

ATTRIBUTE BASED ACCESS CONTROL

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of implementing Attribute Based Access Control (ABAC), a security mechanism that allows organizations to authorize an individual’s access to networks and resources based on granular attributes, through collaborative efforts with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of NIST Cybersecurity Practice Guide SP 1800-3, including the challenge, solution, and potential benefits. As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email abac-nccoe@nist.gov.

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 organizations expand and become more complex, managing the diversity of users and their access needs under current RBAC systems becomes increasingly difficult and inefficient to manage and audit.

SOLUTION

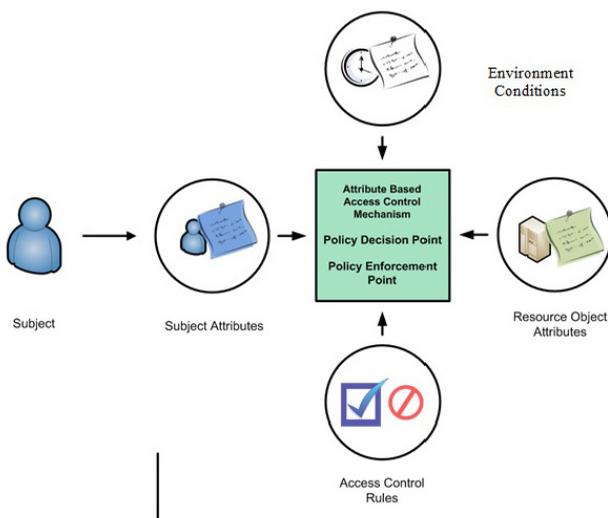
An ABAC system moves beyond roles and their associated privileges. Instead ABAC uses granular attributes, such as title, division, certifications, training, and even environmental conditions, to authorize an individual’s access. The ABAC technology solution demonstrated in this document is designed to be modular, flexible, and centrally managed. Organizations can define attribute-based policy on subjects and objects, and by using a variety of environmental decisions. It also reduces the number of identities managed by the enterprise and allows the enterprise to accept federated identities.

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 potential business benefits of this example solution include:

- flexibility—products and capabilities can be implemented on a component-by-component basis, or as a whole
- reduces “privilege creep”—users only obtain needed access
- reduces costs
- better risk-mitigation decisions
- increases business collaboration
- efficient policy management and associated regulatory compliance



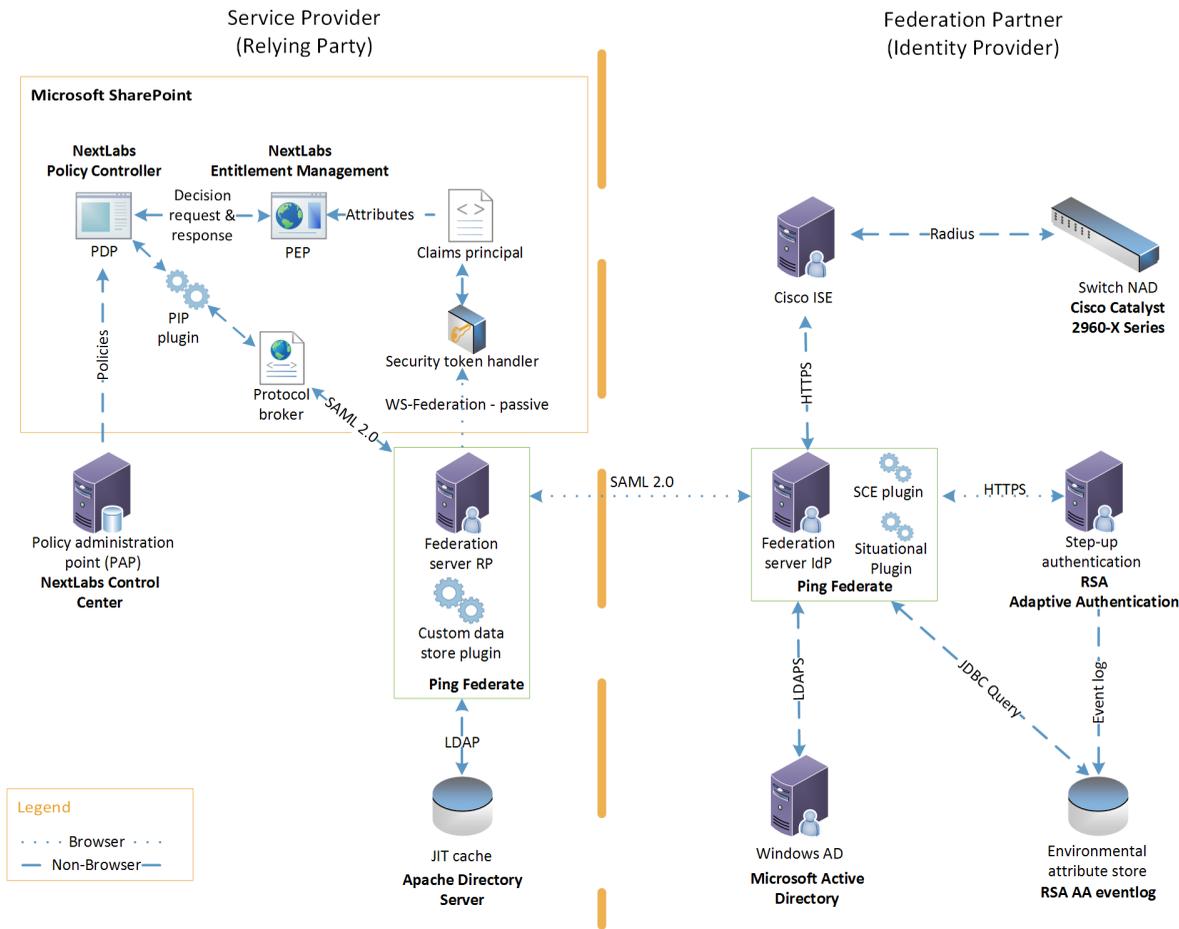
Graphic Credit: NIST 800-162

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

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

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

HIGH-LEVEL ARCHITECTURE



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
- collects environmental context from the CISCO Identity Services Engine

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.



Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit: <https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email abac-nccoe@nist.gov.