QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

Pat Baker – Technologist/Consultant/Futurist
Otakusystems.LLC
info@otakusystems.com

Penguicon 2019

About Me

Philosophy, Information Assurance (CyberSecurity), Intelligence Analyst

OtakuSystems LLC
otakusystems.com
twitter: @otakusystems

Technologist, Futurist, Philosopher, Geek

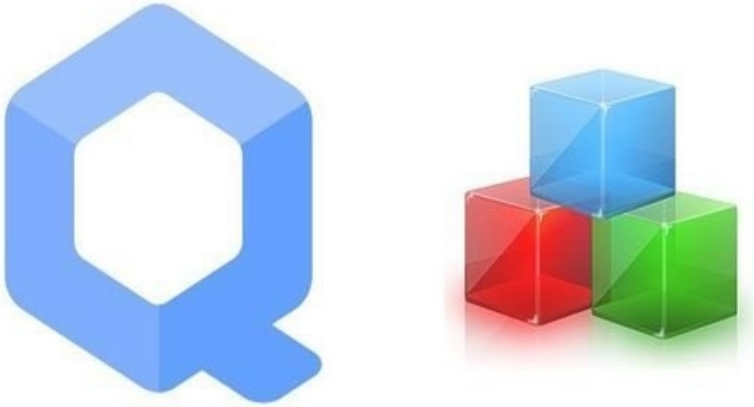
- Seeker of wisdom and knowledge -

-Disclaimer-

Not responsible for any damage done to you, your friends, your accounts, your gold fish, etc. All information is for education or general knowledge purpose. Information held within may or may not be legal by your country state or region.

If its not legal, then you should not do it?

Qubes OS



QUBES OS

Qubes OS is a security-focused desktop operating system that aims to provide security through isolation. Virtualization is performed by Xen, and user environments based on Fedora, Debian, and Whonix.

On February 16, 2014, Qubes was selected as a finalist of Access Innovation Prize 2014 for Endpoint Security Solution.

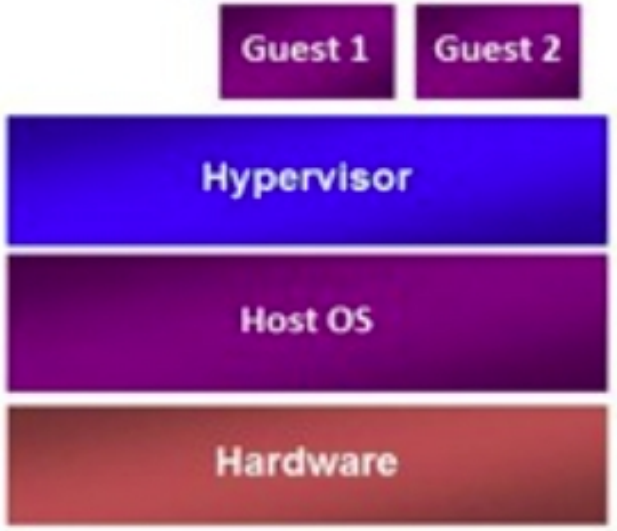
What is Qubes?

- Qubes OS is a security-oriented ‘Security by Isolation’ operating system.
- “Type 1” or “Bare Metal” Xen based hypervisor. www.xenproject.org
- Programs are isolated (compartmentalize) in their own separate qubes, but all windows are displayed in a single, unified desktop environment with colored borders.

Hypervisor Design:

Two approaches

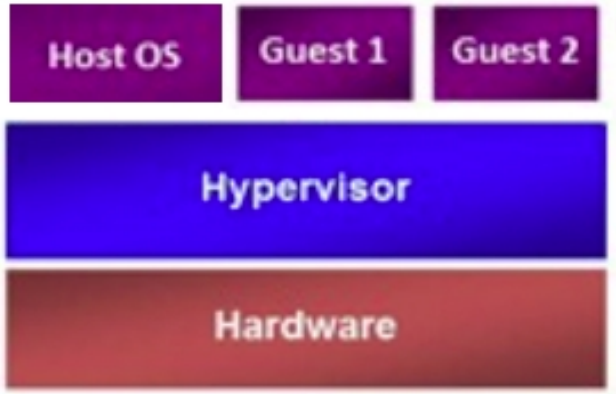
Type 2 Hypervisor



Examples:

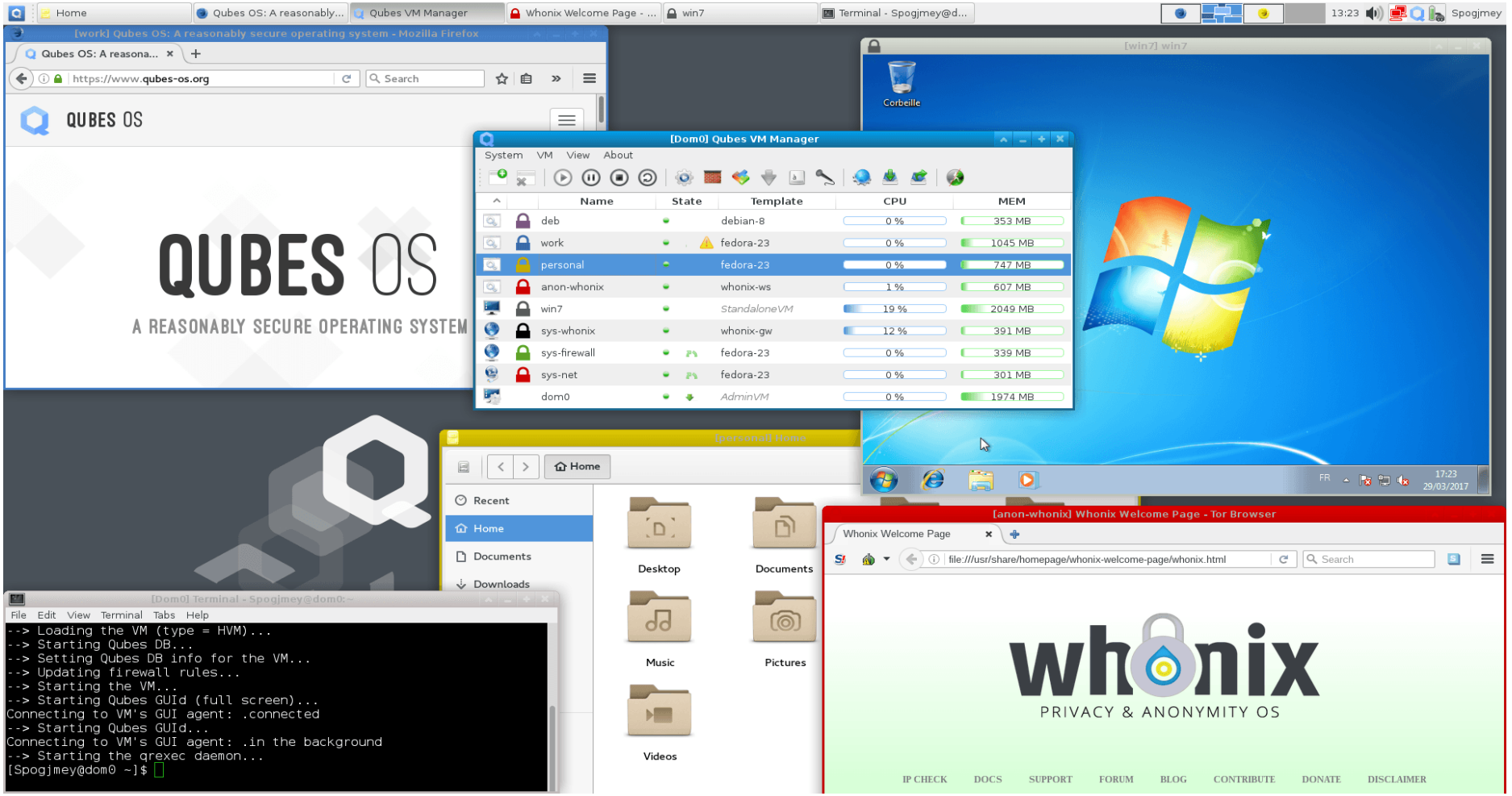
- Virtual PC & Virtual Server
- VMware Workstation
- KVM

Type 1 Hypervisor



Examples:

- Hyper-V
- Xen
- VMware ESX


Home
Qubes OS: A reasonably...
Qubes VM Manager
Whonix Welcome Page - ...
win7
Terminal - Spogjmey@d...
13:23
Spogjmey
[work] Qubes OS: A reasonably secure operating system - Mozilla Firefox
Qubes OS: A reasona...
https://www.qubes-os.org
Search
QUBES OS
QUBES OS
A REASONABLY SECURE OPERATING SYSTEM
[Dom0] Qubes VM Manager
System VM View About
Name State Template CPU MEM
deb debian-8 0 % 353 MB
work fedora-23 0 % 1045 MB
personal fedora-23 0 % 747 MB
anon-whonix whonix-ws 1 % 607 MB
win7 StandaloneVM 19 % 2049 MB
sys-whonix whonix-gw 12 % 391 MB
sys-firewall fedora-23 0 % 339 MB
sys-net fedora-23 0 % 301 MB
dom0 AdminVM 0 % 1974 MB
[win7] win7
Corbeille
FR
17:23
29/03/2017
[personal] Home
Home
Recent
Home
Documents
Downloads
Desktop
Documents
Music
Pictures
Videos
[Dom0] Terminal - Spogjmey@dom0:~
File Edit View Terminal Tabs Help
--> Loading the VM (type = HVM)...
--> Starting Qubes DB...
--> Setting Qubes DB info for the VM...
--> Updating firewall rules...
--> Starting the VM...
--> Starting Qubes GUId (full screen)...
Connecting to VM's GUI agent: .connected
--> Starting Qubes GUId...
Connecting to VM's GUI agent: .in the background
--> Starting the qrexec daemon...
[Spogjmey@dom0 ~]$
[anon-whonix] Whonix Welcome Page - Tor Browser
Whonix Welcome Page
file:///usr/share/homepage/whonix-welcome-page/whonix.html
Search
whonix
PRIVACY & ANONYMITY OS
IP CHECK DOCS SUPPORT FORUM BLOG CONTRIBUTE DONATE DISCLAIMER

- Isolation of each qube from other qubes and hardware.
- Templets are used as source for appVM’s.
- Qubes base templets, Fedora 29, Debian 9, Whonix 14.
- Versions 3.2.1 (EOL) and 4.0 (4.0.1 in final testing, (Fedora 30)).

- Integration of Whonix with Qubes, which makes it easy to use Tor securely.
- Qubes can set so every E-mail attachment gets opened in its own single-use disposable qube.
- Able to install stand-alone VM style OS's, OSX, Windows, BDS, Dos, etc.

- Each AppVM has its own private directory structure even if using shared template image.
- Able to create Disposable VM that will be destroyed after use.
- Most controls are command line base.
- ctrl-shift-c/v top copy between appVM clipboard.

- Plugin support for other Hypervisors in future, (V4.0 and onward)

- Hardware and resource heavy (check site).

Memory:

- 4Gig can install,
- 8Gig will run,
- 16Gig will run nicely (my current laptop setup),
- 20+Gig runs $#& sweet.
- CPU needs VT-x and VT-d virtual extents in the CPU.

- Should install on a SSD, but HDD will work as well.

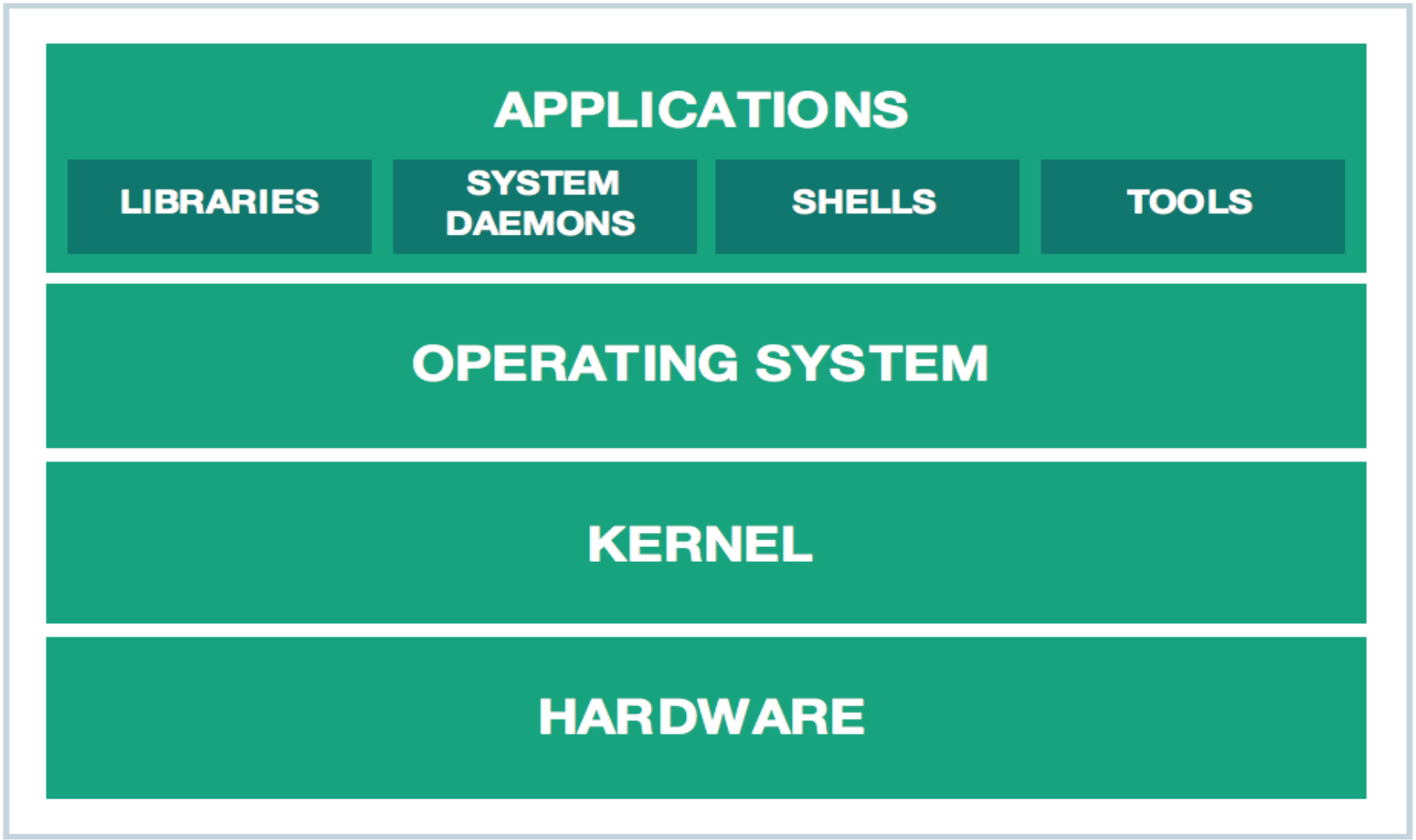
- Fedora uses yum/dnf package management.
- Debian uses apt-get /apt package management.
- Whonix uses whonix apt-get via tor network for package management.
- Web Site : www.qubes-os.org

Who uses Qubes?

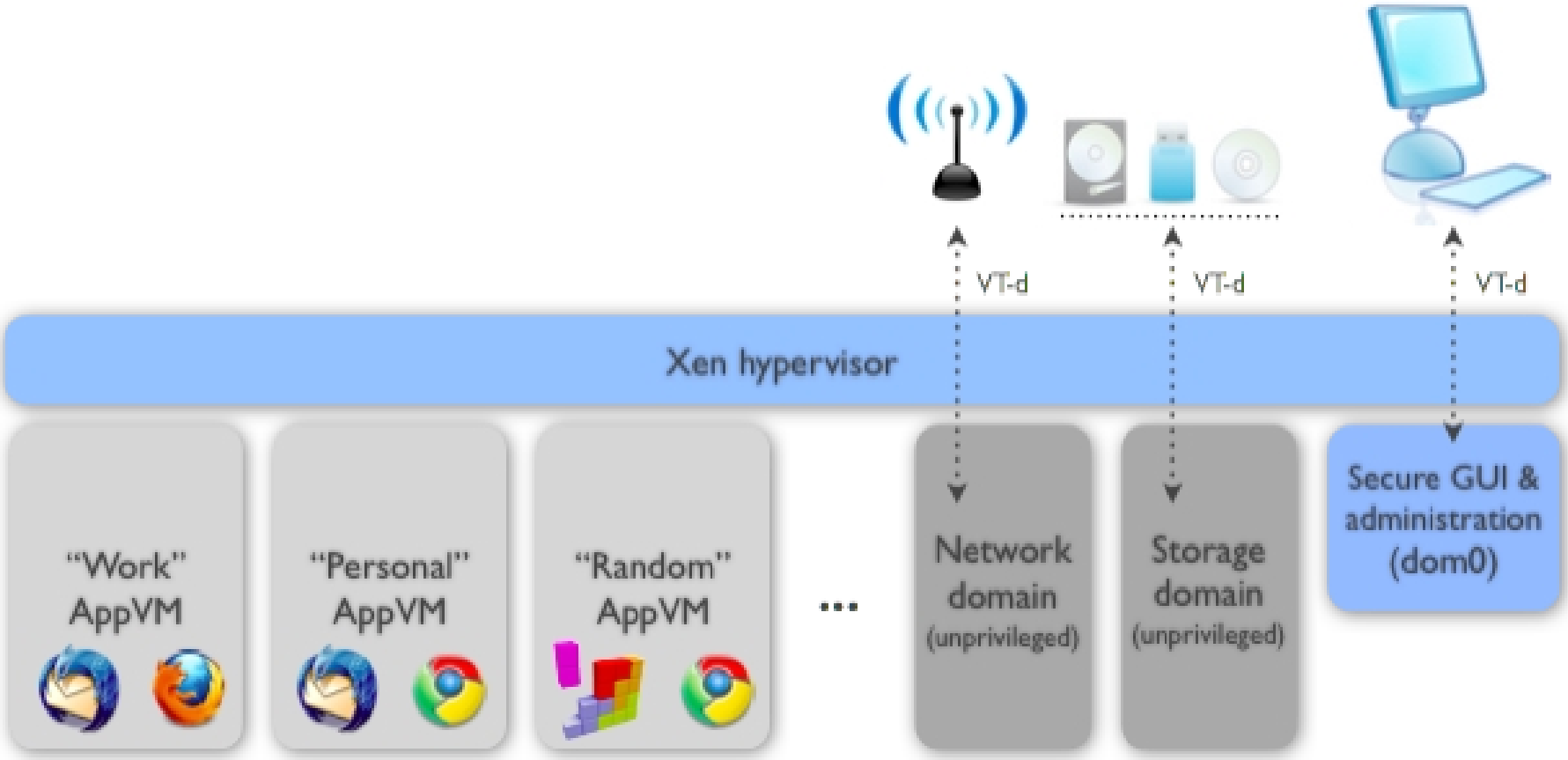
- Some people and groups that use it..
  - Edward Snowden
  - NLnet Foundation
  - Accessnow
  - Micah Lee – ‘Freedom of the Press Foundation’
  - Bill Budington - ‘Electronic Frontier Foundation’
  - Kenn White - ‘Open Crypto Audit Project’
  - Yep (Me) as well.

Qubes Design

General OS Design



Qubes OS Design (Type 1)



Qubes Glossary

- VM/Xen – Virtual Machine / Xen based, what you run in.
- Qube – the main running AppVM virtual machine that you run in.
- Dom0 – started by the Xen Hypervisor, runs management tools, only systems that has direct hardware access, handles GUI functions of windows.

Qubes Glossary

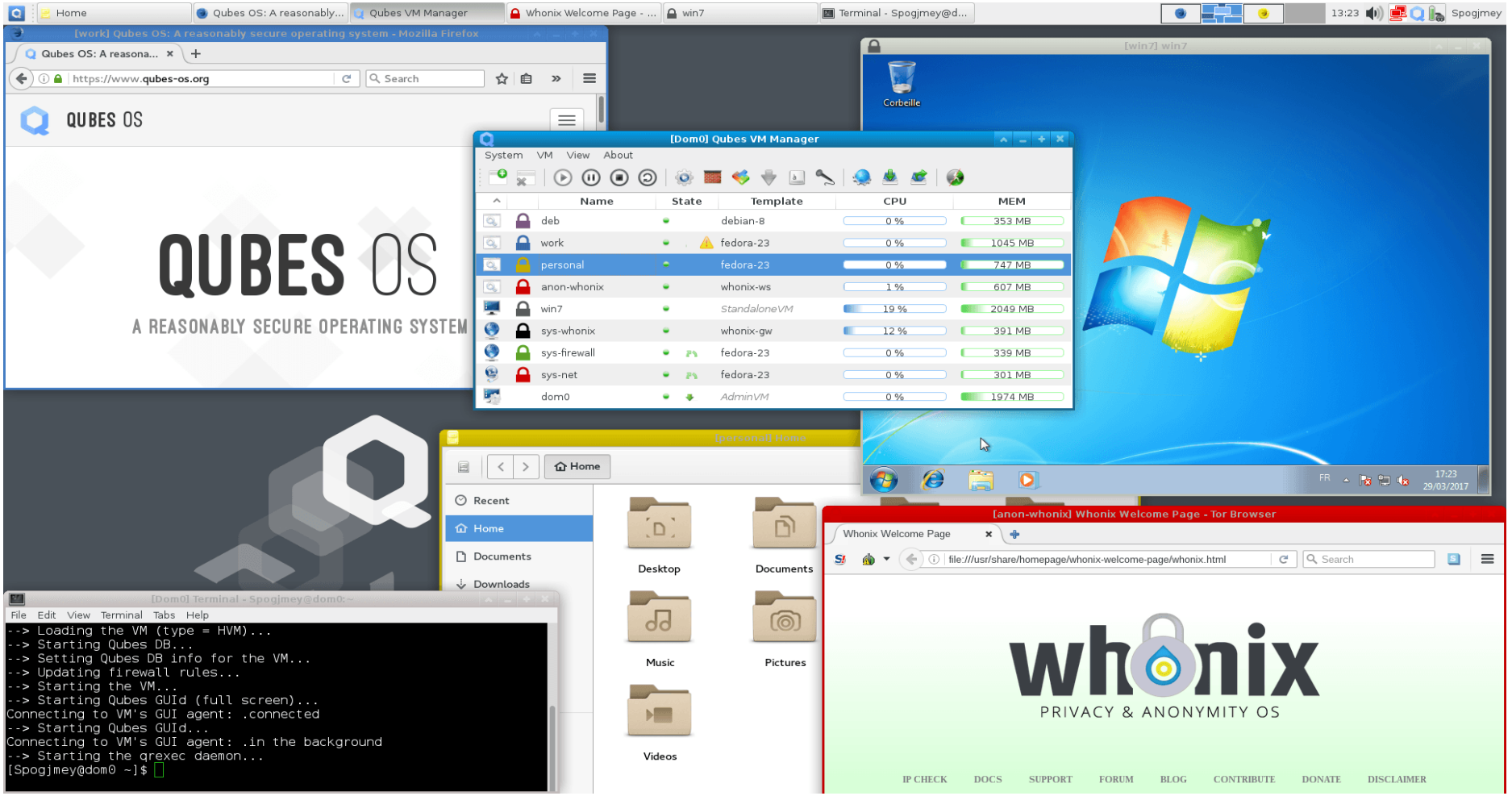
- NetVM – Network Virtual Machine, runs the networking functions, uses FirewallVM as well to route packets to I/F card. Only these VM's handle networking.
- FirewallVM – Firewall Virtual Machine, enforces network level polices, firewall rules, for any qube accessing this VM.

Qubes Glossary

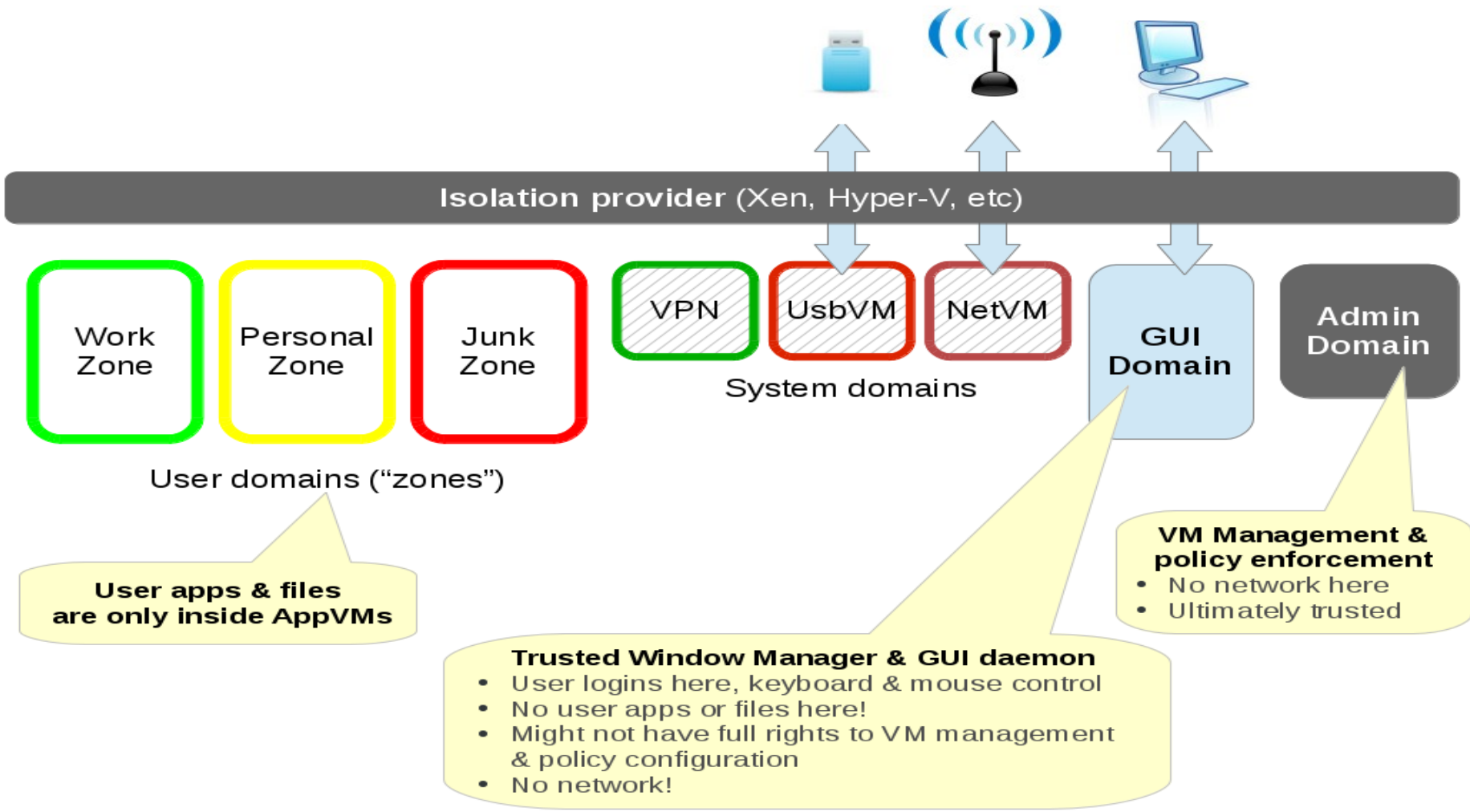
- Templet VM – Read only image that is used to create the Qubes AppVM for use.
- AppVM's include - Personal, Work, Untrusted, Vault. All color coded for visualization.
- You can also create your own Stand Alone VM to run Windows, BSD, Apple OSX..

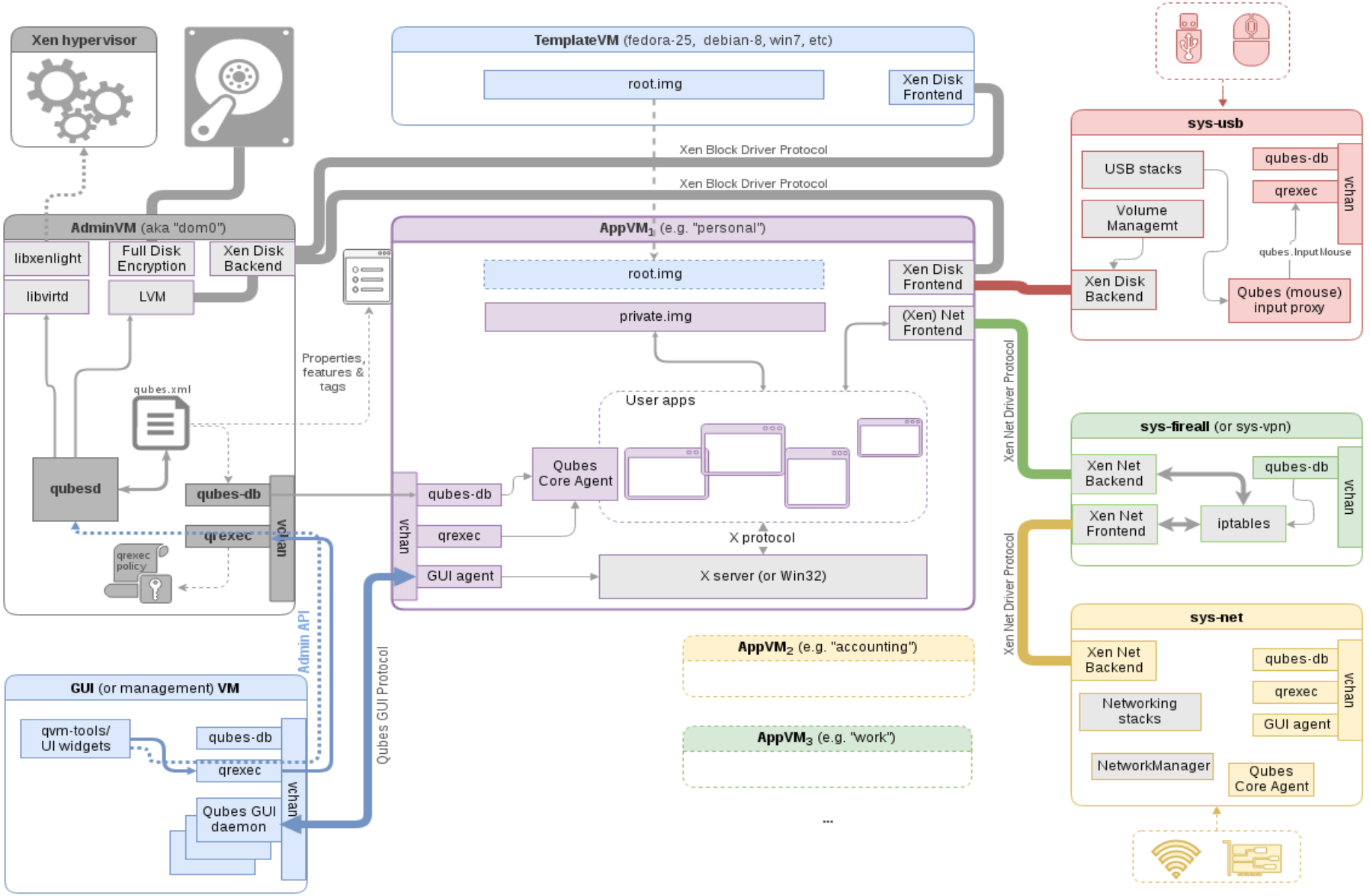
Qubes Glossary

- Whonix – a seamless combination based on Debian and Tor to utilize Tor isolation functionality. Use of Work Station and Gateway for Tor routing traffic of browsers and other qube installed applications.
- Disposable VM's – only created during the time used, then all data and stored files are erased from the system.

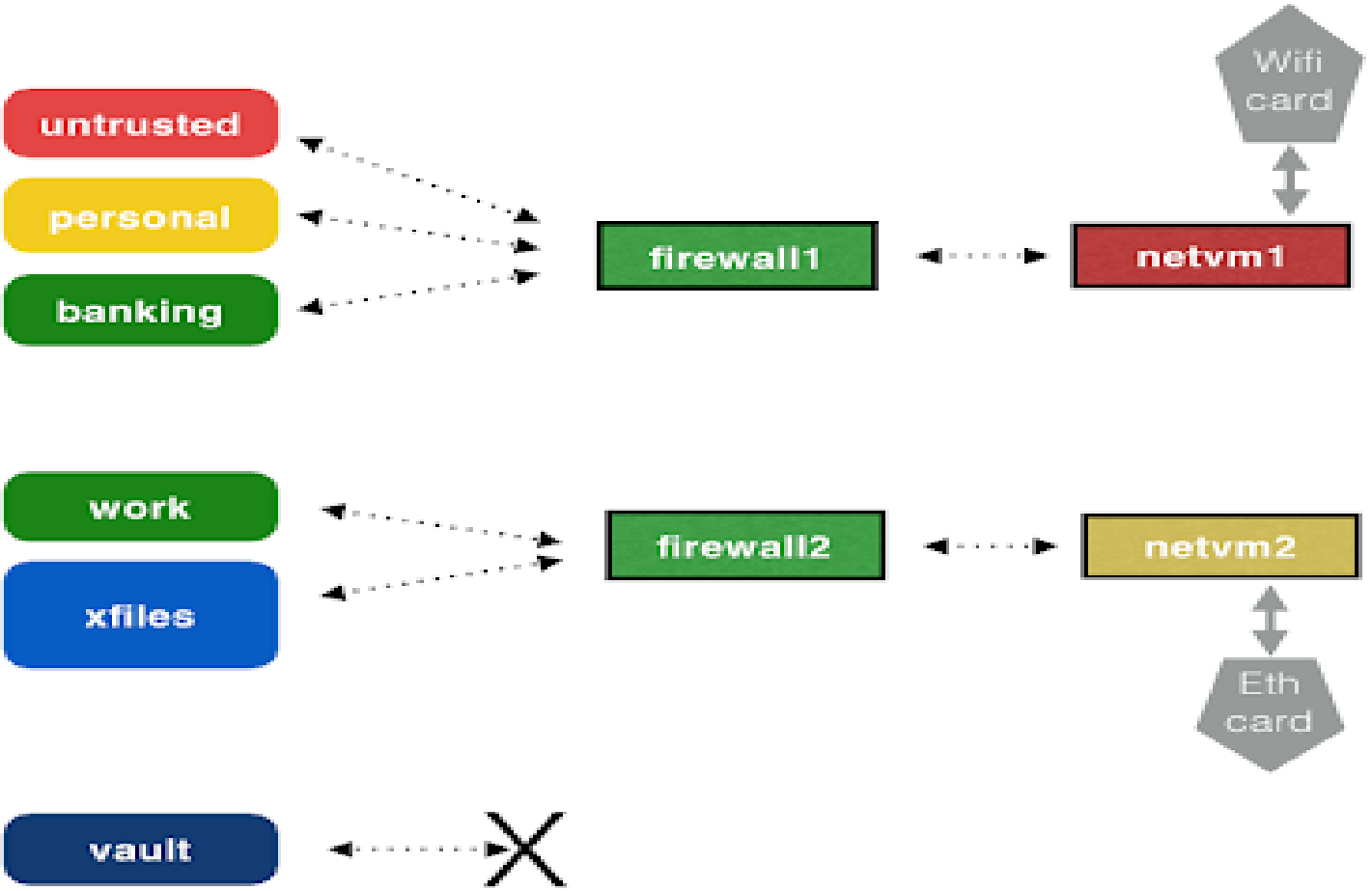

Home
Qubes OS: A reasonably...
Qubes VM Manager
Whonix Welcome Page - ...
win7
Terminal - Spogjmey@d...
13:23
Spogjmey
[work] Qubes OS: A reasonably secure operating system - Mozilla Firefox
Qubes OS: A reasona...
https://www.qubes-os.org
Search
QUBES OS
QUBES OS
A REASONABLY SECURE OPERATING SYSTEM
[Dom0] Qubes VM Manager
System VM View About
Name State Template CPU MEM
deb debian-8 0 % 353 MB
work fedora-23 0 % 1045 MB
personal fedora-23 0 % 747 MB
anon-whonix whonix-ws 1 % 607 MB
win7 StandaloneVM 19 % 2049 MB
sys-whonix whonix-gw 12 % 391 MB
sys-firewall fedora-23 0 % 339 MB
sys-net fedora-23 0 % 301 MB
dom0 AdminVM 0 % 1974 MB
[win7] win7
Corbeille
FR
17:23
29/03/2017
[personal] Home
Home
Recent
Home
Documents
Downloads
Desktop
Documents
Music
Pictures
Videos
[Dom0] Terminal - Spogjmey@dom0:~
File Edit View Terminal Tabs Help
--> Loading the VM (type = HVM)...
--> Starting Qubes DB...
--> Setting Qubes DB info for the VM...
--> Updating firewall rules...
--> Starting the VM...
--> Starting Qubes GUId (full screen)...
Connecting to VM's GUI agent: .connected
--> Starting Qubes GUId...
Connecting to VM's GUI agent: .in the background
--> Starting the qrexec daemon...
[Spogjmey@dom0 ~]$
[anon-whonix] Whonix Welcome Page - Tor Browser
Whonix Welcome Page
file:///usr/share/homepage/whonix-welcome-page/whonix.html
Search
whonix
PRIVACY & ANONYMITY OS
IP CHECK DOCS SUPPORT FORUM BLOG CONTRIBUTE DONATE DISCLAIMER


work: Untitled 1 - Open...
work: - Mozilla Thunderbird
random: Mozilla Firefox
facebook
personal: Mozilla Firefox
bank: Mozilla Firefox
shopping: Mozilla Firefox
work: Untitled 1 - OpenOffice.org Cal
Enter Master Key
vault: /rw/home/user/jo...

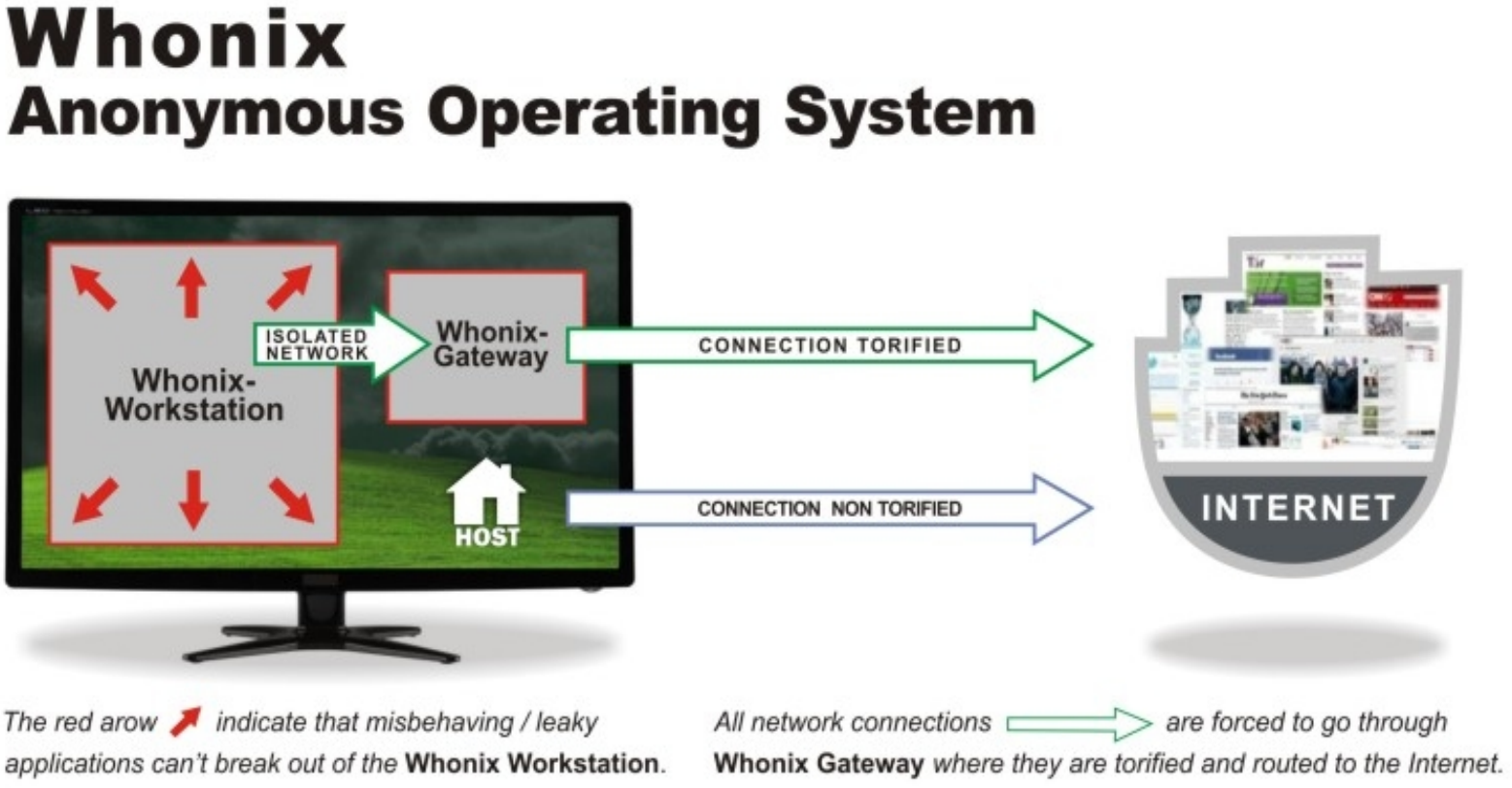

Isolation provider (Xen, Hyper-V, etc)
Work Zone
Personal Zone
Junk Zone
VPN
UsbVM
NetVM
GUI Domain
Admin Domain
System domains
User domains (“zones”)
User apps & files are only inside AppVMs
Trusted Window Manager & GUI daemon
• User logins here, keyboard & mouse control
• No user apps or files here!
• Might not have full rights to VM management & policy configuration
• No network!
VM Management & policy enforcement
• No network here
• Ultimately trusted


Xen hypervisor
TemplateVM (fedora-25, debian-8, win7, etc)
root.img
Xen Disk Frontend
Xen Block Driver Protocol
Xen Block Driver Protocol
AdminVM (aka "dom0")
libxenlight
Full Disk Encryption
Xen Disk Backend
libvirtd
LVM
qubes.xml
Properties, features & tags
qubesd
qubes-db
qrexec
qrexec policy
vchan
Admin API
AppVM1 (e.g. "personal")
root.img
private.img
Xen Disk Frontend
(Xen) Net Frontend
User apps
qubes-db
qrexec
GUI agent
vchan
Qubes Core Agent
X protocol
X server (or Win32)
Qubes GUI Protocol
AppVM2 (e.g. "accounting")
AppVM3 (e.g. "work")
...
GUI (or management) VM
qvm-tools/ UI widgets
qubes-db
qrexec
Qubes GUI daemon
vchan
sys-usb
USB stacks
Volume Managemt
Xen Disk Backend
qubes-db
qrexec
vchan
qubes.InputMouse
Qubes (mouse) input proxy
Xen Net Driver Protocol
sys-firewall (or sys-vpn)
Xen Net Backend
Xen Net Frontend
qubes-db
iptables
vchan
Xen Net Driver Protocol
sys-net
Xen Net Backend
Networking stacks
NetworkManager
qubes-db
qrexec
GUI agent
vchan
Qubes Core Agent

Some Qube designs



Whonix in Qubes



Whonix in Qubes

- Its based on Tor with Debian as its template base.
- Its split into two systems one a gateway (provides networking) and one a workstation.
- Current version of 14 for both gateway and workstation.

Special note

- Can run VM that when shut-down its information and logs are destroyed.
- Designed for Sand-boxing from start.
- Will run standalone OS systems.
- Yes can run Windows, well kinda…
- Bugs
- Not good for games … needs supported hardware and good amount of memory.

Things not so good

- Games – forget it.
- Burning CD/DVD – depends on your hardware.
- Windows – v7 works best, v10 so so, older versions (xp,2000,95 work), no sound and USB not working.
- Some GUI commands, most are command line based.
- Hardware dependent, check web site for compatibility issues and some fixes.

Things not so good

- 3D graphics.
- BlueTooth devices complicated, and not always work, do to Xen subsystem. (I have never got any bluetooth devices to work)
- No bridging of network, NAT only support.
- Launch lag, first time run.
- Stand alone VM's do not always support external hardware. (DVD, I/F cards, Scanners, USB drives)

How I use Qubes

- My current setup for my system.
  - Demo and Description.

- What I use each Qube for.
  - Demo and Description.

Questions

Will answer what I can…..

Me

Philosophy, Psychology, Information Assurance CyberSecurity, Intelligence Analyst

OtakuSystems LLC

otakusystems.com

twitter: @otakusystems

Technologist, Futurist, Philosopher, Geek

- Seeker of wisdom and knowledge