NVIS INVISIBLE INTERNET

Network Operational Tests

Abstract

This documents tests to verify the NVIS SDP performance and invisibility in connected and disconnected states

Phil Smith, CTO

phils@nvis.info

Contents

What NVIS does

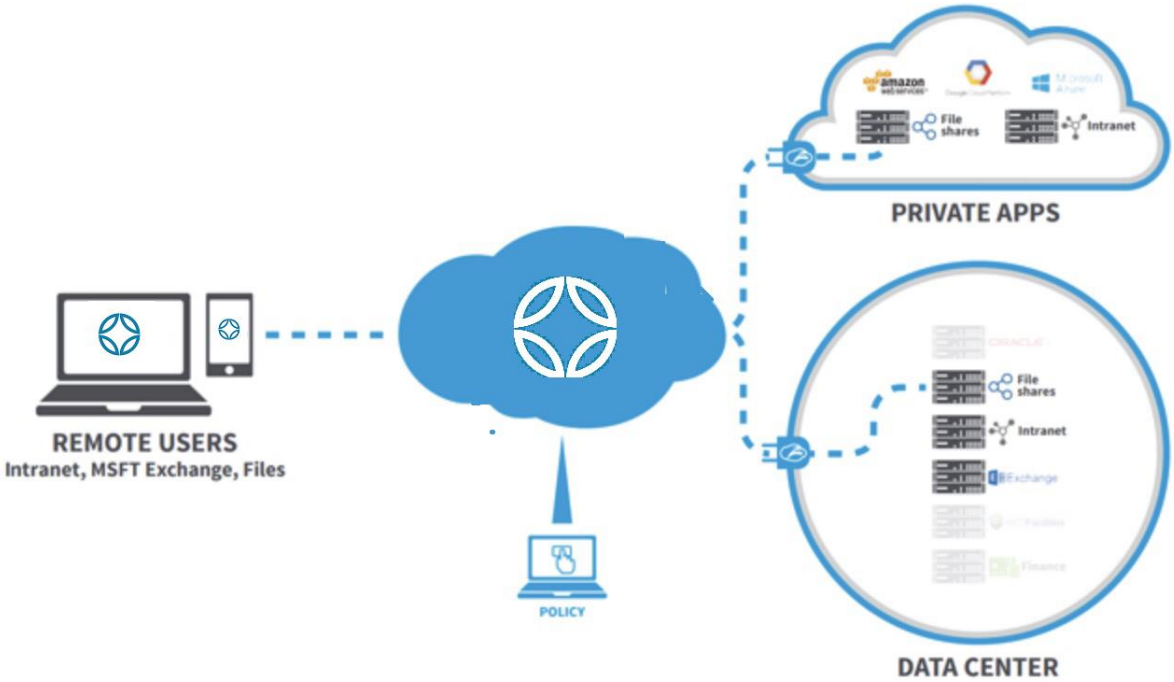
Hackers can't hack what they can't see.

- ✓ NVIS lets you create your own personal "invisible internet" that can't be hacked, blocked, traced or censored due to Layer 2 encryption.
- ✓ NVIS is an SDP (Software Defined Perimeter) that lets you rapidly create a private cloud of nodes (laptops, computers, smartphones, devices) you want to connect.
- ✓ With Intelligent Auto-Provisioning, it's easier, simpler to setup than a VPN, but offers better security and less complexity.
- ✓ NVIS can do things a VPN can't, like encrypted full-stack protection and nodes can talk to each other, peer-to-peer.

Nodes can be anywhere in the world but operate as one network and members can't be geolocated.

Test Overview

These tests show invisibility using NVIS on a Windows laptop to connect to a web server in a private cloud. In this case, our test network tlcnet. Policy is managed by the customer's network administrator and Intelligent Provisioning Agent.



Test Procedures

Quick install

An administrator can remotely install NVIS or email the user the instructions and assigned (Ethereum) address via their myNVIS portal for multi-platform downloads (Windows, Android, MacOSX, Linux). For this Windows test, here is a shortcut:

Download https://nvisnet.com/dist/nvis_windows_inst_beta_0.5.3.0-64bit.exe

Install nvis_windows_inst_beta_0.5.3.0-64bit.exe -a <address>

This makes it easier for administrators to do remote installation via PowerShell or other automation tools.

The Provisioning Agent will automatically assign the network configuration using the assigned address which is the Universal Identity.

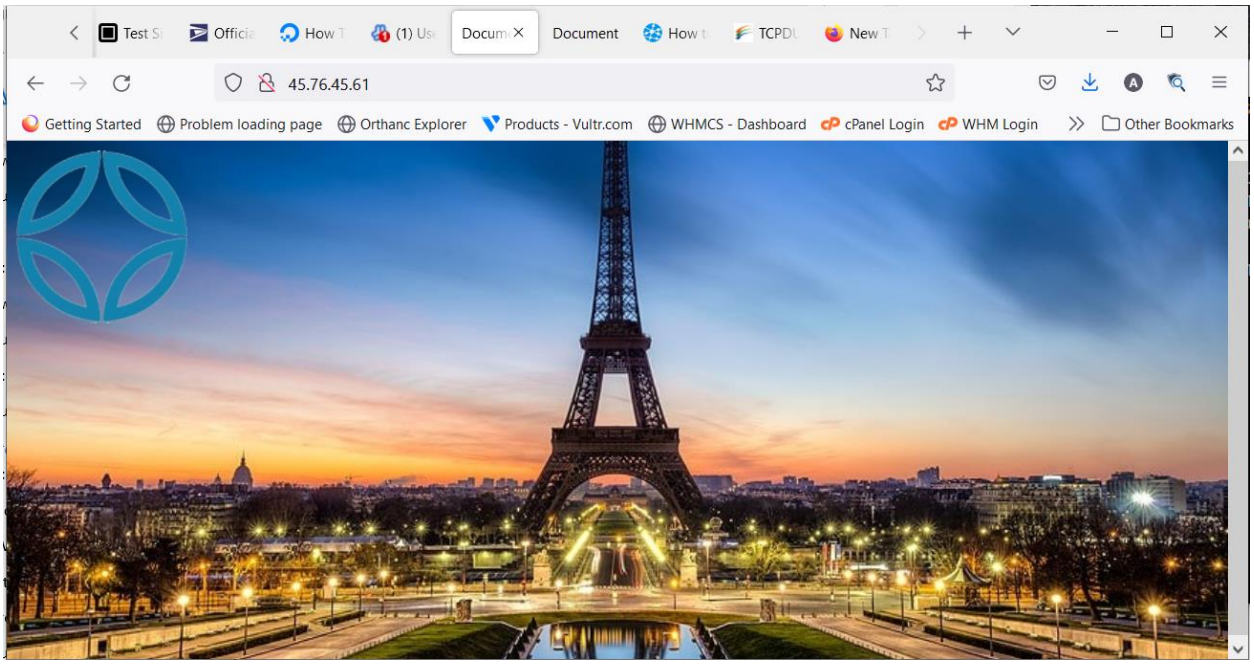
Display a host inside the customer network

Client connects to services and websites on their company network wen NVIS is on:

Test 1: Open the test webhost in Paris via the unencrypted public IP

Browser to http://45.76.45.61 or ping 45.76.45.61

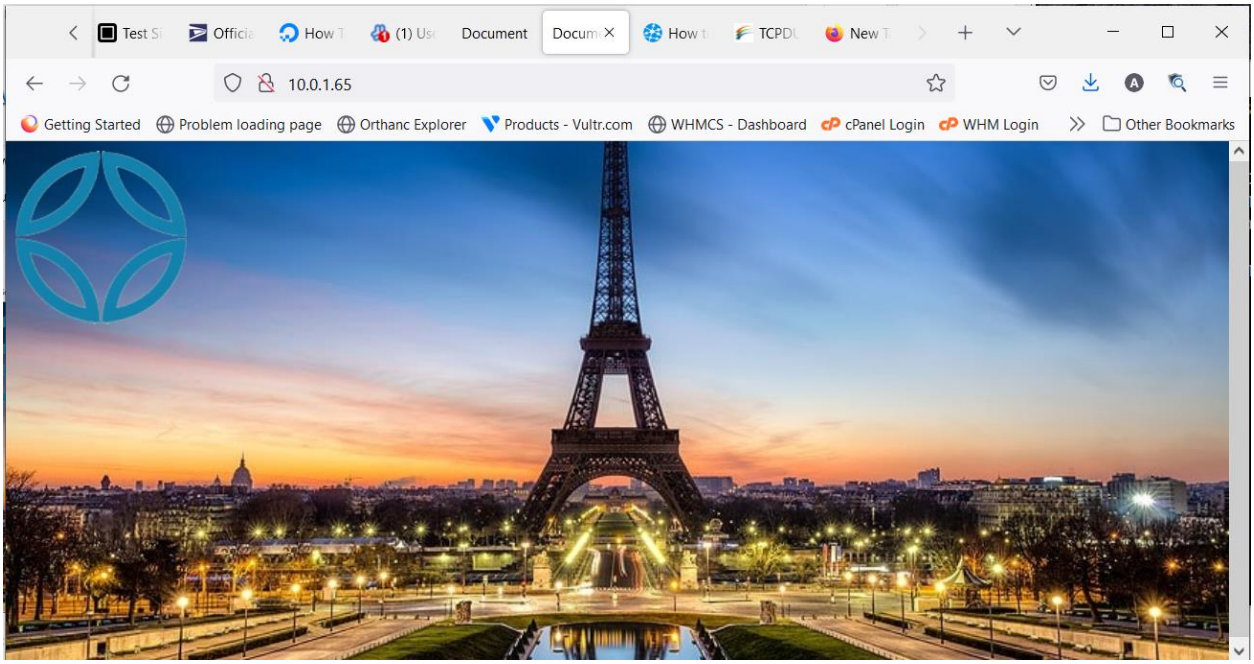
Result: Output is normal.



Test 2: Open the test webhost in Paris via the encrypted NVIS IP when NVIS is ON:

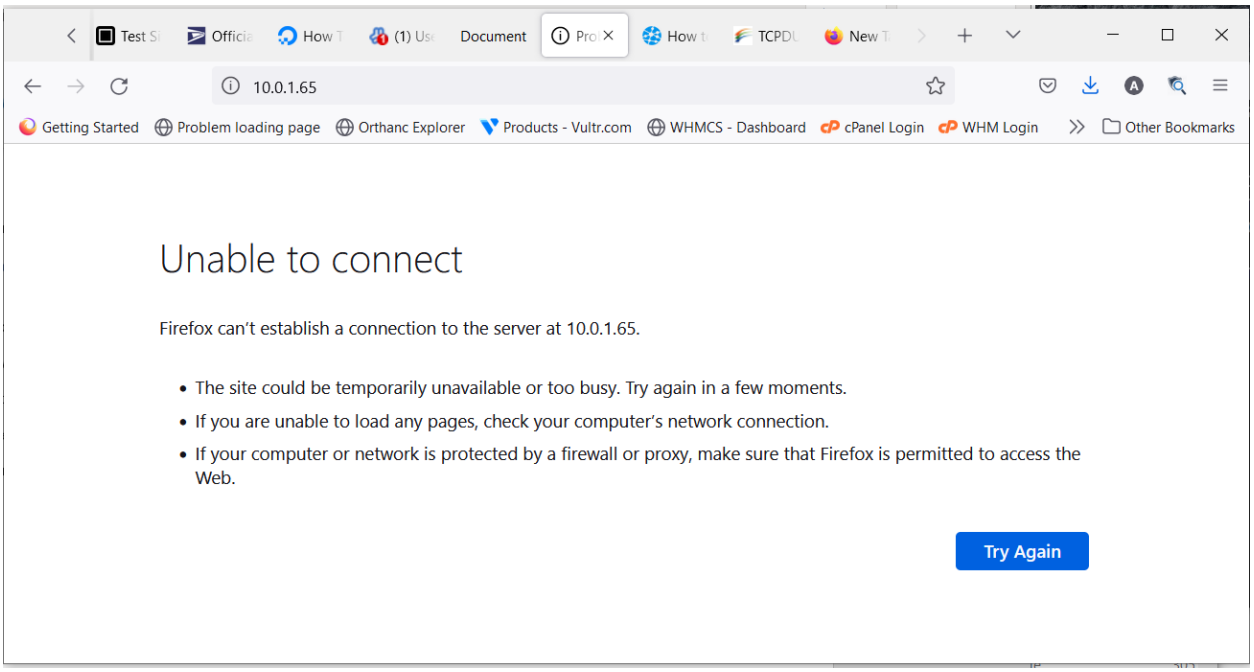
Browser to http://10.0.1.65 or ping 10.0.1.65

Result: Output is normal.



Test 3: Repeat Test 2 with NVIS OFF:

Result: Output shows timeout / failure for browser and ping.



Wireshark Test

Test 4: Try to capture traffic on the public IP address for Paris

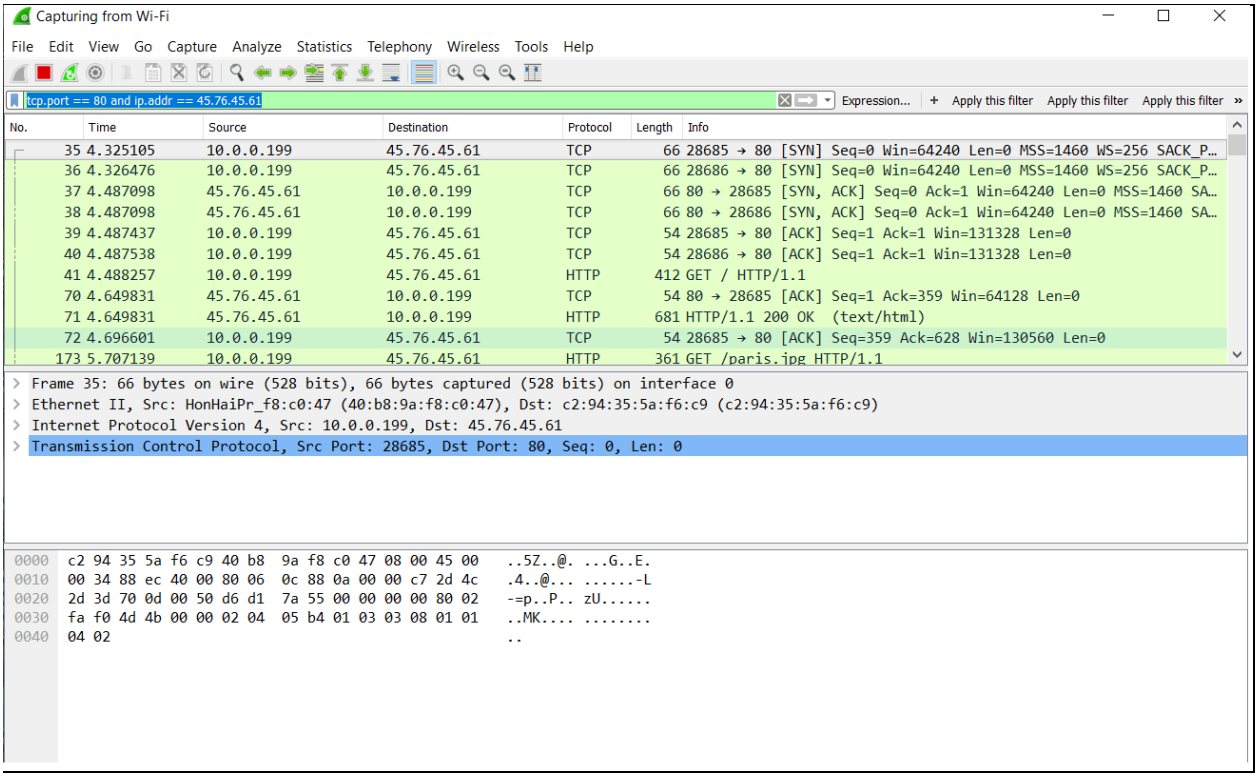
Select Wireshark capture device to the WIFi Adapter

Set Wireshark filter to tcp.port == 80 and ip.addr == 45.76.45.61

Start capture

Refresh browser http://45.76.45.61

Result: Output shows HTTP and TCP packets.



Test 5: Try to capture traffic on the NVIS IP address for Paris (invisibility test)

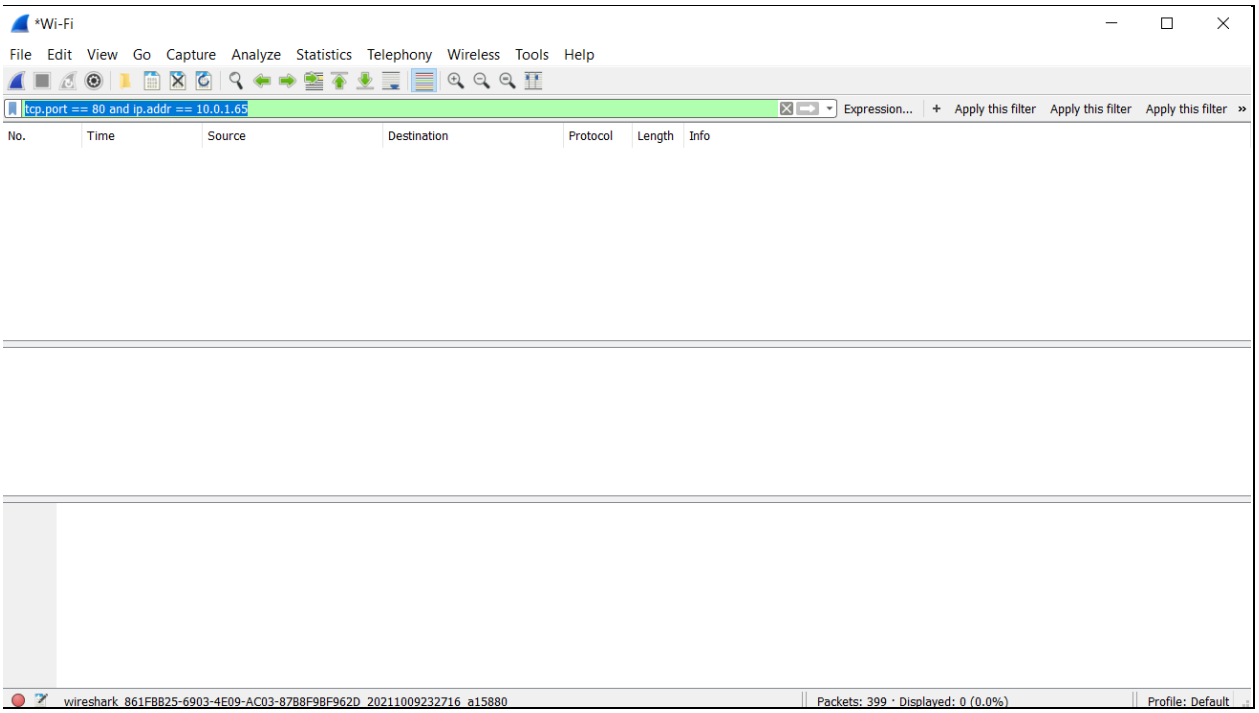
Make sure NVIS ON

Set Wireshark filter to tcp.port == 80 and ip.addr == 10.0.1.65

Start capture

Refresh browser http://10.0.1.65

Result: No output showing traffic from 10.0.1.65



Tcpdump Tests

Make sure NVIS is ON

Run cmd.exe as Administrator

Find the WiFi Adapter Device number: tcpdump -D (in this case, **6** is the 802.11ac network adapter)

Test 6: Look for public IP packets

From the command line, capture raw output to find packets from the public IP:

tcpdump -i 6 -s96 -w traffic.txt

Refresh browser http://45.76.45.61

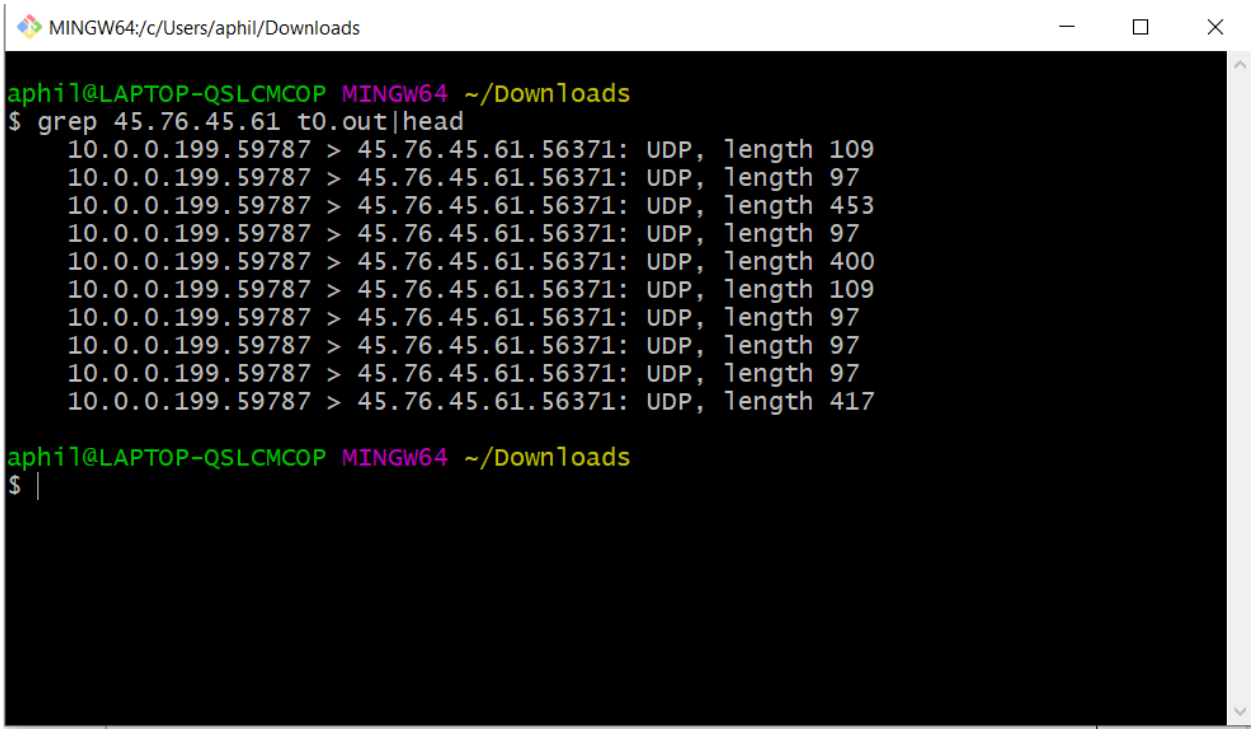
Press ctrl-C from the command window to end the capture

Extract IP header infro

tcpdump -e -nn -vv -r traffic.txt > t0.out

Search for the IP address in the capture log, e.g., grep 45.76.45.61 t0.out

Result: Output shows many packets from IP 45.76.45.61



Test 7: Look for public IP packets (invisibility test)

From the command line, capture raw output to find packets from the NVIS IP:

tcpdump -i 6 -s96 -w traffic1.txt

Refresh browser http://10.0.1.65

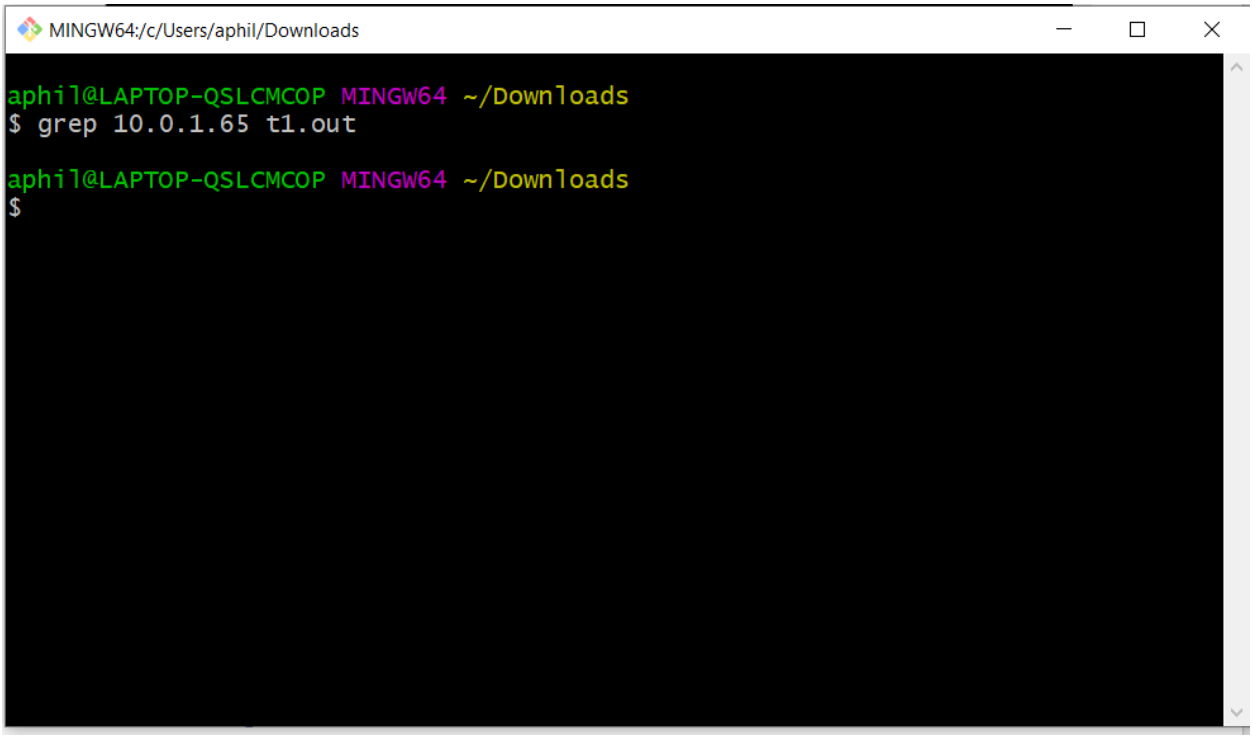
Press ctrl-C from the command window to end the capture

Extract IP header infro

tcpdump -e -nn -vv -r traffic1.txt > t1.out

Search for the IP address in the capture log, e.g., grep 10.0.1.65 t1.out

Result: Output shows no packets from 10.0.1.65



Port Scanning

Test 8: Port Scanning with NVIS ON

Turn NVIS ON

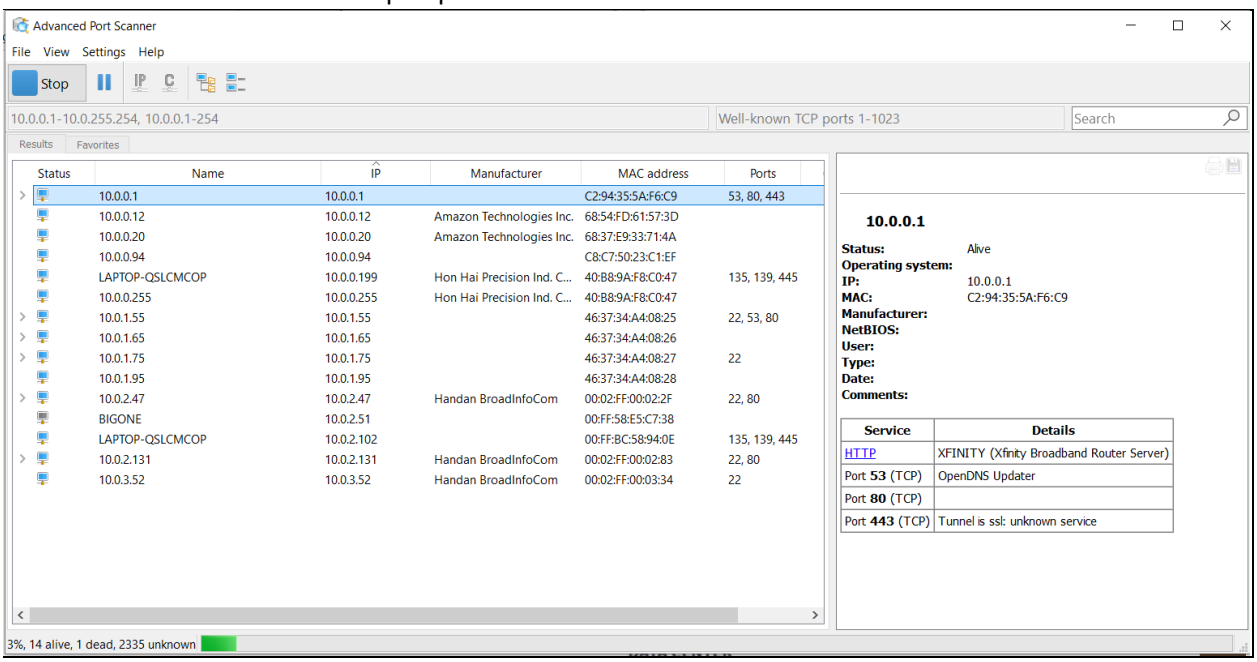
Launch Advance Port Scanner

Set filter to: 10.0.0.1-10.0.255.254, 10.0.0.1-254

Press Scan

Press Stop after 2 minutes

Result: shows tlcnet hosts and open ports:



Test 9: Port Scanning with NVIS OFF

Turn NVIS OFF

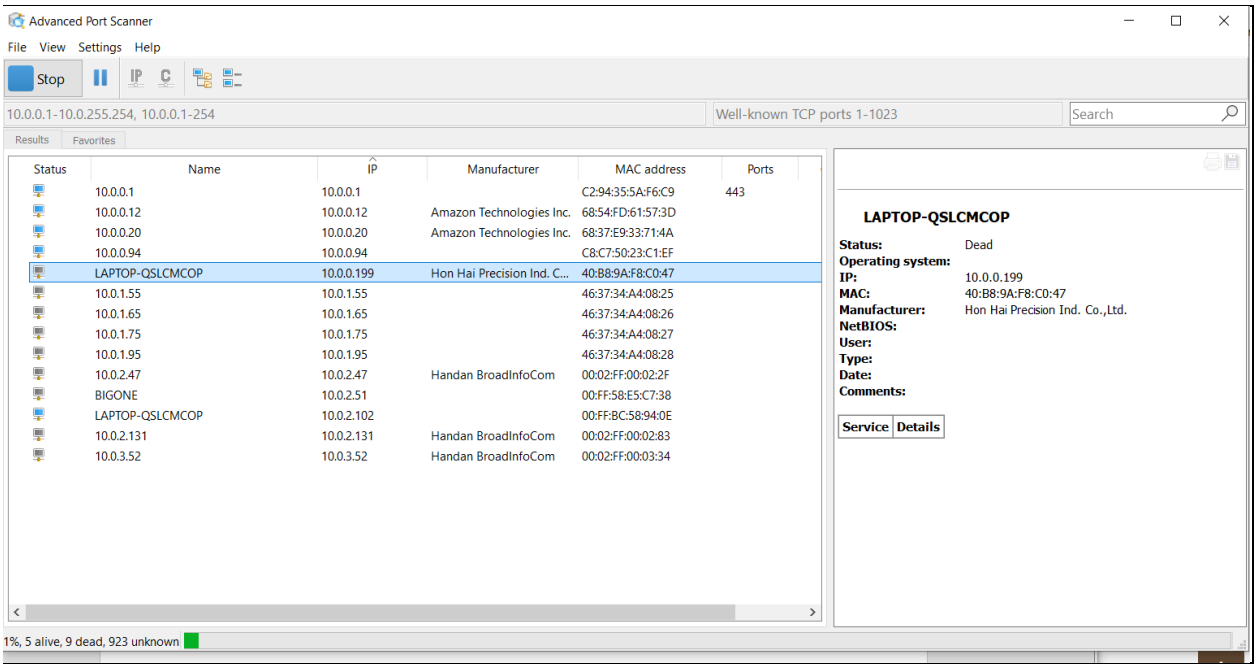
Launch Advance Port Scanner

Set filter to: 10.0.0.1-10.0.255.254, 10.0.0.1-254

Press Scan

Press Stop after 2 minutes

Result: shows tlcnet hosts but NO open ports:



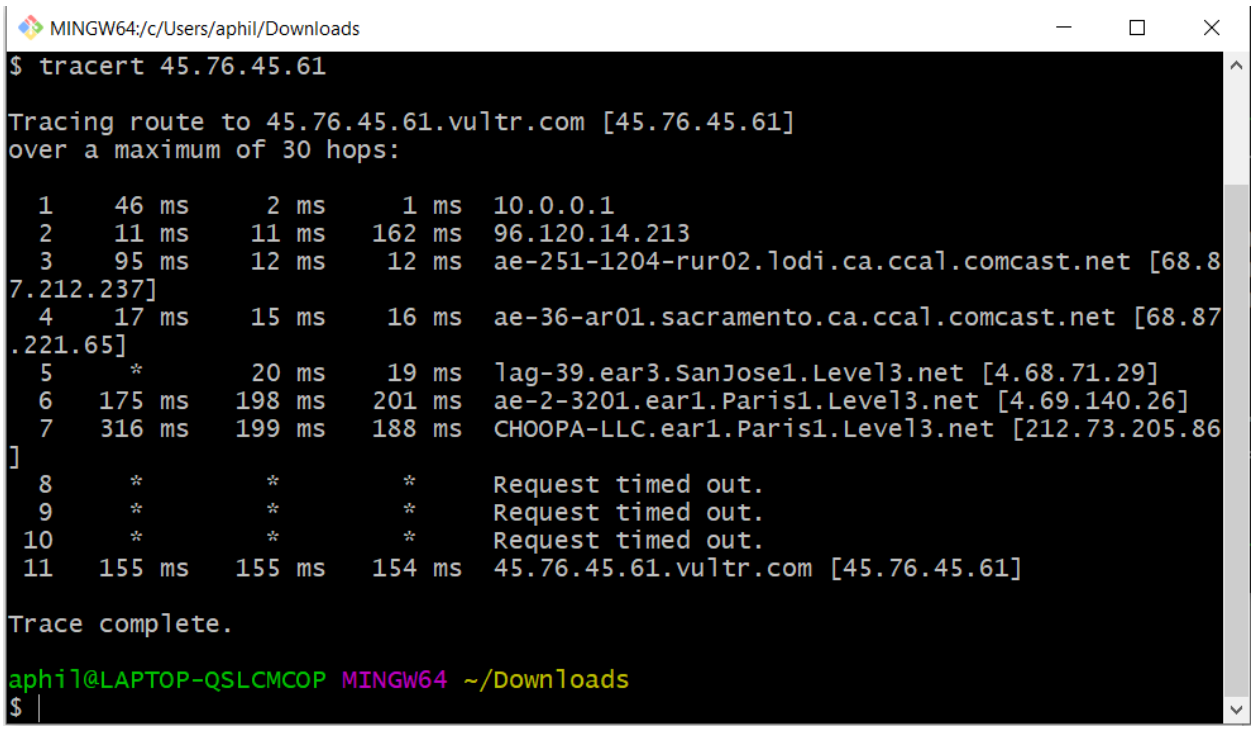
Performance Tests

Route Cost Test

Test 10: Show routes and transit delays to the Paris node when using the public Internet.

tracert 45.76.45.61

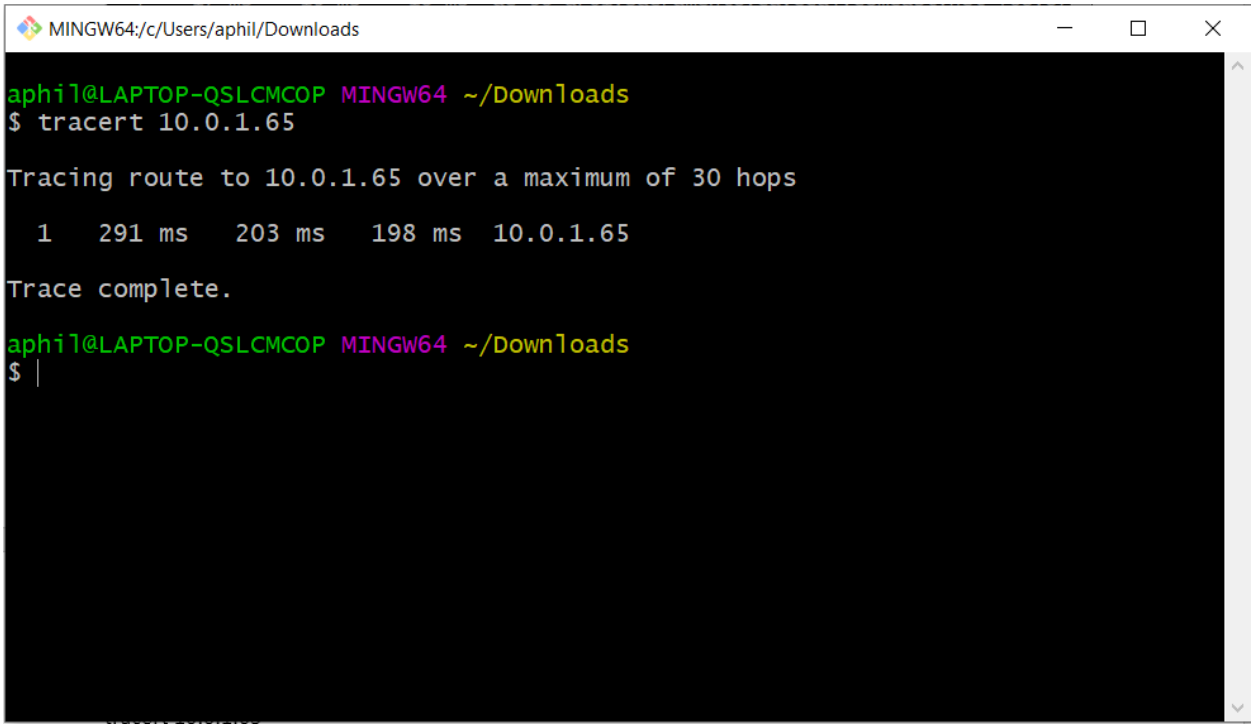
Result: several hops and packet delays seen.



Test 11: Show cost to reach Paris via the NVIS network:

tracert 10.0.1.65

Reesult: Output shows significantly less round trip time to reach the same host without multiple hops:



File Download Test

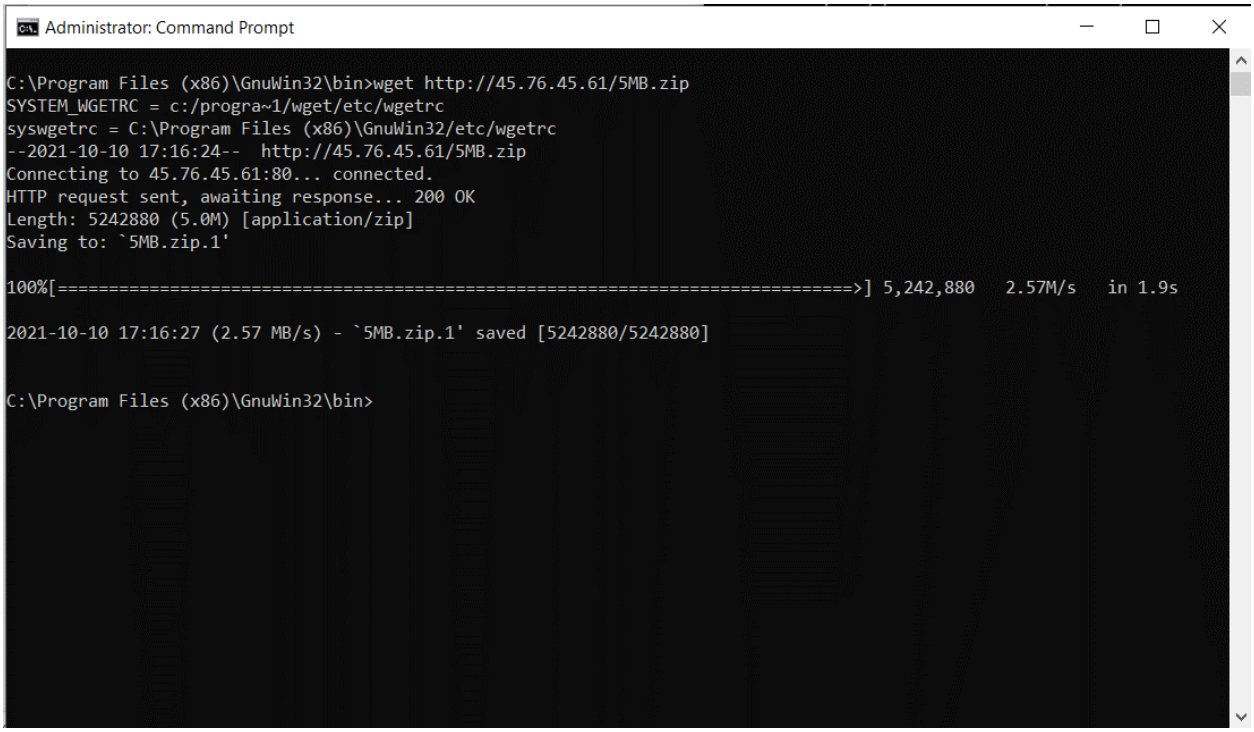
Uses WGET for Windows https://sourceforge.net/projects/gnuwin32/

Uses the 10MB file from https://www.thinkbroadband.com/download

Test 12: Download test file from Paris via the public Internet

wget http://45.76.45.61/5MB.zip

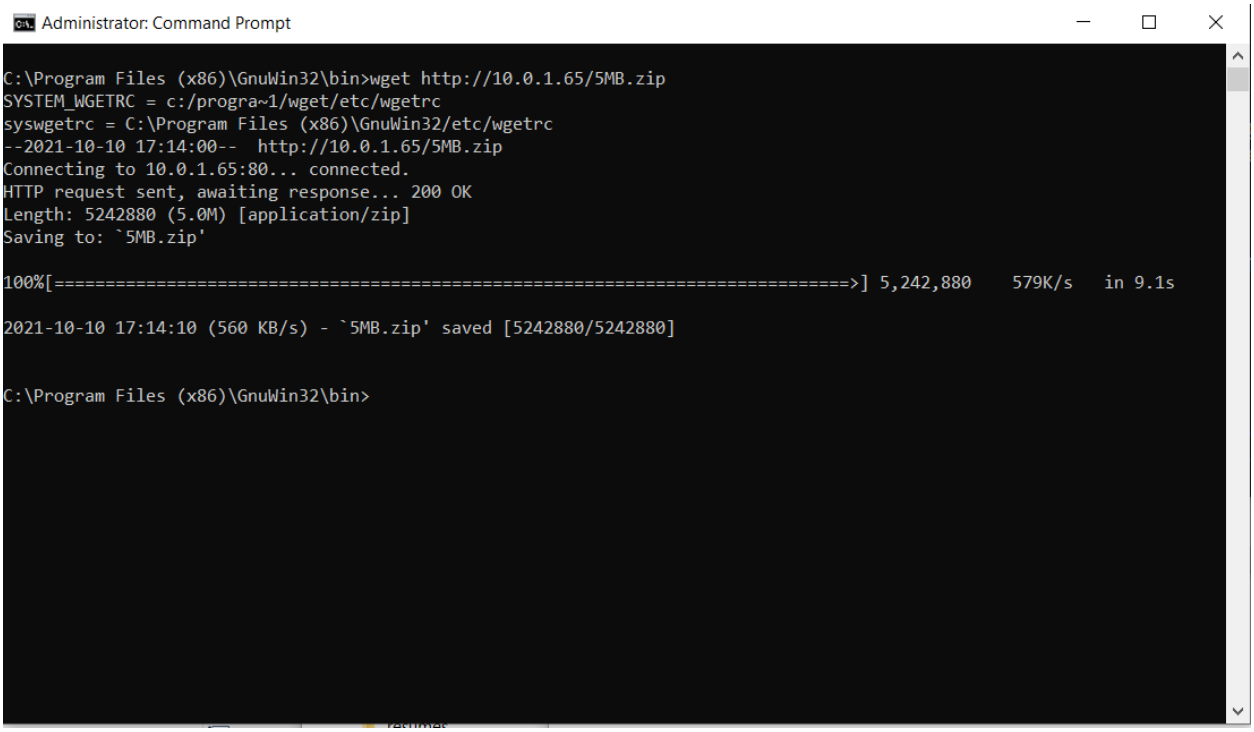
Result:



Test 13: Download test file from Paris via the NVIS network

wget http://10.0.1.65/5MB.zip

Result: Download varies, but encrypted speed is often much slower

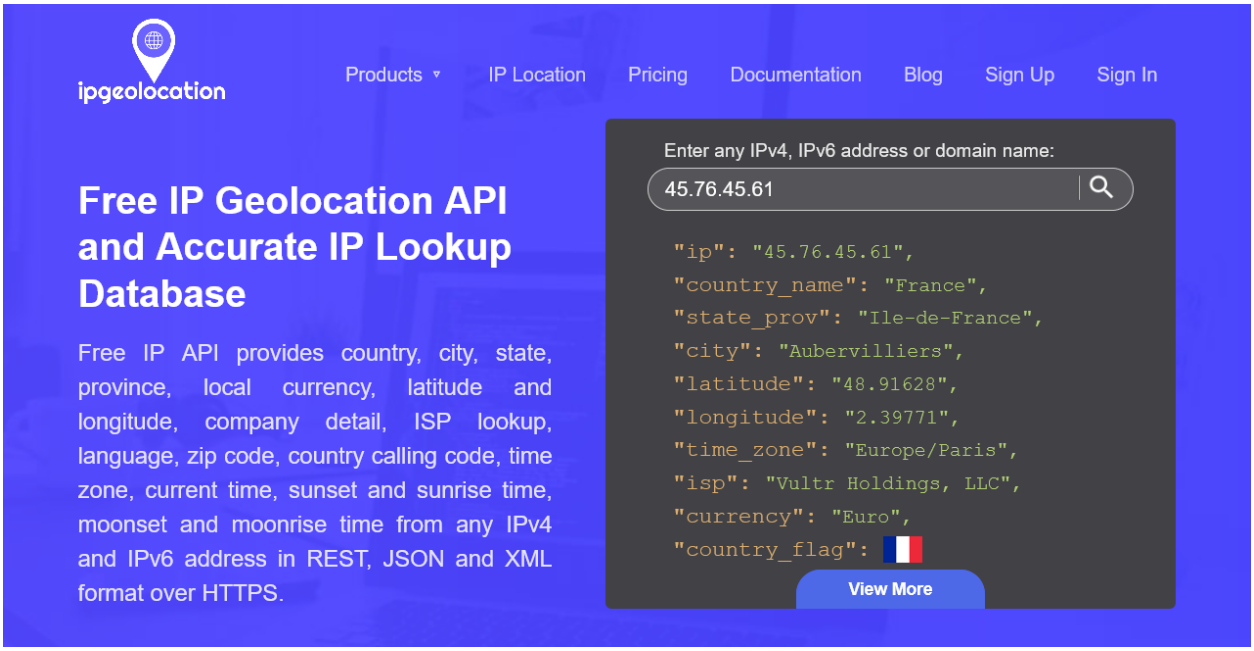


Geolocation Tests

Test 14: Locate Paris host from public IP

Use the service at https://ipgeolocation.io to find 45.76.45.6145.76.45.61

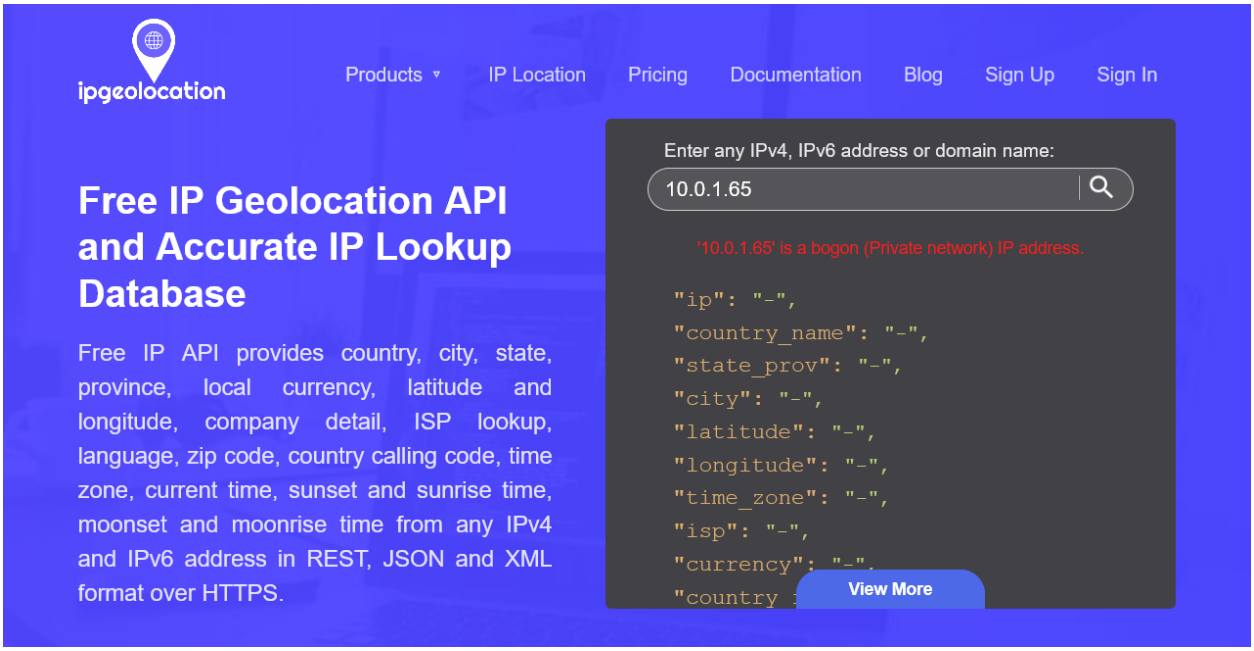
Result: Displays physical coordinates in France



Test 15: Locate Paris host from NVIS IP

Use the service at https://ipgeolocation.io to find 10.0.1.65

Result: Shows an error – cannot locate the host


ipgeolocation
Products
IP Location
Pricing
Documentation
Blog
Sign Up
Sign In
Free IP Geolocation API and Accurate IP Lookup Database
Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.
Enter any IPv4, IPv6 address or domain name:
10.0.1.65
'10.0.1.65' is a bogon (Private network) IP address.
"ip": "-",
"country_name": "-",
"state_prov": "-",
"city": "-",
"latitude": "-",
"longitude": "-",
"time_zone": "-",
"isp": "-",
"currency": "-",
"country
View More

Access Control Tests

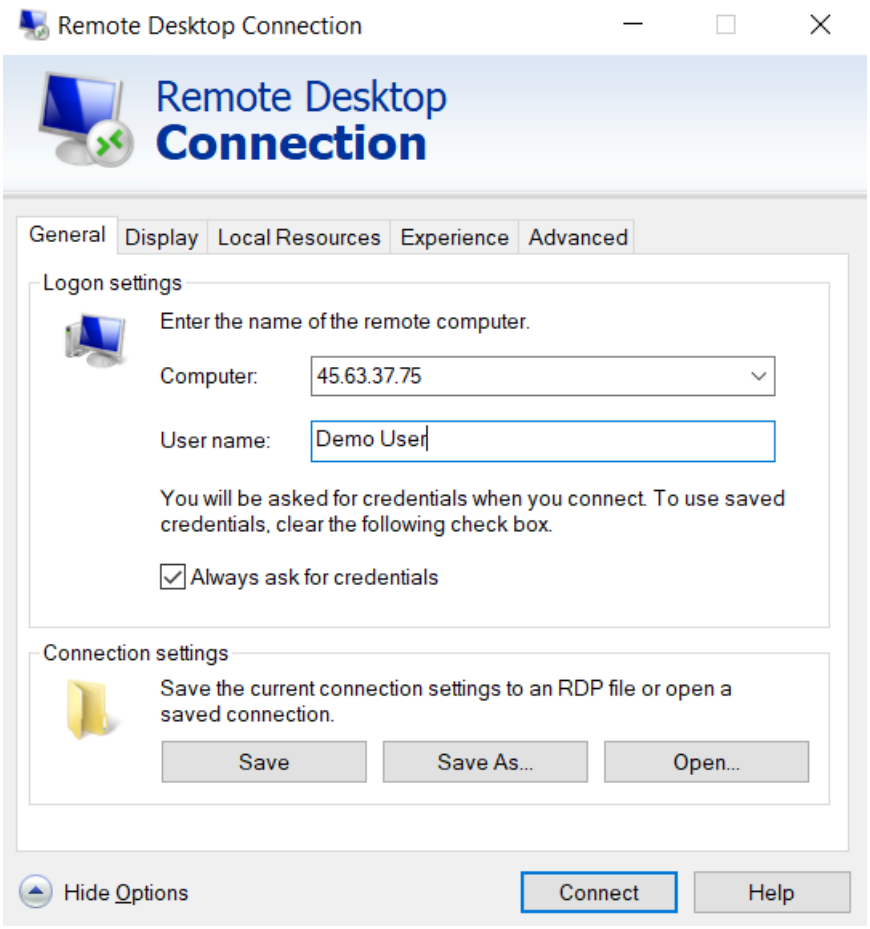
Windows Remote Desktop (RDP) Test

Test 16: Login Remote Desktop using public IP

Launch Remote Desktop Connection to the public IP 45.63.37.75

Select Show Options and Always Ask for Credentials

Result:



Press Connect

Enter Password: SopranoCastle36!

Accept certificate

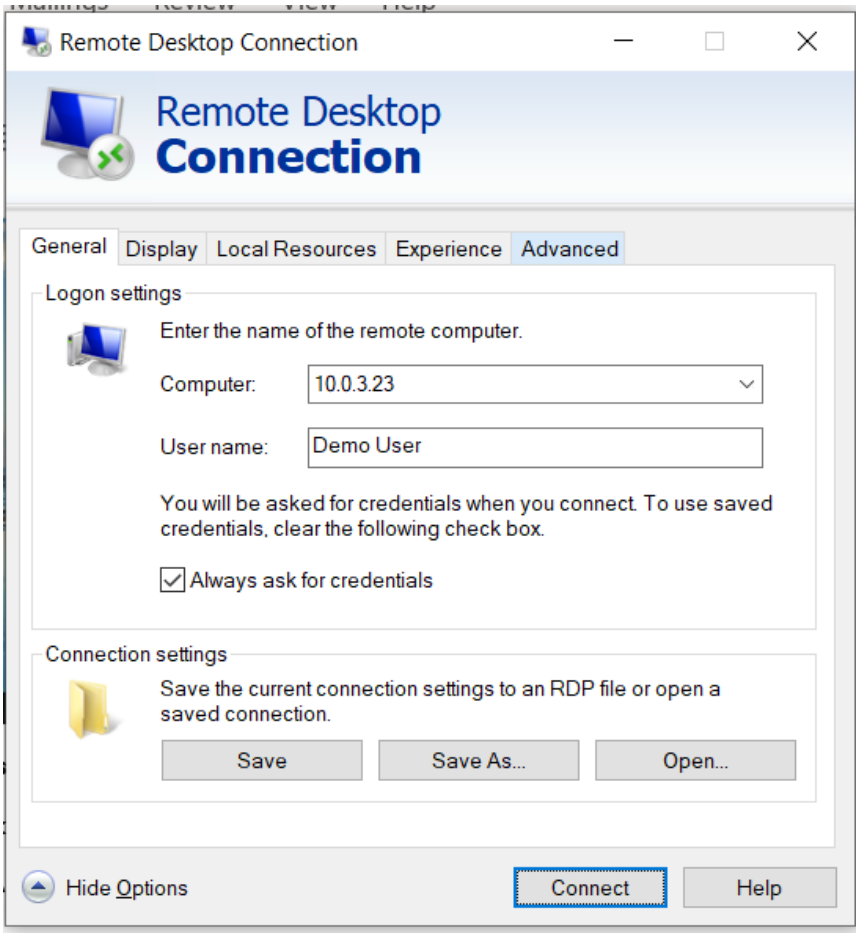
Result: User is remotely connected to the Azure desktop

Test 17: Login Remote Desktop using NVIS IP

Launch Remote Desktop Connection to the public 10.0.3.23

Select Show Options and Always Ask for Credentials

Result:



Press Connect

Enter Password: SopranoCastle36!

Accept certificate

Result: User is remotely connected to the Azure desktop

SSH Access Tests

Test 18: SSH Login to the public IP of Linux Host

ssh demo@45.32.184.36 (use Git Bash or Putty)

Enter password SopranoCastle36!

Result:

Demo logged in to bash shell

Test 19: SSH Login to the NVIS IP of Linux Host

Ssh demo@10.0.1.95 (use Git Bash or Putty)

Enter password SopranoCastle36!

Result:

Demo logged in to bash shell

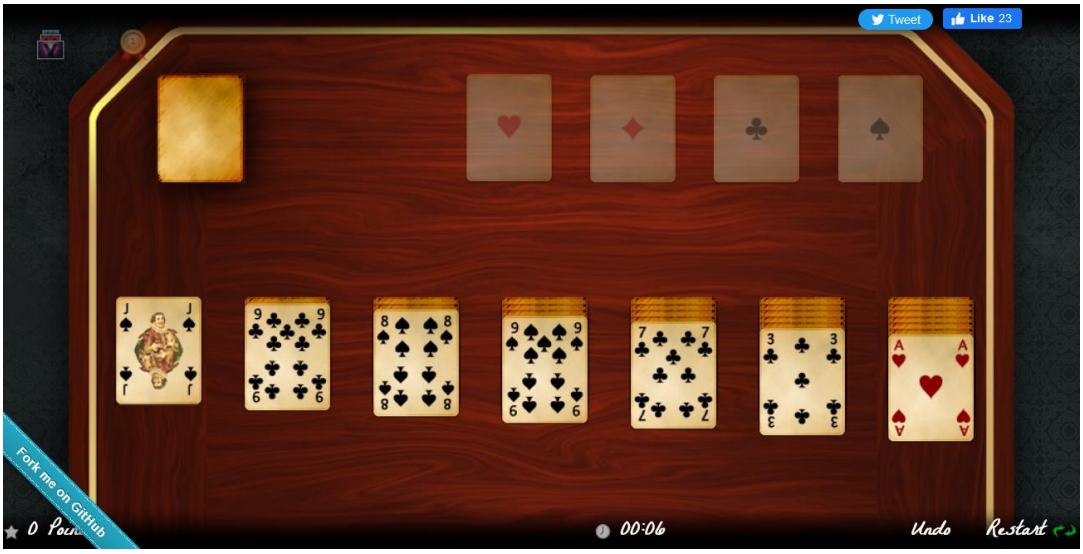
Miscellaneous Examples

Invisible Games (Javacript)

Example 1: Solitaire

https://amsterdam.nvis-inc.com/solitaire/ (10.0.1.95)

Result:



Invisible Streaming Video (NVIS TV)

Example 2: NVIS TV stream URL here

Result:

Invisible Video Chat (NVIS Meet)

Example 3: NVIS Meet URL https://meet.nvisnet.com/ (node 10.0.1.75)

Result: