



# CA SITEMINDER

## Integrating the FirePass Controller and CA SiteMinder

### Executive Summary

Identity and access management solutions help provide organizations secure access to enterprise information assets and manage the identities of users accessing those assets. These solutions combine authentication management, access control, user administration and resource provisioning to create a comprehensive and efficient approach to managing digital identities in a heterogeneous environment. Many customers have deployed identity and access management solutions to deliver secure application access for internal users and would like to extend access to remote users on home computers, kiosks, and other devices.

F5's FirePass controller, a SSL VPN appliance, provides secure application access from any web-enabled device. The FirePass controller can authenticate users against a SiteMinder server and then present the session cookie provided by the server to Web applications on the internal network. Thus, a user only enters credentials once and can remotely access any authorized internal web application. The FirePass controller also delivers client and application security to ensure that data integrity is not compromised by access from unmanaged devices, such as public kiosks or home computers.

### Challenges

When users are connected to the corporate network, identity and access management solutions enable granular access to applications without requiring a separate sign-on to each application. When connected remotely, users would like to sign-on once and achieve the same seamless access to applications without compromising security.

### Solution

The FirePass controller supports authentication using a forms-based login against the CA SiteMinder server (formerly Netegrity SiteMinder). After the user enters credentials on the FirePass sign-on page, the FirePass controller sends the user ID and password to the SiteMinder server which authenticates the user and returns a cookie for the user's session. The FirePass controller caches the session cookie and presents this cookie to Web servers accessed through the FirePass Web adapter (MyIntranet). Based on the session cookie, the user is authorized or blocked from accessing the Web application(s).

In addition to authenticating the user, FirePass offers many security features to ensure secure access for remote users. These features include:

- The FirePass reverse proxy secures access to internal applications not designed for remote access. The FirePass device masks the internal name and address of the Web application to ensure that the identity of the server is not exposed in the browser history files. In fact, all network access appears as if it were going to the FirePass controller which has been hardened to protect against outside attacks.
- The FirePass device enforces policies which minimize the risk of providing access to sensitive corporate information from a public device. One example of a client security policy is to only allow downloads, such as mail attachments, when cache cleanup is active. The FirePass cache cleaner removes temporary/cached files, cookies, and other information from the client computer after normal or abnormal (e.g. browser crash) session termination.
- The FirePass content inspection engine scans the Web traffic for malicious characters and other anomalies to block application-layer attacks (e.g. cross-site scripting attacks) on the internal Web hosts. Together, the FirePass controller and SiteMinder server provide secure access to Web applications based on the policies established by the enterprise customer.

### About CA SiteMinder

CA SiteMinder provides an enterprise-scale security infrastructure that enables you to provide access to Web applications and Web sites for employees, customers, and business partners—both securely and efficiently.

### About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability—all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to [www.f5.com](http://www.f5.com).