An Evaluation of a Homemade VPN Service Compared to a Consumer VPN Service.

Thomas MacKinnon (1704872)

CMP320: Ethical Hacking 3

BSc Ethical Hacking Year 3

2019/20

.

Abstract

Virtual Private Networks (VPNs) have become an essential tool in many people's lives, allowing them to evade organizations from monitoring their internet traffic, such as the government or their Internet Service Providers. Many VPN providers have popped up in the last ten years, aiming to profit from their customers' fears by promising high end encryption to deny any hacking attempts. Each of these providers charge their customer base around £5 a month to use their service, normally with long contract lengths that are hard to escape.

In this white paper a homemade VPN is created and deployed to see if it can outperform one of the commercial VPN giants in a series of tests. The homemade VPN has a flat price of $5 a month, with the ability to end the subscription at any time. Each test aims to evaluate the VPNs effectiveness on many fronts, finding which the better choice is overall. The security of the VPNs are also evaluated, exposing the hidden flaws that the big VPN providers do not want you to know.

The results proved to be quite surprising, and somewhat defamed the lesser VPN, as it under performed in almost every test. The better VPN performed so well that it even outdid the raw internet connection on all fronts, crowning it as the best solution to your VPN needs.

.

+Contents

.

1 INTRODUCTION

1.1 BACKGROUND

A Virtual Private Network (VPN) is a connection method used to connect devices to a private network through a secure tunnel. VPNs are a common security tool, being advertised to be able to prevent hacking attempts, stop government monitoring and protect your data. VPNs work by creating an encrypted tunnel from the Virtual Private Server (VPS) to the user, that can be connected to with some sort of authentication, such as a password. Data can then be sent to the private network securely, in the case of internet browsing, the data is routed through the VPN to the requested location, rather than just through the Internet Service Provider (ISP).

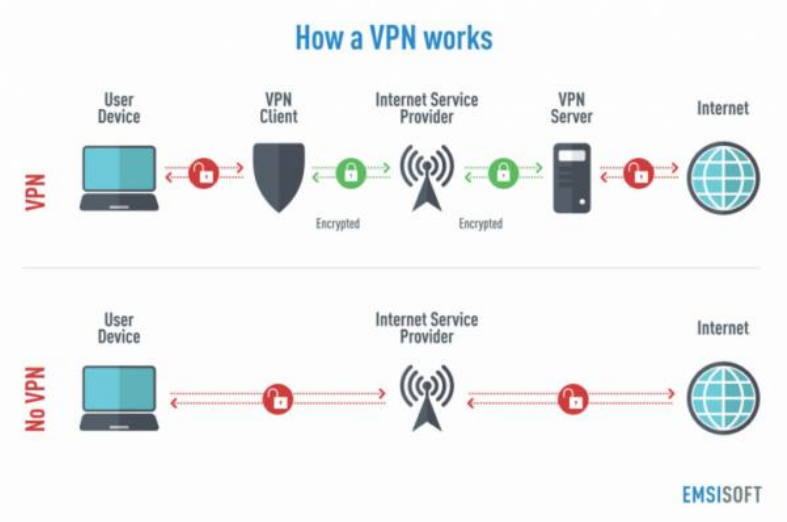


Figure 1: How a VPN works (Security Boulevard, 2020)

VPNs have become widely used in today's world, becoming an essential tool for many people. The main uses for a VPN are:

1. Connecting to a business' network to access content that otherwise wouldn't have been available, i.e. working from home. This allows businesses to keep employees working even when they cannot be physically present.
2. Protecting yourself from an untrustworthy network, like a coffee shop's free Wi-Fi, where the user is worried that a hacking attempt might be made on them. This can also apply to your ISP.
3. Accessing restricted content, such as websites banned by the government, or region locked content on streaming services.
4. Hiding your IP from other internet users/organizations. This could be to avoid an IP ban on Discord (Social messaging/calling application) in order to continuing using the platform.

Many VPN services have started in the past 10 years, advertising to their users that their software can completely protect them from any malicious hacker or imposing government. The price varies drastically from each application, some being free whilst others making their users pay a premium for protection. However, these services do not guarantee protection, and use fear tactics to make users believe that they are vulnerable without a VPN. Most VPN services convince their customers that their data is protected from start to end, this is not true, and instead the data is encrypted up until it leaves the private network, as seen in Figure 1. Websites that users are trying to access aren't expecting encrypted requests, so the VPN must decrypt the data before transmission. This means that hackers can attack the users' data, the only thing that has changed is the location (GitHub Gist, 2015).

A common pitch made by VPN services is that they do not keep logs of users activities, meaning that any browsing cannot be used against them in the future. This is a promising statement that cannot be verified at all by the customer. It makes little sense for a VPN service not to keep logs, as if they were in hot water for the actions of a customer they can easily deflect the blame. This is not an unwarranted claim, as HideMyAss, a UK based VPN service, has provided courts with user logs in the past. Chris Dupuy was arrested for harassing an ex-girlfriend by creating fake ads for her on escort websites, HideMyAss exposed Chris, a paid user, to the courts using his logs (ProPrivacy, 2016).

With this knowledge many people interested in security have gone off the idea of commercial VPNS, knowing that their data isn't completely protected, and assuming that the service is keeping logs. This has led to people creating their own VPNs from home, using an online network service and creating a secure tunnel to it. This prevents the VPN service from keeping logs, as there is no provider being used, only an online space for data.

Standard users are not informed on these facts, so blindly trust their provider of choice, believing that their £5 a month fee will stop any malicious attacker. Standard users are more concerned with the speed of their VPN, or the price they are paying rather than the inbuilt flaws of the system.

1.2 AIM

The aim of this project is to find out whether consumer grade Virtual Private Network (VPN) services are more effective than homemade VPNs. This will be done through several tests, showing the differences in speed, price and other factors to find which solution is best for users.

1.3 VPN TUNNELING PROTOCOL

VPNs use tunnels to send data and requests to the private server, there are several tunneling protocols that a service can use, each with their own flaws and benefits.

Point-to-Point Tunneling Protocol (PPTP) uses point-to-point protocol to create a secure tunnel to a Virtual Private Server (VPS). Strong passwords are used to authenticate connections between client and VPS, and connects through TCP port 1723. This Protocol was developed by Microsoft and is used widely throughout Windows systems (ResearchGate, 2016, Saugat Bhattarai).

Layer Two Tunneling Protocol (L2TP) is a combination of PPTP and L2F (a Cisco tunneling protocol) that uses layer two of the OSI model, being the Data link layer.

IPsec is a suite of protocols that enables secure communication between two points, by encrypting every IP packet sent from broadcaster to receiver. IPsec is commonly used in VPN applications, and can be seen in Nord VPN and Algo VPN.

1.4 MILITARY GRADE ENCRYPTION

Military Grade Encryption is a buzz word often thrown around by VPN providers to gain customers' trust, however, this is just another marketing scheme. When a provider mentions military grade encryption, they are normally referring to AES (Advanced Encryption Standard), which is an algorithm considered usable by the military, rather than the go to standard. AES does encrypt and decrypt data, but that does not mean it is secure at the ends of the tunnel, which are often the places malicious hackers attack, rather than the encryption methods itself (The Salty Hash, 2019). Military Grade encryption has quickly become the snake oil of VPNs, leading users to falsely assume that it is the miracle cure for cybercrime. Knowing this fact is important in avoiding the far reaching marketing of VPN services as they try to advertise themselves as being better than they ever could be.

PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The Procedure for this project involved the creation and installation of the homemade Algo Virtual Private Network. Algo VPN setup involved many steps, so a tutorial has been made to thoroughly explain each step. Commercial VPNs do not need to be covered here, as the installation process is very simple, since the installer does all the work for the user.

2.2 ALGO VPN SETUP

Algo VPN was the homemade solution selected for this experiment, as it is widely used amongst the information security community and is reliable. Algo VPN is an open-source software bundle that simplifies the setup for homemade VPNs to cloud data providers. A tutorial has been created to aid users in the setup of the VPN, whilst measuring the setup time for the later results.

The first stage to deploying Algo VPN is to setup a droplet on Digital Ocean, which will be the access point to the internet. Choose the Ubuntu option and select all the default options, as seen in figure 2. Here is also were the price of Algo VPN comes in, the minimum cost is $5 a month, which is sufficient for the VPN to work.

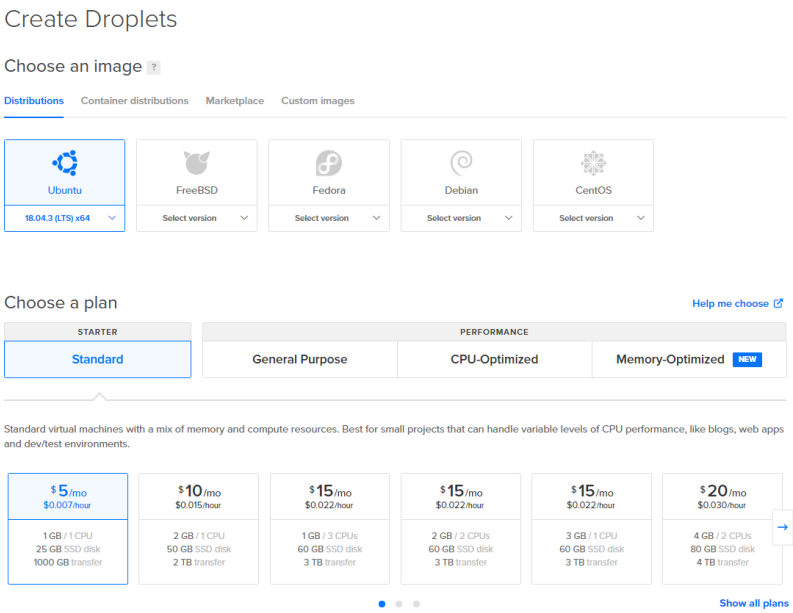


Figure 2: Creating an Ubuntu droplet in Digital Ocean

Digital Ocean will send the required password to the droplet in the associated email address, which can be used to SSH into the system using the username of "root". It's recommended to change the default password provided by Digital Ocean, since it is very complex. Update the server with the following commands and install python3 to the system.

```
apt-get -y update
```

```
apt-get -y upgrade
```

```
apt install -y python3-virtualenv
```

Algo can be downloaded now that the system is up to date, to do so simply clone the GitHub link (GitHub, 2020) to the server, as seen in figure 3.

```
root@vpnsecurityproject-droplet-1:~# git clone https://github.com/trailofbits/al
go
Cloning into 'algo'...
remote: Enumerating objects: 14, done.
remote: Counting objects: 100% (14/14), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 6658 (delta 4), reused 4 (delta 2), pack-reused 6644
Receiving objects: 100% (6658/6658), 2.76 MiB | 4.80 MiB/s, done.
Resolving deltas: 100% (3796/3796), done.
root@vpnsecurityproject-droplet-1:~#
```

Figure 3: Cloning Algo files to the droplet

Use the following commands to install the needed packages for Algo VPN, you may also change the username of the system if you wish.

```
apt install virtualenv
```

```
cd algo
```

```
python3 -m pip install -U pip virtualenv
```

```
python3 -m pip install -r requirements.txt
```

```
  GNU nano 2.9.3                        config.cfg                          Modified

---

# This is the list of users to generate.
# Every device must have a unique username.
# You can generate up to 250 users at one time.
# Usernames with leading 0's or containing only numbers should be escaped in double quotes, e.g. "$
# Emails are not allowed
users:
  - laptop
  - desktop

### Review these options BEFORE you run Algo, as they are very difficult/impossible to change afte$

# Change default SSH port for the cloud roles only
# It doesn't apply if you deploy to your existing Ubuntu Server
ssh_port: 4160

# Deploy StrongSwan to enable IPsec support
ipsec_enabled: true

# Deploy WireGuard
# WireGuard will listen on 51820/UDP. You might need to change to another port
# if your network blocks this one. Be aware that 53/UDP (DNS) is blocked on some
File Name to Write: config.cfg
^G Get Help          M-D DOS Format       M-A Append           M-B Backup File
^C Cancel            M-M Mac Format       M-P Prepend          ^T To Files
```

Figure 4: Adding users in the Algo config file

After the packages have finished installing the configuration can be set, access “config.cfg” with the command below and add any users to the users section.

```
sudo nano config.cfg
```

Now all there's left to do is to install Algo, do this by typing the command below to begin the installation. When prompted select option eleven, since the Digital Ocean Droplet is an Ubuntu 18.04 server, as seen in figure 5.

```
./algo
```

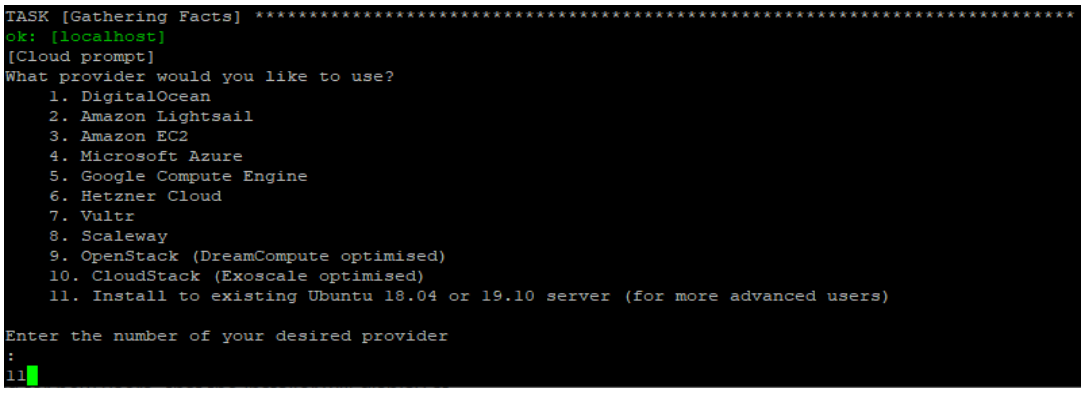


Figure 5: Selecting Ubuntu in Algo install

Accept the default options for each choice during the rest of the installation, except for the IP address, which will be the IP address of the Digital Ocean Droplet.

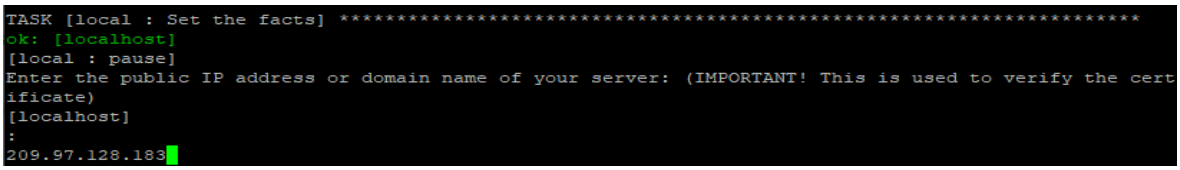


Figure 6: Entering IP address for the droplet

The screen seen in figure 7 will appear once the installation has finished, which shows the IP address needed to connect to Algo and the p12/SSH password. In this case the password has been hidden with the red block.

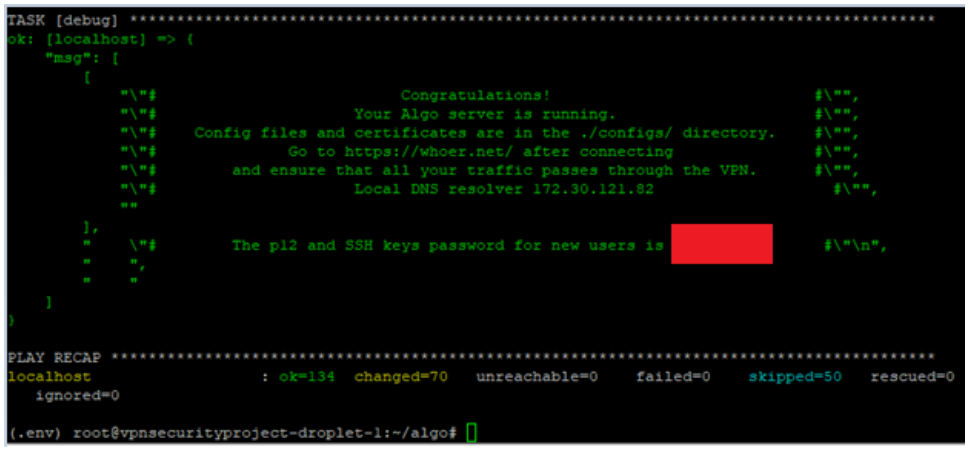


Figure 7: Algo succesful install

A configuration file was created for each user set previously, and should be copied across to your computer. The files are located inside */algo/configs/<ip of your droplet>/wireguard.*

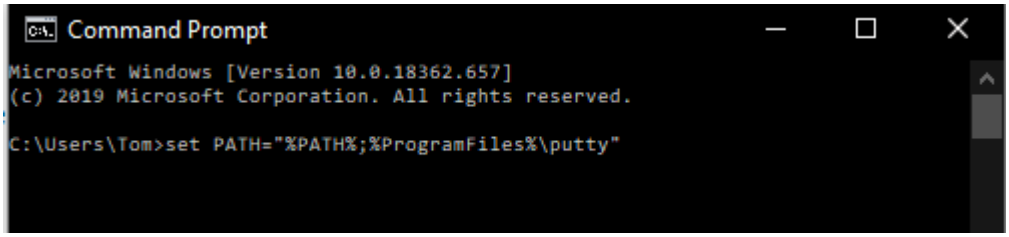


Figure 8: Setting path to PuTTY

A path is created in figure 8 to PuTTY so that the file can be securely transferred from the server to your home computer. Use the command below to copy the file to your Windows 10 system, replacing the IP address and the *.conf* file name with your own.

```
pscp root@<ip address of your droplet>:algo/configs/@<ip address of your droplet>/wireguard/<your config file> c:\<folder of your choice>
```

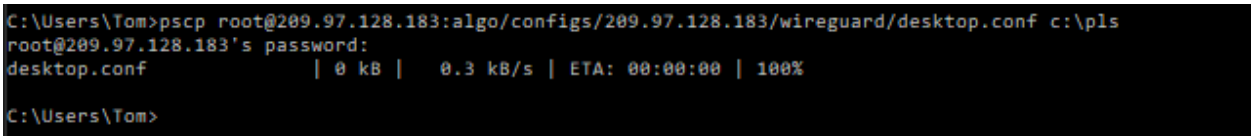


Figure 9: Copying the user config file from droplet

The final step involves the program WireGuard (WireGuard, 2019) which creates the tunnel to the server. Click the add tunnel button and select the configuration file, then simply click Activate to start flowing traffic through the VPN.

This ends the Procedure section of the paper, as the homemade VPN and the commercial VPN have both been installed.

RESULTS

3.1 TEST PLAN

Testing the VPNs can be separated into four different categories, each adding to the overall evaluation of the service. The four pillars of the test plan are:

1. **Price –** The overall cost of the application for a month and then a year will be compared between the selected VPNs and other services. VPN services that haven't been tested in other areas can be used to compare price information, as it is freely available online.
2. **Speed –** Arguably the most important factor for standard users, as the speed of the connection makes or breaks the VPNs effectiveness. After each hour of testing, an online internet speed test will be conducted on the VPN connection, which can be compared to the base internet speed before any VPNs were activated.
3. **Bandwidth Usage –** The bandwidth usage will be compared to see if the VPNs show a significant difference between applications, and how much it increases from the baseline. BitMeter OS (CodeBox, 2020) is used to see how much bandwidth is being used throughout the experiment, which runs in the background and outputs to a web display in real time.
4. **Setup Speed –** Each VPNs setup time will be compared, with a rating for how complex the setup was. The latter point is more subjective, but still is useful for the evaluation.

Testing will be done through hour long slots to maintain fair testing, each VPN will be tested 5 times throughout the day. The testing will be conducted on a desktop computer with Ethernet, and will have a 24 hour YouTube stream running for the entire length of the test. The desktop will not be used for any other internet activities, other than internet speed tests. An excel spreadsheet has been constructed to show the time table for testing and the test fields.

TIME	VPN BEING TESTED	SPEED	UPLOAD SPEED	DOWNLOAD SPEED	AVERAGE UPLOAD SPEED	AVERAGE DOWNLOAD SPEED	BANDWIDTH USAGE
12:00 PM	No VPN						
1:00 PM	Nord VPN						
2:00 PM	Algo VPN						
3:00 PM	No VPN						
4:00 PM	Nord VPN						
5:00 PM	Algo VPN						
6:00 PM	No VPN						
7:00 PM	Nord VPN						
8:00 PM	Algo VPN						
9:00 PM	No VPN						
10:00 PM	Nord VPN						
11:00 PM	Algo VPN						
9:00 AM	No VPN						
10:00 AM	Nord VPN						
11:00 AM	Algo VPN						

Figure 10: Test results spread sheet

3.2 PRICING RESULTS

The cost for each VPN and two extra services were compared with the graph seen in figure 11. Each service offered a monthly subscription, and those that offered longer options were also added to the table, having calculated the monthly equivalent.

	Monthly Plan	Yearly Plan	2 Year Plan	3 Year Plan
Nord VPN	9.2	5.38	3.84	2.68
Express VPN	10.3	6.62		
Hotspot Shield	6.16			
Algo VPN with Digital Ocean	3.85			

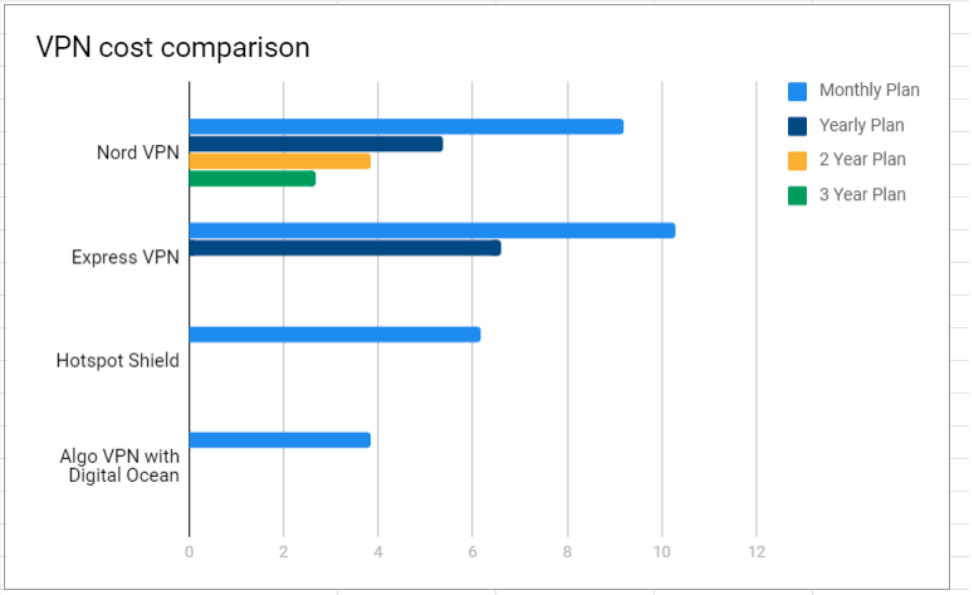


Figure 11: Pricing Results

3.3 SPEED AND BANDWIDTH USAGE RESULTS

The ping of the Internet connection was measured every hour using Google's internet speed tester, and recorded into the spreadsheet. Bandwidth usage was also measured every hour using BitMeter OS, tracking the average download and upload speeds as well. The final results can be seen in figure 12, after the testing was complete. The full results and screen shots can be found in Appendix A and B.

TIME	VPN BEING TESTED	SPEED	UPLOAD SPEED	DOWNLOAD SPEED	AVERAGE UPLOAD SPEED	AVERAGE DOWNLOAD SPEED	BANDWIDTH USAGE
12:00 PM	No VPN	27ms	17.0 Mb/s	8.92 Mb/s	25.36 kB/s	123.33 kB/s	321.75 MB
1:00 PM	Nord VPN	21ms	21.8 Mb/s	4.92 Mb/s	45.89 kB/s	285.53 kB/s	453.27 MB
2:00 PM	Algo VPN	20ms	24.1 Mb/s	8.80 Mb/s	39.23 kB/s	155.70 kB/s	392.92 MB
3:00 PM	No VPN	27ms	18.0 Mb/s	3.90 Mb/s	17.40 kB/s	126.68 kB/s	291.59 MB
4:00 PM	Nord VPN	19ms	22.6 Mb/s	6.27 Mb/s	59.86 kB/s	293.21 kB/s	611.07 MB
5:00 PM	Algo VPN	20ms	23.7 Mb/s	8.60 Mb/s	3.02 kB/s	82.94 kB/s	256.54 MB
6:00 PM	No VPN	27ms	17.8 Mb/s	8.98 Mb/s	2.10 kB/s	77.03 kB/s	325.32 MB
7:00 PM	Nord VPN	21 ms	20.0 Mb/s	7.90 Mb/s	69.19 kB/s	274.60 KB/s	473.70 MB
8:00 PM	Algo VPN	20ms	23.0 Mb/s	8.70 Mb/s	37.54 kB/s	116.45 kB/s	182.04 MB
9:00 PM	No VPN	28ms	18.0 Mb/s	3.61 Mb/s	14.62 kB/s	60.56 kB/s	530.12 MB
10:00 PM	Nord VPN	21ms	18.7 Mb/s	7.63 Mb/s	66.30 kB/s	287.31 kB/s	632.76 MB
11:00 PM	Algo VPN	20ms	23.7 Mb/s	8.8.2 Mb/s	2.89 kB/s	82.64 kB/s	447.51 MB
9:00 AM	No VPN	27ms	18.0 Mb/s	8.96 Mb/s	2.60 kB/s	66.36 kB/s	283.55 MB
10:00 AM	Nord VPN	21ms	22.1 Mb/s	7.86 Mb/s	71.77 kB/s	289.75 kB/s	592.29 MB
11:00 AM	Algo VPN	20ms	19.4 Mb/s	8.67 Mb/s	85 kB/s	85 kB/s	692.28 MB

Figure 12: Speed and Bandwidth Usage Results

3.4 SETUP SPEED RESULTS

Setup speed is rather hard to judge for applications, as it relies on the user's proficiency with technology, internet speed and hardware limitations. The setup of each VPN was timed and rated on difficulty of setup to effectively evaluate the services.

Nord VPN:

Setup for Nord VPN was incredibly simple, once the application was downloaded and installed only the users credentials were needed to start up the service. Nord VPN clearly have streamlined the process in order to not exclude novice tech users, and have provided an appealing display that effectively shows the users how to operate it.

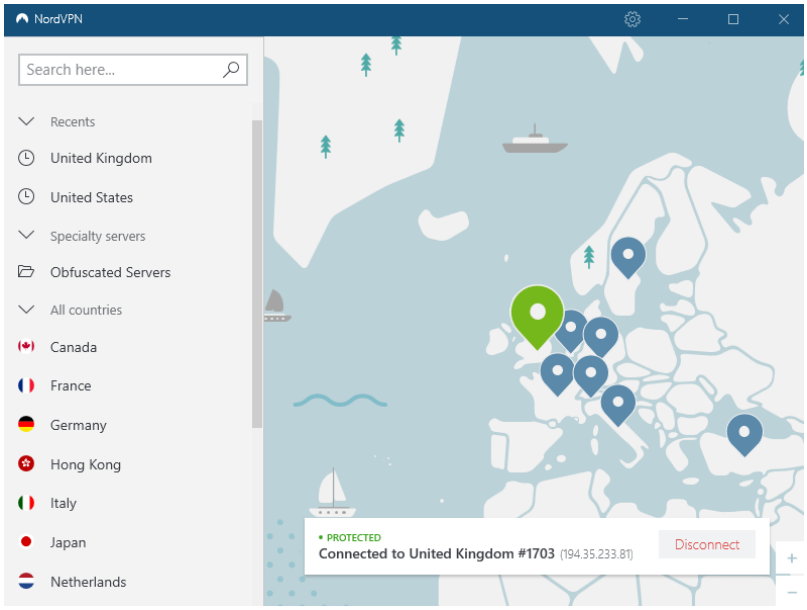


Figure 13: Nord VPN home screen

Time taken to setup = 5.46 Minutes

Difficulty rating = 2/10

Algo VPN:

The setup for Algo VPN is much harder for the average user, as it relies on knowledge of Linux command line. However, Algo have made the process easier, with a detailed GitHub installation guide and a community of users who have provided helpful tutorials. The user interface isn't great, but Algo has done the best they can to make setup smoother.

Time taken to setup = 34.08 Minutes

Difficulty rating = 7/10

DISCUSSION

4.1 RESULTS DISCUSSION

Pricing Results:

The pricing results were quite interesting for this experiment. Nord VPN clearly has the lowest price out of the options looked at, but is only available if the user takes out a 36 month contract. The money for the total length of the contract is taken from your account immediately, and not on a monthly basis, meaning it's an upfront cost of £116 (including VAT). This makes the cheaper prices less available to users, meaning that yearly and monthly plans are more likely to be purchased, which seem around average compared to other VPN services.

	Monthly Plan	Yearly Plan	2 Year Plan	3 Year Plan
Nord VPN	9.2	5.38	3.84	2.68
Express VPN	10.3	6.62		
Hotspot Shield	6.16			
Algo VPN with Digital Ocean	3.85			

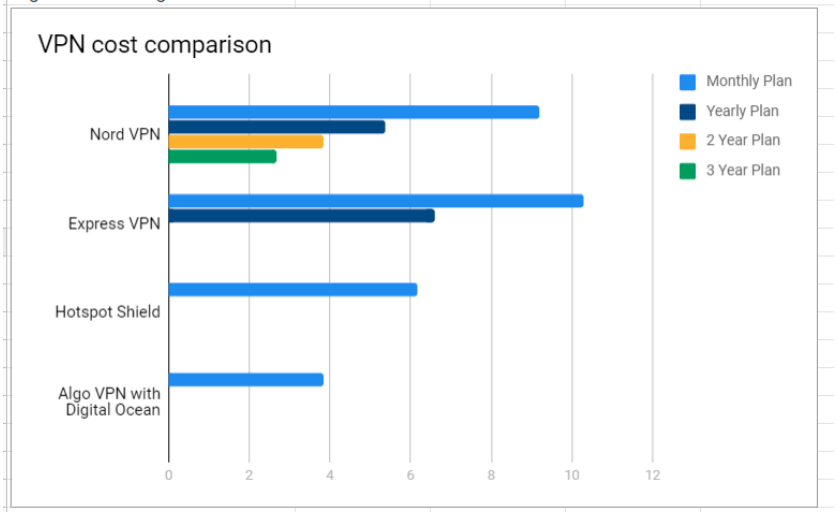


Figure 14: Pricing Results with graph

Algo VPN uses Digital Ocean to provide the VPS, which has a flat rate of $5 a month (£3.85), which beats all the competition for monthly subscriptions. Digital Ocean also offers new users $100 free credit that will expire after two months, making homemade VPN free for a time. This allows new users to trial Algo (or any other Digital Ocean application) before beginning payment. Nord VPN also others a free trial, but it only lasts a month.

Nord VPN is technically cheaper, but only if users choose to commit for the longest contract length. Algo payments are cheaper in the short term and more flexible. Nord VPN doesn't allow cancellations mid-way through a contract, whilst a Digital Ocean subscription can be ended at any time. Through these factors Algo comes out on top for price evaluation.

Speed Results:

Results for speed have been separated into two sections, one being Ping results and the other being Upload/Download speed. The raw internet connection was presumed to be the fastest, with Nord VPN being second and Algo VPN being the slowest.

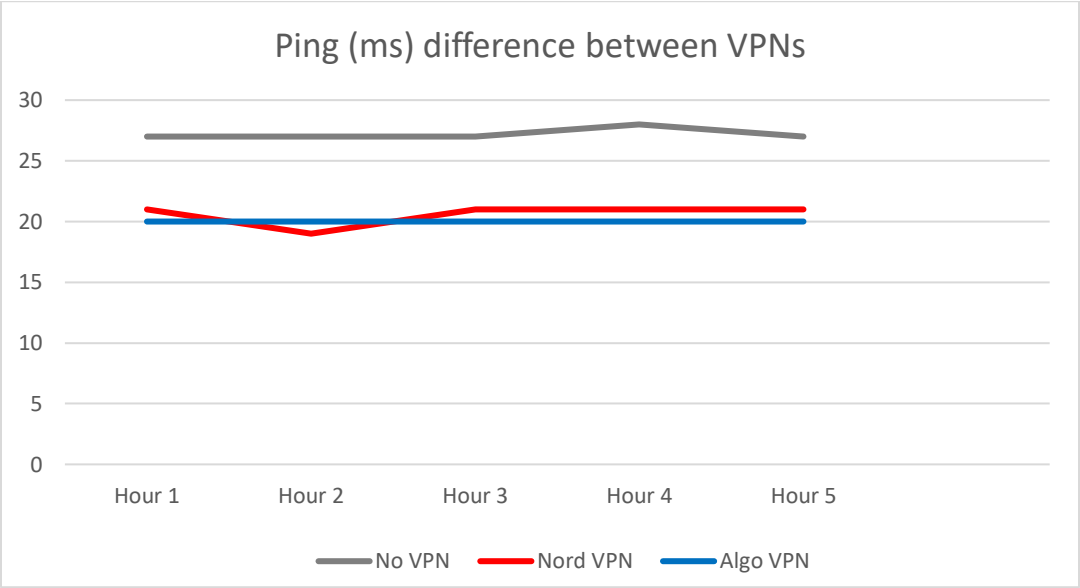


Figure 15: Ping results graph

Average Ping

No VPN = 27 ms **Nord VPN = 20.6 ms** **Algo VPN = 20 ms**

As seen in Figure 15, Ping results were consistent for each solution, remaining the same with only a change of 1ms or so. This left the raw internet connection having the highest Ping, and therefore being consistently the slowest out the tests. Nord VPN and Algo VPN were very close together, and the average difference is only 0.6 ms, however, Algo is still the fastest out of the options.

Looking at the result for each internet speed test reveals that the raw internet connection goes to the Dublin server, whilst both VPNs go to the London servers. This could be a reason why the raw connection was slower than the VPNs.

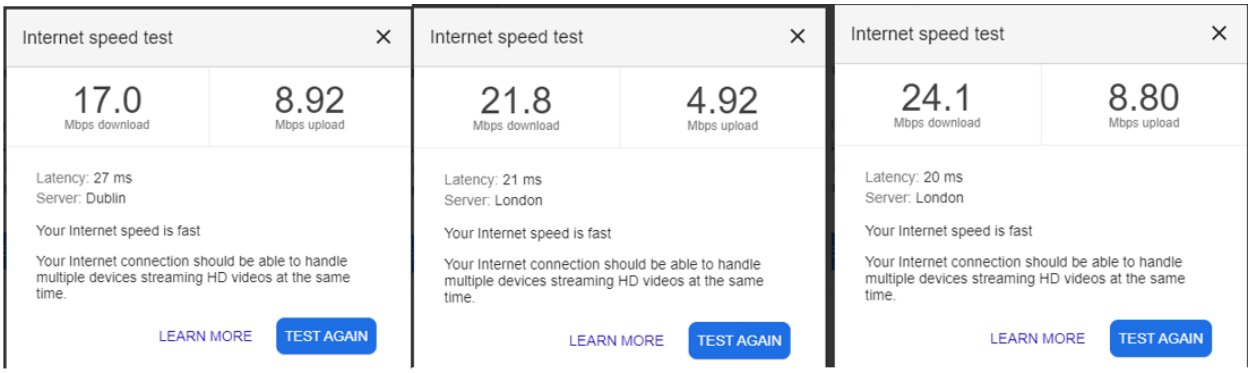


Figure 16: Internet speed test for hour 1 for no VPN (left), Nord VPN (middle), and Algo VPN (right)

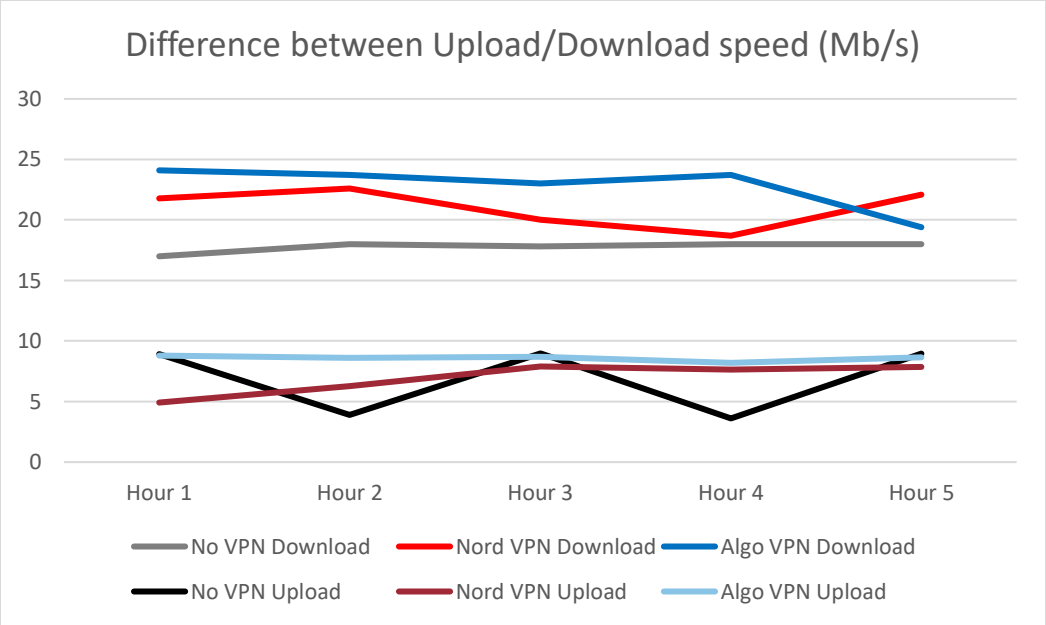


Figure 17: Upload/Download speed results graph

Average Download Speed

No VPN = 17.76 Mb/s **Nord VPN = 21.04 Mb/s** **Algo VPN = 22.78 Mb/s**

Average Upload Speed

No VPN = 6.87 Mb/s **Nord VPN = 6.92 Mb/s** **Algo VPN = 8.59 Mb/s**

The results for Upload and Download speed reveal a similar story, as Algo VPN shows itself to be the fastest, followed by Nord VPN and then the raw connection. The raw internet connection was yet again connected through the Dublin servers rather than the London servers, which could have caused the lower result. Nord VPN displayed similar speeds to Algo VPN, but was just slightly slower, leaving Algo VPN being the fastest option for Ping, Download and Upload speeds.

Bandwidth Usage Results:

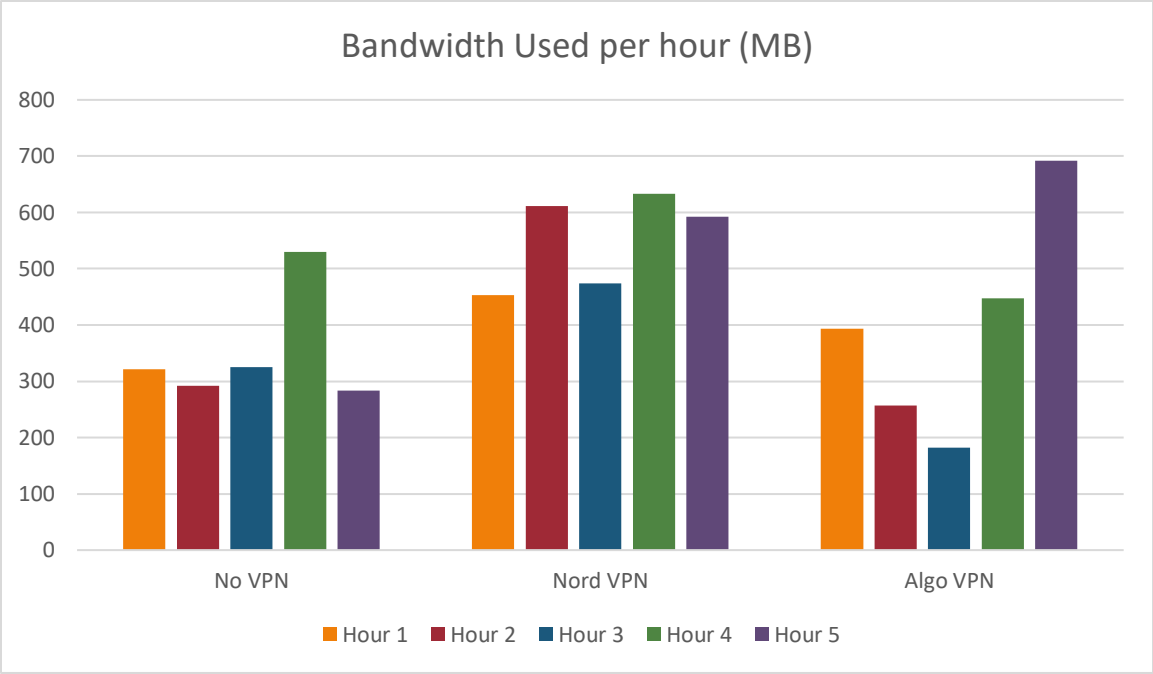


Figure 18: Bandwidth Used graph

Average Bandwidth used

No VPN = 350.47 MB **Nord VPN = 552.61 MB** **Algo VPN = 394.26 MB**

Bandwidth usage was predicted to be consistent for each VPN, with the no VPN tests producing lower uses. This ended up being the case, with Nord VPN using the most bandwidth, followed by Algo VPN and then the raw internet connection. Nord VPN used far more bandwidth than the other solutions, which could be a problem for users with limited internet bandwidth. Each test had a YouTube stream in the background so consistent bandwidth usage occurred, with no other internet operations taking place to avoid effecting the results.

The results for Algo VPN were closer to the raw internet connection than predicted, however, there was one outlier in the results, being the fifth hour of testing. This hour of testing seemed to use much more bandwidth than any other hour, and did not reflect in the other solutions fifth hour results. This was discovered to be the fault of the tester, as an application that had been left open began updating midway through the test. This led to a drastic rise in usage for that hour of testing, so a new average was calculated, this time without the fifth hour.

Average Bandwidth used (without fifth hour)

No VPN = 367.2 MB **Nord VPN = 542.69 MB** **Algo VPN = 319.76 MB**

These new results paint a different picture, with Algo VPN using the least bandwidth, followed by the raw internet connection and Nord VPN using the most. Surprisingly Algo comes out as best for bandwidth usage in this evaluation.

Setup Speed Results:

Setup speed has a rather obvious winner, as Algo VPN took almost 7 times longer to setup than Nord VPN's impressive 5 minutes. This is due to Algo being a more complicated system, needing setup of several different things just to work, whilst Nord VPN is streamlined for customers.

It is important to note that Algo VPN could be setup at a similar speed to Nord VPN if the Digital Ocean VPS was set up beforehand. In this instance all that would need installing is Wire Guard with the respective configuration file, whilst Nord VPN needs the installer and the user to login before it can begin working.

Nord VPN clearly has a better setup process, and so comes out as best for setup speed evaluation.

4.2 GENERAL DISCUSSION

The results of this experiment revealed a lot of information about which VPN service is the best for users, both standard and those interested in cybersecurity.

Algo VPN came out as the best option overall. It proved to be faster, used far less bandwidth, and cost less than Nord VPN. These results were rather shocking at first, as how could a small homemade VPN work better than a VPN with one of the largest user bases (Comparitech, 2020). Algo VPN's only flaw is its complex setup process, which requires understanding of Linux command line, which most users don't have.

Nord VPN still proved to be better than the raw internet connection, and was close to Algo VPN in results, but was still the lesser of the two. Nord VPN also proved to be more unreliable than the rest, as it disconnected several times throughout the testing period, and seemed to prevent access to some websites, including Amazon.

The raw internet connection was thought to be the fastest before testing began, but very quickly revealed itself to be the slowest. This was interesting, as Nord VPN and Algo VPN have to encrypt and decrypt packages, whilst the raw connection doesn't, but still it ended up being slower.

Algo VPN is also the safest VPN tested, as the logs kept are available on the Ubuntu droplet, and so can be deleted or edited by the user. Nord VPN claims they do not keep logs, but there is no possible way to prove this, and as mentioned in the Background of this whitepaper, it makes financial sense for them to keep logs of user searches.

Nord VPN was hacked in March of 2018, a data center in Finland was accessed by a hacker and Nord did not inform their customer base about this attack until months later (Tech Crunch, 2019). This shows that their "military grade encryption" does nothing if they can't even secure their own servers, which leaves all their users unknowingly at risk. The worst part is they didn't stop their far reaching advertising campaign during the investigation into the vulnerability. This is morally wrong, as they were risking the online safety of all their current users, whilst trying to attract more to their insecure business.

4.3 CONCLUSIONS

In conclusion, Algo VPN proved to be the best VPN option for users, outperforming in all fields except for setup time. Algo VPN is much safer than the commercial VPN options, and considerably cheaper. Algo is hard to setup, but with good tutorials available online and in this whitepaper the user should have no trouble in running their own VPN.

Nord VPN proved itself to be inferior in almost every way, and is much more of a risk to users than Algo, leaving it as a pointless service. The marketing tactics used by Nord VPN makes it seem like the perfect application to keep users safe whilst online, but in reality it is much more dangerous.

When it comes to VPNs, always go with the homemade option, having control over your internet is far better than giving it away to some faceless company with a bad record.

4.4 FUTURE WORK

The evaluation of VPN services revealed a lot about efficiency and the truth of VPNs effectiveness against hackers. The experiment involved two VPNs, one being homemade and the other being commercial, with the base internet connection also being tested.

If given more time a larger number of commercial VPNs would have been tested, to see if Nord VPN was standard or an outlier in terms of data. This also extends to homemade VPNs, as there are other options than Algo that could have been explored given more time.

Five hours of testing was conducted on each VPN, which is enough to gain an average for each piece of testing data. However, the VPNs were only tested on one network, so a further five hours of testing on a new network could have revealed more data. The tests also only took place on a Desktop computer with an Ethernet connection, if given more time tests conducted from a laptop's Wi-Fi and mobile devices would have been attempted.

4.5 CALL TO ACTION

Algo VPN is an excellent solution to online security, if you wish to contact the tester about anything to do with this project please feel free to use the information below.

Thomas MacKinnon 1704872@uad.ac.uk

REFERENCES

Research Papers:

Research Gate (2016) Saugat Bhattarai. *VPN research (Term Paper)*. Available at:

https://www.researchgate.net/publication/289120789_VPN_research_Term_Paper (Last accessed on 17/05/2020)

Research Gate (2016) Kuwar Kuldeep Veer Vikram Singh, Himanshu Gupta. *A New Approach for the Security of VPN*. Available at:

https://www.researchgate.net/publication/307090754_A_New_Approach_for_the_Security_of_VPN (Last accessed on 17/05/2020)

Google Scholar (1999) Niels Ferguson, Bruce Schneier. *A Cryptographic Evaluation of IPsec*. Available at:

http://www.cs.fsu.edu/~yasinsac/Papers/ipsec.pdf (Last accessed on 17/05/2020)

Articles:

GitHub Gist (2015) Sven Slootweg. *Don't use VPN services*. Available at:

https://gist.github.com/joepie91/5a9909939e6ce7d09e29 (Last accessed on 17/05/2020)

SaferVPN (2019). *The Dark Side of Free VPNs: What You Need to Know.* Available at:

https://www.safervpn.com/blog/use-free-vpn-hola-risks-cybercrime/ (Last accessed on 17/05/2020)

Security Boulevard (2020) Marc Kranat. *VPN: A Key to Securing an Online Work Environment*. Available at:

https://securityboulevard.com/2020/03/vpn-a-key-to-securing-an-online-work-environment/ (Last accessed on 17/05/2020)

ProPrivacy (2016) Douglas Crawford. *HMA (formerly Hide My Ass) User Arrested*. Available at:

https://proprivacy.com/privacy-news/hma-formerly-hide-my-ass-user-arrested (Last accessed on 17/05/2020)

The Salty Hash (2019) Patrick Walsh. *Military Grade Encryption*. Available at:

https://blog.ironcorelabs.com/military-grade-encryption-69aae0145588 (Last accessed on 17/05/2020)

Tech Crunch (2019) Zack Whittaker. *NordVPN confirms it was hacked*. Available at:

https://techcrunch.com/2019/10/21/nordvpn-confirms-it-was-hacked/ (Last accessed on 17/05/2020)

Comparitech (2020) Rebecca Moody. *VPN Market Report 2020: Who's got the biggest VPN market share?*. Available at:

https://www.comparitech.com/blog/vpn-privacy/vpn-market-share-report/ (Last accessed on 17/05/2020)

Tools:

CodeBox (2020). *BitMeter OS- Downloads*. Available at:

https://codebox.net/pages/bitmeteros-downloads (Last accessed on 17/05/2020)

Digital Ocean (2020). *Digital Ocean*. Available at:

https://cloud.digitalocean.com/marketplace?i=12b9d5 (Last accessed on 17/05/2020)

GitHub (2020) Trail of Bits. *Algo VPN*. Available at:

https://github.com/trailofbits/algo (Last accessed on 17/05/2020)

WireGuard (2019). *WireGuard*. Available at:

https://www.wireguard.com/ (Last accessed on 17/05/2020)

PuTTY (2020). *PuTTY: a free SSH and Telnet client*. Available at:

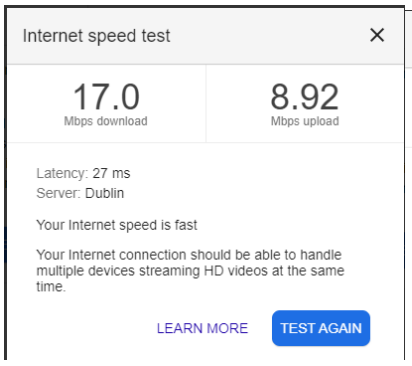
https://www.chiark.greenend.org.uk/~sgtatham/putty/ (Last accessed 17/05/2020)

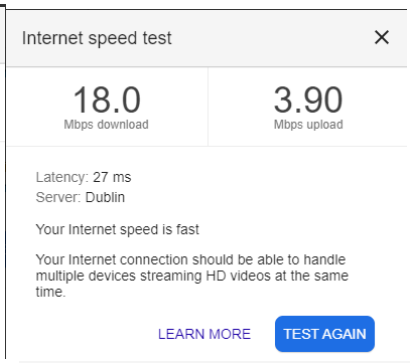
APPENDICES

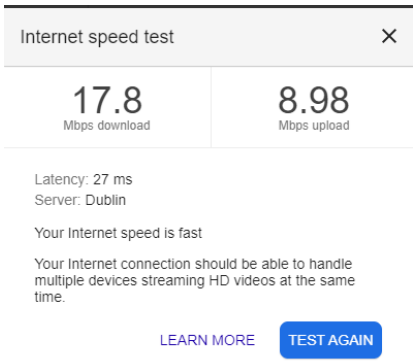
1.1 APPENDIX A – SPEED TEST RESULTS

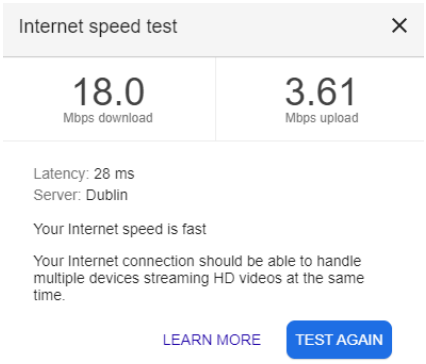
Each screenshot here was taken 3 hours apart

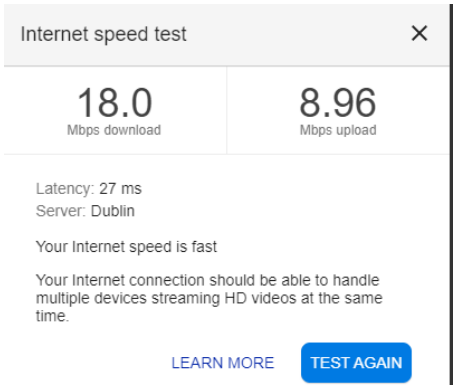
No VPN Results



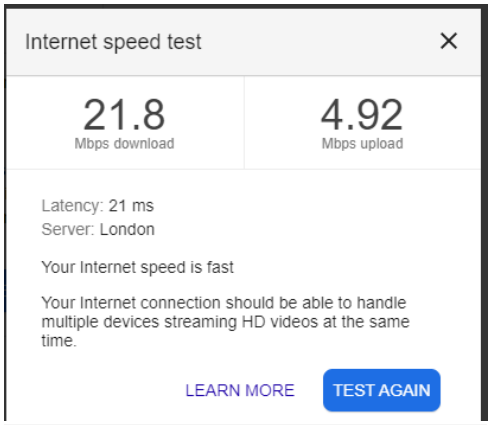


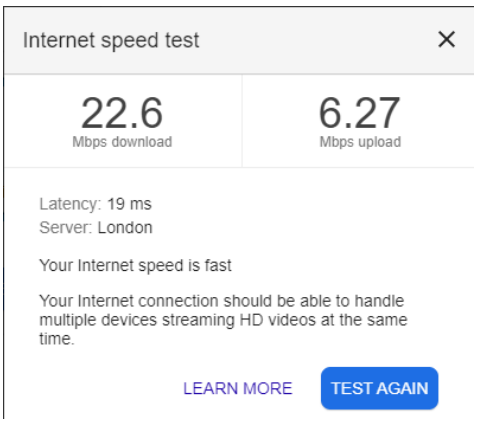


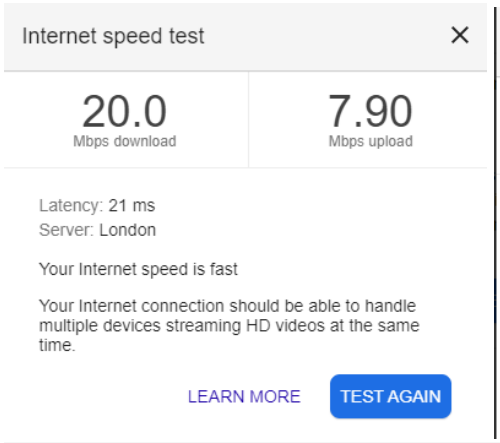


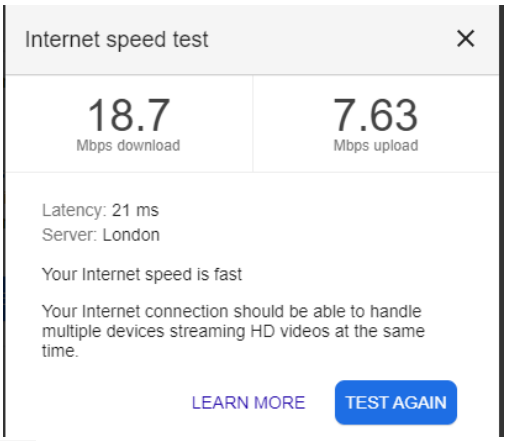


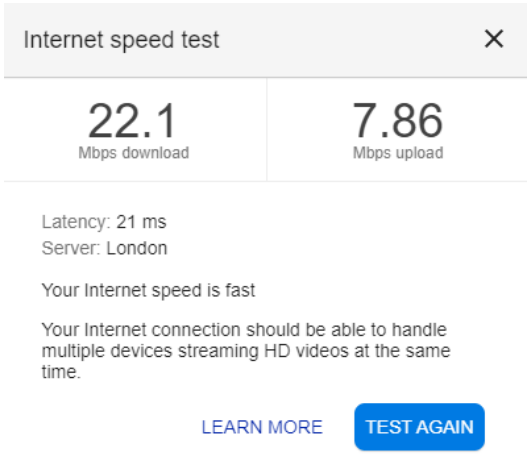
Nord VPN Results



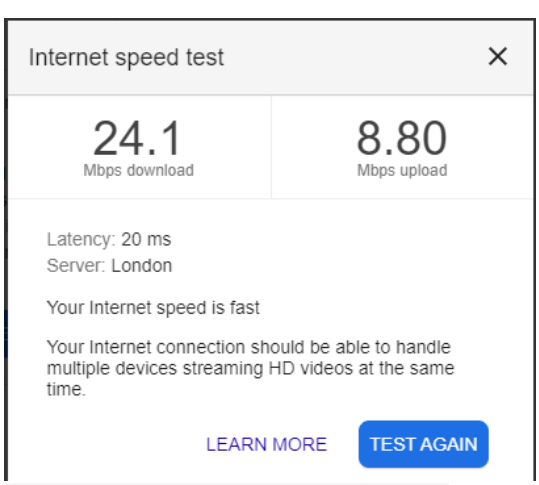


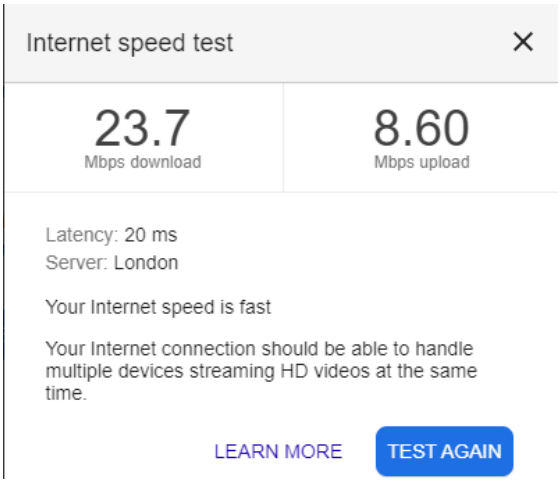


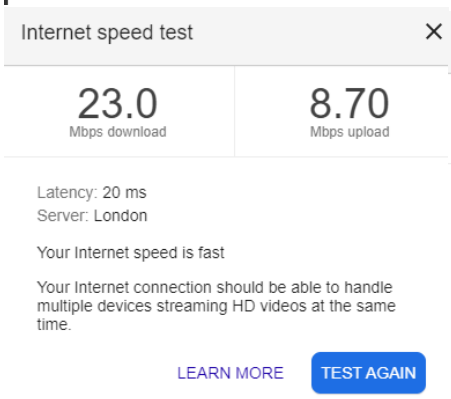


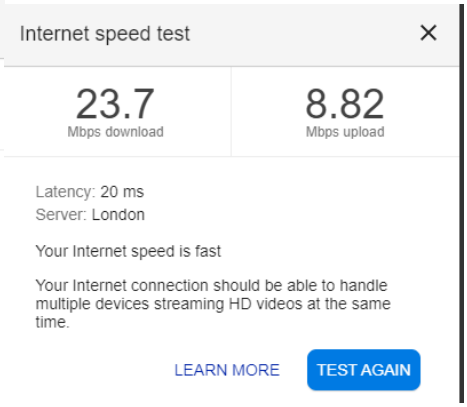


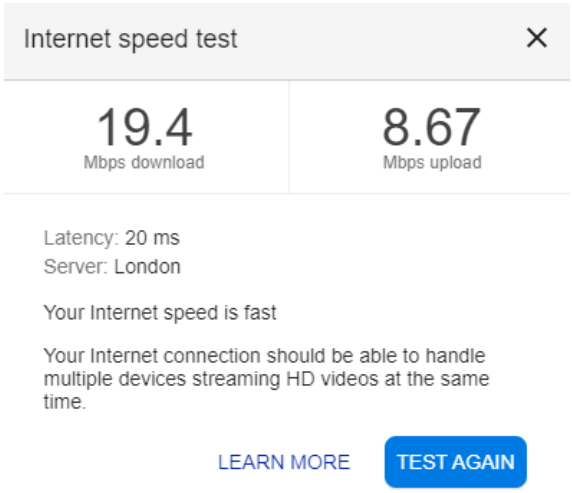
Algo VPN Results





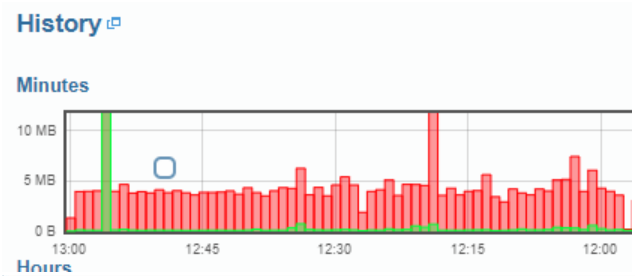


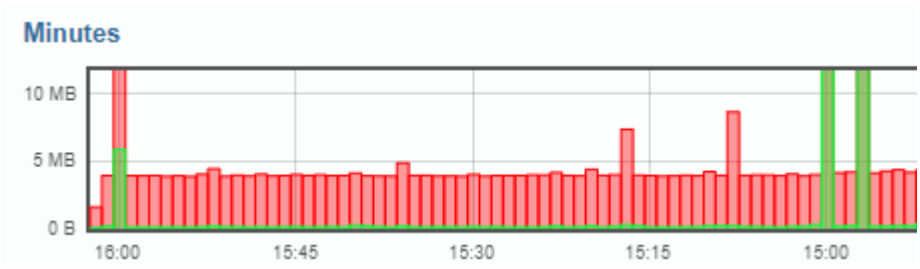


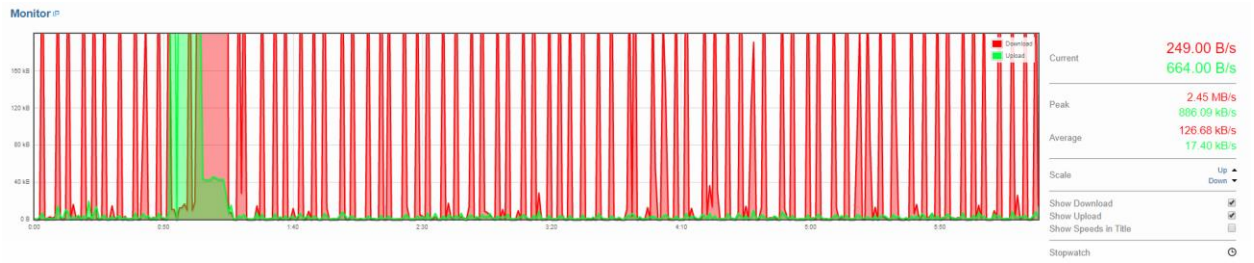


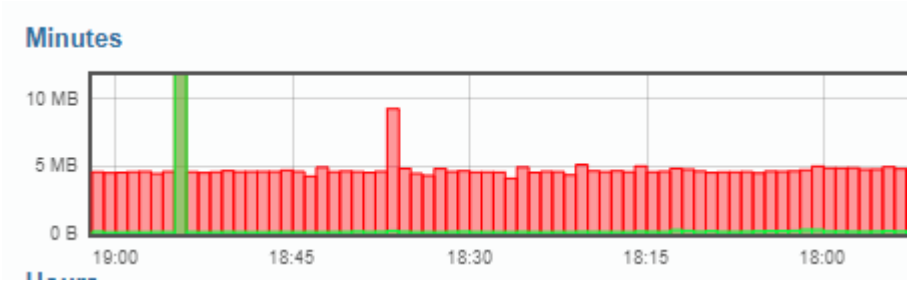
1.2 APPENDIX A – BANDWIDTH USAGE TEST RESULTS

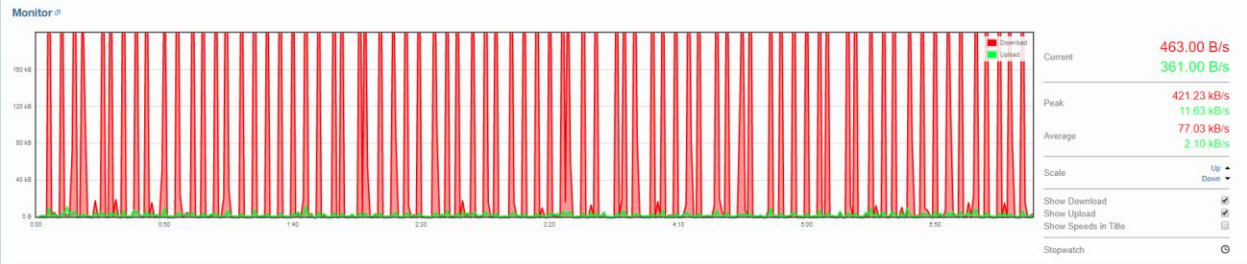
No VPN Results

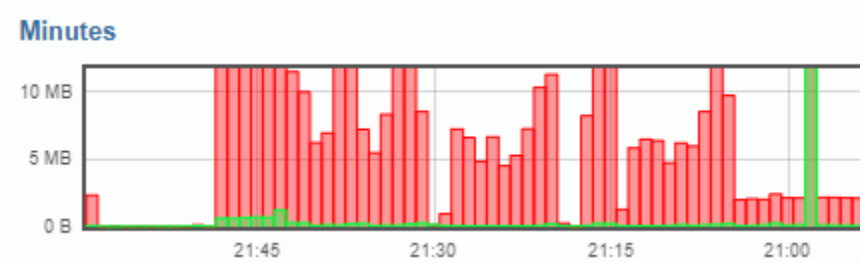


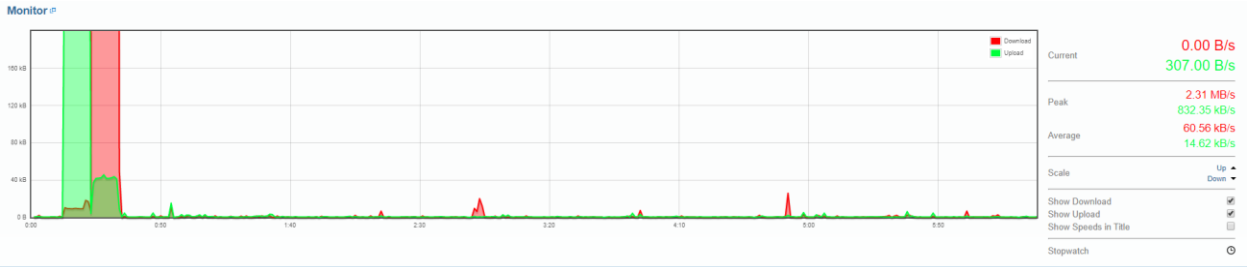


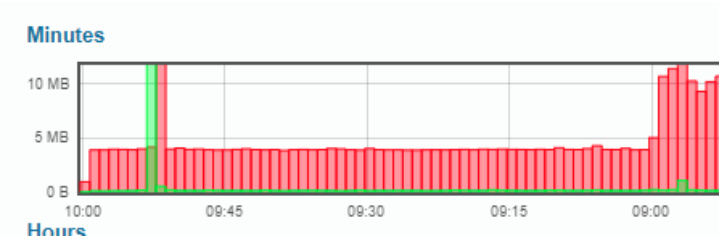


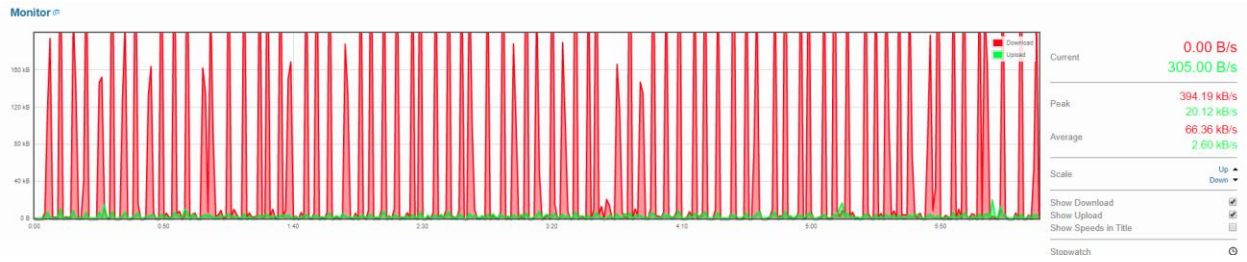




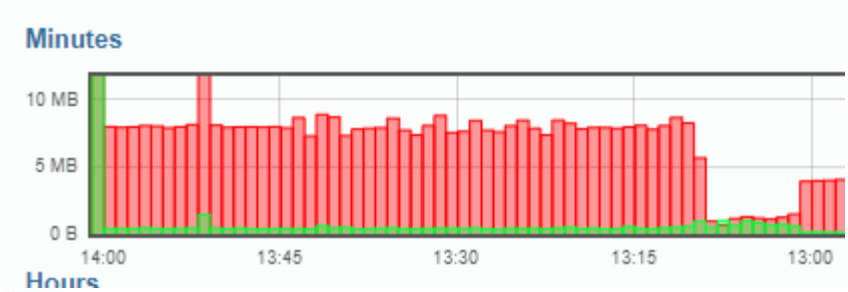


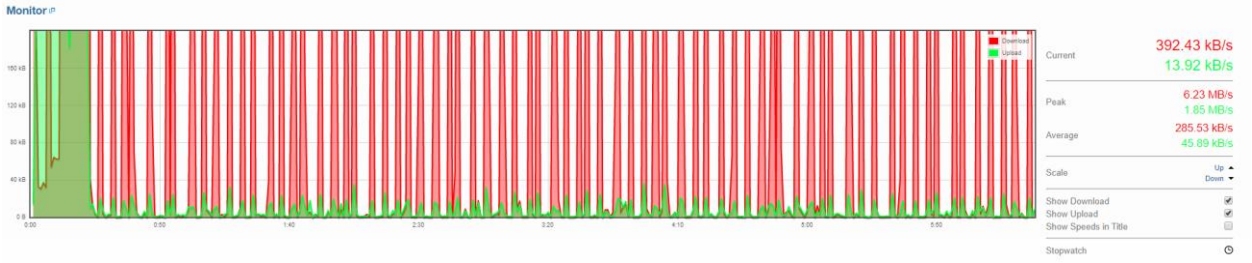


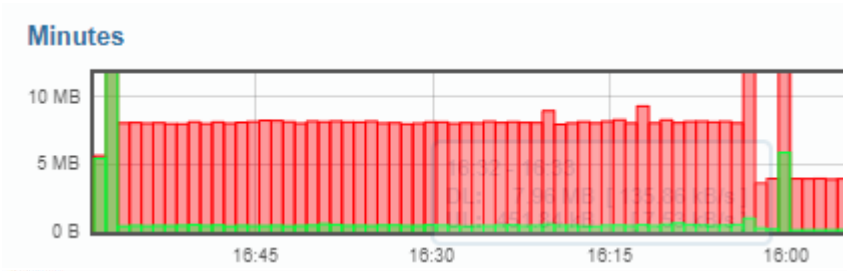


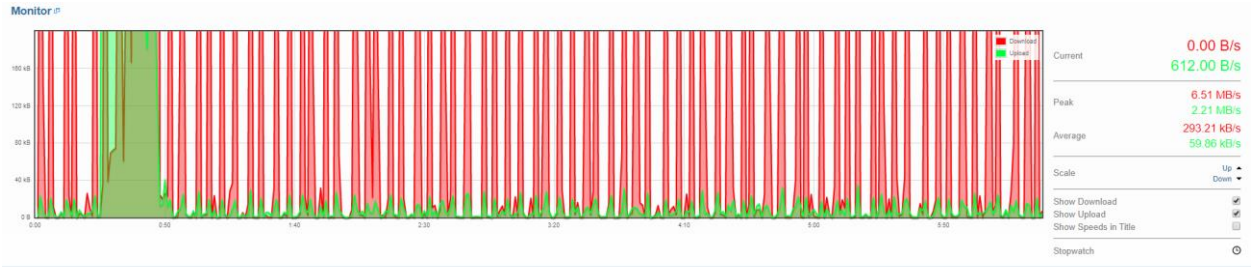


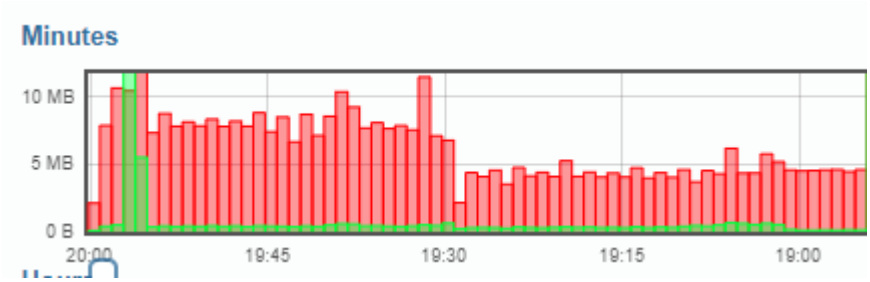
Nord VPN Results

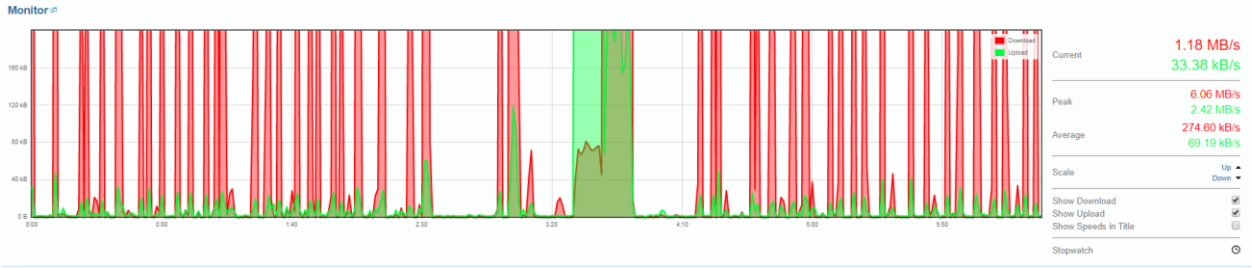

Minutes
10 MB
5 MB
0 B
14:00
13:45
13:30
13:15
13:00

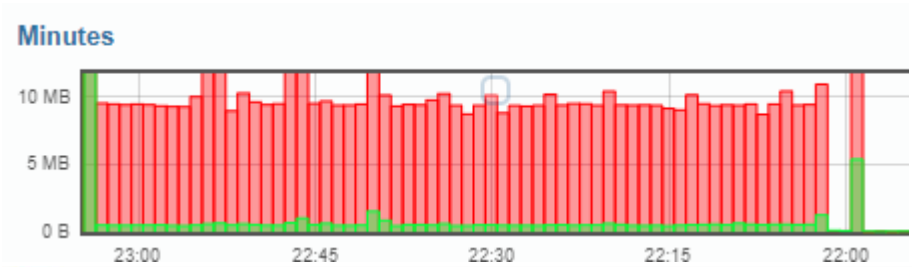

Monitor
Current
392.43 kB/s
13.92 kB/s
Peak
6.23 MB/s
1.85 MB/s
Average
285.53 kB/s
45.89 kB/s
Scale
Show Download
Show Upload
Show Speeds in Title
Stopwatch

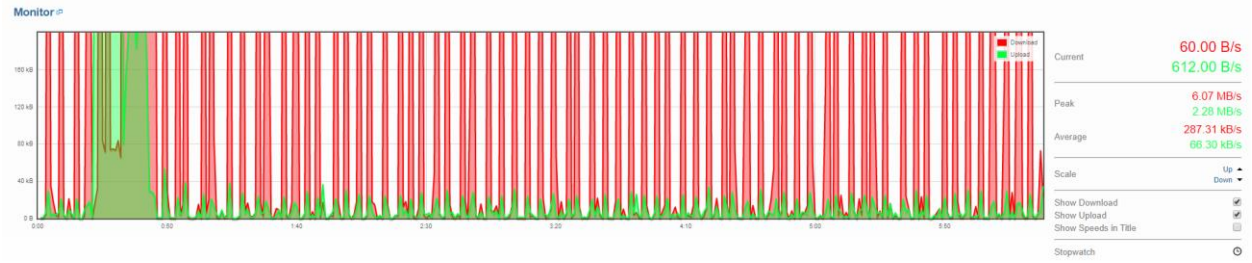

Minutes
10 MB
5 MB
0 B
16:45
16:30
16:15
16:00

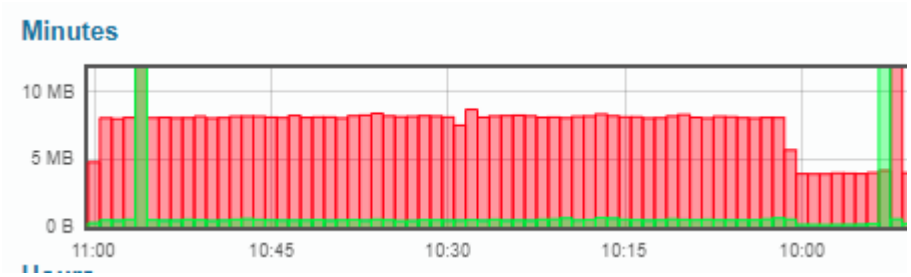

Monitor
Current
0.00 B/s
612.00 B/s
Peak
6.51 MB/s
2.21 MB/s
Average
293.21 kB/s
59.86 kB/s
Scale
Show Download
Show Upload
Show Speeds in Title
Stopwatch

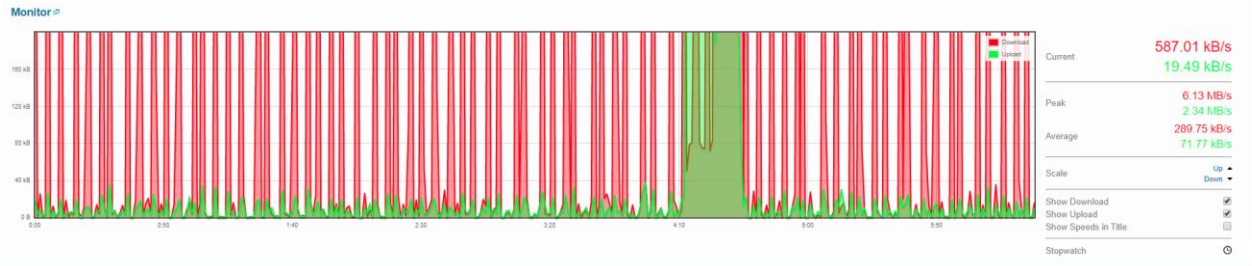

Minutes
10 MB
5 MB
0 B
20:00
19:45
19:30
19:15
19:00


Monitor
Download
Upload
Current
1.18 MB/s
33.38 kB/s
Peak
6.06 MB/s
2.42 MB/s
Average
274.60 kB/s
69.19 kB/s
Scale
Up
Down
Show Download
Show Upload
Show Speeds in Title
Stopwatch

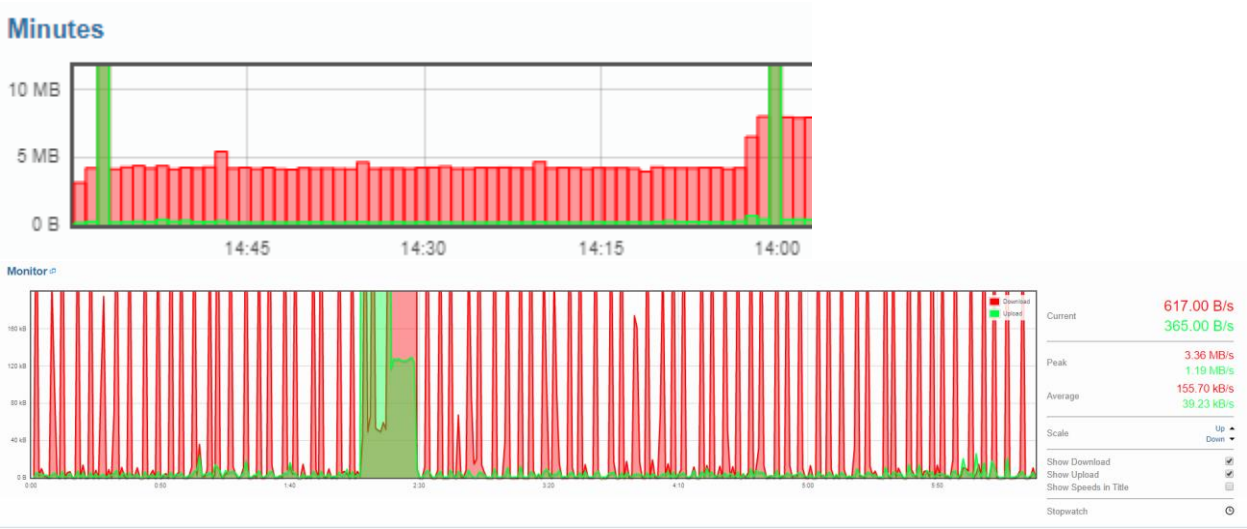

Minutes
10 MB
5 MB
0 B
23:00
22:45
22:30
22:15
22:00

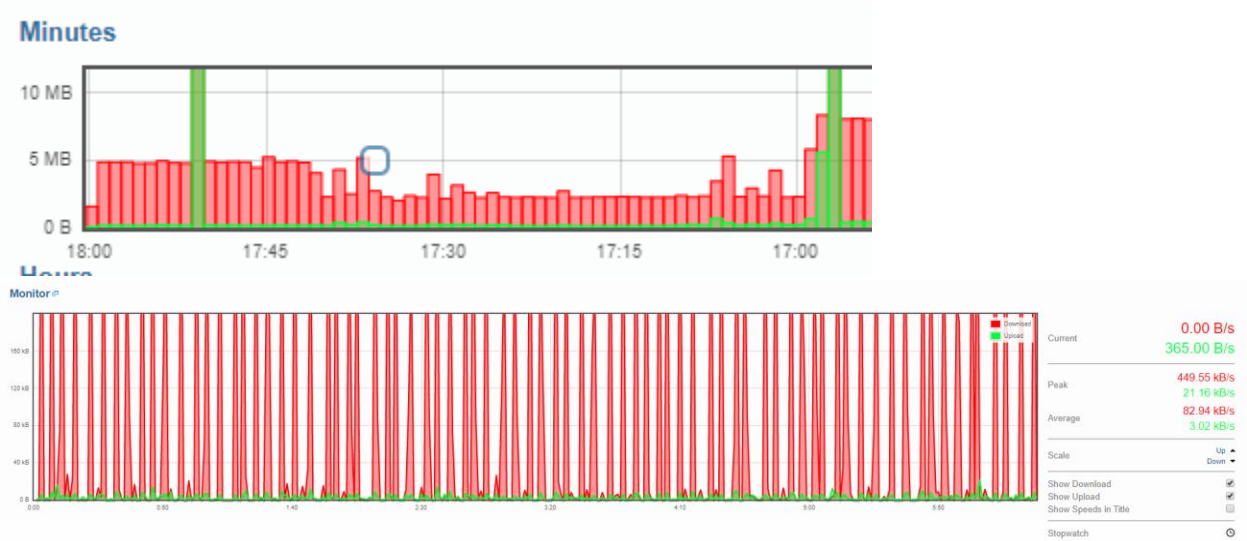

Monitor
Download
Upload
Current
60.00 B/s
612.00 B/s
Peak
6.07 MB/s
2.28 MB/s
Average
287.31 kB/s
66.30 kB/s
Scale
Up
Down
Show Download
Show Upload
Show Speeds in Title
Stopwatch

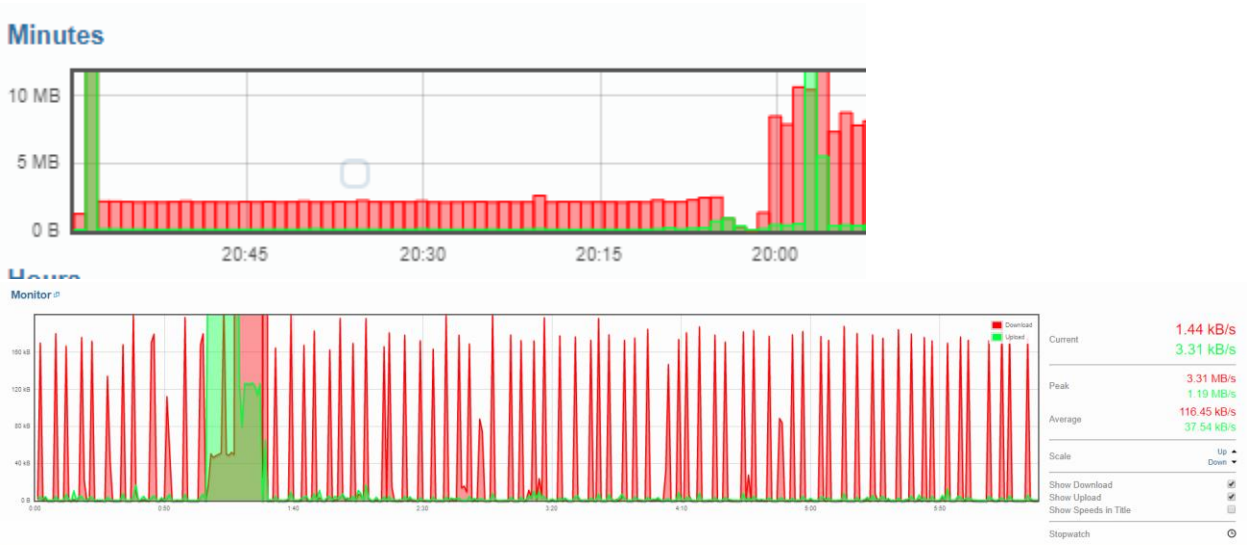

Minutes
10 MB
5 MB
0 B
11:00
10:45
10:30
10:15
10:00

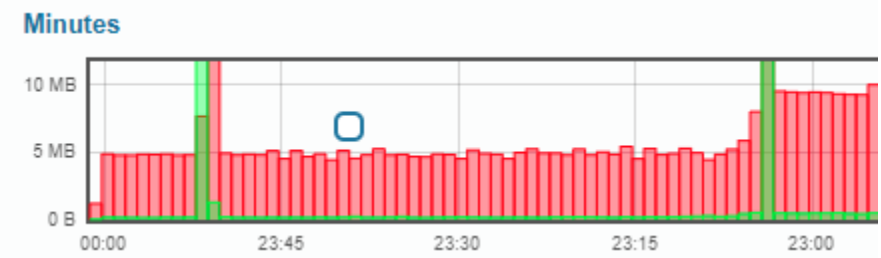

Monitor
Download
Upload
Current
587.01 kB/s
19.49 kB/s
Peak
6.13 MB/s
2.34 MB/s
Average
289.75 kB/s
71.77 kB/s
Scale
Up
Down
Show Download
Show Upload
Show Speeds in Title
Stopwatch

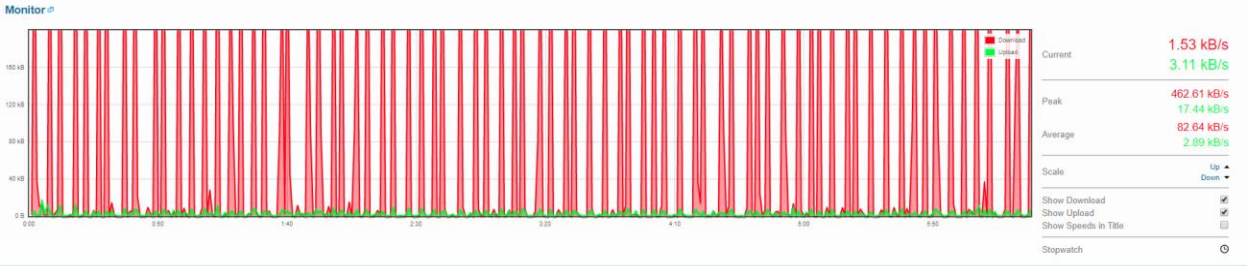
Algo VPN Results

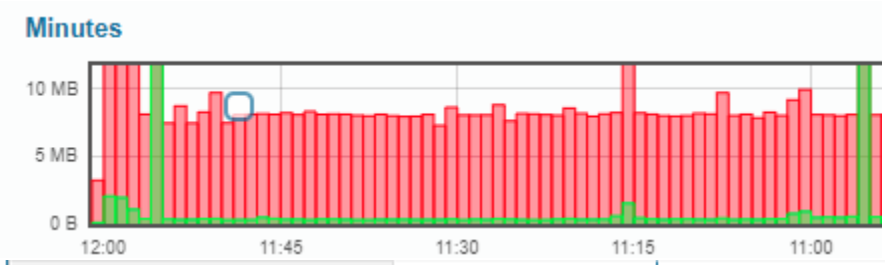












11:00-12:00 19 May 2020	641.92 MB	50.36 MB	692.28 MB
10:00-11:00 19 May 2020	538.00 MB	54.29 MB	592.29 MB
09:00-10:00 19 May 2020	260.73 MB	22.82 MB	283.55 MB

23:00-00:00 18 May 2020	398.57 MB	48.94 MB	447.51 MB
22:00-23:00 18 May 2020	600.36 MB	32.41 MB	632.76 MB

Date	Download	Upload	Combined
21:00-22:00 18 May 2020	363.55 kB	14.64 kB	378.19 kB
20:00-21:00 18 May 2020	160.04 MB	22.00 MB	182.04 MB
19:00-20:00 18 May 2020	426.24 MB	47.46 MB	473.70 MB

Date	Download	Upload	Combined
18:00-19:00 18 May 2020	303.60 MB	21.72 MB	325.32 MB
17:00-18:00 18 May 2020	231.48 MB	25.07 MB	256.54 MB
16:00-17:00 18 May 2020	557.53 MB	53.55 MB	611.07 MB
15:00-16:00 18 May 2020	269.36 MB	22.24 MB	291.59 MB
14:00-15:00 18 May 2020	351.91 MB	41.01 MB	392.92 MB
13:00-14:00 18 May 2020	424.42 MB	28.85 MB	453.27 MB
12:00-13:00 18 May 2020	297.31 MB	24.45 MB	321.75 MB