A picture containing logo

Description automatically generated

DESIGN AND IMPLEMENTATION OF

SECURE HOME NETWORK WITH OPENWRT

B9CY101: Networks and System Administration

:

Table of Contents

Acronyms 2

Introduction 3

Background 3

Tools and Technologies used 5

Scope 5

Advantages of system 5

Technical Description 5

1. Topology to build secure home network 7
2. IP Address 8
3. DHCP & DNS 8
4. SSH Access 9
5. Security Zones 9
6. Netdata: Real Time Monitoring Dashboard 10
7. QoS Traffic Shaping 10
8. OpenVPN Client using LuCI 13
9. Capture, filter and inspect packets using tcpdump 14

Conclusion 15

References and Bibliography 16

**Acronyms**

**CAKE** – Common Application Kept Enhanced

**DNS** – Domain Name Server

**DHCP** – Dynamic Host Configuration Protocol

**IoT** – Internet of Things

**IP** – Internet Protocol

**LAN** – Local Area Network

**OpenWrt** – Open Wireless Router

**OSS** – Open-Source Software

**Pcap** – Packet Capture

**QoS** – Quality of Service

**RAM** - Random Access Memory

**SSH** – Secure Shell

**SSL** – Secure Socket Layer

**SQM –** Smart Queue Management

**TCP** – Transmission Control Protocol

**TLS** – Transport Layer Security

**UCI** – Unified Configuration Interface

**UDP** – User Datagram Protocol

**VDI** – Virtual Desktop Infrastructure

**VM –** Virtual Machine

**VPN** – Virtual Private Network

**WAN** – Wide Area Network

**Introduction**

Cyberattacks are one of the most serious threats to businesses of all sizes. As sophisticated ransomware assaults increase, the development of remote work is exposing new risks to data breaches. Although this risk is causing some businesses significant financial pain, it is also providing opportunity for security providers.

Chart, treemap chart

Description automatically generated

**Figure 1: Cybersecurity spending, 2021**

The objective of this project is to design and implement a Secured Home Network in a virtual environment and with Open-Source Software (OSS) that provides end-users with a consistent experience. Many of us don’t have resources to flash our router to give OpenWrt or Linux a try or bringing it to life on a real hardware we will be building the test lab in a virtual environment using VirtualBox. OpenWrt will be hosted in Oracle VirtualBox with two network ports along with an Ubuntu and Windows systems for demonstration. For this, we will build two networks, the LAN (Local Area Network) – an internal network where we can incorporate our local PC’s, any IOT devices, Guest Network, and the WAN (Wide Area Network) – the internet.

**Background**

While virtual environments are beneficial for accelerating innovation and cutting computing costs, they also introduce a growing number of security and compliance issues not seen in traditional data centers. Decentralized infrastructures, where applications, data, and workloads are deployed from multiple endpoints rather than a single dedicated resource, are often targets for new types of attacks that bypass traditional perimeter security, making comprehensive visibility and security difficult to achieve. Another security risk is the speed with which consumers now demand virtualized environments to supply services. Security experts must balance DevOps speed with security problems that increasingly span multiple locations. The correct next-generation virtual firewall can enable your IT environment, including private clouds, public clouds, and branch sites, maintain a consistent network security posture.

OpenWrt is a Linux distribution for embedded devices that may be deployed on a variety of routers. OpenWrt provides a web interface and may be more stable than the default firmware on your gear. You're a candidate for OpenWrt if you find yourself having to restart your router every few days because it's grown bogged down. OpenWrt was created by network professionals and people who care about their network's performance. Many algorithms from current research have been incorporated into OpenWrt, and they perform significantly better than vendor-supplied firmware.

Diagram

Description automatically generated

**Figure 2: OpenWrt general topology**

**Performance & Stability**

* OpenWrt is a stable operating system that can be relied on for lengthy periods of time.
* Bufferbloat control mechanisms in OpenWrt reduce latency/lag and boost network throughput.
* Wi-Fi upgrades provide better data rates and equal airtime distribution between stations.
* Long after the manufacturer stops delivering updates, older devices are still supported by OpenWrt enhancements (as long as your device's RAM/Flash can accommodate new releases).

**Security**

* Hardware vendors did not leave any hidden backdoors.
* Because of its Linux OS, OpenWrt is immune to typical weaknesses and is unaffected by many popular attacks.
* Because OpenWrt is constantly updated, any vulnerabilities are patched as soon as they are detected.
* The default OpenWrt setup is very conservative, providing full internet access while protecting your router and associated devices from attacks.
* Many older devices are supported by OpenWrt and can benefit from the added security that OpenWrt provides, even after OEMs stop issuing firmware upgrades.

The goal of this project is to employ virtualization technology with OpenWrt to create a simple and secure home network, or to protect IoT devices from cybercriminals and vulnerabilities that could damage the entire network. It is possible to investigate the workflow and efficacy of the virtual firewall hosted in Oracle VirtualBox using this virtual network. In addition, this virtual network can be valuable while constructing a real network since it can control traffic and identify threat elements that may affect the network.

**Tools and Technologies used**

* Oracle VirtualBox
* Openwrt vdi
* Ubuntu
* Windows
* USB pen drive

**Scope**

* Firewall
* SSH Server
* OpenVPN
* Traffic-shaping and QoS
* Guest Network
* IOTZone
* Capture and Analyze Network Traffic

**Advantages of the system**

* Cost-effective, and can be used to secure a small network, such as a home network or IoT devices.
* Stable, and operates reliably for a long time.
* Reduces latency and increased network throughput via bufferbloat control algorithms.

**Technical Description**

In this section we will discuss all the technical characteristics required to deploy secure home network with OpenWrt. VirtualBox 6.1 version is installed which allows users and system administrators to easily manage and run various guest OS on a single host.

OpenWrt 19.07.4 stable release build is installed to create an Edge Router. We need x86 bit of OpenWrt and there are two versions of them.

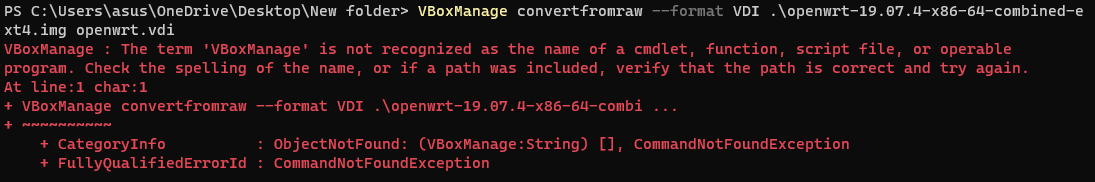
* combined-squashfs.img.gz
* combined-ext4.img.gz

In this project we will use *openwrt-x86-64-combined-ext4.img.gz* because it has less limits. Convert openwrt.img to VBox drive.

* Go to the downloaded directory and open terminal.
* Convert native VBox format with following command.

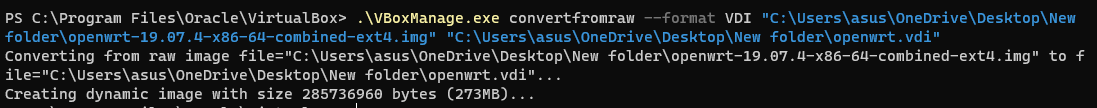
VBoxManage convertfromraw --format VDI openwrt-\*x86-64-combined\*.img openwrt.vdi

if encountering error as below



**Figure 3: VBoxManage error**

Go to > C:\Program Files\Oracle\VirtualBox\ open terminal from this path



**Figure 4: VBoxManage vdi output**

Enlarge the image to a useful size (512MB)



Let’s create new virtual box image as OpenWrt Edge Router, its Linux machine and version to selected as 2.x or later 64bit.



512MB RAM should be plenty for a little router. After that we have to add Edge Router image going into settings. Select Hard Disk and map the vdi image which we created.

For OpenWrt to work out of the box then we need to give LAN adapter as the first adaptor, so that will be Internal Network. The second adaptor will connect to the Internet and here we select bridged adaptor.

After booting the image, we can see that by default the OpenWrt router has 192.168.1.1 address. We will be changing the ip address to 192.168.99.1.

The command to do this is uci – that’s basically the command line interface into openwrt.

*#uci set network.lan.ipaddr=192.168.99.1*

*#uci commit*

*#reboot*

Text

Description automatically generated

**Figure 5: uci show network**

We can now able to access OpenWrt Edge Router using SSH from the Home PC which is on the same network with IP address 192.168.99.1 and user “root”

1. **Topology to build Secure Home Network**

**Diagram

Description automatically generated**

**Figure 6: Topology**

1. **IP Address**

The Internet Protocol address is the address that network devices use to communicate with one another. There are two types of IP addresses: Ipv4 and Ipv6. Ipv4 addresses are the older version of the internet protocol, with a capacity of 2 32 IP addresses, whereas Ipv6 addresses have a capacity of 2 128 IP addresses. Ipv6 has advantages over Ipv4 such as no IP collisions, auto-configuration, and no need for network address translation, although most devices are still running on Ipv4. Private IP addresses and public IP addresses are the two types of IP addresses available.

Private IP addresses are assigned to interact with devices over the internet in a small network with a small number of network devices, whereas public IP addresses are issued to communicate with devices over the internet in a large network with many network devices. The Internet Service Provider (ISP) assigns public IP addresses, whereas the Network Administrator can assign private IP addresses.

1. **DHCP & DNS**

The Domain Name System is abbreviated as DNS. we will use domain names to access webpages and other internet services, while IP addresses will be used for actual communication. Every internet service housed on the internet has its own unique IP address, making it difficult for humans to remember them. The IP records of the Internet Service that the user is seeking for are stored on DNS servers, making it simple for people to find the service they are looking for. DNS operates by translating a hostname into a computer-readable IP address, which is known as a forward lookup. Additionally, these DNS servers can translate an IP address to a domain name.

A DHCP server assigns an IP address and other required information to hosts on the network so that they can communicate with endpoints efficiently. The DHCP server sends information such as the host's assigned IP address, Domain Name Server address, Default Gateway, and other setup data to the client. Because it may eliminate the same IP address for the same host devices in the network, DHCP can be used to simplify IP address management in the network.

Graphical user interface, text, application, email

Description automatically generated

**Figure 7: DHCP Entries**

1. **SSH Access**

OpenWrt listens for incoming SSH connections on port 22/tcp by default. We can either use any windows terminal emulators (cmd.exe, powershell.exe) or Putty to get the command-line-access to openwrt.

**Graphical user interface, application

Description automatically generated**

**Figure 8: Putty**

1. **Security Zones**

Security zones on the firewall are a logical approach to arrange physical and virtual interfaces to restrict and log traffic that passes through certain network interfaces. Before an interface on the firewall can process traffic, it must be allocated to a security zone. Multiple interfaces of the same type (such as tap, layer 2, or layer 3 interfaces) can be allocated to a zone, but an interface can only belong to one zone. Using OpenWrt web interface we have created some important firewall rules with creating multiple security zones categorized as LAN (Local Area Network – all home PC’s), WAN (Internet), GuestZone (All guest devices) and IOTZone (all IOT devices).

**Graphical user interface

Description automatically generated**

**Figure 9: Security Zones in OpenWrt**

1. **Netdata : Real Time Monitoring Dashboard**

Netdata is meant to install without disrupting any of the system's running apps. It uses only idle CPU cycles and operates according to the user's memory requirements. Beyond logging, the application will not conduct disk I/O after it has started. Upon the end of its execution, the utility saves to disk and reloads at startup. It comes with a few plugins that collect key system metrics by default, but its functionality can be extended via the plugin API. Netdata is a Linux-based program that can operate on almost any machine and has graphics that can be embedded in web sites.

**A screenshot of a computer screen

Description automatically generated with medium confidence**

**Figure 10: Netdata system overview**

1. **QoS Traffic Shaping**

Shaping is a QoS (Quality of Service) technique for enforcing lower bitrates than the physical link can support. To enforce "traffic contracts" with their consumers, most ISPs will use shaping or policing. When we use shaping, the traffic is buffered to a specific bitrate, however when we use policing, the traffic is dropped when it surpasses a given bitrate.

Graphical user interface, text, application

Description automatically generated

We need to install luci-app-sqm package to configure QoS for our interface. Here we have 3 interface created, br-lan (lan) , eth0 (lan) , eth1 (wan). We will be enabling sqm instances for ingress and egress shaping on br-lan(lan) interface.

**Graphical user interface, text, application, email

Description automatically generated**

**Figure 11: SQM interface**

We will limit the Download and Upload speed by 50000Kbps to reserve the resource for other critical services.

**Graphical user interface, text, application, email

Description automatically generated**

**Figure 12: SQM settings**

QoS for gateways uses the Common application kept enhanced (CAKE) scheduler. It uses advanced fair queue mechanism that distributes bandwidth while considering packet delays. CAKE isn't like other traffic shapers or policers in that it aims to offer each traffic flow a fair part of the road. It prevents fat flows from taking up the entire circuit. CAKE was designed with internet-based uplinks in mind, making it excellent for dynamic WAN throughput. CAKE dynamically adjusts to traffic variations throughout the day, giving more bandwidth when traffic demands it and less bandwidth when traffic demands it.

**Graphical user interface, text, application, email

Description automatically generated**

**Figure 13: SQM CAKE**

After configuring SQM QoS with Luci we can notice that the traffic is limited to what configured.

Graphical user interface

Description automatically generated

**Figure 13: Netdata overview of QoS traffic**

1. **OpenVPN Client using LuCI**

OpenVPN is a virtual private network (VPN) system that uses techniques to construct secure point-to-point or site-to-site connections, as well as remote access facilities, in routed or bridged configurations. It can run both client and server programs. Peers can utilize pre-shared secret keys, certificates, or username/password to authenticate each other with OpenVPN. It allows the server to release an authentication certificate for each client utilizing signatures and a certificate authority when used in a multiclient-server arrangement. It makes considerable use of the OpenSSL encryption library, as well as the TLS protocol, and has numerous security and control features.

In order to use OpenVPN using web interface, we must install below packages

* *Openvpn-openssl*
* *Luci-app-openvpn*

To connect to their service, all self-respecting commercial OpenVPN providers will supply self-contained OpenVPN config files that you can load into your consumer router or network device.

Here, we have downloaded us.atlanta.ovpn file and uploaded in web interface.

Graphical user interface, text, application, email

Description automatically generated

**Figure 14: Ovpn config**

**Graphical user interface

Description automatically generated**

**Figure 15: OpenVPN instances**

Also, we need to configure tun0 interface in WAN zone. Once if we click Save & Apply it should start the service. Unfortunately, the OpenWrt virtualbox image has got some limitations and its not starting the service.

1. **Capture, filter and inspect packets using tcpdump**

OpenWrt is a flexible platform based on GNU/Linux that provides cutting-edge solutions. You may use tcpdump, Wireshark, or even a switch to capture data and transfer it to a remote analysis system. tcpdump is a utility for capturing and analyzing network traffic. It can be used to capture packets on the fly and/or save them to a file for analysis later on. Because tcpdump is based on libcap, it may generate standard pcap analysis files that can be handled by other tools.

To install tcpdump on OpenWrt

*#opkg install tcpdump*

To capture all packets on WAN interface eth1

**Text

Description automatically generated**

**Figure 16: tcpdump output**

**Conclusion**

Based on the logs from the hosted virtual firewall, it appears that it can control over 10 devices in a home network. As a result, this prototype model can be used to create a real-world physical network that is protected from external threats. IoT devices, internal media streaming servers, file servers, database servers, and other devices can all benefit from this network approach. A physical firewall running any opensource firewall image can be used to ensure packets pass past the firewall. The report's installation and implementation process can be used to solve a variety of network security issues.

**References and Bibliography**

Bursi, A. (2016). *OpenWrt on VirtualBox HowTo*. [online] OpenWrt Wiki. Available at: https://openwrt.org/docs/guide-user/virtualization/virtualbox-vm [Accessed 24 Nov. 2021].

‌

Brown, R. (2016). *Documentation*. [online] OpenWrt Wiki. Available at: https://openwrt.org/docs/start [Accessed 24 Nov. 2021].

Wich, J.-P. (2009). *The UCI system*. [online] OpenWrt Wiki. Available at: https://openwrt.org/docs/guide-user/base-system/uci [Accessed 24 Nov. 2021].

‌