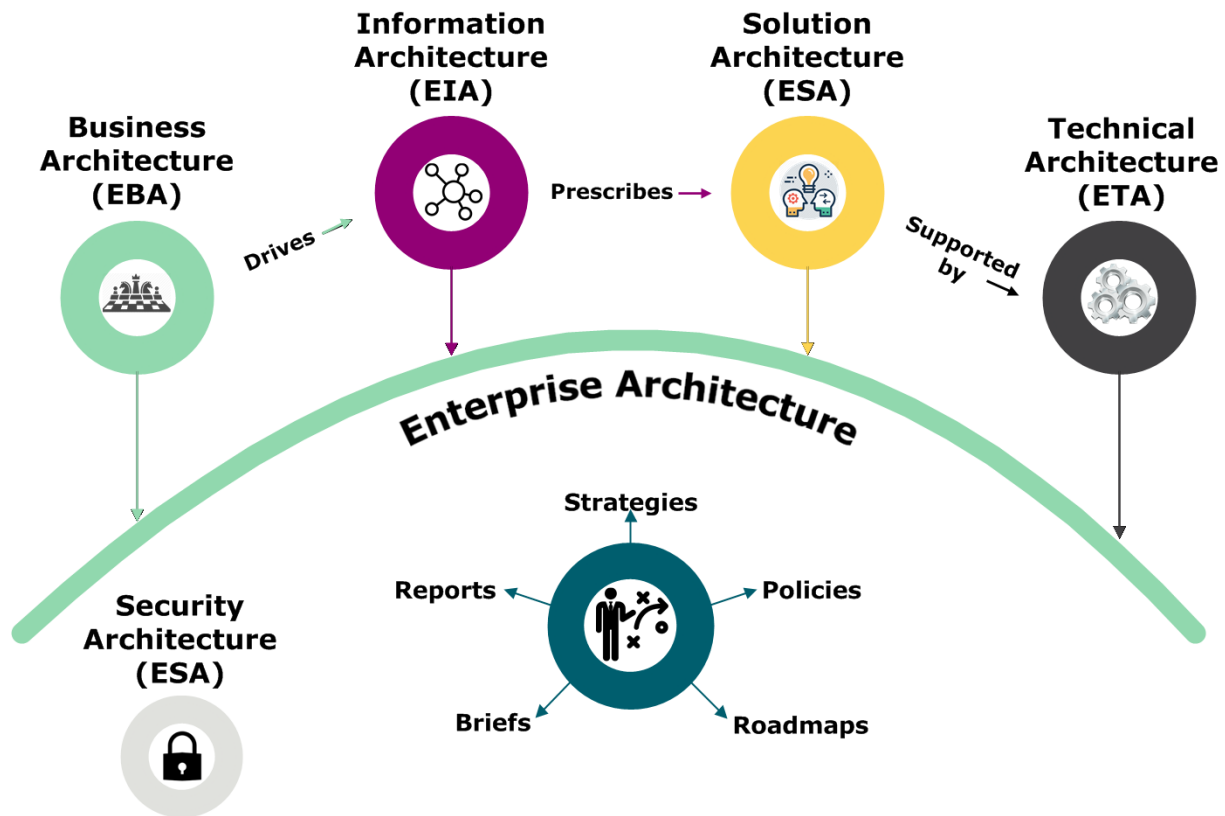


# ENTERPRISE ARCHITECTURE TECHNICAL BRIEF

## Remote Connectivity



Robert Kowalke

April 2021

# OVERVIEW

This technical brief researches remote connectivity (RC) in support of VITA enterprise architecture policies, standards, and guidelines. Research from this technical brief intends to help Commonwealth agencies make their implementation determinations regarding RC through providing needed RC background information to save research time or provide an initial overview for those who simply want to be informed quickly on RC.

As organizations expand and join an increasingly global market, the need to interconnect offices and remote locations has become essential to operations. The current internet implements this concept of making information accessible to anyone in the world, from any location. Subsequently, as technology advances, the demand and necessity for seamless connectivity and stable access to servers and networks is increasing exponentially.

A system interconnection has three basic components:

- IT system A.
- IT system B.
- The mechanism by which they are joined (the “pipe” through which data is made available, exchanged, or passed one-way only).

In the following figure, System A and System B are owned and operated by different organizations.

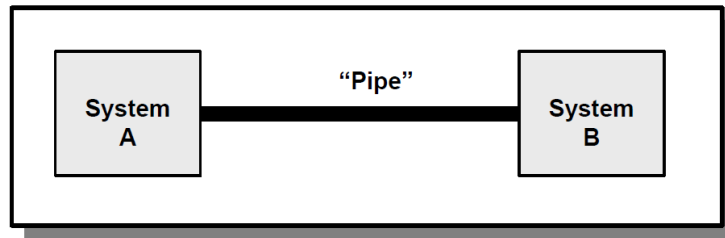


Figure 2-1: Interconnection Components

NIST SP-800-47 of August 2002

Organizations can connect their IT systems using a dedicated line that is owned by one of the organizations or is leased from a third party (e.g., an Integrated Services Digital Network [ISDN], T1, T3, or T10 line). The private or leased line is the “pipe” that connects the IT systems. In many cases, this solution is expensive, but it can provide a high level of security for the interconnected systems, because the line may be breached only through a direct physical intrusion.

A less expensive alternative is to connect systems over a public network (e.g., the Internet), using a virtual private network (VPN). A VPN is a data network that enables two or more parties to communicate securely across a public network by creating a private connection, or “tunnel,” between them. This replaces the need to rely on privately owned or leased lines.

At a fundamental level, remote connectivity access allows users to log onto networks remotely, making files and network resources available across distances such as locally, in a city, in a state, or around the world.

Remote connectivity is vital to enabling remote workers to communicate with each other and to provide redundancy in case of force majeure events that interrupt business as usual. Because of the expansion of networks today, user demands for connectivity are increasing dramatically, and those demands include the ability to connect to network resources from remote locations.

Gartner mentions:

- “I&O leaders must adapt provision of IT support as pandemics force business consumers and IT service desk analysts to work from home.” For instance, during periods of quarantine and/or lockdown, IT staff must stay away from the “office,” requiring IT service desks be staffed differently using accessible contact channels. In some cases, the unavailability of telephone-based support for business users is driving I&O leaders to offer alternative support methods that are new or have not been fully supported previously such as live chat, voice and video conferencing, and softphones/dialers (WebRTC leveraged for web-based SIP softphone if sufficient internet capacity is available for VoIP quality).
- Business consumers will come to rely on these alternative support channels after employees return to the office, which will further increase remote access bandwidth requirements. By 2023, crowdsourcing, work at home (WAH), telecommuting, and the gig economy will account for 35% of the customer service workforce, up from 5% in 2017, driven by changing labor practices and business continuity planning.

This technical brief is located on the EA Library web page at the following link:

<https://www.vita.virginia.gov/policy-governance/enterprise-architecture/ea-library/>

For any comments, questions, and/or concerns with this technical brief, please contact VITA EA:  
ea@vita.virginia.gov

**OVERVIEW** ..... 2

**REMOTE CONNECTIVITY TECHNOLOGY RESEARCH** ..... 5

**REMOTE CONNECTIVITY METHODS** ..... 6

*Tunneling*..... 6

*Portals* ..... 7

*Remote desktop access* ..... 9

*Direct application access* ..... 10

**REMOTE CONNECTIVITY SOLUTIONS**..... 12

*Secure Access Service Edge (SASE)* ..... 13

*Cloud Access Security Broker (CASB)* ..... 21

*Zero Trust Network Access (ZTNA)* ..... 23

*Software Defined Networking (SDN)* ..... 26

*Virtual Private Network (VPN)* ..... 27

*Multi-protocol Label Switching (MPLS) VPNs* ..... 32

**REMOTE CONNECTIVITY REQUIREMENT CONSIDERATIONS** ..... 35

*Remote Site Connectivity to Enterprise WAN*..... 39

**ENTERPRISE REMOTE CONNECTION SERVICE (ERCS)** ..... 41

*ERCS Architecture* ..... 42

*Network Services* ..... 43

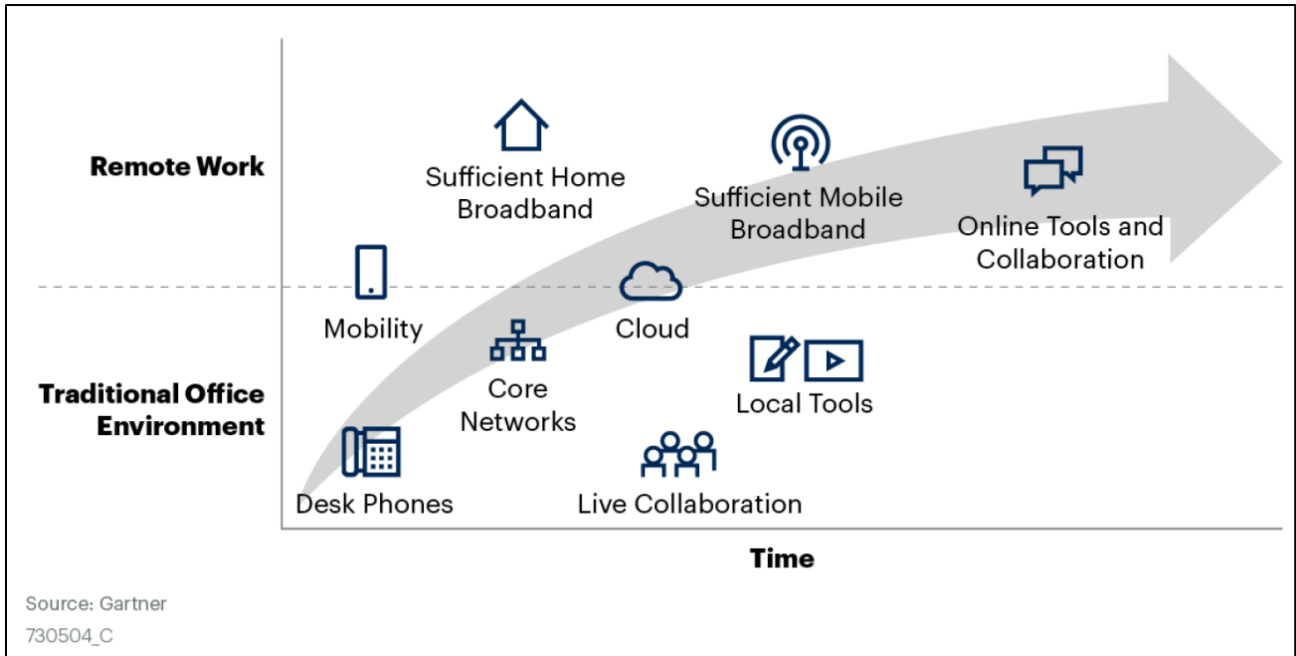
**TELEWORK CLIENT DEVICE SECURITY** ..... 44

**REMOTE CONNECTIVITY PICTORIAL RESEARCH** ..... 46

**APPENDIX A: GLOSSARY** ..... 127

**COV ITRM GLOSSARY:**..... 127

**TERMS DERIVED FROM OTHER VITA DOCUMENTS OR ACCEPTED GLOSSARIES:** ..... 127



**Work at home is driving increased internet-based traffic. Gartner – November 2020**



## Remote Connectivity Methods **1 2 3 4 5 6**

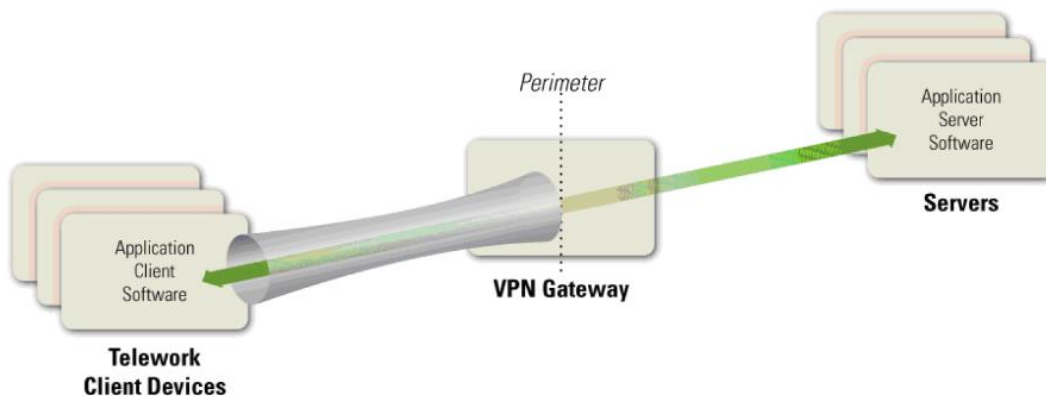
The remote access methods most commonly used for remote workers as divided into four categories based on their high-level architectures:

### Tunneling

Tunnels use cryptography to protect the confidentiality and integrity of transmitted information between the client device and VPN gateway. Tunnels can also authenticate users, provide access control (such as restricting which protocols may be transmitted or which internal hosts may be reached through remote access), and perform other security functions. Tunneling does not provide any protection for communications between the VPN gateway and internal resources.

The types of VPNs most commonly used for remote workers are Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) tunnels. Tunneling by using Secure Shell (SSH) is less commonly used, and is often considered more difficult to configure and maintain than IPsec or SSL tunnel VPNs.

Different tunneling systems can tunnel various protocols; for example, IPsec has standardized extensions that allow it to tunnel Layer 2 protocols such as the Point-to-Point Protocol (PPP) and Multiprotocol Label Switching (MPLS). In general, almost any communication encryption protocol can be made to tunnel almost any layer.



### Tunneling Architecture

<sup>1</sup> Mike Meyers' CompTIA Network+ Guide to Managing and Troubleshooting Networks, Chapter 14 - Remote Connectivity. March 10, 2015.

<sup>2</sup> Remote Connectivity, April 9, 2020. <https://sourcedaddy.com/networking>

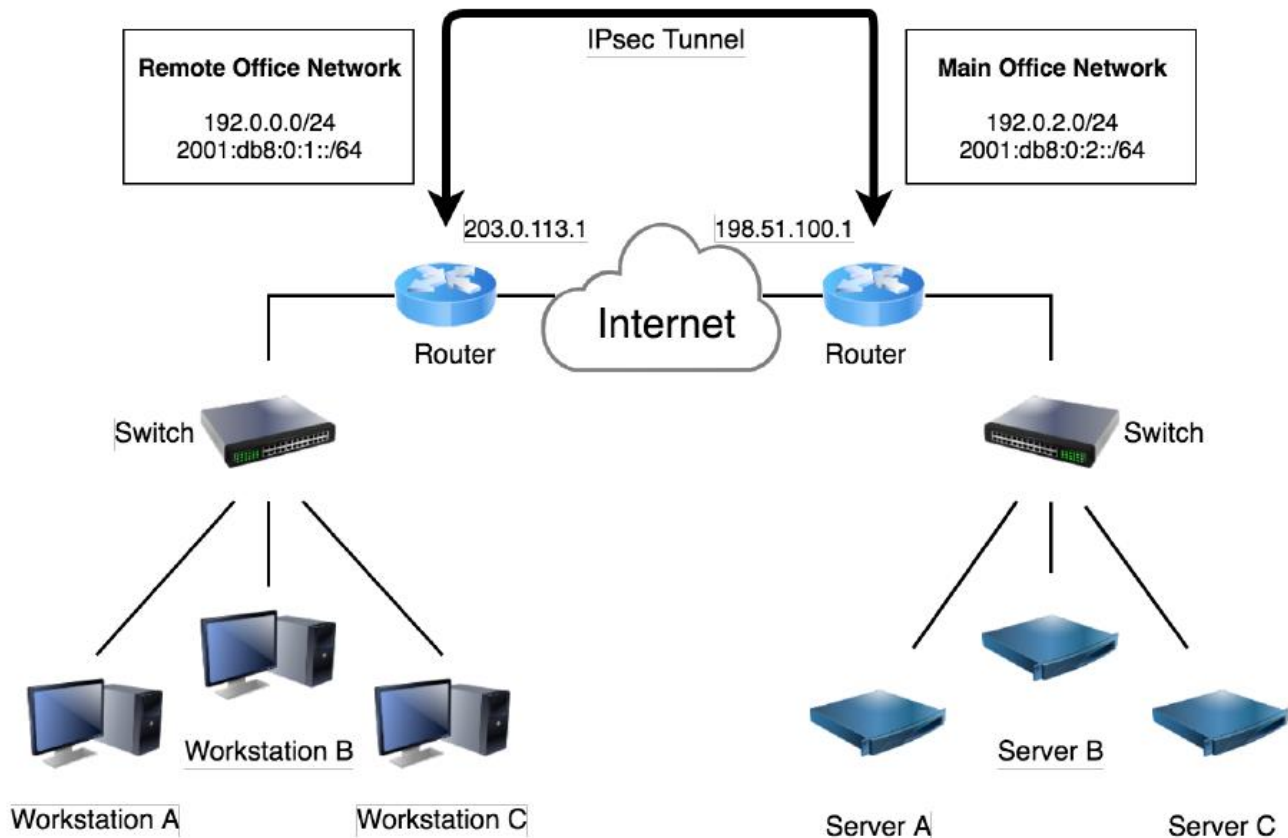
<sup>3</sup> Running an Effective IT Service Desk During and After a Pandemic. Gartner ID G00724378 of April 17, 2020.

<sup>4</sup> Security Guide for Interconnecting Information Technology (IT) Systems. Recommendations of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, August 2002.

<sup>5</sup> Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, July 2016. <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>

<sup>6</sup> Guide to IPsec VPNs. NIST Special Publication 800-77, Revision 1, Draft. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. July 2019. <https://doi.org/10.6028/NIST.SP.800-77r1-draft>

The VPN gateway can control access to the parts of the network and the types of access that the remote worker gets after authentication. For example, a VPN might allow a user to only have access to one subnet, or to only run particular applications on certain servers on the protected network. VPNs are usually established and managed by VPN gateway devices owned and managed by the organization being protected.



**Gateway-to-Gateway VPN for Remote Office Connectivity.**

## Portals

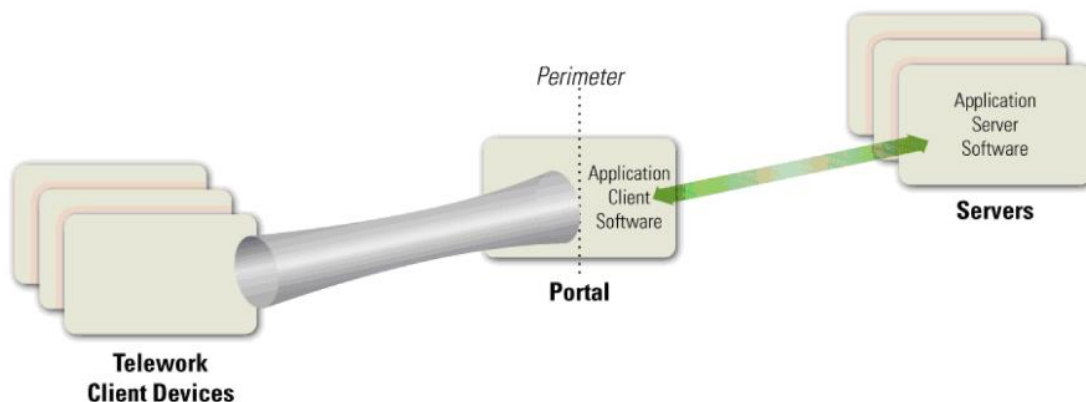
A portal is a server that offers access to one or more applications through a single centralized interface. A remote worker uses a portal client on a telework client device to access the portal. Most portals are web-based, which means for the remote worker, the portal client is a regular web browser. The application client software is installed on the portal server, and it communicates with application server software on servers within the organization. The portal server communicates securely with the portal client as needed.

In terms of security, portals have most of the same characteristics as tunnels: portals protect information between client devices and the portal, and they can provide authentication, access control, and other security services. However, there is an important difference between tunnels and

portals—the location of the application client software and associated data. In a tunnel, the software and data are on the client device; in a portal, they are on the portal server. A portal server transfers data to the client device as rendered desktop screen images or web pages, but data is typically stored on the client device much more temporarily than data for a tunneled solution is. Portals limit the access a remote worker has to particular application clients running on the portal itself. Those applications further limit the access the remote worker has to servers inside the network.

There are a few types of portal solutions commonly used for remote access:

1. **Web-based portal** – provides a user with access to multiple web-based applications from a single portal website. An SSL portal VPN is a common form of web-based portal.
2. **Terminal server access** – gives each remote worker access to a separate standardized virtual desktop. The terminal server simulates the look and feel of a desktop operating system and provides access to applications. Terminal server access requires the remote worker either to install a special terminal server client application on the client device or to use a web-based interface, often with a browser plug-in or other additional software provided by the organization.
3. **Virtual desktop infrastructure (VDI)** – involves the user connecting to a system that contains virtual images of standardized, non-simulated operating systems and desktops. When the remote worker is finished with a remote access session, the virtual image is discarded so that the next user will have a clean virtual desktop. VDI is particularly helpful for safeguarding telework on BYOD and third-party-controlled devices, which are more likely than organization-issued devices to not meet the organization’s security requirements.



### Portal Architecture (aka Application Portals)

Interface mechanisms vary among portals:

- Terminal server access and VDI present a standardized virtual desktop to the remote worker and are primarily meant for PCs
- SSL portal VPNs present each application through a web page
- Virtual mobile infrastructure (VMI) delivers a secure virtual mobile device environment to a



telework mobile device.

It is important to understand that VPNs do not remove all risk from networking. While VPNs can greatly reduce risk, particularly for communications that occur over public networks, they cannot eliminate all risk for such communications.<sup>7</sup>

## Remote desktop access

Remote desktop access gives a remote worker the ability to remotely control a particular PC located at the organization, most often the user's own computer at the organization's office, from a telework client device. The remote worker has keyboard and mouse control over the remote computer and sees that computer's screen on the local telework client device's screen. Remote desktop access allows the user to access all of the applications, data, and other resources that are normally available from their PC in the office. A remote desktop access client program or web browser plug-in is installed on each telework client device, and it connects directly with the remote worker's corresponding internal workstation on the organization's internal network.

There are two major styles of remote desktop access:

1. Direct between the telework client and the internal workstation

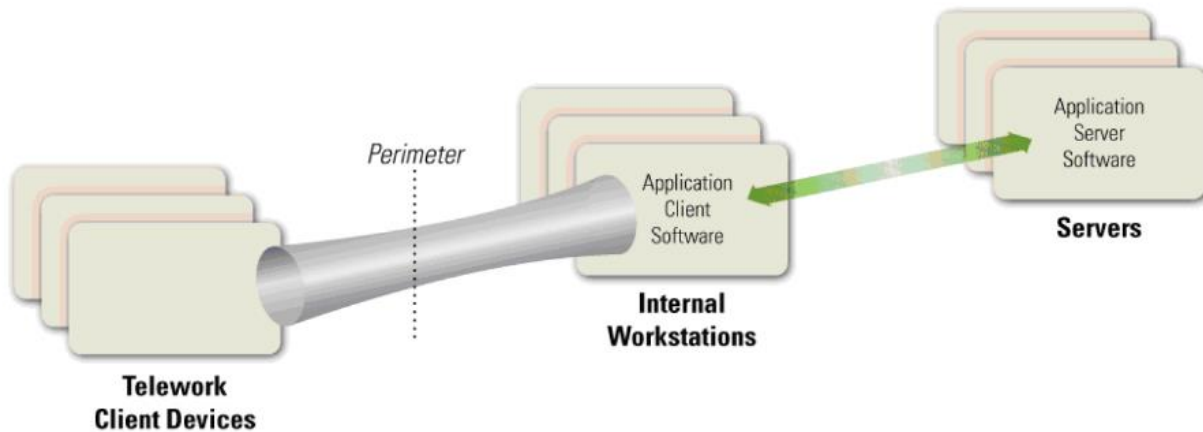
Direct access is often not possible because it is prevented by many firewalls. For example, if the internal workstation is behind a firewall performing network address translation (NAT), the telework client device cannot initiate contact with the internal workstation unless either the NAT allows such contact, or the internal workstation initiates communications with the external telework client device (e.g., periodically checking with the client device to see if it wants to connect).

2. Indirect through a trusted intermediate system

Indirect remote desktop access is performed through an intermediate server. This server is sometimes part of the organization's firewall, but is more often run by a trusted commercial or free third-party service outside the organization's network perimeter. Usually there are separate connections between the telework client device and the service provider, and between the service provider and the internal workstation, with the intermediate server handling the unencrypted communications between the separate connections. The security of this intermediate server is very important, because it is responsible for properly authenticating remote workers and preventing unencrypted traffic from being accessed by unauthorized parties. Also, if the organization's security policy requires particular kinds of authentication (such as the two-factor authentication required by federal agencies), the intermediate server should support this authentication in both directions.

---

<sup>7</sup> Guide to SSL VPNs - Recommendations of the National Institute of Standards and Technology (NIST). Special Publication (SP) 800-113, July 2008. <https://csrc.nist.gov/publications/detail/sp/800-113/final>



### Remote Desktop Access Architecture

Remote desktop access software protects the confidentiality and integrity of the remote access communications and also authenticates the user to ensure that no one else connects to the internal workstation. However, because this involves end-to-end encryption of the communications across the organization’s perimeter, the contents of the communication are hidden from the network security controls at the perimeter, such as firewalls and intrusion detection systems. For many organizations, the increased risk caused by this is not worth the benefits, and direct connections from external client devices to internal workstations are prohibited.

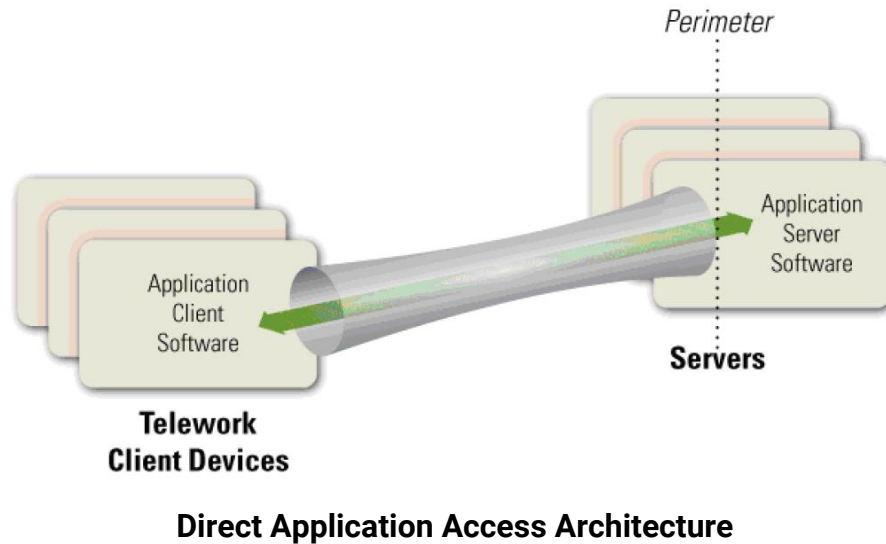
Another serious security issue with remote desktop access software is that it is decentralized; instead of the organization having to secure a single VPN gateway server or portal server, the organization instead has to secure each internal workstation that may be accessed through remote desktop access. Because these internal workstations can be accessed from the Internet, either directly or indirectly, they generally need to be secured nearly as rigorously as full-fledged remote access servers, yet such workstations were usually not designed with that degree of security in mind. Applying compensating controls for each workstation to raise its security to an acceptable level often involves a significant amount of time and resources, as well as acquisition of additional security controls. Also, authentication solutions such as two-factor authentication capabilities may need to be deployed to each internal workstation using remote desktop access.

Generally, remote desktop access solutions, such as those using the Microsoft Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC), should only be used for exceptional cases after a careful analysis of the security risks. The other types of remote access solutions described in this section offer superior security capabilities.

### Direct application access

Remote access can be accomplished without using remote access software. A remote worker can access an individual application directly, with the application providing its own security (communications encryption, user authentication, etc.) The application client software installed on

the telework client device initiates a connection with a server, which is typically located at the organization’s perimeter (e.g., in a demilitarized zone [DMZ]) or in an Internet-facing cloud architecture.



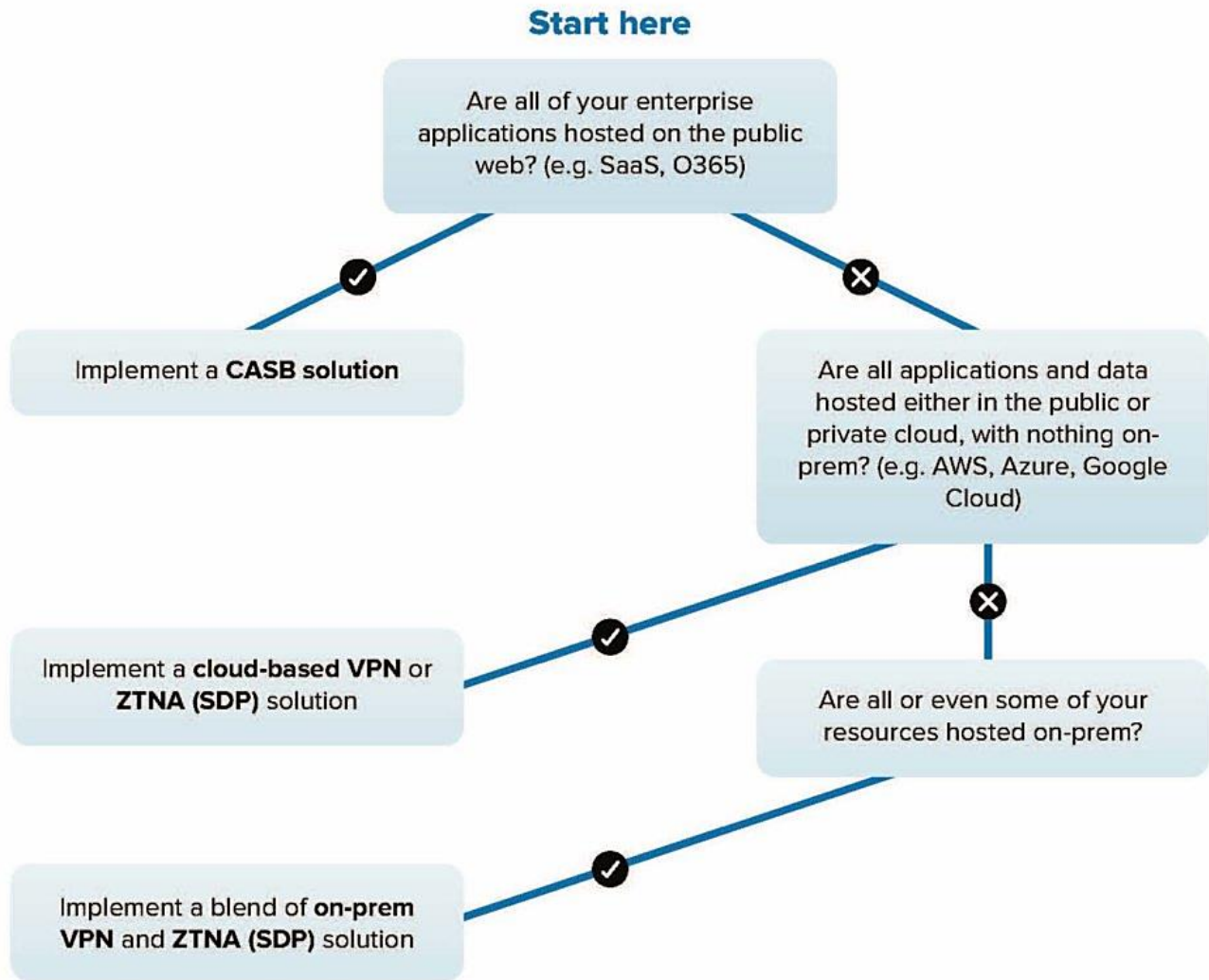
Examples of direct application access:

- Webmail. The remote worker runs a web browser and connects to a web server that provides email access. The web server runs HTTP over TLS (HTTPS) to protect the communications, and the webmail application on the server authenticates the remote worker before granting access to the remote worker’s email. For cases such as webmail that use a ubiquitous application client (e.g., a web browser), direct application access provides a highly flexible remote access solution that can be used from nearly any client device.
- Smartphone app (client software) that connects to a service provided by one of the organization’s servers through HTTPS.

For the same reasons discussed in the remote desktop access section, the direct application access architecture is generally only acceptable if the servers accessed by the remote workers are located on the organization’s network perimeter or in a public-facing cloud, and not internal networks. Many organizations choose to provide direct application access to only a few lower-risk applications that are widely used, such as email, and use tunnel or portal methods to provide access to other applications, particularly those that would be at too much risk if they were directly accessible from the Internet.

## Remote Connectivity Solutions

The intent of this section is to provide example RC solutions and a quick overview for that solution.



### Solving the Challenges of Modern Remote Access by Gartner.

CASB = Cloud Access Security Broker; SDP = Software Defined Perimeter;  
VPN = Virtual Private Network; ZTNA = Zero Trust Network Access

**Secure Access Service Edge (SASE)** <sup>8 9 10 11 12 13 14 15</sup>

SASE (secure access service edge) is an emerging architecture that delivers a seamless and secure connection to applications in any environment from anywhere while streamlining networking and security functions for IT.

Per Cisco, Gartner describes SASE in terms of five primary functions:

- Software-defined wide area networking (SD-WAN)
- Firewall as a service (FWaaS)
- Secure web gateway (SWG)
- Cloud access security broker (CASB)
- Zero trust network access (ZTNA)



General SASE statements:

- SASE converges cloud networking and cloud security to deliver flexibility, agility, security and scale for enterprises of all sizes.
- SASE is a cloud-based security model that combines SD-WAN with core network security services and delivers them on the cloud edge – most SASE offerings are characterized by five primary capabilities as a starting point: 1) Building and Managing Networks; 2) Filtering Traffic; 3) Connecting Users to Applications; 4) Protecting Applications and Infrastructure; 5) Securing Data.
- Users are moving to “everywhere.”
- Current centralized security solutions no longer make sense.
- SASE coined by Gartner in 2019.
- Motivation comes from the keywords – simple, flexible, secure, and agile.
- Convergence of network services (secure WAN, CASB, FW onto a unified single broker fabric)
- Cloud native “as a service” model.
- Enables secure communication by using Virtual point-to-point connection.

<sup>8</sup> How SASE can help move securely from the PSN - December 9, 2020. VMware and Breeze Networks. Retrieved March 15, 2021 from slideshare.net.

<sup>9</sup> My Perspective of Enterprise Network Services by Nagarai Shenoy of Juniper Networks, June 14, 2020. Retrieved March 15, 2021 from slideshare.net.

<sup>10</sup> Zscaler SASE at a glance. Retrieved March 17, 2021 from zscaler.com/gartner-secure-access-service-edge-sase.

<sup>11</sup> Modeling SASE with Categories and Prioritization Levels, by Ian Flaherty - February 2021. Gartner Community. Retrieved March 19, 2021 from <https://community.gartner.com/t/do-you-have-any-recommendations-while-building-sase-strategy-roadmap/281030/7>

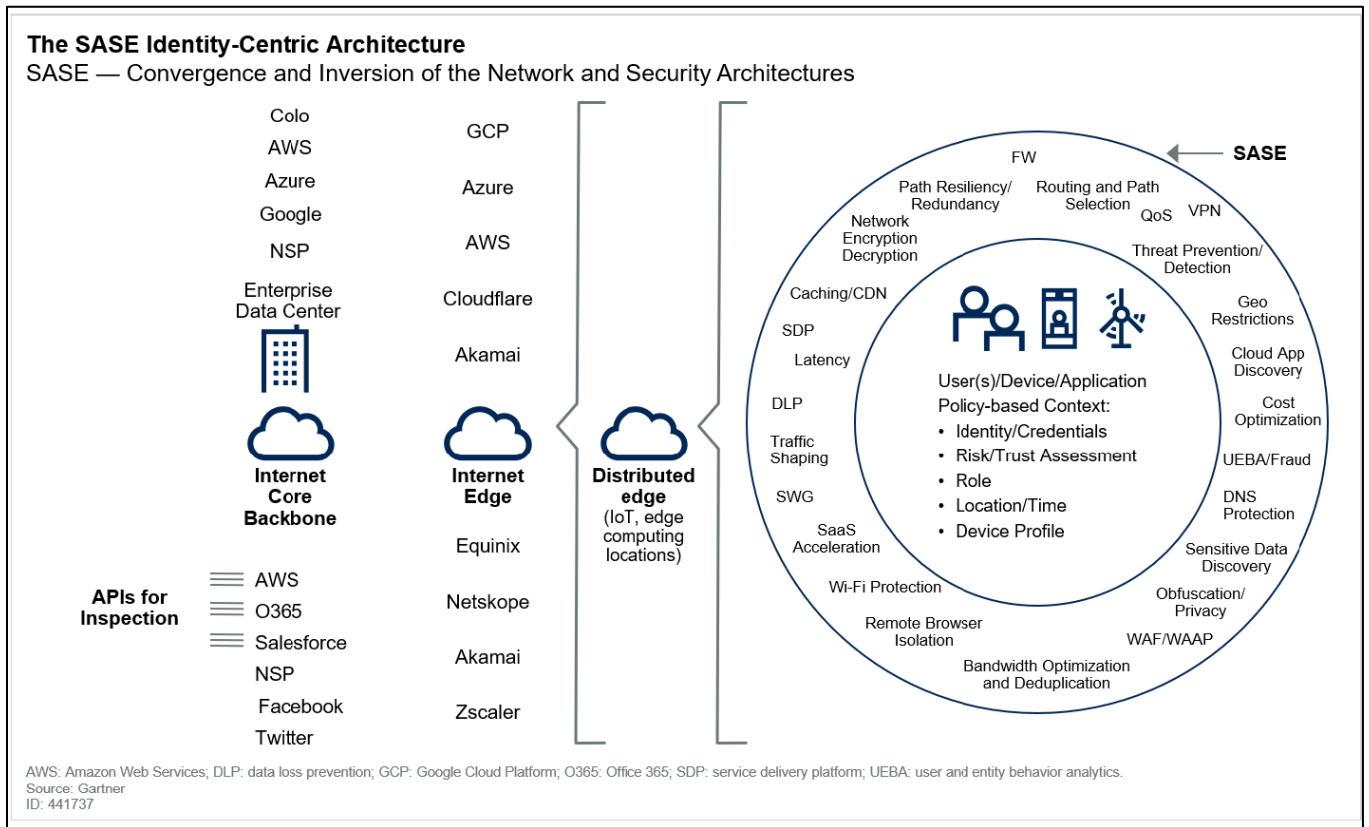
<sup>12</sup> Magic Quadrant for WAN Edge Infrastructure - September 23, 2020. Gartner ID-G00465582.

<sup>13</sup> Getting started with SASE: A guide to secure and streamline your network infrastructure - Whitepaper by CloudFlare. November 11, 2020.

<sup>14</sup> Six Considerations for Your SASE Setup by CloudFlare. Retrieved from the Gartner Asia-Pacific (APAC) Security & Risk Management Summit held March 23-24, 2021 in Australia.

<sup>15</sup> Secure Access Service Edge (SASE) At a Glance by Cisco SECURE. Retrieved from the Gartner Asia-Pacific (APAC) Security & Risk Management Summit held March 23-24, 2021 in Australia.

- Encrypts traffic between the two end-points over a shared public network (such as internet).
- Enables remote access to the organization resources in a secure manner.
- Most basic, cost effective, and reliable solution.
- Most common application is remote access (that enables working-from-home today).
- Limited scalability – as users increase, solution can get complex.
- Focus is on connecting endpoints to centralized cloud.
- SASE appears to be a logical evolution path for SD-WAN.
- By 2024, to enhance agility and support for cloud applications, 60% of enterprises will have implemented SD-WAN, compared with about 30% in 2020.
- By 2024, more than 60% of software-defined, wide-area network (SD-WAN) customers will have implemented a SASE architecture, compared with about 35% in 2020.



**SASE Identity-Centric-Architecture – Gartner**

Some SASE roadmap modeling considerations in order of priority:

User Ingress – In this set, the following components are:

- MFA
- Federated Identity
- Zero trust services and network - (note - this can be the same as SD WAN or different)
- Device Posture
- End Point Protection, EDR
- UEBA
- Deception-aaS
- Sensitive data discovery

Network – The interconnection technologies that provide data and application flows throughout the hybrid compute environments. In this set, the following components are:

- SD WAN
- Application Microsegmentation
- WAN Optimization
- Service provider peering

User Egress SASE controls – Those capabilities that help users gain access to services anywhere on the internet in a secure manner. In this set, the following components are:

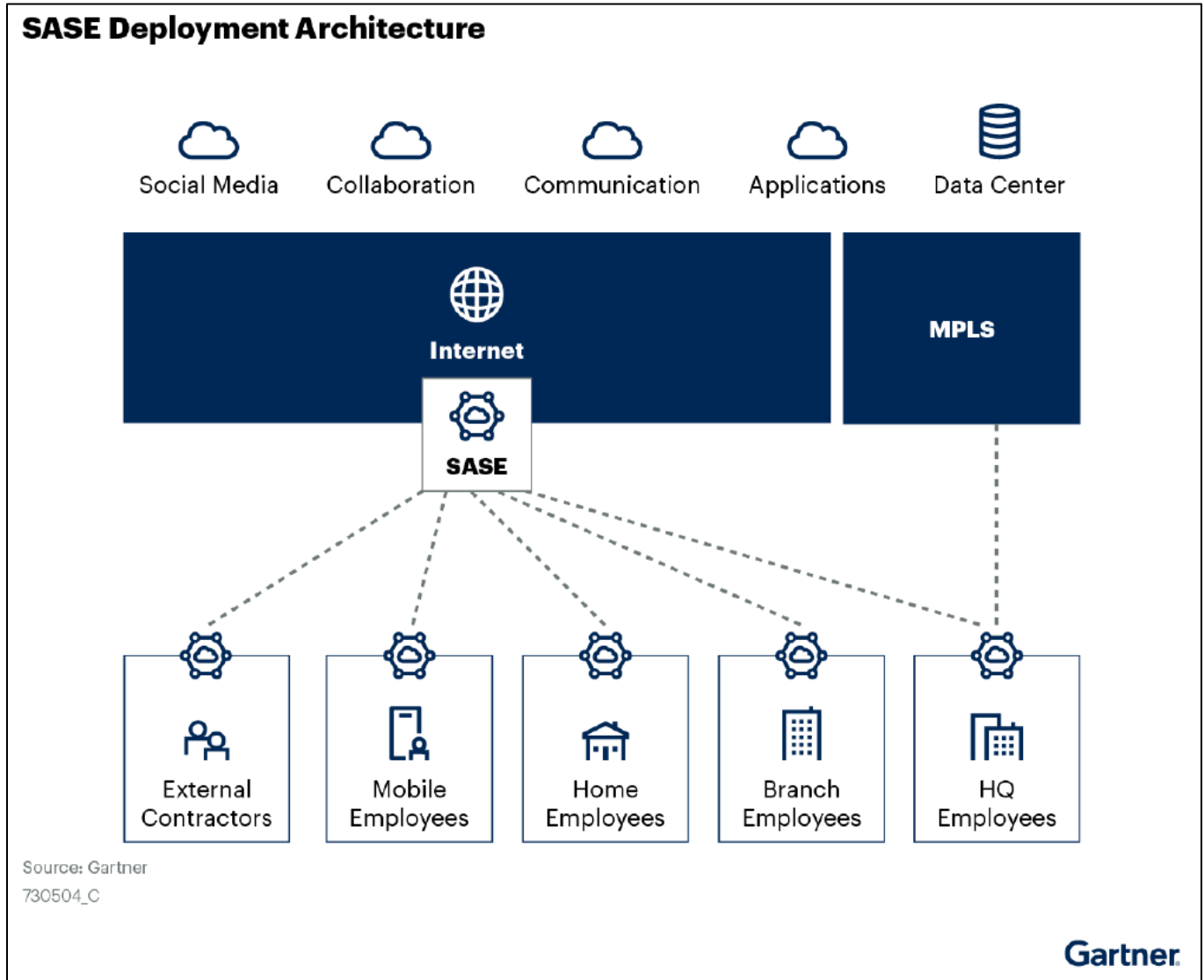
- CASB (Cloud Access Security Broker)
- SWG (Secure Web Gateway)
- RBI
- Sensitive data discovery

Ingress SASE controls – Provide access from outside to internal applications within the extended enterprise. Ingress is worth splitting into two elements to provide a division of context for us as a publisher.

Customer Ingress – In this set, the following components are:

- WAF (Web Application Firewall)
- WAAP (Web Application & API Protection)
- CDN (Content Delivery Network)
- FWaaS / NGFWaaS
- Access control services
- IDS (Intrusion Detection System)
- DeceptionaaS

- Sensitive data discovery



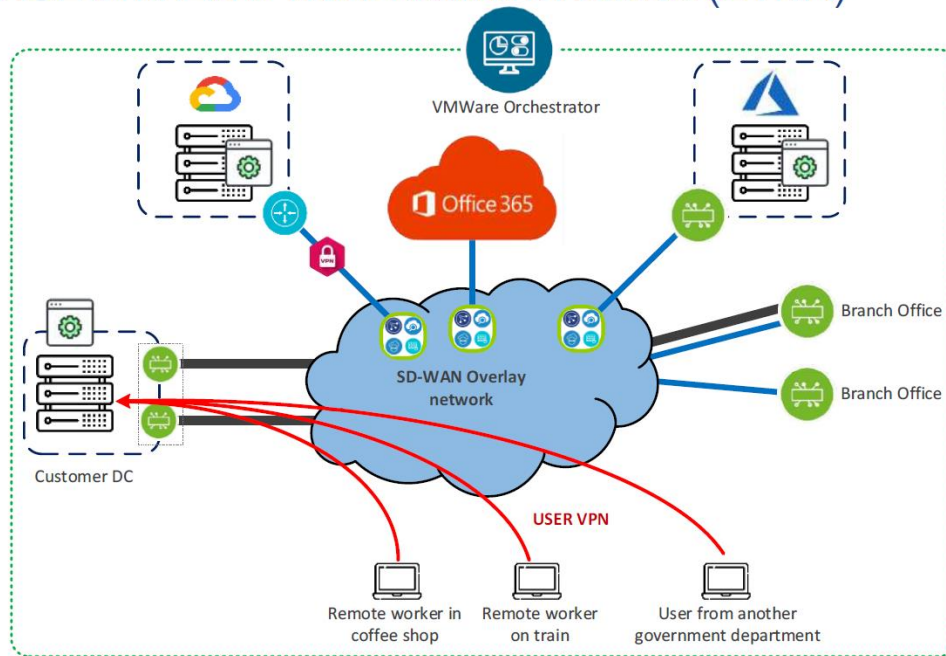
**SASE Deployment Architecture. Gartner ID 730504C of November 5, 2020.**

- Pascal Heger, Global Network Architect in California via Gartner mentions they treat SASE as “Zero Trust Networking”. Neither can be addressed with a single product / solution / vendor, and are more of a best-practices philosophy. You can measure yourself against them to identify gaps or areas of improvement within the organization based on the framework. We are 200% SD-WAN implemented - meaning, all our sites have been on SD-WAN since 2016, and have since continued to evolve our SD-WAN into the cloud. Our network has been extended into the cloud globally in order to connect to spoke VPC’s, provide secure internet egress, provide Business Partner Connectivity, terminate Employee SSL VPN, etc.



- Most SASE solutions, however, share several key advantages over on-premise and hybrid network security configurations:
  - Streamlined implementation
    - By consolidating networking and security services, SASE eliminates the need to onboard cloud-based services, set up on-premise appliances, and invest time, money, and internal resources to keep both updated against the latest threats.
  - Simplified policy management
    - SASE allows organizations to set, monitor, adjust, and enforce access policies across all locations, users, devices, and applications.
    - Attacks and incoming threats can be identified and mitigated from a single portal, rather than individually monitored and managed with multiple single-purpose security tools.
  - Identity-based network access
    - SASE leans heavily on a zero trust security model, in which user identity and access is granted based on a combination of factors:
      - user location
      - time of day
      - enterprise security standards
      - compliance policies
      - and an ongoing evaluation of risk/trust
    - This level of security – a significant step up from the overly permissive and inherently vulnerable VPN – protects against both external and internal data breaches and other attacks.
  - Reduced latency
    - SASE reduces latency and improves performance by routing network traffic across an expansive edge network in which traffic is processed as close to the user as possible. Routing optimizations can help determine the fastest network path based on network congestion and other factors.
  - Global network
    - A SASE framework is constructed on top of a single global network, enabling organizations to expand their network perimeter to any remote user, branch office, device, or application and gain more visibility and control across their entire network infrastructure.

## VMWare SASE and Zero Trust Network Access (ZTNA)



vmware

breezenetworks

### VMware SASE and ZTNA – December 2020

- Here are six steps that will guide you through the first stage of your SASE journey:
  - 1) Evaluate your network traffic.
    - a) Before you implement any SASE solution, conduct a full assessment of where your users work, what applications they access, and which network and security resources they interface with most frequently.
      - (1) Then, you can start to determine the level of privilege and access that should be applied to your workforce on a role-by-role basis.
    - b) Assess your total application landscape.
    - c) Once you know where your users are and what degree of network access they require, it is time to decide which applications to bring into a SASE framework first.
    - d) Evaluate these on the axes of total data sensitivity and breadth of employee impact.
    - e) Consider prioritizing access control for applications with broader adoption and usage, as well as more stringent security requirements.
  - 2) Prioritize your remote workers.
    - a) A network is only as strong as its weakest endpoint – in this case, employees who access your network from remote locations and unsecured devices.

- b) Equip your remote workforce with cloud-based firewalls and zero trust access control so they can safely access your network from any location and device.
- 3) Reimagine your branch offices.
  - a) After you secure your remote workforce with a SASE framework, find ways to strengthen the security of your smaller branch offices.
    - (1) This may be as simple as replicating the model used for remote workers and allowing local offices to function as an Internet café.
  - b) By routing network traffic to a SASE solution, you can ensure firewalls and logging remain consistent for all employee devices connecting to the Internet.
- 4) Extend SASE to high-density locations.
  - a) Unlike smaller branch offices, high-density offices will likely have SD-WAN solutions, cloud firewalls, and other network protections in place.
  - b) However, this is still the most complicated phase of SASE adoption, since legacy on-premise security tools will need to be carefully migrated to the cloud, while the volume and diversity of employee access requirements must be thoughtfully considered and managed.
- 5) Identify areas for improvement.
  - a) Although many cloud providers are on their way to offering the five core components of a true SASE solution, some may have gaps in their product suites.
  - b) Evaluate vendors on the breadth of their current SASE offering, while keeping an eye out for any critical additions and security integrations that may be included in the future.

<b>SASE Services</b>		
<b>Core features:</b>	<b>Recommended:</b>	<b>Optional:</b>
<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• SWG</li> <li>• CASB</li> <li>• ZTNA</li> <li>• FWaaS</li> <li>• Sensitive data and malware</li> <li>• Line rate operation</li> </ul>	<ul style="list-style-type: none"> <li>• WAAP</li> <li>• Remote browser isolation</li> <li>• Network sandbox</li> <li>• DNS protection</li> <li>• API-based access to SaaS for data context</li> <li>• Supports managed and unmanaged devices</li> </ul>	<ul style="list-style-type: none"> <li>• Wi-Fi hot spot protection</li> <li>• Network obfuscation or dispersion</li> <li>• Legacy VPN</li> <li>• Edge compute protection</li> </ul>

**Gartner**

**SASE Services - Neil MacDonald – Gartner - March 2021.**

The Future of Network Security is in the Cloud: Introducing the Secure Access Service Edge (SASE).

### Sample SASE Vendor Landscape by Gartner:

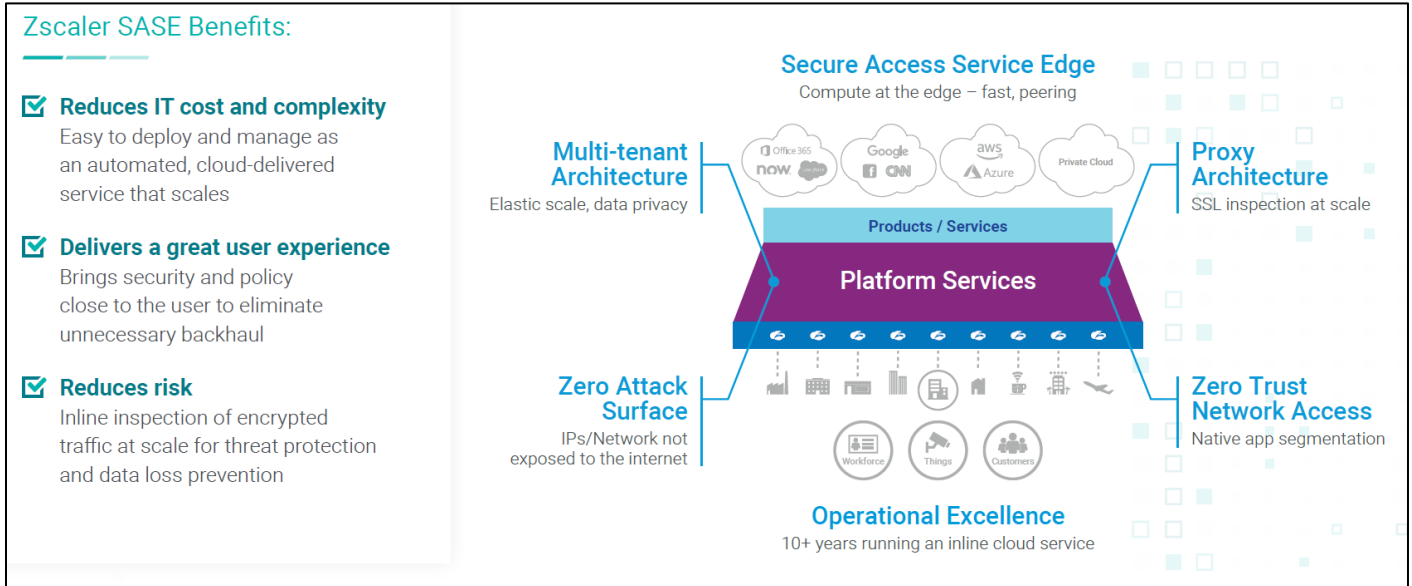
- Akamai
- Barracuda
- Cato Networks
- Cisco
- Cloudflare
- Forcepoint
- Fortinet OPAQ
- iboss
- McAfee
- Broadcom Symantec
- Netskope
- Open Systems
- Palo Alto Networks
- Proofpoint
- Versa Networks
- VMware
- Zscaler

To assist the commonwealth in this new world of remote work that we find ourselves in, VITA has had to make some rapid adjustments to our infrastructure to increase the capacity and bandwidth for remote work and has increased our service offerings to include tools that will enhance the remote work experience. Specifically, VITA upgraded our infrastructure to support upwards of 30,000 users on VPN from 5000, and upgrading our internet circuits. In addition, the following services have been implemented or are in the process of being deployed for agencies now:

- Zscaler Private Access (ZPA), which is known as VITA Secure Remote Access (VSRA) is an application-level product that allows secure access to applications, data and file shares without connecting to VPN. (VSRA), allows applications to securely communicate with VITA hosted systems through an application level secure tunnel without the need for a VPN connection. This service provides users the ability to access essential applications from anywhere. <sup>16</sup>

---

<sup>16</sup> VITA IT Strategic Plan 2020-2022 v4.0.



**Zscaler SASE Benefits – 2019**

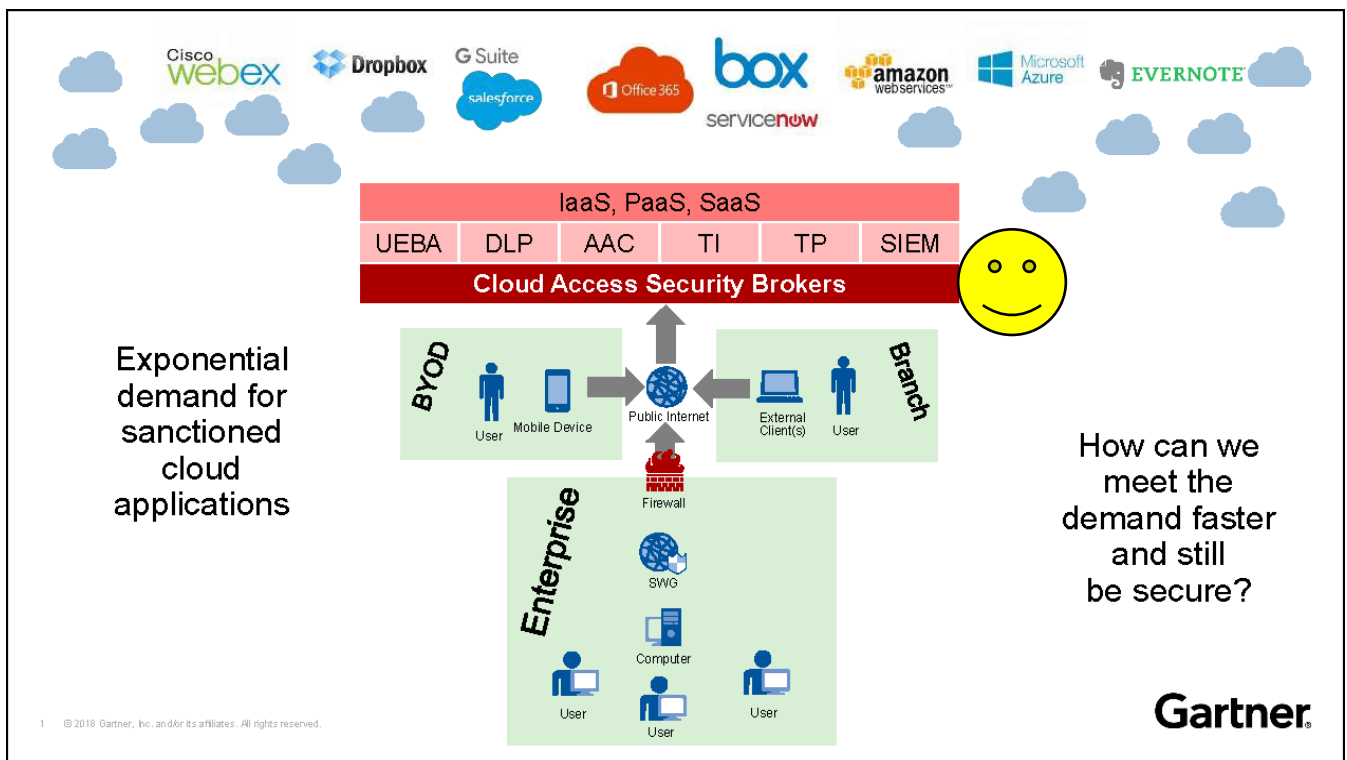
**Cloud Access Security Broker (CASB) <sup>17</sup> <sup>18</sup>**

- Accelerates safe adoption of cloud
- Provides cloud application visibility and in-line protection
- Cloud-based UEBA, DLP, AAC, TI, ATP, and SIEM
  - UEBA = User Entity Behavior Analytics
  - DLP = Data Loss Prevention
  - AAC = Adaptive Access Control
  - TI = Threat Intelligence
  - ATP = Advanced Threat Protection
  - SIEM = Security Information and Event Management
- Example things you can do with a CASB:
  - Apply consistent policy across multiple SaaS applications

<sup>17</sup> CASB = (UEBA + DLP + AAC + TI + ATP + SIEM) for SaaS and IaaS, by Ramon Krikken of Gartner.

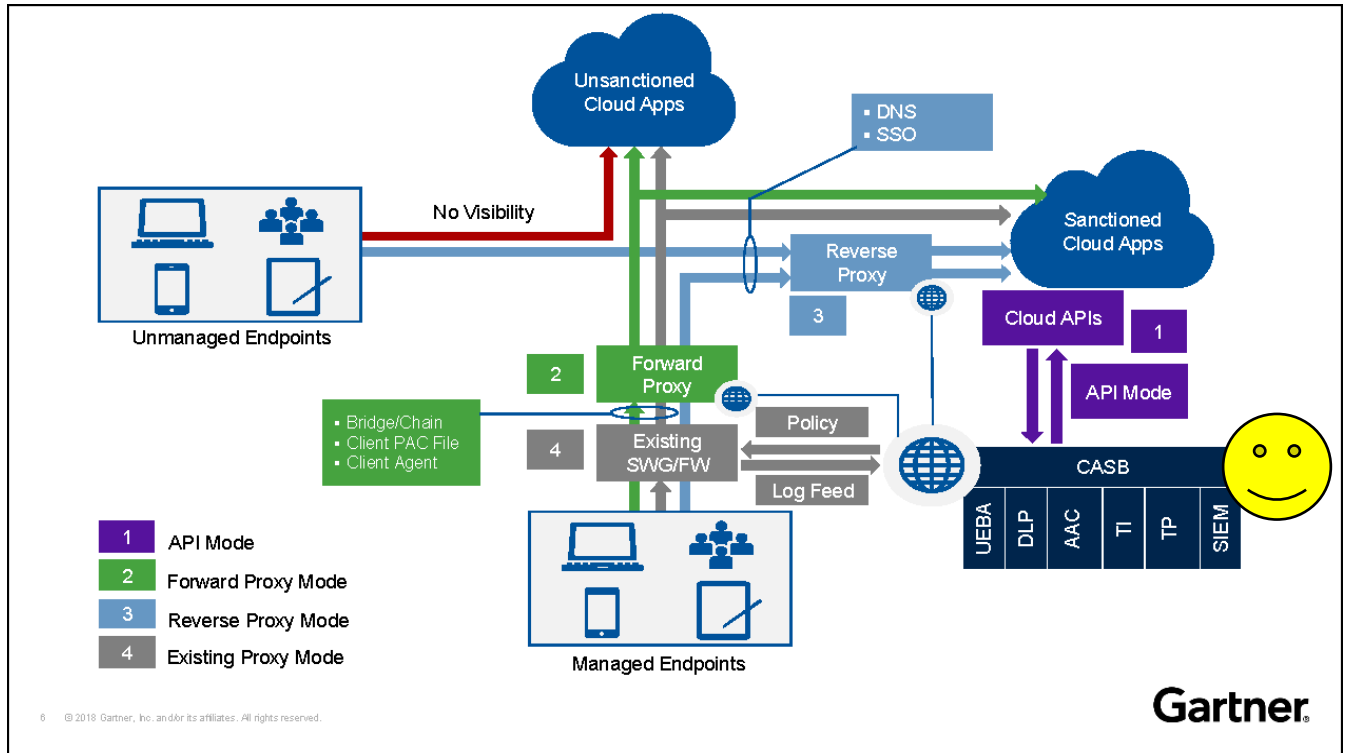
<sup>18</sup> The difference between a CASB, ZTNA, SDP, and VPN, and when do you need them? Retrieved from the Net Motion Software Security Blog – netmotionsoftware.com/blog/ security.

- Track behavior of an "interesting" user over times and places
- Search for and close "open but likely abandoned" file shares
- CASBs are to cloud as firewalls are to data centers
- CASB caveat: A CASB will help to secure any cloud resources stored in the public cloud by an organization, but they do nothing to protect on-premise applications and data. According to a recent article in CIO Dive, a staggering 98% of companies in 2019 were still operating on-premise servers, which CASB solutions cannot protect.
- Use CASB and ZTNA to protect the device in a cloud world.



**How can we meet user demand faster and remain secure?**

CASB = UEBA + AAC + TI + TP + SIEM + DLP. Gartner – August 2018



**What CASB looks like under the hood.**  
 CASB = UEBA + AAC + TI + TP + SIEM + DLP. Gartner – August 2018

**Zero Trust Network Access (ZTNA)** <sup>19 20 21 22</sup>

- ZTNA replaces traditional technologies, which require companies to extend excessive trust to employees and partners to connect and collaborate. Security and risk management leaders should plan pilot ZTNA projects for employee/partner-facing applications.
- Zero Trust is a concept and not a product in the strictest sense. However, products built around this framework are starting to take shape within the security landscape. One of the most promising is Zero Trust Network Access (ZTNA), otherwise known as Software Defined Perimeter (SDP).
  - Note: Over the near-term, the majority of SDP deployments will co-exist with VPN to provide end-to-end access security.
- IP addresses and location are no longer practical to establish sufficient trust for network access.

<sup>19</sup> Solving the Challenges of Modern Remote Access, by Gartner (ID G00722990).

<sup>20</sup> The difference between a CASB, ZTNA, SDP, and VPN, and when do you need them? Retrieved from the Net Motion Software Security Blog - netmotionsoftware.com/blog/ security.

<sup>21</sup> Zero Trust Architecture and Solutions - 2020. Research by Gartner and the Qi An Xin Group.

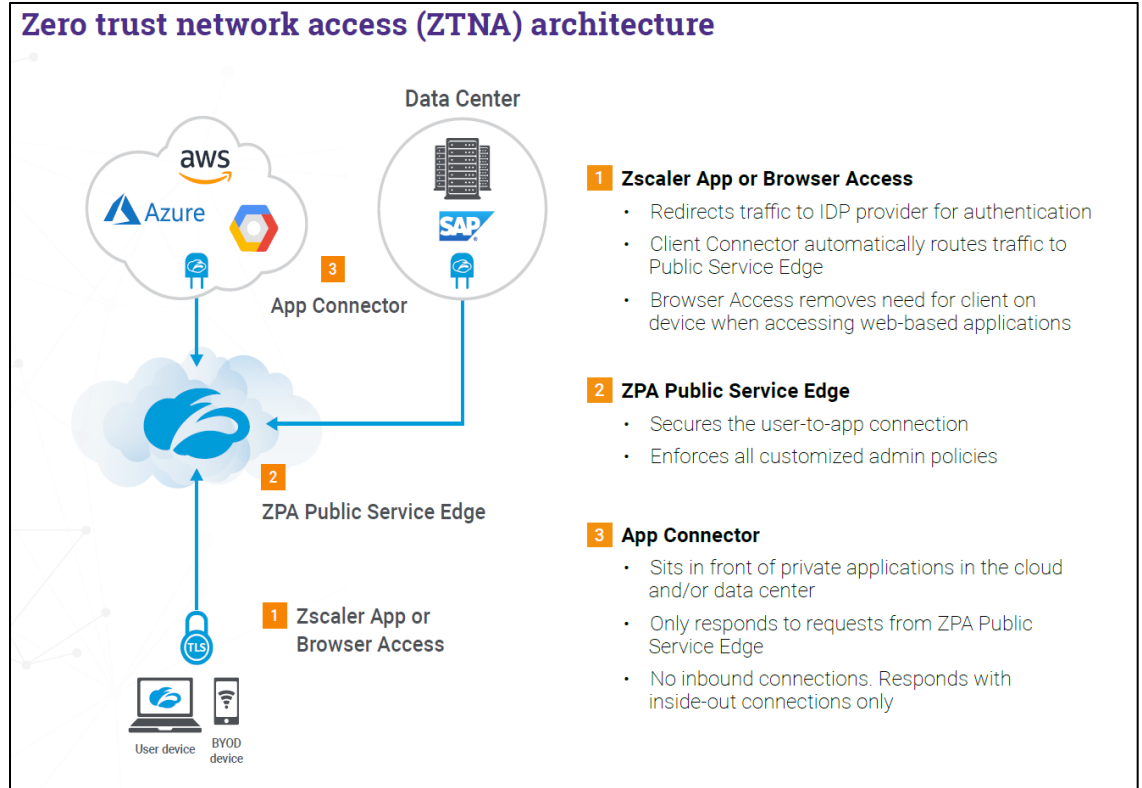
<sup>22</sup> Market Guide for Zero Trust Network Access – Shareable Summary by Gartner, April 29, 2019

- Shortening the network path to entry points through more routing options can improve connectivity performance for end-users.
  - ZTNA can improve security and simplify bring your own device (BYOD) programs by reducing full management requirements and enabling more-secure direct application access – enables users on personal devices.
- As more organizations transition to remote work, ZTNA has piqued the interest of organizations seeking a more flexible alternative to VPNs and those seeking more precise access and session control to applications located on-premises and in the cloud.
- The earliest prototype of zero trust came from Jericho Forum, founded in 2004, whose mission was to define cyber security under de-perimeter-ization trends and to find solutions.
- The actual term “zero trust” was officially coined in 2010, indicating that all network traffic is untrusted by default, and all access requests for all resources need to be securely controlled.
- Phase out legacy VPN-based access for high-risk use cases and begin phasing in ZTNA.
  - This reduces the ongoing need to support widely deployed VPN clients and introduces clientless identity- and device-aware access.
  - Support unmanaged devices for employees.
- As of March 2021, per NetMotion: <sup>23</sup>
  - Similar to SDP, ZTNA operates on a ‘deny by default’ basis, keeping unwanted users or bad actors from accessing sensitive enterprise resources.
  - NetMotion is the only solution to provide ZTNA as part of its platform alongside a VPN, offering the 98% of organizations with a mix of on-prem and cloud applications with the optimum choice for adopting ZTNA while also retaining a VPN that is there when they need it.

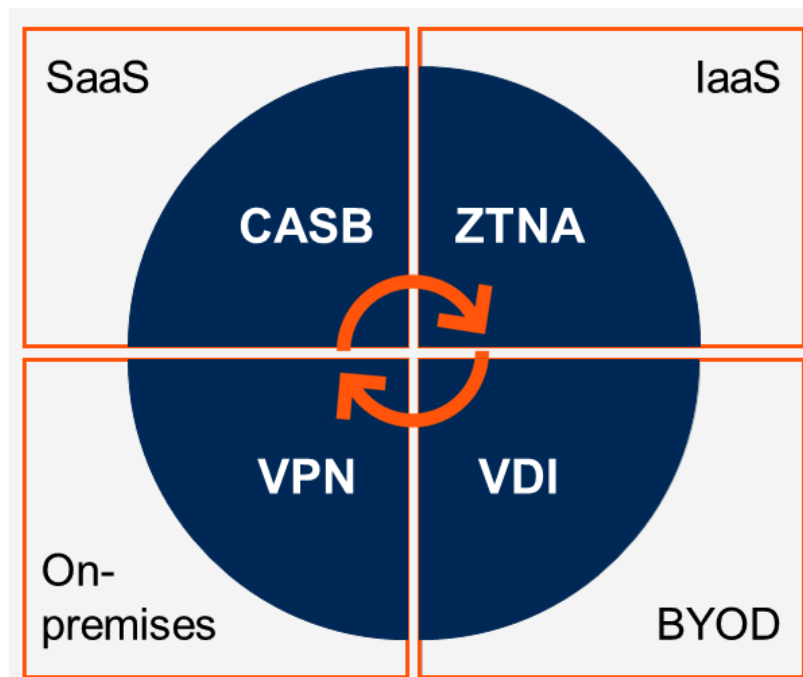
---

<sup>23</sup> Uncompromised Secure Access webpage. Retrieved March 17, 2021 from <https://www.netmotionsoftware.com/solutions/zero-trust-network-access>.





**Zero Trust Network Access (ZTNA) Architecture by ciosummits.com.**



**Solving the challenges of modern remote access. Gartner – July 2020**

## Requirements Gathering

<p><b>Who are the users and what is their job function?</b></p>	<ul style="list-style-type: none"> <li>• Executives or mission-critical employees</li> <li>• Users with intense data analysis needs</li> <li>• Users with “normal” requirements</li> </ul>
<p><b>What kind of device is being used and who owns it?</b></p>	<ul style="list-style-type: none"> <li>• PC vs. mobile device</li> <li>• Organization vs. user-owned</li> <li>• Phone/tablet</li> <li>• PC-class</li> </ul>
<p><b>What kind of applications and data do users need access to and are they located on-premises or in the cloud?</b></p>	<ul style="list-style-type: none"> <li>• Browser-based, on-premises</li> <li>• Windows-based on-premises</li> <li>• Browser-based cloud</li> <li>• Windows-based cloud</li> </ul>
<p><b>Where in the world is a user located?</b></p>	<ul style="list-style-type: none"> <li>• Verify user’s policy complies with all local labor and privacy laws</li> </ul>

Source: Gartner  
722990\_C

## Solving the Challenges of Modern Remote Access – Requirements Gathering – Gartner

### Software Defined Networking (SDN) <sup>24</sup> <sup>25</sup> <sup>26</sup>

- SDN technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management.
- A Software Defined “Network” is a centrally managed network infrastructure where the entire configuration is sent to generic devices to configure them to provide services.
- SDN makes the network programmable by separating the system that decides where traffic is sent (the control plane) from the underlying system that pushes packets of data to specific

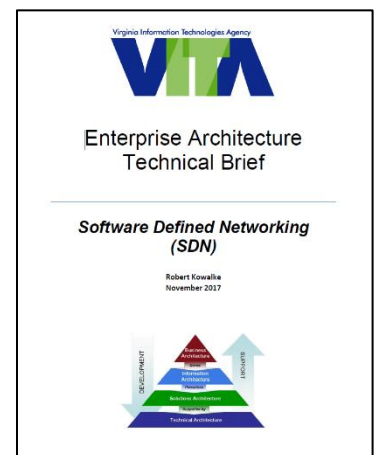
<sup>24</sup> 2020 Integrated Annual Technology Plan Summary prepared by SAIC (MSI) for VITA.

<sup>25</sup> The difference between a CASB, ZTNA, SDP, and VPN, and when do you need them? Retrieved from the Net Motion Software Security Blog - [netmotionsoftware.com/blog/security](https://netmotionsoftware.com/blog/security).

<sup>26</sup> 5 Differences between SDN and Network Functions Virtualization by Ingram Micro Advisor. Retrieved March 2021 from <https://www.ingrammicroadvisor.com/data-center/5-differences-between-sdn-and-network-functions-virtualization>.

destinations (the data plane).

- SDN operates in a campus, data center and/or cloud environment.
- SDN software targets cloud orchestration and networking.
- SDN is supported by the Open Networking Foundation (ONF).
- Verizon Managed Software-Defined Wide Area Network (SD-WAN)
  - SD-WAN removes artificial barriers that route all data to a hub for services such as Internet Service Gateway and the associated expenses of homing all data to a key location before routing to a key external location.
  - SD-WAN pushes policy to the edge of the Commonwealth's WAN and LAN Enhanced Security, high availability capabilities, and policy-driven routing services.
- For additional information regarding SDN, please peruse the VITA originated November 2017 technical brief on Software Defined Networking located at the following URLs:
  - Direct report link → [https://www.vita.virginia.gov/media/vitaviriniagov/it-governance/ea/pdf/TNE\\_Networking\\_SDN-Software-Defined-Networks\\_Technical-Brief.pdf](https://www.vita.virginia.gov/media/vitaviriniagov/it-governance/ea/pdf/TNE_Networking_SDN-Software-Defined-Networks_Technical-Brief.pdf)
  - VITA page link (scroll down to view) → <https://www.vita.virginia.gov/policy-governance/enterprise-architecture/ea-library/>



## Virtual Private Network (VPN) <sup>27</sup> <sup>28</sup>

Please note the section on tunneling (at the beginning of this brief for additional VPN information.

- VPN is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and other information transmitted between two endpoints.
  - Because a VPN can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks.
  - Although SSL VPNs are flexible enough to meet many needs, there are certain cases when other types of VPNs may provide a better solution. <sup>29</sup>
    - Network layer VPN protocols – primarily IPsec

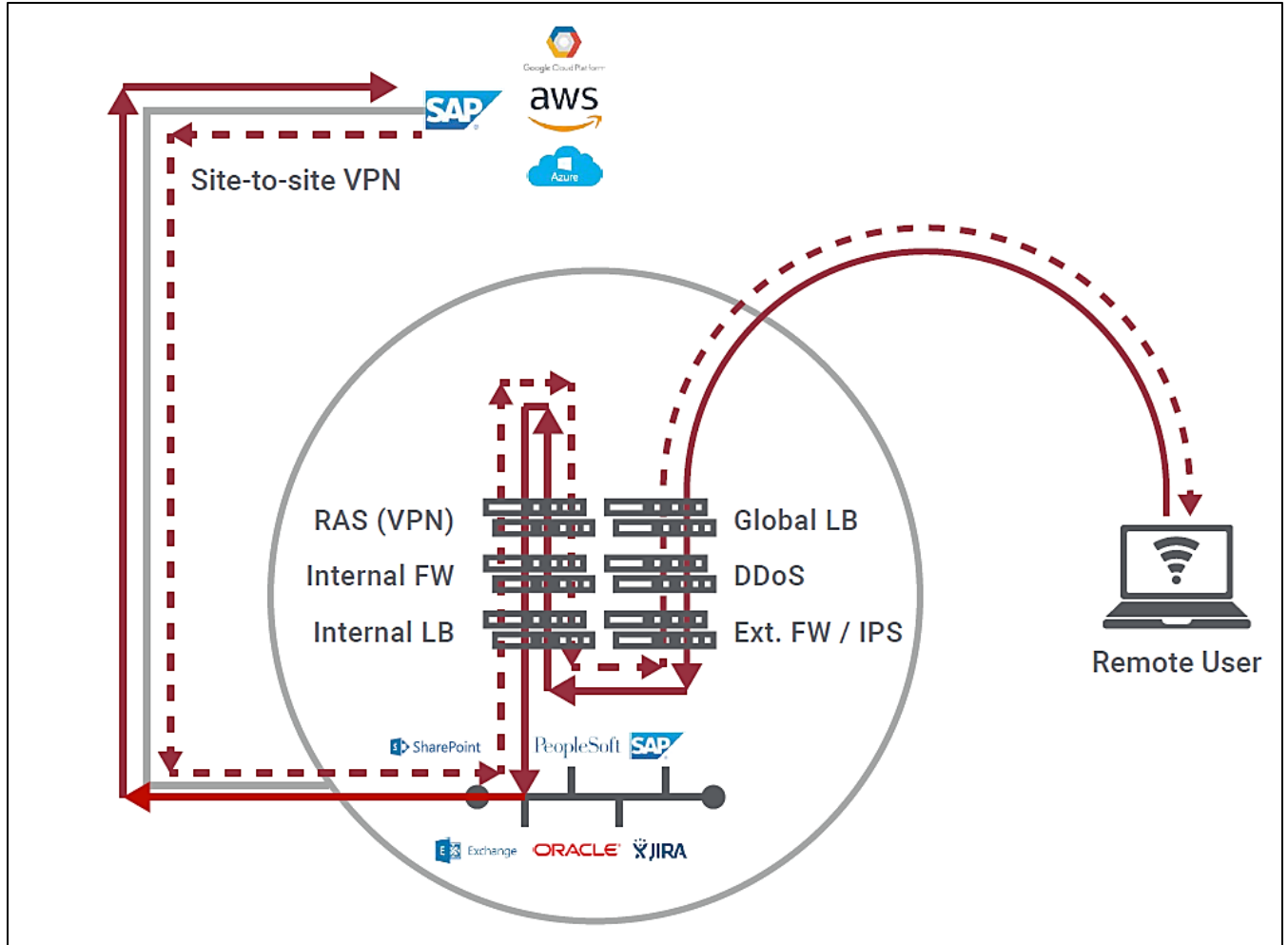
<sup>27</sup> My Perspective of Enterprise Network Services by Nagarai Shenoy of Juniper Networks, June 14, 2020. Retrieved March 15, 2021 from slideshare.net.

<sup>28</sup> Solving the Challenges of Modern Remote Access, by Gartner (ID G00722990).

<sup>29</sup> Guide to SSL VPNs. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), Special Publication (SP) 800-113 of July 2008. <https://csrc.nist.gov/publications/detail/sp/800-113/final>

- Data link layer VPN protocols:
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Layer 2 Forwarding (L2F)
- Application layer security protocols:
  - OpenPGP
  - Secure Shell (SSH)
- With a VPN, all remote user traffic is backhauled through the centralized data center security stack just to go back through the entire stack on the return trip.
- Do not use always-on VPN unless you have to.
- Legacy VPNs remain popular, but they might not provide sufficient risk management for exposed services and can be more difficult to manage, given the dynamic nature of digital business.
  - Legacy VPNs may also create scale and bandwidth issues for mostly mobile workforces.
  - Always-on VPNs that require device and user authentication provide similar outcomes as ZTNA; however, basic network-access VPNs do not.
  - Factor security requirements into VPN models and user satisfaction expectations.
  - For third-party privileged access into enterprise systems, a PAM tool can be a useful alternative to a VPN.
- VPN - Since the late 1990s, enterprises have relied on remote access technologies like the VPN that allows employees to 'tunnel' into corporate data and applications. With companies transitioning away from on-premise data over the last decade in favor of private and/or public cloud-based applications, the traditional VPN has somewhat faded from the limelight.
  - Legacy VPNs, in particular, generally take an all-or-nothing approach to remote access. What that means is that if the VPN is turned off, there won't be any data encryption or tunneling, and the user will be blocked from accessing corporate data and applications. When the VPN is turned on, however, users are given access to the corporate resources they need.
  - In years past, that wasn't a problem. As mentioned above, most resources were contained on-premise and employees used a VPN to access them. But with the advent of applications and data being hosted in private and public clouds, the VPN actually becomes a bottleneck, effectively eating up huge amounts of network bandwidth to carry traffic that could have been sent directly to the cloud.

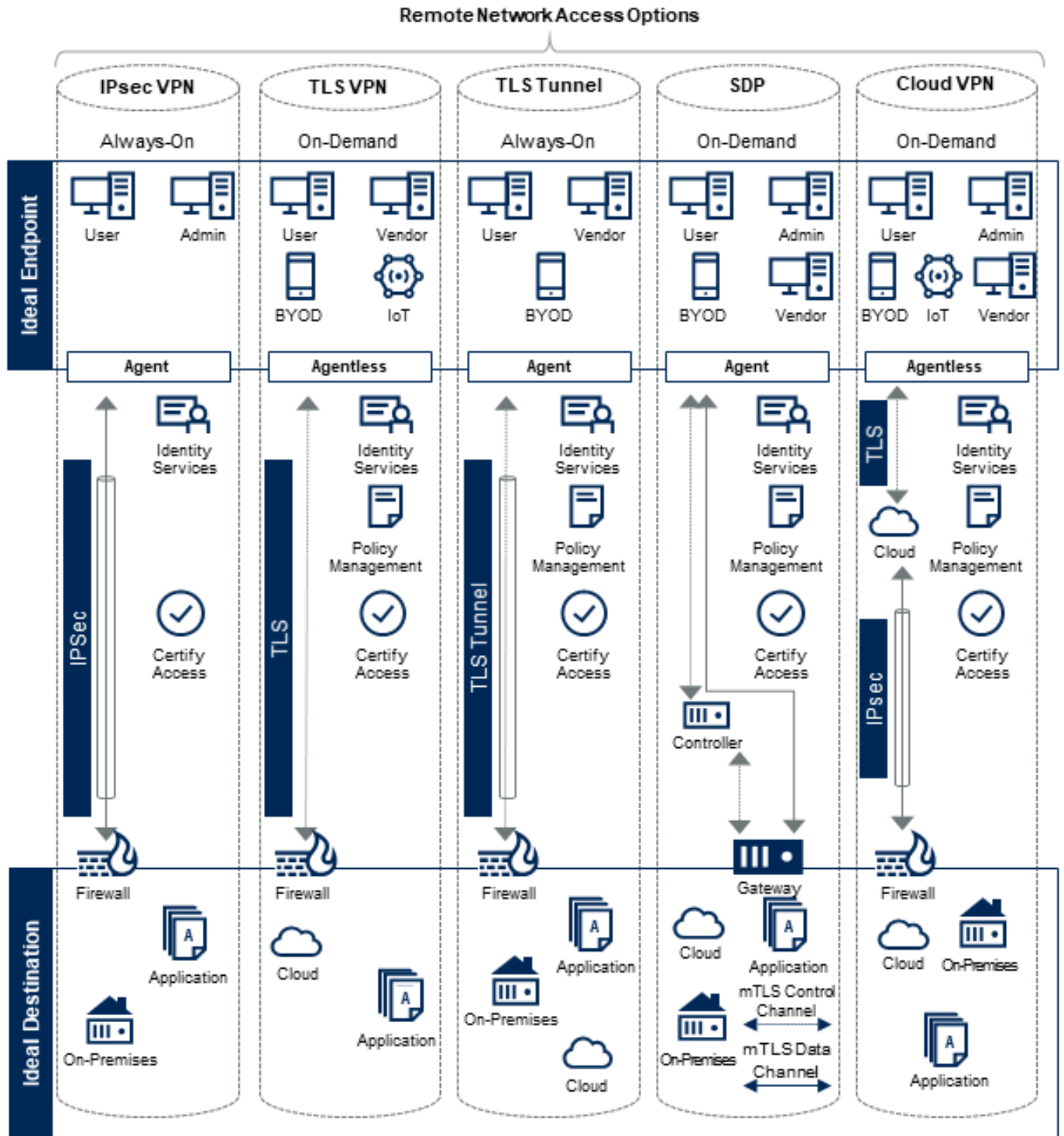
- By far, one of the biggest criticisms of traditional, always-on VPNs is they lack the ability to offer split tunneling, which would allow them to intelligently separate data into what can go directly to house, say for example a SaaS application running in a browser window, and other data that has to go down a tunnel to an on-premise resource. Depending on their function, many employees today primarily use Office365 and other SaaS applications that require very little tunneling.
- From a usability perspective, users have long criticized VPNs for network slows down, as well as frustrating reauthentication requests whenever the connection is lost or an app crashes. This was particularly frustrating for employees at the beginning of the shelter-in-place restrictions in March, because they were not only suddenly forced to work from home, they were also experiencing less than ideal work performance, even when they had an otherwise fast home internet connection.
- Is CASB the answer?
  - Comparatively speaking, CASB tools are the new kids on the block - since around 2015. They are designed specifically to let IT administrators manage applications and data in the cloud. And they are especially adept at things like monitoring cloud service usage, helping IT teams set up cloud-related policy controls, and enabling threat protection and regulatory compliance for the enterprise.
  - To some extent, CASB solutions pick up where VPNs fall flat. They offer much better edge-to-edge visibility of the network, allowing IT teams to see and control much more of what is going on – even down to individual file names and data elements.
  - The best way to know whether a CASB solution could be a good fit for your organization is to see where the enterprise applications and data are stored. If the enterprise runs completely on SaaS applications hosted on the public web, then a CASB may be a good choice. For the majority of companies, however, a CASB solution is far less effective if they also maintain data and applications on-premise.



**It is time to rethink application access?**

Zscaler VPN Alternative by ciosummits.org – 2018.

# Overview of Remote Network Access Options



Source: Gartner  
ID: 390285

## Overview of Remote Network Access Options (VPNs) – Gartner – June 14, 2019

## Multi-protocol Label Switching (MPLS) VPNs <sup>30 31 32 33</sup>

- MPLS VPN is a family of methods for using multiprotocol label switching (MPLS) to create virtual private networks (VPNs).
- MPLS VPN is a flexible method to transport and route several types of network traffic using an MPLS backbone.
- MPLS switches packets using labels instead of IP addresses or Layer 3 information.
  - It is protocol-agnostic and speeds up packet forwarding and routing.
  - Back when MPLS was first introduced, it showed a considerable boost in speed and took substantial load off networks by laying off IP address inspection.
  - Today, MPLS is used not only to facilitate higher speed requirements but to develop advanced and augmented applications and services over the existing network infrastructure.
- There are three types of MPLS VPNs deployed in networks today:
  1. Point-to-point (Pseudowire)
    - a. Point-to-point MPLS VPNs employ VLL (virtual leased lines) for providing Layer2 point-to-point connectivity between two sites. Ethernet, TDM, and ATM frames can be encapsulated within these VLLs.
  2. Layer 2 (VPLS)
    - a. VPLS (virtual private LAN service) offer a “switch in the cloud” style service.
    - b. VPLS provides the ability to span VLANs between sites.
    - c. L2 VPNs are typically used to route voice, video, and AMI traffic between substation and data center locations.
  3. Layer 3 (VPRN)
    - a. VPRN (virtual private routed network), utilizes layer 3 VRF (VPN/virtual routing and forwarding) to segment routing tables for each customer utilizing the service.
    - b. The customer peers with the service provider router and the two exchange routes, which are placed into a routing table specific to the customer.

---

<sup>30</sup> MPLS VPN Wikipedia Page. Retrieved March 17, 2021 from [https://en.wikipedia.org/wiki/MPLS\\_VPN](https://en.wikipedia.org/wiki/MPLS_VPN).

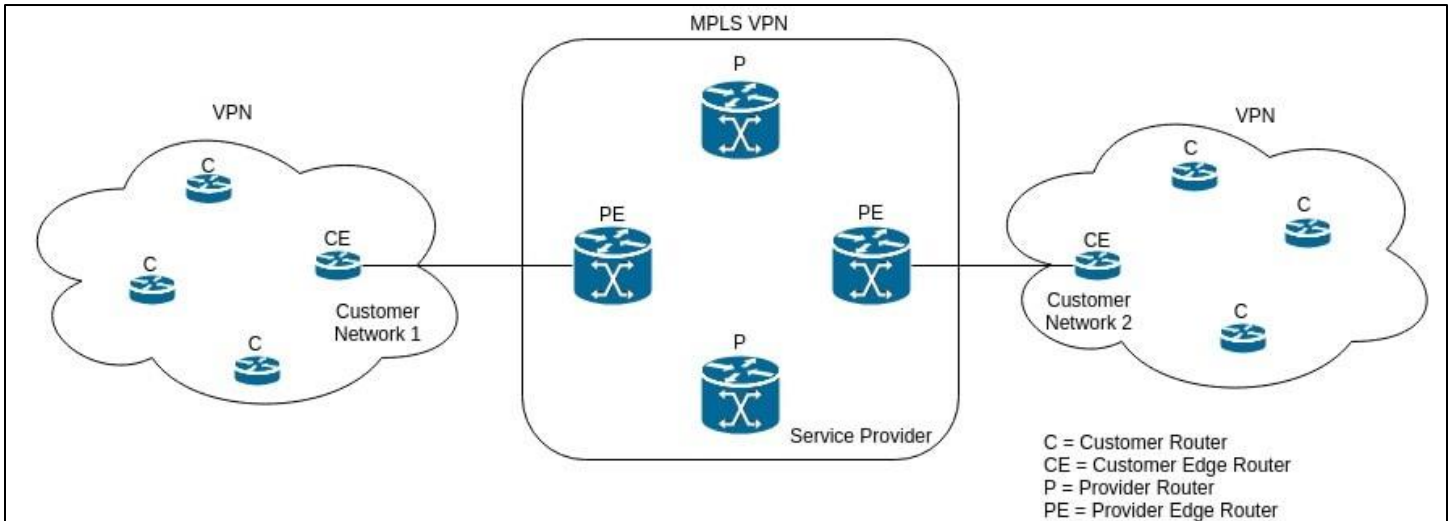
<sup>31</sup> Introduction to MPLS and MPLS VPN Technology by Shreya A N of Cisco - July 20, 2020. Retrieved March 17, 2021 from <https://www.section.io/engineering-education/introduction-to-mpls-and-mpls-vpn-technology/>

<sup>32</sup> Typical MPLS LSR Multiprotocol Label Switching MPLS Explained by Towards Data Science - August 10, 2019. Retrieved March 17, 2021 from <https://towardsdatascience.com/multiprotocol-label-switching-mpls-explained-aac04f3c6e94>

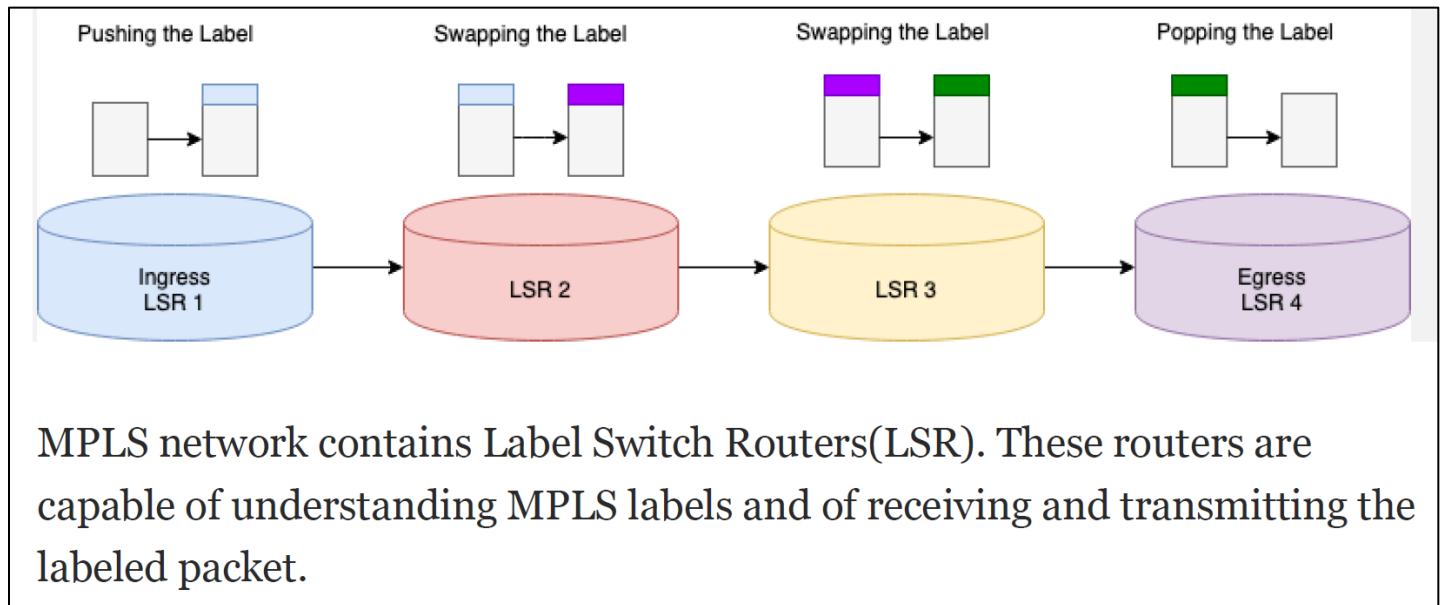
<sup>33</sup> 4 reasons why an MPLS VPN is a great way to connect to the cloud by AT&T. Retrieved March 17, 2021 from <https://www.business.att.com/learn/tech-advice/4-reasons-why-an-mpls-vpn-is-a-great-way-to-connect-to-the-cloud.html>



- c. Multiprotocol BGP (MP-BGP) is required in the cloud to utilize the service, which increases complexity of design and implementation.
  - d. L3 VPNs are typically not deployed on utility networks due to their complexity; however, a L3 VPN could be used to route traffic between corporate or datacenter locations.
- MPLS Virtual Private Network, or MPLS VPN, is the most sought-after and widespread implementation of MPLS technology.



Typical MPLS VPN by Cisco - July 20, 2020



Typical MPLS LSR Multiprotocol Label Switching MPLS Explained

- MPLS VPNs can offer improved performance and traffic control
  - MPLS VPNs help provide quality performance for cloud-based applications chiefly because they enable enterprises to prioritize certain types of their traffic, a concept known as Class of Service (CoS).
  - This takes on added importance when you consider the sorts of applications that may be getting shifted to the cloud, everything from delay-sensitive voice-over-IP traffic to enterprise applications like enterprise resource planning or sales force automation.
  - With CoS, enterprises can dictate which types of their traffic is given priority, so they can avoid an employee conducting a massive file transfer causing a hiccup in the CEO's conference call.
- More reliable and secure than the public Internet
  - MPLS VPNs are carried over a single carrier's network, not over the public Internet. That sets the table for better reliability, because the traffic won't be subject to the vagaries of the public Internet.
  - Also, it offers an added level of network security as compared to Internet Protocol Security (IPSec) VPNs. With MPLS VPNs, customers have the added assurance of knowing their traffic is never out "in the wild." Rather, it remains within the confines of their carrier's private virtual network.
  - MPLS VPNs are carried over a single carrier's network, not over the public Internet. That sets the table for better reliability...
- Reduces bandwidth requirements
  - MPLS VPNs enable each site on the network to connect to every other site via a single connection to the MPLS network. This can significantly reduce the amount of bandwidth customers need, especially at their main headquarters and cloud provider sites.
- Provides flexibility
  - Similar to how cloud services enable you to quickly add capacity on an as-needed basis, it's far easier to add capacity to an MPLS VPN than via traditional carrier services. And being able to expand the capacity of your cloud applications and services may not do you much good if you can't increase the capacity of the connections to them at the same time.
  - The combination of cloud services and MPLS VPNs really can make the cloud seem like an extension of your premise-based network and services, creating what's known as a "virtual private cloud."

## Remote Connectivity Requirement Considerations <sup>34</sup>

Determining interconnection requirements is an important part of an overall connectivity plan. The planning team should identify and examine all relevant technical, security, and administrative issues surrounding a proposed interconnection. This information may be used to develop an Interconnection Security Agreement (ISA) and a Memorandum of Understanding or Agreement (MOU/A) or equivalent documents. Moreover, this information may be used to develop an implementation plan for establishing the interconnection.

Remote connectivity planning should include the following issues:

- **Level and Method of Interconnection:**
  - Define the level of interconnectivity that will be established between the IT systems, ranging from limited connectivity (limited data exchange) to enterprise-level connectivity (active sharing of data and applications).
  - Describe the method used to connect the systems (dedicated line or VPN).
- **Impact on Existing Infrastructure and Operations:**
  - Determine whether the network or computer infrastructure currently used by both organizations is sufficient to support the interconnection, or whether additional components are required (e.g., communication lines, routers, switches, servers, and software).
    - If additional components are required, determine the potential impact that installing and using them might have on the existing infrastructure, if any.
    - In addition, determine the potential impact the interconnection could have on current operations, including increases in data traffic; new training requirements; and new demands on system administration, security, and maintenance.
- **Hardware Requirements:**
  - Identify hardware that will be needed to support the interconnection, including communications lines, routers, firewalls, hubs, switch, servers, and computer workstations.
  - Determine whether existing hardware is sufficient, or whether additional components are required, especially if future growth is anticipated.
    - If new hardware is required, select products that ensure interoperability.
- **Software Requirements:**
  - Identify software that will be needed to support the interconnection, including software for firewalls, servers, and computer workstations.
  - Determine whether existing software is sufficient, or whether additional software is required.

---

<sup>34</sup> Security Guide for Interconnecting Information Technology (IT) Systems. Recommendations of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, August 2002.

- If new software is required, select products that ensure interoperability.
- Data Sensitivity:
  - Identify the sensitivity level of data or information resources that will be made available, exchanged, or passed one-way only across the interconnection.
    - Identifying data sensitivity is critical for determining the security controls that should be used to protect the connected systems and data. Examples of sensitive data include financial data, personal information, and proprietary business data.
    - See NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, for further guidance.
- User Community:
  - Define the community of users who will access, exchange, or receive data across the interconnection.
  - Determine whether users must possess certain characteristics corresponding to data sensitivity levels, such as employment status or nationality requirements, and whether background checks and security clearances are required.
  - Devise an approach for compiling and managing the profiles of all users who will have access to the interconnection, including user identification, workstation addresses, workstation type, operating system, and any other relevant information.
    - Each organization should use this information to develop and maintain a comprehensive database of its users.
- Services and Applications:
  - Identify the information services that will be provided over the interconnection by each organization and the applications associated with those services, if appropriate.
    - Examples of services include e-mail, file transfer protocol (FTP), RADIUS, Kerberos, database query, file query, and general computational services.
- Security Controls:
  - Identify security controls that will be implemented to protect the confidentiality, integrity, and availability of the connected systems and the data that will pass between them.
    - Controls should be appropriate for the systems that will be connected and the environment in which the interconnection will operate.
- Segregation of Duties:
  - Determine whether the management or execution of certain duties should be divided between two or more individuals.
    - Examples of duties that might be segregated include auditing, managing user profiles, and maintaining equipment.

- Segregation of duties reduces the risk that a single individual could cause harm to the connected systems and data, either accidentally or deliberately.
- Incident Reporting and Response:
  - Establish procedures to report and respond to anomalous and suspicious activity detected by either technology or staff.
  - Determine when and how to notify each other about security incidents that could affect the interconnection.
  - Identify the types of information that will be reported, including the cause of the incident, affected data or programs, and actual or potential impact.
  - Identify types of incidents that require a coordinated response, and determine how to coordinate response activities.
  - Consider developing a joint incident response plan for this purpose.
    - For more information, see NIST Special Publication 800-3, Establishing a Computer Security Incidence Response Capability (CSIRC), and Federal Computer Incident Response Center (FedCIRC) publications.
- Contingency Planning:
  - Each organization should have a contingency plan(s) to respond to and recover from disasters and other disruptive contingencies that could affect its IT system, ranging from the failure of system components to the loss of computing facilities.
  - Determine how to notify each other of such contingencies, the extent to which the organizations will assist each other, and the terms under which assistance will be provided. Identify emergency points of contact (POC).
  - Determine whether to incorporate redundancy into components supporting the interconnection, including redundant interconnection points, and how to retrieve data backups.
  - Coordinate disaster response training, testing, and exercises.
  - See NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, for more information.
- Data Element Naming and Ownership:
  - Determine whether the data element naming schemes used by both organizations are compatible, or whether new databases must be normalized so the organizations can use data passed over the interconnection.
  - Determine whether ownership of data is transferred from the transmitting party to the receiving party, or whether the transmitting party retains ownership and the receiver becomes the custodian.
  - As part of this effort, determine how transferred data will be stored, whether data may be re-used, and how data will be destroyed.
  - Determine how to identify and resolve potential data element naming conflicts.

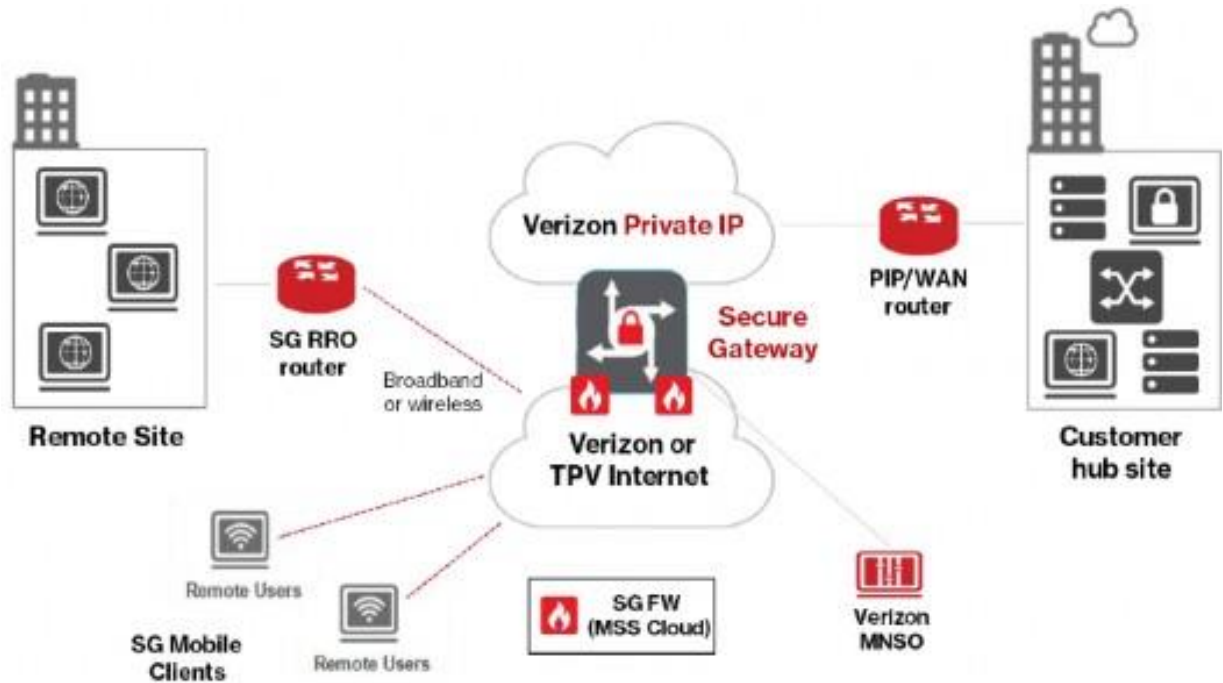
- Data Backup:
  - Determine whether data or information that is passed across the interconnection must be backed up and stored.
  - If backups are required, identify the types of data that will be backed up, how frequently backups will be conducted (daily, weekly, or monthly), and whether backups will be performed by one or both parties.
  - Determine how to perform backups, and how to link backups to contingency plan procedures.
  - Critical data should be backed up regularly; stored in a secure off-site location to prevent loss or damage, and retained for a period approved by both parties.
    - Similarly, audit logs should be copied; stored in a secure location, and retained for a period approved by both parties.
- Change Management:
  - Determine how to coordinate the planning, design, and implementation of changes that could affect the connected systems or data, such as upgrading hardware or software, or adding services.
  - Establish a forum with appropriate staff from each organization to review proposed changes to the interconnection, as appropriate.
  - Coordinating change management activities will reduce the potential for implementing changes that could disrupt the availability or integrity of data, or introduce vulnerabilities.
- Rules of Behavior:
  - Develop rules of behavior that clearly delineate the responsibilities and expected behavior of all personnel authorized to access the interconnection.
  - Rules should be in writing, and state the consequences of inconsistent behavior or noncompliance.
  - Explain rules in a security training and awareness program.
- Security Training and Awareness:
  - Define a security training and awareness program for all authorized personnel who will be involved in managing, using, and/or operating the interconnection.
  - The program may be incorporated into current security training and awareness activities.
  - Identify training requirements, including frequency and scheduling, and assign responsibility for conducting training and awareness activities.
  - Design training to ensure that personnel are familiar with IT security policy, procedures, and the rules of behavior associated with the interconnection.
  - Require users to sign an acknowledgement form indicating that they understand their

- security responsibilities, if appropriate.
- If shared applications are used, ensure users know how to use them properly.
- If the interconnection is used to exchange or transfer sensitive data, ensure users understand special requirements for handling such data, if required.
- See NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, for guidance.
- Roles and Responsibilities:
  - Identify personnel who will be responsible for establishing, maintaining, or managing the interconnection, including managers, system administrators, application designers, auditors, security staff, and specialists from such fields as insurance and risk management.
  - Choose personnel who have appropriate subject matter expertise.
    - If contractors are involved, one or both organizations may be required to develop a nondisclosure agreement to safeguard the confidentiality and integrity of exchanged data.
- Scheduling:
  - Develop a preliminary schedule for all activities involved in planning, establishing, and maintaining the interconnection.
  - Determine the schedule and conditions for terminating or reauthorizing the interconnection.
    - For example, both parties might agree to review the interconnection every 12 months to determine whether to reauthorize it for continued operation.
- Costs and Budgeting:
  - Identify the expected costs required to plan, establish, and maintain the interconnection.
  - Identify all associated costs, including labor, hardware, software, communications lines, applications, facilities, physical security, training, and testing.
  - Identify costs for certifying and accrediting the interconnection, if appropriate.
  - Develop a comprehensive budget, and determine how costs will be apportioned between parties, if required.

## Remote Site Connectivity to Enterprise WAN

The Supplier's Secure Gateway (SG) service is a network-based service that securely connects the Customer's private network to the public Internet through a logical, virtual port (Universal Port).

The following highlights the Supplier's Secure Gateway Universal Port components.



**Verizon Secure Gateway Universal Port Components.**

With Retail and Remote Office (RRO), the Supplier provides Customer with an end-to-end logical connection between Customer’s corporate resources on the Supplier’s Private IP network and Customer’s remote sites connected to the Internet or the Supplier’s IP network – via either a Universal Port or a Universal Port UBB..

The Supplier provides the following standard features:

- **Router Management:** For RRO, the Supplier provides router management that includes configuration, set- up, administration, monitoring, support, and reporting (if applicable) for the RRO devices selected by the Customer (each, a Managed Device) upon installation of such devices
- **RRO Site CPE Monitoring:** The Supplier provides monitoring, alarm response, and email notification of the RRO CPE on a 24 x 7 x 365 basis.
- **Reporting:** With RRO, the Customer may also select WAN Analysis Reporting.
- **Alternative Internet Service Provider:** Customer may use RRO with Internet service from an alternative service provider (ASP) that offers appropriate Ethernet interface, speed, protocol, and remote access capabilities. Where Customer chooses Internet service provided via an ASP, Customer is responsible for the installation and maintenance of all Customer-provided connections.
- **WAN Analysis Reporting** is a web-based reporting tool that provides customers with a consolidated view of their Supplier-provided network infrastructure for network bandwidth of 1Mbps to 10GB circuits.



The following optional service features are included and configured if desired:

- **Managed Device Feature – WAN Backup Service:** For RRO routers, the Supplier will configure a Managed Device to support backup access (over separately-provided Supplier or Third Party Internet service) in the event the primary circuit fails.
- **Backup Service Configuration Option:** With the Backup Service Configuration Option, the Supplier will configure RRO at implementation to be used as a primary service for Customer remote locations to connect to the Supplier’s Private IP Service, or as a backup service to connect to its Supplier-provided Private IP network and Managed Devices under the Supplier’s Managed WAN Service.
- **Quality of Service Support:** With Quality of Service (QoS) support on the RRO CPE routers, the Supplier will route Customer traffic based on the priority assigned by the Customer using different classes of service designations, which follow the Internet Engineering Task Force Differentiated Services or “Diff-Serv” model.
- If the Customer does not set different classes, the Supplier will route all Customer traffic using the BE class as the default priority designation.

#### Site-to-Site Secure Access (VPN)

In the near-term, the existing Customer solution, ERCS, utilizing DMVPN technology, will continue to be used for Site-to-Site Access VPN.

### Enterprise Remote Connection Service (ERCS) <sup>35</sup>

ERCS utilizes secure tunnels across the internet to connect to the Commonwealth network. ERCS can securely connect End-Users with broadband or wireless internet connectivity to the VITA WAN using dynamic IPsec tunnels that protect data from unauthorized access. ERCS provides the following benefits:

- **Low cost network connectivity:**
  - Broadband internet access such as Digital Subscriber Line (DSL) or Cable and 3G wireless internet access can be utilized.
  - Reduction in equipment costs have the potential to translate into reduced cost of service as compared to traditional T-1 technology.
- **Security**
  - All End-User traffic will traverse encrypted tunnels (IPsec) to the Commonwealth Enterprise Solution Center or other ERCS Eligible Customer Location. No direct access

---

<sup>35</sup> VITA Services, Catalog Services webpage. Obtained June 10, 2020 from <https://www.vita.virginia.gov/services/catalog-services/>

to the internet (split tunneling) is allowed.

- All traffic destined for the internet will flow through the Internet Secure Gateway (ISG) at CESC providing centralized firewall and web filtering protection.
- Authorization of ERCS routers will be controlled by certificates to prevent connections by unauthorized devices.
- Monitoring
  - 24 x 7 equipment monitoring
- Broadband Service
  - Eligible Customer Locations will be required to have an existing broadband service (DSL or Cable) or wireless service subscription in place prior to the deployment of this service.

## ERCS Architecture

ERCS is suitable for locations that have modest bandwidth needs and do not desire Voice over IP (VoIP) or video services. ERCS is intended for backup to MPLS, but not a replacement for MPLS except for sites not transformed to MPLS, or are not currently using MPLS.

The connection from the customer site to CESC is across the internet broadband through an IPsec tunnel. The initial tunnel setup is between the site router and the DMVPN hub routers at CESC. If the intended destination of the customer site network traffic is determined by the DMVPN routers to be another ERCS site, an IPsec tunnel is end pointed onto the destination site's router and the DMVPN hub routers then drop out of the traffic pathway. If the destination is the internet or conventional MPLS sites, the traffic will traverse the IPsec tunnel to the CESC hub routers and then follow the standard MPLS paths. Internet traffic will flow through the CESC ISG and back out to the internet to ensure secure firewall and intrusion detection for all internet communications.

ERCS has limited SLA's on broadband services; may be subject to extended outages and/or cellular data throttling.

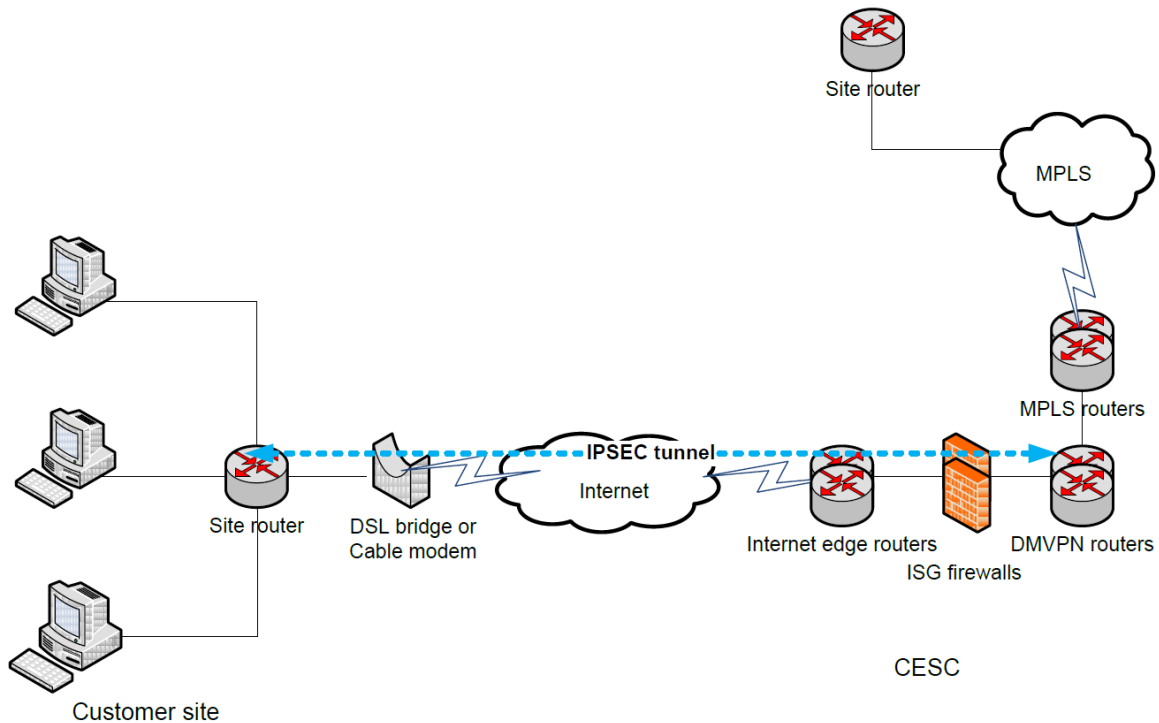
## Security

ERCS provides a secure connection method over the internet to both internal and external resources. The solution includes the following security functionality:

- IPsec tunnels using AES 256 encryption
- No ability to split tunnel – No direct access to the internet (split tunneling) is allowed.
- Centralized firewalls with redundancy for all external (internet) communications
- Network-based Intrusion Detection Service (NIDS), Host-based Intrusion Detection Service (HIDS), and Network / Host-based Intrusion Prevention Services (NIPS/HIPS)

Due to technical and security considerations, ERCS is not suitable for site locations requiring high availability and throughput greater than 15Mbps. Prior to implementing an ERCS work request, Vendor will work with the Eligible Customer to determine if throughput, availability, or degradation of WAN performance is possible.

Voice over IP and Video services are not supported at Eligible Customer Locations utilizing ERCS.



### Enterprise Remote Connection Service Diagram

Wi-Fi network service offered with ERCS will only be available in 802.11n standard and only allows for a single access point. No additional access points will be available. As the Wi-Fi access emanates from the router, the placement of the router will affect service area coverage.

Wi-Fi service provisioned with Vendor’s ERCS does not constitute Vendor’s Wireless Network Service as described in Appendix 8 to Schedule 3.3 of the CIA.

NOC monitoring will not be available for wireless component of this service.

### Network Services

This service category encompasses Wide Area Network (WAN), ERCS, Local Area Network (LAN) network access, managed router, and secure wireless services.

While it might be expedient, for example, to choose backbone VPN services from one vendor, TLS/browser portal experiences from another, and self-encrypting app tools from yet another, the complexity of three separate vendor solutions could easily become unmanageable. Buyers must find a balance between essential and unnecessary variety. The lowest risk approach is to begin with mainstream infrastructure VPN providers, and cautiously add innovative methods (such as app-level solutions).

Therefore, minimize the number of secure communications solutions in play to avoid costly redundancies and interoperability challenges. <sup>36</sup>

<b>Secure Enterprise Data Communications Representative Vendors</b>							
Vendors	Product	Originating Market *	Access Use Cases				Endpoint Platform Support **
			Site-to-Site Secure Gateways	Device-Level Secure Access	App-Level Secure Access	Cloud Based Services Offered	
AT&T	AT&T VPN Portfolio	MNS	X	X	X	X	A, I, M, W
Bitglass	Next-Gen CASB	CASB		X	X	X	A, C, I, L, M, W
Cato Networks	Cato Cloud Cato Socket Cato Client	SDP SD-WAN	X	X	X	X	A, I, L, M, W
Check Point Software Technologies	Endpoint Remote Access VPN Software Blade Ipsec VPN Software Blade Mobile Access Software Blade	FW	X	X	X	X	A, I, L, M, W
Cisco	Adaptive Security Appliance (ASA) Cisco Firepower Next-Generation Firewall (NGFW) Cisco AnyConnect Secure Mobility Client	FW	X	X	X	X	A, C, I, L, M, W
Citrix	Citrix ADC Citrix SD-WAN	VDI	X	X	X	X	A, C, I, L, M, W
F5	BIG-IP BIG-IP Access Policy Manager (APM)	Load balancing / Acceleration	X	X	X		A, I, M, W
Microsoft	Always On Virtual Private Network (VPN) DirectAccess	OSs		X	X	X	W
MobileIron	MobileIron Sentry MobileIron Tunnel	UEM		X	X		A, B, I, M, W
Perimeter 81	Perimeter 81	NaaS	X		X	X	A, B, C, I, L, M, W
Symantec	Luminate Secure Access Cloud	EPP		X	X	X	A, B, C, I, L, M, W
Zscaler	Zscaler Internet Access (ZIA) Zscaler Private Access (ZPA)	SWG		X	X	X	A, B, I, M, W

The vendors listed in this table do not imply an exhaustive list.  
This table is intended to provide more understanding of the market and its offerings.

\* Refers to the vendor's primary market before, or in addition to, VPN.  
\*\* Refers to supported platforms for vendor's endpoint client app/agent for device-level and app-level VPNs.  
Most of these vendors offer browser support. Android (A); Browser client (B); Chrome OS (C); iOS (i); Linux (L); Mac OS (M); Windows (W)

### **Market Guide for Secure Enterprise Data Communications by Gartner.**

CASB = Cloud Access Security Broker; EPP = Endpoint Protection Platforms; FW = Firewall;  
MNS = Managed Network Security; NaaS = Network as a Service; OSs = Operating Systems; SDP = Software Defined Perimeter;  
SD-WAN = Software Defined Wide Area Network; SWG = Secure Web Gateway; UEM = Unified Endpoint Management;  
VDI = Virtual Desktop Infrastructure

## Telework Client Device Security <sup>37</sup>

Telework client devices are divided into two general categories:

- Personal computers (PC)

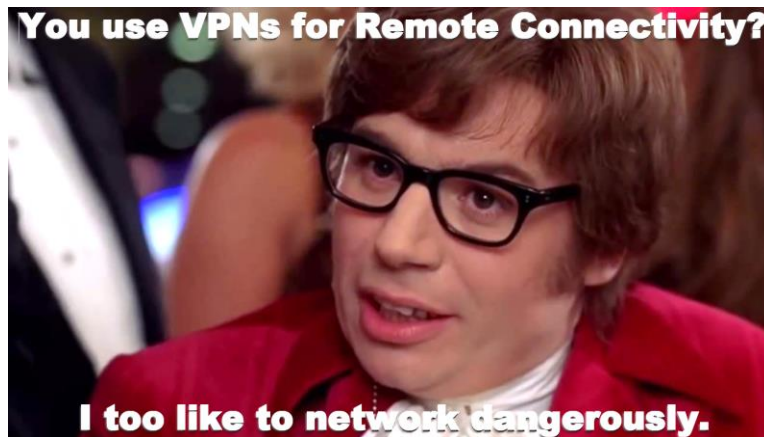
<sup>36</sup> Market Guide for Secure Enterprise Data Communications. Gartner ID-G00356835 of April 11, 2019.

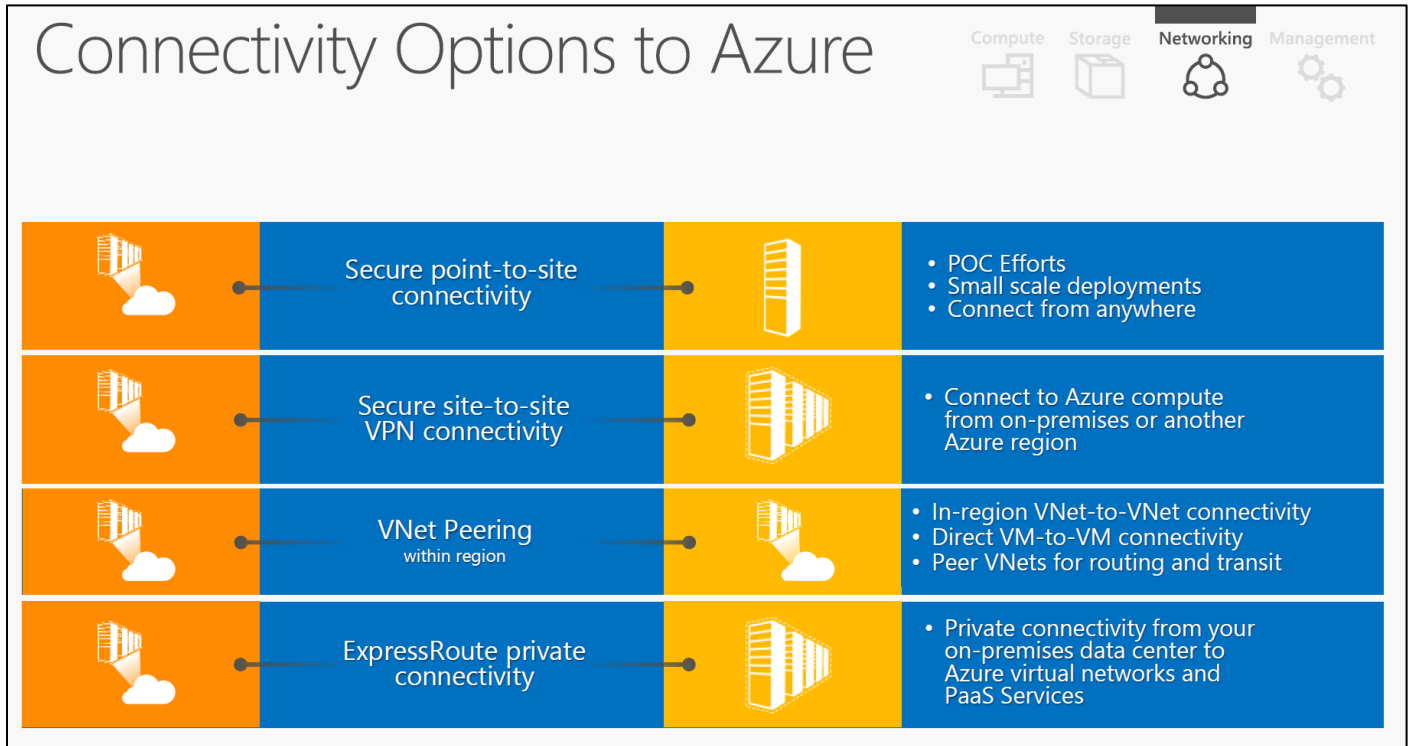
<sup>37</sup> Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, July 2016. <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>

- Includes both desktop and laptop computers
- PCs run operating systems (OSs) such as Windows, Apple OS X, and Linux
- PCs can be used for any of the remote access methods described in this document
- Mobile devices
  - Small mobile computers such as smartphones and tablets, which often run a mobile-specific OS such as Apple iOS and Google Android.
  - Most often used for remote access methods using web browsers, primarily SSL VPNs and individual web application access.
  - Differences between PCs and mobile devices is decreasing; still, the security controls available for PCs and mobile devices are different.

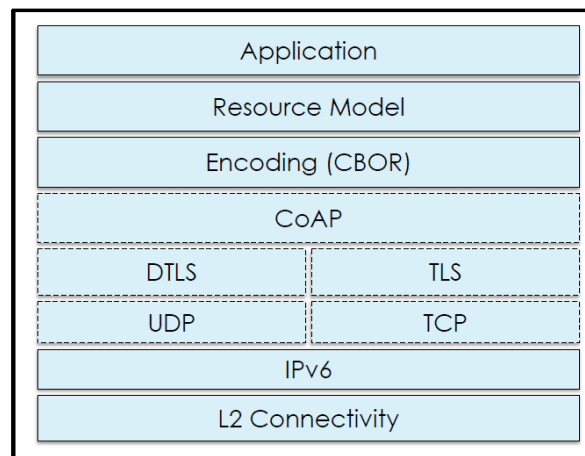
## REMOTE CONNECTIVITY PICTORIAL RESEARCH

- Remote connectivity graphics are to assist with understanding the technology.
  - Some graphics are from already identified sources in this document.
    - Where not applicable, references are provided as known.
- It is understood that some graphics may not help one's understanding at all – viewer discretion is advised.





### Connectivity Options to Azure – 2018



### OCF Stack

### OCF Protocol Stack – Open Connectivity Foundation – March 2020

The details of Bridging may be implemented in many ways, for example, by using a Bridge Platform with an entity handler to interface directly to a Non-OCF device as shown in Figure 1.



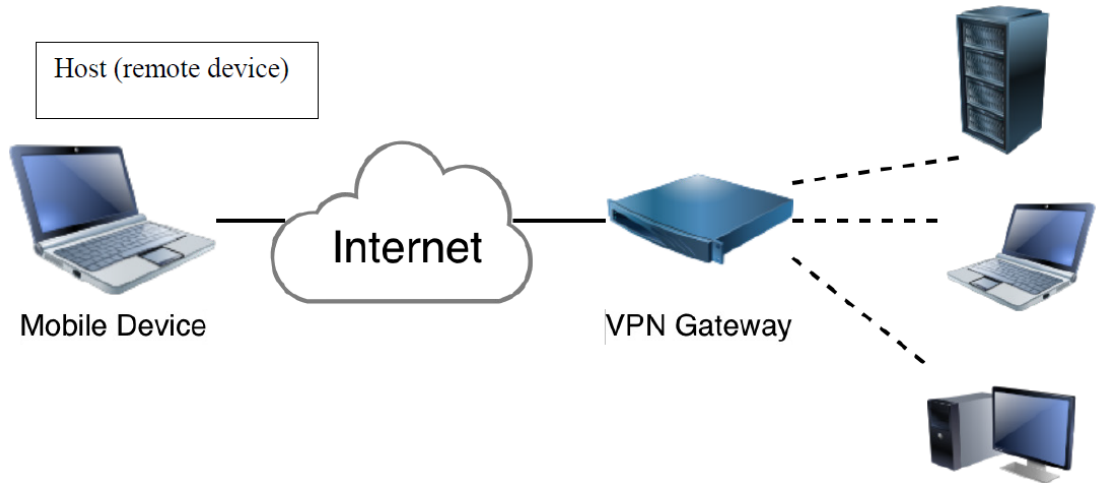
**Figure 1 – Server bridging to Non- OCF device**

On start-up the Bridge Platform runs the entity handlers which discover the non-OCF systems (e.g., Heart Rate Sensor Device) and create Resources for each Device or functionality discovered. The entity handler creates a Resource for each discovered Device or functionality and binds itself to that Resource. These Resources are made discoverable by the Bridge Platform.

**Open Connectivity Foundation – April 2020**

**2.4.2 Remote Access**

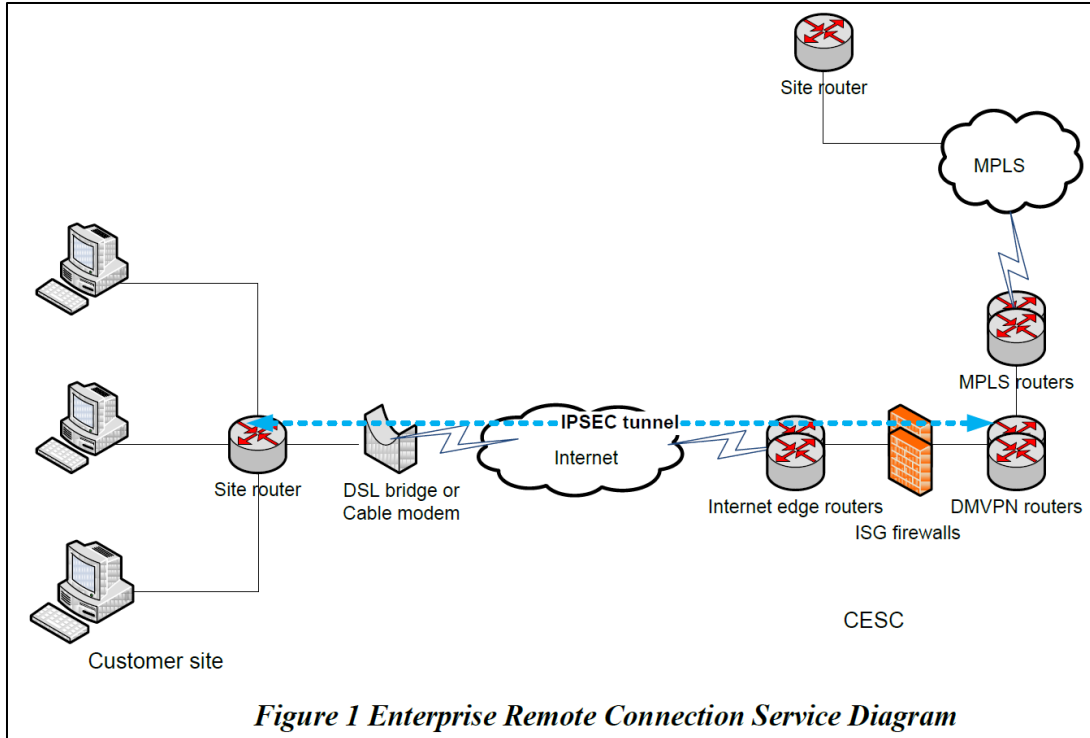
An increasingly common VPN architecture is the remote access architecture. The organization deploys a VPN gateway onto its network; each remote access user then establishes a VPN connection between their device (host) and the VPN gateway. As with the gateway-to-gateway architecture, the VPN gateway may be a dedicated device or part of another network device. Figure 3 shows an example of an IPsec remote access architecture that provides a protected connection for the remote user.



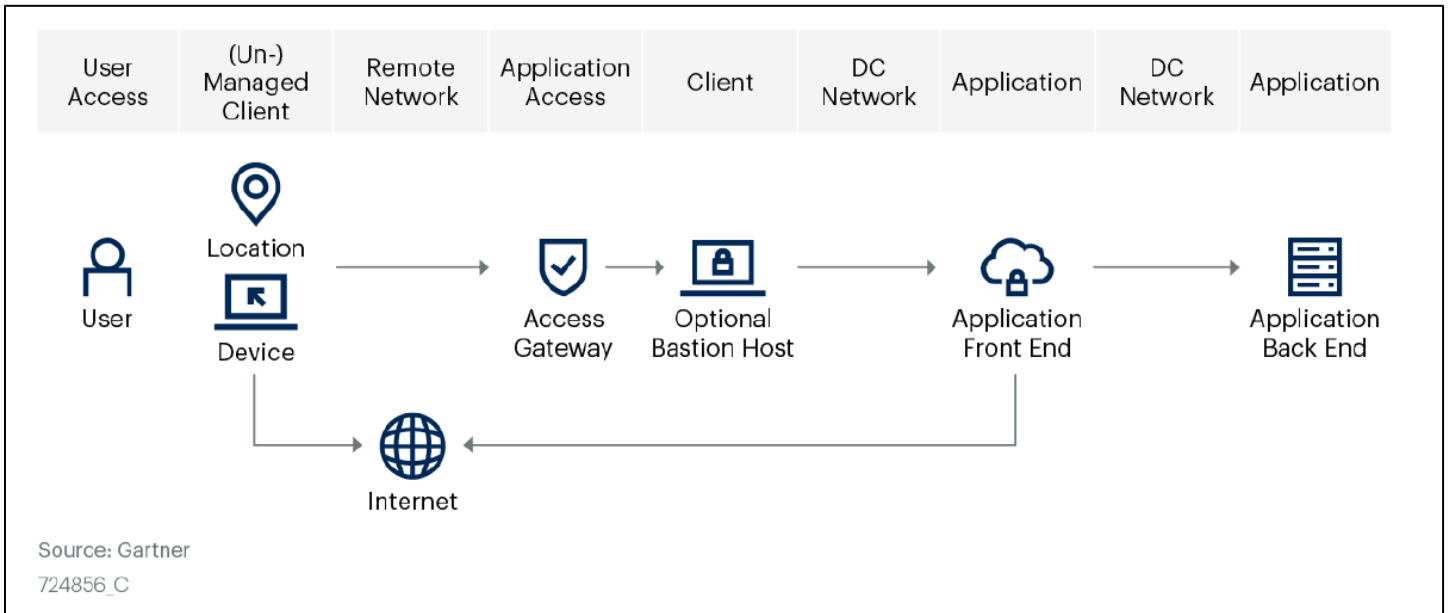
**Figure 3: Remote Access VPN Architecture Example**

**NIST SP-800-71 Rev-1**

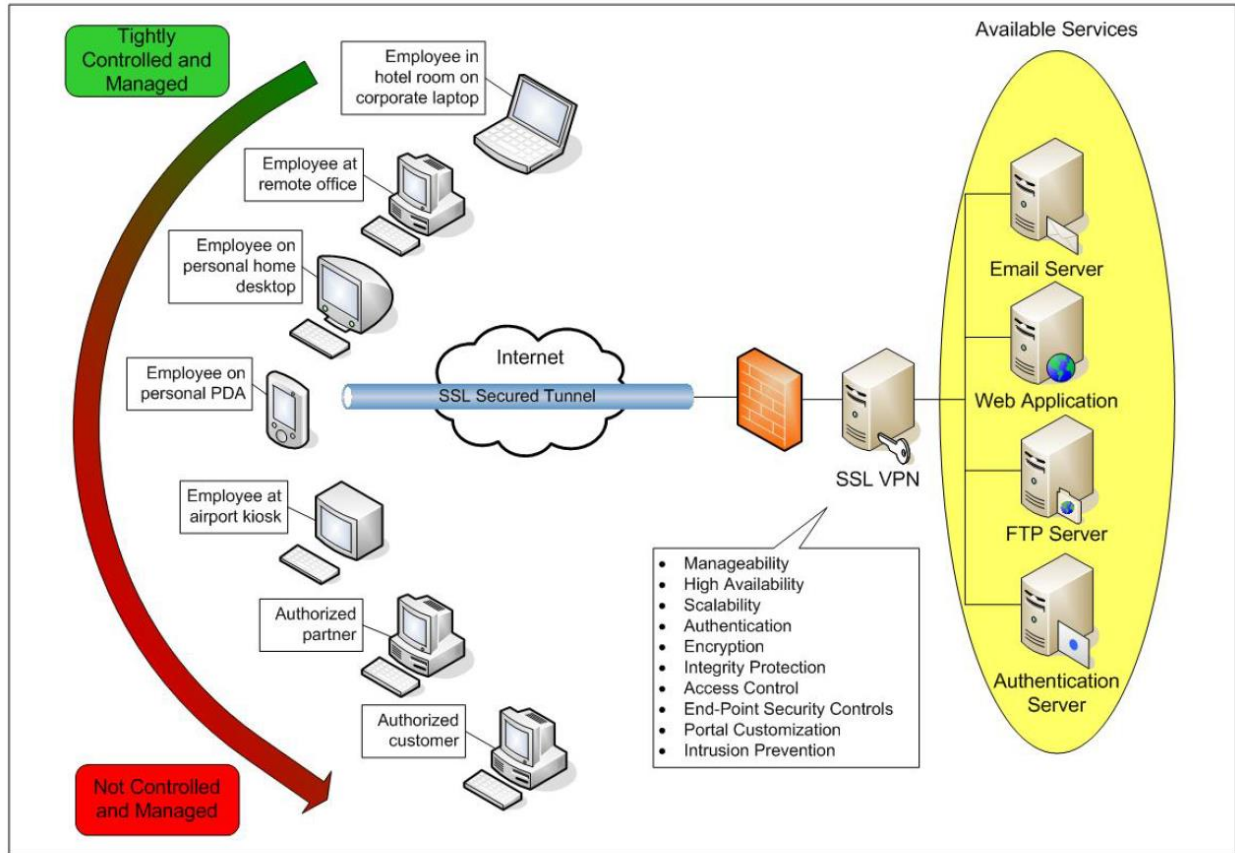




VITA ECRS Service – 2017



Analyzing Traffic Patterns for Remote Work Use Cases – Gartner, June 2020

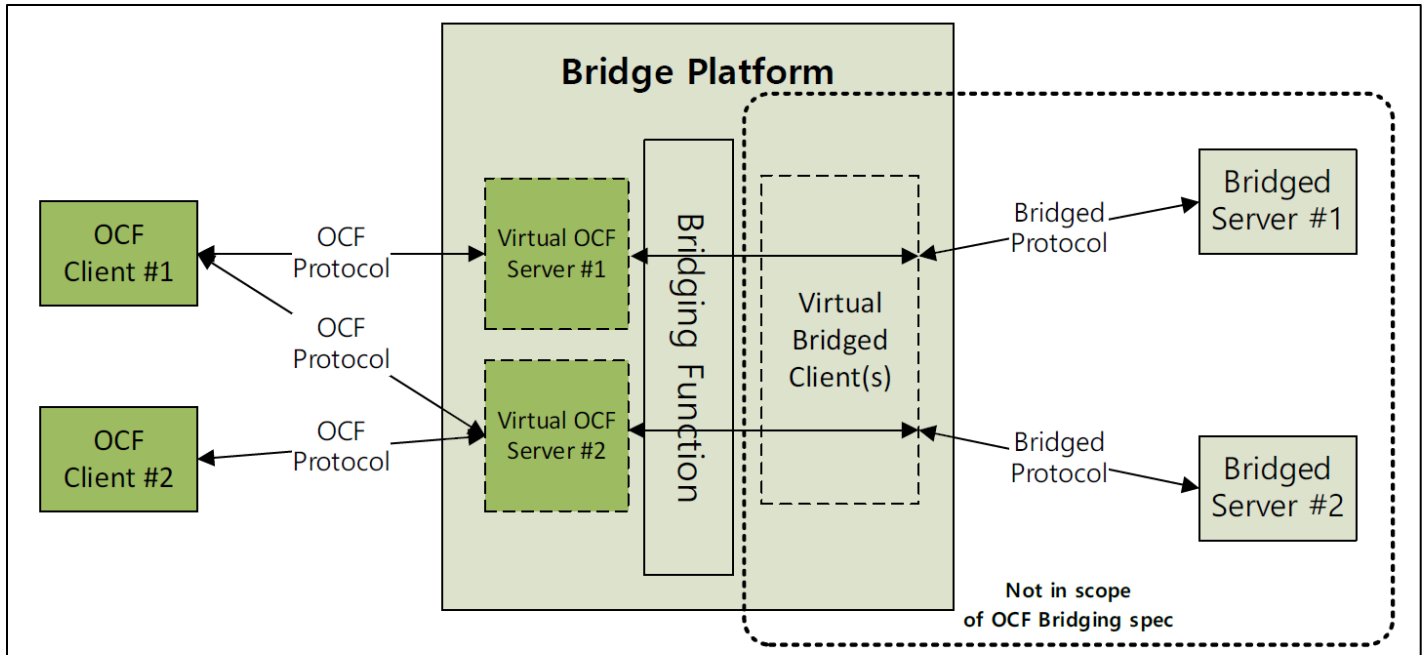


**Figure 3-1. SSL VPN Architecture**

**NIST 800-113**



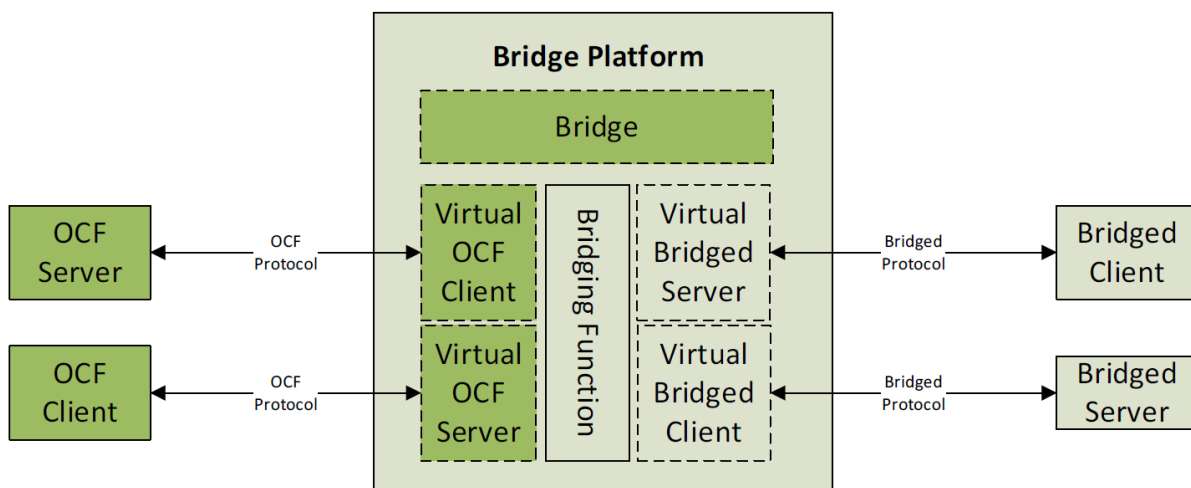
**Remote Access Policy Development – InfoSec Institute**



**Figure 4 – Asymmetric server bridge**

In Figure 4 each Bridged Server is exposed as a Virtual OCF Server to OCF side. These Virtual OCF Servers are same as normal OCF Servers except that they have additional rt value ("oic.d.virtual") for "/oic/d". The details of the Virtual Bridged Client are not in scope of this document.

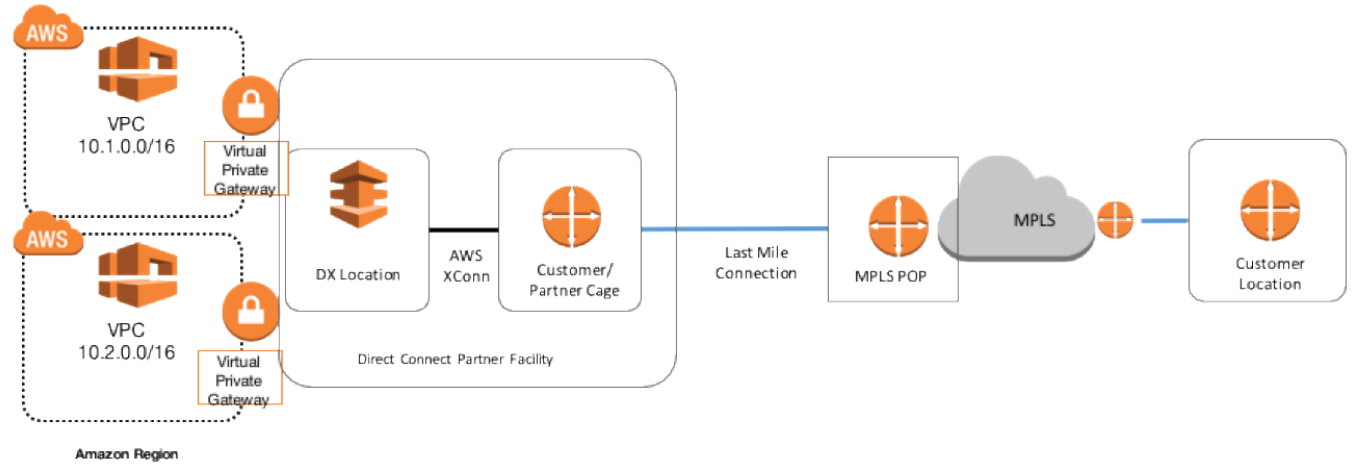
**Open Connectivity Foundation – April 2020**



**Figure 2 – Bridge Platform components**

**Open Connectivity Foundation – April 2020**

Figure 1 shows a physical collocation topology for single data center connectivity to AWS.



**Figure 1: Single data center connection over MPLS with customer-managed CGW in a collocation scenario**

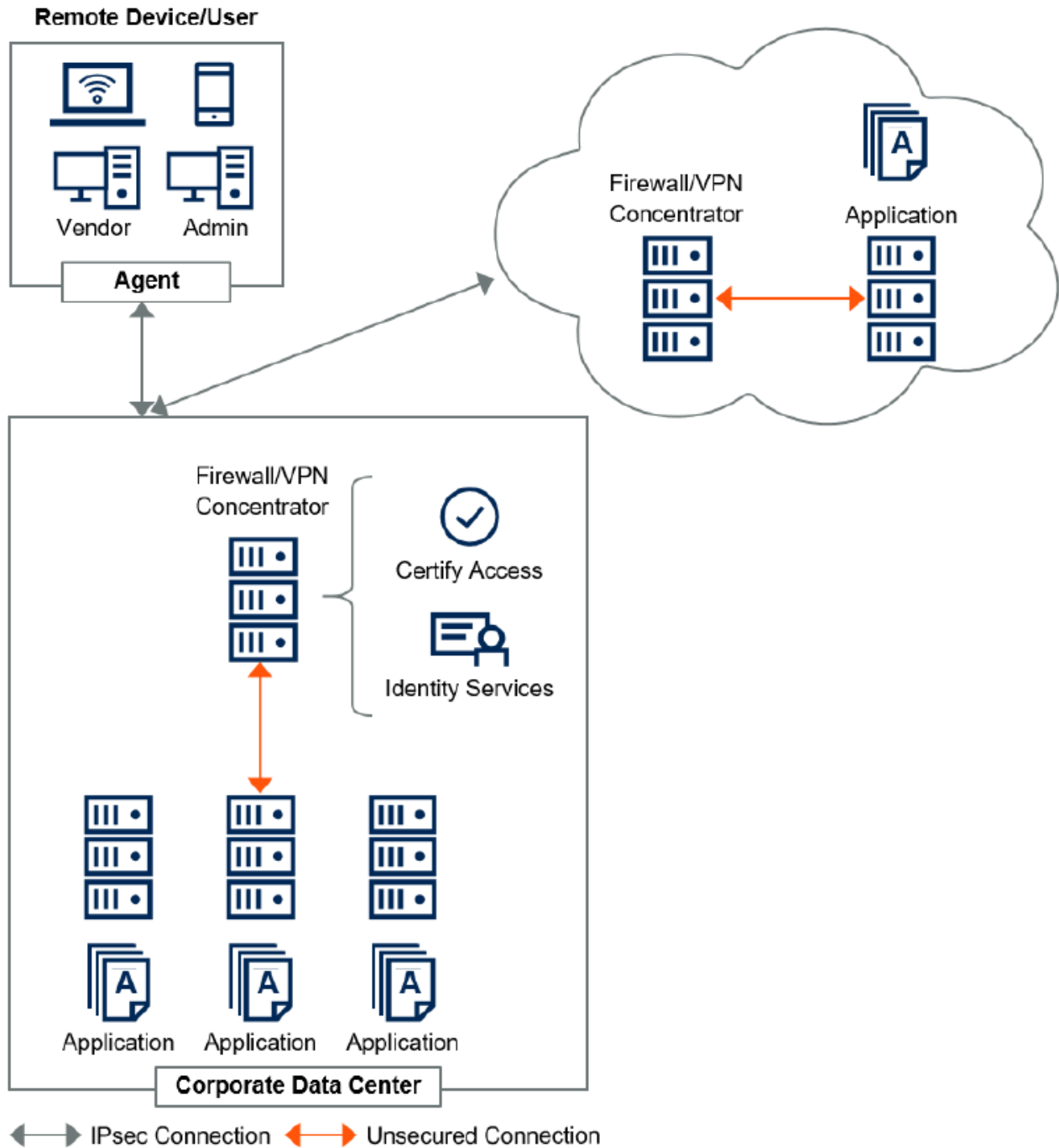
**Physical Collocation Topology for Single DC Connectivity to AWS – March 2020**

Applications	Service Properties
	Priority      Acceleration      Encryption
Corporate applications - ERP - CRM	High      TCP/HTTP      Yes
Unified communications - VoIP - Video conferencing - Screen sharing	High      RTP compression      Yes
SaaS/Cloud applications	Medium      TCP/HTTP      Yes
Email	Medium      TCP/HTTP      Yes
File sharing	Low      TCP/HTTP      Yes
Internet data and video	Low      TCP/HTTP      Yes
Data multicasting – file distribution	Medium      No      No

**Typical Transport Services for Enterprise Applications – ST Engineering Direct – 2020**

Typical enterprise applications can be served with different transport IP services. The service properties vary in the need for encryption, the need for acceleration and the sensitivity to latency and jitter.

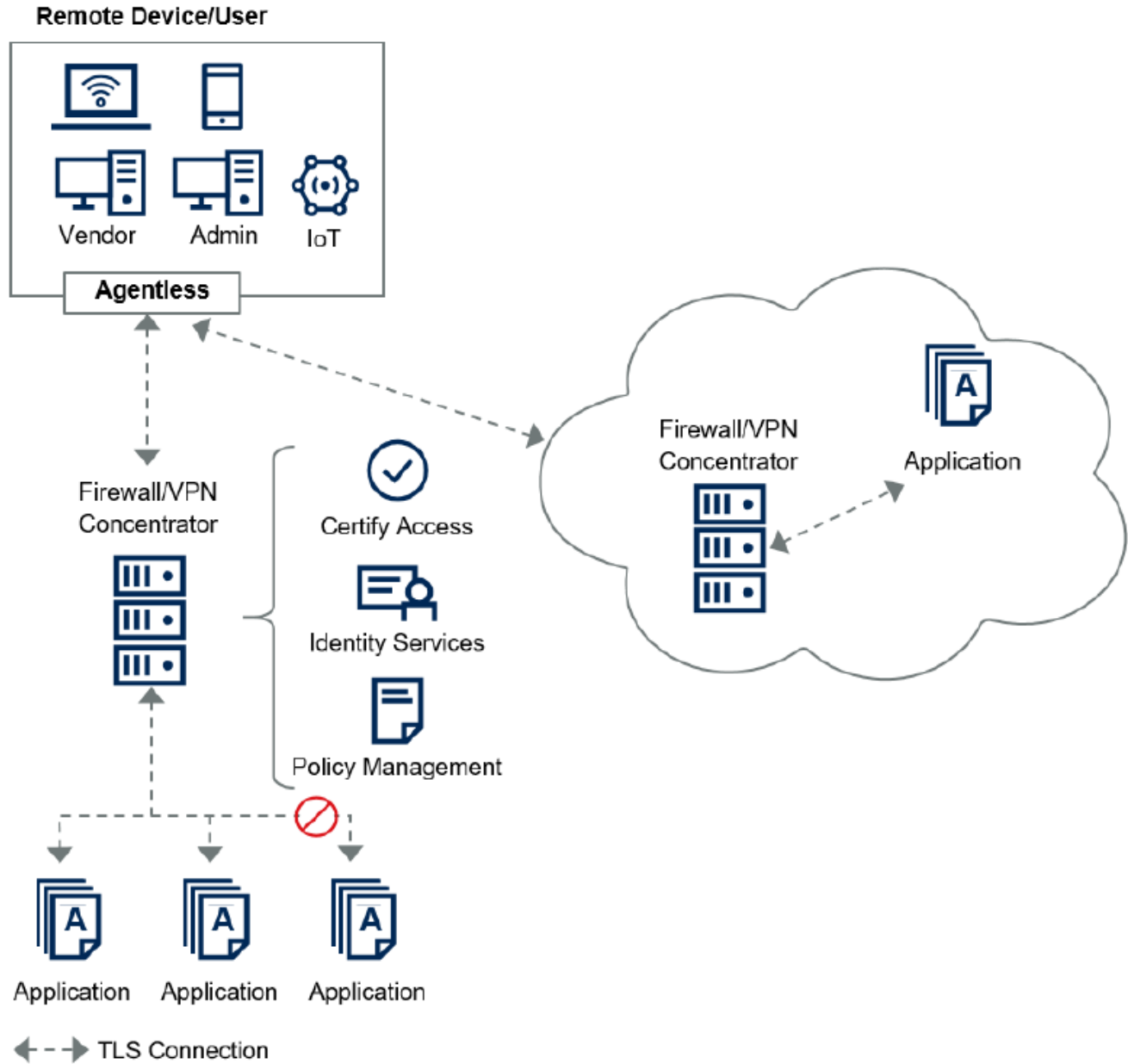
**IPsec VPN**



Source: Gartner  
ID: 380285

**IPsec VPN Remote Network Access Option – Gartner – June 14, 2019**

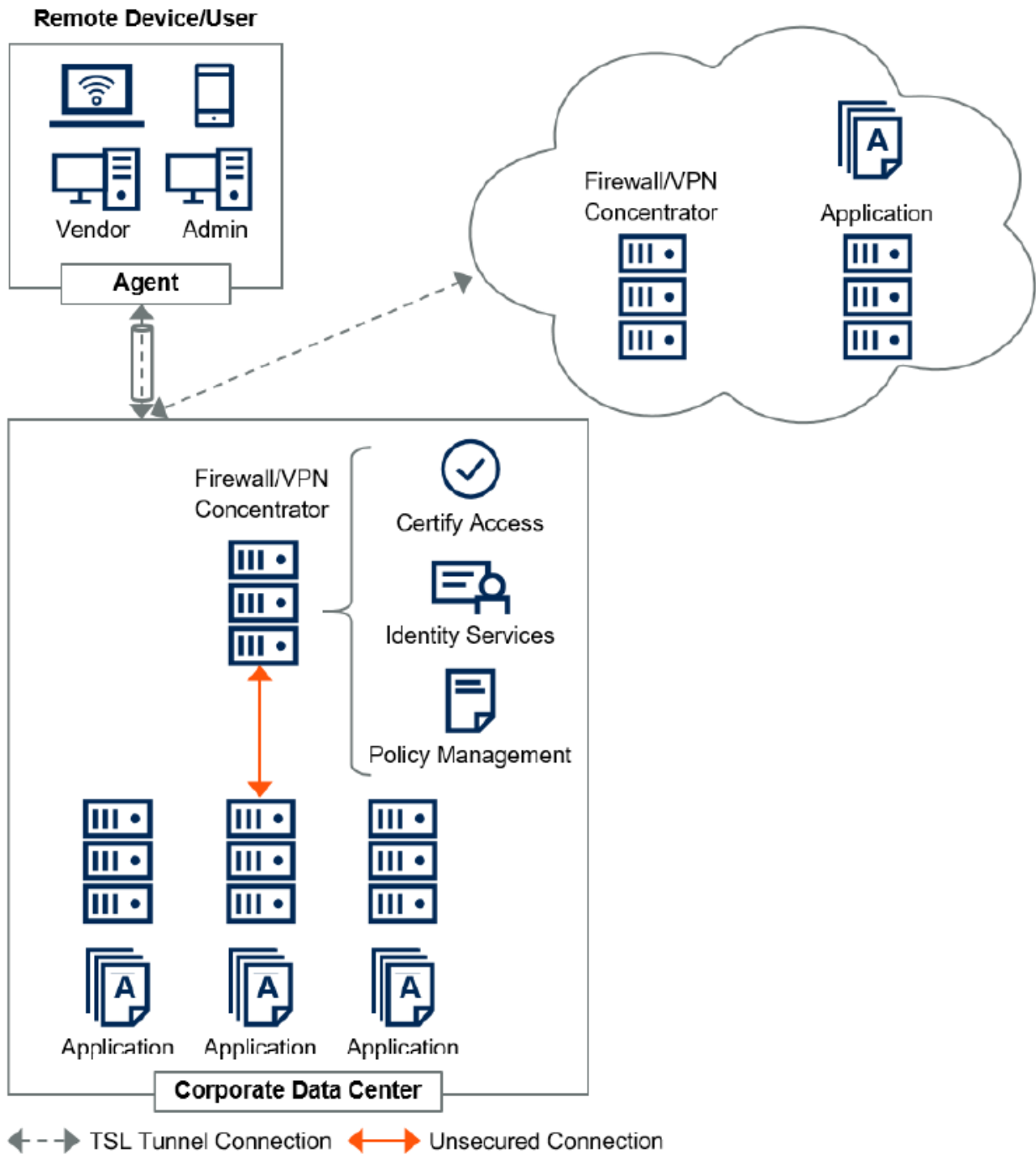
## TLS VPN



Source: Gartner  
ID: 380285

TLS VPN Remote Network Access Option – Gartner – June 14, 2019

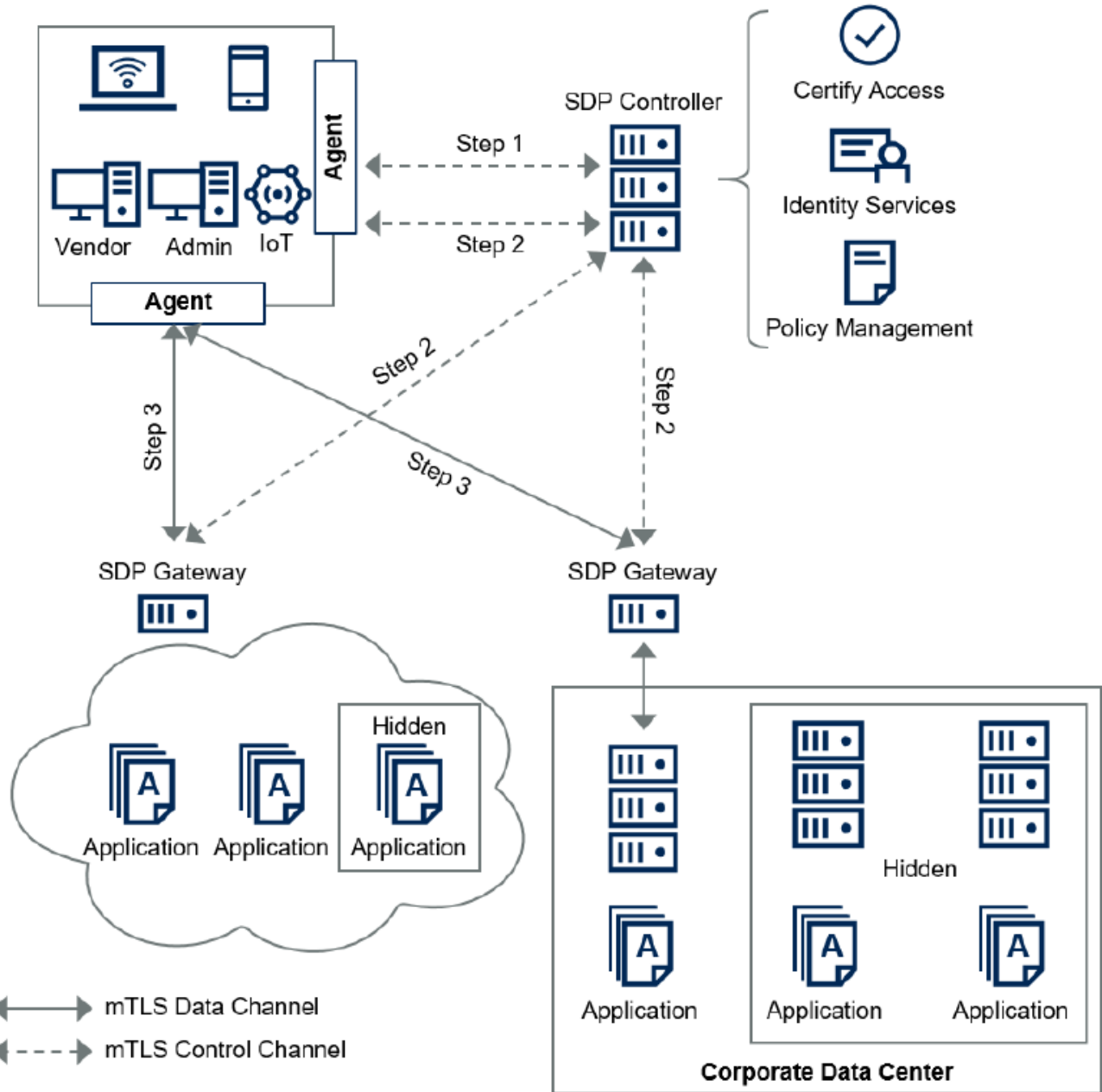
## TLS Tunnel



Source: Gartner  
ID: 380285

### TLS Tunnel Remote Network Access Option – Gartner – June 14, 2019

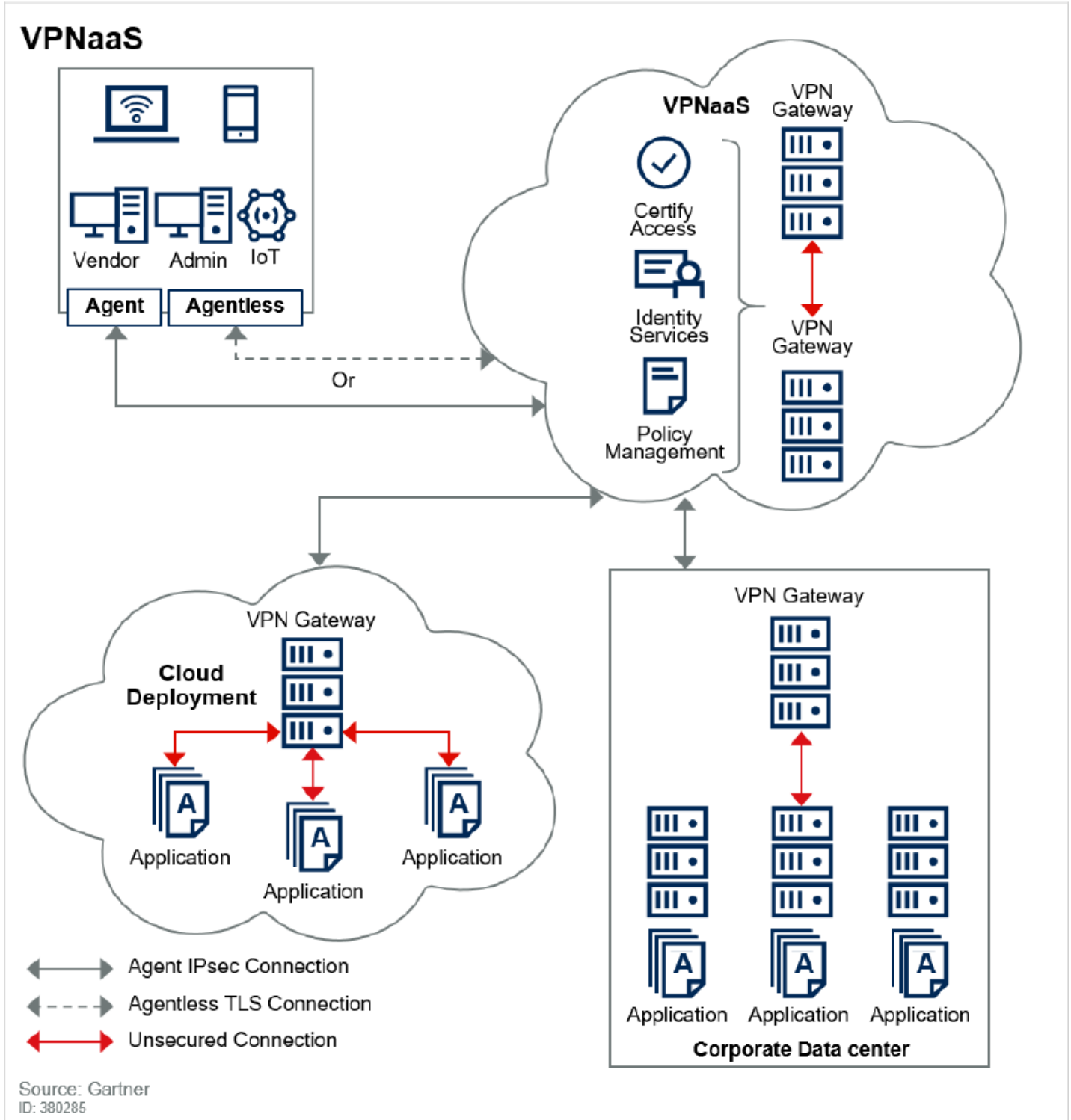
**SDP**



Source: Gartner  
ID: 380285

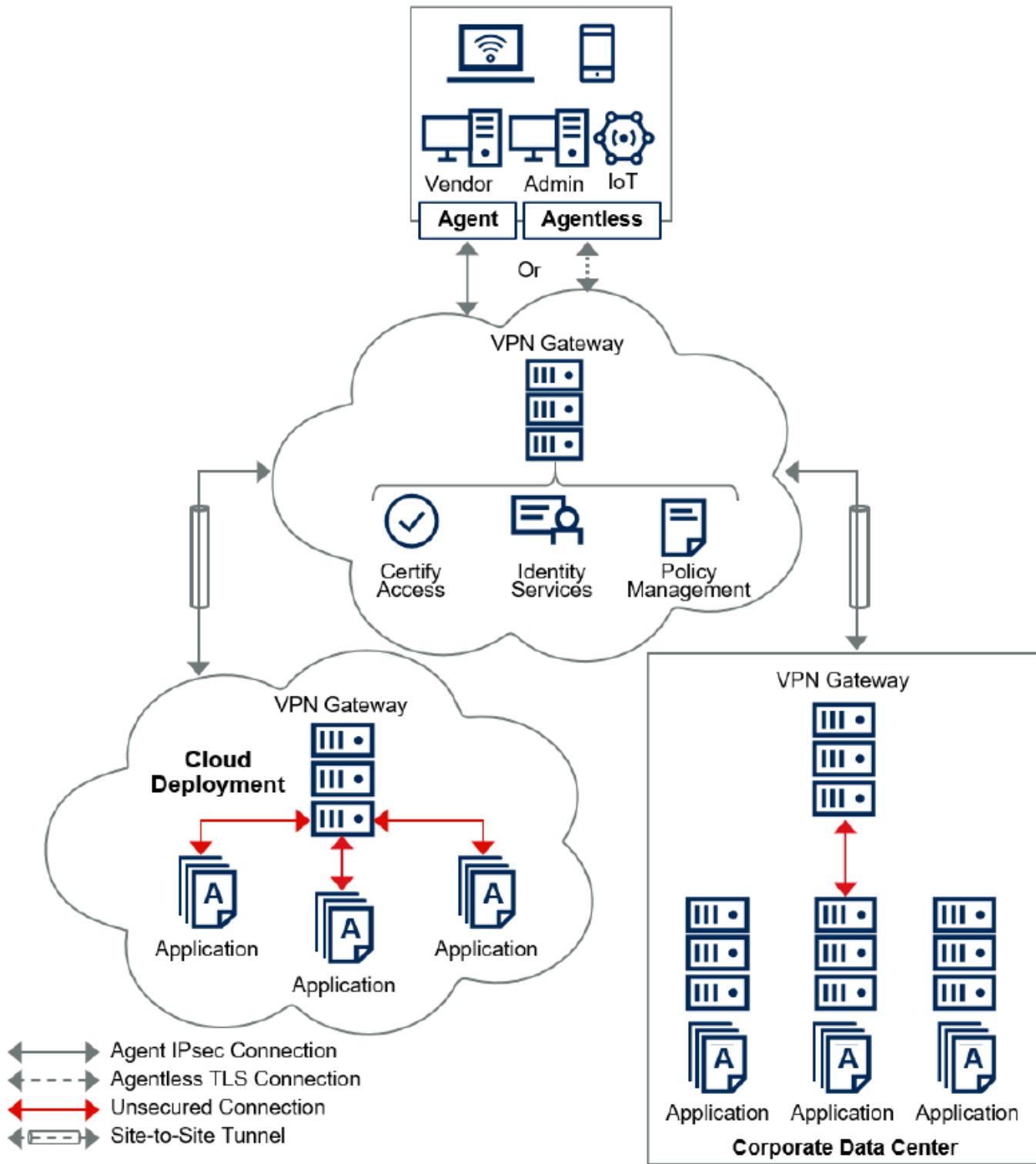
**SDP Remote Network Access Option – Gartner – June 14, 2019**





VPNaaS Remote Network Access Option – Gartner – June 14, 2019

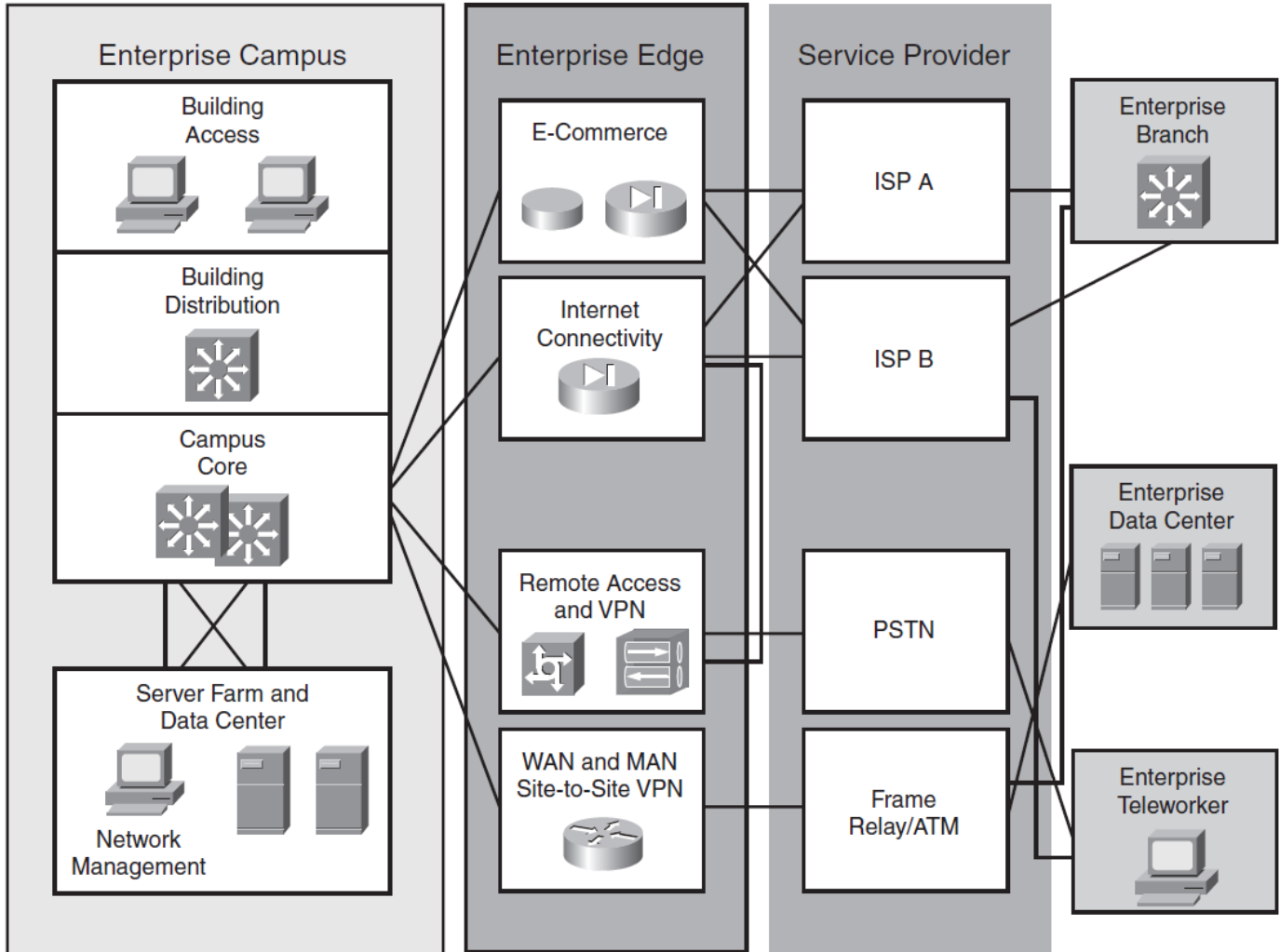
## Customer-Run Cloud VPN



Source: Gartner  
ID: 380285

Customer Run Cloud VPN Remote Network Access Option – Gartner – June 14, 2019

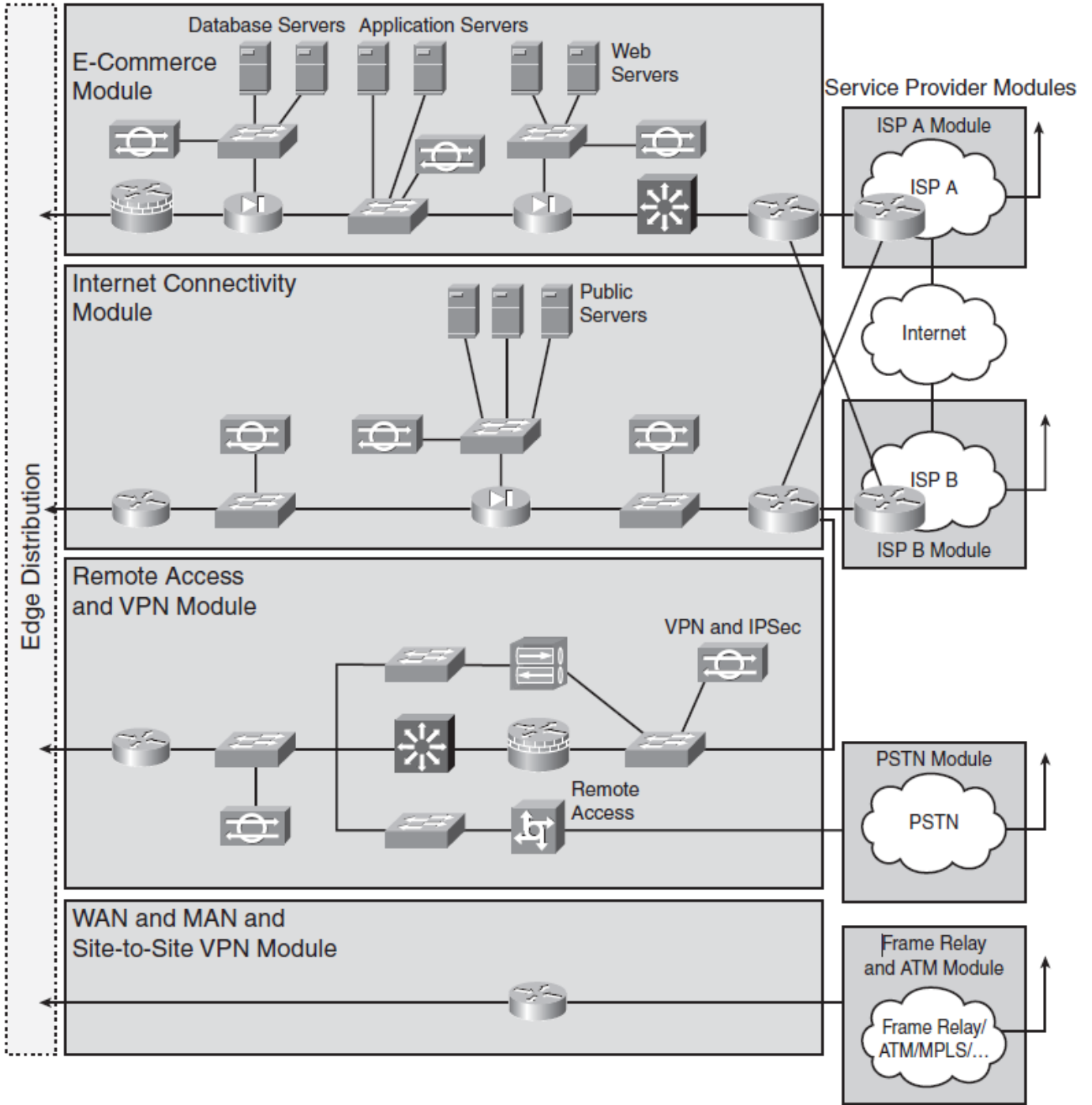
Figure 3-9 Cisco Enterprise Architecture



CISCO Enterprise Architecture Network Model – PTG Media – 2019

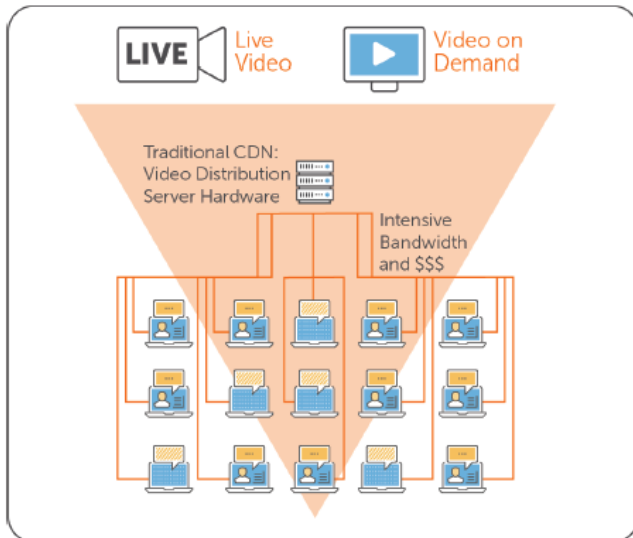
See following diagram for more in-depth view of the Enterprise Edge section of this diagram.

**Figure 3-12 Enterprise Edge Functional Area**

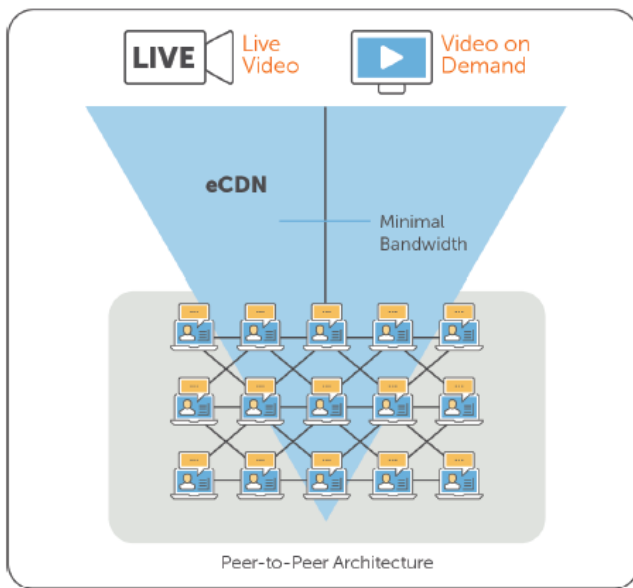


**CISCO Enterprise Edge Functional Area – PTG Media – 2019**

Let's look at old models versus a Software-Defined model for video delivery.



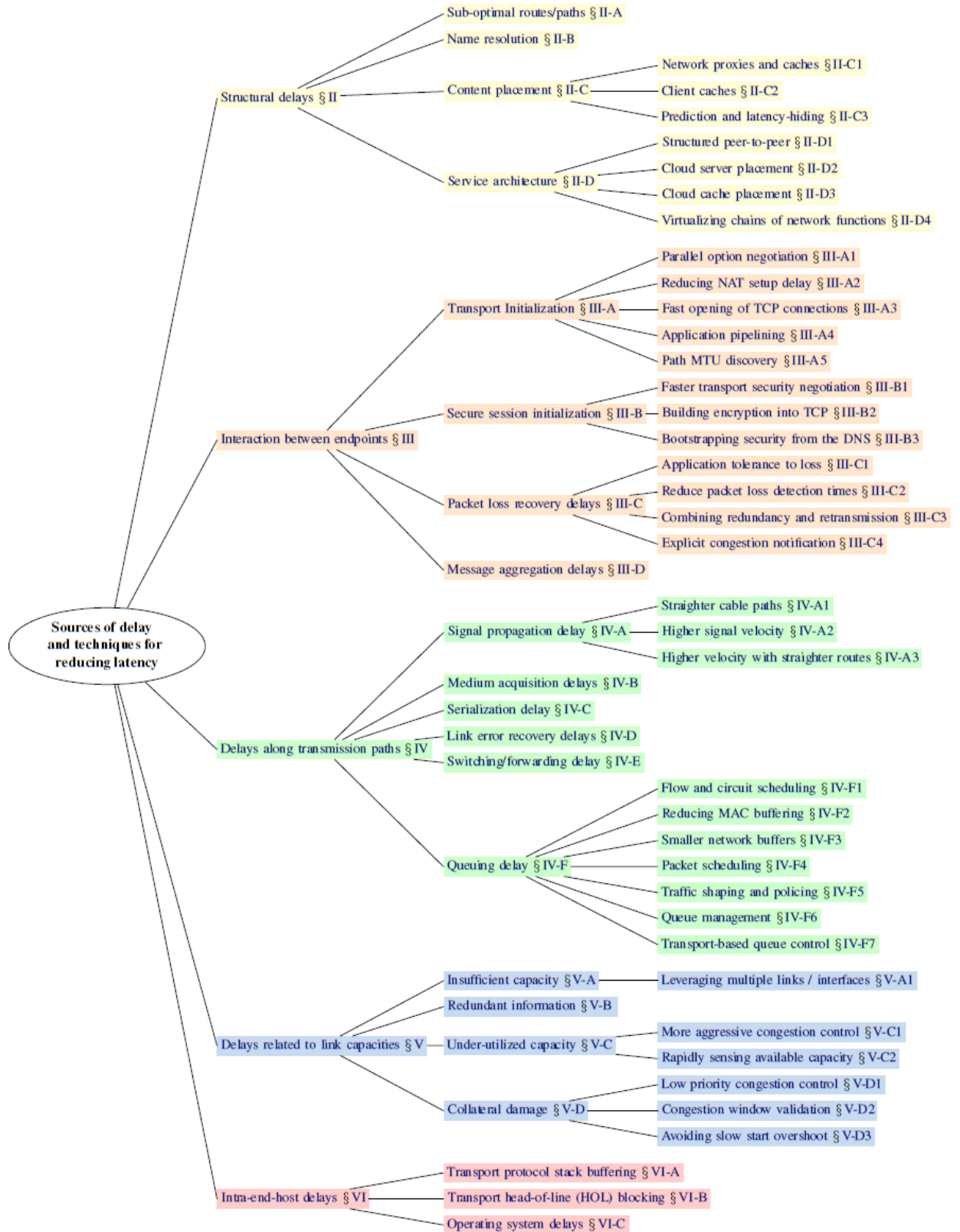
**Figure 1:** With this older model, each endpoint will download the video file from the nearest distribution point server. With the size of a live streaming video, this needs to be done at each location to avoid excessive load on the WAN links. The traditional approach is not only expensive, both short term and long term, but imposes a significant maintenance and operational overhead on the enterprise.



**Figure 2:** With the Riverbed approach, there are no distribution point servers required. The agent intelligently creates a single virtual distribution point spanning all nodes such that content like video files are sent only once over a WAN link. The platform is highly resilient with very low operational overhead. The eCDN built into Riverbed SaaS Accelerator brings several benefits to an enterprise video communication strategy:

- Ability to support increasing video while reducing the impact on the network
- No additional hardware required, reduction in distribution points by up to 99%
- Event analytics and network analytics that are easy to access and immediately actionable
- Automatic adjusting to changes in traffic patterns and physical changes in the underlying network

### Software Defined Video Delivery – Riverbed – 2021



2. Techniques for reducing latency organized by sources of delay.

## Reducing Internet Latency – IEEE Communications Surveys & Tutorials (To appear)

**Table 1. Representative Vendors of ZTNA as a Service**

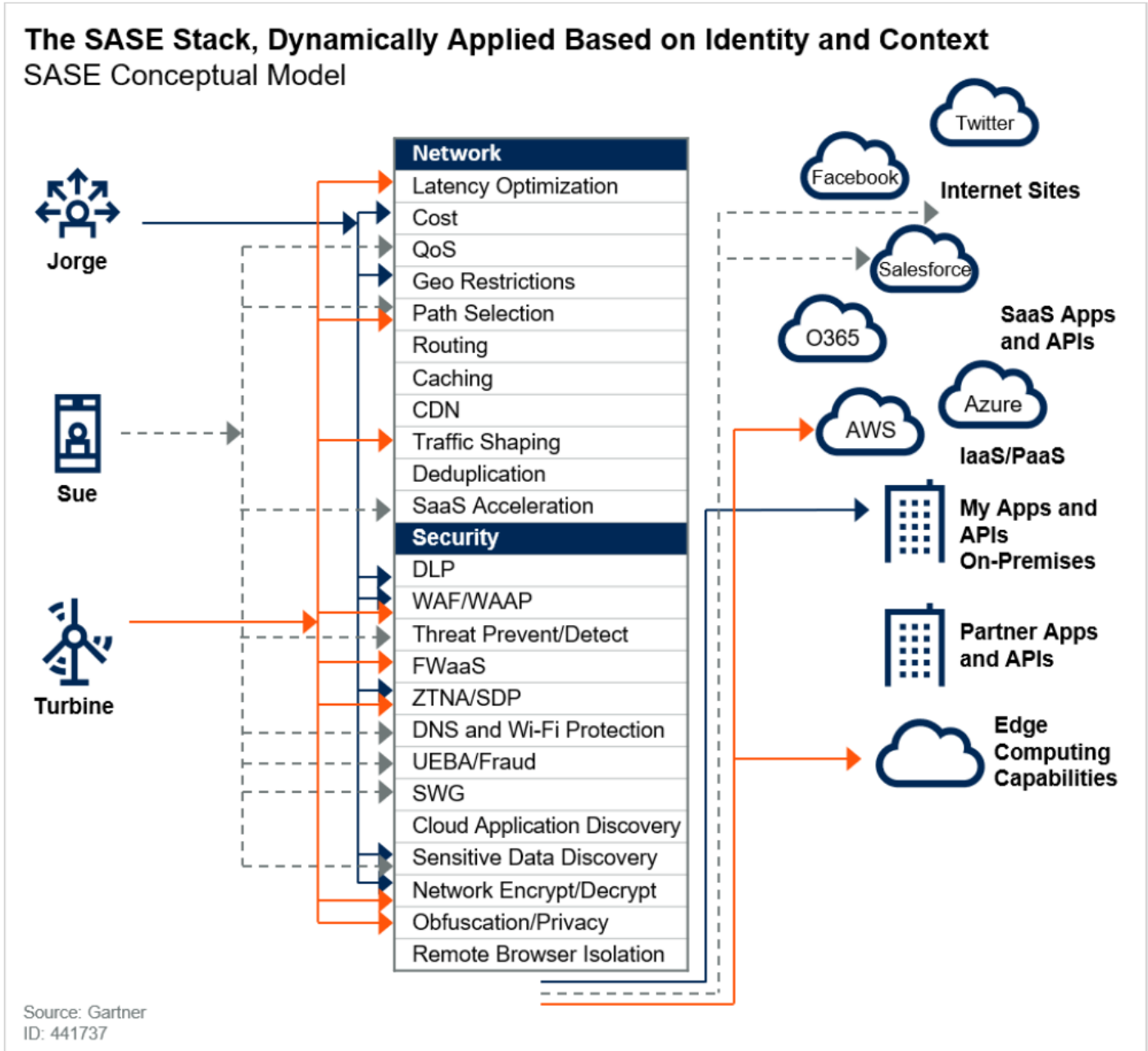
Vendor	Product or Service Name
Akamai	Enterprise Application Access
Cato Networks	Cato Cloud
Cisco	Duo Beyond (acquisition by Cisco)
CloudDeep Technology (China only)	DeepCloud SDP
Cloudflare	Cloudflare Access
InstaSafe	Secure Access
Meta Networks	Network as a Service Platform
New Edge	Secure Application Network
Okta	Okta Identity Cloud (Acquired ScaleFT)
Perimeter 81	Software Defined Perimeter
SAIFE	Continuum
Symantec	Luminate Secure Access Cloud (acquisition by Symantec)
Verizon	Vidder Precision Access (acquisition)
Zscaler	Private Access
Source: Gartner (April 2019)	

### ZTNA as a Service (ZaaS) Representative Vendors – Gartner, 2020

**Table 2. Representative Vendors of Stand-Alone ZTNA**

Vendor	Product or Service Name
BlackRidge Technology	Transport Access Control
Certes Networks	Zero Trust WAN
Cyxtera	AppGate SDP
Google Cloud Platform (GCP)	Cloud Identity-Aware Proxy (Cloud IAP)
Microsoft (Windows only)	Azure AD Application Proxy
Pulse Secure	Pulse SDP
Safe-T	Software-Defined Access Suite
Unisys	Stealth
Waverley Labs	Open Source Software Defined Perimeter
Zentera Systems	Cloud-Over-IP (COiP) Access
Source: Gartner (April 2019)	

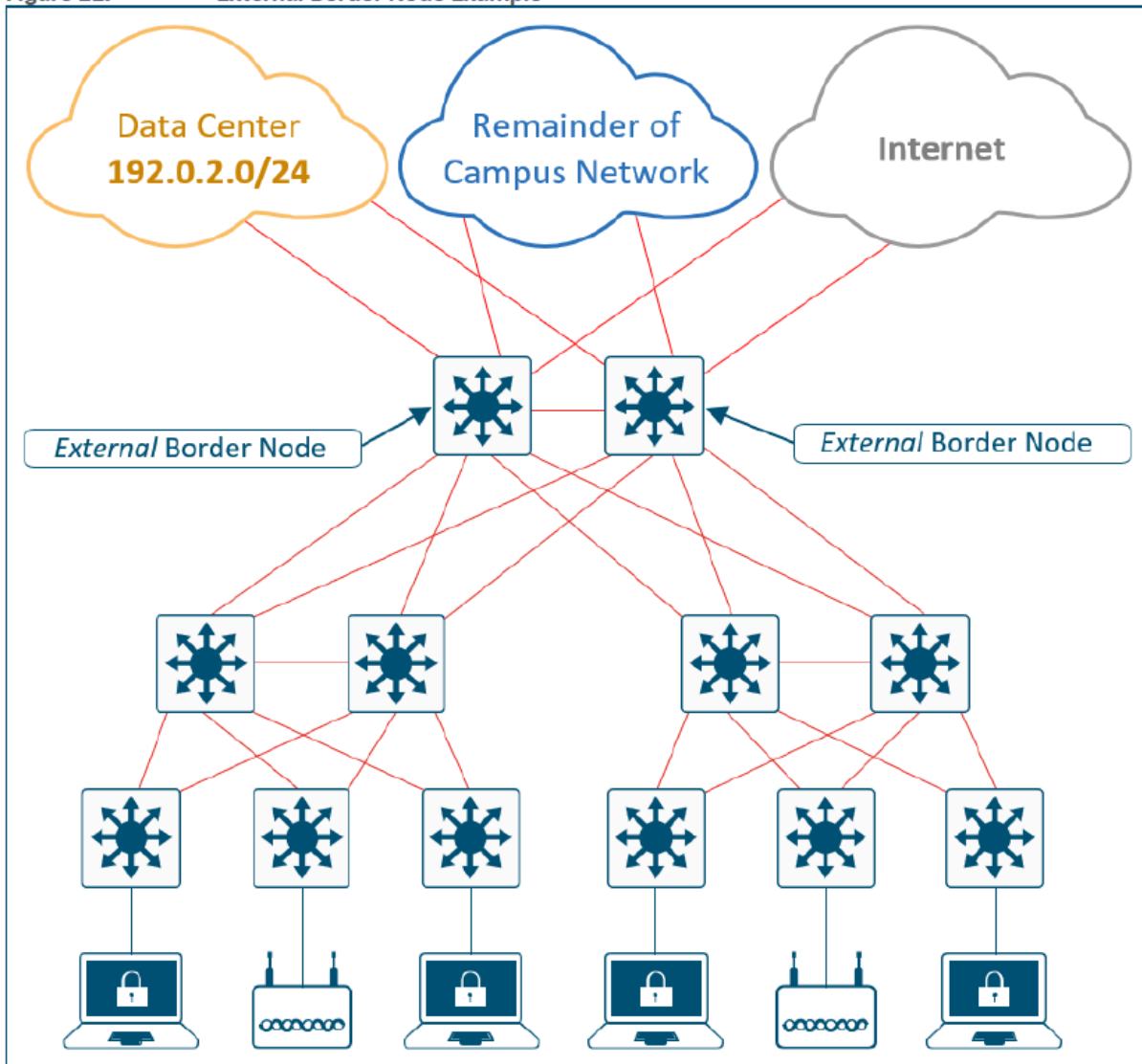
### ZTNA Standalone Representative Vendors – Gartner, 2020



SASE Stack – Dynamically Applied Based on Identity and Context – Gartner



Figure 22. External Border Node Example



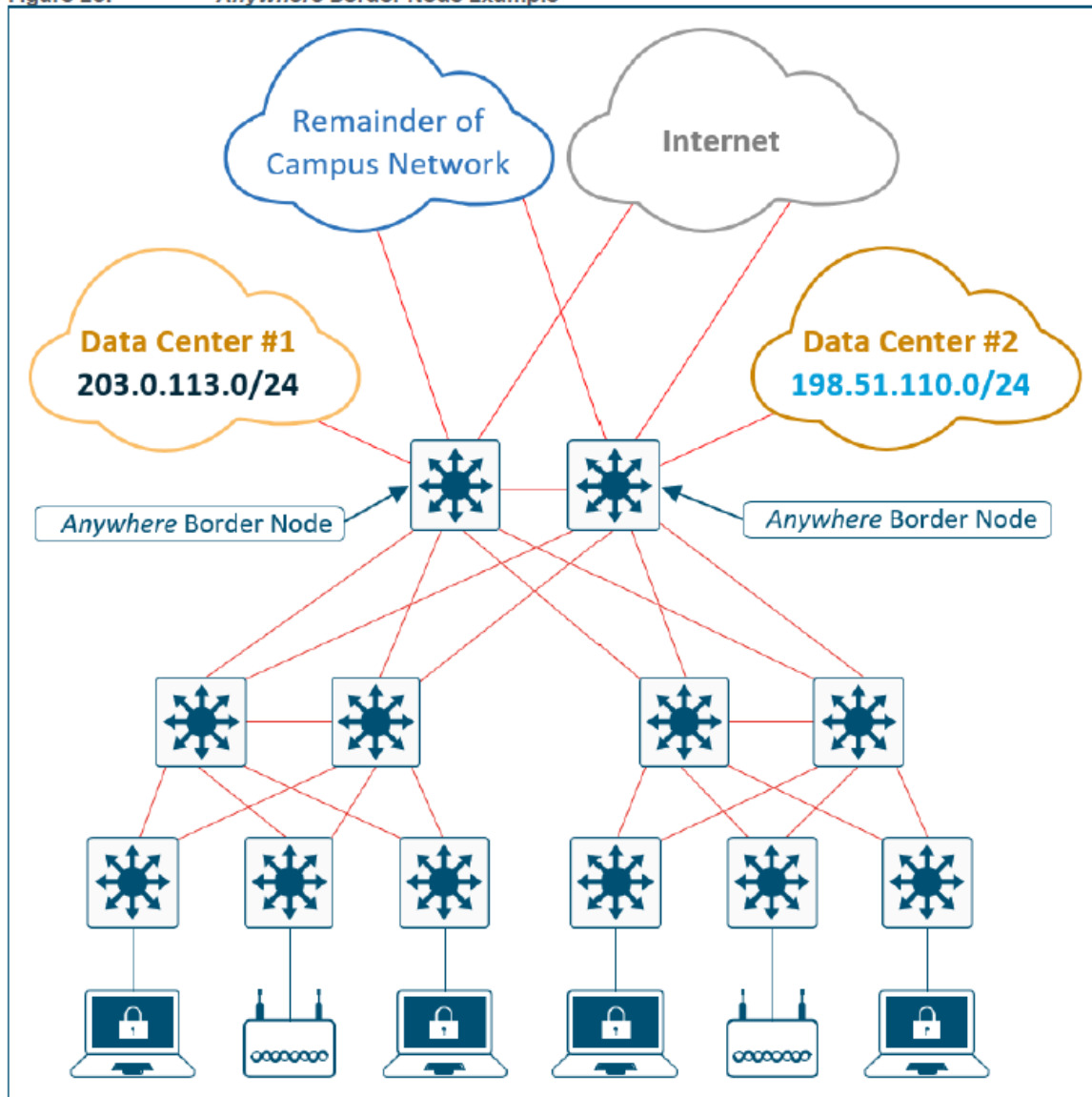
A border node may also be connected to both *known* and *unknown* networks such as being a common egress point for the rest of an enterprise network along with the Internet. What distinguishes this border is that *known* routes such as shared services and data center, are registered with the control plane node rather than using the default forwarding logic described above. This type of border node is sometimes referred to as an *Anywhere* border node.

### External Border Node Example

Software Defined Access Solution Design Guide by Cisco Public - June 2020

In Figure 23 below, both border nodes are connected to the Internet and to the remainder of the campus network. Each border node is also connected to a separate Data Center with different prefixes. If traditional, default forwarding logic is used to reach these prefixes, the fabric edge nodes may send the traffic to a border node not directly connect to the applicable data center. Traffic will have to inefficiently traverse the crosslink between border nodes. By importing the data center prefixes into LISP, the edge nodes can send the traffic to the border node on the left to reach **203.0.113.0/24** and the border node on the right to reach **198.51.100.0/24**. Either border can be used as the default path to the Internet.

**Figure 23. Anywhere Border Node Example**

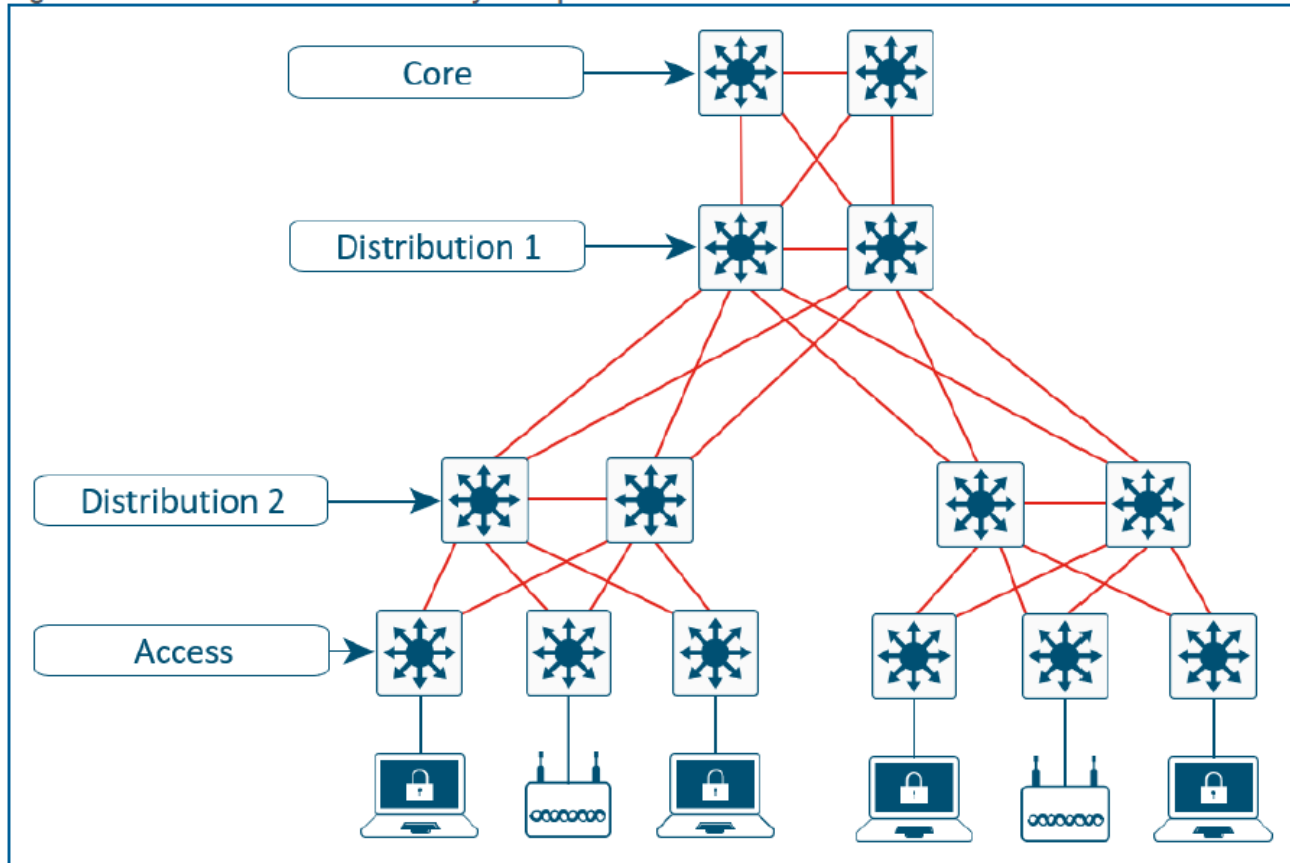


**Anywhere Border Node Example**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

If the network has more than three-tiers, multiple LAN Automation sessions can be performed sequentially. In Figure 26, if the seed devices are the core layer, then the Distribution 1 and Distribution 2 devices can be discovered and configured through LAN Automation. To discover the devices in the Access layer, a second LAN Automation session can be started after the first one completes. This second session could define Distribution 1 or Distribution 2 as the seed devices for this new LAN Automation workflow.

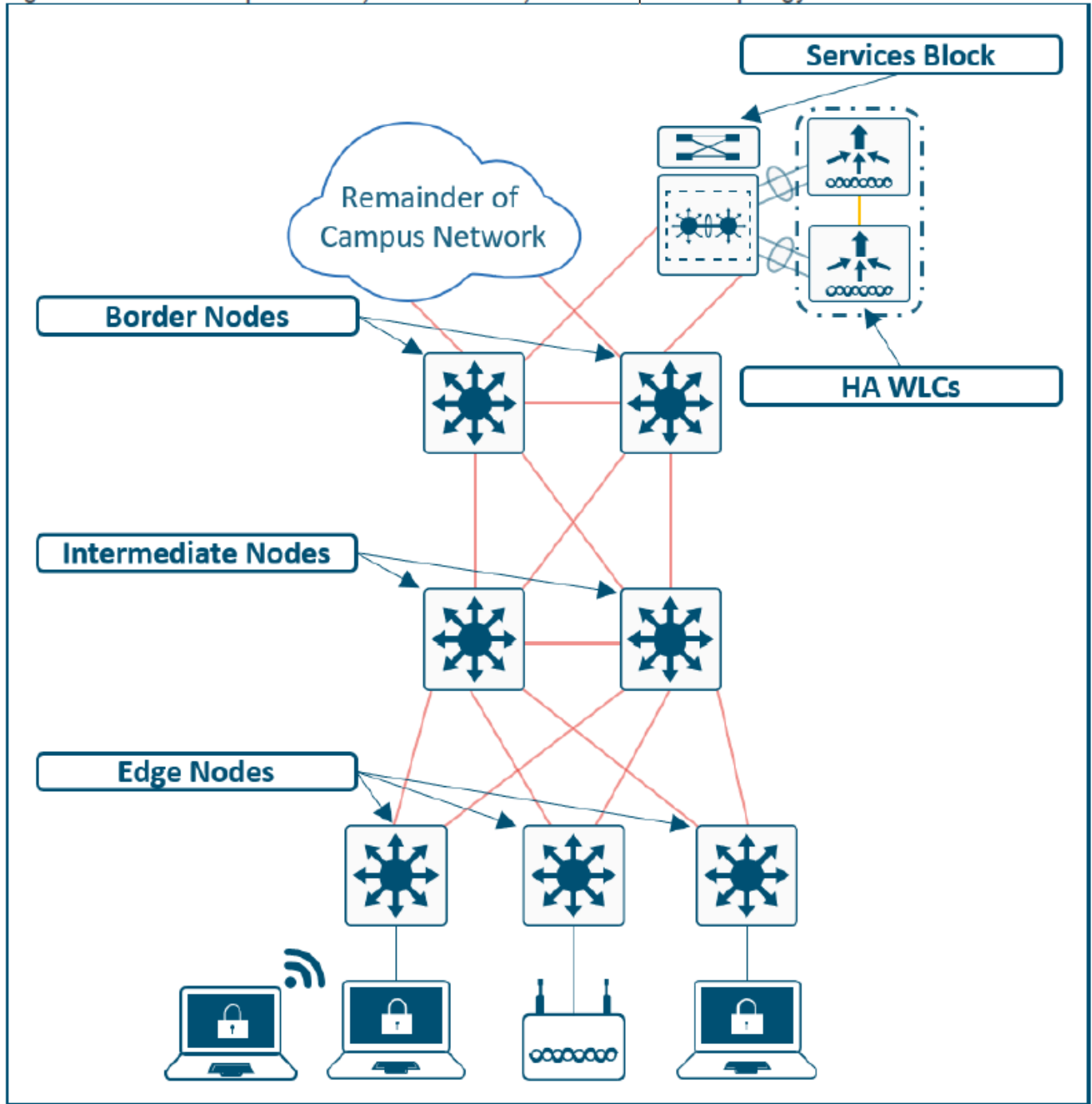
**Figure 26. Four-Tier Hierarchy Example**



**Four-Tier Hierarchy Example**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

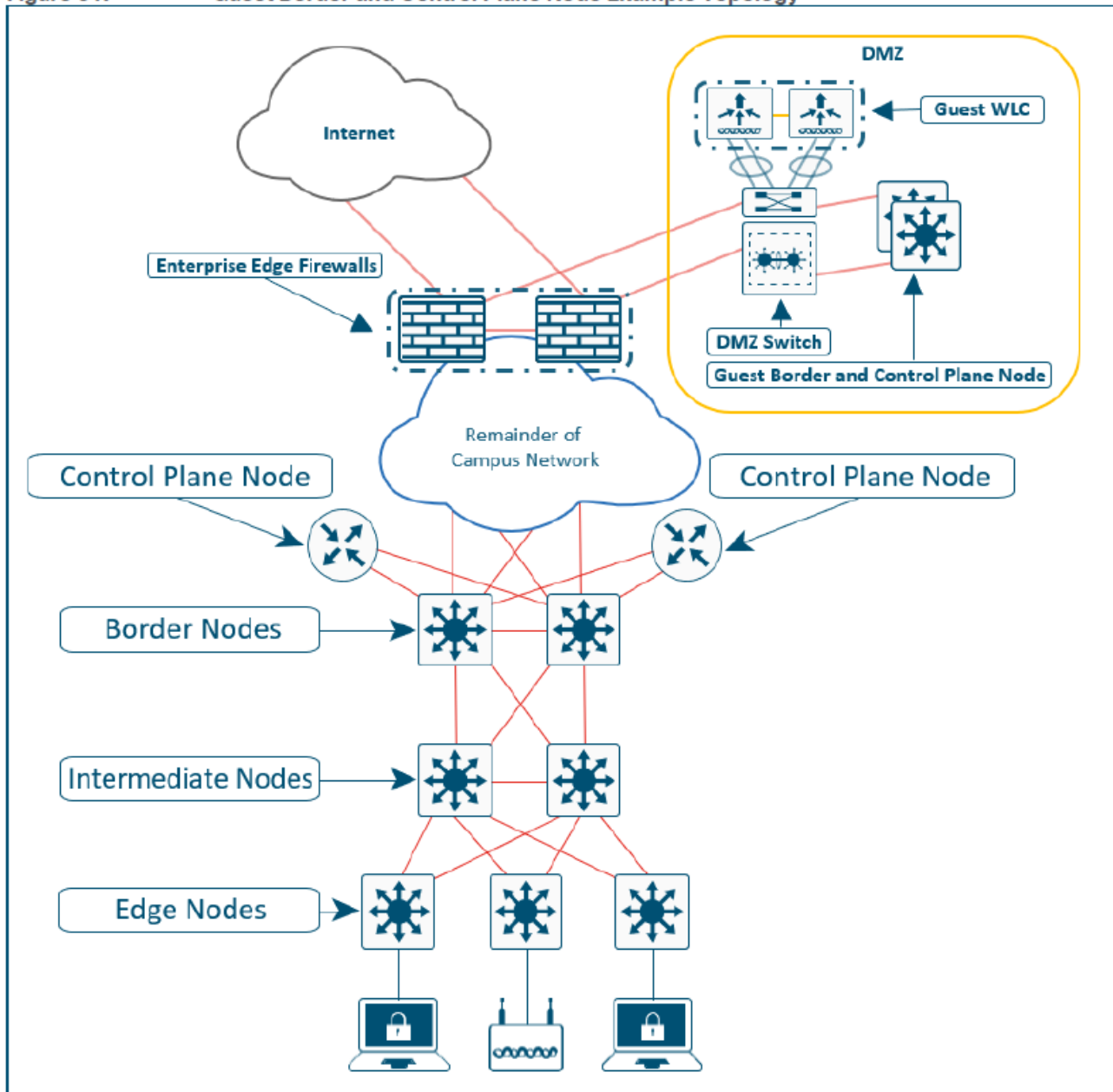
**Figure 29. Simplified WLC, Services Block, and Border Node Topology**



**Simplified WLC, Services Block, and Border Node Topology**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

**Figure 31. Guest Border and Control Plane Node Example Topology**

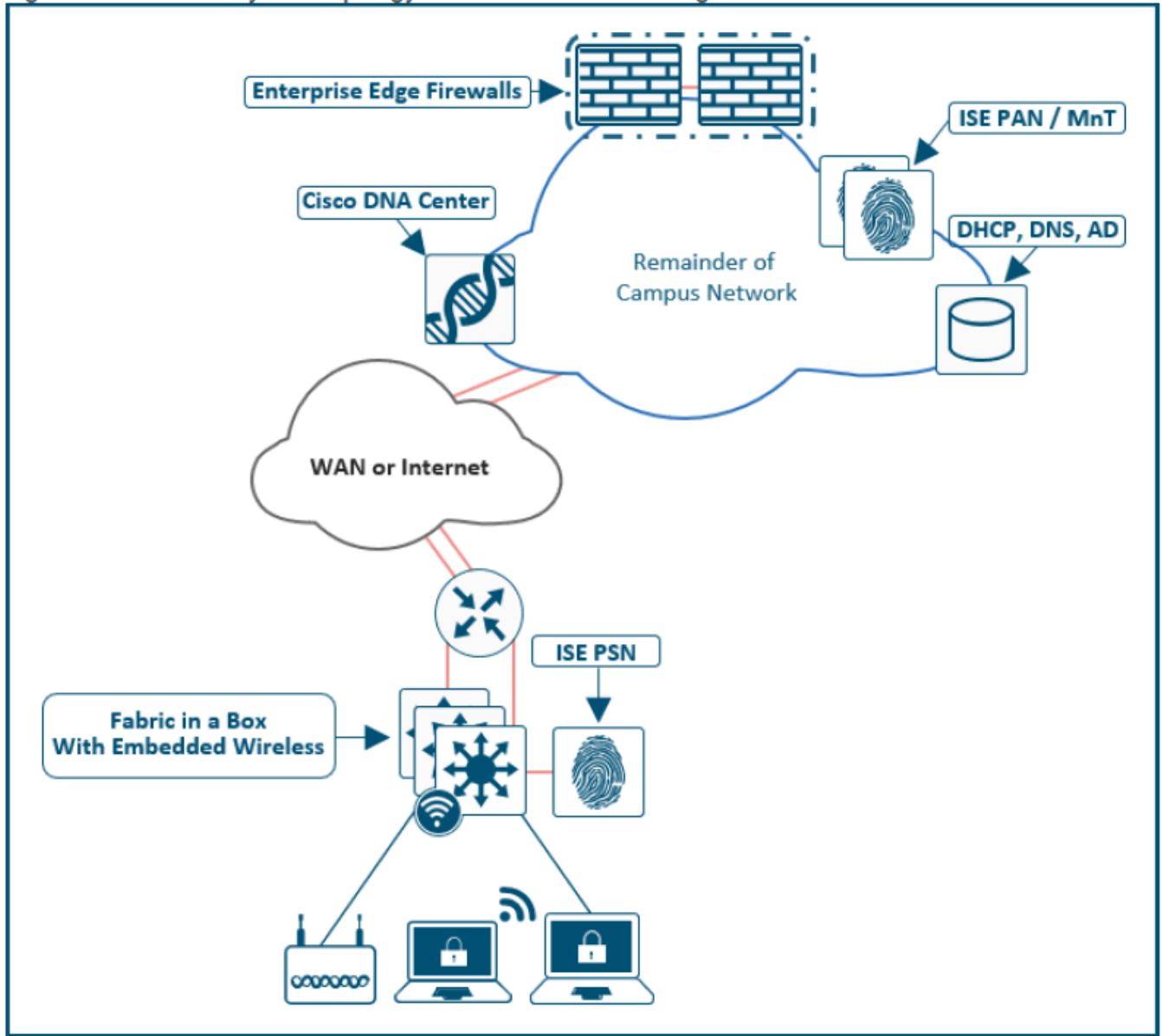


A maximum of two control plane nodes can be deployed for guest traffic. The result is a fabric site can have two control plane nodes for Enterprise traffic and another two for Guest traffic as show in [Figure 20](#).

**Guest Border and Control Plane Node Example Topology**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

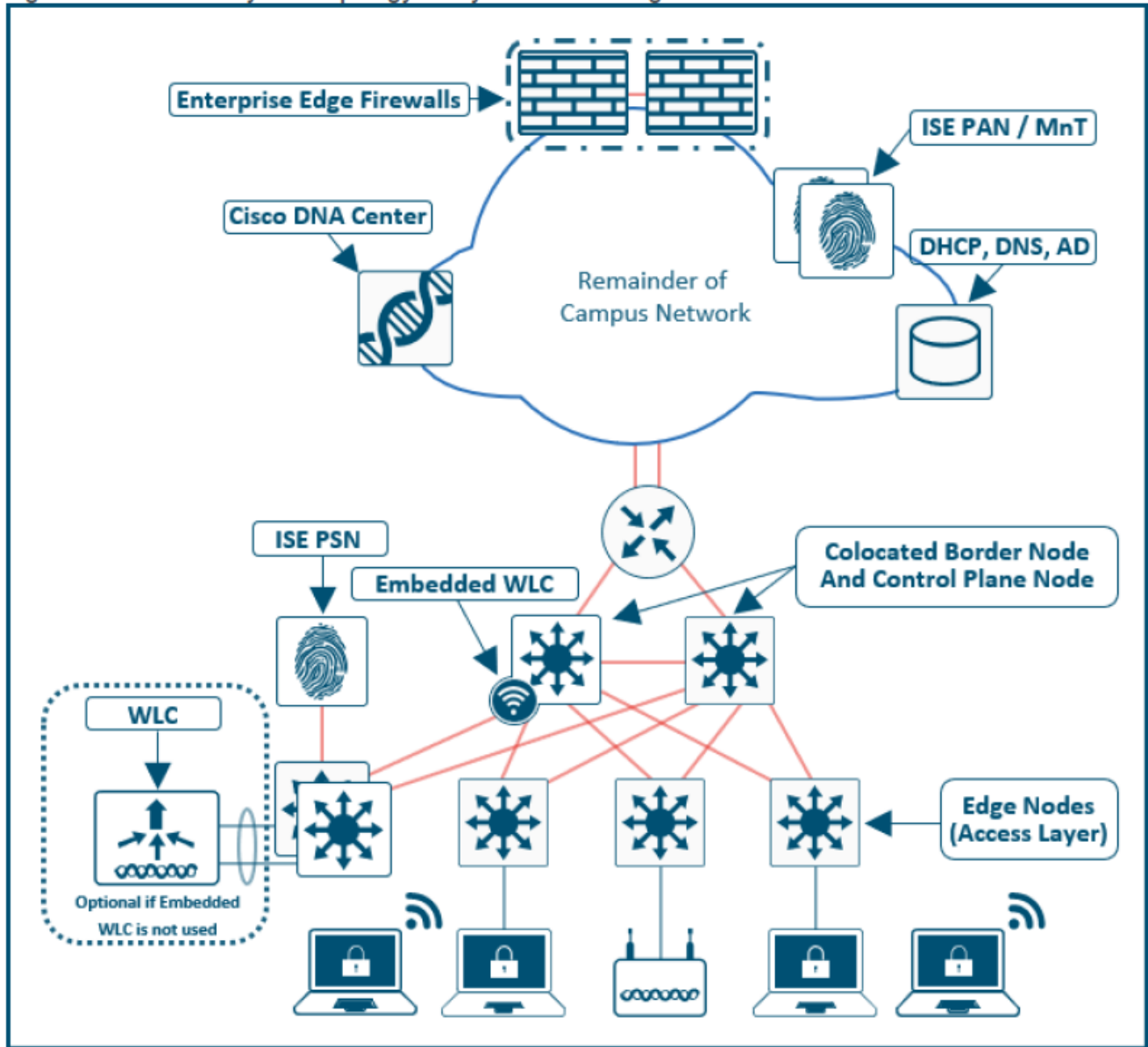
**Figure 37. Physical Topology - Fabric in a Box Site Design**



**Physical Topology – Fabric in a Box Site Design**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

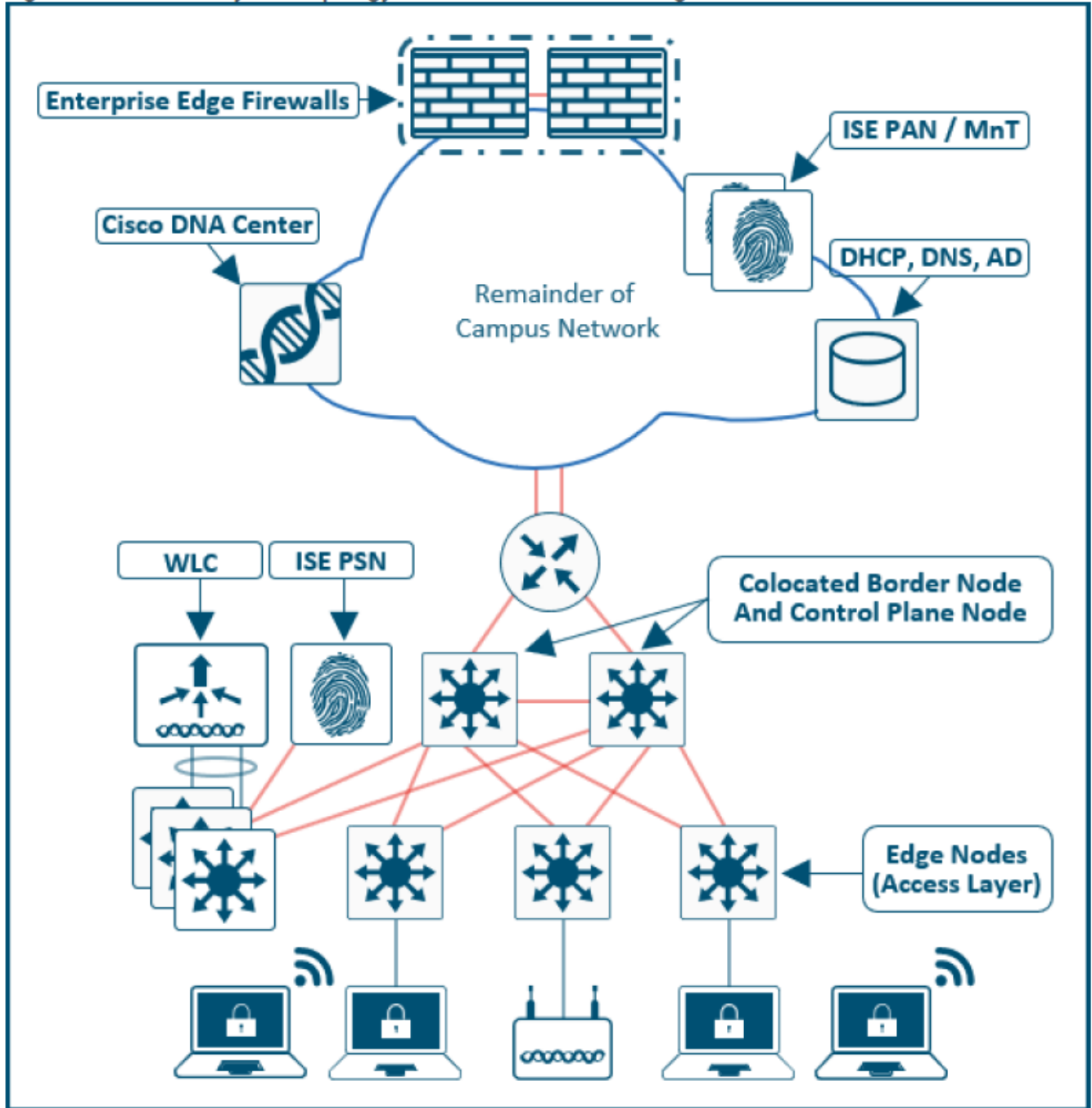
**Figure 38. Physical Topology - Very Small Site Design**



**Physical Topology – Very Small Site Design**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

**Figure 39. Physical Topology - Small Site Reference Design**



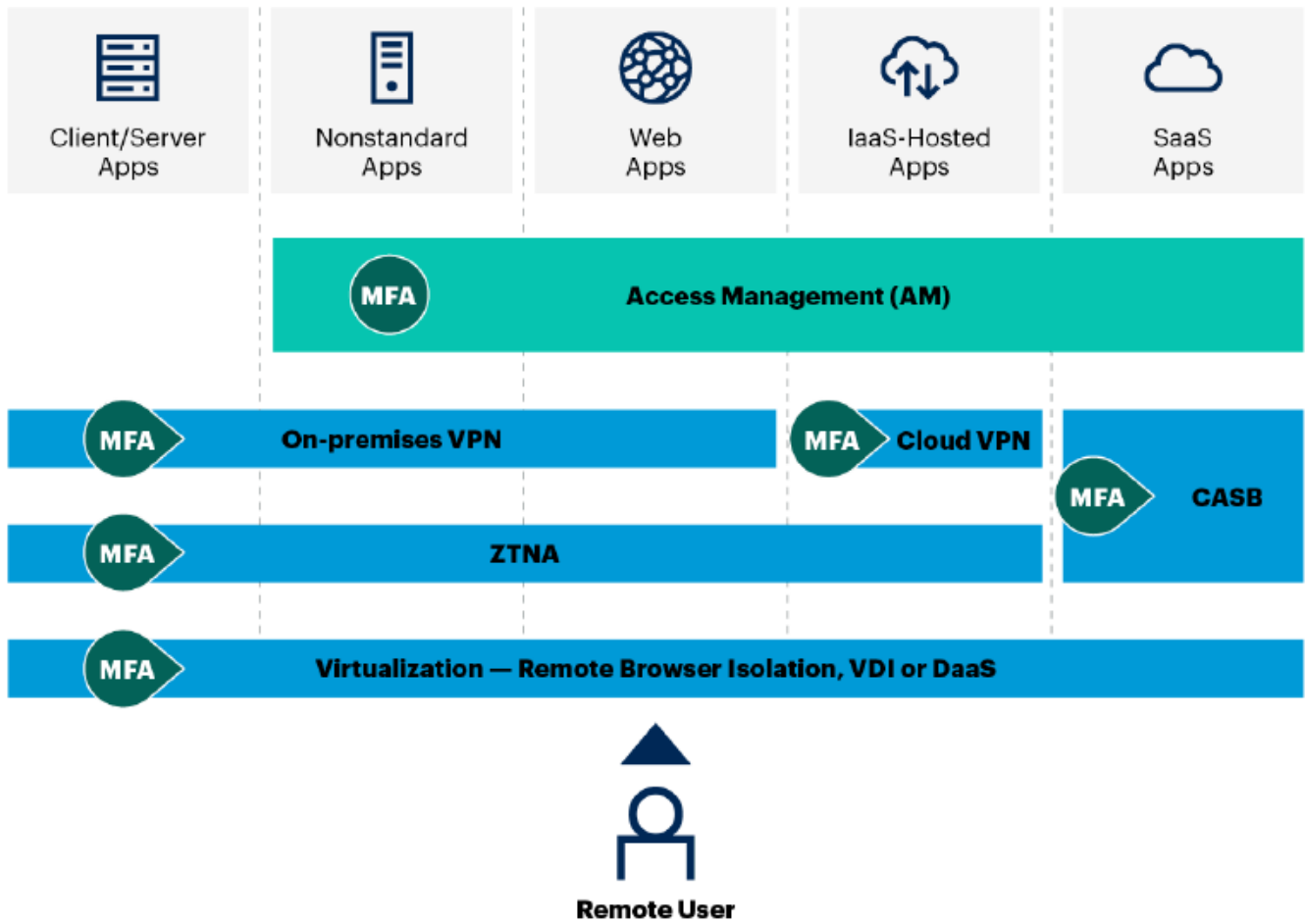
**Physical Topology – Small Site Reference Design**

Software Defined Access Solution Design Guide by Cisco Public - June 2020



## MFA and AM for Remote Access

Remote Access and Virtualization Options\*



Source: Gartner

\* see "Solving the Challenges of Modern Remote Access" (G00722990)

724227\_C

## MFA and Access Management (AM) for Remote Access

Gartner – May 6, 2020

**From Traditional Heavy Branch to Cloud-centric Thin Branch/SASE Models**  
 Heavy-Branch Model Shifting to Thin-Branch/Heavy-Cloud Model

Heavy Branch	Thin Branch	Heavy Cloud
Router	SD-WAN/FW	CASB
VPN	Simple WOC	FWaaS w/ IPS
FW		ZTNA/SDP
WOC		SWG
SWG		DLP
DLP		Threat
		VPN
		WAAPaaS
		Sandbox
		RBI

Source: Gartner  
ID: 441737

**From Traditional Heavy Branch to Cloud-Centric Thin Branch / SASE Models**

Gartner – August 30, 2019

## 5. HOW CLOUDFLARE DELIVERS SASE

Cloudflare One	Core capability	SASE service
<b>Cloudflare Gateway</b> inspects user traffic and blocks malicious content from reaching user devices and spreading within an organization.	Filtering traffic	SWG, CASB
<b>Cloudflare Access</b> strengthens access requirements by applying identity and context filters to every inbound and outbound request.	Connecting users to applications	ZTNA, CASB
<b>Cloudflare Magic WAN</b> provides a control plane to accelerate and route traffic across the Cloudflare network using WARP, Magic Transit, and Cloudflare Network Interconnect (CNI).	Building and managing networks	SD-WAN
<b>Cloudflare Magic Firewall</b> replaces on-premise firewalls with network-level protection for remote users, branch offices, data centers, and cloud-based infrastructure.	Protecting applications and infrastructure	FWaaS
<b>Cloudflare Browser</b> protects user devices from zero-day threats by separating the browser from potentially harmful code.	Securing devices and data	Remote browser isolation

### How CloudFlare Delivers SASE.

Getting started with SASE: A guide to secure and streamline your network infrastructure.

Whitepaper by CloudFlare. November 11, 2020.

## Use Case #2

---

### *Work From Home Users*

#### What:

Companies are forced to transition hundreds or thousands of employees to work from home, which has implications for security and network performance, often requiring upgrades to VPN infrastructure. Home workers need to access their corporate applications with the same high-quality experience as from their office.

## What the Market Says

---

30% Staying Home

According to Gartner, about 25% of those surveyed expect 10% of their employees will remain remote, 17% expect 20% will remain remote, 4% expect 50% will remain remote, and 2% expect over 50% of employees now working from home to permanently work from home after the pandemic subsides.

86% Are Productive

Even more, 86% of employees say they're most productive when they work alone—devoid of distractions like inefficient meetings, office gossip, or loud office spaces.

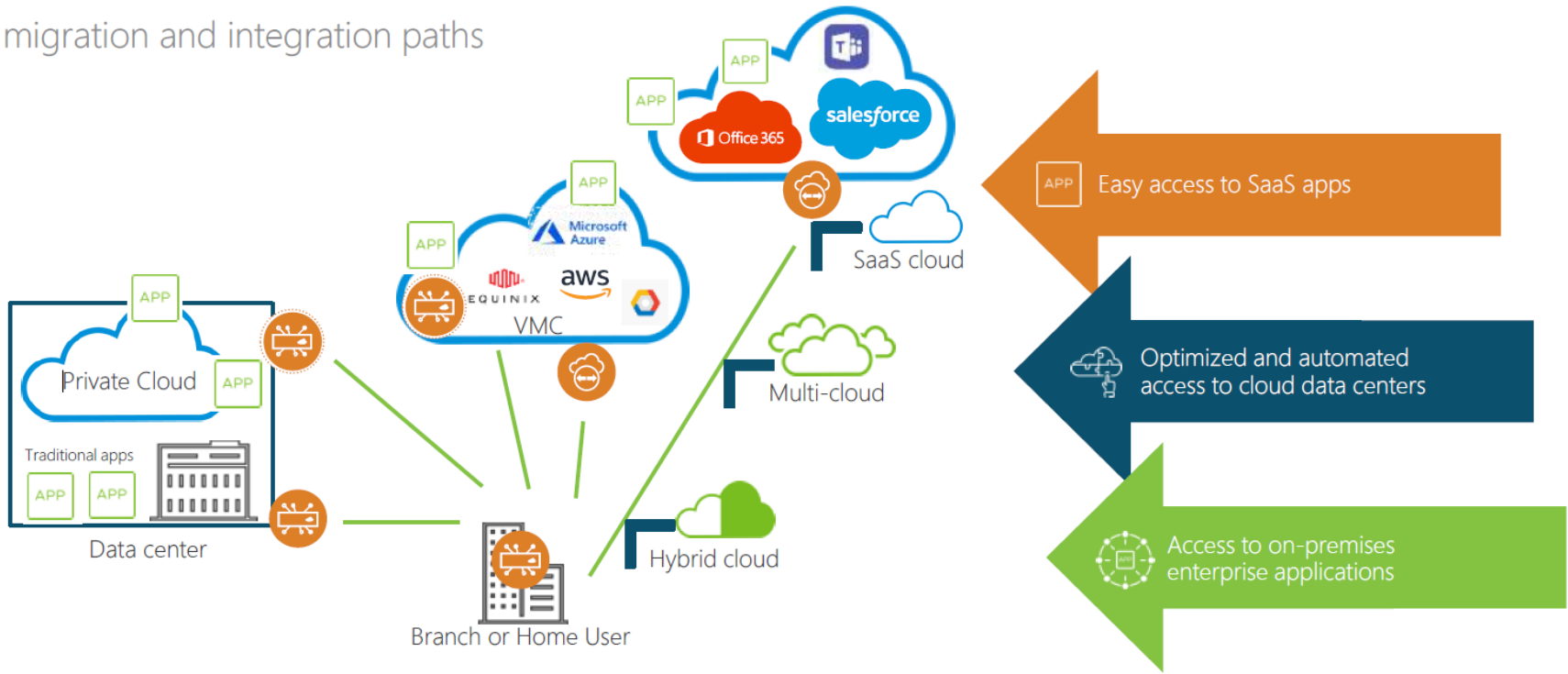
Employee Satisfaction

In a Stanford University study, employers who offered a work from home option had employee turnover rates fall by over 50%



# SD-WAN SUPPORTS HYBRID/MULTI-CLOUD STRATEGY

Easy migration and integration paths



Managed on-ramp to any cloud

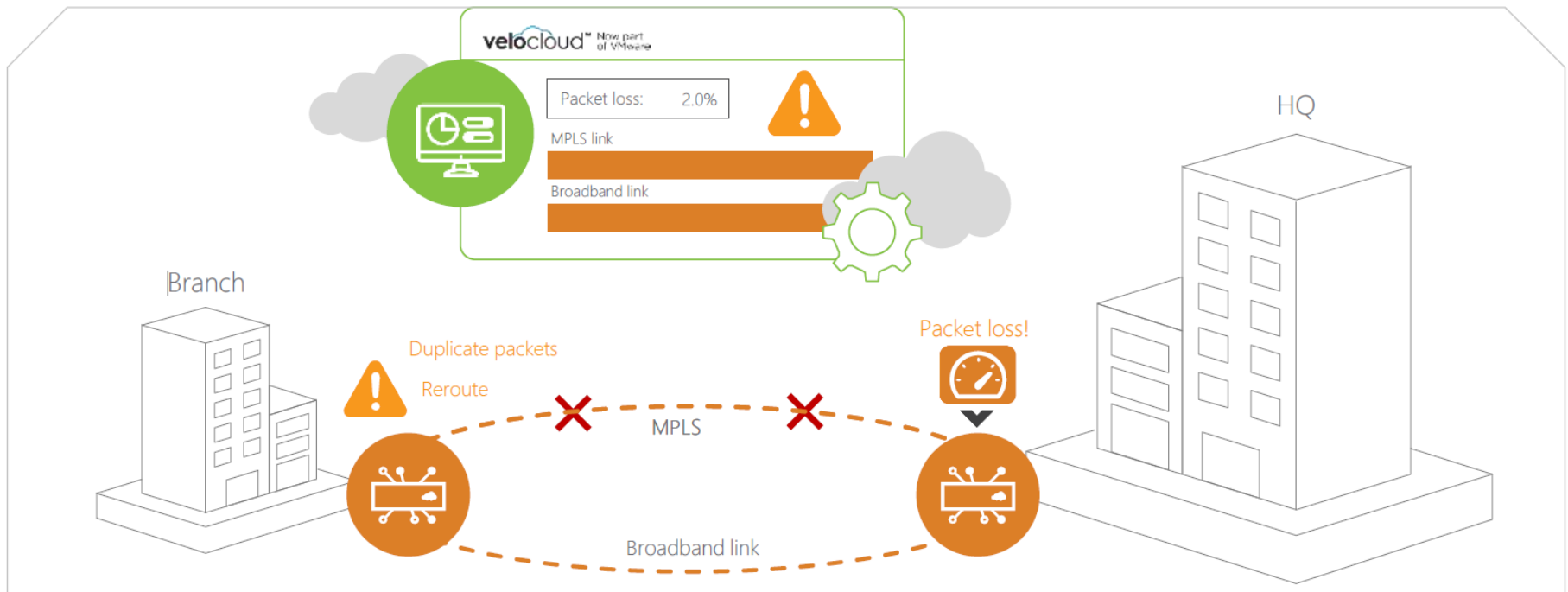


**SD-WAN Supports Hybrid/Multi-Cloud-Strategy. QOS Networks - June 2020**



# DYNAMICALLY ROUTE AND REPLICATE DATA





Increase availability and reduce latency with real-time remediation and steering



**Dynamically Route and Replicate Data - MPLS and Broadband Example. QOS Networks, June 2020**







Questions to ask - CIO

-  Anxiety question: Is your current network keeping up with business demands of your remote locations?
-  Problem-probing question: What does your WAN need in order to be ready to support the business in today' s cloud era?
-  Solution-probing question: What if you could eliminate legacy infrastructure and replace with a software-based, cloud-managed, simple WAN management solution?
-  Probing question: What if you could bring in an over-the-top solution that was simple to manage and deploy, leveraged commercial broadband, and bring down branch Opex by at least 50%?

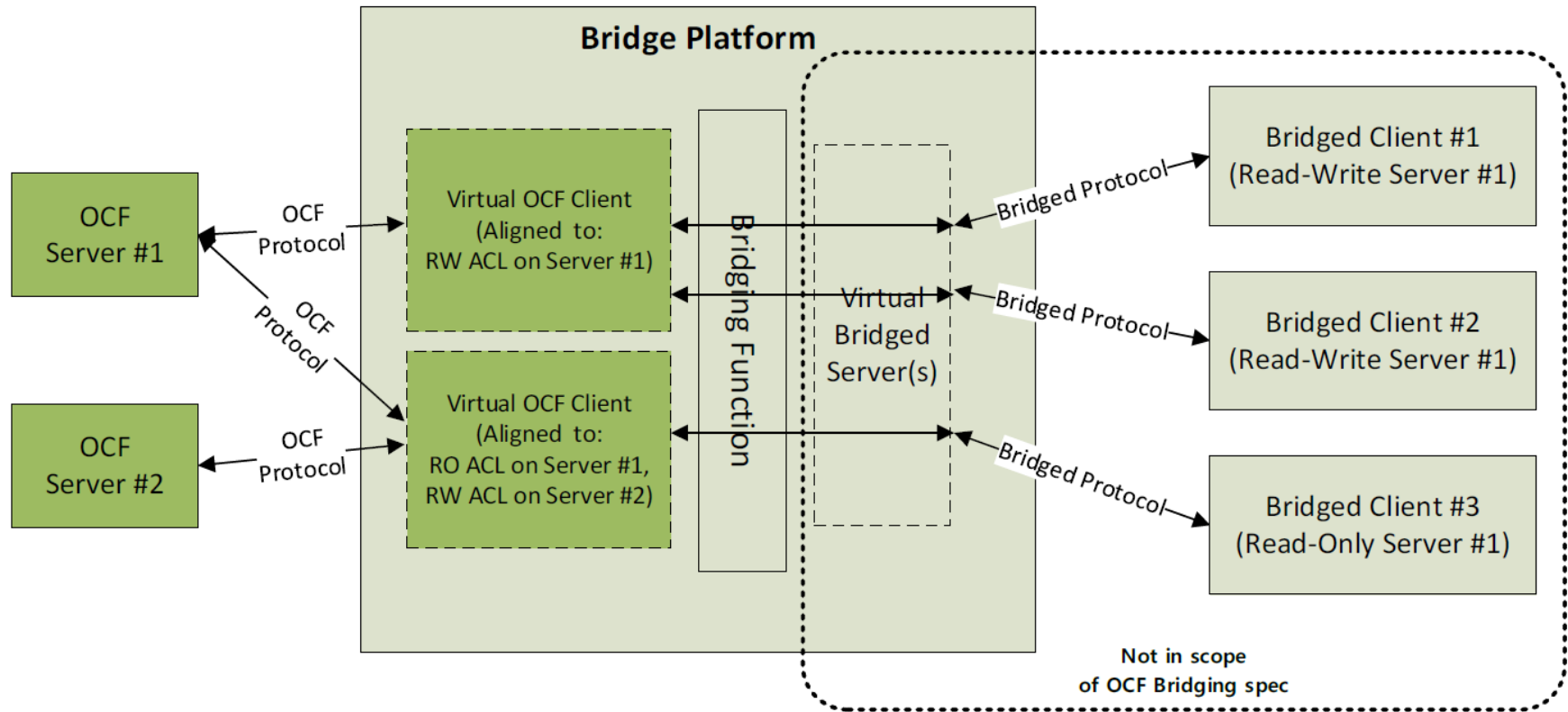


Questions to ask – VP/Director of IT/Networking

-  Anxiety question: Are you concerned with the challenges of accessing applications that are moving to the cloud?
-  Problem-probing question: Can you meet the growing demands of your remote locations while keeping WAN and networking costs in check?
-  Value-probing question: What if you were able to meet application SLAs without investing heavily in WAN management costs?
-  Solution-probing question: Are you looking for a way to improve SLAs for real-time applications, provide transport-agnostic solutions for your branches, and dramatically simplify WAN management, while keeping costs in check?



Probing questions to ask CIO and IT Director. QOS Networks - June 2020

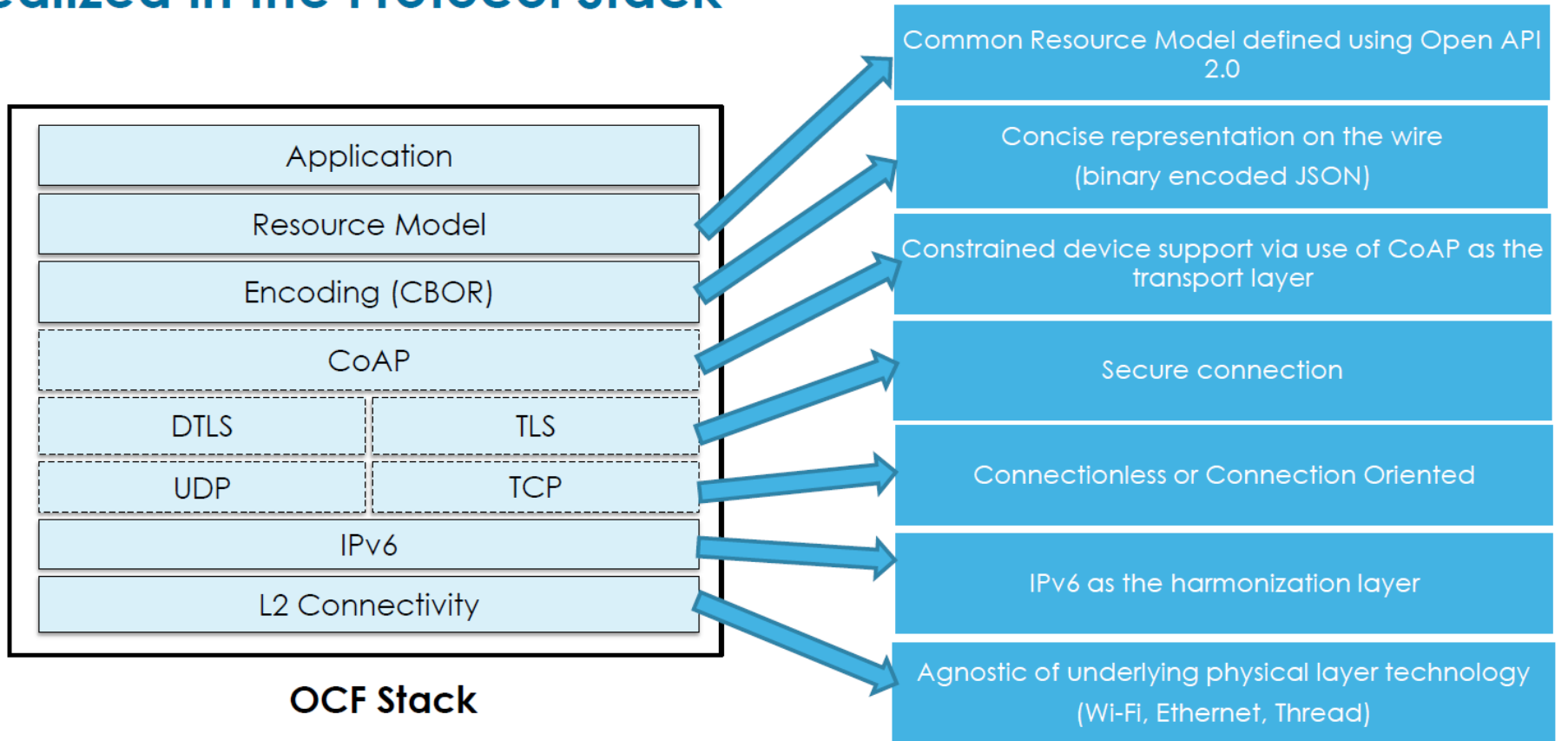


**Figure 5 – Asymmetric client bridge**

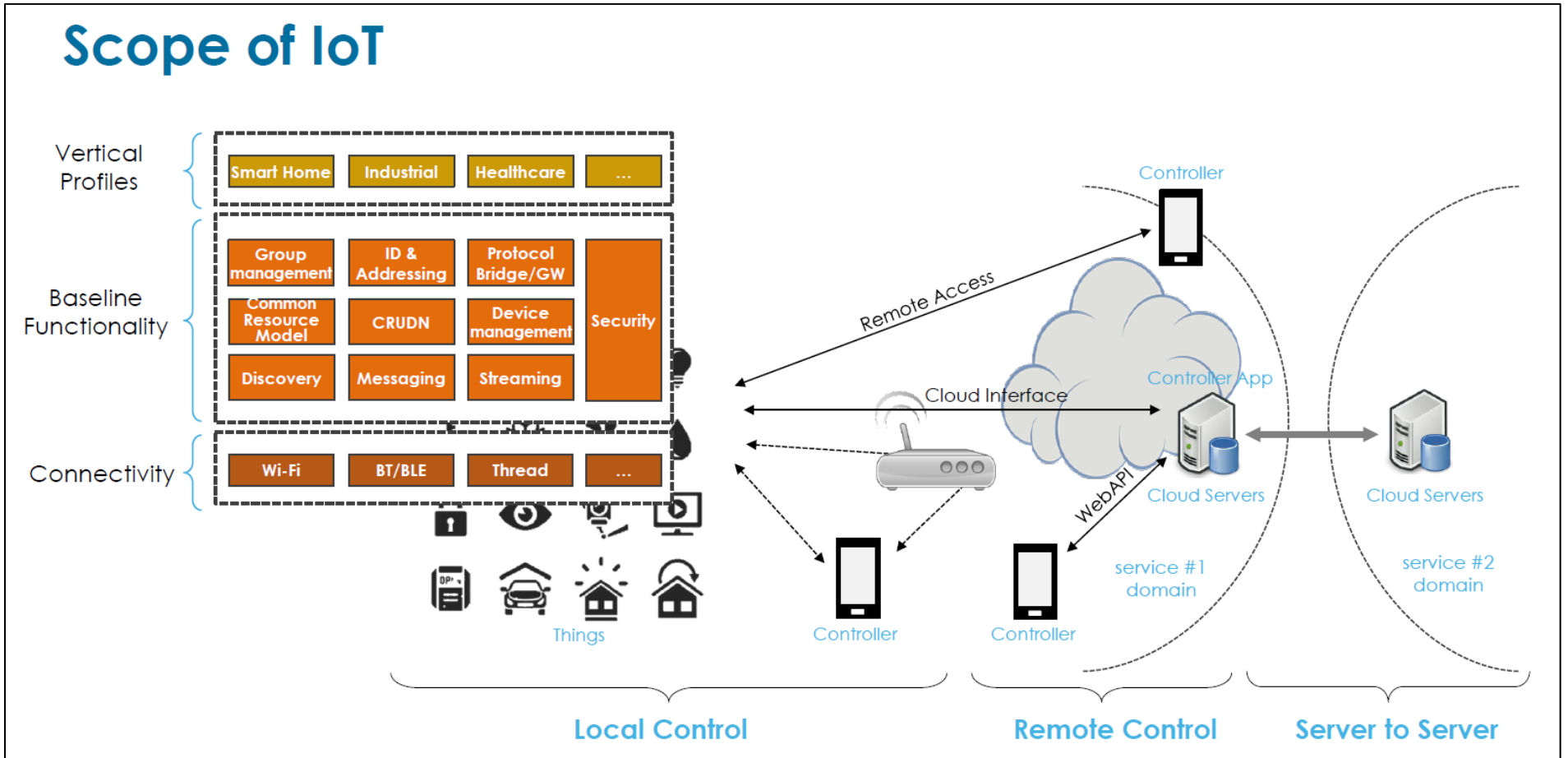
Figure 5 shows that each access to the OCF Server is modelled as a Virtual OCF Client. Those accesses can be aggregated if their target OCF servers and access permissions are same, therefore a Virtual OCF Client can tackle multiple Bridged Clients.



## Core Framework Fundamentals Realized in the Protocol Stack

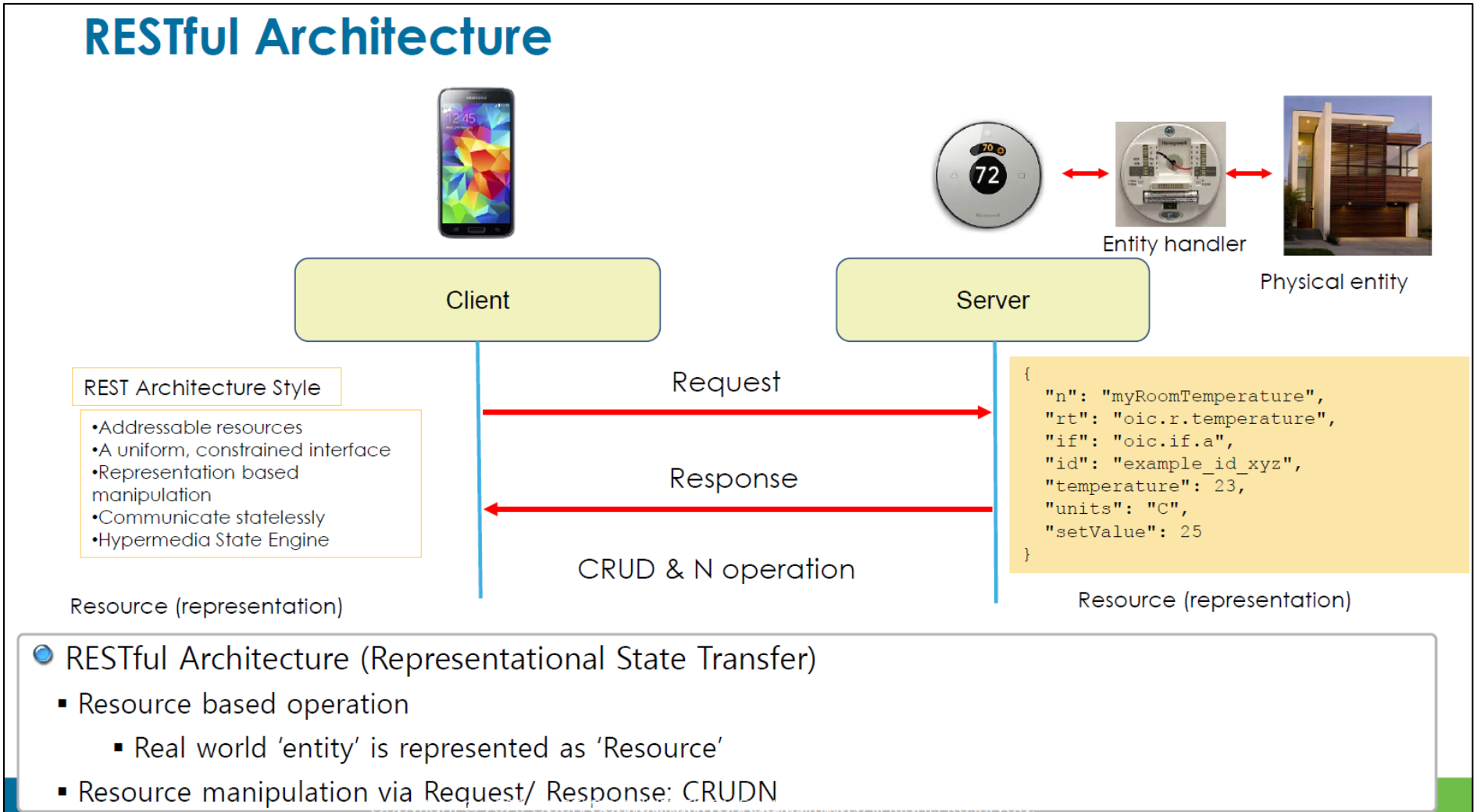


Open Connectivity Foundation – March 2020

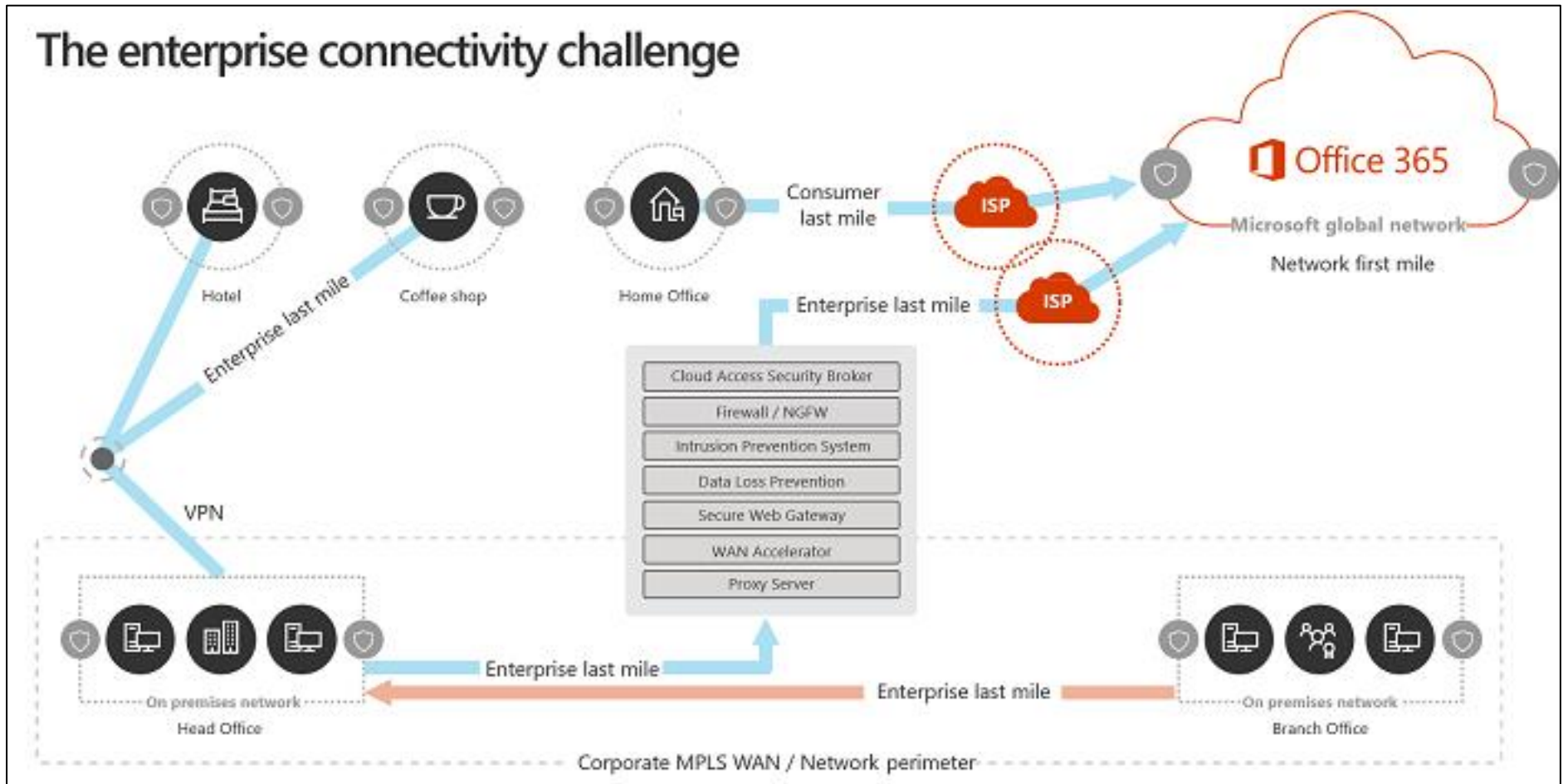


Open Connectivity Foundation – March 2020

# RESTful Architecture

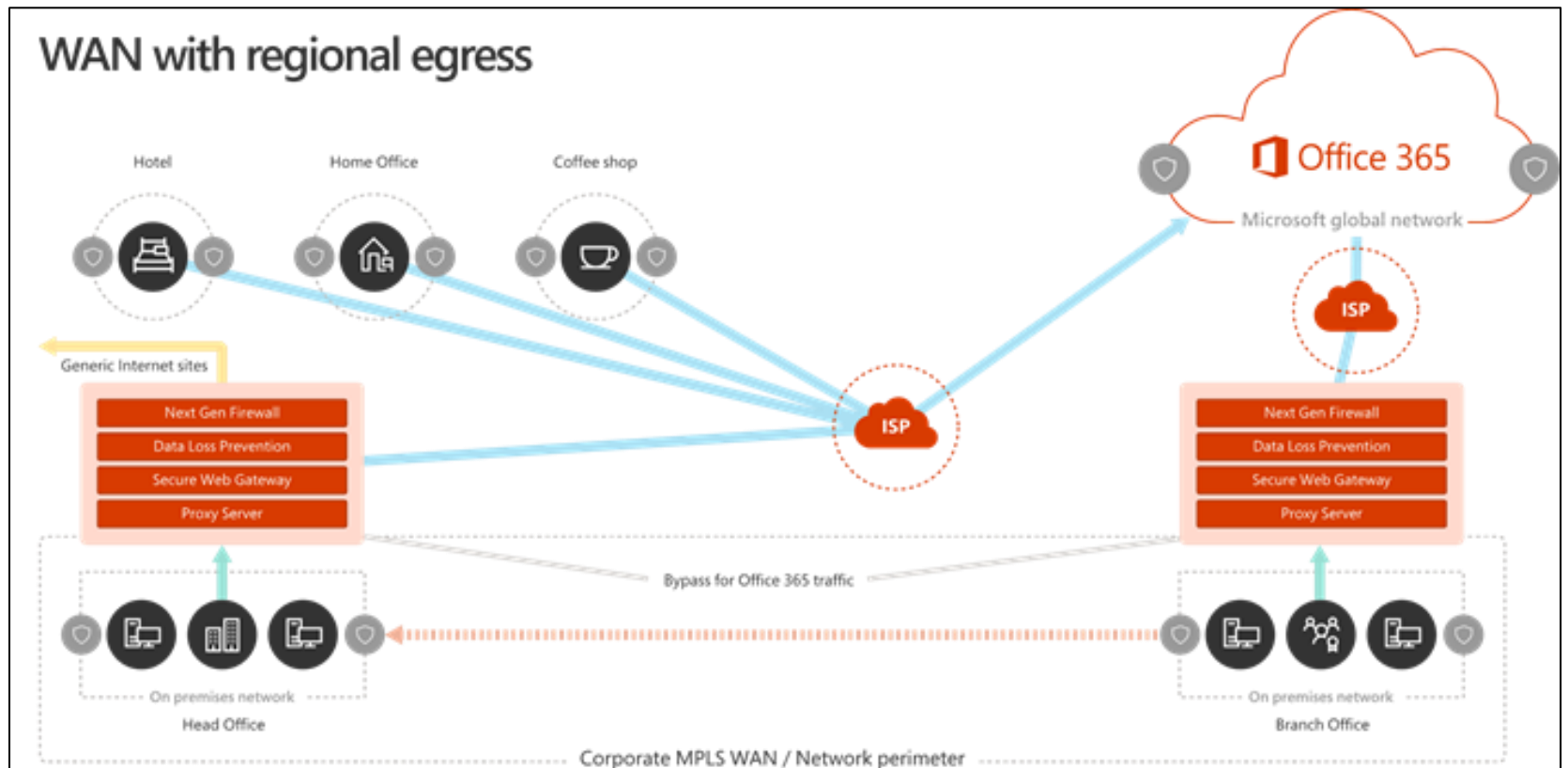


Enterprise WANs are often designed to backhaul network traffic to a central company head office for inspection before egress to the Internet, usually through one or more proxy servers. The following diagram illustrates such a network topology.



**Microsoft 365 Network Connectivity Principles – June 2020**

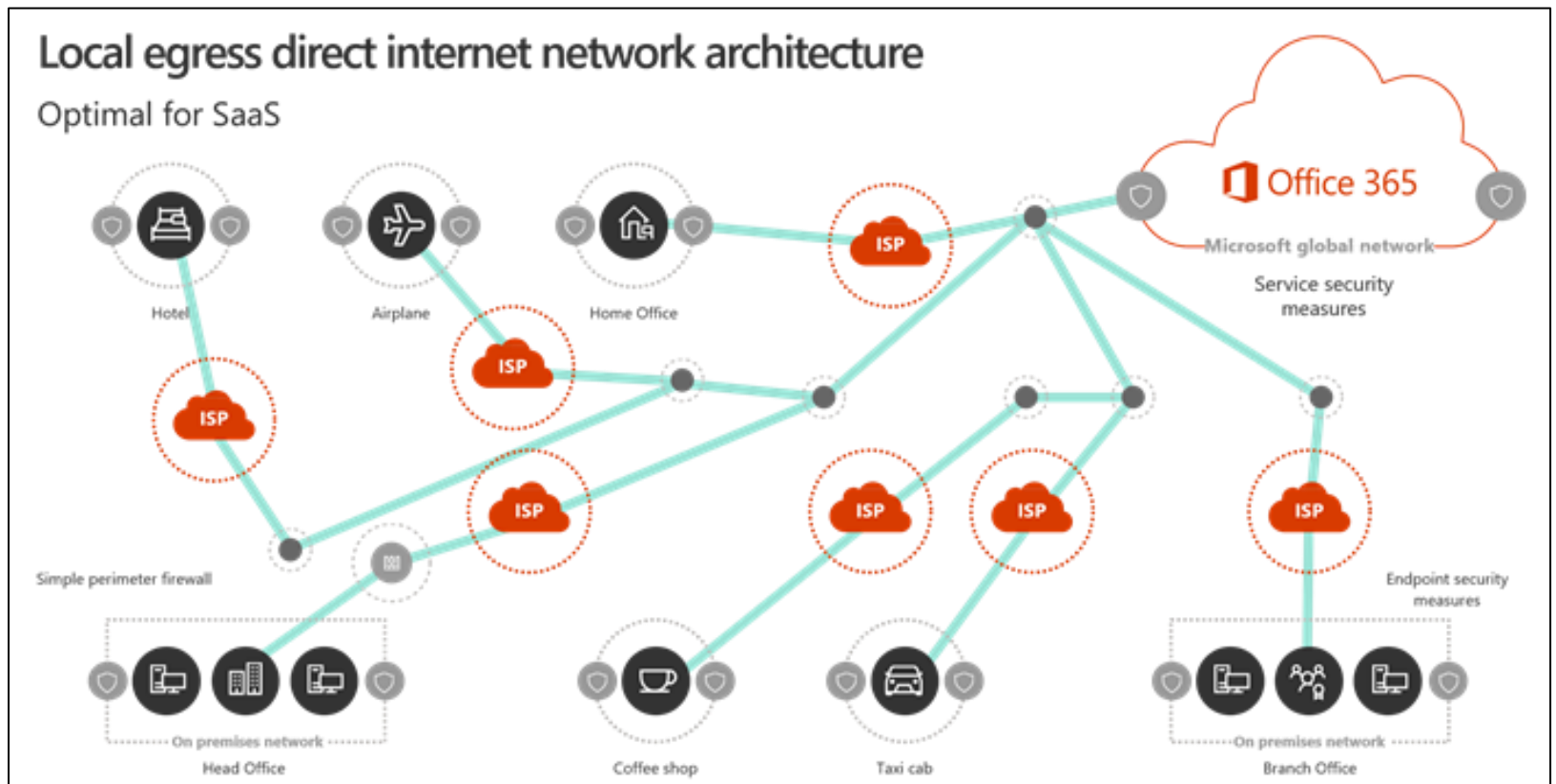
This following diagram shows an example of a network topology that allows users connecting from main office, branch office, and remote locations to follow the shortest route to the closest Microsoft 365 entry point. Shortening the network path to Microsoft 365 entry points in this way can improve connectivity performance and the end-user experience in Microsoft 365. Also, DNS requests can introduce latency if the responding DNS server is distant or busy. One can minimize name resolution latency by provisioning local DNS servers in branch locations and making sure they are configured to cache DNS records appropriately.



Microsoft 365 Network Connectivity Principles – June 2020

The following local egress architecture diagram has the benefits over the traditional model such as:

- Provides optimal Microsoft 365 performance by optimizing route length. End-user connections are dynamically routed to the nearest Microsoft 365 entry point by the Distributed Service Front Door infrastructure.
- Reduces the load on government network infrastructure by allowing local egress.
- Secures connections on both ends by leveraging client endpoint security and cloud security features.



Microsoft 365 Network Connectivity Principles – June 2020

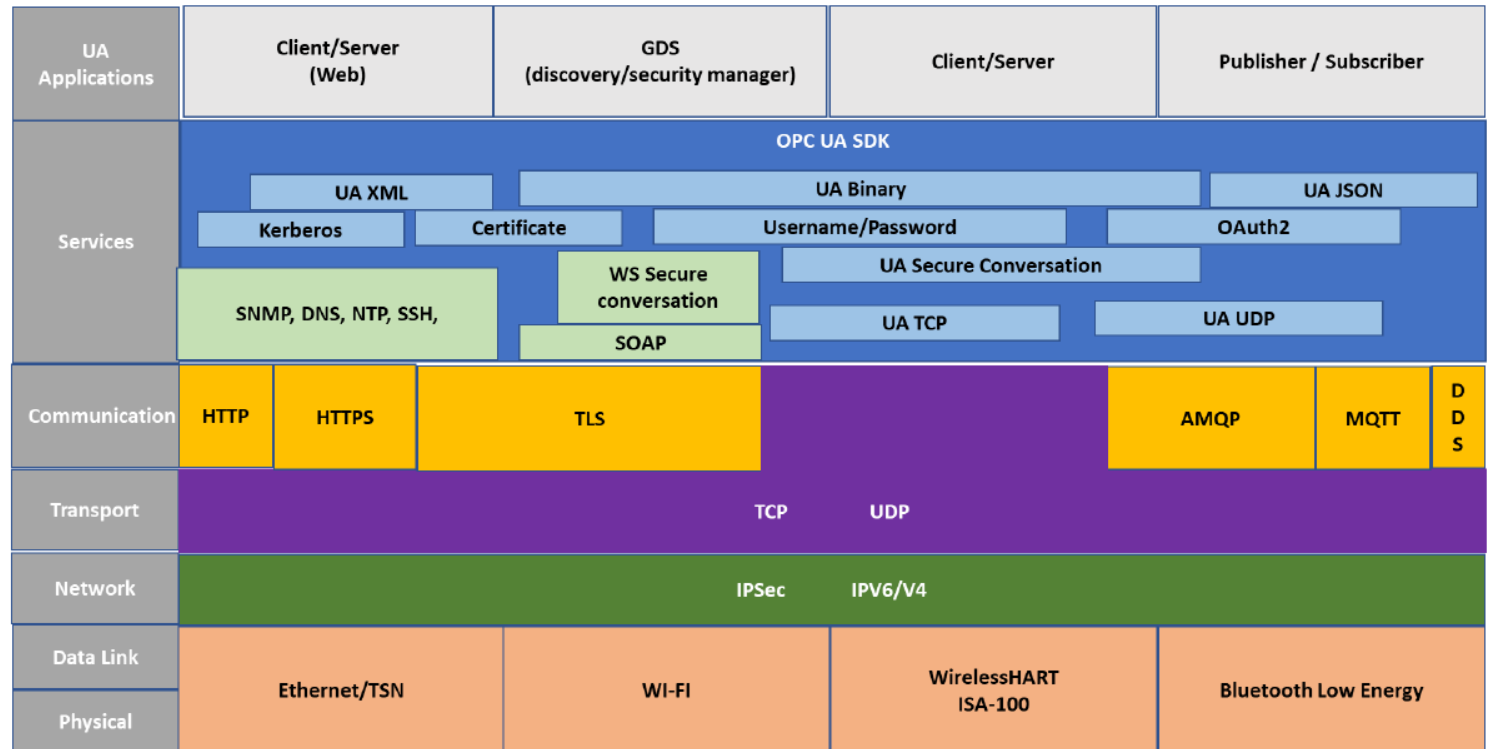


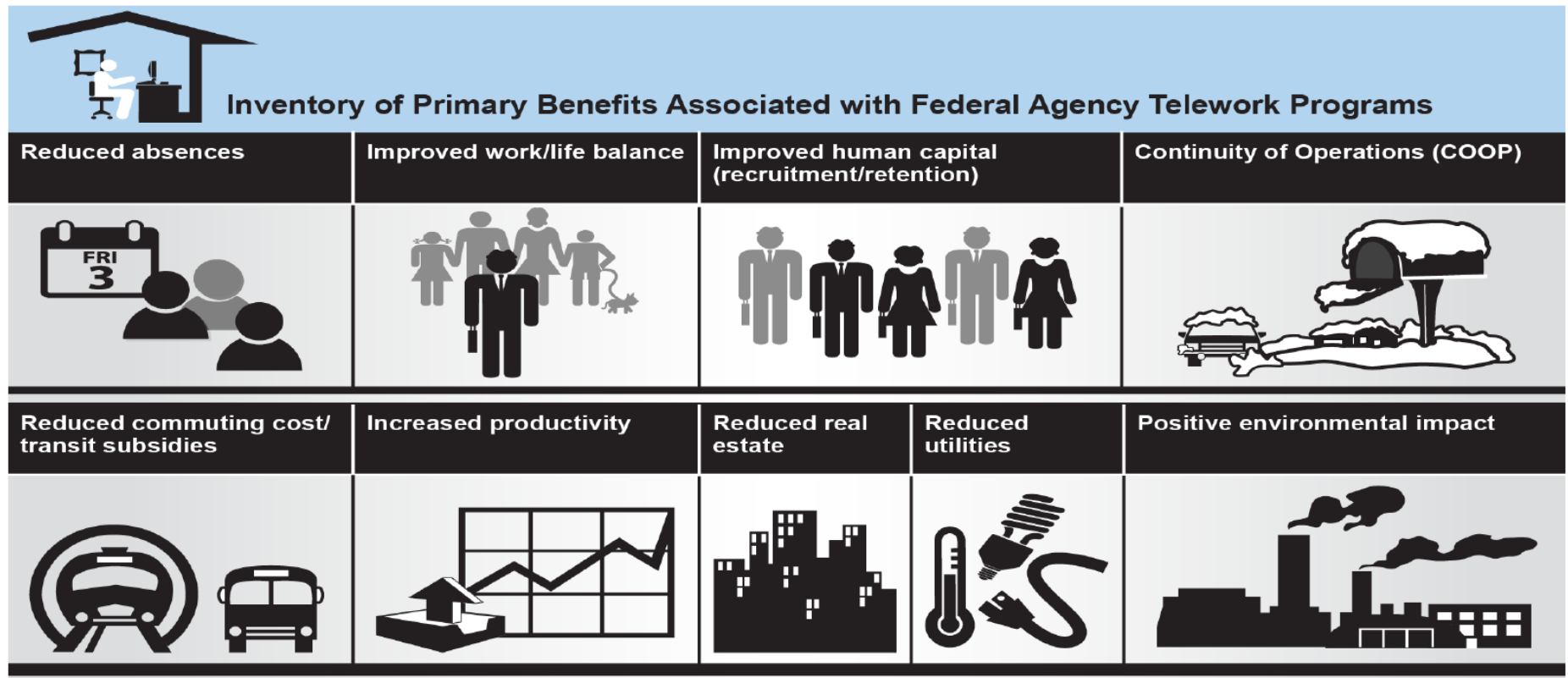
Figure 2 - Nested layered technology

OPC UA transport mechanisms are designed for extensibility and are configurable depending on the overall system requirements. OPC UA provides a unique strategy to allow seamless interoperability across the multitude of transports for timeless durability from the past into the future.

Figure 2 illustrates the relationship of the OPC UA transport, data encode and security with the overall communication stack. The OPC UA services are located just above the Communication layer. Notice the multiple OPC UA protocols identified within the Services layer, from left to right.

### Nested Layered Technology - OPC Unified Architecture - August 2017

Figure 2: Inventory of Primary Benefits Associated with Federal Agency Telework Programs



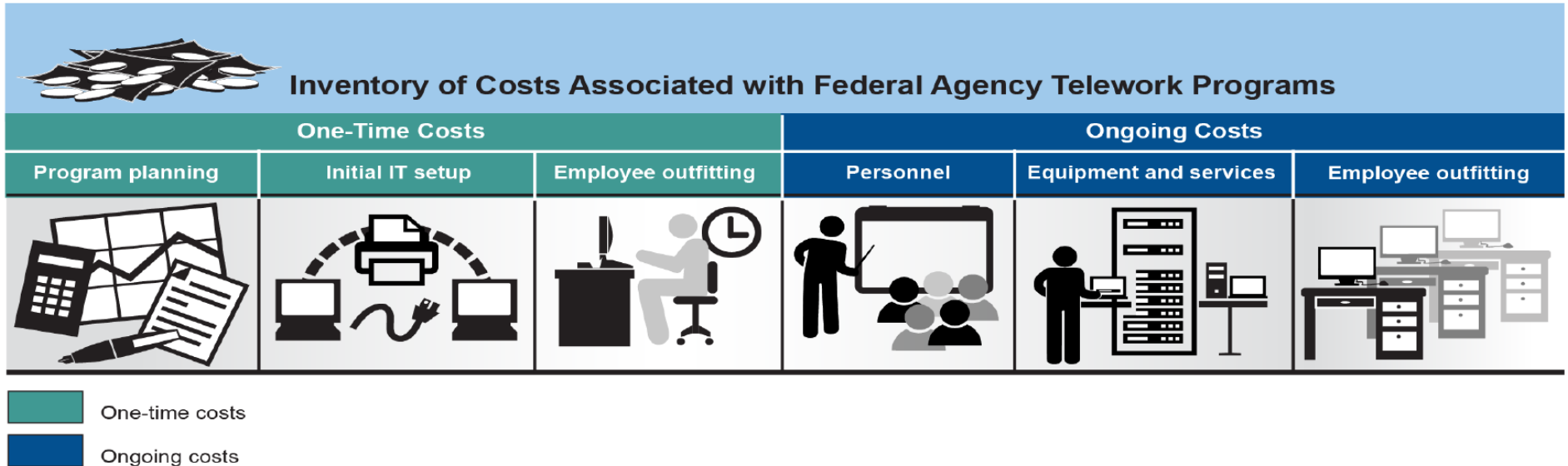
Source: GAO analysis of literature review of benefits associated with telework programs and the experiences of the six selected agencies. | GAO-16-551

Inventory of Primary Benefits Associated with Federal Agency Telework Programs

GAO-16-551 – July 2016



Figure 4: Inventory of Costs Associated with Federal Agency Telework Programs



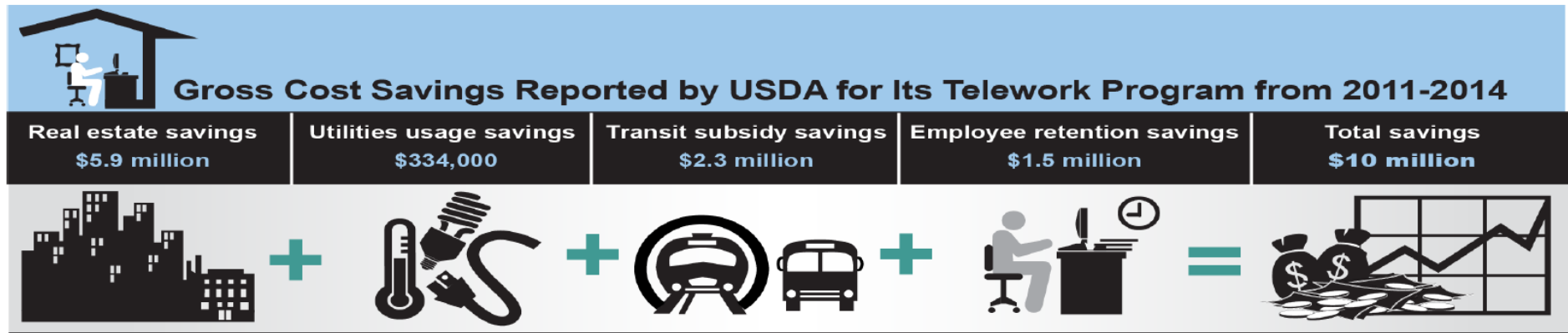
Source: GAO analysis of literature review of costs associated with telework programs and the experiences of the six selected agencies. | GAO-16-551

Note: One-time employee outfitting costs are costs for implementing a telework program, such as purchasing laptops. Ongoing employee outfitting costs are costs to maintain a telework program, such as purchasing computers for new teleworkers.

**Inventory of Cost Types Associated with Federal Agency Telework Programs**

GAO-16-551 – July 2016

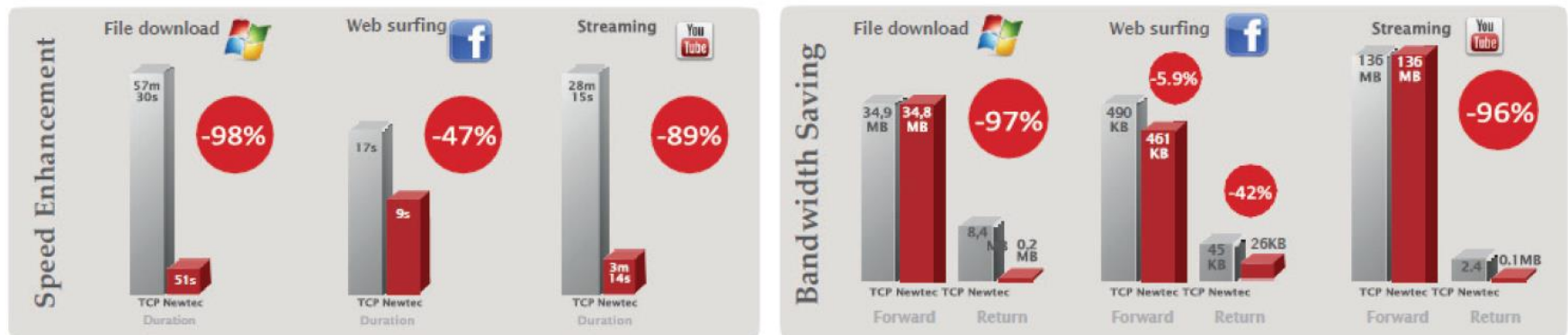
Figure 6: Gross Cost Savings Reported by USDA for Its Telework Program from 2011-2014



Source: GAO analysis of United States Department of Agriculture (USDA) information. | GAO-16-551

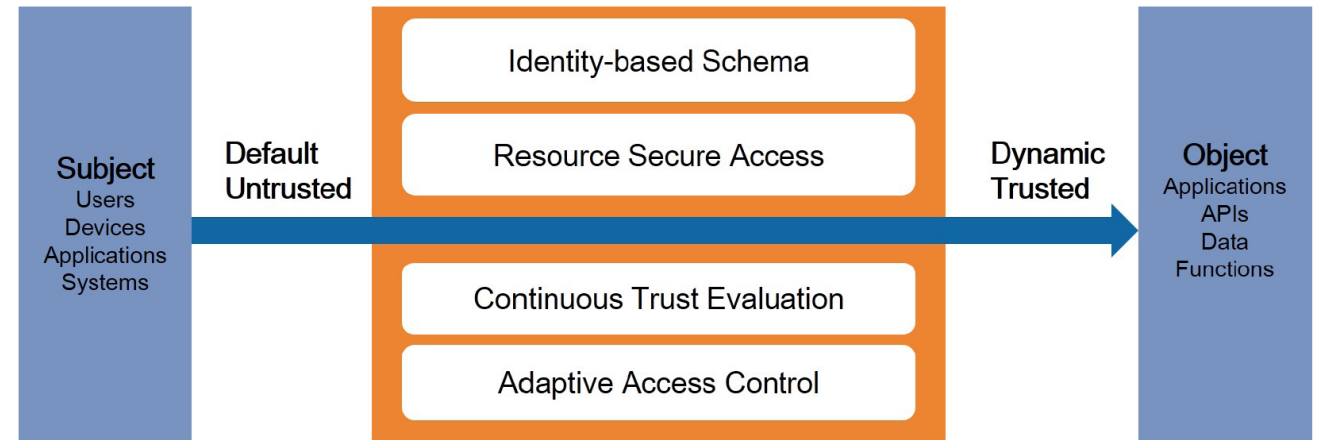
Gross Cost Savings Reporting by USDA for its Telework Program from 2011-2014

GAO-16-551 – July 2016



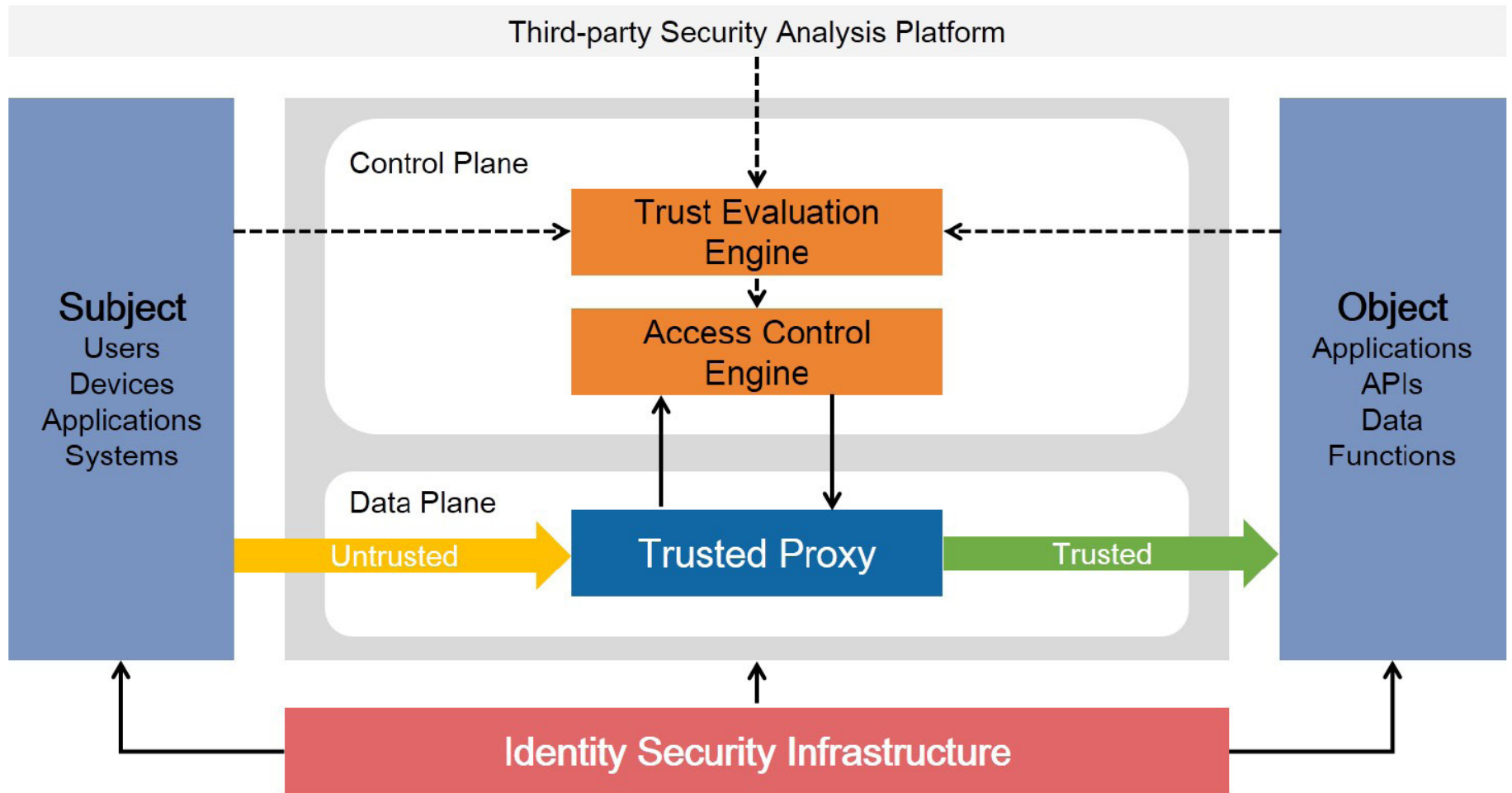
Bandwidth Efficient Technologies by ST Engineering iDirect, December 4, 2020

Figure 1 Key Capabilities of Zero Trust Architecture



Source Qi An Xin Group, 2019

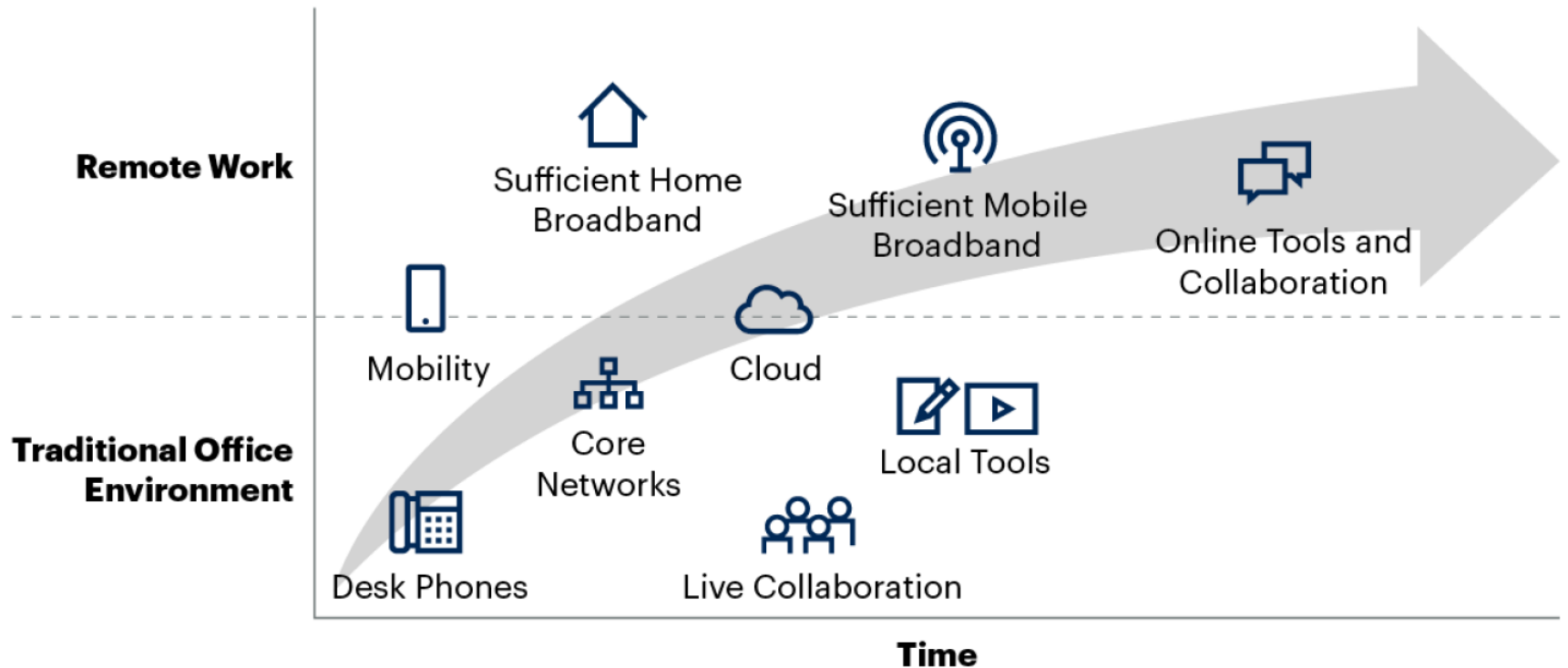
**Key Capabilities of Zero Trust Architecture – Gartner, 2020.**



Source Qi An Xin Group, 2019

**Core Logical Architectural Components of Zero Trust Architecture – Gartner, 2020**

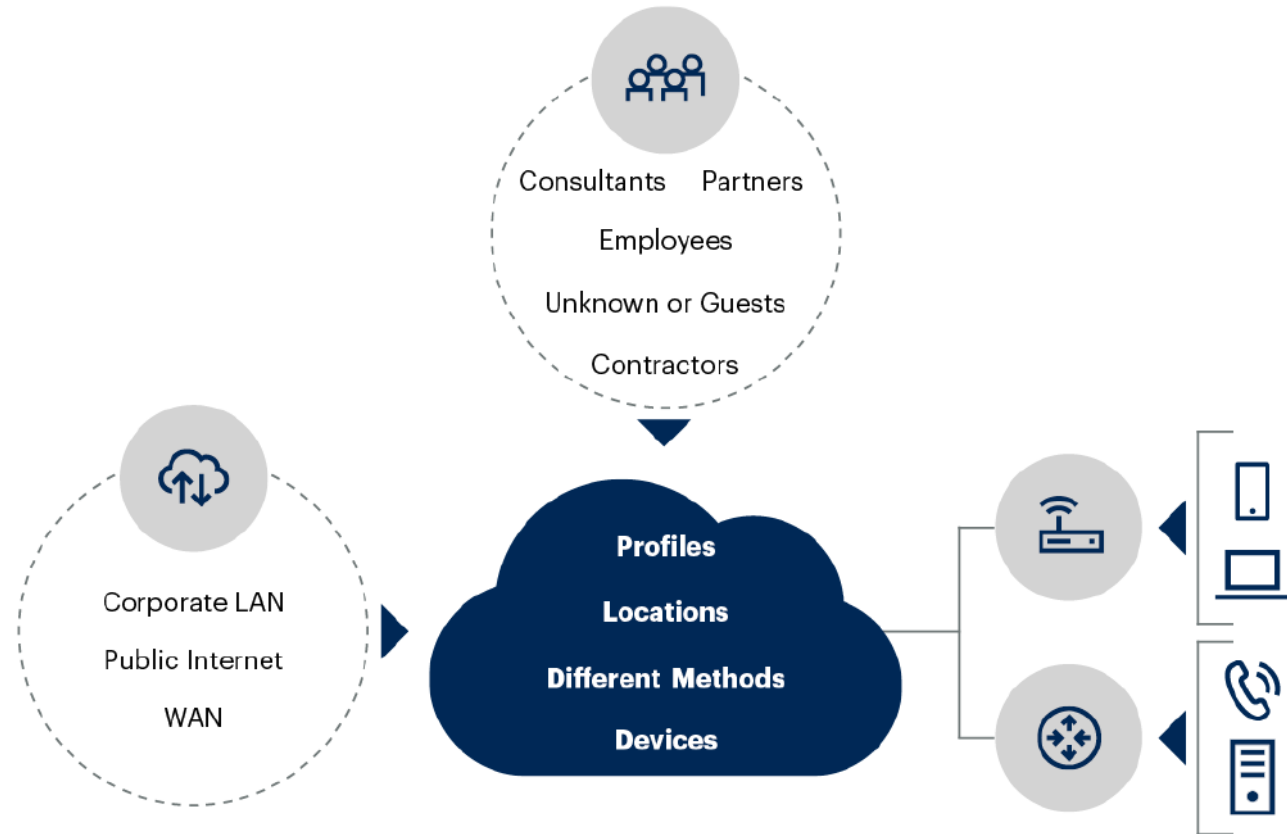
## Work at Home is Driving Increased Internet-Based Traffic Due to Use of Broadband and Online Cloud Collaboration



Source: Gartner  
730504\_C

Work at home is driving increased internet-based traffic. Gartner, November 5, 2020

**Focus on the Needs and Characteristics of Each Guest Access Role**



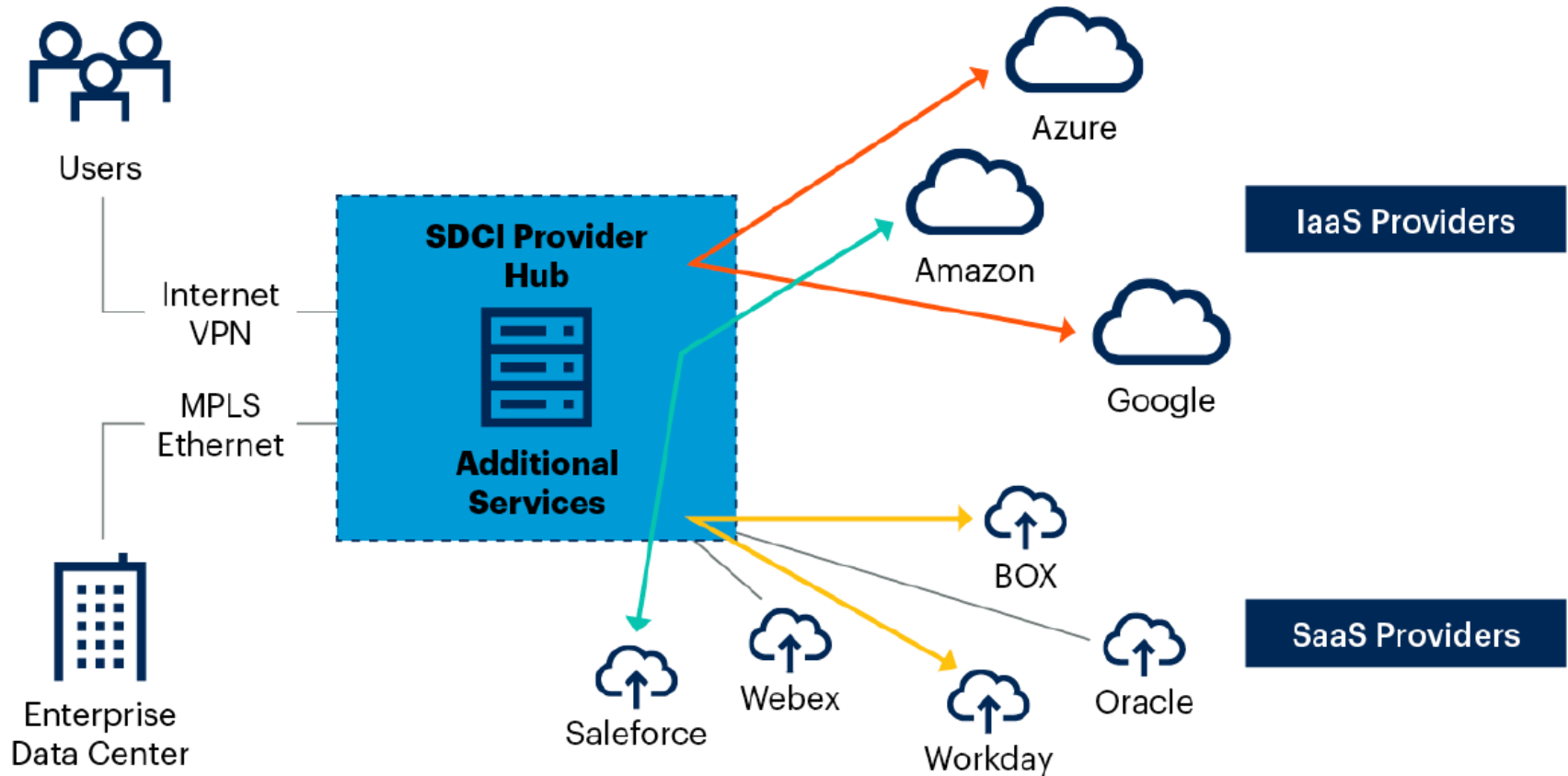
Source: Gartner  
737294\_C



**Guest Access Role Determinations. Software Defined Cloud Interconnection – SDCI. Gartner – October 9, 2020**



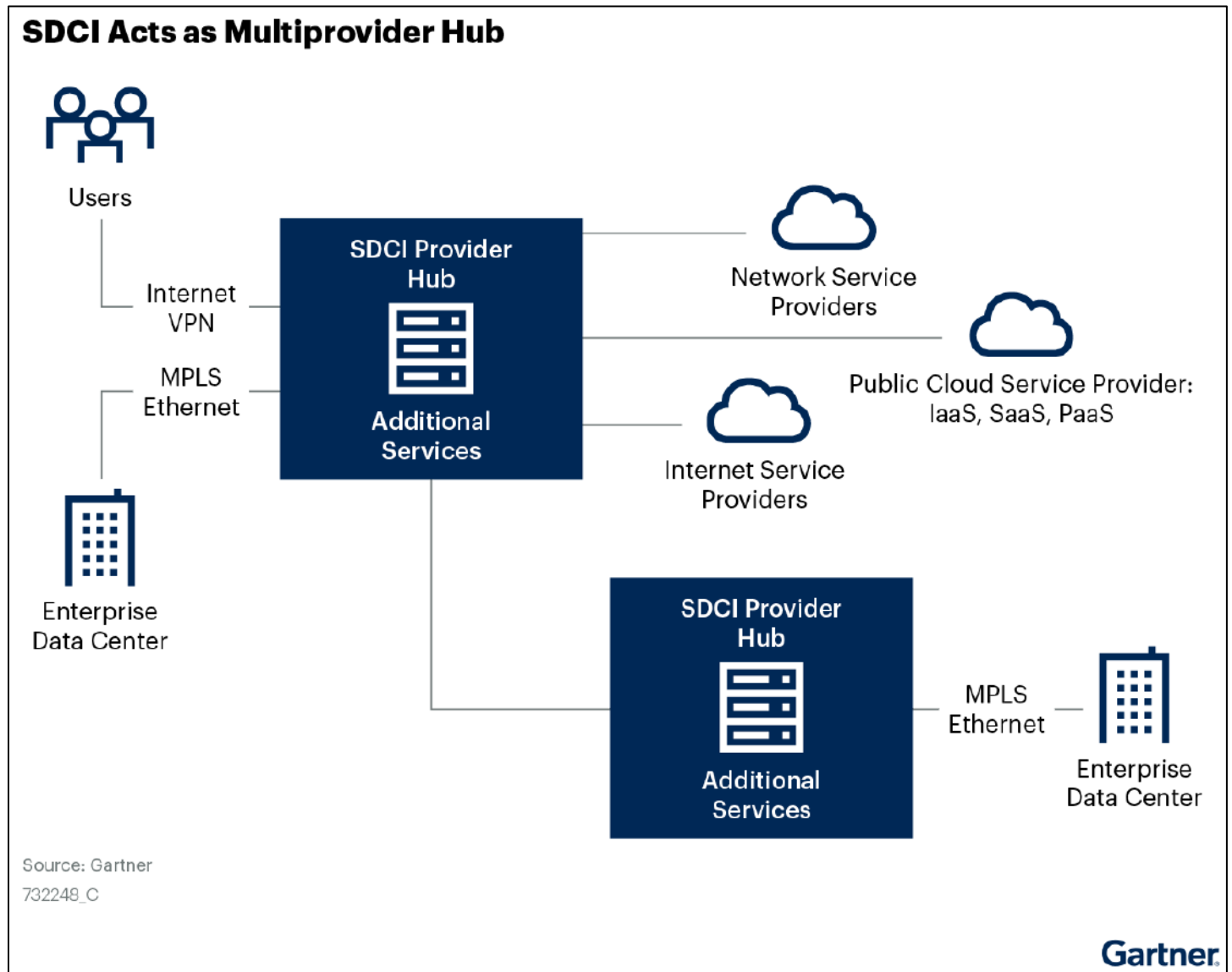
### SDCI Facilitates Multicloud Use Cases



Source: Gartner  
732248\_C



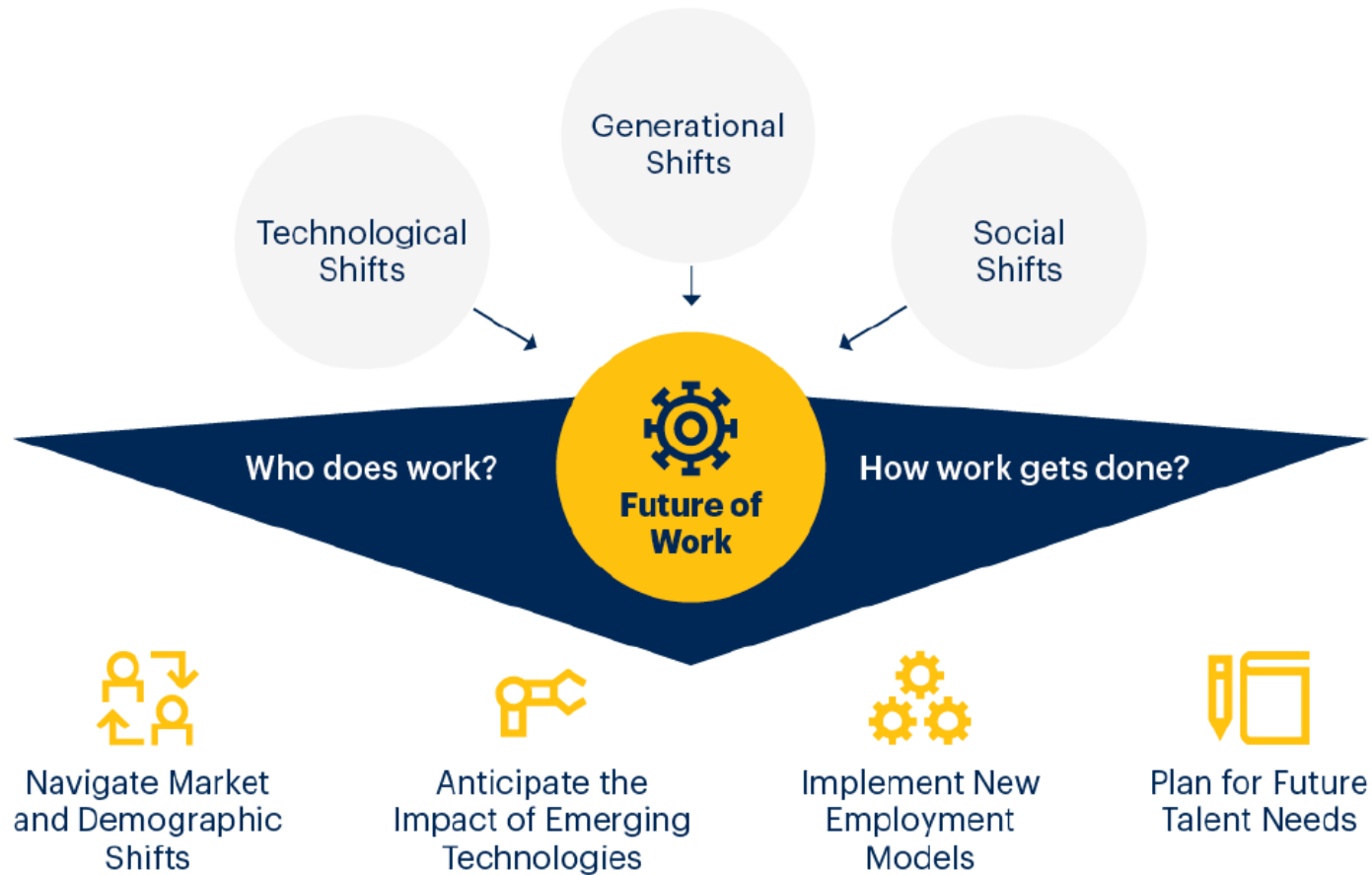
SDCI Facilitates Multicloud Use Cases. Software Defined Cloud Interconnection – SDCI. Gartner – October 9, 2020



**SDCI Acts as Multiprovider Hub. Software Defined Cloud Interconnection – SDCI. Gartner – October 9, 2020**



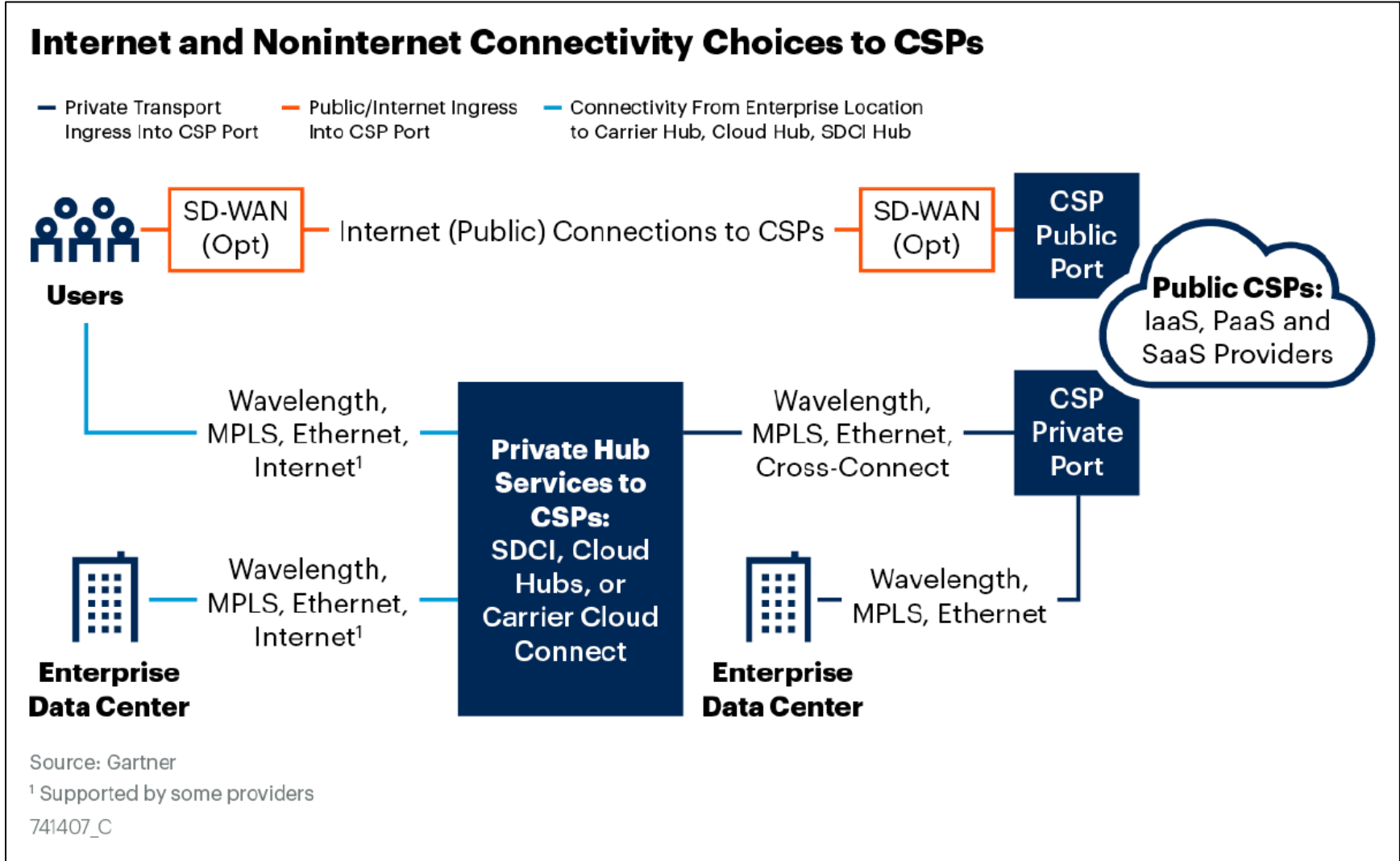
**Future of Work**



Source: Gartner  
714066



**Future of Work. New Work Realities. Gartner – March 9, 2021**



**Internet and Non-internet Connectivity Choices to Cloud Service Providers (CSPs). Gartner – February 2021**

Connect to a wide range of CSPs by using cloud hubs or a software-defined cloud interconnect.

Use cloud hubs when you want simple connectivity without additional functionality.

### Multiple Connectivity Choices to CSPs

	Private Connections to CSPs			Public/Internet Connection to CSP
	Private Cloud Ports	Software-Defined Cloud Interconnection	Cloud Hubs	
Cloud Ecosystem	2	4	4	5
SLAs	3	3	2	2
High Availability	4	4	5	2
Initial Provisioning Time	4	4	2	5
Security	4	4	5	2
Initial Setup Costs	4	3	2	5
Ease of Performance Management	3	4	2	1

**Poor/Difficult** — 1 — 2 — 3 — 4 — 5 — **Good/Easy**

Source: Gartner  
741407\_C

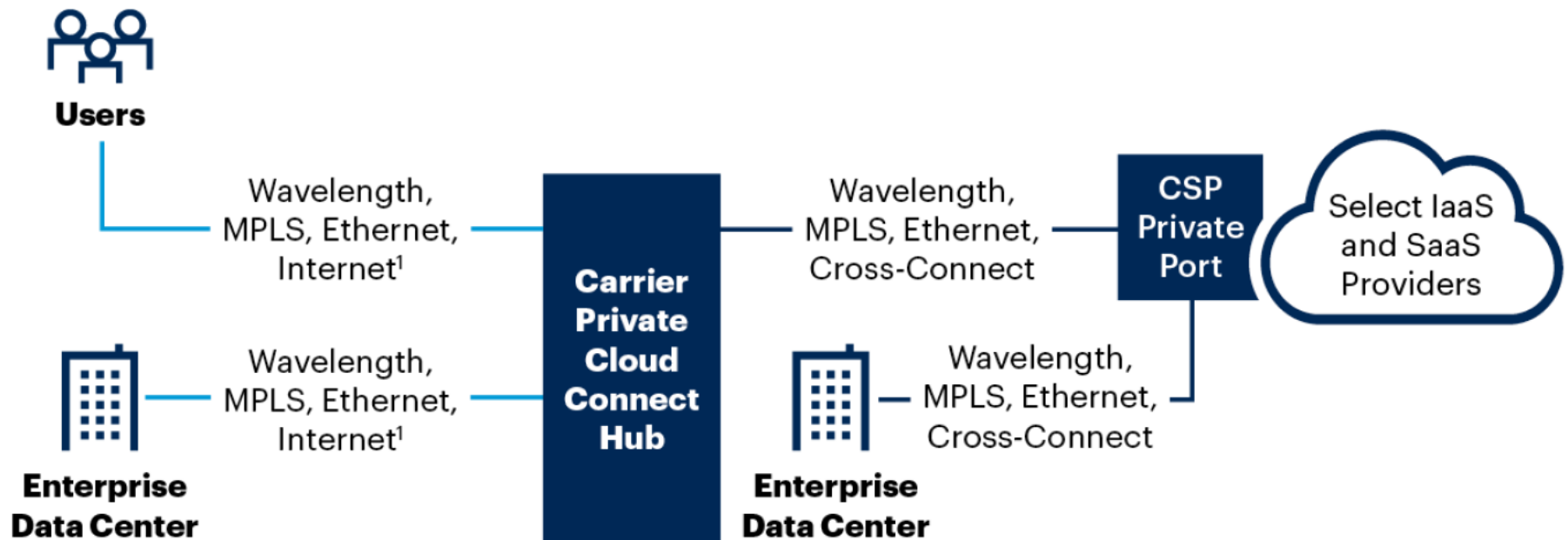
### Multiple Connectivity Choices to Cloud Service Providers (CSPs). Gartner – February 2021

Use both private and public connections driven by specific use-case requirements. It is practical for a telecommuter to access human resources (HR) software as a service (SaaS) app via an internet virtual private network (VPN). However, a data center site with requirements for high bandwidth, enhanced survivability, security, performance and accountability is typically better served by a private connection to the CSP, or by a combination of public and private connections.

## Use Private Cloud Ports for Persistent, High-Volume Use Cases

— Private Transport  
Ingress Into CSP Port

— Connectivity From Enterprise Location  
to Carrier Hub, Cloud Hub, SDCI Hub



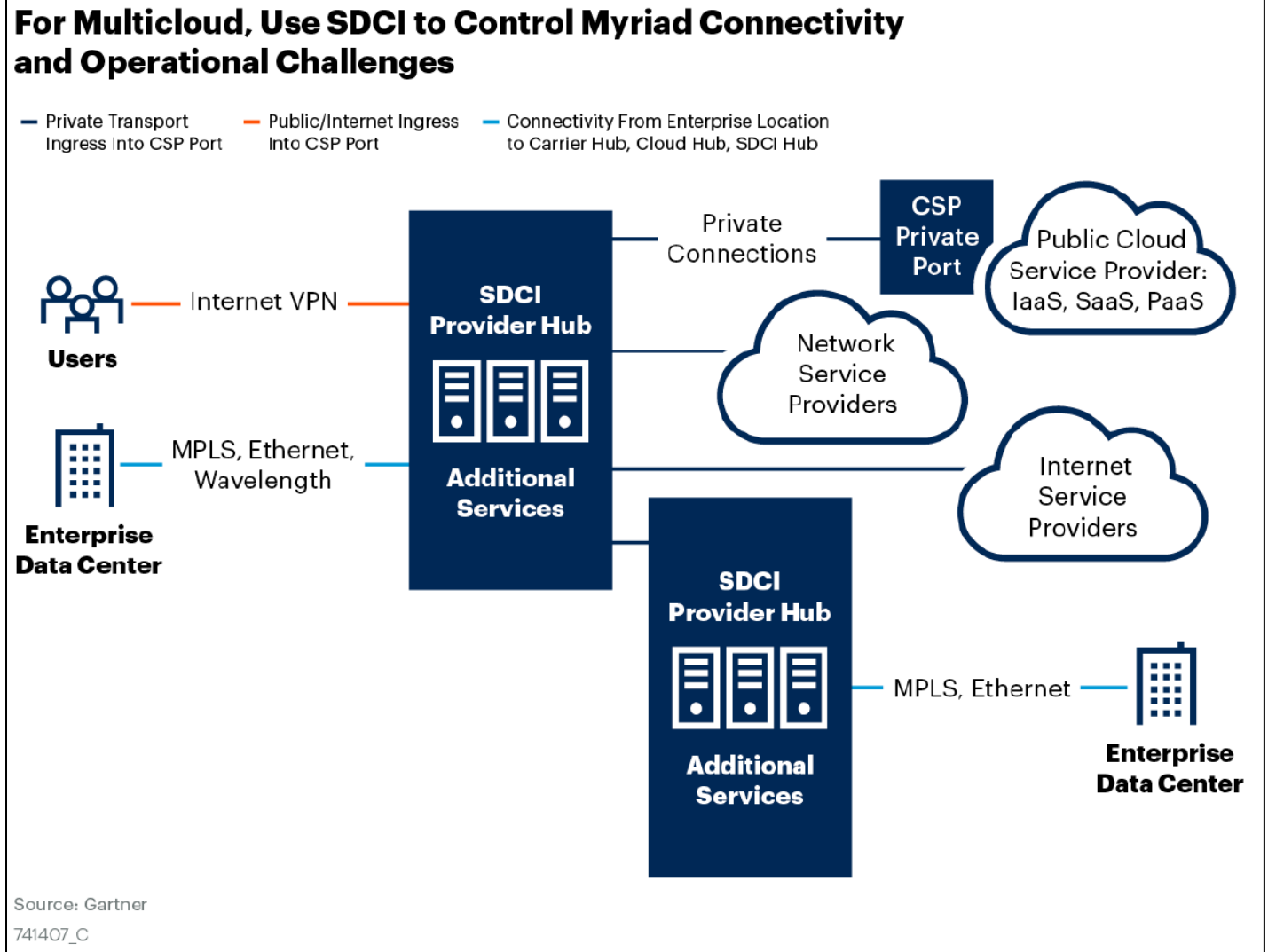
Source: Gartner

<sup>1</sup> Supported by some providers

741407\_C

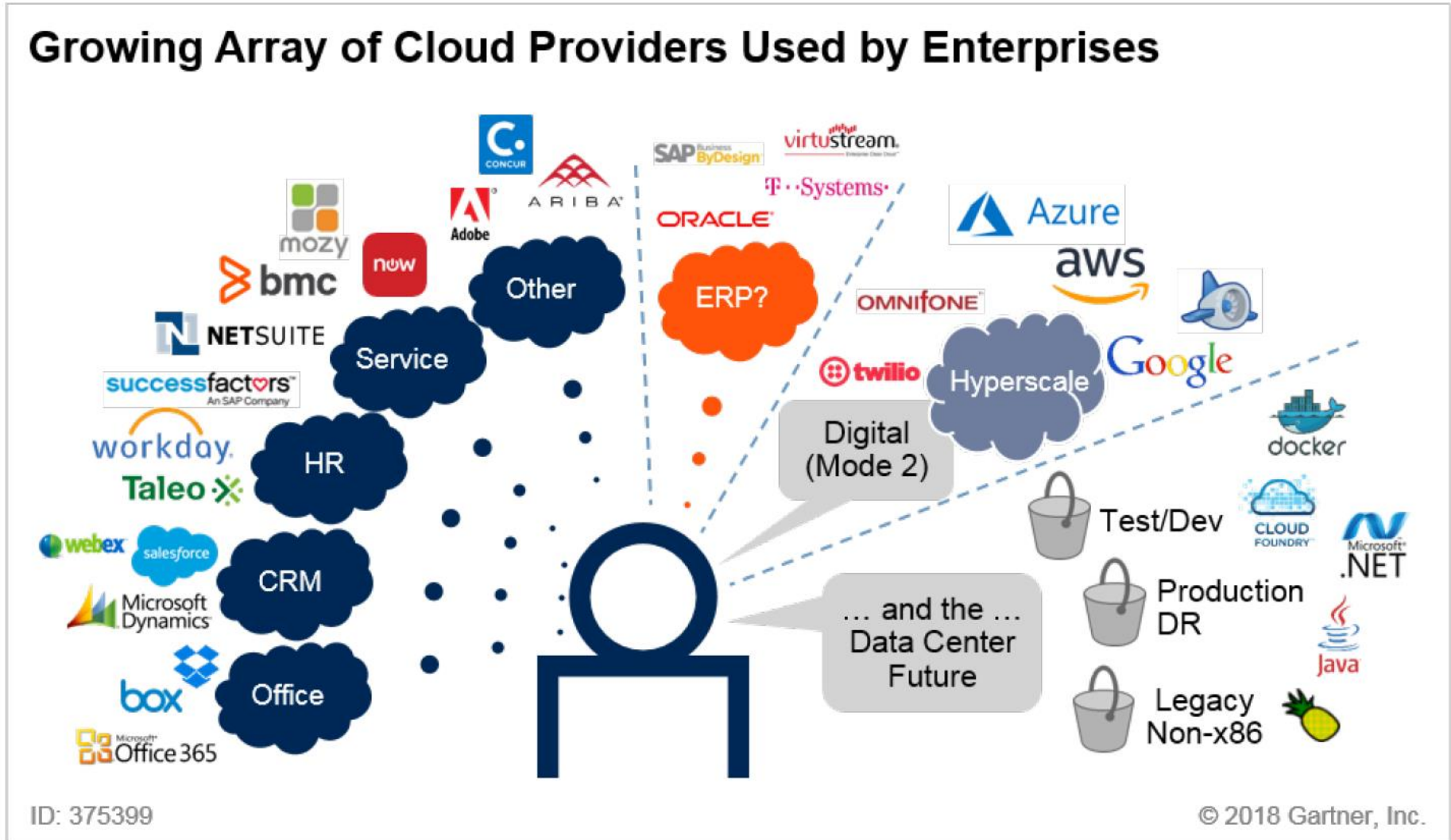
**Use Private Cloud Ports for Persistent, High-Volume Use Cases.**

How to optimize network connectivity into Public Cloud Providers. Gartner ID 741407C – Feb-19-2021



**For multi-cloud, use SDCI to control myriad connectivity and operational challenges.**

How to optimize network connectivity into Public Cloud Providers. Gartner ID 741407C – Feb-19-2021



**Growing Array of Cloud Providers Used by Enterprises – November 2018.**

Five Key Factors to Prepare Your WAN for Multicloud Connectivity. Gartner ID 375399 – April 16, 2020.

## Alternatives to Internet-Based Cloud Connections

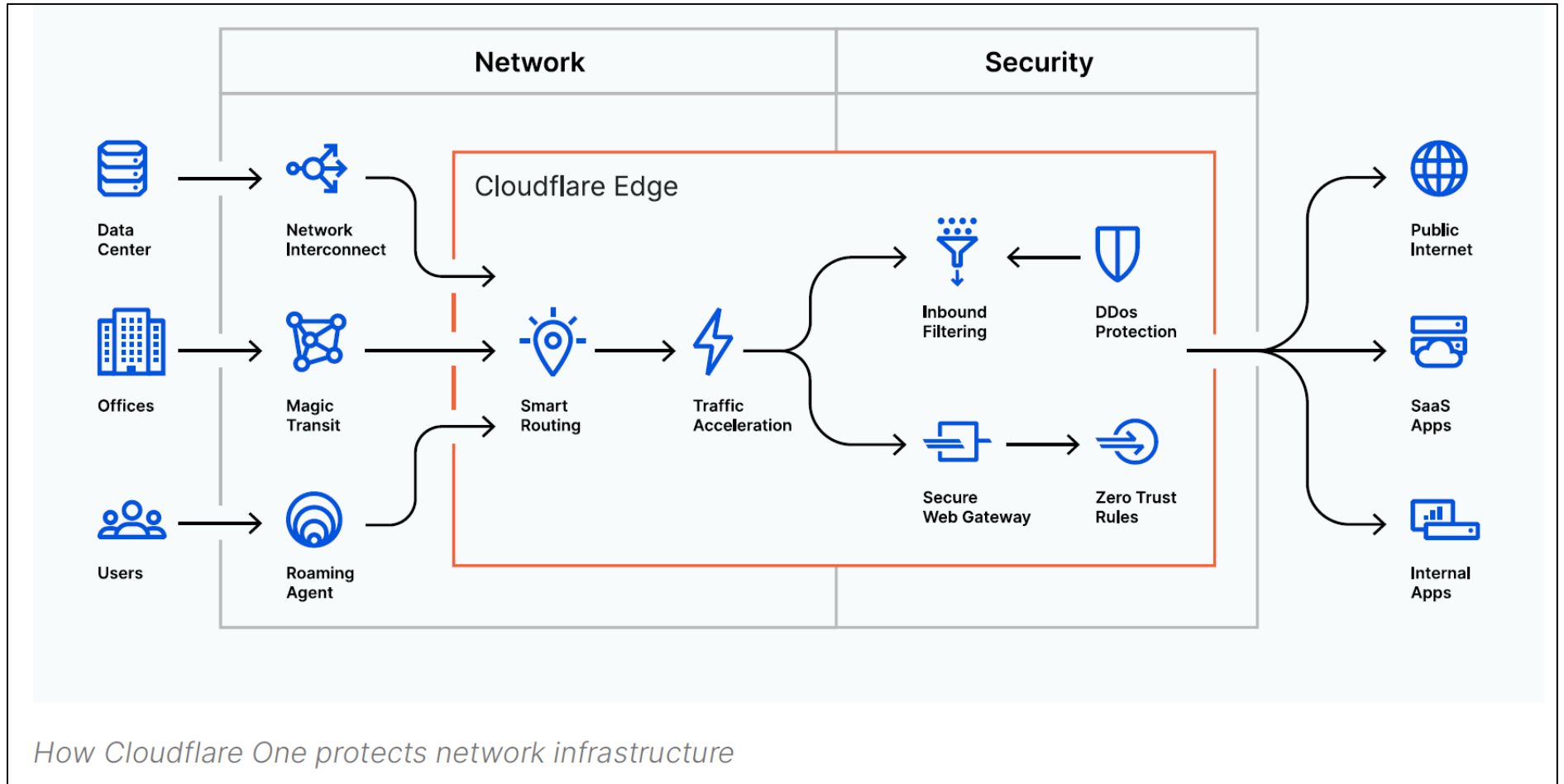
	<b>Carrier-Based Interconnect (CBI)</b>	<b>Software-Defined Interconnect (SDI)</b>	<b>Colocation Hub (CH)</b>
<b>Description</b>	Using CBI, the NSP has preprovisioned capacity to connect to a CSP, SDI or CH.	SDI connects enterprise data centers to CSPs, peering partners and CHs through a software-defined fabric.	A CH connects the enterprise data center to CSPs and peering partners via private high-speed connectivity.
<b>Vendor Examples</b>	Many Tier 1 and Tier 2 NSPs, system integrators and managed service providers	Console Connect, Megaport	CoreSite, Equinix

ID: 375399

© 2018 Gartner, Inc.

### Alternatives to Internet-Based Cloud Connections – November 18, 2018.

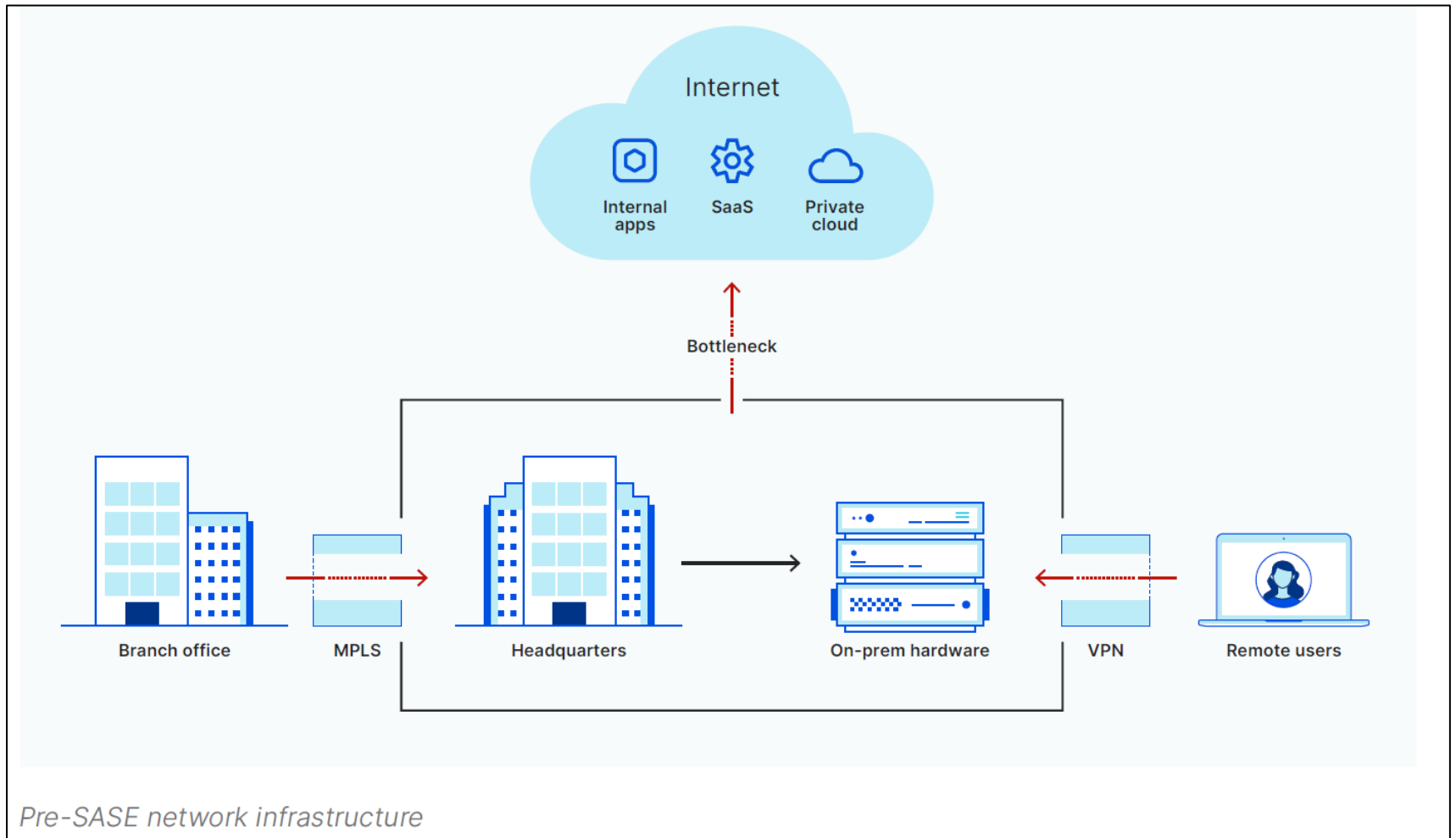
Five Key Factors to Prepare Your WAN for Multicloud Connectivity. Gartner ID 375399 – April 16, 2020.



**How CloudFlare Delivers SASE.**

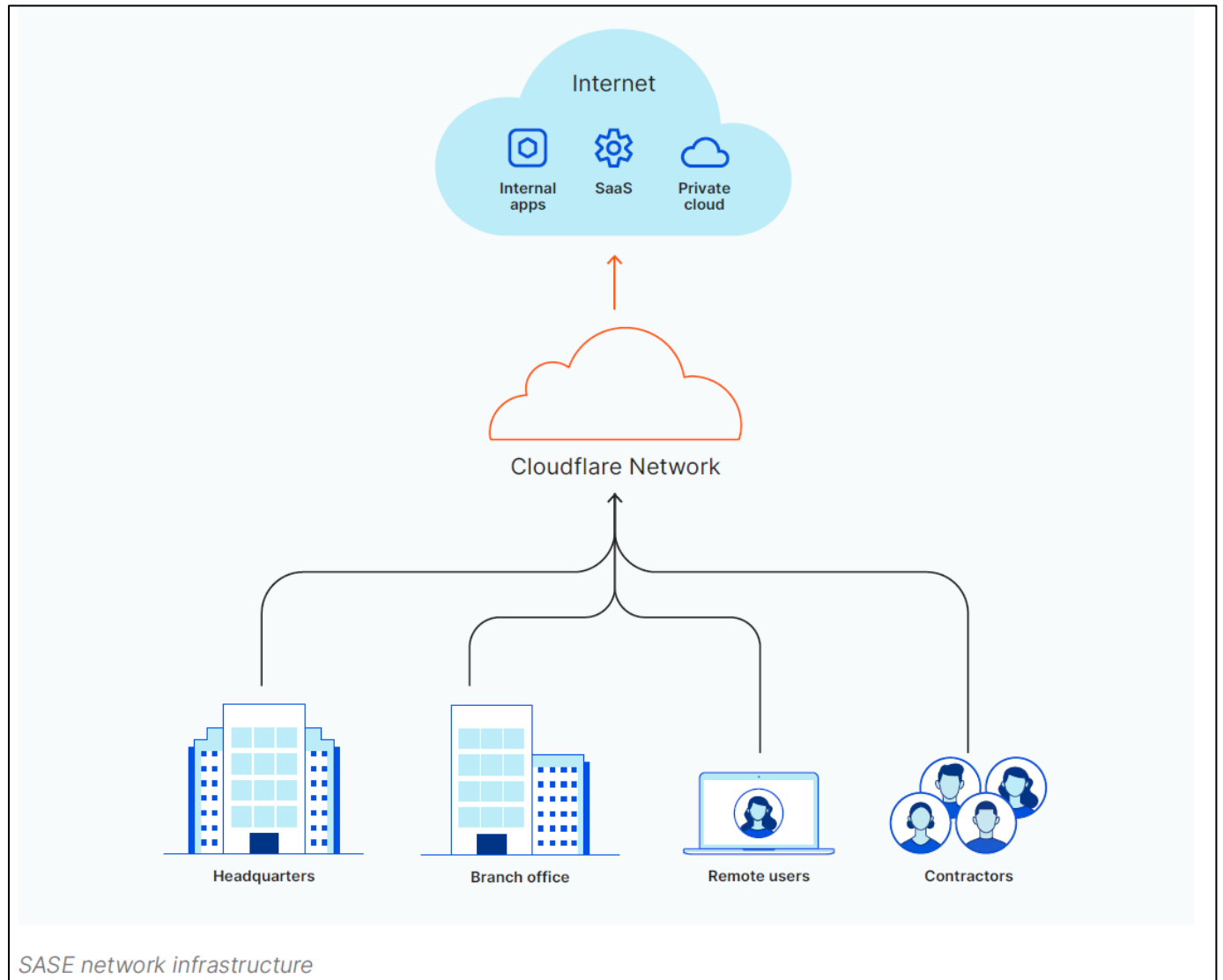
Getting started with SASE: A guide to secure and streamline your network infrastructure – Whitepaper by CloudFlare. November 11, 2020.





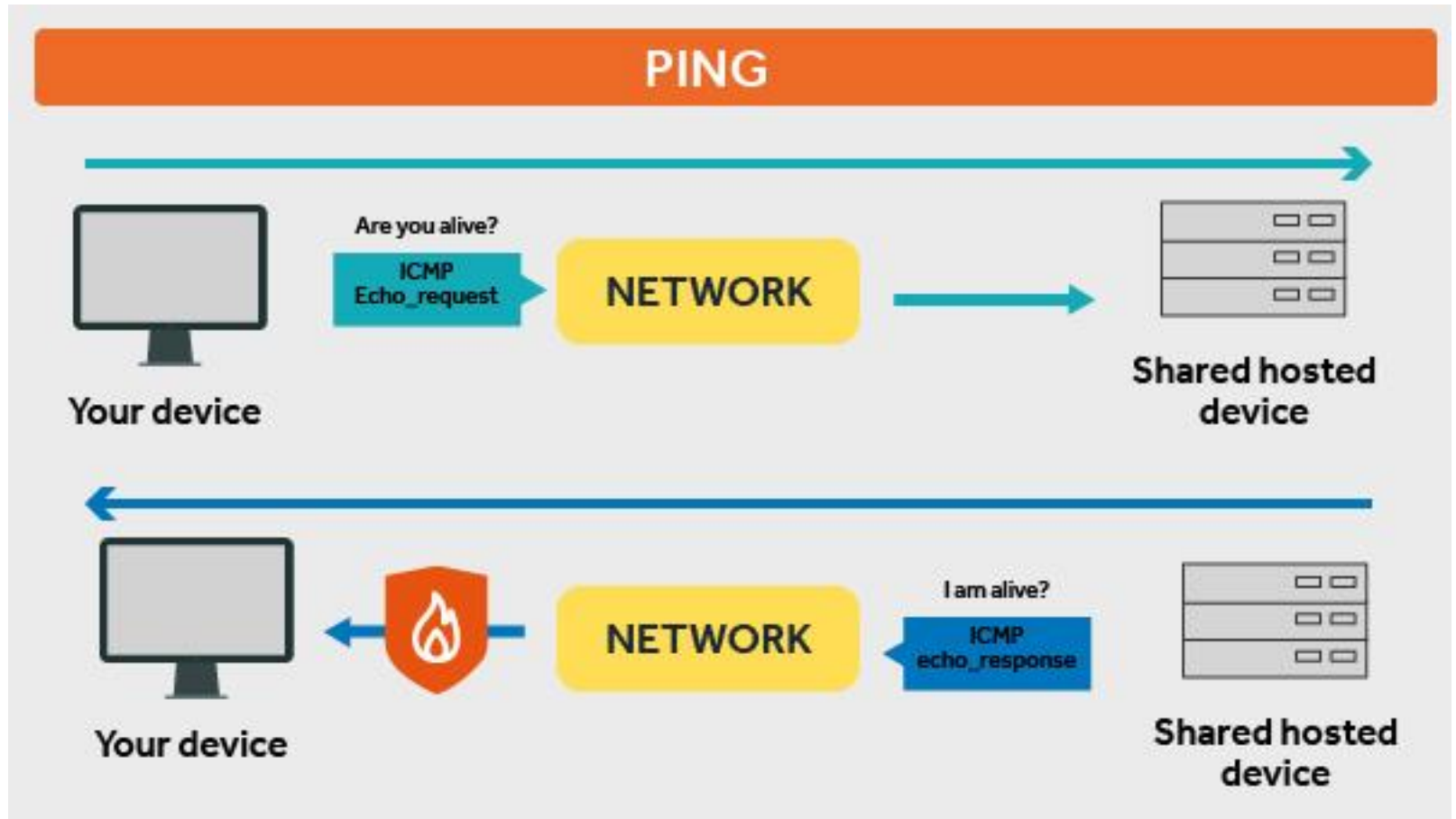
**Pre-SASE Network Architecture Diagram.**

Getting started with SASE: A guide to secure and streamline your network infrastructure. Cloudflare Whitepaper. November 11, 2020



**SASE Network Architecture Diagram.**

Getting started with SASE: A guide to secure and streamline your network infrastructure. Cloudflare Whitepaper. November 11, 2020

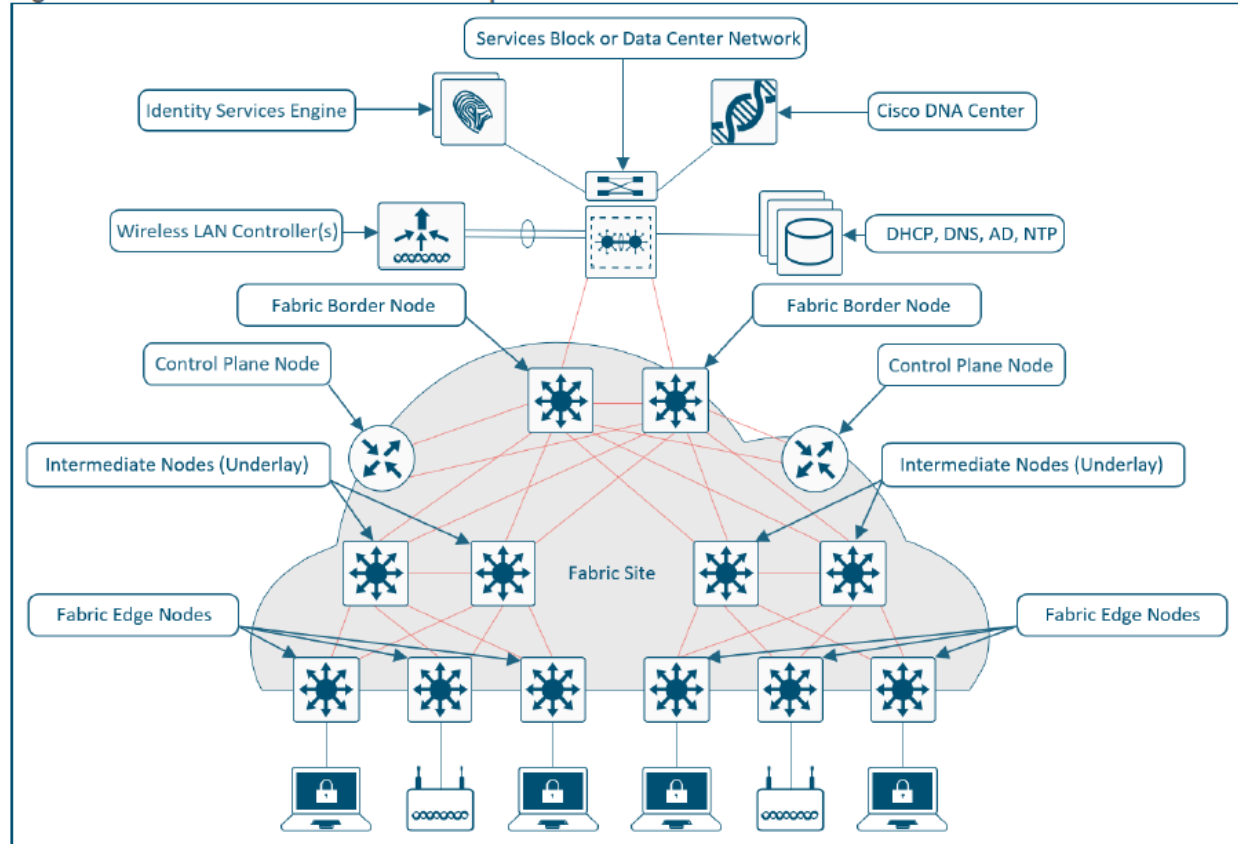


**How Does Ping Work.**

How does a firewall affect ping? Starcom – A Node4 Company – January 27, 2020

<https://starcom.node4.co.uk/how-does-a-firewall-affect-ping/>

Figure 8. SD-Access Fabric Roles - Example



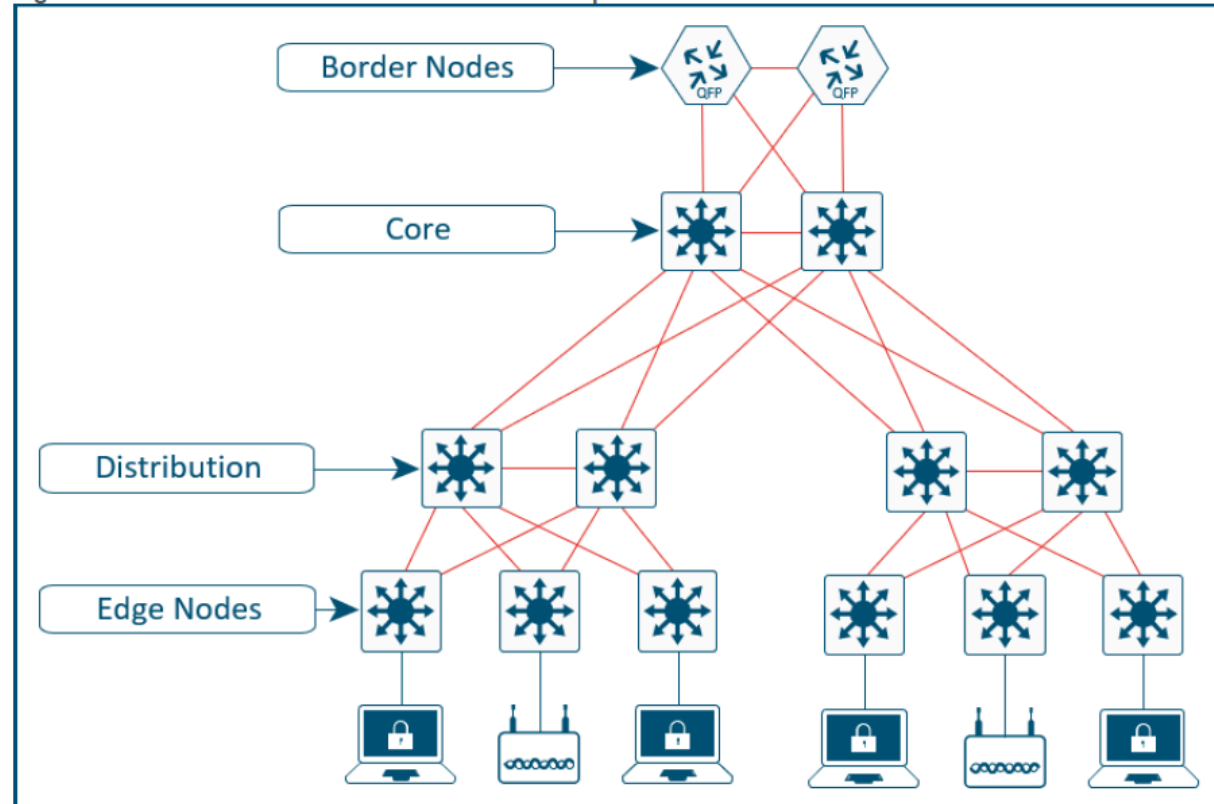
### Control Plane Node

The SD-Access fabric control plane node is based on the LISP Map-Server and Map-Resolver functionality combined on the same node. The control plane node's database tracks all endpoints in the fabric site and associates the endpoints to fabric nodes, decoupling the endpoint IP address or MAC address from the location (closest router) in the network.

### SD Access Fabric Roles – Example

Software Defined Access Solution Design Guide by Cisco Public - June 2020

Figure 9. Intermediate Nodes in SD-Access - Example

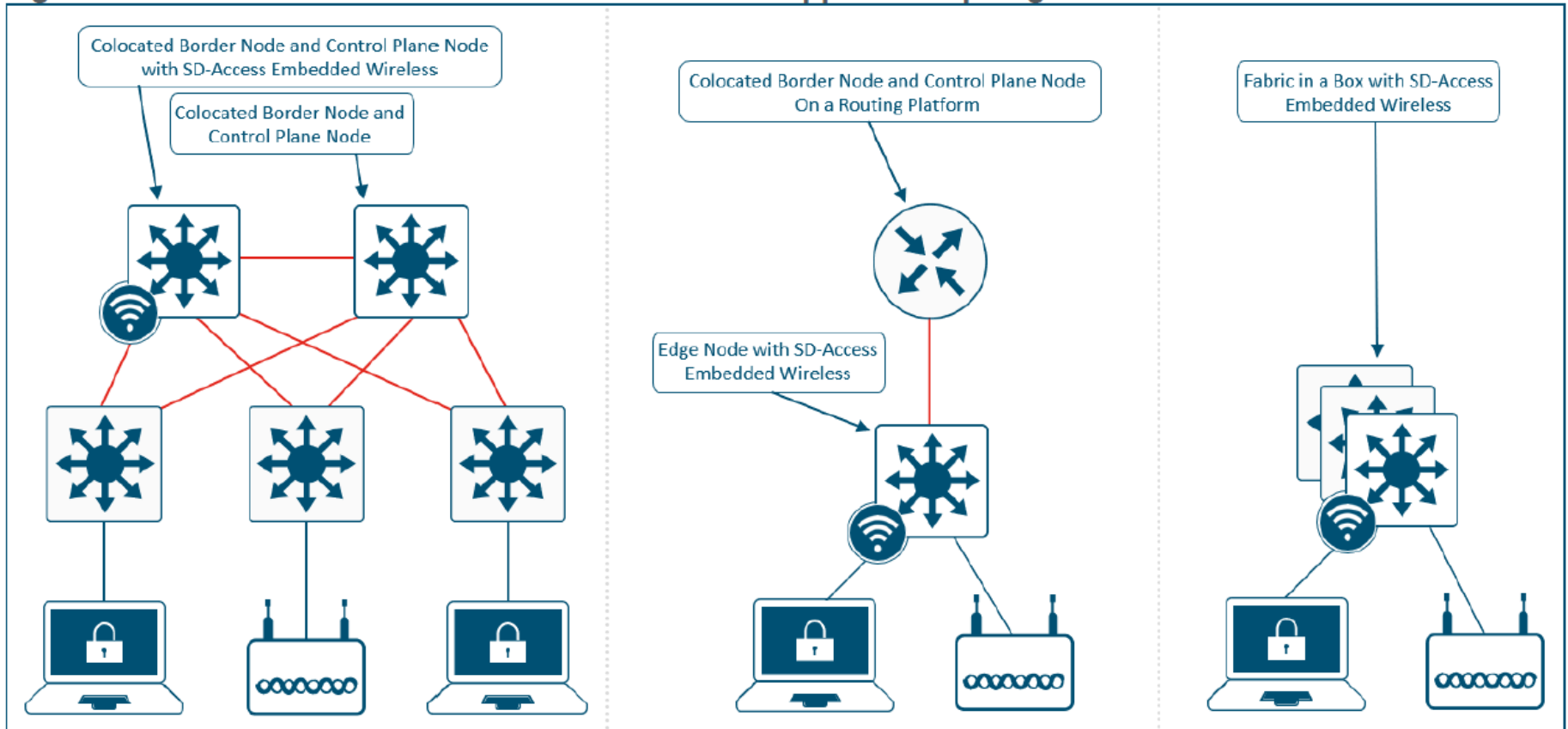


Intermediate nodes do not have a requirement for VXLAN encapsulation/de-encapsulation, LISP control plane messaging support, or SGT awareness. Their requirement is to provide IP reachability, physical connectivity, and to support the additional MTU requirement to accommodate the larger-sized IP packets encapsulated with fabric VXLAN information. Intermediate nodes simply route and transport IP traffic between the devices operating in fabric roles.

### Intermediate Nodes in SD – Example

Software Defined Access Solution Design Guide by Cisco Public - June 2020

**Figure 11. SD-Access Embedded Wireless Supported Topologies**

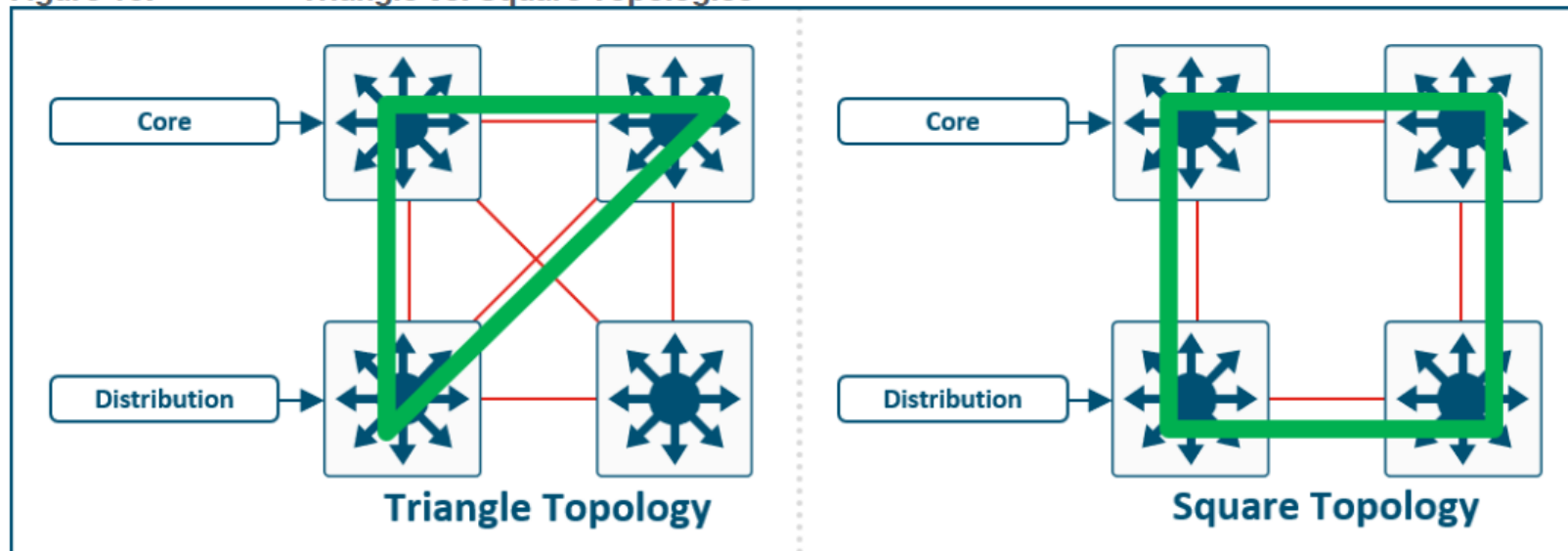


**SD Access Embedded Wireless Supported Topologies**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

SD-Access networks start with the foundation of a well-design, highly available Layer 3 routed access foundation. For optimum convergence at the core and distribution layer, build triangles, not squares, to take advantage of equal-cost redundant paths for the best deterministic convergence. In Figure 15, the graphic on the left shows triangle topologies which are created by devices crosslinking with each other and with their upstream/downstream peers. The graphic on the right shows square topologies that are created when devices are not connected to both upstream/downstream peers. Square topologies should be avoided.

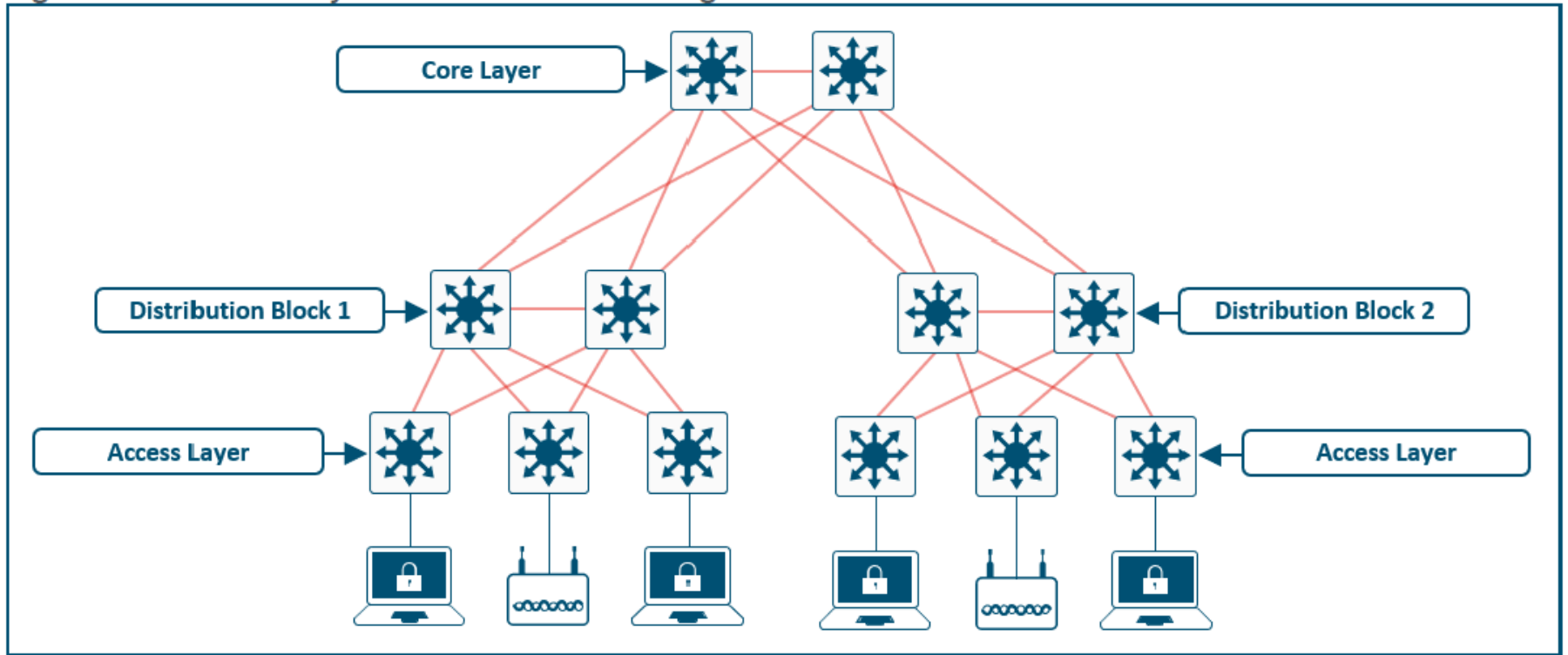
Figure 15. Triangle vs. Square Topologies



**Triangle vs. Square SD-Access Topologies**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

**Figure 16. Layer 3 Routed Access Design**



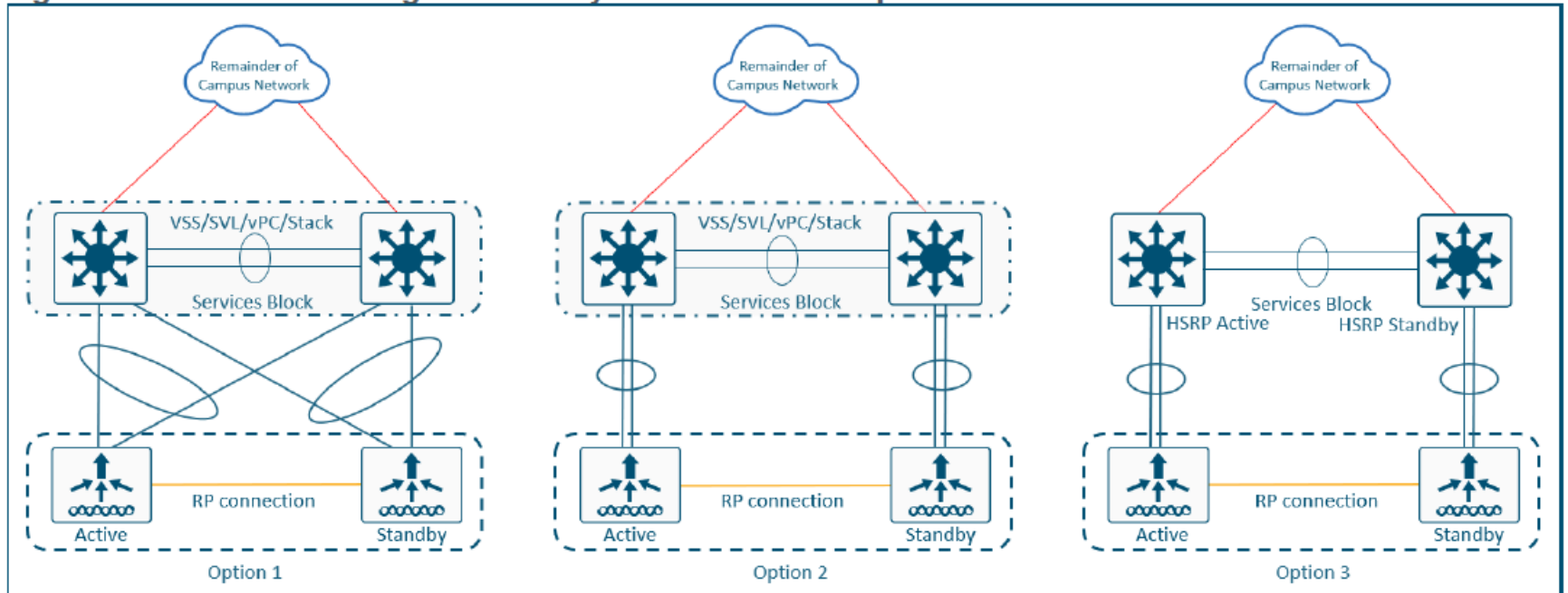
**Layer 3 Routed Access Design**

Software Defined Access Solution Design Guide by Cisco Public - June 2020





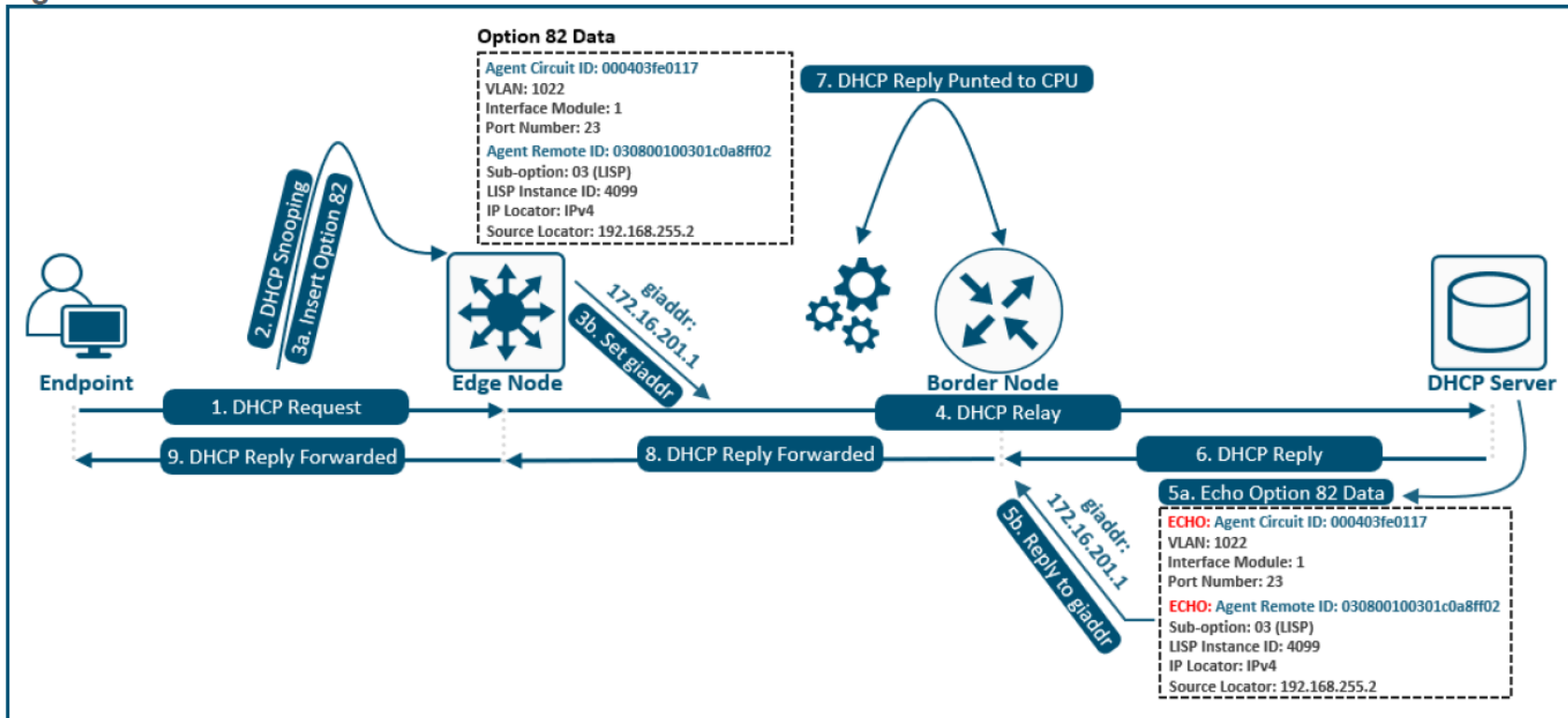
Figure 17. WLC High Availability Pair Connection Options



**WLC High Availability Pair Connection Options**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

Figure 18. Fabric DHCP Packet Flow



## Fabric DHCP Packet Flow

For simplicity, the DHCP Discover and Request packets are referred to as a **DHCP REQUEST**, and the DHCP Offer and Acknowledgement (ACK) are referred to as the **DHCP REPLY**.

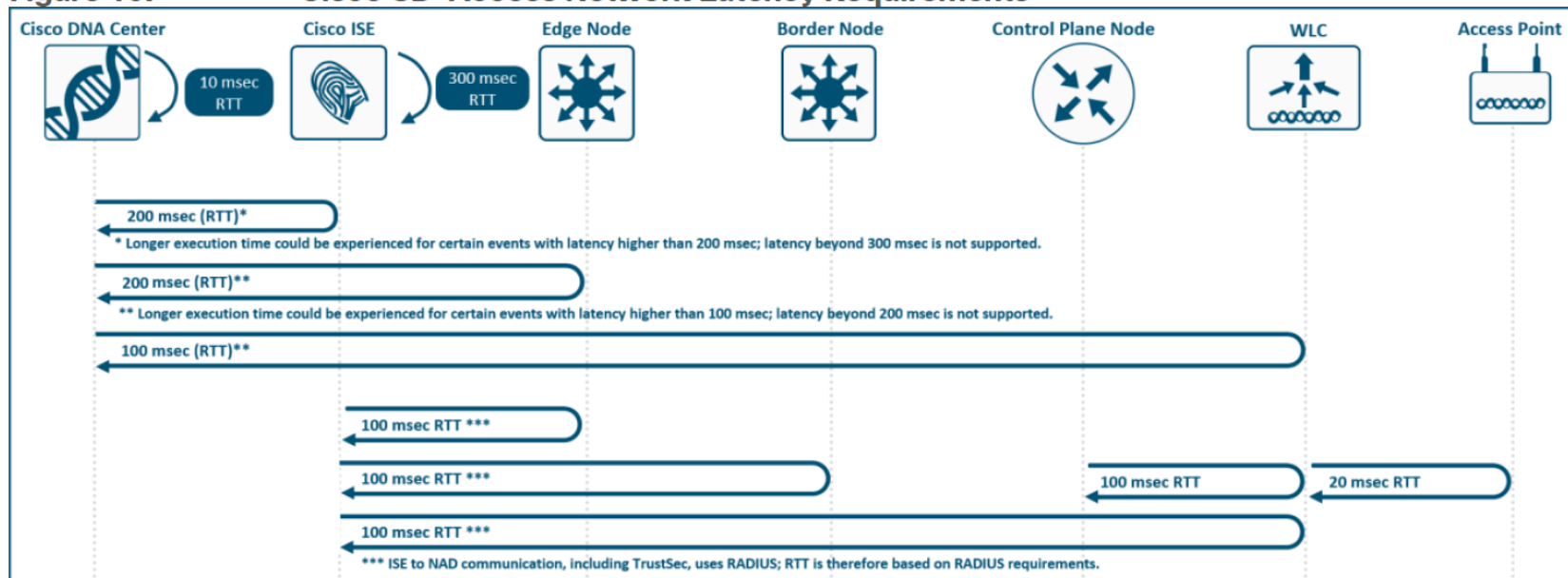
## Fabric DHCP Packet Flow

Software Defined Access Solution Design Guide by Cisco Public - June 2020

## Latency

Latency in the network is an important consideration for performance, and the RTT between Cisco DNA Center and any network device it manages must be taken into strict account. The RTT should be equal to or less than 100 milliseconds to achieve optimal performance for all solutions provided by Cisco DNA Center including SD-Access. The maximum supported latency is 200ms RTT. Latency between 100ms and 200ms is supported, although longer execution times could be experienced for certain functions including Inventory Collection, Fabric Provisioning, SWIM, and other processes that involve interactions with the managed devices.

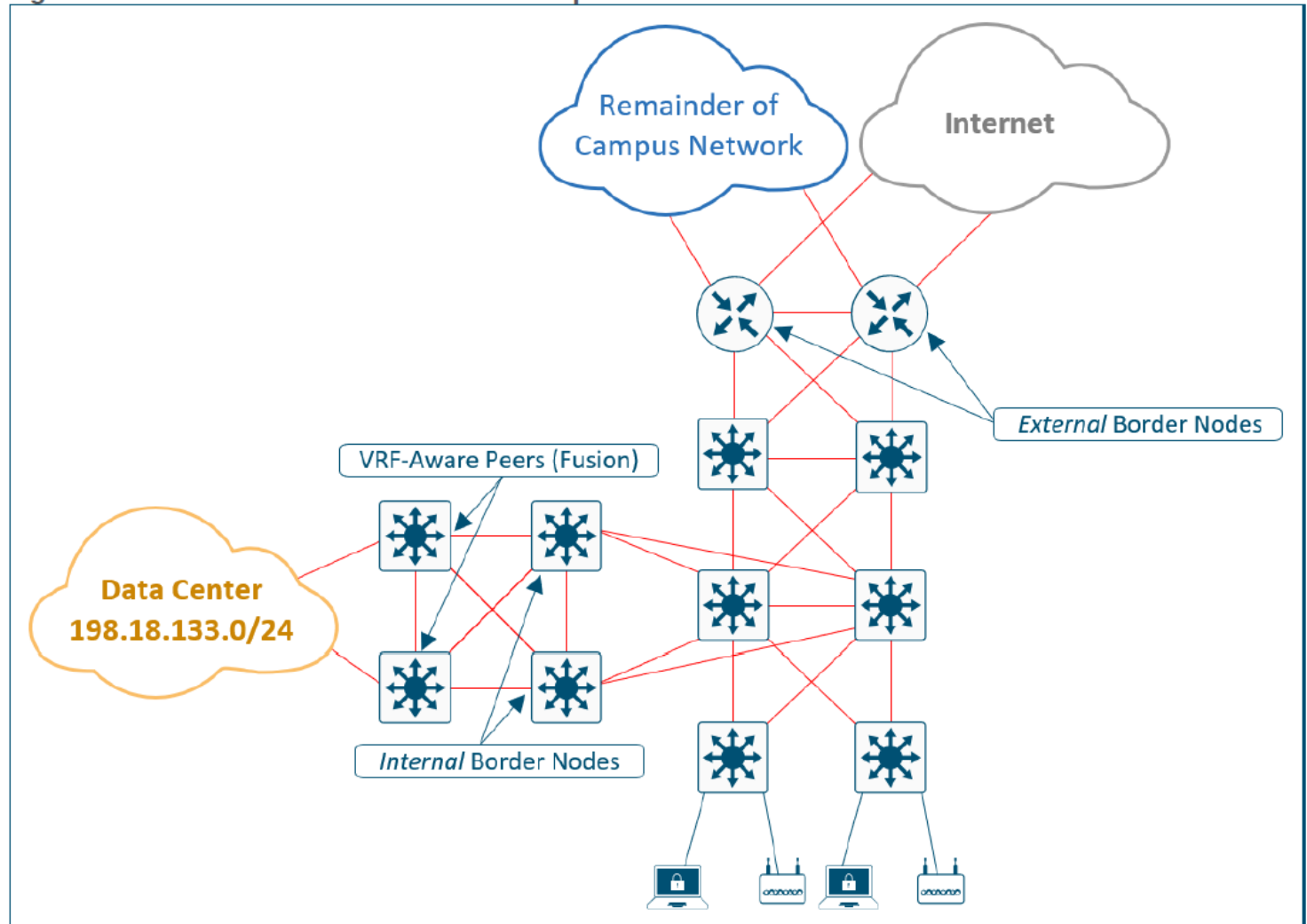
**Figure 19. Cisco SD-Access Network Latency Requirements**



## SD-Access Network Latency Requirements

Software Defined Access Solution Design Guide by Cisco Public - June 2020

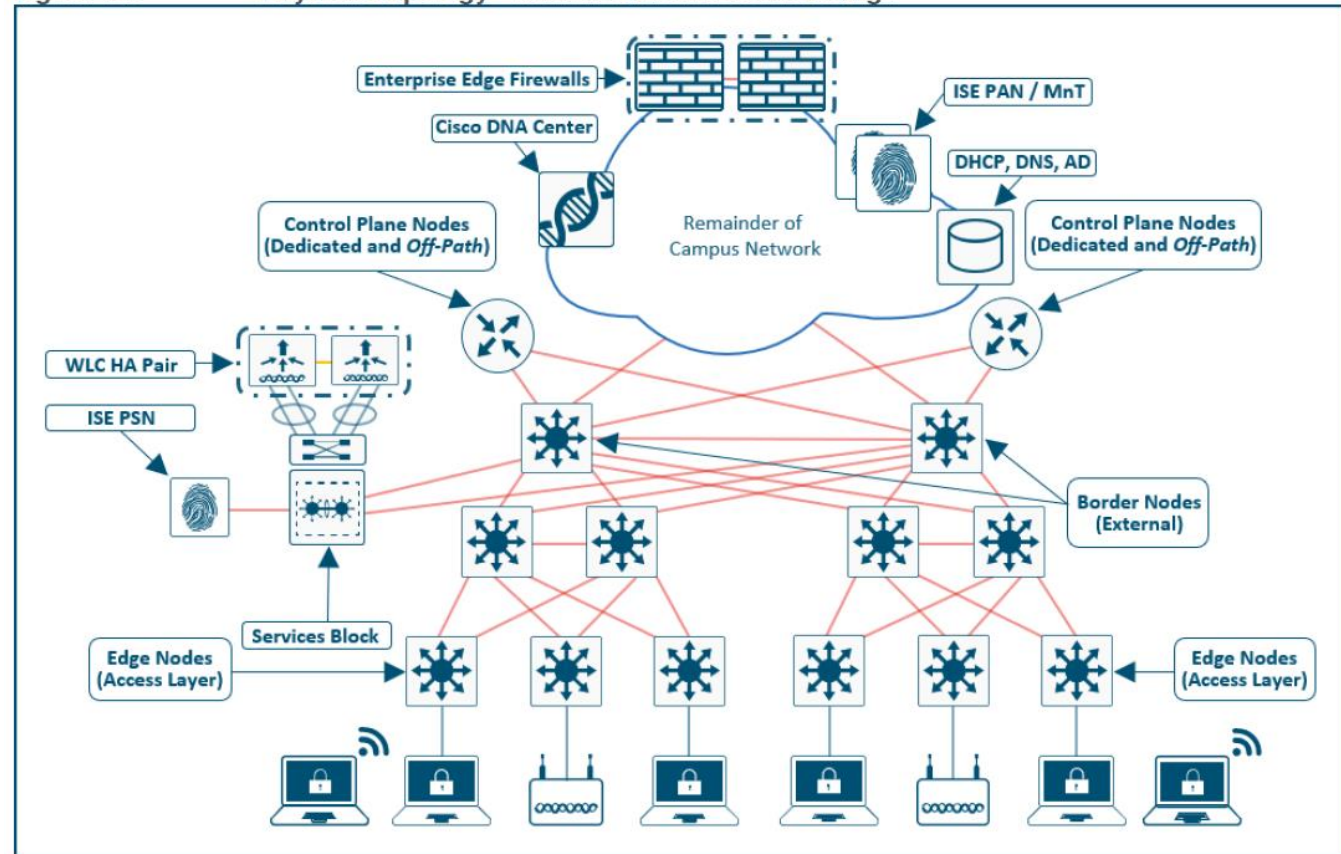
**Figure 21. Internal Border Node Example**



**Internal Border Node Example**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

Figure 40. Physical Topology - Medium Site Reference Design



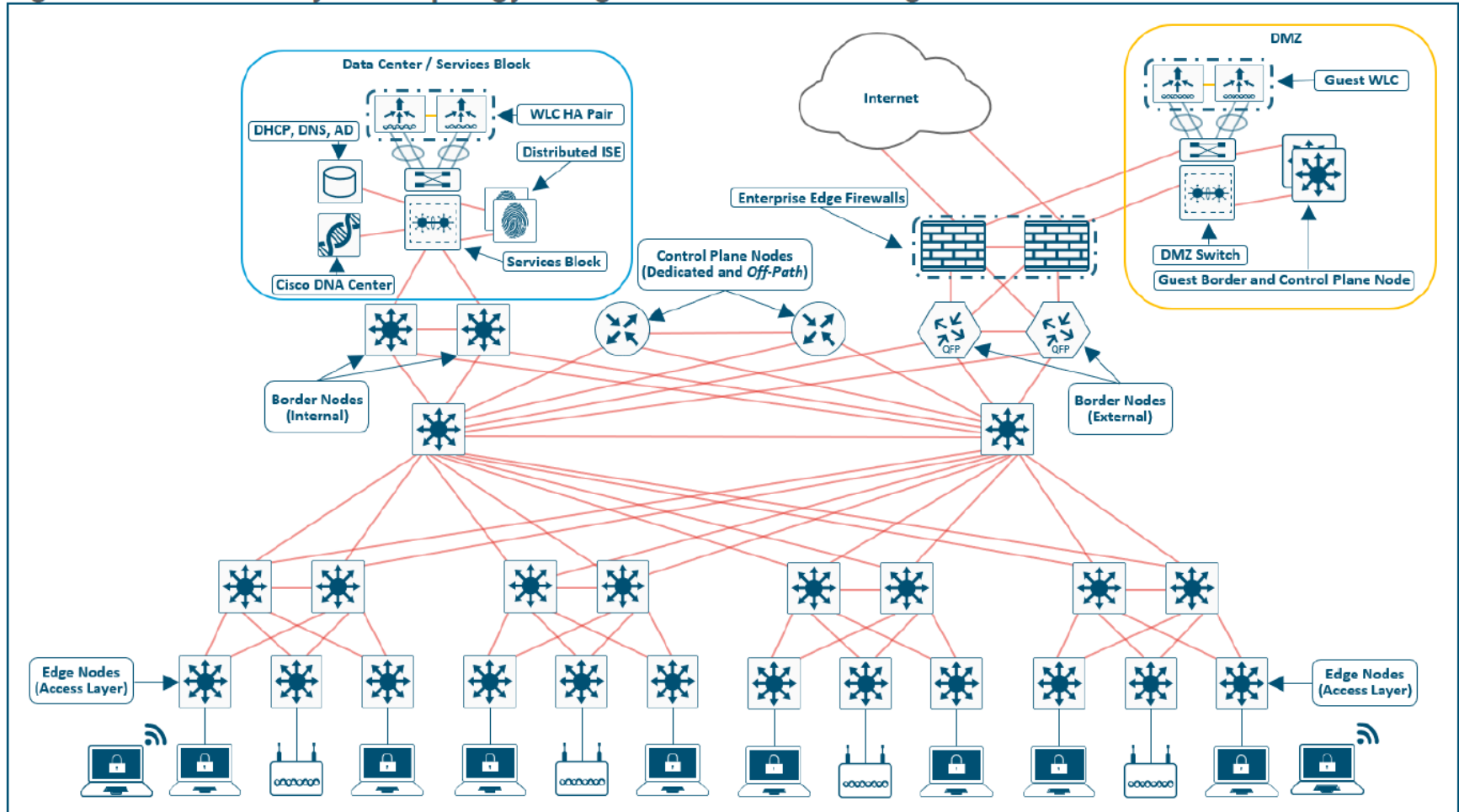
### Medium Site Considerations

In a medium site, high availability is provided in the fabric nodes by dedicating devices as border nodes and control plane nodes rather than collocating the functions together. For both resiliency and alternative

### Physical Topology – Medium Site Reference Design

Software Defined Access Solution Design Guide by Cisco Public - June 2020

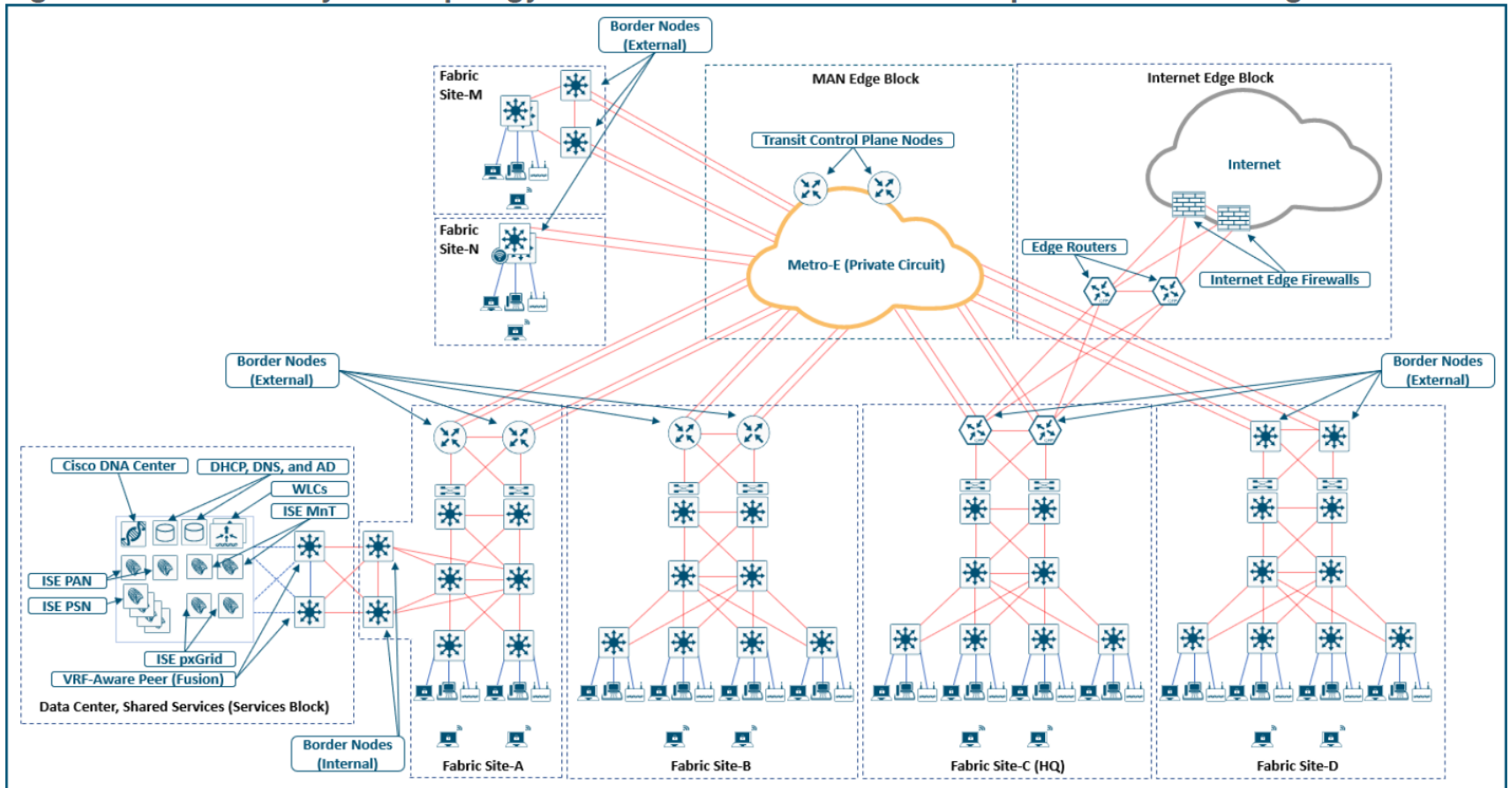
**Figure 41. Physical Topology - Large Site Reference Design**



**Physical Topology – Large Site Reference Design**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

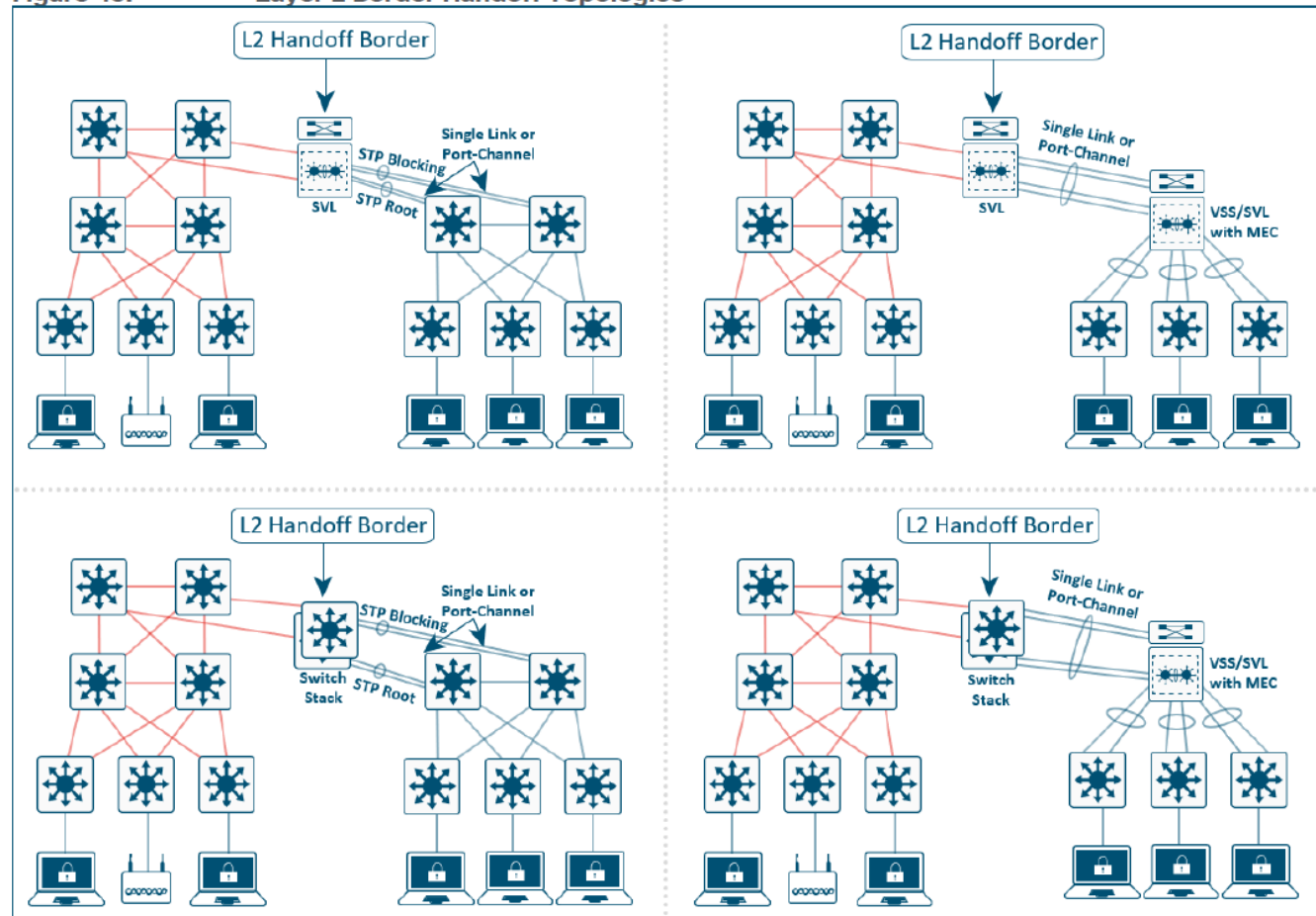
Figure 42. Physical Topology - SD-Access for Distributed Campus Reference Design



**Physical Topology – SD-Access for Distributed Campus Reference Design**

Software Defined Access Solution Design Guide by Cisco Public - June 2020

Figure 43. Layer 2 Border Handoff Topologies

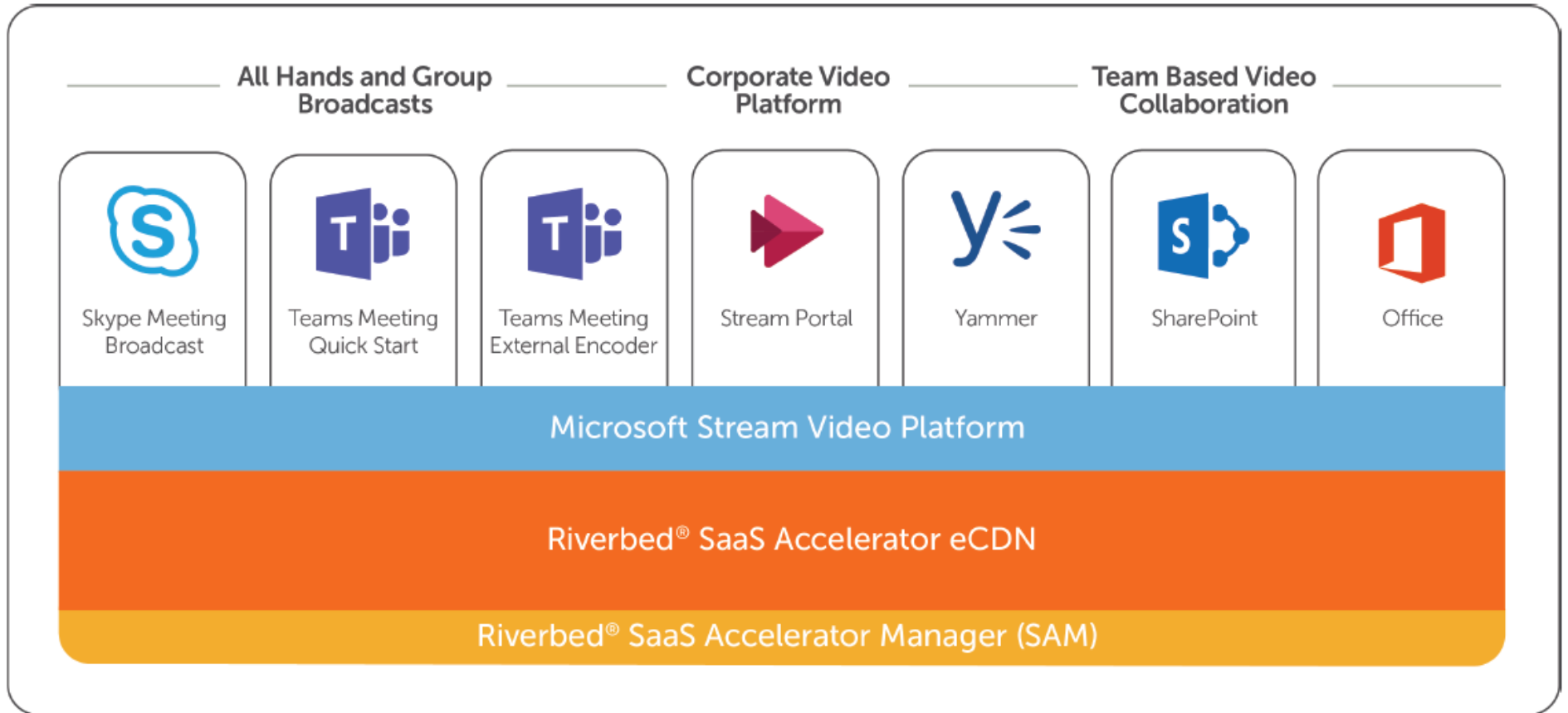


The Border node with the Layer 2 handoff should be a dedicated role. While it is technically feasible for this device to operate in multiple roles (such as a border node with Layer 3 handoff and control plane node), it is strongly recommended that a dedicated device be used. Because this device is operating at Layer 2, it is

### Layer 2 Border Handoff Topologies

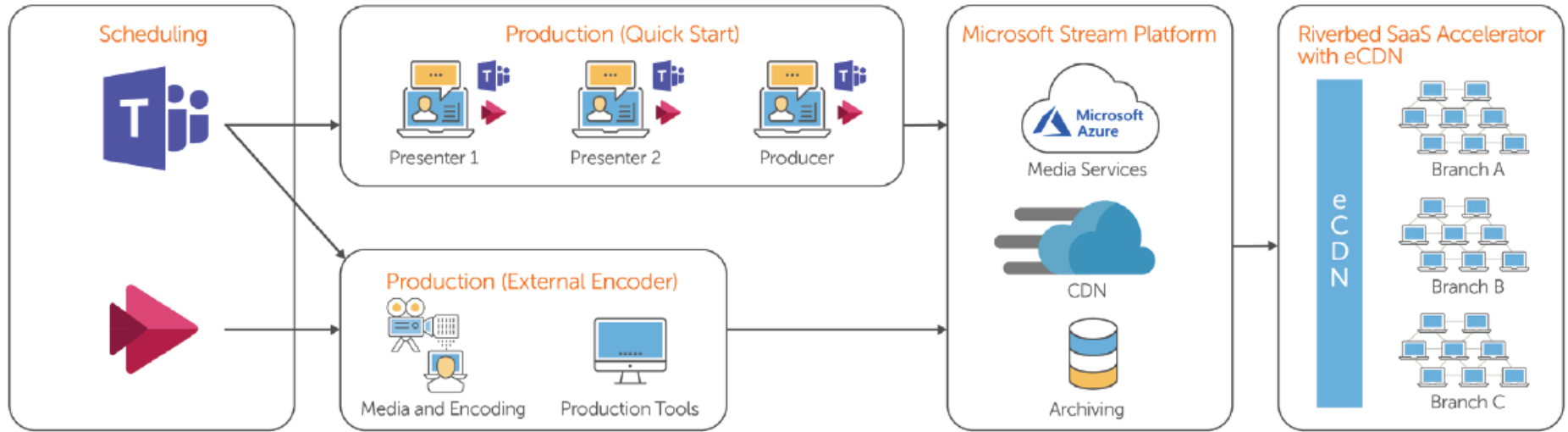
Software Defined Access Solution Design Guide by Cisco Public - June 2020





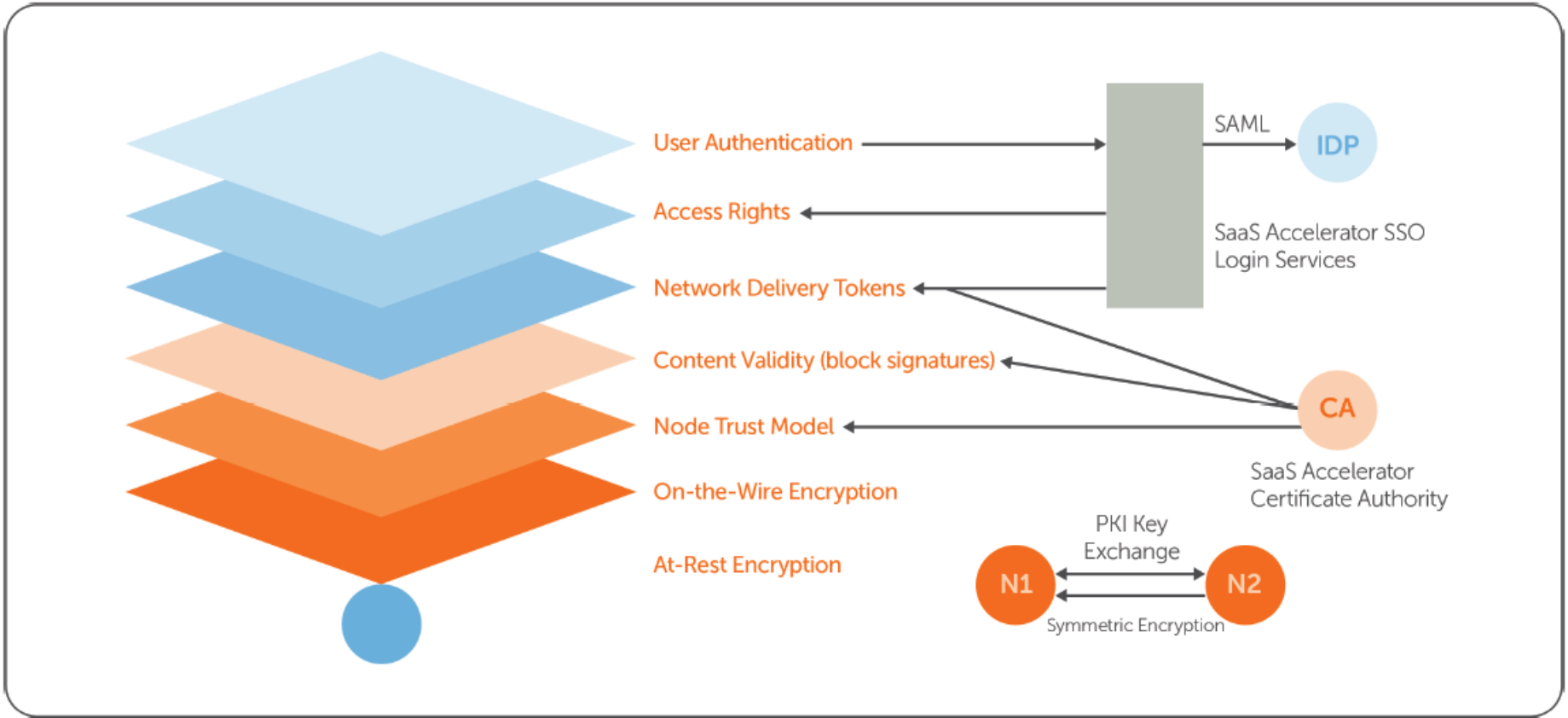
**Riverbed SaaS Accelerator eCDN and SAM**

SaaS Accelerator Integration with Microsoft Stream, Teams for Live On-Demand Video – January 25, 2021



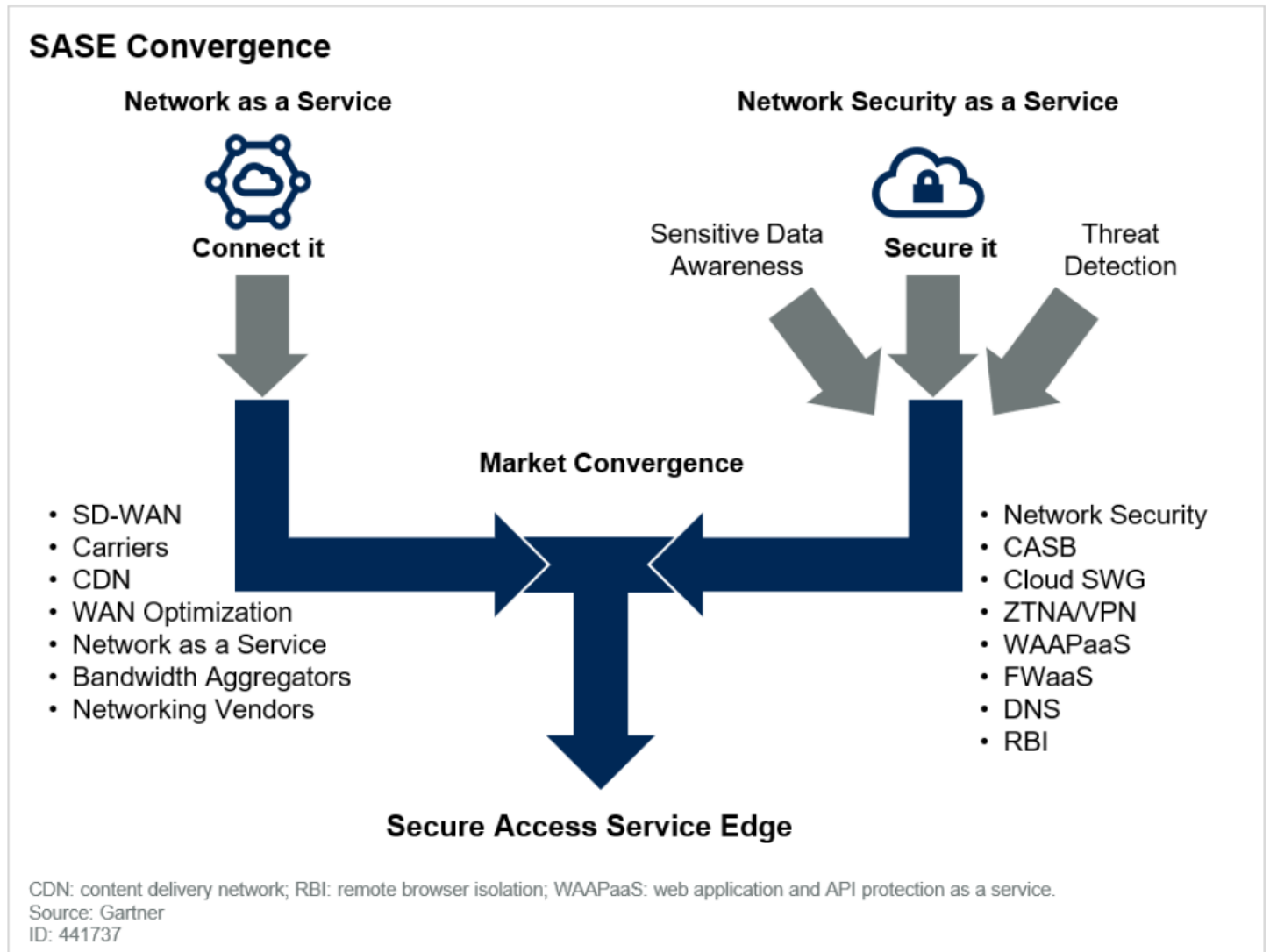
**Azure and Riverbed Delivery Ensured**

SaaS Accelerator Integration with Microsoft Stream, Teams for Live On-Demand Video – January 25, 2021



**SaaS Acceleration**

SaaS Accelerator Integration with Microsoft Stream, Teams for Live On-Demand Video – January 25, 2021



**SASE Convergence**

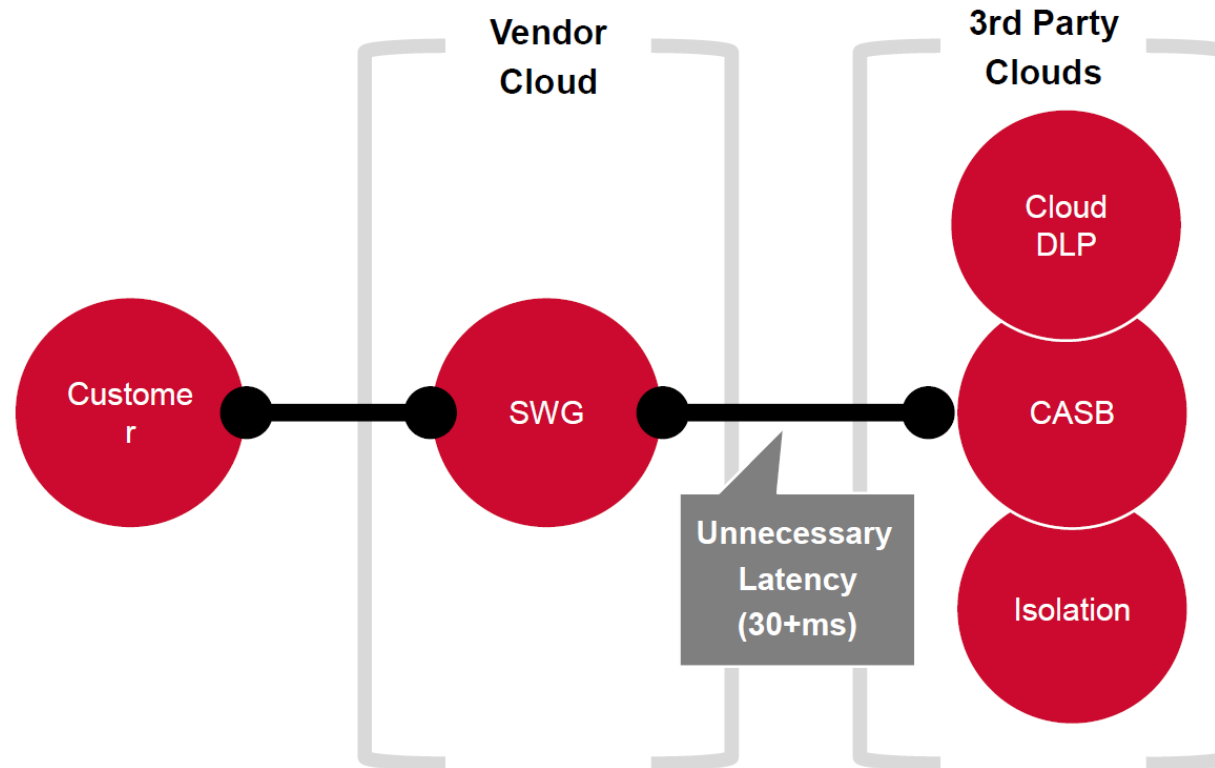
Gartner – August 30, 2019

Data Level	Level 0 Public	Level 1 Internal	Level 2 Sensitive/Confidential	Level 3 Highly Restricted
Data Restriction	<ul style="list-style-type: none"> <li>• Can be stored anywhere</li> <li>• Freely distributed</li> </ul>	<ul style="list-style-type: none"> <li>• Not shared publicly without authorization</li> <li>• Can be stored on University computers</li> <li>• Network drives</li> <li>• Google Drive</li> <li>• Dropbox</li> </ul>	<ul style="list-style-type: none"> <li>• Requires authorization to view</li> <li>• Should not be stored on computer hard drives (Use caution using Dropbox Sync App and Google Drive sync)</li> <li>• Can be stored on network drives and online in Google Drive and Dropbox <u>with limited access</u></li> </ul>	<ul style="list-style-type: none"> <li>• In general, should not be copied or downloaded from the secure location without speaking with the Data Owner, Data Security Officer, Information Security Liaison, or Information Security Compliance Office</li> </ul>
Data Examples	<ul style="list-style-type: none"> <li>→ Job postings</li> <li>→ Press releases</li> <li>→ Marketing material</li> <li>→ Published research, presentations, or papers</li> </ul>	<ul style="list-style-type: none"> <li>→ Department procedures</li> <li>→ Budget information</li> <li>→ Internal memos</li> </ul>	<ul style="list-style-type: none"> <li>→ FERPA data</li> <li>→ Personnel records</li> <li>→ Personally-identifiable information</li> </ul>	<ul style="list-style-type: none"> <li>→ SSNs</li> <li>→ Credit card information</li> <li>→ Restricted research data</li> </ul>

### Remote Work Data Access

IT Services and Remote Access – UNC Charlotte – April 9, 2020

## SASE Service Chaining = Bad



21 | Broadcom Proprietary and Confidential. Copyright © 2021 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



### SASE Service Chaining Equals Bad Diagram.

Leading Cloud Transformation with Symantec's Data Centric SASE.

Gartner Asia-Pacific (APAC) Security & Risk Management Summit – March 23-24, 2021 – Australia.

# APPENDIX A: GLOSSARY

## COV ITRM Glossary:

The most current COV ITRM glossary is available at the following URL:

<https://www.vita.virginia.gov/it-governance/glossary/cov-itrm-glossary/>

## Terms derived from other VITA documents or accepted glossaries:

These terms are listed because they were either not present in VITA’s glossary, or other definitions further defined a term for increased clarity within this document.

***Alternate Worksite*** is a work location outside of the customary physical business site. Alternate worksites may include the employee’s home, a telework center, a client site, a field site, etc. <sup>38</sup>

***Architecture or “Technical Architecture”*** means the design, process, strategies, and specification of the overall structure, logical components, and the logical interrelationships of equipment and software, including system software, a network, or other reasonably related concept. <sup>39</sup>

***Availability or “Available”*** means the full functionality of a service component is available for use by users so that it is not degraded in any material respect. <sup>40</sup>

***Capacity Management*** means the responsibility for ensuring that the capacity of the IT infrastructure matches the evolving demands of the business in a cost effective and timely manner. <sup>41</sup>

***Connectivity*** means the ability to access and exchange data, voice, and/or video electronic impulses between various Infrastructure components and with external sources as approved by VITA and provided to users. <sup>42</sup>

***Continuity or “Business Continuity”*** means the overall, organization-wide plans and activities that are intended to enable continued business operation in the event of any unforeseen interruption (for example, plans and

---

<sup>38</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>39</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>40</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>41</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>42</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

activities to move a department or business unit to a new location in the event of a business disruption). Business Continuity Services consist of the business recovery related Services.<sup>43</sup>

**Documentation** means collectively, written materials, documentation, specifications, technical manuals, training materials, guides, flow diagrams, file descriptions, notes and other written information, including as may be associated with a software Deliverable, System or otherwise in connection with the Services.<sup>44</sup>

**Gateway** means connectivity between network segments, which may include transport, equipment, firewalls, or network address translation.<sup>45</sup>

**IKE (Internet Key Exchange)** is the protocol used by IPsec to negotiate IPsec connection settings; authenticate endpoints to each other; define the security parameters of IPsec-protected connections; negotiate session keys; and manage, update, and delete IPsec-protected communication channels.<sup>46</sup>

**Infrastructure** means the entire portfolio of equipment, system software, and network components required for the integrated provision and operation of VITA and Customer’s IT systems and applications.<sup>47</sup>

**Internet** is an external worldwide public data network using Internet protocols to which COV can establish connections.<sup>48</sup>

**Internet Protocol Security (IPsec)** is a suite of open standards for ensuring private communications over public networks, and is the most common network layer security control, typically used to encrypt IP traffic between hosts in a network.<sup>49</sup>

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack as depicted in the diagram below –

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP, S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

<sup>43</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>44</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>45</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>46</sup> Guide to IPsec VPNs. NIST Special Publication 800-77, Revision 1, Draft. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. July 2019. <https://doi.org/10.6028/NIST.SP.800-77r1-draft>.

<sup>47</sup> Attachment 1 to Amendment 3 to Statement of Work. Modification #5 to Contract Number VA-151028-MCI between the Virginia Information Technologies Agency on behalf of the Commonwealth of Virginia and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services. Effective date: August 15, 2018.

<sup>48</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>49</sup> Guide to IPsec VPNs. NIST SP 800-77 Rev. 1 (Draft). National Institute of Standards and Technology (NIST), U.S. Department of Commerce. July 2019. <https://doi.org/10.6028/NIST.SP.800-77r1-draft>.



**Latency** describes the length of time it takes for a packet of data to go from the computer hosting the user desktop to the RDS Host and back, known as round-trip-time (RTT). Latency is also referred to as ping and expressed in milliseconds in one second (ms).<sup>50</sup>

**Mobile Work** is a formal work arrangement where work is not tied to a single physical location. Instead, it requires the worker to travel to multiple locations for a material portion of the workweek. A formal mobile work agreement must exist between employee and employer that details the terms and conditions of the arrangement. A mobile worker can also be a Teleworker if they utilize an Alternate Worksite rather than a central office location.<sup>51</sup> **Portal** is a server that offers access to one or more applications through a single centralized interface. A teleworker uses a portal client on a telework client device to access the portal. Most portals are web-based—for them, the portal client is a regular web browser.<sup>52</sup>

**Remote Access** is the ability to get access to a computer or a network from a remote distance.<sup>53</sup>

**Remote User** is a user who accesses a computer or a network from a remote distance.<sup>54</sup>

**Situational Telework** is work that while conducted at an Alternate Worksite is unscheduled, project oriented, non-recurring, and/or does not occur on a regular basis. A formal agreement is normally not required.<sup>55</sup>

**Telecommunications** is any origination, transmission, emission, or reception of signals, writings, images, and sounds or intelligence of any nature, by wire, radio, television, optical or other electromagnetic systems.<sup>56</sup>

**Telework** is a formal work arrangement where job duties are performed at an Alternate Worksite for a material portion of the workweek on a regular and recurring basis, reducing or eliminating the employee's commute. A formal agreement must exist between employee and employer that details the terms and conditions of the arrangement. Teleworking as addressed in this document does not include Situational Telework or Mobile Working, and is synonymous with telecommuting.<sup>57</sup>

**Third-Party Provider** is a company or individual that supplies IT equipment, systems, or services to COV Agencies.<sup>58</sup>

**VPN** is a virtual private network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or remote users with secure access to their organization's network.<sup>59</sup>

---

<sup>50</sup> Troubleshooting User Experience over RDP by itopia. Retrieved March 17, 2021 from <https://helpcenter.itopia.com/en/articles/4055294-troubleshooting-user-experience-over-rdp#:~:text=The%20ideal%20latency%20for%20the,latency%20is%20more%20than%20150ms>.

<sup>51</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>52</sup> Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, July 2016. <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>

<sup>53</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>54</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>55</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>56</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>57</sup> Teleworking Guide to Best Practices – Council on Technology Services Mobile Workforce Workgroup March 2007.

<sup>58</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.

<sup>59</sup> Commonwealth of Virginia, Teleworking Guide to Best Practices, March 2007. By the Council on Technology Services (COTS) – Mobile Workforce Workgroup.