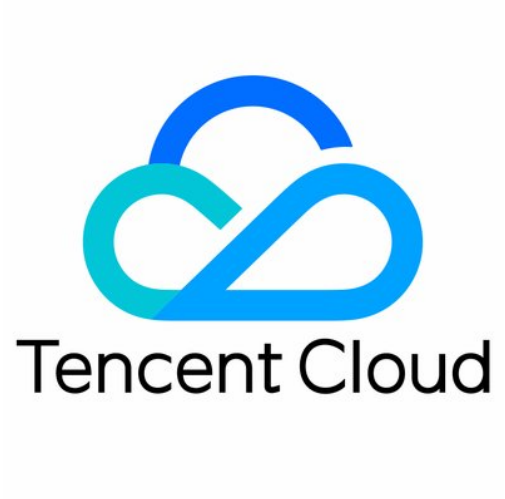
Identity Aware Platform

Product Introduction

Product Documentation



Contents

Product Introduction
Overview

Last updated：2024-11-06 18:01:38

Identity Aware Platform (IAP) enables you to establish a central authentication layer for resources accessed through HTTPS. When IAP is enabled, only users with permissions can access the resources requested through HTTPS, while users without permissions cannot access them.

How It Works

If a resource is protected by IAP, it can be accessed only by users with the correct Cloud Access Management (CAM) permissions. If a user tries to access a resource protected by IAP, IAP will perform identity verification and authorization checks.

Identity Recognition

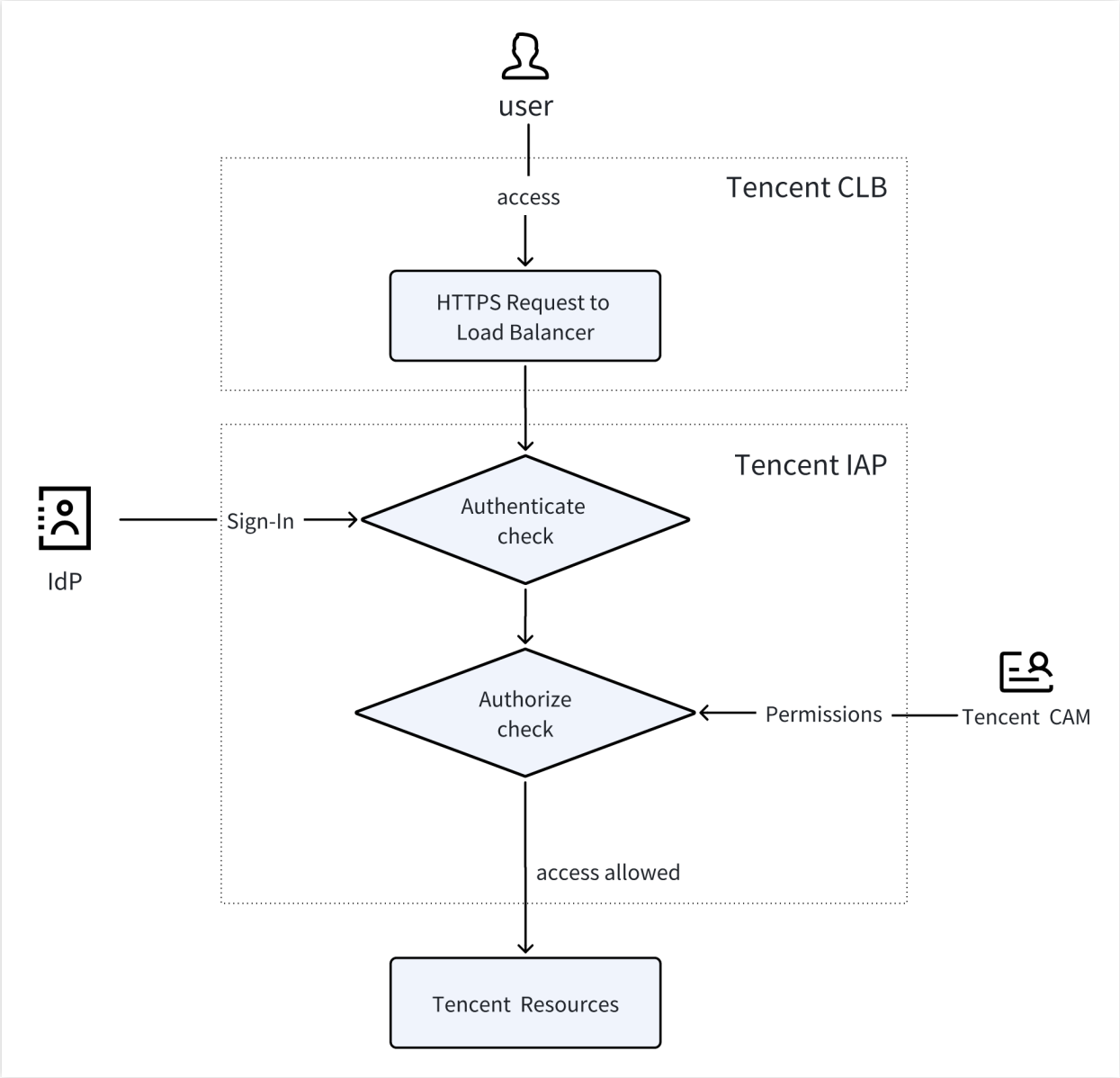
Requests for accessing Tencent Cloud resources are passed in through HTTP(S) CLB. The backend service will check whether the application has enabled IAP. If IAP is enabled, the relevant information of the protected resources will be sent to the IAP server. Therefore, the request header contains the information such as request URL and IAP credentials.

When IAP checks a user's identity credentials, the user will be redirected to the OIDC SSO process for login with the IdP enterprise identity.

After the enterprise identity verification is passed, IAP will check the user's CAM identity. If the user identity recognition succeeds, IAP will perform authentication in the next step.

Authentication

After the identity recognition is completed, IAP will check through CAM policies whether the user has permissions to access the requested resource.



Features

Identity Verification and Authentication

You can use IAP to perform user identity verification and authentication for protected resources.

Enhanced Security

Administrators can specify user identities and resources to develop and implement elaborate access control policies.

Simplified Work

You can access IAP-protected applications by entering a URL accessible from the Internet in a web browser, without using a VPN client.

Concepts

Last updated：2024-11-06 18:01:38

This document introduces the basic concepts of Identity Aware Platform (IAP).

Concept	Description
Identity Recognition	IAP supports joint identity verification based on OIDC, to recognize whether the user identity verified by the Identity Provider (IdP) corresponds to a Tencent Cloud console user.
Authentication	In Cloud Access Management (CAM), the root account can grant resource permissions to a corresponding sub-account through the policy syntax. Authentication indicates recognizing whether a sub-account has been granted with relevant permissions.
Cloud Load Balancer	Tencent Cloud Load Balancer (CLB) distributes traffic to multiple real servers to enhance the service capabilities of applications. For details, see Cloud Load Balancer Overview.
OIDC	OpenID Connect (OIDC) is an authentication protocol built on the basis of OAuth 2.0. OAuth is an authorization protocol, and OIDC adds an identity layer based on the OAuth protocol. Besides the authorization capabilities provided by OAuth, OIDC also allows clients to verify the identity of end users and obtain their basic information via the OIDC API (in the form of HTTP RESTful).