Enabling Your At-Home Workforce: **Three Tips for Successful Collaboration**

Business leaders are looking for ways to ensure their at-home workers can be as productive as those in the corporate headquarters or a remote office. Tools, such as Office 365, Microsoft Teams, Zoom, and others, are designed for just that purpose.

But employee collaboration and productivity take a hit when Zoom calls drop or when Office 365 documents take forever to load, and employee frustration rises. Organizations must ensure that their at-home employees can be as productive as possible while using these bandwidth-intensive tools.

To quickly enable an efficient and productive at-home workforce, organizations must:

- Provide secure connectivity
- Enable a fast user experience at scale
- Ensure ease of deployment

Let's take a closer look at each.

Tip 1 Provide secure connectivity

Having your entire workforce suddenly working from home and accessing their work applications can easily overload legacy hardware-based infrastructures. Employees accessing their work apps via VPN have to deal with latency, sluggish performance, and dropped connections. Ultimately, users will ignore the VPN and go directly to the internet. Can your legacy infrastructure secure these direct connections?

The Challenge

Traditional solutions (non-cloud-native firewall solutions) still expose the home gateway router IP address to the internet, increasing the potential attack surface. In addition, collaboration apps often use a control or signaling channel as well as an audio or video stream, which is spread across different ports and protocols. This leads to challenges in incident management and troubleshooting.

What Zscaler Recommends

A proxy-based firewall architecture shields IP addresses from exposure to the internet. This, coupled with running all of your traffic, including traffic for remote and at-home workers, through a comprehensive cloud-based security stack protects users from phishing and ransomware attacks. Sending all traffic to Zscaler™ also enables you to deliver consistent policies to all users, no matter where they connect. That means, you can easily apply the corporate security posture to home users. And having all the traffic coming to the same platform improves the ability for organizations to correlate data, and quickly address and remediate incidents.

> Routing all traffic through Zscaler Internet Access™ enables you to apply the corporate security posture to at-home and remote workers, wherever they connect.

Tip 2 Enable a fast user experience at scale

Collaboration tools, such as Office 365, Microsoft Teams, and Zoom, work best when employees can use them as quickly and efficiently at home as they do in the office. That requires fast, reliable connections delivered by a scalable architecture that accommodates spikes in bandwidth and traffic demands without any impact to performance.

The Challenge

Cloud collaboration applications demand significant and unpredictable bandwidth. Leveraging public cloud provider connectivity often means there is no special uplink connectivity or peering with vendors, which leaves business-critical traffic, such as Office 365, to suffer the same latency and bottlenecks as YouTube and Facebook traffic. Traditional solutions and virtualized appliance stacks are not architected to absorb these fluctuations and spikes in demand. As a result, as your bandwidth consumption grows, so does user frustration and your bandwidth costs.

It is also important to consider that sending traffic to corporate data centers to be secured, then routing it to the internet and SaaS applications, and then back again to the user, is far from efficient. It creates inconsistency and a poor user experience due to traffic hairpinning.

What Zscaler Recommends

It is essential to have a good strategy to connect users working from home to Office 365, Microsoft Teams, Zoom, and other Unified Communications as a Service (UCaaS) apps. Direct peering with Microsoft and an architecture built on the secure access service edge (SASE) framework, which provides connectivity to all UCaaS providers at all major internet exchanges, provide optimal connectivity to applications. The result is a fast user experience regardless of bandwidth demands.

The Zscaler SASE architecture scales elastically to handle any number of users, including all their voice and video-sharing and SSL-encrypted traffic, with no capacity limitations. Routing all of your traffic to Zscaler avoids hairpins and provides the fastest path to Microsoft and other collaboration applications. Zscaler Internet Access with Zscaler Cloud Firewall provides full security and access control across all users, devices, and locations, and enables you to confidently embrace Office 365, Teams, Zoom, and other low-latency collaboration tools.

Tip 3 Ensure ease of deployment

If a remote workforce solutions is complex to install, configure, and manage, any value provided by that platform will go to waste. Organizations need to quickly and seamlessly enable employees to work from home, the office, or from wherever they connect.

The Challenge

With traditional solutions, deploying policies to new remote users can be complex. Often, support of at-home users requires IT to spin up new VM instances, which slows deployment and adds to an already complex policy infrastructure.

What Zscaler Recommends

Zscaler is a 100 percent cloud service that's fast and easy to deploy because there's no need to install, configure, or manage appliances. With Zscaler, you can easily leverage one single policy configuration for all users across the globe. You simply:

- Push Zscaler Client Connector (formerly Zscaler App) to all users via a Group Policy Object (GPO) or via mobile device management/enterprise mobility management.
- Deploy policies across all users everywhere with one click.
- Make security and firewall policy changes by logging in to the admin portal and, within seconds, your changes are enforced worldwide.

> With Client Connector for the endpoint, organizations can easily enable fast, secure connectivity to collaboration platforms, while ensuring policy is always consistent, regardless of location or connection.

Ready for the new normal

The business landscape has changed. Organizations must provide their at-home workforce with rapid access to their work applications. This can't be done with a VPN or legacy network and security infrastructures. Organizations need a cloud-based platform to protect employees, reduce risk, and secure all traffic.

Learn how the Zscaler Cloud Security Platform delivers fast, secure remote access for an at-home workforce that also helps organizations protect their employees and maintain business continuity.

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com