Securing and Managing Web Resources with IBM SecureWay Policy Director

White Paper

Version 2.0

March 1999

SMW0898

Table of Contents

Abstract

To use technologies that automate mission-critical business processes, organizations must maintain sensitive information on the corporate Intranet. Unfortunately, Web applications and Enterprise management tools provide, at best, piecemeal security. IBM® SecureWay® Policy Director centralizes network security management, providing access control over all corporate information from one console. Policy Director manages the Web space centrally, linking all Web servers into one logical Web space. Policy Director can manage security for the entire network from one central location.

Chapter 1

Introduction

While most organizations used the first waves of Web applications to offer generally available information over the public Internet, many organizations are now using Web technologies to distribute and share sensitive corporate information with both employees and external partners, through Intranets and Extranets

Corporate use of Web technology has expanded significantly in recent years. While most organizations used the first waves of Web applications to offer generally available information over the public Internet, many organizations are now using Web technologies to distribute and share sensitive corporate information with both employees and external partners, through Intranets and Extranets. 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 public Internet, or that want to give their business partners access to some of their Web-based resources, must consider a host of security and management concerns that are unique to these situations.

The nature of threats to security has changed as the way information is managed has changed. More and more sensitive information must be made available on the corporate Web as organizations expand their Intranets, moving from simply posting information to including self-service applications and enabling electronic business. The use of Web technology to perform mission-critical business transactions, use of Web-enabled applications that can access legacy databases, and the formation of Extranets with business partners are examples of Web usage that rely on the ability to maintain the security of sensitive information on the corporate Web. This expansion of Web usage has changed what it means to secure the Web space. An organization must now be able to control not only who accesses its Intranet, but which Web resources each individual user can access. In order to reap the benefits of a sophisticated Intranet environment, an organization must be assured that information stored on the Web can only be accessed by individuals who are authorized to view it, often only a small subset of the employee population.

One concern with corporate Intranets is that they 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. Most companies have many levels of information, and employees with varying needs and permissions must be able to access different resources maintained in the corporate Intranet – and each employee must only be able to access 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 older legacy systems to provide security to all Web resources and Web-enabled applications.

What most companies need are tools that can blend new technology with their older legacy systems to provide security to all Web resources and Web-enabled applications

There are several key requirements that must be met to securely manage information on the corporate Intranet. First, the identity of an individual wishing to access the Intranet must be authenticated. This process is complicated when employees or business partners access information from multiple computers, and often from remote locations over the public Internet. 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 must remember passwords for many servers; and administrators need to manage the access controls for each individual server, adding and removing many separate entries when a user's access privileges change, and when employees join or leave the company. A security solution that lets the organization manage access controls for all of these servers centrally can greatly simplify security management.

Once a user's identity has been authenticated, that user's access rights to Web resources must be established and requests for specific information authorized 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. The ability to maintain a centralized access control database greatly simplifies administration.

For any Web space to be secure, a secure method of communication must be used when any sensitive data is being transmitted. This includes during authentication, when user account names and passwords are transmitted. Secure data transmission is especially important when sensitive data travels over the public Internet, such as when employees access the Intranet remotely, from home or on the road, and when an organization forms an Extranet with its business partners.

For any security solution to be truly effective, it must integrate easily with the organization's existing infrastructure, and the security features must be easy to administer

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

An additional consideration becomes important in a large organization where it is often useful or necessary to delegate the management of security for certain information resources to either the individual or group responsible for them. A security system should facilitate secure delegation of management.

An important concern with any security 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 must 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 error.

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

Chapter 2

Management

One factor that complicates Web administration is the structure of the Web namespace. Static Web information is maintained in a tree structure and Web addresses reflect this, frequently resulting in long and non-intuitive addresses. Additionally, in most organizations, information that goes together is not necessarily stored together. Web administrators make decisions about where to store information based on practical concerns such as space requirements and frequency of use. This can lead to a complicated address scheme for information stored on the corporate Web, and a system that lends itself to service disruptions every time a Web administrator must make changes, such as moving content between servers.

> *Management of information can be simplified if the organization uses a logical Web namespace – in which content is accessed through a URL address that reflects a logical structure chosen by the organization*

Logical Web Namespace

Management of information can be simplified if the organization uses 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, such as by department or on a project basis, instead of the physical location of the resource. Policy Director allows an administrator to create just such a logical Web space.

To do this, Policy Director is positioned in front of a corporate Web tree or sub-tree. When a user requests a resource (using the logical URL), the server intercepts the request and uses Policy Director Smart Junctions to match the logical address with its physical address. 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.

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. Policy Director supports the dynamic URLs used by these applications, allowing them to be managed just like static URLs. This means that information accessed from legacy databases and other back end applications can be secured by Policy Director security, in exactly the same manner as static Web resources. Dynamic URL support will be discussed in greater detail in Section 3. Figure 1 shows how use of Policy Director Smart Junctions facilitates one type of logical addressing scheme.

> *Using Policy Director, an organization can reorganize its Web namespace without having to move Web-based information between servers*

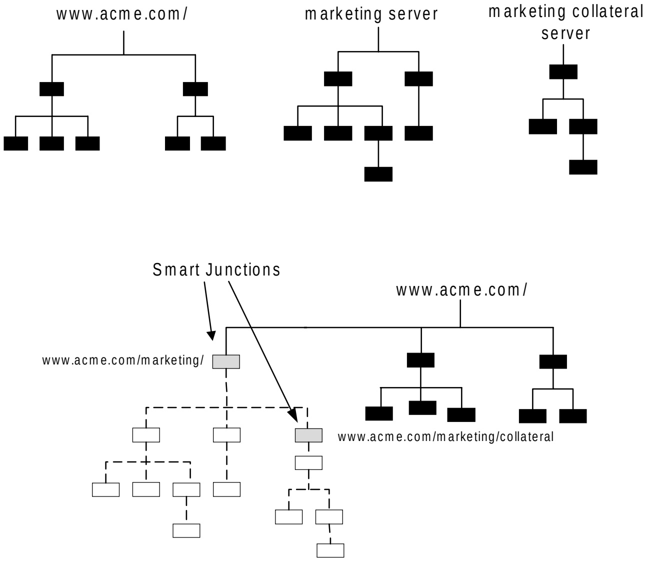


Figure 1. Junctioning in the Web Namespace

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. Policy Director 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 do it, and, as long as he adjusts the Smart Junctions, users will never know a change took place – unless they realize it as greater speed and efficiency.

The use of a logical Web namespace has other benefits when the security of the system is considered. These will be addressed in appropriate parts of the security section of this paper.

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, the Policy Director management services perform load balancing across the replicated servers for improved performance and fault recovery. This ensures that Web resources are 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.

Using Smart Junctions, Web server capacity can be added in a linear fashion as demand on the corporate Web infrastructure increases

Furthermore, Policy Director security services can be replicated the same way. By replicating the authorization services and the access control database over multiple junctioned Policy Director servers, an organization can avoid a bottleneck at the authentication or authorization manager, as well as providing high availability and fail over.

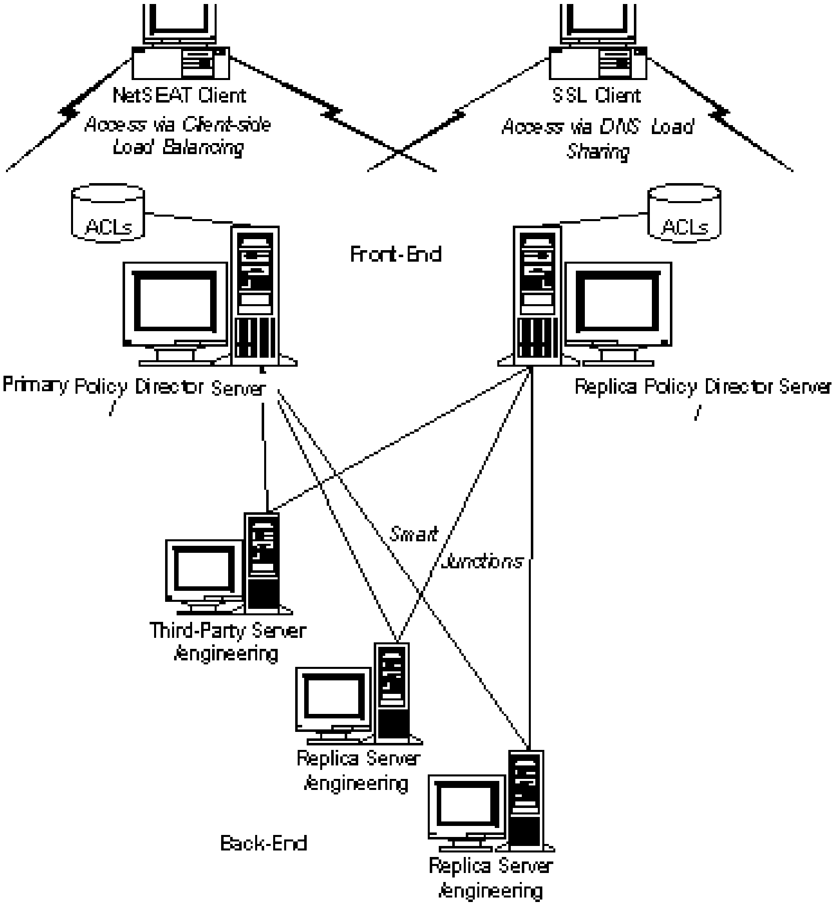

NetSEAT Client
Access via Client-side Load Balancing
SSL Client
Access via DNS Load Sharing
ACLs
ACLs
Front-End
Primary Policy Director Server
/
Replica Policy Director Server
/
Smart
Junctions
Third-Party Server /engineering
Replica Server /engineering
Back-End
Replica Server /engineering

Figure 2. Junctioning of Replicated Policy Director 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.

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

Chapter 3

Security Policy Management

Providing security to a corporate Intranet means several things. Secure communication, authentication of users, control of access privileges, auditing, and logging are all essential elements of any security management solution.

Secure communication, authentication of users, control of access privileges, auditing, and logging are all essential elements of any security management solution

Secure Communication

Policy Director can communicate with a Web browser in three ways: secure communication using an SSL-enabled browser with the Policy Director Public Key Management Service (PKMS), secure communication with the Policy Director NetSEAT client using a secure tunnel built on the GSSAPI (Generic Security Services API), and unsecured HTTP traffic.

The Policy Director Public Key Management Service supports secure communication with SSL-enabled browsers such as Microsoft Internet Explorer and Netscape Communicator. Policy Director NetSEAT establishes a secure tunnel with Policy Director, and intercepts all communications from the client computer, and routes them through the secure tunnel. NetSEAT can be downloaded and installed by a user in a matter of minutes.

In the case of unsecured HTTP traffic, the Policy Director Authorization Service recognizes that the user cannot be securely authenticated and that communication is not secure, and it applies the appropriate access control policy.

Authentication

Policy Director provides a flexible authentication service. Users can authenticate themselves using a DCE/Kerberos login with NetSEAT, a user name and password passed over a secure SSL connection, or using Public Key certificates. Policy Director supports the mapping of public key credentials to access permissions. The Policy Director Public Key Management Service provides the means to integrate Policy Director with an existing corporate public key infrastructure using certificate authorities, X.509 certificates, and revocation lists.

Access Control

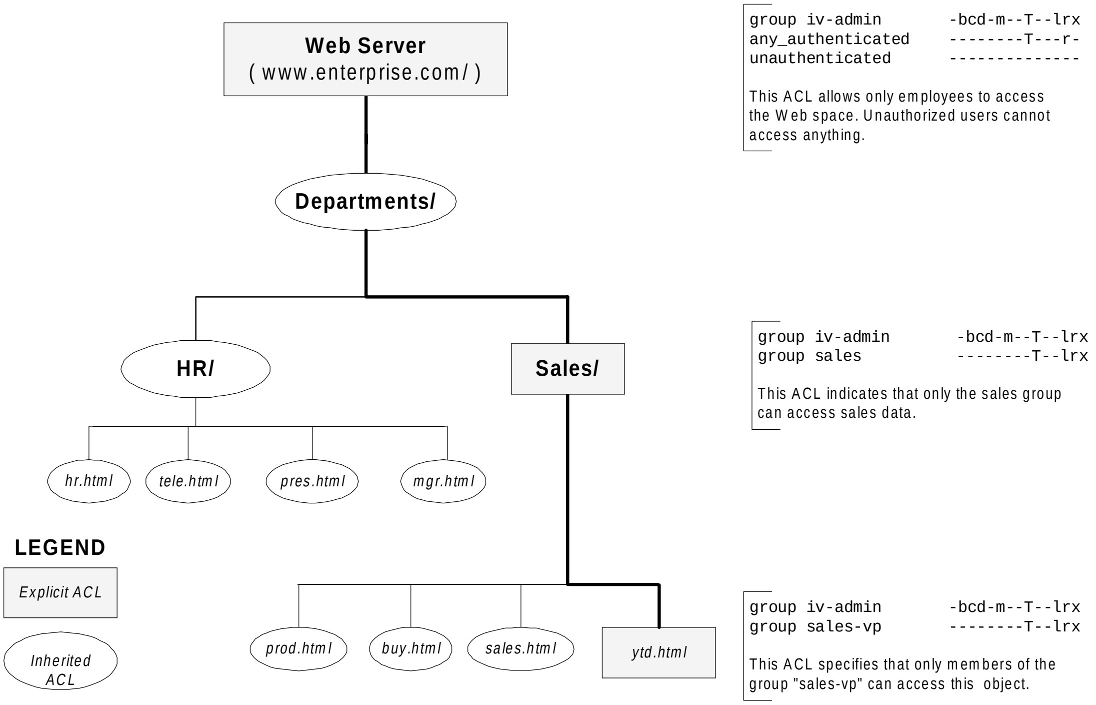
After a user has been authenticated, Policy Director Authorization Services only allow that user to access information for which he or she is authorized. Policy Director Authorization Services use a central database that lists all resources in the secured Intranet and the Access Control Lists (ACLs) associated with each resource. ACLs dictate the conditions that must be met for a user to access and manipulate the resource.

Policy Directory can create, revoke, and modify any user's access privileges in real time. Access privileges change as soon as the administrator enters the changes – there is no need to restart the servers

Policy Director can create, revoke, and modify any user's access privileges in real time. Access privileges change as soon as the administrator enters the changes – there is no need to restart the servers.

The Policy Director authorization database provides ACL inheritance, authorization by group membership, and role-based access control – reducing the size of the database and easing the administrative burden of maintaining it. This database and the authorization services can be replicated for high availability, as was discussed in Section 2.

Policy Director lets an organization structure the authorization database according to the logical structure that the organization chooses. Using this structure, Policy Director applies an inheritance scheme to all resources. Unless an ACL is set explicitly for a resource, it automatically inherits the ACL of the object immediately above it in the tree structure. This means that explicit ACLs only need to be set where access policy changes. Figure 3 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 ACL set explicitly for it inherits the next highest specified ACL in the tree. In the case of sales information, all information besides “year to date” inherits the ACL set at the “sales/” level; the rest of the information in the example inherits the ACL set at the Web server (www.enterprise.com).



```
group iv-admin       -bcd-m--T--lrx
any_authenticated    --------T---r-
unauthenticated      --------------
```

This ACL allows only employees to access the Web space. Unauthorized users cannot access anything.

```
group iv-admin       -bcd-m--T--lrx
group sales          --------T--lrx
```

This ACL indicates that only the sales group can access sales data.

```
group iv-admin       -bcd-m--T--lrx
group sales-vp       --------T--lrx
```

This ACL specifies that only members of the group "sales-vp" can access this object.

Figure 3. ACL Inheritance

Inheritance eliminates the need to explicitly define an ACL for each individual object, reducing the memory requirements for and easing the administrative burden of authorization. This example also illustrates Policy Director's ability to securely delegate the security management of a portion of the Web space (a “sub-tree”). In this example, the company delegated the management of access control of sales information to that department.

Policy Director also integrates with third party authorization databases. Often, an organization already has an extensive database of access privileges for some of their Web resources, and Policy Director features an ACL entry that instructs the authorization manager to 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, and allows 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 also integrate with existing or future application through an authorization API that allows outside applications to access Policy Director Authorization services. Policy Director maintains the trust required to provide security at any level of a multi-tiered application, providing the appropriate credentials at all levels.

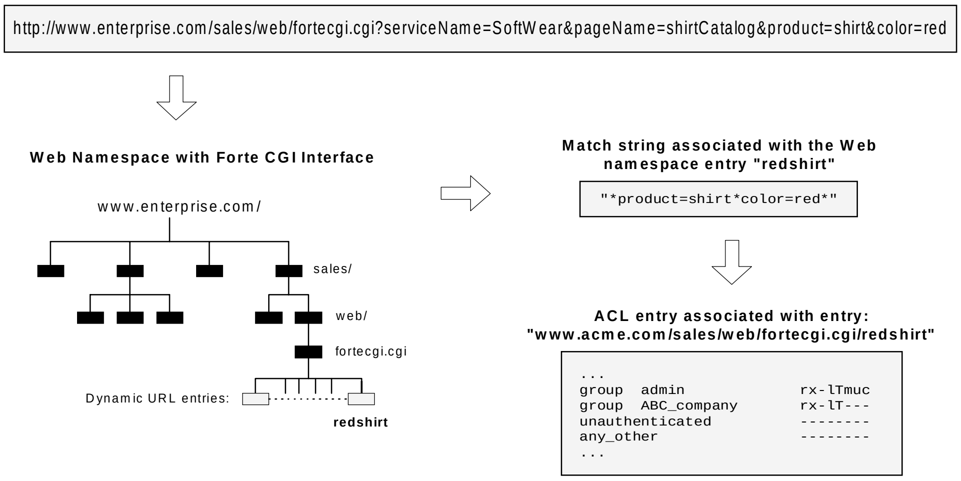
Securing Dynamically Generated Content

Policy Director's ability to manage dynamically generated URLs 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 legacy databases and other back-end applications that are accessed through a Web interface.

> *Policy Director's ability to manage dynamically generated URLs allows an administrator to set access privileges for dynamically generated resources using the same policies that govern static resources*

Policy Director secures dynamically accessed resources by placing access controls on the request for information, that is, on the dynamic URL itself. Policy Director can associate an entry in the authorization database with a Unix-style regular expression, and matches dynamically generated URLs to these expressions. This allows an administrator to set an access control entry for each regular expression, or allow the regular expression to inherit the ACL specified above it in the namespace. More than one dynamically generated URL may map to a single regular expression.

Figure 3 shows an example of this mapping feature using Policy Director with a Forté Web SDK application; however, the concept is equally applicable with any Web-enabled application, such as PeopleSoft 7.5, SAP R/3, Oracle WebServer and Lotus Domino.


http://www.enterprise.com/sales/web/fortecgi.cgi?serviceName=SoftWear&pageName=shirtCatalog&product=shirt&color=red
Web Namespace with Forte CGI Interface
www.enterprise.com/
sales/
web/
fortecgi.cgi
Dynamic URL entries:
redshirt
Match string associated with the Web namespace entry "redshirt"
"*product=shirt*color=red*"
ACL entry associated with entry: "www.acme.com/sales/web/fortecgi.cgi/redshirt"

```
...
group  admin                rx-lTmuc
group  ABC_company          rx-lT---
unauthenticated             --------
any_other                   --------
...
```

Figure 4. Authorization of a Dynamic URL.

Figure 4 shows how a namespace entry "redshirt" is created for a Forté WebSDK URL. The entry matches a string describing the actual red shirt product that was sent as a parameter to the Web application. The administrator can associate explicit ACL entries with this new artificial namespace entry or rely on the inherited security policy set higher up in the tree.

This ability to support fine-grained access control of dynamic URLs lets an organization add transparent fine-grained access control to existing Web-enabled applications without changing a single line of source code

These dynamic-URL entries are part of the logical Web namespace and benefit from all its standard features, such as inherited ACLs, third party authorization engine routing, and Smart Junctioning. This ability to support fine-grained access control of dynamic URLs lets an organization add transparent fine-grained access control to existing Web-enabled applications without changing a single line of source code. The procedure for mapping Dynamic URLs to namespace entries is detailed in the Policy Director Administration Guide.

Logging and Auditing

The ability to log and audit all access attempts is essential to ensure security of the corporate Web. The ability to monitor access attempt by all users lets administrators detect security risks. A unique feature of Policy Director is its ability to centrally log all access attempts and generate 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 provides a single sign-on to the corporate Web space. Policy Director can integrate with web applications that use basic authentication, 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 web applications for which they are authorized. This is shown in Figure 5.

Policy Director is also designed to work with Tivoli® Global Sign-On (GSO) to extend the enterprise level single sign-on that Tivoli GSO offers.

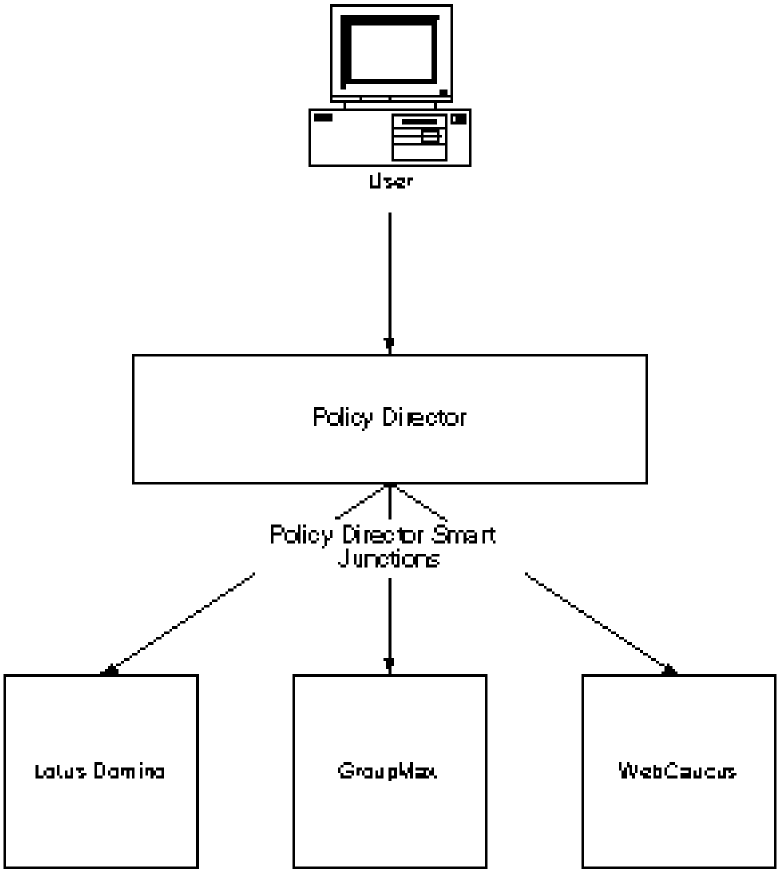


Figure 5: Policy Director Single Sign-on for Web Resources

Chapter 4

Summary

Corporate network professionals 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 provides a secure and highly available Web-based Intranet or Extranet, answering an organization's security management concerns. Policy Director provides centralized authentication and access control administration and 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 with no single point of failure.

Policy Director provides fine-grained access level authorization that protects all Web resources, across multiple operating systems, Web servers and Web-enabled databases. Policy Director provides peace of mind to companies that share Web-based information over an Intranet. With Policy Director, management can be confident that only those with a need to know will be able to access information. Employees also benefit from Policy Director. Because security concerns have been answered, your company can make information available to employees to a far greater degree than was previously possible. And 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.

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. Policy Director 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 WebServer.

Part of IBM Integrated Security Solution

Policy Director is a component of IBM SecureWay FirstSecure, a comprehensive security solution that enables e-business. Policy Director is available separately or as part of SecureWay FirstSecure .

IBM SecureWay Boundary Server, also a component of SecureWay FirstSecure, works with Policy Director to provide an extranet security framework to enable connection to business partners, customers, and remote employees over the Internet.

For More Information

To find out more about IBM SecureWay Policy Director, visit our Web site at:

www.ibm.com/software/security/policy