HP PRAESIDIUM

# DomainGuard
## Web Access and Authorization Managers
## Technical Note

*Effective Web access control is the key to success in the information game*

Use of the Internet as a communication tool is becoming more common throughout the business arena, as innovative enterprises are harnessing this power to streamline business processes through real-time information sharing.

### Executive Summary

Using Web sites on corporate networks, companies can share vital information with on-site and remote employees, suppliers, customers, and distributors. The key to success in this information game, however, is effective access control — utilizing and safeguarding the information resources of the enterprise. Organizations need to be able to quickly and easily grant specific access to authorized outside users. But before information can be shared, customers and partners need to be assured that confidentiality and security are maintained.

To meet customers' needs for secure information sharing, The Hewlett-Packard Company has developed the DomainGuard products as part of its HP Praesidium family. DomainGuard enables real-time Web data sharing between corporate departments, business units, outside partners, and customers securely and efficiently.

HEWLETT® PACKARD

# DomainGuard Access
# DomainGuard Rules

While providing robust security features, HP Praesidium DomainGuard is unique in its ease of use and flexibility. These features enable the enterprise to utilize existing resources more easily, boost productivity by decentralizing administration, and maintain flexibility for future growth.

This paper focuses on the role of DomainGuard in providing effective access control to the enterprise, how the product complements and works with other Internet security solutions, and the administrative features that simplify DomainGuard deployment and use.

### Protecting Corporate Resources through Effective Access Control

In today's competitive business environment, oraganizations are seizing the opportunities offered by new technologies, such as the Internet. Via this medium, real-time communication is possible with vast numbers of users. Enterprises are harnessing this capability to perform a wide range of business applications. While many of these involve e-commerce, the use of this communication channel for sharing vital corporate business information is also emerging as a primary application.

Through Web sites, enterprises are now capable of sharing information in real time with on-site and remote employees, as well as suppliers, distributors, customers, and business partners. And more and more companies are seizing this advantage. Sharing vital corporate information resources in real time streamlines business processes, increases productivity, reduces costs, and eliminates duplicative efforts. Employees and business partners can utilize corporate resources much as they utilize any other Web-based resource.

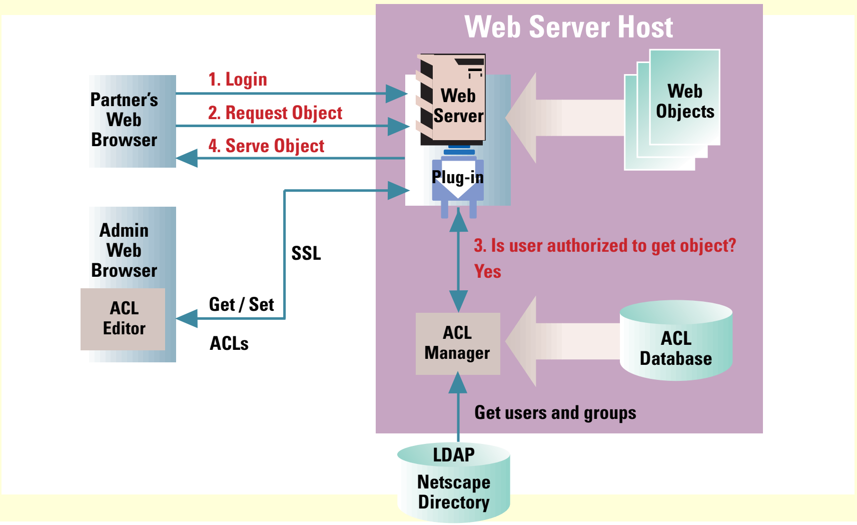
But there are challenges, too, amidst these opportunities. Companies maintain vast stores of information, much of which is not intended for widespread distribution. Whether it be related to sensitive human resources information, strategic business planning, or confidential client data, vital information must be accessible by appropriate individuals while safeguarded from indiscriminate access. Controlling access becomes a central aspect of conducting Internet business securely and effectively.

A second challenge is to integrate access control effortlessly into existing infrastructures and ensure ease of use and administration. Often, implementing a typical access control solution or creating a customized access control solution developed in-house can be costly to develop and creates scalability and support headaches in the future. The most effective access control solution is one that combines robust security with the ease and convenience of simplified administration.

### DomainGuard Product Architecture

In order to access a resource on the Web server, the user must first authenticate to the server, and then request the desired object (Web page, Java applet, graphic, etc.). When the user requests the object, DomainGuard determines what groups the user is in as defined in the LDAP directory, and what associated access rights the user has for the requested object. If theuser has the required rights, the object is served to the browser. If access is not allowed, the user receives a standard Web browser error message.

All administration of DomainGuard is done through an easy-to-use Java interface, accessible from any Java-enabled Web browser.



# DomainGuard Access
# DomainGuard Rules

**Access Control Solutions from Hewlett-Packard:**

***DomainGuard Access***
***DomainGuard Rules***

Hewlett-Packard, a leader in information technology solutions for nearly 50 years, has responded to these challenges with the DomainGuard products. With DomainGuard, enterprises can provide secure access to Web resources for employees, suppliers, customers, and business partners, all within existing Web environments and with minimal administrative requirements.

Domain Guard offers robust security features such as:

- privilege-based access rights
- transaction authorization control
- customer-defined authentication
- strong encryption support

Superior convenience and ease of administration are provided by:

- easy deployment through Web plug-in and LDAP interface compatible with existing environments
- simplified, browser-based administration
- delegable administration
- transparent, "snap-in" operation

A member of HP's prestigious Praesidium family of Internet security products, DomainGuard offers enterprises a secure and efficient tool to maximize their valuable information resources.

### HP Praesidium DomainGuard Products Overview

In developing effective access control solutions, companies have found three aspects to be of primary importance:

- ***Security:*** fine-grained access rights combined with strong user authentication to provide robust access control

- ***Convenience:*** simplified administrative functions to eliminate potential bottlenecks and enable customized access decision making at all levels of the enterprise

- ***Flexibility:*** modular design to speed and simplify implementation, to provide scalability for future growth, and to leverage existing systems and standards

### Security

The DomainGuard products offer sophisticated security features that authorize access from Web browsers to specific Web server objects such as HTML pages, Java applets, and CGI scripts, as well as specific Web-based transactions. Using the product's fine-grained access control, administrators can develop profiles for groups of users as well as individual users to specify exactly what Web-based resources and transactions they can access. Central to DomainGuard's access control capabilities is the Access Control List (ACL), which defines the access privileges each user group or individual user holds. Essentially, the ACL links the names or unique identifiers of individual users together with permission bits that identify the level of access.

DomainGuard also employs LDAP directories to obtain these unique identifiers and simplify access control management. In DomainGuard, the unique identifier that names a group of users defined in an LDAP database is linked with an ACL entry with defined access rights. By linking the two technologies — ACL and LDAP — the product provides comprehensive access definition capabilities as the enterprise expands.

***Privilege-based Access Rights.*** DomainGuard permits essentially three types of access privileges. The first is access that enables the user to take some type of action involving the Web object itself. These access privileges are read, write, or execute. Read access enables a user simply to read the Web object; for instance, a customer with read access might be able to review the status of his or her order. In contrast, write access enables the user to exchange information related to the Web object. In the case of a supply chain management enterprise, a user with write access might be enabled to enter inventory data. With execute access, a user can run

## DomainGuard Access

The DomainGuard products are designed to offer the highest level of security while easily integrating into existing systems. With DomainGuard Access, HP provides security to the object level of the Web server. Users can be granted specific access rights to various objects on the server including Web pages, graphics, Java applets, CGI scripts, etc.

## DomainGuard Rules

With DomainGuard Rules, the additional functionality of transaction authorization control is added. Now an organization can define specific rules for what web-based transactions can be processed, and the ability to block unauthorized transaction from ever accessing back-end resources.

an executable file, such as a CGI script or Java applet. One likely scenario for this access level would be when a user was updating database information via a form, which a CGI script or program would then use to update the database.

## A DomainGuard Administration Case Study

A corporate project manager (PM) would like the project's marketing engineer, who telecommutes part-time from home, to review the team's draft quarterly report before the document is released to the management team. The previous afternoon, the PM asked the engineer to review the document after nine the next morning, and sent feedback by e-mail before lunch. Since the PM has full access privileges over the project directory on the corporate Web server, it will be easy to modify the marketing engineer's access first thing in the morning.

The project manager has already arranged with the company Webmaster to have the document placed in the directory, so only a few minutes is needed to modify the document's ACL to provide appropriate access. The PM accesses the DomainGuard ACL Editor from the desktop, and locates the directory in the document tree display. Opening this directory, the quarterly report document that requires review is located. Its ACL is identical to the project directory ACL via the concept of inherited ACLs. Then to modify the marketing engineer's access to the report, the PM must now modify the report's ACL by adding the engineer's unique identifier to the document's ACL entry. Once this information is located and the engineer's identifier is added to the ACL entry, the PM selects the read access option to enable review of the document.

To finish, the PM clicks the appropriate key to apply the change and exits the ACL Editor. Later that morning, the marketing engineer logs on from home, reviews the report, and sends feedback to the PM before taking the family to the park for lunch.

The second type of access privileges provided by DomainGuard are navigational in nature; that is, they enable a user to move throughout the Web server "tree" of directories and subdirectories. These types of access rights ensure that enterprises safeguard the very presence of sensitive information by preventing users from even seeing the names of files or subdirectories as well as enabling access to specific directories and objects down a branch of the directory tree. "List" access permits appropriate users to see the content of a specific Web server subdirectory. "Traverse" privileges govern access to broad sections of Web servers by permitting or restricting access to entire branches of the directory tree. For instance, a customer might have traverse privileges to the Web directory branch containing order information but not to the branches related to inventory or marketing.

A third type of privilege involves delegation of administration of the access control for other users. This privilege, referred to as "Control" right, enables the user to edit or modify ACLs for specific Web objects. In the case of a project manager, for instance, control access would enable her to manage project team members' access to project information as appropriate. Also, content owners can now be given the ability to decide who has access to the information they already create and manage. This is a great benefit for not only the IT department who no longer has to manage all access control, but also to the content owner who now has more control over the information created.

***Transactional Access Control.*** DomainGuard Rules extends access control to Web transactions. This enables enterprises to establish access criteria using unambiguous business rules. By testing values from fields on Web forms, DomainGuard Rules can enforce specific business rules and ensure that transactions satisfy security policies. Users attempting transactions that fail these rules are prevented from accessing Web resources, while those who satisfy the criteria obtain data transparently.

***Customer-defined Authentication.*** DomainGuard supports different authentication methods to meet various corporate security policies. One method involves the use of user names and passwords for client-side authentication. The password is validated against a value stored in the LDAP directory. Management of user names and passwords is done my using administration tools supplied with the LDAP directory. The other type of authentication involves the use of client-side digital certificates. The Web server will test the certificate, based on the X.509 standard, for validity. If the certificate is determined to be valid, the server opens it and makes it available to DomainGuard. The software verifies access privileges in the process described by the sidebar. This flexibility enables companies to implement access control protection regardless of where they are on the security continuum. And, as an enterprise moves from the use of user names/passwords to certificate-based authentication procedures, DomainGuard will continue to provide effective access control.

***Encryption Support.*** DomainGuard provides strong encryption support to ensure that sensitive information is safeguarded from unauthorized users. The product supports both SSL encryption and VPN (virtual private network) solutions. Regardless of whether an enterprise is employing SSL, available on most Web browsers and servers, or the more robust VPN solution, DomainGuard can continue to provide comprehensive access control.

### Convenience

Among access control products, DomainGuard stands alone with unique features that streamline implementation and ease ongoing administration. Rather than requiring customized code revisions for implementation, the product can be

# DomainGuard Access
# DomainGuard Rules

quickly and easily installed into existing Web environments. Many customers were able to install and configure DomainGuard into an existing Web environment in only a few hours, not days or weeks. Simplified administrative features eliminate IT bottlenecks and boost productivity throughout the extended enterprise.

DomainGuard employs a concept of "sparse ACLs" to achieve many of these streamlined administrative capabilities. Essentially, this means that any object in the directory tree that does not have an ACL explicitly set for it inherits the ACL of the directory above it in the directory tree. For instance, if a directory tree contains a subdirectory `/projectX/docs/`, any object, whether it be a document or another subdirectory, that is added to docs will inherit the ACL of `/projectX/docs/`. Thus, if a project manager has write access to `/projectX/docs/`, he will have write access to everything within it, such as `/projectX/docs/mktgplan.html` as well as `/projectX/docs/results/notice.html.` If, on the other hand, his boss prefers that the project manager only have read access to the results subdirectory, the boss could create an explicit ACL for that subdirectory specifying that access level. Sparse ACLs enable the streamlined administration and ease of access rights modification that is the hallmark of DomainGuard.

***Delegable Administration.*** Central to the convenience of DomainGuard is the capability to delegate administration of access control from one centralized corporate location to a variety of management levels, eliminating potential IT bottlenecks. Since administrative capabilities involve the control right, any user holding this access privilege may delegate any rights to another individual. In practice, this enables companies to eliminate potential bottlenecks in IT departments by providing control access to other individuals throughout the enterprise, such as line of business managers and content owners. For instance, if the Webmaster needs to delegate control access privileges to the marketing department's administrative assistant, he is permitted to manage only those ACLs on Web objects within the marketing directory as defined by the Webmaster. He cannot define access to any other directories, or even see them within the administration GUI.

***Browser-based Administration.*** IT administrators and users with delegated administrative capabilities can easily perform their access control responsibilities with DomainGuard's browser-based ACL Editor (see Figure 1). This feature enables users to manage ACLs from their own

## How DomainGuard Provides Effective Access Control

Consider the accounts payable clerk with ABC Manufacturing. The clerk logs onto the company intranet in the morning to check some inventory levels before processing bills, and enters the URL of the files to be viewed in the browser. Initially, the Netscape Web server checks the clerk's X.509 certificate for validity and finds that it is valid.

Next, DomainGuard verifies that the employee is authorized to review the inventory files (i.e., read access) by checking the ACL database. When the software confirms the accounts payable clerk's access privileges (i.e., read and write access), it processes the URL and delivers the data to the desktop. All this occurs virtually instantaneously and the employee experiences no delay in obtaining access to real-time data.

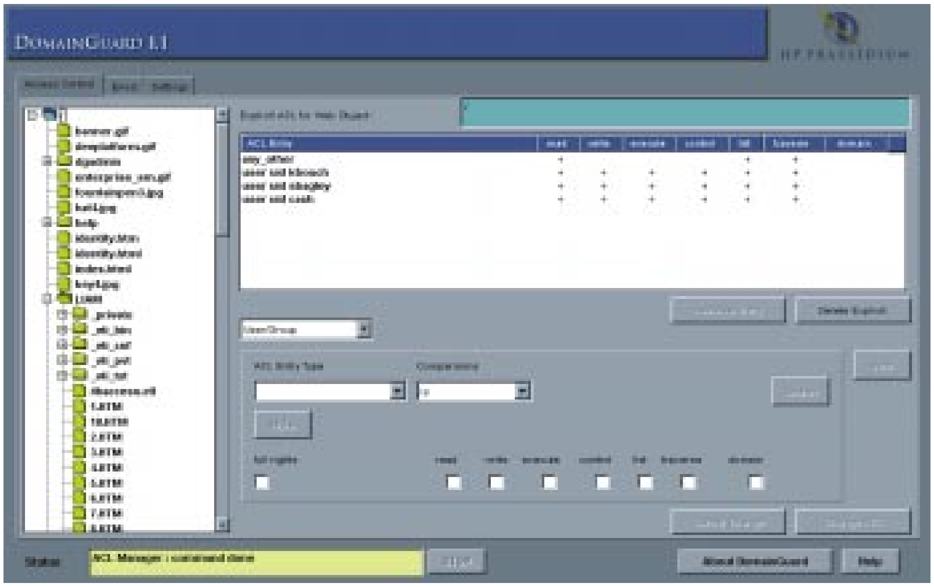


Figure 1

workstations using familiar software tools. In fact, with DomainGuard's uniform Web access control interface, users on different Web servers and host platforms share an identical interface.

The ACL Editor provides a document tree display that represents the Web server's directory tree, as well as detailed information about the ACL of an object selected from the document tree display. Using these displays, individuals can easily view and edit object ACLs to manage appropriate access.

***Easy Modification of Access Rights.*** Using the ACL Editor, individuals can quickly modify access privileges right at their workstations. Moreover, these modifications can be made dynamically without the need to restart Web servers.

**Flexibility**

***Transparent, "Snap-in" Protection.*** The marketplace today is a dynamic one, evolving at an unimaginable rate. Enterprises must keep pace with this change, while continuing to preserve their investments in information technology. Few companies have the luxury of developing customized solutions, or elaborate training programs to educate network users. Moreover, as the enterprise grows, it may need to extend information sharing capabilities to new players, such as new business partners, customers, or employees. The versatility of DomainGuard meets the changing needs of today's businesses regardless of whether the enterprise is just implementing a network or expanding its network access to new users.

DomainGuard offers transparent access control protection, operating unobtrusively in the background so that users are unaware of its operation. The software, written as a Web plug-in, easily snaps into existing Web environments, eliminating the need for time-consuming, potentially costly code changes, or for in-house, customized access control software that may have limited scalability and be difficult to support. Deployment is virtually effortless; Web administratiors simply install DomainGuard and the software registers itself with the Web server. Because DomainGuard employs standards and systems already widely used (e.g., LDAP directories), companies can preserve their long-term IT infrastructure investments.

***Scalability for Future Applications.*** DomainGuard is currently deployed in networks with hundreds of users to those with hundreds of thousands of users. And as these environments expand, the product will accommodate the addition of new users. Scalability is achieved through the use of LDAP technology, which enables users to be organized into groups based on shared parameters.

**Conclusion**

DomainGuard from HP Praesidium is the definitive, hassle-free Web authorization manager. Deploying DomainGuard couldn't be easier — it just 'snaps' into the existing server environment, offering complete control of access to Web pages, forms, server-side CGI, Java programs and Web-based transactions. And, while DomainGuard offers the policy-level security management demands, an easy point-and-click interface together with extensive automation means security administration can be delegated to line-of-business personnel without losing peace of mind. It is this level of security, flexibility and convenience that organizations need in order to share their sensitive internal information with outside partners and customers. It is HP's global reach and reputation that organizations have come to depend on as they enter new markets and deploy new technologies.

# DomainGuard Access
# DomainGuard Rules

### HP Praesidium Enterprise Security

As part of its commitment to provide businesses with stronger and more manageable security solutions, HP continues to expand the Praesidium security software family. These products now include VirtualVault, Authorization Server, DomainGuard, DomainGuard Rules, the Extranet VPN and the e-Firewall.

***HP Praesidium DomainGuard.*** A next-generation Web access control tool, DomainGuard enables enterprises to harness the dynamic capabilities of the Web for sharing information resources securely. With this tool, organizations can share Web data among departments, business units, on-site and remote employees, outside partners, and customers efficiently, utilizing existing Web environments.

***HP Praesidium VPN.*** The HP Praesidium VPN secures communication between third-party users and a company's internal network, with user-based authentication and strong encryption of information sent over the Internet. Such secure connection is critical on an extranet, for one company's security is only as good as the least secure network on the extranet. While complementary products, such as the balance of the HP Praesidium product line, function predominantly at the boundary of the Internet or inside the LAN, the HP Praesidium VPN addresses the *connection* between the LAN and other networks or users.

***HP Praesidium Virtual Vault.*** As companies race to make the most of the expanding market on the Internet, their internal mission-critical business applications may be exposed to suppliers and customers during on-line transactions. To provide security for these applications, businesses need to protect the actual Web server that sits between the Internet and their enterprise. Virtual Vault is a secure Web transaction server that is designed to safely connect enterprise applications and databases to clients on the Internet.

***HP Praesidium Authorization Server.*** At the same time, Authorization Server enables companies to centralize and customize authorization rules to control both users' and applications' access to specific functions and information. With all access rules and individual privileges centralized in one common data repository and a common interface shared across all applications, the likelihood of errors or inconsistencies in security programming, user privileges, and application maintenance is minimized.

***HP Praesidium Firewall.*** The Raptor Firewall is recognized as one of the industry's most robust application-level firewalls available today. It provides secure two-way communications between internal corporate networks and the Internet, and conceals the internal network from the outside world. While DomainGuard, Virtual Vault, and Authorization Server protect an enterprise's Web enabled applications, the Raptor Firewall protects internal enterprise networks from unauthorized access.

## System Requirements

- Netscape Enterprise Server 3.5.1 or 3.6 installed
- LDAP directory installed (i.e. Netscape Directory Server 3.0, 3.1 or 4.0)
- Windows NT™ 4.0 or HP-UX 10.20 and 11.0 or Solaris™ with at least 64 MB RAM and 200 MB hard disk
- Java enabled Web browser (Netscape or Internet Explorer)
- Authentication mechanism (Netscape user name/password mechanism or client-side authentication with users' certificates)

**For More Information**

Visit **http://www.hp.com/security**

HP PRAESIDIUM

*For more information about HP Praesidium enterprise security solutions visit **www.hp.com/security***

HEWLETT® PACKARD