



# ShareTech UTM Solution

Website  
[www.sharetech.com.tw/en-us](http://www.sharetech.com.tw/en-us)

Sales Info  
[sales@sharetech.com.tw](mailto:sales@sharetech.com.tw)

Tech Support  
[help@sharetech.com.tw](mailto:help@sharetech.com.tw)



## UTM and Antivirus Enhance Network Security

### Differences Between Firewalls and Antivirus

As cyberattacks evolve in complexity, from traditional viruses to modern threats like ransomware, APTs, phishing emails, and supply chain attacks, single-layer protection is no longer sufficient. Modern cybersecurity strategies emphasize multi-layered defense. To effectively reduce the attack surface, organizations should implement antivirus technologies at both the endpoint and UTM levels.

Both firewalls and antivirus are cybersecurity defense measures, but they differ in design objectives and deployment layers. Firewalls are primarily used to control and block network traffic at the perimeter, while antivirus software focuses on scanning and isolating threats within files and applications on endpoint devices.

### Differences

Feature	Antivirus Engine on PC	UTM Antivirus Engine
Protection Scope	Primarily protects individual devices, scans files, blocks malware.	Provides protection at the network layer, capable of filtering network traffic, blocking malicious websites, and scanning emails.
Detection Method	Antivirus software typically relies on local endpoint scanning.	Intercepts viruses at the network layer to reduce malware infiltration.



#### Endpoint Protection

Install antivirus on each device for dedicated protection.



#### Gateway Protection

Intercept viruses and malicious websites at the network layer.



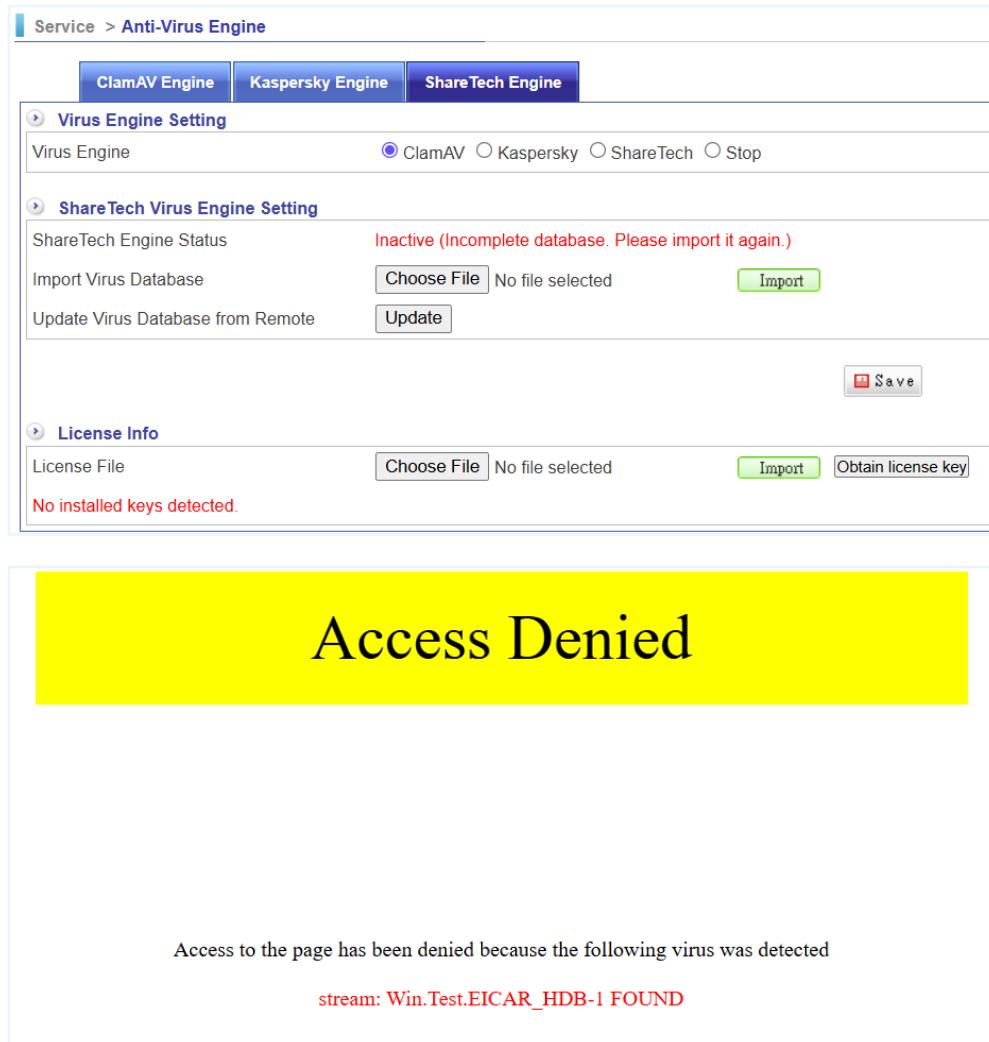
#### Remote Work Protection

VPN encrypts users' internet traffic to enhance privacy.

## Network Risks

Although Mac systems are less frequently targeted compared to Windows or Android, the belief that “Macs don’t get viruses” is a common misconception. As macOS becomes more widely adopted, malware and exploits targeting Mac devices are steadily increasing. That’s why macOS and iOS devices still need to be included in an organization’s cybersecurity strategy. Employees should maintain basic security awareness in their daily operations and internet usage.

Many types of malwares are hidden within seemingly normal websites. Once a user clicks, these threats can infiltrate the device through the browser, degrade system performance, and even cause more serious damage.



The screenshot shows a web-based interface for managing virus engines. At the top, there are three tabs: ClamAV Engine, Kaspersky Engine, and ShareTech Engine. The ShareTech Engine tab is selected. Below the tabs, there are two main sections: 'Virus Engine Setting' and 'ShareTech Virus Engine Setting'. In the 'Virus Engine Setting' section, there is a radio button group for 'Virus Engine' with 'ClamAV' selected. In the 'ShareTech Virus Engine Setting' section, the 'ShareTech Engine Status' is listed as 'Inactive (Incomplete database. Please import it again.)'. There are buttons for 'Import Virus Database' (Choose File, Import), 'Update Virus Database from Remote' (Update), and a 'Save' button. In the 'License Info' section, there is a 'License File' input field with a 'Choose File' button, an 'Import' button, and an 'Obtain license key' button. A message 'No installed keys detected.' is displayed. Below the interface, a large yellow box contains the text 'Access Denied'. Underneath this box, a message states 'Access to the page has been denied because the following virus was detected' and 'stream: Win.Test.EICAR\_HDB-1 FOUND'.

## Enterprise Cybersecurity Defense Mechanisms

Given the above, enterprises should not only install antivirus software on individual computers to enhance endpoint protection but also consider deploying UTM devices equipped with antivirus capabilities. These can provide the first layer of defense by filtering web traffic and isolating malicious content, effectively blocking internet-based threats. This creates a more comprehensive defense-in-depth strategy that combines vertical protection with lateral threat blocking.

To reduce the performance impact of HTTP/HTTPS antivirus scanning, ShareTech Antivirus uses an optimized proxy engine that bypasses unnecessary scanning of HTTP streaming traffic. It only inspects packets that are potentially virus-infected, rather than scanning all traffic on port 80.

In scenarios where servers are running outdated systems that cannot support antivirus software, enterprises can consider deploying ShareTech INF-series internal firewalls in front of the servers to enhance protection.

### Email Protection Example:

- Antivirus software scans email files stored on endpoints, such as .eml, .msg, or .oft formats.
- If emails are processed through a UTM, it will automatically scan attachments for viruses, preventing malicious content from entering the corporate network.

