Managing Permissions in Microsoft SharePoint for Enterprise Security and Compliance

In today's dynamic and collaborative business environment, enterprises must empower their knowledge-workers by connecting them to the right people, applications, processes, and information through the deployment of products such as Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0 (collectively "SharePoint").

Balancing the requirement to share and connect across organizational and geographic boundaries is the need for enterprises to safeguard their confidential information, simplify security procedures, and ensure compliance with regulatory requirements. In order to achieve open and yet secure collaboration, enterprises must augment SharePoint's native security mechanisms.

Cisco® offers an innovative standards-based policy management solution which enables organizations to consistently manage, enforce, and audit access-control policies to any SharePoint resource, including document libraries, lists, search queries, and Web parts. With the Cisco Enterprise Policy Manager, policies can be centrally managed to allow or deny access to distributed SharePoint portals and applications, based on the identity and other attributes of the user, the resource being accessed, and other environmental variables.

SharePoint's Limitations in the Enterprise

SharePoint's native security model is optimized for personal sites and does not adapt well to handle enterprise deployments. The model is based entirely on pre-establishing static permissions, which then must be applied to individual users or groups of users. There are default permissions such as contribute, design, and read. SharePoint also allows the creation of custom permissions. When SharePoint is used in enterprise scenarios, this model suffers from a number of significant limitations.

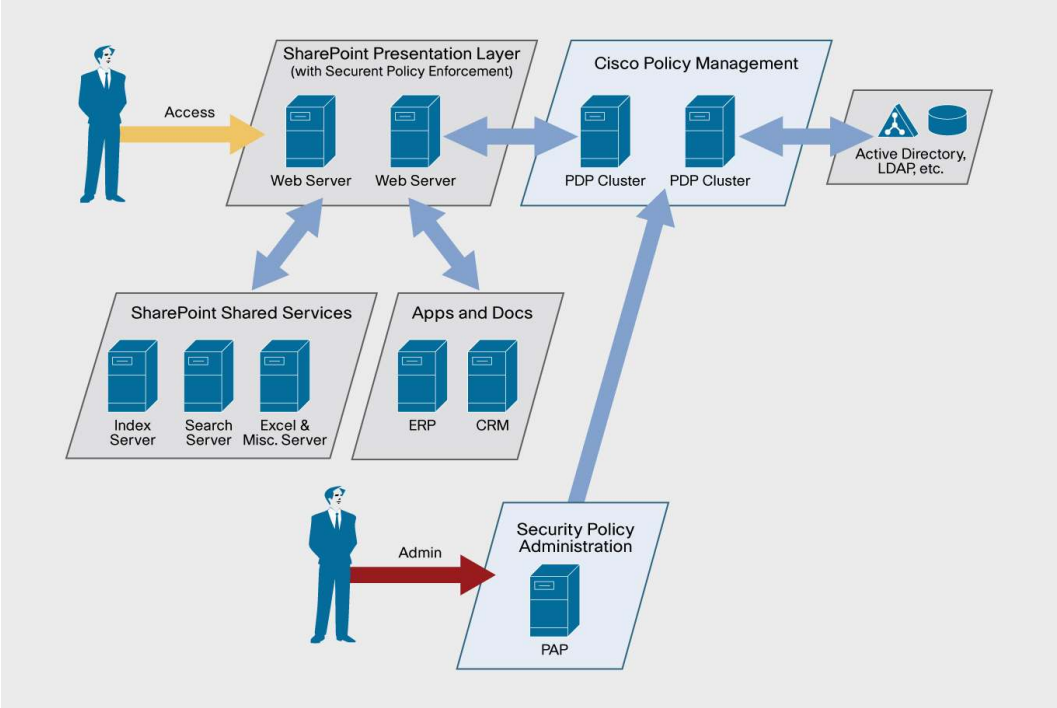
SharePoint security challenges:

- Manually mapping users or groups to permissions becomes very costly and time-consuming as the number of sites grows.
- There is an explosion in the number of pre-established permissions when deploying SharePoint enterprise-wide due to the varying levels at which permissions can be set (for example: site collection, site, list, and item).
- It is difficult to enforce enterprise-level policies (such as preventing external users from accessing resources marked "company confidential") on distributed SharePoint sites, particularly those created and managed by individual end users.
- It is not possible to specify or enforce policies based on dynamic or resource attributes, such as allowing access to a Web part if user is accessing it from inside the firewall, or if the user's security classification is equal to or greater than that of the Web part).
- Specifying and enforcing permissions at a granular level (for example, on individual documents rather than the full document library) is difficult and time-consuming to administer.

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

- It is costly and complex to enforce access control policies consistently between SharePoint and the rest of the enterprise IT and application infrastructure, a challenge that is amplified in heterogeneous environments.

Figure 1. Cisco Policy Management for Microsoft SharePoint



Cisco Enterprise Policy Manager Integration with SharePoint

Cisco Enterprise Policy Manager is designed with a distributed multi-tiered architecture which allows for a seamless integration with SharePoint using “agent” software that painlessly installs and executes natively within the SharePoint server. The Cisco Enterprise Policy Manager agent, deployed as a dynamic-link library (DLL) file, intercepts all requests to the SharePoint server and evaluates the request against policies that are configured using a central Cisco Enterprise Policy Manager administration interface.

Using Cisco Enterprise Policy Manager with SharePoint, your enterprise can achieve the following:

Enhance Security and Visibility

Cisco Enterprise Policy Manager enables SharePoint administrators and information security personnel to set access policies to more precisely match existing business rules and relationships. The Enterprise Policy Manager policy decision engine can account for a number of factors that are impossible to capture in static permission/role definitions. For example, a financial analyst may want to set up a SharePoint site for developing a periodic U.S. Securities and Exchange Commission (SEC) filing in collaboration with other team members. Given the sensitivity of the project, the analyst can apply policies based not only on the identity of the user, but also based on where the user is located, whether the user is on a corporate-managed PC, and what the date and time are (for example, to block access after the filing is submitted).

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

Lower Administrative Cost and Accelerate Time to Deployment

Cisco Enterprise Policy Manager simplifies the administration of SharePoint sites because it logically separates the process of creating access policies and permissions from creating the site itself. SharePoint designers or site owners can focus on compiling content for the site while administrators establish the security for the site. Site administrators can utilize existing policy templates so access rules do not have to be re-created each time a new site is deployed. Moreover, the rich delegation functionality in

Cisco Enterprise Policy Manager enables granular access policies to be administered independently at multiple levels. For example, corporate-wide policies can be specified centrally and applied consistently to all SharePoint instances, while line-of-business or departmental policies can be independently managed and enforced. Custom Web parts that require special-request handling can use the powerful Cisco Enterprise Policy Manager policy engine, eliminating the need to write custom code. Furthermore, policies in Cisco Enterprise Policy Manager can be based on resource or user data in any existing enterprise directory or local database, removing the need to replicate all user resource information into Active Directory and maintain synchronization between multiple stores.

Enforce Compliance and Streamline Audits

Without Cisco Enterprise Policy Manager, meeting regulatory and governance requirements is very challenging, if not impossible, due to an inability to specify and enforce segregation of duty policies, and due to the lack of a central policy authority with which to query access rules and inspect historical activity. Cisco Enterprise Policy Manager provides rich on-demand audit and review functionality, including real-time reports and alerts on user and administrator activity in SharePoint.

As organizations deploy more portal and collaboration tools to empower their information-workers, it is crucial to ensure security and compliance are not compromised. Cisco Enterprise Policy Manager is a unique solution that brings enterprise-class security, privacy, compliance, and governance to SharePoint deployments and enables organizations to deploy SharePoint with confidence.

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, 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 C22-453511-00 02/08

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