NEXTLABS®

White Paper

What is Policy-Based Access Control (PBAC)?

Overview

Keeping IT resources secure while making them availability and easily accessible is a major challenge for enterprises. With an increasingly sophisticated computing environment, how can enterprises ensure scalable and consistent enforcement of access controls?

What is PBAC?

Policy-based access control (PBAC) also known as Policy Based Access Management, is a security model that manages and enforces access to resources based on a set of policies rather than hard-coded rules, static permissions, roles, groups, or user identities alone. In PBAC, access decisions are driven by centrally managed policies that define conditions under which a user or entity is allowed or denied access to resources. By using PBAC, organizations can define, enforce, and manage access in a way that aligns with their business needs, enhances security, reduces administrative overhead, and ensures compliance with regulatory standards. PBAC is particularly useful in dynamic and complex environments where access decisions need to be flexible and scalable.

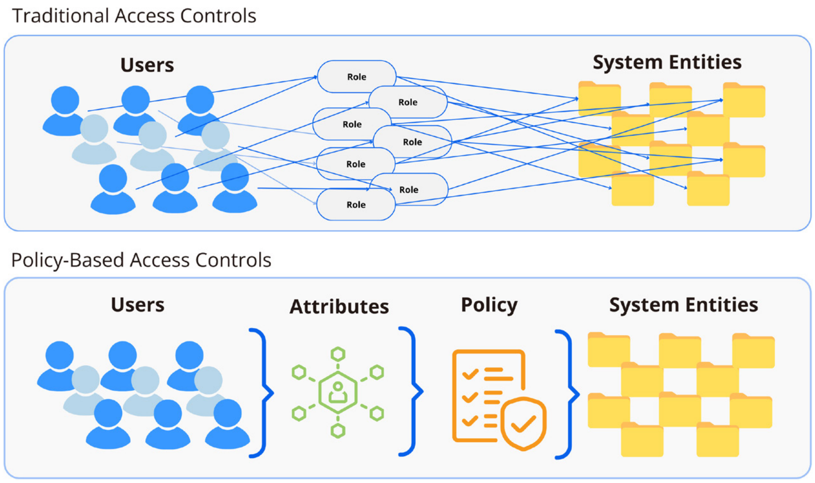

Figure 1: PBAC vs. Traditional Access Control

By using a 3-tier Policy Enforcement Point (PEP), Policy Decision Point (PDP), and Policy Administration Point (PAP) architecture, PBAC allows for efficient and centralized management of complex access control policies across the entire IT landscape. Instead of auditing and modifying roles across the entire organization, PBAC allows quick adjustment of entitlements in response to changes in requirements, ensuring that assets are secured through set rules or policies. PBAC is an adaptable authorization solution because it can support a variety of access points by automating security controls in applications and on data. When PBAC is built with Attribute-Based Access Control (ABAC) support, the approach combines roles and attributes to provide flexible and dynamic access control.

Key Characteristics of PBAC

Policies

These are rules that define what is permissible in the system, often including conditions based on roles, attributes, or other contextual factors. For example, a policy might state, “Only employees in the Finance department can access financial reports after business hours.”

Granularity

Policies can be very fine-grained, considering various factors such as user roles, time of day, location, device being used, and more.

Dynamic Control

PBAC allows access decisions to be made dynamically based on real-time contextual information. For example, a user might be granted access to sensitive data if they are accessing it from a company-approved device but denied if they are using a personal device.

Centralized Management

Policies are often managed centrally, which means administrators can define and adjust access rules for different resources or user groups from one place. This central management makes it easier to update policies and ensure consistency across an organization.

How PBAC Works

Policy Definition

Policies are at the core of PBAC. These are rules that define who can access what resources under what conditions. A policy in PBAC typically involves several factors, such as the user, the resource, the action being performed, and sometimes environmental factors (like time of day or location).Policies are generally written in a human-readable format and can be stored in a central policy repository.

Attributes

Policies in PBAC often use attributes as conditions. These can include:

- User attributes (e.g., role, department, seniority, security clearance).
- Resource attributes (e.g., file type, owner, classification).
- Action attributes (e.g., read, write, delete).
- Environmental attributes (e.g., time of day, location, IP address).

These attributes are typically used in policy conditions to make access decisions more dynamic and fine-grained.

Policy Decision Point (PDP)

The PDP is the component responsible for evaluating access requests against the defined policies. When a user requests access to a resource, the PDP examines the request, retrieves the relevant policies, and makes a decision whether access should be granted or denied.It evaluates the conditions in the policies based on the user’s attributes (e.g., role, department), the resource’s attributes (e.g., classification, ownership), and the action requested (e.g., read, write).The PDP returns an access decision to the Policy Enforcement Point (PEP), which implements the decision.

Policy Enforcement Point (PEP)

The PEP is responsible for enforcing the decisions made by the PDP. When the PEP receives an access decision, it either grants or denies access to the user based on that decision.

The PEP could be a web application, API gateway, or any system component that controls access to resources.

Policy Administration Point (PAP)

The PAP is responsible for managing and administrating the policies. It allows administrators to define, update, or delete policies, which are then stored in the policy repository. The PAP also provides an interface for policy management, usually through a centralized management console.

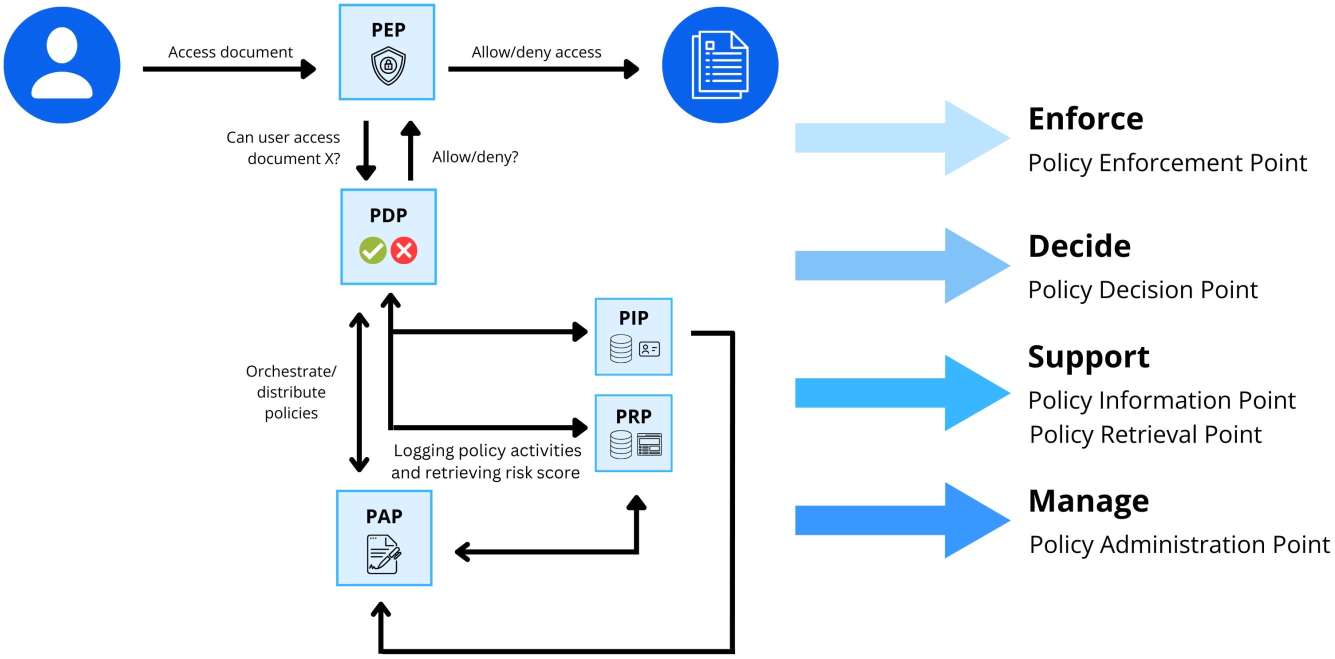

Figure 2: Access Control Diagram

Example of PBAC Policy

A policy can state that if the user attempting to gain access to Financial Report while working from home is a Controller or Auditor and is logged in with the proper credentials, then they can access and make changes to the financial reports. However, the policies are usually more complex, considering location and other factors. For example, if the company policy states that only User in the U.S. only have edit access to Financial Report between the hours of 9 a.m. and 6 p.m. from a Company Device, User requesting access at 7 p.m. would be denied edit access and would only be able to view the reports. These policies could prevent someone with illegitimate credentials on the other side of the world from gaining undue access to a system. PBAC provides more extensive control because it takes attributes and other rules into account while adding an extra layer of control that allows it to be dynamic.

Policy: “Allow access to the financial report if the user is a ‘Controller’ or ‘Auditor’, and the time is between 9 AM and 6 PM from a ‘Company-managed Device’.”

This policy might be broken down as follows:

- User Attributes: Role = ‘Controller’ or ‘Auditor’

- Resource Attributes: Resource = financial report
- Action Attributes: Action = Edit (or other relevant action)
- Environmental Attributes: Time of access = between 9 AM and 6 PM and Device used by the User is a company-managed device

The PBAC Access Control Workflow

A high-level view of how PBAC works during an access request:

1. A user requests access to a resource (e.g., trying to read a document or update a database entry).
2. The PEP intercepts requests and sends them to the PDP, which retrieves policies and evaluates attributes, actions, and conditions. For example, a policy may allow managers to access confidential reports only from 9 AM to 5 PM.
3. The PDP evaluates if the user meets policy conditions, granting or denying access accordingly. If multiple policies apply, it combines them using logical checks to determine the final decision.
4. The PDP returns an Allow or Deny decision to the PEP, which then enforces access by permitting or blocking the request.
5. PBAC systems often include logging and auditing features. The PEP logs the request and the corresponding access decision for monitoring, compliance, and auditing purposes.

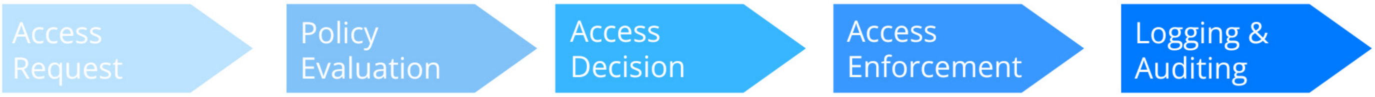

Figure 3: How PBAC Works During an Access Request

Use Cases

Enterprise Security

Large organizations use PBAC to control access to sensitive business data based on roles, departments, and other contextual information.

Cloud Environments

PBAC can help manage access to resources in dynamic cloud environments where users and resources change frequently.

Regulated Industries

Industries such as finance, healthcare, or government that require strict access controls based on legal and compliance requirements.

Advantages of PBAC

Data security is no longer just about protecting perimeters or preventing cyberattacks. It is much more about prevent unauthorized access and keeping confidential information safe from authorized users as well, which includes everyone from employees and contractors to third-party vendors and customers, as the enterprise's entire network is prone to data loss from accidental or malicious leakage. PBAC offers a myriad of advantages.

Advantages of PBAC	
Centralized Control and Management	• Simplified Administration: PBAC enables administrators to define, manage, and enforce access control policies centrally. This means access decisions are governed by a single set of policies, making it easier to oversee, update, and audit access across large, distributed systems. • Consistent Access Policies: With PBAC, policies are managed in a centralized manner, ensuring that access control is consistently enforced in real-time throughout the organization. This reduces the risk of misconfigured and administration costs.
Scalability	• Easier to Scale: In large organizations or complex systems, manually managing permissions for every resource and user can be cumbersome and error prone. PBAC, by centralizing access control, makes it much easier to scale across a growing number of resources, users, and environments. • Dynamic Policies: PBAC allows organizations to scale their access control dynamically. Policies can adapt to changing business needs, regulatory requirements, or the evolving IT environment, without needing to modify individual permissions or roles.
Flexibility and Granularity	• Fine-Grained Access Control: PBAC provides much more granular control than access control lists (ACL) and role-based access control (RBAC) because access is granted based on attributes, policies, and conditions. For instance, you can define access policies based on a variety of factors such as time of day, user role, location, or even the sensitivity of a resource. • Dynamic Context-Aware Policies: PBAC allows access decisions to be based on dynamic factors such as context and environmental conditions (e.g., time, location, or device being used). For example, a policy could state that access to sensitive data is allowed only during business hours and from trusted IP addresses, making it more responsive to real-world conditions. • Flexibility: Policies can be modified without requiring changes to individual access control settings, enabling faster adaptation to new security or business requirements.
Improved Security	• Reduced Human Error: In traditional access control models, mistakes in role or permission assignments can lead to unintended access to sensitive resources. PBAC reduces this risk by managing access based on defined policies that consider a variety of attributes, ensuring that access is only granted when all conditions are met. • Least Privilege Principle: PBAC supports the implementation of the least privilege principle, which means users only get access to the resources they need, based on specific, context-driven policies. This helps minimize exposure to sensitive data. • Fine-grained Auditing: Since PBAC defines and logs every access decision in terms of policies, auditing becomes easier and more detailed. This makes it simpler to track and analyze who accessed what data, when, and under what circumstances.

Advantages of PBAC	
Adaptability to Changing Business, Compliance, and Audit Requirements	• Rapid Policy Updates: PBAC allows organizations to quickly update policies to comply with new regulations or business requirements, without having to overhaul individual permissions or reassign roles. • Compliance with Regulatory Standards: PBAC systems often come with built-in auditing and logging capabilities, which are important for regulatory compliance. PBAC can help organizations meet strict regulatory and industry compliance standards (such as ITAR, GDPR, HIPAA, or SOX) because policies can be designed to enforce access restrictions that adhere to these regulations. Policies can also be easily updated to reflect evolving compliance requirements. • Policy Flexibility: As regulations and business goals evolve, PBAC allows policies to be changed dynamically without requiring manual intervention for each user or resource.
Support for Complex and Hybrid Environments	• Cloud and On-Premises: PBAC is well-suited for modern hybrid environments, where organizations use a mix of cloud-based, on-premises, and third-party resources. PBAC helps organizations enforce consistent access policies across all these resources, regardless of location. • Microservices and APIs: In environments where microservices and APIs are prevalent, PBAC enables fine-grained access control to services and endpoints, ensuring that only authorized users or systems can interact with specific components of the infrastructure.
Reduced Complexity Over Time	• Simplified Permission Management: PBAC allows organizations to manage access control policies at a higher level of abstraction. Instead of assigning specific permissions for each user or resource, access is granted based on predefined rules, which simplifies ongoing management. • Policy Hierarchy: PBAC allows for the creation of policy hierarchies, where policies can be inherited or applied across multiple resources, reducing complexity and minimizing the need to duplicate rules across systems.
Better Decision-Making	• Contextual Access: By incorporating contextual factors into access decisions (such as time, location, or device), PBAC helps ensure that access is granted based on a more comprehensive understanding of the environment in which access is being requested. This leads to smarter, more informed access control decisions. • Real-time Adaptation: PBAC can provide real-time access decisions that adapt to new conditions, improving the overall user experience while maintaining security.
Support for Delegated Administration	• PBAC allows organizations to delegate access control responsibilities to specific departments or business units without sacrificing centralized control. Each department can define policies relevant to their resources, while still adhering to overall organizational access guidelines.

Why is PBAC Important?

PBAC is crucial for modern organizations due to its ability to provide centralized, scalable, flexible, and dynamic access control. It supports the complex and evolving IT landscapes where traditional role-based or rule-based models fall short. By using PBAC, organizations can manage access in a way that aligns with their business needs, enhances security, reduces administrative overhead, and ensures compliance with regulatory standards. This makes PBAC a key enabler of efficient, secure, and agile access management; intelligent enterprises should take advantage of this new security model to achieve the following objectives:

Data-Centric Protection Anytime, Anywhere
A PBAC system protects data in real-time by ensuring that sensitive information stays within its intended boundaries and never becomes vulnerable to being leaked accidentally or maliciously. It is able to provide fine-grained policy controls over every aspect of how users interact with it—from devices they connect through, applications they use on those devices and everything in between (such as files stored in the cloud).

Adherence to Security Compliance
With PBAC, organizations can configure policies to enforce compliance with industry standards and regulations. Enterprises can define granular controls down to the individual object level and apply them across multiple environments, including virtual machines (VMs) in the public cloud or on-premises servers.

In organizations where employees are required to adhere to compliance standards, having an efficient auditing process is critical. PBAC enables an automated auditing process that makes way for enforcing policies and meeting regulatory requirements, which can be time-consuming and error-prone if done manually.

More Efficient Control & Lower Security Costs
PBAC is a more effective approach than traditional access control as it allows organizations to establish policies that are centrally managed, providing consistent and real-time enforcement across applications. Using a centrally managed policy system, policies can be reviewed across the enterprise, reducing administration costs. By increasing business agility and efficiency, PBAC enables enterprises to modernize their IT, extend competitive advantages and prevent data breaches.

For more information on NextLabs PBAC solutions, watch Control Center Policy Authoring: Nextlabs Policy-Based Authorization Management and Control Center Administration Section- NextLabs Policy-Based Authorization Management.
The table below shows the myriad of advantages PBAC offers.

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software & services to protect data anytime and anywhere regardless of where data resides – whether it is across application, database, file or file repository – on-premises or in the cloud. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent violations. NextLabs software prevents unauthorized access and automates enforcement of security controls and compliance policies to enable secure collaboration and information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit https://www.nextlabs.com/company/.