Economy Transdisciplinarity Cognition www.ugb.ro/etc	Vol. 23, Issue 1/2020	78-85

Teleworking and Securing Data with VPN Technology

Radu-Cristian BUCȘĂ
George Bacovia University, Bacău, ROMANIA
radu.bucsa@ugb.ro

Abstract: *In the current pandemic context, more and more activities are moving in the online environment in order to respect the social distance. Most of us have never thought of cyber security risks generated by teleworking activities. In this paper I would like to present a handy solution to avoid these cyber security risks, repetitively using VPN solutions. Virtual Private Network is a solution that uses encrypted internet infrastructure for remote connection to the company / institution server.*

Keywords: *cyber security, teleworking, virtual private network*

Introduction

The COVID-19 pandemic has globally imposed a number of restrictions on population interaction. Among these measures one can be noticed everywhere - social distancing. Taking into account the fact that this leads to the impossibility of carrying out the current activities, in many fields of activity the remote work was implemented.

Teleworking has been a way of working since before the pandemic, it was even provided for a long time in the labor code in our country. Although it was a mode of work found mainly in the IT field, it was taken over and adapted in the conditions of social distancing in many fields of activity.

Today, practically, the economic activities that could implement teleworking have resisted the social and economic measures taken by the states of the world in the pandemic context.

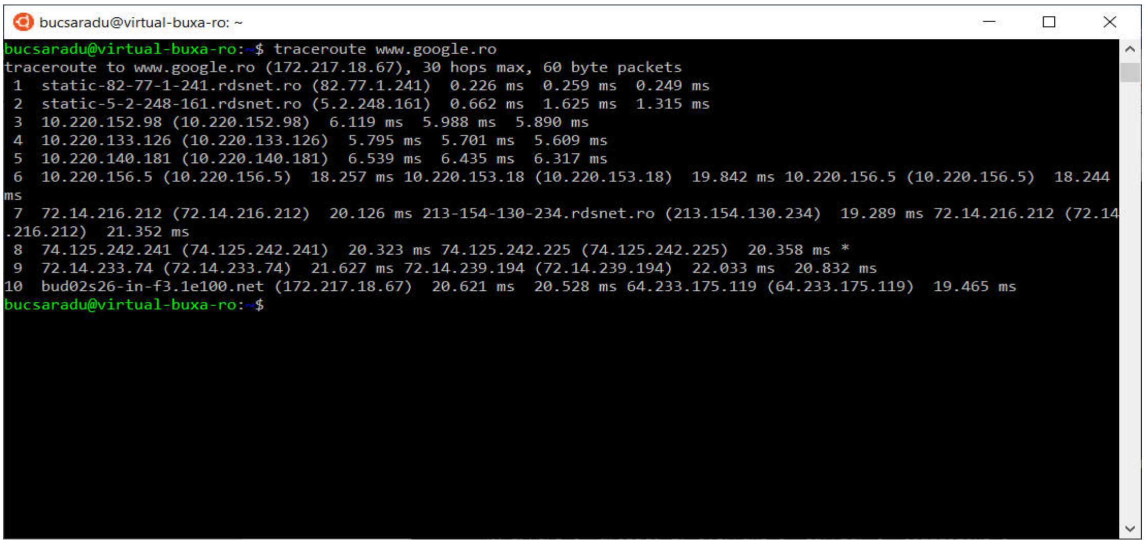
Teleworking is the procedure by which the employee works, most often, in the company / institution network from a remote terminal, often from the employee's home. In the past, teleworking was also used in situations where employees used the IT resources of the company / institution from other locations, often from secondary offices, from customer premises, from means of transport etc.

In any case, to connect the employee's terminal to the employer's network, it is used the internet infrastructure. From the moment when an internet connection is made practically a gateway opens, through which information is transmitted between 2 systems through a series of connection systems.

Everything that is transferred over the internet is subject to cyber risk. To mitigate or eliminate this risk, there are software protection solutions. One of these solutions is VPN technology - virtual private network.

1. Risks and Virtual Private Network Solutions

Connecting a system to the Internet involves assuming security risks. From a technical point of view, by accessing an Internet resource, the system from which the connection is initiated opens a communication path that crosses a suite of network equipment. Each communication node can represent a security break, starting with the initial system, continuing with all the equipment on the route and ending with the destination system.



```
bucsaradu@virtual-buxa-ro:~$ traceroute www.google.ro
traceroute to www.google.ro (172.217.18.67), 30 hops max, 60 byte packets
 1  static-82-77-1-241.rdsnet.ro (82.77.1.241)  0.226 ms  0.259 ms  0.249 ms
 2  static-5-2-248-161.rdsnet.ro (5.2.248.161)  0.662 ms  1.625 ms  1.315 ms
 3  10.220.152.98 (10.220.152.98)  6.119 ms  5.988 ms  5.890 ms
 4  10.220.133.126 (10.220.133.126)  5.795 ms  5.701 ms  5.609 ms
 5  10.220.140.181 (10.220.140.181)  6.539 ms  6.435 ms  6.317 ms
 6  10.220.156.5 (10.220.156.5)  18.257 ms 10.220.153.18 (10.220.153.18)  19.842 ms 10.220.156.5 (10.220.156.5)  18.244
ms
 7  72.14.216.212 (72.14.216.212)  20.126 ms 213-154-130-234.rdsnet.ro (213.154.130.234)  19.289 ms 72.14.216.212 (72.14
.216.212)  21.352 ms
 8  74.125.242.241 (74.125.242.241)  20.323 ms 74.125.242.225 (74.125.242.225)  20.358 ms *
 9  72.14.233.74 (72.14.233.74)  21.627 ms 72.14.239.194 (72.14.239.194)  22.033 ms  20.832 ms
10  bud02s26-in-f3.1e100.net (172.217.18.67)  20.621 ms  20.528 ms 64.233.175.119 (64.233.175.119)  19.465 ms
bucsaradu@virtual-buxa-ro:~$
```

Figure no. 1 Tracing route to www.google.ro

As can be seen in Figure no. 1, tracing an Internet address with the help of the traceroute command, the connection from the computer where it was initiated to the destination system crosses another 10 network equipment. Each equipment, in the context of security risk, can be considered vulnerability. It is true that most of these nodes are secured by Internet service providers, but this fact cannot guarantee the integrity of the data transferred between the origin and destination systems.

Regarding the origin and destination system, if they belong to the same entities (company, institution etc.) then the security of the data managed by these systems can be ensured by specific policies and procedures, as well as with the help of dedicated security tools: antivirus applications, internet security etc.

The above situation is specific to teleworking activities, activities in which the employer provides employees with data processing equipment equipped with all the necessary software for processing and data security.

Other situations of teleworking can be added to this situation, which can be considered ideal. One of these is that where the employer only manages the destination system, the employee using his own system remotely. In this case, the employer cannot control the security of the data processed on the employee's system.

Another teleworking work situation is using cloud technology. Through it, both the systems at the work points of the company / institution, as well as the employees' systems are connected to a cloud platform where they find all the necessary resources for data processing.

In the second and third situations, the employer has no control over the security of the employees' systems. In order to acquire this control, working rules and procedures must be set up to provide a guarantee for the security and integrity of the data processed remotely by the employees.

Assuring the security of the data both from the origin to the destination, respectively from the place of work, as well as to the place where the employee works, one of the problems can be considered solved. The problem of security of the other communication nodes remains. These nodes are different from one case to another; they can be changed automatically depending on the geographical position, the Internet service provider and the loading of its networks etc.

Whatever the situation, internet access cannot be done without the help of these nodes. Also, Internet users cannot control these nodes in any way, they have no way of knowing if someone interferes in one of them, whether or not the internet service provider stores the data transferred through its nodes, in other words these nodes can be a leaked data.

Even if we use the Internet for personal purposes, the problems related to the integrity of the data transferred through a network must be a security concern for the user.

Although national and European legislation obliges Internet service providers to ensure and guarantee the integrity of data transferred through their own networks, and they are really concerned about these problems, at least theoretically there is the possibility of data leakage.

To eliminate these risks there is a solution called VPN - **V**irtual **P**rivate **N**etwork. Through this tool, the data transferred through the Internet are encrypted at a low level over the entire course of them through the Internet communications nodes. Once arrived at the destination, the data is decrypted by the destination system, this being the only system in the world that holds the decryption key.

VPN technology is so efficient that Internet service providers and all their interconnection nodes only know that it is a VPN connection, which is transferred in its context being completely unintelligible. In this way the problem of data leakage through the communications nodes can be considered solved. Even if there are data leaks, these being encrypted can only be decrypted by the destination system, so no one has access to the data.

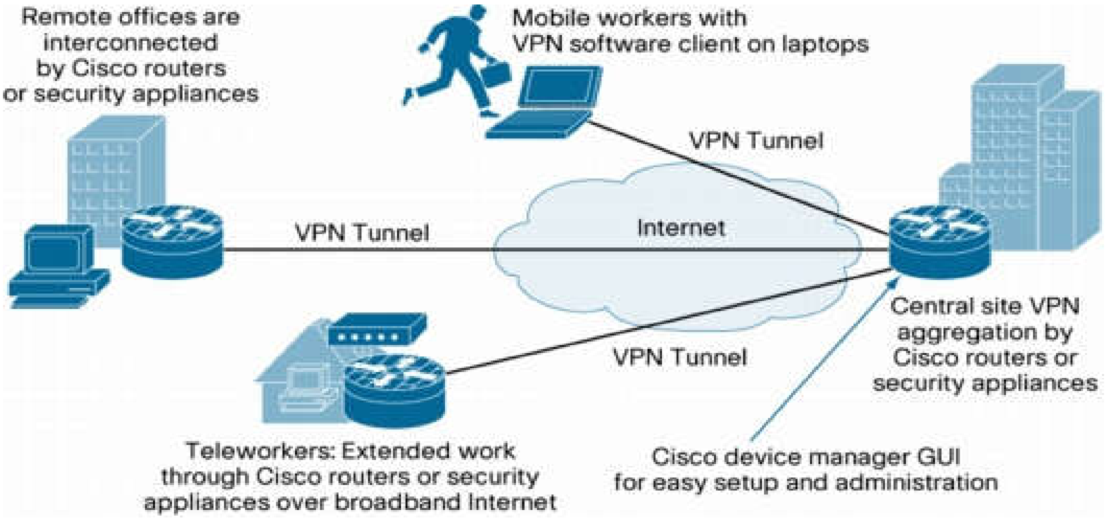

Remote offices are interconnected by Cisco routers or security appliances
Mobile workers with VPN software client on laptops
VPN Tunnel
VPN Tunnel
Internet
VPN Tunnel
Central site VPN aggregation by Cisco routers or security appliances
Teleworkers: Extended work through Cisco routers or security appliances over broadband Internet
Cisco device manager GUI for easy setup and administration

Figure no. 2 Diagram of VPN usage [1]

As shown in Figure no. 2, there is a central office that securely manages the VPN connections of the remote users. This center runs the VPN server and offers to others the facility of secure connection to the informational resources of the company / institution.

We also notice that the VPN connections reach the central server via the Internet, so they pass through the intermediate nodes of the Internet service providers.

Network technicians use the term tunneling for VPN connections in their vocabulary. It's a metaphor that describes technology very well. VPN practically creates a tunnel through the internet that links the headquarters and remote users to its ends. The rest of the Internet does not have access to the tunnel, so it does not have access to the data transferred through it, although it can be found out about its existence.

2. OpenVPN - Virtual Private Network Solution

There are many VPN solutions that can be implemented within an organization. Of all, a very common one is known, namely OpenVPN. This is widely used because it is a stable and reliable solution, but also free because it comes with the open source under the GNU / GPL general public license.

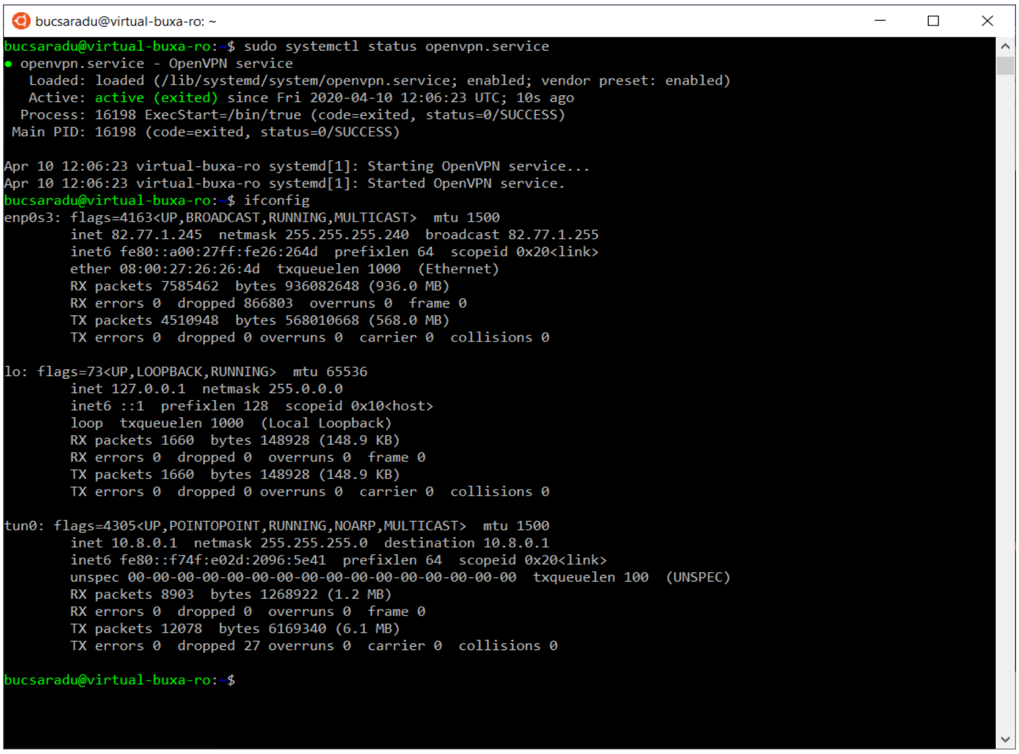
One of the advantages of opensource software solutions is that it can be implemented on any operating system platform. Therefore, OpenVPN also offers server solutions for Linux or Windows operating systems and client solutions for Windows, Linux, Android, iOS etc.

In the last period I noticed an increasingly present approach to VPN server solutions in the cloud. [2] Thus, all cloud services can be securely accessed through a VPN.

I tried another approach by moving the VPN server into a virtualized sandbox, respectively I installed OpenVPN on a virtual server, behind a secure network at the organization level. In this way the clients can connect to the virtual VPN server and all the data transferred by them are monitored and filtered inside the organization. Nothing can leave the network of the organization without being identifiable, both ends of the tunnel being thus secured.

Figure no. 3 shows the active status of the server and the creation of a virtual interface of tunnel type, respectively tunnel0. Another interface, which is regarded by the operating system as a physical interface, is emp0s3. Given the fact that we are considering a virtual machine, this interface is also virtual, and is mapping the physical network interface of the server that hosts the virtual machine.

Thus, the end of the tunnel from the organization's headquarters is virtualized on three levels - the first at the operating system and server application level, the second at the network interface level and the third at the VPN level. Through virtualization there is the possibility of a detailed control of the data traffic carried through these levels. Overlaid on these levels is the physical level of the server that hosts the virtual machine that comes with yet another layer of security for the VPN connection.



```
bucsaradu@virtual-buxa-ro:~$ sudo systemctl status openvpn.service
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
   Active: active (exited) since Fri 2020-04-10 12:06:23 UTC; 10s ago
  Process: 16198 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 16198 (code=exited, status=0/SUCCESS)

Apr 10 12:06:23 virtual-buxa-ro systemd[1]: Starting OpenVPN service...
Apr 10 12:06:23 virtual-buxa-ro systemd[1]: Started OpenVPN service.
bucsaradu@virtual-buxa-ro:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 82.77.1.245  netmask 255.255.255.240  broadcast 82.77.1.255
        inet6 fe80::a00:27ff:fe26:264d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:26:26:4d  txqueuelen 1000  (Ethernet)
        RX packets 7585462  bytes 936082648 (936.0 MB)
        RX errors 0  dropped 866803  overruns 0  frame 0
        TX packets 4510948  bytes 568010668 (568.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1660  bytes 148928 (148.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1660  bytes 148928 (148.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.1  netmask 255.255.255.0  destination 10.8.0.1
        inet6 fe80::f74f:e02d:2096:5e41  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 8903  bytes 1268922 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12078  bytes 6169340 (6.1 MB)
        TX errors 0  dropped 27 overruns 0  carrier 0  collisions 0

bucsaradu@virtual-buxa-ro:~$
```

Figure no. 3 Server side of VPN connection

In order to meet the clients of these services, in our case these being teleworking employees, we looked for a solution that would be extremely easy to use to access the VPN of the organization anywhere in the world.

In the other part of the VPN tunnel are the clients of these services, in our case these are the employees doing teleworking. I have been looking for a technical solution that will be extremely easy to use for accessing the organization's VPN anywhere in the world, especially for those employees who have no advanced technical knowledge in setting up such a connection.

Of course, there is the possibility that the employer can provide its employees with ready-made electronic computing systems for VPN use, but this would, in many cases, involve the acquisition of systems, their installation and configuration, practically requires considerable financial and labor effort.

The solution I propose is much cheaper, easier to use and just as secure as a computer specially configured to use a VPN. This solution consists of programming network equipment so that it automatically connects to the VPN based on the digital certificates and encryption keys offered by the server for each client separately.

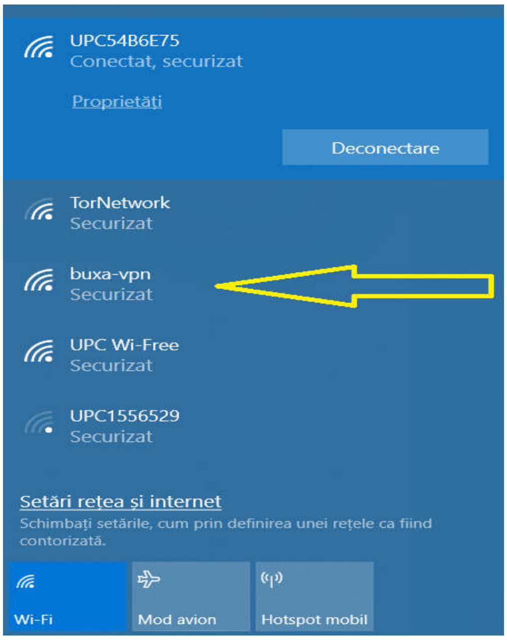
Basically, I took a TP-Link MR3020 [3] wireless router and installed a Linux operating system dedicated to these types of equipment - OpenWRT [4]. After installing and configuring the new operating system, as well as the VPN tunnel, the equipment can be placed in the employee's custody. It can connect the equipment via the ethernet network cable to any other equipment that offers internet connection, such as the home router provided by the internet service provider and connected to the power grid.

Once started, the equipment automatically connects to the internet and initiates a VPN tunnel to the organization's server. In this way, the second end of the VPN tunnel is the employee's home equipment. This equipment performs data routing exclusively through the tunnel, in other words all the data traffic is redirected to the organization's server, the employee being practically connected to all the hardware and software resources located in the headquarters of the organization.

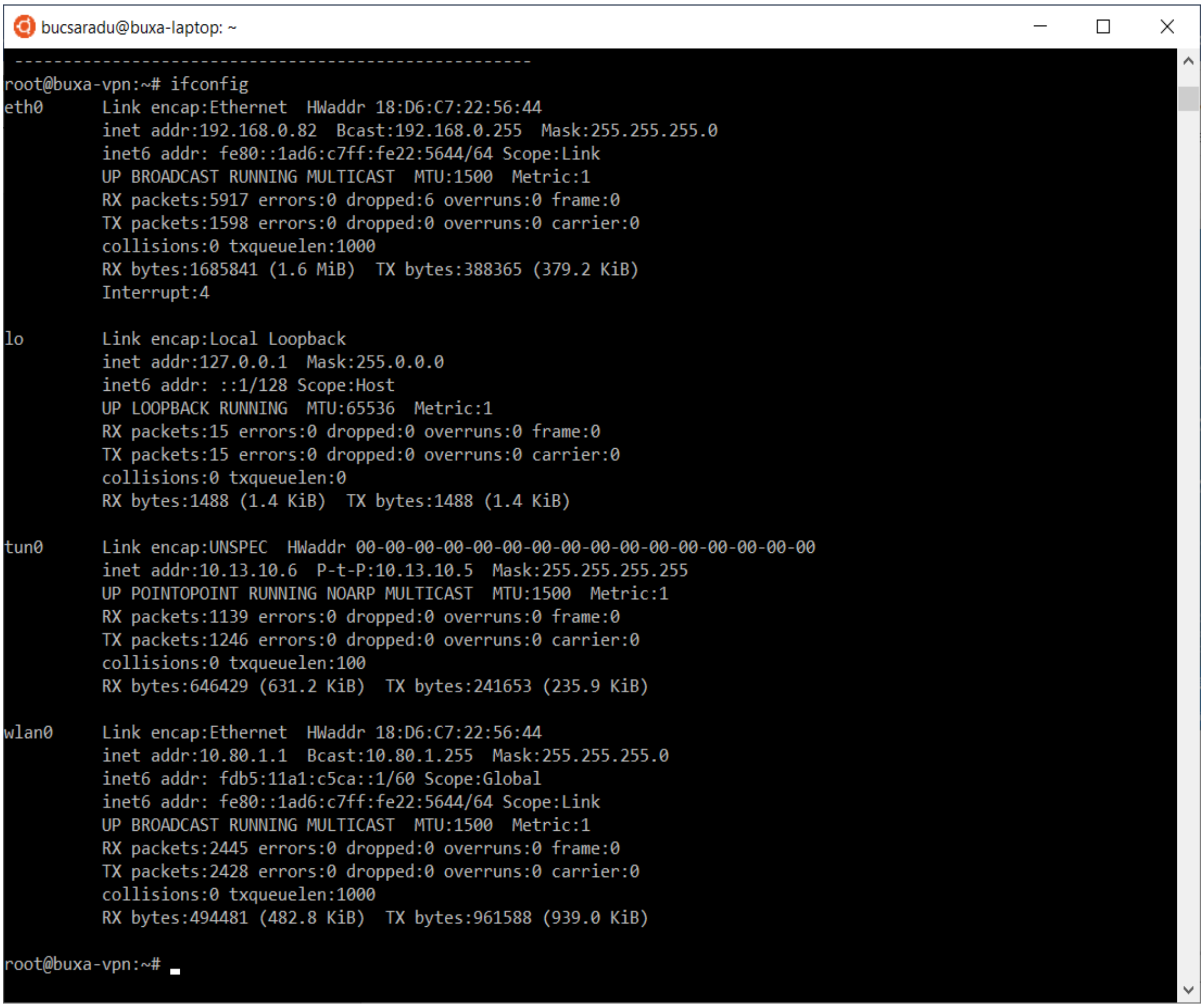
After starting the router, the user will be able to identify a wireless network, which was previously configured on the VPN equipment. We configured the Wi-Fi network using the most efficient data encryption systems available to avoid data leakage at this point.

The client connects to this Wi-Fi network using the credentials received from his employer. From this moment all data traffic on your system is directed through the VPN tunnel.

As you may have guessed, the customer can use to connect to the organization's VPN any device that has Wi-Fi functionality. Here we include any operating system platform for what we call generic PCs (Linux, Windows, MacOS etc.), smartphones and tablets (Android, iOS, Windows Mobile etc.), even other routers or access points available at the employee's location.



Schimbați setările, cum prin definirea unei rețele ca fiind contorizată.



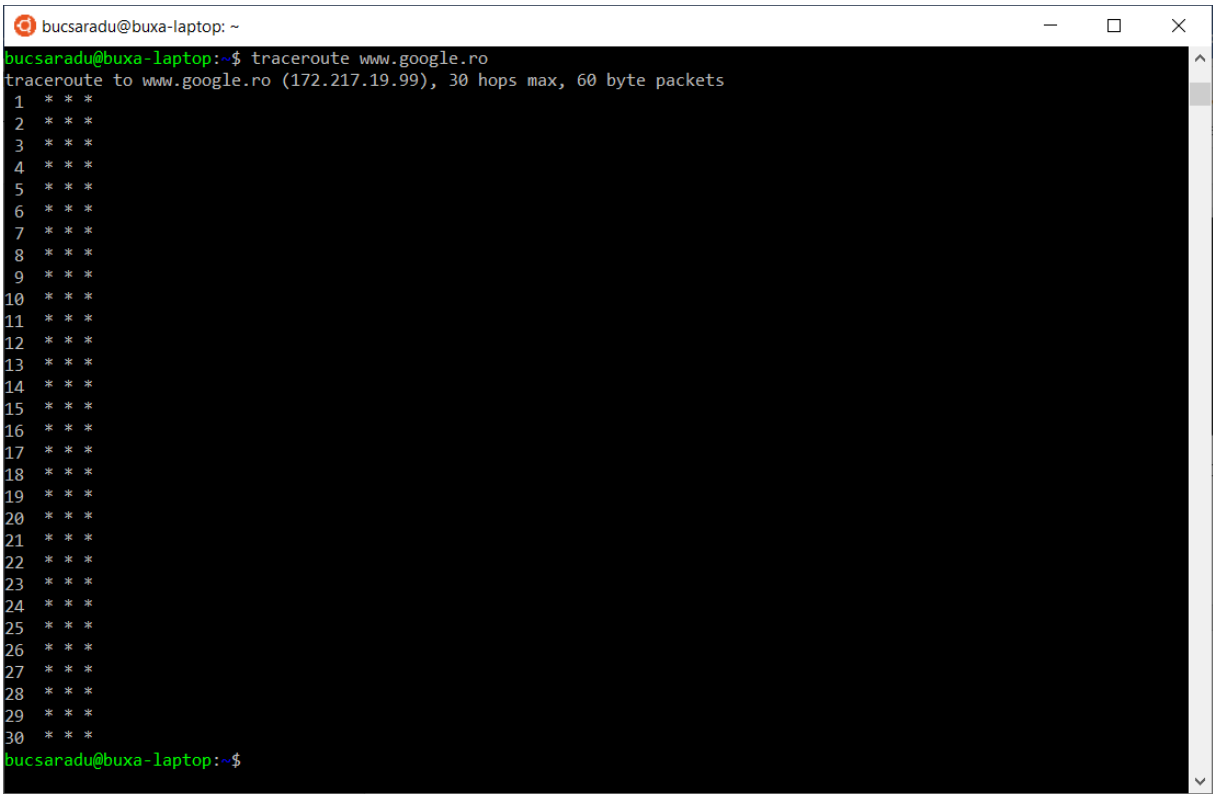
```
-----------------------------------------------------
root@buxa-vpn:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 18:D6:C7:22:56:44
          inet addr:192.168.0.82  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::1ad6:c7ff:fe22:5644/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5917 errors:0 dropped:6 overruns:0 frame:0
          TX packets:1598 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1685841 (1.6 MiB)  TX bytes:388365 (379.2 KiB)
          Interrupt:4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1488 (1.4 KiB)  TX bytes:1488 (1.4 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.13.10.6  P-t-P:10.13.10.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:1139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1246 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:646429 (631.2 KiB)  TX bytes:241653 (235.9 KiB)

wlan0     Link encap:Ethernet  HWaddr 18:D6:C7:22:56:44
          inet addr:10.80.1.1  Bcast:10.80.1.255  Mask:255.255.255.0
          inet6 addr: fdb5:11a1:c5ca::1/60 Scope:Global
          inet6 addr: fe80::1ad6:c7ff:fe22:5644/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2445 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2428 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:494481 (482.8 KiB)  TX bytes:961588 (939.0 KiB)

root@buxa-vpn:~# _
```

Figure no. 4 Server side of VPN connection

Figure no. 4 shows the configuration of the modified router to automatically initiate a VPN connection to the organization. In this configuration we notice two physical interfaces, respectively eth0 and wlan0, as well as the virtual interface of the VPN tunnel - tun0:

- eth0 is the Ethernet (cable) network interface. This is automatically configured based on the information received from the home router provided by the internet service provider.
- wlan0 is a WiFi interface. It automatically configures the connection of the equipment within the range. The client connects to this interface and automatically receives the necessary settings.
- The router is set to initiate the VPN connection using eth0 - physical interface and to create a bridge between this interface and tun0 - virtual interface.

When the client initiates a communication, it is automatically redirected from the wlan0 interface to the tun0 interface, which in turn relays through the tunnel to the organization's server, and will later decide what to do with the request within the organization.



```
bucsaradu@buxa-laptop:~$ traceroute www.google.ro
traceroute to www.google.ro (172.217.19.99), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
bucsaradu@buxa-laptop:~$
```

Figure no. 5 Tracing route to www.google.ro through the tunnel

In figure no. 5 I resumed the traceroute command. If at the beginning this command has 10 communication nodes (Figure no. 1), after the VPN tunnel is started, it can be observed that the same command with the same parameters no longer displays any node. It is a certification of the tunnel operation, practically the system from which we initiated the order is connected directly to the VPN server.

From this moment, the user can work from anywhere connected the modified router to the organization's network and can work remotely exactly as if in the main office. It can access private resources of the organization, it can share resources within the local network, it can even print documents to the printers available in the remote network.

Conclusions

Although VPN technology dates back to 1996, when Microsoft launched PPTP - peer-to-peer tunneling protocol, it has been developed over time to provide the necessary security of data traffic between client and server.

The large-scale extension of teleworking in the conditions of social distance imposed by the governments of the world in the context of the COVID-19 pandemic and beyond, VPN is the technical solution that offers the security of the data transferred between the employee and the employer.

The proposed solution can be efficient due to the fact that it is secure, using the most advanced encryption technologies at the present and at the same time it is cheap, not involving considerable financial efforts. In addition, it is very easy to use by employees, as they have no involvement in configuring the equipment needed to make the VPN connection.

Due to the risks involved in the transfer of data over the Internet, indispensable transfer in teleworking activities, I recommend that any employee working from home or from any other corner of the world, must use a VPN solution in relation to the employer to prevent the risk of data leakage, which can be extremely harmful to the organization.

References

[1] http://www.seogupshup.com/essential-things-know-about-vpn/
[2] https://openvpn.net/download-open-vpn/
[3] https://www.tp-link.com/ro/home-networking/3g-4g-router/tl-mr3020/
[4] https://openwrt.org/