IBM SecureWay Policy Director

Highlights

Adds centralized security to your existing Web and TCP/IP applications

Provides access control to Web objects

Simplifies development of a consistent, manageable access control policy

Supports LDAP-based storage of user credential information

Supports public key infrastructure

Supports the use of external authentication and authorization services

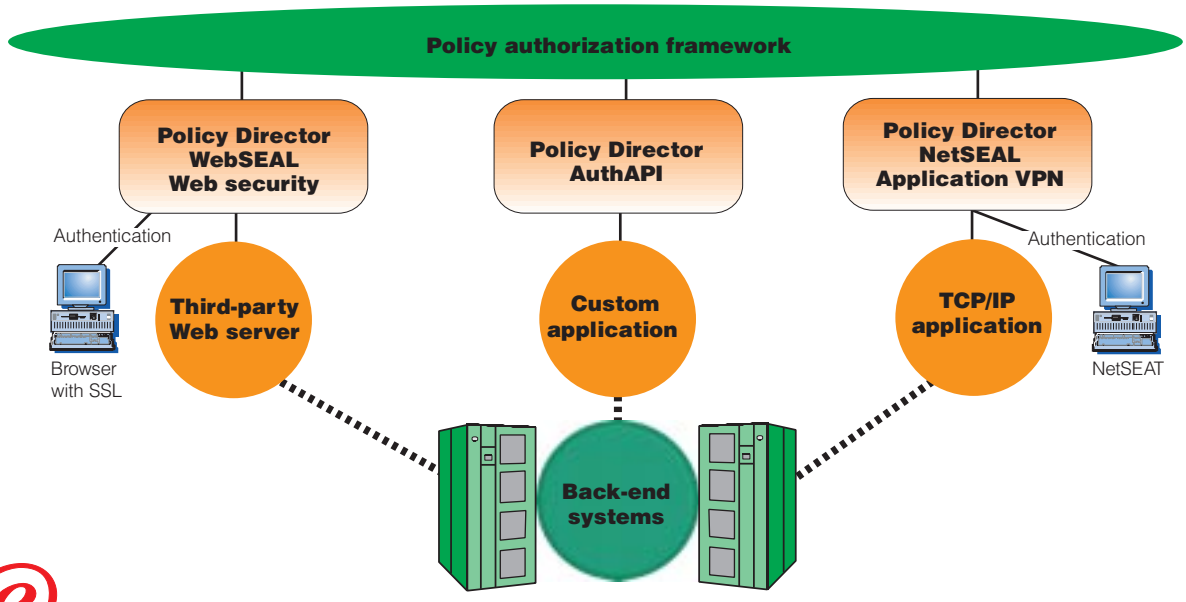
Offers one-time authentication capability with access to multiple Web resources

Is highly scalable through replication and load-balancing facilities

Provides integrated user administration with IBM SecureWay Firewall

IBM SecureWay Policy Director

The rapid evolution of e-business solutions has caused extranets, enterprise portals and intranets to grow dramatically. A secure supply-chain extranet or enterprise portal allows manufacturers, suppliers, customers and employees to collaborate in a cost-effective manner. But, this growth changes the number and nature of the services provided and the volume of corporate information being accessed. As these intranets and extranets carry increasingly valuable data, enterprises face a new set of security issues. The fundamental challenge is to build a user-centric portal, while at the same time securely limit content delivery to only



Policy Director can streamline your security management and provide long-term cost reductions.

e-business

authorized suppliers, employees and customers. To deliver this requires an authorization framework with centralized security policy management and administrative delegation. IBM SecureWay® Policy Director provides this security framework.

IBM SecureWay Policy Director is the central control point for IBM SecureWay FirstSecure, IBM's single integrated solution for your e-business security needs. Policy Director is designed to unite core security technologies—intrusion detection, antivirus, hardened boundary protection, including content filtering, and a public key infrastructure (PKI)—around common security policies. This can reduce implementation time and management complexity, helping to lower the total cost of secure computing.

Centralizing your security policy enables you to easily update or modify it without having to use various product-specific configuration consoles. At the Policy Director console, you can set policy that establishes user credentials and authorizes users based on those credentials. This policy determines what kind of access users have to Web applications and other network resources.

Your users can be placed in groups, which can be the basis for user authorization. Policy Director supports defining and coordinating security policy across:

Enterprise Web servers and the browsers that access them
Policy Director provides support for authentication of specific users through a user ID and password, Kerberos credentials or client-side certificates. Access control can be set to specific URLs, files or common gateway interface (CGI) programs on the Web server.

New applications written to the Policy Director authorization API
Policy Director includes a standards-based authorization API that allows an enterprise to efficiently support access control to Web objects, including HTML pages, graphics, CGI programs, Java™ applications and database queries.

Client/server TCP/IP applications
Policy Director provides support for authentication of specific users through a user ID and password, and Kerberos credentials. It establishes an application virtual private network (VPN) between the client and server to protect data transmission over public networks.

Policy Director includes the following components:

- Policy Director WebSEAL®
- Policy Director authorization server
- Policy Director NetSEAT/NetSEAL™
- IBM SecureWay Directory server
- Policy Director management console

WebSEAL
The WebSEAL server provides authentication and access control services for Web resources. It is independent of network topology and location, meaning security credentials are based on *who* your user is, not *where* your user is—and it allows you to give users access only to the information they need. Your users will also have a single sign-on to Web-enabled applications. WebSEAL manages access to all your Web servers— including third-party servers—allowing you to centrally control your Web resources as a single, logical Web space.

By performing intelligent load balancing over replicated servers, WebSEAL lets your organization scale its deployment of servers without increasing management overhead. It also provides a failover capability, enabling Policy Director to automatically switch to a backup Web server. WebSEAL is designed to use an LDAP-based directory server for authentication of users attempting to access the resources it protects. It also has built-in support to accept and validate client-side digital certificates generated by either IBM SecureWay Trust Authority, IBM Vault Registry or Entrust when presented by a user's browser for authentication.

Authorization server

The authorization server provides an API that can be used from within an application to provide sophisticated access control processing. This API implements the cross-platform aznAPI specification being considered for standardization by The OpenGroup. The authorization server allows custom applications to make finely tuned application- and authorization-level decisions. By using this API, you can build security and authorization directly into your corporate applications that leverage Policy Director services, helping reduce application development time and cost. By taking advantage of this capability, you can have your network centrally managed by Policy Director. This may significantly reduce the total cost of ownership and the likelihood of security breaches. Using the API provided by the authorization server, you can customize your users' network views to match their access privileges and create customized menus based on authorization information.

NetSEAT/NetSEAL

NetSEAT client and NetSEAL server are used to secure traditional Internet services including Telnet and FTP. They can also be used to secure third-party applications including database systems, network management tools and object request brokers. NetSEAT/NetSEAL even enable you to extend access to in-house applications with authorization. Managed access to these network resources is provided to users through the enterprise intranet and to remote users through the Internet. This is accomplished in a non-intrusive manner because no changes are made to existing applications on either the client or the server.

By using NetSEAT/NetSEAL, you can separate the authorization policy and the application which provides a level of abstraction between physical and logical views of your security policy for network data. Security credentials are based on who—not where—your user is. NetSEAL is an authorization engine that, working with NetSEAT, provides end-to-end tunneling. The components have been enhanced in Policy Director to support Secure Sockets Layer (SSL) protocol. This enhancement allows components to work better with your firewall by minimizing the number of ports needed to facilitate NetSEAT/NetSEAL communications.

IBM SecureWay Directory

IBM SecureWay Directory is used to store Policy Director user and group credentials, as well as credential sets for target Web servers. It is an open, cross-platform server optimized for LDAP-enabled applications, like Policy Director. Its architecture allows applications to share data with other applications and network resources. SecureWay Directory uses IBM DB2® Universal Database™ and its transactional store, extending the performance and availability of DB2® to an enterprise directory service. DB2 Universal Database is provided with SecureWay Directory for use only in association with that directory.

Management console
The management console is a graphical Java application used to securely manage the various Policy Director components. The console allows you to add and delete users or groups and to apply access controls to objects using access control lists (ACLs). It can also be used to define and edit user credentials for IBM SecureWay Firewall.

IBM Policy Director and IBM SecureWay Boundary Server
IBM SecureWay Boundary Server brings broad security solutions to help protect your business assets. When you use SecureWay Boundary Server with Policy Director, SecureWay Boundary Server can provide an extranet security framework to enable your company to connect to business partners, customers and remote employees over the Internet.

New functionality for Policy Director
Policy Director includes enhancements that deliver centralized access-control policy, and reduce complexity and costs while exploiting industry standards. These enhancements include:

- LDAP support for storing user information in Policy Director.
- Support for the new aznAPI specification being considered for standardization through The Open Group.
- An interface definition language (IDL) interface between WebSEAL and the Policy Director credential acquisition service. This allows the use of external authentication services, like Radius, with some professional services customization.
- Support for PKI-based authentication using the new credential acquisition services (CAS), including certificate revocation list (CRL) checking using SecureWay Trust Authority, Vault Registry or Entrust certificates.
- Ability to define and edit user credentials for IBM SecureWay Firewall using the Policy Director console.
- A utility to help Policy Director users migrate their user and group credential data to the SecureWay Directory server (LDAP).
- Integration of Web sign-on administration with the Policy Director console.
- Use of a browser to manage Web passwords stored in the Policy Director credential server.
- Access control policy management for the IBM Client Security Solutions.* Support for IBM User Verification Manager, a component of IBM Client Security Solutions, is included. These solutions give enterprise customers an easy way to centrally define access-control policies, manage user access, and manage the levels of user authentication and transactions running on IBM PC 300PL, 300GL and IntelliStation® workstations.
- National Language Support (NLS) translation into 8 languages, including French, German, Spanish, Japanese and traditional Chinese.

Open for trusted e-business with IBM SecureWay FirstSecure
IBM SecureWay FirstSecure enables companies to build and operate secure and trusted environments to conduct e-business. FirstSecure offers an integrated, policy-driven solution for your IT security needs, including digital identities, network boundary protection, detection for viruses and intrusions, and tools for developing secure applications. Policy Director is available separately or as part of SecureWay FirstSecure.

For more information
To find out more about IBM SecureWay Policy Director, visit:
www.ibm.com/software/security/policy

To learn more about IBM SecureWay FirstSecure, visit:
www.ibm.com/software/security/firstsecure

SecureWay Policy Director at a glance

Platforms supported	• IBM RISC System/6000® • Sun SPARC • Intel® x86 or Pentium® processor • IBM AIX® 4.3.2 or higher • Sun Solaris™ operating environment 2.5.1 or 2.6 • Microsoft® Windows NT® 4.0
Client platforms	• Windows® 95 or Windows 98 • Windows NT 4.0 • X/Motif
Disk space	• 50MB RAM
Memory	• 64MB RAM

IBM Corporation
Department VK4A
3039 Cornwallis Road
Research Triangle Park, NC 27709

Produced in the United States of America
10-99

G325-3890-01