August 2019

CHECKMARK CERTIFIED

TEST REPORT

Client: AdvancedVPN
Date: 14th August 2019
Project: VPN Evaluation
Document Version: 1.0

Author(s): Scott Markle, Richard Thomas

Contents

Introduction

This test report was created in response to a proposal put forward by AdvancedVPN, hereafter referred to as "the commissioning vendor" or "AVPN", to Checkmark Certified LLC, hereafter referred to as "the Test Lab" or "Checkmark".

As part of the proposal, AVPN requested that the Test Lab examine the functionality and/or efficacy of one of their security solutions, in particular, their AdvancedVPN, hereafter referred to as "AdvancedVPN" or "Solution Under Test (SUT)".

The purpose of this document is to outline the requirements of the test, as agreed with the commissioning vendor, and to provide further detail regarding the test environment, methodology, and finally the outcome of any testing conducted by the Test Lab.

All information contained within this document shall remain the property of the Test Lab. This version of the document supersedes all previous versions.

Test Overview

The specific requirements of the test are outlined below. These requirements are taken from documentation and/or correspondence provided by the commissioning vendor and features common among those products included in this test.

Test Components:

- Baseline VPN Verification – does the VPN solution correctly establish a connection, does traffic correctly route through the VPN.
- Traffic Encryption – with the VPN connection established, does the associated traffic get encrypted or does it remain in a human-readible format.
- VPN IP/DNS Leak – On connection, is the client's public IP address masked, does the client use VPN DNS.
- Traffic Speed – what effect does the VPN have on network traffic speeds.
- Client Footprint – What effect does the client application have on system memory.
- Device Support – Does the server allow concurrent machine connection up to a minimum of 10.
- Location Masking – When connected, does it allow the client access to geographically restricted services.

Test Network

The following test network diagram (Fig 1.0) depicts a brief overview of the test network used in the testing carried out against the SUT.

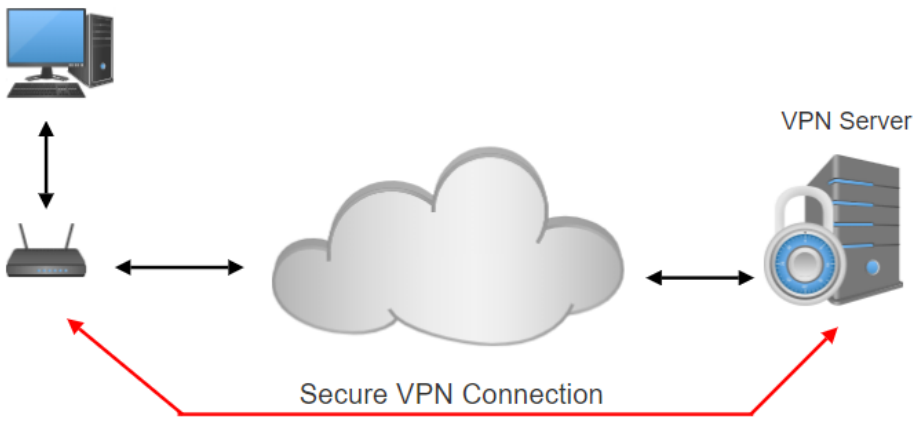


Fig 1.0 – proposed network diagram

Each client was forensically imaged prior to testing, to provide a viable return position in the event any repetition was required. Images were created for each of the following operating systems:

- Windows 10

Furthermore, and as a requirement of the test, each of the above operating systems was patched to the latest version available at the time of installation/configuration.

Test Cases and Results

The following test cases are based on the requirements of the commissioning vendor as communicated to the Test Lab.

Test Case 01 – TC01 – Baseline VPN Functionality Verification

The SUT correctly routes traffic through the VPN.

As a minimum, testing will verify that the VPN client/server does, in fact, establish a secure point-to-point tunnel. Failure at this point renders all successive testing void.

Outcome: As a basic test of its functionality, AdvancedVPN was able to correctly establish a tunnel between the endpoint and server; with the SUT responding quickly to the connection being turned on/off within the GUI.

Result: PASS

Test Case 02 – TC02 – Traffic Encryption

On connection, the SUT sufficiently encrypts all associated network traffic.

Once the VPN client has established, a variety of data will be passed over the connection with software capturing all associated network traffic. The traffic captures will then be reviewed to verify that, as a minimum threshold, the data is no longer in a human readable format.

Outcome: The scenario used for the testing of the SUTs encryption functionality catered around the protection of user information when browsing common social media sites and during basic file download tasks. In each case, the traffic was recorded, examined, and found to be correctly obfuscated.

Result: PASS

Test Case 03 – TC03 – VPN IP/DNS Leak

The SUT correctly masks the client IP address and routes DNS lookups through a secured server.

With traffic verified as routing through the secured connection and in an encrypted state, this test case will verify that the client's public facing IP address is being correctly masked.

Secondary testing will then also establish whether the SUT is routing DNS lookups through the secure connection or is using the standard/ISP DNS server information.

Outcome: AdvancedVPN provides (at time of testing) the option of switching between VPN servers in one of 28 different countries, with several offering further options by city. A cross-section of 20 of these was tested for DNS and IP leaks, in each case the public facing address and was masked and DNS traffic re-routed to those servers used by the SUT. Furthermore, each VPN server was checked for susceptibility to WebRTC IP leaks.

Location	Public IP Mask	DNS Re-routed	WebRTC Leak
US	✓	✓	✓
UK	✓	✓	✓
Belgium	✓	✓	✓
Spain	✓	✓	✓
Latvia	✓	✓	✓
Romania	✓	✓	✓
Israel	✓	✓	✓
Ireland	✓	✓	✓
Moldova	✓	✓	✓
Sweden	✓	✓	✓
Hungary	✓	✓	✓
Lithuania	✓	✓	✓
Finland	✓	✓	✓
Netherlands	✓	✓	✓
Germany	✓	✓	✓
Canada	✓	✓	✓
Norway	✓	✓	✓
UAE	✓	✓	✓
Saudi Arabia	✓	✓	✓
Czech Republic	✓	✓	✓

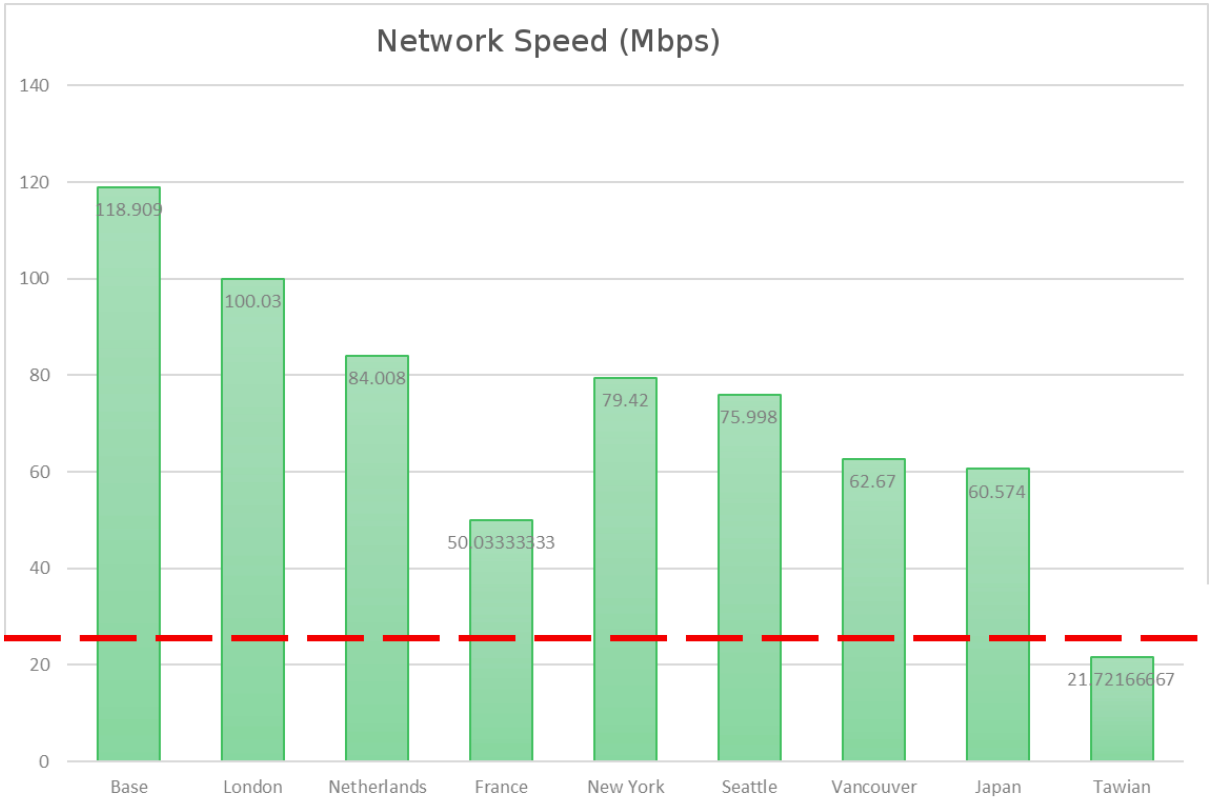
Test Case 04 – TC04 – Traffic Speed/Network Lag

Measure the effect the SUT has on network connection speeds, packet loss, and general network performance.

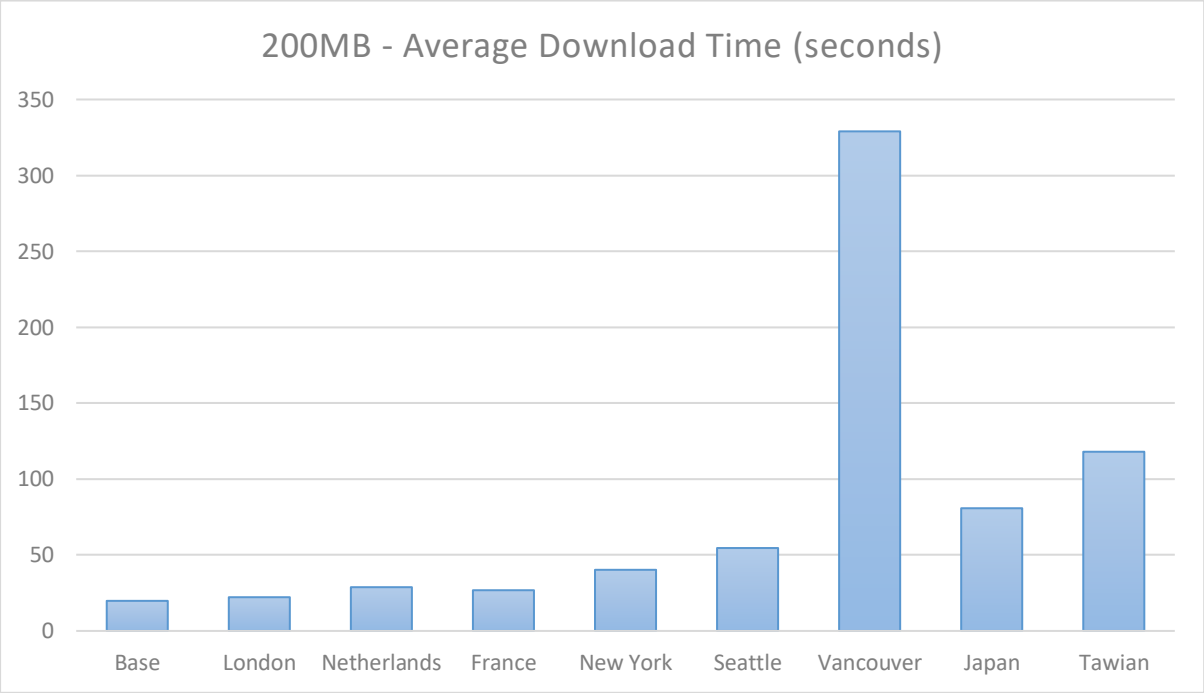
This test will examine the effect that the SUT has on network bandwidth levels and whether this effect would introduce problems in carrying out common Internet activities such as video or music streaming and gaming.

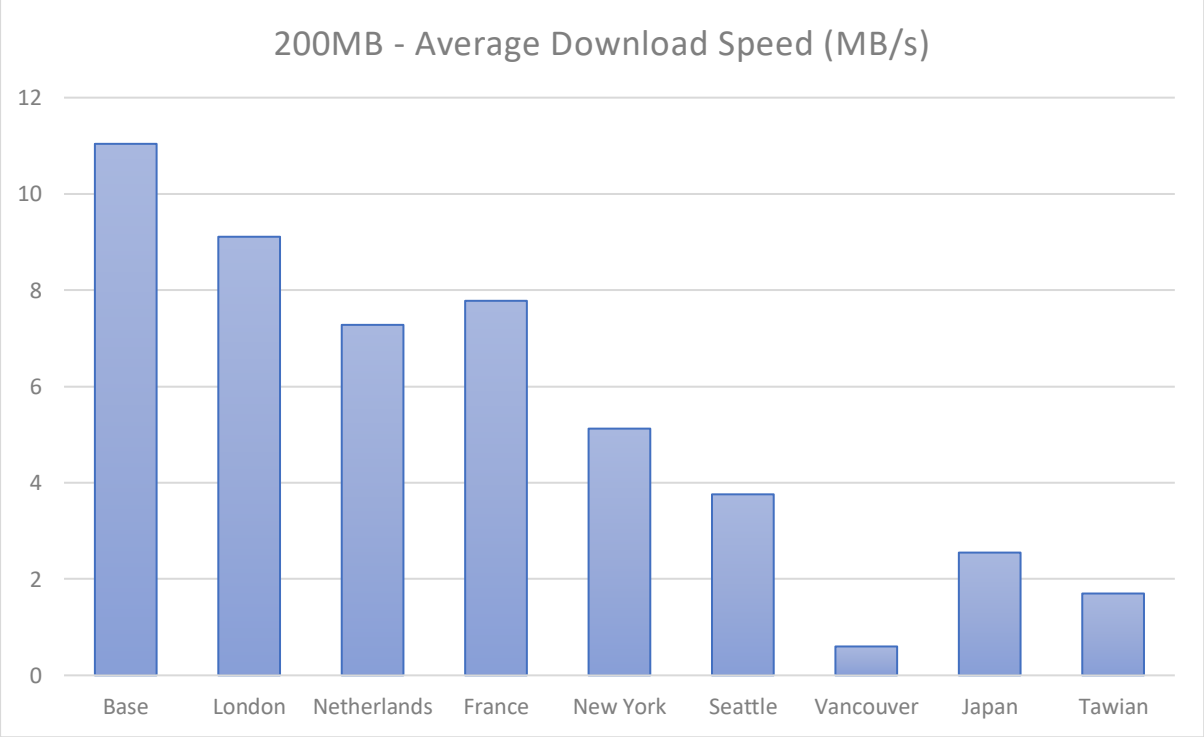
Outcome: Eight of the available VPN servers were selected with an increasing distance from the test location (UK for this test). For each location network speeds and download times were measured, using proprietary tools, with an average calculated.

The chart below displays the average speeds when tested against local regionalised servers, with the red line used as an average benchmark (approximately 25Mbps) for the network speed required for streaming high definition video, audio, and gaming.



After testing against specific regionalised servers, the following charts depict the results of testing against a single fixed server. The first chart displays the average time taken to download a 200MB file. The second chart shows the average download speeds recorded for the same file.





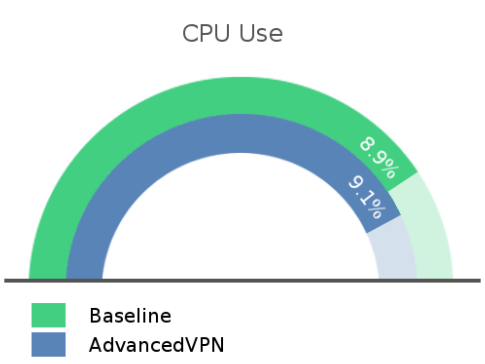
Test Case 05 – TC05 – Client Footprint

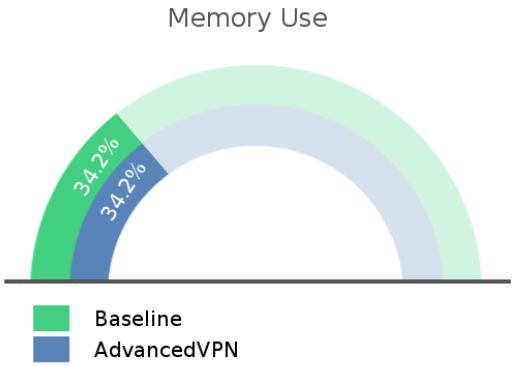
Measure the effect the SUT has on system memory use.

This test will establish where the SUT introduces a noticeable impact on system memory usage. Before connecting to the VPN, measurements will be taken for both CPU and memory use while streaming online video content.

The VPN connection will then be established, the same content loaded, and the same metrics recorded. The data will then be compared to establish what impact the SUT has on general performance.

Outcome: AdvancedVPN was found to have, in comparison to the specification of the machine used in testing, a very small footprint. On average, the SUT introduced an increase of 0.2% CPU use while the impact on memory use was negligible at 241MB.





Test Case 06 – TC06 – Device Connection Limits

Verify whether the SUT has a concurrent connection limit of 10 or fewer.

This test examines the vendor claim that the SUT provides support for more than the average of 6 found in similar VPN providers. Devices will be connected individually, with the continued connection being verified on each existing device as each new device is connected. For the purposes of this test, the device limit will be set at 10 so as to establish a clear threshold.

Outcome: Testing found that, with devices being added 1 by 1, the SUT was able to accommodate 10 simultaneous device connections.

Test Case 07 – TC07 – Location Masking

The SUT masks the geographical location of the client and allows access to region locked services.

This test will be conducted in two stages. The first stage will verify that the VPN connection correctly masks the client's geographical location. Connections will be established and terminated to determine that the location is not reset on disconnection.

The second stage will test that region locked services, previously blocked from the client, are now available. Services will be checked on consecutive connections and not limited to Netflix, Hulu, and Amazon Prime Video.

Outcome: Of the locations available, a cross-section of 20 was selected and each VPN server connected to in-turn. Once each tunnel was established, a variety of online and local tools were used to determine to apparent location of the desktop. Testing found that, while specific locations such as city/town may vary, the servers were all proven to mask the actual location of the test machine.

Location	Mask	Location	Mask
US	✓	Hungary	✓
UK	✓	Lithuania	✓
Belgium	✓	Finland	✓
Spain	✓	Netherlands	✓
Latvia	✓	Germany	✓
Romania	✓	Canada	✓
Israel	✓	Norway	✓
Ireland	✓	UAE	✓
Moldova	✓	Saudi Arabia	✓
Sweden	✓	Czech Republic	✓

Disclaimer

While Checkmark Certified is dedicated to ensuring the highest standard of security product testing in the industry, it is never possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose. Therefore, the test results published within any given report should not be taken and accepted in isolation.

Potential customers interested in deploying any particular product tested by Checkmark Certified should seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations. All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability.

Checkmark Certified provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.