Virtualbox Networks: In Pictures

Locked | Search this topic... | 9 posts • Page 1 of 1

Virtualbox Networks: In Pictures

by scottgus1 » 26. Jan 2020, 04:01

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

The Virtualbox manual, section 6, has lots of good information on the types of Virtualbox networks that are provided with the pre-built Virtualbox installers. There is also a concise table in the manual, section 6.2, that shows the kinds of connections that can be set up and what communications can be had. This thread shows pictures of the more common Virtualbox networks. Hopefully a picture might be worth a thousand words. Or at least a couple hundred.

Virtualbox provides these forms of networking in the "Attached to:" dropdown:
NAT
NAT network (called "Network Address Translation Service" in the manual)
Bridged Adapter
Internal Network
Host-Only Adapter
Generic Driver

"Sandbox" This is not an official Virtualbox network type and is not in the "Attached to:" dropdown. Rather, "Sandbox" is a network setup using some of the above networking types and a router/firewall guest to isolate a guest or set of guests in a private "lab" that cannot see or access the host LAN, but can use the host's internet connection.

Last edited by scottgus1 on 30. Jan 2020, 20:23, edited 2 times in total.

NAT

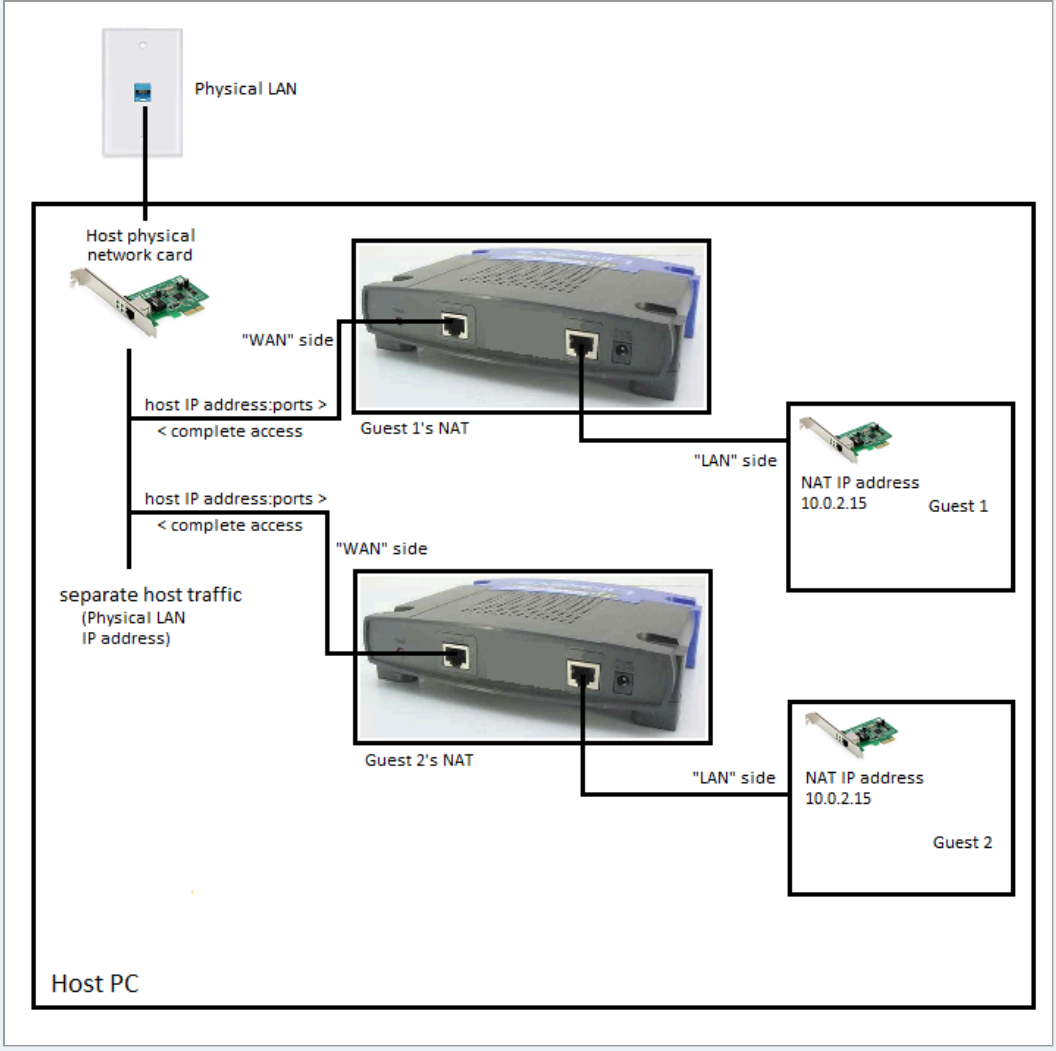
by scottgus1 » 26. Jan 2020, 04:03

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

NAT

Virtualbox manual, section 6.3



NAT.png (100.63 KiB) Viewed 135292 times

NAT behaves like a house router with only one LAN port. Each NAT "router" only connects to one network card in one guest. NAT allows the guest's network card to talk to the host, the host's LAN, and the internet. The host, LAN, and internet can only talk to that guest's network card through forwarded ports. Other NAT-connected guest network cards can also talk to this particular network card only though forwarded ports.

The host can connect to the NAT-connected card via: **localhost:portnumber**

Other guests, internet and the LAN can connect to the NAT-connected card via: **host.ip.add.ress:portnumber**

The default IP address given to the first NAT-connected network card in a guest is 10.0.2.15. If you add another network card to the guest and set its network to NAT too, that card will get 10.0.3.15, and so on. If you start another guest set to NAT, that guest will also get 10.0.2.15 for its first NAT-connected card, 10.0.3.15 for the second, etc. These defaults can be changed, see the Virtualbox Manual. (Please note that references to "NAT network" in this section of the manual are not referring to "NAT Network" type network connections discussed in the next post. They refer to only "NAT" as discussed in this post. The terminology is confusing and effort has to be expended to not confuse them.)

You must choose different ports in each NAT's Port Forwarding to ensure each guest gets the correct traffic originating from outside the NAT. When opening a port, you only need to set the **protocol, host port and guest port** numbers. The traffic only goes through that one card, so the port forwarding rule does not need to know the IP address of the card. Each guest network card set to NAT has

its own Port Forwarding settings under the "Advanced" dropdown.

The "WAN" side of NAT is always connected to the host; it cannot be connected elsewhere. For a NAT-like arrangement where the WAN connection can be positioned differently, use a separate VM with a router OS installed, like in "Sandbox" below.

The "WAN" side of NAT is connected into the host's network stream. So the host's firewall, antivirus, and VPN filter control network traffic to NAT.

NAT Network

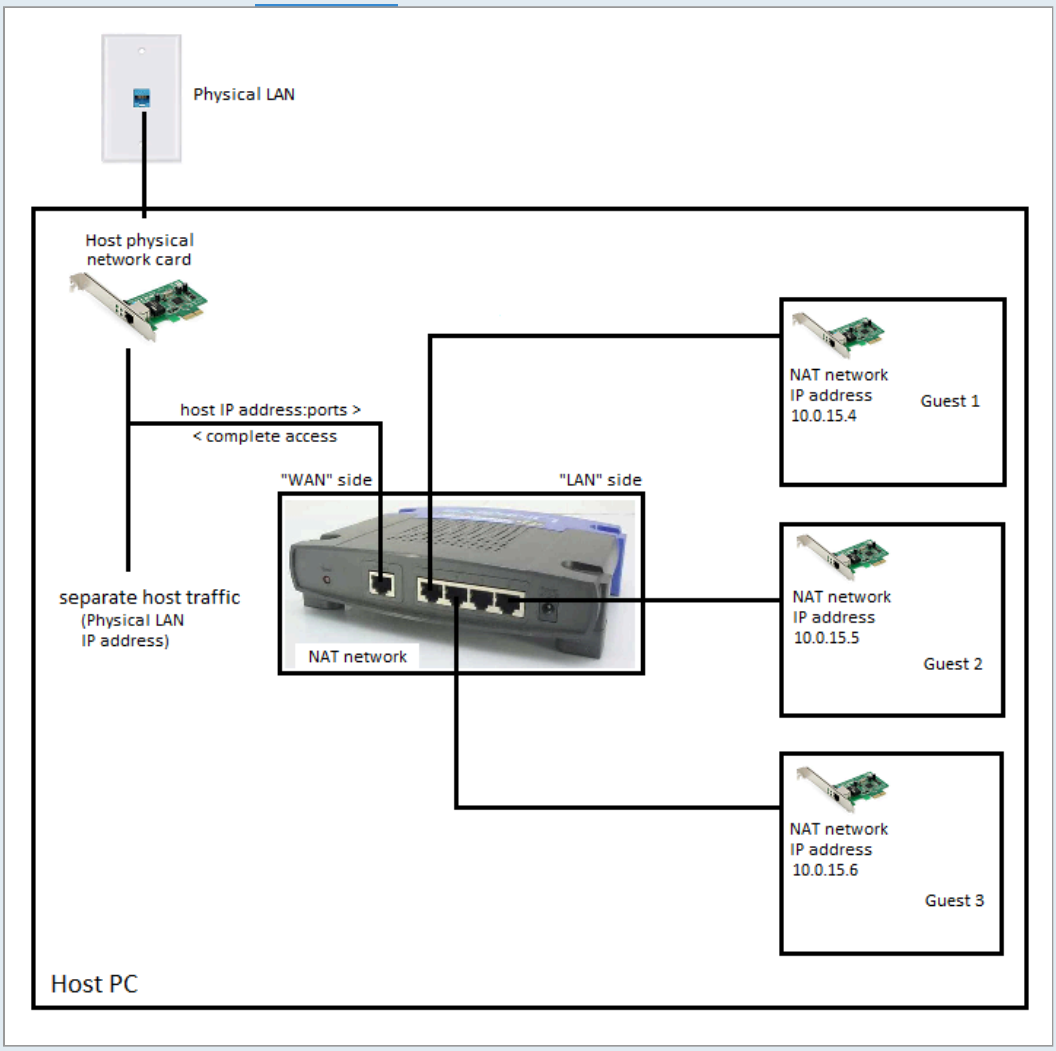
by **scottgus1** » 26. Jan 2020, 04:04

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

NAT Network

Virtualbox manual, section 6.4



NAT network.png (76.12 KiB) Viewed 135292 times

NAT Network behaves more like a typical house router with multiple LAN ports. Each NAT Network has its own 'name', and you pick the NAT Network to connect the guest to by choosing the desired NAT Network 'name'. Any number of guests can be connected to a NAT Network. All of the guests will be in a private "LAN". They will get IP addresses from the NAT Network's DHCP server, and the guests can all communicate freely with each other, just like in a real LAN. Like NAT, the guests can communicate with the host, the host's LAN, and the internet. The host, LAN, other guests not connected to the NAT Network, and the internet can only talk to the NAT Network's guests through forwarded ports.

NAT Network can have its default IP address range change to a desired range. You must do this before you use the NAT Network for the first time. If you change the NAT Network's IP address range after you have used the NAT Network, the DHCP

server associated with the NAT Network will not update to the new IP address range, and the guests will lose their internet access. If you delete the old DHCP-enabled NAT Network, its DHCP server remains behind. To remove a DHCP server use this vboxmanage command to see what DHCP servers are loaded in Virtualbox and what network names they apply to:

```
vboxmanage list dhcpservers
```

and this vboxmanage command to delete an old DHCP server:

```
vboxmanage dhcpserver remove --netname <old_network_name>
```

When opening a port, you will have to pick not only the port number but also which guest's IP address should receive the chosen outside network traffic.

Set up new NAT Networks in the main Virtualbox window, File menu, Preferences, Network.

The "WAN" side of NAT Network is always connected to the host; it cannot be connected elsewhere. For a NAT-like arrangement where the WAN connection can be positioned differently, use a separate VM with a router OS installed, like in "Sandbox" below.

The "WAN" side of NAT Network is connected into the host's network stream. So the host's firewall, antivirus, and VPN filter control network traffic to NAT Network.

Last edited by **scottgus1** on 30. Jan 2020, 20:20, edited 1 time in total.

Bridged Adapter

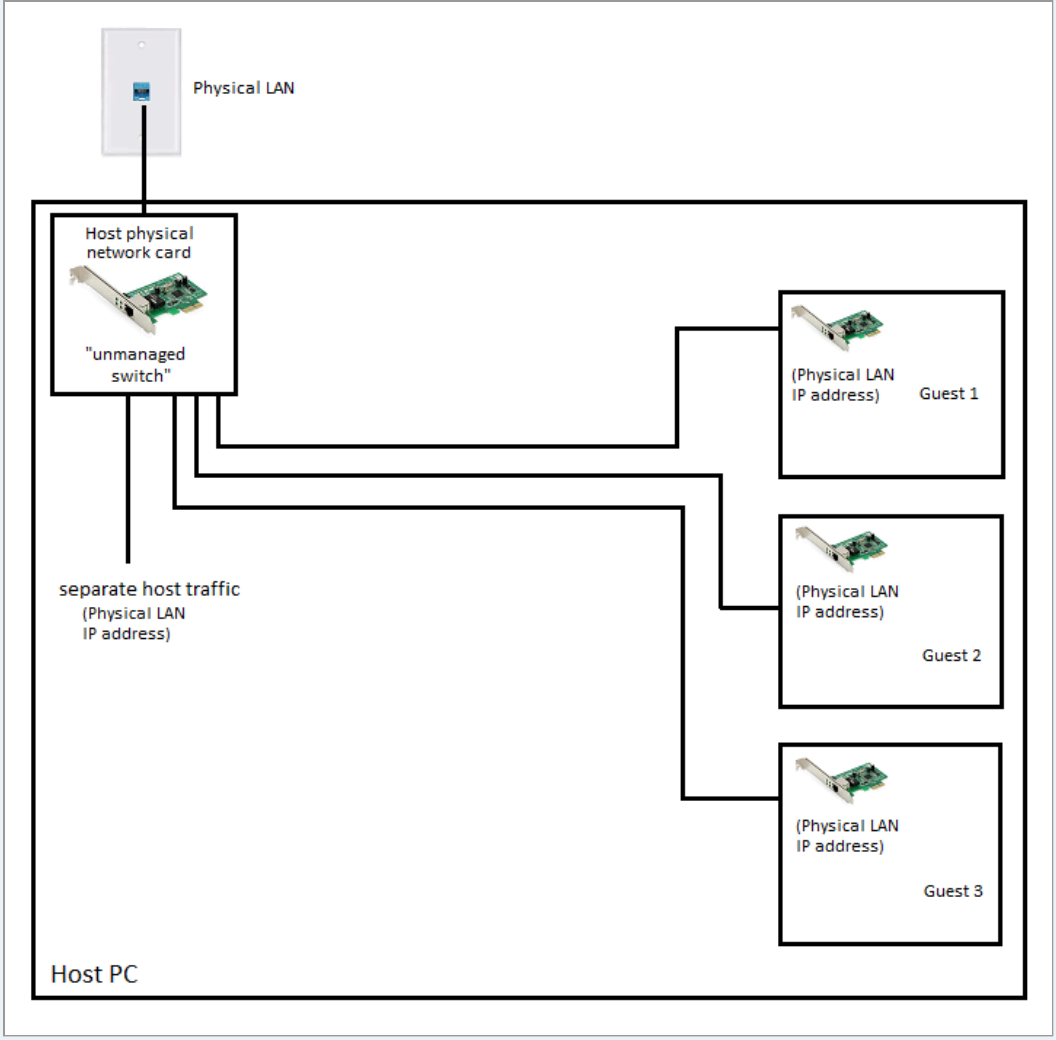
by **scottgus1** » 26. Jan 2020, 04:07

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

Bridged Adapter

Virtualbox manual, section 6.5



Bridged.png (37.24 KiB) Viewed 135292 times

Bridged puts the guests in the host LAN, just as if a virtual "unmanaged switch" were placed in your host's network card, and the host and all the Bridged guests were connected to it. A Bridged guest has complete access to all other Bridged guests, the host, the LAN, and the internet. There is no firewall or port forwarding with Bridged, and Bridged network traffic does not (usually *) get filtered by the host's firewall or antivirus. A VPN on the host might or might not interfere with Bridged.

Bridged should always work with the host's wired Ethernet adapter. Bridged may not always work with a host Wifi adapter, due to strict implementation of Wifi protocols by either the Wifi adapter driver or the access point firmware. Technically Wifi cannot Bridge, but some combinations of Wifi adapter drivers and access point firmware implement Wifi protocols in a lax fashion so Bridged can squeeze through. If it works where you are, good. If not, you need to go to wired Ethernet, pick another Virtualbox network type or two (NAT and Host-Only cover most situations), or use a Virtualbox USB filter to put a USB Wifi adapter directly into the guest. (Setting a correct static IP address inside the VM's OS on the VM's Bridged network adapter *might* get Bridged to work on Wi-Fi where it normally fails.)

The physical host network adapter that Bridged is using must be "up", that is, connected to something, so that the lights are flashing, even if it is another device that is not set up correctly for the host network. If the physical adapter is "down", Bridged will not start.

Also, if you are in a corporate environment with IT overlords, they may have restricted your office's Ethernet port(s) to only respond to your existing physical computer(s). Since Bridged VMs act as completely new computers on the office LAN, the IT restrictions may prevent the VM from connecting. You may have to

register the VM's MAC address or other information with IT to get Bridged to work.

* User 'Axe' reports here: viewtopic.php?f=3&t=109016&p=534132#p534125 that if the Windows host is set to think its network is a Public network, then the Windows Firewall Public rules apply, and Bridged VM traffic might get filtered by the Windows firewall.

Last edited by **scottgus1** on 23. Jul 2020, 18:47, edited 1 time in total.

Internal Network

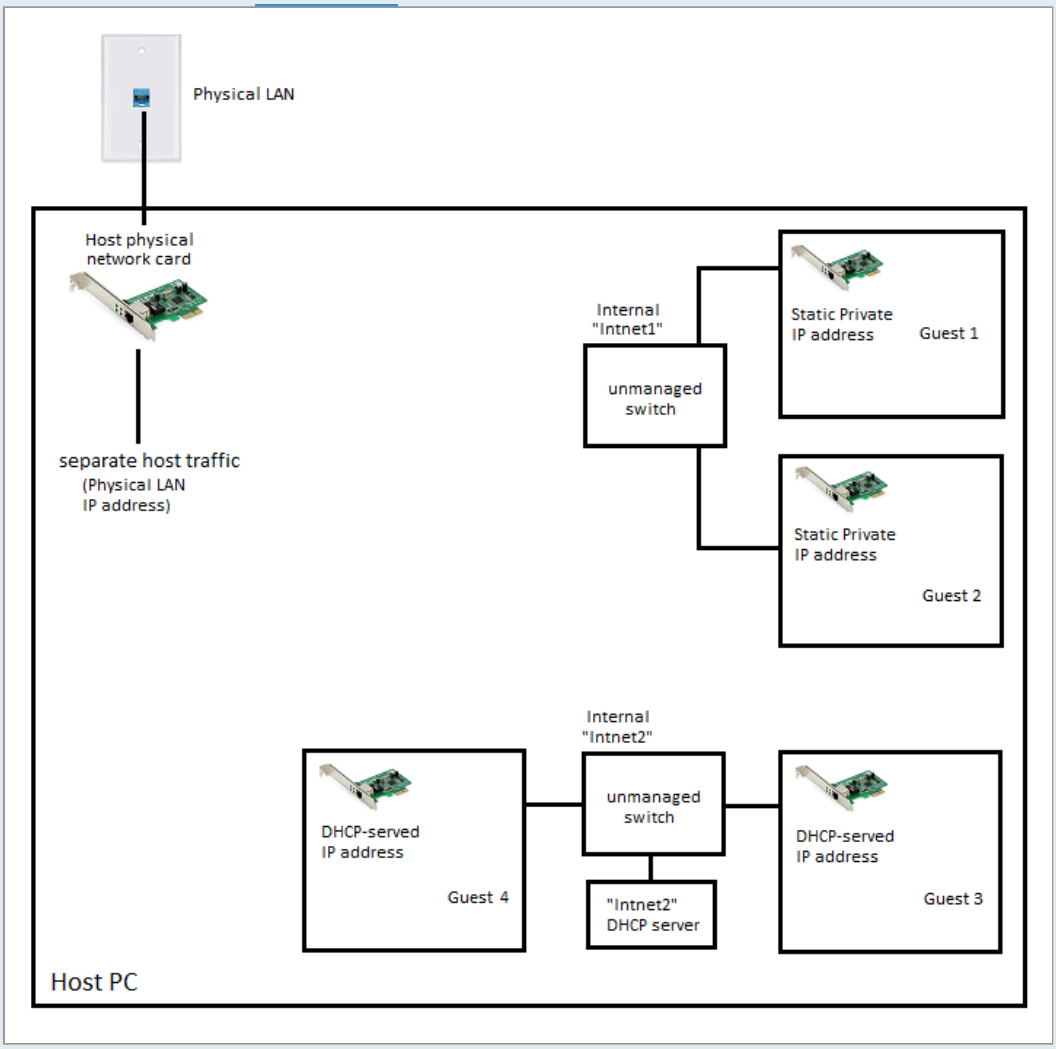
by **scottgus1** » 26. Jan 2020, 04:09

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

Internal Network

Virtualbox manual, section 6.6



Internal.png (40.53 KiB) Viewed 135292 times

Internal is a completely private network only for the guests attached to it. Internal behaves like an unmanaged switch. Each Internal network has its own 'name', and you pick the Internal network to connect the guest to by choosing the desired Internal network 'name'. Any number of guests can be connected to an Internal network. All of the guests will be in a private "LAN". The host, host LAN and other guests cannot access this Internal network. There is no internet provided by Virtualbox to Internal networks.

An Internal network does not have a DHCP server by default. You can set one up with vboxmanage commands, or have one of the guests act as a DHCP server, or have all the guests use static or APIPA addresses.

Host-Only Adapter

scottgus1

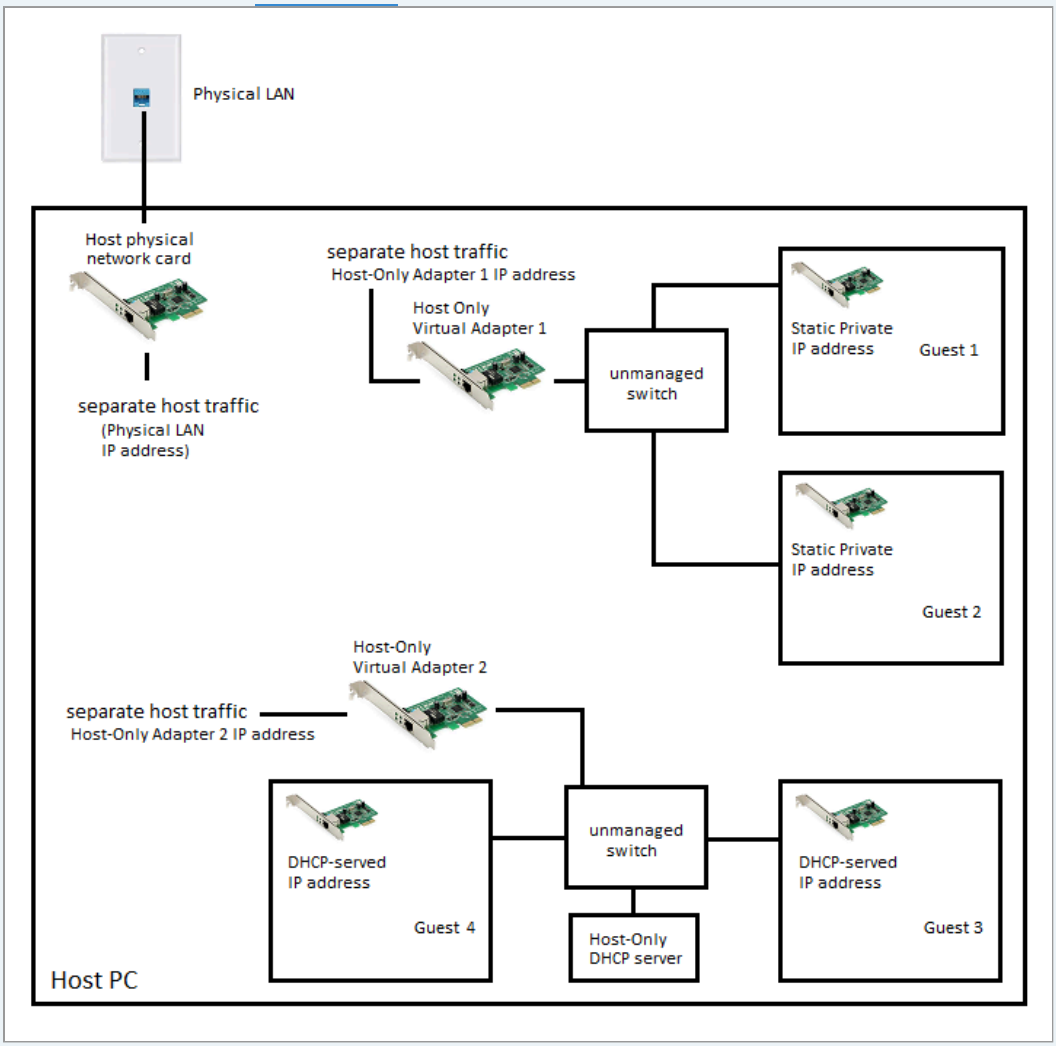
by **scottgus1** » 26. Jan 2020, 04:09

Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

Host-Only Adapter

Virtualbox manual, section 6.7



Host-Only.png (60.35 KiB) Viewed 135292 times

Host-Only is like an Internal network with a private host connection added in. Virtualbox makes virtual Host-Only network adapters that the host can communicate through by IP address. Any number of guests can be connected to a Host-Only network, by picking the desired Host-Only virtual adapter shown in the "Name:" dropdown. Only the host and the connected guests can communicate with each other. The host LAN, other guests, and internet are not able to connect into a Host-Only network.

Set up or modify Host-Only networks in the main Virtualbox window, File menu, Host Network Manager.

Host-Only's IP range must be set before any guest using it starts. You can change the Host-Only IP range, but you must do it before you start the first guest using Host-Only. If you want to change the Host-Only IP range later, you must shut down every guest and any Virtualbox windows, and wait a minute for the Virtualbox backbone service process 'VboxSVC.exe' to quit. Then you can re-open Virtualbox and change the Host-Only IP range.

From Virtualbox version 6.1.28 onward, non-Windows hosts need a configuration file placed in a certain host folder that requires administrator-privileges access to modify. This change plugs a security hole. See https://www.virtualbox.org/manual/ch06. ... k_hostonly the final paragraphs starting with "On Linux, Mac OS X and Solaris Oracle VM VirtualBox will only allow IP addresses..."

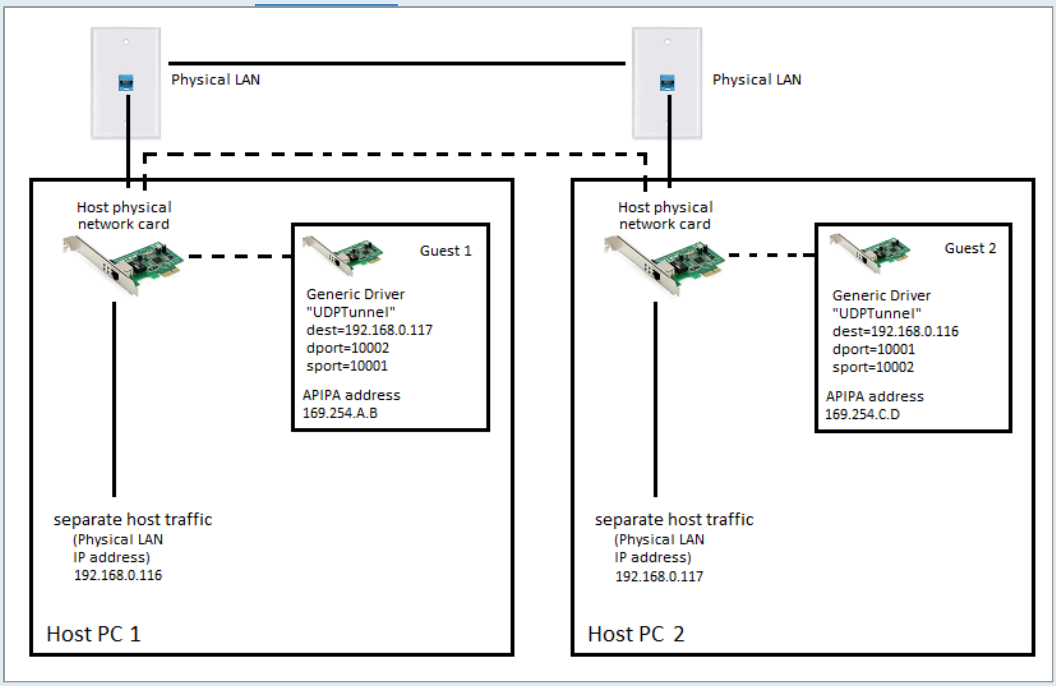
Last edited by **scottgus1** on 24. Jul 2020, 21:15, edited 1 time in total.

Generic Driver

by **scottgus1** » 26. Jan 2020, 04:13

Generic Driver

Virtualbox manual, section 6.8



Generic UDPtunnel.png (32.09 KiB) Viewed 135292 times

There are two forms of "Generic Driver" networking mentioned in the Virtualbox manual: "UDPTunnel" and "Virtual Distributed Ethernet".

"UDPTunnel" provides a way to get a private connection between two guests on different hosts. The "Name:" of this network must be spelled:

UDPTunnel

No other name or spelling will work.

The "Generic Properties" box must show three settings to enable the connection between the two guests on the two hosts:

```
dest=other.host's.IP.address
dport=other_host's_sport
sport=other_host's_dport
```

The 'dport' and 'sport' port numbers should be opened in each host's firewall.

There is no DHCP server on a UDPTunnel. Set static IP's or accept APIPA addresses if the guest OS's provide them.

The displayed Generic Properties in the UDPTunnel picture above enabled my two XP guests on the two hosts 192.168.0.116 and 192.168.0.117 to communicate, ping, and see each other's shared folders, as well as edit files. The XP guests set up APIPA addresses, and each guest was accessible from the other guest via the APIPA address the guest chose for itself.

One possible use of UDPTunnel could be to allow one to network together more guests than one host can handle, while not requiring separate physical network hardware for the test network. If one could get a suitable "un/managed switch" operating system installed in a guest, one could connect multiple UDPTunnels to

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

that guest, each UDPTunnel reaching to another host, and connecting multiple guests in a private multi-host "test lab" using the existing Ethernet network.

"Virtual Distributed Ethernet" (Virtualbox manual, section 6.9) is compatible only with Linux or FreeBSD host OS's, and can only be used when Virtualbox is built from the source code. VDE is not included in the Virtualbox installers. VDE is not illustrated yet.

Re: Virtualbox Networks: In Pictures

by **scottgus1** » 26. Jan 2020, 04:13

Reserved for future Virtualbox networking types.

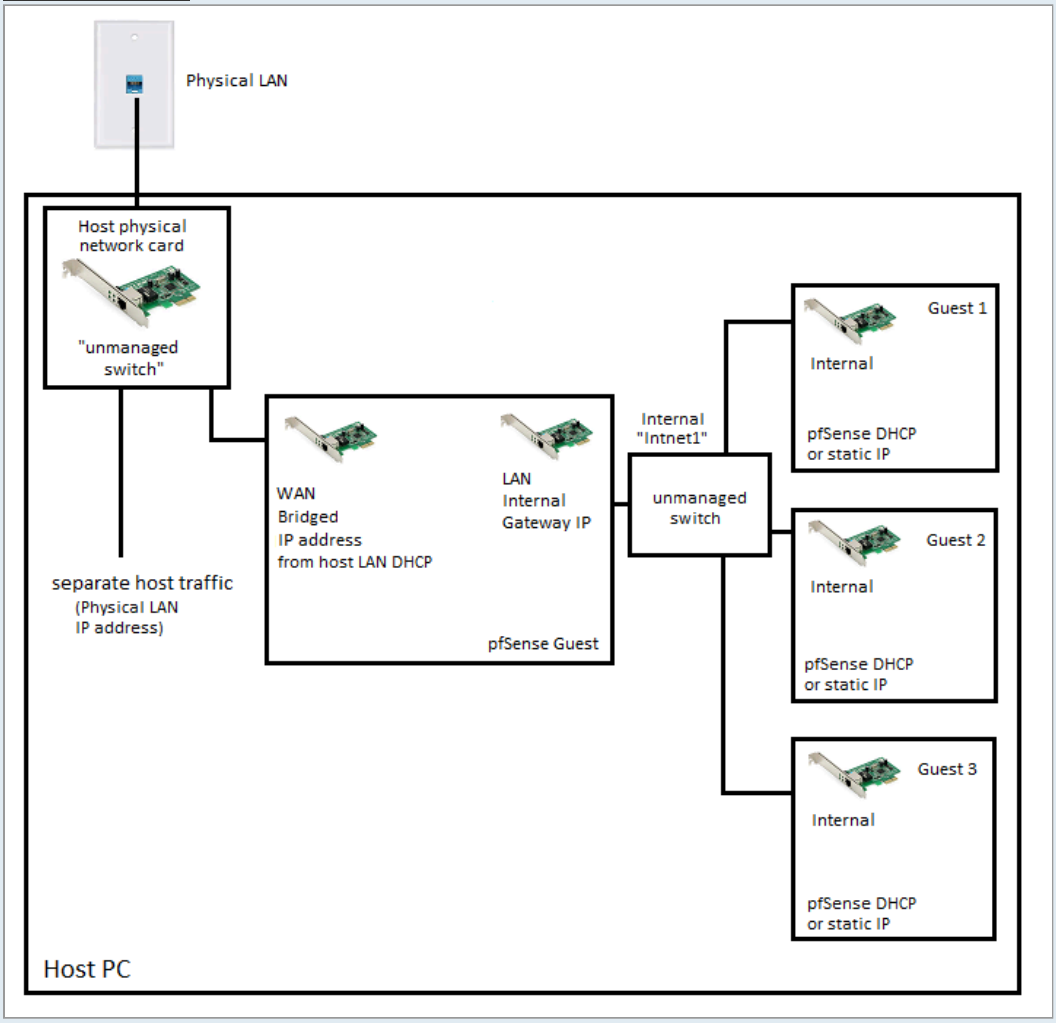
scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

Sandbox

by **scottgus1** » 26. Jan 2020, 04:17

"Sandbox"



pfSense guest network.png (47.52 KiB) Viewed 135292 times

"Sandbox" is not an official Virtualbox networking type and does not appear in the "Attached To:" dropdown. It is a setup using multiple Virtualbox networking types together with a router/firewall guest to make a more private yet internet-connected guest network than other Virtualbox networks can achieve.

Sandbox will let your guests access the host's internet connection without being able to access the host or host LAN. From the network perspective, the guests see the host's internet but they don't know there's a host.

scottgus1
Site Moderator

Posts: 20945
Joined: 30. Dec 2009, 20:14
Primary OS: MS Windows 10
VBox Version: VirtualBox+Oracle ExtPack
Guest OSses: Windows, Linux

This separation-yet-connection is achieved by using a guest with a router & firewall, which makes a new LAN with a different IP address range than the host's physical LAN, and setting up an outbound firewall rule that blocks the host LAN IP address range. Internet can get through, but nothing from the LAN can be reached.

Sandbox can enable such "labs" as testing internet-connected domain controllers without risking damage to the host LAN and other domain controllers. Sandbox does require the "lab's" LAN IP address range to be different than the "WAN" side of the router/firewall guest. However, one can set up two router/firewall guests, each blocking the next stage's IP range, and then achieve a lab LAN IP range the same as the host's LAN IP range with internet, but the lab still cannot access the host LAN. This "double-NAT-firewall" setup would enable testing changes to copies of production domain controller guests without having to change the domain's IP address in order to bring the guests into the lab or back into production settings. (See below for a double-NAT-firewall setup that worked.)

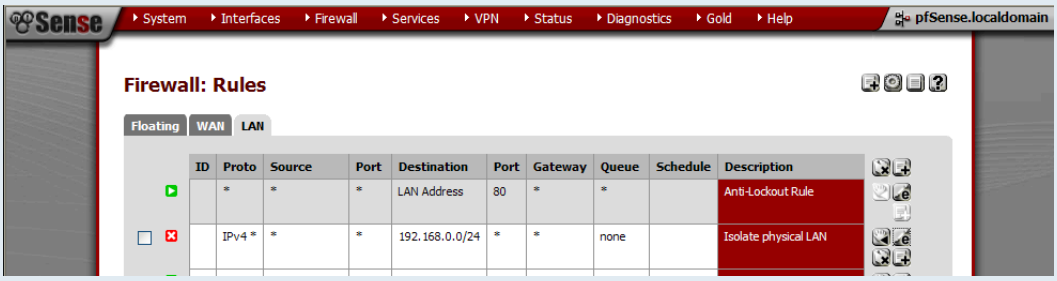
pfSense is a good, low-impact, free router/firewall operating system that can block host LAN access yet allow internet into the "lab".

The pfSense router guest has two networks. One is used as the "WAN" and connects to the host network via Virtualbox's Bridged. The other is the "LAN" port, and connects to the sandbox guest(s) via Virtualbox's Internal network.

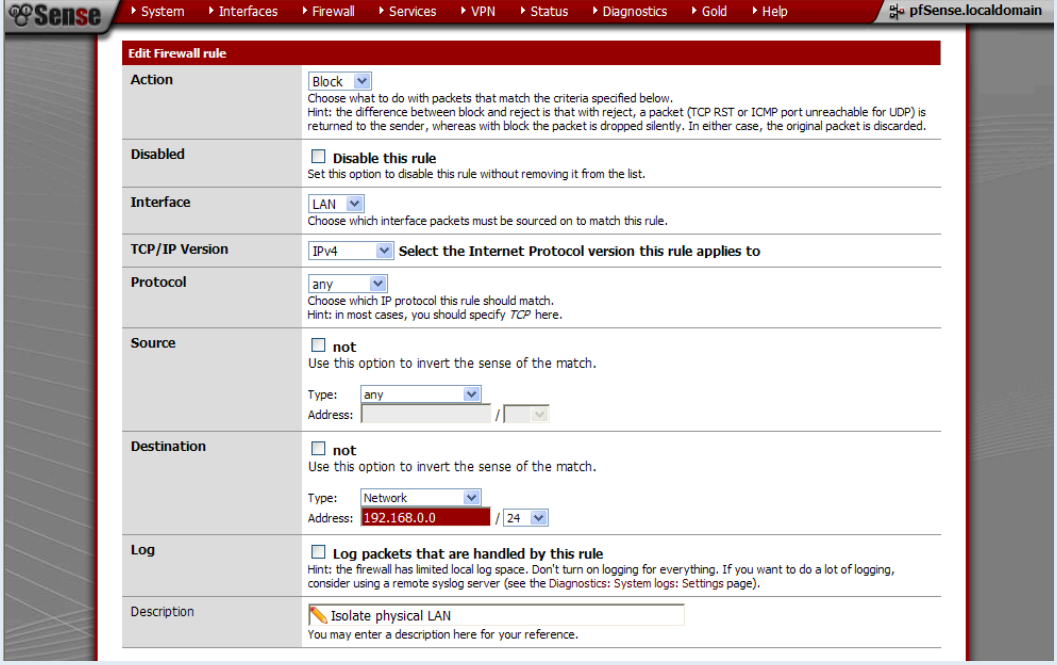
The WAN side will receive an IP address from the host LAN DHCP server. Turn the pfSense router's DHCP on, or have a guest run DHCP, and serve IP addresses in a different IP range than the WAN network. In the pfSense firewall, set an LAN outgoing block rule set to the WAN side's IP address range. Here are example settings, with the host's LAN being 192.168.0.#/24, and the lab's LAN set to 10.#.#.# or 172.16.#.#.

Put the rule as the second rule on the LAN tab, and your sandbox guest will not be able to find the host network on the WAN side, but will access the internet.

Credit goes to thetrevster, who figured out the correct settings:



Here's the settings to make the rule:



Action: Block
Disabled: not checked
Interface: LAN
TCP/IP Version: IPv4
Protocol: Any
Source: nothing entered, don't change
Destination: Type = "Network"; Address = host LAN IP range & subnet mask bit number
Log: if desired
Name: as desired

****

The following "double-NAT-firewall" was used to set up a test lab with an Active Directory domain controller & DHCP server and two clients in the 192.168.0.0/24 IP range, on a Virtualbox host with an existing physical LAN controlled by a DHCP-serving house router using the same 192.168.0.0/24 IP range. Internet was present in the lab, but the host LAN's computers could not be seen or controlled by the domain controller:

Virtualbox host:
IP range 192.168.0.0/24

pfSense VM 1 (default Virtualbox FreeBSD 64-bit settings, one processor, 256MB RAM reported 36% used):
WAN adapter, Bridged to host LAN, IP address served via host LAN's DHCP (192.168.0.0/24 range)
LAN adapter, Internal network "sandbox1", static IP 172.16.0.1
DHCP server enabled, serving 172.16.0.0/24
DNS Resolver disabled, DNS Forwarder enabled, no special settings (*)
Firewall rule as above, blocking 192.168.0.0/24

pfSense VM 2 (default Virtualbox FreeBSD 64-bit settings, one processor, 256MB RAM reported 38% used):
WAN adapter, Internal network "sandbox1", IP address served via pfSense VM 1's DHCP (172.16.0.0/24 range)
LAN adapter, Internal network "sandbox2", static IP 192.168.0.1
DHCP server disabled
DNS Resolver disabled, DNS Forwarder enabled, no special settings (*)

Firewall rule as above, blocking 172.16.0.0/24

Domain controller VM (Windows Server 2008 r2)
adapter, Internal network "sandbox2", static IP 192.168.0.2
DHCP server enabled, serving 192.168.0.0/24 & gateway 192.168.0.1
DNS enabled, pointing at 192.168.0.2
&
client VMs (XP)
adapters, Internal network "sandbox2", IP addresses served via Domain controller's DHCP (192.168.0.0/24 range)
attached to the domain
internet available on DC and clients, no pings possible to host LAN PCs

(A standalone VM can be attached to Internal network "sandbox1" to access pfSense VM 1's configurator website.)

* The pfSense Community Edition 2.4.4 I had on hand for this test lab had DNS Resolver enabled, DNS Forwarder disabled by default. A client VM attached to the LAN Internal network "sandbox1" on pfSense VM 1 could not get internet until I disabled Resolver and enabled Forwarder. I don't know why this was necessary. I did the same for pfSense VM 2 and the lab worked.