Date: 8/2022
Project: Blog Post
Client: VTS
Writer: Debby Wadsworth, Freelancer
SME: Dylan Kerling, VTS Technician
TOPIC: The Role of VPN

Debby Wadsworth
Writer & Consultant
DW-writer.com
debby@DW-writer.com
cell 763-350-8506

The Role of VPN

A Virtual Private Network (VPN) is a basic and effective way to securely connect remote users to a company's internal network. It gives remote employees access to internal applications and data, or to create a single shared network between multiple office locations. It achieves the goal of preventing proprietary data from being exposed on the open Internet.

There are different types of VPNs used by business like Remote Access, and Site-to-Site. Remote Access VPNs use up-to-date cryptographic protocols that can effectively encrypt traffic between remote employees or teams and their company’s internal network. They are less expensive and easier to manage as compared to legacy solutions like buying a secure ‘leased line’ from an ISP or a manually ‘allowlisting’ individual IP addresses that belong to remote workers.

Site-to-Site VPNs are used to create a connection between multiple networks. They facilitate prioritizing private, protected traffic and are particularly helpful for organizations with more than one office spread out over large geographical locations. Plus, you can

use a server as an operational hub of an application essential to the company's business. However, they lack integrated security and can limit scalability.

Both types of VPNs have limitations that include security risks, latency penalties, Cloud and hybrid cloud complexities, more costs, and require a lot of IT time.

- **Security Risks:** If an attacker gains access to a remote employee's VPN credentials, that attacker will be able to access all applications and data on the corresponding network.
- **Latency Penalties:** If a company uses a cloud-based VPN, their NAS exists in a data center in a different physical location from the company's internal network. This extra step adds latency to every single request between employees and the network.
- **Cloud and Hybrid Cloud Complexities:** Many business applications are hosted in the cloud instead of on a business's internal network, making them incompatible with VPNs. Those applications typically use their own security tools to ensure secure access. But IT teams cannot fully control those tools and might struggle to understand who exactly is accessing these applications — both critical security factors.
- **More Costs:** If a company uses an on-premises NAS to connect with its employees' VPN clients, the company must regularly replace that hardware to ensure it is able to withstand the latest cyber threats. A similar situation arises if employee VPN usage outstrips the NAS's capacity to handle traffic. The company must replace that NAS, or it could become overloaded and crash.
- **Lots of IT Time**: VPNs require a lot of effort to maintain, especially if a business uses more than one VPN to provide different varieties of access to different types of employees. For example, IT teams must install the right VPN client on every remote employee's computer, and ensure employees are keeping that software up-to-date.

For more information about VPNs visit www.vts.com.