A LIVE DEMONSTRATION OF "WANNACRY" RANSOMWARE

by Francis Chao
fchao2@yahoo.com

TUCSON COMPUTER SOCIETY

WINNERS
WINdows usERS

apcug
An International
Association of Technology
& Computer User Groups

Web location for this presentation:

http://aztcs.org

Click on “Meeting Notes”

SUMMARY

To see a real copy of the "WannaCry" ransomware in action, you can safely run it in a virtual machine that has a Windows.. running as a "guest" operating system if the virtual machine is carefully isolated by means of a network configuration consisting of multiple routers.

TOPICS

- Using a virtual machine as a throwaway computer
- Isolating the virtual machine from it's host computer
- A two+ router configuration for isolation
- Downloading the "Wannacry" dropper

TOPICS (continued)

- WannaCry Infection Process

USING A VIRTUAL MACHINE AS A THROWAWAY COMPUTER

- A virtual machine inside it's host computer as a single window (that then contains lots of other windows)
- Unlike for real computers, you can make as many copies of a virtual machine or it's virtual hard drive as you like

USING A VIRTUAL MACHINE AS A THROWAWAY COMPUTER (continued)

- When you use "File Explorer" (= "Windows Explorer" prior to "Windows 8") to clone an entire virtual machine, the cloned virtual machine will retain the same "motherboard UUID" and "motherboard serial number" as the original virtual machine

USING A VIRTUAL MACHINE AS A THROWAWAY COMPUTER (continued)

- When you start up the cloned virtual machine for the first time, it will ask you if you moved or copied it:
  If you click on "moved", it will retain the same motherboard UUID as the original virtual machine.

USING A VIRTUAL MACHINE AS A THROWAWAY COMPUTER (continued)

- If you click on "copied", the virtual motherboard of the cloned virtual machine will get a fresh, new UUID that is not the same as the motherboard UUID of the original virtual machine.

USING A VIRTUAL MACHINE AS A THROWAWAY COMPUTER (continued)

- Changing the motherboard UUID is okay for any version of Windows.. prior to "Windows 10"
- Change the motherboard UUID inactivates Microsoft's activation for any copy of "Windows 10"

USING A VIRTUAL MACHINE AS A THROWAWAY COMPUTER (continued)

- You can use a text editor to edit the *.vmx of a virtual machine so that the virtual machine, even when it is cloned, never asks you if you "Moved" or "Copied" it:
  Just add in
  uuid.action = "KEEP"

ISOLATING A VIRTUAL MACHINE FROM IT'S HOST COMPUTER

- "WannaCry" has the capability for "worm-like behavior":
  If it does not see it's hard-coded "killswitch URL" as an active Web site, it uses SMB (file sharing" and RDP (remote desktop protocol) to replicate itself to other computers on your local network

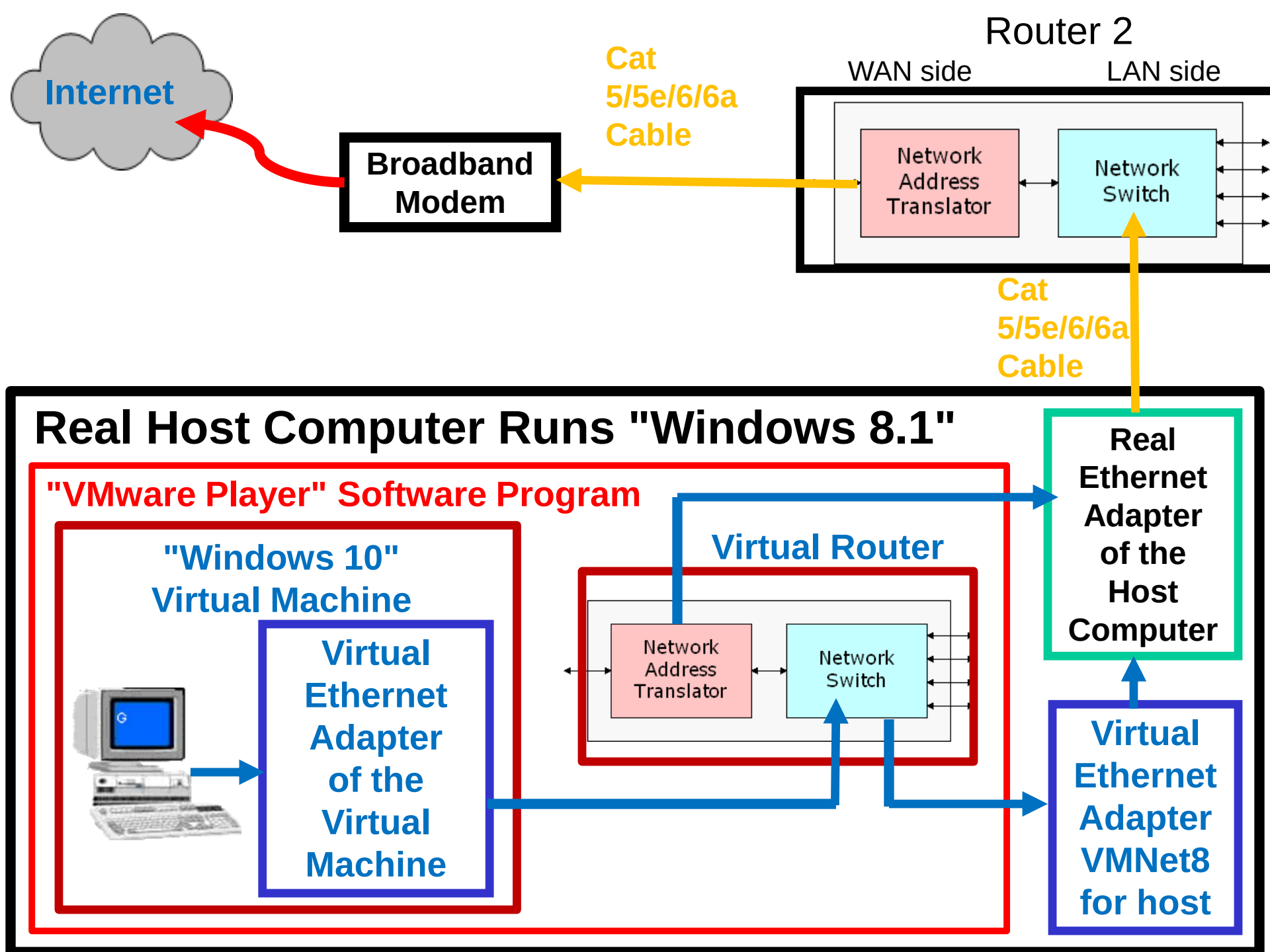
Two Problems With Accessing the Internet From a Typical "Windows.." Computer

- Problem 1: When you add a real or virtual "Windows.." computer to an existing local area network, "Windows.." automatically defaults to file sharing. File sharing provides an "attack vector" for any malware that finds its way into your computer when you are accessing the Internet.

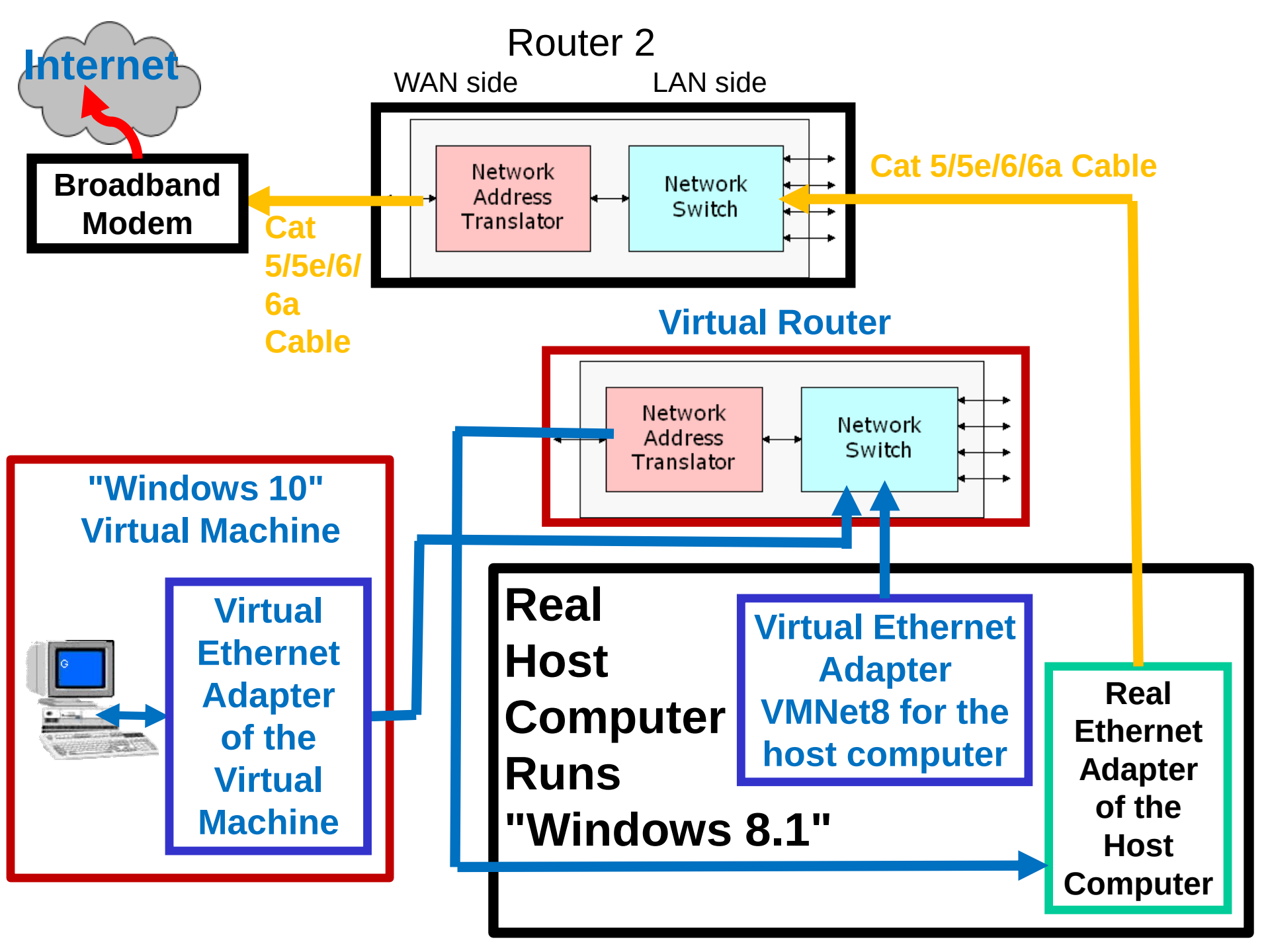
Two Problems With Accessing the Internet.. (continued)

- Problem 2: Even when you proactively turn off file sharing in various configuration screens in "Windows..", it is easy for the unsuspecting end-user or malware from the Internet to turn it back on.

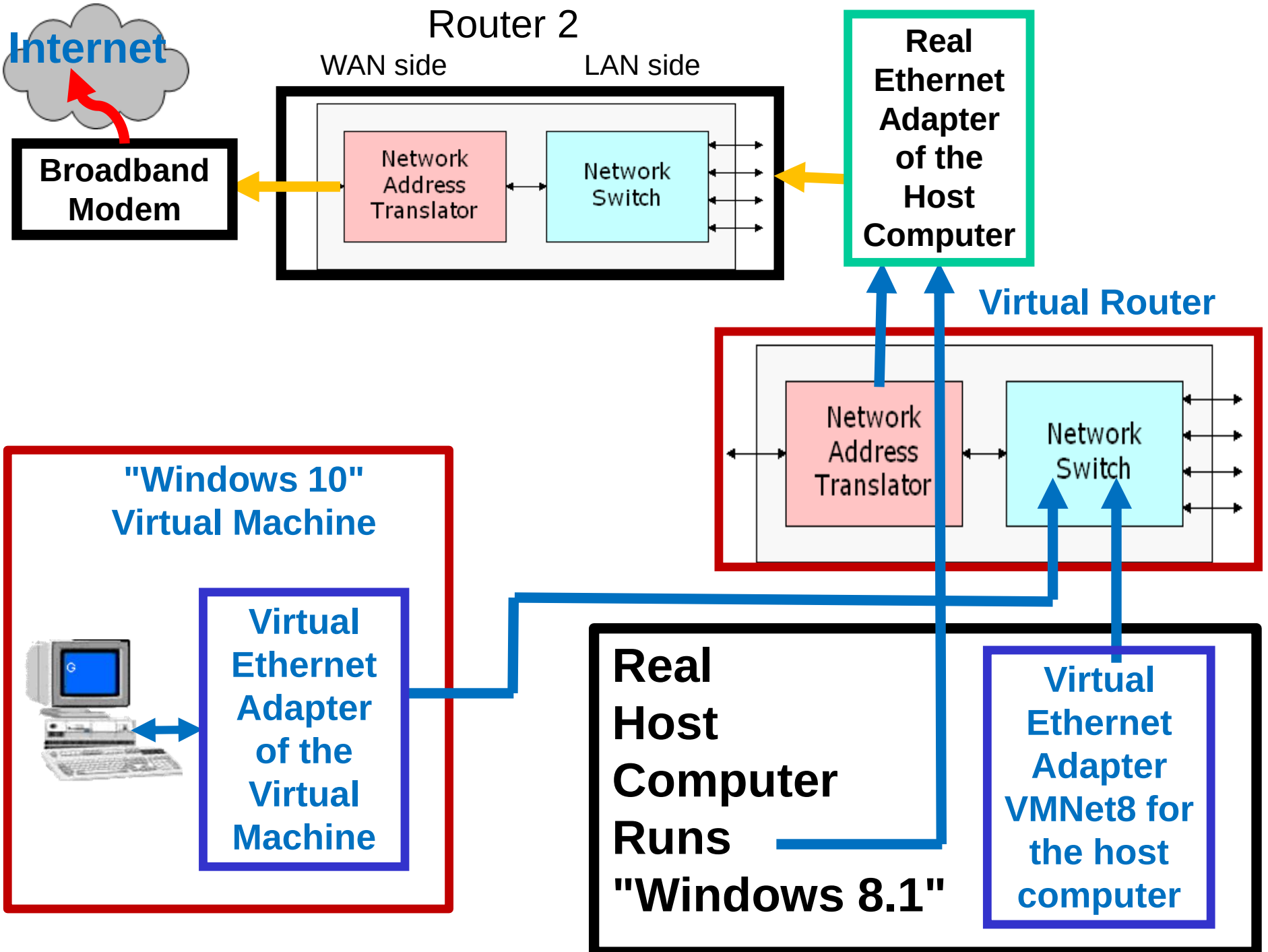
Physical configuration diagram for an unsecure, default virtual machine:


Internet
Broadband Modem
Cat 5/5e/6/6a Cable
Router 2
WAN side
LAN side
Network Address Translator
Network Switch
Cat 5/5e/6/6a Cable
Real Host Computer Runs "Windows 8.1"
"VMware Player" Software Program
"Windows 10" Virtual Machine
Virtual Ethernet Adapter of the Virtual Machine
Virtual Router
Network Address Translator
Network Switch
Real Ethernet Adapter of the Host Computer
Virtual Ethernet Adapter VMNet8 for host

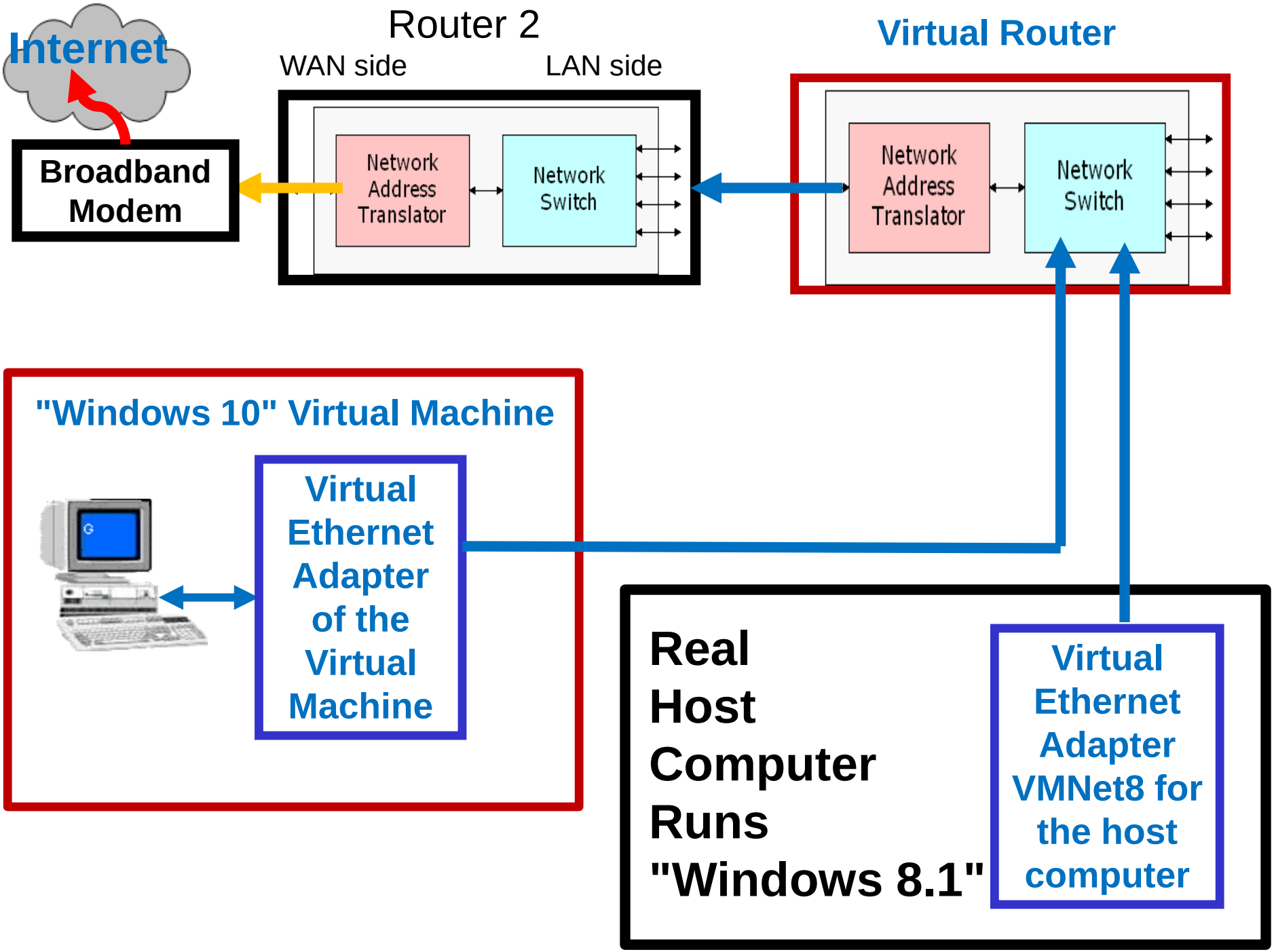
Logical configuration diagram for an insecure, default virtual machine:


Internet
Router 2
WAN side
LAN side
Broadband Modem
Network Address Translator
Network Switch
Cat 5/5e/6/6a Cable
Cat 5/5e/6/6a Cable
Virtual Router
Network Address Translator
Network Switch
"Windows 10" Virtual Machine
Virtual Ethernet Adapter of the Virtual Machine
Real Host Computer Runs "Windows 8.1"
Virtual Ethernet Adapter VMNet8 for the host computer
Real Ethernet Adapter of the Host Computer

Simplified, logical configuration diagram for an unsecure, default virtual machine:


Internet
Router 2
WAN side
LAN side
Broadband Modem
Network Address Translator
Network Switch
Real Ethernet Adapter of the Host Computer
Virtual Router
Network Address Translator
Network Switch
"Windows 10" Virtual Machine
Virtual Ethernet Adapter of the Virtual Machine
Real Host Computer Runs "Windows 8.1"
Virtual Ethernet Adapter VMNet8 for the host computer

Further, simplified, logical configuration diagram for an unsecure, default virtual machine:


Internet
Router 2
WAN side
LAN side
Virtual Router
Broadband Modem
Network Address Translator
Network Switch
Network Address Translator
Network Switch
"Windows 10" Virtual Machine
Virtual Ethernet Adapter of the Virtual Machine
Real Host Computer Runs "Windows 8.1"
Virtual Ethernet Adapter VMNet8 for the host computer

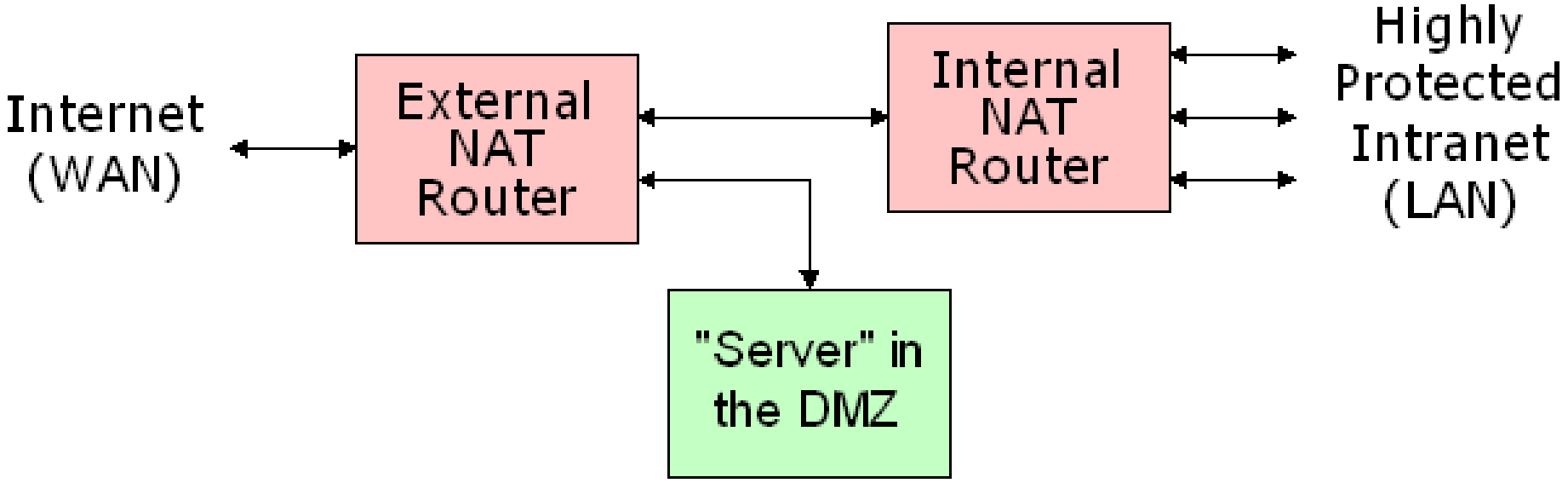
A TWO+ ROUTER CONFIGURATION FOR ISOLATION

- When dealing with malware with "worm-like behavior", you also need to isolate the virtual machine from other computers on your local network
- The standard configuration is a two+ router configuration in a "De-militarized Zone" setup:

"De-Militarized Zone" (= "DMZ") Using A Second Router Interjected Into An Existing Local Network":

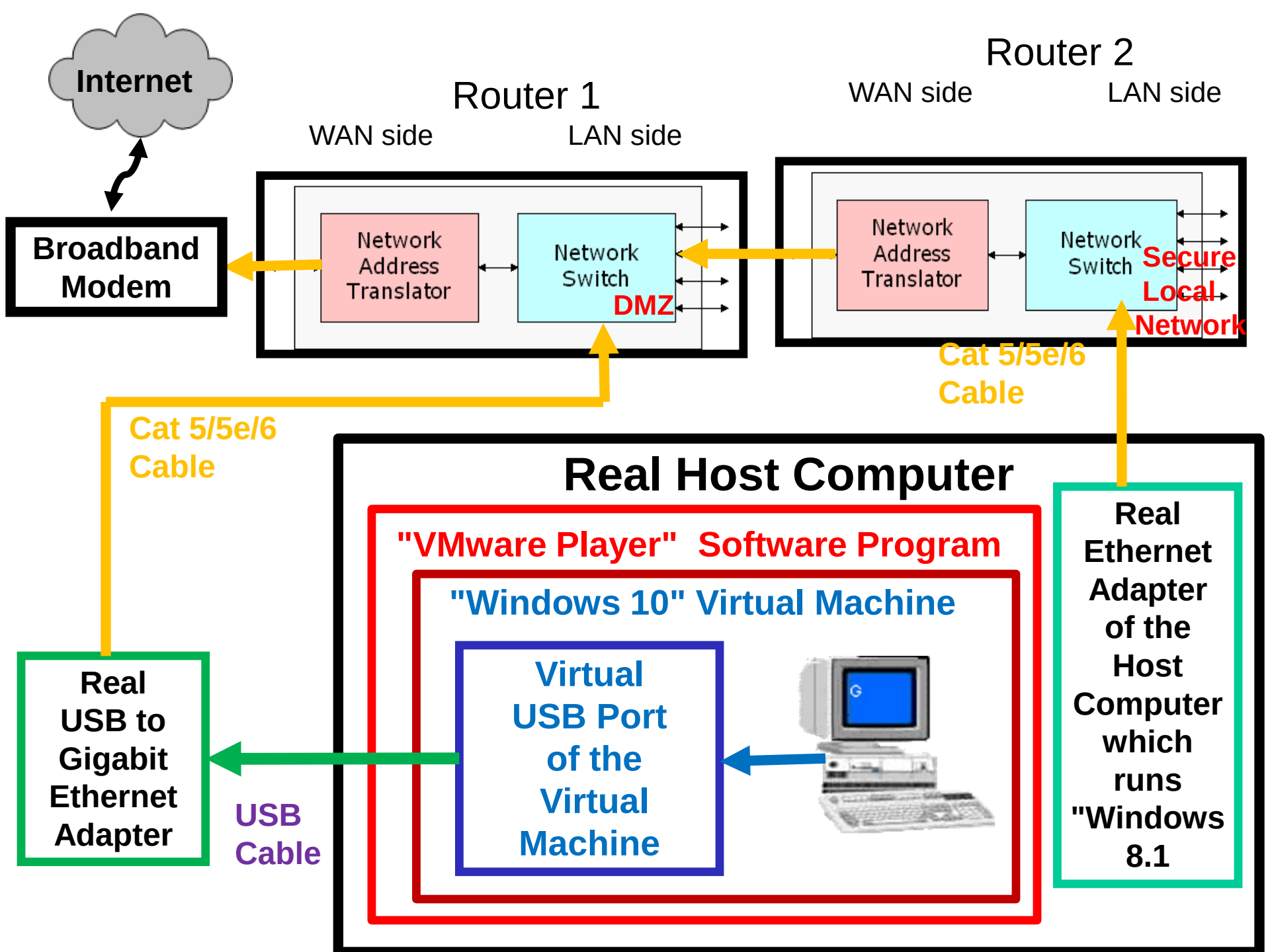
To make the network more secure:
Insert a second "Secure" router between the current router and the host computer.

Insert a "USB to .." network adapter between the virtual machine and the original router.
Disconnect the virtual Ethernet adapter of the virtual machine:

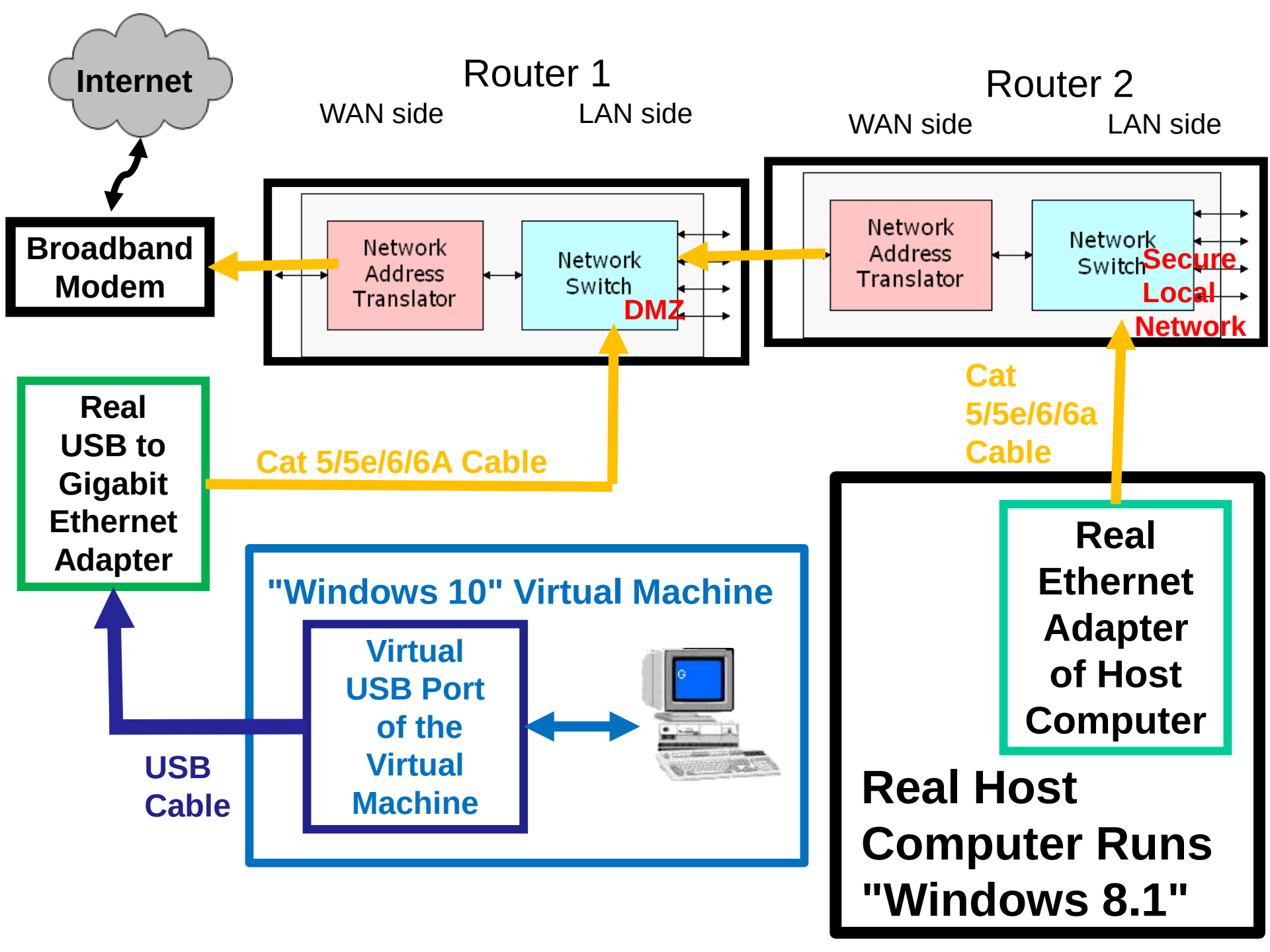

Internet
(WAN)
External
NAT
Router
Internal
NAT
Router
Highly
Protected
Intranet
(LAN)
"Server" in
the DMZ

Reference:
https://www.grc.com/nat/nat.htm

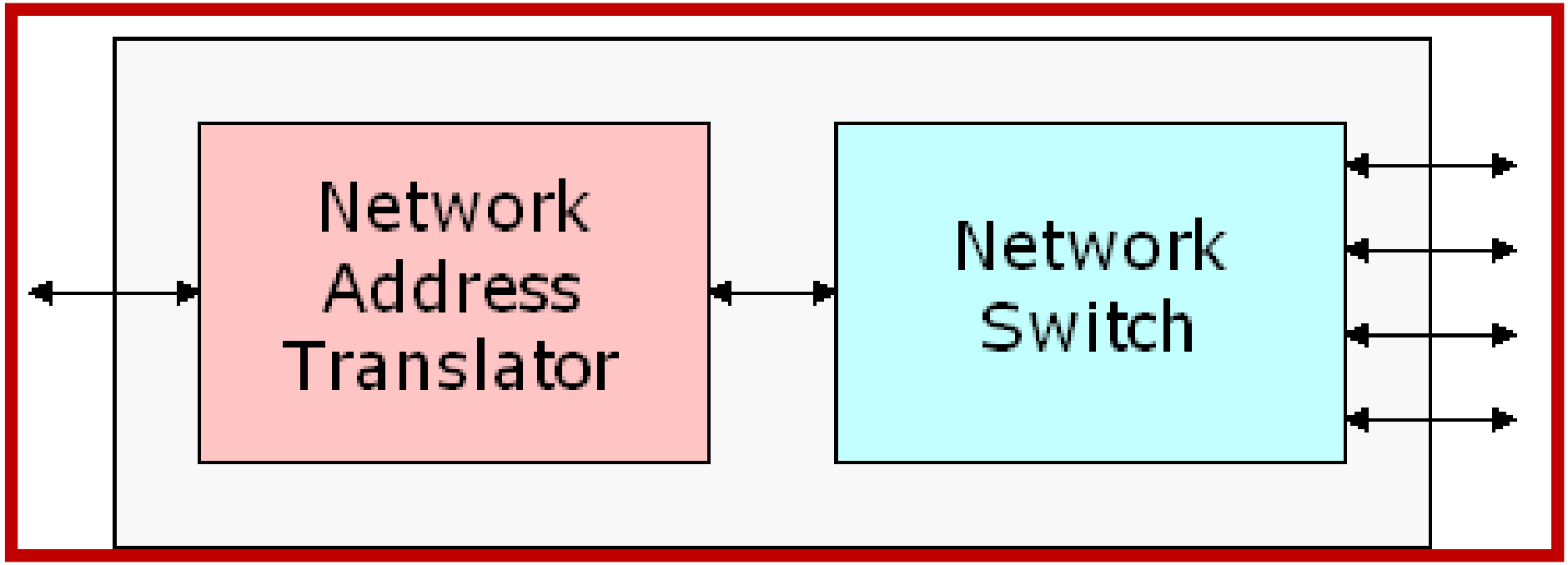
Physical configuration diagram for the "Secure Web" virtual machine:


Internet
Router 1
WAN side
LAN side
Router 2
WAN side
LAN side
Broadband Modem
Network Address Translator
Network Switch
DMZ
Network Address Translator
Network Switch
Secure Local Network
Cat 5/5e/6 Cable
Cat 5/5e/6 Cable
Real Host Computer
"VMware Player" Software Program
"Windows 10" Virtual Machine
Virtual USB Port of the Virtual Machine
Real USB to Gigabit Ethernet Adapter
USB Cable
Real Ethernet Adapter of the Host Computer which runs "Windows 8.1

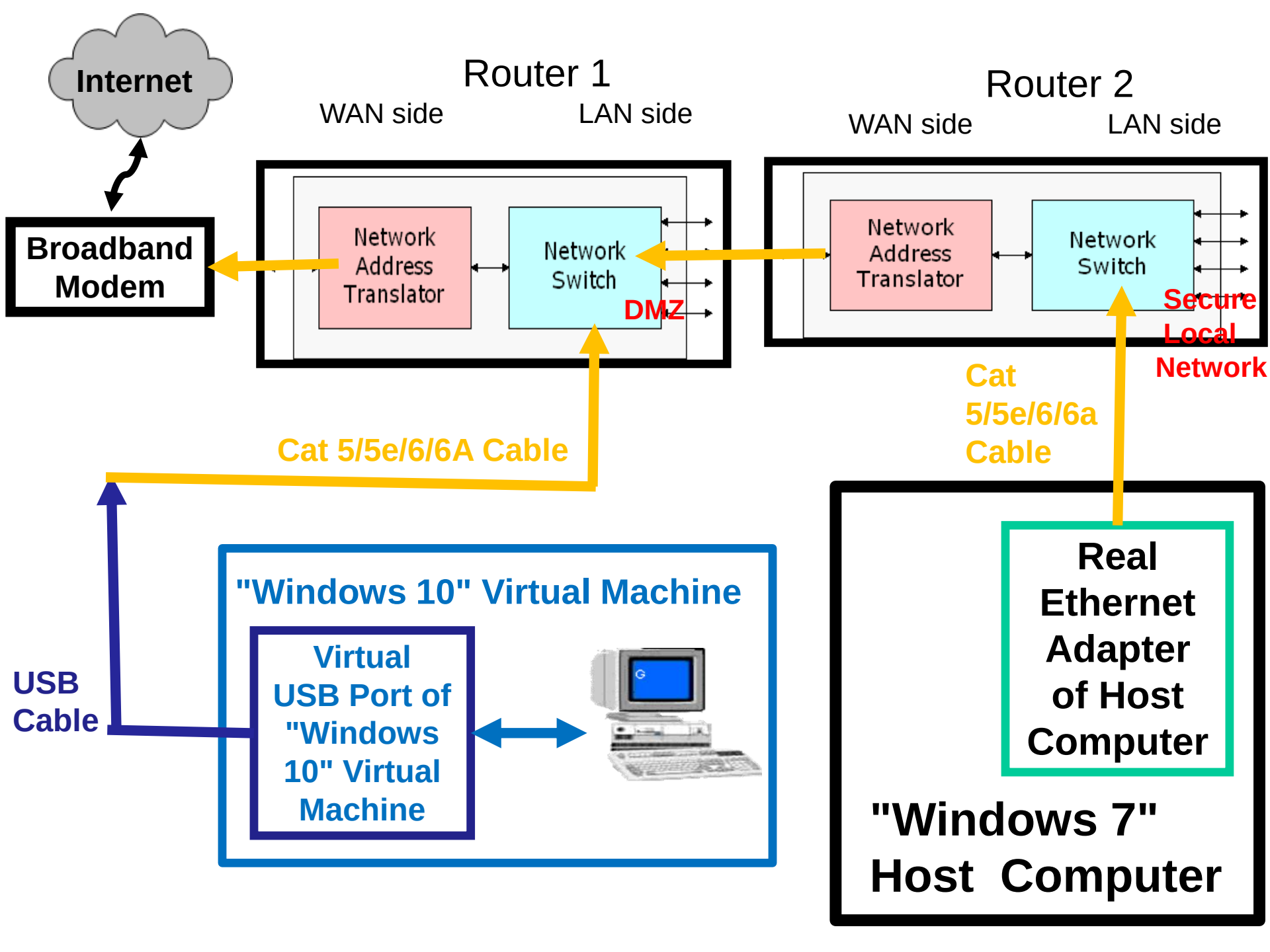
Logical configuration diagram for the "Secure Web" virtual machine:


Internet
Router 1
WAN side
LAN side
Router 2
WAN side
LAN side
Broadband Modem
Network Address Translator
Network Switch
DMZ
Network Address Translator
Network Switch
Secure Local Network
Real USB to Gigabit Ethernet Adapter
Cat 5/5e/6/6A Cable
Cat 5/5e/6/6a Cable
"Windows 10" Virtual Machine
Virtual USB Port of the Virtual Machine
USB Cable
Real Ethernet Adapter of Host Computer
Real Host Computer Runs "Windows 8.1"

The virtual "NAT Router that is provided by "VMware Player" is not in use:



Simplified, logical configuration diagram for the "Secure Web" virtual machine:


Internet
Router 1
WAN side
LAN side
Router 2
WAN side
LAN side
Broadband Modem
Network Address Translator
Network Switch
DMZ
Network Address Translator
Network Switch
Secure Local Network
Cat 5/5e/6/6A Cable
Cat 5/5e/6/6a Cable
"Windows 10" Virtual Machine
USB Cable
Virtual USB Port of "Windows 10" Virtual Machine
Real Ethernet Adapter of Host Computer
"Windows 7" Host Computer

A Four-Part Solution for Secure Web Access

- Solution Part 1: Disconnect the default virtual Ethernet network adapter of the virtual machine.
- Solution Part 2: Provide the virtual machine with a USB-to-Gigabyte Ethernet adapter.

A Four-Part Solution for Secure Web Access (continued)

- Solution Part 3: Add an extra router to your local network in order to create a two-router "De-Militarized Zone" (DMZ).

A Four-Part Solution for Secure Web Access (continued)

- Solution Part 4: Connect the virtual machine to the two-router De-Militarized Zone (DMZ), using the USB-to-Gigabit Ethernet adapter that you installed in "Solution Part 2".

DOWNLOADING THE "WANNACRY" DROPPER

- Go to https://www.youtube.com/watch?v=0RuIMdQWyVQ
- Click on "SHOW MORE"
- Click on the download link
- Click on "Download through your browser

DOWNLOADING THE "WANNACRY" DROPPER (continued)

- Click on the Save button at the top or bottom of your Web browser
- Use 7Zip or WinZip to extract the WannaCry.exe from the WannaCry.rar file
- Do not double-click on the WannaCry.exe file unless you need the excitement

INSTALLING WannaCry.exe INTO "WINDOWS 10"

- In "Windows 10", "Windows Defender" is always running in the background:
  To get the WannaCry.exe ransomware dropper to install and do it's havoc, you have to edit the registry and then reboot the computer:

INSTALLING WannaCry.exe INTO "WINDOWS 10" (continued)

- See https://www.tenforums.com/tutorials/5918-turn-off-windows-defender-windows-10-a.html
- (In versions of Windows.. prior to Windows 10, it is much easier to initiate a WannaCry.exe infection.)

WANNACRY INFECTION PROCESS

- Step 1:
  End user clicks on the dropper (file)
- Step 2:
  WannaCry attempts to contact it's hard-coded kill-switch URL
- Step 3:
  If the hard-coded kill-switch is alive out on the Web, go to Step 6

WANNACRY INFECTION PROCESS (continued)

- Step 4:
  If the kill-switch URL is not successfully found as a live Web site, WannaCry searches for Remote Desktop Protocol (RDP) and files shared by means of Server Message Blocks (SMB) on other computers on the local network

WANNACRY INFECTION PROCESS (continued)

- Step 5:
  If WannaCry locates any RDP or SMB-connected computers, it does it's worm-like activity of executing an infection on those other computers

WANNACRY INFECTION PROCESS (continued)

- Step 6:
  WannaCry starts searching through the original computer for specific types of data files:
  When it finds a target file, it encryst and renames it

WANNACRY INFECTION PROCESS (continued)

- Step 7:
  WannaCry displays text instructions on the desktop of the originally-infected computer
- Step 8:
  WannaCry displays the "Ooops, your files have been encrypted!" window

WANNACRY INFECTION PROCESS (continued)

- Step 9:
  WannaCry's "Load PerfMon Counters" keeps popping up the window in Step 8, even if you close this window.