Best Network Practices to Support Work-From-Home Initiatives

Published 23 September 2020 - ID G00729822 - 10 min read
By Analysts Andrew Lerner, Neil Rickard, Mike Toussaint

Initiatives: Cloud and Edge Infrastructure

Many organizations intend to sustain large-scale remote work options in the wake of COVID-19. I&O leaders must employ the best networking practices outlined in this research to optimize user experience and improve security for remote workers.

Overview

Key Challenges

■ The COVID-19 pandemic created a sudden demand for organizations to support remote workers at an unprecedented scale, yet without adequate preparation and planning time.

■ Many enterprise networks were not optimized to accommodate the rapid scale in work-from-home (WFH) users, resulting in performance, security and/or cost inefficiencies.

■ Traditional network security and network monitoring solutions often fall short in addressing appropriate enterprise requirements for WFH users.

Recommendations

I&O leaders responsible for cloud and edge infrastructure must:

■ Fortify connectivity for WFH users by establishing a minimum standard for connectivity and funding employees’ connectivity.

■ Optimize availability, security and performance for WFH users by enabling split tunneling, offering backup and optimization options.

■ Improve visibility and user experience for WFH users by investing in cloud-based infrastructure services, such as unified communications as a service (UCaaS) and experience monitoring.

■ Bolster network security by evolving toward zero trust network access (ZTNA) principles.

Strategic Planning Assumption

By 2023, the number of workers who work remotely at least part-time will increase to 60%, up from 30% prepandemic.
Introduction

While many organizations have supported working from home for a decade or more, the COVID-19 pandemic has dramatically increased the number of personnel doing so, encompassing a far wider range of job roles than was previously the case (see Figure 1).

So far, much of the focus has been rapidly scaling to support users in an “all-hands-on-deck” and “just make it work” approach, given the priority and timeline. Thus, a huge focus has been on the secure connectivity aspect, including VPN and ZTNA. However, properly supporting a large remote workforce requires a proper network design that covers connectivity, infrastructure services (such as UC), monitoring and security.

Further, this is not just a temporary issue of coping during the pandemic, as Gartner predicts there will be a permanent increase in home working. Therefore, enterprises need to look beyond the tactical solutions that were deployed during the pandemic to longer-term solutions to successfully deliver networking for home working. This research provides best practices for improving network connectivity, user experience and security at scale to fulfill immediate user needs and develop a longer-term remote workforce strategy.

Figure 1: Percentage of Employees Working Remotely, Pre- and Post-Pandemic (Projected)

Fortify Connectivity for WFH Users

To optimize network performance, I&O leaders must set minimum network connectivity standards for remote work. This includes recommended standards for network performance, such as...
bandwidth upload and download speeds. For example:

- Minimum download speed: 100 Mbps
- Minimum upload speed: 10 Mbps
- Average latency: Not more than 100 ms round trip to key real-time communications POPs
- Average latency: Not more than 200 ms round trip to other application locations

These guidelines may vary based on apps being run and what network services/providers are locally available. This is not to say that not achieving the above equates to poor performance, and it is important to note that the service levels above will not be available to some rural employees. However, the likelihood of issues due to the network dramatically increases if the above factors are not met.

Further, to increase the likelihood of adherence to these minimum standards, organizations should negotiate blanket service offerings and prices that cover substantial percentages of their user base. Discounts from bulk negotiating for enterprises usually results in per-user savings of 25% to 50% versus what individual employees would be able to negotiate on their own.

To further ensure appropriate network performance at home, I&O should fund and/or reimburse home internet broadband costs, where appropriate, to better guarantee network access, which may require co-funding through internal partnerships with finance or facilities. While this may seem odd for enterprises that have not instituted this previously, it is very similar in principle to issuing a mobile phone or a laptop and should be considered part of a WFH package.

The cost to the enterprise varies widely per geography and availability of services but generally is within the $40 to $150 per-month per-user range and usually in the $60 to $90 range. While this may seem high (for example 1,000 users would equate to $1.2M per year), it can be fully or partially offset by the reduction of costs for facilities, including real estate and security.

Optimize Availability and Performance for WFH Users

**Split Tunnel**

Wherever possible, I&O leaders should reduce the backhaul of traffic to networking infrastructure by enabling split tunneling (see Designing Security for Remote-Work-First Enterprises). The benefits of split tunneling include:

- Avoiding the added latency caused by backhauling all traffic to the corporate network.
- Providing better performance for remote workers accessing globally distributed cloud services.
- Reducing bandwidth requirements for traffic redirected through the corporate network’s security stack.
However, the risks of split tunneling include:

- Internet traffic does not pass through the corporate security stack. This could potentially allow malicious traffic to the device. This risk can be mitigated through the use of a cloud-based secure web gateway (SWG), such as Zscaler.

- IP-based split-tunnel deployments can be cumbersome for networks with overlapping or noncontiguous IP ranges/subnets.

We believe the benefits of split tunneling outweigh the risks for most organizations. However, split tunneling may not be suitable for organizations that operate within strictly regulated industries or environments (see A Comparison of Remote Network Access Products for Enterprise Endpoints for more information regarding split tunneling).

Use CDN to Improve Web and Video Performance

CDNs have traditionally been used to primarily support customer-facing applications. In the same manner, CDNs can also improve performance for WFH users. CDN providers deliver optimization and security for web applications and video streams (see Market Guide for Global CDN).

Improve Network Uptime at Home

In some instances, the availability of home broadband services will not suffice for enterprise employees. Uptime for broadband/consumer-grade services is generally in the 99% range, with time to repair for outages often measured in multiple business days, while enterprise-grade SLAs in office locations are often an order of magnitude better. For employees that require higher availability, cellular backup is recommended. Cellular backup can be built into the user's home router or dispatched to users in the event of outages. If this is not being used for always-on connectivity, the price is typically reasonable.

Fill Connectivity Shortcomings With Client-Based Network Optimization

In a relatively small percentage of the time (we estimate less than 25% of WFH users), application performance will not suffice even if minimum network standards are met. Or in some instances, broadband services will not be available that meet minimum standards. In these instances, I&O leaders can use client-based network optimization tools (such as software agents installed on devices) to help address remaining gaps in network connectivity. For example, Replify and Riverbed offer client-based optimization products, and we expect additional SD-WAN vendors to release products in this area throughout 2020.

Selectively Deploy SD-WAN Edge Devices to Home-Based Users

In some cases, it may be appropriate to deploy small SD-WAN appliances to users' home locations, typically offering Wi-Fi connections. Although these represent a significant additional cost that can be several times higher than the hardware/software cost of typical consumer-grade equipment, they can deliver enhanced resilience, improved visibility and troubleshooting. They also allow the
secure connection of corporate devices that might not easily be able to support the full remote working security stack. Some examples where this makes sense include remote contact center agents, emergency response dispatchers, job roles where financial transactions are occurring, such as traders and senior executives, and roles where poor performance can have a direct impact on the business.

**Invest in Cloud-Based Infrastructure Services**

We recommend that I&O leaders deliver several infrastructure services to WFH via cloud-based as-a-service platforms, rather than building out these services (and backhauling traffic) via centralized data centers. Based on inquiry and our analysis, most global infrastructure providers that deliver via an as-a-service model provide better performance versus the alternative of backhauling centrally. This is in large part due to their scale and commercial interest in improving the end-user experience via building out robust POP infrastructures and/or applying multiple network optimizations, including network protocols, CDN and DNS. In addition to augmenting performance, these as-a-service offerings scale far more readily than most enterprise on-premises solutions. I&O networking leaders will have direct and indirect influence over these decisions. Specific services we recommend deploying via public as-a-service offerings in a WFH scenario include DEM tools, UCaaS and file sharing.

**Digital Experience Monitoring**

Most enterprises already have tools in place to support end users working from corporate-owned locations. However, we find that the level of monitoring for WFH users is years behind users in corporate locations. Thus, in order to provide the appropriate end-user experience, I&O leaders must invest in monitoring tools that can predict and detect issues that impact users, specifically digital experience monitoring (DEM) tools. These end-user monitoring tools enable consistent application experience and proactive troubleshooting capabilities (see Market Guide for Digital Experience Monitoring).

**Unified Communications**

In conjunction with split tunneling, we believe that unified communications will deliver better experience for WFH users compared to when deployed as a service, versus backhauling traffic compared to UC deployed in corporate data centers (see Magic Quadrant for Unified Communications as a Service, Worldwide). This is based on user inquiry and the fact that UCaaS providers often have optimized several networking characteristics of their service to support a globally distributed installed base, while central UC solutions are often designed to support corporate locations. Thus, latency and underlying protocol enhancements are improved when using UCaaS, compared to traditional UC. Lack of voice redundancy and failover for remote users can be mitigated by utilizing the end user’s mobile phone number in case the broadband circuit fails or performance falls out of spec.

**File Sharing and Backup**
Similarly, we recommend I&O leaders prefer cloud-based file-sharing services such as Box and Google Drive versus backhauling file-sharing services centrally (see Market Guide for Content Collaboration Tools). This is for the same reason as UCaaS, in that cloud-based file-sharing providers have typically enhanced network designs to mitigate latency and enhance protocols that improve application performance.

**Broader Application Movement**

In addition to infrastructure services, SaaS-based applications can offer better performance for WFH users as well. Gartner refers to this as the “new work nucleus,” and it was essential to effective home work during the early stages of the COVID-19 pandemic (see Workforce Resilience in the Eye of the Pandemic: Overcoming the Current Remote Work Situation While Planning for the Future).

While I&O networking leaders often don’t have final say in the application selection or deployment, they should inform appropriate app and business leaders to prefer SaaS applications to reduce latency for WFH users. Similarly, as organizations refresh applications that are used by remote workers, I&O leaders should prioritize opportunities to migrate these applications to SaaS or public cloud platforms.

**Evolve Security Toward ZTNA**

Zero trust network access (ZTNA) is defined as products and services that create an identity- and context-based, logical-access boundary encompassing a user and an application or set of applications. ZTNA delivers VPN as a service (cloud-delivered) while offering additional functionality such as application discovery. Therefore, ZTNA improves the flexibility, agility and scalability of remote access and is often delivered via consumption-based pricing, for a few dollars per user per month. In addition, some ZTNA providers offer new features such as automated application discovery.

We recommend that enterprises phase out legacy “full-tunnel” VPN implementations for users who don’t need full network access and begin phasing in ZTNA principles. Also, we recommend using ZTNA, if traditional VPN solutions are experiencing limitations in capacity or bandwidth limitations because of an expanded remote workforce. There are many viable ZTNA offerings on the market today, with additional ones emerging (see Market Guide for Zero Trust Network Access). Some offer a combined ZTNA plus SWG product, important for organizations looking to deploy both technologies while preferring fewer vendors and fewer additional management consoles. Refer to Designing Security for Remote-Work-First Enterprises for an in-depth comprehensive analysis on this topic.

**Evidence**

Gartner client inquiry, which includes:

- More than 5,000 client interactions regarding networking from June 2019 through June 2020
More than 850 client interactions regarding network security from June 2019 through June 2020

More than 20,000 interactions regarding COVID-19 since February 2020

Recommended by the Authors

9 Predictions for the Post-COVID Future of Work
A Comparison of Remote Network Access Products for Enterprise Endpoints
Magic Quadrant for Unified Communications as a Service, Worldwide
Networking Best Practices for Microsoft Teams
Market Guide for Digital Experience Monitoring
Tool: Prepare I&O for the Everywhere Enterprise
Solving the Challenges of Modern Remote Access
Market Guide for Zero Trust Network Access

Recommended For You

Summary Translation: Building Organizational Resilience Is a Strategic Imperative
Summary Translation: 4 Essential Definitions to Create Effective Digital Business Strategies
ERP Primer for 2020
Compliance Reviews
Third-Party Supplier Risk Governance

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."