

2-4-1 OpenVPN

You Want a VPN

But a SIMPLE One  
and IPsec is Not Simple

# OpenVPN

Open Protocol  
Open Source Tools  
Not Known to be Pwned  
by the NSA, GCHQ, ...

Easy to Install  
Free Server(s)

Easy to Install  
Free Clients

They Interoperate!

# OpenVPN Server

**Sense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

## Status / Dashboard

### System Information

Name	pfs0.sea.rg.net
System	pfSense Serial: 5a9d09f4-f598-11e6-a03b-65155a9e9cb3
Version	2.3.2-RELEASE-p1 (i386) built on Tue Sep 27 12:13:32 CDT 2016 FreeBSD 10.3-RELEASE-p9  The system is on the latest version.
Platform	pfSense
CPU Type	QEMU Virtual CPU version 2.1.2
Uptime	02 Hours 46 Minutes 06 Seconds
Current date/time	Sat Feb 18 7:53:56 UTC 2017
DNS server(s)	<ul style="list-style-type: none"><li>127.0.0.1</li><li>147.28.0.15</li><li>147.28.0.3</li></ul>
Last config change	Fri Nov 11 6:52:23 UTC 2016
State table size	0% (29/99000) <a href="#">Show states</a>
MBUF Usage	3% (760/26584)
Load average	0.00, 0.00, 0.00
CPU usage	0%
Memory usage	14% of 991 MiB
SWAP usage	0% of 2048 MiB
Disk usage ( / )	18% of 5.8GiB - ufs
Disk usage ( /var/run )	3% of 3.4MiB - ufs in RAM

### Services Status

Service	Description	Action
✓ dpinger	Gateway Monitoring Daemon	<a href="#">C</a> <a href="#">O</a>
✓ ntpd	NTP clock sync	<a href="#">C</a> <a href="#">O</a>
✓ openvpn	OpenVPN server: RGnet Westin UDP	<a href="#">C</a> <a href="#">O</a>
✓ sshd	Secure Shell Daemon	<a href="#">C</a> <a href="#">O</a>
✓ unbound	DNS Resolver	<a href="#">C</a> <a href="#">O</a>

### Interfaces

Interface	IP Address	MAC Address
WAN	147.28.0.32	2001:418:1::32

### Traffic Graphs

In 13 Kbps Out 5 Kbps 2/18/2017 14:54:05 [Switch to bytes/s](#) [AutoScale \(up\)](#) Graph shows last 1200 seconds

### OpenVPN

RGnet Westin UDP UDP:443

Name/Time	Real/Virtual IP
-----------	-----------------

# VPN Server

[System ▾](#)[Interfaces ▾](#)[Firewall ▾](#)[Services ▾](#)[VPN ▾](#)[Status ▾](#)[Diagnostics ▾](#)[Gold ▾](#)[H](#)

VPN / OpenVPN / Servers

[IPsec](#)[L2TP](#)[OpenVPN](#)[Servers](#)[Clients](#)[Client Specific Overrides](#)[Wizards](#)[Client Export](#)[Shared Key Export](#)

## OpenVPN Servers

Protocol / Port	Tunnel Network	Description
UDP / 443	10.0.1.0/24	RGnet Westin UDP

# Configuration!

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

### General Information

Disabled

☐ Disable this server  
Set this option to disable this server without removing it from the list.

Server mode

Remote Access ( SSL/TLS )

Protocol

UDP

Device mode

tun

Interface

WAN

Local port

443

Description

RGnet Westin UDP  
A description may be entered here for administrative reference (not parsed).

### Cryptographic Settings

TLS authentication

☒ Enable authentication of TLS packets.

Key

#  
# 2048 bit OpenVPN static key  
#  
-----BEGIN OpenVPN Static key V1-----  
4af648f42e6f785c1cc4e50b35651b37  
842f23512663df42d67d04cbeacd2e9c  
Paste the shared key here

Peer Certificate Authority

OpenVPN Root

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

Server certificate

OpenVPN Server crt/key (Server: Yes, CA: OpenVPN R...

DH Parameter length (bits)

2048

Encryption Algorithm

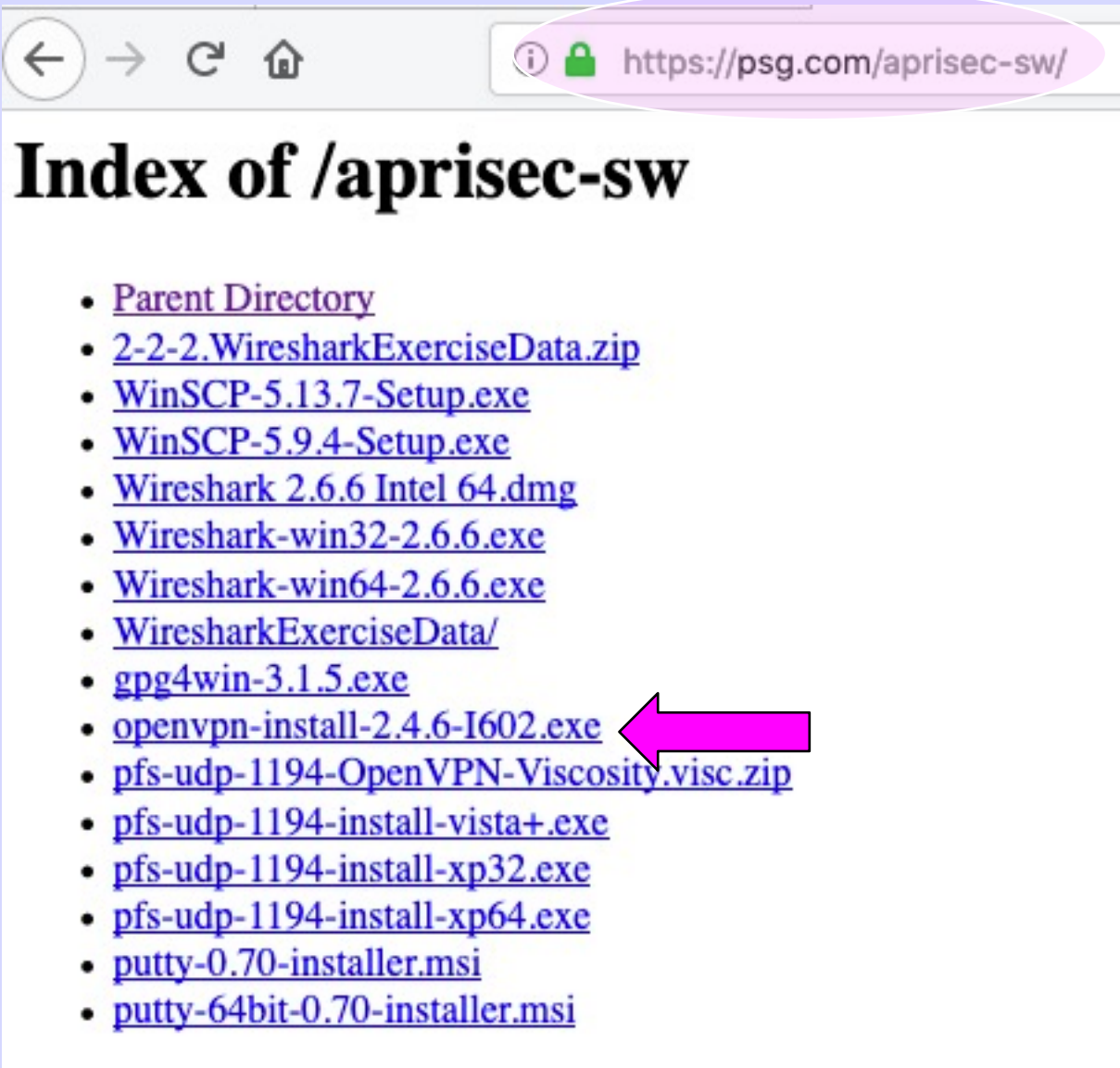
BF-CBC (128-bit)

# Select a Client

<http://psg.com/1.html>



# Or Get One Here



A screenshot of a web browser window. The address bar shows the URL <https://psg.com/aprisec-sw/>. Below the address bar, the page title is "Index of /aprisec-sw". A list of files and directories is displayed, including "Parent Directory", "2-2-2.WiresharkExerciseData.zip", "WinSCP-5.13.7-Setup.exe", "WinSCP-5.9.4-Setup.exe", "Wireshark 2.6.6 Intel 64.dmg", "Wireshark-win32-2.6.6.exe", "Wireshark-win64-2.6.6.exe", "WiresharkExerciseData/", "gpg4win-3.1.5.exe", "openvpn-install-2.4.6-I602.exe", "pfs-udp-1194-OpenVPN-Viscosity.visc.zip", "pfs-udp-1194-install-vista+.exe", "pfs-udp-1194-install-xp32.exe", "pfs-udp-1194-install-xp64.exe", "putty-0.70-installer.msi", and "putty-64bit-0.70-installer.msi". A large pink arrow points to the "openvpn-install-2.4.6-I602.exe" file.

Index of /aprisec-sw

- [Parent Directory](#)
- [2-2-2.WiresharkExerciseData.zip](#)
- [WinSCP-5.13.7-Setup.exe](#)
- [WinSCP-5.9.4-Setup.exe](#)
- [Wireshark 2.6.6 Intel 64.dmg](#)
- [Wireshark-win32-2.6.6.exe](#)
- [Wireshark-win64-2.6.6.exe](#)
- [WiresharkExerciseData/](#)
- [gpg4win-3.1.5.exe](#)
- [openvpn-install-2.4.6-I602.exe](#)
- [pfs-udp-1194-OpenVPN-Viscosity.visc.zip](#)
- [pfs-udp-1194-install-vista+.exe](#)
- [pfs-udp-1194-install-xp32.exe](#)
- [pfs-udp-1194-install-xp64.exe](#)
- [putty-0.70-installer.msi](#)
- [putty-64bit-0.70-installer.msi](#)

# OpenVPN Clients for Various Platforms

OpenVPN Community Client - Binaries for Windows, Source for other platforms.

OpenVPN For Android - Recommended client for Android

FEAT VPN For Android - For older versions of Android

OpenVPN Connect: Android (Google Play) or iOS (App Store) - Recommended client for iOS

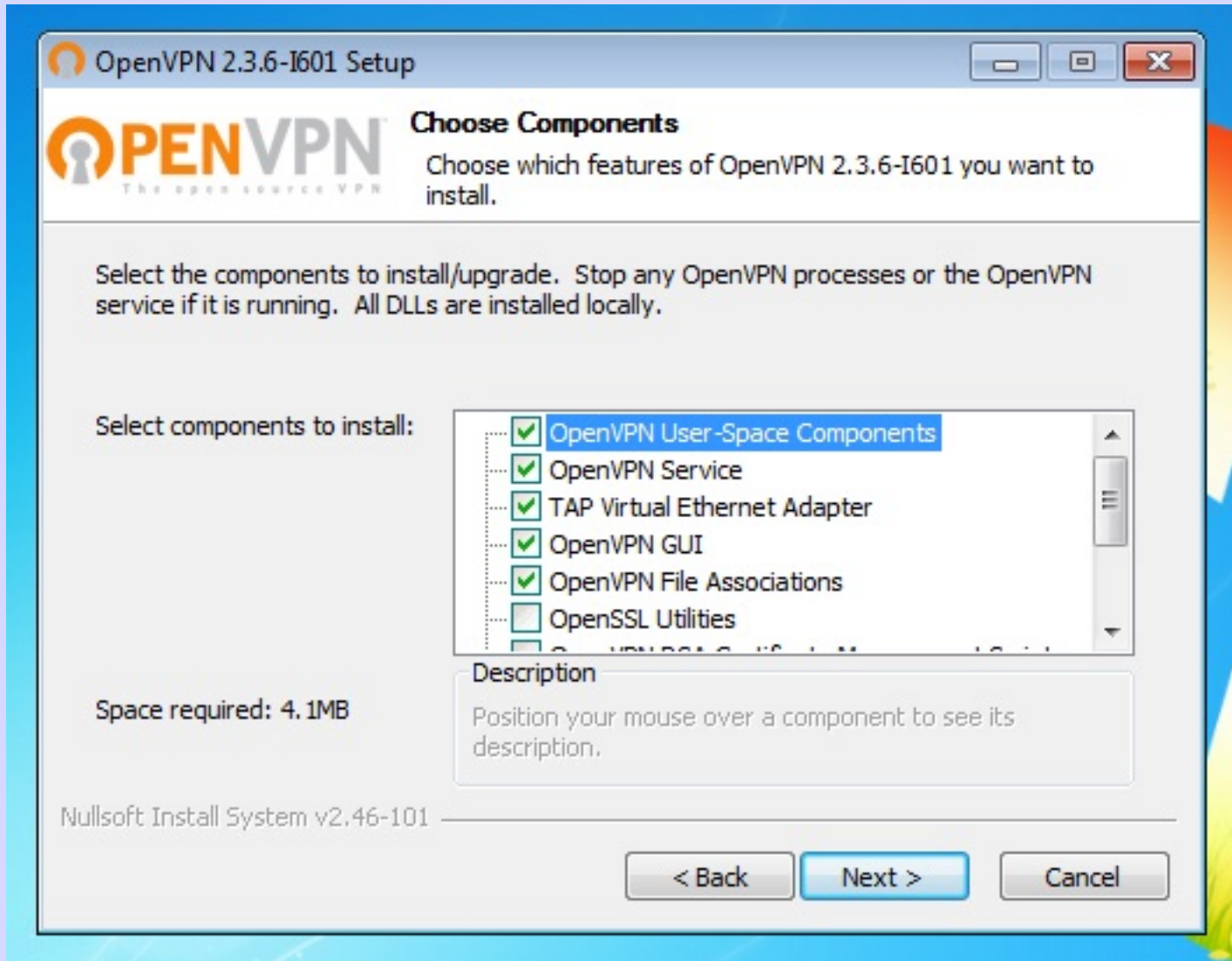
Viscosity - Recommended GUI client for Mac OSX \$\$

Tunnelblick - Free client for OSX

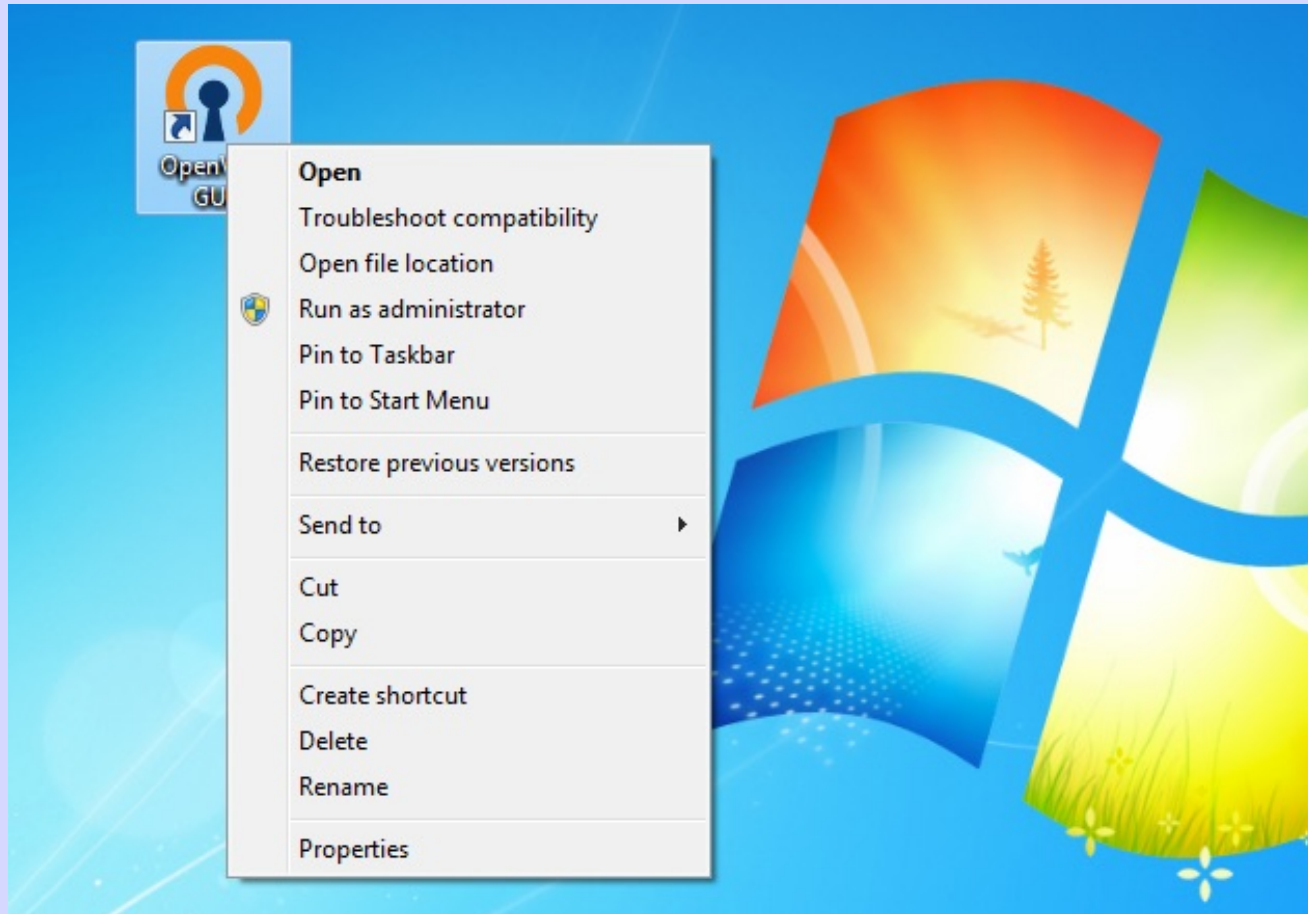
# Download Installer



# Run Installer

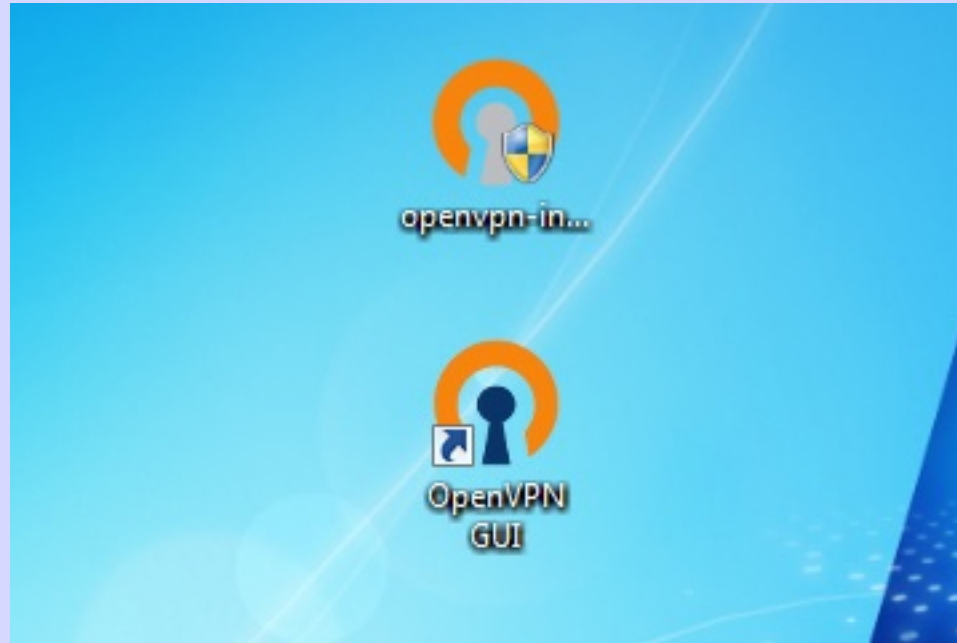


# Set RunAsAdmin



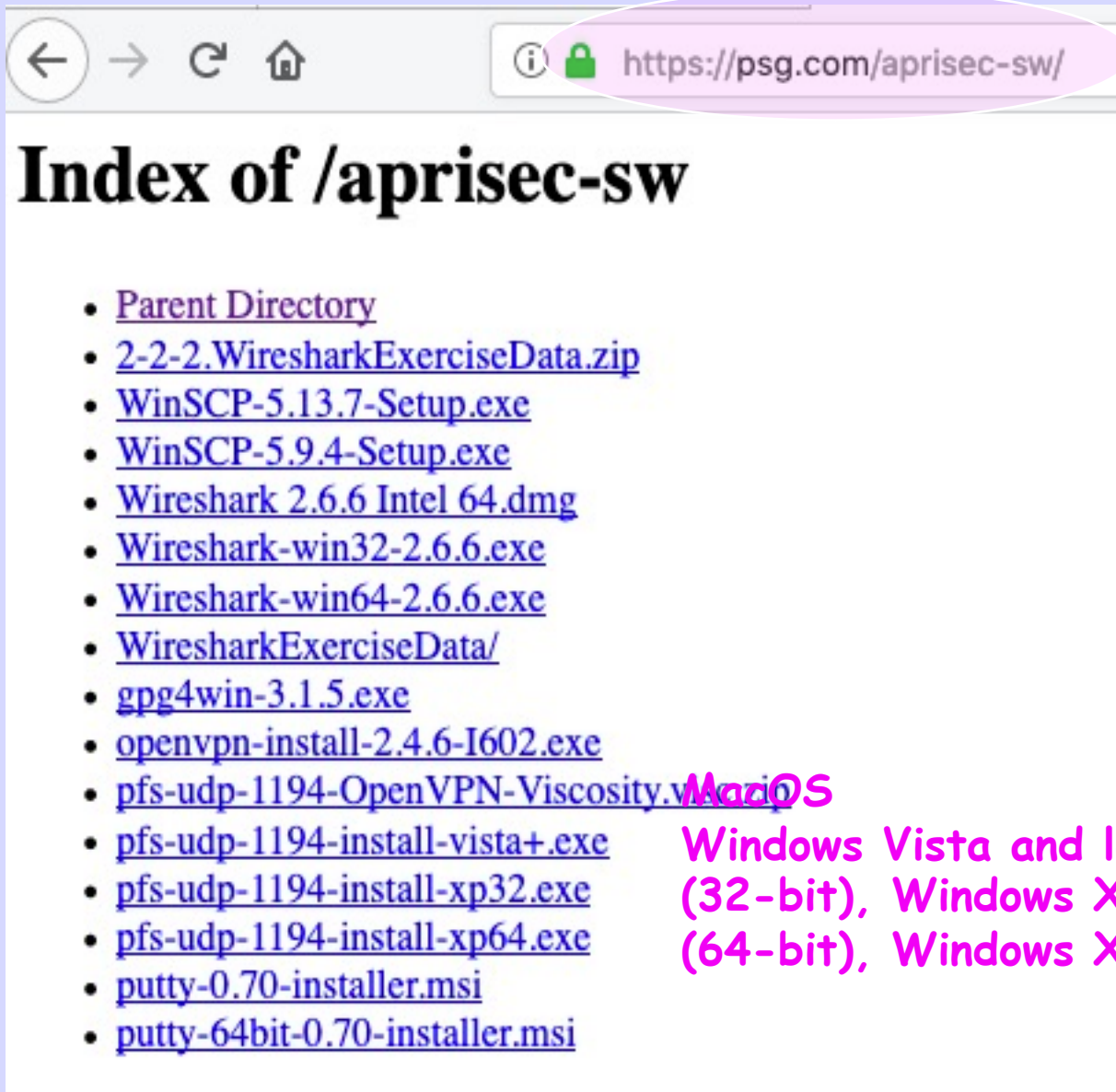
So Client Can Install Routes

# Open GUI (invisible)



You Can Delete Installer

# Get Credentials



The screenshot shows a web browser window with the address bar displaying <https://psg.com/aprisec-sw/>. The page title is "Index of /aprisec-sw". Below the title is a list of files and directories:

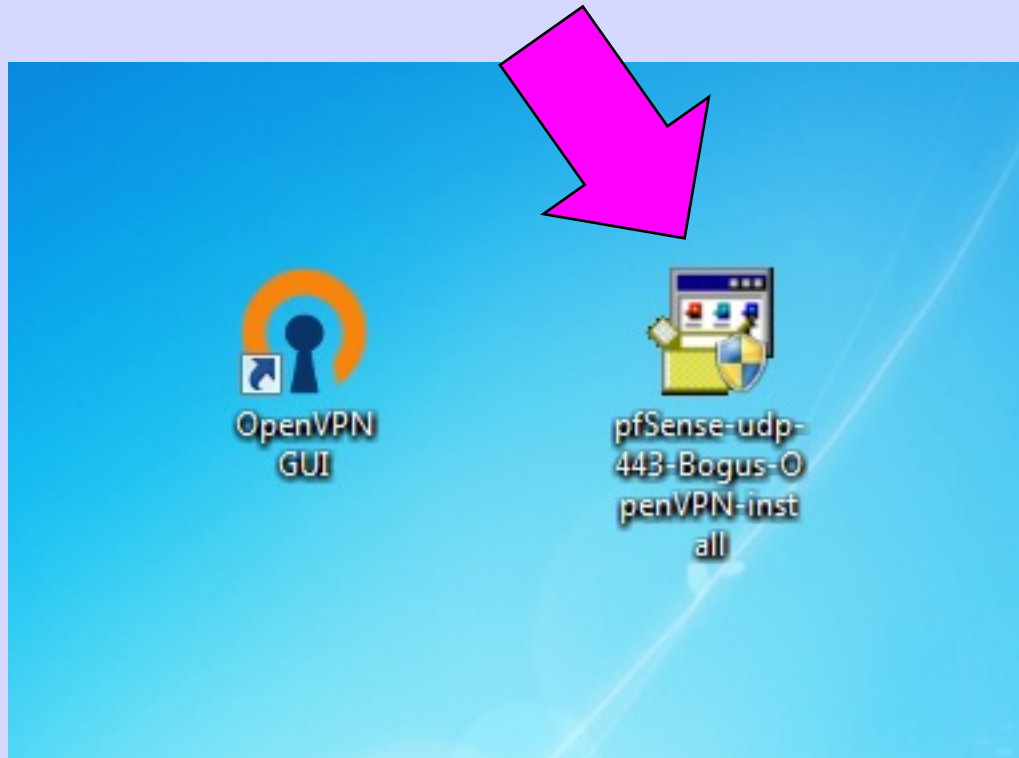
- [Parent Directory](#)
- [2-2-2.WiresharkExerciseData.zip](#)
- [WinSCP-5.13.7-Setup.exe](#)
- [WinSCP-5.9.4-Setup.exe](#)
- [Wireshark 2.6.6 Intel 64.dmg](#)
- [Wireshark-win32-2.6.6.exe](#)
- [Wireshark-win64-2.6.6.exe](#)
- [WiresharkExerciseData/](#)
- [gpg4win-3.1.5.exe](#)
- [openvpn-install-2.4.6-I602.exe](#)
- [pfs-udp-1194-OpenVPN-Viscosity.vnc](#)
- [pfs-udp-1194-install-vista+.exe](#)
- [pfs-udp-1194-install-xp32.exe](#)
- [pfs-udp-1194-install-xp64.exe](#)
- [putty-0.70-installer.msi](#)
- [putty-64bit-0.70-installer.msi](#)

Mac OS

Windows Vista and later  
(32-bit), Windows XP  
(64-bit), Windows XP



# Execute Credential EXE

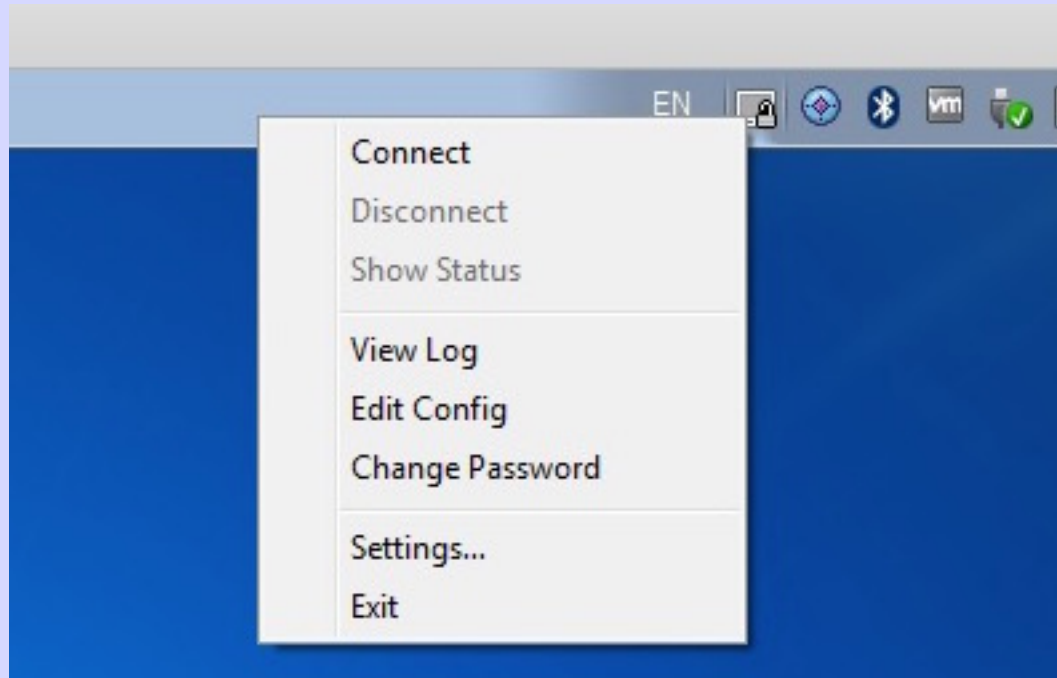




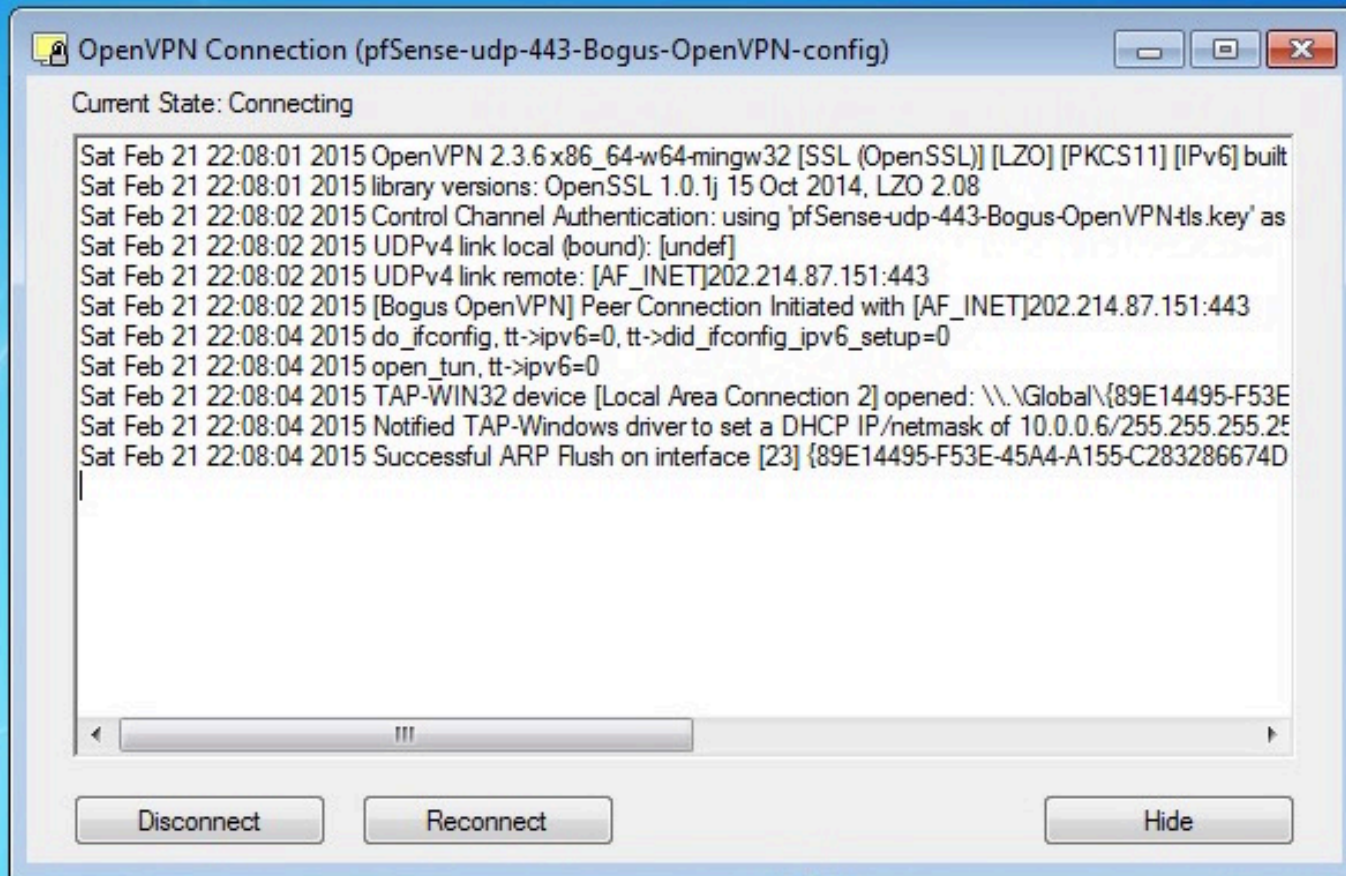
# Install Credentials



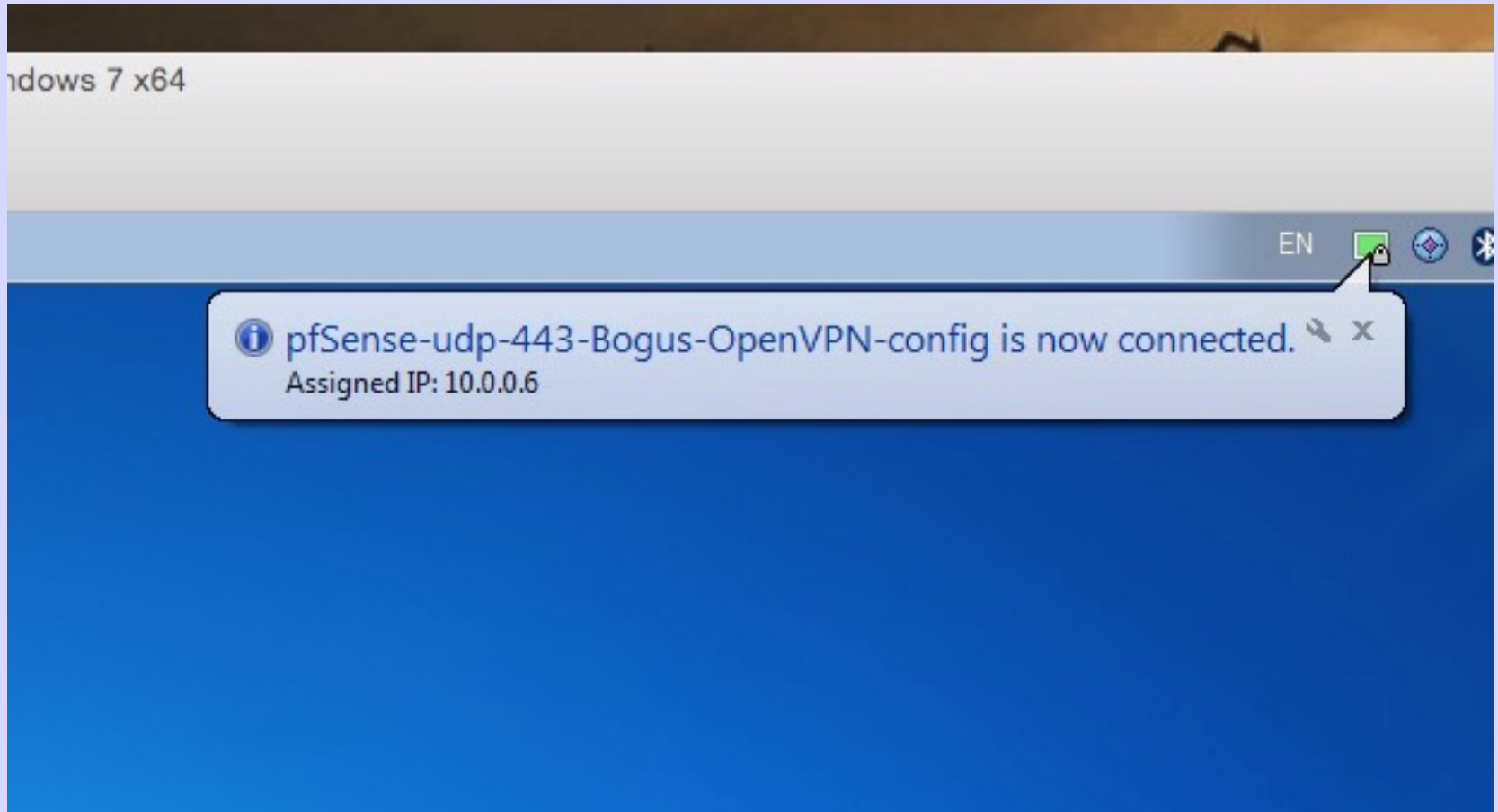
# Connect



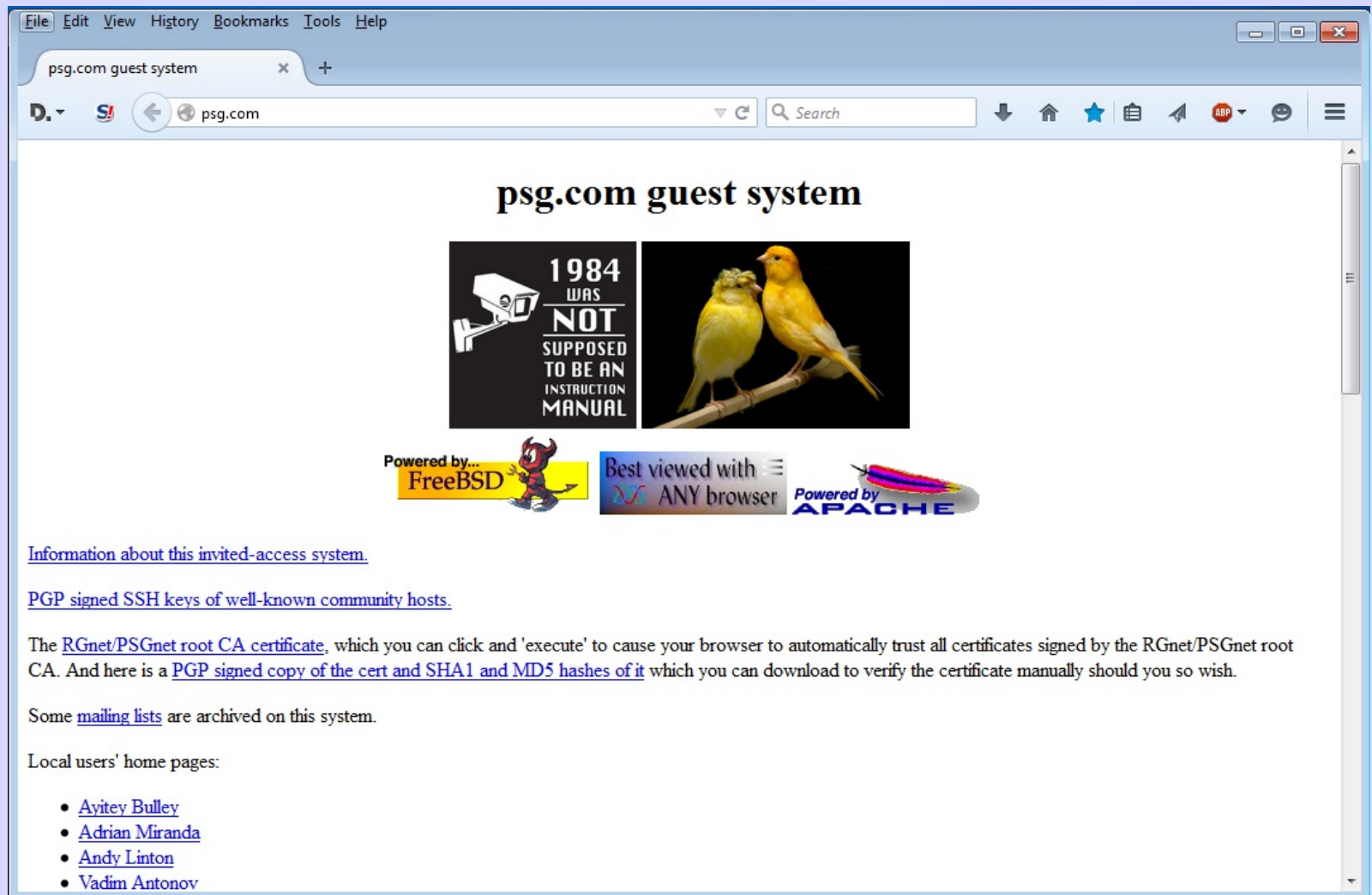
# Connecting



# You're Connected!



# Try It - Browse



# But How Do You Know It Works?

Is your traffic encrypted?

Use Wireshark!

Where are you?

[tracert psg.com](http://tracert.psg.com)

# Without VPN

ryuu.rg.net:/Users/andy> traceroute psg.com

traceroute to psg.com (147.28.0.62), 64 hops max, 52 byte packets

```
1 1.144.dhcp.conference.apricot.net (220.247.144.1) 9.212 ms 1.477 ms 1.233 ms
2 134.75.14.41 (134.75.14.41) 28.347 ms 1.212 ms 1.426 ms
3 kreonet-dj-bb1-kreonet2-gr-bb2.daej.kreonet2.net (134.75.105.113) 1.369 ms 1.334 ms 1.210 ms
4 134.75.2.1 (134.75.2.1) 4.076 ms 3.990 ms 3.922 ms
5 134.75.5.210 (134.75.5.210) 3.963 ms 4.002 ms 4.001 ms
6 203.234.255.165 (203.234.255.165) 4.161 ms 4.031 ms 4.370 ms
7 112.174.85.21 (112.174.85.21) 4.004 ms
  112.174.85.29 (112.174.85.29) 4.167 ms
  112.174.85.17 (112.174.85.17) 5.151 ms
8 112.174.83.142 (112.174.83.142) 5.129 ms
  112.174.83.106 (112.174.83.106) 4.748 ms
  112.174.83.90 (112.174.83.90) 4.878 ms
9 112.174.87.122 (112.174.87.122) 162.453 ms 196.357 ms 182.862 ms
10 sl-mpe51-sea-sprintlink.net (144.224.113.125) 136.197 ms 176.248 ms 136.314 ms
11 144.232.0.108 (144.232.0.108) 171.518 ms 186.838 ms 204.470 ms
12 144.232.9.62 (144.232.9.62) 210.499 ms 132.683 ms 172.015 ms
13 psg.com (147.28.0.62) 167.441 ms 159.632 ms 187.141 ms
```

Boo Hiss !

No Reverse DNS



# With VPN

ryuu.psg.com:/Users/presenter> traceroute psg.com

traceroute to psg.com (147.28.0.62), 64 hops max, 52 byte packets

```
1 10.0.1.1 (10.0.1.1) 1773.479 ms 103.112 ms 103.036 ms
2 202.214.87.130 (202.214.87.130) 104.809 ms 104.118 ms 103.963 ms
3 210.138.9.201 (210.138.9.201) 109.969 ms 105.199 ms 103.556 ms
4 tky009ipgw11.iij.net (58.138.112.53) 104.284 ms 106.700 ms 104.392 ms
5 tky009bb01.iij.net (58.138.112.157) 104.760 ms 104.872 ms 105.114 ms
6 sea001bb00.iij.net (58.138.88.230) 236.930 ms 239.763 ms *
7 six (206.81.80.23) 237.853 ms 237.146 ms 237.147 ms
8 147.28.0.62 (147.28.0.62) 216.686 ms 211.543 ms 210.681 ms
```