

Logical Access Controls



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



Access Controls Concepts for the CC® Certification

Agenda:

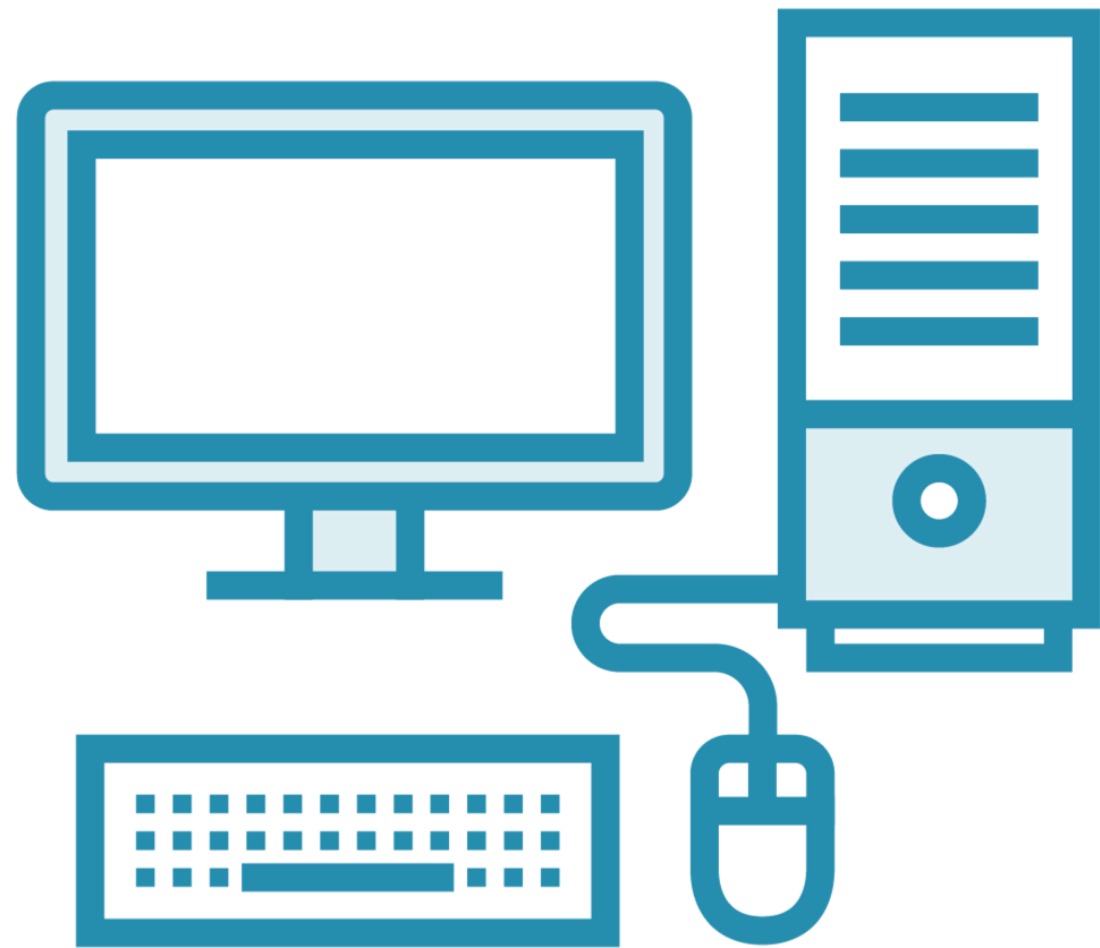
**Access Controls
Concepts**

**Physical Access
Controls**

**Logical Access
Controls**



Logical/Technical Access Controls



Access Controls implemented using technology into systems, networks and applications

- Passwords
- Network Access Controls
- Wireless
- Firewalls

Logical Access Theory



Discretionary Access Control



Most common form of access control



Access permissions are set by the owner



Access rights can be delegated



Mandatory Access Control



High security systems

- Expensive
- Requires labels and separation of duties

Access permissions are mandated by policy

- Access is only granted if the owner and the policy agree
- Access cannot be delegated

Common Methods of Access Control

Rule-based access control

**RBAC – Role-based
access control**

**ABAC – Attribute-based
access control**

Temporal access control



Role-based Access Controls (RBAC)

Based on the user's job position

**Cost-effect way to implement
need-to-know**

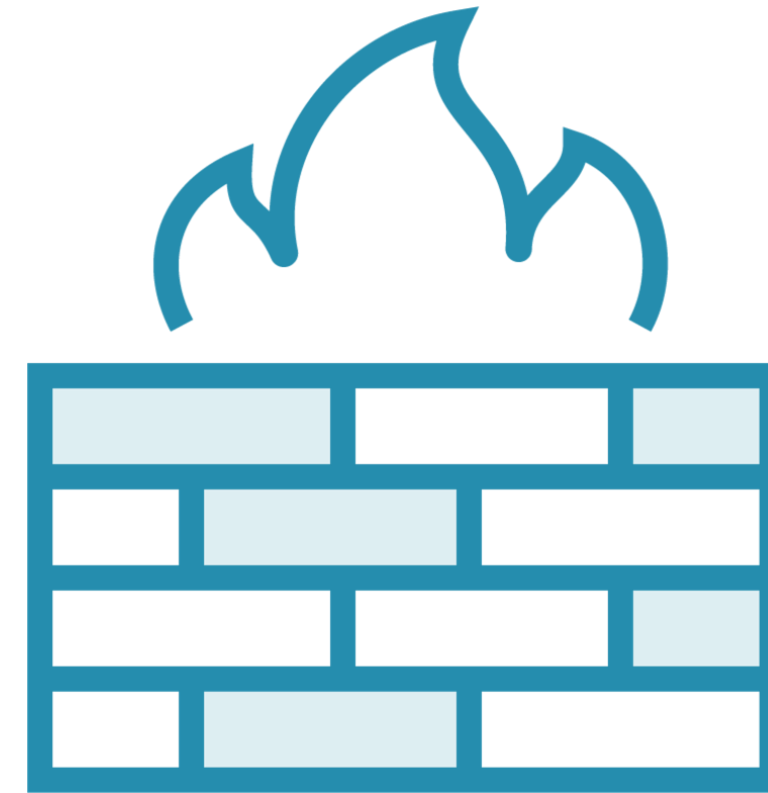
**Easy to enforce through large enterprises
with multiple business units**



Rule-based Access Control



Based on list of rules



Firewall rule sets is good example



Attribute-based Access Control

Evaluation and access granted based on attributes

Flexibility

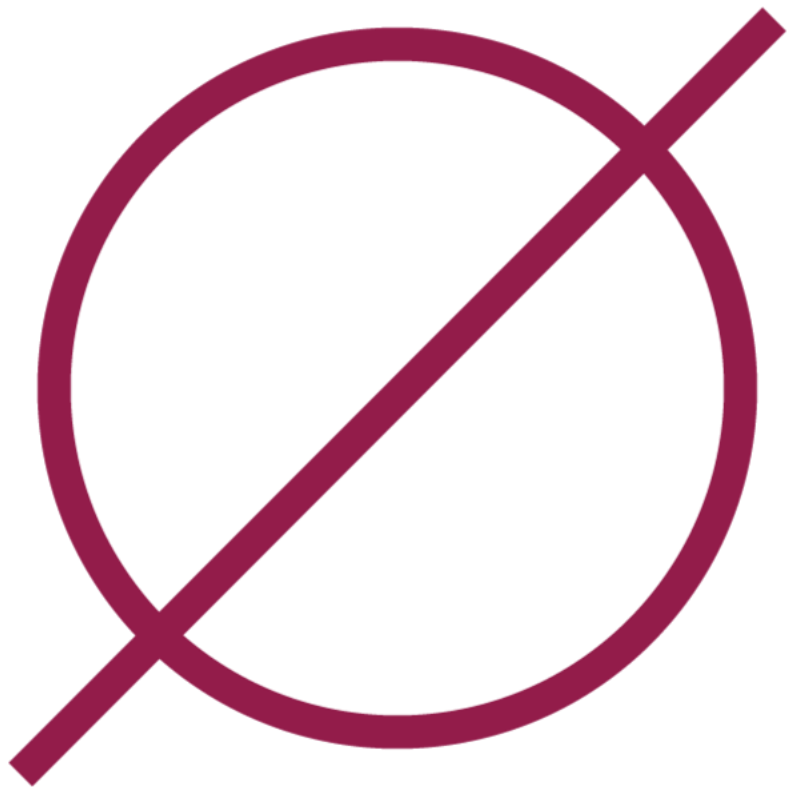
Decisions based on

- Subject attributes
- Objects attributes
- Environmental conditions
- Formal relationship or access control rule

Zero Trust and Single Sign-on



Zero Trust



Each part of a systems must be secure in itself — not trust on security from another part

- External connections



Implementing Zero Trust

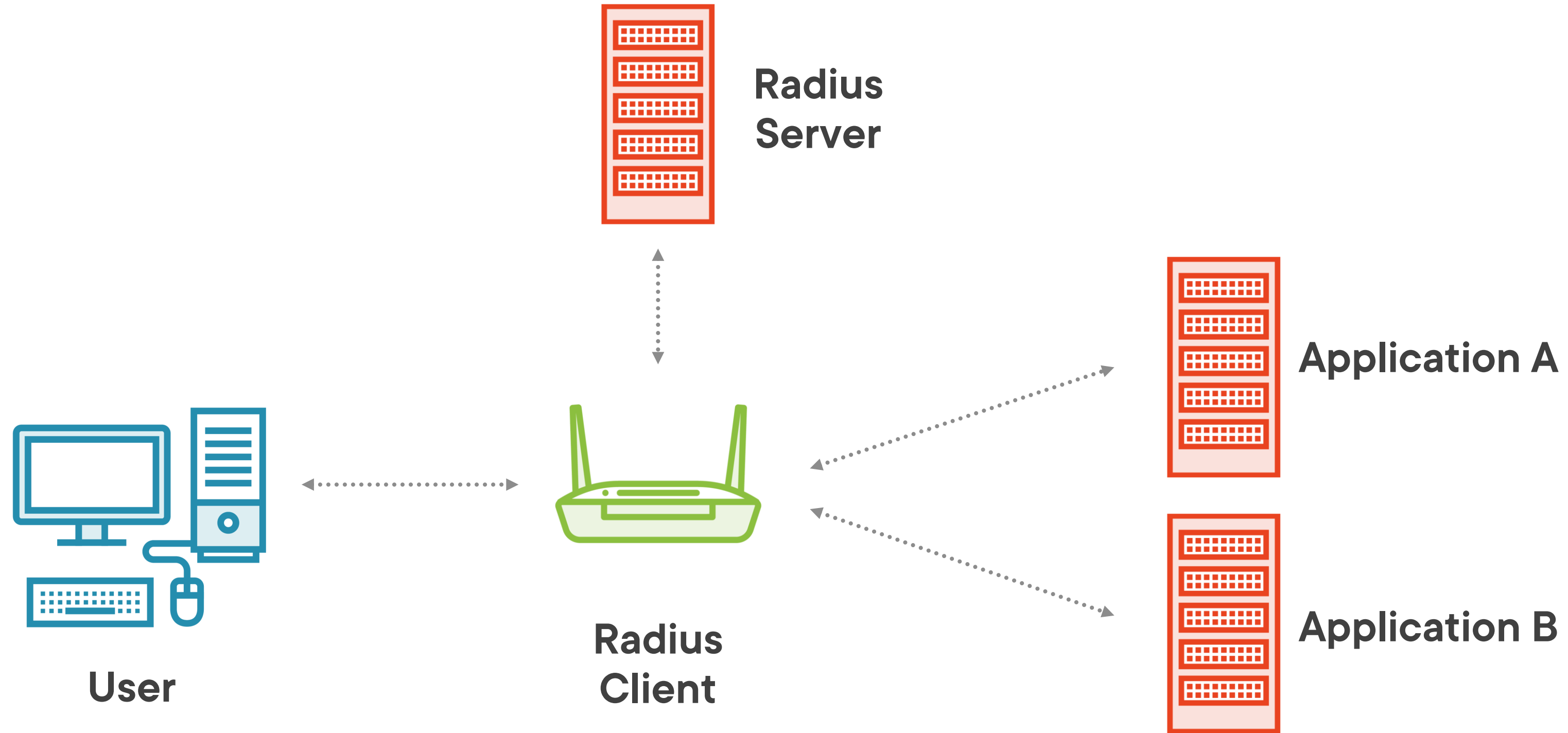
**End-point
device validation**

**Multi-factor
authentication**

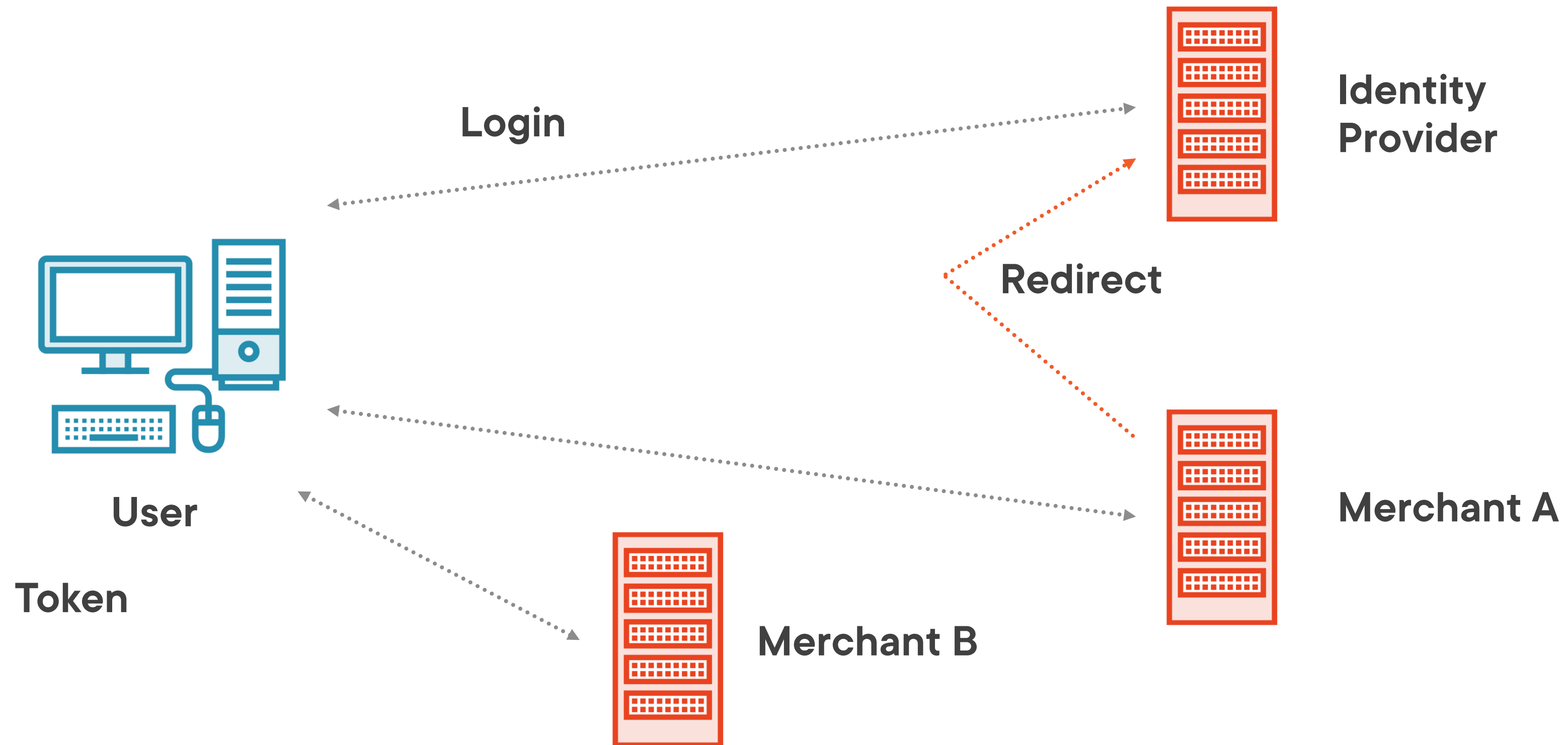
**Network
segmentation**



SSO Implementations



Federated Identity Management



Directory Services

**Lightweight
Directory Access
Protocol (LDAP)**

**Network Information
Services (NIS)**

**Domain Name
System (DNS)**

X.400

X.500

Active Directory



Key Points Review



Discretionary Access Control allows owners and users to grant access to other users.

Mandatory Access Control does not permit users to grant access to other users.

Role-based Access Control works well in an environment with many users needing similar permissions.

