



CUSTOMER TESTIMONIAL

CISCO IT DEPARTMENT DEPLOYS INNOVATIVE CISCO APPLICATION-ORIENTED NETWORKING SOLUTION

EXECUTIVE SUMMARY

CUSTOMER NAME

- Cisco IT

INDUSTRY

- Networking

BUSINESS CHALLENGE

- Consolidate disparate B2B and Web-hosted environments
- Reduce the significant infrastructure, maintenance, and development costs of hosting disparate environments
- Eliminate inconsistent implementation of application-level security policy

NETWORK SOLUTION

- Cisco Application-Oriented Networking products provide intelligent network-based infrastructure services. Embedding these services in the network fabric enables applications to communicate more effectively and to extend information resources transparently across the extended enterprise.

BUSINESS VALUE

- Lowered capital and operating costs by unifying functions in the network
- Greater application-level security by using enforceable enterprise policy
- Dramatically increased visibility into business activities and infrastructure events

Visionary Technology Provides New Model for Application Infrastructure Services

BACKGROUND

The mission of the Cisco Systems® business-to-business (B2B) operation is to become “the easiest company to do e-business with.” To further this mission, Cisco® is in the process of deploying Cisco Application-Oriented Networking (AON), the first and only network-embedded intelligent message routing system that enables applications and the network to work together as an integrated system.

CHALLENGE

The Cisco IT department manages a mix of dissimilar hosted environments that thousands of customers, partners, and suppliers use to interact with Cisco. Customers order products or search for information on these sites, and partners and suppliers purchase products, check order status, manage inventory, and track the fulfillment of orders. These environments evolved over the years and reflect the various technologies in use at the time and the particular needs of each Cisco business unit (Figure 1). Some also had to be designed for compatibility with the particular needs and technologies of various partners.

As part of a new initiative to become a “process-driven enterprise” that would enable Cisco to deploy new business initiatives more quickly, Cisco committed itself a few years ago to building a Service-Oriented Architecture (SOA). An SOA is based on a technology model in which business functions are organized as a collection of services, each with a clear business identity and strict formal interfaces. This model differs from earlier methodologies that relied on custom development and proprietary interfaces and were, therefore, largely inflexible and difficult to change.

To implement an SOA approach, Cisco deployed new integration technologies in each of its hosted environments including Enterprise Application Integration (EAI) tools and Web services based on Extensible Markup Language (XML) and the Standard Object Access Protocol (SOAP) standard.

Although these technologies helped overcome earlier challenges by bridging incompatible

application protocols in each environment, each was implemented in isolation using disparate tools to manage and secure these services. The result has been a patchwork of integration technologies that have been costly to maintain and difficult to manage without a consistent, standardized way to implement, manage, and secure services across all of the environments.

The maze of patchwork technologies is especially difficult in a B2B situation when, for example, a Cisco executive wants to see a complete view of all transactions between Cisco and a particular customer. To gain this perspective, a Cisco analyst must access each environment using different tools and processes, download the necessary information, and then combine this into a meaningful report. This process could take days to accomplish and still might not capture all the relevant information.

These challenges not only affect Cisco internally; they also affect how Cisco and its external suppliers and partners transact business. In the B2B environment, for instance, customers must obtain multiple certifications for each Cisco environment in which they interoperate. They also require a range of technologies to maintain compatibility with each environment.

APPLICATION-LEVEL SECURITY IS VULNERABLE

Cisco, in turn, faces difficulty trying to integrate its suppliers and partners in the B2B environment into its enterprise systems. Security is a primary concern. Although Cisco maintains stringent *connectivity* security in its DMZ—a specially secured area that is maintained outside the enterprise firewall, application-level security is provided by the individual applications. As a result, application-level transactions are a potential security hole because application security can only be applied deep within the enterprise at the application server layer.

What's more, application-level security is currently the responsibility of each programmer, a significant vulnerability because different programmers might implement security incorrectly or not all. No universal mechanism exists to ensure that security features in the applications are applied consistently and accurately.

“Ultimately, you don't want security to be in the hands of each developer,” said Brook Schoenfield, senior security architect with the Cisco Security Program Office (CSPO), “because you can't enforce it consistently. If a programmer implements security incorrectly, it leaves a hole. Also, security at the application layer slows application performance.

“Security should be part of the infrastructure, which would make it easy for the developer to get the security he or she needs. Our goal is ‘security for the developers, not by developers.’ ”

CISCO AON SOLUTION

Cisco plans to deploy AON devices throughout its various hosted environments in three phases as follows:

- **Phase 1 (internal implementation)**—Provide Web services security and management, and AON will provide common security mechanisms within the internal hosted environments.
- **Phase 2 (external implementation)**—Provide security and management for external-facing Web services. Also, additional Cisco AON management and security capabilities will be deployed.
- **Phase 3 (external implementation)**—Install an intelligent message-level router that complements B2B gateways to provide visibility into customer transactions (Table 1).

When it performs Web services security in Phase 1, Cisco AON will manage such functions as digital signature verification, Secure Sockets Layer (SSL) termination, content inspection, message-based routing, and transaction logging. During Phase 2, Cisco AON will be deployed externally to secure and manage external-facing Web services. Along with the features in Phase 1, Cisco AON will perform protocol translation, message-level encryption and decryption, and service versioning. Today, to perform all of these security functions requires different tools, languages, and capabilities in each hosted environment.

“Our implementation of Web services security and management today is very human-resource-intensive,” said Hicham Tout, system architect in the Internet Technology Group at Cisco. “The disparity of tools and technologies required to perform all of these features across various environments requires significant overhead and administration.”

Cisco AON will provide Cisco IT a central, network-based device that will provide a standards-based approach for performing all of the above functions consistently.

WEB SERVICES MANAGEMENT: MESSAGE INSPECTION AND ROUTING

Much as it is standardizing Web services security, Cisco IT also plans to use Cisco AON to standardize Web services management tasks that include content inspection and content-based routing. Today, the applications perform these tasks. If an order status request comes in, for example, the application checks the header of the request, determines that it is an order status request, and then routes it to the back-end Oracle application server, if that is the indicated destination. To provide this intelligence, however, requires a programmer to code the logic manually into the application. Unfortunately, each application handles this content routing differently, requiring specialty programmers who understand how to program in each application environment.

The goal with Cisco AON is that it will act as a smart router that sits ahead of all application environments and receives these requests based on specific rules: both business and security or infrastructure rules. It will then extract the message, perform validations and transformations, and then route the message to the proper destination.

“If we can make this a standard flow, and have Cisco AON enforce certain templates, we could ensure that before the message even reaches the endpoint—the application—we have performed all of these functions without the application even knowing that they were done,” said Tout.

“From a security perspective, it provides an additional layer of protection. We’d be enforcing security much earlier in the network, in the DMZ before the firewall, way before the messages entered the enterprise and reached the applications.”

The other benefit of this approach, as mentioned previously, is that security is taken out of the hands of programmers. With Cisco AON, it becomes a security device in the network that cannot be circumvented.

PHASE 3: B2B FOR VISIBILITY

In the third phase, Cisco IT plans to create a B2B *virtual gateway* through which outside traffic will pass. Cisco AON devices will sit in front of B2B gateways and perform all Web services security and management functions safely in the DMZ: authenticating, encrypting, and decrypting messages and routing them to the proper back-end system for processing. In addition to much more stringent application-level security, this virtual gateway will provide Cisco management with full visibility into B2B transactions with customers.

SERVICES OF CISCO AON

Cisco intends to move the following application features into Cisco AON:

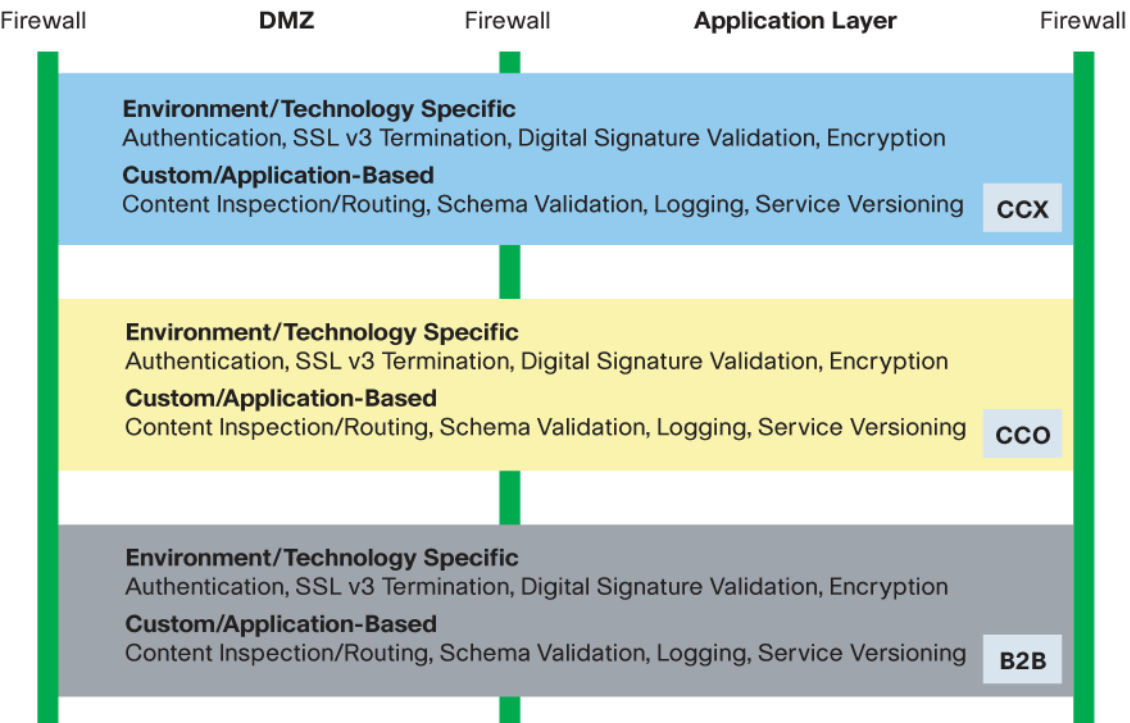
- Authentication
- Monitoring
- Versioning
- Transport and message-level encryption and digital signatures
- Failover
- Load balancing and distribution
- Logging
- Message and content-based routing
- Protocol translation
- Virtual gateway
- SLAs
- Contracts
- Billing

BUSINESS VALUE

Cisco AON’s unique capabilities are bringing a range of business benefits to Cisco. By ensuring that certain application functions are handled in a consistent, standardized way across all hosted environments, Cisco will reduce the redundancies of programming effort in each environment. Instead, Cisco will use standard, uniform approaches. Also, as functions once handled on hardware appliances or within third-party software are integrated into Cisco AON, capital and operating costs will decrease because of lower integration costs. As discussed earlier, Cisco AON will enhance security because it cannot be circumvented; it operates within the network devices, which look at all packets crossing the wire. The final

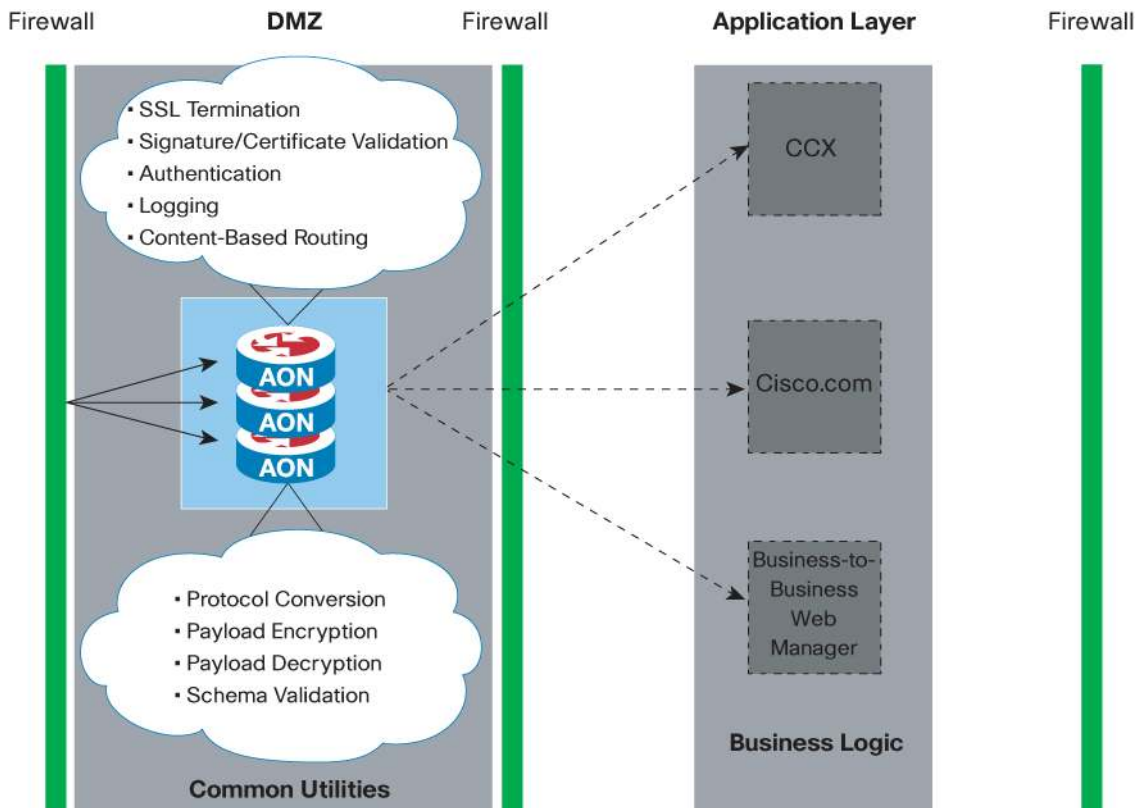
advantage of Cisco AON is that it will provide management with greater visibility into transactions with customers and will also make it simpler and less costly for Cisco partners and suppliers to do business with Cisco.

Figure 1. Cisco IT Today



Cisco IT now maintains disparate hosted environments—CCX (Cisco Connection eXternal), Cisco.com, and B2B, and each requires dissimilar tools and processes to perform application message processing.

Figure 2. Cisco AON Unifies Message Processing



Once Cisco AON is deployed, it provides a common set of utilities across all Cisco hosted environments. Cisco AON also provides more stringent security as all authentications and validations are done in the network in the DMZ.

Cisco AON is an intelligent message routing system that makes customers' existing infrastructures more:

- **Safe**—Application-level security embedded in the network that is policy enforced and takes full advantage of network security
- **Visible**—Automatic event capture everywhere, in real time
- **Responsive**—Streamlined communication, autonomic “sense and respond,” and hardware acceleration
- **Flexible**—Policy-oriented control, transparent to applications, highly scalable, open software development kit

FOR MORE INFORMATION

To find out more about the Cisco AON and Cisco networking solutions go to

http://www.cisco.com/en/US/products/ps6692/Products_Sub_Category_Home.html,

http://www.cisco.com/en/US/products/ps6438/prod_module_series_home.html and <http://www.cisco.com/en/US/netsol/index.html>.

**Americas Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Cisco Systems, Inc.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 6 of 6