What is AON to Cisco IT?
Architecture and Function

Hicham Tout—IT Engineer, IT Infrastructure
Sandeep Puri—IT Engineer, IT Infrastructure
Khaldoun Rayes—IT Engineer, IT Infrastructure
AON: Application Oriented Networking Is—

• A blade/module
• Delivering a set of application and service support utilities
• That help clients to communicate safely and well with applications by providing
• Security
  Reliability
  Manageability
  Targeted Service
What Is AON to Cisco IT vs. What AON Is Not!

What AON is:

- A Message Router between end points
- A message transformer/mapper
- A service and integration hub with WS management capabilities

What AON is not:

- A general purpose application Server
- An orchestration engine
What Role Does AON Play?

- Service Broker in SOA
- Integration Broker in Application Integration
- Security Integrator
AON and the OSI Stack

Content-based Routing

Content Inspection, Transformation, Security & Mapping

Message Level Protocol (SOAP)

Application
Presentation
ASCII, MPEG, GIF, etc...

Session
RPC, NFS,

Transport
TCP, UDP

Network
IP, Logical Addressing

Data Link
Data Translation to frames

Physical
Data Bits transmission
AON Components

ADS (AON Design Studio)
Used for Developing Application Policies

AMC (AON Mgmt Console)
Used for Configuring and Provisioning AON Modules

AON Blades
AON Delivers the Following Support Utilities for:

**Security**

- Transport-level encryption termination (SSL v3)
- Payload encryption termination (XML)
- Protocol translation (HTTP <-> JMS)
- Digital Signature (for strong authentication)
- DMZ-to-Application Layer Secure Connector (like SSH or STA)
These AON Security Functions…

…Are Currently Being Performed by Custom Code or Vendor-proprietary Tools Built into Dozens of Cisco External-Facing Services

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption using SSL V3 With Bi-Directional Authentication</td>
<td>Limited</td>
<td>• WebMethods specific. Requires significant setup effort</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>XML Payload Encryption</td>
<td>Custom written by each app using java libraries</td>
<td>Limited.</td>
<td>Custom written by each app</td>
<td>Limited</td>
</tr>
<tr>
<td>Protocol Translation</td>
<td>Custom written by each application</td>
<td>• WebMethods specific.</td>
<td>Custom written by each application.</td>
<td>Custom written and/or Product/technology specific</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>Custom written by each app using java libraries</td>
<td>Limited</td>
<td>STA (Secure Transport Architecture)—Custom.</td>
<td>Varies for each environment</td>
</tr>
<tr>
<td>DMZ-2-App Layer Secure Connector</td>
<td>mod_IIOP over SSH pipes</td>
<td>Reserve Proxy</td>
<td>STA (Secure Transport Architecture)—Custom</td>
<td>Varies for each environment</td>
</tr>
</tbody>
</table>
AON Delivers the Following Support Utilities for:

**Reliability**
- Reliable Delivery

**Manageability**
- Message and Transaction-Level Logging
- Transaction Monitoring

**Targeted Service**
- Service Versioning (allows multiple versions of single service to run simultaneously)
- Message/Content-Based Routing (routes messages based on contents and/or business rules)
These AON Reliability and Manageability Functions…

…Are Currently Being Performed by Custom Code or Vendor-Proprietary Tools Built into Dozens of Cisco Services

<table>
<thead>
<tr>
<th>AON Reliability Function</th>
<th>External App Environment 1</th>
<th>B2B (WebMethods)</th>
<th>External App Environment 2</th>
<th>Other Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption using SSL V3 With Bi-Directional Authentication</td>
<td>Custom written with limited capabilities</td>
<td>• WebMethods specific. Requires significant setup effort</td>
<td>Custom written with limited capabilities</td>
<td>Custom written with limited capabilities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AON Manageability Function</th>
<th>External App Environment 1</th>
<th>B2B (WebMethods)</th>
<th>External App Environment 2</th>
<th>Other Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption using SSL V3 With Bi-Directional Authentication</td>
<td>Custom written by each app</td>
<td>WebMethods specific</td>
<td>Custom written by each app</td>
<td>Limited</td>
</tr>
<tr>
<td>Monitoring (Transaction level)</td>
<td>Custom written by each application</td>
<td>• Webmethods specific • Limited to WM transactions</td>
<td>Custom written by each application</td>
<td>Custom written and/or Product/technology specific</td>
</tr>
</tbody>
</table>
These AON Targeted Service Functions…

…Are Currently Being Performed by Custom Code or Vendor-Proprietary Tools Built into Dozens of Cisco Services

<table>
<thead>
<tr>
<th>AON TARGETED SERVICE FUNCTION</th>
<th>External App Environment 1</th>
<th>B2B (WebMethods)</th>
<th>External App Environment 2</th>
<th>Other Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption using SSL V3 With Bi-Directional Authentication</td>
<td>Custom written with limited capabilities</td>
<td>Custom written with limited capabilities</td>
<td>Custom written with limited capabilities</td>
<td>Custom written with limited capabilities</td>
</tr>
<tr>
<td>Message/Content-Based Routing</td>
<td>Custom written with limited capabilities</td>
<td>• WebMethods specific</td>
<td>Custom written by each application</td>
<td>Custom written and/or Product/technology specific.</td>
</tr>
</tbody>
</table>
The Goal is to Have AON Play the Role of Services Management Broker/Gateway and Pass the Single, Virtual Gateway for all Web and B2B Services; Below is a List of Important Features of Which Many Have Been Formalized as Requirements:

- Authentication
- Monitoring
- Service Versioning
- Encryption and Digital Signatures
- Message-level Load Balancing and Distribution
- Logging
- Message and Content-Based Routing
- Protocol Translation
- Secure Tunneling across Firewall
- Contracts
- Billing
Before AON: Current Location of Application and Service Support Utilities

- **Environment/Technology specific:**
  - Authentication, SSL V3 Termination, DSIG Validation, Encryption

- **Custom/Application-based:**
  - Content Inspection/Routing, Schema Validation, Logging, Service Versioning

**External Env 1**

**External Env 2**

**B2B**

**DMZ**

**Application layer**

**Firewall**
After AON: Future Location of Application and Service Support Utilities

Firewall → DMZ → Application layer → Firewall

DMZ:
- Common Utilities
  - SSL Termination
  - SIG/Cert Validation
  - Authentication
  - Logging
  - Content-based Routing
  - Protocol Conversion
  - Payload Encryption
  - Payload Decryption
  - Schema Validation

Application layer:
- Java
- PERL
- B2B

Internal DB → Internal DB
Who Would Benefit From AON!

**Service Developers:**
- Reduces development lifecycle
- Builds on existing services

**Business:**
- Time-to-market
- Lower development and maintenance cost

**Information Security:**
- Simpler security model
- Better visibility

**Infrastructure:**
- Reduced complexity
- Better visibility

**Enterprise Architects:**
Cisco IT Recommended AON Architecture

SSL Termination, DSIG/Cert Validation, Authentication, logging, etc...
Payload Decryption, Schema Validation, Content Inspection/Routing, logging
Protocol Conversion (HTTP-2-JMS), Content-based Routing, logging
Payload Encryption, DSIG, logging, etc...
Before AON: Transformation and Mapping

Diagram showing the relationship between external services (SOAP/HTTP(s)), messaging bus, and back-end systems/packages/databases. The diagram includes components such as Proxy Web Service, JMS Lib, OCM, JDBC, Internal Env 1 and 2, SQL, HTTP, Web Services, and Adaptor.

Back End Systems/Packages/Databases:
- SQL
- HTTP
- Web Services
- JDBC
- Internal DB
- Internal DB
- Internal DB
- Transformation Mapping Automated BP
- Custom Applications

Messaging Bus:
- Proxy Web Service
- JMS Lib
- OCM

External Env 1:
- SOAP/HTTP(s)
- External Env 1

Internal Env 1:
- Internal DB
- JDBC
- Internal Env 1
- Transformation Mapping Automated BP
- JMS Lib

Internal Env 2:
- JDBC
- Internal Env 2
- Custom Applications
- JMS Lib
After AON-Phase I

Back End Systems/Packages/Databases

- SQL
- HTTP
- Web Services

Adaptor

JDBC

AON Blades Replace Proxy Web Services on External Env 1

SOAP/HTTP(s)

OCM

Transformation Mapping Automated BP

Custom Applications

JMS Lib

Internal DB

Internal DB

Internal DB

JMS Lib

Web Services

JDBC

Internal Env 1

Internal Env 2
AON Blades Could Also Replace Business Process and Transformation Engine by Providing Transformation/mapping Capabilities in Addition to Proxy web Service Layer (Phase 2)
After AON-Phase II

AON Blades Could Also Replace Business Process and Transformation Engine by Providing Transformation/mapping Capabilities in Addition to Proxy web Service Layer (Phase 2)
Using AON vs. B2B Gateway

- Internet
  - Customers
  - Partners
  - SOAP/HTTP(S)
  - XML/HTTP(S)
  - Flat File/HTTP(S)
  - RNIF
  - EDI/AS2

- Enterprise Network
  - AON
  - Distributed Enterprise Services
  - Legacy B2B Gateway
Protocol Relationships

Web Services Protocol Set

- TCP/IP
- HTTP
- SOAP
- WS-Security
- AON (Service Broker)
- XML-Digital Signature (DSIG)
- XML-Encryption (XENC)
- WSDL
- UDDI

Out of Band Exchange
What Role Does AON Play in SOA?

• Service Broker
  Application-Level Message Routing
  Application/Service Security
  Application-Level Monitoring
  Service Abstraction
  Protocol Translation
  Transformation and Mapping

• Message Schema Validation
What Role Does AON Play in Application Integration?

Application Integration:

- Protocol Translation
- Transformation and Mapping
- Message Schema and Data Validation
Cisco IT AON Production: Intangible Benefits

• Faster time to delivery by reducing development lifecycle
• Better security made possible by a common and simplified implementation, provisioning, and configuration process
• Reduced complexity of applications and infrastructure
• Architecture lends itself to the future of SOA
• Reduced resource requirements by individual applications
• Moving intelligence into the network
An invisible message router/gateway in the network that routes, transforms, monitors, and authenticate/authorize messages between end points.
How Can AON Be Invisible?

An AON node resides in the network as an inline application-aware device; the device acts as an intelligent intermediary gateway that can either be explicitly addressed by applications or as a pass-through proxy that is transparent to applications.
AON Modes of Operation

**Transparent Mode:**
Intercept with No Change to Applications

Based on WCCP Re-Direct ACL Intercept Traffic and Forward to AON

Sending Application A

http://B/Service1

Integrated Switch/AON Blade

Receiving Application B
AON Best Practices:
A Cisco IT Perspective
Cluster AON blades based on functionality
- Identify common capabilities that span across multiple applications to be owned by Infrastructure
- Move common/infrastructure capabilities into a separate set of AON clusters while keeping application-dependent capabilities into its own set of clusters
- For external-facing Web Services, infrastructure AON cluster should exist in the DMZ, while the application AON cluster should reside in the protected net
- Standardize on AONP(S) as the inter-cluster communication protocol
- Standardize on a naming convention for resources, flows, and properties

SSL Termination, DSIG/Cert Validation, Authentication, logging, etc...
Payload Decryption, Schema Validation, Content Inspection/Routing, logging
Protocol Conversion (HTTP-2-JMS), Content-based Routing, logging
Payload Encryption, DSIG, logging, etc...
Best Practices: Provisioning and Management

- Implement a standard SDLC strategy (dev/test/prod)
- Implement collision prevention utilizing standard name spacing
- Implement isolation by sandboxing development environment by project teams
- Allow for an automated promotion process
- Implement a promotion strategy that takes into account all of the above

SSL Termination, DSIG/Cert Validation, Authentication, logging, etc…
Payload Decryption, Schema Validation, Content Inspection/Routing, logging
Protocol Conversion (HTTP-2-JMS), Content-based Routing, logging
Payload Encryption, DSIG, logging, etc…
Cisco IT Services Leveraging AON

- Product Configurator
- Order Status
- RMA (Return Merchandize Authorization)
- Background Check
- Salesforce.com Integration (contacts, leads, etc…)

© 2006 Cisco Systems, Inc. All rights reserved.
Q and A
Intermission

Coming up in the next hour:

• Security with AON
• AON Deployment Timelines within Cisco IT
• AON Business Case within Cisco IT
Security with AON

Brook Schoenfield,
Senior Security Architect
CSPO
Agenda

• Where Does AON Fit into the Bigger Picture?
• What is AON?
• AON Security Features
  Architecture
  Combining Layer 3/4 and Layer 7+
  Common Security Functions
  Deep Content Inspection
  Access Controls
Agenda

• Where Does AON Fit into the Bigger Picture?
  What is Service Oriented Architecture (SOA)?
  What is Application Integration?
• What is AON?
• AON Security Features
  Architecture
  Combining Layer 3/4 and Layer 7+
  Common Security Functions
  Deep Content Inspection
  Access Controls
Service Oriented Architecture is a different mindset

Focus on delivering a service offering (an invoice, a purchase order, an item or unit that has intrinsic business understanding and value)

No longer focus on the programmatic interface (message standards take care of that)
SOA Is Now!

“By 2005, the aggressive use of Web services will drive a 30% increase in the efficiency of IT development projects”


This Is FYQ06; Enterprises Are Looking for that 30% Gain
AON and SOA

- AON can be a key part of an SOA build out
- AON provides the necessary security functions
- Common functions become “part of the network”
Cisco IT Specific Drivers for SOA

- Move from functionally focused IT to business process focused
- Single source of truth
- Development cycles—reusability
- Business responsiveness
- Consistency
- Security functions
Example of Cisco Distributed Services (SOA)

- Product Configurator
- Order Status
- RMA (Return Merchandize Authorization)
- Lead management integration (contacts, leads, etc...)
Complexity (and Risk) Increase with Adoption
Healthy Distrust = Security Controls

- Services should be distrustful of the outside world
- Not everyone will be served
- Inspect, validate and authenticate requests
  The code’s internal state is not openly exposed
- Only well defined requests are serviced
- Requests do not reveal the service’s algorithms
- Requests do not describe the service’s state
- Requests provide services, not data access
  Services should not share ACID transactions
- Transactions imply a certain level of trust
  Locks may be held for a long time
- Transactions imply a level of coupling
  —Microsoft Incorporated
Agenda

• Where Does AON Fit into the Bigger Picture?
• What is AON?
• AON Security Features
  Architecture
  Combining Layer 3/4 and Layer 7+
  Common Security Functions
  Deep Content Inspection
  Access Controls
What Role Does AON play?

- Service Broker in SOA
- Integration Broker in Application Integration
- Message Security Integrator
AON and the OSI Stack

- Content-Based Routing
- Content Inspection, Transformation, Security & Mapping
- Message Level Protocol (SOAP)

**Application**
- ASCII, MPEG, GIF, etc...

**Presentation**
- RPC, NFS, TCP, UDP

**Session**
- IP, Logical Addressing

**Transport**
- Data Translation to Frames

**Network**
- Data Bits Transmission

**Data Link**
- Physical
Pre-AON Inspection and Operation

Switches, Routers, Firewalls, “Content Inspection” Operate Around the Payload

IP  TCP  HTTP  Opaque
AON Is Inside the TCP/IP Wrapper

Session Protocol + Content Inspection ==
Session and Payload

<?xml version="1.0"?>
<purchaseOrder orderDate="1999-10-20">
  <shipTo country="US">
    <name>Alice Smith</name>
    <street>123 Maple Street</street>
    <city>Mill Valley</city>
    <state>CA</state>
    <zip>90952</zip>
  </shipTo>
  ...
</purchaseOrder>
AON Is Inside the TCP/IP Wrapper

Session Protocol + Content Inspection == Session and Payload

Payload/Message

<?xml version="1.0"?>
<purchaseOrder orderDate="1999-10-20">
  <shipTo country="US">
    <name>Alice Smith</name>
    <street>123 Maple Street</street>
    <city>Mill Valley</city>
    <state>CA</state>
    <zip>90952</zip>
  </shipTo>
  ...
</purchaseOrder>

Optimized for XML Payloads
AON == Message Content and Envelope

HTTP, Envelope (SOAP), Messages (XML envelope standards + custom XML) == “Deep Inspection”

Existing Message Bodies + Custom Parsing
Why XML?

- TCP/IP gives you network H/W independence
- JAVA gives you platform independence
  (sort’a, kind’a: for the first few years it was, “write once, debug everywhere”)
- XML gives you data independence
- Ubiquitous adoption
AON Delivers the Following Support Utilities for:

Security

• Transport-level encryption termination (SSL v3)
• Payload encryption termination (XML)
• Protocol translation (HTTP <-> JMS)
• Digital Signature
• DMZ-to-Application Layer Secure Connector (like SSH or STA)
These AON Security Functions…

…Are Currently Being Performed by Custom Code or Vendor-Proprietary Tools Built into Dozens of Cisco External-Facing Services

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption using SSL V3 With Bi-Directional Authentication</td>
<td>Limited</td>
<td>• WebMethods specific. Requires significant setup effort</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>XML Payload Encryption</td>
<td>Custom written by each app using java libraries</td>
<td>Limited.</td>
<td>Custom written by each app</td>
<td>Limited</td>
</tr>
<tr>
<td>Protocol Translation</td>
<td>Custom written by each application</td>
<td>• WebMethods specific. • Limited to WebMethods transactions. • Interoperates with a limited number of Messaging technologies</td>
<td>Custom written by each application.</td>
<td>Custom written and/or Product/technology specific</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>Custom written by each app using java libraries</td>
<td>Limited</td>
<td>Custom written by each app</td>
<td>Limited</td>
</tr>
<tr>
<td>DMZ-2-App Layer Secure Connector</td>
<td>mod_IIOP over SSH pipes</td>
<td>Reserve Proxy</td>
<td>STA (Secure Transport Architecture)—Custom</td>
<td>Varies for each environment</td>
</tr>
</tbody>
</table>
Before AON: Current Location of Application and Service Support Utilities

**DMZ**

- **Environment/Technology specific:**
  - Authentication, SSL V3 Termination, DSIG Validation, Encryption
- **Custom/Application-based:**
  - Content Inspection/Routing, Schema Validation, Logging, Service Versioning

**Application layer**

- **Environment/Technology specific:**
  - Authentication, SSL V3 Termination, DSIG Validation, Encryption
- **Custom/Application-based:**
  - Content Inspection/Routing, Schema Validation, Logging, Service Versioning

**External Env 1**

- **External Env 2**

**B2B**

- **Internal DB**

---

© 2006 Cisco Systems, Inc. All rights reserved.
After AON: Future Location of Application and Service Support Utilities

Common Utilities

- SSL Termination
- SIG/Cert Validation
- Authentication
- Logging
- Content-based Routing

- Protocol Conversion
- Payload Encryption
- Payload Decryption
- Schema Validation

Application layer

Java

PERL

B2B

Business Logic

Internal DB
Agenda

• Where Does AON Fit into the Bigger Picture?
• What is AON?
• AON Security Features
  Architecture
  Combining Layer 3/4 and Layer 7+
  Common Security Functions
  Deep Content Inspection
  Access Controls
AON Security

• AON fosters a better network security architecture
  Because of the reduction of unprotected segments between applications and AON

• Use of layer 3/4 to protect layer 7 functions (i.e., layer 7 security implemented in the network device)

• Common and consistent implementation of security functions
  Digital signatures (DSIG), encryption/decryption, authentication, access control lists (ACL), validation

• PKI implementation that is correct, tested, and validated

• Separation of design/development and implementation
Pre-AON Web Security Architecture

Firewall  
DMZ  
Firewall  
Application Layer  
Firewall

Web Servers

Business Logic

Java
PERL
B2B

Internal DB
Internal DB
Internal DB
Pre-AON SOA/Web Services Security Architecture

**DMZ**
- Web Servers
  - WS
  - WS
  - WS
  - WS GW

**Application Layer**
- Business Logic
  - Java
  - PERL
  - B2B

**Firewall**
- DMZ
- Application Layer
- Internal DB
Pre-AON Attack Vectors

Firewall  DMZ  Firewall  Application Layer  Firewall

Web Servers

Business Logic

Java

PERL

B2B

Internal DB

Internal DB

Internal DB
Pre-AON Attack Vectors

The GW is **NOT** part of the network. Compromise of layer 3/4 can attack the application layer, going around the GW.

Net architecture must be changed for GW. (more switches and routers = more ACs to manage)

Web Servers

Business Logic

Java

PERL

B2B

Internal DB

Internal DB

© 2006 Cisco Systems, Inc. All rights reserved.
A Possible (Simplified) AON Architecture

Firewall → DMZ → Firewall

AON Is part of the Network. App Layer Is Directly Connected to Network Device.

Web Servers

Message Protection Is Terminated at AON. No attack Vector Is Exposed.

Application Layer

Business Logic

Java

PERL

B2B

Internal DB

Internal DB

AON Can Be Dropped into an Existing Layered Architecture without Changing the Security Boundaries
AON Potential Architecture

SSL Termination, DSIG/Cert Validation, Authentication, logging, etc...
Payload Decryption, Schema Validation, Content Inspection/Routing, logging
Protocol Conversion (HTTP-2-JMS), Content-based Routing, logging
Payload Encryption, DSIG, logging, etc...
AON Potential Architecture

- Replace web servers with AON
- AON terminates HTTP/S and provides other DMZ functions

SSL Termination, DSIG/Cert Validation, Authentication, logging, etc...
Payload Decryption, Schema Validation, Content Inspection/Routing, logging
Protocol Conversion (HTTP-2-JMS), Content-based Routing, logging
Payload Encryption, DSIG, logging, etc...

Common functions in Application layer provided by AON protect services and logic in application layer
Implementation Consistency

• The devil is in the details; most exploitable vulnerabilities are found in implementations rather than algorithms

• A good maxim is to implement common or tricky services as part of an infrastructure, “For application developers, not by application developers”

• AON provides common and consistent implementations of message level security functions
Some of AON’s Security Functions

- Digital signatures (DSIG)
- Encryption/decryption at transport (SSL) or message (XENC)
- Authentication (HTTP BASIC, LDAP stores, X-509 Certificate, etc.)
- Something very like access control lists (flows can be used as message level ACLs)
- Data and schema validations (flows can contain XSLT expressions)
Key XML Standards

• **WS-SEC or WSEC (WS-Security):** An envelope and semantic for:
  - XML-Signature (DSIG) == Digital signature use
  - XML-Encryption (XENC) == Encrypt/decrypt use
  - Authenticators

• **+ More standards proposed; Alphabet soup!**
  - Web Services Description Language (WSDL)
  - Universal Description, Discovery, and Integration (UDDI)
  - Web Services Flow Language (WSFL)
  - Other Business Rules. (BPEL4WS)
AON Implements Messaging Standards

XML Protocol Set

- XML-Expressions (XLST)
- XML-Encryption (XENC)
- XML-Digital Signature (DSIG)

AON
Security Integrator/SOA

- WS-Security
- SOAP
- HTTP
- TCP/IP
Standards Relationships

XML Protocol Set

- XML-Expressions (XLST)
- XML-Encryption (XENC)
- XML-Digital Signature (DSIG)

AON: Accelerated XML Services

- WS-Security
- SOAP
- HTTP
- TCP/IP

© 2005 Cisco Systems, Inc. All rights reserved.
Digital Signatures (X.509 + DSIG)

- Authentication credentials
- Non-repudiation
- Integrity
- Used at the entire message or for parts of a message, use Certificate or key enveloping (WSSEC); DSIG is very general purpose
Encryption/decryption

- Confidentiality
- Integrity
- Of the transport (SSL)
- Or in the message (XENC)
- Entire message or parts of a message
Authentication

- HTTP BASIC
- SOAP Enveloped (header)
- Enterprise LDAP (Directory) stores
- Different types of credentials:
  - X-509 Certificate
  - Signature validation (XENC, certificate based)
Flow Security Mechanisms

- Validation of the message format
- Validation of data ranges
- Rules defining authorization
- One could even write XML firewall signatures (though this functionality does not come out-of-the-box)
- A very general purpose mechanism for controlling message access and routing
Deep Content Inspection

- Content inspection delivers the ability to build Intrusion Detection (IDS) or even firewall signatures
- Expressions and logic can be applied with inspection
- Signatures can fire off alarms (content IDS)
- Message flow can be stopped via signatures (firewall functionality)
- Write java “bladelets”, code that can use the same services as AONs internal content handling code; ergo, handle custom content types
- This functionality is available to users (for instance, the IDS or firewall security team)
- AON is NOT a Firewall (because signatures do not come out-of-the-box)
AON Components

**ADS (AON Design Studio)**
Used for Developing Application Policies “Flows”

**AMC (AON Mgmt Console)**
Used for Configuring and Provisioning AON Modules

**AON Blades**
Access Controls

- Allows staging of flows
- Stages can be proofed before deployment
- Verification stages can be easily added
  (Development, staging, production)
- Approval processes can be easily added
- Different user types can be assigned different roles and accesses (designers, developers, approvers, administrators, etc.)

  Implemented at device, AON component, and through AON access controls
Summary

- Cisco is building out a SOA
- AON is being piloted to play a strong role in Cisco’s SOA
- AON security features
  - Architecture
    - Combining Layer 3/4 and Layer 7+ security controls
    - Common security functions: signatures, encryption, PKI
    - Deep content inspection ➔ content level ACLs
    - Reasonable administrative access controls
Q and A