Cisco Enterprise Policy Manager

Cisco® Enterprise Policy Manager helps application-development teams implement fine-grained security at a fraction of the time and cost of custom development. On an enterprise wide basis, Cisco helps security teams deliver consistent policy while helping risk and audit teams review and change policy to meet with compliance requirements. It comprises three distinct but transparently integrated components:

- Cisco Policy Administration Point provides centralized administration, management, and monitoring of entitlement policies, and delegation and integration with enterprise information repositories.
- Cisco Policy Decision Point (PDP) provides run-time resolution of role-based and rule-based authorization policies.
- Policy enforcement points enforce policy decisions made by the PDPs.

Product Overview

Controlling access to corporate applications, data, and infrastructure has never been more important – or more costly. Enterprises needing to control access based on numerous attributes, from user profile to nature of request to time of day, have historically had only one solution: to custom code security policy into every application.

Cisco Enterprise Policy Manager fundamentally changes and simplifies the process of deploying, managing, and auditing application security. By externalizing fine-grained authorization policy from core application logic and delivering it as a XACML standards-based service, Cisco is changing the nature of application entitlement management.

- Streamline Application Security: Untangle authorization controls from applications and cut your project schedules and budget by up to 30% while enhancing security.
- Assure Persistent Compliance: Gain centralized control and visibility over fine-grained access policies and instantly remediate audit exceptions.
- Empower New Business Scenarios: Enable a more agile, extended and service-oriented enterprise, with business users empowered via self-service and delegation.

Features and Benefits

- Streamline application security:
  - Consistently define and enforce fine-grained access control per application, across the infrastructure, and across the enterprise.
  - Rich, rule-based contextual entitlements take advantage of multiple distributed roles, rules, and attribute repositories.
  - The solution offers snap-on integration with existing identity and authentication management infrastructure.
  - Powerful delegation and modeling capabilities (subject and resource hierarchies, inheritance, exceptions, and scoping) offer ease of administration.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- There is no need to serialize behind identity management, single sign-on, or corporate role reconciliation initiatives.

- Assure consistent compliance:
  - The solution offers centralized and automated audit review across applications regardless of enforcement mechanism.
  - The solution offers audit capabilities within applications and across the enterprise.
  - The solution provides real-time reports and alerts on who can access what, who accessed what, and who made what administration change.
  - You can easily create “Chinese Walls”, and enforce and audit segregation of duties.
  - Forecast “What If?” scenarios to help security administrators understand the ramifications of policy changes.
- Empower new business scenarios:
  - Rich entitlement policies are configured, deployed, and updated without application modification – allowing organizations to begin reaping the benefits of a service-oriented architecture (SOA).
  - Maximum flexibility is achieved through central and application-specific role-based, attribute-based, and rule-based entitlements.
  - Increased organizational agility is achieved through delegation to business users, removing IT as the bottleneck for urgent business-process changes.
  - The solution offers time- and cost-effective deployment, including 45-minute installation and rapid realization of return on investment (ROI).

Product Architecture

Cisco brings the industry’s most robust enterprise-class XACML standards-based solution that externalizes application entitlement policies. The Cisco solution is deployable in a federated environment and includes 3 components:

1. Centralized policy administration point
   a. Browser-based, point-and-click UI for creation of granular entitlement policies (based on subject, resource, message content, action, and other environmental attributes)
   b. Ability to set per-application as well as enterprise wide policies
   c. Ability to view and audit security policies for all applications – regardless of enforcement mechanism
   d. Ability to administer entitlements including ability to group users and resources, clone and inherit entitlements, and delegate the administration of the entitlement policies
   e. Ability to administer the distributed entitlement management solution from one virtually central location
2. High-performance, highly available, distributed policy decision points (PDPs)
   a. High performance resolution of role-based and rule-based policies and management of distributed decision caches
   b. Snap-on integration with user information repositories (LDAP, Active Directory) and existing Identity Management solutions

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

c. Flexibility in deploying the decision points to be local or remote to the resources for which they resolve the entitlement policies

d. Standards-based solution with native support for XACML, SOAP, and SAML

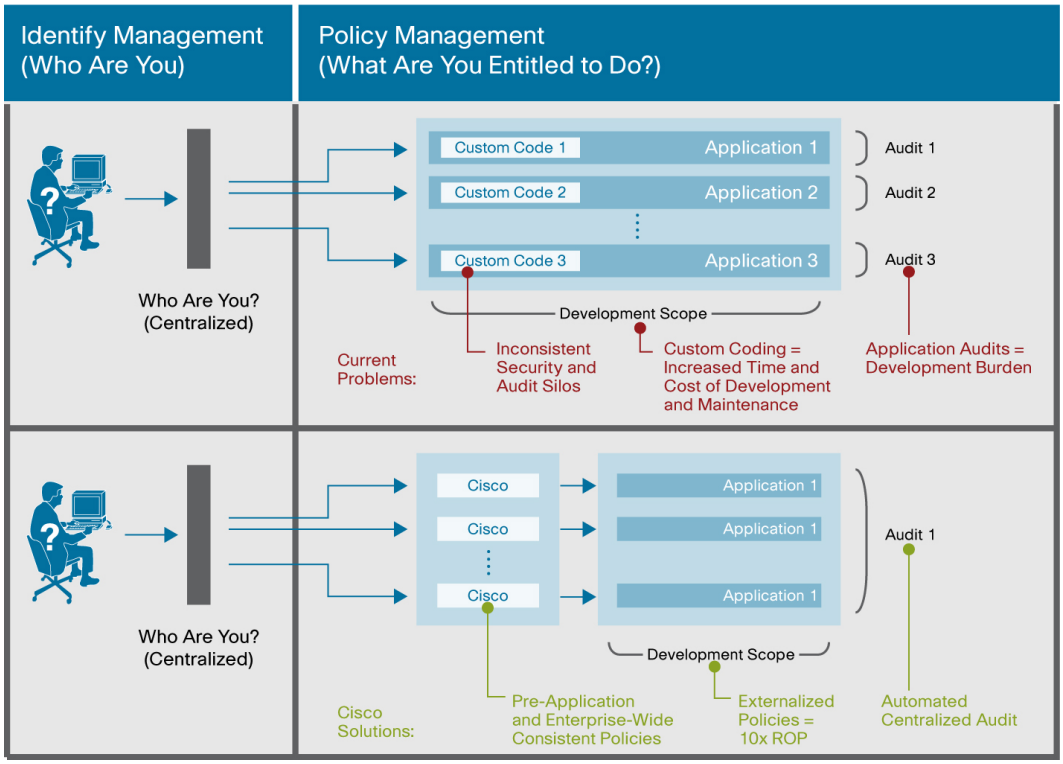
3. Fine-grained, optimized policy enforcement points (PEPs)

a. XACML compliant enforcers plug into J2EE and .NET servers while also supporting portals, content management, email, IM, web, and FTP servers

b. Optimized performance and availability through optional pre-fetching and local caching of entitlement policy decisions

c. Extensive logging capabilities for audit

Figure 1. Product Architecture



To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center.

Service and Support

Using the Cisco Lifecycle Services approach, Cisco and our partners provide a broad portfolio of end-to-end services and support that can help increase the business value of your network and your return on investment. This approach defines the minimum set of activities needed, by technology and by network complexity, to help you successfully deploy and operate Cisco technologies and optimize their performance throughout the lifecycle of your network.

For More Information

For more information about Cisco Enterprise Policy Manager, please go to http://www.cisco.com/go/policy.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, 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, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, 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, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0801R)

Printed in USA C78-453502-00 02/08

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.