Dedicated Firewall HiGuard VI / XI

X86 Dual-Core Memory-Optimized Storage
4 Gigabit Ethernet Ports, 4G RAM, and 32G Storage
NAT reaches 1.9 Gbps

ShareTech HiGuard Series offers an all-around security appliance best suited to deployments in retail stores, branch offices, and smaller business environments. 4 Gigabit ports provide Gigabit Ethernet connectivity for users under 50. The desktop security solution has high-reliability storage and memory space to maximize performance, supports USB 3.2 ports, and provides 3G/4G LTE USB as a WAN fail-over backup. Based on the zero trust principles, the software system is designed to prevent data breaches.

The HiGuard Series — The supreme security package

The desktop solution provides substantial benefits that allow businesses to reduce IT costs, deploy faster, and save physical space. A rich set of security services can deliver protection to the smallest unit.

Firewall

Built-in SPI provides DoS detection and prevention against DoS attacks such as SYN flood, ICMP flood, and UDP flood. ShareTech applies the concepts of reasonable traffic packets and connections. If the number of data packets exceeds the threshold, the firewall will selectively block data packets to avoid influencing user service experience.
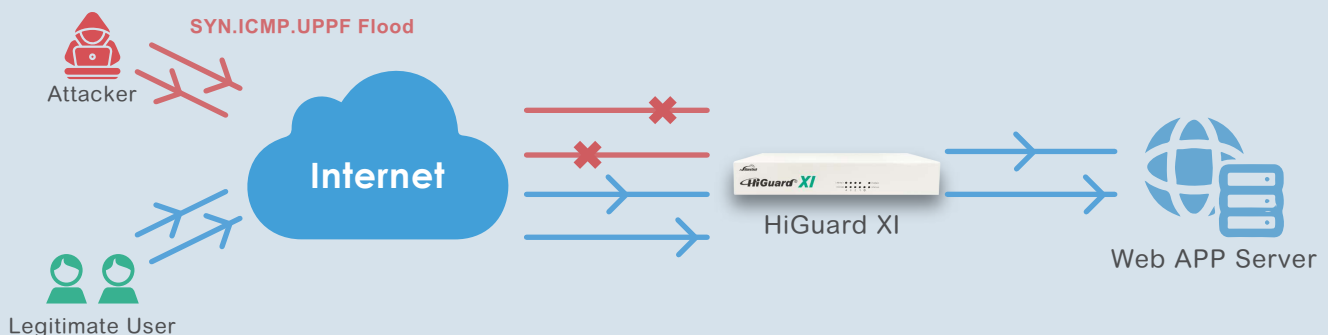

QoS

All the servers and users can be configured with their minimum and maximum bandwidth; the remaining bandwidth will be allotted to the other users according to their configuration. A QoS policy can be applied to single or multiple zones, controlling or prioritizing traffic by policy application, traffic direction (TX/RX), and source IP address.
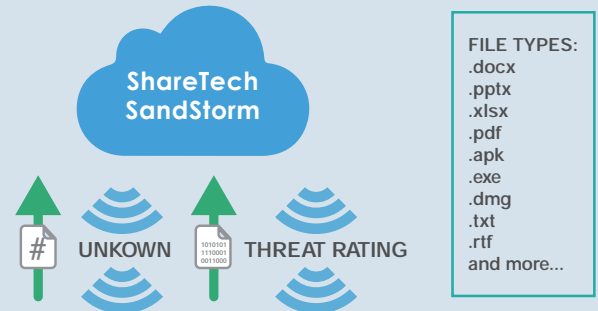
SD WAN

ShareTech supports SD-WAN with IPSec VPN. Flexible WAN connectivity allows for the efficient use of bandwidth between sites and the data center by reducing latency and using multiple routes to help reduce costs. Employees will always have access to their data no matter what happens with their internet connections.
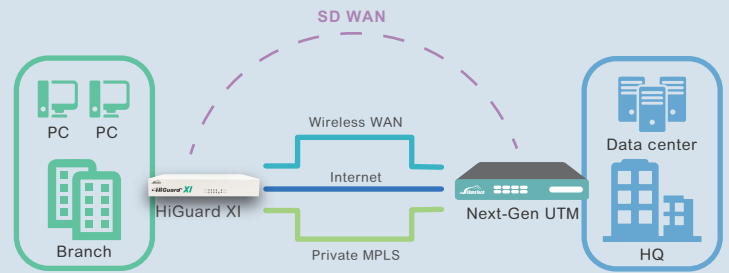

Sandstorm

To detect unknown attached files, such as Word, Excel, PowerPoint, PDF, ZIP or RAR format. Threatening emails will be quarantined and will not have the opportunity to affect the operation of the email system. HiGuard Series supports Sandstorm IP that compares suspicious files with our database.

ShareTech SandStorm

\# UNKOWN | THREAT RATING

FILE TYPES:
.docx
.pptx
.xlsx
.pdf
.apk
.exe
.dmg
.txt
.rtf
and more...

Load Balance

The HiGuard Series supports outbound and inbound load balancing, providing at least 2 WAN links. Multi-homing load balancing is supported to spread a business's Internet traffic among multiple access links to increase the aggregate throughput and to divert traffic away from non-functional links when they fail. An additional 3G/4G/LTE USB can also be attached to one of the USB ports to add a backup wireless connectivity.
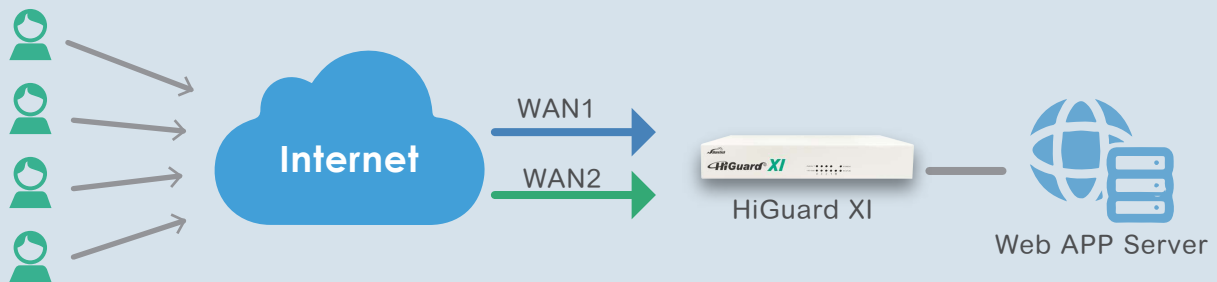
## Complete VPN Solutions (IPSec/PPTP/L2TP/SSL VPN/IP Tunnel)

• Supports IPSec, PPTP, L2TP, SSL, and GRE Tunnel
• Supports DES, 3DES, AES, AES128, AES192, and AES256 encryption and SHA-1, SHA256, SHA512, and MD5 authentication algorithms
• SSL VPN mobility client for Android and Apple iOS
• Controls connectivity of remote sites from the central site

Cloud-Based service system (Eye Cloud)

ShareTech-branded devices can be remotely monitored and efficiently maintained. Multi-region wireless APs and switches can be accessed via UTMs as well. HQ admins can customize tasks based on sites and then select UTM series, devices, config. files/firmware, and intervals. Tasks can be published and targeted to relevant locations in real-time. (HX v9.0.2.3 or above)

URL Database (1-year license)

Integrated with a third-party database, the HiGuard Series can automatically detect and enforce policies for malicious URLs. They are classified into 6 categories. Admins can easily manage entries for URLs, customize the display message when a website is blocked, retain loggings, and keep a query available for future use.

Trusted websites

Phishing, Scam, Violence,18+ banned websites

HiGuard XI

PC
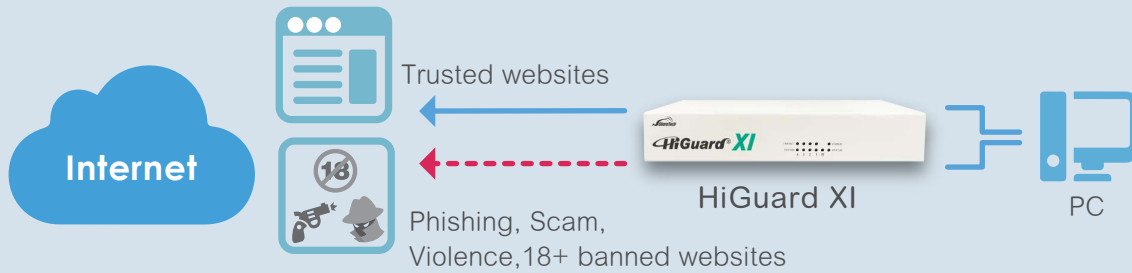
Application Control (1-year license)

To prevent data leakage and ensure regulatory compliance, admins have to take an ongoing active role in managing access to work-related applications during working hours. Integrated with a third-party database, the HiGuard Series can enforce policies for 17 types of applications.

Internet

AWS

Allowed apps

PC
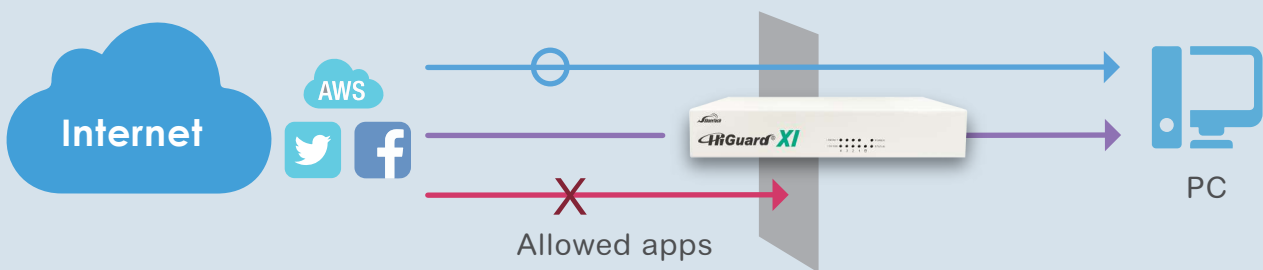
Anti-Virus Engine(s) HiGuard XI Security Solutions

Clam AV is enabled to perform automatic email scanning by default. It can detect millions of viruses, worms, and Trojans. Its virus database is available for updates 24/7 and supports searching for virus-infected emails by conditions. Moreover, admins can define how frequently to check for new virus signatures, virus definition versions, update logs, and update servers. Customers may purchase Kaspersky for advanced security.

Internet

HiGuard XI

PC

Intrusion Prevention System (IPS) HiGuard XI Security Solutions

Built-in IPS inspects the packets from OSI layers 4-7, and blocks concealed malicious code and worms delivered in TCP/IP protocols. Its severity level is defined as low, medium, and high. ShareTech regularly updates the predefined attack signature database to keep the protection current.

Technical Specifications

Front View		Performance	
		Firewall throughput	1.9 Gbps
		Concurrent connections	200,000
		New connections/sec	65,000
		Firewall throughput	380 Mbps
Back View		VPN throughput	800 Mbps

Software specifications	HiGuard VI	HiGuard XI
Wizard	O	O
Firewall	O	O
2FA	O	O
Anti-virus	X	ClamAV
URL/APP control	1-year	1-year
Intranet protection	O	O
IPS	X	O
Web service	X	O
Switch / AP mgmt.	O / 50pcs	O / 50pcs
HA	X	O
Bulletin board	X	O
Dashboard	Optional	Optional

Physical specifications	
Recommended users	Under 50
Storage	32GB eMMC
RAM	4G
Ethernet interfaces	4 x GbE copper
Management ports	1 x COM RJ45
Other I/O ports	2 x USB 3.2 (rear)
Power supply	110-240 /12V
Power consumption	40W
Status LEDs	Power/System