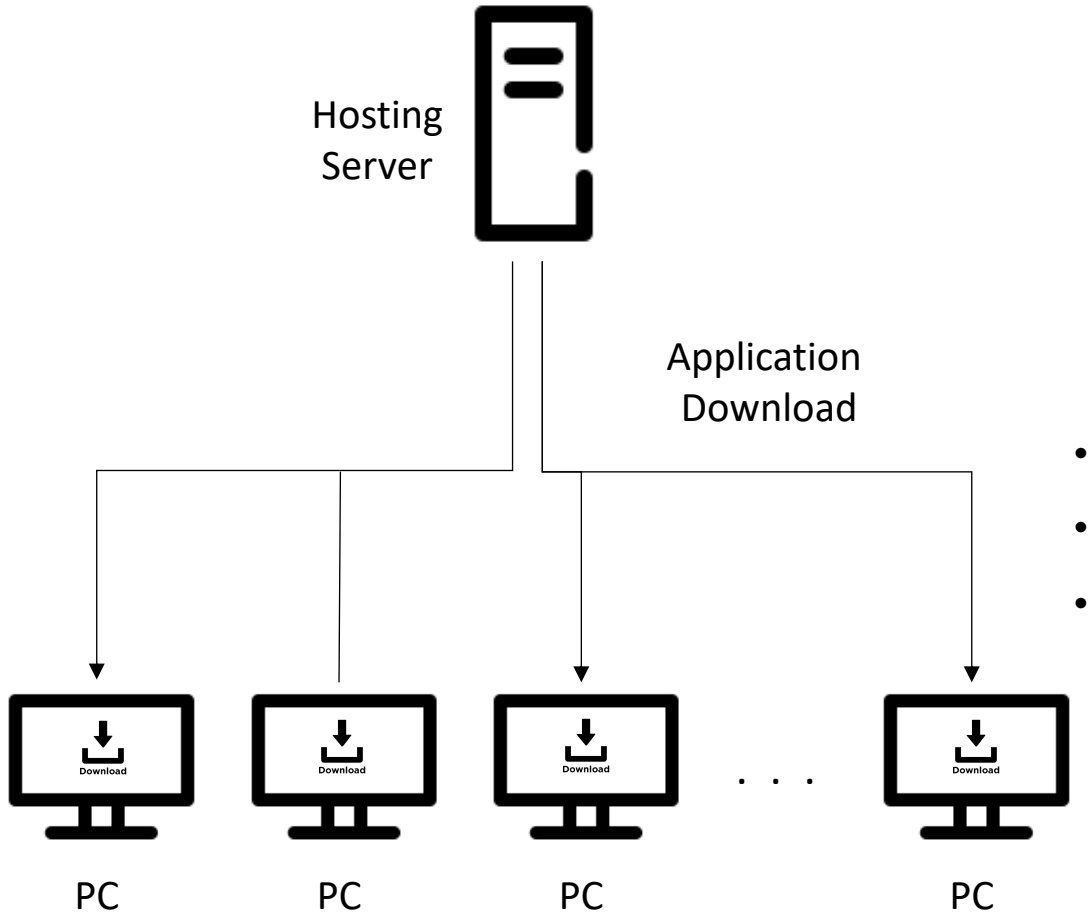

# Week 13: Securing Kubernetes, SASE, and Other Current Topics

# How Are Modern Microsegmented Cloud Apps Really Secured?

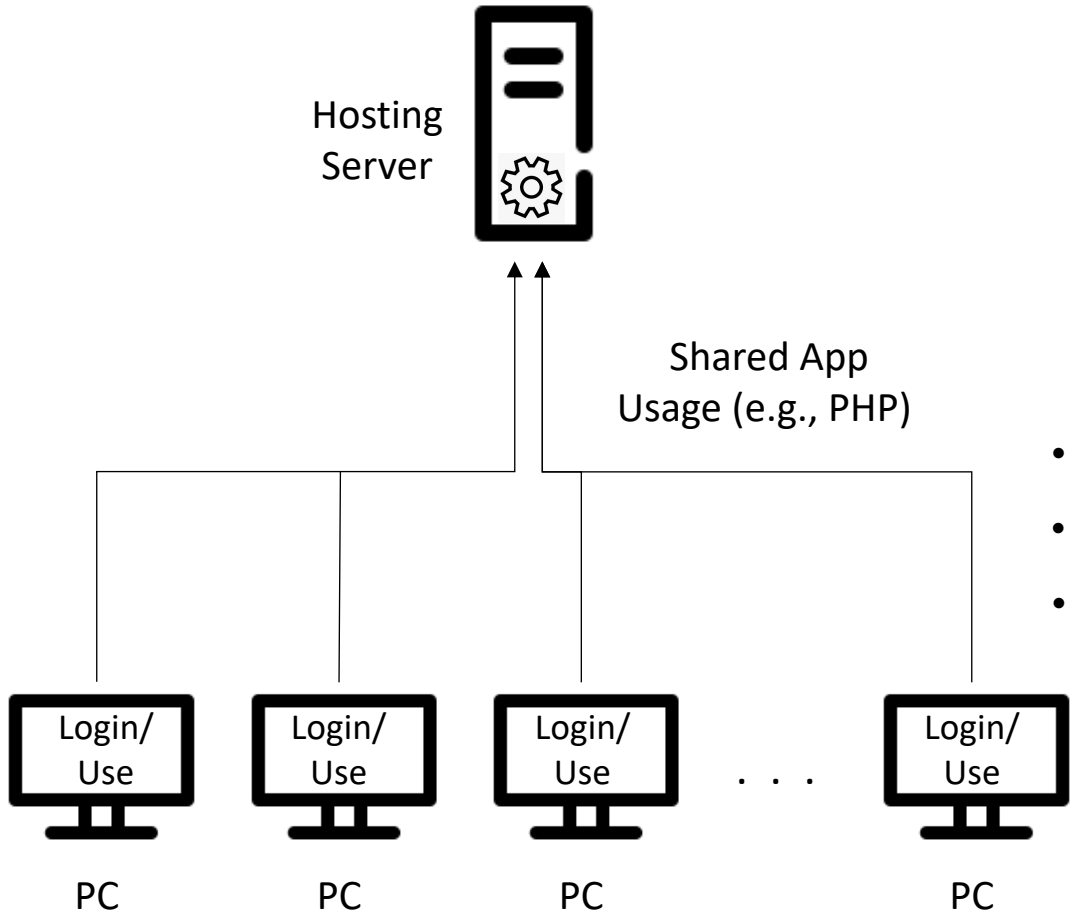
Week 13




- Distributed execution on PCs
- No runtime collision on PCs
- Distributed maintenance issue

# Traditional App Download Process – One Server to Many PCs

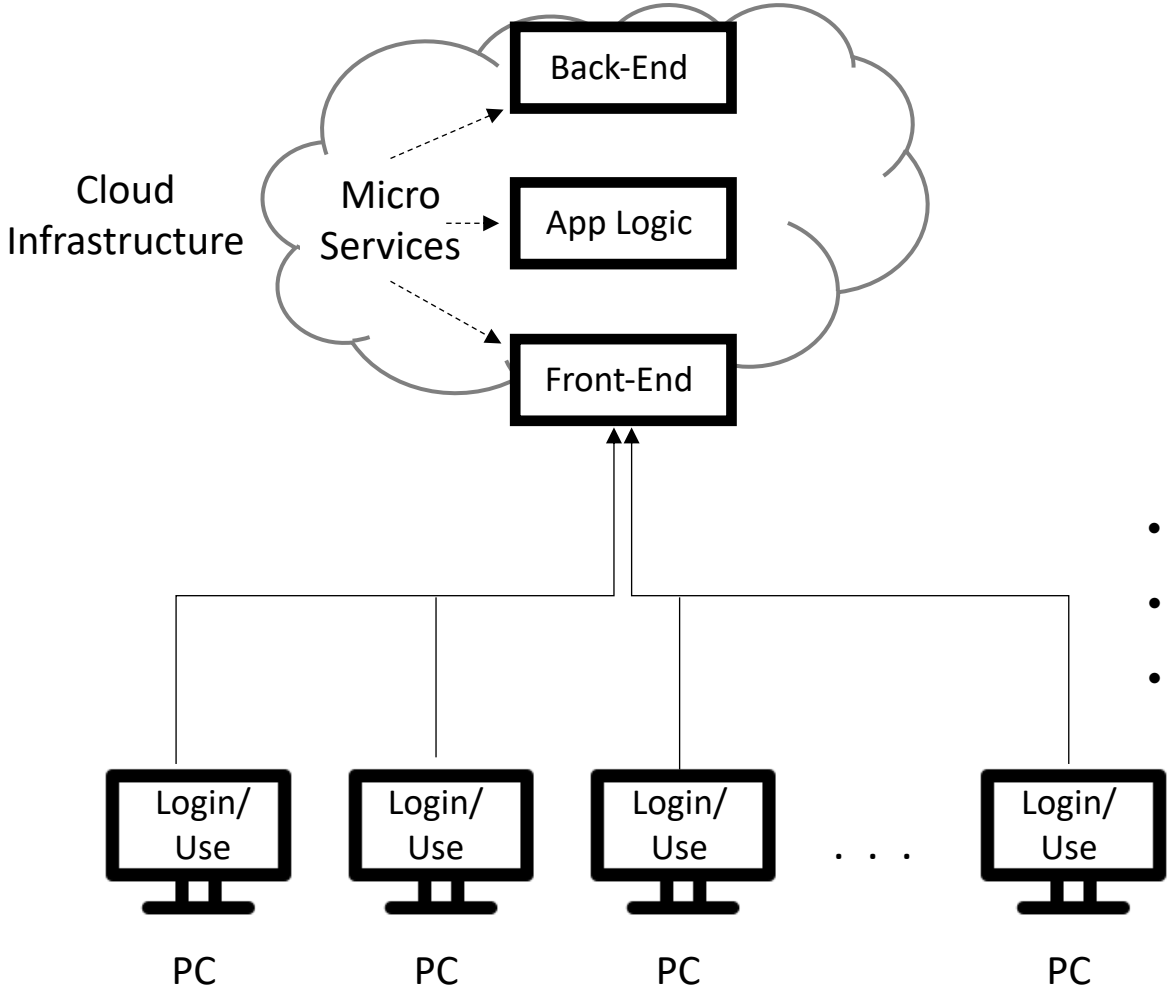
Week 13




- Centralized execution in hosting
- Runtime collision in hosting
- Centralized maintenance in hosting

# Initial App Sharing Process – One Shared App to Many PCs

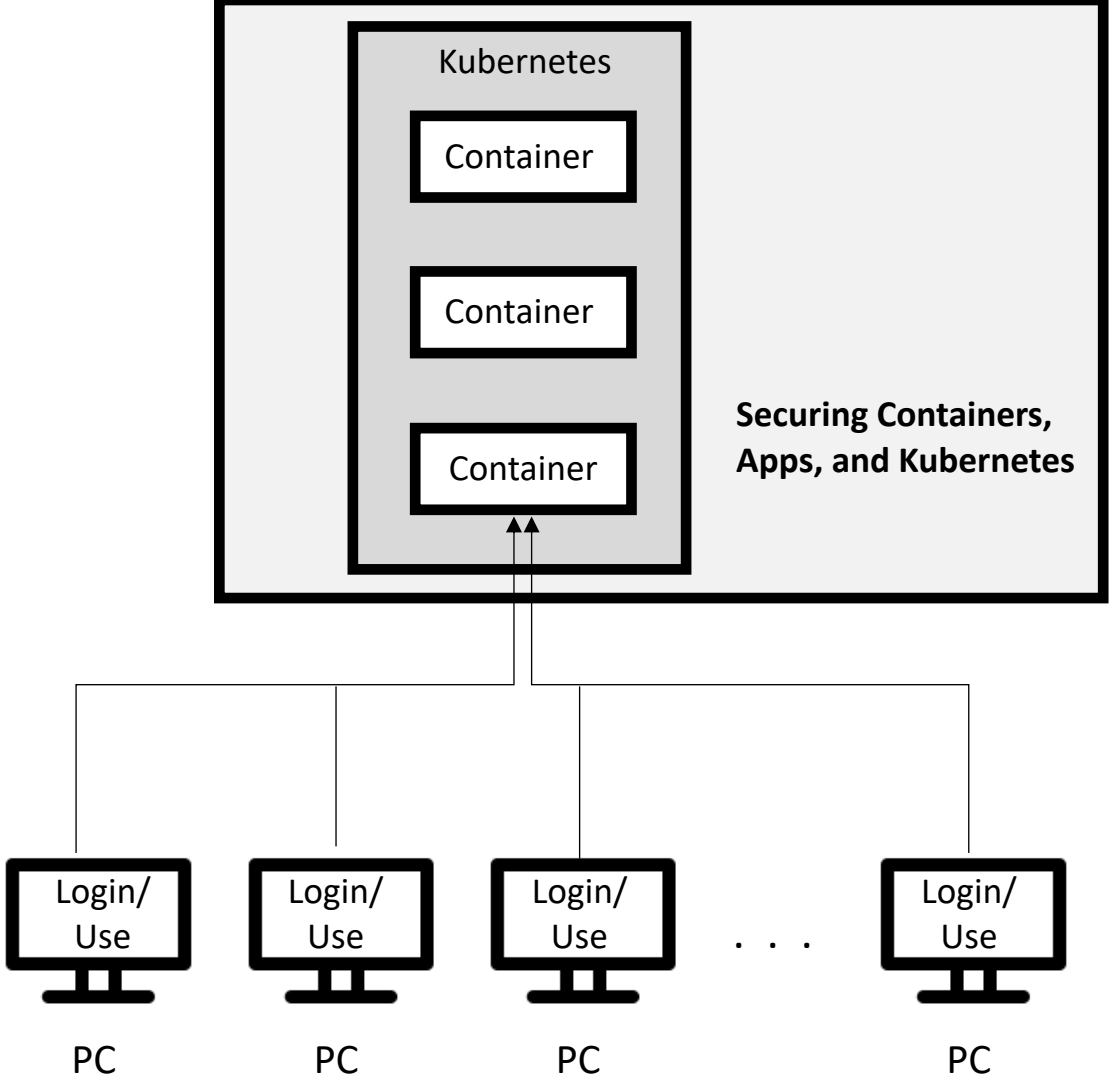
Week 13




- Distributed execution in cloud
- Front/back-ends lessen collision
- Microservices need orchestration

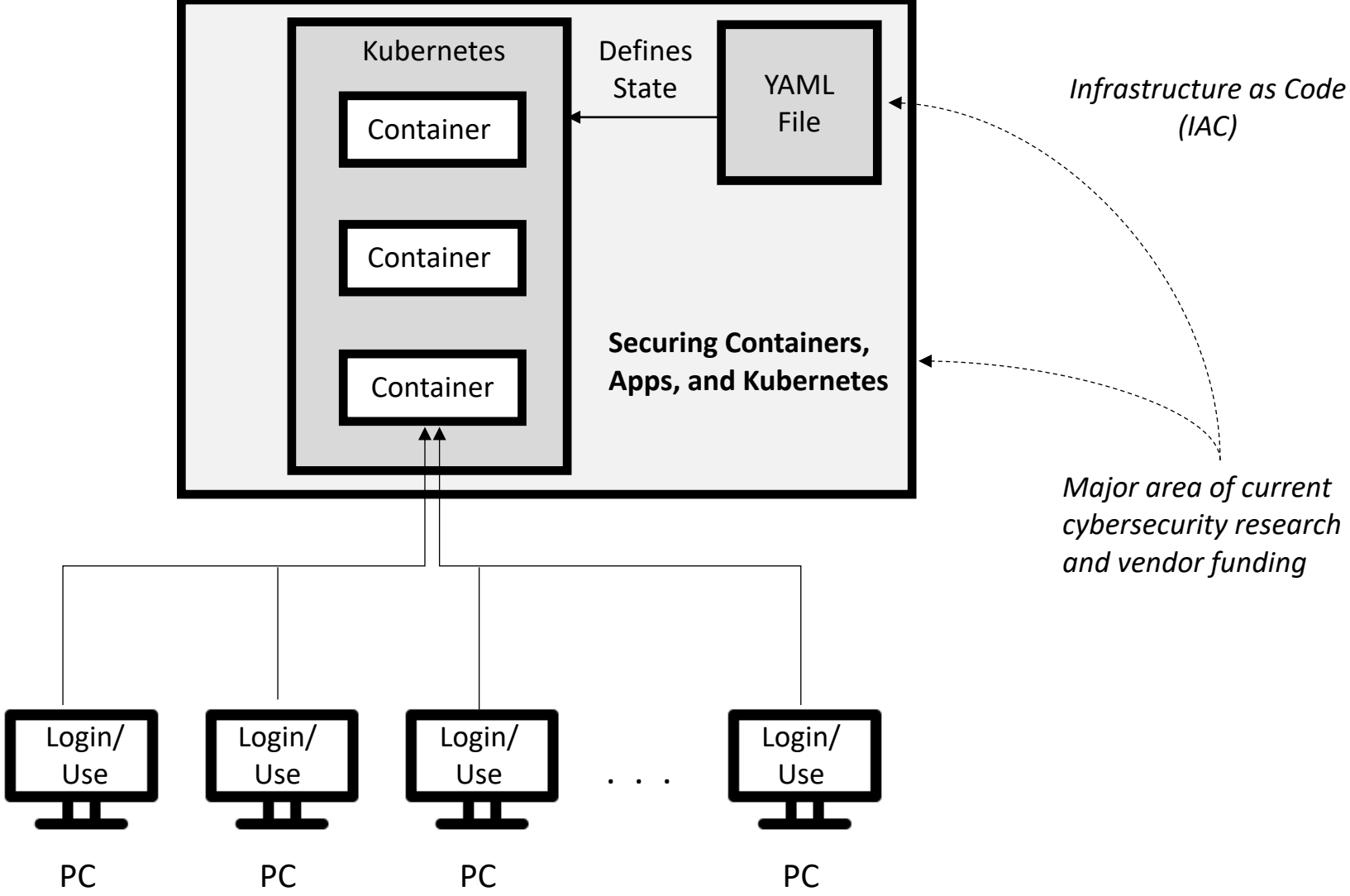
# Microservices Design Process – Distributed Workloads

Week 13




# Kubernetes Orchestration

Week 13




# Kubernetes Orchestration and YAML State Design

Week 13

# Risky image prevention via admission control

Block unscanned or vulnerable images from being deployed onto the cluster with the Sysdig Admission Controller. Define criteria based on flexible conditions (i.e., namespace, CVE severity level, fix availability, image size, etc.) in order for the image to be approved.

Sysdig Secure also prevents vulnerabilities early by integrating image scanning into the CI/CD pipelines and registries.


# Typical Commercial Solution – Software Image Scanning

Week 13


The Illustrated Children's Guide to Kubernetes

498,997 views • Jun 9, 2016

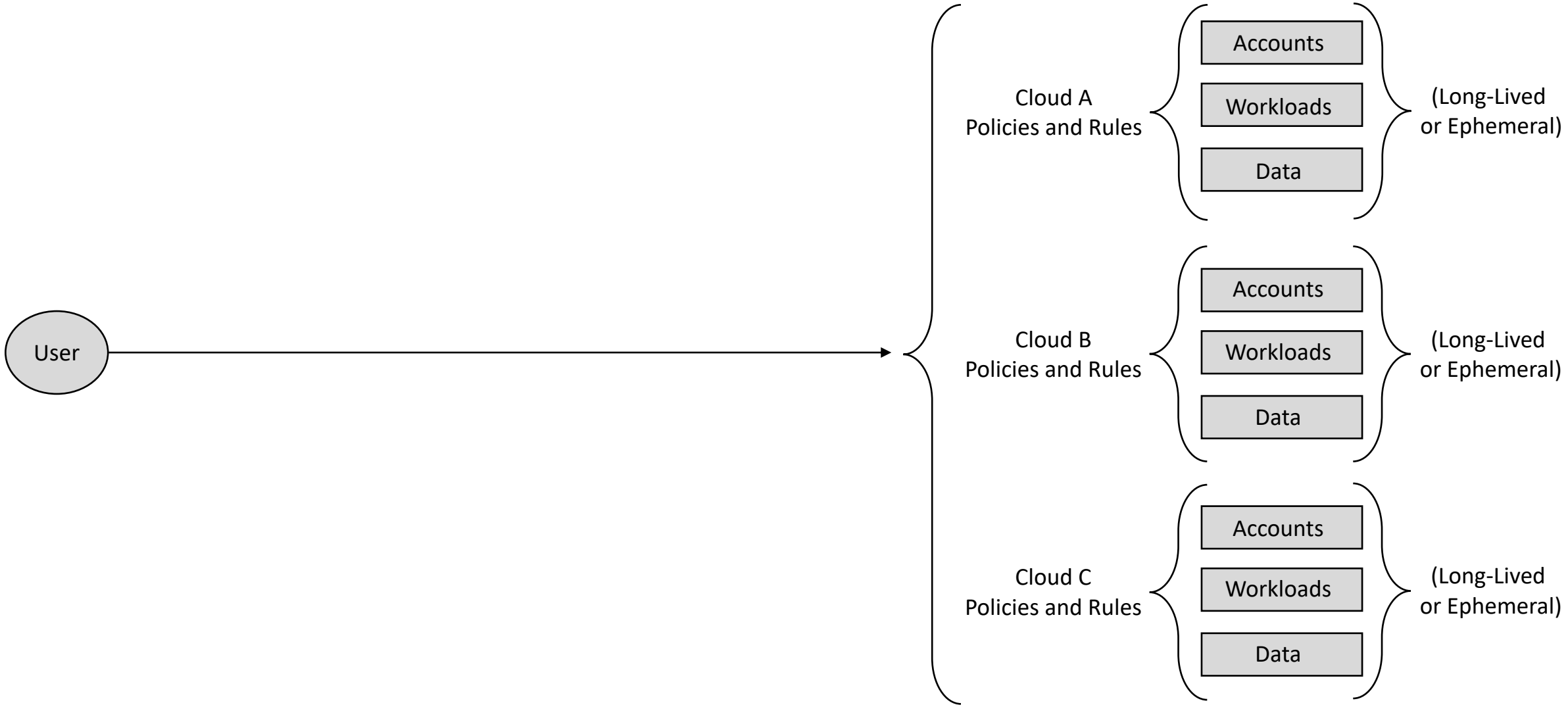
12K 148 SHARE SAVE

# Awesome YouTube Video on Apps, Containers, and Kubernetes

# How are Multi-Cloud Entitlements Managed?

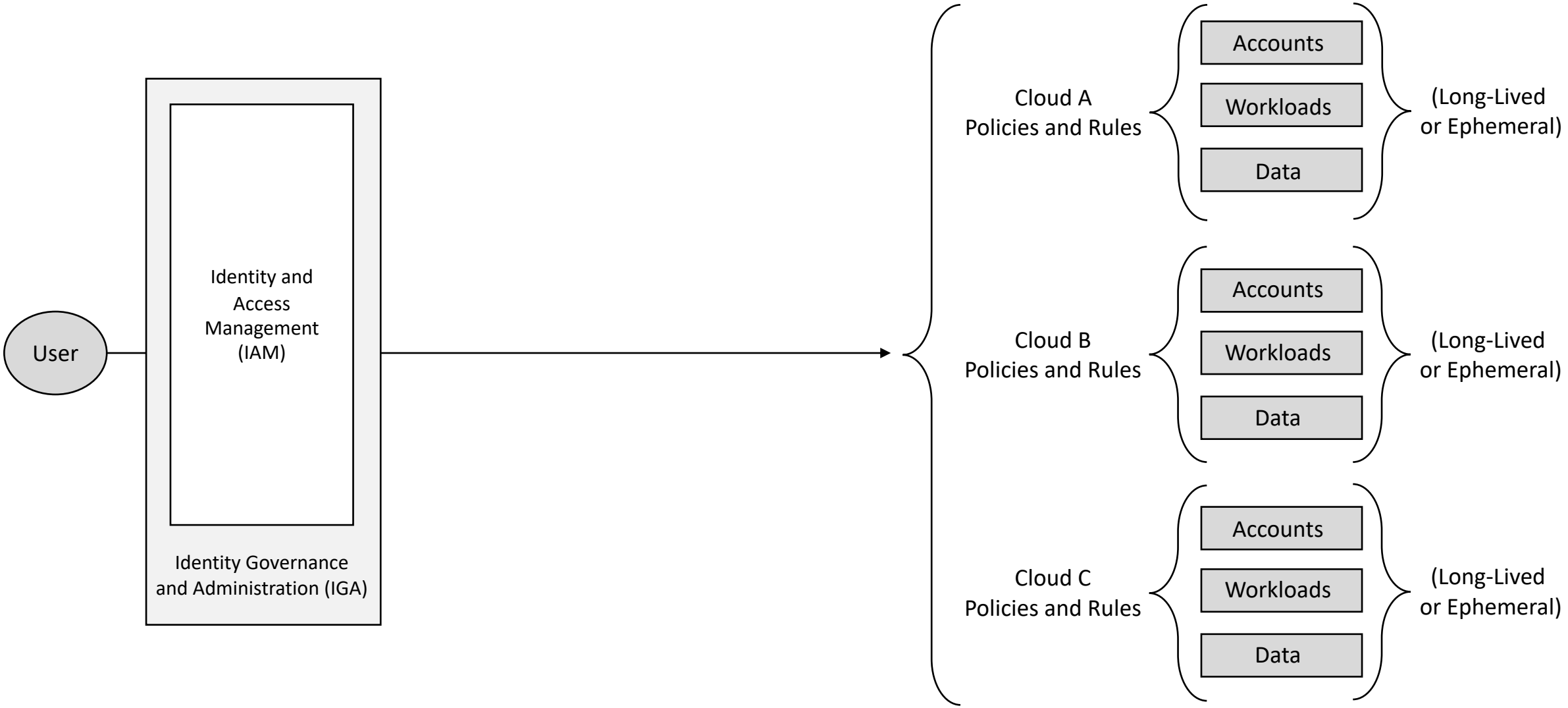
Week 13

# What is Cloud Infrastructure Entitlement Management (CIEM)?



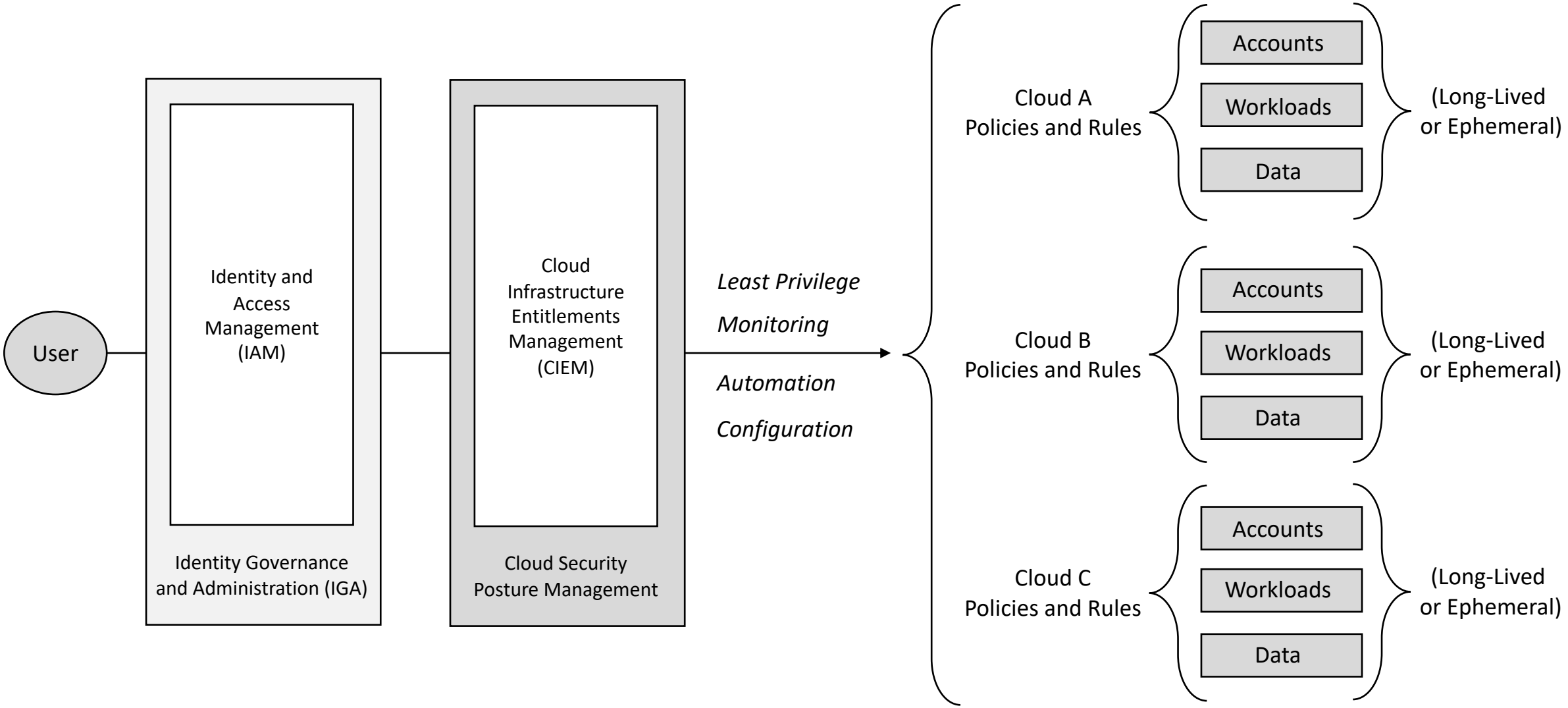
Week 13

# What is Cloud Infrastructure Entitlement Management (CIEM)?



Week 13

# What is Cloud Infrastructure Entitlement Management (CIEM)?



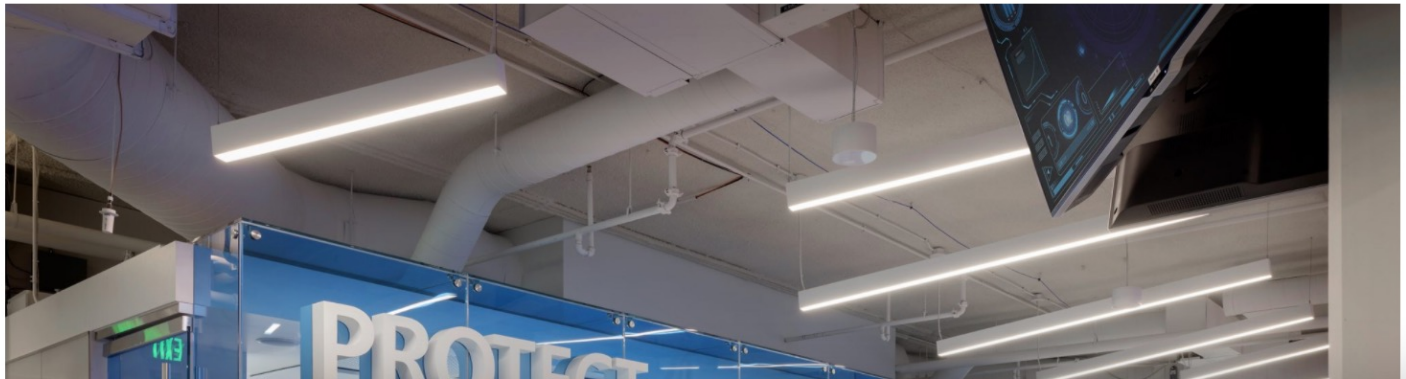
Week 13

# Microsoft acquires CloudKnox Security to offer unified privileged access and cloud entitlement management

Jul 21, 2021 | Joy Chik - Corporate Vice President, Microsoft Identity

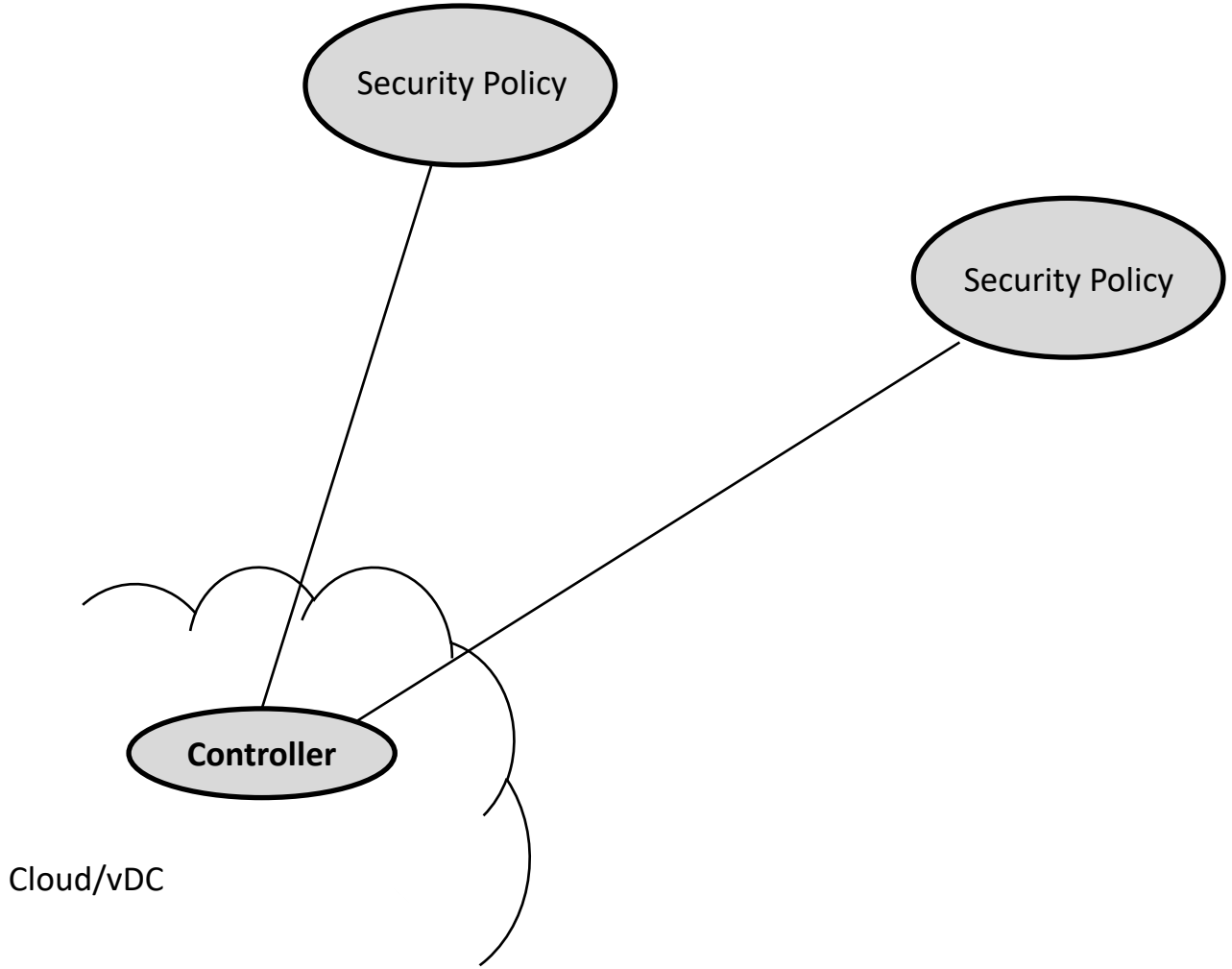
*Helping organizations strengthen cloud security and Zero Trust*

At Microsoft, we are committed to supporting organizations in their digital transformation and helping them to deliver secure and seamless experiences. Since IT modernization often spans multiple clouds, cloud security and identity are top of mind for most of our customers. Modern identity security needs to protect all users and resources consistently across multi-cloud and hybrid cloud environments. Today, Microsoft is taking a significant step toward this goal with the acquisition of CloudKnox Security, a leader in Cloud Infrastructure Entitlement Management (CIEM). CloudKnox offers complete visibility into privileged access. It helps organizations right-size permissions and consistently enforce least-privilege principles to reduce risk, and it employs continuous analytics to help prevent security breaches and ensure compliance. This strengthens our comprehensive approach to cloud security.



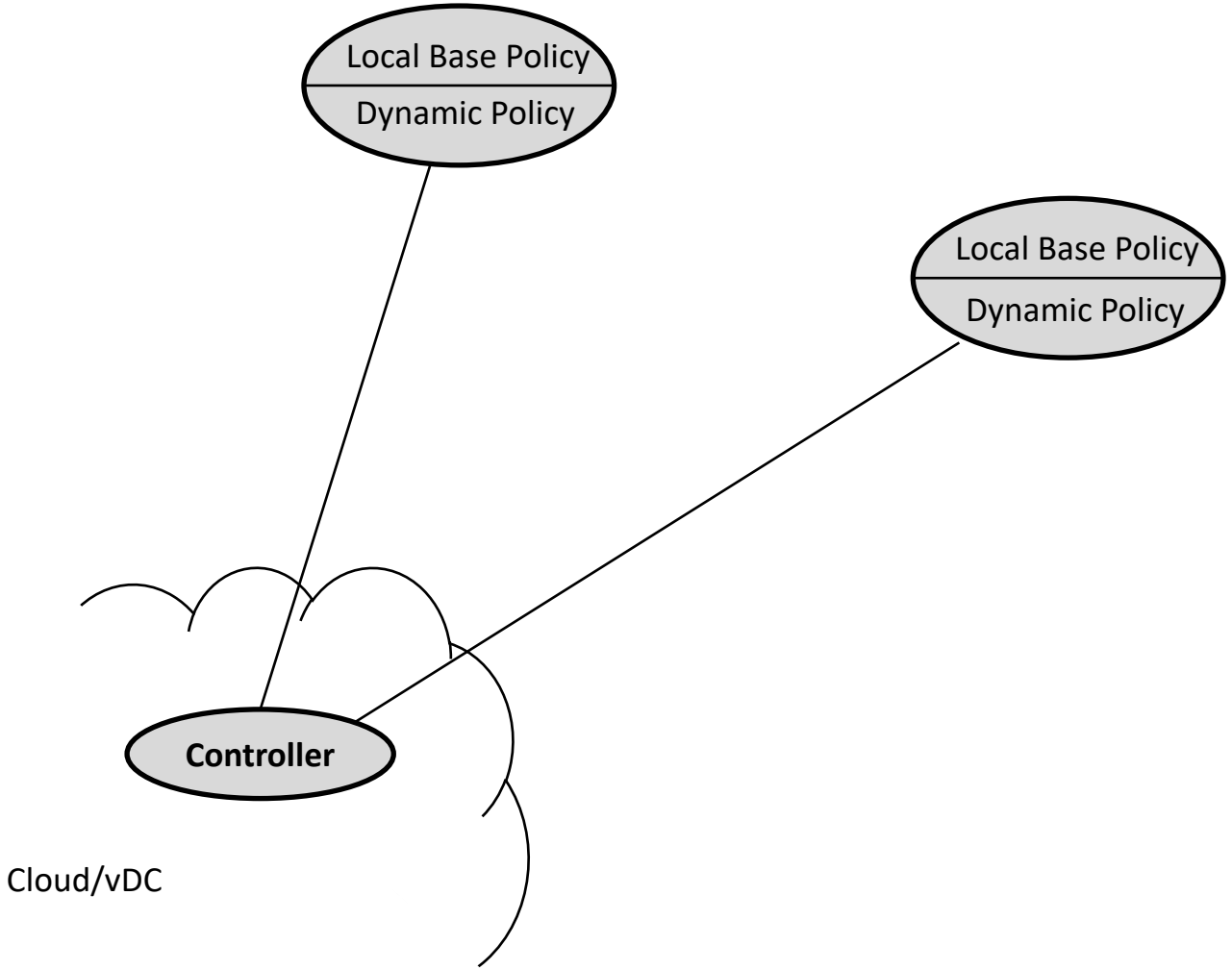
# How is Multi-Cloud Security Policy Orchestrated?

Week 13



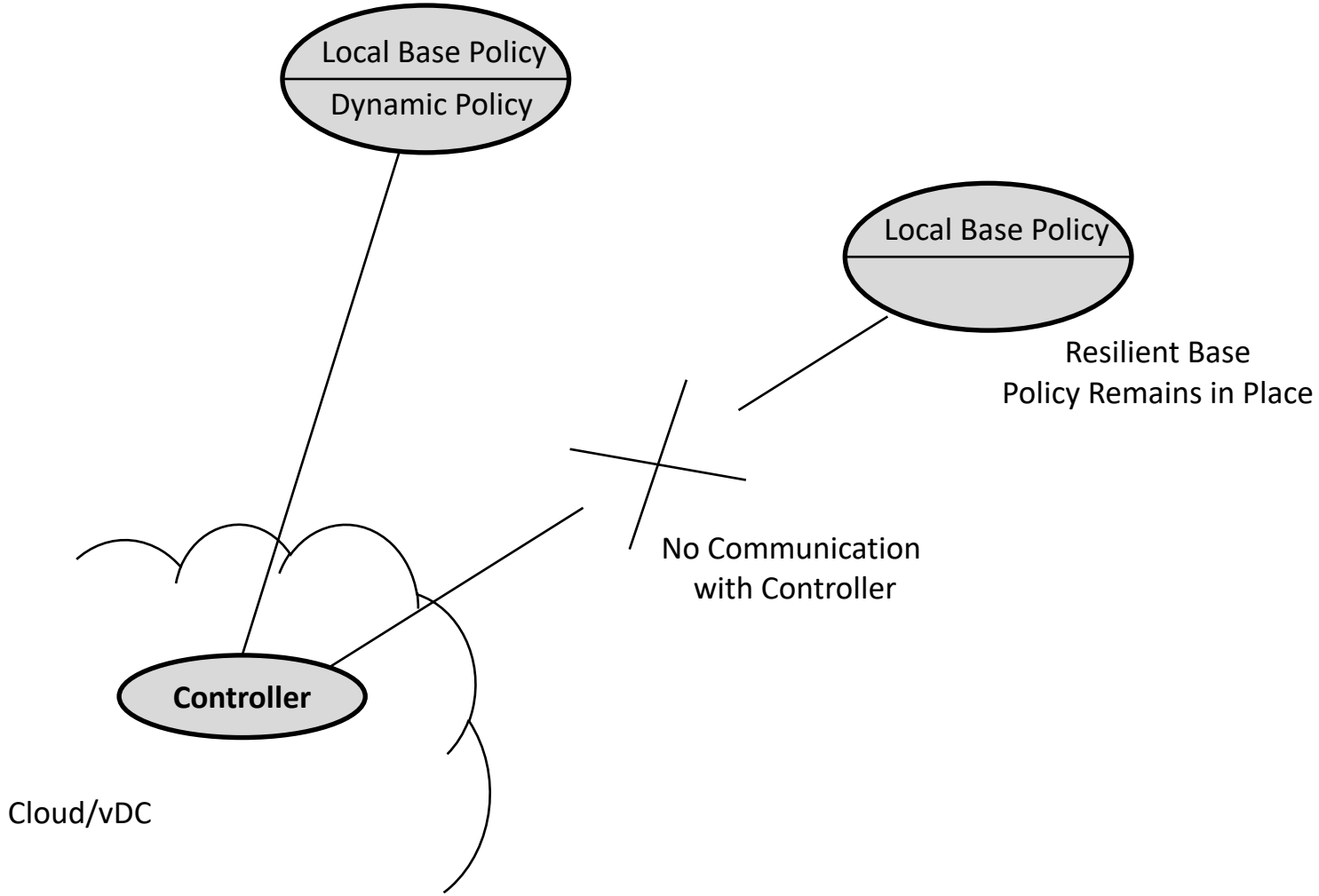

# Controller is SPOF for Security Policy Management

Week 13



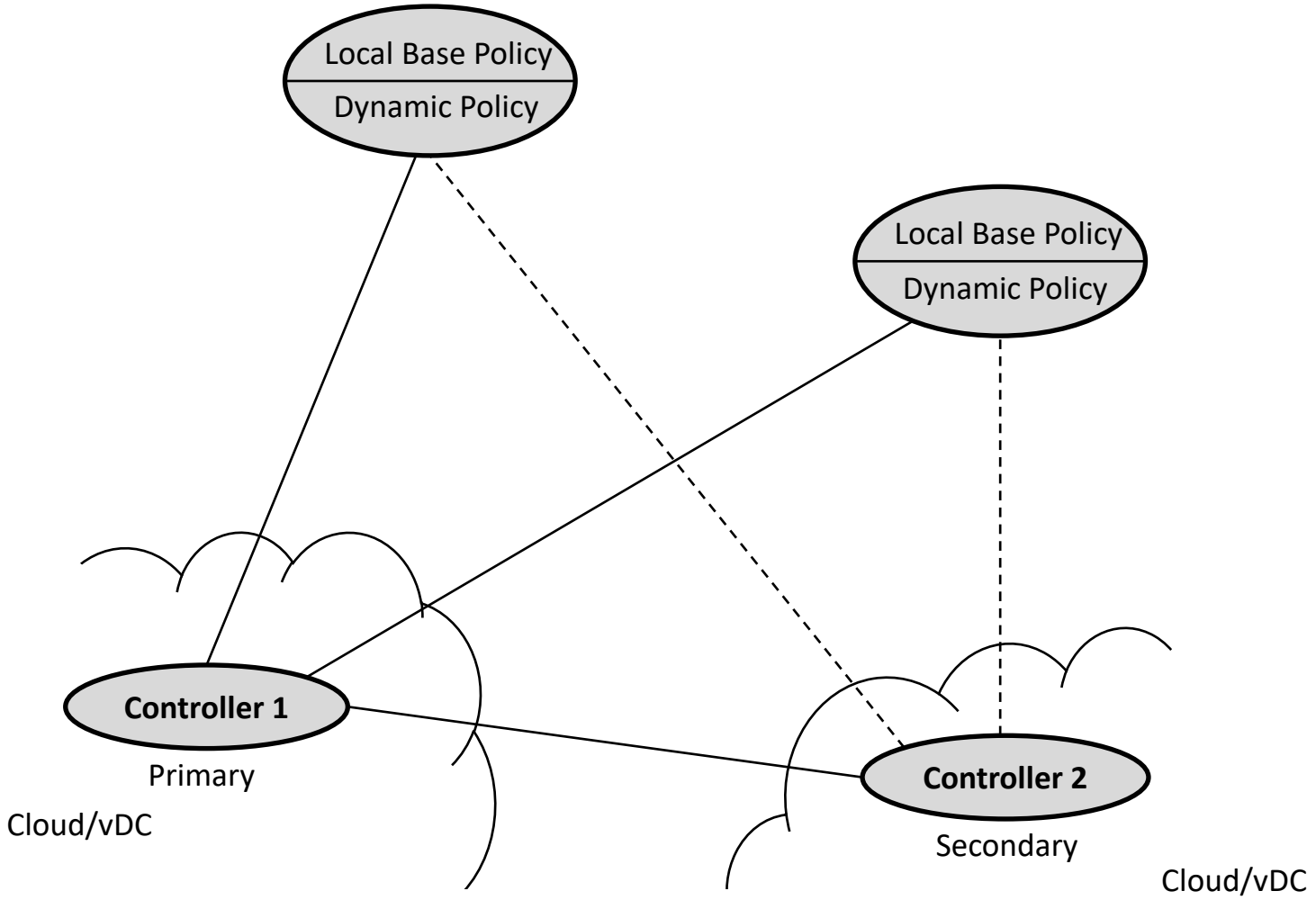

# Typical Solution: Locally Stored Policy Back-Up Strategy

Week 13



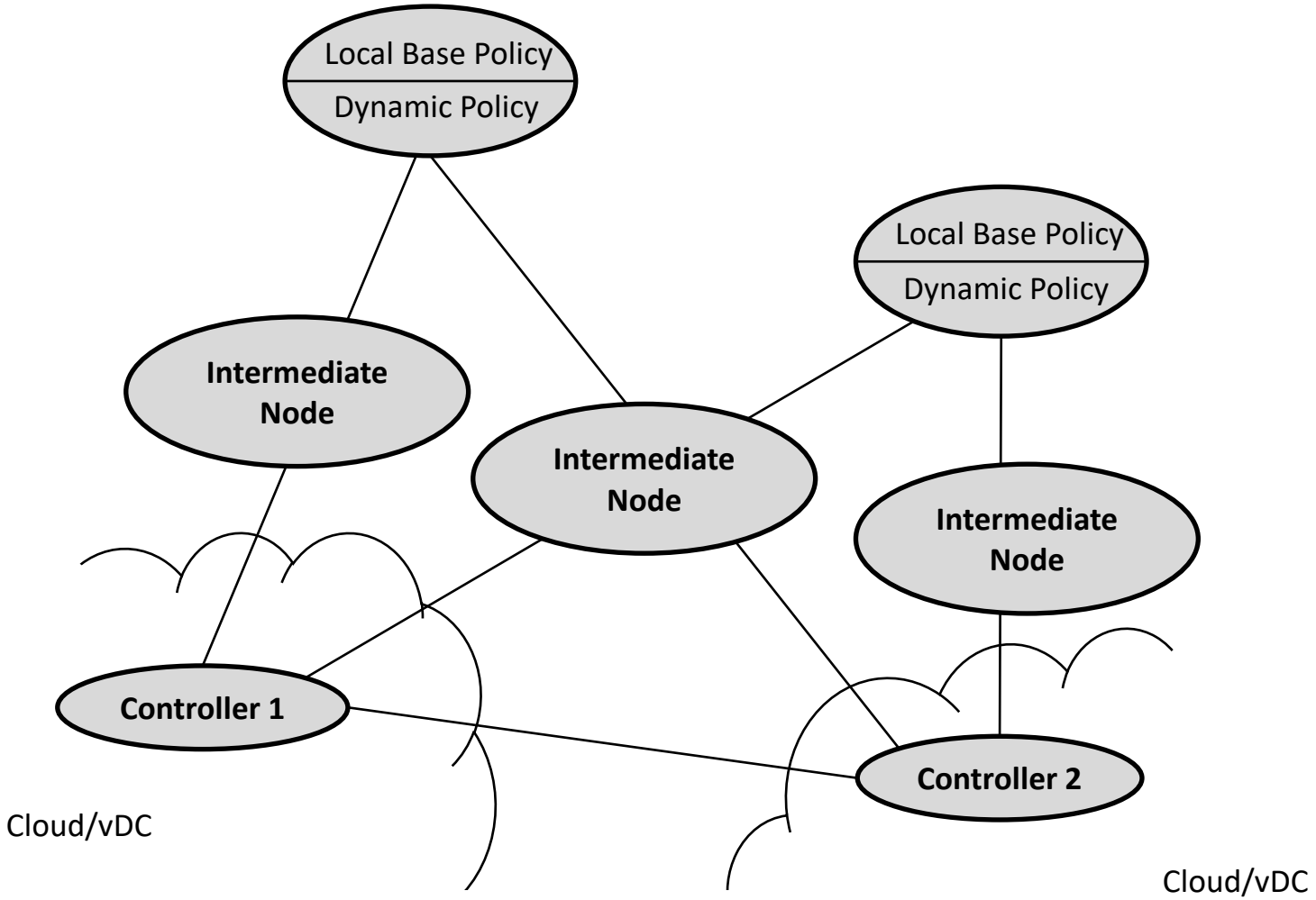

# Local Back-Up Policy Used in Presence of Failure

Week 13



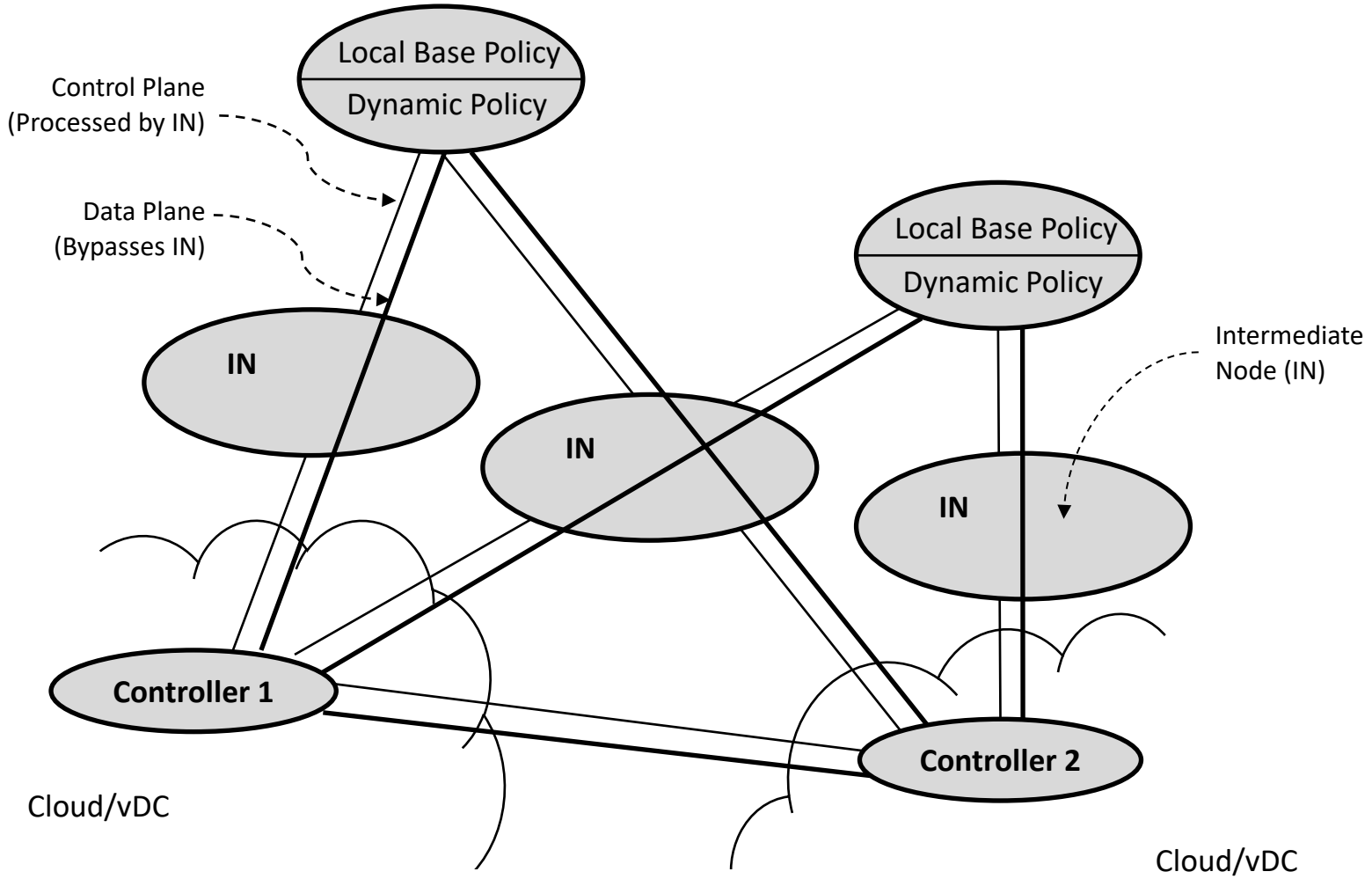

# Primary-Secondary Architectural SPOF Removal

Week 13



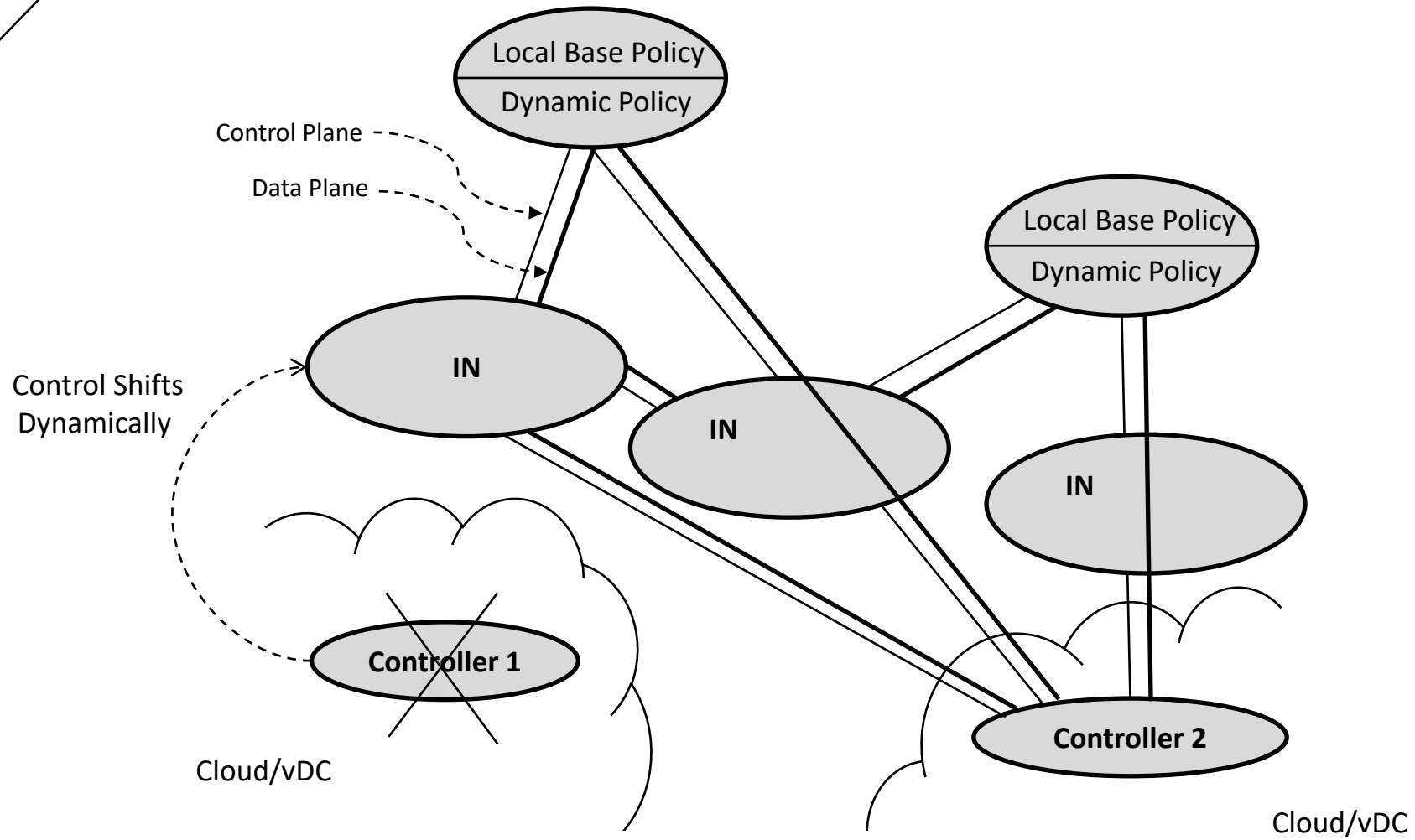

# Adding Intermediate Notes to Improve Resilience

Week 13



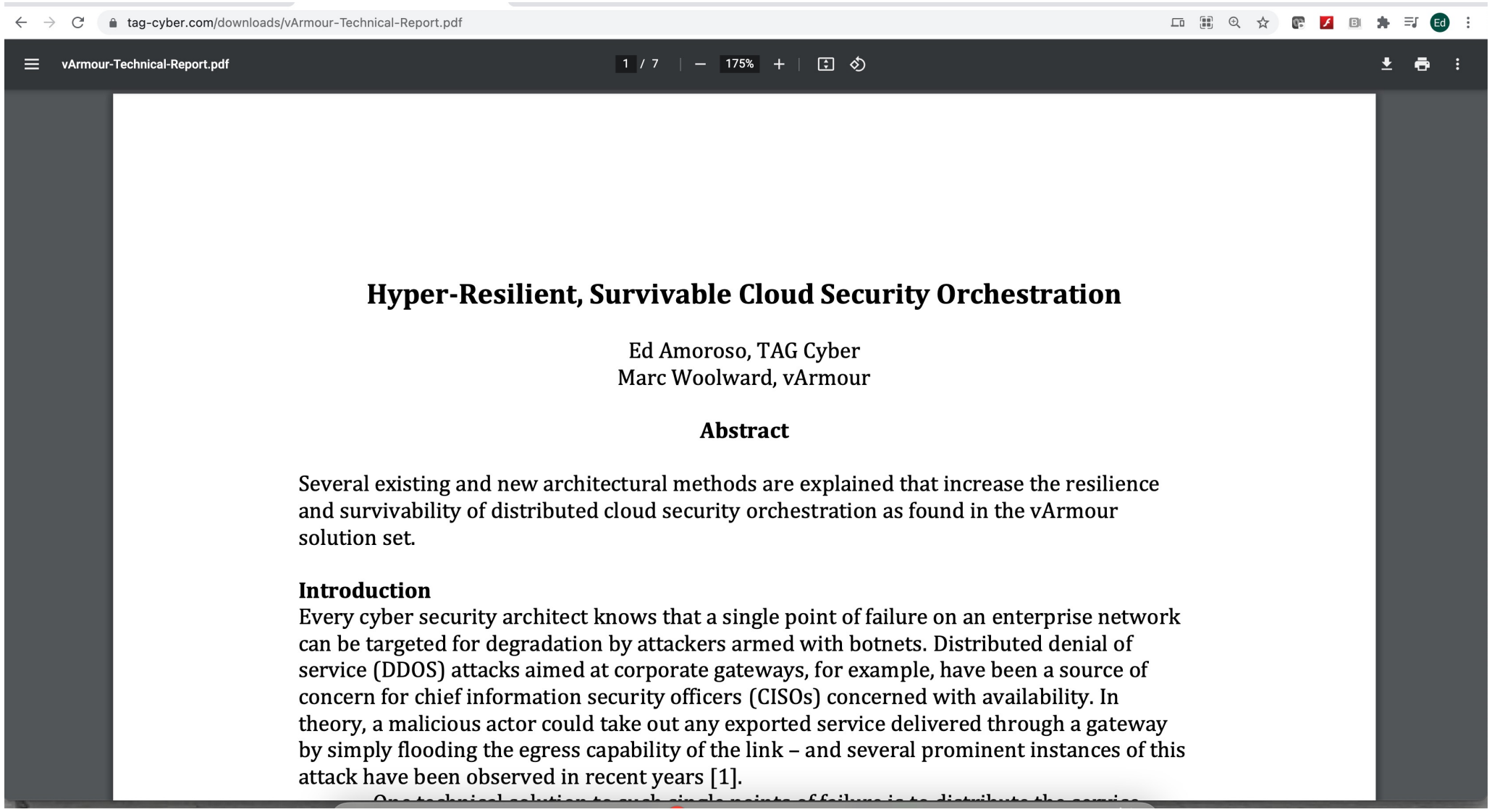

# Separating Data and Control Planes to Improve Resilience

Week 13




# Shifting Intermediate Nodal Support on Failure

Week 13




# Hyper-Resilient, Survivable Cloud Security Orchestration

Ed Amoroso, TAG Cyber
Marc Woolward, vArmour

## Abstract

Several existing and new architectural methods are explained that increase the resilience and survivability of distributed cloud security orchestration as found in the vArmour solution set.

## Introduction

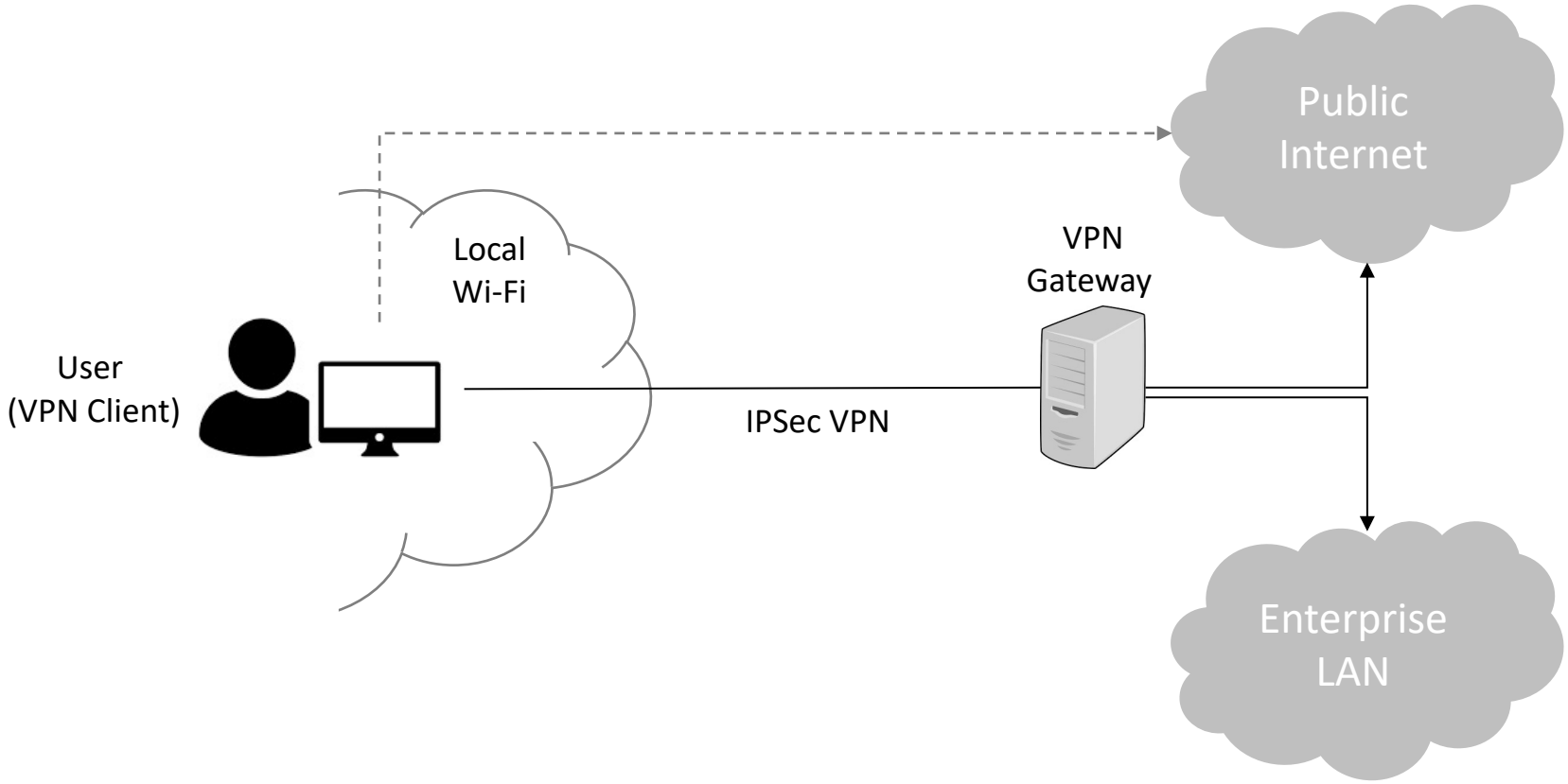
Every cyber security architect knows that a single point of failure on an enterprise network can be targeted for degradation by attackers armed with botnets. Distributed denial of service (DDOS) attacks aimed at corporate gateways, for example, have been a source of concern for chief information security officers (CISOs) concerned with availability. In theory, a malicious actor could take out any exported service delivered through a gateway by simply flooding the egress capability of the link – and several prominent instances of this attack have been observed in recent years [1].

**Paper on How This Works**

# What is ZTNA?

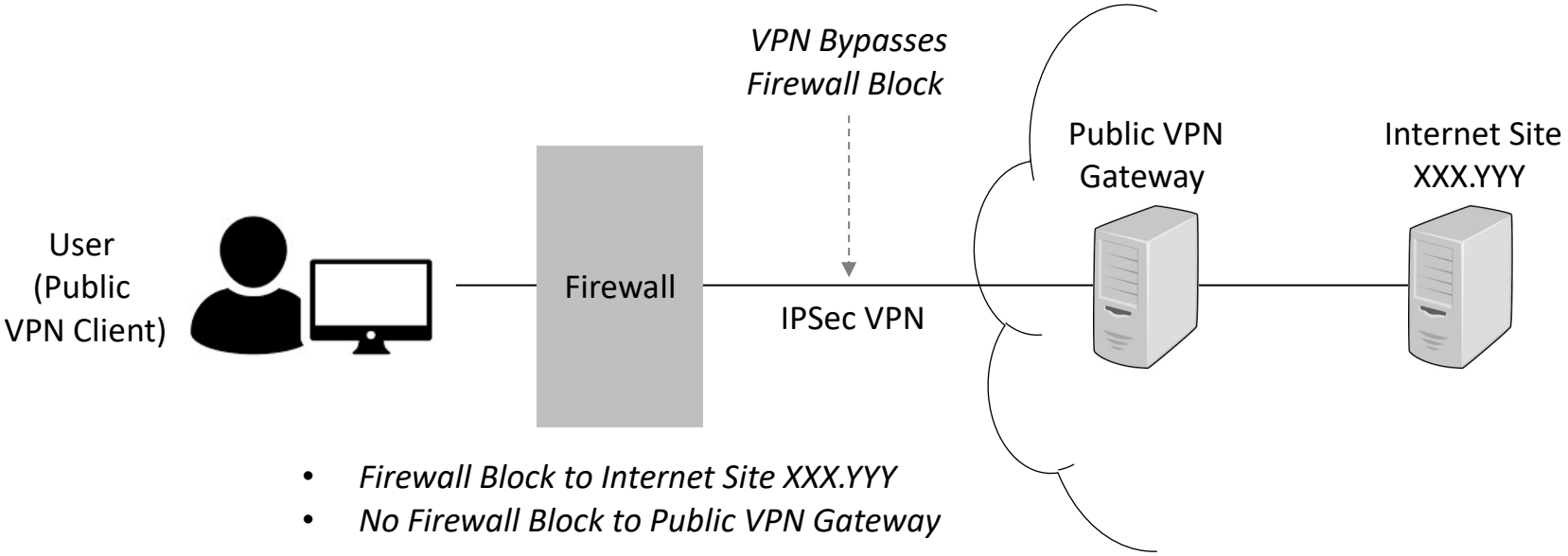
Week 13

# Current End-User Access – Virtual Private Network (VPN)



Week 13

# Public VPN Use-Case – Avoiding Local Blocks




- *Firewall Block to Internet Site XXX.YYY*
- *No Firewall Block to Public VPN Gateway*

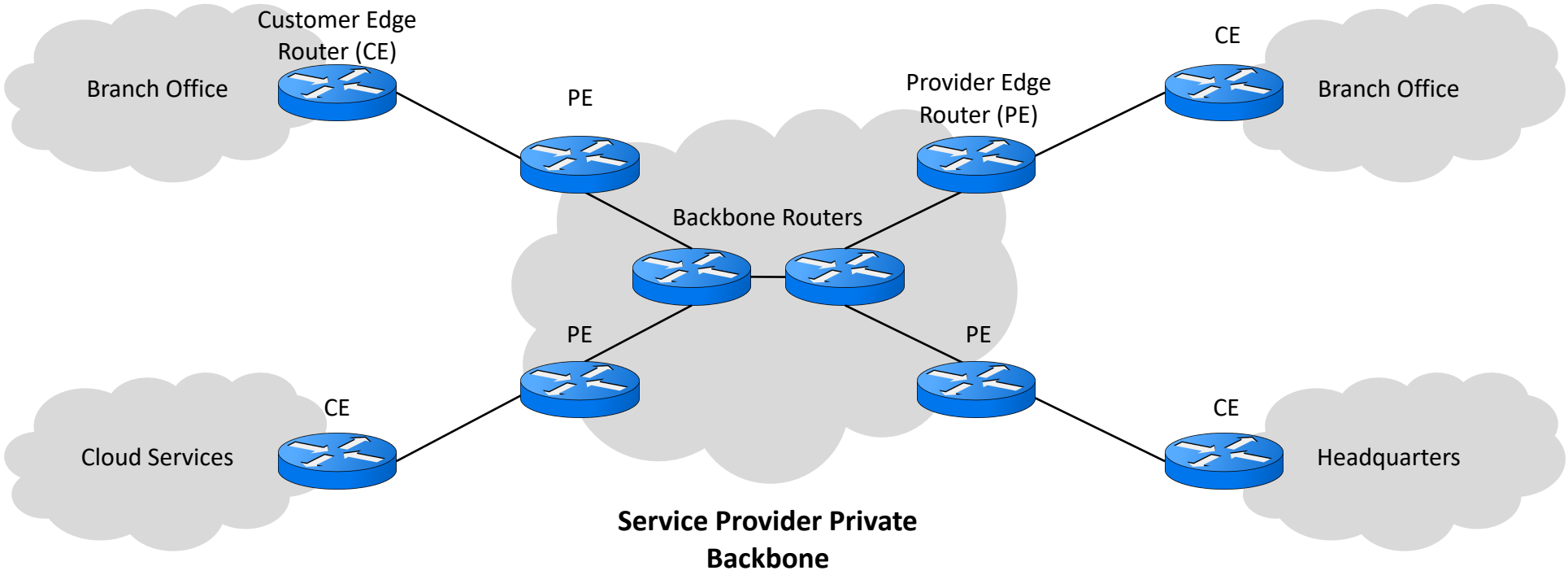
Week 13

# Pros and Cons of End-User VPN for Secure Access

- **Pros**
  - Secured connection for remote users
  - Inexpensive deployment
  - Familiar approach
- **Cons**
  - Slower connection speeds
  - Awkward Internet access (Wi-Fi)
  - Awkward configurations for users
  - Addresses only end-user use-case

Week 13

# Current Branch Office Access – Multi-Protocol Label Switching (MPLS)



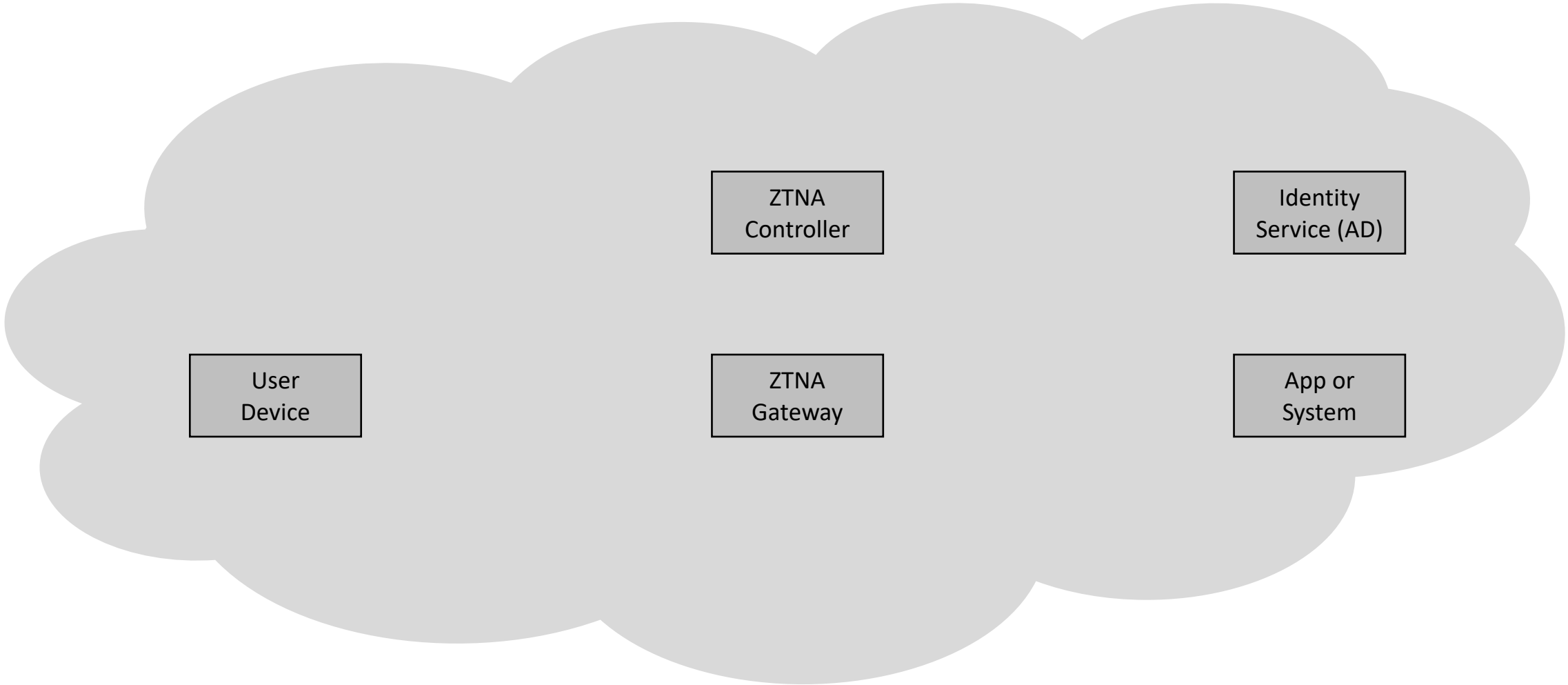
Week 13

# Pros and Cons of MPLS for Secure Access

- **Pros**
  - Carrier support for QoS
  - Carrier support for packet loss avoidance
  - Carrier provided security
- **Cons**
  - High cost
  - Complex administration
  - Inconsistency with cloud-first, zero trust
  - Addresses only branch office use-case

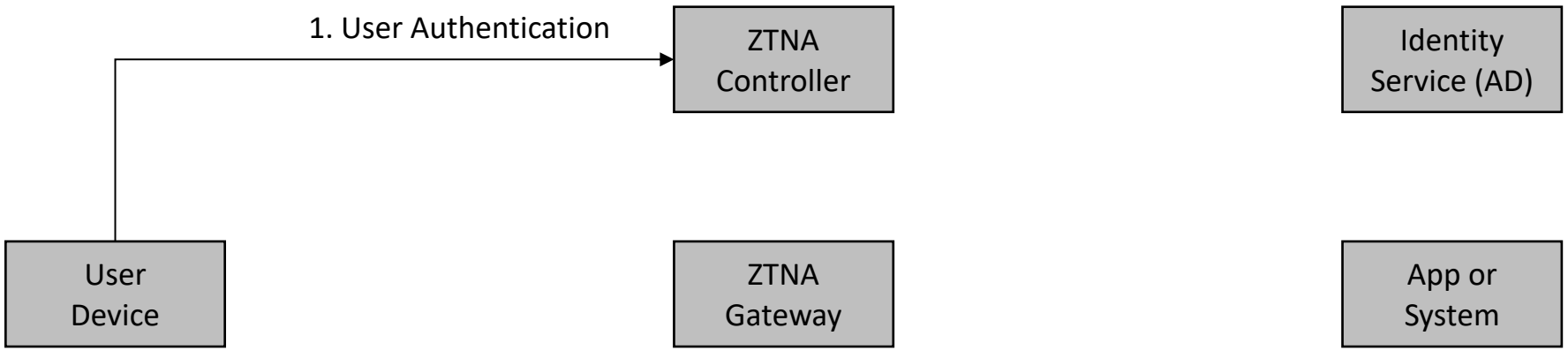
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



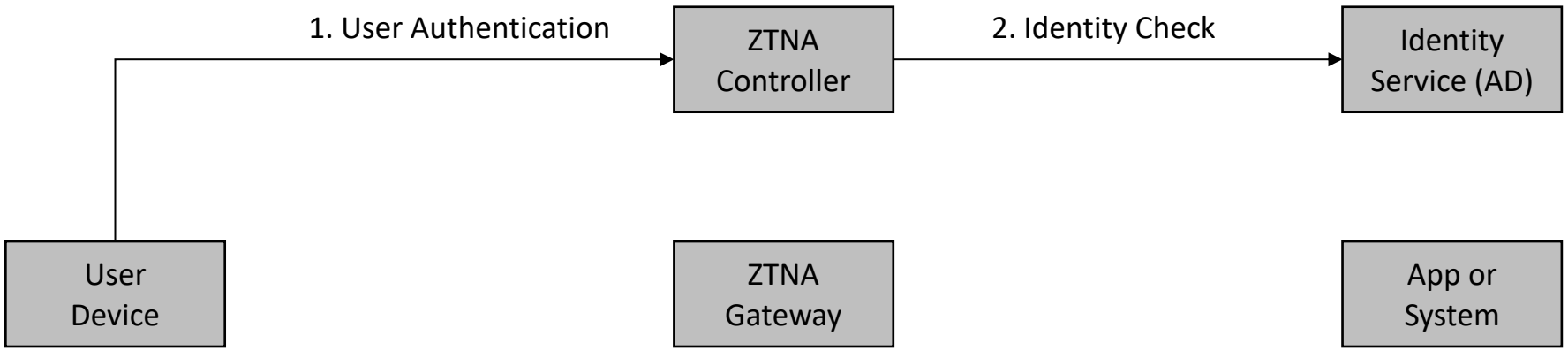
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



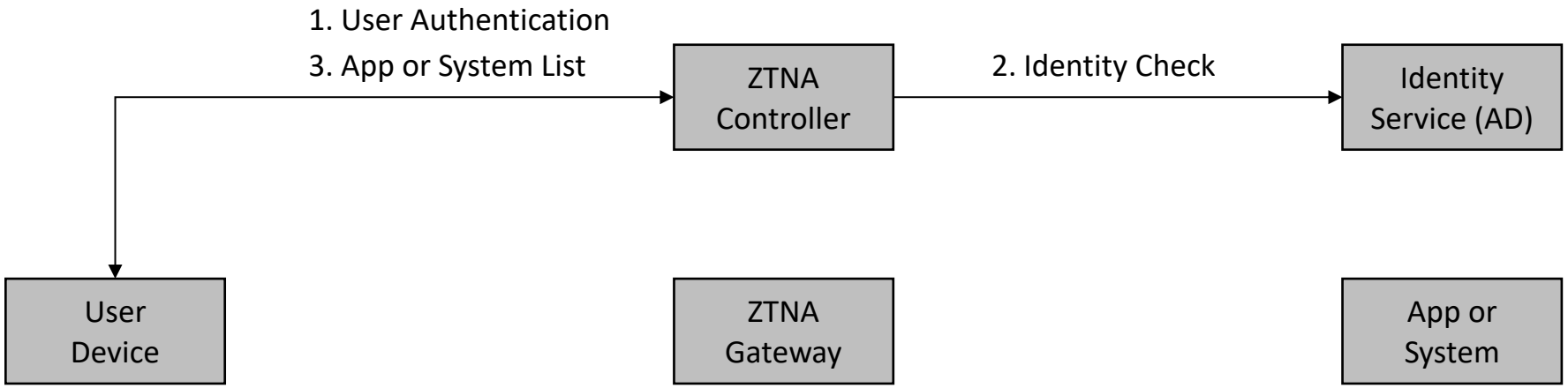
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



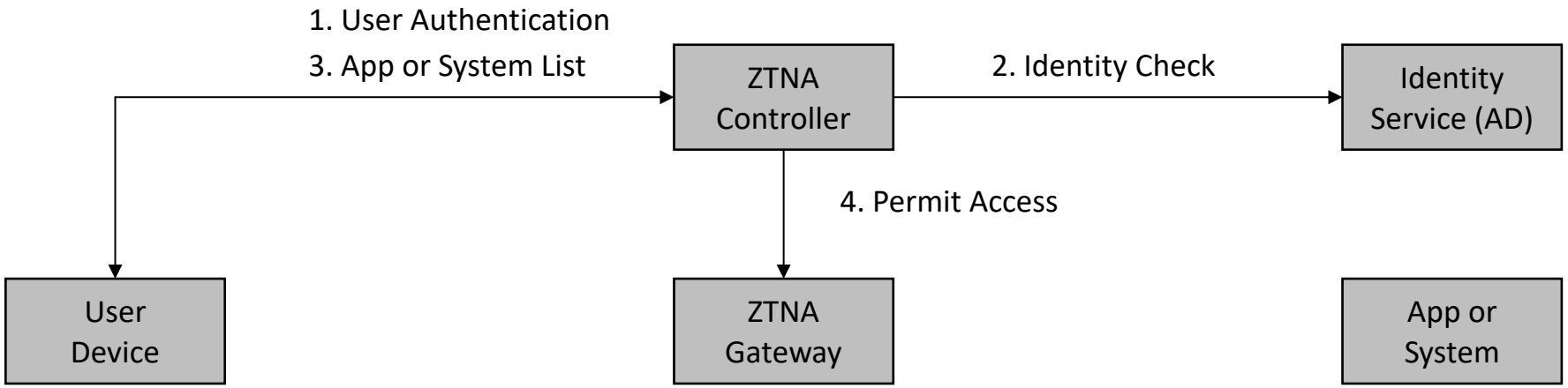
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



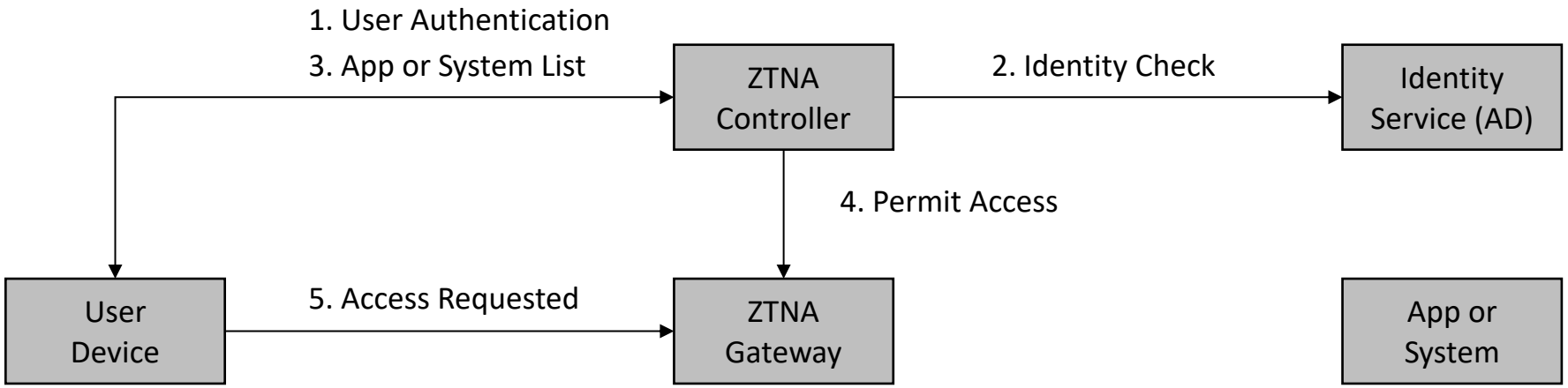
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



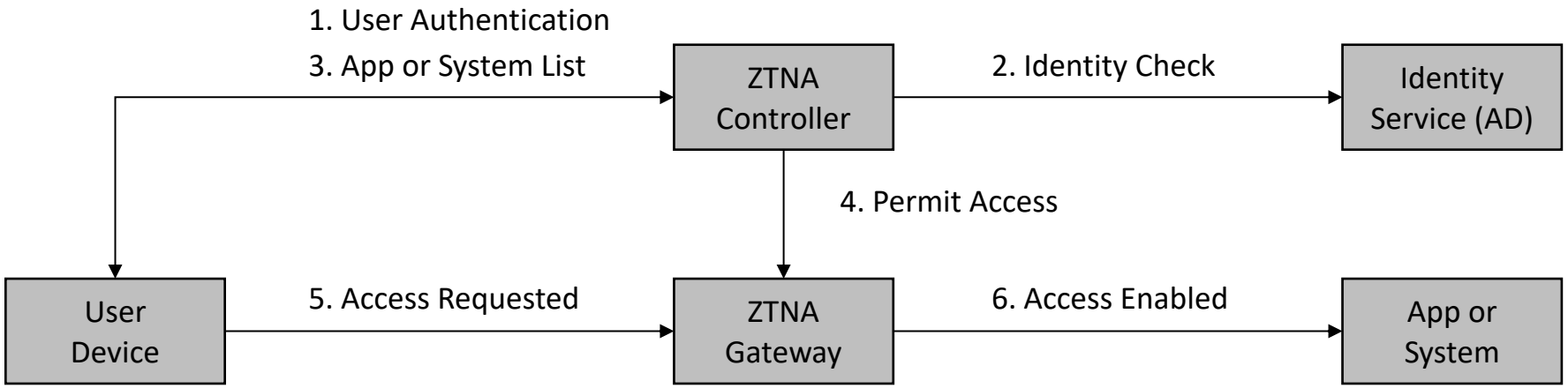
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



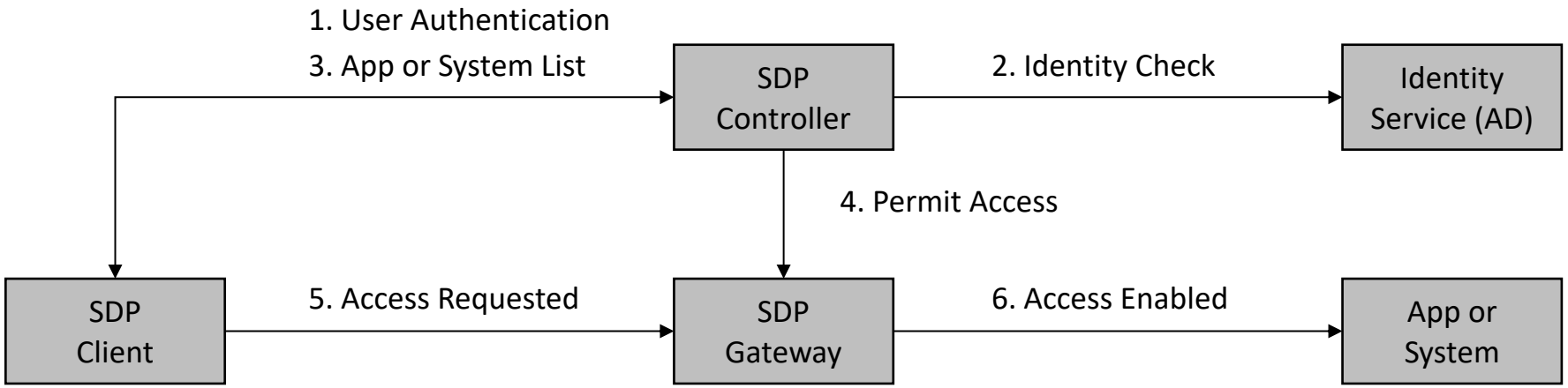
Week 13

# Zero Trust Network Access (ZTNA) – Canonical Model



Week 13

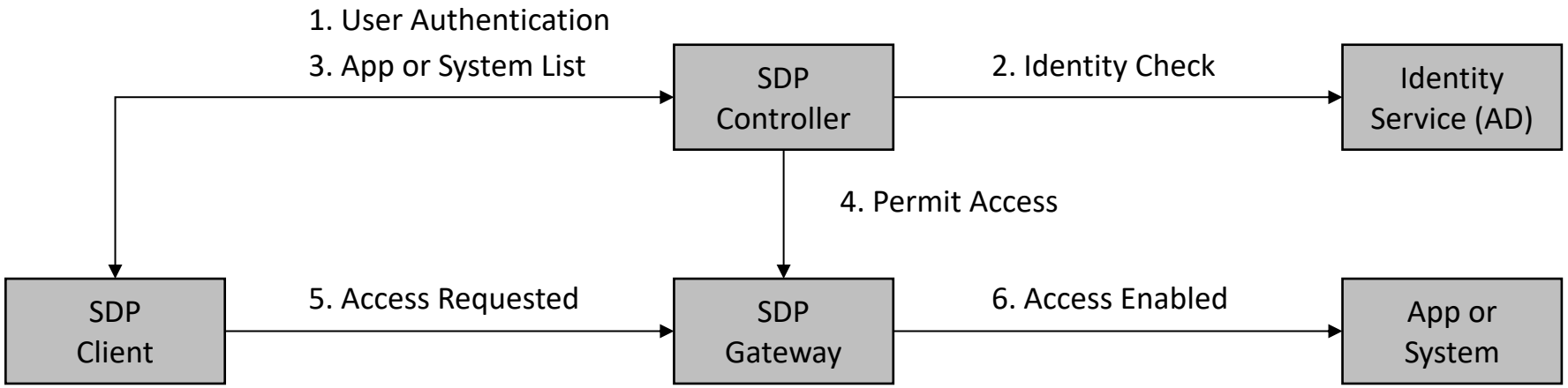
# Software Defined Perimeter (SDP) – Canonical Model



Week 13

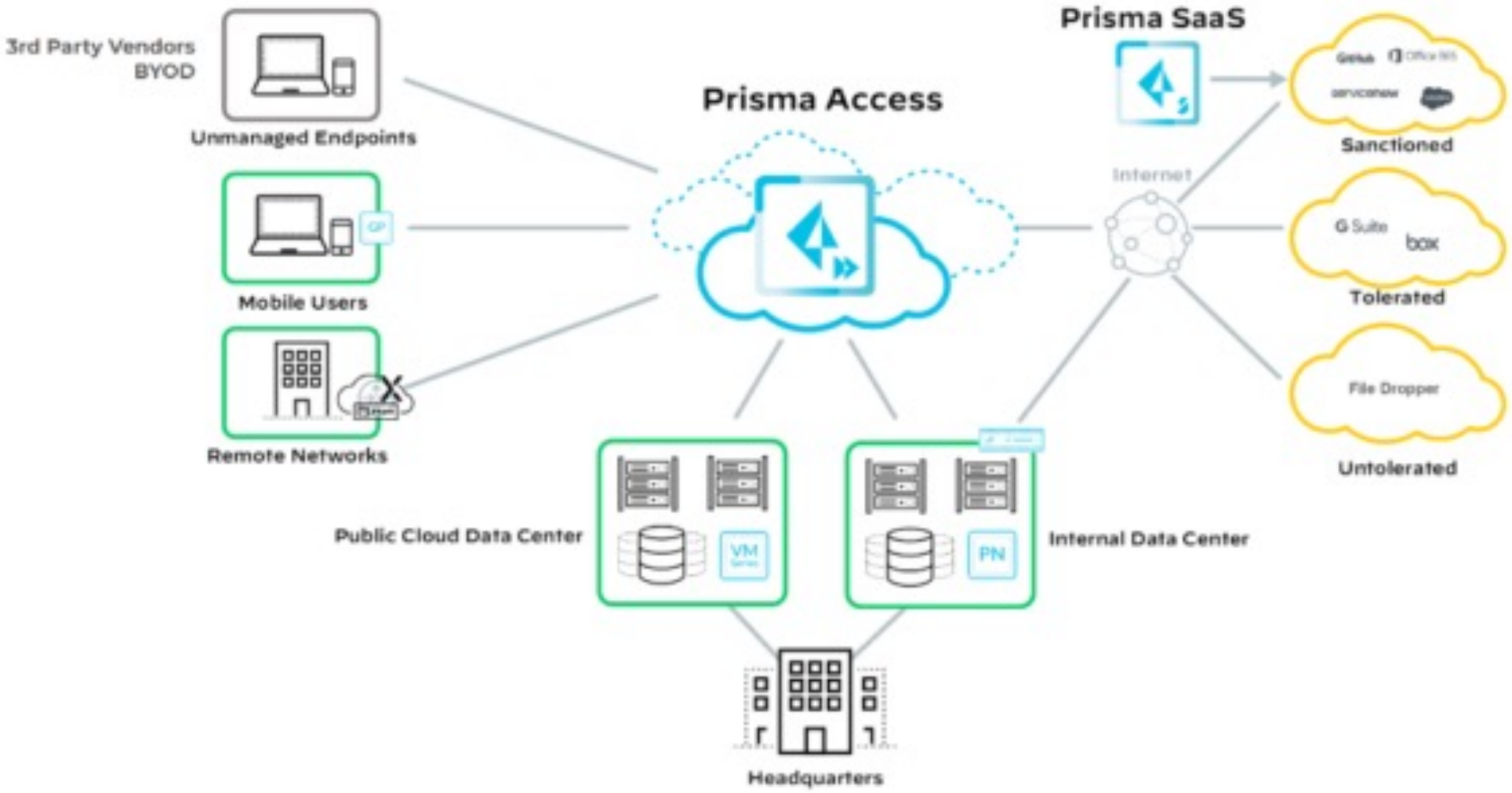
# Software Defined Perimeter (SDP) – Canonical Model

*ZTNA and SDP Do Not Appear to Include Meaningful Differences*



Week 13

# Typical ZTNA Commercial Vendor – PAN Prisma Access



# What is SD-WAN?

Week 13

# What is SD-WAN?

- **New approach to wide area network (WAN) management**
  - Driven by shift from data center-centric computing to cloud
  - Relies on virtual computing to separate data and control plane management

Week 13

# What is SD-WAN?

- **New approach to wide area network (WAN) management**
  - Driven by shift from data center-centric computing to cloud
  - Relies on virtual computing to separate data and control plane management
- **Uses software for more flexible control and security**
  - Software controls allow for dynamic allocation and improved visibility

Week 13

# What is SD-WAN?

- **New approach to wide area network (WAN) management**
  - Driven by shift from data center-centric computing to cloud
  - Relies on virtual computing to separate data and control plane management
- **Uses software for more flexible control and security**
  - Software controls allow for dynamic allocation and improved visibility
- **Important foundational component of SASE model**
  - Cloud-first SASE model requires a cloud-first WAN management model

Week 13

# What is SD-WAN?

- **New approach to wide area network (WAN) management**
  - Driven by shift from data center-centric computing to cloud
  - Relies on virtual computing to separate data and control plane management
- **Uses software for more flexible control and security**
  - Software controls allow for dynamic allocation and improved visibility
- **Important foundational component of SASE model**
  - Cloud-first SASE model requires a cloud-first WAN management model
- **Many commercial vendor options for SD-WAN**
  - SD-WAN solutions from cybersecurity vendors as well as traditional service providers

Week 13

# Three Primary Enterprise Network Use-Cases

- **Branch Offices**
  - Traditional access to data centers through MPLS
  - SD-WAN supports this use case in modern SASE context

*Primary Use-Case Involving Shift from MPLS*

Week 13

# Three Primary Enterprise Network Use-Cases

- **Branch Offices**
  - Traditional access to data centers through MPLS
  - SD-WAN supports this use case in modern SASE context
- **End Users**
  - Traditional access to data centers through corporate VPN
  - Cloud-based secure access solutions included in SASE model

*Primary Use-Case Involving Shift from MPLS*

Week 13

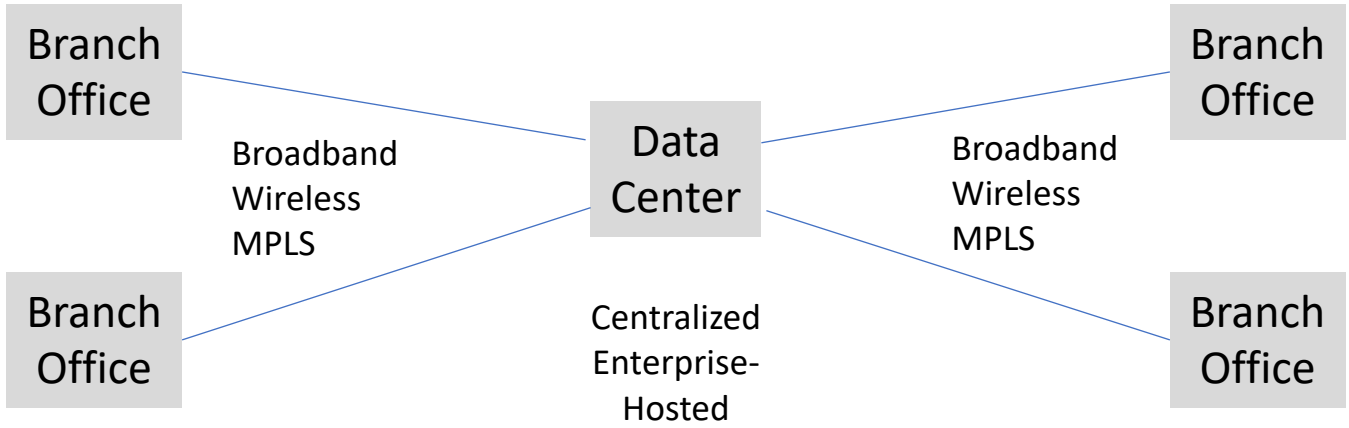
# Three Primary Enterprise Network Use-Cases

- **Branch Offices**
  - Traditional access to data centers through MPLS
  - SD-WAN supports this use case in modern SASE context
- **End Users**
  - Traditional access to data centers through corporate VPN
  - Cloud-based secure access solutions included in SASE model
- **Third-Parties**
  - Traditional access to data centers through private B2B connections
  - Cloud-based secure access solutions included in SASE model

*Primary Use-Case Involving Shift from MPLS*

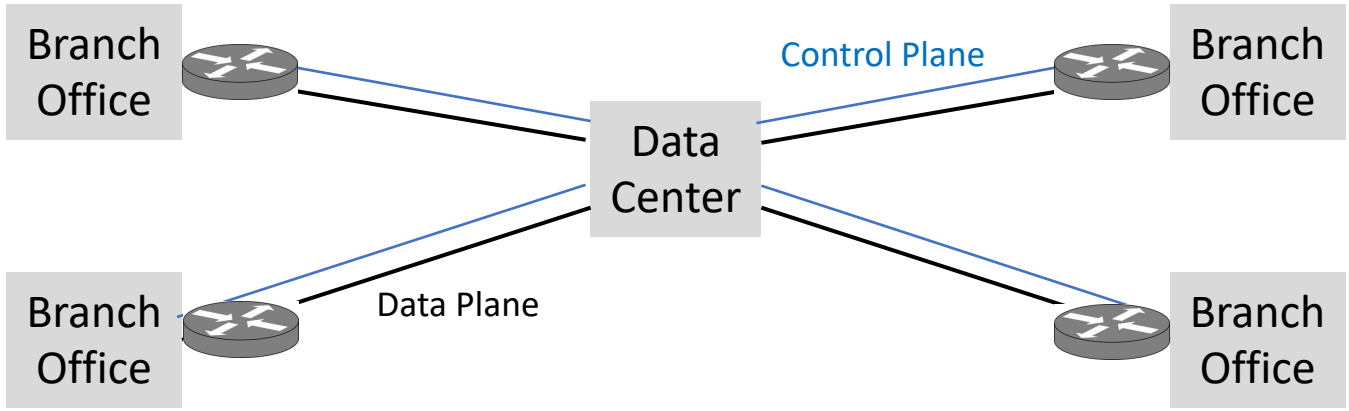
Week 13

# Traditional Branch Office WAN – Basic Configuration



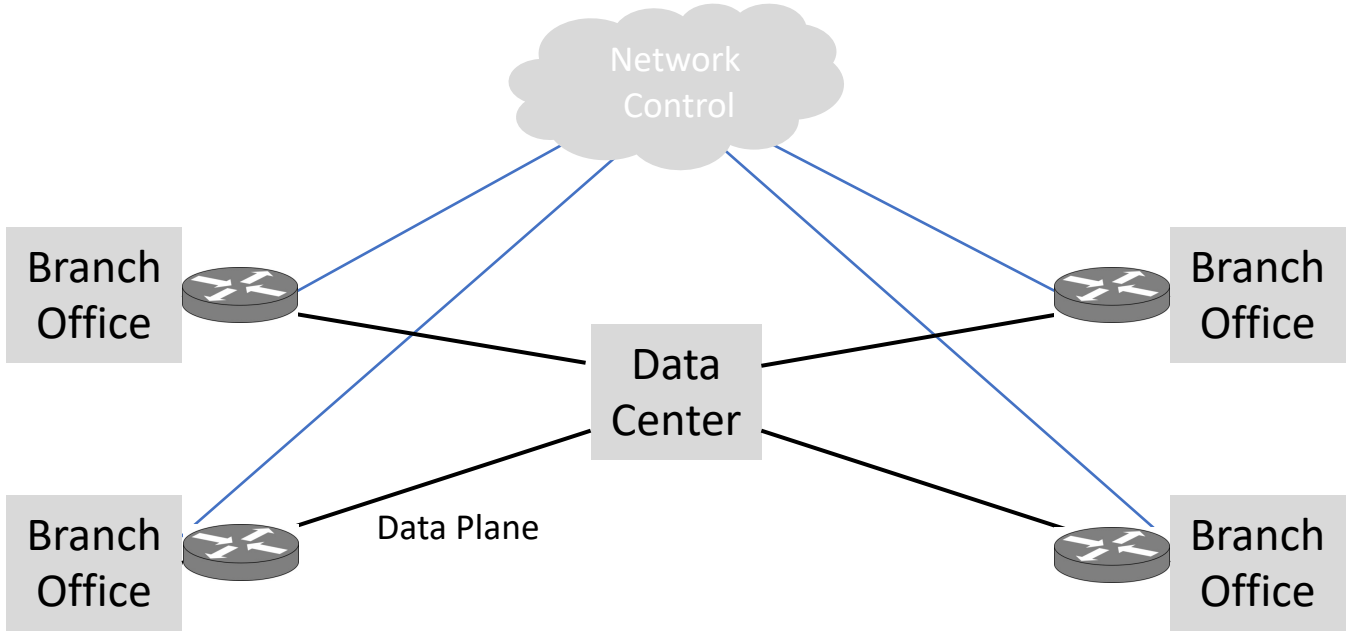
Week 13

# Traditional Branch Office WAN – Control and Data Plane Separation



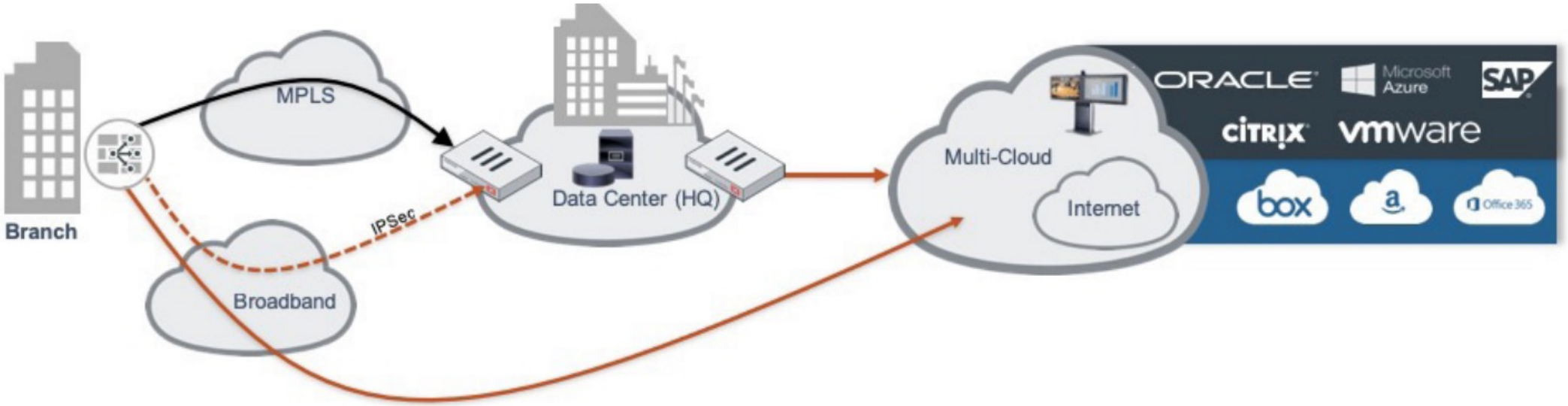
Week 13

# Traditional Branch Office WAN – Cloud-Based Network Control



Week 13

# Typical Commercial SD-WAN: Fortinet Reference Architecture



# What is SASE (Secure Access Service Edge)?

Week 13

# What are the Components of SASE?

- **Management of cloud native microservices**
  - Microservice support is best provided in a single platform architecture

Week 13

# What are the Components of SASE?

- **Management of cloud native microservices**
  - Microservice support is best provided in a single platform architecture
- **Ability to perform real-time inspection**
  - Inspection of encrypted traffic, endpoints, and workloads must be done at cloud scale

Week 13

# What are the Components of SASE?

- **Management of cloud native microservices**
  - Microservice support is best provided in a single platform architecture
- **Ability to perform real-time inspection**
  - Inspection of encrypted traffic, endpoints, and workloads must be done at cloud scale
- **In-line proxy capable of decoding cloud and web traffic**
  - Proxy capability is generally provided in the context of a secure web gateway (SWG)

Week 13

# What are the Components of SASE?

- **Management of cloud native microservices**
  - Microservice support is best provided in a single platform architecture
- **Ability to perform real-time inspection**
  - Inspection of encrypted traffic, endpoints, and workloads must be done at cloud scale
- **In-line proxy capable of decoding cloud and web traffic**
  - Proxy capability is generally provided in the context of a secure web gateway (SWG)
- **Firewall and intrusion protection for all ports and protocols**
  - This capability is often integrated as a virtual firewall as a service or network-based firewall

Week 13

# What are the Components of SASE?

- **Management of cloud native microservices**
  - Microservice support is best provided in a single platform architecture
- **Ability to perform real-time inspection**
  - Inspection of encrypted traffic, endpoints, and workloads must be done at cloud scale
- **In-line proxy capable of decoding cloud and web traffic**
  - Proxy capability is generally provided in the context of a secure web gateway (SWG)
- **Firewall and intrusion protection for all ports and protocols**
  - This capability is often integrated as a virtual firewall as a service or network-based firewall
- **Integration with SD-WAN architectures**
  - Such integration is especially important for larger networks with many nodes

Week 13

# What is a Large-Scale SASE Implementation?

- **Phased implementation to branches and regions**
  - SASE roll-out benefits from a careful roll-out plan

Week 13

# What is a Large-Scale SASE Implementation?

- **Phased implementation to branches and regions**
  - SASE roll-out benefits from a careful roll-out plan
- **Support for remote and work-from-home team members**
  - Secure access requires support for many remote work scenarios

Week 13

# What is a Large-Scale SASE Implementation?

- **Phased implementation to branches and regions**
  - SASE roll-out benefits from a careful roll-out plan
- **Support for remote and work-from-home team members**
  - Secure access requires support for many remote work scenarios
- **Coordination with WAN management team**
  - SD-WAN integration with MPLS and mobility requires expert attention

Week 13

# What is a Large-Scale SASE Implementation?

- **Phased implementation to branches and regions**
  - SASE roll-out benefits from a careful roll-out plan
- **Support for remote and work-from-home team members**
  - Secure access requires support for many remote work scenarios
- **Coordination with WAN management team**
  - SD-WAN integration with MPLS and mobility requires expert attention
- **Project management to shift applications to cloud**
  - Rehosting applications in public cloud demands careful planning and design

Week 13

# What is a Large-Scale SASE Implementation?

- **Phased implementation to branches and regions**
  - SASE roll-out benefits from a careful roll-out plan
- **Support for remote and work-from-home team members**
  - Secure access requires support for many remote work scenarios
- **Coordination with WAN management team**
  - SD-WAN integration with MPLS and mobility requires expert attention
- **Project management to shift applications to cloud**
  - Rehosting applications in public cloud demands careful planning and design
- **Enhancing cloud and web security services**
  - Security services in SASE context must be delivered via cloud and network

Week 13

# What are Secure Networking Future Direction Areas?

- **Massive implications of 5G mobility**
  - SD-WAN includes 5G as a transport option

Week 13

# What are Secure Networking Future Direction Areas?

- **Massive implications of 5G mobility**
  - SD-WAN includes 5G as a transport option
- **Accelerated use of networks by machines (including cars)**
  - M2M dramatically increases complexity and scale of endpoint

Week 13

# What are Secure Networking Future Direction Areas?

- **Massive implications of 5G mobility**
  - SD-WAN includes 5G as a transport option
- **Accelerated use of networks by machines (including cars)**
  - M2M dramatically increases complexity and scale of endpoint
- **Merged implementation of IT and OT infrastructure**
  - Operational technology (OT) will be overtaken by IT services

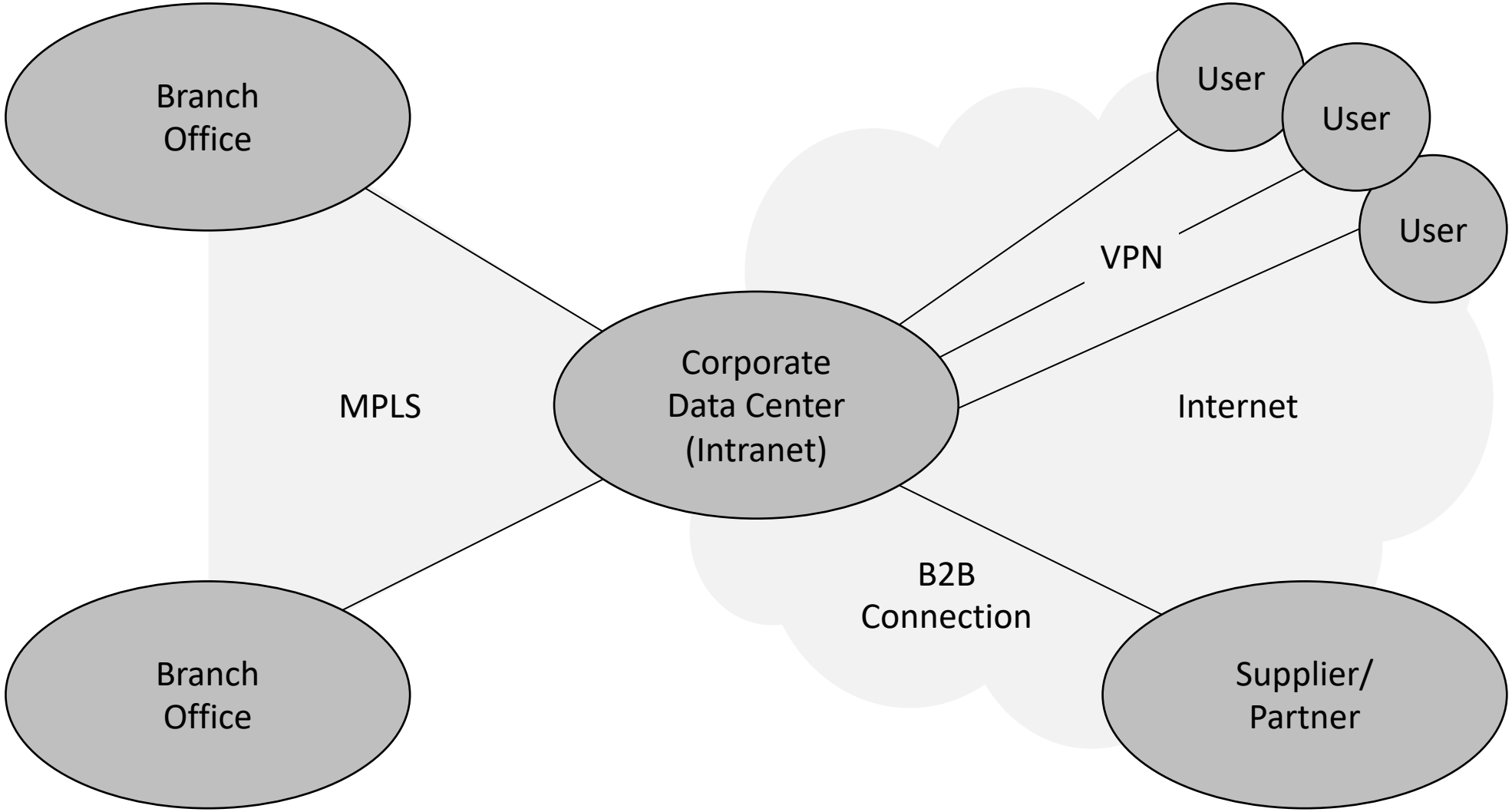
Week 13

# What are Secure Networking Future Direction Areas?

- **Massive implications of 5G mobility**
  - SD-WAN includes 5G as a transport option
- **Accelerated use of networks by machines (including cars)**
  - M2M dramatically increases complexity and scale of endpoint
- **Merged implementation of IT and OT infrastructure**
  - Operational technology (OT) will be overtaken by IT services
- **Increased use of human-augmented technology**
  - Humans will wear and embody computing, which increases life-critical threats

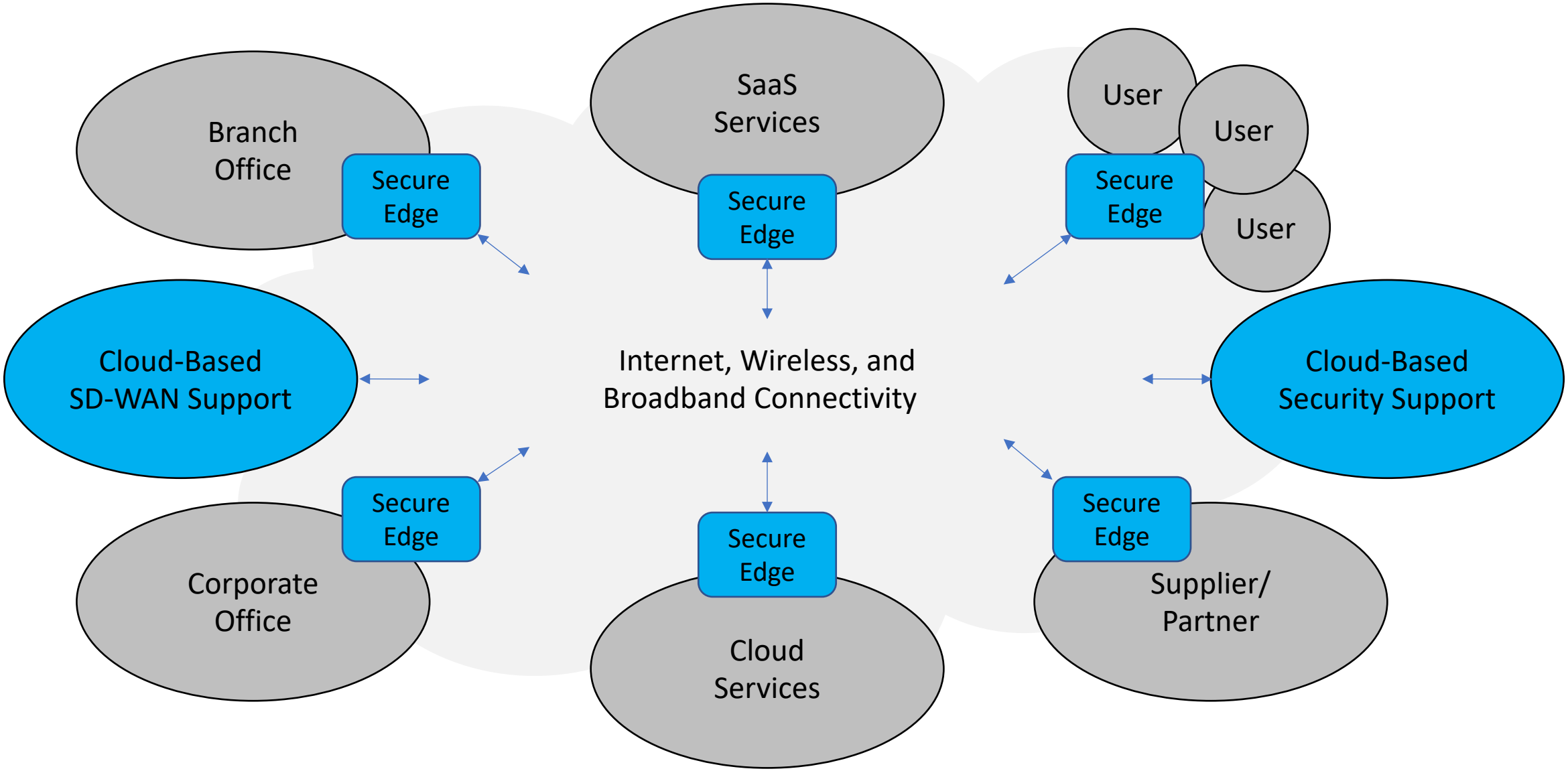
Week 13

# Traditional Secure Business Network



Week 13

# Next Generation Secure Business Network – SASE



Week 13

# Typical SASE Point of Presence (POP) Concept Design