Paweł Rajba
pawel@cs.uni.wroc.pl
http://pawel.ii.uni.wroc.pl/

Identity and Access Control

Agenda

- Introduction
- AAA Introduction
- Authentication
  - Concepts, Methods, Factors
- Authorizations
- Accounting
- Access Control
  - Models, Solutions
- IAM as a process

Introduction

Identity and access management (IAM) is the security discipline that enables

the right individuals to access

the right resources at

the right times for

the right reasons.

Gartner

http://www.gartner.com/it-glossary/identity-and-access-management-iam

Introduction

- Authentication, Authorization, Accounting (AAA)
- Access Control
- AAA & Directory Services
- Single Sign-On (SSO)
- User Provisioning and Deactivation
- Access Management
- Delegated administration
- Password Administration and Synchronization
- Federated Identity
- Trunsitive trust/authentication

Introduction

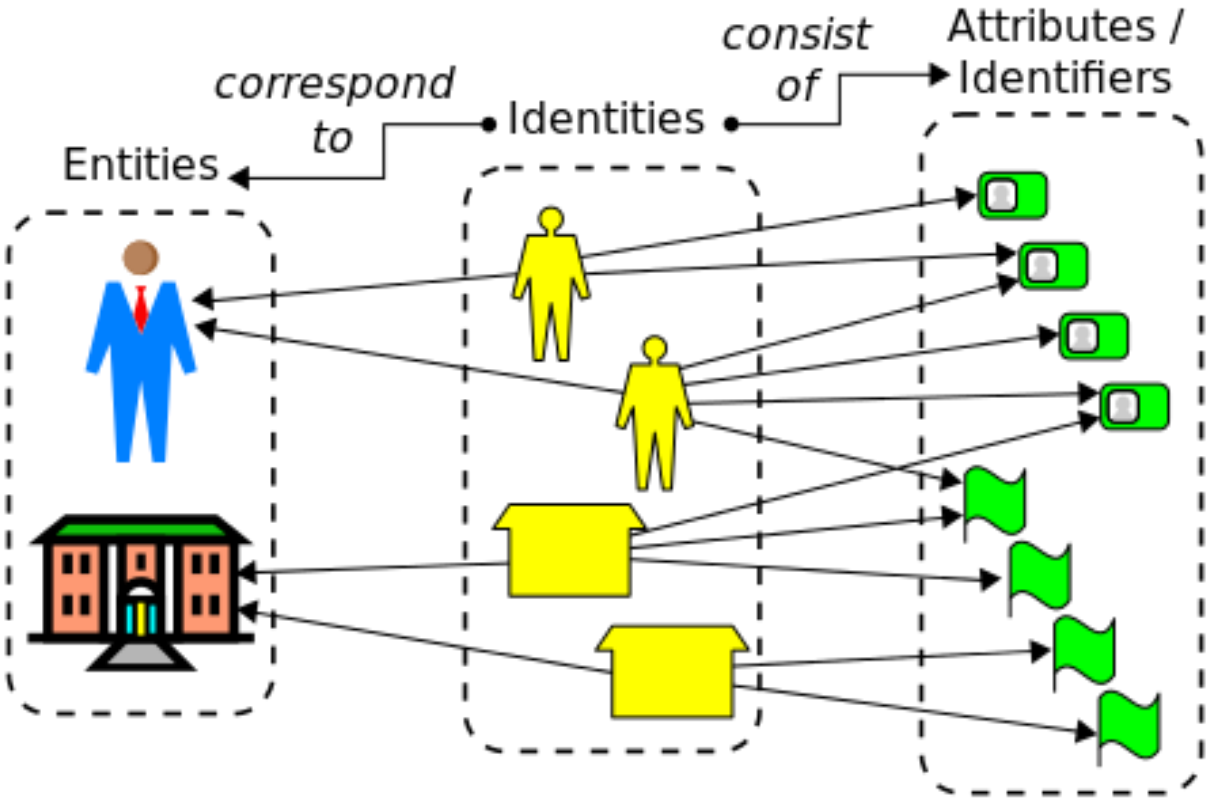
- Related topics

- Access control
- Authentication
- Authorization
- Claims-based identity
- Computer security
- Digital card
- Digital identity
- Directory service
- Dongle
- Federated identity management
- Hardware security module
- Identity assurance
- Identity driven networking
- Identity management systems
- Identity provider
- Identity-based security
- Information privacy
- Initiative For Open Authentication
- List of single sign-on implementations
- Loyalty card
- Mobile identity management
- Mobile signature
- Multi-factor authentication
- Mutual authentication
- OAuth
- Online identity management
- OpenID
- Password management
- Personally Identifiable Information
- Privileged identity management
- RBAC
- SAML 2.0
- SAML-based products and services
- Security token
- Service provider
- Single sign-on
- Software token
- Two-factor authentication
- User modelling
- Web service
  - WS-Security
  - WS-Trust
- Workflow application

https://en.wikipedia.org/wiki/Identity_management

Introduction

- Identities



AAA introduction

- Identification
  - Introduction + entry in memory
- Authentication (AuthN)
  - Identification + proof
- Authorization (AuthZ)
  - Permissions is the subject
- Accounting (auditing)
  - Trace information

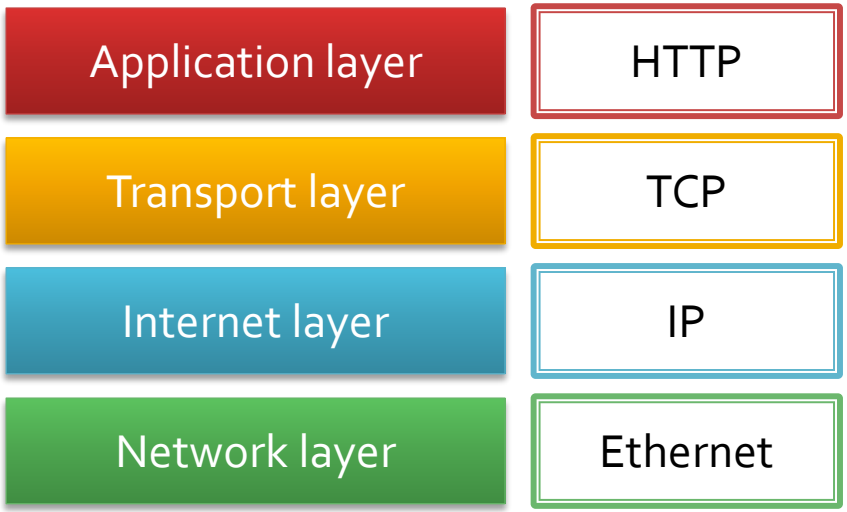
AAA introduction

- Access Control System
  - Combining AAA with additional rules, policies
  - Examples
    - Rules on passwords (complexity, regular changes, history)
    - Object owner is able to determine or define object perms
    - Access denied by default

Authentication

- Purpose
  - Verify a user, verify a service
- Common scenarios
  - User to service
  - Service to user
  - Service to service
  - User to network
  - Service to network

Authentication



Authentication concepts

- Network level
  - RADIUS
  - TACACS+
- Service level
  - PAP, CHAP
  - HTTP Basic
  - Form-based
  - NTLM
  - Kerberos
  - OpenID Connect (don't confuse with OpenID)
  - SAML2
  - Smart Cards
    - Includes chip
    - Requires device + PIN
    - Usually combined with multifactor authN

Authentication concepts

- Multifactor authentication
  - Something…
    - you know (e.g. a password)
    - you have (e.g. a token)
    - you are (e.g. a fingerprint)
- Type of authentication
  - Single factor
  - Dual-, multi-factor
    - E.g. smartcard + PIN
    - (password, OTP, PIN, Biometrics)

Authentication concepts

- Single Sign-On
  - Concept
  - Protocols supporting SSO
    - Kerberos, SAML2, WS-Trust, WS-Federation, OAuth2
  - Common solution based on web portals
  - Frequent challenge: cross-domains SSO
- Authentication Services
  - Local
  - Remote

Authentication concepts

- Trunsitive trust (actually, not only authN)
  - One way trust
    - A trusts B / B doesn't trusts A
  - Two way trust
    - A trusts B / B trusts A
  - Non-transitive trust
    - A trusts B, but doesn't allow to extend the trust
  - Transitive trust
    - A trusts B, B trusts C, so A trusts C

Authentication methods

- PAP
  - Password Authentication Protocol
  - Username/Password is sent to server and verified
  - Password sent in clear text, no longer used
- CHAP
  - Challenge Handshake Authentication Protocol
  - Hash based on shared secret (password) and compared on client and server
  - Used to authenticate PPP clients

Authentication Methods

- HTTP Basic
  - A client sends a request to a protected resource
  - A server answers with 401 HTTP status
    - Additionaly a Realm (area description) is attached
  - In the client's browser usually a prompt for a login and password pops up
    - With every subsequent request a new header is attached Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
      - In data login:password sequence is encoded using Base64 algorithm
  - After providing a correct credentials the client is able access the resource on the server

Authentication Methods

- Forms authentication
  - Based on login form and authentication cookie
  - Commonly used in simple scenarios
  - HTTPS required
  - Supported in many frameworks

Authentication Methods

- OpenID Connect, SAML2
  - Support federation with third party application
  - We will cover that in details in next presentation

Authentication Methods

- CAPTCHA (usually also considered as CRAM)
  - Stands for
    - Completely Automated Public Turing test to tell Computers and Humans Apart
  - Common challenges
    - Finding good ballance (too hard for a user)
    - Applying OCR
    - Social engineering attacks
    - Hire people (e.g. from Asia) to resolve

Authentication factors

- Authentication factors
  - Sth you know
    - Challenge questions
    - Simple/Complex password
    - Swipe gesture
  - Sth you have
    - Certificate
    - OTP (SMS, Digipass)
    - Smart Card
  - Sth you are
    - Fingerprint, retina
  - Where you are
    - Based on location (e.g. GPS)
  - Example combinations
    - Smartcard + PIN
    - Password + OTP
    - Certificate + Password
    - Password + fingerprint

Authentication factors

- Accounts/Passwords – threats
  - Shared/group accounts
  - User can forget the password
  - Weak recovery challenge questions or methods
    - E.g. after 1h discussion you can answer all questions (what a nice dog…)
  - Attacker may see or record when one is typing
  - Keyloggers
  - Stolen passwords database (online vs. offline attacks)
  - Sniffing (e.g. local network)
  - Phishing
  - Dictionary and brute force attack
  - Social attack
  - Re-use attack
    - E.g. the same password in different places

Authentication factors

- Accounts/Passwords – how to protect?
  - Central accounts/passwords management (AD)
  - Policy enforcement for whole domain
  - Encrypt or hash passwords
  - Apply salt and pepper for hashes (why?)
  - Don’t use default accounts (admin, guest)
  - Smart policy in case authentication failed
    - Lock after 6 tries (is it a good idea?)
    - 3s delay to the next try

Authentication factors

- Accounts/Passwords – how to protect?
  - Password policy
    - Complexity
      - Password vs. passphrase
      - Specials chars, upper/lower
    - Expiration (when by default?)
    - Minimum length
      - Do we really need 16 characters long passwords? Why PINs are only 4 digits long?
    - Password history
      - With minimum time of usage – why?
  - Masked password
  - Remember password (ORLY?)

Authentication factors

- Smart cards – threats
  - Steal card
  - Hack an issuer of cards
- One-time passwords – threats
  - We consider both
    - Synchronic (generators on both sides)
    - Asynchronic (challenge-response protocol)
  - Again, steal device, hack device
  - Find a initial value for generator
    - Through hacking an issuer server

Authentication factors

- Biometrics – threats
  - Retina scan, finger print, voice recognition, signature recognition
  - Main problem: biometrics accuracy
    - False Rejection Rate (FRR) – false negative
    - False Acceptance Rate (FAR) – false positive
  - Accuracy problem implies that one may pretend by getting e.g. victims fingerprints
  - Accuracy ranking
    - retina > fingerprint > signature > voice

Authorizations

- Define who is allowed to do what
  - Very often expressed as a matrix
- Make sure they are documented, consistent and complete
- Put special attention to privileged and administrative accounts
- Authorizations can be
  - very simple (expressed by roles)
  - very complicated (with business logic)
- Related area: authorizations management

Accounting

- Mechanism to trace activities in the solution
- Can be local or centralized
- Usually mandatory for priviliged and admin accounts
- What to trace?
  - Login attempts (successful or/and not)
  - Modification of records
  - Reads of records
  - Many others (should be defined in policies & directives)
- Challenges
  - Strategy for log retention
  - Make sure that log is protected
  - No repudiation

Access Control

- Combining AAA with additional policies
- Execute check if a subject should access the resource or activity
- Usually we consider
  - Decision Point
  - Enforcement Point
- Role of „jump-host”
- Common pricinples
  - Least privilege, Need to know
  - Separation of duties
    - Prevents one person get to much power
    - Can be defined on the permissions level
- Time of day restrictions

Access Control Models

- Discretionary Access Control
  - Owner of an object is able to decide who is allowed to access it
  - Very flexible, but less secure
  - Common example: file system ACL
- Mandatory Access Control
  - Access rules defined centrally
  - Inflexible and hard to manage
  - … but offers the higher security
  - Usually based on hierarchical sensitive labels

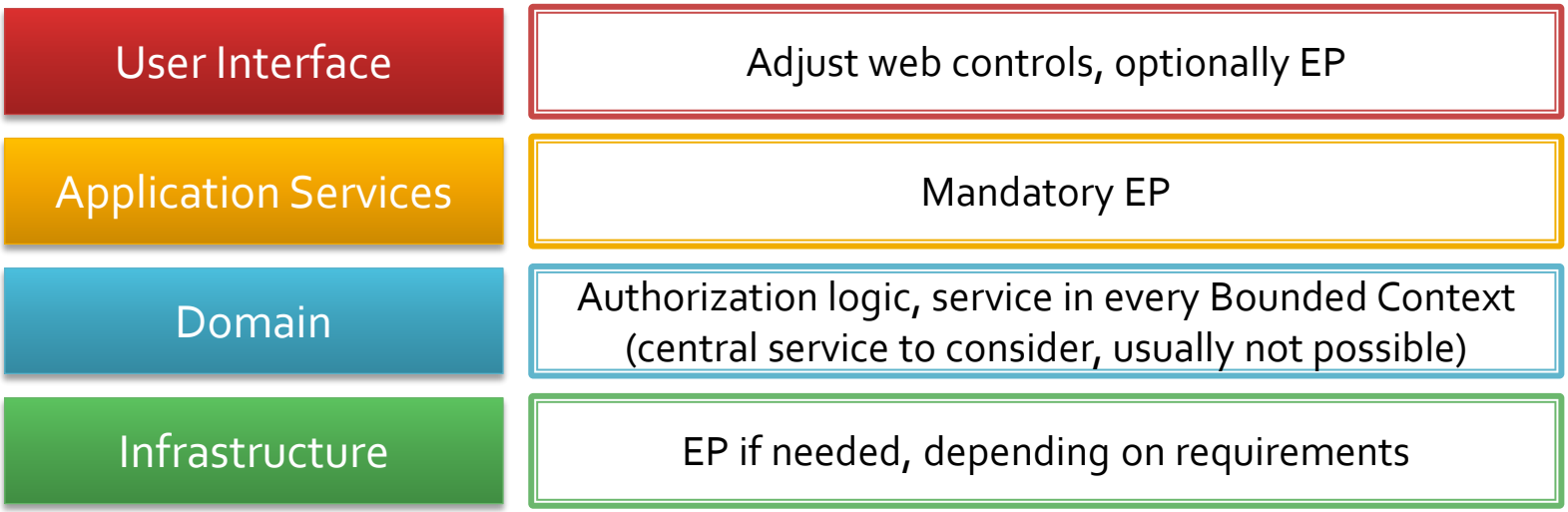
Access Control Models

- Role-based access control
  - Based on roles/groups
  - Roles are usually organized in a hierarchy
  - Roles are controlled centrally
    - MAC model is intended for only read and write
    - Roles are considered as set of permissions and give more flexibility
  - A lot of systems implement RBAC
- Attribute-based access control
  - Not based on rights assigned to subject
  - Based on attributes which are used to prove the truth of statements (i.e. claims)
  - Example:
    - Claim: „older than 18"
    - Anyone, who can prove that statement, has granted access

Source: http://en.wikipedia.org/wiki/Computer_access_control

Access control solution

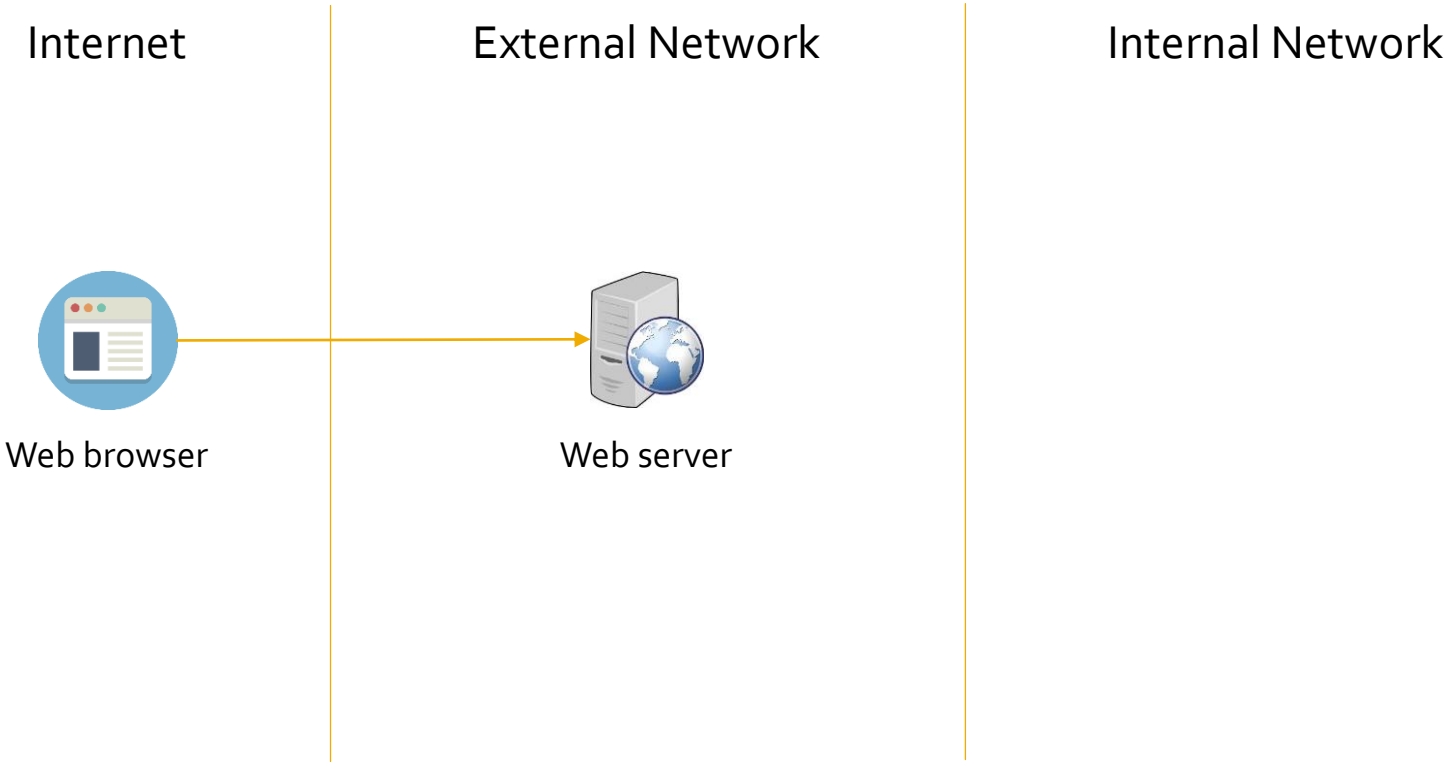
- Access control in software architecture



- Consider CQS

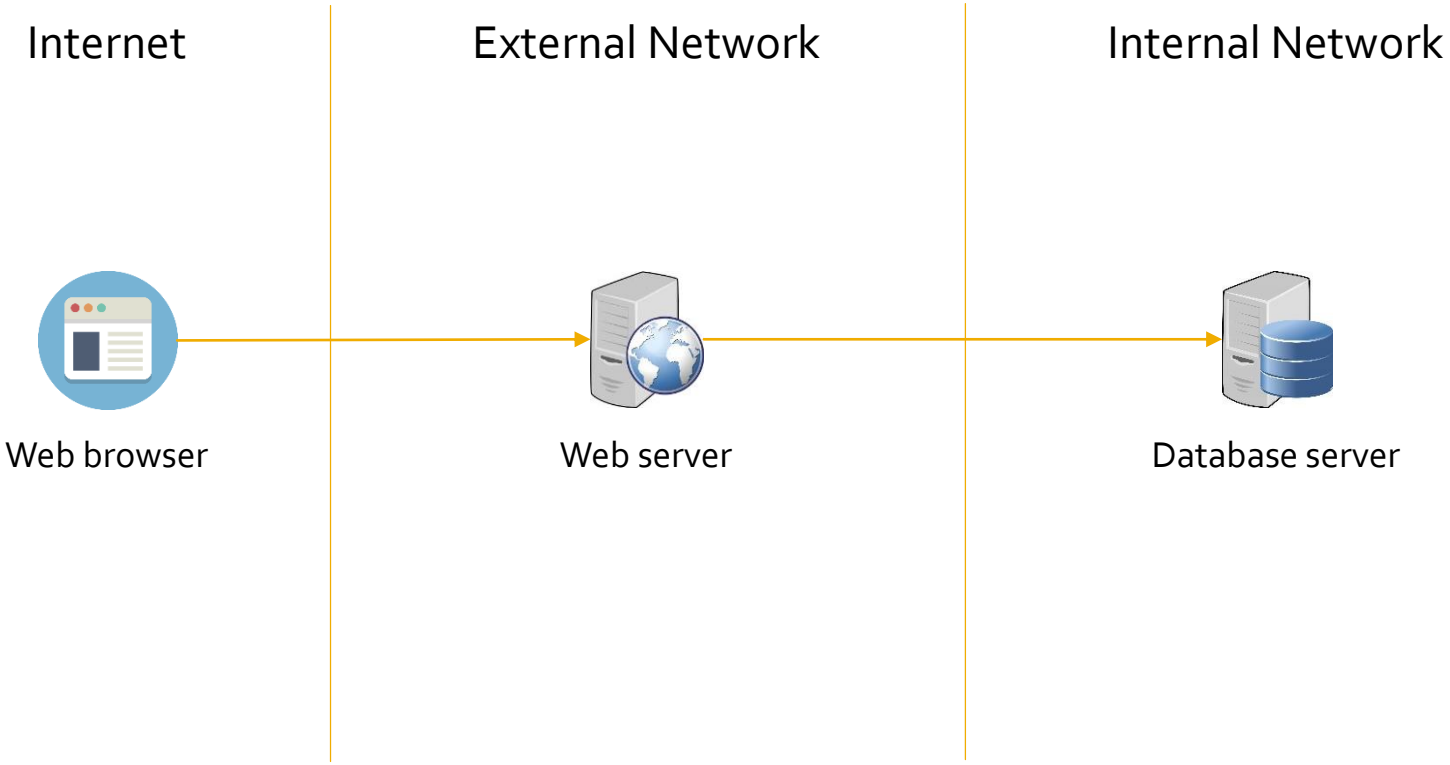
Access control solution

- Simple scenario



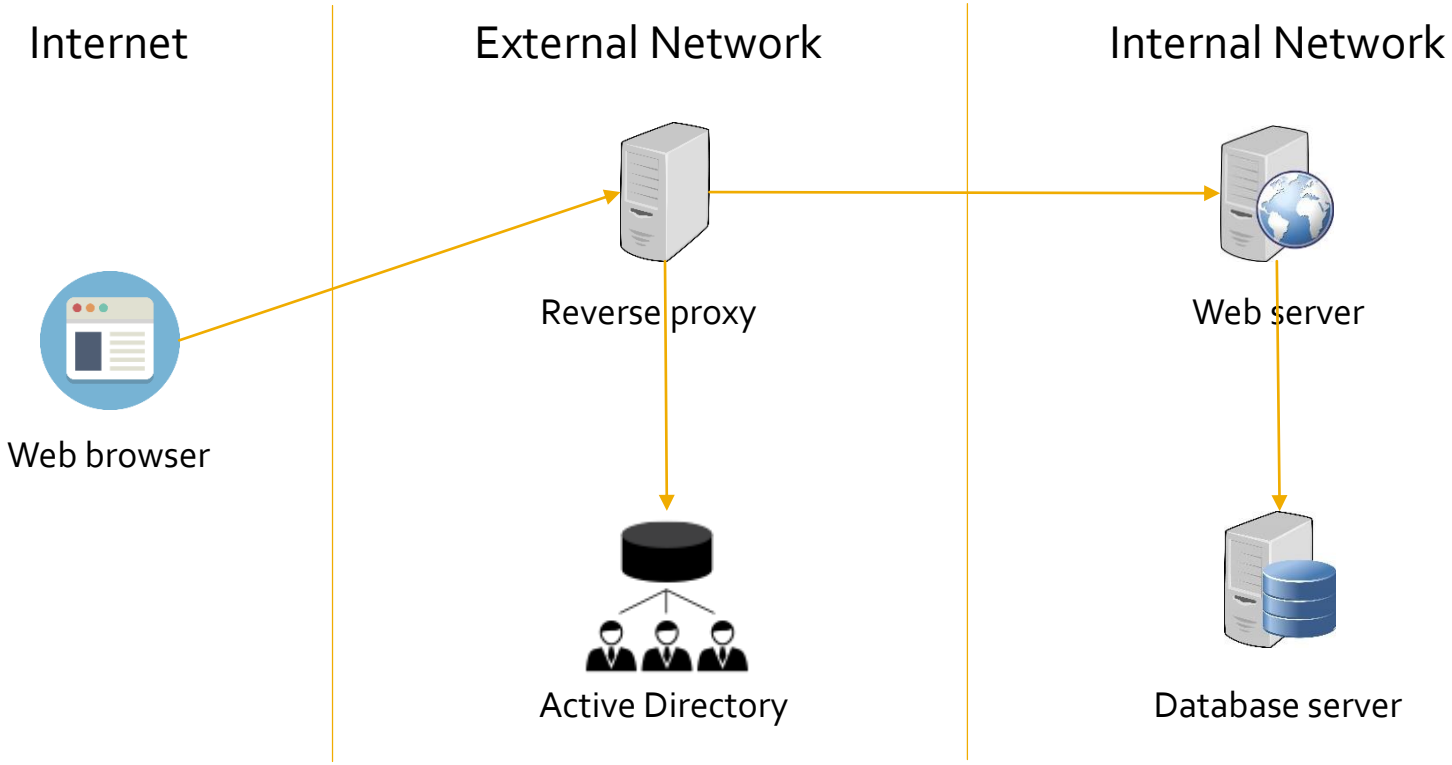
Access control solution

- Simple scenario with a database



Access control solution

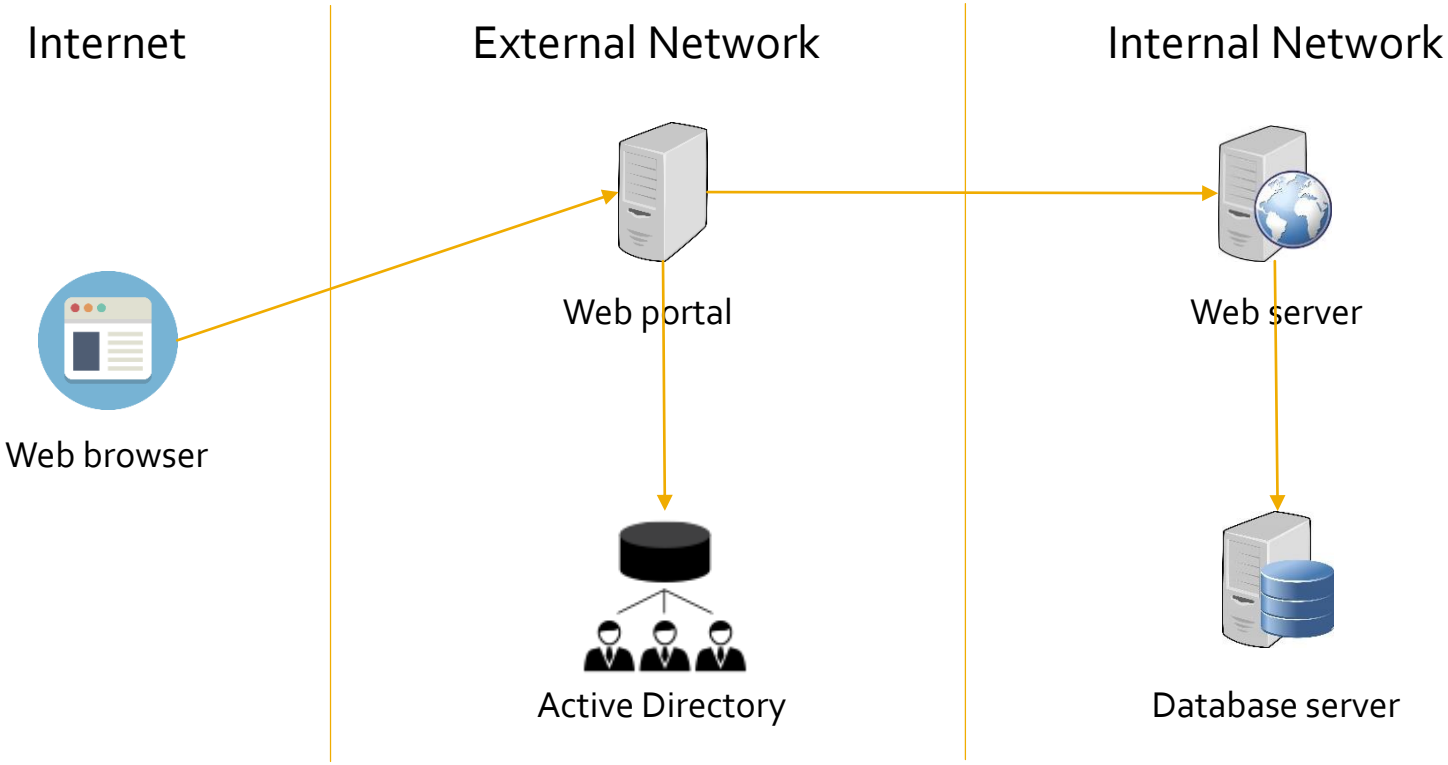
- Scenario with a reverse proxy



Q: Where is the EP? What is the split between Reverse Proxy and Web server?
Role of Web Access Management

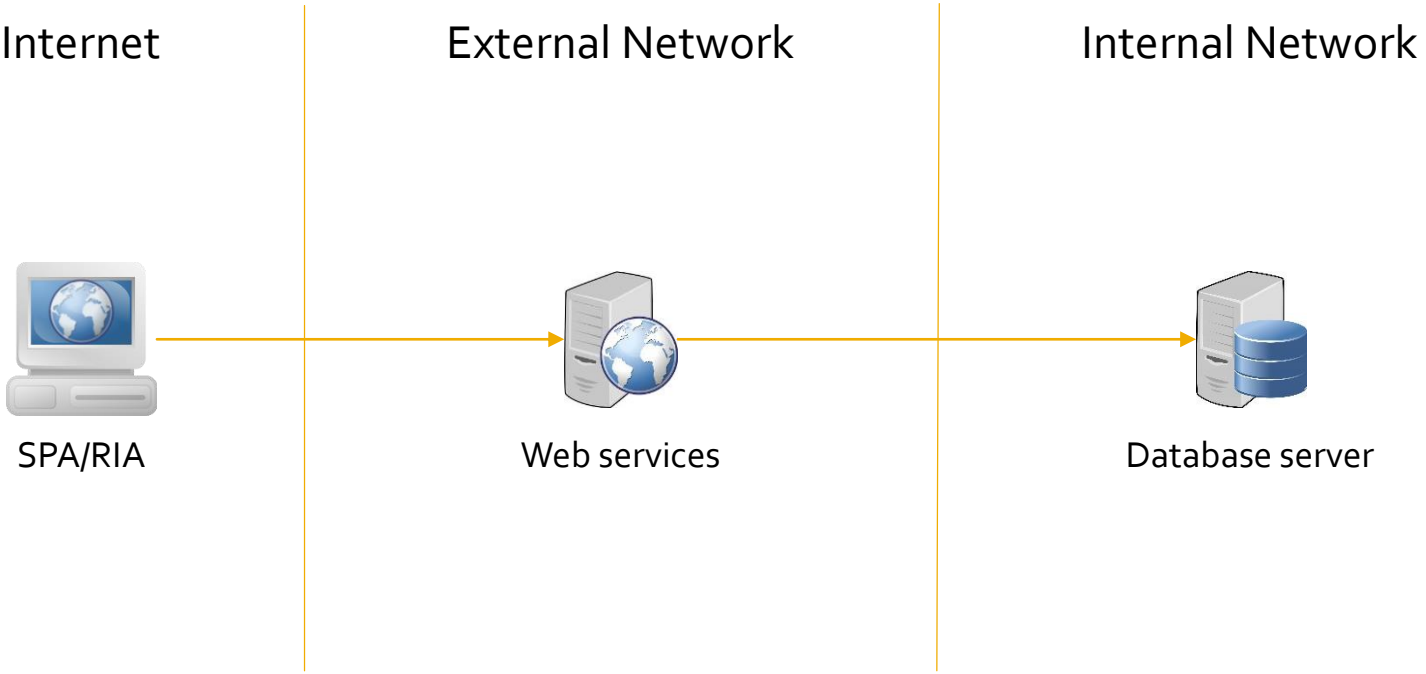
Access control solution

- Scenario with a web portal (including SSO)



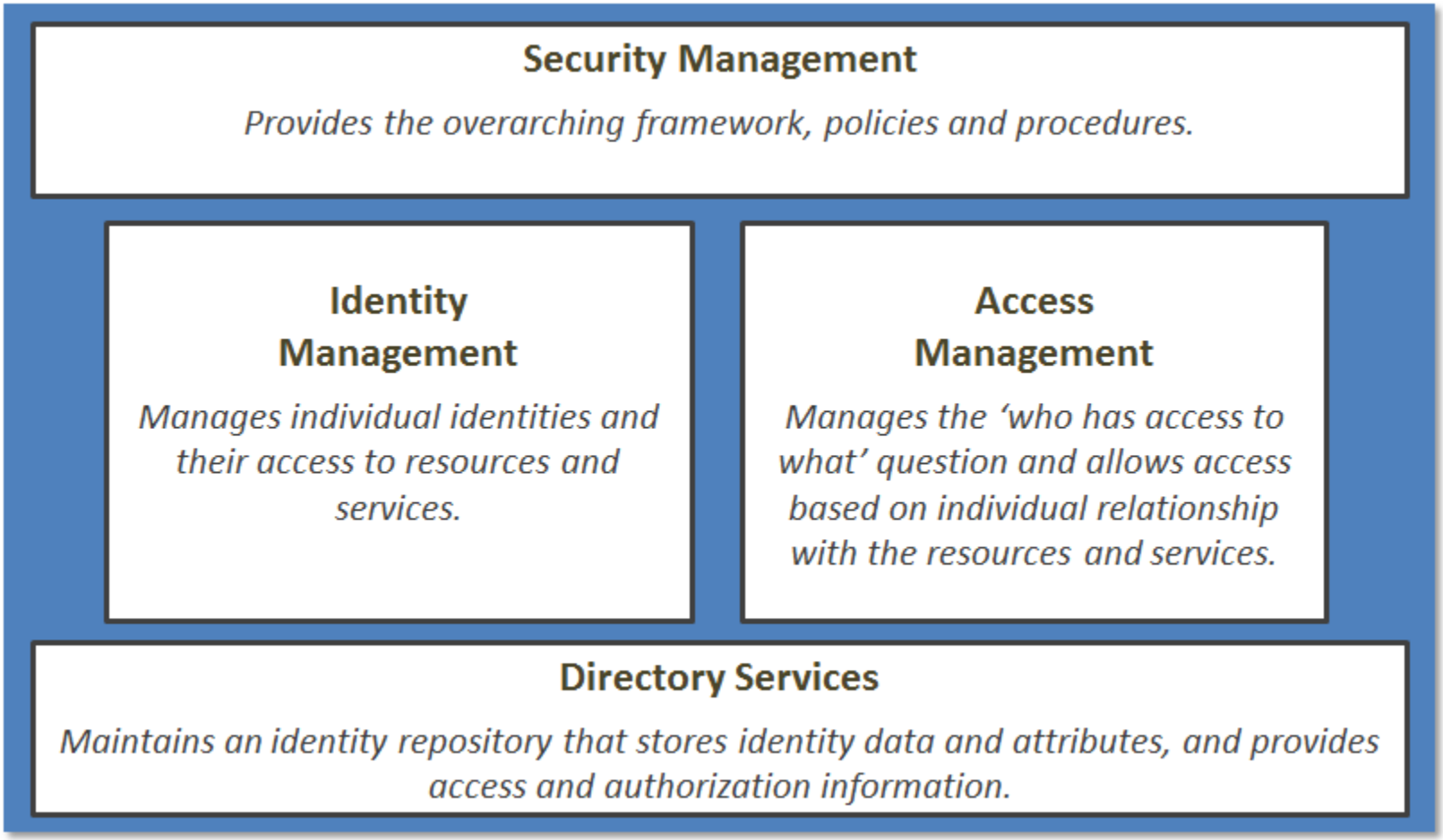
Access control solution

- Simple scenario with a SPA/RIA



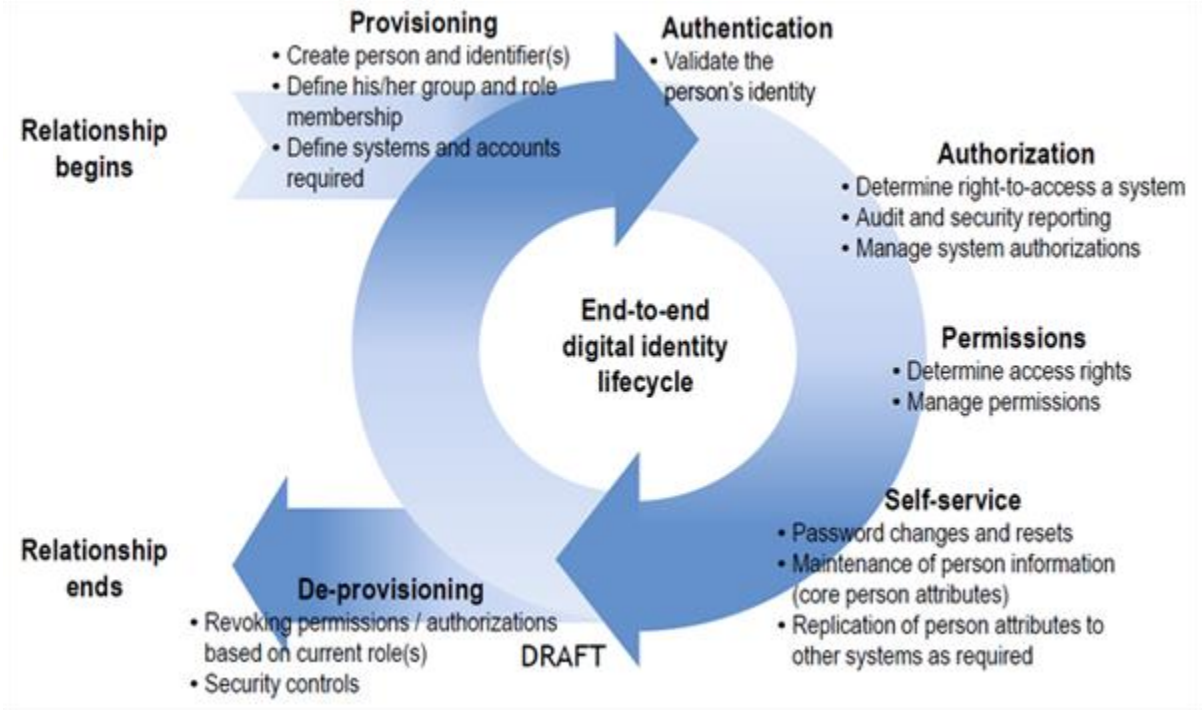
Q: What if client needs to support offline mode?

As a process



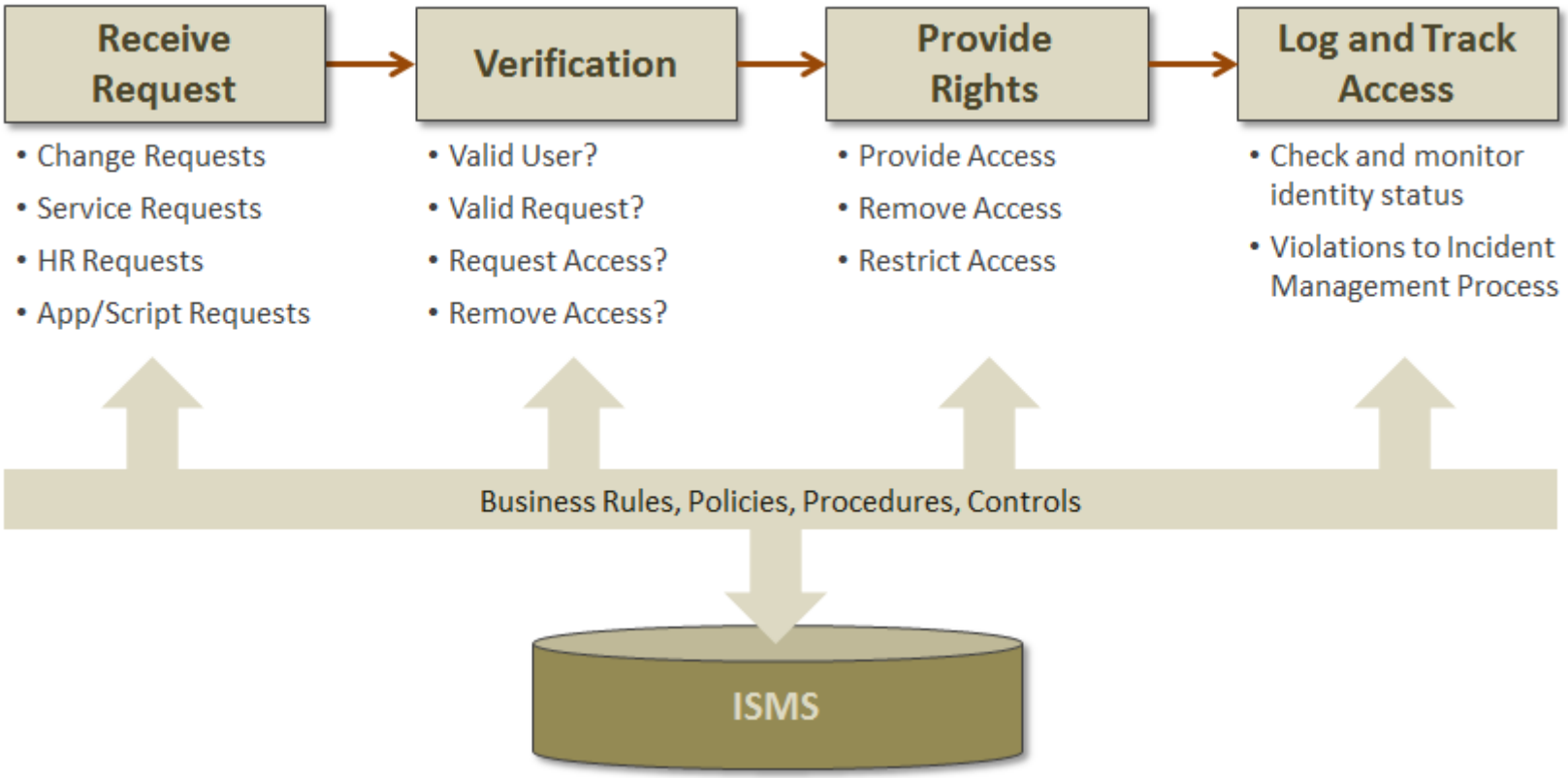
https://www.interfacett.com/blogs/access-management-control-it-just-tools/

As a process



https://it.ubc.ca/what-identity-and-access-management

As a process



https://www.interfacett.com/blogs/access-management-control-it-just-tools/