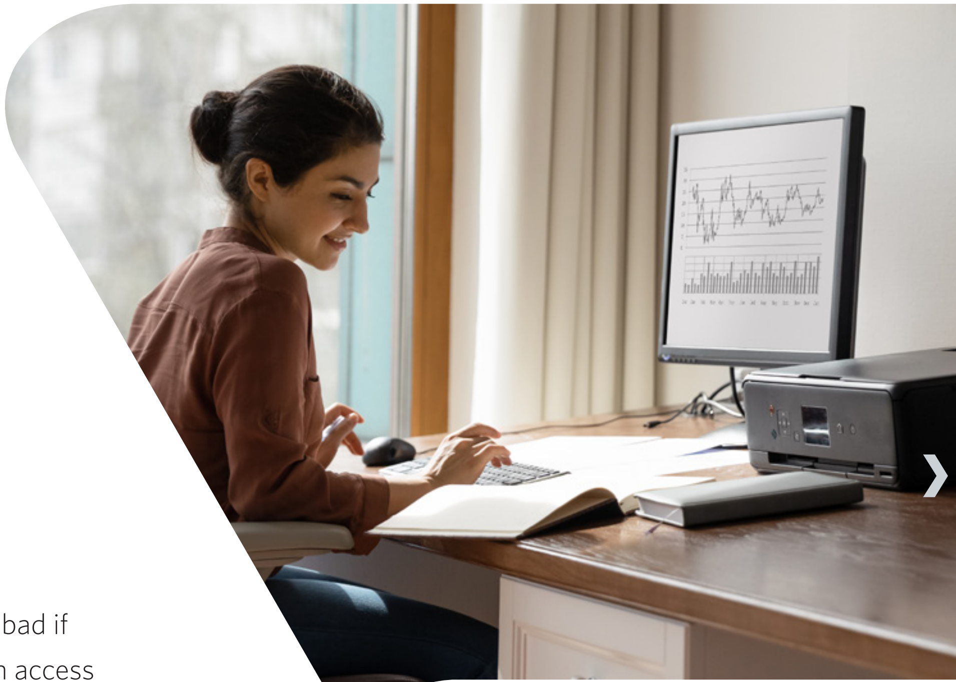
VERSA
NETWORKS

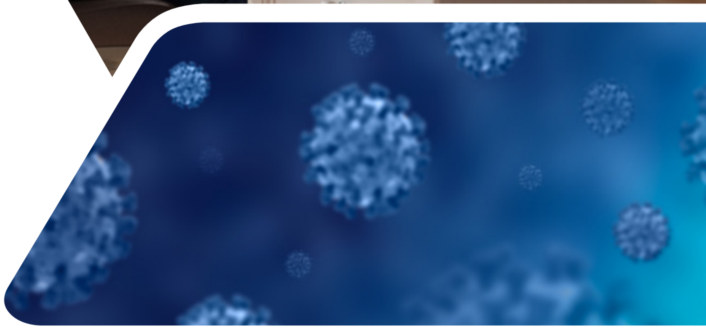
Simple Do's and Don'ts to consider when transitioning from a legacy VPN solution to a remote ZTNA solution

❯

COVID-19 ushered in a new era of work. Companies shut down their physical offices and sent people home to work. Companies were forced into an untenable position: either use a legacy remote access VPN solution or limit the access necessary to accommodate their workforce. During this period, longstanding flaws with legacy VPNs were exacerbated:

- Legacy VPNs grant virtually unrestricted network access. This inherently does little to prevent lateral movement throughout the private network.
- It provides very poor visibility. Its logs normally show what resources/IP addresses were accessed within the network and not what applications or data was accessed.
- It assumes that once a user or device is connected to the corporate network, they can be trusted without continuously being monitored. This is especially bad if a threat actor was to break the simplistic authentication mechanism and gain access to the network.





This issue initiated the rapid adoption of global Zero Trust Network Access (ZTNA) solutions – and continues today as the workforce becomes increasingly hybrid. Adopting a ZTNA solution doesn't come without risks. If the adoption isn't well planned, it exposes both user experience and security gaps.

This guide provides notables items to consider when transitioning from a legacy VPN solution to a remote ZTNA solution:

Do's

1. Start with Assessing Your Requirements

Evaluate your organization's remote access requirements. This includes user locations, device types, applications, and overall security needs. Understand which applications and services need to be accessed remotely and define access policies accordingly.

2. Carefully Plan the Transition

Develop a well-defined migration plan that outlines the necessary steps and timeline for the transition. Consider factors that include communications to and training for the user community, potential infrastructure changes, and pilot testing.

3. Pilot Test the Solution

Conduct pilot testing with a small group of users before deploying ZTNA on a large scale. This allows you to gather feedback, identify issues, and make necessary adjustments before implementing ZTNA across the organization.

4. Consider the Security Needs of The Business

Ensure that the ZTNA solution you choose provides robust security features. Look for features such as multi-factor authentication, device posture assessment, encryption, and granular access controls based on user identity and context.

5. Train the Users

Educate your users about the benefits and usage of ZTNA. Provide training on how to turn the solution on if it is not enabled by default and access applications and/or services using the new access method. Address any concerns or questions they may have during the transition.

6. Monitor Everything and Optimize

Continuously monitor the performance and effectiveness of your ZTNA implementation. Collect metrics, analyze data, and adjust as needed to optimize the solution and align it with evolving security requirements.

Don'ts

As with the Dos there is always a list of Don'ts that complement them. These are the most common things an organization shouldn't do when transitioning from a legacy VPN solution to a remote ZTNA solution:

1. Overlook Compatibility

Ensure that the ZTNA solution that is chosen is compatible with your existing infrastructure and applications. Always consider the integration requirements and potential challenges during the migration process.

2. Rush the Transition

Take the proper time to plan and execute the transition carefully. Rushing the process will lead to errors, user dissatisfaction, or security vulnerabilities. Follow the migration plan and address any issues that arise before proceeding.

3. Don't Neglect the User Experience

Ensure that accessing applications and services through ZTNA is seamless and intuitive for users. If it isn't users will reject the solution and try to find workarounds so that they do not have to use the ZTNA solution. Also minimize disruptions and provide necessary support during the transition period.

4. Forget to Decommission VPN!!!!!

Once you have successfully migrated to the ZTNA solution and ensured that all users and applications are functioning well, remember to decommission your VPN infrastructure. Properly decommissioning VPN helps reduce unnecessary complexity and unintended security risks.

The specifics of your migration will vary depending on your organization's needs along with the chosen ZTNA solution. For custom and expert guidance on your transition plan, please visit https://versa-networks.com or contact Versa at https://versa-networks/contact.

Do you need help with your VPN replacement or ZTNA deployment?

Request a free 30 mins consultation

❮

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com