Secbase.org
Hopefully, A Safer Way to be on the Internet :-)

June 06, 2023

By Aaron Grothe

Introduction

If anybody has any questions or comments at any time please let me know.

If I start to mumble please let me know as well :-)

The project will be live at https://secbase.org when I get closer to finished :-)

Secbase.org???

Components of a secbase system

Host machine - where everything runs
Virtualization layer
Secured VM running on Virtualization Layer
Safe Network Layer

Untrusted VM on Virtualization Layer

Secured VM could also be running on hardware (spare pc, raspberry pi, router, etc)

Goals

- A simple VM that you can use to protect your system when you fire up a different VM
- This provides a protected environment that you can use to securely test a VM
- Something that people can easily recreate by following instructions. Don't need to trust an .iso or .img from me, you can make your own
- Lots of options to how to build your system
- Provide the ability to do things like beat GeoIP blocks and the like
- Get it to the point where you can run it from a USB drive

Website

- Eventually there will be several writeups for options for the secbase.

Current Status

- It wasn't working until last night :-)
- Current setup has had a lot issues - will go into some of those later
- Have been learning a lot the last couple of weeks trying to get this working in a consistent manner

Current Attempt

This is the breakdown of the current system I'm working with

Virtualization Layer: Oracle Virtualbox
Trusted VM: OpenWRT
Anonymization Layer: OpenVPN
Untrusted VM: Debian 11. 12 is around the corner :-)

Wasn't working until Monday night

Current Attempt - Issues (Fixed?)

Lot of the issues came down to the OpenWRT layer having issues

Virtualbox doesn't like to work with Tun (Level 3)
OpenWRT's OpenVPN software is giving me issues with Tap (Level 2)

So having trouble getting the system to work either of the two routing options

Mostly devices aren't showing up and without that you're kind of doomed.

Current Attempt - Issues (Fixed?)

Other big issue was the VPN I was using wasn't working.

????

It would come up, but it would not be able to finish the connection. So no tun device, didn't figure it out until I started reading the logs

Tun/Tap?

TAP carries Ethernet frames
TUN carries IP packets (routing)

TUN/TAP - devices used by Wireguard and OpenVPN

L2TP/IKE doesn't use TUN/TAP

Haven't really played with TUN/TAP in years, mostly back when I was doing User Mode Linux (UML).

Demo

Time to do a quick demo.

Hopefully, it'll go smoothly tonight

Demo

Lets do an ipleak test

https://ipleak.net
https://ipleak.com

Lets do a Panoptiklik test

https://coveryourtracks.eff.org/

Demo

IPleak

Does a pretty good job hiding your IP information

PanOpticlick / Cover Your Tracks

We still have some bits of uniquely identifiable data :-(

Time to Talk about some of the Options

We'll go over options for the following

- Virtualization Options
- Trusted VM Options
- Secure Network Options

There are a lot of options here, so let's get started

Virtualization Options

- Oracle VirtualBox
- Vmware Workstation Player
- Qemu/KVM
- Gnome Boxes
- Hyper-V
- Docker???
- Xen and many others

What you want in a Virtualization Option

- The ability to have internal/host only networks - you're counting on this to force all traffic to go through the internal-only network to the Trusted VM
- The ability to run multiple VMs concurrently
- You're counting on the VM to separate and isolate the VMs from the underlying system
- The ability to checkpoint/restore both the VMs is really nice - get the Trusted VM locked down and then restore it before every use

Oracle VirtualBox

Oracle VirtualBox is a cross-platform Virtualization product

Pros

- Free (if you don't use the Extension Pack)
- Cross-platform - works on Linux/Windows/Mac OS
- Pretty good - version 7, works pretty well
- Open Source version is available

Cons

- Performance can be an issue

VMware Workstation Player

VMware Player is VMware's free virtualization product

Pros:

- Free
- Works on Linux/Windows

Cons:

- Have to jump through hoops to create a new VM
- Commercial product, no Source code for you

Qemu/KVM

Qemu (Quick Emulator) is an Open Source emulator, that uses KVM as an optional accelerator

Pros

- Open Source
- Multiple Platforms

Cons

- Not always the most user friendly, there are guis that help with that aqemu

Others

- Gnome Boxes - is a GUI wrapper for virtualization, still early days - Linux only, Gnome Only
- Hyper-V - Windows only
- Docker - works well on Linux, on other platforms works with a virtualization layer, networking can be a bit of a pain

Ideally guides can be written for any of these as part of the projects, but they won't be a part of it too early

Trusted VM Options

Several options seem to stand out for the Trusted VM

- OpenWRT
- Cut down Debian/Fedora/etc…
- IPfire
- PFsense
- DD-WRT, Tomato, etc
- Others

What you're looking for in a Trusted VM

What you want in a Trusted VM

- Small
- Fast
- Secure
- Software for the VPN option you choose
- Updateable

OpenWRT

OpenWRT is a very small distro that works on many routers

Pros

- Has x86-64 version which is the one that interests us
- Size (1gb disk and 128Mb of ram is plenty)
- Has a Web GUI
- Web Plugins for Wireguard, Open VPN

Cons

- Being minimal distro doing things can be tough
- Don't have a GUI for everything

Cut Down Debian/Fedora, etc.

Cut Down Debian/Fedora, etc is a minimal install of a regular distro

Pros

- Use your favorite distribution as a base
- Lot of tools are available, some vendors have custom VPN software packages

Cons

- Probably can't get it as small as OpenWRT

DD-WRT/Tomato Router

Similar distributions to OpenWRT, designed for routers

Pros

- Small distributions
- If you have experience with either of them might be a better choice than OpenWRT

Cons

- Less hardware support
- Lack of a regular package manager can be annoying

IPfire/PFsense

Another couple of other security distros

Pros

- Some of the distros have specialized tools to do things like OpenVPN and so on
- Small distributions, customized, special security options and so on

Cons

- Can be a bit tough to use that way

Secure Networking Options

For this we're considering the following network options

- WireGuard
- OpenVPN
- L2TP/IKE
- Tor
- Others

What you're looking for in a VPN

What you're looking for in a VPN solution

- Secure
- No logs
- Owned by a US Company
- Can you buy it via bitcoin or other crypto-currency

Wireguard

Wireguard is the up and coming VPN solution

Pros

- Pretty small code base (in the Linux kernel)
- Pretty efficient

Cons

- Not all VPN services support it yet
- Setup can be difficult

OpenVPN

OpenVPN is the most common VPN solution

Pros

- Works on about any system
- Most VPNs support it
- Works with UDP and TCP

Cons

- Slower than wireguard
- Not part of Linux kernel

L2TP/IPsec

OpenVPN is the most common VPN solution

Pros

- Faster than OpenVPN
- Considered secure

Cons

- Suggested that NSA may have compromised the protocol
- Dropped from TAILS due to concerns about security
- Not all implementations are considered equal

TOR

The Onion Router (TOR) was developed by the US Navy

Pros

- Can be pretty secure

Cons

- Performance
- If an exit node is controlled by a bad actor it is very insecure

VPNs

VPN Options

Pretty much break down into three major options

1. Pick a well regarded one: SurfShark, NordGuard, etc…
2. Go with a cheap one - StackSocial.com anyone
3. Go with a free one - not sure about that

Stacksocial - has options from $20.00 on up. How much you trust any VPN based on reputation and so on.

VPNs

VPN Options

Read the requirements for your VPN

- Some allow torrenting, some don't
- Don't put too much trust into any VPN, it is defense in depth
- Try and use the UDP version of the OpenVPN it tends to be faster
- Some VPNs will work with services like Netflix, some won't

Similar Systems

Whonix has a version of their software that works on some of the same concepts

Whonix has two Debian based VM images
Whonix uses Tor for routing

They have a lot of really good documentation on their site

There is also a version of Qubes that has some of these potential capabilities

Similar Systems

Another options is that you can easily buy a router with OpenWRT already installed

We'll head over to Amazon - GL.iNet GL-SFT1200 (Opal) Secure Travel WiFi Router – AC1200 Dual

Is one of the ones I have. I use it with Windscribe and it is pretty good. Works with Netflix and other things pretty well.

Things I wish I knew/Did differently

- Make a VM and just get the VPN software working on it. That will help you isolate the VPN issues from OpenWRT/Virtualbox issues
- The option on openwrt to read the logs of the system is logread - use that
- Don't believe what the OpenWRT GUI tells you, it will show things are up and they might be fully configured
- Run benchmarks with speedof.me and other network tools if you want to see the VPN impact

Links

- Secbase - https://www.secbase.org - currently empty - will hopefully be getting some content over the next couple of months
- OpenWRT - https://www.openwrt.org - good basic router software
- StackSocial - https://www.stacksocial.com - good place to buy a cheap VPN license
- Whonix.org - https://www.whonix.org - interesting project, with some good documentation

Thanks and Q&A

That's all I've got for tonight.

Thanks for Listening.

Any Questions???