

## Building a Secure Router

### What is a Secure Router?

A secure router is a device that provides a secure data plane for packets. The secure data plane provides a secure environment for packets to travel through internet, ensuring that the packets are not compromised or tampered with.

Automation using high speed monitor traffic based on XDP Hook and Artificial Intelligence to detect, preventing possible vulnerabilities and attacks in earlier stages. Saving time and money with quicker reactions.

### OpenWRT

Our secure router is based on the OpenWRT operating system, which provides a secure and reliable platform for the secure data plane. Using the advantages that provide [eBPF](#) and [XDP](#).

### Build System Usage

```
git clone https://git.openwrt.org/openwrt/openwrt.git
cd openwrt
git pull

# Use
# This Commit "xdp-tools: update to version 1.2.8 - Mon, 19 Sep 2022"
# Or Upper
REV_HASH="4c73c34ec4215deb690bf03faea2a0fe725476f0"
git checkout ${REV_HASH}
REV_BRANCH="$(git rev-parse --abbrev-ref HEAD)"

sed -e "/^src-git\S*/s//src-git-full/" feeds.conf.default > feeds.conf

./scripts/feeds update -a

sed -n -e "/^src-git\S*\s/{s///;s/\s.*$/p}" feeds.conf \
| while read -r FEED_ID
do
REV_DATE="$(git log -1 --format=%cd --date=iso8601-strict)"
REV_HASH="$(git -C feeds/${FEED_ID} rev-list -n 1 --before=${REV_DATE} $
{REV_BRANCH})"
sed -i -e "/\s${FEED_ID}\s.*\s.git$/s/^\${REV_HASH}/" feeds.conf
done

./scripts/feeds update -a
./scripts/feeds install -a

# Configure the firmware image and the kernel
make menuconfig
```

#### Advanced configuration options (for developers)

- Target options checked
- BPF toolchain (Build LLVM toolchain for eBPF)
- Toolchain Options
  - o Binutils Version 2.39
  - o GCC Compiler Version 12.x
  - o C library musl

```
Target System (Marvell EBU Armada) --->
Subtarget (Marvell Armada 3700LP (ARM64)) --->
Target Profile (Marvell ESPRESSObin V7 Non-eMMC) --->
Target Images --->
[*] Enable experimental features by default
Global build settings --->
[*] Advanced configuration options (for developers) --->
[*] Build the OpenWrt Image Builder
[*] Include package repositories (NEW)
[*] Build the OpenWrt SDK
[*] Build the LLVM-BPF toolchain tarball
[*] Package the OpenWrt-based Toolchain
[*] Image configuration --->
Base system --->
Administration --->
Boot Loaders --->
Development --->
Extra packages --->
Firmware --->
Fonts --->
Kernel ----
Kernel modules --->
Languages --->
Libraries --->
LuCI --->
Mail --->
Multimedia --->
Network --->
Sound --->
Utilities --->
Xorg --->
```

## Target images

```
[*] ramdisk (NEW) --->
    *** Root filesystem archives ***
[ ] cpio.gz (NEW)
[*] tar.gz (NEW)
    *** Root filesystem images ***
[*] ext4 (NEW) --->
[*] squashfs (NEW) --->
[*] GZip images (NEW)
    *** Image Options ***
(16) Kernel partition size (in MiB) (NEW)
(104) Root filesystem partition size (in MiB) (NEW)
[ ] Make /var persistent (NEW)
```

## Toolchain Options

```
-- Toolchain Options
[ ] Enable an extra toolchain target architecture (NEW) ----
    *** Binary tools ***
    Binutils Version (Binutils 2.39) --->
( ) Additional binutils configure options (NEW)
[ ] Build pahole (NEW)
    *** Compiler ***
    GCC compiler Version (gcc 12.x) --->
[ ] Compile in support for the new Graphite framework in GCC 4.4+ (NEW)
( ) Additional gcc configure options (NEW)
[ ] Build executable with PIE enabled by default (NEW)
[ ] Build executable with Stack-Smashing Protection enabled by default (NEW)
[ ] Use setjump()/longjump() exceptions (NEW)
[ ] Build/install fortran compiler? (NEW)
    *** C Library ***
    C Library implementation (Use musl) --->
[*] Include crypt() support for SHA256, SHA512 and Blowfish ciphers (NEW)
    *** Debuggers ***
[ ] Build gdb
```

make -j \$(nproc) kernel\_menuconfig

## Add XDP Hook

- Networking Support -> Networking Option -> XDP Socket

```
<*> Packet socket
< > Packet: sockets monitoring interface
<*> Unix domain sockets
< > UNIX: socket monitoring interface
< > Transport Layer Security support
< > Transformation user configuration interface
< > PF_KEY sockets
[*] XDP sockets
<M> XDP sockets: monitoring interface
[*] TCP/IP networking
[*] IP: multicasting
[*] IP: advanced router
[ ] FIB TRIE statistics
[*] IP: policy routing
[*] IP: equal cost multipath
[*] IP: verbose route monitoring
[ ] IP: kernel level autoconfiguration
< > IP: tunneling
< > IP: GRE demultiplexer
[ ] IP: multicast routing
[*] IP: TCP syncookie support
< > Virtual (secure) IP: tunneling
< > IP: Foo (IP protocols) over UDP
< > IP: AH transformation
< > IP: ESP transformation
< > IP: IPComp transformation
< > INET: socket monitoring interface
[*] TCP: advanced congestion control --->
[ ] TCP: MD5 Signature Option support (RFC2385)
< > The IPv6 protocol ----
[ ] MPTCP: Multipath TCP
v(+)
```

<Select> < Exit > < Help > < Save > < Load >

```
# Build the firmware image
make -j $(nproc) defconfig download clean world
```

## Secure Channel Traffic

Our secure channel will be implemented using Wireguard VPN, creating a secure point to point connection between them and providing security to all your devices inside of your LAN.

## Configuring Wireguard on OpenWRT

<https://openwrt.org/docs/guide-user/services/vpn/wireguard/start>  
<https://www.wireguard.com/>

## Monitoring Traffic using XDP and eBPF

<https://github.com/tohojo/xdp-paper/blob/master/xdp-the-express-data-path.pdf>

### Reference Links

<https://openwrt.org/docs/guide-developer/toolchain/use-buildsystem>

#### XDP – Tutorial

<https://github.com/xdp-project/xdp-tutorial>

<https://www.tigera.io/learn/guides/ebpf/ebpf-xdp/>

#### eBPF – Kernel Observability

<https://github.com/bpftools/linux-observability-with-bpf>

#### XDP – Loader

<https://github.com/xdp-project/xdp-tools/tree/master/xdp-loader>

#### BPF – Docs

<https://github.com/iovisor/bpf-docs/blob/master/bpf-internals-2.md>

#### Cilium – XDP

<https://docs.cilium.io/en/stable/bpf/>

#### Life Packet

<https://docs.cilium.io/en/stable/concepts/ebpf/lifeofapacket/>

#### NetOptimizer

<https://github.com/netoptimizer/prototype-kernel>

#### NetDev 2.1

[https://legacy.netdevconf.info/2.1/slides/apr7/gospodarek-Netdev2.1-XDP-for-the-Rest-of-Us\\_Final.pdf](https://legacy.netdevconf.info/2.1/slides/apr7/gospodarek-Netdev2.1-XDP-for-the-Rest-of-Us_Final.pdf)

#### MocchaBin Getting Started

[https://espressobin.net/mochabin\\_wiki/tiki-index.php?page=Build+Instruction](https://espressobin.net/mochabin_wiki/tiki-index.php?page=Build+Instruction)

#### Compiling u-boot

<https://github.com/globalscaletechnologies/u-boot-marvell>

#### Documentation u-boot

<https://u-boot.readthedocs.io/en/latest/>

<https://u-boot.readthedocs.io/en/latest/develop/index.html>

#### MocchaBin – u-boot-marvell

<http://weng-blog.com/2017/03/24/ARMv8-manual-boot.html>

MocchaBin – u-boot-marvell version

U-Boot 2018.03-devel-18.12.3-gb794de0054 (Sep 05 2022 - 14:38:22 +0800)

aarch64-linux-gnu-gcc (Linaro GCC 7.3-2018.05) 7.3.1 20180425 [linaro-7.3-2018.05 revision  
d29120a424ecfbc167ef90065c0eeb7f91977701]  
GNU ld (Linaro\_Binutils-2018.05) 2.28.2.20170706

MocchaBin ATF-marvell

<https://github.com/globalscaletechnologies/atf-marvell>

<https://github.com/globalscaletechnologies/atf-marvell/blob/atf-v1.5-armada-18.12/docs/user-guide.rst>

Serial Connection – Kermit

<http://wiki.espressobin.net/tiki-index.php?page=Serial+connection+-+Linux>

x86\_64 Linux Error: gnu/stubs-32.h Missing Error and Solution

[https://www.cyberciti.biz/faq/x86\\_64-linux-error-gnustub-32h-missing-error-and-solution/](https://www.cyberciti.biz/faq/x86_64-linux-error-gnustub-32h-missing-error-and-solution/)