#225151

October 2025

Commissioned by
Zyxel Networks

Zyxel USG FLEX 100H vs. SonicWall TZ270

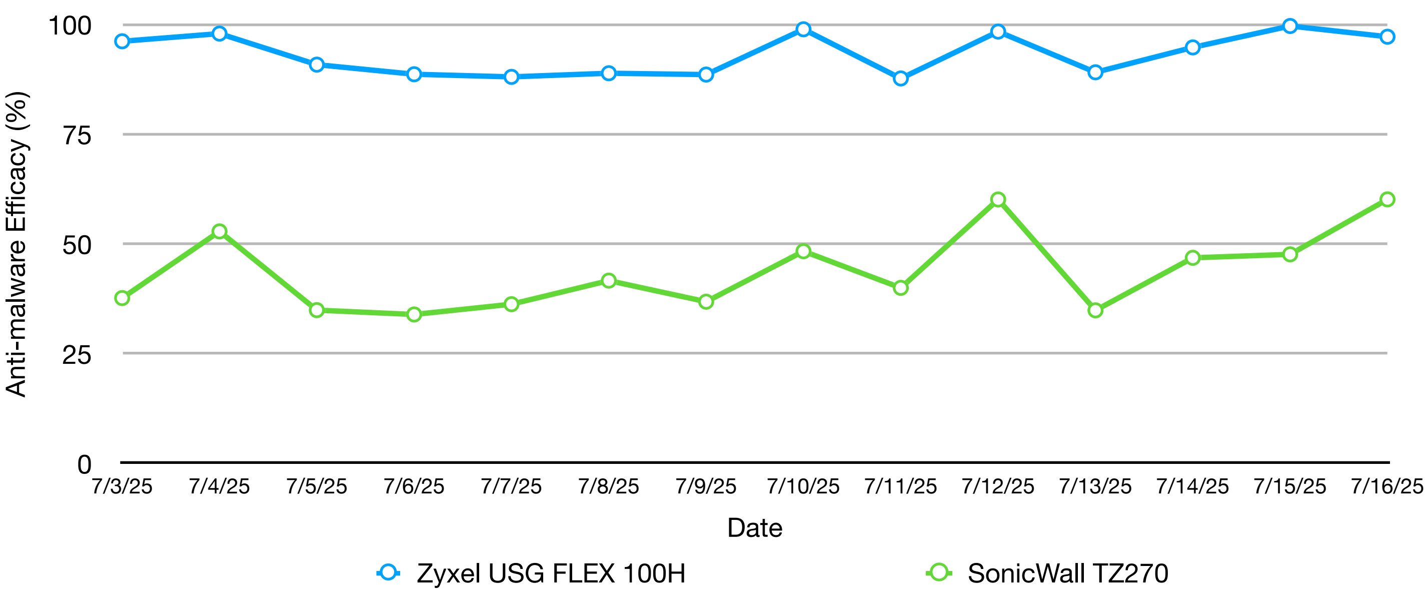
Firewall Anti-malware Efficacy and Subscription License Evaluation

Executive Summary

Ongoing security subscriptions for firewall devices are essential because threats evolve constantly, and outdated protection leaves networks exposed. Subscriptions ensure devices receive the latest threat intelligence, malware signatures, and policy updates, keeping defenses effective against new attacks.

Tolly evaluated the Zyxel USG FLEX 100H firewall with the Gold Security UTM Bundle license and the SonicWall TZ270 with the Advanced Protection Security Suite license in terms of anti-malware efficacy, URL filtering efficacy, prices, and other key features. Zyxel USG FLEX 100H provided higher anti-malware and URL filtering efficacy with a lower subscription price. It also includes cloud management with the Gold Security UTM Bundle license and free lifetime firmware upgrades.

Anti-malware Efficacy (Detection and Blocking Rate) Results



Note: Please see Table 1 for detailed results.

Source: Tolly, September 2025

Figure 1

Report link: https://www.tolly.com/publications/225151

Test Results

Anti-malware Efficacy

The test was conducted using the topology shown in Figure 3 on Page 5. Malware samples used in the test were stored on a web server. On the test client, malware samples were downloaded from the web server via HTTP GET. The number of malware downloads successfully blocked by the DUT (Device Under Test) was determined by checking the log information of the DUT and by verifying whether the files in the destination folder matched the original files. Based on this, the anti-malware efficacy (detection and blocking rate) was calculated.

As shown in Figure 1 on page 1, the anti-malware efficacy of the Zyxel USG FLEX 100H was higher than 87% on each date, with an average of 91.8%. The SonicWall TZ270 had an average anti-malware efficacy of 41.8%. The anti-malware efficacy of the Zyxel USG FLEX 100H was significantly higher than that of the SonicWall TZ270 in the test.

Anti-malware Efficacy (Detection and Blocking Rate) Detailed Results

Date	Number of blocked malware samples		Number of malware samples tested
	Zyxel USG FLEX 100H	SonicWALL TZ270	
7/3/25	227	89	236
7/4/25	237	128	242
7/5/25	577	222	635
7/6/25	556	213	627
7/7/25	473	195	537
7/8/25	529	248	595
7/9/25	591	246	667
7/10/25	274	134	277
7/11/25	493	225	562
7/12/25	368	225	374
7/13/25	508	199	570
7/14/25	455	225	480
7/15/25	299	143	300
7/16/25	315	195	324
Total	5,902	2,687	6,426

Notes: Malware samples are collected from MalShare, URLhaus and MalwareBazaar. The samples are filtered using VirusTotal. If five or more security vendors classify a sample as malware, it will be included in the test. The test includes 6,426 total malware samples.

Source: Tolly, September 2025

Table 1

Malicious URL Detection Rate

The test was conducted using the topology shown in Figure 3 on Page 5. On the test client, engineers used a script to run HTTP queries to each URL in the list. The number of malicious URLs successfully blocked by the DUT (Device Under Test) was determined by checking the DUT log information and by verifying whether HTTP queries failed. Based on this, the malicious URL detection rate was calculated.

As shown in Figure 2, the malicious URL detection rate of the Zyxel USG FLEX 100H was higher than 74% on each date, with an average of 84.8%. The SonicWall TZ270 had an average malicious URL detection rate of 27.1%. The malicious URL detection rate of the Zyxel USG FLEX 100H was significantly higher than that of the SonicWall TZ270 in the test. See Table 2 for detailed results.

Malicious Domain/URL Detection Rate Detailed Results

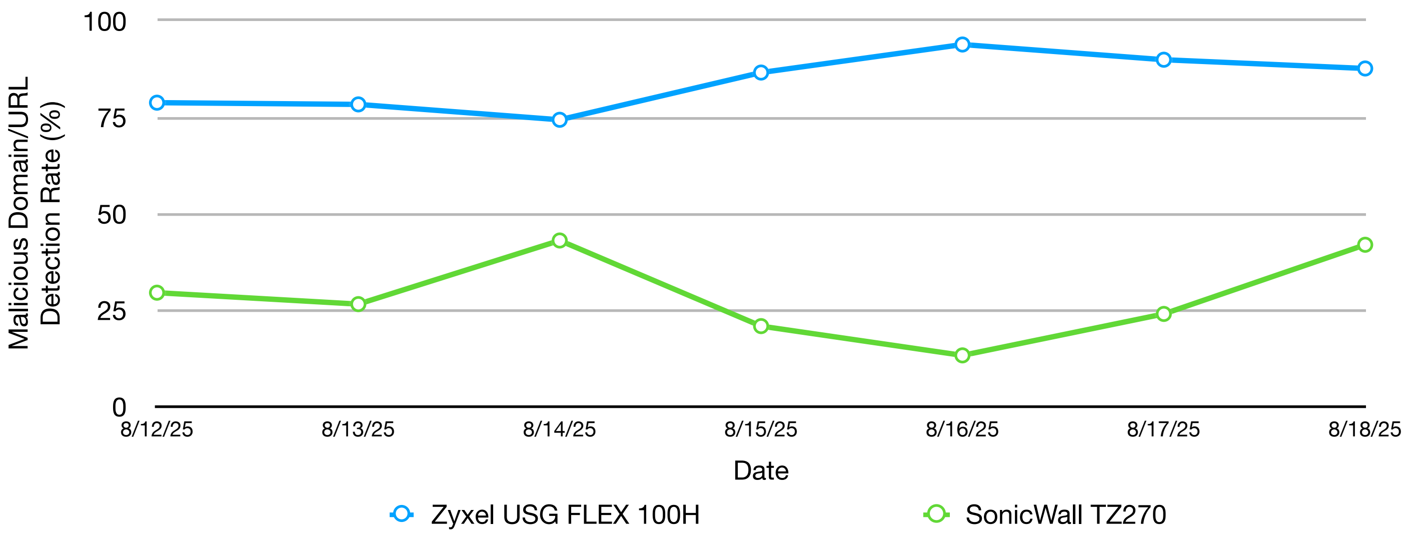
Date	Number of blocked malicious URLs		Number of malicious URLs tested
	Zyxel USG FLEX 100H	SonicWALL TZ270	
8/12/25	267	100	339
8/13/25	242	82	309
8/14/25	304	176	409
8/15/25	374	90	432
8/16/25	503	71	536
8/17/25	356	95	396
8/18/25	255	122	291
Total	2,301	736	2,712

Notes: URL samples are collected from OpenPhish, URLhaus and PhishTank. The samples are filtered using VirusTotal. If five or more security vendors classify a sample as malicious URL, it will be included in the test. The test includes 2,712 total malicious URL samples.

Source: Tolly, September 2025

Table 2

Malicious Domain/URL Detection Rate Results



Note: Please see Table 2 for detailed results.

Source: Tolly, September 2025

Figure 2

Firewall License Renewal Price and Feature Evaluation

	Zyxel USG FLEX 100H		SonicWall TZ270	
	1Y Gold Security UTM Bundle License Renewal	**2Y Gold Security UTM Bundle License Renewal**	**1Y Advanced Protection Security Suite License Renewal**	**2Y Advanced Protection Security Suite License Renewal**
STREET PRICE (US)	$224.99	$399.99	$383	$651
FEATURES				
Sandboxing	✓	✓	✓	✓
Gateway AV	✓	✓	✓	✓
Anti-Spyware	✓	✓	✓	✓
Intrusion Detection	✓	✓	✓	✓
Application Firewall	✓	✓	✓	✓
Content Filtering	✓	✓	✓	✓
Anti-Spam	✓	✓	✓	✓
DNS Filtering	✓	✓	✓	✓
IP Reputation Filtering	powered by Webroot, not just for Email but for other types of services (to detect/block botnet command and control as well as malicious website IPs)		For Email Anti-spam	For Email Anti-spam
Tech Support	Free[1]	Free	Requires separate support contract	Requires separate support contract
Firmware Upgrades	Free Lifetime	Free Lifetime		
Warranty	Free Limited Lifetime	Free Limited Lifetime		
Alerting/Logging	365-Day Alert/Logging / SecuReporter Advanced Reporting & Analytics	365-Day Alert/Logging / SecuReporter Advanced Reporting & Analytics	7-Day Alert / Advanced Reporting & Analytics	7-Day Alert / Advanced Reporting & Analytics
Cloud Management	✓ include 1Y Nebula Pro	✓ include 2Y Nebula Pro	✗ (need additional license)	✗ (need additional license)

Notes: 1. Free means it does not require any license on the appliance. 2. Zyxel's street price is provided by Zyxel in September 2025. SonicWall price is from SonicGuard (sonicguard.com) which is an authorized online reseller in September 2025. The price is subject to change.

Source: Tolly, September 2025

Table 3

License Renewal (Price and Features)

Tolly engineers used publicly available information to compare the license renewal pricing and included security features of the Zyxel USG FLEX 100H and the SonicWall TZ270. The Zyxel USG FLEX 100H demonstrated a significant cost advantage, with renewal prices 58% lower for a one-year license and 61% lower for a two-year license.

Both devices provide a comprehensive set of security features and services; however, the Zyxel USG FLEX 100H additionally supports IP reputation filtering for Email and other types of services (to detect/block botnet command and control as well as malicious website IPs), whereas the SonicWall TZ270 limits IP reputation functionality to Email anti-spam protection. Also, customers need to purchase additional license for SonicWall TZ270 on support and cloud management while these features are either free or included in Zyxel's Gold Security UTM Bundle license. Detailed results are presented in Table 3 on Page 4.

Test Methodology

Zyxel USG FLEX 100H

The Zyxel USG FLEX 100H running VuOS-fw 2025-08-14 was tested with the Gold UTM License pack applied. The anti-malware feature was enabled with all available file types selected. The DNS threat filter was configured to include all security threat categories, with the action set to "redirect." Content filtering was also enabled, with actions configured to "block" for both the P2P File Sharing and Potentially Unwanted Programs (PUPs) managed categories.

SonicWall TZ270

The SonicWall TZ270 was tested with SonicOS 7.2.0-7015. During testing, the gateway anti-virus and cloud-based anti-virus database were enabled, with signatures updated on August 29, 2025. The content filtering service was activated, and DNS filtering was configured to return a forged IPv4 address for blocked queries. Within the DNS filtering profile, all categories were set to "forged IP reply." In the content filtering profile (CFP) object, nine categories—including Keyloggers and Monitoring, Malware, Phishing and Other Frauds, Proxy Avoidance, Spyware and Adware, Bot Nets, SPAM URLs, and Open HTTP Proxies—were set to "Block."

Efficacy Calculation

Anti-malware

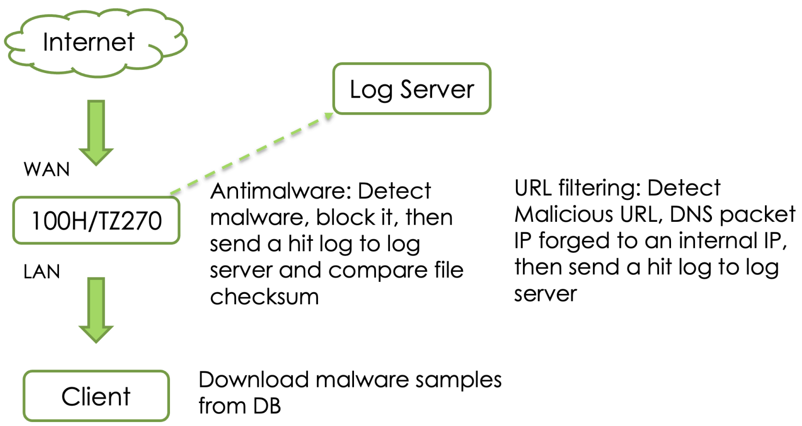
When a file is detected as malware, the two firewall products block the malware portion of the file, resulting in a partial download. Engineers compared the checksum of the files in the destination folder with the original files to determine how many malware samples were fully downloaded (not blocked by the firewall product), and how many malware samples were partially or not downloaded (blocked by the firewall product). Anti-malware efficacy = (number of malware samples blocked by the firewall product) / (total number of malware samples) * 100%.

Malicious URL Detection

For the URL filtering test, the test client was configured to use the device under test (DUT) as its DNS server.

As several malicious URLs in the test list were no longer active, engineers relied on the Device Under Test (DUT) log records to determine the number of URLs detected and blocked. DNS filtering on both DUTs was configured to return a forged IPv4 address, and the test script tracked the number of HTTP requests that failed as a result of DNS redirection. The results demonstrated that both DUTs successfully blocked the majority of malicious URLs through DNS filtering, while a smaller subset was mitigated by additional security mechanisms on the DUT. The outcomes recorded by the test script were consistent with the DUT log data.

Test Bed Topology


Internet
Log Server
WAN
100H/TZ270
LAN
Client
Antimalware: Detect malware, block it, then send a hit log to log server and compare file checksum
URL filtering: Detect Malicious URL, DNS packet IP forged to an internal IP, then send a hit log to log server
Download malware samples from DB

Source: Tolly, September 2025

Figure 3

About Tolly

The Tolly Group companies have been delivering world-class ICT services for over 35 years. Tolly is a leading global provider of third-party validation services for vendors of ICT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

225151 ajqpij2-yx-20251003-VerC