BUILDING BLOCK

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

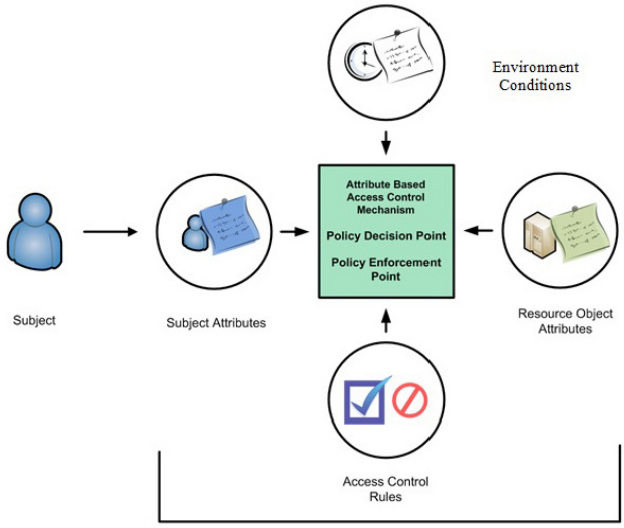
ATTRIBUTE BASED ACCESS CONTROL

Attribute Based Access Control (ABAC) is a security mechanism that allows organizations to authorize an individual's access to networks and resources based on granular attributes, such as title, division, certifications, training, etc. The National Cybersecurity Center of Excellence (NCCoE), in collaboration with members of the IT community and vendors of cybersecurity solutions, has developed an example ABAC implementation. The example solution is detailed in a NIST Cybersecurity Practice Guide, SP 1800-3. We understand that the fast-moving cybersecurity technology market will likely improve to develop other solutions that could contribute to an ABAC system. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at abac-nccoe@nist.gov.

THE CHALLENGE

Today, access to a company's network and assets is defined by a user's job or role within the organization using a Role Based Access Control (RBAC) system. If roles change or an employee leaves the company, an administrator must manually change access rights accordingly—oftentimes within several systems.

However, as technology advances and businesses expand, so does the diversity of users and their access needs. With current RBAC systems, these types of transactions become increasingly difficult and inefficient to manage and audit.



Graphic Credit: NIST 800-162

THE SOLUTION

An ABAC system moves beyond roles and their associated privileges. Instead ABAC uses granular attributes, such as title, division, certifications, training, and even environmental conditions, to authorize an individual's access.

To demonstrate the applicability of ABAC, the NCCoE used commercially available technology to develop an example ABAC solution, leveraging identity and attribute federation between enterprises. These technologies enhance the granularity of access control policies by increasing the range of possible attributes available when making automated access control decisions in an enterprise.

The ABAC technology solution stack demonstrated in this document is designed to be modular, allowing corporations flexibility in their implementations based on their current infrastructures.

THE BENEFITS

ABAC implementations that leverage identity federation can reduce organizational costs by diminishing the burden of identity storage and management. Through the use of attribute based policy definitions, enterprise risks—including insider threats, loss of personally identifiable information, and fraud—are reduced.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

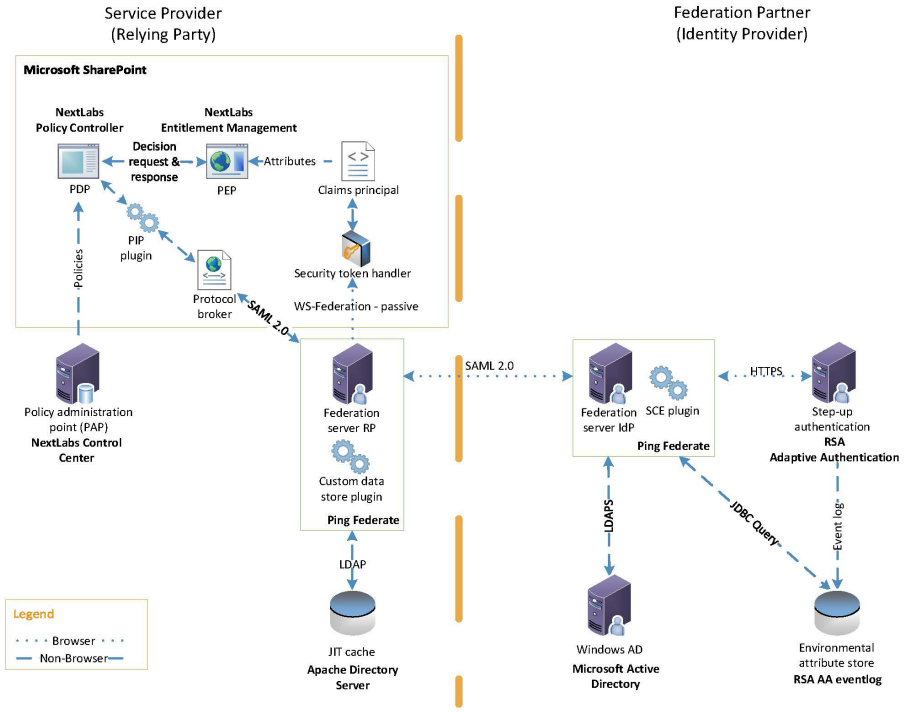
LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

THE NCCOE'S ABAC PROJECT:

- supports organizations with a diverse set of users and access needs through efficient provisioning of access and highly specific policy definitions
- through identity federation, reduces the number of identities managed by the enterprise, thereby reducing costs associated with those management activities
- enables a wider range of risk decisions by allowing organizations to define attribute based policy on subjects and objects and to employ a variety of environmental decisions
- strengthens collaboration among organizations by allowing an enterprise to accept federated identities from outside the organization
- supports the centralization of auditing and access policy management, creating efficiencies of policy management and reducing the complexity of regulatory compliance

ABAC IMPLEMENTATION OVERVIEW



SERVICE PROVIDER:

- manages the Microsoft SharePoint instance containing the resources a user would like to access
- provisions, manages object attributes by tagging resources in SharePoint
- uses ABAC components to protect SharePoint resources, granting or denying access based on attribute based policies defined by the service provider via NextLabs Control Center
- relies upon identity and attribute information from the federation partner for access decisions

FEDERATION PARTNER:

- serves as the identity provider by authenticating users
- leverages RSA AA for two-factor authentication and environmental attributes
- provisions, manages subject attributes in Microsoft Active Directory
- implements identity federation via Ping Identity's PingFederate

TECHNOLOGY PARTNERS

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partnership partners.

Microsoft NEXTLABS® Ping Identity RSA Symantec

DOWNLOAD THE PRACTICE GUIDE
Visit https://nccoe.nist.gov/projects/building_blocks/attribute_based_access_control to learn more about this project.

HOW TO PARTICIPATE
Share your thoughts on the relevance and usefulness of the project and practice guide. Contact us at abac-nccoe@nist.gov.