TEST REPORT

Tolly.

#225150

October 2025

Commissioned by

Zyxel Networks

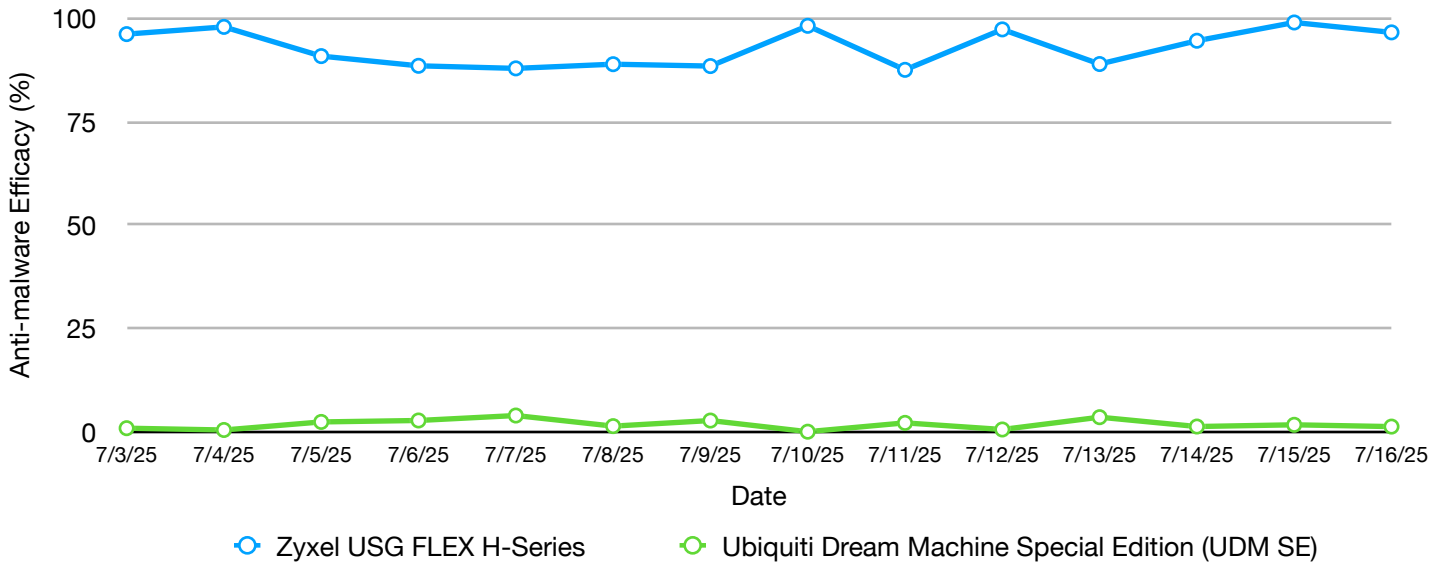
Zyxel USG FLEX H-Series vs. Ubiquiti Dream Machine

Firewall/gateway Anti-malware Efficacy Evaluation

Executive Summary

In today's evolving threat landscape, integrating anti-malware capabilities into a firewall device is essential to protect against data theft, ransomware, downtime, and business risk. While traditional SPI and IPS/IDP firewalls block unauthorized access, more advanced cybersecurity firewalls with Unified Threat Management (UTM) use embedded anti-malware capabilities to detect and stop malicious files, ransomware, and advanced threats before they spread across the network. This not only prevents sensitive data from being stolen or corrupted but also reduces costly downtime from infections and ensures critical business systems remain operational. By combining access control and malware protection in a single device, organizations gain a stronger, more efficient defense against today's most damaging cyber risks.

Tolly evaluated Zyxel USG FLEX H-Series firewall with a UTM license and Ubiquiti Dream Machine's anti-malware efficacy. The anti-malware efficacy of the Zyxel USG FLEX H-Series was significantly higher than that of the Ubiquiti Dream Machine (UDM) in the test.



Note: Two Zyxel models were tested, the USG FLEX 100H and the USG FLEX 500H. Results were almost identical. Please see Table 1 for detailed results.

Source: Tolly, September 2025

Figure 1

Report link: https://www.tolly.com/publications/225150

Test Results

Anti-malware Efficacy

Two Zyxel USG FLEX H-Series models - 500H and 100H, and one Ubiquiti UDM model - Ubiquiti UDM SE were tested. The test was conducted using the topology shown in Figure 2 on the next page. Malware samples used in the test were stored on a server. On the test client, malware samples were downloaded from the server via HTTP GET. The number of blocked samples by the DUT (Device Under Test) was determined by checking the DUT log information 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 H-Series was higher than 87% on each date, with an average of 91.6%. The Ubiquiti Dream Machine Special Edition (UDM SE) had an average anti-malware efficacy of 2%. The anti-malware efficacy of the Zyxel USG FLEX H-Series was significantly higher than that of the UDM SE in the test. See Table 1 for detailed results.

Features

Zyxel USG FLEX H-Series appliances are Unified Threat Management (UTM) firewall devices with multiple security features and services combined into a single device. The UTM license enables antivirus/anti-malware, sandboxing, intrusion detection, application control, content filtering, anti-spam and more features.

The Ubiquiti Dream Machine (UDM) does not provide a complete UTM suite. For example, it does not provide security services like sandboxing or spam filtering.

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

Sample Date	Number of blocked malware samples			Number of malware samples tested
	Zyxel USG FLEX 500H	Zyxel USG FLEX 100H	Ubiquiti UDM SE	
7/3/25	227	227	2	236
7/4/25	237	237	1	242
7/5/25	577	577	15	635
7/6/25	555	556	17	627
7/7/25	472	473	21	537
7/8/25	529	529	8	595
7/9/25	590	591	18	667
7/10/25	272	274	0	277
7/11/25	492	493	12	562
7/12/25	364	368	2	374
7/13/25	507	508	20	570
7/14/25	454	455	6	480
7/15/25	297	299	5	300
7/16/25	313	315	4	324
Total	5,886	5,902	131	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.

Source: Tolly, September 2025 Table 1

Test Methodology

Zyxel USG FLEX H-Series

The Zyxel USG FLEX 500H with VuOS-fw 2025-0806 and the Zyxel USG FLEX 100H with VuOS-fw 2025-08-14 were tested. The Gold UTM License pack was applied, and anti-malware feature was enabled with all available file types.

UDM SE

Ubiquiti Dream Machine Special Edition (UniFi OS UDM SE 4.3.6) was used in the test. The CyberSecure by Proofpoint and Cloudflare feature was active. The Intrusion Prevention feature was on. Signature update was on the test date in September 2025. The detection mode was set to Notify and Block. All active detections categories were enabled other than ICMP. There was no ICMP test traffic.

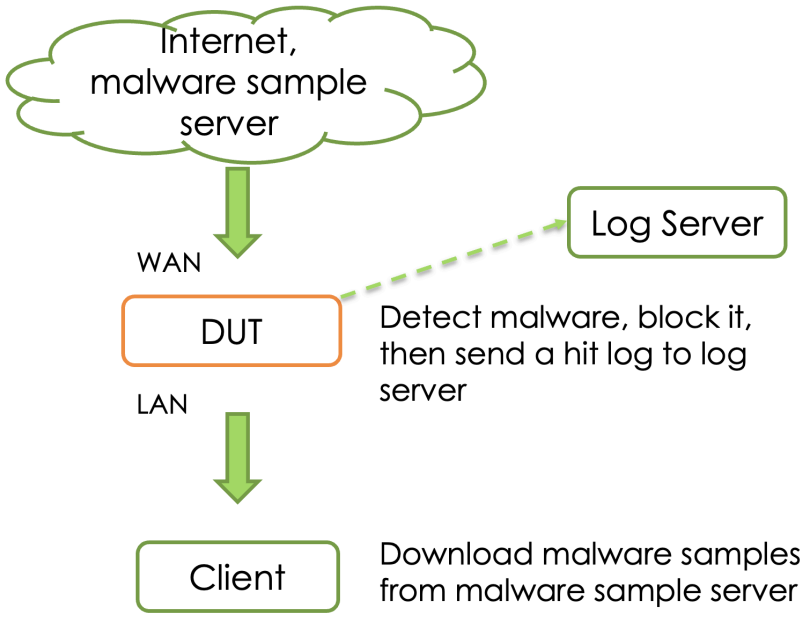
After detecting malware, the UDM SE blocks downloads from the same source for a period of time. Once the download of a malware sample is blocked, the test script pauses for five minutes before continuing to download the next sample.

Anti-malware Efficacy Calculation

When a file is detected as malware, some firewall products completely block the download of the file, while others block only 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%.

Anti-malware Efficacy Test Bed Topology



Source: Tolly, September 2025

Figure 2

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.

225150 ajqpij2-yx-20251003-VerC