FICHE PRODUIT

WEB ACCESS MANAGER

Simplifier l'accès et accroître la sécurité des applications avec UBIKA WAAP Gateway et UBIKA WAAP Cloud

La prolifération des applications et des mots de passe associés constitue un défi pour les services informatiques des entreprises. Il est devenu difficile pour eux de protéger les données de l'entreprise et de traiter les tickets de réinitialisation de mot de passe. Il est important d'identifier les utilisateurs, mais il est compliqué pour les utilisateurs de se souvenir d'un grand nombre de mots de passe. Les utilisateurs passent trop de temps à se connecter à des applications une par une. De plus, les atteintes à la sécurité proviennent principalement de mauvaises pratiques en matière de mots de passe. Lorsqu'il s'agit de services cloud, il est également important de savoir qui a accès à quelles applications et comment ils les utilisent. Les portails à authentification unique (SSO) sans authentification multifacteurs (MFA) peuvent entraîner une diminution de la sécurité. Les entreprises doivent pouvoir appliquer le même niveau de sécurité à toutes leurs applications.

Aperçu de la solution

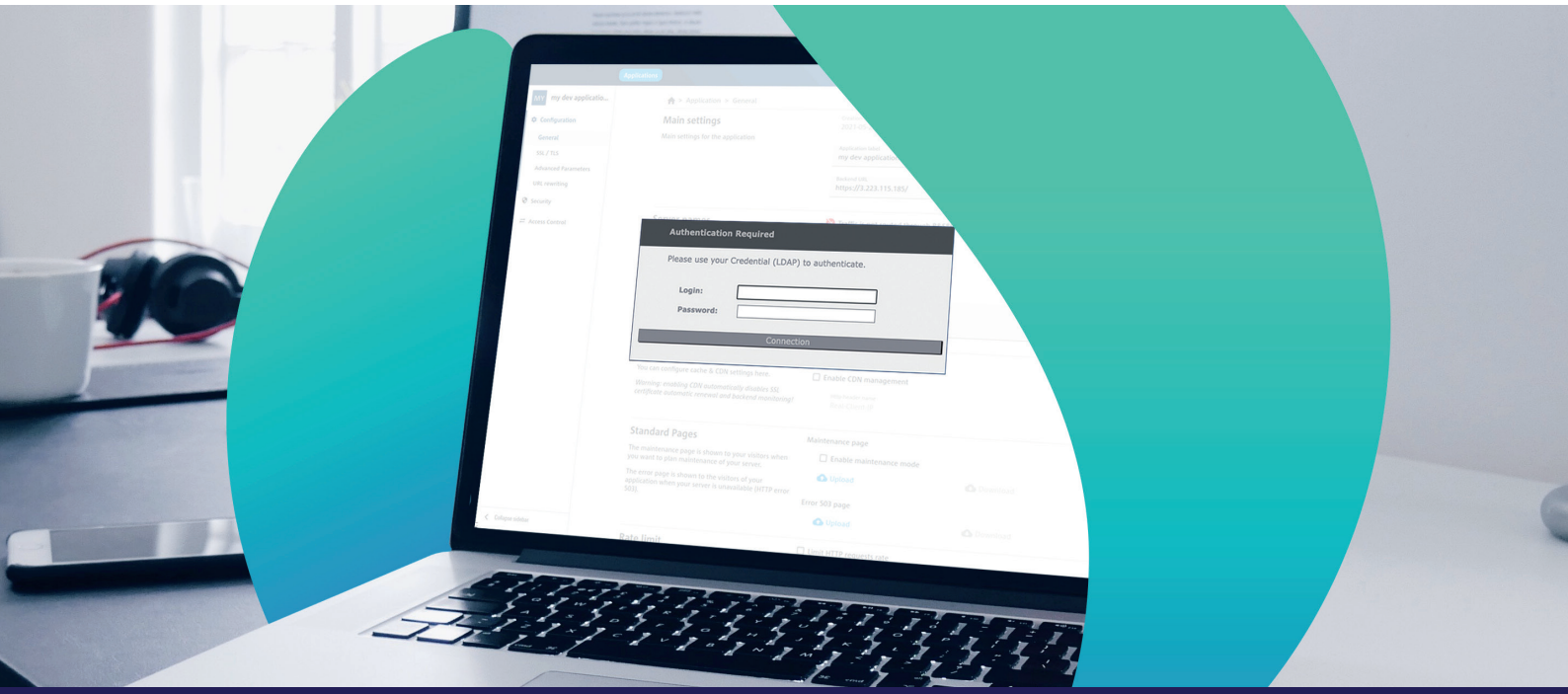
Le Web Access Manager (WAM) est un module optionnel de UBIKA WAAP Gateway et UBIKA WAAP Cloud (version cloud public d'UBIKA WAAP Gateway) qui contrôle l'accès aux applications web en fournissant divers services dont l'authentification unique sur le web (WebSSO).

Le WebSSO permet l'accès à de multiples applications basées sur l'authentification unique d'un utilisateur tout en maintenant les règles de contrôle d'accès et d'autorisation pendant la session de l'utilisateur. Pour l'authentification, le monde du WebSSO est divisé en deux types d'entités :

- **Fournisseurs d'identité :**
  un composant qui certifie l'identité d'un individu sur la base de facteurs d'authentification et qui propage cette identité à l'aide de jetons (tokens) cryptographiques
  (SAML Assertion, JSON Web Token, cookies chiffrés)
- **Les prestataires de services :**
  un composant qui fournit l'application et qui utilise l'identité (jeton cryptographique)

WAM peut traiter le cas précédent en utilisant un Active Directory, une base de données SQL ou un serveur Radius pour l'authentification multi-facteurs (MFA).

Par conséquent, Web Access Manager intégré à UBIKA WAAP Gateway et UBIKA WAAP Cloud permet d'avoir de meilleures politiques de sécurité et joue un rôle clé dans l'optimisation de la sécurité des applications modernes et plus anciennes.



Avantages

- **Simplification et centralisation des accès utilisateurs à toutes les applications web**

  La multiplication des mots de passe représente un défi majeur. Grâce à WAM, il suffit de mémoriser un seul identifiant & mot de passe pour accéder à différentes applications et il n'est pas nécessaire de le saisir à nouveau avant la fin de la journée. Cette capacité à améliorer la productivité et le confort de l'utilisateur final est l'un de ses plus grands avantages.

- **Approche sans agent et transparente pour les applications**

  Étant le point de contrôle unique pour l'authentification et l'autorisation, WAM simplifie la gestion et l'usage des applications. Il permet une traçabilité complète de qui a accès à quoi via un audit centralisé.

- **Authentification adaptative et sécurisée basée sur le contexte (Authentification basée sur le risque)**

  Il permet de surveiller le comportement des utilisateurs, la géolocalisation, quels appareils sont utilisés pour ajouter une couche de sécurité supplémentaire. L'option WAM intégrée à UBIKA WAAP Gateway et UBIKA WAAP Cloud est pertinent pour tous types de scénarios de sécurité, c'est l'une des principales raisons pour lesquelles les clients choisissent UBIKA WAAP Gateway et UBIKA WAAP Cloud.

- **Combinaison de différents facteurs d'authentification (authentification multifactorielle) à partir de différents annuaires (B2E, B2B, B2C)**

  WebSSO combiné à MFA améliore la sécurité en fournissant l'authentification pour toutes les applications protégées. Il vérifie si l'utilisateur est actif, ou si le mot de passe a expiré, auquel cas l'utilisateur est redirigé vers un écran de modification du mot de passe. Il crée une session chiffrée de bout en bout afin que l'utilisateur puisse être authentifié en toute sécurité.

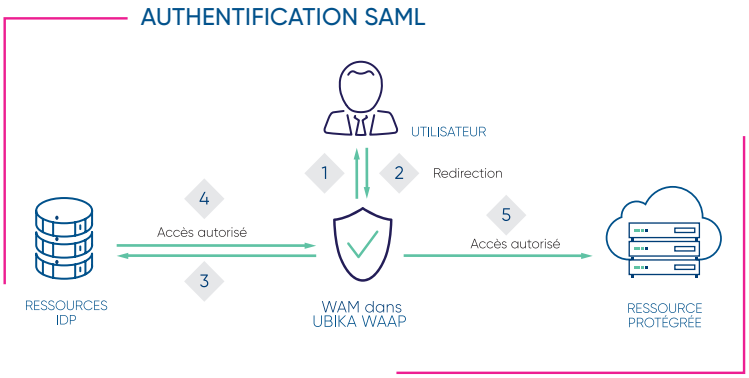
Comment cela fonctionne-t-il ?

L'autorisation se fait à l'aide du groupe LDAP (RBAC ou Role Based Access Control), mais elle peut également être définie sur la base d'un attribut (ABAC ou Attribute Based Access Control). La séquence d'authentification est très simple (ici un exemple de SAML) :

1. L'utilisateur se connecte à la ressource protégée.
2. S'il n'est pas authentifié, il est redirigé vers le fournisseur d'identité (IDP) pour authentification.
3. Il s'authentifie sur l'IDP.
4. Une fois authentifié et autorisé, il est redirigé vers la ressource protégée.
5. La preuve d'authentification est validée et l'utilisateur peut accéder à la ressource protégée.

Le SAML est principalement utilisé pour les SSO d'entreprises. Comme SAML, OAuth est un autre protocole permettant de déléguer l'autorisation des ressources. Le processus OAuth est similaire au processus SAML décrit ici.

Après l'authentification de l'utilisateur sur le périmètre de WAM, son authentification se propage sur l'application par différents protocoles de propagation d'informations d'identification comme le rejeu d'informations d'identification, l'en-tête HTTP, etc.



Version 01.00 | juin 2022
Données sous réserve de modification
Image : Adobe Stock

UBIKA
9-11 rue Jeanne Braconnier - 92366 Meudon | France
Tel +33 (0)1 46 20 96 00 | www.ubikasec.com