Review: ASUSWRT router firmware

Are you considering to get an ASUS wireless network product? This will be a fairly lengthy and in some places technical review of the many shortcomings of the ASUSRWRT firmware that might change your mind about choosing ASUS networking products.

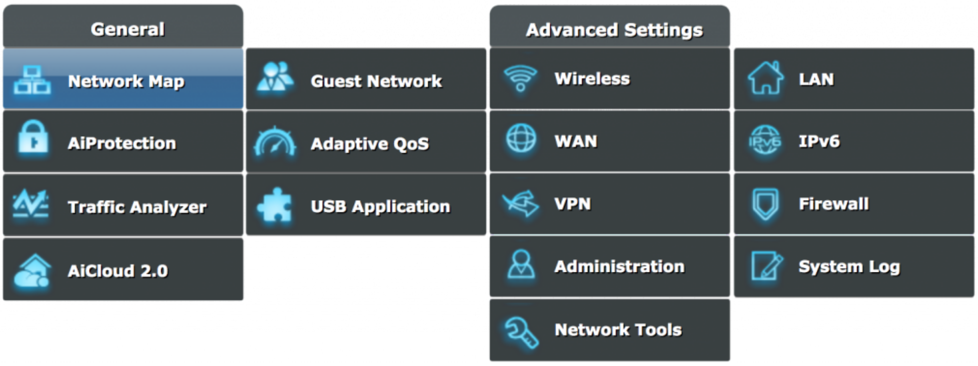
I’m not reviewing the router I used for testing, a higher-end ASUS RT-AC87U★, but rather the ASUSWRT (ASUS’ “Wireless Receiver/Transmitter”) firmware. The same firmware is used on all recent wireless network products from ASUS, but feature availability may differ from router to router. (Routers with more memory will have more features available.)

Contents

Preamble: ASUSWRT is built on a Linux kernel running a standard GNU/Linux toolset. To users, ASUSWRT appears as an app or web administration interface to a minimal Linux server. In this review, I'll focus on the front-end but will dip in to some of the underlying programs when more details are needed.

Web administration interface

The user interface looks promising at first glance! It has all the features you might want, and even seems quite easy to configure — assuming you know what you want. The first time you log into the web interface, you're guided through an "Internet Setup" followed by a "Router Setup" wizard that sets you up with a basic router configuration.



After completing the initial setup, you're bumped out to the main administrative interface and presented with a lot of options. I suspect that most customers will be done at this point, as they're already online and probably have no need for any of the other features available in ASUSWRT. However, as my router cost $200 USD, I'd really like to put the remaining features to the test.

Every section presents a tabbed interface with tons of different options in each category. Some options have hidden tooltips/help text if you hover your mouse cursor on the option, but about ⅓ of options don't. There is no way to know before you try.

The English translations are pretty shoddy in places. You might smile when you're asked to watch an "Introduce video" for an advanced feature, but you might be frustrated when you realize that "Connect to DNS Server automatically" actually means "Overwrite the below DNS server settings with DNS servers broadcast by your ISP". Likewise, if you switch between different languages – you might notice that some "dos" are translated as "don'ts" in other languages.

My favorite badly translated sentence is found on the Parental Control settings page: "Block adult content can prevent child from visiting sexy violence and illegal related content." Whatever the reason for the poor translations, it sure isn't a sign of quality.

One of my largest gripes with ASUSWRT is that **you can't copy-and-paste data to any input fields** using the keyboard. This can be frustrating when you want to copy MAC addresses to assign static IP addresses or copy-and-paste DNS settings from your ISP. You also can't undo using the good old `Ctrl+Z`. The problem here is a simple case of badly written JavaScript client validation of key events that happens too early and causes **all keyboard shortcuts to break**. Client-side validation is, as every developer should know, hard and shouldn't be relied upon to provide any data directly to a backend system without also validating it on the backend. You can force the router to accept inputs and apply settings it won't accept through the web interface by bypassing the web interface and submitting them directly to the backend.

Overall, ASUSWRT's web interface is quite capable but there are weird exceptions. I'll get into those in more details in the next couple of sections.

Local network services

Earlier this year, two years after I first purchased the RT-AC87U, a new line of text appeared in the user interface for configuring the LAN DHCP server:

> **"RT-AC87U supports up to 253 IP addresses for your local network."**

This new limitation says you can only delegate a single /24 subnet. This limitation isn't mentioned anywhere in the manual, product spec sheet, nor in marketing. It's also interesting to note that I've had the router for almost two years before this limitation was introduced retroactively.

However, there **isn't actually any such limitation!** You can configure the DHCP server to assign IPv4 addresses for an entire IPv4 class A address space (a /8 subnet) of 16,7 million addresses; and it will happily give out addresses until it runs out of memory. I've tried using 16 different subnets and have had the router delegate addresses in all subnets and had devices communicate between the subnets.

The new limitation actually refers to an old limitation that has been in ASUSWRT since at least 2015 April and isn't documented anywhere. The /24 subnet limitation only applies to the Deep Package Inspection (DPI) tool that powers features like the Network Map, Network Analyzer, Quality-of-Service, and Bandwidth Monitor. I'll cover the DPI and these features more extensively in the next two sections.

You also can't configure the router to use an IPv6-only DNS server by setting a IPv6 address as the DNS server. The backend fully supports it, but the ASUSWRT web front end will only let you type in an IPv4 address. The router is full of restrictions like this, imposed by ASUS' interface, that can limit what you can do with an otherwise capable router.

ASUSWRT has a simple Dynamic DNS client that would work with just about any DynDNS service, if ASUS hadn't decided to hard-code a list of 10 providers. If your DNS provider is not on the list, you're out of luck. In most other DynDNS clients, you'll have the option to enter a username, password, and the web address that should be notified on IP address changes. This is also how ASUSWRT's client works, but you can't manually configure the web address of the service provider.

There are other local network services on offer, including simple network attached storage from a USB disk, media streaming, and network sharing of a printer. I'll not go in to these services in any detail, but I'll look more closely at some strictly network related services in the next two sections.

Built-in OpenVPN server

ASUSWRT makes for a surprisingly good VPN server. You can think of a VPN server as a remote router you connect to over the internet. Rather than routing your traffic through the local network, you can configure your devices to encrypt all traffic and send it through your router at home.

You probably want to set up your router as a VPN and configure your smartphone and other luggable devices to connect to it while you're outside your home. You can most likely trust your ISP more than you should trust any random hotel or café free WiFi option. Having a VPN server available even if you don't normally need to use one is a good tool to have in your security toolbelt.

The OpenVPN server is enabled by flicking a switch in the web administration interface. After that, you can click 'Export' and get a .ovpn configuration profile file. You copy this file onto your devices and open it with any OpenVPN client (clients available for all major desktop and mobile operating systems), and you're done. Be sure to keep this file safe as it allows access in to your local homenet.

The router is running a recent version of OpenVPN with a conservative configuration and security policy. However, the .ovpn configuration profile sets the current external IP as the "remote" option even when a DynDNS hostname has been configured as a reliable way to reach the router. This means the profile will stop working if your ISP assigns you a new IP address. It's an easy problem for ASUS to fix, especially when they've already implemented a possible solution for it, but the VPN service doesn't appear to have been a priority.

Network management and Deep Package Inspection

ASUSWRT comes with some advanced network management and traffic shaping tools that can be surprisingly useful even in a regular household with just a couple of devices. Devices and known network services can be prioritized using the Quality-of-Service service to ensure a Chromecast or other streaming device has network priority over over devices. Time scheduling let you set which hours and days of a week a given device is allowed to connect to the internet.

There is, however, a catch in using these services. ASUSWRT will **collect and transmit data about which websites you visit** to Trend Micro, if you use any of the following features in ASUSWRT:

- Apps/traffic Analysis
- Bandwidth Monitor

- Bandwidth Monitor
- Network Analyzer
- Network Protection (AiProtection), blocks known malware domains
- Parental Controls, including time scheduling
- Quality-of-Service
- Web History

To use any of these functions, you'll be asked to agree to a long-winded End-User License Agreement (EULA) from Trend Micro. At the very bottom of the EULA, you'll find a section devoted to [the lack of] privacy. Here are some snippets from that EULA:

> "[…] certain information ("Forwarded Data") to be sent to Trend Micro-owned or -controlled servers for security scanning and other purposes as described in this paragraph. This **Forwarded Data may include information on potential security risks as well as URLs of websites visited** that the Software deem potentially fraudulent and/or executable files or content that are identified as potential malware. Forwarded Data may also include email messages identified as spam or malware that contains personally identifiable information or other sensitive data stored in files on Your router. […]"
>
> […] "Trend Micro **reserves the title, ownership and all rights and interests to any intellectual property or work** product resulting from its use and analysis of Forwarded Data."

Now this is a real bummer! Most people will not expect their router to be prying in to their network traffic! — I mean, not beyond what is needed to route the traffic to the correct destination and back again. The EULA also contains language holding the router's owner responsible for notifying their friends, family, and house guests who connect to the internet through the ASUS router that any network activity may be recorded and shared with Trend Micro. This clause is laughable and I highly doubt any friend, family member, or guest has ever been informed about this nonsense in the course of human history. **People simply don't make their friends sign waivers before connecting to their wifi or lending them their restrooms.**

Strictly speaking, you also need to agree to the EULAs when using the Network Map feature. The various device icons that can identify operating systems and some 250 known devices also uses data and [on-device] analysis from Trend Micro. The ASUSWRT firmware doesn't enforce that you agree to the EULA before you use this feature, so Trend Micro and ASUS seem to have agreed on an exception for this feature.

⁂

ASUS' license with Trend Micro makes Quality-of-Service (QoS) accessible to regular users. Configuring a QoS ruleset can be quite complicated and requires indepth knowledge of networking protocols and the services and applications you wish to handle in QoS. Early versions of ASUSWRT let users get in the thick of things and make manual adjustments to the QoS policies, and even let users create their own rules. However, this feature has been removed in later updates, leaving some 540 predefined apps and services. You can no longer manually prioritize any one service over others but are limited to sorting a list of generic categories including: Gaming, VoIP and IM, Audio/Video Streaming, Web Surfing, File Transfers, and Others. Almost every network enabled service that isn't web browsing or a game from the early 2000s will end up in the "Others" category.

Security

ASUS releases security and feature updates to ASUSWRT at random intervals. Updates are released on average every 10 weeks, but there was no update for over half a year in 2016. Customers are unlikely to be running the latest version of the firmware anyway, as there is no automated updates nor a system for notifying them of any updates.

There is no push-notification to the mobile app, email list where you can be notified, appcast (an RSS feed with updates), or any other method to be notified of updates. Users are expected to regularly visit the router's web administration interface or app and click "check for updates". The lack of any kind of update notifications is a serious problem considering that the updates regularly contain patches for remotely exploitable vulnerabilities.

ASUSWRT contains various features which are hyped as security and protection tools. The trouble is of course, that most operating systems and web browsers already provide the same functionality. (Assuming they're not using a fringe web browser without these protections.) The only slightly useful feature, powered by the Trend Micro DPI module, offers to block devices that try to communicate with known botnets.

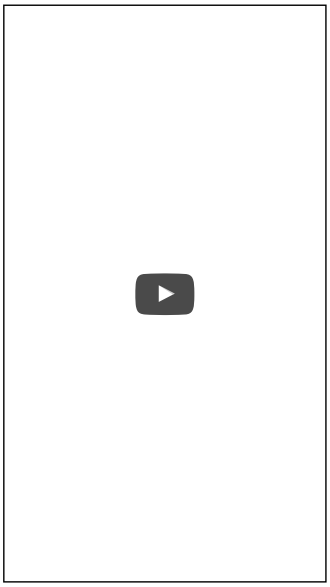
Any website blocked due to parental controls or that were believed to be malicious, or any device trying to communicate with a known botnet can be reported by email. This requires your email to be hosted with either AOL, Google Mail, Tencent QQ, or 163. Your router will act as a email to be hosted with either AOL, Google Mail, Tencent QQ, or 163. Your router will act as a standard SMTP client and use your email provider to send the notifications. This requires you to save your email password in plain-text on the router and thus exposing it to anyone exploiting one of the many known remote access vulnerabilities. This is a bigger security concern than these notification emails could ever make up for.

The number of remote access and arbitrary code execution vulnerabilities that regularly shown up in ASUSWRT's changelog is worrying. The same type of attacks is fixed in release after release. Don't get me wrong — bugs will happen! However, many of the issues ASUS have to repeatedly fix would have turned up early during a security audit. They're the kind of issues you'd see informatics students try to identify and exploit as part of a training assignment.

Speaking of security audits, there is clearly no security audits and only minimal — if any — security testing prior to release. Enabling the Telnet and SSH services would expose these to the public internet with no brute-force login protection. Neither service is enabled by default, but one really would expect that as part of release testing — ASUS would turn on every service and verify that they aren't exposed to the public internet as a bare minimum!

ASUS doesn't seem to have the routines nor the required security culture to ship a secure networking product, and that shows through in ASUSWRT.

The ASUS Router app



A fake sci-fi UI? No, its the ASUS app.

The ASUS Router app does look a bit like a fake mock-up user interface for a sci-fi movie, but it's a greatly simplified version of the web interface for Android and iOS. It appears to have been developed by a separate team at ASUS who have never logged in to the web administration interface, and instead decided on doing everything their own way.

This simplified interface is probably better for most users, but as an advanced user I find it frustrating that they have diverged so greatly in terms of naming and presentation. In the web interface, you can assign devices icons from a list of generic product icons to help identify them. These icons are not shared in the app; which instead encourages its users to take photos of each device. These photos does of course not show up in the web interface.

While the app has an option called "Wi-Fi ECO Mode" with a green "eco-looking" icon that you can toggle on and off, the web administration interface has the same setting hidden away in "Wireless: Professional: Tx power adjustment". The app has an app/feature like list of options that give access to a subset of the functionality exposed on the web administration interface.

I believe ASUS would have had a better product for everyone if they had taken some of the design and development effort sunk into the app and spent it on improving the web interface instead. Making it mobile friendly, and potentially wrapping that up as an app seems like a better way to go.

The minute before midnight

Some of ASUSWRT's many features inexplicably only work for 1439 minutes out of the day's 1440 minutes. One minute to midnight every day, the router turns off a seemingly random set of features to observe a one-minute break from user demands.

The wireless scheduler function allows users to disable WiFi for periods of the day to preserve power, or to encourage the access point's users to head home from work, leave the café table they've been occupying for hours, or maybe find their way to bed. Older firmware versions would by default enable this feature between 23:59 and 00:00 every day. In this time period, every wireless device is disconnected while wired devices continue to operate normally. The feature is still present in the most recent versions of the firmware, but is not on by default.

Another new feature that is on by default in newer firmware models is a new "Time of Day to Reboot" option which is also set to 23:59. This time is user-configurable, so customers who enjoy late night gaming or Netflix can find — if they dig through all their router's options — the option and reschedule it to some more sensible time like 04:00.

The "URL Filter" firewall ruleset — built on iptables' webstr extension; meaning it only works for uncompressed and unencrypted HTTP — inexplicably also creates time sensitive blocklist rules. The URL filters are only active between 00:00 and 23:59. This is non-configurable, and there is no documentation that indicates that the filter isn't active for one minute out of the day.

The VPN service also kicks all clients at a minute to midnight.

I'm not entirely sure what is going on with the minute before midnight. ASUS support haven't been able to give me any details about why this one-minute service stop is necessary. My best theory is that it has to do with memory usage, which consistently drops at midnight, but I can't really tell for sure what the purpose might be.

Conclusion

ASUSWRT is probably not the ideal router firmware, but it gets the job done. The web interface requires a lot of existing knowledge of how local area networking works once you go beyond the initial setup wizard. What concerns me the most is the overall lack of quality in the web interface and what is clearly a relaxed security culture at ASUS.

I **recommend that you *don't* buy any network product from ASUS**, and advise that you also stay away from any other router advertising Trend Micro security solutions. Network security doesn't seem to be a priority for ASUS, and they clearly didn't set their A-team to develop the web administration interface.

Be sure to review the terms of service and privacy policy of any router you consider purchasing. I certainly will! You can consider it a red flag if the router requires you to agree to any terms from third-party (or indeed any) online services.

Sources

- ASUSWRT 3.0.0.4.380_7378 firmware and sources
- ASUSWRT changelogs

This review is based on ASUSWRT 3.0.0.4.380_7378 released in 2017 April and provides historical comparisons against version 3.0.0.4.378.5134 released in 2015 April.

Screenshots may have been compacted for more efficient use of space, but aren't otherwise modified.

Daniel Aleksandersen
Published: 2017-05-02
Updated: 2017-05-02

Topics: Networking — Review — Security

Subscribe to the weekly newsletter!

Recommended articles

Managing Wi-Fi latency and dynamic power savings on Linux

Most of the time we want our battery powered devices to consume as little power as possible. We all get…

How to tell if your Chromecast is connected via an Ethernet adapter or Wi-Fi?

There is no easy way to identify whether your Google Chromecast is connected to your wired or wireless network when…

How-to protect SSH remote login in Fedora with SSHGuard and FirewallD

SSHGuard 2 provides a new FirewallD backend that makes it easier to work with in Linux distributions that use FirewallD…

Review: Ethernet Adapter for Google Chromecast

Why get an Ethernet adapter for what is intended to be a wireless display device? Well, like me – you…

What’s new in SSHGuard 2.0

SSHGuard is an intrusion prevention utility that parses logs and automatically blocks misbehaving IP addresses with the system firewall. It’s…

InvizBox review: Tor anonymity in a box

InvizBox is a transparent proxy in a compact device that sends all your network traffic into the Tor anonymizing network…

Leave a Reply

Your email address will not be published. Be courteous and on-topic. Comments are moderated prior to publication.

Comment:

Name *:

Email *:

Website:

□ Sign me up for the weekly email newsletter!

Post Comment

Get weekly updates

your@email.com | Subscribe | Join **2 210+** readers!

Sign-up now and get Ctrl.blog delivered in your inbox weekly!

I’m Feeling Lucky