

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



# 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

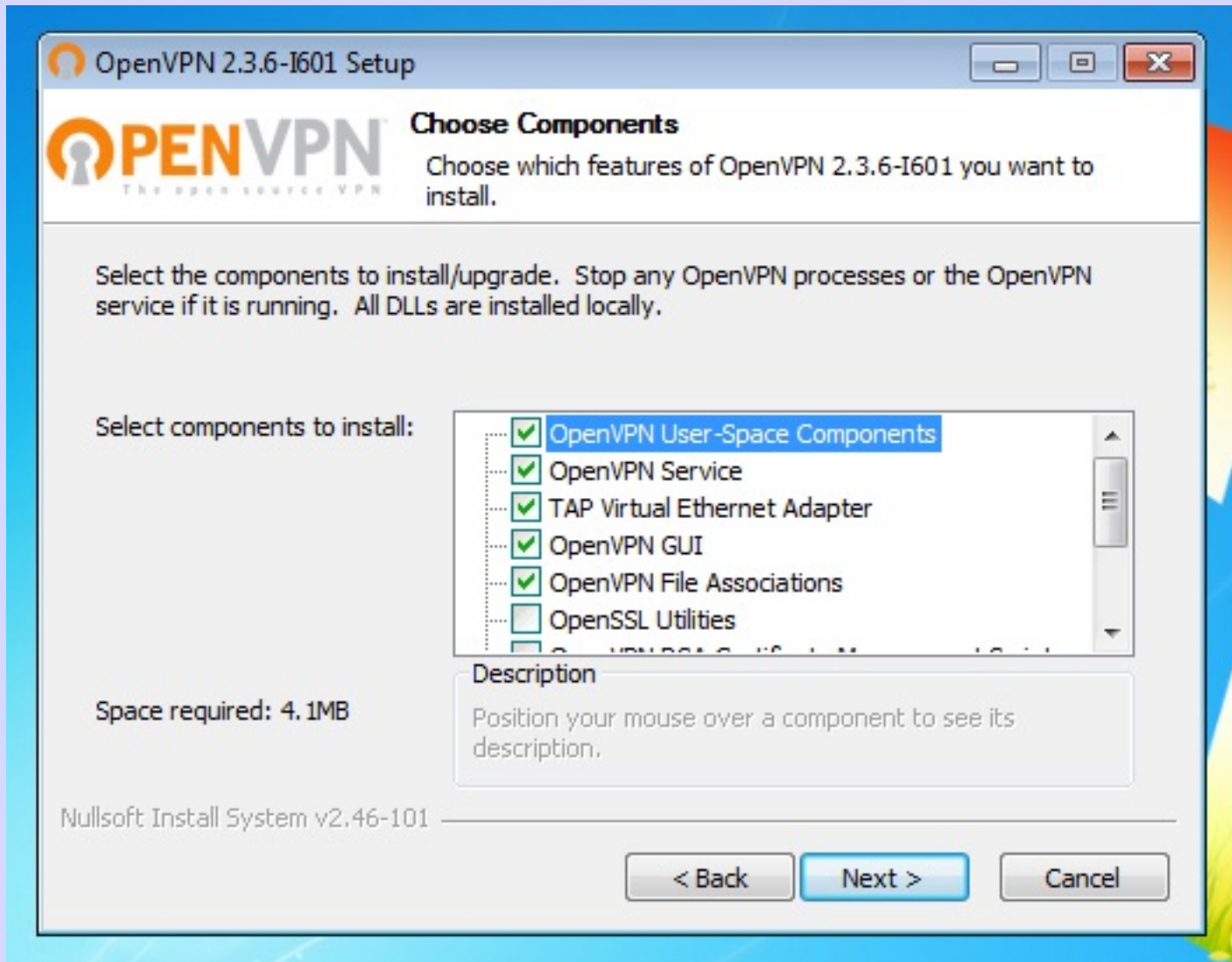
# If on Linux

```
openvpn --config pfs-udp-1194-  
Tokyo_OpenVPN-config.ovpn
```

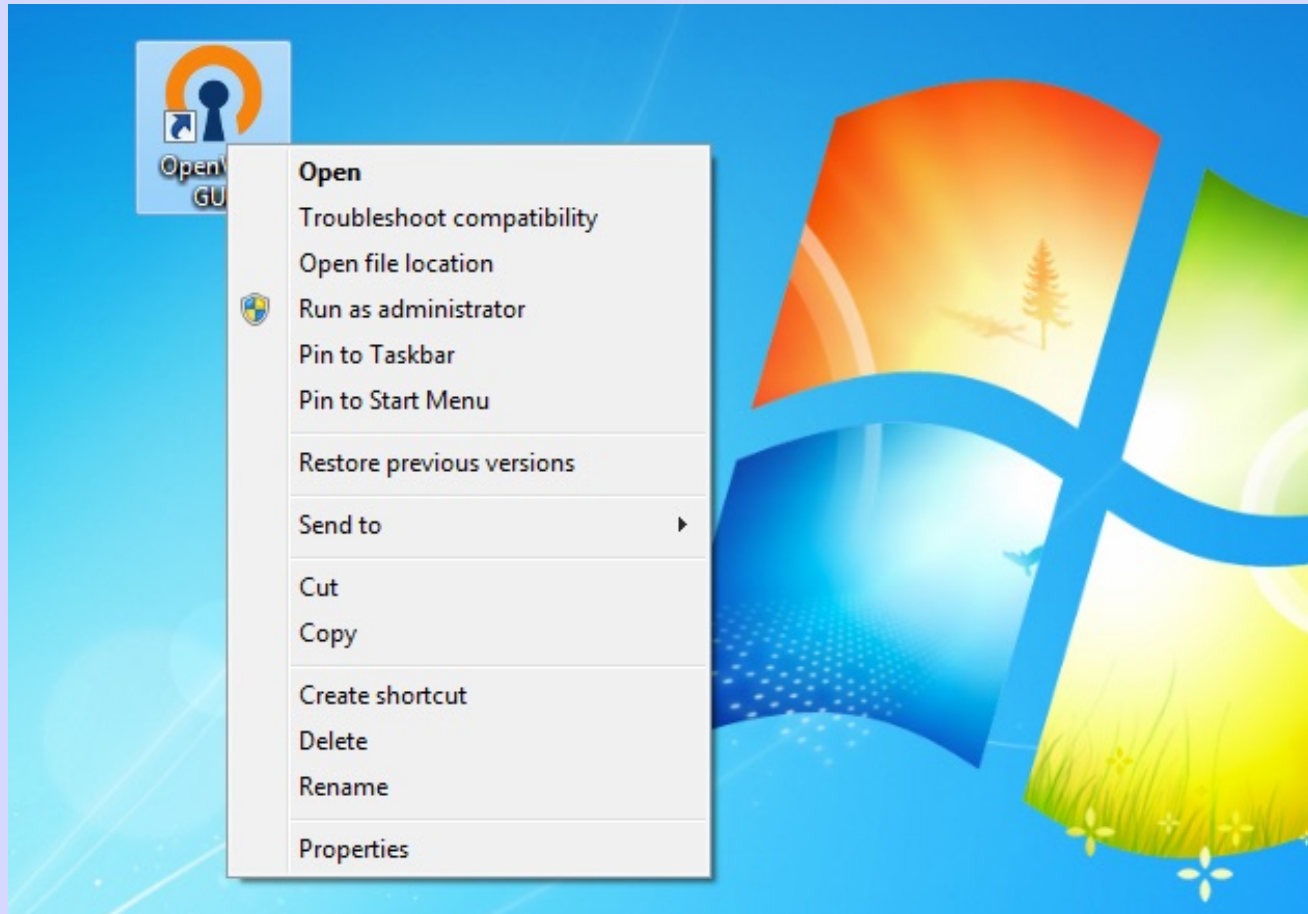
# Download Installer



# Run Installer

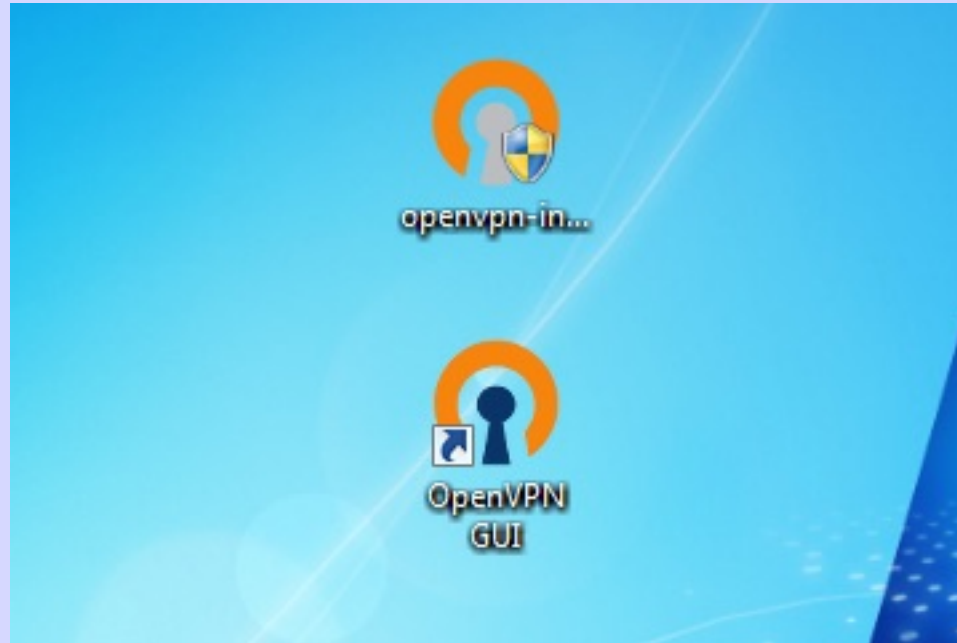


# Set RunAsAdmin



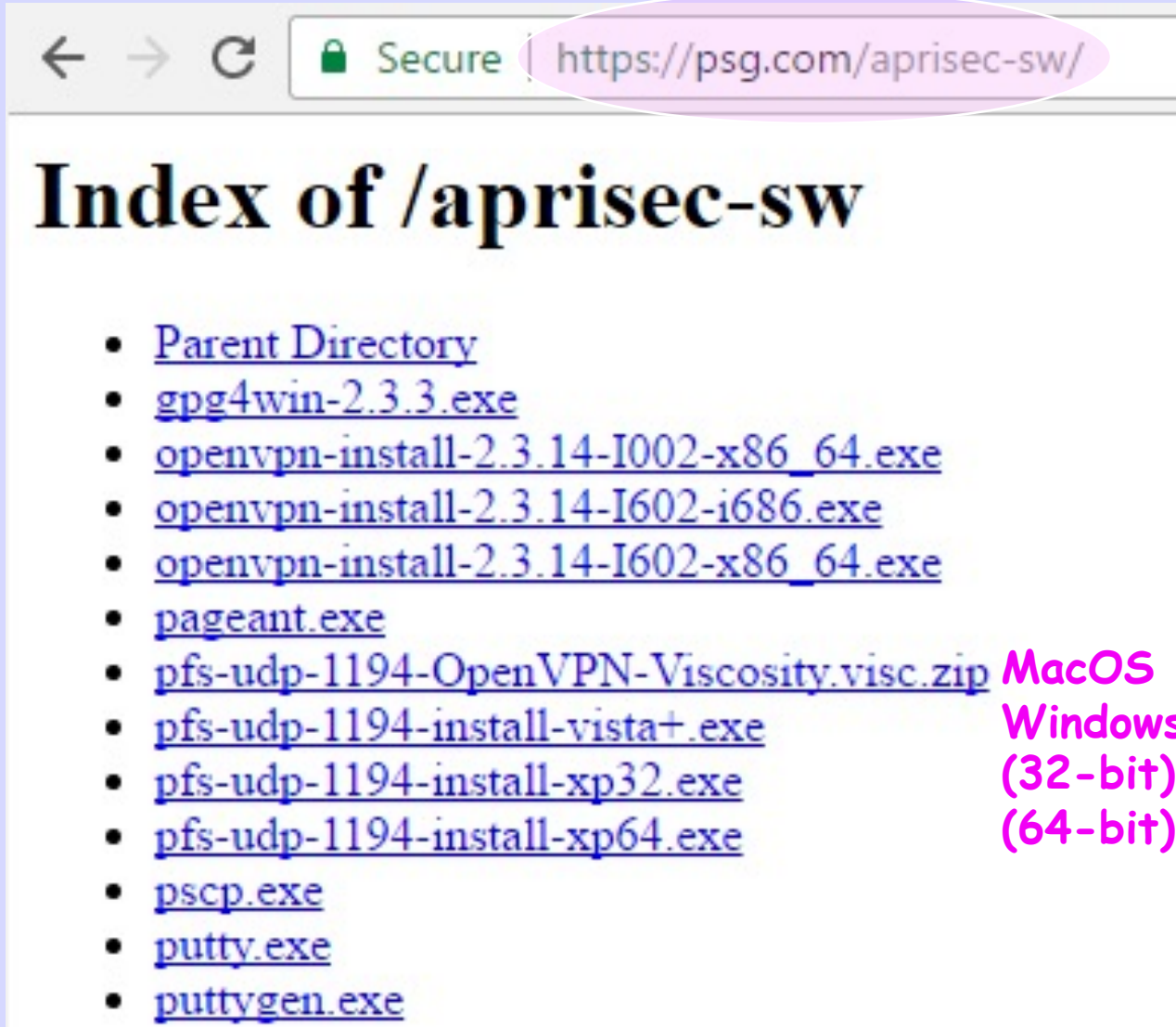
So Client Can Install Routes

# 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/" and a "Secure" indicator. The main content area is titled "Index of /aprisec-sw" and lists a directory of files and executables. The files listed are: Parent Directory, gpg4win-2.3.3.exe, openvpn-install-2.3.14-I002-x86\_64.exe, openvpn-install-2.3.14-I602-i686.exe, openvpn-install-2.3.14-I602-x86\_64.exe, pageant.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, pscp.exe, putty.exe, and puttygen.exe.

Index of /aprisec-sw

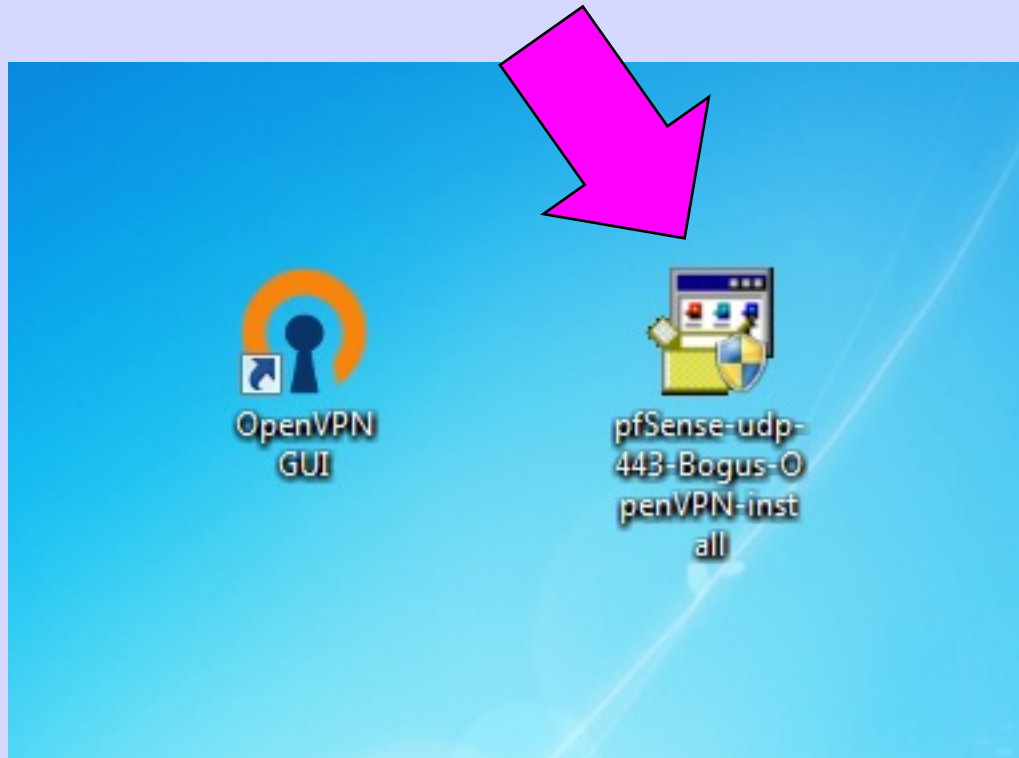
- [Parent Directory](#)
- [gpg4win-2.3.3.exe](#)
- [openvpn-install-2.3.14-I002-x86\\_64.exe](#)
- [openvpn-install-2.3.14-I602-i686.exe](#)
- [openvpn-install-2.3.14-I602-x86\\_64.exe](#)
- [pageant.exe](#)
- [pfs-udp-1194-OpenVPN-Viscosity.visc.zip](#)
- [pfs-udp-1194-install-vista+.exe](#)
- [pfs-udp-1194-install-xp32.exe](#)
- [pfs-udp-1194-install-xp64.exe](#)
- [pscp.exe](#)
- [putty.exe](#)
- [puttygen.exe](#)

MacOS

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



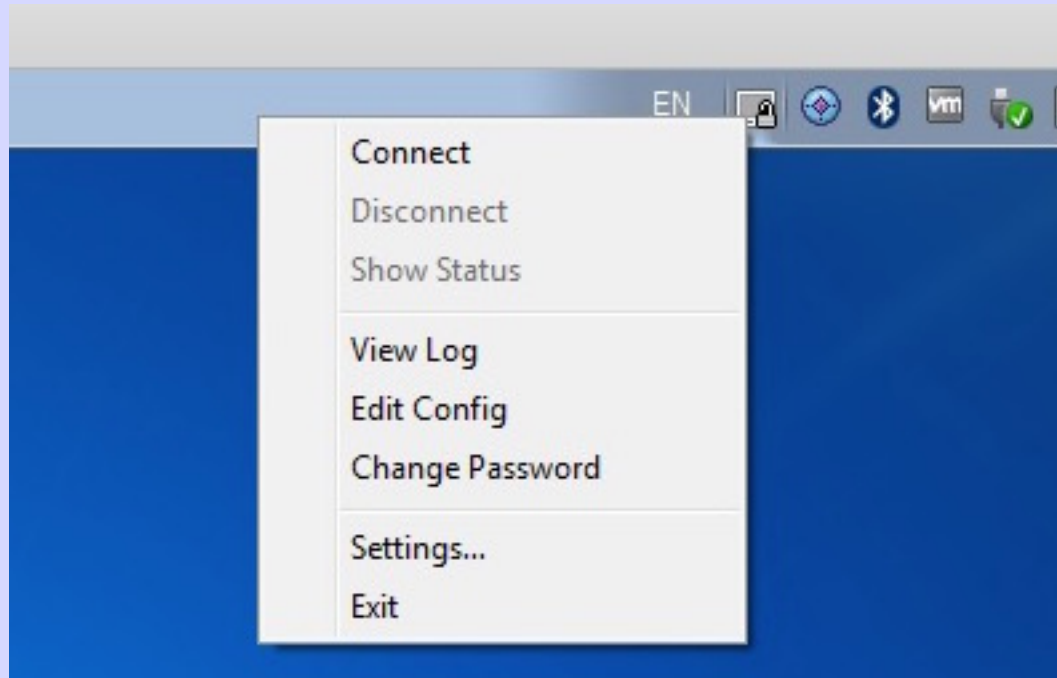
# Execute Credential EXE



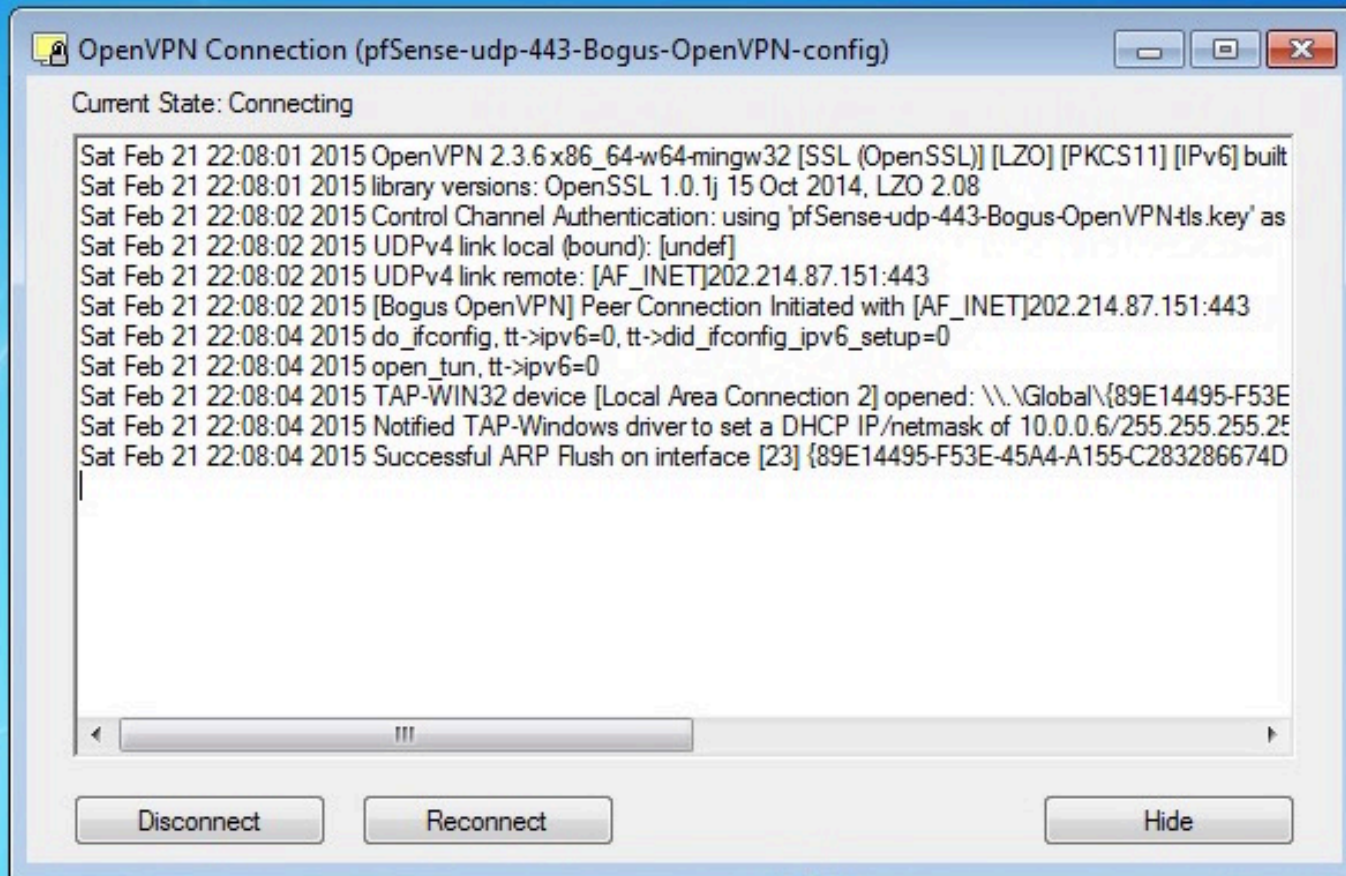
# Install Credentials



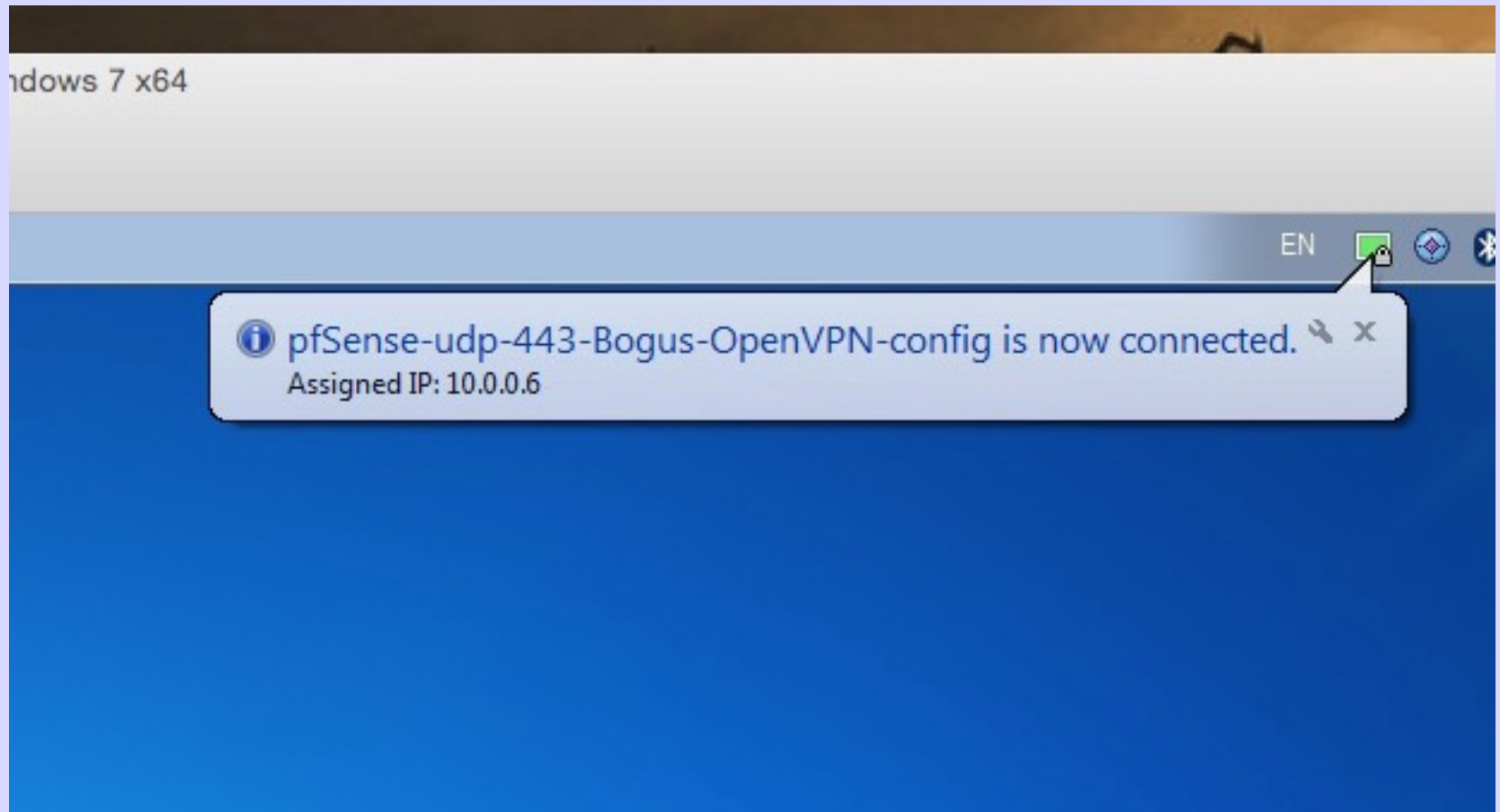
# Connect



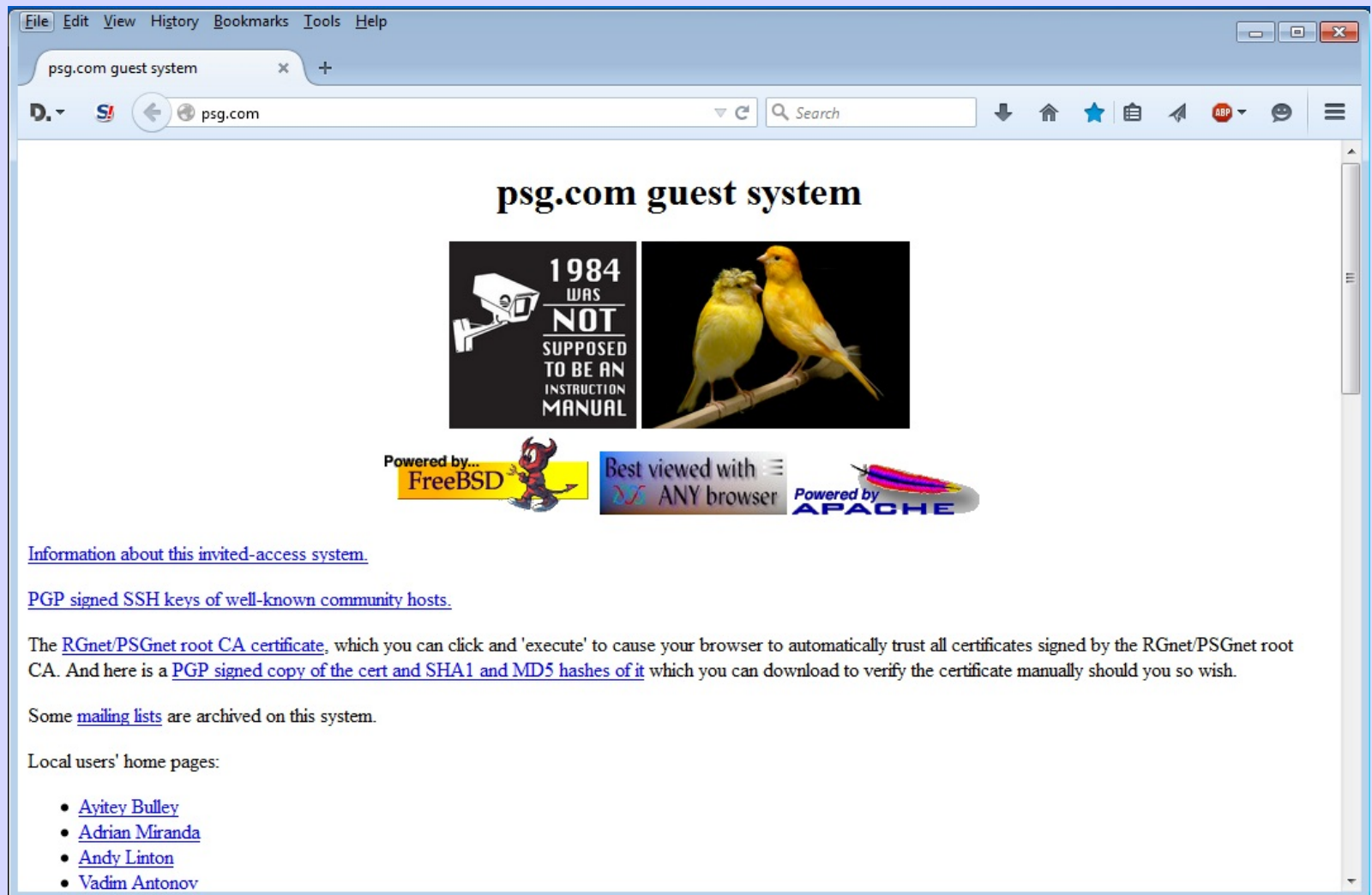
# Connecting



# 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.psg.com:/Users/presenter> traceroute psg.com
traceroute to psg.com (147.28.0.62), 64 hops max, 52 byte packets
 1 252.151.dhcp.conference.apricot.net (220.247.151.252) 1343.693 ms 1.342 ms 1.108 ms
 2 ci53.23-213.netnam.vn (101.53.23.213) 1.390 ms 1.635 ms 1.551 ms
 3 172.20.1.2 (172.20.1.2) 1.625 ms 1.587 ms 1.734 ms
 4 1-43_2313.r0.409.mi.hk.iptp.net (103.6.131.174) 66.879 ms 51.207 ms 53.409 ms
 5 63-218-211-141.static.pccwglobal.net (63.218.211.141) 266.357 ms 207.636 ms 224.782 ms
 6 hundredge0-5-0-0.br02.hkg08.pccwbtn.net (63.223.29.198) 54.618 ms 52.381 ms 51.697 ms
 7 63-218-205-86.static.pccwglobal.net (63.218.205.86) 52.479 ms 56.466 ms 52.707 ms
 8 ae-12.r24.osakjp02.jp.bb.gin.ntt.net (129.250.2.223) 104.518 ms * 105.996 ms
 9 ae-4.r20.sttlwa01.us.bb.gin.ntt.net (129.250.2.39) 180.351 ms 182.174 ms
   ae-12.r24.osakjp02.jp.bb.gin.ntt.net (129.250.2.223) 104.324 ms
10 ae-4.r20.sttlwa01.us.bb.gin.ntt.net (129.250.2.39) 182.066 ms
   ae-29.r05.sttlwa01.us.bb.gin.ntt.net (129.250.2.89) 211.749 ms
   ae-4.r20.sttlwa01.us.bb.gin.ntt.net (129.250.2.39) 184.729 ms
11 ae-29.r05.sttlwa01.us.bb.gin.ntt.net (129.250.2.89) 209.519 ms
   ae-28.r05.sttlwa01.us.bb.gin.ntt.net (129.250.2.45) 208.254 ms
   ae-29.r05.sttlwa01.us.bb.gin.ntt.net (129.250.2.89) 209.292 ms
12 psg.com (147.28.0.62) 216.953 213.717 218.281
```



# 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
```