Cherylmc, M. (2022). *About azure VPN gateway*. About Azure VPN Gateway | Microsoft Learn. Retrieved December 27, 2022, from https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

With the company being pleased with my plans for implementing Microsoft Azure into their system to limit access to only authorize agents in the company. They now want me to come up with a plan for securely transmitting data created by cloud-based instances of the application back inside the corporate firewall. Specifically, they want to know how they can leverage VPN technologies to accomplish this. For this project we will be using Azure VPN gateway which is a part of the original cloud provider Microsoft Azure. With Azure VPN Gateway being different from the main cloud service provider it would be best for the company to first understand how it works, how to implement it to allow the company to securely transmit data, and what are the next steps to keep moving forward.

Before being able to implement the Azure VPN Gateway its best to understand; what is a VPN Gateway? While reading the article “Cheryl Mc, M. (2022). *About azure VPN gateway*. About Azure VPN Gateway | Microsoft Learn. Retrieved December 27, 2022, from https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways”
It gives a very detailed explanation about VPN Gateways ``A VPN gateway is a type of virtual network gateway. A virtual network gateway is composed of two or more Azure-managed VMs that are automatically configured and deployed to a specific subnet you create called the *gateway subnet*. The gateway VMs contain routing tables and run specific gateway services.” By having the knowledge of what a VPN Gateway is, the consumer / the company is able to understand more of what they are investing their money into. One way to put it is that the more knowledge the consumer gets it's like getting closer to the center of a tootsie pop. With VPN Gateways there are two different types: one VPN gateway and one ExpressRoute gateway. The gateway type 'Vpn' specifies that the type of virtual network gateway created is a VPN gateway. This distinguishes it from an ExpressRoute gateway, which uses a different gateway type. There are subtle differences but it can change how the system would perform.

With now having the knowledge of what is a VPN Gateway, we need to know how its implemented using Azure VPN Gateway. According to the article “Cherylmc, M. (2022). *About azure VPN gateway*. About Azure VPN Gateway | Microsoft Learn. Retrieved December 27, 2022, from
https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways”
It states in its introduction paragraph that “ Azure VPN Gateway is a service that uses a specific type of virtual network gateway to send encrypted traffic between an Azure virtual network and on-premises locations over the public Internet. You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. Multiple connections can be created to the same VPN gateway. When you create multiple connections, all VPN tunnels share the available gateway bandwidth.” By picking apart from this piece of text we are given that Azure VPN Gateway has a specific type of virtual network gateway to send encrypted traffic. For the consumer this is great news that Azure VPN Gateway is able to securely send encrypted traffic which is able to solve our concerns about sending data.

The next sentence tells us “You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.” This solves the consumers' other concern of securely transmitting data created by cloud-based instances of the application back inside the corporate firewall. This shows that even inside of the network it is encrypted which helps the company a lot.

With connecting to the VPN Gateway there are 2 different ways of configuring your connection: site-to-site, point-to-site. “A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.S2S connections can be used for cross-premises and hybrid configurations. A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it.” While “A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.” i found both of these definitions that give good examples of what situation would be best used in depending on how many clients a consumer needs on the article “Cherylmc, M. (2022). *About azure VPN gateway*. About Azure VPN Gateway | Microsoft Learn. Retrieved December 27, 2022, from https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways “
With an insurance company receiving a lot of traffic and it being domestic to one area the best solution would be S2S or site-to-site. According to what is stated earlier P2S is more for connecting to a service at home and only using a few clients while a S2S is best for staying at 1 location because the VPN device is located on premise.and for each office they have they can setup a VPN device because from what i'm assuming is that they don't work from home.