Regional Insurance Group VPN Deployment

VPN Recommendation

For Regional Insurance Group, an SSL/TLS VPN is the most appropriate option for a remote access solution. An SSL/TLS VPN uses web browsers to operate and uses Transport Layer Security to encrypt the communication between remote and internal users. This makes it suitable for a worskforce that is distributed, like workers are at home, and for anyone using personal devices and home networks.

Compared to IPSec VPN's, SSL/TLS provide ease of use, firewall compatibility, granular access control and scalability. No VPN client is needed, users can connect using a web browser. When it comes to firewall compatibility SSL/TLS use HTTPS which is rarely blocked. Granular access control allows administrators to allow access to specific segments of the network, and certai applications rather than full network access. Finally, SSL/TLS VPNs leave room for growth in the company and do not pose a long term scalability problem.

TLS protocol combines both symmetric and asymmetric encryption types to ensure both confidentiality and integrity for all data being transported. This provides a safe connection, key exchange and bulk data transfer.

SSL/TLS VPN inherently encapsulates traffic securely without requiring tunnel configuartio complezit, making it more suitable for end users.

To strengthen remote access security, multifactor authentication, Zero trust network access, and endpoint security controls should be implemented. MFA will prevent the misuse of credentials, ZTNA will block everyone and everything until the user can prove they are allowed into the network. Devices should also be checked for compliance which includes antivirus, and patching. Unsafe devices can pose a risk to the network.

Additional Remote Access Options

While a SSL/TLS VPN can serve as Regional Insurance Group's primary remote access solution, additional complementary systems can and should also be in place to strengthen security, increase usability and align with best practices for an always available remote network.

RDP, or Remote desktop protocol is a very popular option. It is built in to all windows machines and lets users access their desktop from another device. This option does require specific configuration and security measures in order to alleviate any potential threats. This would not be recommended for all of the remote workers due to the configuration and security concerns, but it is a great backup option.

There are also several remote access softwares available including one from chrome. Again this provides a lightweight, semi-secure option but should not be the first option to use. Using outside software introduces the chance that the connection could be interrupted, or compromised by any bugs, or security issues with the software. This can be a short term solution if absolutely necessary but should not be used for the day to day operations of a remote worker. What this would be great for is temporary connections that the IT team may need to make, but the Remote Desktop protocol built in to windows would even be a better option.

Resources

7 types of remote access and how to pick the right one. RemoteToPC. (2025, December 16). https://remotetopc.com/types-of-remote-access/

SSL VPN vs. IPSec: What are the differences?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/ipsec-vs-ssl-vpn

Symmetric encryption vs asymmetric encryption: How it works and why it's used. Device Authority. (2024, November 29). https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/