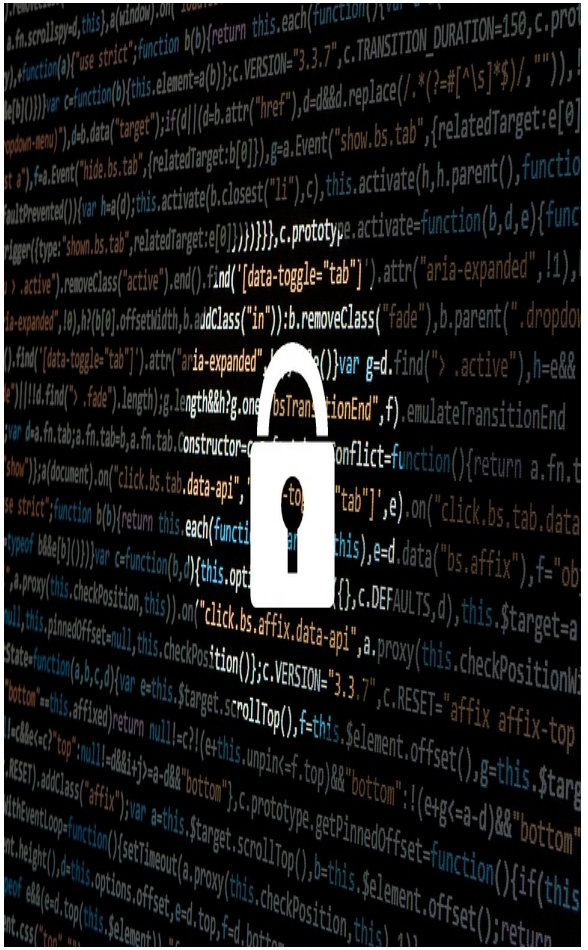
Securing SD-WAN

Richard Vidil

September 7, 2018

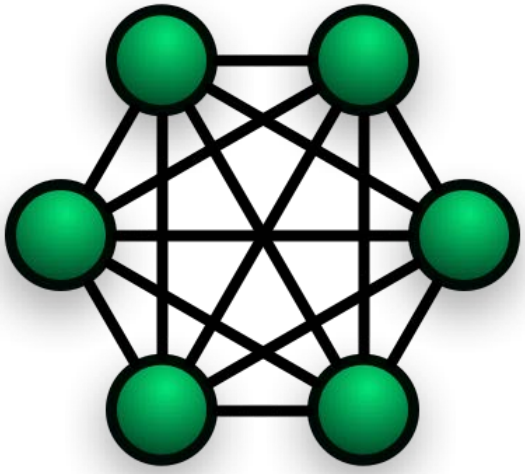
Network Security Overview

- Why do businesses secure their networks?
  - Networks carry valuable information
  - Security considerations
    - Integrity of data
    - Availability of data
    - Privacy and confidentiality
    - Authorization
    - Authentication
- How are they secured?
  - Physical security
    - Cables
    - Switches
    - Routers
    - Servers
  - Perimeter security
    - External access control
      - Firewalls
    - Content filtering
      - Deep Packet Inspection (DPI)
      - Application proxies
  - Data encryption

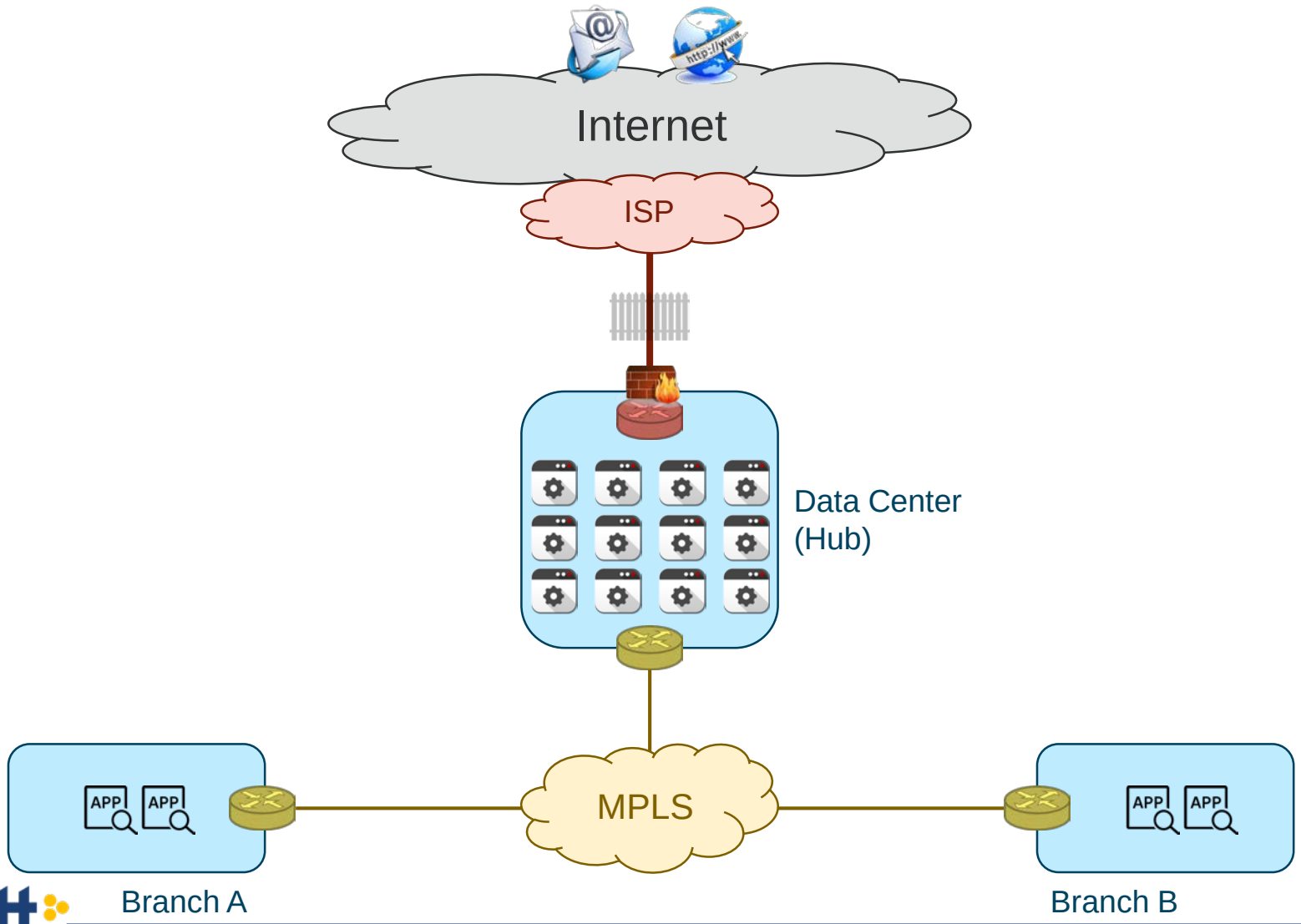


Internet Security Challenges

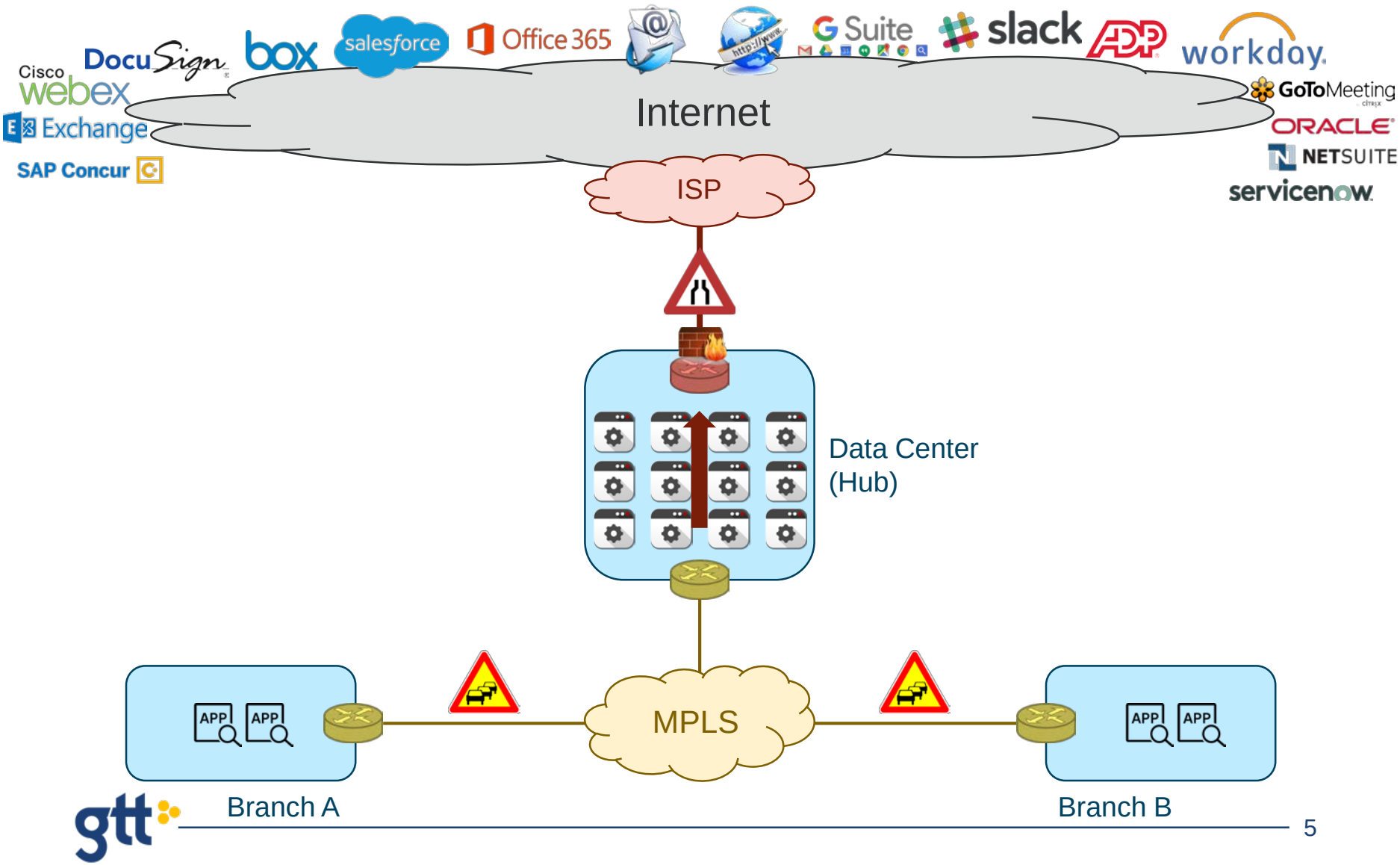
- Traditionally businesses utilized private WANs for performance and security
  - Wholly owned/operated
  - Leased from service providers
    - TDM services
      - Private lines
      - SONET
    - Packet services
      - ATM
      - Frame Relay
      - MPLS
- Today, public networks (i.e., the Internet) play increasingly important role
  - Many business-critical applications are SaaS via Internet
- Internet Security is difficult because datagrams may traverse intermediate networks not owned or controlled by sender or recipient
  - Datagrams can be intercepted or compromised
    - Eavesdropping
    - Source spoofing
    - Replay attacks
  - Conclusion: Internet datagram contents cannot be trusted



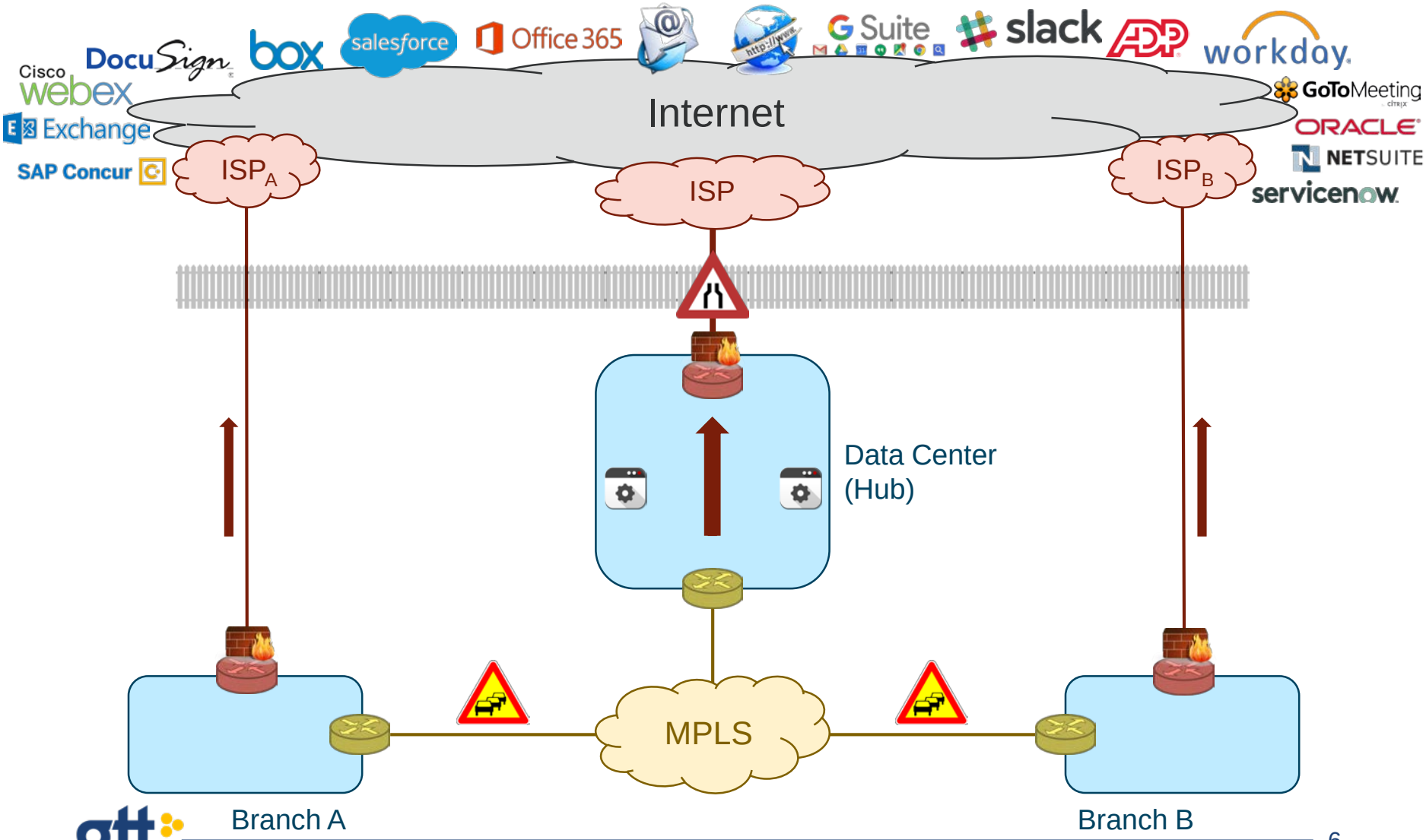
The Traditional Enterprise WAN



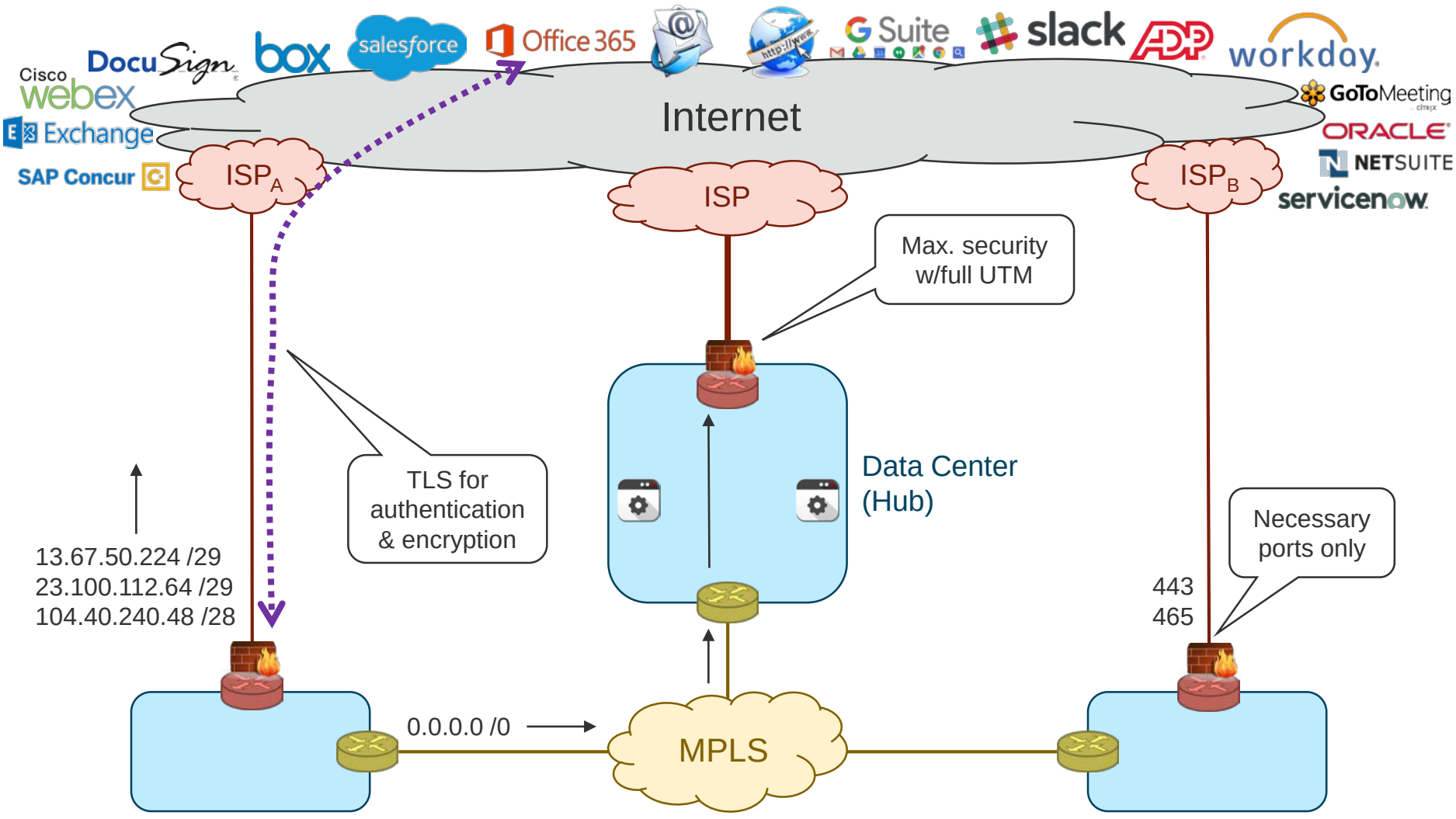
The Shift to the Cloud (SaaS)



The Hybrid WAN

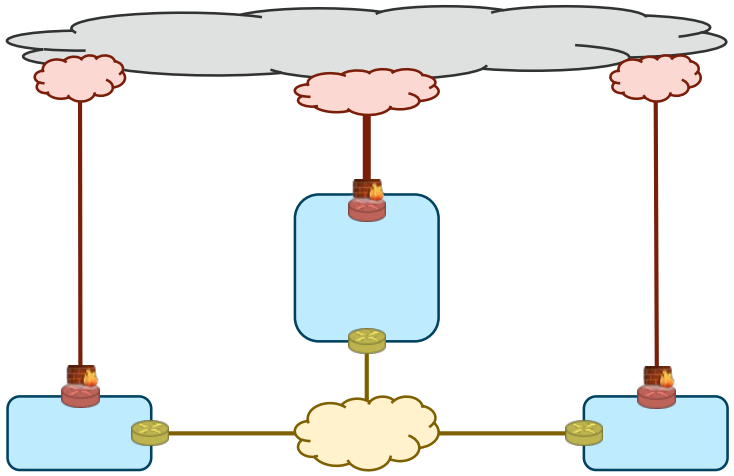


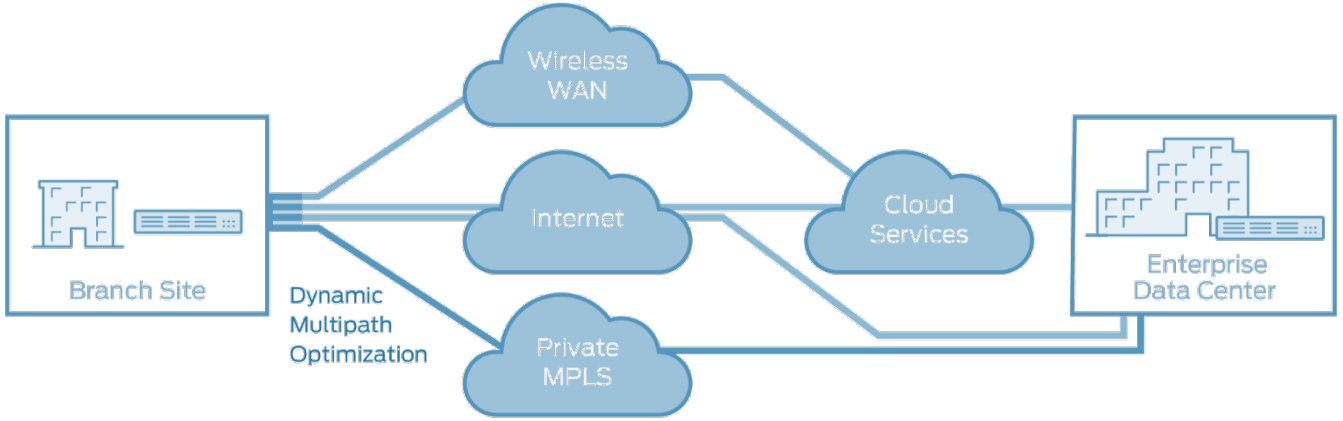
Hybrid WAN Security



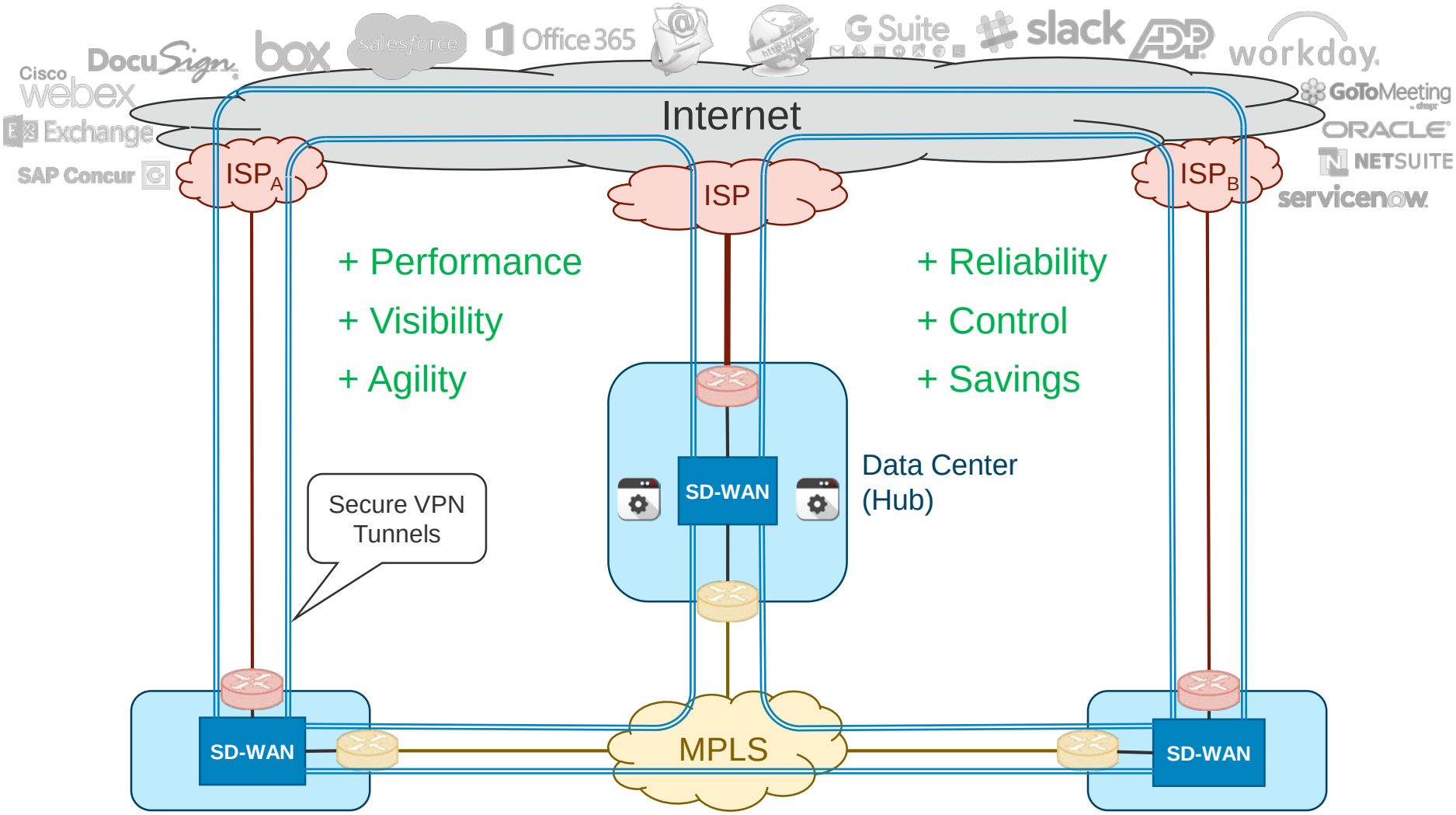
Limitations of Hybrid WAN

- Two disparate networks to manage
- Limited failover capability
  - Internet to MPLS straightforward but not instantaneous
  - MPLS to Internet requires more
    - IPsec VPN for private traffic
    - Complex routing environment
- Internet service is best effort only
  - No traffic shaping, QoS enforcement
- SD-WAN addresses these limitations

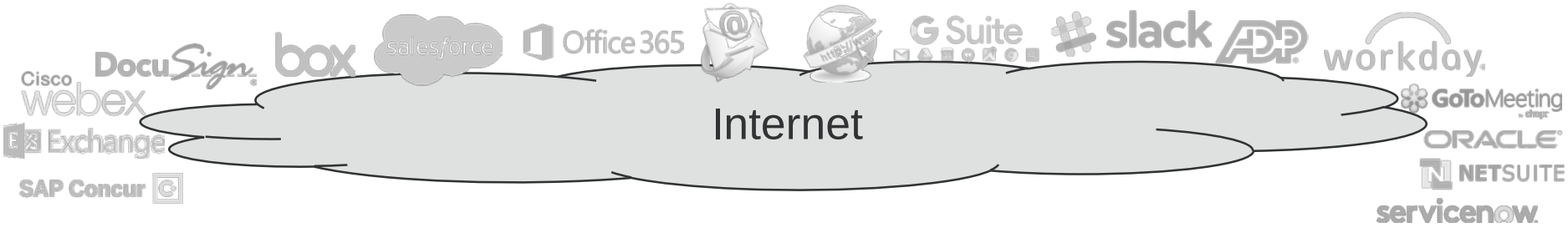


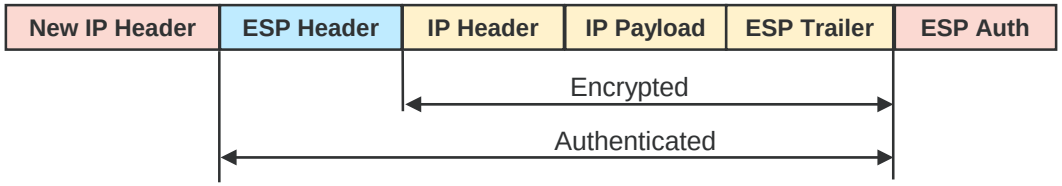


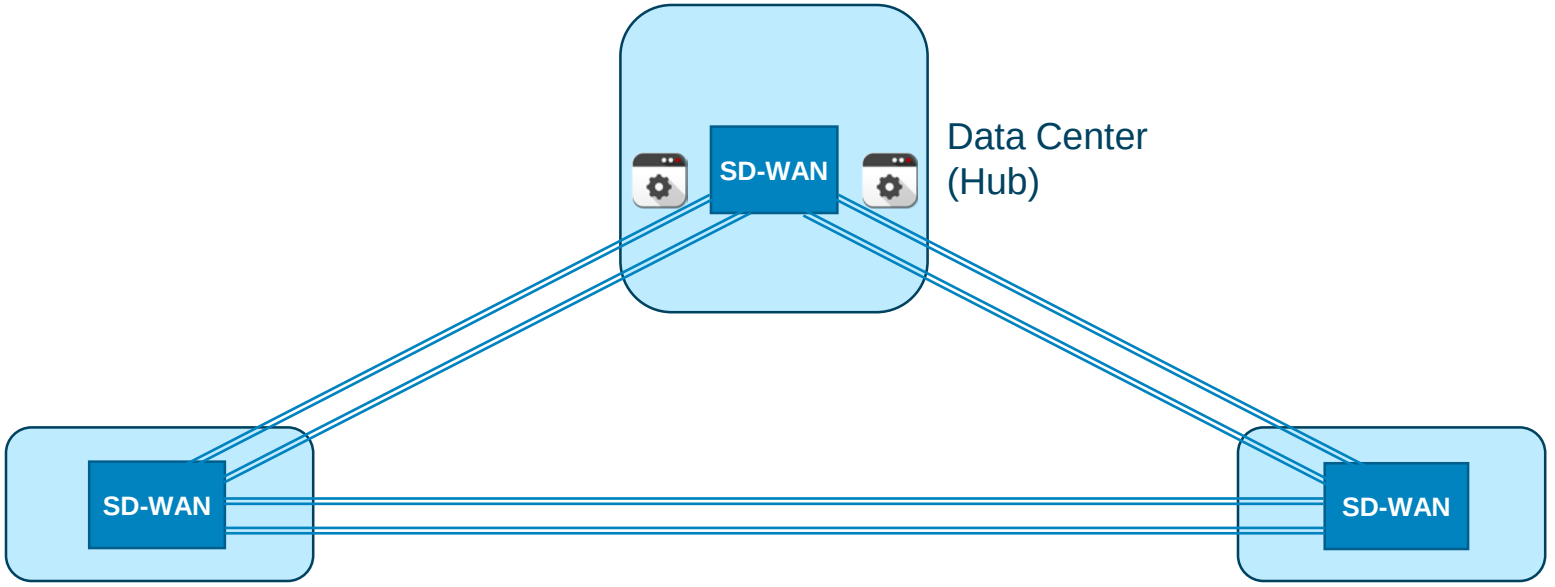
Harmonizing Hybrid WAN With SD-WAN



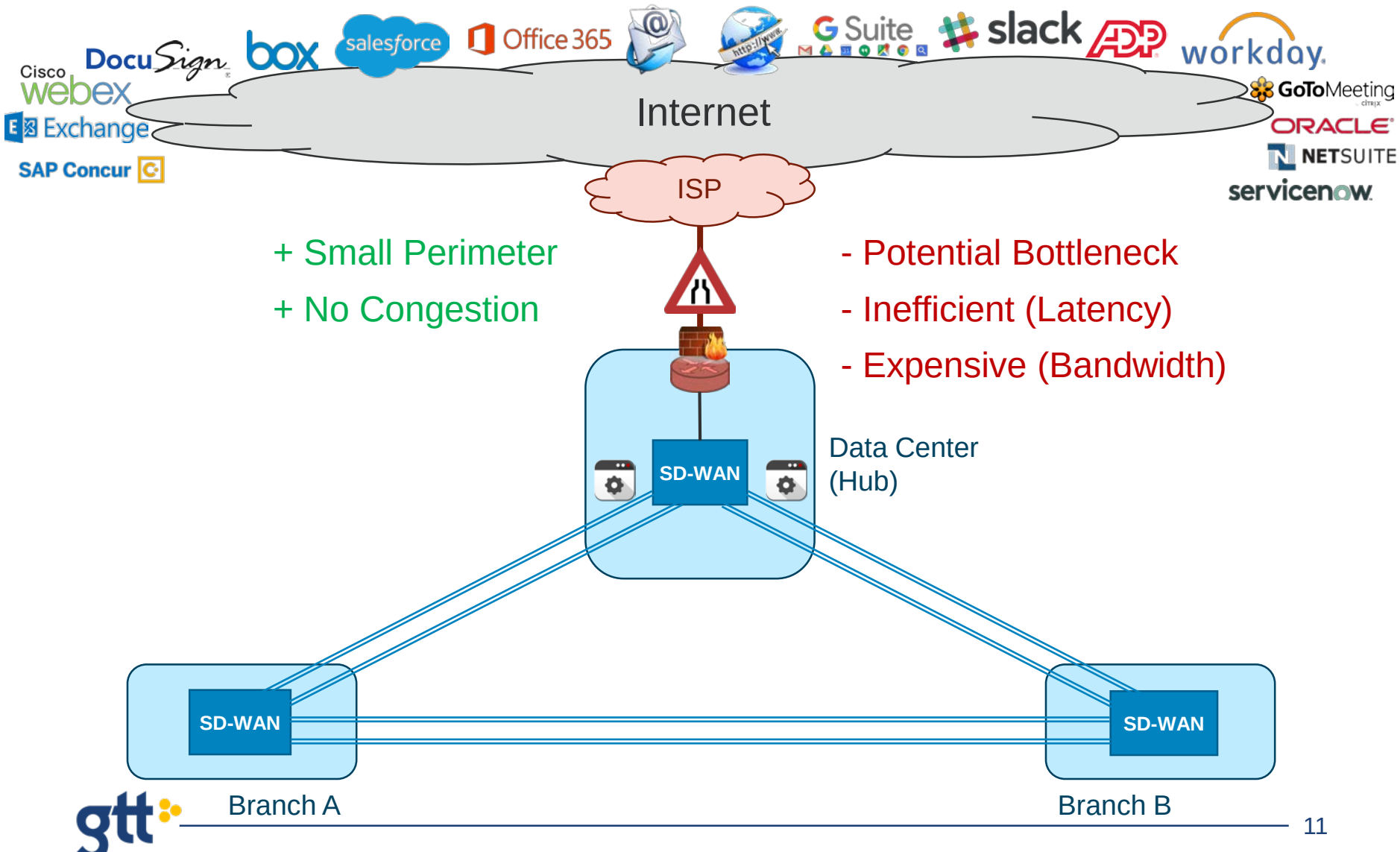
SD-WAN: A Secure Overlay Network



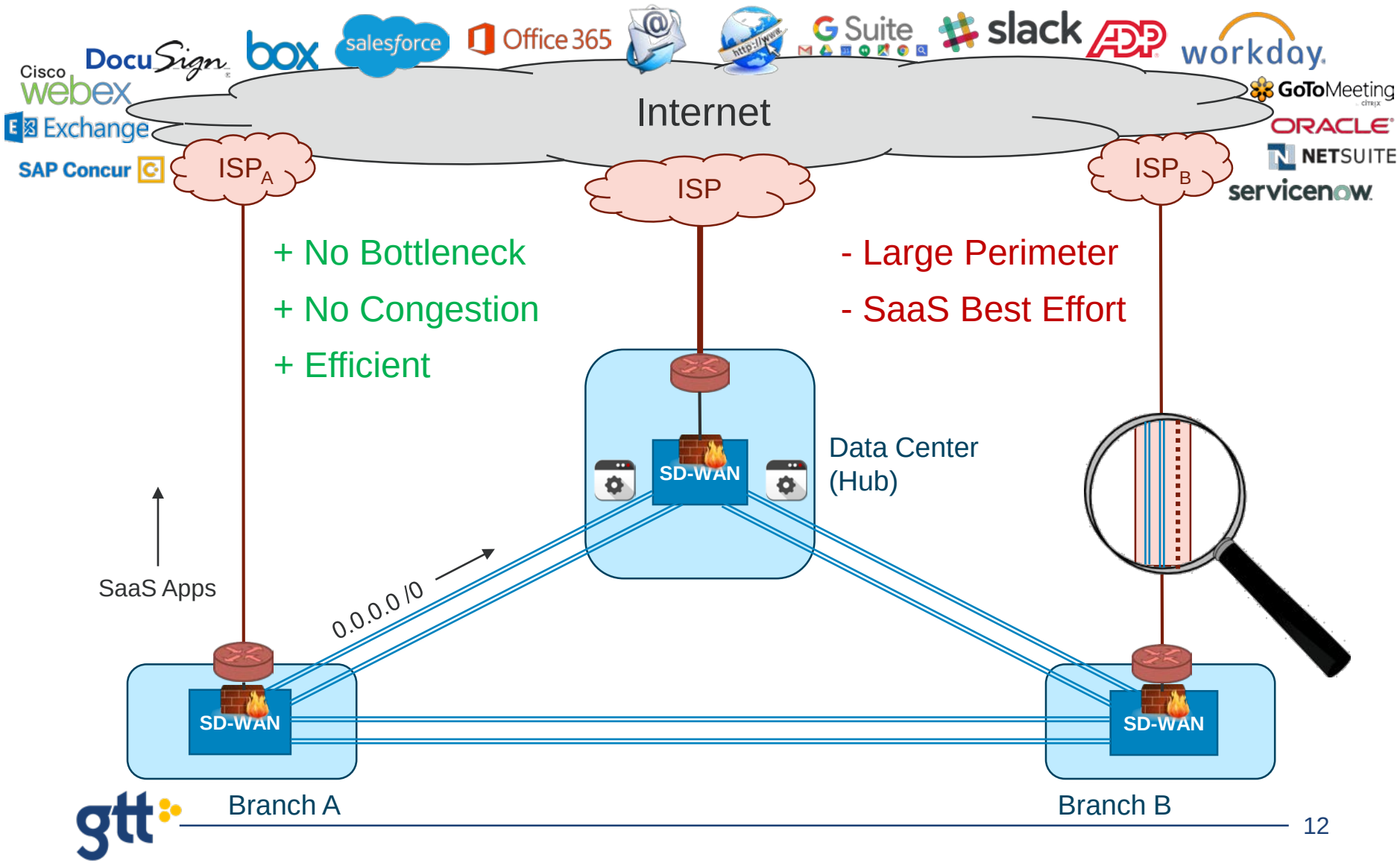




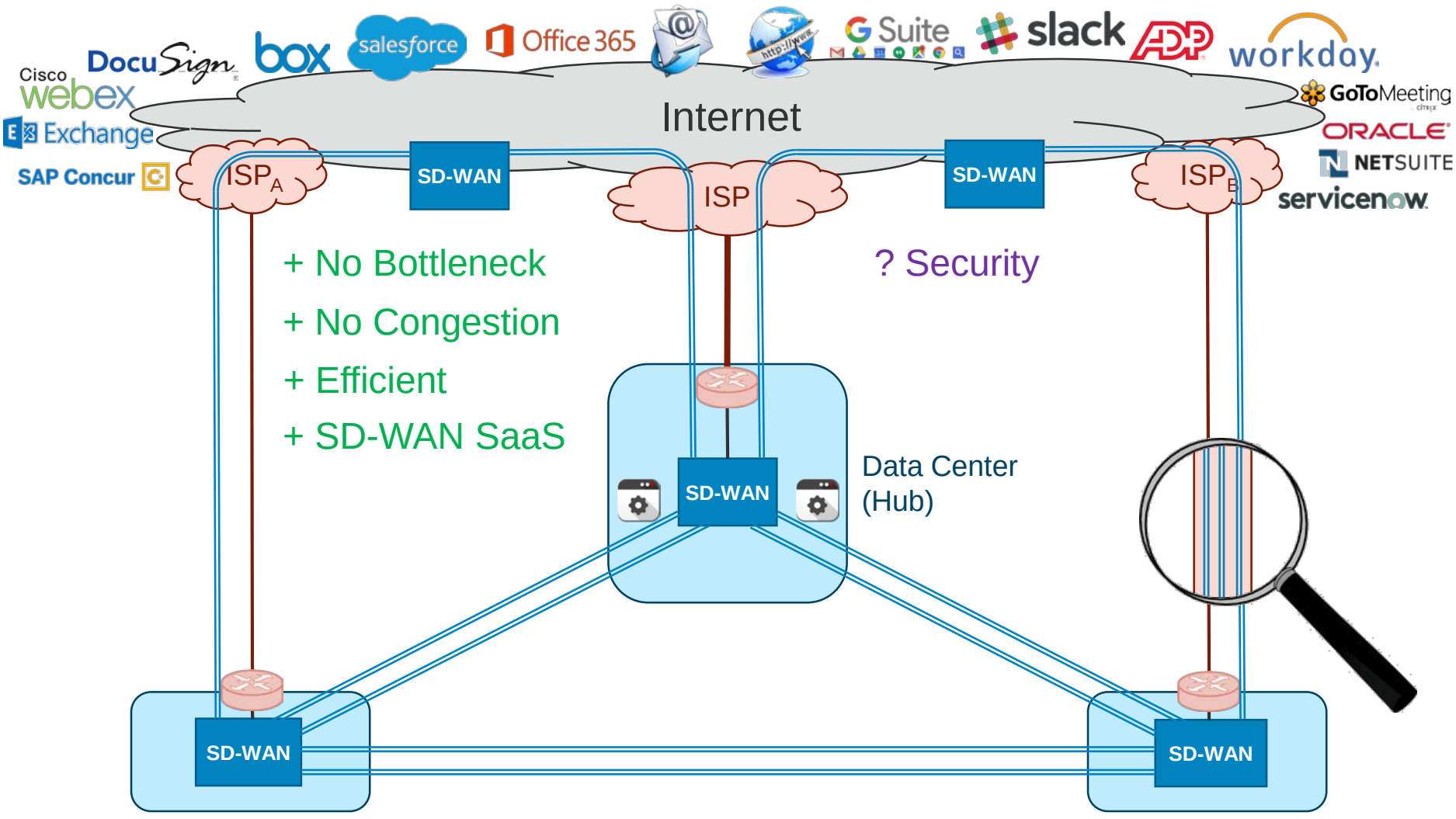
SD-WAN Internet: Centralized



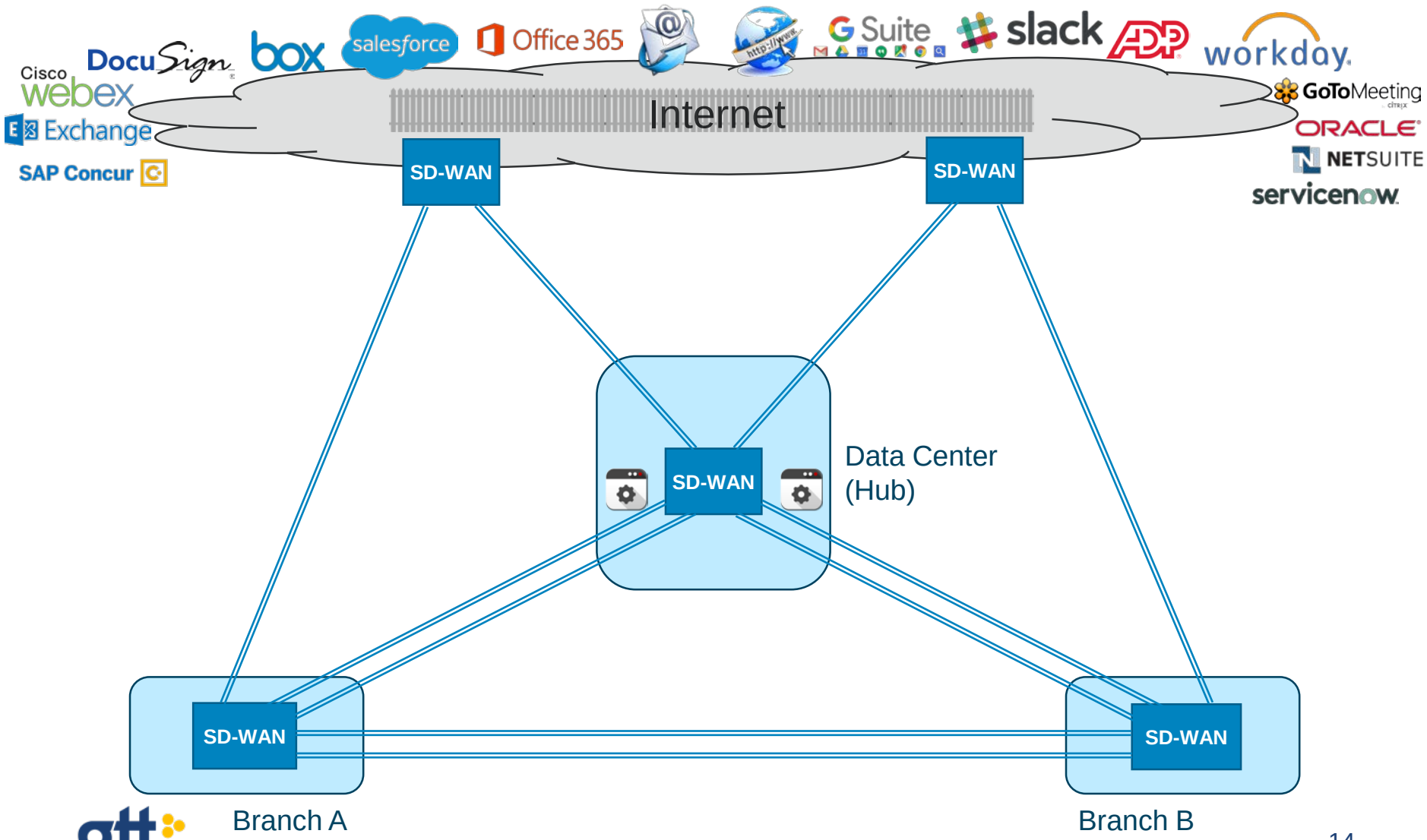
SD-WAN Internet: Distributed (Split Tunnel)



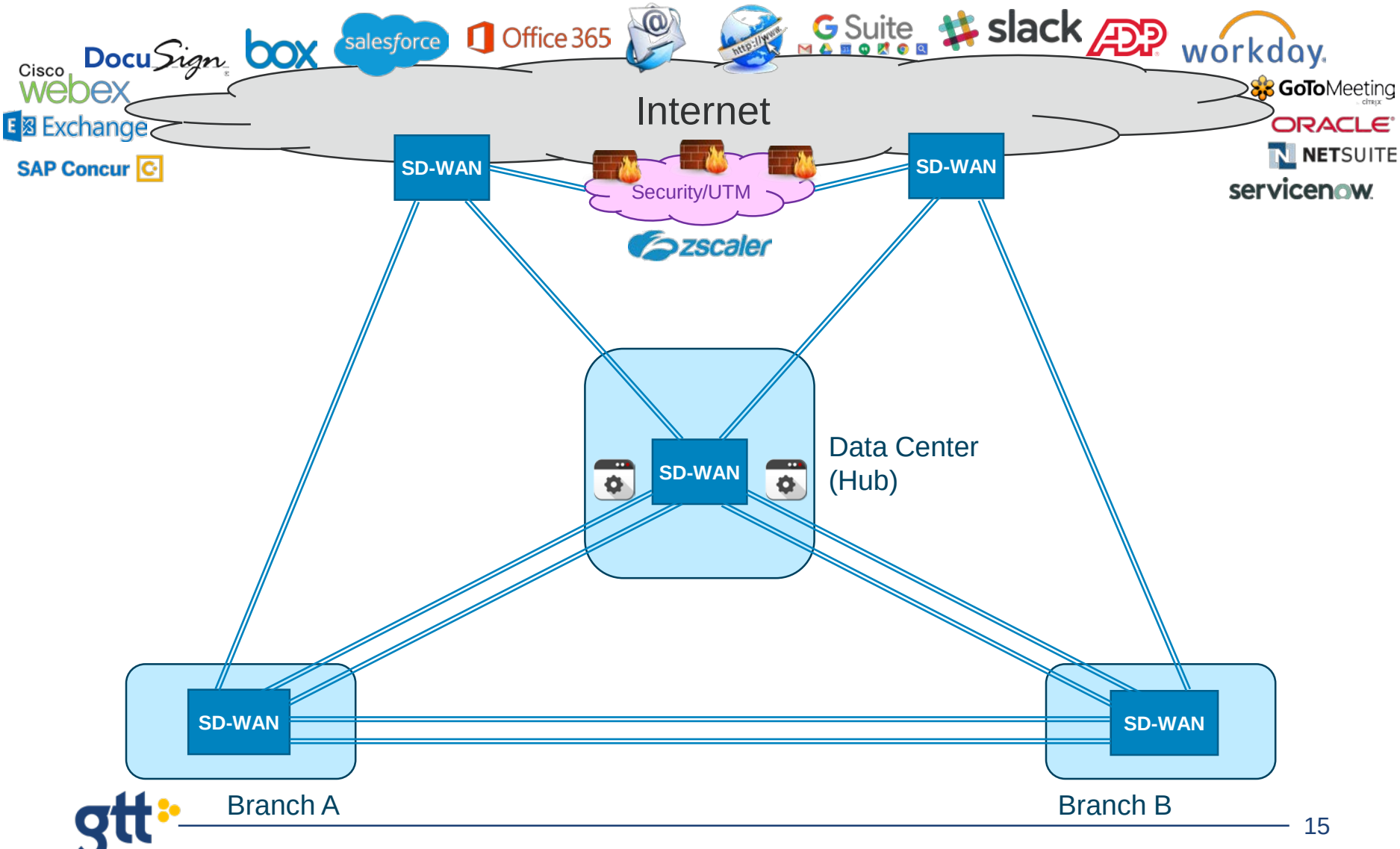
SD-WAN Internet: Cloud Gateways



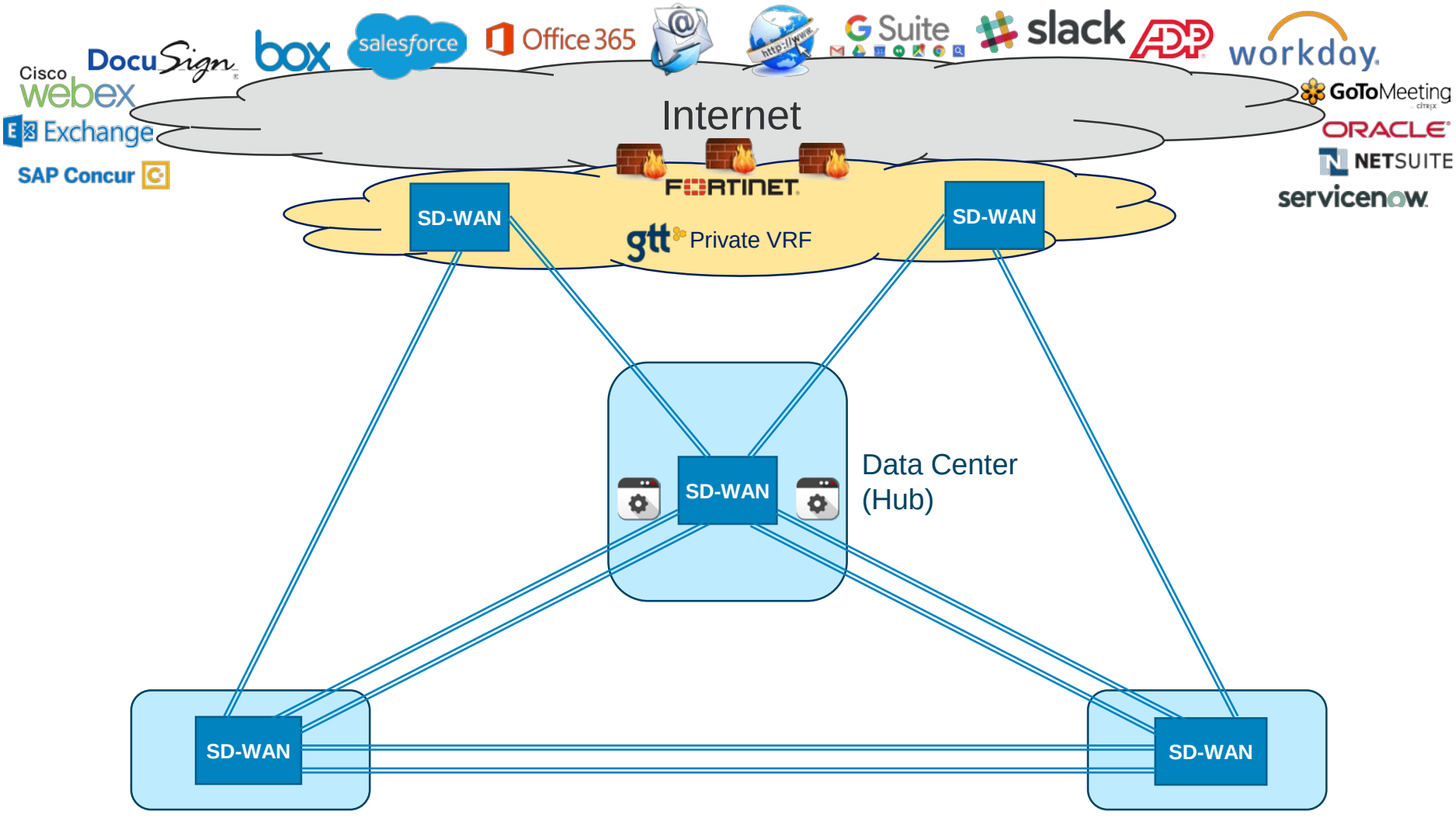
Security Perimeter in the Cloud



Cloud Based Security



GTT SD-WAN Security Model



Summary & Conclusions

- Migration to Cloud / SaaS stresses traditional WAN designs
- Hybrid WAN eases stress points but adds complexity
  - Multiple networks
  - Limited failover capabilities
  - No Internet QoS
  - Increased security perimeter
- SD-WAN harmonizes Hybrid WAN
  - Improves performance & reliability
  - Enhances visibility & control
  - Increases business agility
  - Lowers aggregate bandwidth & management costs
- SD-WAN vendors have different approaches to Internet/SaaS
  - Simple site-to-site: Internet/SaaS outside of SD-WAN
  - Split Tunnel: Internet/SaaS similar to Hybrid WAN
  - Cloud Gateways: Internet/SaaS managed via SD-WAN (best approach!)
- Cloud Gateway SD-WAN shifts security perimeter to the cloud
  - Third party cloud security solutions (e.g., Zscaler)
  - Network Service Provider cloud firewalls / UTM solutions
    - GTT offers Fortinet
- Approach to SaaS and security are key differentiators of SD-WAN solutions!