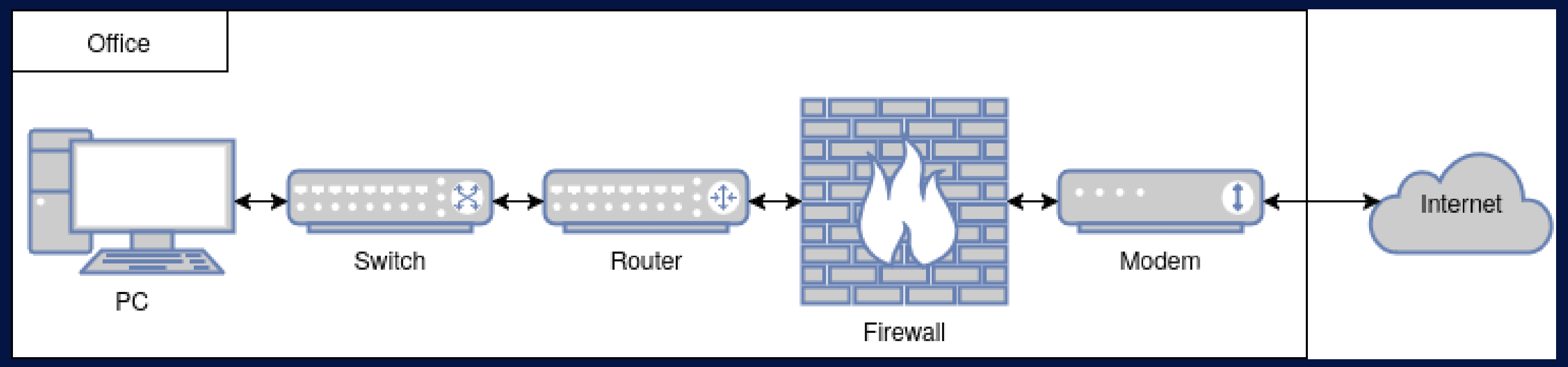
Zone Based Firewall

Graduate student: Austin Hunt

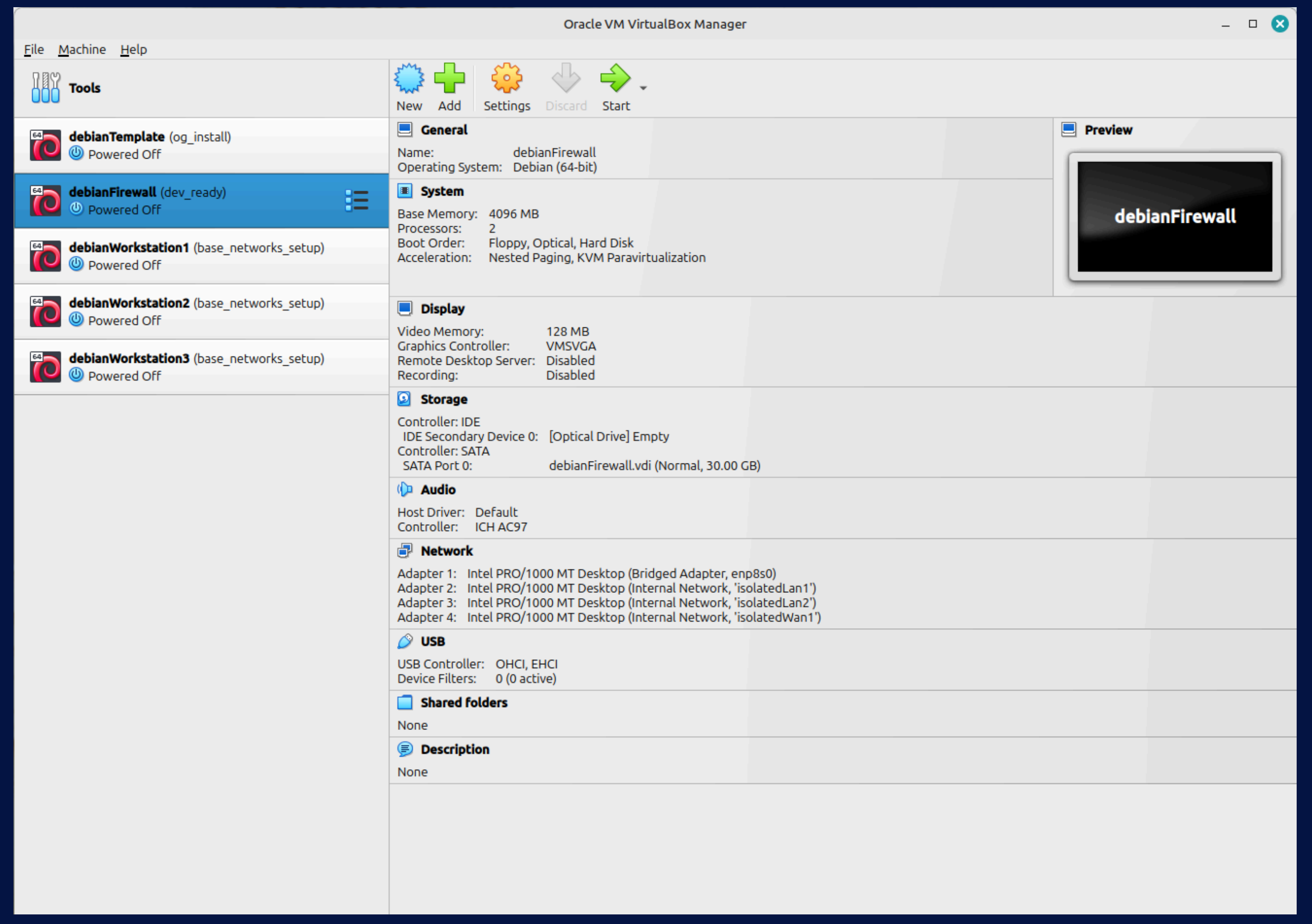
Advisor: Jingpeng Tang

Abstract

- Topic
  - Network firewall
- Long-term goal
  - Create an enterprise-level firewall with the below features.
- Project goal
  - Create the prototype of the firewall portion of this long-term goal.
- Features
  - Open-source
    - Free, easy to change, easy to audit the code, make improvements to, etc.
  - Linux based
    - Greater hardware support, faster upstream development of new features compared to BSD kernel.
  - Nftables
    - Nftables is the packet classification framework which does the firewalling. It is the replacement for iptables, ip6tables, ebtables, arptables. It is more robust and flexible to work with.
  - Zone and policy based
    - Simplify firewall logic by using one or more zones; which are a level of trust. A policy governs what traffic may leave or enter zones. Policies are comprised of rules.
  - Easy-to-use interface
    - Simple and modern management user interface.
  - Multiple sites
    - Be able to support multiple firewalls and configure them all from a central location. This eases the management burden for administrators when there are many to configure and maintain.
  - High-availability
    - Be able to have multiple firewalls act as a group for redundancy purposes.
- Outcome
  - Successful prototype created for the nftables firewalling portion. More work needed to improve the API design so that it is simpler to use.



Simple office network topology showing where the firewall is at



Oracle VM VirtualBox Manager

debianTemplate (og_install) Powered Off
debianFirewall (dev_ready) Powered Off
debianWorkstation1 (base_networks_setup) Powered Off
debianWorkstation2 (base_networks_setup) Powered Off
debianWorkstation3 (base_networks_setup) Powered Off

General
Name: debianFirewall
Operating System: Debian (64-bit)

System
Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Preview
debianFirewall

Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: debianFirewall.vdi (Normal, 30.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

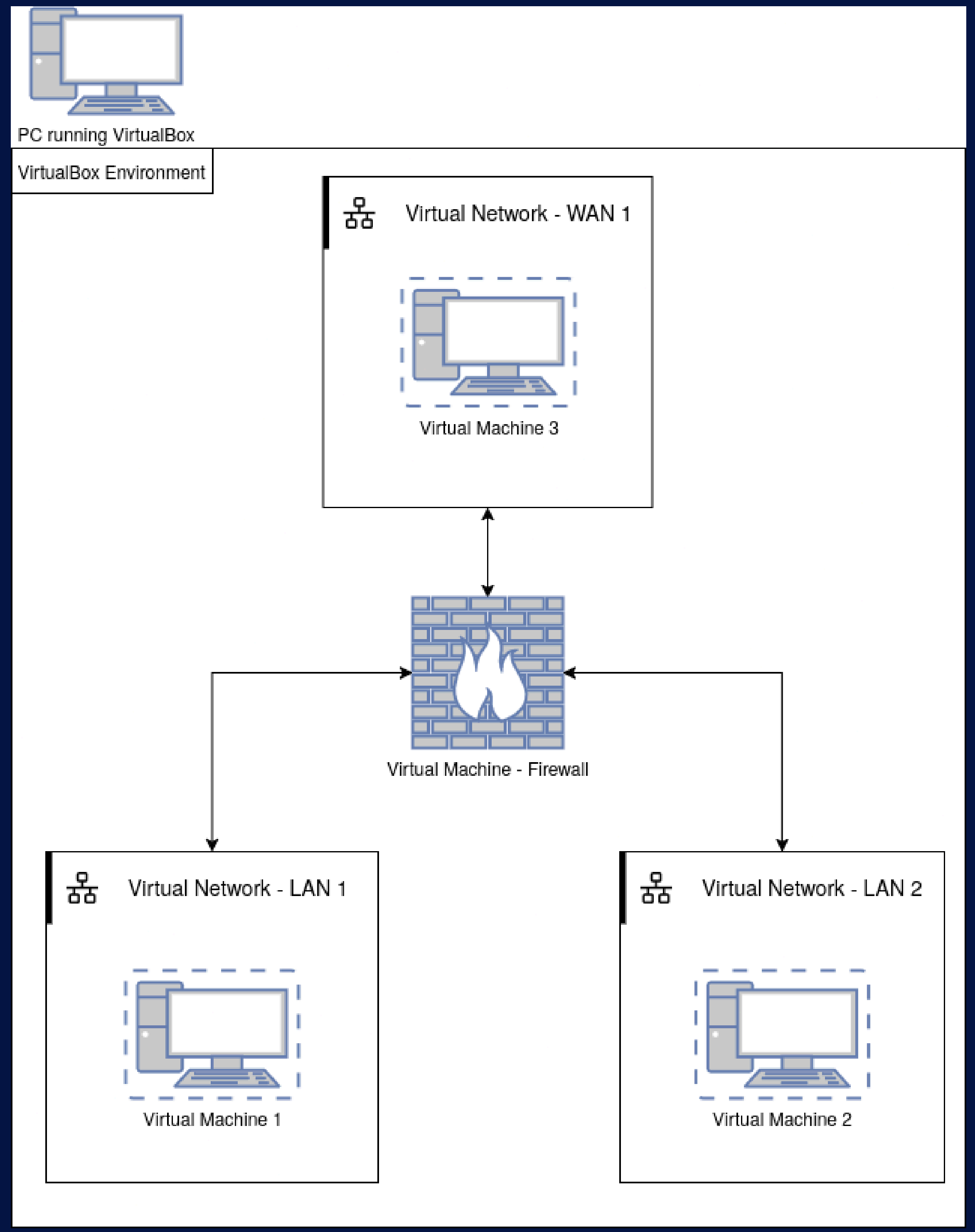
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, enp8s0)
Adapter 2: Intel PRO/1000 MT Desktop (Internal Network, 'isolatedLan1')
Adapter 3: Intel PRO/1000 MT Desktop (Internal Network, 'isolatedLan2')
Adapter 4: Intel PRO/1000 MT Desktop (Internal Network, 'isolatedWan1')

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

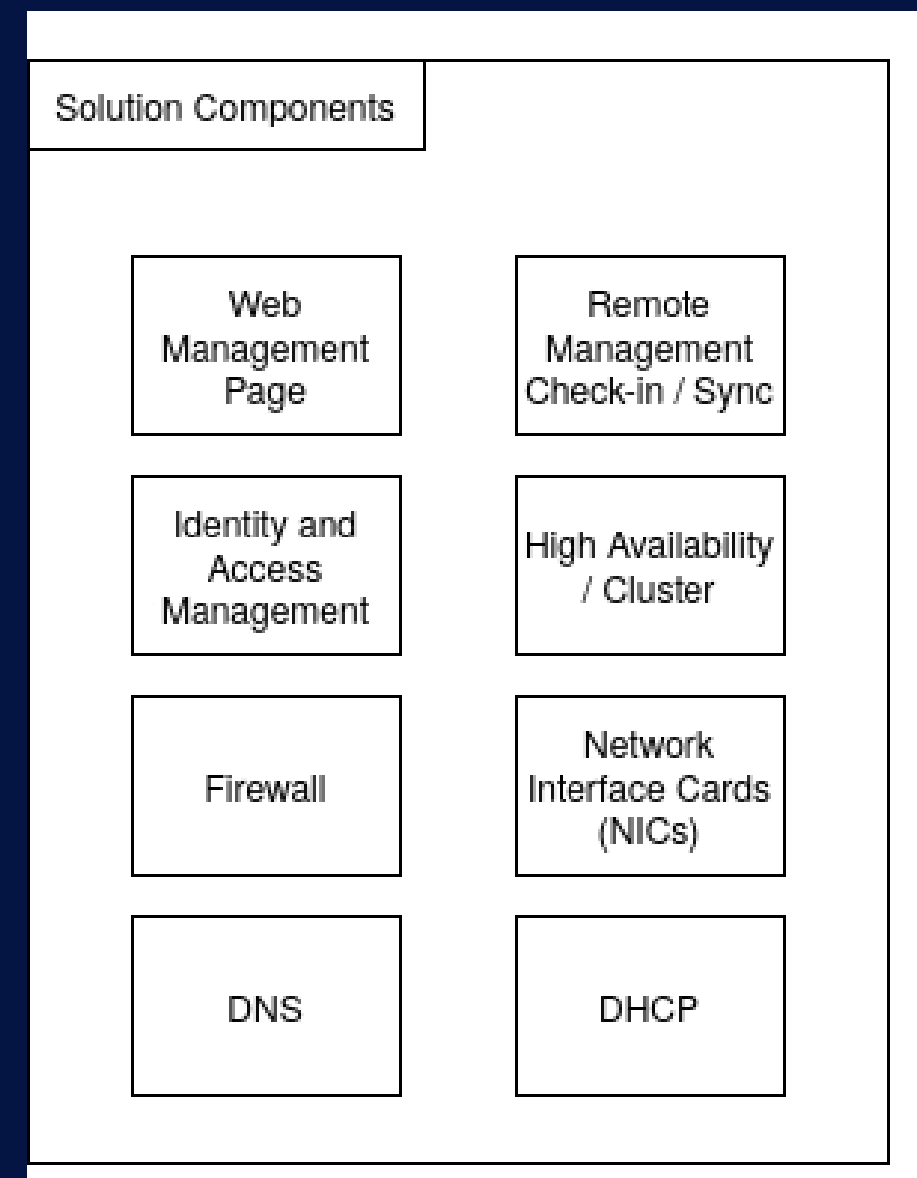
Shared folders
None

Description
None

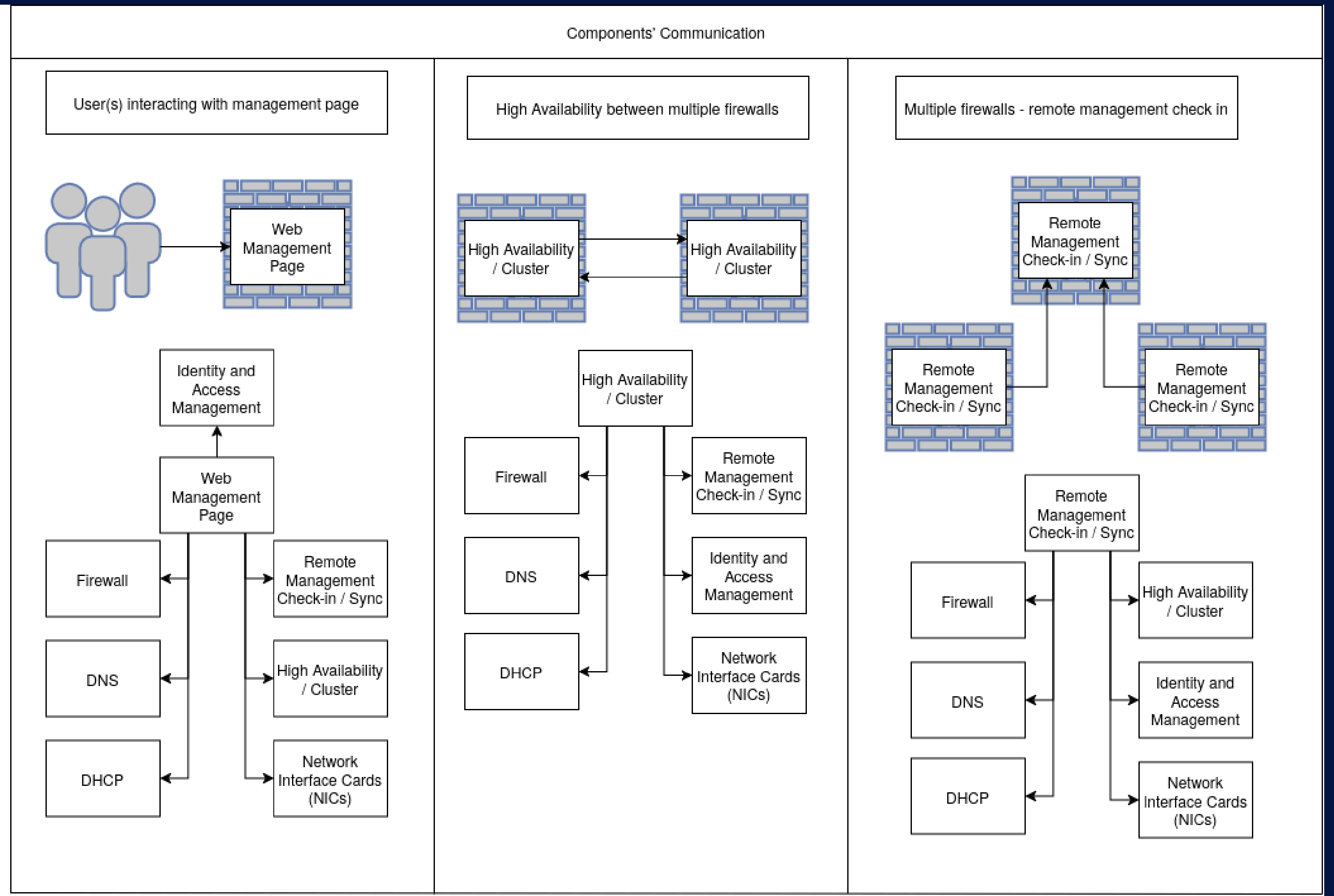
VirtualBox testing environment



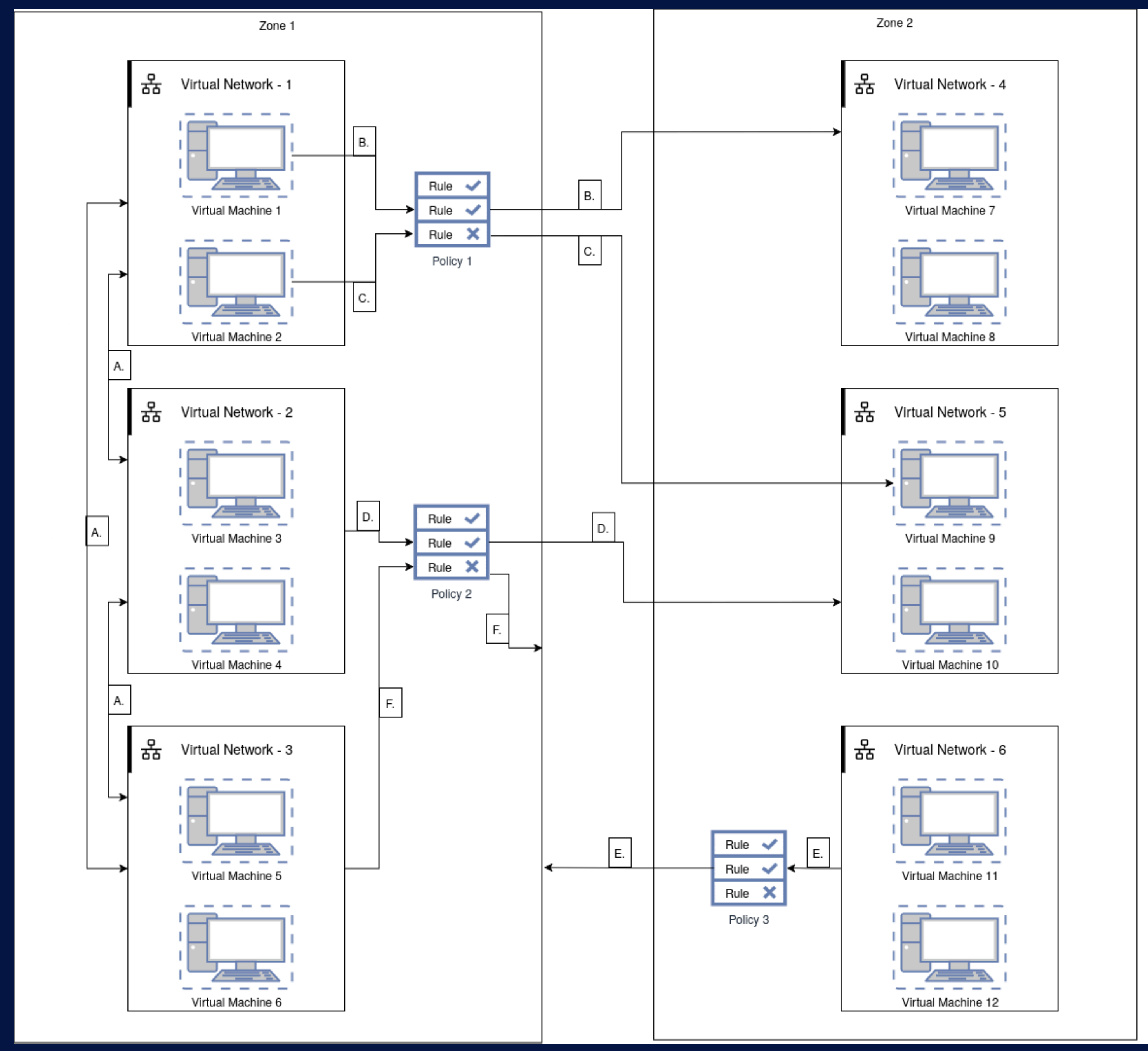
Logical representation of the above VirtualBox environment


Solution Components
Web Management Page
Remote Management Check-in / Sync
Identity and Access Management
High Availability / Cluster
Firewall
Network Interface Cards (NICs)
DNS
DHCP

System's components


Components' Communication
User(s) interacting with management page
Web Management Page
Identity and Access Management
Web Management Page
Firewall
Remote Management Check-in / Sync
DNS
High Availability / Cluster
DHCP
Network Interface Cards (NICs)
High Availability between multiple firewalls
High Availability / Cluster
High Availability / Cluster
High Availability / Cluster
Firewall
Remote Management Check-in / Sync
DNS
Identity and Access Management
DHCP
Network Interface Cards (NICs)
Multiple firewalls - remote management check in
Remote Management Check-in / Sync
Remote Management Check-in / Sync
Remote Management Check-in / Sync
Remote Management Check-in / Sync
Firewall
High Availability / Cluster
DNS
Identity and Access Management
DHCP
Network Interface Cards (NICs)

Communication between specific components for 3 scenarios



Explanations:

A. Connections between networks in the same zone are allowed.

B. Virtual machine 1 is allowed to talk to virtual network 4.

C. Virtual machine 2 is allowed to talk with virtual machine 9, but it can't talk with virtual machine 10.

D. Virtual network 2 can talk with virtual network 5.

E. Virtual network 6 can talk with all of zone 1.

F. Virtual network 3 is not allowed to leave zone 1.

Example of multiple zones, policies, networks, and their interactions