Headquartered @ Home – Convenience Paradise or Security Hell?

COVID-19 Pandemic Triggered a Pivot That Comes *with its Own Pros & Cons*

The month of Feb 2020 would be remembered in world's history as a watershed period. Towards the end of this eventful month, the novel corona virus and the disease it brings along – covid-19 caused the world to almost 'shut down'. As of April 2020, there is no end in sight for this extra ordinary global disruption of unprecedented nature.

> The world headquartered at its homes en masse leaving the IT departments scrambled for reactionary measures.

Thanks to our global fast and reliable telecommunication and data networks – both private networks and public Internet – there was a quick and massive transition of most of the digital work from commercial office spaces to peoples living rooms and bedrooms.

There were no marshal orders for this change to take place. It was as natural as breathing. People just switched to work from home when their movements were restricted.

Internet-device search engine Shodan has a recent report that says VPN use is up 33% while Remote Desktop Protocol (RDP) use is up 41% over the period.

The CIOs were used to of a certain population of staff doing work from home or working while travelling. The world headquartered at its homes en masse leaving the IT departments scrambled for reactionary measures.

WFH brings in lots of security issues that need to be addressed now. Even when the pandemic is hopefully over, there will be valuable lessons to be learned and remembered.

Train, Empower and Audit Users & Their Security

Business users must be essentially trained for information security basics. This is not optional anymore. This concise 1 hour online free tutorial at Udemy can be a good starting point for this action item.

Review & Audit Credentials Credibility for your business users if this has not yet been automated via strong identity management at the organization level. For smaller businesses that do not have directory services, consider Jump Cloud services that let you build a strong directly for users, devices, networks and cloud resources without the need for any infrastructure at the organization data center. Jump Cloud is locally available in Pakistan via authorized business partners.

Encourage your staff to invest in their network infrastructure and bandwidth at home. The costs saving achieved due to restrictions on physical movements can be diverted towards enhancing the network hardware and bandwidth at home for smooth WFH experience. The users or the organization can share any additional costs alone or jointly.

Some Immediate Actions at the HQ

Ensure your organization has an on-prem or cloud-based VPN gateway that your WFH users can use to connect to corporate resources. VPN-free access is already a no-no in corporate networks but urgency and convenience often conspire together and the one-off exceptions start kicking in. Sometimes it is a senior leadership team member who needs to access something, sometimes it's a project or a customer who demands something at the eleventh hour and environments with slack implementation of policy and governance often fall for the trap.

A recent Internet connectivity bug announced by Microsoft affects PCs and servers running all supported versions of Windows 10 devices that are using a proxy, especially with a virtual private network (VPN). Install update suggested by Microsoft from here.

Zoom's UNC Chat Links Problem: Anyone who has not heard about Zoom has by now known it very well. The popular video conferencing application has come in handy during the lockdowns around the world. And with this surge, came the security risks. The group chat feature lets users send messages to other participants in a meeting and converts URLs into hyperlinks for the recipient to direct them to webpages. Zoom client not only converts normal URLs into a clickable link but also Windows networking Universal Naming Convention (UNC) paths. The UNC paths could be that of an attacker computer containing harmful executable code that users could click inadvertently. While Zoom works to fix this UNC path links problem, Microsoft has advised network administrators to restrict outgoing NTLM traffic to remote servers.

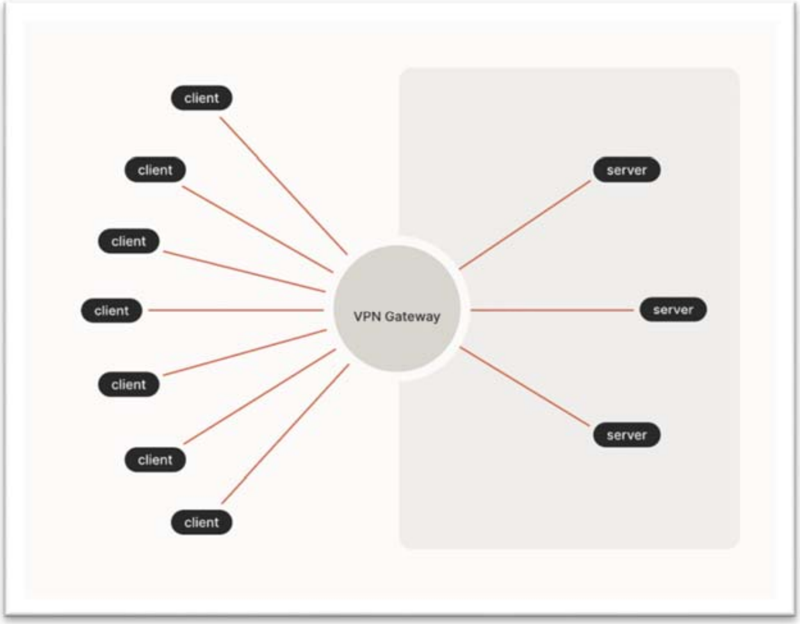
While Zoom works to fix this UNC path links problem, Microsoft has advised network administrators to restrict outgoing NTLM traffic to remote servers.

Ensure volume snapshots backups of critical machines are kept off-site and are taken under a well-defined and well-structured backup life-cycle plan.

Security & Access Considerations

Modern IT infrastructure is typically a hybrid of on-prem and cloud resources that users access frequently for all their digital work. Accessing these digital assets should always be via modern VPN that is both secure and efficient. VPN gateways come in both hardware and software versions. See Figure 1.1

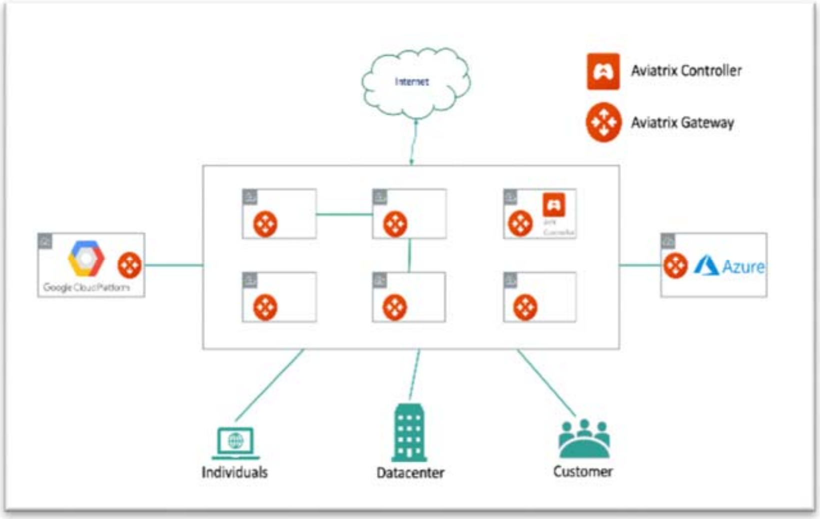
Figure 1.1



More recently, VPN gateways are being provisioned right in the cloud with interesting new capabilities and ease of provisioning. These VPN gateways – such as those bring provided by Aviatrix and SDN solutions – such as that provided by tailscale are redefining how enterprise handle VPNs and remote users engaged in serious and continuous WFH.

Aviatrix solutions come as an AWS or Azure image that could be deployed in the respective cloud in minutes and connects with the enterprise resources present in the VPC (AWS) or VNet (Azure). See figure 1.2.

Figure 1.2



Tailscale solutions provides the ease of access that is typical of VPNs but optimize it using control and data planes separations that result in optimized performance and consistent user experience.

Consider Upgrading to Zero Trust Security Architecture

The perimeter-centric security model is now clearly showing its limitations with its binary assumption that all insiders are good and that all outsiders are to be challenged before being trusted. With so many WFH users, consider the better Zero Trust Architecture for your Information Security needs.

Instead of assuming everything behind the firewall isn't a threat, the Zero Trust security model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust follows the “never trust, always verify" approach.