



Geneko Remote Access Solutions

Document Version: 1.0.0
Date: April 24, 2020

Introduction

In a situation caused by extraordinary circumstances, it is necessary to ensure continuity of business and provision of services. In such situation, when employees usually are not able to reach their office, it is very important to provide them safe and efficient way to work remotely from home and access company resources.

If the situation calls for a quick response, the most appropriate are the technical solutions that employees can easily apply without any prior knowledge of information technology.

Geneko solutions

Geneko is able to quickly and efficiently meet the requirements for establishing remote access to IT resources. This is possible by using the GWG 3G / 4G Gateway series of devices. The devices are equipped with cellular 3G or 4G interfaces which means not only remote access to company resources from fixed remote location but also mobility - the employee is not bound to one location, but can be in any remote location and work on the move is possible.

Practical implementation

Each remote location or employee should have a single 3G GWG or 4G GWG device equipped with internet SIM card. Data Internet SIM cards are publicly available at kiosks and can be recharged in the usual way for prepaid recharge. Alternatively, choose the appropriate postpaid mobile net package.

Every GWG device on remote location is already configured and ready for communication as follows:

- mobile connection parameters are set so that the device automatically connects to the Internet
- the VPN tunnel parameters are tuned to the company central location and the VPN tunnel is automatically established
- DHCP server is set up over the LAN port so that the employee's computer automatically receives network settings
- routing is set up - this means that only traffic intended for communication with company resources will go through the encrypted tunnel while usual Internet traffic will go out of the tunnel to the public Internet without encryption (*split tunneling*)
- the device has all the necessary digital certificates for authentication and encryption of data as well as automatic time update

Based on the above, employee has only to plug the device into a power supply and connect his computer with a network cable to the Ethernet port of the GWG device. The computer only needs to set the network settings to automatic, and it will be possible to access all IP subnets that are in the company network, and in parallel to be able to access the Internet. All additional company IP subnets can be configured on central location by network administrator.

In practical implementation, there are two options that differ primarily in the central location:

Option 1: Tunnel termination on a company firewall or central router

In this case, one side of the VPN tunnel is on the GWG Gateway, and the other terminates on the company firewall or central router. Routing itself to internal company networks is performed by a firewall or central router. It is important here to properly map the facilities in a central location so that they can serve the required number of employees.

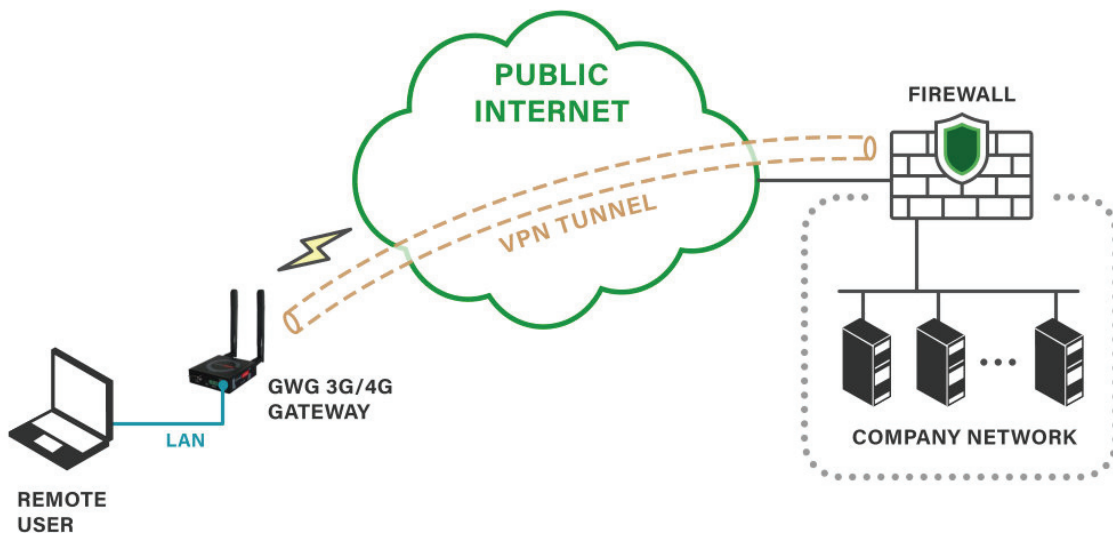


Figure 1: Option 1 – terminantion on a firewall

Option 2: Tunnel termination on a VPN server

In this case, everything is the same on the employee's device. However, in this option the tunnel is terminated on a VPN server located on the company's internal network, most often in the DMZ. The GWG device connects to the public IP address of a company firewall that performs port forwarding to a VPN server. VPN server capacities should be taken into account here.

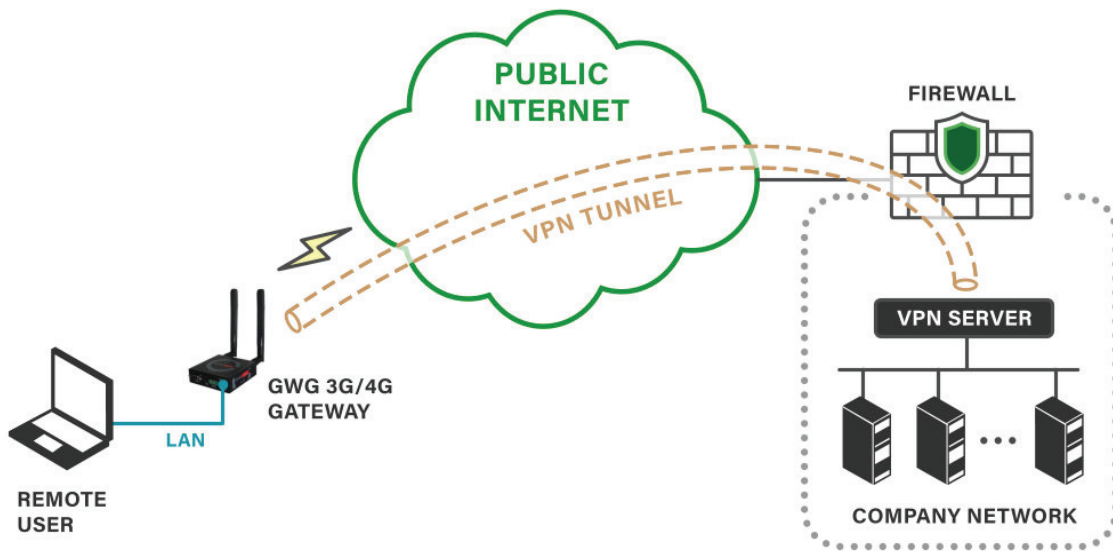


Figure 2: Option 2 – termination on a VPN server

Solution with Geneko devices at both ends

This solution is for specific purposes when you need to connect a pair of locations, for example, one has a monitoring computer and another has equipment or a computer network. The solution is more limited than the previous two because both devices must be equipped with SIM cards that are “visible” to each other; therefore, they have to be in same private APN.

For this solution, ordinary internet SIM cards cannot be used. Instead, SIM cards in same private APN have to be used. A VPN tunnel establishes between two GWGs. This solution is suitable for monitoring equipment in remote locations such as wind turbines, pumping stations, oil pipelines, etc.

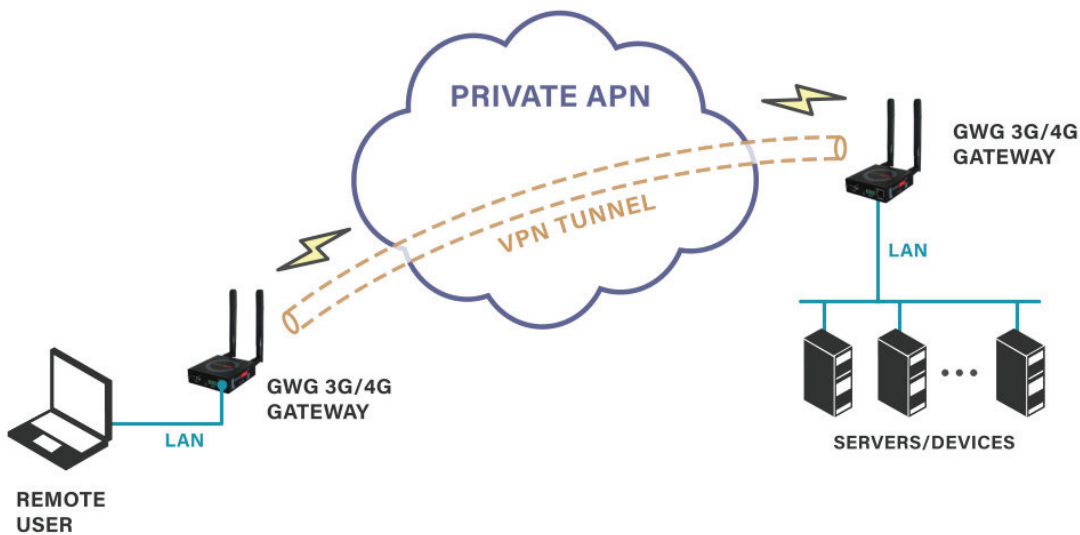


Figure 3: Geneko GWG devices at both ends

GENEKO

Bul. Despota Stefana 59a
11000 Belgrade ▪ Serbia

Phone: +381 11 3340-591, 3340-178

Fax: +381 11 3224-437

e-mail: gwrsupport@geneko.rs

www.geneko.rs