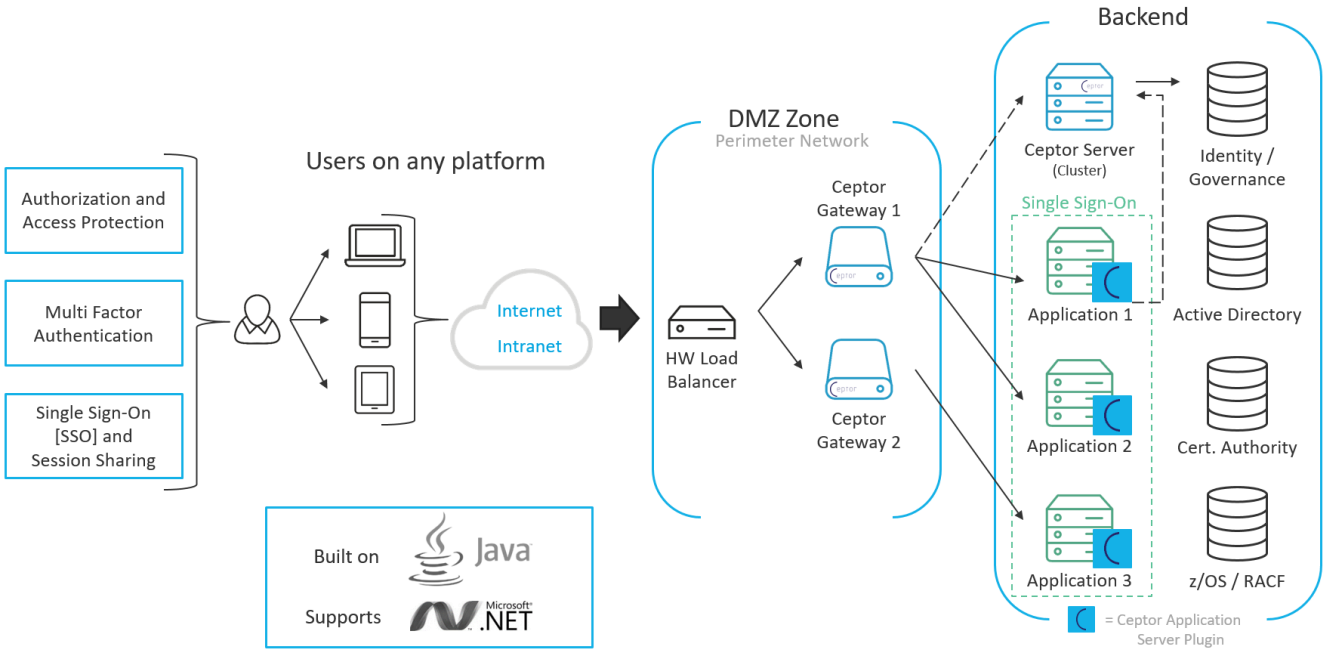
What is Ceptor

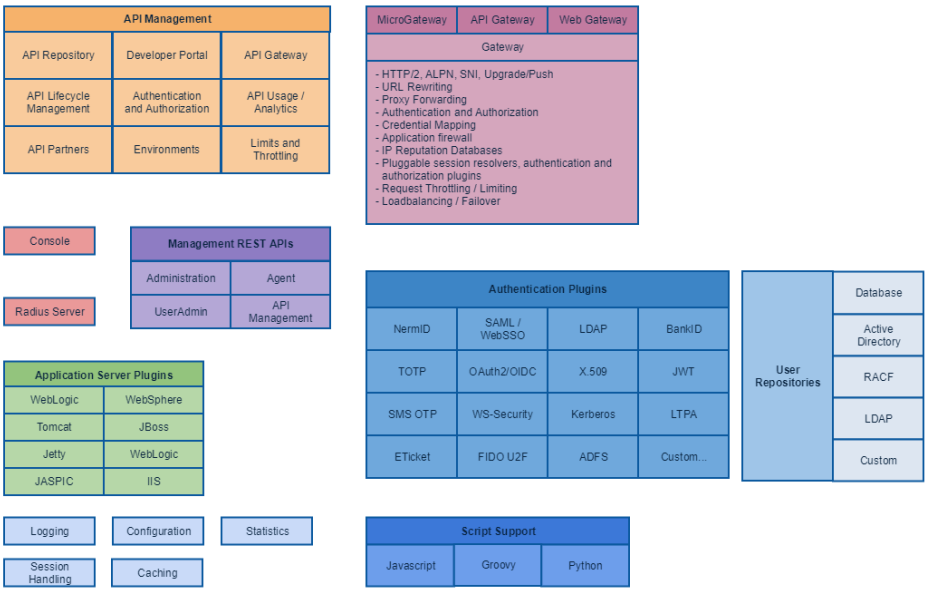
Ceptor is and provides:

- API Management
- Access Management
- Single Sign On (SSO)
- Multifactor Authentication
- And more...

Solution Overview

Ceptor protects access to your applications and APIs - the following shows a typical setup, where Ceptor Gateway is deployed in a DMZ zone, providing secure and authenticated access to applications, sharing a users identity between them.





API Management

Ceptor API Management provides the 5 pillars of API Management;

1. **Expose enterprise data and functionality in API-friendly formats**
   Convert complex on-premise application services into developer-friendly RESTful APIs.
2. **Protect information assets exposed via APIs to prevent misuse**
   Ensure that enterprise systems are protected against message-level attack and hijack
   Protecting your APIs and operations providing the flexibility you need.
3. **Authorize secure, seamless access for valid identities**
   Deploy strong access control, identity federation and social login functionality.
   Allow any standard or non-standard authentication method, keeping options simple for small companies, but scaling up the the large complex requirements of large enterprises.
4. **Optimize system performance and manage the API lifecycle**
   Maintain the availability of backend systems for APIs, applications and end users.
   Publish the same API with different implementations in all your environments
5. **Engage, onboard, educate and manage developers**
   Give developers the resources they need to create applications that deliver real value.
   Allow developers access to sandbox environments where they can safely test your mock implementations.

Building on top of the proven security and flexibility of Ceptor itself, Ceptor API Management allows you full control over managing your APIs - multiple formats and methodologies supported.

Go in detail here: Ceptor API Management

Access Management

Ceptor offers many different forms of Access Management, allowing you to tailer the configuration to match your environment and requirements.

You can authenticate users using any standard or custom authentication method, assign individual security levels to their various forms of authentication, depending not just on the method used, but also the way the credentials were distributed to your users - e.g. there is a difference in the security level of users who have self-registered and the users you have identified and been in personal contact with, done address verification of etc.

You can perform complex authorization decisions using RBAC (Role Based Access Control) or ABAC (Attribute Based Access Control) within either Ceptor Gateway before reaching your applications, or within Ceptor Agent callable from your applications.

Single Sign On (SSO)

One of the core features within Ceptor, is its ability to offer Single Sign On (SSO) to all applications within simple or complex environments.

Once a user is authenticated, Ceptor Gateway can be configured to share this information with your individual applications - many different methods are available for this, including Application Server Integrations which provides plugins to your favorite application server, allowing integration to its specific security APIs.

Adding new authentication methods is simple, and applications does not need to have any knowledge about the fact - this allows you to change or add authentication methods such as Multi Factor authentication without changing a single line of code in any of your applications.

You can even federate identity information to or from your partners using either custom methods, or industry standards such as OpenID Connect or SAML WebSSO

Multifactor Authentication

Ceptor provides Multifactor authentication to your applications.

These are examples of some types of multifactor authentication types you can use:

- TOTP Authenticator (e.g. Google Authenticator) - Works with hardware tokens as well as software tokens, mobile apps. etc. - supports QR code generation for registration.
- SMS OTP codes - generates and sends SMS/Text messages to your users with one-time-passwords.
- FIDO U2F - Authenticate using FIDO U2F tokens, either separate tokens or the builtin ones in newer laptops.
- NemID

Adding a new authentication method is as simple as creating an authentication plugin in Ceptor Session Controller and configuring the gateway to use it (or one of your own applications if you prefer to host the authentication interface within your own application) - more info here: Authentication Plugins

And more...

Besides the functionality mentioned above, Ceptor provides much more, including:

- Centralized configuration, statistics and monitoring
- SLA Report generation

- Radius Server, integrating SSO with your network peripherals
- WS-Security, with proxying support - protects SOAP services without modifying application code.