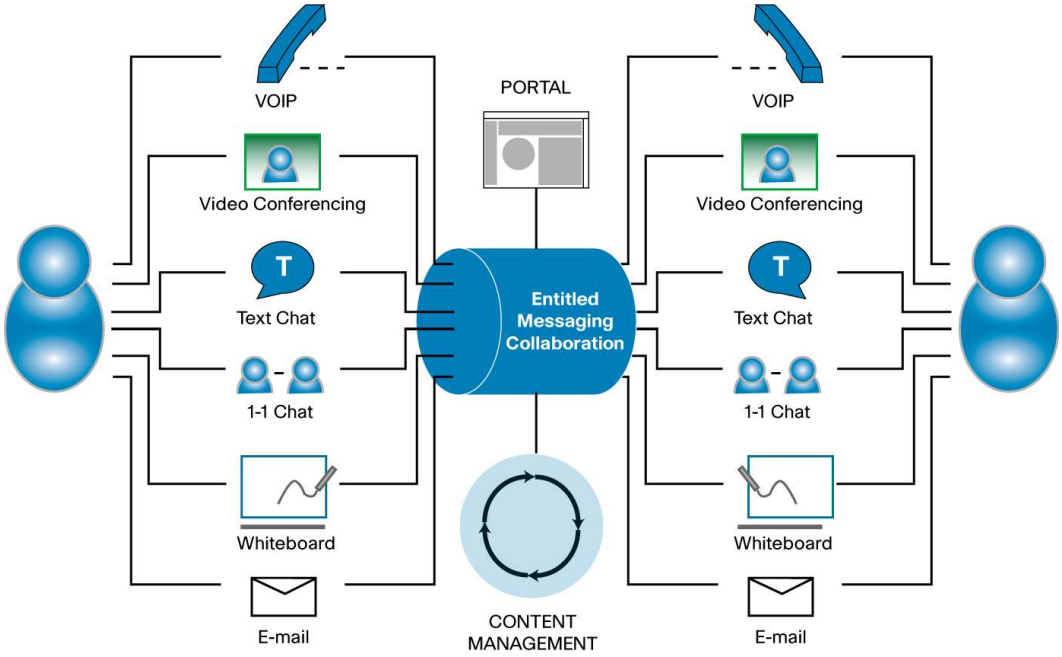
A Cisco Solution Guide: Secure Enterprise Portals, Collaboration, and Messaging with Cisco Enterprise Policy Manager

Enterprises increasingly rely on collaborative, multi-modal electronic communications between employees, customers, and partners. With the heightened emphasis on security and compliance, enterprises are seeking standards-based, flexible, and policy-based solutions that they can use to consistently and comprehensively manage, enforce, and audit access to their infrastructure. The solution needs to span various communication and collaboration channels including portals, content management systems, instant messaging (IM), voice over IP (VoIP), e-mail, white-boards, text chatting, and video conferencing. Furthermore, the solution needs to have enterprise-class scalability, availability, and performance to prevent disrupting or inhibiting critical business processes.

Cisco® Enterprise Policy Manager provides an entitlement and access control solution that addresses this need by externalizing authorization from the core portal, collaboration, content management, and messaging infrastructure using agents that intercept traffic flowing through these channels. Policies can be centrally configured to allow or deny access based on the identity and presence attributes of the users, the channel of communication, the resource being accessed, the content of the message being communicated, and other environmental variables (such as the time of day).

Figure 1. Entitled Messaging and Collaboration



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

With this model, enterprises can:

- **Declaratively specify fine-grained access polices** to avoid unorganized implementations of disparate authorization solutions
- **Deploy an eXtensible Access Control Markup Language (XACML) standards-compliant entitlement/authorization service** that can be consistently applied across all communication and collaboration channels
- **Centrally manage and delegate administration of policies** for enhanced administrative scalability
- **Enable policies to be resolved locally,** closer to the applications, to improve performance and reliability
- **Model complex role- and rule-based policies** with inheritance and exceptions
- **Specify Separation-of-Duty (SoD) policies** that can eliminate the risk of inadvertent or deliberate inappropriate access to sensitive systems and resources
- **Gain increased visibility with consolidated audit logs** of all administrative transactions and authorization decisions throughout the entire communications infrastructure

Cisco supports the leading enterprise messaging and collaboration products, including Microsoft Office SharePoint Server, Windows SharePoint Services, IBM Lotus Sametime, IBM Lotus Notes Domino, Jabber XCP, and Documentum, using customized agents that integrate with these offerings.

The Cisco entitlement solution consists of three components:

- **An administration server (Policy Administration Point or PAP)** that is used to centrally author, change, and audit policies
- **A policy decision engine (Policy Decision Point or PDP)** that is responsible for resolving policies including dynamic user role membership
- **An agent (Policy Enforcement Point or PEP)** that enforces these policies in real time

The solution is architected to work in a heterogeneous environment for consistent policy enforcement across disparate platforms such as Microsoft SharePoint/.NET, IBM Lotus Domino/WebSphere, Jabber XCP, Documentum, and multiple Session Initiation Protocol (SIP) stacks. As shown in Figure 1, consistent policy authoring and enforcement is achieved with a reusable PAP and PDP infrastructure that integrates with platform-specific PEPs.

Two examples of the Cisco policy-resolution solution are described below:

Cisco's Microsoft SharePoint agent executes natively within the SharePoint server. The agent intercepts requests to WebParts, documents and search functionality incorporated into any SharePoint portal. The agent, deployed as a dynamic-link library (DLL), also performs caching and pre-fetching to optimize the performance of enforcing run-time policy decisions. Role- and rule-based contextual policies (authored by the PAP) are resolved by the PDP. These policies can either be deployed natively in the Common Language Runtime (CLR) or as an infrastructure service shared by multiple applications.

Cisco's Jabber XCP Server agent (for versions 4.2 and later) executes within the same process as the Jabber server. The agent subscribes to, and processes, relevant events from the Jabber server. If the agent already has a cached, valid decision for the communicating parties and the resource (such as a file or a named chat room), the agent enforces the policy. If the agent does not have the decision cached locally, the Cisco PDP resolves the policy decision based on

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

the context of the IM session and attributes (user or resource) obtained from external sources such as enterprise directories (LDAP, Active Directory, etc.). The types of communication that can be protected include: one-on-one chat sessions, text conferencing, community groups and persistent chat rooms, file transfer, and presence.

The PDP resolves policies by evaluating rules that compute based on attributes (user or resource) from external sources such as enterprise directories (LDAP, Active Directory, etc.) or other custom attribute sources. The resolved policies can be used to enforce policies on other platforms in a manner similar to the two prior examples, using platform-specific agents running on third-party SIP stacks, document management systems, and other Java-based application server and collaboration suites. Additionally, Cisco's PAP can be configured to update rules and access control lists (ACLs) in native form to applications that may continue to use their native policy-resolution logic.

Table 1 provides a nonexhaustive list of features supported by the Cisco Enterprise Policy Manager.

Table 1. Cisco Enterprise Policy Manager Features

Hierarchical Role- and Rule-Based Policies	Collaboration Policy Management	Scalability and Administration
Smooth integration with multiple, existing attribute sources for rule- and role-based policy evaluation	Arbitrarily nested resource hierarchy (including named chat rooms, files/reports, portal pages, portlets, buttons, etc.)	Supported agents for multiple collaboration infrastructure including portals, e-mail, and EIM
Validation of user identities from external LDAP and Active Directory directories, and databases	Exception rules that allow access to all resources in a hierarchy except for selected users in a role	Delegated administration of administration console and APIs
User-to-group mapping	Drag-and-drop capabilities to specify entitlement policies for each resource	XACML decision queries from PEP to PDP
User-to-role mapping	Allow and deny role to resource-mapping policies	Central administration of all PEP and PDP configurations
Group-to-role mapping	Automatic traversal of resource and role hierarchy to determine decision	All PDP, PEP, and console communications are secured
Search users, roles, and groups	Configurable pre-fetch of authorization decisions from the PDP	Conflict-resolution policies including rule-combining policies, Separation-Of-Duties policies, etc.
Arbitrarily nested role hierarchies	Configurable caching of entitlements at agent (PEP)	All administration actions and authorization decisions logged
Arbitrarily nested group hierarchies	Exception rules that allow access to all resources in a hierarchy except selected sub-resources	Scalable and highly available deployments
Create/read/update and delete functions for users, groups, and roles	Create/read/update and delete functions for users, groups, and roles	Support for multiple platforms (Windows, Linux, and Solaris) and collaboration/messaging stacks (Domino, SharePoint, Jabber)

Enterprises today have a wealth of tools that unlock productivity and collaboration in their user base.In addition, the mainstream use of IM platforms and Voice over IP (VOIP) open additional avenues for enterprise users to connect with one another.However, these new opportunities also mandate the need for a policy-based governance mechanism to ensure that they are exploited in an effective manner.Cisco Enterprise Policy Manager provides the capabilities that empower Cisco's clients to capitalize on these trends and remain aligned with their security and risk management policies.

For More Information

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

For more information about Cisco Enterprise Policy Manager contact your Cisco account executive or visit http://www.cisco.com/go/policy

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, CCENT, 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, CCVP, 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, 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. (0803R)

Printed in USA C22-452111-00 04/08

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