Concept Guide

Identity and Access Management

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

What is Identity Access Management?

IAM is a set of processes, policies and tools that enables management, control and assurance of digital identities. IAM technologies provide the ability to store identity and profile data securely and govern identity data so that only necessary and relevant information is shared as needed. IT staff can manage and control end-user access to information and resources within their organizations by employing a proper IAM framework.

IAM systems can be deployed as on-premises physical or virtual appliances or as virtual appliances hosted in a public cloud.

They can also be provided "as-a-service" through a cloud-based subscription model. Another possibility is deployment in a hybrid mode, where some of the IAM function is hosted on-prem and some in the cloud.

IAM fundamentally provides for and/or enables functions for:

- How identities are represented, generated, maintained, and authenticated in a system
- How roles are defined in a system and how they are assigned to individuals and groups
- Adding, removing, and updating identities and their roles in a system
- Assigning access controls to identities or groups of identities, and
- Protecting the sensitive data within the system and securing the system itself.

Intended audience

Mid-level network and security architects in companies of all sizes and verticals should find this guide helpful.

About this guide

This guide aims to provide a broad overview of IAM concepts and introduce products in the Fortinet portfolio that work together to implement a scalable IAM solution.

Industry-standard terminologies are introduced to Fortinet-specific terms, concepts, and technologies. Readers can proceed to the IAM Architecture and IAM Deployment guides when they are familiar with the concept and terminology and are ready to explore different designs to use in their environment.

IAM concepts

IAM concepts can be viewed from 3 different perspectives: convenience (UX), security, and platform. The following diagram summarizes the most important features of each viewpoint.

Terms and definitions

Identity

Identity, specifically digital identity, is used by computer systems to represent an entity. This could be a person, organization, application, or device. For example, an identity can define a person who can be a web server system administrator or an application's end-user.

Digital identity usually includes a username, credentials, and profile attributes.

Identity Provider

The IdP creates, maintains, and manages end-user identity information and provides authentication services to relying applications within a federation or distributed network.

Identity providers are responsible for authenticating users. Relying party applications, such as web applications, outsource the user authentication step to a trusted IdP. Such a relying party application is said to be federated because it consumes federated identity.

An IdP allows single sign-on (SSO) to access other websites. SSO enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface.

Identity providers can facilitate connections between cloud computing resources and users, thus decreasing the need for users to re-authenticate when using mobile and roaming applications.

IdP Proxy

The IdP Proxy serves as the IdP to configured Service Providers or Relying Parties. The IdP Proxy will proxy authentication requests to the actual user identity source (or directory), which can be on-prem (e.g., Active Directory) or in the cloud (e.g., Azure AD).

The IdP proxy can work with more than one of the actual user identity sources, thereby facilitating BYOId (Bring Your Own Identity).

Zero Trust

Zero trust is a network security philosophy that states that no one inside or outside the network should be trusted to access resources unless their identification has been thoroughly checked. Zero trust operates on the assumption that threats both outside and inside the network are an omnipresent factor. Zero trust also assumes that every attempt to access the network or an application is a threat. These assumptions inform the thinking of network administrators, compelling them to design stringent, trustless.

See Zero trust tunnels.

Authentication

Authentication in the context of IAM means ensuring that identity is valid when an Authentication Request is submitted to the IAM product or service by an Authentication Client. For example, consider an online identity in the form of a username submitted by a RADIUS client (generically referred to as an Authentication Client) in a RADIUS Access-Request message (generically referred to as an Authentication Request) to a RADIUS Server (i.e., the IAM product or service).

That username can be validated by challenging the user to provide a secret password.

See Authentication to learn more about how to configure different authentication services on FortiAuthenticator.

Next, we will review some primary ways to authenticate an identity.

Authentication Client

Authentication Client generally refers to the application, website or service the end-user is trying to access. The Authentication Client is the entity that submits the Authentication request, either directly over some communications protocol or indirectly via a protocol that orchestrates redirection to the IAM product or service.

Password Authentication

Password Authentication is the most basic and popular legacy authentication method, where a password is specified as the credential for validation. Organizations can impose rules on length, complexity and constitution on passwords, but password-only authentication is the main weakness leading to online attacks.

Multi-Factor Authentication

Multi-Factor Authentication is the most common robust authentication method used today to authenticate an online identity. This method requires the user to provide two or more verification factors to access an online resource. The factors are something you know (e.g., password), something you have (e.g., One Time Password token), and something you are (e.g., fingerprint).

Adaptive Authentication

Adaptive Authentication allows for adjusting the type and strength of authentication required by using the context of the login attempt. Attributes like the user's location, IP address, device hygiene and time of day/day of the week can be used

to determine if a user's login attempt should be accepted, further challenged, or blocked entirely.

FIDO Passwordless Authentication

Based on PKI principles, Fast Identity Online (FIDO) is an emerging technology that allows users to sign in securely without using a password for any website or application that supports it. FIDO2 protocols are supported by all major web browsers and devices, including smartphones, desktops, laptops, tablets, and smartwatches. Besides the convenience of passwordless authentication, FIDO is also phishing resistant, making it a more secure authentication method.

A user must first register a security key at the FIDO2-supported application or website to choose a security key, which can be either a roaming (e.g., USB device or smartphone) or a built-in platform authenticator (e.g., Windows Hello).

The private key never leaves the user's authenticator. When the user signs into the same application or website, the device selects the private key associated with that application or website. It signs a challenge and sends it to the online FIDO2 service. The service verifies the challenge against the known public key and grants the user access. To access the private key, the user must identify themself with a biometric (or PIN) locally to the authenticator and then the authenticator uses FIDO2 protocols to authenticate to the app or website.

Certificate Authentication

Also based on PKI. Certificate-based authentication has been used by government agencies and other organizations requiring the strictest security environments for decades, long pre-dating FIDO.

Users and Groups

In general, a user is an entity represented by a digital identity.

A group is a collection of users that usually have something in common.

For example, a role can be assigned to a group of users.

See User management to learn more about creating and managing FortiAuthenticator user database.

Roles, Permissions and Policies

Permission refers to the ability to access a given resource. A role is a collection of permissions. All the permissions the role contains are granted if a role is assigned to an identity.

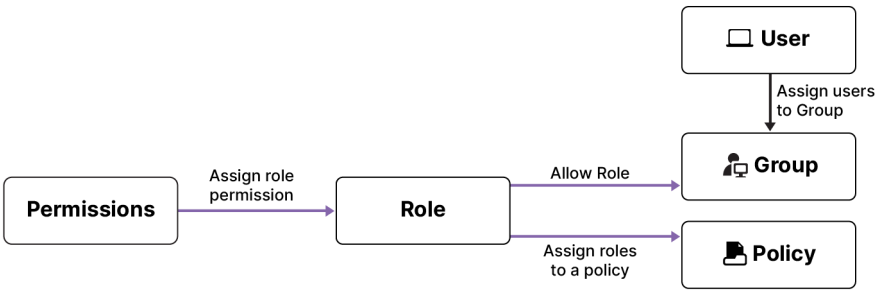
See Admin profiles.

Policy is a set of role bindings that bind one or more identities to specific roles. A policy is created to define which identities have access and what type of access to a resource.

See User account, RADIUS, TACACS+, OAuth, captive, and self-service policies.

FortiAuthenticator is designed to provide information from authentication sources to other systems for privileged access to effect role-based access to an organization's resources.

This concept is shown in the diagram:



User Directory

User directories maintain user information, including username, password, email address and other user profile information. They provide services that allow the sharing and validating information about a user in an organization. Windows Active Directory is an example.

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol. For example, a client can use LDAP to query Windows Active Directory to obtain user profile attributes or to authenticate the user's password.

Policy Enforcement Point (PEP)

Policy Enforcement Point is a system that requests, receives, and subsequently enforces authorization decisions that determine whether a request to access a resource will be allowed or denied.

Policy Decision Point (PDP)

Policy Decision Point is a system that makes authorization decisions for itself or for other system entities requesting such decisions. The Policy Decision Point can be further decomposed into Policy engine and Policy administrator but can be viewed simply as the Policy Decision Point in the context of IAM concepts.

Fortinet ZTNA solutions incorporate the concepts of PEP and PDP and integrate with FortiAuthenticator to receive information necessary to associate ZTNA policies with specific users and groups.

Federation

Federated identity is characterized by a trust relationship between separate organizations and third parties, such as SaaS providers or enterprise partners, that allows them to share identities and authenticate users across domains. An entity can authenticate in one organization and then access another organization's resources without having to perform another login when an identity is federated.

Single Sign On (SSO)

As the name implies, SSO allows users to access multiple resources (e.g., HR, payroll, inventory) with a single authenticated login. Several protocols are used in the industry to accomplish this:

SAML

Security Assertion Markup Language is an XML-based open standard for transferring identity data between an identity provider (IdP) and a service provider (SP). The IdP can be an on-prem directory, database, or cloud-based (e.g., Azure,

Okta, Ping). The SP is an on-prem or cloud application that users need to access.

See SAML.

OIDC

OpenID Connect is an identity layer built on the OAuth 2.0 framework. It allows third-party applications to verify the end-user's identity and obtain basic user profile information. OIDC uses JSON web tokens obtained using flows conforming to the OAuth 2.0 specifications. OAuth 2.0, or "Open Authorization," is a standard designed to allow websites and applications to access resources hosted by other web apps on behalf of a user. It was not meant for authentication, which OIDC achieves by adding an identity layer to the OAuth flow.

See OAuth.

Fortinet SSO (FSSO)

FSSO is a proprietary protocol and system and method used to collect login and logoff event date from various external systems and send them to Fortinet devices to authenticate users transparently.

See Fortinet SSO.

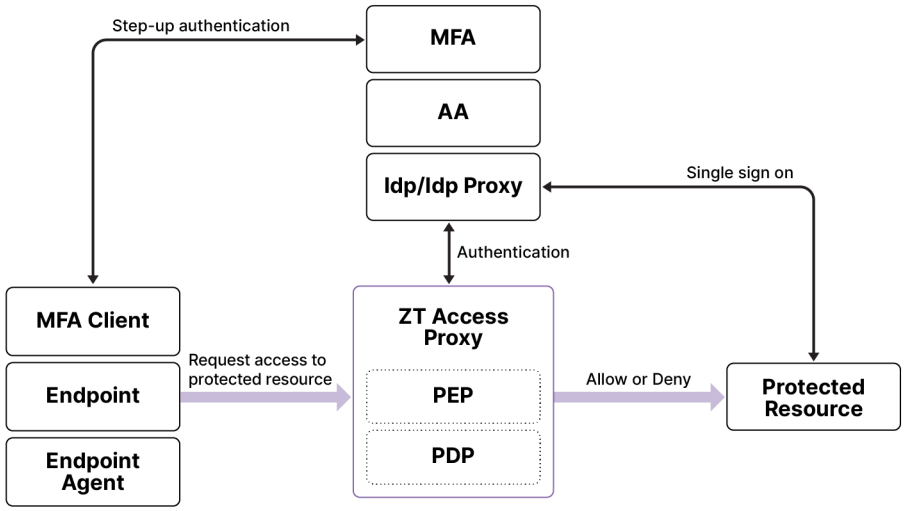
Endpoint Agent

An endpoint is any device that is physically an endpoint on a network. Laptops, desktops, mobile phones, tablets, servers, and virtual environments can all be endpoints.

An endpoint agent is a lightweight background application installed on a device's operating system to perform one or more functions. In the IAM context, the agent continuously gathers information about the endpoint and reports the data to a server. The collected information can include login status, device type, OS version and patch level, IP address, and user agent.

High level solution architecture

A high level IAM Conceptual Architecture in the context of ZTNA showing the relationship between the main concepts described above is shown in the diagram below:



HIGH LEVEL SOLUTION ARCHITECTURE

In this context, a user at an endpoint tries to access a resource protected by a Zero Trust Access Proxy that contains the PEP and PDP. The proxy will use the IdP to verify that the user identity has been authenticated. The Access Proxy enforces the configured policy based on parameters such as device type, device posture, OS, patch level location and time of day/day of the week to decide whether to allow or deny access. Suppose access is permitted to a relying application. In that case, the relying application can use the IdP to determine if the user has already been authenticated and whether additional authentication (i.e., MFA) is required.

A concrete example would flow like this:

1. The user opens the computer and logs in to Azure AD. Azure AD is the actual source of the user identity.
2. The user has a ZTNA agent installed on the computer, so requests are proxied through the ZT Access Proxy.
3. The user navigates to a SaaS (e.g., Salesforce) federated with a SAML IdP. The request is proxied via the ZT Access Proxy. The SAML IdP, in the role of IdP Proxy, uses AAD as a remote authentication server.
4. The ZT Access Proxy recognizes the user is logged in to AAD and applies the appropriate policy to the endpoint
5. If the endpoint is allowed to access the SaaS, then the request is proxied to the SaaS.
6. The SaaS requests authenticate to the IdP Proxy, which will assert that the user is logged in to the actual IdP
7. The SaaS will then allow the user access with no further authentication required or can decide to step up the authentication and require MFA if, for example, the user is trying to log in from a new location.

Fortinet products are easily integrated over the Security Fabric to realize these concepts into concrete systems that can solve real-world IAM challenges.

Fortinet IAM products offer highly versatile and scalable authentication features.

FortiAuthenticator supports a wide range of authentication protocols, including RADIUS, TACACS+, SAML, OIDC, Oauth2 and FIDO webauth, allowing for many types of authentication clients to use it for identity management and verification.

While FortiAuthenticator provides limited MFA and Adaptive Authentication features, FortiToken Cloud brings many enhanced features for managing the security and convenience of these features that can be applied en masse or tailored to the individual level.

IAM components

FortiAuthenticator

FortiAuthenticator is Fortinet's primary IAM server. Various products, applications, and services can use FortiAuthenticator to centralize authentication locally or against remote authentication servers. FortiAuthenticator supports legacy and modern authentication protocols and has a comprehensive REST API. It also can perform FIDO passwordless registration and authentication.

FortiAuthenticator is deployed as a physical or virtual appliance or as a FortiAuthenticator Cloud service hosted by Fortinet.

FortiAuthenticator Cloud is only available as part of the FortiTrust Identity subscription, which bundles FortiAuthenticator Cloud and FortiToken Cloud.

Another major feature of FortiAuthenticator is that of a PKI Certificate Manager. FortiAuthenticator can be configured as a Certificate Authority and can be used to enroll server and user certificates for secure authentication.

FortiAuthenticator can be configured as a SAML SSO Identity Provider or as an IdP proxy to federate multiple third-party directories. It can also serve as an OIDC Provider for SSO, which is especially useful for use cases involving mobile and native apps.

FortiAuthenticator acts as a central collector to channel login/logoff status from various external sources and makes them available to FortiGate Single Sign On (FSSO).

FortiToken Cloud

Although Fortinet Inc. appliances can provide native MFA to centralize MFA management, it lacks the depth of features afforded by FortiToken Cloud.

FortiToken Cloud offers unparalleled flexibility with features such as Realms and User Aliasing. It can also be used to dynamically control the authentication strength required on each login based on the context.

FortiToken

FortiToken is the client side of MFA. Several form factors are available, including hard token OTP, soft token (FortiToken Mobile) OTP, email and SMS OTP, FIDO and client certificate authentication.

ZTNA

ZTNA is an integrated component of the Fortinet Security Fabric, giving administrators the assurance that only trusted and validated users/devices can access sensitive data stored in corporate and SaaS applications from anywhere.

A ZTNA deployment consists of 2 parts:

- FortiClient ZTNA Agent installed on the endpoint can connect from anywhere to access applications hosted in the company, data center, cloud data center or SaaS.
- FortiGate Access Proxy sits between the endpoints and applications and continuously validates the posture and identity of each connection, providing secure micro-segmented access for each session.

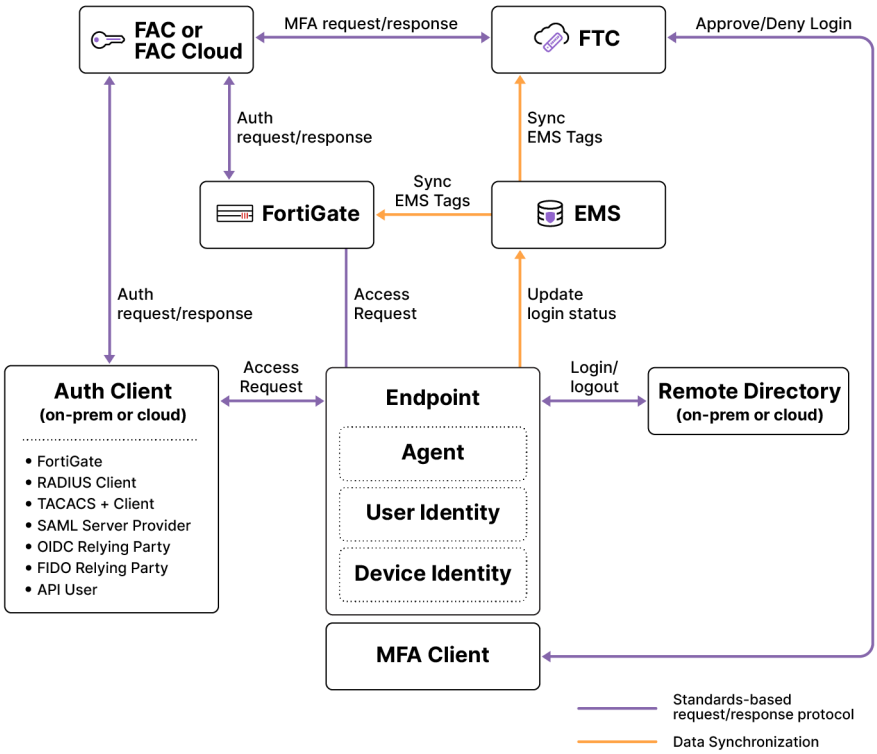
FortiClient Enterprise Management Server

EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. These profiles are synchronized with the FortiGate for use in authorization policies.

Concepts to product mapping

The table below shows how the concepts map to products:

Concept	Component
Identity, Authentication, Federation, SSO	FortiAuthenticator/FortiAuthenticator Cloud
MFA server, Adaptive Authentication	FortiToken Cloud
MFA client	FortiToken/FortiToken Mobile
Policy Enforcement Point	FortiGate
Policy Decision Point	FortiClient EMS
Endpoint Agent	FortiClient



These components can scale from very small SMB deployments to very large enterprise deployments.

Conclusion

IAM aims to ensure that the right people and organization roles (identities) can access the resources they need to do their jobs.

In other words, the goal is to enforce that only the right identities can access any given computer, hardware, software app, IT resource, or perform specific tasks.

More information

MFA resources

www.fortinet.com

23-660-935262-20231211