Independent Tests of
Anti-Virus Software

IoT Router Test 2024

Commissioned by Bitdefender

TEST PERIOD: AUGUST 2024

LAST REVISION: 6TH NOVEMBER 2024

WWW.AV-COMPARATIVES.ORG

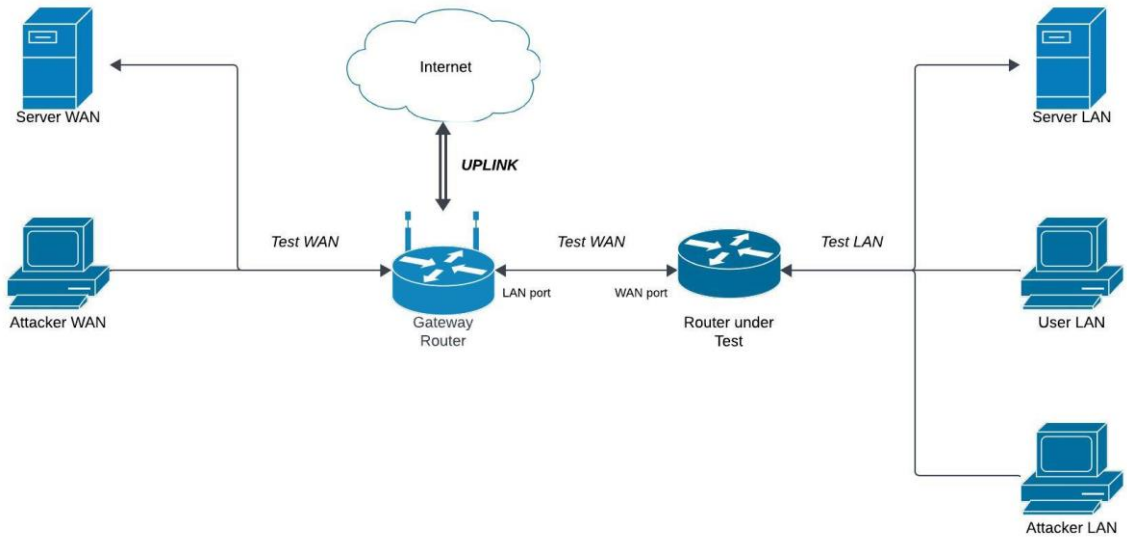
Contents

Introduction

On behalf of Bitdefender, four selected routers were tested for their security and protection capabilities. This evaluation involved penetration tests across various attack scenarios, along with detection tests. While Bitdefender proposed some of the potential attack scenarios, the testing lab independently developed the detailed test procedure and determined which scenarios were included. Additionally, we conducted basic router security checks to assess the level of protection provided right after the initial setup.

It is important to note that not all security and protection features may be activated by default during setup. Prospective buyers should carefully verify which protection features are freely included and which require a paid subscription. Moreover, some subscription-based features may be unavailable in certain countries, even if the device itself is sold there.

Test Setup



The router to be tested (*Router under Test*) is placed within the lab network as depicted in the figure above. Its WAN port is connected to the LAN port of the *Gateway Router*, which serves as the gateway to the Internet and as a local DNS server. We set up virtual machines representing both an attacker (*Attacker LAN*, *Attacker WAN*) and a server (*Server LAN*, *Server WAN*) on both the LAN and WAN sides. The server, running Debian, exposes several vulnerable services (e.g., HTTP, FTP, SSH) that can be targeted and exploited by the attacker from the opposite network. The attacker's virtual machine runs Kali Linux and is equipped with various open-source network utilities and penetration testing tools/frameworks. The *User LAN* virtual machine, with Windows 10 installed, is used to browse the test URLs and manage the router from the LAN for further administration.

Test Procedure

For this evaluation, we conducted a series of tests focusing on the following key aspects:

- **Malicious URL Protection**: Testing the ability to block both HTTP and HTTPS URLs using a variety of fresh malicious websites.
- **Brute-force Protection**: Assessing the effectiveness of mechanisms that recognise the exploitation of weak or default credentials and detect repeated failed login attempts.
- **Denial-of-Service (DoS) Protection**: Evaluating whether the router can prevent DoS attacks targeting the router or network services.
- **Sensitive Data Protection:** Testing the ability to prevent the transmission of sensitive data, such as usernames, passwords, or credit card numbers, in plain text over unsecured HTTP connections.
- **Command Injection Protection**: Checking for the router's capability to detect or prevent attempts to execute commands via URLs.
- **Exploit Protection**: Evaluating the ability to detect or prevent the exploitation of vulnerabilities in network devices or services.

In addition to the above, we also created a checklist to assess basic security features of the routers, including checks for open ports, known vulnerabilities, default passwords, password policy, and remote access settings.

The testing lab exercises discretion over the specific number and complexity of the subtests while ensuring they are indicative and relevant for the evaluation. This approach maintains both the reliability and representativeness of the results in assessing the product's protection capabilities.

Tested Products

Bitdefender selected and purchased the following routers, along with the required subscriptions. Below, we list the firmware version available at the beginning of the test (August 2024).

Vendor	Product	Firmware	Antivirus Engine
ASUS	RT-BE96U	3.0.0.6.102_34488	ASUS AiProtection by Trend Micro
eero	Max 7	7.5.0-2654	eero Plus by OpenDNS
NETGEAR	Orbi RBR860B	7.2.6.31_5.0.24	NETGEAR Armor by Bitdefender
TP-Link	Deco BE9300	1.0.8 Build 20240723 Rel. 26458	TP-Link HomeShield by Avira

Product Settings

The product was set up according to the instructions provided in the respective router app, which was downloaded from the app store. We configured the settings and features as recommended by the app during the initial setup. Products for which we altered default settings to test specific protection features are listed below. Additionally, port forwarding rules were created to expose LAN services to the WAN, making them vulnerable to attacks for the penetration tests.

ASUS

We enabled “AiProtection” with all related options, “DoS protection” under “Firewall”, and “Safe Browsing” for the device that browsed the test URLs.

eero

Since eero Plus was not available in our country during the testing period, we activated the subscription by connecting the eero device to an additional router linked to a VPN server in the US. This setup made the eero device appear as if it were located in the US. After activation, we enabled all available eero Plus security features (“Advanced Security” and “Ad Blocking”).

NETGEAR

The product was tested with its default settings.

TP-Link

We enabled all options for “Security+” (“Web Protection”, “Intrusion Protection”, “IoT Protection”).

Test Results

In this section, we present the results of each test in tables. The symbols below indicate whether the product passed or failed the test and whether the attack was detected or not. A short discussion about notable findings can be found in *Summary*.

✔ Test passed / Attack detected

✘ Test failed / Attack not detected

Penetration Tests

The table below outlines several attacks against devices and services located in the test LAN and WAN.

	ASUS AiProtection	eero Plus	NETGEAR Armor powered by Bitdefender	TP-Link HomeShield
Brute-force Attack				
Brute-force credentials LAN-WAN	✔	✘	✔	✔
Brute-force credentials WAN-LAN	✔	✘	✔	✔
Denial-of-Service (DoS) Attack				
ICMP flood LAN-WAN	✘	✘	✔	✘
ICMP flood WAN-Router	✔	✘	✔	✔
TCP SYN flood LAN-WAN	✘	✘	✔	✘
TCP SYN flood WAN-LAN	✔	✘	✔	✔
UDP flood WAN-LAN	✔	✘	✔	✘
Sensitive Data Attack				
Data transmission via unsecured HTTP connections	✘	✘	✔	✘
Command Injection Attack				
Command injection LAN-WAN	✔	✘	✘	✘
Command injection WAN-LAN	✔	✘	✔	✔
Exploit Attack				
Botnet behaviour LAN-WAN	✔	✘	✔	✘
FTP vulnerability WAN-LAN	✔	✘	✘	✔
HTTP vulnerability WAN-LAN	✔	✘	✔	✔
Path traversal WAN-LAN	✔	✘	✔	✔
XSS vulnerability LAN-Router	✔	n/a	✔	n/a

Router Security Features

The table below outlines basic security checks conducted during or immediately after the initial router setup. The results reflect the router's default configuration post-setup.

	ASUS RT-BE96U	eero Max 7	NETGEAR Orbi RBR860B	TP-Link Deco BE9300
Open ports on LAN	53, 80, 8083, 49152	53, 1900, 3001	53, 80, 443, 5000	53, 80, 443, 1900
Open ports on WAN	None	None	None	None
Detects port scans	✗	✗	✗	✓
Uses secure Wi-Fi protocol by default	WPA2/WPA3-Personal	WPA2	WPA2	WPA2/WPA3-Personal
Prompts to change default router credentials	✓	✓	✓	✓
Prompts to change default Wi-Fi passwords	✓	✓	✓	✓
Shows password strength/restrictions	✓	✓	✓	✓
Enforces password policy (e.g., length, characters)	✗	✗	✓	✗
HNAP disabled on LAN/WAN	✓	✓	✓	✓
Remote access from WAN disabled by default	✓	✓	✓	✓
Ping from WAN disabled by default	✓	✗	✓	✓
No router vulnerabilities	✓	✓	✓	✓
Identifies vulnerable LAN devices	✗	✗	✓	✗
Anomaly detection feature	✗	✗	✓	✗

Detection Tests

The test results for the detection tests can be found in the table below. All routers offer protection against malicious websites. A detection means that either the website or connection to it is blocked. We defined the results in ranges[1].

Malicious Websites	ASUS AiProtection	eero Plus	NETGEAR Armor powered by Bitdefender	TP-Link HomeShield
Detection rate	Low	Low	Medium	Low

It appears that eero solely detects and blocks malicious websites actively browsed by the user, rather than preventing network-level attacks (see *Penetration Tests*). Additionally, eero's in-app *Activity Center* only displays the total count of certain metrics, such as scanned websites or blocked threats/ads, without providing detailed information.

[1] 0-30%: Very low, 31-60%: Low, 61-80%: Medium, 81-90%: High, 91-100%: Very high

Summary

	ASUS RT-BE96U	eero Max 7	NETGEAR Orbi RBR860B	TP-Link Deco BE9300
Penetration Tests	12/15 (80%)	0/14 (0%)	13/15 (87%)	8/14 (57%)
Router Security Features[2]	7/11 (64%)	6/11 (55%)	10/11 (91%)	8/11 (73%)

Penetration Tests

It was found that nearly all routers effectively block brute-force attacks. NETGEAR Armor powered by Bitdefender stood out for their ability to prevent the transmission of sensitive data over unsecured HTTP connections. Attacks originating from the WAN were blocked more effectively than those from the LAN; however, none of the routers managed to detect or prevent the "UDP flood LAN-WAN" or "FTP vulnerability LAN-WAN" test cases. Notably, NETGEAR Armor powered by Bitdefender was able to prevent an attack by blocking the originating IP address, whereas other routers only detected the attack and displayed in-app notifications without blocking the attacking IP. Testing for "XSS vulnerability" on eero and TP-Link was not feasible as eero lacks a web console and TP-Link's web console does not allow for necessary changes. Overall, eero failed to block any of the common network attacks tested, indicating a significant lack of attack protection mechanisms.

Router Security Features

No unusual ports are open on either the LAN or WAN. On the LAN side, essential ports for DNS (53), HTTP (80), and possibly HTTPS (443) are open by default to ensure proper router functionality and Internet access. All routers have UPnP activated by default, which exposes certain LAN ports (e.g., 1900, 5000, 49152). The remaining open ports are typically used for proprietary router services. Notably, TP-Link detected the port scans during testing and flagged them as potential attacks. By default, all routers employ secure Wi-Fi protocols, prompt users to change the default login credentials for both the router and Wi-Fi networks, have HNAP disabled, and prevent remote WAN access. While all routers visually indicate password strength/restrictions, only NETGEAR enforces setting a strong password; others allow weak passwords (e.g., "password"). Nearly all routers have the "Ping from WAN" feature disabled, protecting against ICMP flood attacks from the WAN. None of the routers, with the respective firmware versions tested, were found to have serious vulnerabilities. NETGEAR distinguishes itself by automatically detecting and alerting users to vulnerable devices on the LAN.

Detection Tests

eero, NETGEAR, and TP-Link offer an endpoint protection solution (EPP) depending on the subscription plan. NETGEAR Armor powered by Bitdefender covers up to 50 devices for different platforms and is powered by Bitdefender. An EPP enhances malware protection through features like behavioural detection[3]. NETGEAR Armor powered by Bitdefender ranks higher in detecting malicious websites among the tested routers, though there is still room to enhance its overall protection capabilities.

[2] Based on the selected/tested features on the previous page.
[3] https://www.av-comparatives.org/tests/malware-protection-test-september-2024/

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(November 2024)