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
Test Overview
Test Procedures
Quick install
Display a host inside the customer network
Wireshark Test4
Tcpdump Tests
Port Scanning
Performance Tests
Route Cost Test
File Download Test11
Geolocation Tests13
Access Control Tests15
Windows Remote Desktop (RDP) Test15
SSH Access Tests
Miscellaneous Examples
Invisible Games (Javacript)19
Invisible Streaming Video (NVIS TV)19
Invisible Video Chat (NVIS Meet)

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 <u>http://45.76.45.61</u> 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 <u>http://10.0.1.65</u> 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 <u>http://45.76.45.61</u>

Result: Output shows HTTP and TCP packets.

(Capturing from Wi-Fi				- 🗆 X
File	Edit View Go C	apture Analyze Statistics	Telephony Wireless To	ols Help	
	i 🖉 🛞 i 🗈 🕅	🕅 🕼 🔍 🔶 🔿 🖉 👔	🖢 📜 🔲 🔍 Q, Q, 🧃		
tcp	.port == 80 and ip.addr	== 45.76.45.61			Expression + Apply this filter Apply this filter Apply this filter >>
No.	Time	Source	Destination	Protocol	Length Info
Г	35 4.325105	10.0.0.199	45.76.45.61	TCP	66 28685 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
	36 4.326476	10.0.0.199	45.76.45.61	TCP	66 28686 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
	37 4.487098	45.76.45.61	10.0.199	TCP	66 80 → 28685 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA
	38 4.487098	45.76.45.61	10.0.0.199	TCP	66 80 → 28686 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA
	39 4.487437	10.0.0.199	45.76.45.61	TCP	54 28685 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
	40 4.487538	10.0.0.199	45.76.45.61	TCP	54 28686 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
	41 4.488257	10.0.0.199	45.76.45.61	HTTP	412 GET / HTTP/1.1
	70 4.649831	45.76.45.61	10.0.0.199	TCP	54 80 → 28685 [ACK] Seq=1 Ack=359 Win=64128 Len=0
	71 4.649831	45.76.45.61	10.0.0.199	HTTP	681 HTTP/1.1 200 OK (text/html)
	72 4.696601	10.0.0.199	45.76.45.61	TCP	54 28685 → 80 [ACK] Seg=359 Ack=628 Win=130560 Len=0
	173 5.707139	10.0.0.199	45.76.45.61	HTTP	361 GET /paris.jpg HTTP/1.1
> F	rame 35: 66 byte	s on wire (528 bits)	, 66 bytes captured (528 bits) o	n interface 0
> E	thernet II, Src:	HonHaiPr_f8:c0:47 (40:b8:9a:f8:c0:47), D	st: c2:94:3	5:5a:f6:c9 (c2:94:35:5a:f6:c9)
> I	nternet Protocol	Version 4, Src: 10.	0.0.199, Dst: 45.76.4	5.61	
> T	ransmission Cont	rol Protocol, Src Po	rt: 28685, Dst Port:	80, Seq: 0,	Len: 0
000	0 c2 94 35 5a f	6 c9 40 b8 9a f8 c0	47 08 00 45 00	5Z@G.	E.
001	0 00 34 88 ec 4	10 00 80 06 0c 88 0a	00 00 c7 2d 4c .4.	@	L
002	0 2d 3d 70 0d 0	00 50 d6 d1 7a 55 00	00 00 00 80 02 -=	oP zU	
003	0 fa f0 4d 4b 0	00 00 02 04 05 b4 01	03 03 08 01 01	1K	
004	04 02				

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 <u>http://10.0.1.65</u>

Result: No output showing traffic from 10.0.1.65

/ *W	/i-Fi															_		×
File E	dit View	Go Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help										
		1 🗋 🕱 🙆	۹ 🖛 🖬) 😫 有 🤉	¥ 其 📘	\oplus \bigcirc $($	् 🎹											
tcp.p	ort == 80 ar	nd ip.addr == 10.0).1.65								×	<	Expression	+	Apply this filter	Apply this filter	Apply this	s filter »
No.	Time	So	ource		Destinatio	n		Protocol	Length	Info								
0 7	wireshark	861FBB25-6903-4	1E09-AC03-8	7B8F9BF962D	20211009232	716 a15880	0					Pac	kets: 399 · I	Displayed	1: 0 (0.0%)		Profile: [Default .:

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 <u>http://45.76.45.61</u>

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

MINGW64:/c/Users/aphil/Downloads	_	×
<pre>aphil@LAPTOP-QSLCMCOP MINGW64 ~/Downloads \$ grep 45.76.45.61 t0.out head 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 109 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 97 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 453 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 97 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 400 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 109 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 97 10.0.0.199.59787 > 45.76.45.61.56371: UDP, length 417</pre>		^
aphil@LAPTOP-QSLCMCOP MINGW64 ~/Downloads \$		~

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 <u>http://10.0.1.65</u>

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:

Contract of the second	and Dark Common	· · ·	•					
Adva	nced Port Scanner						L	
File Vie	w Settings Help							
Sto	p 🚺 🗜 🕻 🗄 🗄							
10.0.0.1-	10.0.255.254, 10.0.0.1-254				Well-known TCP p	oorts 1-1023	Search	2
Results	Favorites							
Statu	is Name	ÎP	Manufacturer	MAC address	Ports			88
> 📮	10.0.0.1	10.0.0.1		C2:94:35:5A:F6:C9	53, 80, 443			
	10.0.0.12	10.0.0.12	Amazon Technologies Inc.	68:54:FD:61:57:3D		10.0.0.1		
	10.0.20	10.0.0.20	Amazon Technologies Inc.	68:37:E9:33:71:4A		C1-1-1-1	A.L	
	10.0.0.94	10.0.0.94		C8:C7:50:23:C1:EF		Operating syst	Aive em:	
	LAPTOP-QSLCMCOP	10.0.0.199	Hon Hai Precision Ind. C	40:B8:9A:F8:C0:47	135, 139, 445	IP:	10.0.0.1	
	10.0.255	10.0.255	Hon Hai Precision Ind. C	40:B8:9A:F8:C0:47		MAC:	C2:94:35:5A:F6:C9	
> 📮	10.0.1.55	10.0.1.55		46:37:34:A4:08:25	22, 53, 80	Manufacturer:		
> 📮	10.0.1.65	10.0.1.65		46:37:34:A4:08:26		User:		
> 📮	10.0.1.75	10.0.1.75		46:37:34:A4:08:27	22	Type:		
	10.0.1.95	10.0.1.95		46:37:34:A4:08:28		Date:		
> 📮	10.0.2.47	10.0.2.47	Handan BroadInfoCom	00:02:FF:00:02:2F	22, 80	Comments:		
	BIGONE	10.0.2.51		00:FF:58:E5:C7:38		Service	Details	
	LAPTOP-QSLCMCOP	10.0.2.102		00:FF:BC:58:94:0E	135, 139, 445	JUTTO		
> 📮	10.0.2.131	10.0.2.131	Handan BroadInfoCom	00:02:FF:00:02:83	22, 80	HIP	XFINITY (Xfinity Broadband Router Server)	
₽	10.0.3.52	10.0.3.52	Handan BroadInfoCom	00:02:FF:00:03:34	22	Port 53 (TCP)	OpenDNS Updater	
						Port 80 (TCP)		
						Port 443 (TCP)	Tunnel is ssl: unknown service	
<					>			
201 4 4 1	4 4 4 2020 4							
3%, 14 aliv	re, 1 dead, 2335 unknown							

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 <u>NO open ports</u>:

Cila Viano	ed Port Scanner						_	
File View								
Stop								
10.0.0.1-10	.0.255.254, 10.0.0.1-254				Well-known	TCP ports 1-1023	Search	Q
Results	Favorites							
Status	Name	ÎP	Manufacturer	MAC address	Ports			
	10.0.0.1	10.0.0.1		C2:94:35:5A:F6:C9	443			
	10.0.0.12	10.0.0.12	Amazon Technologies Inc.	68:54:FD:61:57:3D		I APTOP-OSI	CMCOR	
	10.0.0.20	10.0.0.20	Amazon Technologies Inc.	68:37:E9:33:71:4A		LAPTOP-Q3L	СМСОР	
	10.0.0.94	10.0.0.94	-	C8:C7:50:23:C1:EF		Status:	Dead	
	LAPTOP-QSLCMCOP	10.0.0.199	Hon Hai Precision Ind. C	40:B8:9A:F8:C0:47		IP:	10.0.0.199	
-	10.0.1.55	10.0.1.55		46:37:34:A4:08:25		MAC:	40:B8:9A:F8:C0:47	
	10.0.1.65	10.0.1.65		46:37:34:A4:08:26		Manufacturer:	Hon Hai Precision Ind. Co.,Ltd.	
	10.0.1.75	10.0.1.75		46:37:34:A4:08:27		NetBIOS: User:		
-	10.0.1.95	10.0.1.95		46:37:34:A4:08:28		Type:		
-	10.0.2.47	10.0.2.47	Handan BroadInfoCom	00:02:FF:00:02:2F		Date:		
	BIGONE	10.0.2.51		00:FF:58:E5:C7:38		Comments:		
	LAPTOP-QSLCMCOP	10.0.2.102		00:FF:BC:58:94:0E		Coursian Dataila		
-	10.0.2.131	10.0.2.131	Handan BroadInfoCom	00:02:FF:00:02:83		Service Details		
	10.0.3.52	10.0.3.52	Handan BroadInfoCom	00:02:FF:00:03:34				
<						>		
1%, 5 alive, 9	dead, 923 unknown							

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.

```
MINGW64:/c/Users/aphil/Downloads
                                                                               \times
$ tracert 45.76.45.61
Tracing route to 45.76.45.61.vultr.com [45.76.45.61]
over a maximum of 30 hops:
       46 ms
                 2 ms
                           1 ms
                                  10.0.0.1
  \mathbf{1}
       11 ms
  2
                         162 ms
                                  96.120.14.213
                 11 ms
  3
       95 ms
                 12 ms
                          12 ms
                                  ae-251-1204-rur02.lodi.ca.ccal.comcast.net [68.8
 .212.237]
       17 ms
                 15 ms
                          16 ms
                                  ae-36-ar01.sacramento.ca.ccal.comcast.net [68.87
 4
221.65]
        ÷
                 20 ms
                          19 ms
                                  lag-39.ear3.SanJose1.Level3.net [4.68.71.29]
  5
  6
      175 ms
               198 ms
                         201 ms
                                  ae-2-3201.ear1.Paris1.Level3.net [4.69.140.26]
  7
               199 ms
                                  CHOOPA-LLC.ear1.Paris1.Level3.net [212.73.205.86
      316 ms
                         188 ms
8
        *
                                  Request timed out.
 9
                                  Request timed out.
10
        *
                  *
                                  Request timed out.
11
      155 ms
               155 ms
                         154 ms 45.76.45.61.vultr.com [45.76.45.61]
Trace complete.
aphil@LAPTOP-QSLCMCOP MINGW64 ~/Downloads
```

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

ipgeolocation	Pricing Documentation blog sign up sign in						
	Enter any IPv4, IPv6 address or domain name:						
Free IP Geolocation API	(45.76.45.61 Q						
and Accurate IP Lookup	"ip": "45.76.45.61",						
Database	"country_name": "France", "state prov": "Ile-de-France",						
Free IP API provides country, city, state,	"city": "Aubervilliers",						
province, local currency, latitude and	"latitude": "48.91628",						
longitude, company detail, ISP lookup,	"longitude": "2.39771",						
language, zip code, country calling code, time	"time_zone": "Europe/Paris",						
zone, current time, sunset and sunrise time,	"isp": "Vultr Holdings, LLC",						
moonset and moonrise time from any IPv4	"currency": "Euro",						
and IPv6 address in REST. JSON and XML	"country_flag":						
format over HTTPS	View More						

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



Products V IP Location Pricing

Blog Sign Up

gn 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 Q							
'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:

퉳 Remote	Desktop Conne	ection			_		×			
	Remote Conne	Desk ctic	top DN							
General D	isplay Local Re	sources	Experience	Advand	ed					
	Enter the name	of the re	mote compute	er.						
	Computer:	45.63.3	7.75			\times				
	User name:	Demo	User							
	You will be asked for credentials when you connect. To use saved credentials, clear the following check box.									
Connection	n settings									
	Save the current connection settings to an RDP file or open a saved connection.									
	Save		Save As	§	0	pen				
Hide Op	tions			Con	nect	Hel	p			

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:

mannings	11011011 1101	w.	T C I P				
Nemote	e Desktop Connect	ion		_	-		×
-	Remote D Connec	esk tic	top >n				
General D)isplay Local Reso	urces	Experience	Advanced			
-Logon set	tings						
	Enter the name of	the re	mote compute	r.			
	Computer: 1	0.0.3.2	23			\sim	
	User name:	emol	User				
	You will be asked credentials, clear	for cre the fol	edentials wher llowing check b	n you connec box.	t. To us	e saved	
	Always ask for	crede	entials				
Connectio	on settings						
	Save the current c saved connection	onneo	ction settings to	an RDP file	or ope	na	
	Save		Save As		Ор	en	
Hide <u>O</u> p	otions			Connec	t	Help	p

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 <u>demo@10.0.1.95</u> (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 <u>here</u>

Result:



PEWDIEPIE - 09/14/20 - AMONG

Invisible Video Chat (NVIS Meet)

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

Result:

