z can be part of the solution.

2

Smarter computing with zEnterprise

Pervasive access to IT is changing the way we use it, such as through social networking, “Web 2.0 style” access to rich content, and a highly interactive user experience. The growth of mobile smart devices is creating massive volumes of data that in turn drives the need for advanced analytics. The key trends can be characterized in several ways:

- **Big data**: Enterprises want to capture an ever-increasing amount and variety of information for analysis, forecasting and predictive modeling.
- **Optimized systems**: IT managers want cost-effective solutions that use systems optimized for the task at hand, whether it be general transaction processing or specific tasks such as complex database queries or XML processing.
- **Cloud**: IT leaders are looking at new service delivery models, like cloud computing, that can enable them to support innovation in a more sustainable manner.

These and other trends are driving a new generation of IT workloads that are diverse in their functional and processing requirements and universal in their insatiable consumption of processing power. The need to innovate drives IT transformation, and crucial to these projects is the delivery of highly integrated solutions encompassing both software and hardware.

Smarter Computing is an approach to IT transformation which applies architectural choices to *integrate, automate,* and *secure* IT infrastructures, as shown in Figure 2-1. Transforming IT starts with leveraging standards to *integrate* data, systems, and services to connect siloed resources and ensure consistency of deployment. Next, processes and services are *automated* by employing software, algorithms, and decision rules to reduce the need for human intervention to manage servers, storage, and other resources. Finally, infrastructure is *secured* by applying a combination of technology and governance processes to critical data, systems, and services.

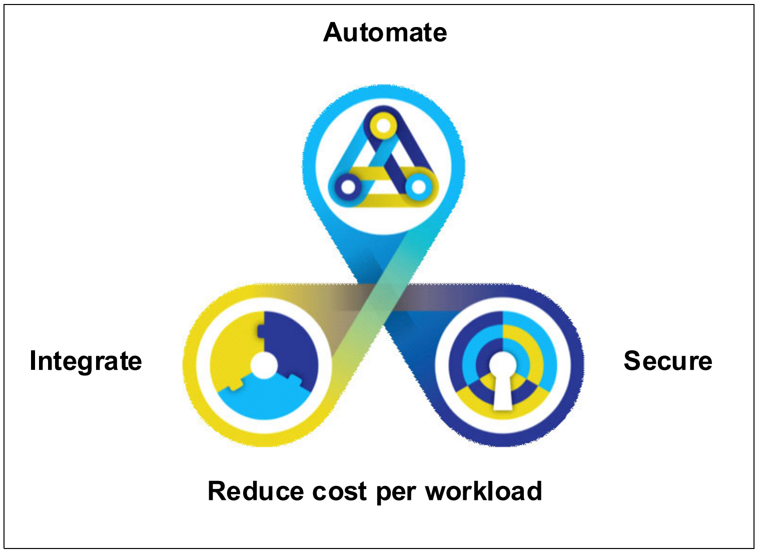

Figure 2-1 Smarter computing

A smarter computing approach includes the following objectives:

- Making sure that you take advantage of the price and performance advantages of integrated software and hardware and that systems that have been optimized for the particular needs of your workloads.
- Leveraging every opportunity to self-tune and automate capabilities provided by systems. Eliminating manual repetitive tasks will cut down systems management and administration costs and service level agreements.
- Making sure your computing foundation is rock solid in terms of security, privacy, and compliance requirements and ensure your data is secure in all phases of use, whether at rest or in motion.

Enterprises strive to attain these objectives at the same time as maintaining a constant or declining IT budget.

2.1 IBM zEnterprise value proposition

Increasingly, business applications span heterogeneous platforms, appliances, and devices, and this wide range of resources creates real issues for IT shops trying to meet business objectives. Simply adding servers, routers, and other IT equipment ultimately will not solve your IT challenges and might even make them worse. Even using virtualization techniques can only go so far in helping you to manage a massive number of servers, routers, and other devices. The ability to manage resources for these heterogeneous applications as one logical entity has been lacking until recently. The IBM zEnterprise System technology, referred to as zEnterprise, combines scalable computing power with a groundbreaking new architecture that is able to manage heterogeneous workloads from a single point of control.

With its built-in management capabilities, zEnterprise is perfectly positioned to meet customers' integration, automation, security, and cost requirements. To address these IT transformation issues, the zEnterprise System provides a new architecture consisting of heterogeneous virtualized processors that work together as one infrastructure. The system introduces a revolution in the end-to-end management of heterogeneous systems and offers expanded and evolved traditional System z capabilities.

Forrester Research[1] also outlines five key benefits of zEnterprise.

2.2 IBM zEnterprise System overview

The zEnterprise System consists of the following three components, as shown in Figure 2-2.

- IBM zEnterprise central processor complex (CPC), which is either a z196 or z114
- IBM zEnterprise BladeCenter Extension (zBX)
- IBM zEnterprise Unified Resource Manager

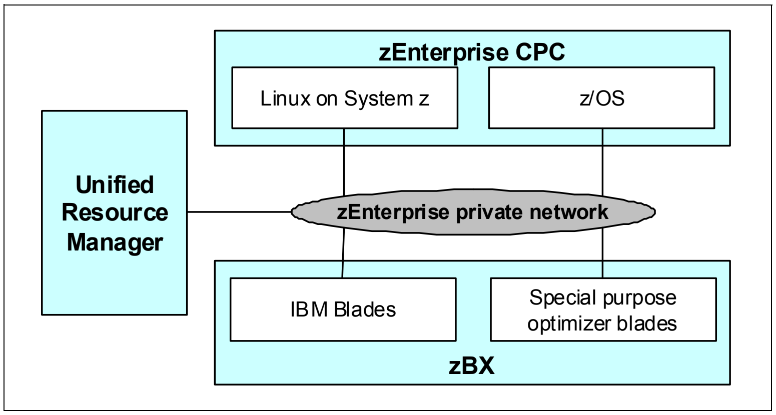

Figure 2-2 Three components of the IBM zEnterprise System

2.2.1 zEnterprise CPC: High-end mission-critical platform

Improving upon the capabilities of its IBM System z10® Enterprise Class predecessor, the z196 is the industry's fastest and most scalable enterprise server, capable of 50 billion instructions per second. The z196 not only has the capabilities and scalability of physical resources (for example, processor, memory, I/O, and so on), but also offers better reliability, availability, and serviceability (RAS). It is the ideal platform for mission-critical enterprise workloads.

[1] *Five Reasons To Choose IBM Enterprise Mainframe*, from http://www.forrester.com

IBM recently introduced the zEnterprise 114 (z114), which is a smaller machine but has the same excellent architecture and RAS capabilities as its bigger brother, the z196. From now on, we refer to both the z196 and z114 as the “zEnterprise central processing complex (CPC)” or just “zEnterprise CPC.”

Traditional workloads and data serving: z/OS

The z/OS Operating System offers extremely high scalability and performance for applications and data serving, and high availability and cross-system scalability enabled by IBM Parallel Sysplex® and IBM GDPS® solutions. z/OS provides a highly optimized environment for application integration and data management, with an additional performance benefit if both the application and the data are hosted on z/OS. It provides the ideal environment for both traditional application workloads and leading-edge technologies and large scalable data serving, especially for mission-critical workloads.

Mission-critical scale-out workload: z/VM and Linux

The z196 and z114 offer software virtualization through IBM z/VM®. The extreme virtualization capabilities provided by z/VM enable the high virtualization of thousands of distributed servers on Linux on System z. Linux on System z is an ideal platform for mission-critical scale-out workloads, such as web applications, business intelligence applications, and more.

2.2.2 zBX

The zBX is a unique new component of the zEnterprise and is an infrastructure that supports blade-based servers and optimizers that share a private management network and a private data network with mainframe resources on the z196 or z114. This provides the opportunity to integrate distributed components and System z components under a single management platform.

IBM blades

The IBM server blades provide the ability to run the wide variety of applications typically found in UNIX and x86[2] architectures. This provides opportunities for lower-cost consolidation of distributed workloads.

Special purpose optimizer blades

zEnterprise provides an architecture that allows you to attach IBM special purpose optimizer blades. The first blade of this kind was the *IBM Smart Analytics Optimizer for DB2® for z/OS V1.1*, which dramatically accelerates certain data warehouse queries for DB2 for z/OS running on the z196, contributing to reducing operational costs and improving the performance of business intelligence processes.

The second available special-purpose optimizer blade described in this Redpaper, is the *IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise*, referred to hereafter as the *DataPower XI50z.*

2.2.3 zEnterprise Unified Resource Manager

The *zEnterprise Unified Resource Manager* is Licensed Internal Code (LIC), also known as firmware, that is part of the Hardware Management Console (HMC). Unified Resource Manager is a key component of zEnterprise. It provides integrated management across all

[2] In the second half of 2011, IBM intends to offer x86 blade-running selected versions of Linux or Windows in the IBM zEnterprise System on zBX Model 002.

elements of the system. Unified Resource Manager will improve your ability to integrate, monitor, and dynamically manage heterogeneous server resources as a single, logical, virtualized environment, contributing to cost reduction, risk management, and service improvement.

zEnterprise ensemble

A zEnterprise *ensemble* is a collection of up to eight nodes, each composed of a zEnterprise CPC and, optionally, a zBX. The physical resources of servers are managed as a single virtualized pool by the Unified Resource Manager using the Hardware Management Console.

Private networks

Two new internal secure networks are introduced for the zEnterprise ensemble. These networks are the *intraensemble data network* (IEDN) and the *intranode management network* (INMN). Connectivity to the zEnterprise from existing external networks is supported as well. The IEDN is used for application data communications. The INMN is used for platform communications.

Hypervisors

Server blades provide a hypervisor which interacts with the Unified Resource Manager to provide virtualization and workload management capabilities. The IBM POWER7™ blade provides *PowerVM™* as its hypervisor. PowerVM offers industry-leading virtualization capabilities for IBM AIX®. This hypervisor is managed, along with the hypervisors of the zEnterprise CPC (IBM PR/SM™ and z/VM), by using Unified Resource Manager, which provides a single point of control.

2.3 About DataPower XI50

The DataPower XI50 is a purpose-built service-oriented architecture (SOA) appliance for delivering highly manageable, security-enhanced, and scalable SOA solutions. As specialized SOA hardware, it provides many core functions to SOA deployments in a hardened device, including integrated Enterprise Service Bus (ESB) capabilities, data enablement and integration features, and the capacity to improve web services management and SOA governance. Figure 2-3 illustrates typical DataPower XI50 use.

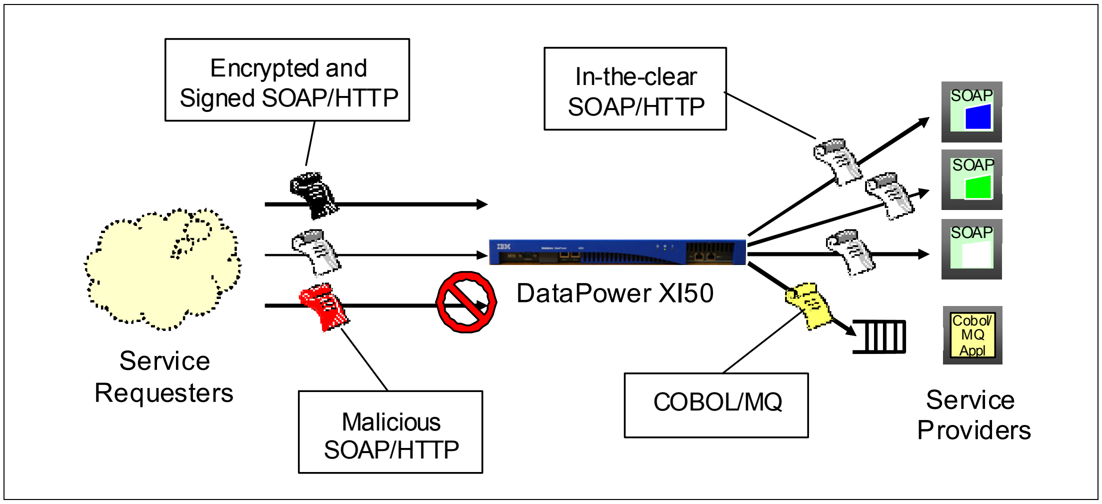

Figure 2-3 Using DataPower XI50

DataPower XI50 is typically used in the following ways:

- To process encrypted or signed SOAP or XML messages
- To intercept and reject malicious SOAP or XML messages
- To transform XML data to non-XML data, for example, COBOL binary data
- To switch from the HTTP protocol to another protocol, for example, WebSphere MQ
- To implement an authentication, authorization, and auditing (AAA) policy
- To dynamically route service requests
- To implement service level management

The DataPower XI50 functionality is provided in both rack-mounted and blade forms:

- Rack-mounted:
  - XI50 1U-height rack-mounted appliance
  - XI52 2U-height rack-mounted appliance
- BladeCenter forms:
  - XI50B for BladeCenter types H, HT, and E
  - XI50z for zEnterprise BladeCenter Extension (zBX)

This Redpaper focuses on the DataPower XI50z, but to understand its positioning within the DataPower product family, it helps to have a little background on the other XI50 models that are available today.

2.3.1 DataPower XI50 and XI52

DataPower has for many years offered a variety of 1U-height rack-mountable appliances with the primary goal of helping clients to secure, simplify, accelerate, and govern their IT infrastructures. These multiple objectives of securing, simplifying, accelerating, and governing, imply that the DataPower products are versatile, and this is certainly the case.

The XI50 integration appliance was first introduced by DataPower in 2004, the year prior to the acquisition of DataPower by IBM. The XI50 has been continually enhanced since its introduction, with added functionality from each new firmware release and with refreshes of its underlying hardware platform.

The XI50 provides all of the XML security functionality of the XS40 XML Security Gateway with additional integration functionality added on top. The integration capabilities include protocol mediation, message transformation, and routing, with support for a wide variety of transport protocols and message formats. The XI50 is often thought of as a '*hardware enterprise service bus (ESB)*' and is therefore considered a key part of the IBM portfolio of solutions for clients' ESB requirements.

The XI50, like all DataPower products, is designed to help clients deploy solutions quickly. One way this goal is achieved is by providing graphical user interfaces that allow the user to perform many setup, configuration, and development tasks through GUI actions without having to write any code. This simplicity is complemented with the ability to provide customized extensible stylesheet language transformations (XSLT), which are virtually limitless in what they can do. The XI50 makes it possible to use simple GUI actions to satisfy a very large number of use cases, enabling quick time-to-production, but also the flexibility to use XSLT to craft customized solutions for those use cases that the GUI does not cover.

The XI52, a 2U high-density design, is the latest rack-mounted appliance that delivers higher performance, more memory, and larger flash size and hard drive space than the XI50.

In summary, the XI50 and XI52 appliances provide several advantages:

- XML acceleration
- A connectivity infrastructure with ESB capabilities
- Integration capabilities for System z assets including CICS, IBM IMS™, and DB2
- Security for SOA, Web 2.0, and Cloud environments
- Governance for your evolving IT architecture

2.3.2 DataPower XI50B and XI50z

The DataPower XI50B was the first blade form-factor model of XI50 that allowed deployment of DataPower capabilities within the IBM BladeCenter infrastructure. The XI50B supports two 10 Gb network interfaces. Use of IBM BladeCenter technology can reduce the overall datacenter footprint and reduce power consumption.

The DataPower XI50z shares the same double-width blade form factor of the DataPower XI50B. Like the XI50B, the DataPower XI50z provides the same application functionality as the XI50, the 1U-height rack-mountable appliance. It therefore contains all of the integration, security, and governance capabilities DataPower clients have come to expect.

Migration note: Due to the extensive integration testing IBM performs with the DataPower XI50z and the zEnterprise Unified Resource Manager, it is expected that the support for new firmware levels on the DataPower XI50z will lag behind the availability on the rack-mountable appliance family by a few months. Keep this in mind to ensure a smooth migration when considering a migration of workload from rack-mountable DataPower appliances to the DataPower XI50z.

Figure 2-4 shows how to use DataPower XI50z to implement the SOA scenarios we have discussed.

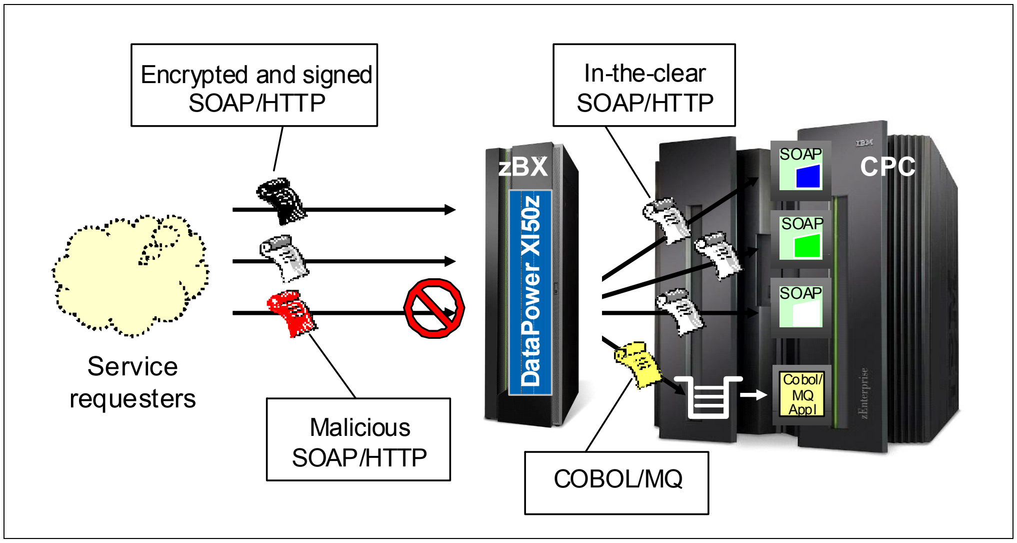

Figure 2-4 Using DataPower XI50z

What makes the DataPower XI50z unique is the physical integration within the zEnterprise system. The DataPower blade is installed as an optimizer within the zBX. For zEnterprise customers, this provides additional value opportunities in areas such as security and extended System z integration. In addition to the physical integration within zEnterprise, the DataPower XI50z benefits from the integrated management provided by Unified Resource Manager. The DataPower XI50z blades are managed as part of the zEnterprise *ensemble*.

The DataPower XI50z provides the following additional benefits:

- Secure integration between DataPower and the virtual servers within the zEnterprise through the use of the high-speed IEDN
- Extended ESB integration across the zEnterprise
- Centralized installation, operations, and management of DataPower using the Unified Resource Manager
- Improved systems management and monitoring, and automatic “call home” in the event of hardware problems

Important: The DataPower XI50z benefits from the physical integration with zEnterprise and the management capabilities of the Unified Resource Manager.

Continue to learn how the DataPower XI50z can address the integration challenges that we discussed previously. The next chapters will discuss general approaches that can improve business agility, transform IT service delivery and minimize risk, all within the context of managing IT costs. We will focus on the specific value and role of the DataPower XI50z within a zEnterprise implementation.

3

Improving business agility

The Business Agility Study findings revealed three major benefits of an agile company:

- Agility shows rapid improvement and innovation.
- Agility meets strategic directives quickly and intelligently.
- Agility drives company-defined changes and goals.

Business agility requires not only flexible business processes, but also flexible architectures to accommodate heterogeneous best-of-breed services and platforms that can be set up and changed quickly on demand.

The following principles play a major role in achieving flexibility in business processes and flexible architectures:

- Loose coupling of solution components
- Standards-based architectures
- Easy and centralized governance
- Speed of development and deployment
- Ability to Integrate with internal and external applications and services using multiple formats and protocols
- Virtualization of resources
- Secure communications between solution components
- Ability to meet a range of service level management criteria

The *IBM SOA Reference Architecture* outlines the key capabilities that are required for comprehensive, enterprise-wide service-oriented architecture (SOA) solutions. These capabilities can be implemented on a build-as-you-go basis, allowing capabilities and project-level solutions to be easily added as new requirements are addressed over time. The IBM SOA Reference Architecture can be used as a template for addressing business agility principles.[1]

[1] More information about the IBM SOA Reference Architecture can be found in the IBM developerWorks® article “Design an SOA solution using a reference architecture” at `http://www.ibm.com/developerworks/library/ar-archtemp/`.

An enterprise normally has older applications, pre-packaged applications, enterprise data stores (including relational, hierarchical, and nontraditional, unstructured sources such as XML and text), and so forth. The enterprise service bus (ESB) provides access to these applications and data using a consistent approach. These access services expose the data and functions of the existing enterprise applications, allowing them to be fully re-used and incorporated into functional flows that represent business processes.

Another method of invoking services exposed to the enterprise is with the use of Web 2.0 standards. Web 2.0 can be described as the desktop experience (from a graphical and usability perspective) brought to the web browser. There is a growing demand to use these new protocols and technologies to interact with existing enterprise systems. *Representational State Transfer (REST)* is an important Web 2.0 technology that has become a popular alternative to other web-based services, such as SOAP-based web services and Enterprise JavaBeans (EJB). A common scenario is to expose a RESTful interface in front of an existing older application, where the ESB performs the role of transformation, protocol switching, and routing to the appropriate back-end older system.

ESBs can be software-based or hardware-based SOA appliances. One of the ways an ESB can be implemented is by using an SOA appliance, such as the DataPower XI50z. The DataPower XI50z is essentially an appliance or device that has been designed, built, and configured to enable the implementation of an SOA, enable strong peripheral security, and provide quick integration of back-end systems. There are several advantages to implementing the DataPower XI50z appliance as part of an ESB solution, a key benefit being the quick and easy deployment of the DataPower XI50z when compared to a traditional server-based software solution.

DataPower XI50z is uniquely positioned to bridge Web 2.0, web services, SOA, and older systems. DataPower XI50z can service Web 2.0 requests, such as an ATOM feed message or a REST invocation, and bridge to enterprise protocols, such as CICS web services, Java Message Service (JMS), MQ (IMS and CICS bridges), and IMS (IMS Connect).

3.1 DataPower XI50z architecture patterns

The DataPower XI50z can participate in two major architecture patterns: the *SOA gateway* and *enterprise service bus*. Figure 3-1shows both patterns at a high level in the context of a logical SOA.

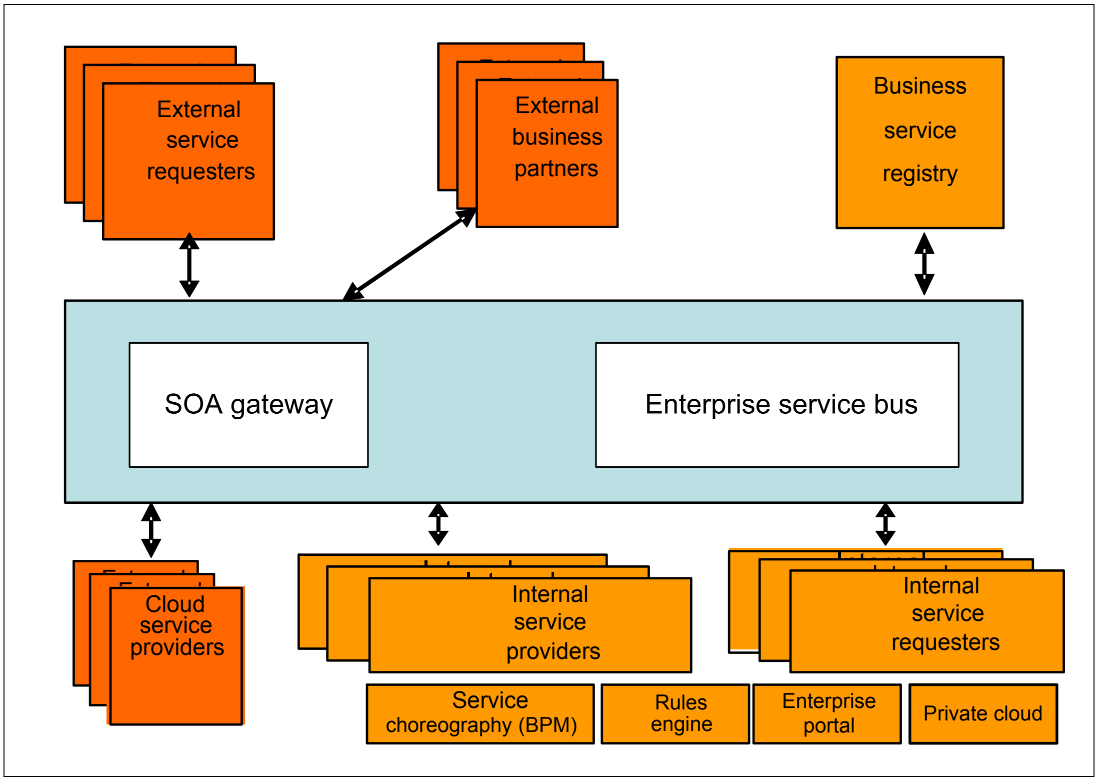
External service requesters
External business partners
Business service registry
SOA gateway
Enterprise service bus
Cloud service providers
Internal service providers
Internal service requesters
Service choreography (BPM)
Rules engine
Enterprise portal
Private cloud

Figure 3-1 Simplified view of the SOA gateway and enterprise service bus

Table 3-1 outlines the logical architecture components of SOA shown in Figure 3-1 on page 21.

Table 3-1 SOA logical architecture components

Component	Description
SOA gateway	Used to provide a controlled point of external access to services where the ESB does not provide this natively. Larger organizations are likely to keep the SOA gateway as a separate component. See 3.1.1, “SOA gateway” on page 23 for more information.
Enterprise service bus (ESB)	Provides an integrated communication, messaging, and event infrastructure for an SOA consistent with the needs of the enterprise, to provide service interaction capabilities under suitable service levels and manageability, that can operate in a heterogeneous environment. See 3.1.2, “ESB” on page 23 for more information.
Cloud service providers	Offer *Software as a Service* (SaaS, such as SalesForce.com), *Platform as a Service* (PaaS, for example, Microsoft Azure), or *Infrastructure as a Service* (IaaS, for example, Amazon EC2). These providers have security and connectivity, quality of service, and security requirements that might differ from internal providers or business partners over a virtual private network.
Business service registry	Provides a taxonomy and catalog of available services to systems that participate in an SOA. The ESB can access the registry dynamically at run time and might be directly integrated to the mediation flow through a special mediation component on the ESB. The ESB can also subscribe to a service on the service registry statically at design time.
Private cloud	Provides Cloud-based services within the enterprise. Corporations that want the scalability, metering, and agility benefits of a public cloud service without ceding fine-grained control, security, and recurring costs to an external provider might use a private cloud solution.
Business rules engine (BRE)	Used to execute business rules and might be part of a business rules management system that enables organizational policies and the operational decisions associated with those policies to be defined, deployed, monitored, and maintained separately from application code.
Service choreography	Used to orchestrate sequences of service interactions into short or long-lived business processes. The Business Process Management engine can be a provider or consumer of services offered through the ESB.
Enterprise portal	Provides a unified web experience that consolidates applications and content with search, personalization, and security capabilities. The portal can be a consumer of services offered on the ESB or a service provider.

The roles shown in Table 3-2 interface with the SOA.

Table 3-2 SOA roles

Internal service providers and internal service requesters	Service providers and consumers within the organization or enterprise who might differ from external service providers or requesters in security and connectivity requirements.
External business partners and external service requesters	Business partners, service providers, or service consumers outside the organization or enterprise who might differ from internal service providers and requesters in security, quality-of-service, and connectivity requirements.

3.1.1 SOA gateway

The SOA gateway provides a controlled point of external access to services where the ESB does not provide this natively. Additionally, the DataPower XI50z, as an SOA gateway, can act as a service facade to existing older applications to enable new channels and clients to securely access those services through various standards-based protocols. Figure 3-2 shows the DataPower XI50z used in this role.

An SOA gateway can also be used in tandem with an ESB. This is explained further in 3.1.2, “ESB” on page 23.

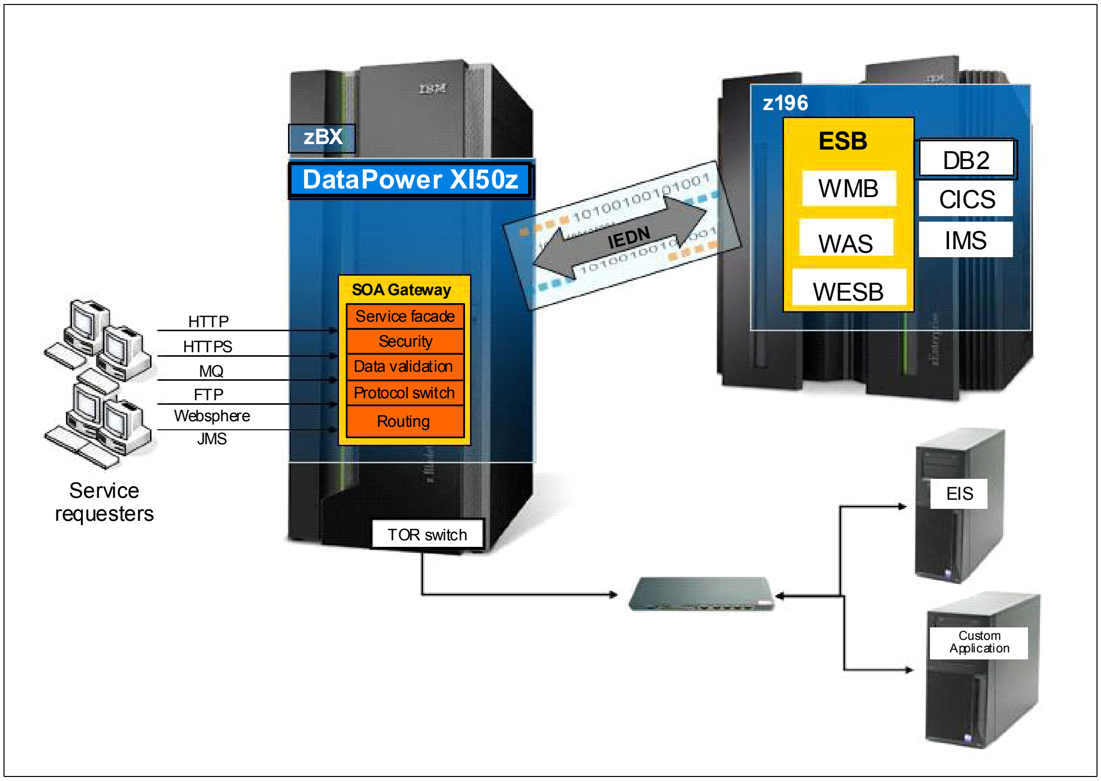

Figure 3-2 The role of DataPower XI50z as an SOA gateway

3.1.2 ESB

The ESB pattern is a key enabler for an SOA and provides a platform to integrate service providers and service consumers that can operate in a heterogeneous environment under suitable service levels and centralized manageability.

The XI50z provides several capabilities as an ESB, as listed in the orange ESB block in Figure 3-3 on page 24. Larger organizations are likely to keep the SOA gateway as a separate component to provide an additional layer of protection and to also gain the ability to federate to several ESBs from the gateway. Alternately, certain enterprises might choose not to use the SOA gateway as a separate component and rather incorporate the capabilities of the SOA gateway within the ESB.

The reference architecture that uses the capabilities of the XI50z as an SOA gateway in tandem with an ESB is shown in Figure 3-3. For a description of the capabilities shown in the orange blocks in this figure, see 3.2, “DataPower XI50z capabilities and features” on page 25.

.

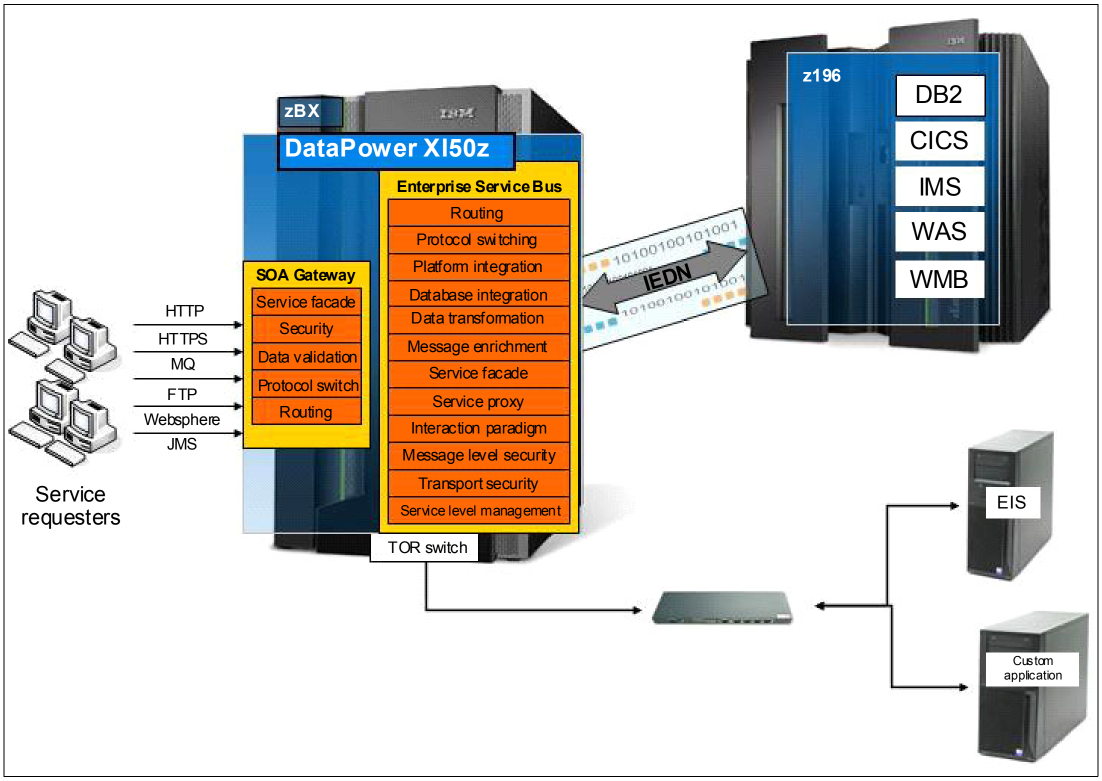

Figure 3-3 DataPower XI50z as both an SOA gateway and an ESB

In the following section we discuss how DataPower XI50z provides capabilities for both the ESB and the SOA gateway pattern.

3.2 DataPower XI50z capabilities and features

DataPower XI50z can participate both in an ESB role and SOA gateway role and provides the capabilities to an enterprise architecture as described in Table 3-3.

Table 3-3 DataPower XI50z capabilities and features

DataPower XI50z feature	Description
Routing	Based on fields in the input content or in a URL, DataPower XI50z has the ability to route to separate logical partitions (LPARs) or TCP ports on separate back ends: ► DataPower XI50z can route to the appropriate LPARs based on content in the input payload. ► DataPower XI50z can perform content-based routing to separate versions of a service running in CICS, thus enabling new service consumers who need a newer service version without requiring modifications by the existing consumers of the older version of the service. This can also include the endpoints being retrieved from a service registry using an endpoint lookup.
Protocol switching	Service requesters and providers might utilize unique and separate communication protocols. By using the DataPower XI50z as an ESB, which supports most of the popular protocols (for example, HTTP, JMS, MQ, and TIBCO EMS), the consumer does not need to be aware of what protocol the provider utilizes. DataPower XI50z converts protocols between two systems using separate protocols for communication. DataPower provides Web 2.0 front-end interfaces (such as REST, AJAX, DoJO, JavaScript Option Notation (JSON), SOAP, and so forth) for traditional back-end service providers (like CICS, IMS DB, IMS DC, DB2, WAS, and so on) with few or no provider application changes. For example, an XI50z can take REST, SOAP, or XML input over HTTP or HTTPS, transform the message to the format required by the back-end service provider, and then send the message over another supported transport protocol, such as WMQ, FTP, WebSphere Java Message Service (JMS), TIBCO EMS, and other protocols.
Platform integration	DataPower XI50z enables applications and services running on separate platforms, such as Microsoft .Net, Java Enterprise Edition (JEE), or z/OS, to participate in and interact with an SOA: ► Integrating .Net and z196: If a SOAP client on .Net needs to query older COBOL programs running under CICS, DataPower XI50z can transform SOAP to COBOL copybook (CPY) and send the message over the WebSphere MQ (WMQ) CICS Bridge and vice versa (back to the SOAP client). ► Integrating JEE and z196: If a REST client residing on WAS wants to query data available on z196 through CICS web services. DataPower XI50z can convert the REST message to a SOAP request for CICS web services and vice versa (back to the REST client).

DataPower XI50z feature	Description
Database integration	DataPower XI50z can serve as an enabler to rapidly integrate a database on z196 to systems internal or external to the z196 platform: ▶ In a non-transactional query, a REST service on an open systems platform to DataPower XI50z invokes a stored procedure on DB2 using IBM DRDA® and sends results back to the REST service consumer without the use of DB2 connect. ▶ A SOAP consumer can send a SOAP message to DataPower XI50z, which can look up a database table to enrich the message and transform to CPY to forward to an existing CPY/CICS service.
Data validation	DataPower XI50z provides the validation of schema in SOAP or XML messages or conformity to a profile (such as BSP 1.0) with easy configuration steps. DataPower XI50z can perform schema or Web Services Description Language (WSDL) validation on incoming SOAP or XML messages for a CICS web service resident on z196. DataPower XI50z can reject the message if it is invalid so that the service cycles of the CICS back-end service are not wasted. This also provides additional security by preventing a message going to the CICS system that might have been tampered with by adding or removing mandatory attributes.
Data transformation	DataPower XI50z can provide any-to-any data transformation services and enable two systems with separate message models or schemas to communicate with each other in the required format: ▶ JSON to JSONX XML to SOAP using XSLT: DataPower XI50z can transform data from one schema to another. Forinstance, a REST client can send a JavaScript Object Notation (JSON) message to DataPower XI50z, which then can convert to JSONX and transform the JSONX XML message to a SOAP message.This message can then be consumed by a back-end web service on WAS. ▶ SOAP to CPY using on-board WTX engine: A SOAP consumer can send a SOAP request that requires data through an older CICS COBOL program. DataPower XI50z can convert the SOAP request to COBOL Copybook format using a map built on WTX Studio and loaded onto a binary transformation on the DataPower XI50z. DataPower then sends the resulting message over CICS MQ Bridge to the CICS program on z196.
Message enrichment	DataPower XI50z can add additional value to existing data in the message in transit on the ESB by using a map, database tables, or a call to an internal or external service provider to enhance the data. If a SOAP/HTTP web service needs to be enriched with a static map stored as an XML file on an HTTP server or a Network File System (NFS), the SOAP input to DataPower XI50z can be enriched with an XPATH lookup into an XML file fetched from an HTTP server and delivered to the back end.
Service façade and proxy	DataPower XI50z can rapidly enable an older application to be available to new channels and clients using various standards-based protocols and on several platforms. DataPower XI50z can provide SOAP/HTTP or Web 2.0 access to an existing CICS or IMS application without the need for changing the code on the z196 platform.

DataPower XI50z feature	Description
Service proxy	DataPower XI50z can rapidly provide a proxy to an existing service on zEnterprise, providing loose coupling and service level management to its service consumers and providers. Also, DataPower XI50z can help in virtualizing web services running in WAS or CICS on a z196 by providing a *service proxy* that can provide loose coupling between the consumer and z196 provider, and a common platform for logging, auditing, and security to the back-end web services layer on z/OS.
Interaction paradigm switching	DataPower XI50z can be a bridge between two separate systems with separate interaction paradigms, like publish/subscribe, synchronous request/response, fire and forget, and asynchronous messaging: ▸ Synchronous request/response to publish/subscribe: A SOAP message sent to the DataPower XI50z can be transformed and distributed to a list of subscribers to a topic on WMQ Version 7 or WebSphere Message Broker on z/OS. ▸ Synchronous request/response to asynchronous messaging: A REST message sent to the DataPower XI50z can be transformed and sent as a WMQ message to the WMQ IMS Bridge and onward to an IMS back end with a REST acknowledgement sent to the client.
Transport-level security	DataPower XI50z can provide point-to-point security between a client and the DataPower XI50z and between the DataPower XI50z and the service provider using the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol and other mechanisms: ▸ SSL/TLS termination (as SSL client or SSL server): The DataPower XI50z can act as an SSL termination point for secure transport to the zEnterprise. Within the zEnterprise, HTTP might be used to reduce the performance overhead without increasing risk. ▸ SSL mutual authentication: The DataPower XI50z can provide mutual SSL authentication to its consumers and to its providers on various platforms.
Message-level security and trust	DataPower XI50z can protect the integrity and confidentiality of a message and provide a mechanism for associating security-related claims with the message. For example, a business partner might want to securely access a company web service over the Internet. The partner signs the message, which is then sent over HTTPS to the DataPower XI50z, where the signature is verified using the business partners certificate. This solution provides confidentiality, integrity, and non-repudiation and can be used to authenticate the identity of the business partner. See 4.2.4, “Message security” on page 40 for more information.

DataPower XI50z feature	Description
Service level management / Quality of Service (QoS) and Governance	► If traffic patterns meet certain configurable criteria, DataPower XI50z can provide service level management (SLM) that has the ability to monitor traffic and to take action: ► DataPower XI50z can act as a traffic modulator by rejecting messages during peak hours from specific identifiable sources (forexample, internal traffic) trying to access specific resources residing on the zEnterprise system. ► DataPower XI50z can obtain metadata information from a service registry and repository. This enables the DataPower devices to be decoupled from the service and service-policy life cycle and only refer to the service repository of record for the latest metadata at design time or at run time. Such metadata includes WSDL, XML Schema Definition (XSD), and WS-Policy.
Support various assured delivery paradigms	DataPower XI50z supports various assured delivery paradigms on both the front and back ends, like WebSphere MQ, TIBCO EMCS, and so forth. For example, a system that uses TIBCO EMS messaging needs to update information about IMS. XML message input to DataPower XI50z can be transformed to the appropriate message and sent to IMS over a WebSphere MQ IMS Bridge or IMS Connect and vice versa. Persistent queues and durable topics are used.

3.2.1 Integration use cases

In this section we discuss the following integration use cases:

- Integration with CICS TS
- Integration with IMS
- Integration with DB2 on z/OS
- Integration with other ESBs on z/OS

3.2.2 Integration with CICS TS

Organizations that own a zEnterprise CPC often have many of their core business applications running under CICS. The DataPower XI50z enables the reuse of these proven core business applications that have been developed over the years, with practically no change to the base CICS programs. The DataPower XI50z integrates with CICS to help expose the business logic contained within CICS systems as services to the enterprise. This allows the various modern-day graphical user interface (GUI) productivity tools to use and exploit the business logic assets contained in CICS systems.

Figure 3-4 displays the integration patterns used by DataPower XI50z to integrate and take advantage of the valuable business logic embedded in z/OS-based CICS systems.

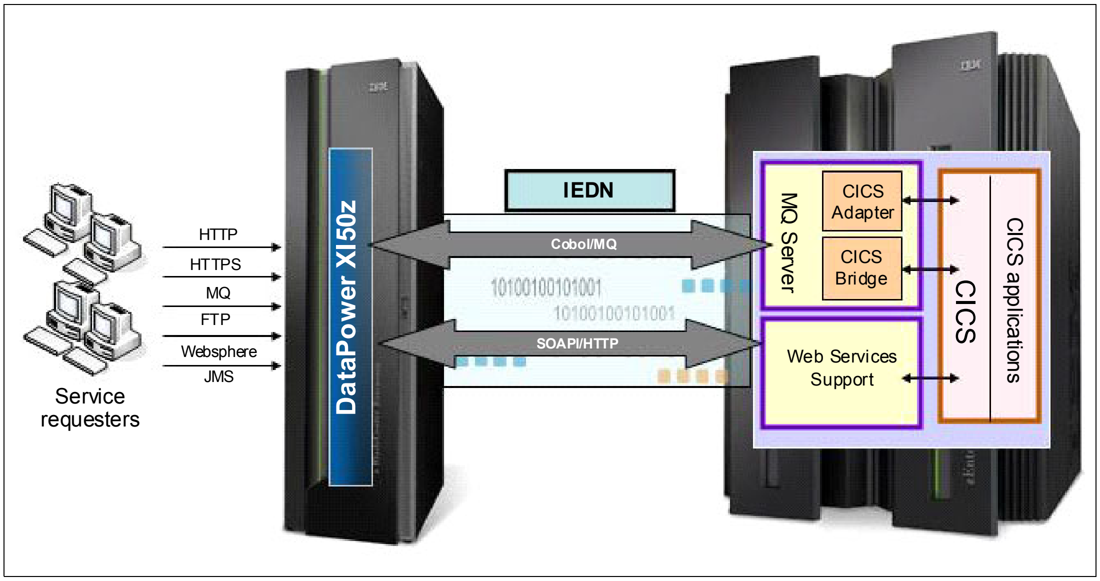

Figure 3-4 DataPower XI50z integration with CICS on z/OS

In this scenario, a client sends a request message through one of the various supported protocols to DataPower XI50z. The DataPower XI50z transforms the message into a format that can be consumed by the target CICS application. The message is transported from the DataPower XI50z over the private and secure 10 Gbps Intra-Ensemble Data Network (IEDN) that connects the zBX to the z/OS LPARs running the core business applications.

We now discuss two options:

- Integration with CICS TS through WebSphere MQ
- Integration with CICS TS through web services support

Integration with CICS TS through WebSphere MQ

In this integration pattern, the DataPower XI50z receives a request message from a client application through the external network. The DataPower XI50z performs gateway security functions as required on the request message. These security functions include authentication, authorization, verifying message integrity, and decryption.

The DataPower XI50z then transforms the request message to the format required by the CICS application. The DataPower XI50z then makes a connection or uses an established connection to the WMQ Queue Manager running on z/OS over the IEDN. The WMQ Queue Manager is connected to the CICS region using well-proven components, such as the CICS Adapter or CICS Bridge for WebSphere MQ. When the DataPower XI50z receives a message, it does the necessary processing and transformation and then routes the response message back to the client application.

In this case, security processing, XML parsing, and schema validations, which are all processor-intensive, are executed on the DataPower XI50z.

Integration with CICS TS through web services support

In this integration pattern, the DataPower XI50z receives a request message from a client application through the external network. The DataPower XI50z performs gateway security functions as required on the request message. It then processes the message, transforming it into the format required by the CICS web service and encapsulating the request in a SOAP envelope with the appropriate SOAP headers.

The DataPower XI50z transfers the SOAP message to the z/OS LPAR running the CICS subsystem over the intraensemble data network (IEDN).

The CICS sockets listener receives the message and passes it to another transaction for pipeline processing. A message handler in the pipeline extracts the message from the body of the SOAP envelope. The extracted message is passed to a data mapper, which transforms the message to the format required by the CICS program. The transformed message is then sent to the CICS program using the COMMAREA or container. The CICS program completes the processing of the message, and the resulting response message is passed back to the pipeline to be transformed appropriately, wrapped in a SOAP envelope, and sent back to the DataPower XI50z as the HTTP response.

The DataPower XI50z performs any additional processing and transformation that might be required on the response message and then routes it back to the requesting client application.

3.2.3 Integration with IMS

This section addresses the integration of DataPower XI50z with IMS on z/OS. IMS-based application programs have been serving the critical business needs of organizations for years. The costs and risks associated with rebuilding these applications are significantly high, which makes enabling them for reuse as services in an SOA a winning proposition for all companies. DataPower XI50z gives IMS the flexibility and agility to quickly adapt to an SOA-based framework. This way, modern applications using the latest technologies, such as Web 2.0, have access to all the valuable assets contained in IMS systems.

Figure 3-5 displays the integration patterns used by DataPower XI50z to integrate and take advantage of the IMS IT assets of an organization with minimal development and testing effort.

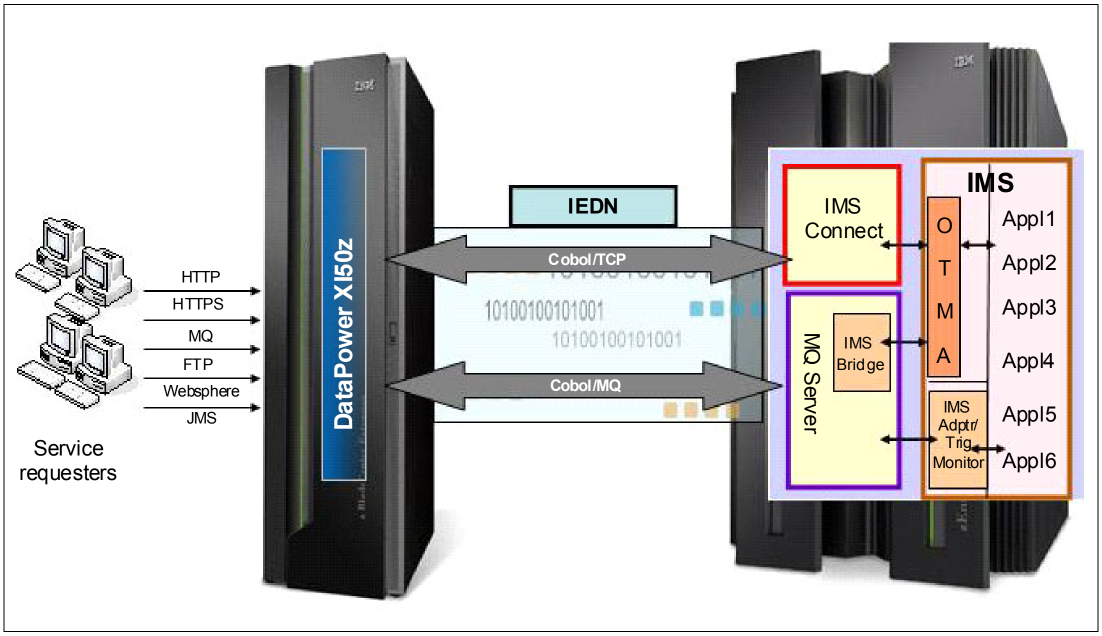

Figure 3-5 DataPower XI50z integration with IMS on z/OS

DataPower XI50z integrates with the IMS using either the MQ interface or through a TCP/IP connection directly to IMS Connect.

The client application sends a request message over HTTP to the DataPower XI50z. The DataPower XI50z transforms the message to a format that can be consumed by the target IMS application. The message is transported from the DataPower XI50z over the IEDN that connects the zBX hosting the DataPower XI50z to the z/OS LPARs running the core business applications.

We now discuss two options:

- Integration with IMS through IMS Connect
- Integration with IMS through WebSphere MQ

Integration with IMS through IMS Connect

IMS Connect is a TCP/IP server that enables TCP/IP clients to exchange messages with IMS Open Transaction Manager Access (OTMA).

The DataPower XI50z receives client request messages. The DataPower XI50z performs gateway security functions as required on the request message. The message is then parsed, mapped, and transformed into the COBOL format, which is normally the format required by IMS programs.

The DataPower XI50z then uses the IMS Connect Client to make the backend TCP/IP connection over the IEDN to the z/OS LPAR running the IMS Connect Server.

The IMS Connect Server passes the message to the OTMA, which initiates an IMS program by dropping the message into an IMS Message Queue in the IMS Transaction Manager. The response message is sent back to the DataPower XI50z using the same path.

The DataPower XI50z maps and transforms the response message into SOAP/XML by using transformation maps generated by the WTX Studio and sends the SOAP response message to the requesting client application.

Integration with IMS through WebSphere MQ

In this use case the DataPower XI50z receives a request message from a client application through the external network. The DataPower XI50z performs gateway security functions as required on the request message. It then transforms the request message to the specific COBOL format required by the backend IMS program. The DataPower XI50z then makes a client connection or uses an established client connection to the WMQ Queue manager over the IEDN to the z/OS LPAR running the Queue Manager and puts the message on a specific queue.

The WMQ Queue Manager is connected to the IMS region using well-proven components, such as the IMS Adapter or IMS Bridge for WebSphere MQ. When the response message is received, it does the necessary processing and transformation and then routes the response message back to the client application.

3.2.4 Integration with DB2

Data Web Services (DWS) is a solution to significantly ease the development, deployment, and management of web services-based access to DB2 database servers.

IBM Data Studio lets you take data manipulation statements (such as Select, Insert, Update, Delete, and XQuery) and stored procedure calls, and generate web services without writing a single line of code.

DWS provides a full web services interface, including support for SOAP and REST-styled bindings. All this is part of IBM Data Studio Developer, which means you can develop web services and database applications in one environment. The generated web services (WSDL, data mapping, and query XSLT) are packaged in a form that can be easily deployed to DataPower XI50z.

Figure 3-6 shows the integration pattern used with DataPower XI50z to expose DWS to the enterprise by using the IEDN to connect to the z/OS-based DB2 servers.

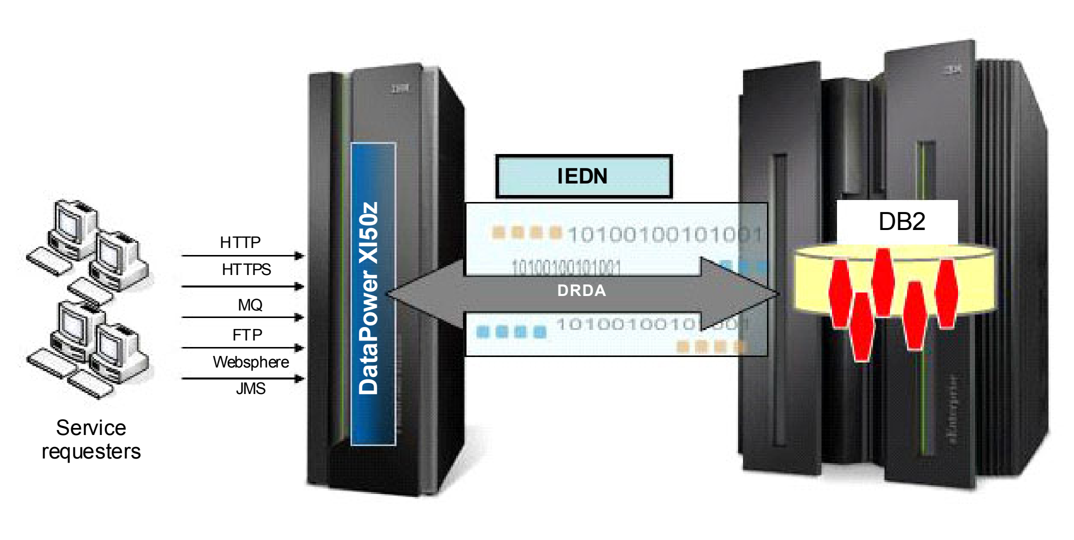

Figure 3-6 DataPower XI50z integration with DB2 on z/OS

IBM Distributed Relational Database Architecture™ (DRDA) is a database interoperability standard from The Open Group. DataPower XI50z can access DB2 data using the DRDA protocol without the use of IBM DB2 Connect™. The DataPower XI50z connects directly to DB2 on z/OS over the IEDN that connects the zBX to the z/OS LPAR that hosts DB2.

Using DataPower XI50z as the hosting environment for data web services takes advantage of the superior support of the network protocols and gives a wide variety of clients the ability to access DB2 without even being database-aware.

3.2.5 Integration with other ESBs on z/OS

The zEnterprise CPC can have other ESB solutions running directly on z/OS or Linux for System z. Many organizations have already invested in an ESB solution to expose the wealth of older applications to the enterprise as business services. We now discuss the DataPower XI50z integration with the following IBM solutions on the CPC:

- WebSphere Application Server (WAS)
- WebSphere Enterprise Service Bus (WESB)
- WebSphere Message Broker (WMB)

DataPower XI50z integrates with all of the ESBs running on the CPC over the IEDN that connects the zBX to the z/OS LPAR or Linux for System z system hosting the ESB.

Figure 3-7 shows the transport protocols that the DataPower XI50z can use to connect to the ESBs on z/OS over the IEDN.

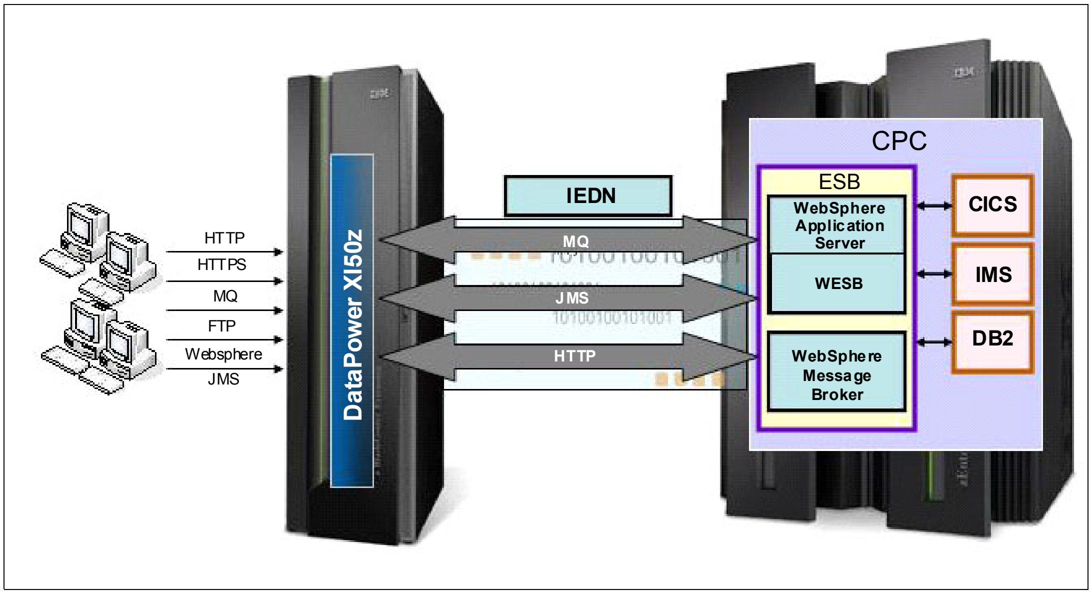

Figure 3-7 DataPower XI50z integration with other IBM ESBs on z/OS

In this use case, the DataPower XI50z is used as an SOA gateway to the services exposed by the ESBs running on z/OS, taking on the role of security and routing gateway. The consumer applications will send request messages to the DataPower XI50z, which will perform the gateway security functions as required on the request message for each message and optionally execute XML-to-XML transformations on the message where required. DataPower then forward the request to the ESB server over the IEDN that connects the zBX to the CPC running the target ESB. The ESB on the CPC executes the necessary mediations to communicate with the back-end applications on CICS or IMS or with the DB2 database.

As the SOA gateway, the DataPower XI50z can take on all the processor-intensive tasks such as digital signature verification and signing, encryption and decryption requirements, and various other security-related tasks described in Chapter 4, “Managing risk” on page 35.

4

Managing risk

In this chapter, we enumerate several concerns regarding risk management and then outline both general solutions and specific solutions using the DataPower XI50z.

Many of the features discussed in this section use core functionality available on the entire DataPower product line, including the non-blade 1U and 2U form factor appliances. These devices are well described in other publications, such as *IBM WebSphere DataPower SOA Appliance Handbook,* ISBN 978-0-13-714819-6. In this Redpaper, we focus on the functionality specific to DataPower XI50z and identify added value for our featured product.

4.1 Risk categories

We break risk management down into three broad categories and we discuss each of those in the following sections:

- Security
- Resilience
- Auditing

4.2 Security risks

Poor security exposes a business to risk on many levels. Risk must be managed at each slice of the IT stack. DataPower has always provided tremendous capabilities across the board in terms of security functionality. This is due to its heritage, going back to the earliest days of the product's original inception and design, providing acceleration and security through a dedicated, purpose-built hardware and firmware.

4.2.1 Network security

Networks must be protected carefully to ensure that attacks such as end-around, man-in-the-middle, denial of service, or sniffing of traffic do not succeed. Often, network topologies make use of a secure *demilitarized zone (DMZ)* at the front of their infrastructure. The idea is for outside traffic to always enter here and then to receive requests from the client and allow only our own trusted intermediaries in this zone to send those requests by proxy to our back-end systems (and receive the responses for the clients). Given this responsibility, the DMZ must in turn be a secure environment: simple, barren, and hostile toward any potential intruders. Bear in mind that we must also ensure that intruders cannot reach our back-end systems by going around or circumventing the DMZ (an end-around attack). Another common aspect of network security is transport-level encryption, whereby the traffic is encrypted dynamically. This helps to prevent network sniffing and exposure of message data.

With the DataPower XI50zand heritage DataPower appliances, a wide variety of network security features and tools are available. These include, but are not limited to, typical things like preventing network-level attacks such as *denial of service (DoS)*. These features also include handling service-level management (SLM) policies, network access control lists, SSL/TLS on the many supported protocols, and interface isolation. As stated earlier, the DMZ must be a highly secure environment, and due to its design, DataPower is the epitome of this type of security. For this reason, DataPower is highly popular for DMZ use in network topologies and often the only component found there, displacing load balancers, web servers and proxy servers for higher security, simpler network design and associated cost savings.

This common topology, with a network DMZ fronting the back-end infrastructure, is viable for System z customers, and can even include a heritage 1U or 2U DataPower appliance as an SOA gateway for security functions.This appliance can front a DataPower XI50z inside the System z platform used as a back-end ESB, as shown in Figure 4-1.

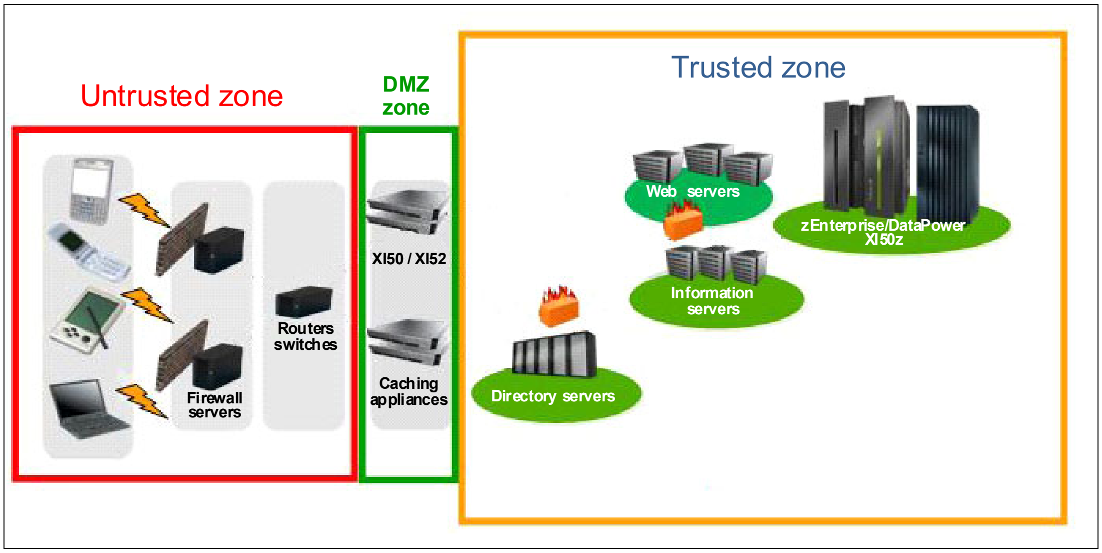

Figure 4-1 Common networking topology with DataPower appliances in the DMZ

Many clients, having standardized zEnterprise as their platform of choice, might prefer a topology that completely leverages that platform by placing the DMZ network zone within zEnterprise and using the DataPower XI50z for both external security and internal use cases. This topology is shown in Figure 4-2, which shows DMZ traffic routed directly to the DataPower XI50z through zBX Top-of-Rack (TOR) switches. (The TOR switches are not shown in the diagram but are located between the external router and the DataPower XI50z).

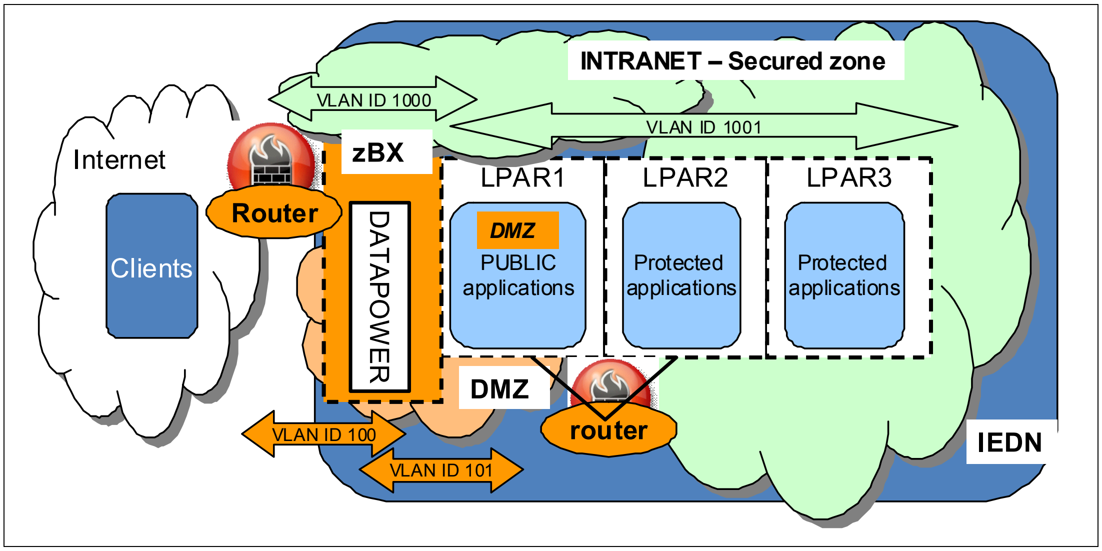

Figure 4-2 Topology with external DMZ traffic routed directly to DataPower XI50z

Note that in Figure 4-2, separate VLANs (100 and 101) are provided for DMZ traffic to isolate that traffic from the secure intranet traffic, which is using VLANs 1000 and 1001.

The DataPower XI50z supports access to multiple VLANs across its network interfaces. Inbound traffic from one VLAN can be sent to another VLAN defined to the DataPower XI50z without the need for this traffic to exit the TOR switch and pass through an external router as is normally required when servers in the zBX communicate on separate VLANs.

For example, in Figure 4-2 on page 37, even though LPAR1 and LPAR2 are both within the intraensemble data network (IEDN), if they are on two separate VLANs and want to communicate, the network traffic will exit the IEDN through the terminal-owning region (TOR) switch (not shown), pass through the external router (shown in the figure), and return to the IEDN through the TOR switch. However, if servers on two separate VLANs within the IEDN (for example, 1000 and 1001 as shown) communicate through the DataPower XI50z, the traffic between them does not need to exit the IEDN and go to an external router. The traffic stays within the secure, private IEDN.

DataPower XI50z value addition: An additional benefit of the DataPower XI50 is that the location of the DataPower XI50z within the zBX allows a reduced network pathlength that is both private and secure for the portion of the network path that resides within the zEnterprise ensemble.

As an alternative to the last scenario, traffic can be routed through an logical partition (LPAR), rather than directly to the DataPower XI50z layer through the TOR to make use of Parallel Sysplex load distribution capabilities. This topology is shown in Figure 4-3.

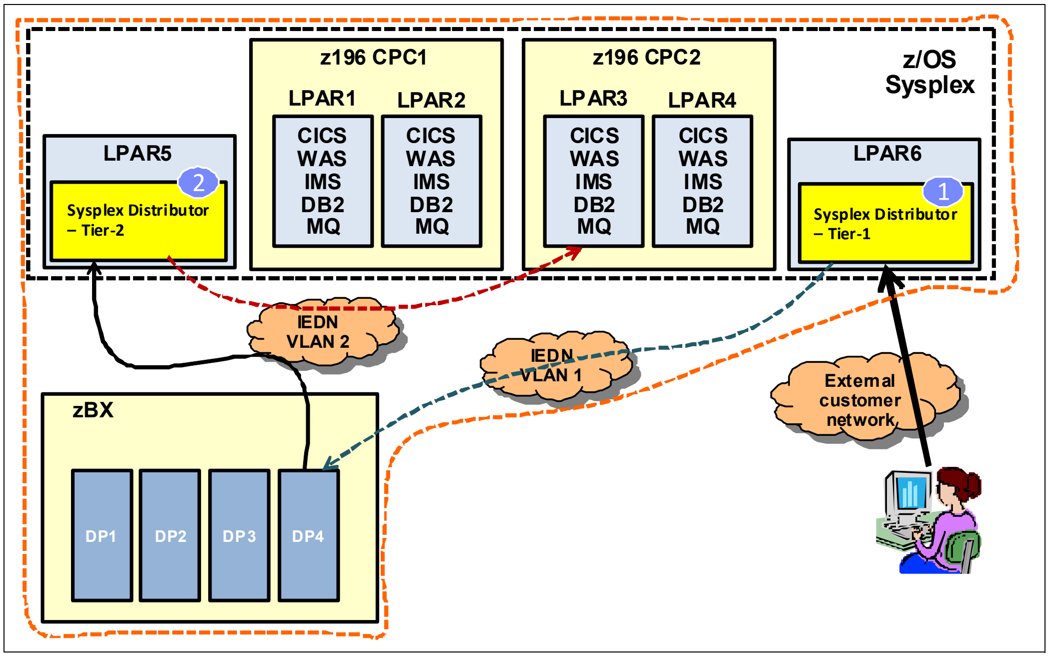

Figure 4-3 Topology with external traffic entering z/OS first and then sent to DataPower XI50z

DataPower XI50z value addition: The security of the IEDN means that the complexity and overhead of configuring mutual (two-way) SSL “secure tunnels” is not needed when the XI50z is used as a DMZ component within zEnterprise.

4.2.2 Operating system security

Operating systems (O/Ss) are often hardened by enterprises to prevent attacks or compromises targeted at known weaknesses. The Center for Internet Security[1] publishes benchmarks, guidelines, and tools for hardening common O/S platforms. Good O/S security at install time typically means removing potential hacker tools such as sendmail, telnet, and Java Runtime Environments (and certainly Java Development Kits). The security of the O/S is ensured by a process that involves monitoring sites that publish known vulnerabilities and applying fixpacks that fix them in a timely manner.

Because the DataPower operating system is proprietary and closed, it is much more secure and less prone to attack than O/Ss that are available in software form for hackers to analyze and reverse engineer. The DataPower O/S is already hardened for you and is tuned to provide security and perform at its best with the DataPower onboard hardware components. Many of the OS parameters can also be changed using DataPower administrative interfaces to better mesh with your particular environment.

4.2.3 User security

Unwanted intruders can silently steal or modify information that they are not supposed to have access to, or they can often damage infrastructure to cause outages that might even occur long after they are gone. User security ensures that only legitimate users of the systems can access the services and information that they are entitled to. This is achieved by authentication (having users provide proof of their claimed identity) and authorization (ensuring that they can only access services or data they are authorized to).

When users are authenticated, often a stateful security credential is created as proof of the user identity. This allows systems to prevent the overhead of repeatedly authenticating the same user by caching the credential or providing it to the user with the response. The credential is normally signed and encrypted and has a limited lifetime for security purposes. The credential can also be used for single-signon purposes when the same user sends requests to separate systems that understand that same credential format. Common security credentials are based on standards such as X.509 digital certificates, Security Assertion Markup Language (SAML), and Kerberos tickets.Credentials also take proprietary formats such as IBM WebSphere, Lightweight Third Party Authentication (LTPA) tokens and Windows .Net Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO). However, it is common for several platforms to use several credential types, making true enterprise-wide single-signon more of a dream than reality.

DataPower has always provided extensive capabilities for user-level security in the areas of authentication, authorization, and auditing (AAA). There are integration points at each step of the AAA process for ubiquitous older technologies, such as basic authentication and LDAP; standards-based technologies such as SAML; Extensible Access Control Markup Language (XACML); WS-Security; and third-party security products, such as those from IBM Tivoli®.

[1] Center for Internet Security, found at http://cisecurity.org/

Another component of user security, as discussed in 4.2.3, “User security” on page 39, is single signon and the user credential (proof of identity). DataPower is useful as a tool to achieve that holy grail of true enterprise-wide single-signon because it can validate and create the credential types listed in that section. In fact, DataPower provides identity propagation support for z/OS by passing the client-supplied credentials as an *Extended Identity Context Reference (ICRX)* credential to z/OS, which can identify the user based on a Resource Access Control Facility (IBM RACF®) IDIDMAP profile. Identity propagation is an identity assertion capability provided by z/OS V1R11 and CICS Transaction Server (CICS TS) V4.1. Together with DataPower, this method of identity propagation supports a cross-platform, end-to-end security solution, providing for identity assertion, control, and auditing. An advantage of this approach is that the original caller's identity is not lost; it is stored as an extension to the RACF identity.

DataPower XI50z value addition: The DataPower XI50z enables close integration with RACF for sharing keys and certificates and for the propagation and mapping of user identities.

4.2.4 Message security

As mentioned earlier, encryption is sometimes done at the network transport (dynamic) level. In that case, the message flows through an encrypted transmission “pipe” but is often “in the clear” before and after it is sent (including its “at rest” state wherever it is stored). Encryption of the message data when en-route and at rest is important as well. Message security protects the data in the messages themselves. This often entails the use of message encryption to ensure privacy. Thus in certain cases, the message itself (or a certain part of it that contains sensitive data) is encrypted, and then that encrypted message is sent over an encrypted connection. Security in layers is a good thing! Another element to message security is ensuring that any message or transaction received by our systems has actually been sent by a client whom you trust and has not been modified by someone else on its way to you. These concepts are respectively called *non-repudiation* and *message integrity* and are typically enforced by use of digital signatures.

Encryption, decryption, and digital signature processing also involve the use of digital certificates and keys for Public Key Infrastructure (PKI), as do the transport security measures discussed in 4.2.1, “Network security” on page 36. PKI uses cryptographic material called *keys* and *certificates*. These are physical files which are, in essence, the keys to the kingdom regarding your security infrastructure and must be handled and managed carefully. Of course, this is another great example where not just secure products, but secure processes, are paramount in terms of reducing and managing risk.

Aside from the crypto aspects of message-level security, you must ensure that back-end systems only receive well-formed messages that do not contain malicious content. This pertains to XML, where message formation, schema validation, and XML threats[2] must be checked, but non-XML as well. In either case, any attachments such as Multipurpose Internet Mail Extension (MIME), Direct Internet Message Encapsulation (DIME), SOAP with Attachments, or Message Transmission and Optimization Mechanism (MTOM) must be virus-scanned for potential threats. Doing this with DataPower as an intermediary allows our back-end systems to run more healthy and spend their resources processing business logic and transactions, rather than in exception or error handling, or worse, in recovering from attacks.

[2] See the developerWorks article “The (XML) threat is out there...” by Bill Hines at http://www.ibm.com/developerworks/websphere/techjournal/0603_col_hines/0603_col_hines.html.

A common usage for DataPower is to provide message-level security quickly, easily, and inexpensively, without any coding. For example, with web services, DataPower automatically makes sure the messages are well-formed, schema are validated, and XML threat protection is in place (which is tunable). Message-level security often emerges as a requirement after back-end applications have been written and deployed to production. For example, if an enterprise has been told it must comply with PCI regulations to protect credit card information flowing through its system by encrypting that information, this measure can be taken with a few clicks in DataPower, as opposed to the expensive proposition of changing, retesting, and redeploying application code.

An interesting option related to DataPower and z/OS integration is the ability to pull the crypto material (keys and certificates) from z/OS. There are several possible ways to do this. DataPower acts as a z/OS Network Security Services (NSS) client to request System Authorization Facility (SAF) services from the z/OS Communications Server. This makes DataPower a logical extension of z/OS security. By taking advantage of this capability, you can avoid the need to physically place the PKI keys and certificates on the appliance; instead, you can request them dynamically from the RACF keyring, after which they can be cached in DataPower's memory. An alternative method, for cases where it is not desired to have the crypto material pushed to DataPower, is to have the appliance send the message to z/OS for the crypto operations to be performed.

DataPower XI50z value addition: In addition to standard DataPower System z key/certificate integration options, there are fewer concerns about the crypto material traveling “over the wire” and outside of it when using the DataPower XI50z from within the zEnterprise infrastructure.

4.2.5 Platform security

Often, platforms have their own risks and means of security exposure and hence risk protection. For example, the wide open nature of service-oriented architectures (SOAs) and ESB-based architectures brings inherent risk as messages travel around the bus between providers and consumers. Adoption of newer platforms such as Web 2.0 brings risks associated with cutting-edge technologies as the security model might not yet be mature.

Specific platforms such as Java Enterprise Edition and Microsoft .Net have their own security frameworks and often credential formats with which one must integrate, and often, due to the nature of SOA, must build bridges between the two. These integration points are all potential places for security gaps to occur as the technologies are often complex in the area of security and require highly skilled personnel to design and configure.

DataPower has always provided a depth and breadth of compliance with standards and also integration points for popular platforms. This is evident in the wide array of security credentials discussed in 4.2.3, “User security” on page 39, and in other features, such as integration with Microsoft .Net Windows Communication Foundation (WCF), Tivoli Access Manager, Tivoli Federated Identity Manager, Netegrity SiteMinder, and RACF.

In terms of the zEnterprise platform, this integration is advantageous because the benefits we identify throughout this section show that the integration between System z and the DataPower XI50z is easier, quicker, and more secure.

DataPower XI50z value addition: The DataPower XI50z secures the integration of services within the zEnterprise through the use of a secure layer 2 private network.

4.2.6 Last mile security

All too often, when thinking about security, we are focused on the front door to our infrastructure. We build rock-solid secure DMZs, which provide a measure of comfort in risk management. However, it is no good to lock the front door when you have left the windows and back door open[3]. Studies have cited that the majority of attacks on enterprises occur from within the corporation, so back-end security is critical as well. In the DMZ, a common mistake is to secure the connections between the clients and intermediaries in the back end but leave the connections between the intermediaries and back-end systems unencrypted or improperly configured (for example, neglecting to remove the common Certificate Authority (CA) signer certificates from the trust stores). Another DMZ mistake is to not lock down the network routing to the systems behind the DMZ, allowing for end-around attacks where intruders competely bypass the DMZ, as illustrated in the photo in Figure 4-4.

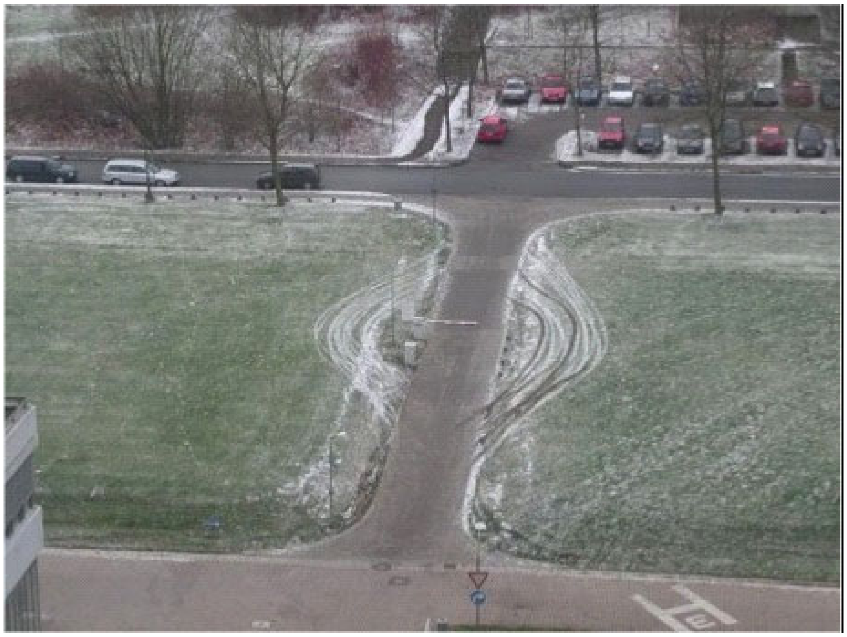

Figure 4-4 An end-around attack that bypasses the security gate

A more secure approach to this type of last-mile security is to use mutual, that is, two-way, transport encryption and even have the system components themselves provide certain means of authentication to each other, again providing security in layers.

[3] See the developerWorks article “Lookin’ out my back door” by Bill Hines at http://www.ibm.com/developerworks/websphere/techjournal/0804_col_hines/0804_col_hines.html

DataPower provides a plethora of tools to use for last-mile security. As previously discussed, there are a wide variety of choices for transport and user-level security that can be implemented to achieve this goal. The DataPower XI50z provides a critical value addition here in that if the components are all running on the zEnterprise platform, the secure IEDN can be used for communication, and hence the extra configuration for last-mile security is not as important or can be eliminated, depending on the circumstances.

DataPower XI50z value addition: The DataPower XI50z secures the “last mile” and can alleviate the need for configuration such as secondary server-to-server authentication and mutual SSL tunnels through the use of the IEDN, a secure layer 2 private network.

4.3 Resiliency risks

An important component of managing risk is ensuring availability of the critical IT infrastructure, applications, and services that your business provides to its users. As previously indicated, when systems are down, you are usually losing revenue by the minute, and incurring a damaged reputation which can cause your clients to move to a competitor. Resiliency in IT systems is typically addressed in terms of making systems highly available (HA) and redundant and having a solid and well-tested disaster recovery (DR) plan.

With HA systems and DR plans, the critical thing is in testing them carefully and frequently to ensure that they will work if and when you need them. Nobody likes to “pull the plug” during system or load testing, but this is the only way to tell if the intended failover works as expected. DR drills are costly and sometimes time-consuming to run but are the only way to validate all components and gain the peace of mind that good risk assurance brings. It is important that every dependency on highly available systems must be made highly available.For example, it does no good to make your ESB highly available if the Lightweight Directory Access Protocol (LDAP) server that it relies on for authentication is the single point of failure.

Typically, high availability is achieved by using a load balancer tier in front of each layer of the topology to spray traffic to the cluster of servers behind it. The load balancers use various algorithms to distribute load and perform health checks to remove servers that are not responding from the configuration until they become healthy again. A typical network topology for high availability is shown in Figure 4-5.

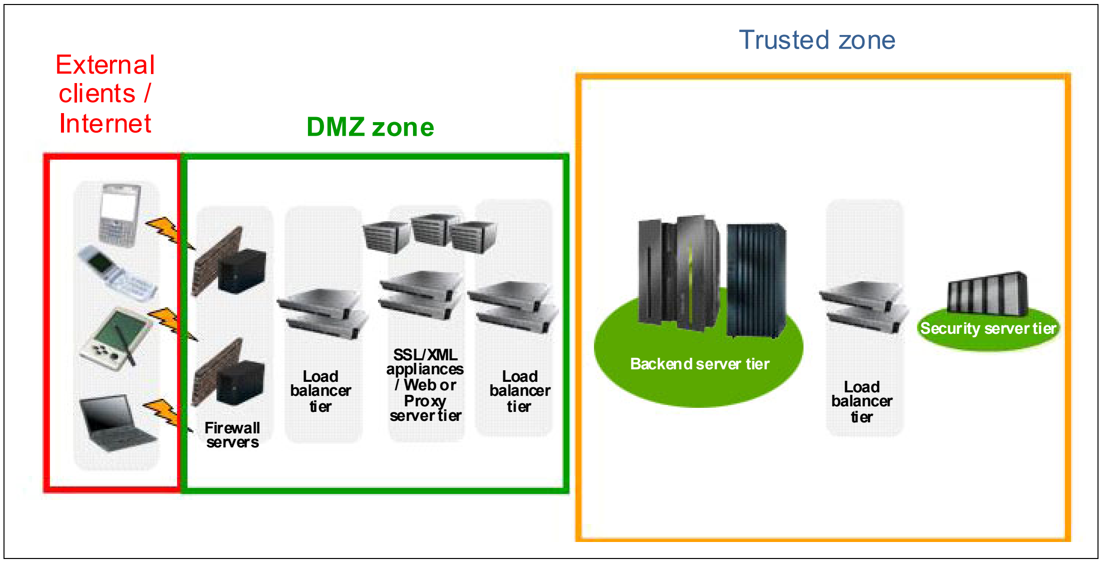

Figure 4-5 High availability network topology

DataPower has always been able to load balance to the back-end servers behind it and LDAP server groups. Using those capabilities allows one to remove the load balancer tiers from the network topology, which results in cost savings in terms of hardware maintenance, licenses, and administration. It also means a more simple, efficient, and faster network topology with fewer hops.

DataPower also has an option called *Application Optimization (AO)* that makes this back-end load balancing more intelligent, for example, by intelligently communicating with the back-end clusters to add new servers to the group dynamically, adjust to any weighting changes in the cluster, and allow group and atomic application version rollouts. AO also provides a feature called *self-balancing* that allows one to remove the load balancer tier in front of DataPower, allowing the appliances to be configured in a cluster that balances loads within itself. All of these measures provide for a much more efficient network topology in terms of administrative, hardware, and licensing costs, and performance (fewer hops) and security (simplicity), as portrayed in Figure 4-6.

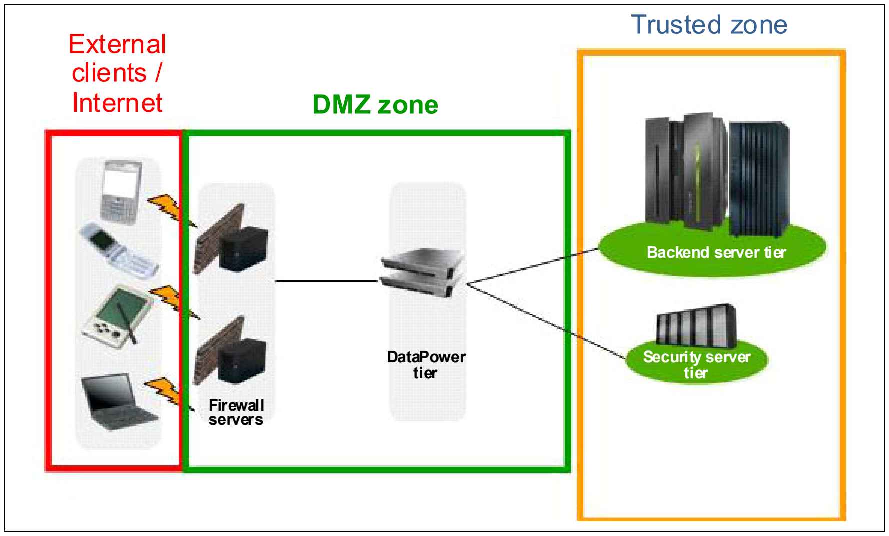

Figure 4-6 Simplified high-availability topology with DataPower providing load balancing

Of course, with the DataPower XI50z and the DMZ implemented on zEnterprise, this system can be self-enclosed, as depicted in Figure 4-2 on page 37.

In terms of the DataPower XI50z, the great news is that the AO option is included. The self-balancing feature can be used in cases such as that shown in Figure 4-2 on page 37, where the inbound traffic is coming directly into the DataPower XI50z. If the topology in Figure 4-3 on page 38 is used, where inbound traffic first comes through an LPAR, the native zEnterprise Sysplex Distributor can be used (and provide back-end load balancing by DataPower XI50z). These provide plenty of powerful options for building a highly available, resilient system.

DataPower XI50z value addition: The AO option and the Tivoli Access Manager features are both standard on the DataPower XI50z but optional for other DataPower models.

The ability to choose between AO, standard on the DataPower XI50z, and Sysplex Distributor gives you flexibility to build highly available infrastructures. You can use both the AO option and the Sysplex Distributor for both front-end and back-end load balancing,

4.4 Auditing risks

In today’s world, compliance with government and industry regulations is a much more commonplace requirement than in the past. Almost every industry sector is affected by regulations that require user privacy to be maintained. For example, Payment Card Industry (PCI) compliance for businesses that process credit card information, and various worldwide government regulations affecting medical and health care providers require such user privacy.

Complying with these regulations not only requires incorporation of the runtime application code and policies to satisfy the regulations, but also capturing the data that is required to be shown in the event of a compliance audit. It can be costly in terms of business stoppage, fines and penalties, and reputation to not have this data available and hence fail an audit. To solve the problem, IT systems must have solid auditing capabilities to capture the required logs and data.

As mentioned in 4.2.3, “User security” on page 39, the last “A” in DataPower’s AAA object stands for “Auditing.” This feature provides for auditing user and message events, such as who has executed which transaction and when. These audit events can be stored on the appliance or sent off-device using a number of formats and protocols. The appliance itself has a secure audit log to capture administrative events, such as when configurations are updated. There are auditing configuration points in several of the other integration options as well, such as WebSphere Transformation Extender (WTX) and Tivoli Access Manager (TAM).

DataPower allows log records to be transferred off-device in many formats, for example, Common Base Event, SOAP, text, and so forth, using several protocols. One possible example of audit integration between the DataPower XI50z and the rest of the subsystems on System z is to use DataPower’s syslog capabilities to merge audit records with those of the rest of the infrastructure.

> **DataPower value addition:** The auditing logs can be merged because both DataPower and System z subsystems use syslog.

5

Managing IT infrastructure complexity

This chapter describes how a centralized computing model helps to manage and reduce IT infrastructure complexity, how the zEnterprise facilitates movement towards this centralized model, and how the DataPower XI50z, as part of the zEnterprise system, helps to meet the objective of managing and reducing IT infrastructure complexity.

5.1 Centralized computing model

According to the Global Chief Information Officer Study conducted by IBM in 2009[1], three-fourths of all CIOs anticipate having a *strongly centralized infrastructure* in five years to control costs. A move towards centralized computing can be accomplished in several ways, including by consolidating the physical server and by virtualizing the logical server. Benefits might include reduction in costs associated with hardware, software, labor for administration and operations, and environmental factors, such as floor space, power, and cooling.

The zEnterprise system is an ideal solution for clients who want to move towards the goal of centralized computing. Its flexibility in supporting both traditional mainframe workloads and distributed workloads allows a variety of ways to meet this goal. Several of the ways that zEnterprise can help are by enabling server consolidation, enabling virtualization, or providing a unified systems management and monitoring platform that provides a single, integrated view of the diverse components that make up a zEnterprise ensemble.

5.2 Server consolidation

Server consolidation aims to reduce the complexities associated with server sprawl. Consolidating a larger number of underutilized servers to a smaller number of servers reduces complexity and cost in several areas:

- Reduced hardware footprint
- Reduced software licensing costs
- Simplified administration
- Reduced energy usage
- Reduced floor space requirements
- Simplified cabling infrastructure

Opportunities exist to reduce complexity and lower costs even without reducing the number of physical servers. For instance, by moving stand-alone servers to a blade configuration, even if the number of physical servers were to remain the same, most of these savings can be realized, such as reduced costs for energy, floor space, connectivity, and cabling.

5.2.1 Server consolidation with zEnterprise

Physical server consolidation is possible with the zEnterprise in a number of ways:

- Consolidation to Linux on System z: An LPAR on the zEnterprise CPC running z/VM can host multiple guests running Linux on System z.
- Consolidation to POWER7 blades in the zBX: Stand-alone POWER7 servers can be consolidated onto POWER7 blades in the zBX, reducing physical footprint and associated environmental costs. Multiple AIX operating system images can be defined on a single blade, further enhancing cost savings.
- Consolidation to x86 blades in the zBX[2]: In the future, stand-alone Linux and Windows servers will be able to be consolidated onto an x86 blade in the zBX, reducing physical footprint and associated environmental costs. Multiple operating system images will be able to be defined on a single blade, further enhancing cost savings.

[1] ”The New Voice of the CIO: Insights from the Global Chief Information Officer Study,” (CIO Study 2009), p. 25, available at `http://www-935.ibm.com/services/c-suite/series-download.html`

[2] This Statement of Direction at the time of writing this document is subject to change.

5.2.2 Server consolidation and the DataPower XI50z

The DataPower XI50z provides an opportunity to consolidate rack-mountable DataPower appliances to the BladeCenter chassis infrastructure provided by the zBX. The BladeCenter infrastructure can provide savings in energy costs, IT footprint, and cabling costs.

Tip: For existing DataPower users migrating to the DataPower XI50z from rack-mountable DataPower appliances, you might reduce the number of DataPower XI50z blades needed to handle the same workload required by a larger number of appliances. This depends on your particular workload and the particular DataPower model from which you are migrating.

The possibility to reduce the number of DataPower XI50z blades targeted to take over a workload currently running on DataPower XI50 rack-mountable appliances is dependent on your workload and the hardware family of your existing DataPower XI50 appliances. Figure 5-1 shows an example of such consolidation.

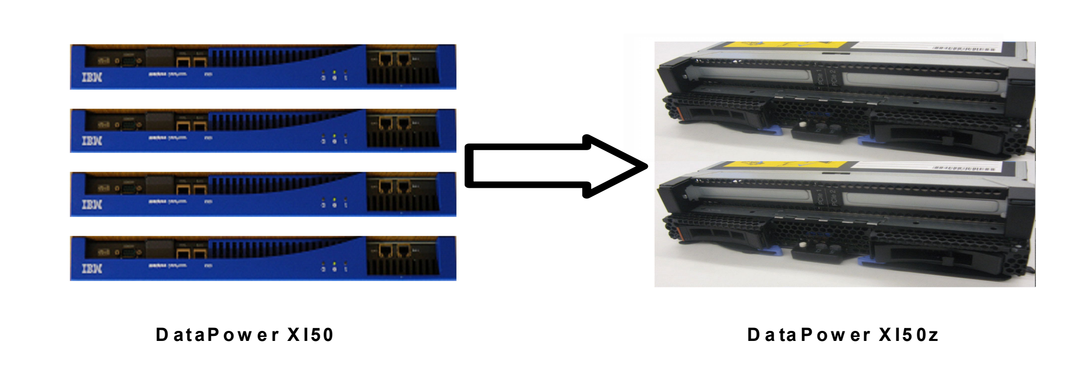

Figure 5-1 Example of a DataPower XI50 and DataPower XI50z consolidation

5.3 Virtualization

Virtualization, in IT terms, refers to a strategy that adds a layer of abstraction somewhere in the computing model. Although the term “virtualization” has become pervasive in the distributed computing world in the last several years, virtualization is a concept that has been employed for decades in IT. For example, IBM mainframes with virtual memory architectures and virtual machines implemented by the IBM VM operating system, have been commercially available since the 1970s.

In the context of moving towards a centralized computing model, virtualization today usually refers to server, desktop, storage, or network virtualization. The goal of virtualization is to make more efficient use of physical resources. Reductions in physical resources might reduce the complexity of managing them; however, the extra layer of abstraction brought about by virtualization does require administration, so it is important that virtualization solutions provide effective tools to administer the virtualized resources.

5.3.1 Virtualization with zEnterprise

zEnterprise supports virtualization in many ways at the server, networking, and storage level. The Unified Resource Manager is used to define all aspects of virtual servers, such as CPU, memory, networking, and disk storage. On the zBX, multiple virtual servers can be defined on a server blade (that is, a POWER7 blade or in the future an x86 blade). Among similar blades, for example, between two POWER7 blades, a virtual server definition can be moved from one blade to another.

5.3.2 Virtualization and the DataPower XI50z

Note that in the zBX, server blades have a hypervisor that works in conjunction with the Unified Resource Manager to allow virtualization and workload management capabilities. Although the Unified Resource Manager can manage and monitor the special purpose optimizer blades, several of the virtualization and workload management capabilities that are available for the server blades are not available with the special purpose optimizer blades because many of these capabilities are provided by the hypervisor, which the special purpose optimizer blades lack.

Despite this limitation, the DataPower XI50z still participates in the virtualization story in at least a couple of ways.For example, it supports service virtualization and network virtualization.

5.3.3 DataPower XI50z service virtualization

Service virtualization refers to the capability of the DataPower XI50z to provide a front-end proxy for the calling client so that the details of the service implementation are hidden from the client. This service virtualization provides simplicity and security. The calling client has the benefit of simplicity as the client is shielded from changes in the location of the back-end service implementation. This change is made in the DataPower XI50z configuration, which is transparent to the client. The back-end service implementation gains security in that its location details are not exposed to the client, providing less of a target to hackers.

5.3.4 DataPower XI50z and network virtualization

The DataPower XI50z participates in the network virtualization functionality of the zEnterprise. The zEnterprise provides a secure, private data network called the *intra-ensemble data network (IEDN)*. All routes within this network are virtualized through *virtual LANs (VLANs)* that are defined using Unified Resource Manager and are fully contained within the IEDN.

zEnterprise resources, such as virtual servers, switch ports, and optimizer blades, DataPower XI50z included, are given access by the administrator to only those VLANs that it requires. The Unified Resource Manager restricts traffic to those VLANs authorized for that resource. A zEnterprise ensemble can have a large number of VLANs defined for it for usage across a number of workloads, but for any particular DataPower XI50z blade, it can be given access only to that subset of the VLANs that it needed.

5.4 Systems management and monitoring

In the typical modern data center, with its heterogeneous mix of hardware platforms, operating systems, and middleware, multiple tools are required to manage, monitor, and troubleshoot the various systems. Troubleshooting problems in a transaction that flows across numerous disparate platforms can often be difficult. Isolating the true source of the problem can be difficult. You need to use multiple tools, each usually providing only a partial view of the end-to-end flow.

Moving from a heterogeneous sprawl towards a more consolidated, centralized model can reduce the number of several IT infrastructure components, and thus the number of administrative and monitoring software suites required to manage the IT infrastructure.

Although reducing the number of IT infrastructure components is a desirable goal, it is a rare case where consolidation to a single, homogenous platform is possible. Therefore, systems management and monitoring software that can manage multiple hardware platforms is a desirable component of a solution to reduce and manage IT infrastructure complexity.

5.5 Unified Resource Manager

zEnterprise uses the Unified Resource Manager to manage and monitor physical blades, virtual servers, and workloads. For monitoring at the service level, traditional tools such as Tivoli’s ITM and ITCAM suites are recommended. See 7.4.2, “IBM Tivoli Monitoring” on page 64 for an example of Tivoli service monitoring implementation.

The zEnterprise Unified Resource Manager dramatically simplifies operations across multiple application environments. The Unified Resource Manager provides energy monitoring and management, goal-oriented policy management, increased security, virtual networking, and information management, all consolidated into a single, easy-to-use interface firmly grounded in real-world business requirements.

The Unified Resource Manager is firmware that manages the integration of multiple platform resources as a single virtualized system and provides a single point of control for zEnterprise. The Unified Resource Manager allows clients to inspect, report on, and manage all connected resources and automate their deployment. The Unified Resource Manager allows the definition of prioritized workload goals and automation to align with meeting these goals. For example, Unified Resource Manager can dynamically adjust the allocation of processor capacity in individual hypervisors to balance the allocation of processing capacity across the virtual guests hosted by that hypervisors.

The benefits of the network virtualization functionality provided by Unified Resource Manager were introduced in 5.3.4, “DataPower XI50z and network virtualization” on page 50. It is worth noting that the access control provided by this VLAN provisioning does not require external client-managed switches or routers. This helps to reduce the need for firewalls and encryption, simplifying network configuration and management, and providing full redundancy for high availability. The management of the network provides enforcement of strict access control across heterogeneous environments, further augmenting security and simplicity.

5.5.1 Unified Resource Manager administration of DataPower XI50z

The Unified Resource Manager aids in simplifying administration and monitoring of the DataPower XI50z.

During the initial setup of a DataPower XI50z, several tasks that need to be performed manually on other DataPower products, are performed automatically by Unified Resource Manager:

- Setting the device to disaster recovery mode to enable secure backup and restore functionality
- Initializing the device's RAID-1 hard disk array
- Enabling the Web Management Interface

Several tasks are now performed manually using the Unified Resource Manager, rather than using traditional DataPower interfaces:

- Network configuration
- Firmware updates
- Device shutdown
- Device start
- Secure restore

> **DataPower XI50z value addition:** The DataPower XI50z benefits from the integrated firmware management provided by the Unified Resource Manager. Firmware updates to the DataPower XI50z are downloaded to the zEnterprise ensemble, at which time the updates are available to all DataPower XI50z's in the ensemble. The administrator chooses when to install the firmware on each individual blade, allowing an orderly migration of updates, for example, from the development, to test, to production dedicated DataPower XI50z.

5.5.2 Unified Resource Manager problem detection for DataPower XI50z

The Unified Resource Manager aids in problem detection, reporting, and resolution. The DataPower XI50z benefits from this integration in the area of reliability, availability, and serviceability (RAS):

- If the Unified Resource Manager detects a problem with the DataPower XI50z, it will automatically "call home" to report the problem to IBM.
- If a service visit by IBM is necessary, the DataPower XI50z is warranted under the terms of the zBX in which it resides. Quite often this will mean 24x7 support.
- Unlike any of the rack-mountable DataPower appliances, **all** parts on the DataPower XI50z are Field-Replaceable Units (FRU) serviced by an IBM Service Support Rep (SSR).

The Unified Resource Manager allows you to assign the DataPower XI50z devices to logical groups, making it possible for group operations such as start and shutdown to be performed on multiple devices simultaneously.

> **Note:** Even when performing operations on individual DataPower devices, being able to display a logical group consisting of multiple DataPower devices spread over several BladeCenter chassis in a node, or over several nodes in an ensemble, offers the convenience of having all of the devices in the group listed together in the Unified Resource Manager GUI.

6

Reducing IT costs

Smarter computing aims to address the two critical challenges faced by IT organizations: lowering costs and enabling innovation.

In Chapter 5, “Managing IT infrastructure complexity” on page 47, we described how a centralized computing model with zEnterprise can reduce complexity and save costs. In this section, we look at how service-oriented architecture (SOA) appliances in general, and the DataPower XI50z specifically, can also play a part in reducing IT costs. First, we introduce the concept of “workload-optimized systems,” which is an approach to improve efficiency and reduce costs by deploying workloads on the most appropriate platforms and by exploiting specialized processors for specific tasks.

6.1 Workload-optimized systems

One common question is “On what platform should I run my workload?” This question can be either generic in nature or can be specific to an existing workload. The relative technical fit of a workload and a platform (along with other factors) will impact the amount of capacity needed to be deployed and ultimately the cost of running that workload.

It is the view of IBM that no size fits all, that is, no single platform is the best fit for all types of workload. Therefore, a workload is most likely to be best deployed within a heterogeneous infrastructure which is made up of multiple platforms and architectures. It is normally composed of other types of components, often including traditional COBOL applications and newer Java components typically accessed as web services and frequently encrypted or secured in other ways.

When considering where a workload should run, or more likely, where specific applications of a workload should run, we need to take account of the workload characteristics of the application, that is, whether the application is single- or multi-threaded, whether or not it uses shared data, what degree of parallelism is required, and so on. In the SOA world, it is usual for a specific service to be used in multiple applications, and therefore we might be making best fit decisions for services, or specific service processing, rather than the applications themselves.

An appliance has a specific purpose in workload-optimized systems: it is dedicated to the role of optimizing a particular type of processing such as database queries, or in the case of an SOA appliance, service-related processing such as XML acceleration, security, or enterprise service bus (ESB) functions. The appliance does this for all workloads that have a need for this specific type of processing.

6.2 Using an SOA appliance to reduce IT costs

IT economics can be improved by making the appropriate best-fit decisions for workload deployment, and appliances can play an important role in reducing IT costs. In particular, using an SOA appliance as an SOA gateway or an ESB can help to reduce software and labor costs.

An appliance can be used to offload expensive operations by processing the complex part of XML messages (such as a digital signature). Other operations like encryption, parsing of long or complex XML messages, and XML schema validation are also expensive operations and can benefit from the optimized processors of an appliance. The appliance frees up the general processors for other workloads.

Note: The DataPower XI50z can be used as an optimizer for expensive security and XML processing so that valuable System z resources are freed up for other work.

Following the fit-for-purpose approach, performing these operations in an appliance means that we might avoid the software and licensing costs that are otherwise incurred if these operations were performed in a software-based system.

Note: The DataPower XI50z might reduce software costs compared to other ESB solutions by performing processing that are included in software licensing charges.

An appliance is typically easy to configure and allows solutions to be “dropped in” quickly, saving time and labor costs. Figure 6-1 shows the configuration differences between an appliance and a typical software-based ESB.

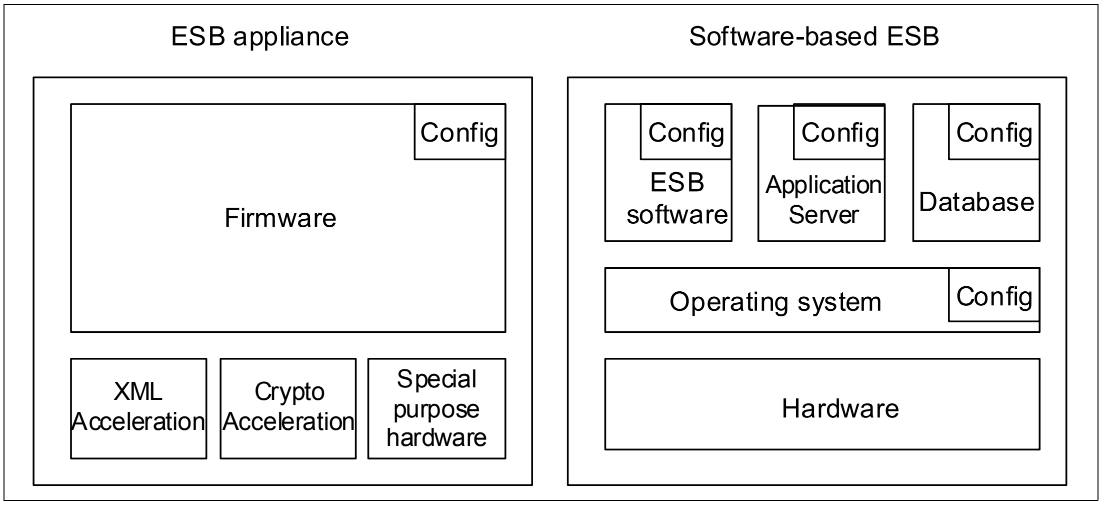

Figure 6-1 How an appliance saves labor costs

An ESB appliance can save labor costs by providing one configuration point and no programming. However, a software-based ESB typically has broader reach through a full programming model, but with a wider set of configuration points.

Note: The DataPower XI50z might reduce labor costs compared to other ESB solutions by minimizing configuration and administration costs.

6.3 Using DataPower XI50z to reduce zEnterprise CPC processing cycles

In 3.2.1, “Integration use cases” on page 28, we saw that a popular deployment pattern for the DataPower XI50z is to service-enable traditional mainframe applications. In addition to the business flexibility benefits of service enablement, such enablement can also offer cost benefits by reducing processing cycles on the zEnterprise CPC and the associated software licensing costs.

Figure 6-2 shows two ways to service-enable a System z application for the case in which the SOAP request message must be encrypted using XML encryption. In the first scenario, the encrypted XML is processed by the z/OS subsystem, which incurs expensive XML processing. In the second SOA gateway scenario, the DataPower XI50z decrypts the XML before calling the System z application, offloading expensive processing from the mainframe.

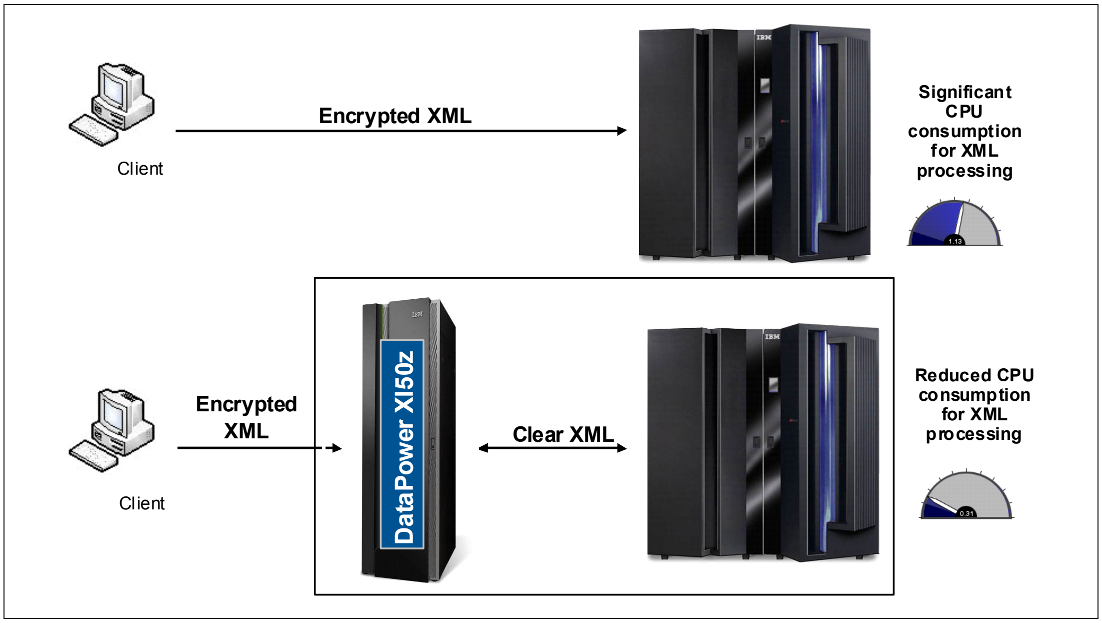
Client
Encrypted XML
Significant CPU consumption for XML processing
1.13
Client
Encrypted XML
DataPower XI50z
Clear XML
Reduced CPU consumption for XML processing
0.31

Figure 6-2 How DataPower XI50z saves software costs

Note: In Figure 6-2, the fuel gauges are shown for illustrative purposes and are not meant to imply a specific performance advantage or guarantee. Every workload has separate characteristics.

In the second scenario, XML is still being processed on System z using one of the efficient XML parser technologies; however, the high processor-intensive XML decryption processing is being done by DataPower, which is a specialized processor that is optimized for such processing. Other types of processing that are appropriate for this pattern include:

- XML signature processing: An XML digital signature applies integrity to a message to ensure that no one illegally modifies the message at the same time as it is in transit, and the signature can also be used for non-repudiation when legal proof is required that the sender did actually send the message.
- XML schema validation: By default, schema validation is enabled in DataPower.
- XML parsing and transformation of large messages: The processing cost of an XML message is dependent on the length and complexity of the message. For long and complex messages, it can be more efficient to transform the message to a non-XML format in the DataPower XI50z and pass the appropriate format message (for example, COBOL binary data) to the target system in a Message Transmission and Optimization Mechanism (MTOM) attachment or as a message over WebSphere MQ.

  The DataPower XI50z can perform a variety of separate transformations:

  - XML to XML
  - XML to non-XML
  - non-XML to XML
  - non-XML to non-XML

6.4 DataPower XI50z TCA considerations

In order to understand the true economic benefits of one solution over another, we need to understand the true cost of delivering the workload deployed within the separate target infrastructures. Often, when people compare the cost of deployment options, they limit the comparison to the cost of hardware acquisition. This can be quite misleading. It is important to consider all of the key elements of cost.

For a total cost of acquisition (TCA) calculation, the separate elements of cost include software acquisition costs, software support and subscription costs, hardware maintenance costs, and so forth, in addition to the base hardware acquisition costs. A Total Cost of Ownership (TCO) calculation is broader still and includes many other relevant elements of cost, such as administration and labor costs, systems management costs, power and cooling costs, facilities costs, refresh costs, and so forth.

Figure 6-3 on page 58 shows an IBM case study comparing the TCA for two separate ESB solutions:

- Eleven ESB servers running a vendor software ESB solution on Intel servers, each with four sockets, 32 cores, and 128 GB of memory
- One DataPower XI50z

The test consists of measuring maximum throughput of each ESB solution and performing a variety of message mediation workloads, including pass-through, routing, transformation, and XML schema validation.

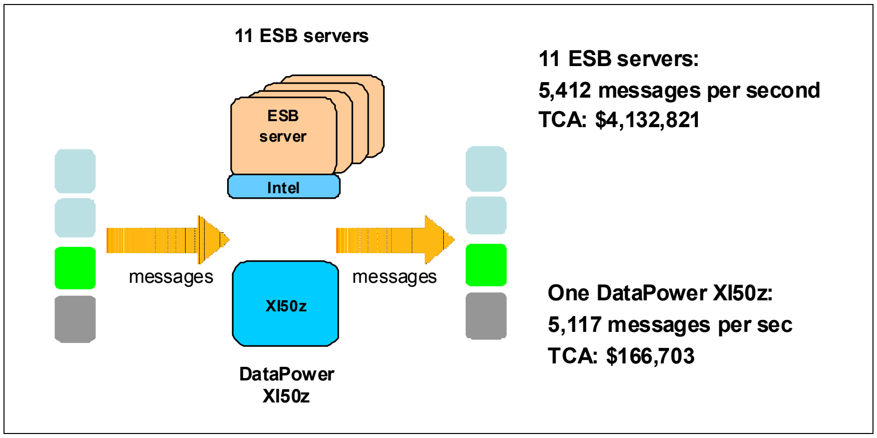

Figure 6-3 How DataPower XI50z saves acquisition costs

This comparative test shows that the TCA for the DataPower XI50z solution is significantly less than the vendor software-based ESB solution. The costs included in the study include hardware[1] and software costs, licenses, and support for a three-year period, but did not take into account power, floor space, or labor costs.

Note: The DataPower XI50z TCA shown in Figure 6-3 includes the cost of a single (double-width) blade; however, for high availability, we recommend a minimum of two blades.

Clearly, results vary based on customer workload characteristics, and costs also vary by country. However, this TCA study shows how using the DataPower XI50z can significantly reduce IT costs for an ESB workload.

[1] The DataPower XI50z hardware cost includes a prorated share of the cost of a zBX.

7

Banking case study

In this chapter, we review a case study based on a DataPower XI50z implementation within a banking infrastructure.

Many banks have embarked on a core banking transformation strategy to gain flexibility and reduce cost. A service-oriented architecture (SOA) is normally the preferred architecture because it facilitates maximum reuse of existing assets.

CICS applications are among the most valuable assets of many large companies, particularly in the financial sector. Without these COBOL and PL/I programs, many banks cannot do business. Reusing these proven assets can result in delivering new business processes much more quickly, and it is significantly less expensive to reuse existing applications than to write new ones.

This chapter looks at the example of a bank that wants to extend several of its CICS core banking services, such as account transfers and posting inquiries, to internal distributed systems and selected business partners. We review how the implementation of the DataPower XI50z improves the bank’s business agility, reduces IT costs, minimizes risk and simplifies IT complexity.

7.1 Improving business agility

CICS applications can be exposed as services with well-defined interfaces.Such services enable loose coupling, providing the necessary flexibility to build composite applications, thereby improving interoperability and reuse.

Web services can be used to enable integration based on a common set of standards covering message format, protocol, and security.

An SOA gateway or an ESB pattern provides the greatest flexibility, providing the ideal location for functions such as data transformation, protocol switching, and enforcement of security policy. The DataPower XI50z provides these capabilities with an ease of use and performance that is unmatched by other ESB solutions. Figure 7-1 shows the bank's chosen deployment pattern for the DataPower XI50z.

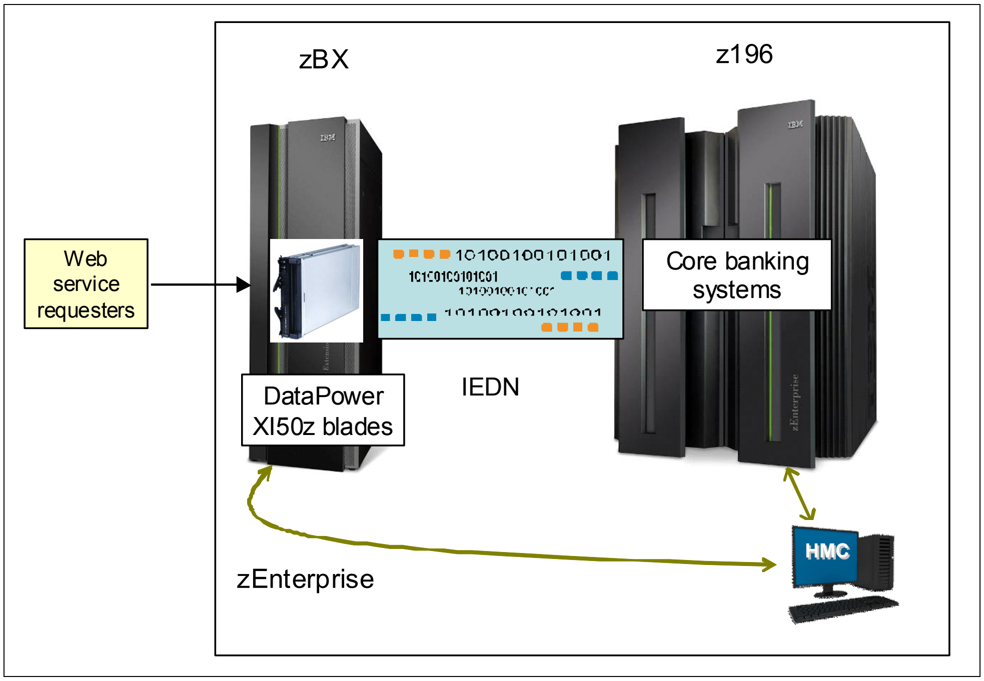

Figure 7-1 Using DataPower XI50z to service enable core banking systems

DataPower XI50z value: The DataPower XI50z is an ideal choice for an SOA gateway or ESB when the target services are traditional z/OS assets such as CICS and IMS applications, data residing in DB2 for z/OS, or other services deployed on virtual servers within the zBX.

Deploying the DataPower XI50z as part of the bank's ESB infrastructure means that DataPower functionality can now be used for internal zEnterprise integration, for example, if there is a need for XML transformation or web services security processing for service interactions between certain applications running on the zEnterprise. These service interactions then benefit from the fast secure intraensemble data network (IEDN) connecting the virtual servers within the ensemble.

7.2 Reducing IT costs

Deploying the DataPower XI50z in this way fits well with the bank's strategy to deploy certain components of workloads on the “best fit” platform. DataPower is a clear best fit for heavy XML processing and security functions. This fit is optimal for the following reasons:

- When DataPower is used to parse the SOAP body of very large messages, the bank's tests show that this reduces the processing cost in CICS by up to 75%.
- Using DataPower to validate XML signatures is shown to be more than five times more efficient than a software-based solution.

Using the DataPower XI50z as an optimizer in this way frees up resources for other processing such as transactional, data access, and business logic.

Note: The DataPower XI50z fits well with the bank's strategy to deploy certain components of workloads on the “best fit” platform.

In addition, performing such processing in a special-purpose optimized blade has additional benefits for the bank in lowering power consumption, reducing overall cost, and improving scalability. Perhaps the major cost saving associated with this approach is the savings associated with the reuse of existing core banking functions, compared with the cost of replacing these functions with new packages or custom-built solutions.

7.3 Minimizing risks

Deploying the DataPower XI50z minimizes the bank’s risks in the following ways:

- It enables tight integration between the bank’s security domains and user registries, minimizing the risk of unauthorized access to the core banking systems.
- It minimizes the risk of outage by benefiting from the unparalleled availability and workload management capabilities of zEnterprise.

7.3.1 End-to-end security

The bank has to prepare for more stringent compliance regulations which dictate that all service invocations must be audited and that the originating user's identity must be included in the audited record. The current security model does not fulfill this requirement because when the distributed identity is mapped to a Resource Access Control Facility (RACF) user ID, the originating user's identity is lost.

New identity propagation support available with DataPower V3.8.1, CICS TS V4.1, and z/OS V1.11 solves the bank's security challenge. Figure 7-2 shows how the bank addresses the end-to-end security challenge.

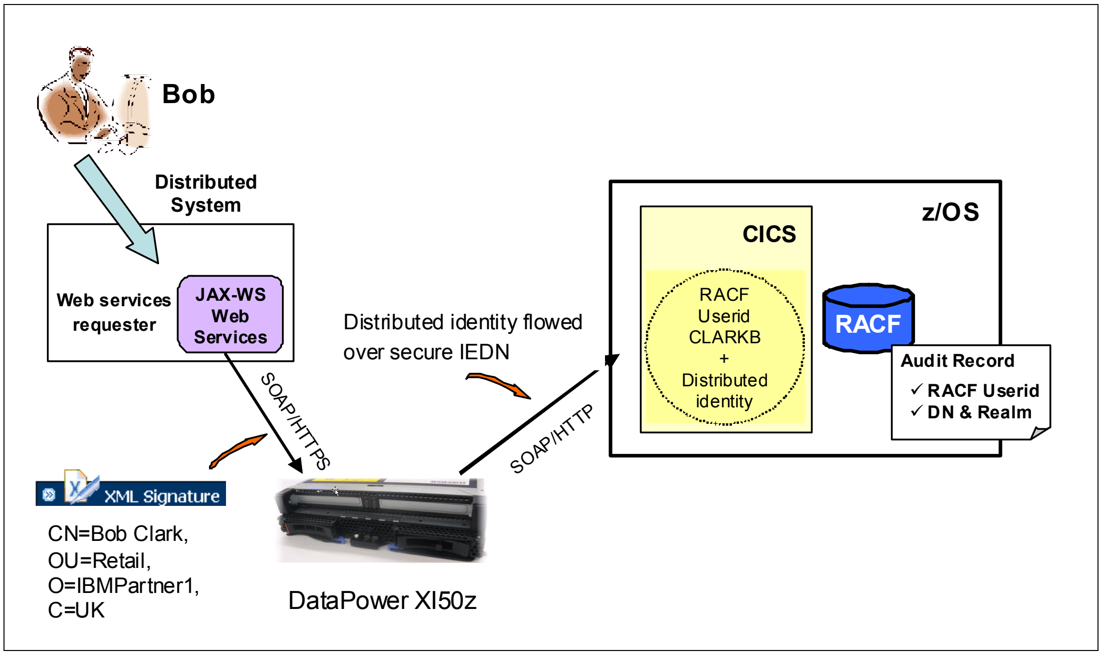

Figure 7-2 Using DataPower XI50z to integrate with RACF

The DataPower XI50z authenticates the credentials supplied by the client and maps them to a z/OS-specific identity token which contains the distributed identity of the user. The request is then forwarded to CICS over the secure IEDN, and CICS passes the token to RACF so the client's identity can be mapped to a RACF user ID. The advantage of this solution is that the original caller's identity is not lost; it is stored as an extension to the RACF identity.

DataPower XI50z value: The additional security of the IEDN means that the bank does not need to encrypt the messages that are passed between the DataPower blades and the CICS core banking systems.

7.3.2 High availability

The bank uses Sysplex Distributor to intelligently distribute TCP/IP connection requests across the separate z/OS partitions that host the core banking systems. The bank chooses to also use Sysplex Distributor to distribute requests across the DataPower blades within the zBX, shown in Figure 7-3. This simplifies workload management and improves availability. It also allows the bank to remove the external workload distribution appliances that have been used previous to this solution

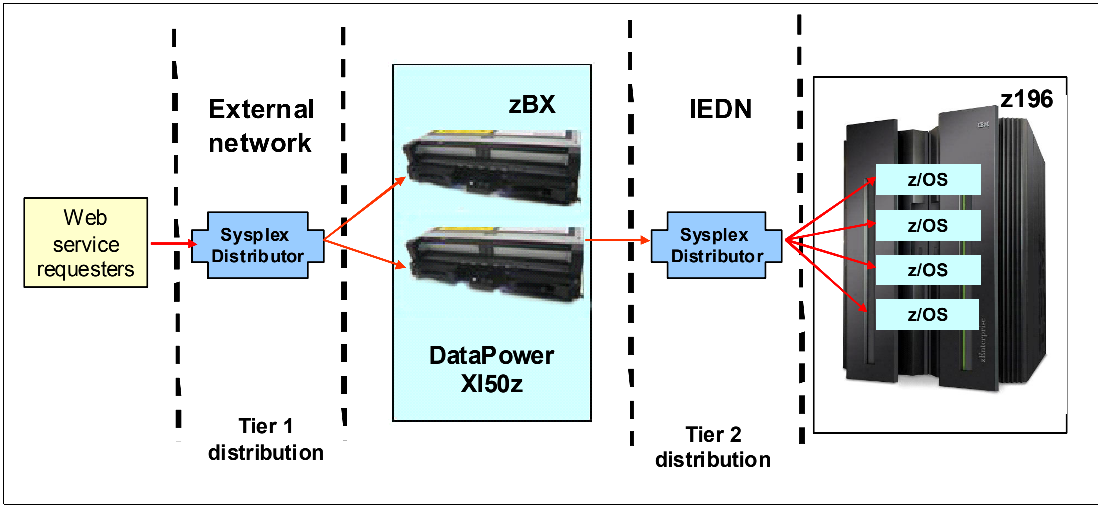

Figure 7-3 DataPower XI50z within the IBM Tivoli Monitoring infrastructure

7.4 Managing IT complexity

The choice of the DataPower XI50z also fits with the bank's aim to minimize infrastructure management by managing several platforms in a consistent way.

7.4.1 Unified Resource Manager

The zEnterprise Unified Resource Manager simplifies the bank’s platform management by providing a single operations console. It also does these things:

- Monitors the health and energy consumption of the DataPower XI50z blade.
- Consolidates error logging across the ensemble which consists of the DataPower XI50z blade and all resources (z196 and zBX components) that are part of the workload.
- Simplifies problem determination by providing “call home” support for current or expected problems.

7.4.2 IBM Tivoli Monitoring

The bank has extended its existing IBM Tivoli Monitoring infrastructure, which provides the enterprise infrastructure dashboard through the IBM Tivoli Enterprise Portal, as shown in Figure 7-4.

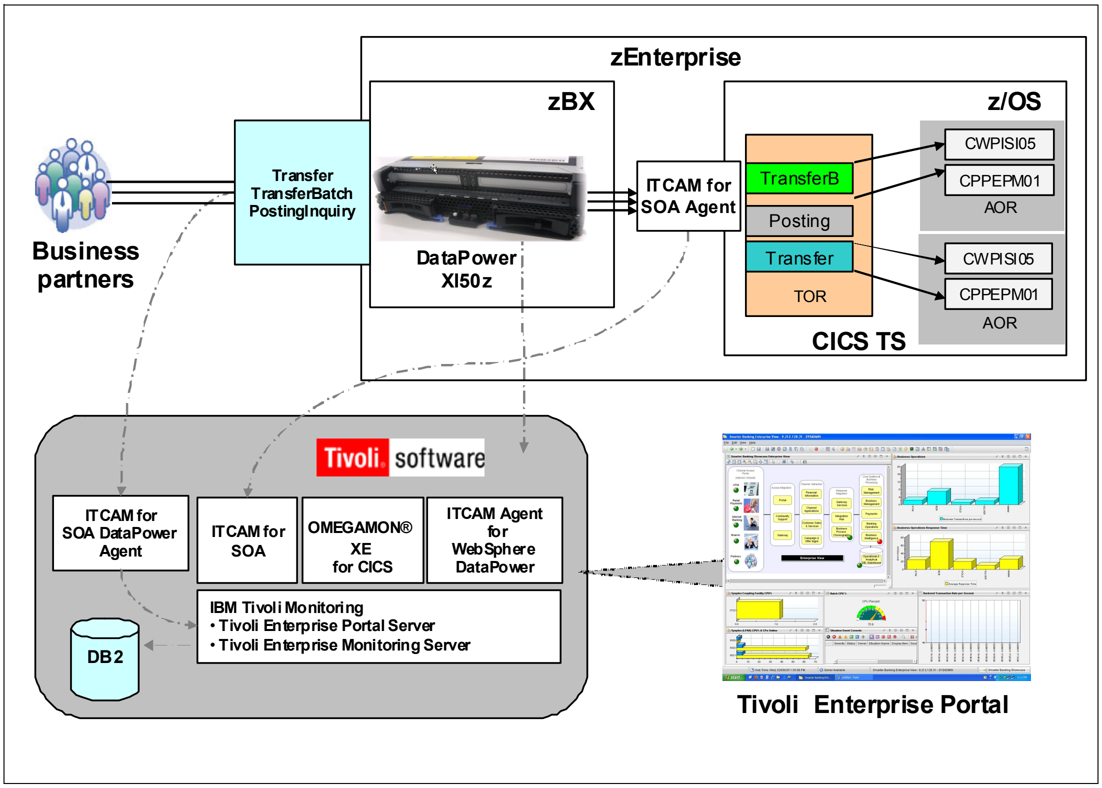

Figure 7-4 DataPower XI50z within the IBM Tivoli Monitoring infrastructure

This configuration functions in the following ways:

- IBM Tivoli Composite Application Manager Agent for WebSphere DataPower Appliance is used to perform detailed monitoring of DataPower.
- IBM Tivoli OMEGAMON® XE for CICS is used for detailed analysis of web services in CICS, including tracking against service response-time goals.
- IBM Tivoli Composite Application Manager for SOA is used to monitor the end-to-end performance of the web services across both the CICS and DataPower runtime environments.

This case study is based on the IBM Smarter Banking™ Showcase. To obtain more about how the DataPower XI50z is used within the showcase, contact your IBM representative or visit this link:

http://ibm.com/redbooks/residencies.html

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

You can search for, view, download, or order these documents and other Redbooks, Redpapers, web documents, and draft materials at the following website:

`http://www.redbooks.ibm.com/`

For all IBM Redbook publications containing content related to IBM WebSphere DataPower, use the following link:

`http://www.redbooks.ibm.com/cgi-bin/searchsite.cgi?query=DataPower`

Other publications

These publications are also relevant as further information sources:

- *IBM WebSphere DataPower SOA Appliance Handbook*, ISBN 978-0-13-714819-6
- White paper *Integrate Banking Services with IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise*

  `http://public.dhe.ibm.com/common/ssi/ecm/en/zsw03184usen/ZSW03184USEN.PDF`

Online resources

For additional information about the DataPower XI50z, start with the following website:

`http://www-01.ibm.com/software/integration/datapower/xi50z/index.html`

For more information about DataPower in general (not specific to the XI50z), you might want to start with the following resources:

- IBM main website

  `http://www.ibm.com/software/integration/datapower/`

- IBM Redbooks (search on “DataPower”)

  `http://www.redbooks.ibm.com`

- IBM developerWorks articles (search on “DataPower”)

  http://www.ibm.com/developerworks/

  See these developerWorks articles in particular:

  – *The (XML) threat is out there...*

    http://www.ibm.com/developerworks/websphere/techjournal/0603_col_hines/0603_col_hines.html

  – *Lookin’ out my back door*

    http://www.ibm.com/developerworks/websphere/techjournal/0804_col_hines/0804_col_hines.html

Other resources we used for this Redpaper:

- *The Essential CIO, Insights from the Global Chief Information Officer Study*

  http://www-935.ibm.com/services/c-suite/cio/study.html

- *The New Voice of the CIO: Insights from the Global Chief Information Officer Study,* (CIO Study 2009)

  http://www-935.ibm.com/services/c-suite/series-download.html

- *Five Reasons To Choose IBM zEnterprise Mainframe*

  http://www.forrester.com

- Center for Internet Security

  http://cisecurity.org

- IBM Smarter Banking Showcase

  http://www.ibm.com/systems/z/solutions/banking.html

Help from IBM

- IBM support and downloads

  http://ibm.com/support

- IBM Global Services

  http://ibm.com/services

Simplifying Integration with IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise

Redpaper™

Integration challenges

DataPower XI50z value proposition

Architecture patterns and case study

This IBM Redpaper publication illustrates how the IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise provides a secure, fast, cost-effective, easy-to-manage, all-in-one enterprise application integration solution. On top of all the benefits that the DataPower XI50 and XI52 already provide, incorporating the DataPower XI50z into zEnterprise also provides a number of additional benefits:

- Exploitation of the high speed intraensemble data network (IEDN) connecting the zEnterprise Blade Extension (zBX) with the zEnterprise central processor complex (CPC), either a zEnterprise 196 (z196) or zEnterprise 114 (z114)
- Secure incorporation of the DataPower XI50z appliance into a virtual local area network (VLAN) on the zBX
- Unified management of the DataPower XI50z, along with other blades and optimizers using a common management tool
- A centralized computing model, resulting in more efficient use of floor space, lower energy costs, and a lower total cost of ownership (TCO)

The DataPower XI50z provides a variety of powerful integration scenarios specifically for mainframe legacy applications, making it a natural choice to include the appliance in your centralized zEnterprise server.

This publication is intended for potential and actual users of the DataPower XI50z.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

REDP-4783-00