

2-3-1 OpenVPN

OpenVPN Server

pfSense

The screenshot displays the pfSense web interface. At the top, a navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Status: Dashboard'. It features two primary panels: 'System Information' on the left and 'Interfaces' on the right. The 'System Information' panel contains a table of system details and several progress bars for resource usage. The 'Interfaces' panel shows the 'WAN' interface with its IP address and speed. A large 'pfSense' watermark is overlaid on the center of the dashboard.

Status: Dashboard

System Information

Name	pfSense.localdomain
Version	2.2-RELEASE (i386) built on Thu Jan 22 14:04:25 CST 2015 FreeBSD 10.1-RELEASE-p4 You are on the latest version.
Platform	pfSense
CPU Type	QEMU Virtual CPU version 1.1.2
Uptime	1 Day 09 Hours 51 Minutes 35 Seconds
Current date/time	Mon Feb 23 0:48:37 UTC 2015
DNS server(s)	127.0.0.1 8.8.8.8
Last config change	Sun Feb 22 8:21:22 UTC 2015
State table size	0% (93/47000) Show states
MBUF Usage	2% (510/26584)
Load average	0.06, 0.03, 0.00
CPU usage	0%
Memory usage	11% of 479 MB
SWAP usage	0% of 1024 MB
Disk usage	/ (ufs): 5% of 6.8G /var/run (ufs in RAM): 3% of 3.4M

Interfaces

WAN	↑	1000baseT <full-duplex> 202.214.87.151
-----	---	---

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [\[view license\]](#)

VPN Server

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'VPN' menu is expanded, showing options for IPsec, L2TP, OpenVPN, and PPTP. The main content area is titled 'OpenVPN: Server'. Below the title are tabs for Server, Client, Client Specific Overrides, Wizards, Client Export, and Shared Key Export. The 'Server' tab is active, displaying a table with the following data:

Disabled	Protocol / Port	Tunnel Network	Description
NO	UDP / 443	10.0.1.0/24	Workshop OpenVPN

Below the table, there is a text box with the message: 'Additional OpenVPN servers can be added here.'

Configuration!

Server	Client	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 Workshop OpenVPN
You may enter a description here for your reference (not parsed).

Cryptographic Settings

TLS Authentication ☒ Enable authentication of TLS packets.

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
d8762c03b6376ac5273019ef71c7b80c
c01da0ae9c3bd535f529ad353fcee46
-----END OpenVPN Static key V1-----
```

Paste your shared key here.

Peer Certificate Authority OpenVPN Client CA

Peer Certificate Revocation List No Certificate Revocation Lists (CRLs) defined.
Create one under System > Cert Manager.

Server Certificate Bogus OpenVPN (CA: OpenVPN Client CA) *In Use

DH Parameters Length 2048 bits

Encryption algorithm BF-CBC (128-bit)

Auth Digest Algorithm SHA1 (160-bit)
NOTE: Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.

Hardware Crypto No Hardware Crypto Acceleration

Certificate Depth Two (Client-Intermediate-Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Tunnel Settings

IPv4 Tunnel Network 10.0.1.0/24
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)

IPv6 Tunnel Network
This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (eg. fe80::/64). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)

Redirect Gateway ☒ Force all client generated traffic through the tunnel.

Concurrent connections
Specify the maximum number of clients allowed to concurrently connect to this server.

Compression No Preference
Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

Type-of-Service ☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication ☐ Allow communication between clients connected to this server.

Select a Client

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

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

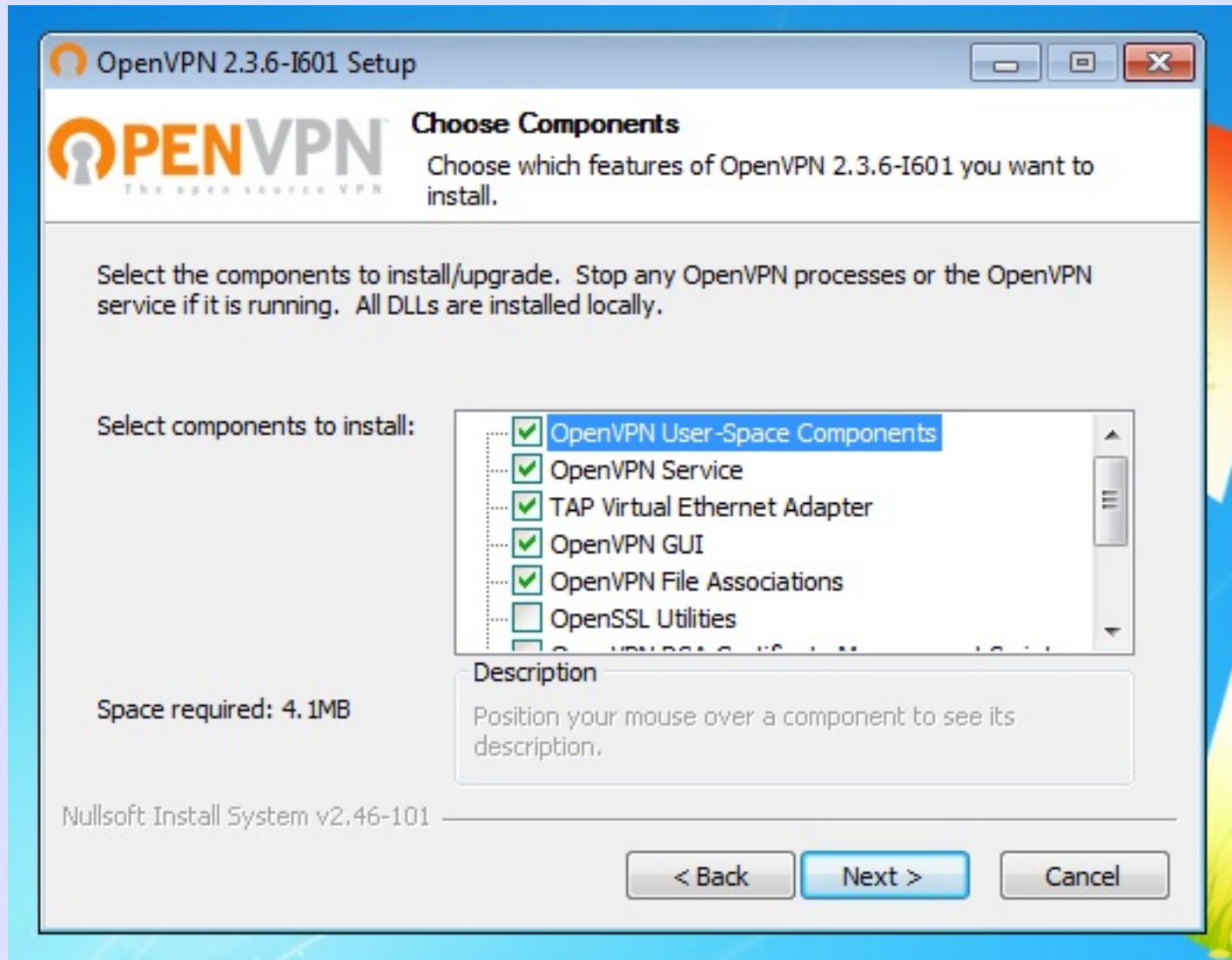
Viscosity - Recommended GUI client for Mac OSX \$\$

Tunnelblick - Free client for OSX

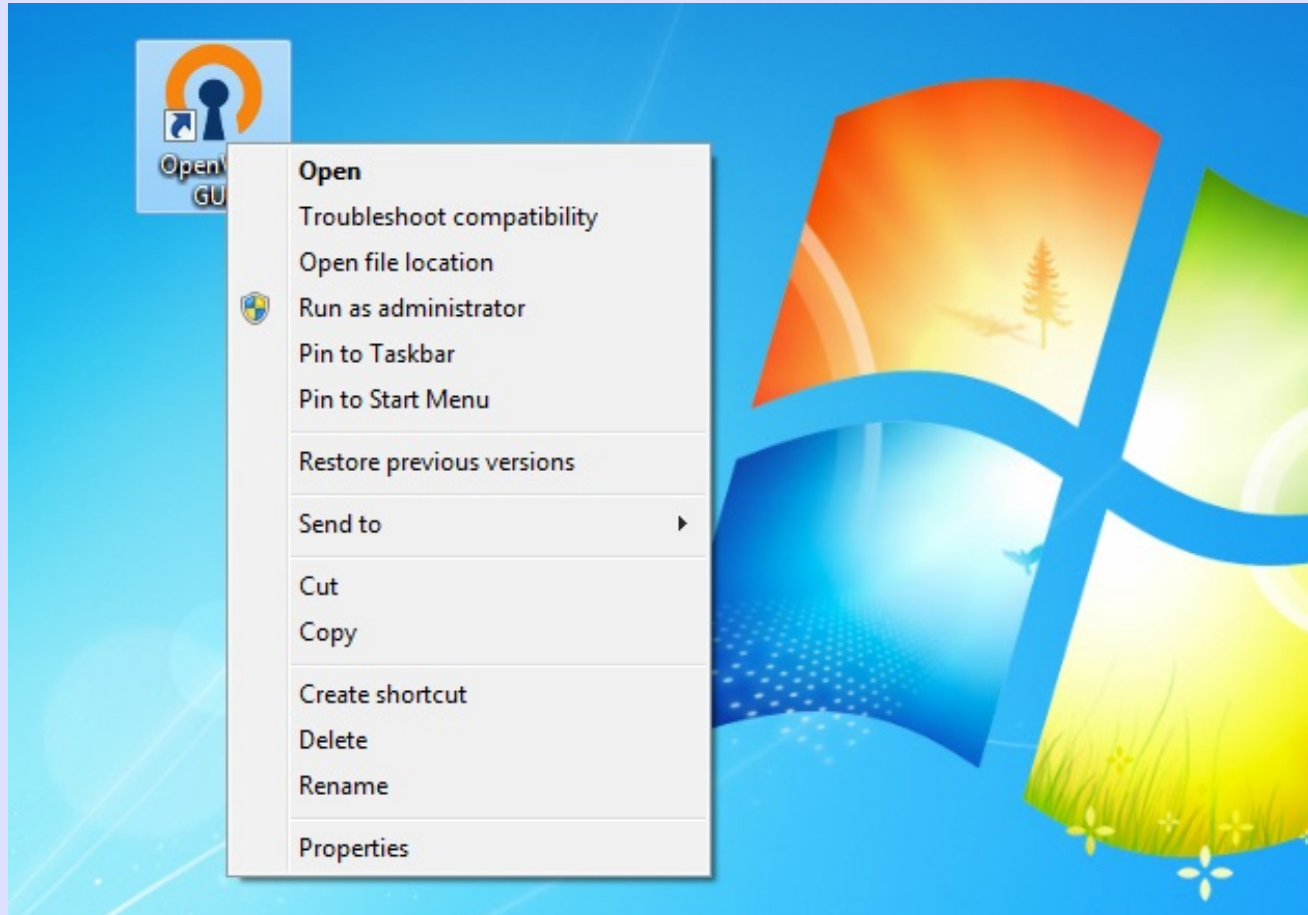
Download Installer



Run Installer

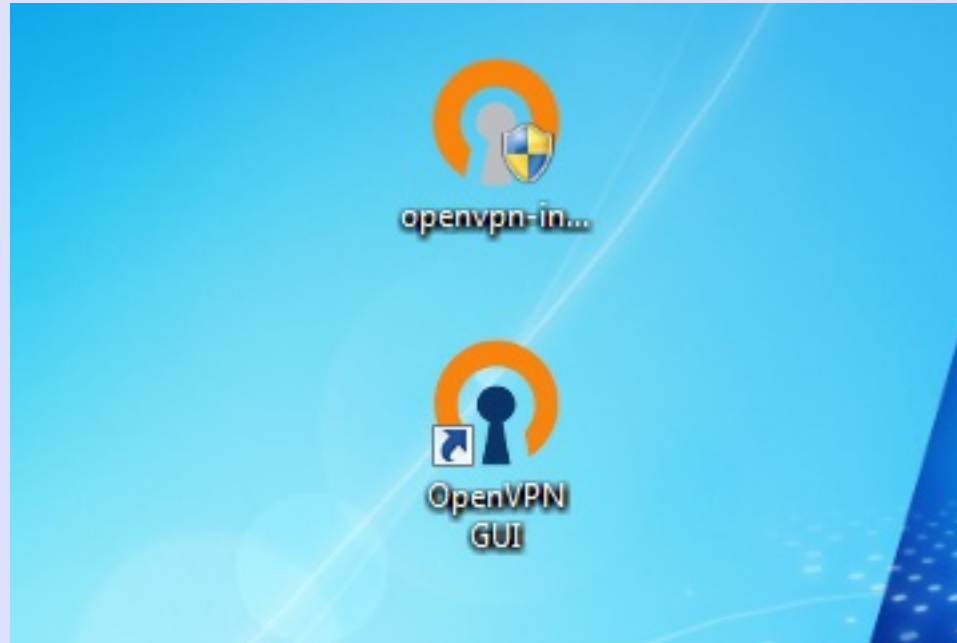


Set RunAsAdmin



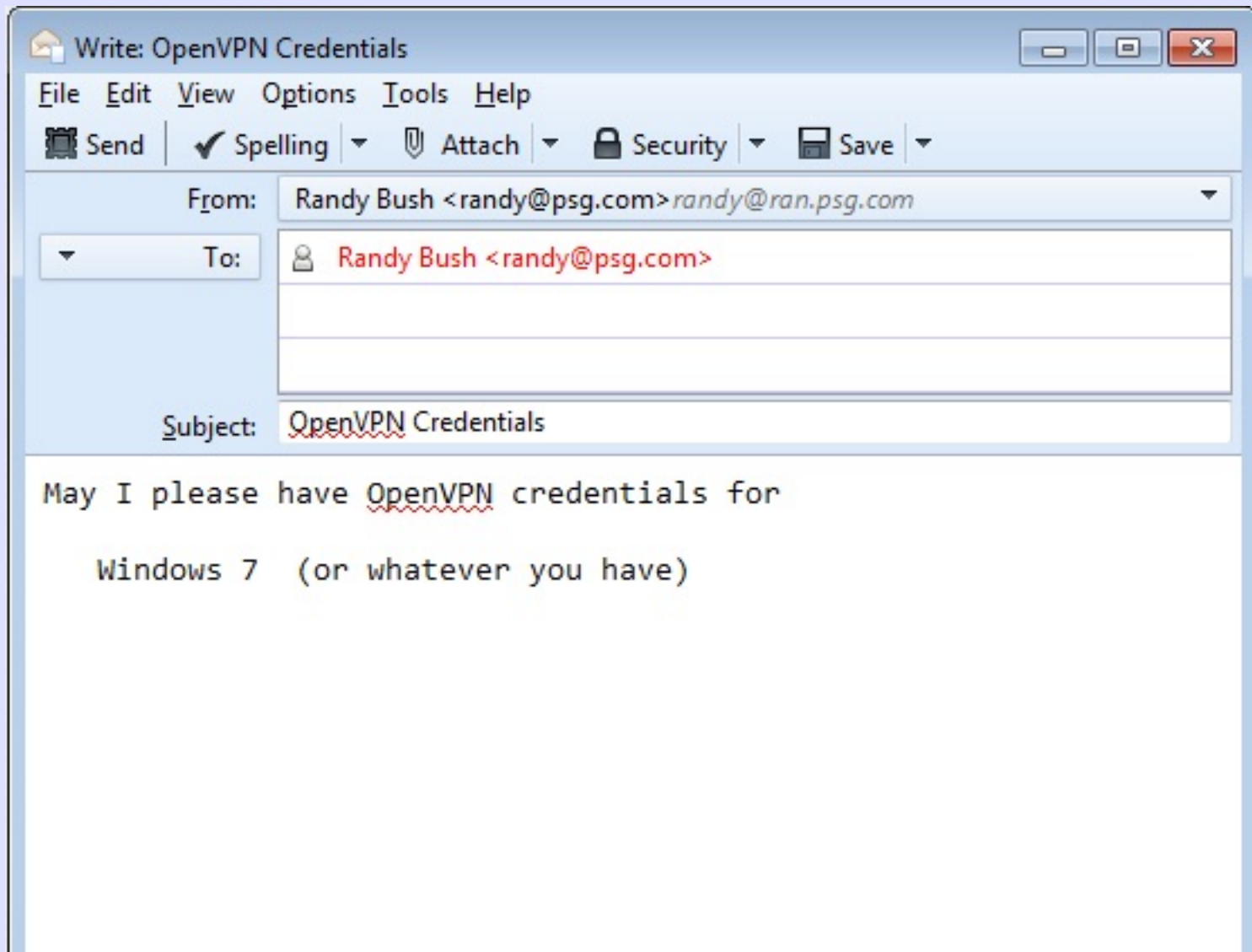
So Client Can Install Routes

Open GUI (invisible)



You Can Delete Installer

Ask For Credentials



Save Credentials

From Me★

Subject **Re: OpenVPN Credentials**

To Me★

21:39

Other Actions ▾

1 attachment: pfSense-udp-443-Bogus-OpenVPN-install.exe 1.9 MB

Save ▾

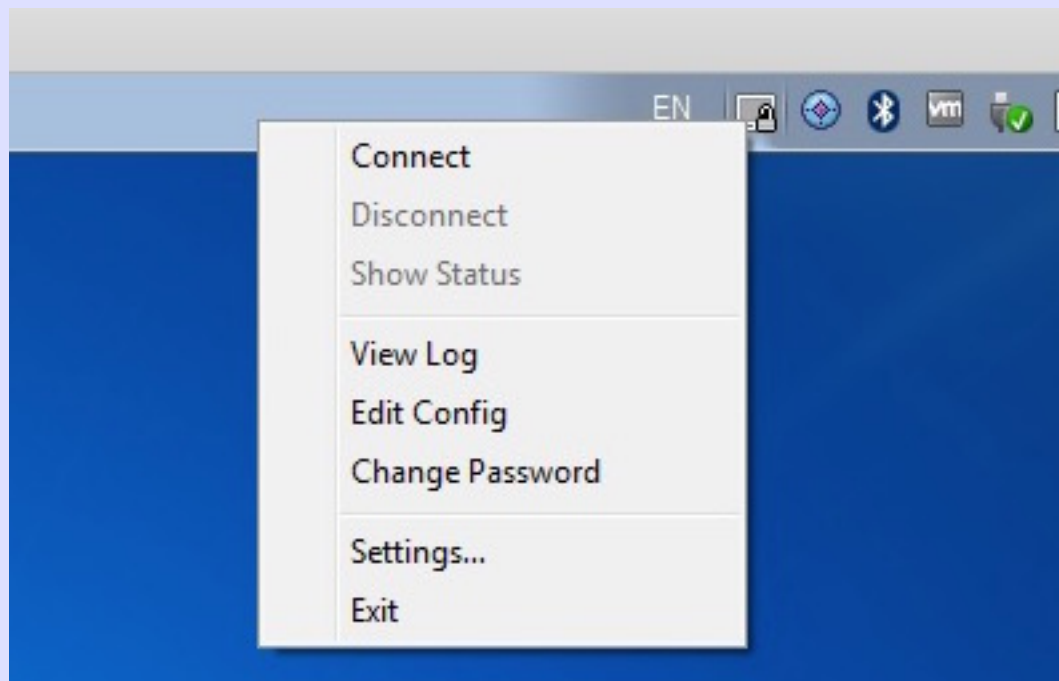
Execute Credential EXE



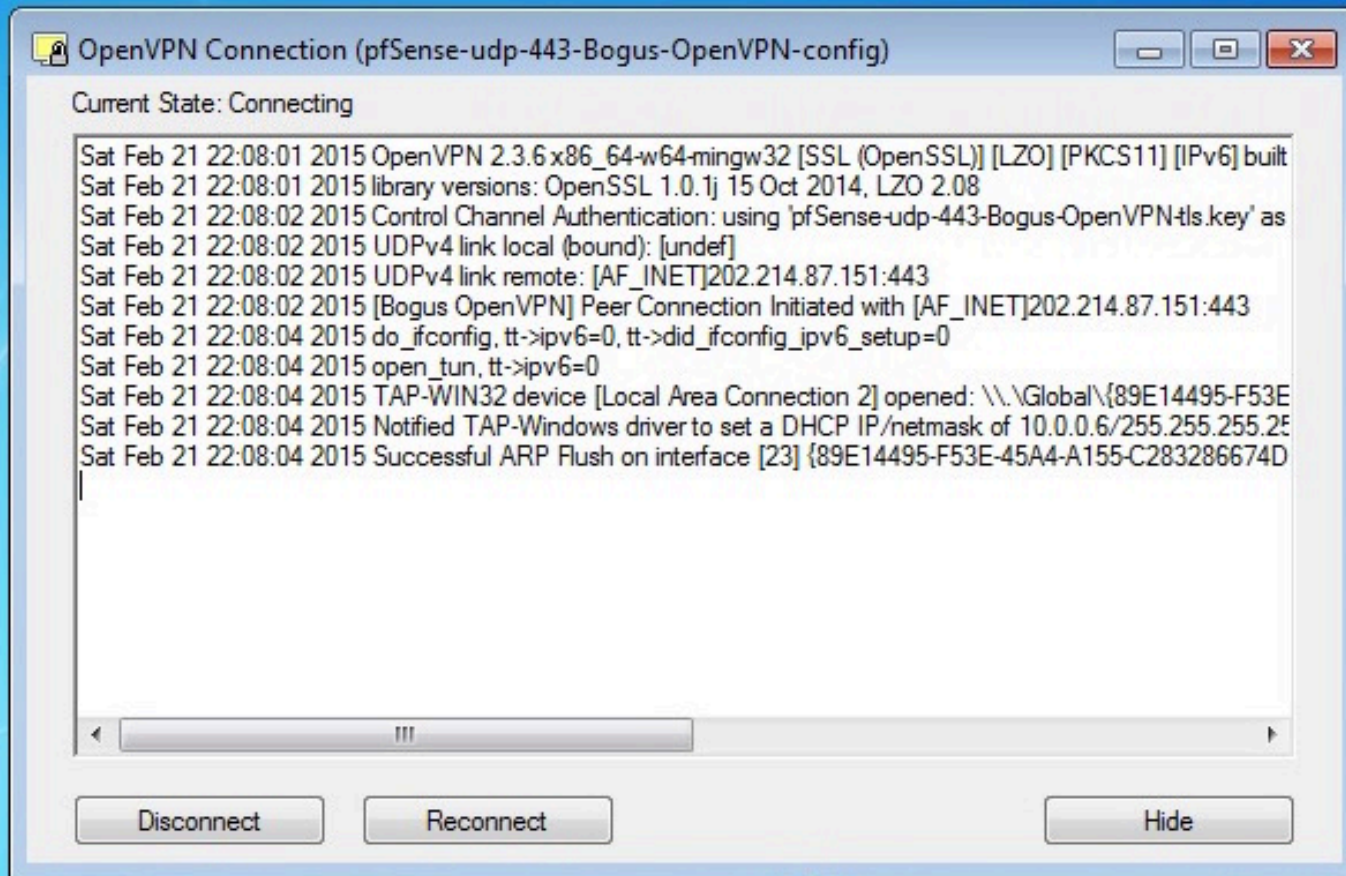
Install Credentials



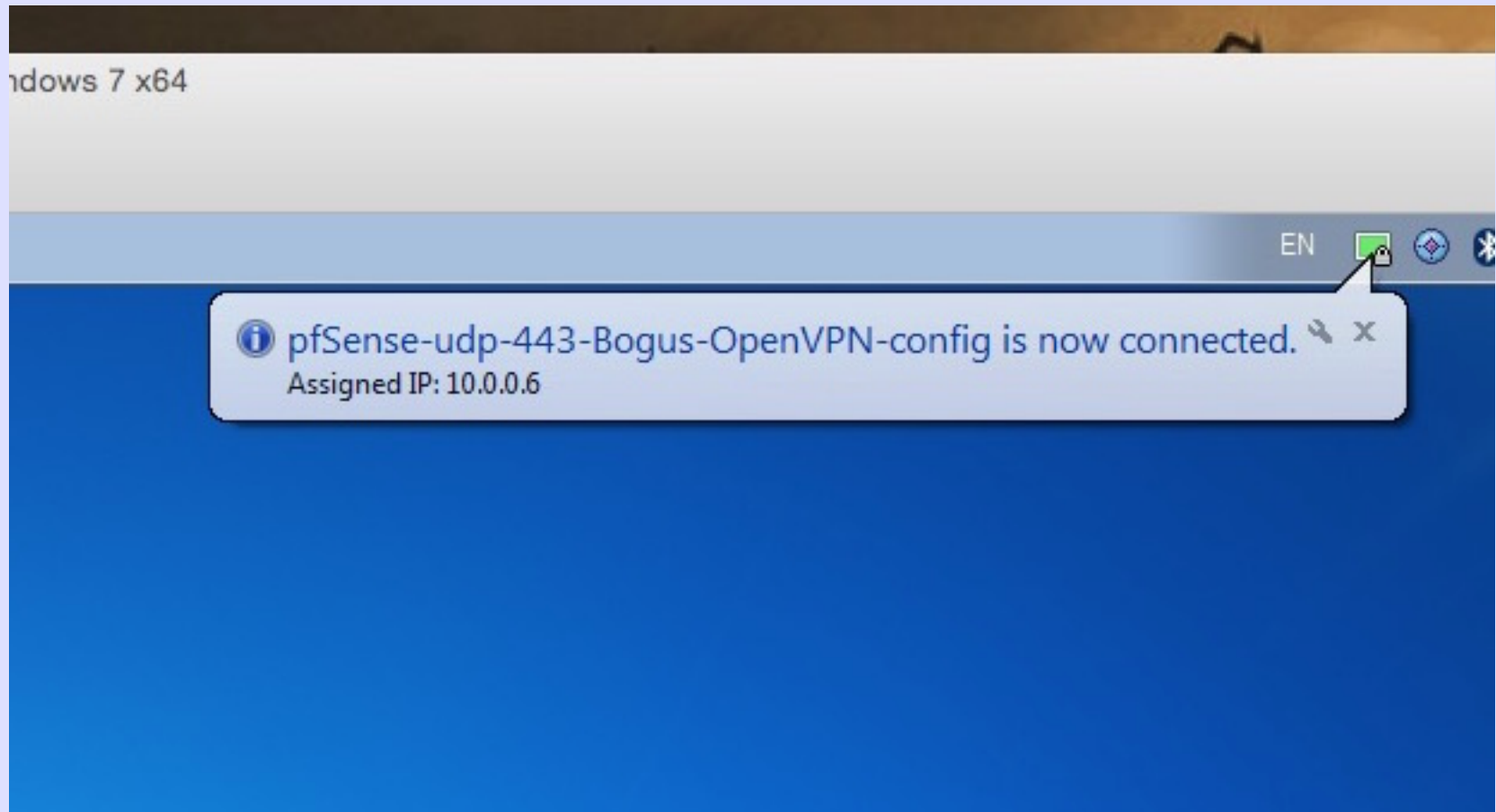
Connect



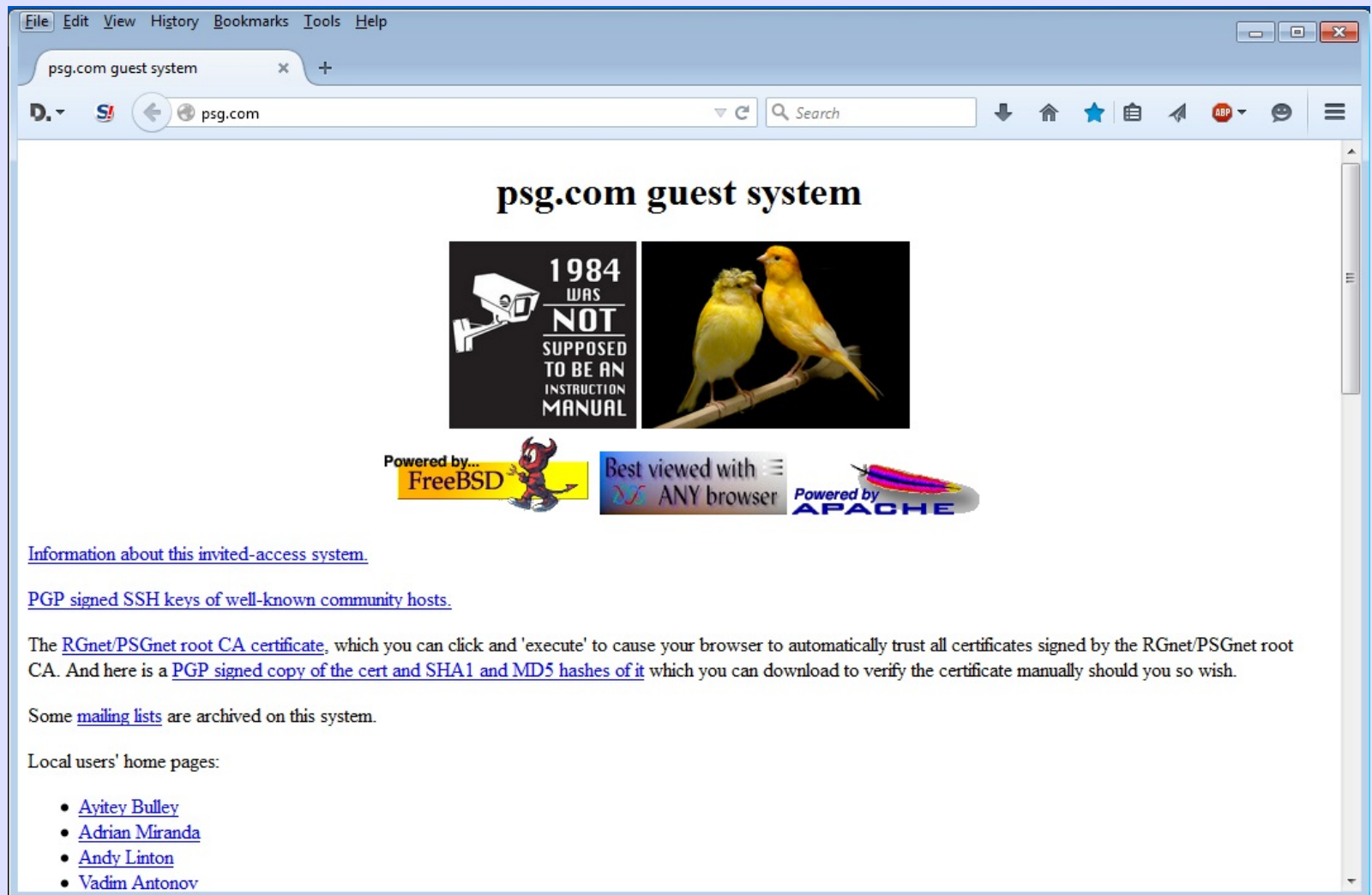
Connecting



You're Connected!



Try It - Browse



But How Do You Know It Works?

Is your traffic encrypted?

The WireShark lab will teach you
how to look at the packets