



ShareTech HiGuard Series offers an all-around security appliance best suited to deployments in retail stores, branch offices, and smaller business environments. 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 of an organization, which is not less critical than headquarters. HiGuard XI has high-reliability storage and memory space to maximize its 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. In addition to basic firewall features, it also offers an extraordinary range of security features such as VPN connections (IPSec and SSL), gateway security protection (Anti-Virus, IPS, Sandstorm IP, SYN Flood protection), 2FA (user accounts, authentication, and SSL VPN), collaborative controls (switches and wireless APs), intuitive management (URL/APP control and database, bandwidth control, user online behavior, and load balancing), etc.

HiGuard Series provides an on-premises CRM platform (Client-Side) allowing admins to monitor operating status via UTM. Moreover, Eye Cloud, a cloud-based platform, provides centralized management of ShareTech-branded devices. The system administrator can maintain appliances efficiently, expand a view to multi-region edge switches and wireless APs, and receive an alert when an anomaly is detected.

Highlights

SECURITY	MANAGEMENT	PERFORMANCE
Gateway Security VPN Secure Tunnels	2FA & Behavior Analysis Dashboard Panel	X86 Dual-Core Memory-Optimized Storage
<ul style="list-style-type: none"> • IPSec/SSL site-to-site and remote access VPN • Virus Engine • IPS • Sandstorm IP • SYN Flood Protection 	<ul style="list-style-type: none"> • 2FA • QoS/Flow/APP Control • Co-Defense & AP Mgmt. • Client-Side CRM • Eye Cloud Mgmt. 	<ul style="list-style-type: none"> • 4 Gigabit Ethernet Ports • 4G RAM & 32G Storage • Intel Dual-Core CPU • NAT reaches 1.9 Gbps • Offline Signature Update • USB Recovery

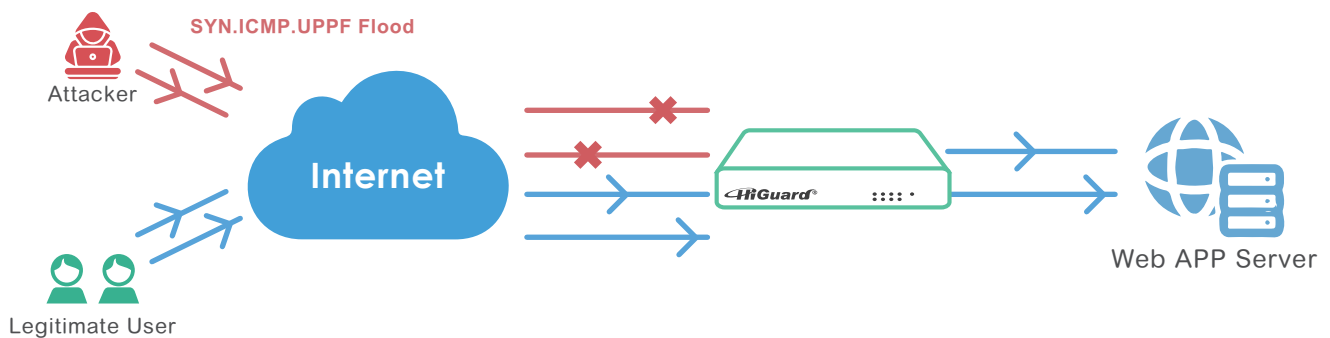
HiGuard XI Security Solutions

Best-Suited UTM for SOHO/SMB

HiGuard XI is a powerful desktop security solution designed for SMBs. With the idea of automation, it combines deployment, structure, management, and monitoring into one single unit. It is fast to deploy and easy to use. Its fanless design can ensure silent operation in quiet office environments. 4 Gigabit ports provide Gigabit Ethernet connectivity for users under 50. HiGuard XI has a fully integrated security layer that adds two-factor authentication and a wireless solution. Because of the perfect balance between price and performance, it become the best choice for small businesses.

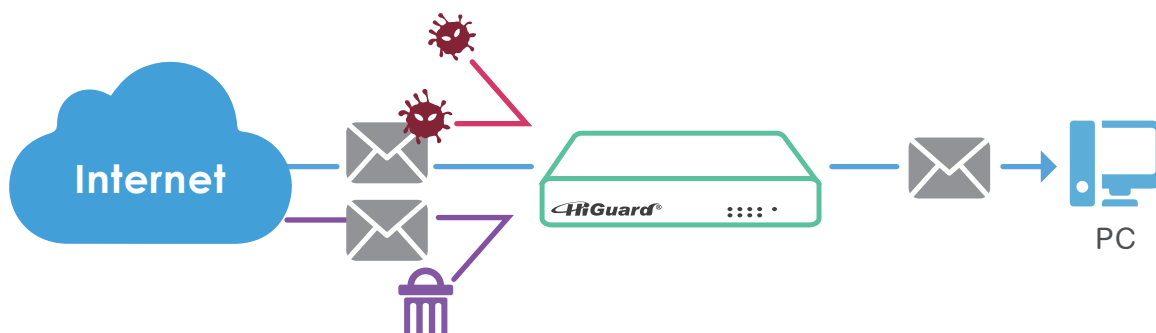
Firewall

Built-in SPI (Stateful Packet Inspection) provides DoS detection and prevention against denial-of-service (DoS) attacks such as SYN flood, ICMP flood, and UDP flood. When unusually high rates of the new connection are detected, the system will issue an alert notification or block an anomalous session. In addition, HiGuard XI SPI protects against packet-injection attacks by checking several components of TCP and UDP sessions. ShareTech applies the concepts of reasonable traffic packets and connections. Typically, each source will not generate too many data packets simultaneously per second. If the number of data packets exceeds the threshold, the firewall will selectively block data packets to avoid influencing user service experience.



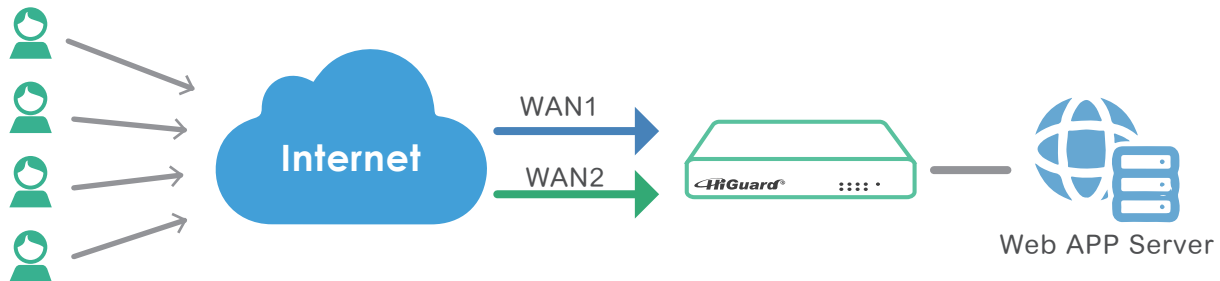
Anti-Virus Engine

Clam AV is enabled to perform automatic email scanning by default. The virus scanning can detect over 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. Calm AV scans inbound, outbound, and internal mail for viruses. Admins can further decide to delete the infected email automatically, quarantine ones with unwanted file extensions, or send notifications.



Load Balance

The HiGuard Series supports outbound and inbound load balancing, providing businesses with 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

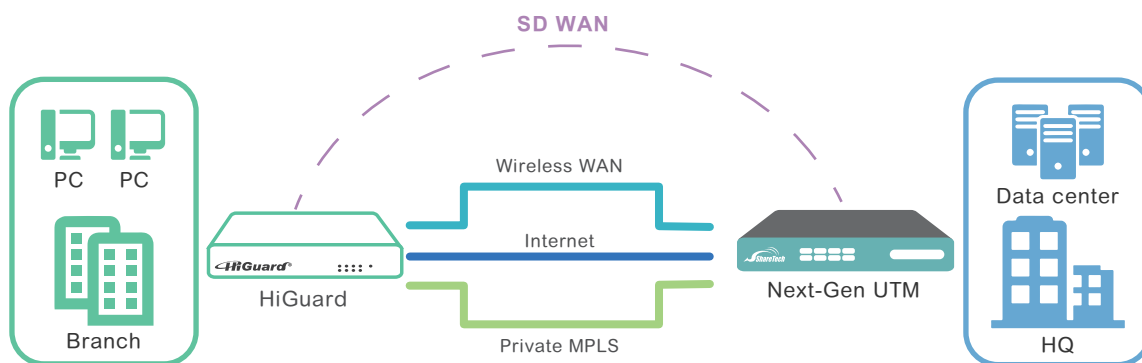


Improved Performance and Memory and Storage Capacity

Internet service providers (ISPs) are offering higher-speed internet lines to businesses. To satisfy existing customers, the HiGuard Series provides better support for the explosive growth in data traffic, offering 4 Gigabit ports (1 fixed LAN and 3 custom ports), 4G RAM, and 32G storage. Hardware-accelerated NAT operates at gigabit speeds up to 1.9 Gbps, making HiGuard XI a basic unit with comparable performance and remarkable stability.

SD WAN

MPLS services typically require dedicated and private network connections from the service provider. On the contrary, ShareTech supports SD-WAN with IPsec VPN, which promises to remove the constraints of legacy connectivity technology. 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. With ShareTech SD-WAN, geographic boundaries get erased, and all data of an organization stays connected. Employees will always have access to their data no matter what happens with their internet connections so that they'll never have to worry about missing important emails or ERP data.



QoS

QoS offers more agile bandwidth management for industries and organizations. 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. In this way, any network can take advantage of QoS for optimum efficiency.

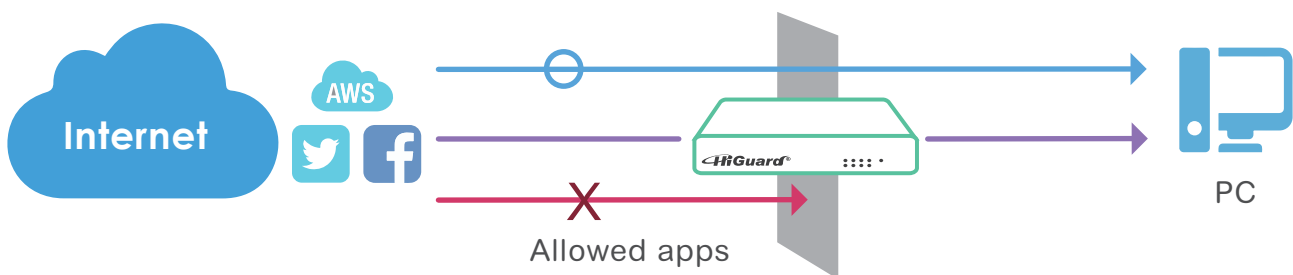
URL Database (1-year license)

Integrated with a third-party database, the HiGuard Series can automatically detect and enforce policies for malicious URLs. They are classified into 6 categories according to their attack type and lexical analysis. Admins can easily manage entries for URLs whether they are using either HTTP or HTTPS protocol, customize the display message when a website is blocked, retain loggings, and keep a query available for future use. Users do not have to fear they might stumble on a malicious URL and get infected with malware. The URL database is updated daily at the time specified.



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 like P2P, VPN and Remote Control, Streaming and VoIP, Network Service, Online Sharing and Storage, Web Service, Social Networks, Instant Messaging, System and Update, News and Media, Shopping and Auction, Entertainment and Arts, Sports and Travel, Food and Drink, Finance and Insurance, Gambling and porn, Games, etc. The application database is updated daily at the time specified.

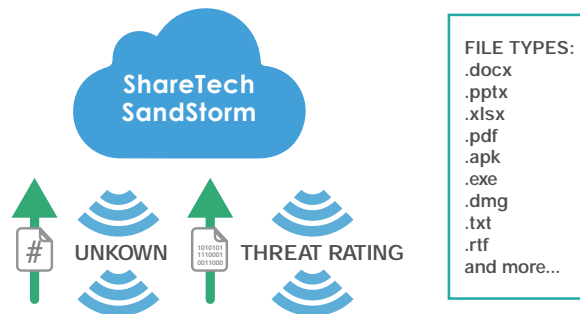


Intrusion Prevention System (IPS)

Built-in IPS inspects the packets from OSI layers 4-7 (transport to application layer) and blocks concealed malicious code and worms delivered in TCP/IP protocols. IPS uses signatures to identify the attacks in progress, and its severity level is defined as low, medium, and high. ShareTech regularly updates the predefined attack-signature database to keep the protection current. The IPS signature matchings can give visibility of triggered IPS alerts; admins will be notified immediately and can select grant or block access packets.

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.



Wireless AP Management

Wireless connectivity plays a central role in increasing businesses' agility. Employees rely on WiFi more than ever to perform their jobs and stay productive. By supporting SNMP or Telnet/SSH, the HiGuard Series can be a wireless controller, grouping wireless APs and assigning the same configurations. Admins can obtain brief information about login IP address, MAC address, the amount of time, and the number of users per SSID. Moreover, admins can debug, improve user experiences, and optimize wireless connectivity by remotely restarting an AP managed by firewalls.

Complete VPN Solutions (IPSec/PPTP/L2TP/SSL VPN/IP Tunnel)

Using IPsec, PPTP, L2TP, and SSL VPN connections, HiGuard XI provides data confidentiality, data integrity, and data authentication. At the same time, popular protocols such as web, SMTP, and POP3 that contain packets transmitting within tunnels can be controlled.

- 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

Dashboard (Optional)

The dynamic dashboard in the web user interface (web UI) presents a graphic view of the system status. HiGuard XI supports real-time concurrent connections, network resource usage, threat intelligence, flow analysis, defense, IPS, web service and control, email, application control, Geo IP, and DNS query. The design makes it easier for admins to drill down to the root cause. Administrators can define reports by time, data ranking, IPv4/v6, and document in PNG/PDF format. The dashboard gives the admins an overview of the HiGuard XI and improves agility, reduces risk, and cuts IT costs in a business.

HiGuard VI Features

BASIC FIREWALL

- **Routing** : Supports static/dynamic route, designated gateway group, and default gateway.
- **IPv4/v6** : Supports IPv4, IPv6, and IPv4/IPv6 dual-stack. Admins can quickly swap between at the click of a button.
- **IEEE VLAN 802.1Q** : The Intranet can be divided into multiple segments, isolating different traffic logically.
- **GEO IP** : Geo IP restriction allows admins to configure a geolocation-based policy by specifying source and destination locations.
- **Network Services** : HiGuard Series supports DHCP, DDNS, SNMP, and DNS Proxy.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) prevention** : TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks can all be mitigated by blocking bad bot traffic before it reaches the targeted site.
- **VPN** : Supports IPSec, PPTP, L2TP VPN, SSL VPN, and IP Tunnel.
- **SD-WAN:** : SD-WAN can combine from the designated gateway or VPN tunnels, enable optimized traffic routing over multiple transport links, and select a route for applications based upon configured policies and priorities.
- **IP Tunnel** : A secure VPN can be created via IP Tunnel between two ShareTech UTMs, and traffic passed through the VPN can be monitored.
- **Auto IPSec VPN** : To create an IPSec VPN between two sites having massive/dynamic IP addresses, Auto VPN can reduce the complexity of deployment and increase stability.
- **Loggings** : HiGuard XI includes loggings for system operation and status, wizard, configuration, networking, policies, objects, services, advanced protection, IPS, email security, VPN, etc.

NETWORK & EMAIL PROTECTION

- **Clam AntiVirus** : HiGuard XI supports ClamAV, an open-source anti-virus engine that detects millions of trojans, viruses, malware, and other malicious threats.
- **Intrusion Prevention System (IPS) & Signature Database** : HiGuard XI supports IPS that proactively detects intrusion behaviors and matches the signature database. IPS Protection' s severity level is defined as LOW, MEDIUM, and HIGH.
- **Sandstorm** : HiGuard Series supports Sandstorm IP.
- **Anomaly IP Analysis** : Flow/behavior-based anomaly detection allows both up and down sessions to be analyzed. An anomaly can be blocked, recorded, and notified to subscribers.
- **Email Filtering & Logging** : HiGuard XI supports email scanning for viruses, queries on SMTP communication logs, infected email quarantine, and queries on email logs .

WEB PROTECTION

- **Transport Layer Security (TLS)** : TLSv1.3 inspection on IPv4 and IPv6
- **Deep packet inspection (DPI)** : DPI is a form of packet filtering that locates, classifies, and reroutes packets. It has higher detection accuracy than port-based TCP/UDP.
- **WEB Service** : HiGuard XI supports HTTPS scanning in Anti-Virus, SSL certificate installation, loggings for HTTPS proxy action, and certificate allowlist.
- **URL Filtering** : A third-party database sorts malicious URLs into six categories. Users can renew the license to get real-time updates or periodically apply firmware upgrades for free updates.
- **Application Control** : A third-party database sorts applications into 17 categories. Users can renew the license to get real-time updates or periodically apply firmware upgrades for free updates.

ACCESS CONTROLS & FLOW MANAGEMENT

- **Authentication** : The system can authenticate users with accounts on hosts, POP3/IMAP, Radius, and AD servers. Admins can add users to groups, view logs, and get status information.
- **Two-Factor Authentication (2FA)** : Two-factor authentication can add an additional layer of login security to user accounts, authentication, and SSL VPN access. Users can download mobile security apps (Google/Micro soft authenticator) to generate codes for 2FA.
- **Load Balance** : Inbound and outbound can be reviewed to make sure traffic patterns are expected. Admins can set up traffic rules in priority order so that all traffic can be evenly distributed among multiple WAN links.
- **QoS** : Ensure an adequate bandwidth for high-priority tasks and applications, maximum bandwidth limits, and priority levels.

INTRANET PROTECTION

- **Switch Co-Defense** : Common SNMP switches and advanced L2/L3 switches (a topology included) can be centrally managed. Zyxel switches support IP Source Guard (static IP-MAC-Port binding) to perform DHCP Snooping. Moreover, the PoE schedule can be configured via UTM to manage power consumption.
- **AP Management** : It displays the status of AP and online users. Quick deployment (config. files) can be delivered for large numbers of access points.
- **Intranet Protection** : ARP spoofing prevention, IP & MAC spoofing prevention, notification, and block status.



CENTRAL ORCHESTRATION

- **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. Flexible options (Free, VIP, and Distributor) are offered to match requirements. 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. (Supported version: HX v9.0.2.3 or above)
- **Client-Side CMS** : HiGuard Series supports regularly passing data from the client side to the server side. The system makes periodic backups (config. file) automatically.
- **Dashboard** : A real-time Dashboard reporting module can be purchased in the HiGuard Series, showing a graphical presentation of the current status.

OTHERS

- **Operation Mode** : Transparent Bridge, Transparent Routing, and NAT.
- **Operation Management Interface** : Management interface and Dashboard GUI (optional module for HiGuard Series)
- **Diagnostic Tools** : IStandard net tools such as Ping, Traceroute, DNS lookup, and port scanners are available to help users identify and fix connection problems. Test widgets like IP Route, Wake Up, SNMP, and IPv6 tools can test your connection and readiness.
- **Remote Log Server** : Log data can be forwarded in the Syslog format to a remote Syslog server that receives, categorizes and stores log messages for advanced analysis.
- **Initial Setup Wizard** : The wizard simplifies the configuration process by setting up LAN, WAN, URL Blacklisting, Security Settings, and Email Management.
- **Distributed administration** : Authority can be delegated to one or more administrators, such as Admins and assistant admins. Admins can assign three types of privileges (READ, WRITE, and ALL privileges).
- **Custom Password Policy** : password length and complexity requirements, unable to reuse old passwords, and change passwords at regular intervals.
- **Interrupt** : Hardware interrupts (via CPU) and software interrupts (via ZONE) are supported, allowing the CPU to perform specific tasks. IT administrators can optimize system performance and troubleshoot issues more effectively.
- **Offline Signature Update via USB drives** : HiGuard XI supports the following items: IPS, the default APP&URL Blocklistings, ClamAV, and Sandstorm IP.
- **E-Bulletin Board** : HiGuard XI supports the bulletin board to ensure all users read important messages before accessing a webpage.
- **High Availability (HA)** : HiGuard XI supports Hot-Standy (Active-Passive) mode.
- **Warranty & Firmware** : 2-year warranty and free firmware update

Technical Specifications

Front View		Performance		
		Firewall throughput	1.9 Gbps	
		Concurrent connections	200,000	
		New connections/sec	65,000	
		VPN throughput	380 Mbps	
		Anti-virus throughput	800 Mbps	
Back View				
		Software specifications	HiGuard VI	HiGuard XI
		Wizard	O	O
		Firewall	O	O
		2FA	O	O
		Anti-virus	X	ClamAV
Physical specifications		URL/APP control	1-year	1-year
Recommended users	Under 50	Intranet protection	O	O
Storage	32GB eMMC	IPS	X	O
RAM	4G	Web service	X	O
Ethernet interfaces	4 x GbE copper	Switch / AP mgmt.	O / 50pcs	O / 50pcs
Management ports	1 x COM RJ45	HA	X	O
Other I/O ports	2 x USB 3.2 (rear)	Bulletin board	X	O
Power supply	110-240 /12V	Dashboard	Optional	Optional
Power consumption	40W			
Status LEDs	Power/System			

