Securing and Managing Web Resources with IBM SecureWay Policy Director

Abstract

Web technologies have revolutionized the delivery of information and services. Providing business functions such as customer service, sales, and purchasing via the Web has become a prerequisite to be competitive. Customers, partners and business constituents need real-time access to corporate information. To automate core business processes, a company should give its users, who are as likely to be customers or suppliers as employees, access to corporate information and applications through a comprehensive extranet.

Unfortunately, Web applications and enterprise management tools provide, at best, piecemeal security and access control. Organizations need a framework for making authorization decisions, instead of relying on a custom access control service for each server and application. IBM SecureWay® Policy Director centralizes network security management, providing centralized access control for corporate information. In addition, Policy Director manages security for Web, CORBA®, legacy and custom applications centrally. Policy Director WebSEAL® is the component that provides access policy management to Web-based resources, application servers and traditional enterprise applications. WebSEAL manages the Web space centrally, linking all Web servers into one logical Web space.

Introduction

Corporate use of Web technology has exploded in recent years. While most organizations used the first Web applications to offer generally available information over the public Internet, intranets and extranets that support key business functions have become requirements for many competitive businesses. As a result, more corporate information and applications are being made available over the Web. Successfully managing and securing corporate Web resources has become a more complex challenge as Web use has matured. Organizations that need their employees to access their intranet remotely via the Internet, or that want to automate their supply chain through an extranet, should consider a host of security and management concerns that are unique to these situations.

The nature of threats to security and the way information is managed have changed. As organizations expand their intranets, moving from static content to including self-service applications and enabling electronic business value chains, more sensitive information is made accessible via the Web. For example, providing access to account information for customers and business partners and forming extranets to automate the supply chain are strategies that require sensitive information to be securely provided on the corporate Web. This expansion of Web usage has changed what it means to secure the Web space. An organization should control not only who accesses its corporate Web, but also which resources each individual user can access. In order to reap the benefits of a sophisticated intranet or extranet, an organization should

control access to all information available through the Web, allowing users to access everything they need, but nothing more.

Businesses can no longer afford to focus solely on “keeping the bad guys out.” The ability to provide ubiquitous access to information means that corporate intranets can leave an organization vulnerable to internal attacks if they are not adequately secured. In a March 1999 report, the Computer Security Institute (CSI) noted that unauthorized access by insiders rose for the third straight year, and that 55% of the organizations surveyed reported intrusions by employees.

In order to take advantage of the Internet, organizations should provide Web-based access to confidential information. Internal and external users with varying needs and permissions should be able to access different resources maintained in the corporate intranet - and each user should be able to access only information for which he or she is authorized. Adding to the complexity of the problem, few organizations have the luxury of building their information systems from scratch. What most companies need are tools that can blend new technology with their existing legacy systems to provide security to all resources and applications accessed through the Web.

There are several key requirements that should be met to manage information securely on a corporate intranet. First, the identity of an individual wishing to access the intranet should be authenticated. This process is complicated when employees or business partners access information from multiple computers, and often from remote locations over the Internet. Users should be able to authenticate from a Web browser, with no client software requirements. In addition, there are often hundreds of Web servers in a large enterprise, and users need access privileges for each server they access. This can lead to many problems: users should remember passwords for many servers, administrators need to manage the access controls for each individual server, and the adding and removing of many separate entries when a user’s access privileges change or when employees join or leave the company. A security solution that lets the organization manage access controls for all of these servers centrally and presents users with a single sign-on to the Web space can greatly simplify security management as well as the user’s experience and productivity.

Once a user’s identity has been authenticated, his or her access privileges should be determined. An authenticated user does not necessarily have any permissions to access resources. Security policies should explicitly grant access rights to Web resources. An access control decision function must establish whether requests for specific information should be granted or denied. Again, administration is complicated if access controls must be configured at each Web server. Furthermore, it is difficult to construct a comprehensive picture of a user’s privileges in the Web space if an administrator must consult each Web server’s configuration information. A centralized authorization framework greatly simplifies administration.

Additionally, a system needs to log all attempts to access corporate resources to determine that the system is secure. This logging can also facilitate management decisions by allowing analysis of use patterns.

A final consideration becomes important in large businesses where it is often necessary to delegate the management of security and privileges for certain information resources to either the individual or group responsible for them. A security system should facilitate secure delegation of privilege management.

An important concern with any security management solution, along with how effectively it provides secure transmission, authentication, access control, and auditing, is how easy it is to implement and administer. For any security solution to be truly effective, it should integrate easily with the organization's existing infrastructure, and the security features must be easy to administer. Any difficulties in security management increase the possibility of human errors.

This paper will discuss these management and security issues in greater detail and will explain how Policy Director WebSEAL answers these concerns.

Security Policy Management

Providing security to a corporate Web environment means several things. Authentication of users, control of access privileges, auditing, and logging are all essential elements of any security management solution.

Authentication

WebSEAL provides a flexible authentication service, and can be integrated with an authentication mechanism through the Policy Director Credential Acquisition Service (CAS). Out of the box, WebSEAL can authenticate users with a username and password passed over a secure SSL connection or using Public Key certificates. Policy Director supports custom certificate signature and revocation checking. Policy Director integrates with Public Key Infrastructure (PKI) from leading vendors such as Baltimore, Entrust, and VeriSign, and supports the mapping of public key credentials to access permissions.

Once a user is authenticated, Policy Director grants the user authorization credentials that include identity information such as to which groups the user belongs and with which roles they are associated.

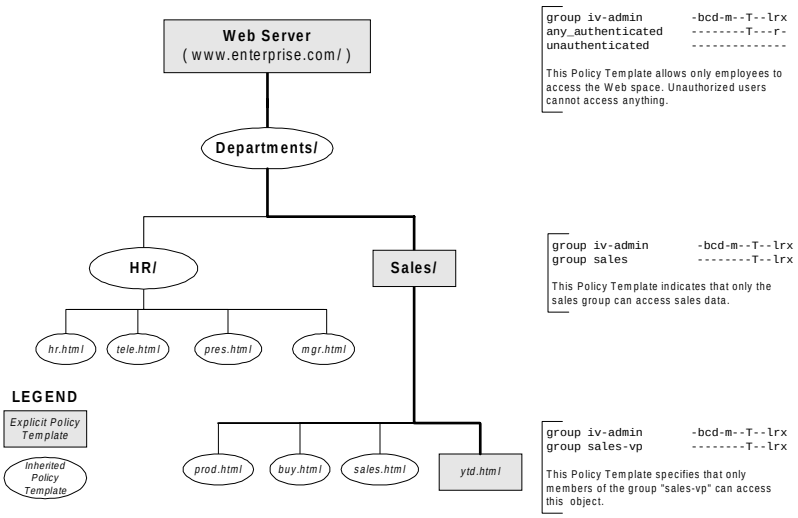
Authorization

Access Policy Management is the key to enabling Web-based e-commerce. Once a user's identity is determined, the most important question becomes what can this user do and see?

After a user has been authenticated, Policy Director Authorization Services allow that user to access only information for which he or she is authorized. Policy Director WebSEAL creates a logical Web space for the association of access control information with resources. This namespace is discussed in more detail in the Management and availability section of this paper. Authorization Services maintains authorization policy in a central repository, which lists all resources in the secured intranet and the Policy Templates (Access Control Lists) associated with each resource. Policy Templates dictate the conditions that must be met for a user to access and manipulate the resource. Each time a user attempts to access a resource, their credentials are checked against the authorization policy for that resource. This model allows authorization policy information to be maintained centrally - not passed to the user desktop.

The Policy Director Authorization Services provide access policy inheritance, authorization by group membership, and role-based access control. The Authorization Services can be replicated for high availability. Availability will be discussed in more detail in the “Management and availability” section of this paper.

WebSEAL lets an organization structure the repository of authorization information according to the logical hierarchical structure that the organization chooses. Using this structure, Policy Director applies an inheritance scheme to all resources. Unless a Policy Template is set explicitly for a resource, it automatically inherits the Policy Template of the object immediately above it in the tree structure. This means that Policy Templates need to be applied only where access policy changes. Figure 1 shows an example of this structure. In this example, the general corporate security policy is set at the top of the tree. This limits intranet access to employees only. Below this, the “sales group” has established its own authorization policy for its departmental sub-tree, and the “year to date” information has been set explicitly to be accessed only by members of the group “sales vp.” All information that does not have an explicit Policy Template inherits the next highest specified Policy Template in the tree. In the case of sales information, all information except for “year to date” inherits the Policy Template set at the “sales/” level; the rest of the information in the example inherits the Policy Template set at the Web server (www.enterprise.com/).



Explicit and Inherited Policv Template

Figure 1. Policy Template Inheritance

Inheritance eliminates the need to explicitly define a Policy Template for each individual object, reducing the memory requirements for and easing the administrative burden of authorization. This example illustrates how WebSEAL can be used to securely delegate the security management of a portion of the Web space. In this example, the company delegated the management of access control of sales information to the sales department.

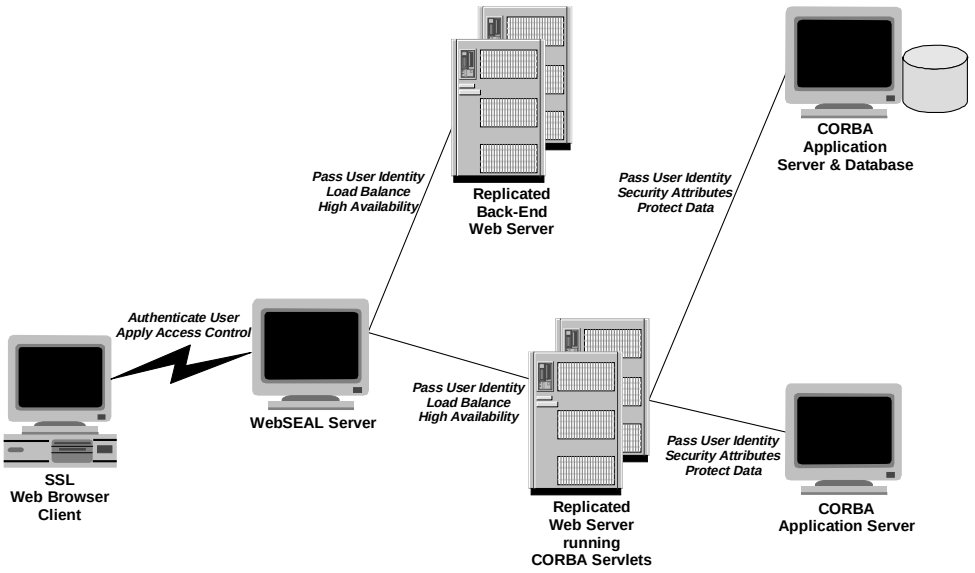
Policy Director also integrates with many third-party-authorization engines. Often, an organization already has an extensive database of access privileges for some of their network resources, and the Policy Director External Authorization Service can incorporate existing authorization and rules engines, such as RACF. The External Authorization Service can call out to the appropriate application to determine if a user has access privileges for a resource. This allows Policy Director to integrate with an organization's existing security policy and infrastructure. This integration enables extension of the Policy Director security model to use rules, such as allowing access to certain resources only at certain times of the day.

Policy Director can integrate with existing applications through an authorization API (aznAPI, submitted as the specification to be standardized by the Open Group) that allows third-party or custom applications to implement authorization decisions. Policy Director maintains the trust required to provide security at any level of a multi-tiered application, providing the appropriate credentials at all levels.

Policy Director allows an administrator to set access privileges for dynamically generated resources using the same policies that govern static resources. This lets an organization secure access to databases and other back-end applications that are accessed through a Web interface.

Logging and Auditing

The ability to log and audit all access attempts is essential to secure the corporate Web.



Monitoring access attempts by all users lets administrators detect security risks. Policy Director centrally logs all access attempts using a standardized format and generates easy-to-read reports. This log can be securely passed to a third-party database system for analysis of usage patterns.

Single Sign-on

Policy Director WebSEAL provides a single sign-on to the corporate Web space. Policy Director can integrate with Web applications, passing a user's login information to the application transparently to the user. With Policy Director, users must only log in once. They can then access all Web-based resources and Web applications for which they are authorized. In addition, WebSEAL used with IVCorba™, the Policy Director CORBA security solution, provides a single sign-on to Web and CORBA resources. This is shown in Figure 2.

Figure 2. WebSEAL Single Sign-on for Web and CORBA Resources

Management and Availability

Large companies have tens to hundreds of Web servers and Web-enabled applications that should be secured. Managing user access individually on each server, either with the server's native capabilities or with a plug-in access control mechanism is time consuming and can result in a huge duplication of effort. Furthermore, keeping access privileges accurate, and making changes to all systems, such as removing an employee when he or she leaves the company, is difficult.

Policy Director WebSEAL provides a gateway to your network. WebSEAL is a secure front-end to your Web resources, providing logical view of your resources that simplifies both administration and the user experience. Furthermore, Policy Director Smart Junctions™ enables replication of resources to provide a highly available environment.

Logical Web Namespace

Management of information can be simplified if the company organizes corporate Web resources in a logical Web namespace - in which content is accessed through a URL (Universal Resource Locator) address that reflects a logical structure chosen by the organization. This allows information to be organized logically, such as by department or on a project basis, instead of by the physical location of the resource.

To create a logical Web space, WebSEAL is positioned in front of an existing Web server and its corporate Web resource tree. WebSEAL associates a user-defined logical name (as part of the logical URL) to refer to the Web server content. When a user requests a resource (using the logical URL), the server intercepts the request and uses Smart Junctions to match the logical name with the physical address of the Web server. In effect, Policy Director translates the logical URL, locates the information and returns it to the user - who does not need to know anything about the physical location of the information.

This structure allows access policy to be set at WebSEAL, rather than individually at the physical servers on which the information resides. Smart Junctions enable support for any back-end Web server, including Microsoft® IIS, Netscape and Apache.

In addition to transparently supporting any Web server, the Policy Director logical Web space can also include resources accessed by Web-enabled applications such as PeopleSoft 7.5 and SAP R/3. This means Policy Director controls access to information accessed from legacy databases and other back-end applications in exactly the same manner as static Web resources. Figure 3 shows how use of Smart Junctions facilitates one type of logical addressing scheme.

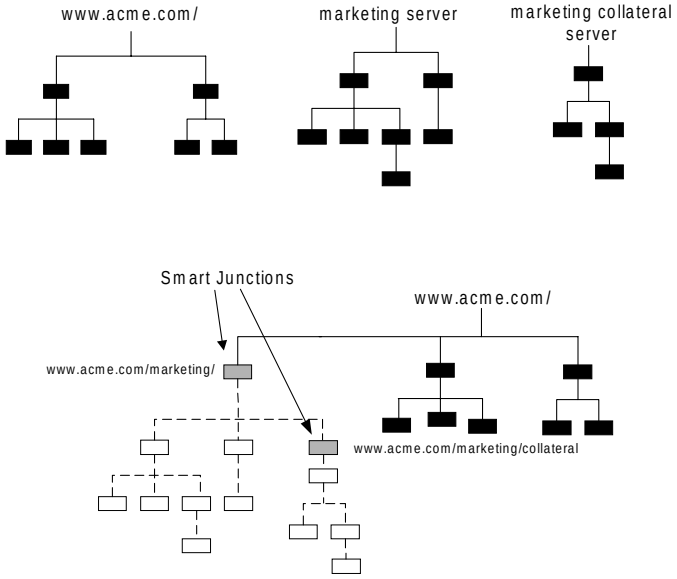


Figure 3. Junctioning in the Web Namespace

In this example, the company has developed an address scheme in which all the information for one department can be found in a single location, marketing, even though it is maintained on multiple machines. This makes it easier for a user to access information and makes the Web easier to administer. Smart Junctions allow an organization to create whatever type of address structure will be most useful for it. For example, information could be grouped on a project basis or by subject matter, rather than by department. Also, the groupings can be easily adjusted as the needs of the organization change. Using Policy Director, an organization can reorganize its Web namespace without having to move Web-based information between servers.

The logical addressing scheme also makes it easier to make changes to the network. If information must be moved between servers, or a new server added, the Web administrator can

make the change and then adjust the Smart Junctions. Users will never know a change took place - unless they realize it as greater speed and efficiency.

As discussed in the “Security Policy Management” section of this paper, the use of a logical Web namespace also simplifies security administration as WebSEAL can set access policy against the logical Web space instead of at each server.

Load Balancing and High Availability

Smart Junctions can be used to mount multiple Web servers with replicated contents at the same point in the logical Web space. When this is done, WebSEAL performs intelligent load-balancing across the replicated servers for improved performance and fault recovery. This allows that security administration of Web resources is available at all times, even in the event of system maintenance or failure. Using Smart Junctions, Web server capacity can be added in a linear fashion as demand on the corporate Web infrastructure increases.

Furthermore, all Policy Director services can be similarly replicated, providing high availability and fail-over.

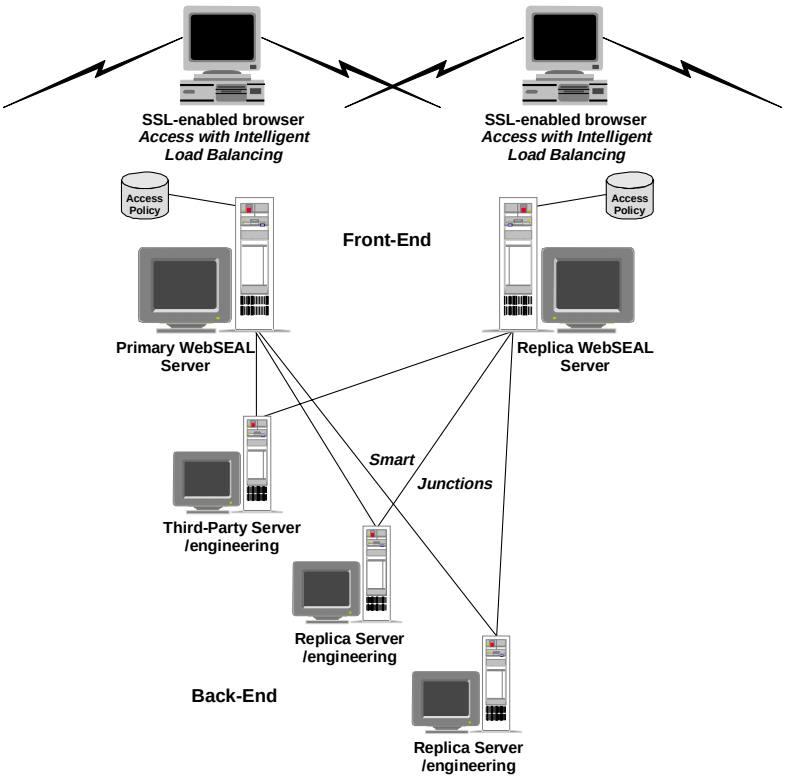


Figure 4. Junctioning of Replicated WebSEAL and Back-end Servers

Administration

The Policy Director management console provides central management of Policy Director security services. The Java™-based console lets an administrator easily manage users, groups, and roles for the entire network from one central location. This means administrators no longer need to manage accounts on the hundreds of Web servers and applications used in a modern Web-driven enterprise.

Policy Director integrates with existing security infrastructure, such as PKI, and maintains user information in an LDAP-compliant directory. The management console can be used to manage the directory.

The Policy Director management console also gives administrators a centralized view of user privileges. Because all access rights information is maintained centrally, an administrator can easily examine a user's total privileges in the Web space, and can easily change those privileges.

Policy Director provides a flexible administration model. Administrative ability can be delegated, meaning the administration of subsets of resources can be delegated to the appropriate business units. Also, the definition of security policy can be separated from its implementation.

Summary

Businesses today need solutions that address security, scalability and management for all Web-based traffic. Policy Director is the authorization and management solution that scales across the entire enterprise.

Policy Director WebSEAL provides centralized authentication and access control administration. WebSEAL allows replication of Web servers and immediate updates to access control information. Policy Director improves system performance by load-balancing traffic and maintaining a highly available system. It can significantly reduce administration costs by delegating privilege-management functions to business owners.

Policy Director WebSEAL provides fine-grained access level authorization that protects Web resources, across multiple operating systems, Web servers and Web-enabled databases and applications. By providing a centralized access control solution, WebSEAL enables the deployment of e-commerce infrastructure. With Policy Director, management can be confident that only those with a need to know will be able to access information. Because security concerns have been answered, your company can make information available to users to a far greater degree than was previously possible. Policy Director users have complete mobility. Their identities follow them wherever they go, allowing secure access to corporate information from home or a hotel room across the country.

SecureWay Policy Director products are based on open standards; they support both symmetric-key and public-key encryption and authentication. Policy Director supports junctioning of all third-party Web servers, including those developed by Apache, Microsoft, and Netscape. WebSEAL support of dynamic URLs allows access controls to be applied to any application with a Web interface, including PeopleSoft 7.5, SAP R/3, Lotus® Domino™, and Oracle Web Server. WebSEAL provides a single sign-on to all resources accessed through the Web.

Trademarks

IBM and SecureWay are trademarks of International Business Machines Corporation in the United States and/or other countries.

WebSEAL, IVCorba, and Smart Junctions are trademarks or registered trademarks of DASCOM, Inc.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Domino and Lotus are trademarks of Lotus Development Corporation in the United States and/or other countries.

Microsoft, Windows, Windows NT and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Other company, product and service names may be trademarks or service marks of other companies.