Next-Generation UTM

NU-860C

ShareTech NU series is the next phase of technology change which will help service providers to launch the services in a single click, delivering exceptional performance, superior multi-layered threat protection, and role-based administration to SMBs.

NU-860C carries advanced protection across your network security deployments: deep packet inspection (DPI), IPS, SSL inspection, web filtering, QoS, virus scanning, spam filtering, and two-factor authentication (2FA) to prevent potential attacks launched by hackers and legitimate authorized users from accessing the network. Moreover, high availability (HA) is supported to ensure smooth network operation.

NU-860C goes beyond traditional firewalls and brings a new approach to the way administrators define their firewalls with 14 Gigabit Ethernet ports. One Gigabit Ethernet port is dedicated to management, and the other 13 Ethernet ports can be user-defined into LAN, WAN, or DMZ. To enhance internal security, NU-860C unifies and deploys consistent security policies across both wired and wireless networks, and centrally manages and monitors internal wireless APs and switches. ShareTech also introduces a cloud-based service system providing a new way to deploy, operate, and manage distributed networking appliances. When anomalies occur in network traffic, the system sends notifications to IT administrators and helps them to resolve issues quickly.

Guardian of Gateway Security

ShareTech NU Series fully integrates firewall, deep packet inspection (DPI), virus scanning, ISP, SSL inspection, and blocking, moreover, extended APT prevention and IPS detection are provided to stay one step ahead for improved compliance and security.

- Stateful packet inspection (SPI) firewall technology examines the packet header and destination port for authentication and checks the entire packet’ s content before determining whether to allow its passage into the network. SPI firewalls can drop any packet that is identified as potentially dangerous and automatically blocks DoS, DDOS, and UDP Flood attacks.
- Web filtering to block HTTP/HTTPS access
- Intrusion prevention system (IPS)
- Application control
- Virus scanning and spam filtering
- Network traffic monitoring and Co-Defense

A Compact x86 Network Appliance with Intel Processors Reinforces Internal Management

NU-860C is a real-world firewall based on a 4 Core Intel-branded processor, with 14 Gigabit Ethernet ports, firewall throughput up to 12 Gbps, and improved VPN throughput of 850 Mbps.

Supports SD-WAN

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.

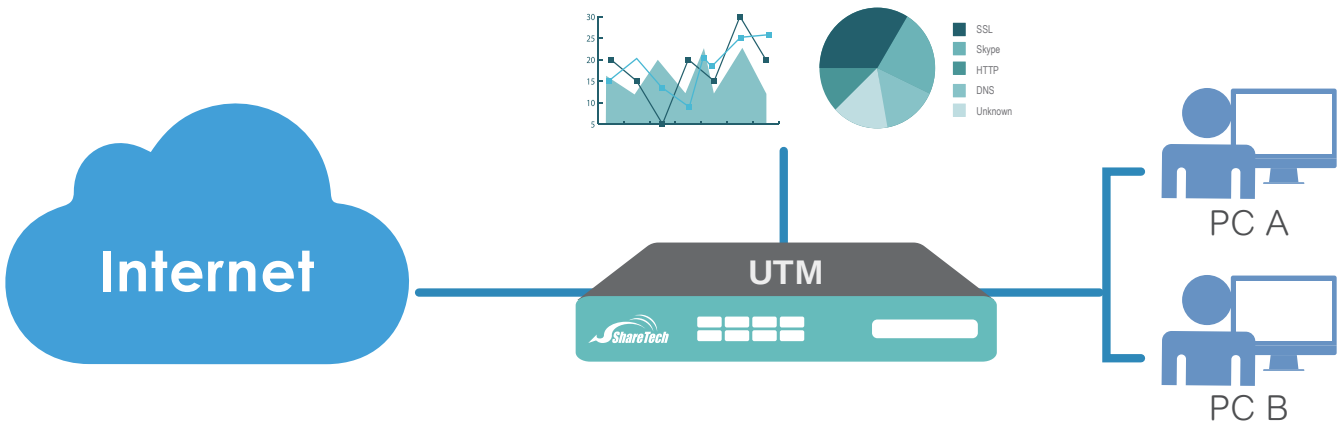
Deep Packet Inspection (DPI) and Application Control

Unique DPI performs traffic signature analysis by inspecting all packets for new application signatures, scoring up the signatures, and appending them to the relevant database. More importantly, having recorded these collected data will be available for future audits.

- Supports for protocols and applications, including video streaming, peer-to-peer communication, social networking, and instant messaging
- Detailed control over file sharing, remote control, VoIP, online games, browsers, etc.
- SSL/HTTPS inspection
- Cloud database updates

Single-Pane-of-Glass Dashboard

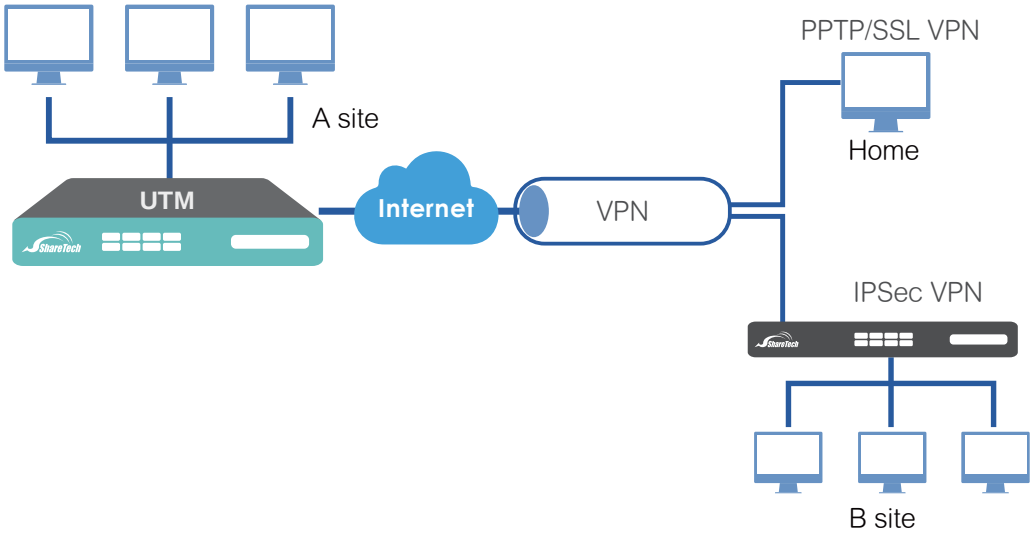
The ShareTech dashboard is available through the GUI and presents a graphic view of the real-time system information. It allows administrators to have visibility into UTM information and includes server status, indicators for events, connection activity, and performance alters. The continuous monitoring allows the analyst to identify important data without having to log into multiple devices. Problems can be rapidly identified to increase potential concerns.



Complete VPN Solutions

VPN connections provide 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 Tunnels
- Supports DES, 3DES, and AES encryption and SHA-1/MD5 authentication algorithms
- SSL VPN mobility client for Android and Apple iOS
- Supports Auto VPN (Server & Client)
- Controls connectivity of remote sites from the central site



Central Management (CMS, Eye Cloud, and AP management)

A central management system (CMS) designed for multi-site network security appliance deployments allows administrators to remotely restart, reboot, and monitor devices. Moreover, Eye Cloud, a cloud service platform, provides users user-friendly interface to support instant equipment maintenance and management. It is an all-inclusive solution to monitor various networking appliances deployed in either external or internal networks such as UTM, wireless APs, or switches. When an anomaly occurs, administrators will be notified of the problem.

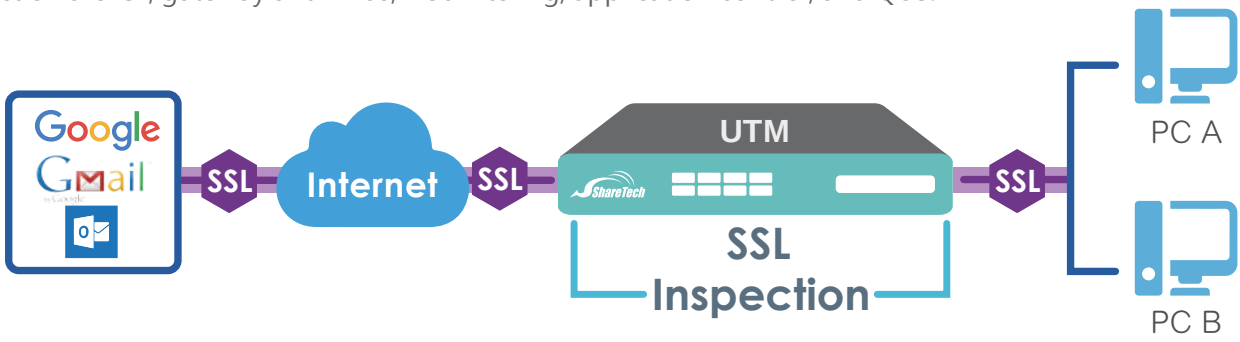
I. Features

Exceptional Performance and Consolidated Security Features

ShareTech NU Series adopts a best-on-class multi-core x86 CPU platform to deliver exceptional performance and intelligent network security features. ShareTech develops high-performance security modules, delivers high connection capacity connectivity, and supports USB instant recovery.

SSL Inspection

To protect your network from network threats, SSL inspection is the key used to unlock encrypted sessions, see into encrypted packets, find threats, and block them. Several security features that can be applied using SSL certificate inspection are ISP, gateway anti-virus, web filtering, application control, and QoS.



Anti-Virus

Clam AV is available by default for virus scanning which can detect millions of viruses, worms, and Trojans. Once suspicious emails are detected, the administrator can decide to delete or block them. Moreover, websites will be scanned once the function of anti-virus is enabled in policy. By default, NU-860C contains a 1-year Kaspersky license. Customers may renew Kaspersky protection for their security needs.

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. As soon as an attack is suspected, IT administrators will be notified immediately, and later an extensive range of reports will be available for analysis. ShareTech regularly updates the predefined attack signature database and makes it available as an IPS security package.

ShareTech Sandstorm (Malicious Programs Filtering System)

To detect unknown attached files, such as Word, Excel, PowerPoint, PDF, ZIP, or RAR format, IT administrators can apply ShareTech Sandstorm inspection with four types of security inspection: file hash, Web URL, domain, and IP. Threatening emails will be quarantined and will not have the opportunity to affect the operation of the email system.

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

WAF

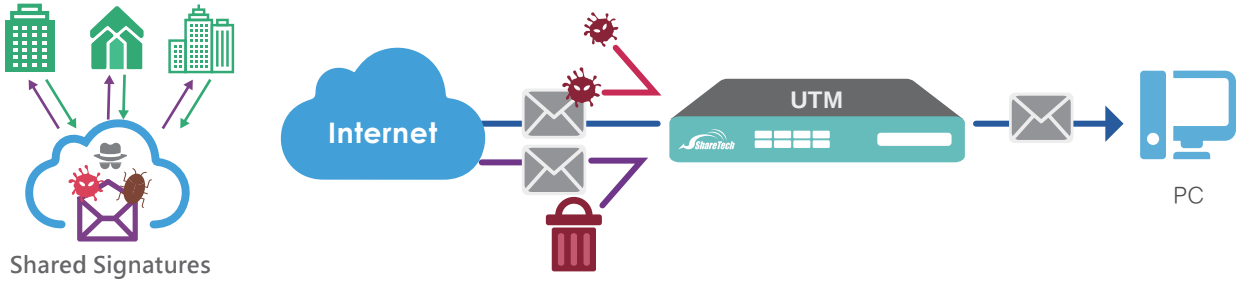
To minimize the risks of web application attacks, an organization should adopt a multi-layered approach to web application security. A web application firewall (WAF) functions as an intermediary that monitors and controls incoming and outgoing traffic to and from a web application, detecting and blocking attacks before they reach the web application. It operates at the application layer (L7) and protects against cross-site scripting (XSS) attacks, SQL injection attacks, remote command execution (REC) attacks, and webshell uploads to avoid severe consequences.

IP Traffic Streams Analysis

Outgoing/incoming concurrent sessions, upload/download flow, and time duration are flow parameters collected for packet-based traffic analysis. Using a combination of pattern matching can determine whether an activity is performing normally or abnormally. If employees are violating the rules and exceeding more downloading flow, IT administrators are allowed to define the trusted IP list and take appropriate actions to block network access, limit maximum bandwidth, block ports on switches (Co-Defense), or simply receive a notification.

Anti-Spam and Shared Signatures

ShareTech NU Series employs multi-spam filters: ST-IP network rating, Bayesian filtering, spam characteristics filtering, fingerprinting, auto-learning, and personal B/W list. It also gives administrators the flexibility to enforce custom filtering. These help industries create their database by importing the latest spam updates. Following actions like forward, delete, and quarantine can be taken on the mail identified as spam. Moreover, the shared signatures mechanism shares the signature of an early receiver with the rest of the group so that higher spam detection accuracy can be obtained.



Mail Gateway

For companies that have deployed mail servers in their network environments but lack advanced filtering, NU Series can be placed at the gateway to secure your email and get simple and powerful protection from spam, viruses, and malware.

Content Filtering

IT administrators can configure Web filtering profiles that block URLs to inappropriate webpages like violence and pornography and hacking attacks like malware and viruses. Moreover, the NU Series filters out ActiveX objects, Cookies, or Java applets that may pose a security threat in certain situations. Both keywords and URLs of specified websites can be added to Blacklist and Whitelist.

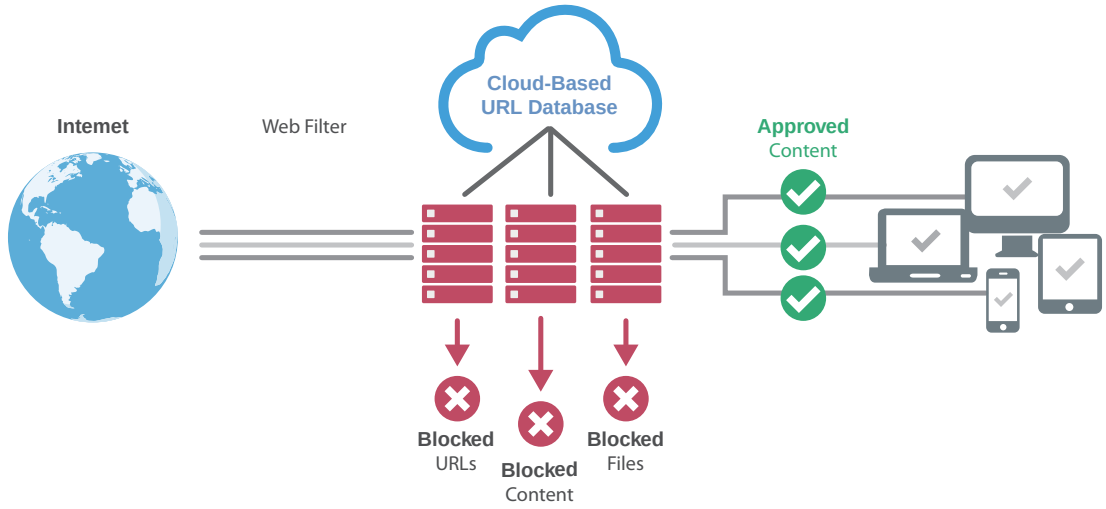
Advanced URL Control and Database

Advanced URL database collects millions of URLs and updates every period. All these URLs and their contents were analyzed and classified, including Pornography & Violence, Network & Cloud Service, Organizations & Education, Security Risks & Criminal, Life Information, and Others. IT administrators can block any category in the database with ease without entering keywords or desired URL addresses one by one. By default, NU-860C contains 1-year URL license. Customers may renew the license for an instantly updated database.

Advanced Application Control and Database

To prevent data leakage and ensure regulatory compliance, access to unrelated applications during working hours should be controlled. The advanced application database contains 1000+ modernized applications like P2P, VOIP, GoToMyPC, Webpages, Games, Media Player, Bit Torrent, Foxy (Gnutella), stock market, Instant Messaging, Xunlei, Gator, Yahoo Manager, Virus and Malware, filename extension, Kazaa, Facebook, Zalo, etc. By default, NU-860C contains 1-year application license. Customers may renew the license for an instantly updated database.

.



AP Management

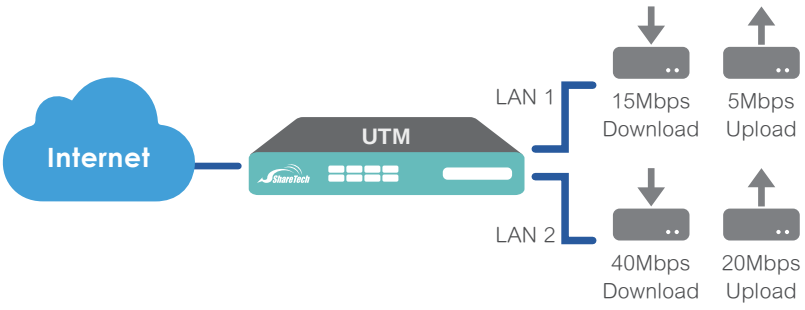
By supporting SNMP or Telnet/SSH, the NU Series can be a wireless controller, grouping wireless APs and assigning the same configurations. IT Administrators can obtain brief information about login IP address, MAC address, the amount of time, and the number of users per SSID. Moreover, admins can debug, improve user experiences, and optimize wireless connectivity by remotely restarting an AP managed by firewalls.

Co-Defense

IT Administrators can know the deployment of the switch architecture and the usage status of each node through the network topology. The Co-Defense feature keeps attackers outside the internal network when internal users are. The IP address, MAC address, and attack time will be recorded for quick discovery of the infected device. If the traffic (such as abnormal traffic, sessions, and IPS) exceeds the limit quota, the system will notify the admins and close the abnormal port to minimize the impact.

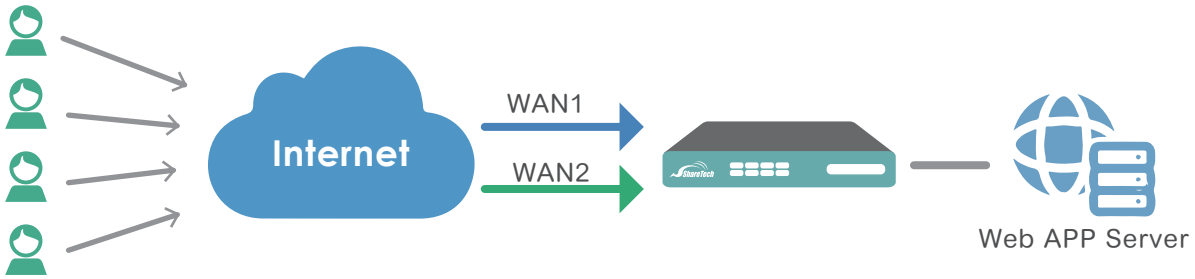
QoS

QoS offers more agile bandwidth management for industries and organizations. Since bandwidth can be limited using source IP in both directions, 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. Moreover, an efficient priority scheme can be available for minimum/maximum bandwidth guarantee.



Inbound/Outbound Load Balance

The NU 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.

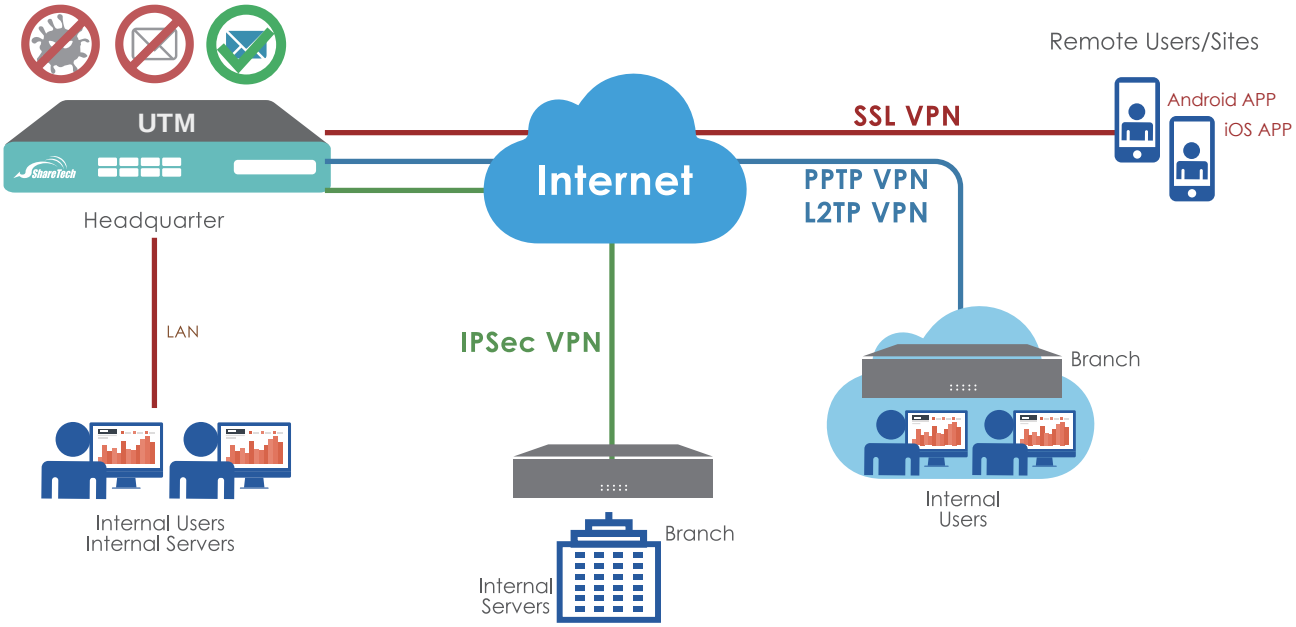


Graphical Reports

ShareTech Dashboard reporting allows administrators to select an SMTP server, customize and preview the subject for email, change the number of backup files, select log sources, customize time intervals (day/week/month/season), format, top ranking, and language. Reports can be directly exported in PDF or PNG format which helps IT administrators track and diagnose.

VPN

Remote-access VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. ShareTech offers IPSec, PPTP, L2TP, and SSL VPN technologies on a single platform. Site-to-site IPsec VPN allows headquarters and their branch offices to be on the same network and share resources among offices. Point-to-point PPTP VPN, natively supported by Windows, is easy to set up and maintain and requires user-level authentication. L2TP which encrypts the authentication process and avoids your transmission being intercepted is a bit more powerful than PPTP. Moreover, SSL VPN provides remote-access connectivity from almost any Internet-enabled location using a web browser and its native SSL encryption.



II. ShareTech NU Series Protection

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：**
  The NU Series supports Client/Server DHCP, DDNS, SNMP, and DNS Server and 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 affic 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 ultiple 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：**
  The NU Series includes loggings for system operation and status, wizard, login/logout, system anomaly & control, configuration, networking, policies, objects, services, advanced protection, IPS, WAF, email security, content record, VPN, etc.

NETWORK & EMAIL PROTECTION

- **Clam AntiVirus：**
  Supports ClamAV, an open-source anti-virus engine that detects millions of trojans, viruses, malware, and other malicious threats.
- **Kaspersky AntiVirus：**
  Supports built-in 1-year Kaspersky license (NU-860 models and above)
- **Intrusion Prevention System (IPS) & Signature Database：**
  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：**
  The NU Series supports four types of security inspection: file hash, Web URL, domain, and IP.
- **WAF：**
  Cyberattacks are classified into 19 categories. The NU Series supports a host-based WAF that sits between external users and web applications to block and log requests.
- **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：**
  The NU Series supports incoming/outgoing/received email scanning for virus/spam/auditing/backup, 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 ort-based TCP/UDP.
- **WEB Service：**
  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/Microsoft 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 that gives an instant view of the operational status and speed of each port) 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: NU v9.0.2.4 or above)
- **Server-Side and Client-Side CMS：**
  The NU 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 is built in the NU series (Available in SSD storage models) (optional module for NU-840H and NU-860H), 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. (Available in SSD storage models) (optional module for NU-840H and NU-860H)
- **Diagnostic Tools：**
  Standard 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. (Available in NU-840 and NU-860 models)
- **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：**
  Supports the following items: IPS, the default APP Blocklistings, anti-virus (ClamAV & Kaspersky), and Sandstorm.
- **Backup & Restore：**
  Offers USB system backup, system backup, and auto backup (Available in SSD storage models). A system recovery can be ready to minimize the damage imposed by an incident.
- **UPS：**
  Provides backup power as quickly as possible in the event of data loss and some protection from power quality issues.
- **E-Bulletin Board：**
  Ensure all users read important messages before accessing a webpage.
- **LAN Bypass：**
  Supports at least 1 pair of LAN bypass as a fault-tolerance to protect business communication in the event of a power outage. (NU-860 models and above)
- **High Availability (HA)：**
  Supports Hot-Standy (Active-Passive) mode.
- **Web Interface Languages：**
  English, Traditional Chinese, and Simplified Chinese.
- **LCM Display：**
  Equipped with a parallel LCM display with 4-key buttons. (NU-860 models and above)
- **Warranty & Firmware：**
  2-year warranty and free firmware update.

III. SPECIFICATION

	NU-840	NU-840H	NU-860H	NU-860T
Hardware				
Platform size	1U	1U	1U	1U
Recommended users numbers	Under 100	Under 100	Under 200	Under 300
Ethernet interfaces	6 x Gigabit	6 x Gigabit	6 x Gigabit	6 x Gigabit 2 x 10G SFP+
Custom ports	5	5	5	7
USB	3.0 x 2	3.0 x 2	2.0 x 2	2.0 x 2
LAN bypass	x	x	•	•
Power consumption	65W	65W	120W	120W
Capacity				
Max firewall throughput	4.2 Gbps	4.2 Gbps	9 Gbps	15 Gbps
Max. concurrent sessions	2,000,000	2,000,000	3,000,000	3,400,000
New sessions per second	65,000	65,000	100,000	120,000
Mail scan per day	3,100,000	3,100,000	4,800,000	5,200,000
Anti-virus throughput	750 Mbps	750 Mbps	950 Mbps	950 Mbps
IPS throughput	750 Mbps	750 Mbps	1 Gbps	1 Gbps
VPN throughput	650 Mbps	650 Mbps	800 Mbps	850 Mbps
VPN Tunnels				
IPSec VPN	2,000	2,000	3,000	3,000
PPTP/L2TP/SSL VPN	600	600	1,200	1,200
IP tunnel	300	300	600	600
Network Protection				
Anti-virus engine	Clam AV	Clam AV	Clam AV	Clam AV
Kaspersky	Optional	Optional	1-year	1-year
IPS database	•	•	•	•
Sandstorm	•	•	•	•
Spam filtering & shared signatures	•	•	•	•
Mail audit	Optional	Optional	Optional	•
URL control & database	1-year	1-year	1-year	1-year
APP control & database	1-year	1-year	1-year	1-year
WAF	•	•	•	•
Geo IP	•	•	•	•
Dashboard	x	Optional	Optional	•
Co-Defense (switch)	•	•	•	•
Switch compatibility	ML-9324E | GS2220-28 | GS2220-50 | XGS2210-52 | XGS2210-28 | XS3800-28			
AP management	100 pcs	100 pcs	100 pcs	100 pcs
AP compatibility	NWA50-AX | NWA90-AX | NWA110-AX | NWA210-AX | NWA1123-ACv3 | NWA90AX PRO			
Load balance (Out/In)	• / •	• / •	• / •	• / •
Virtual server	•	•	•	•
Authentication	•	•	•	•
2FA	•	•	•	•
High availiability	•	•	•	•
VPN	•	•	•	•
IPSec Tunnel	•	•	•	•
SD-WAN	•	•	•	•
Wizard	•	•	•	•
CMS	•	•	•	•
Eye Cloud	•	•	•	•

III. SPECIFICATION

	NU-860C	NU-8700C	NU-8700F	NU-8700T	NU-8800T
Hardware					
Platform size	1U	1U	1U	1U	1U
Recommended users numbers	Under 300	Under 400	Under 400	Under 400	1000-2000
Ethernet interfaces	14 x Gigabit	14 x Gigabit	6 x Gigabit 8 x 1G SFP	6 x Gigabit 4 x 10G SFP+	* 10 x Gigabit 8 x 1G SFP 4 x 10G SFP+
Custom ports	13	13	5 / 8	5 / 4	9 / 8 / 4
USB	2.0 x 2	3.0 x 2	3.0 x 2	3.0 x 2	2.0 x 2
LAN bypass	•	•	•	•	•
Power consumption	120W	220W	220W	220W	400W
Capacity					
Max firewall throughput	12 Gbps	18 Gbps	18 Gbps	25 Gbps	50 Gbps
Max. concurrent sessions	3,400,000	3,500,000	5,000,000	5,000,000	6,000,000
New sessions per second	120,000	170,000	170,000	200,000	300,000
Mail scan per day	5,200,000	5,200,000	5,200,000	5,200,000	6,000,000
Anti-virus throughput	950 Mbps	1.2 Gbps	1.2 Gbps	1.5 Gbps	2 Gbps
IPS throughput	1 Gbps	1.1 Gbps	1.1 Gbps	1.4 Gbps	1.8 Gbps
VPN throughput	850 Mbps	2.1 Gbps	2.1 Gbps	2.4 Gbps	2.5 Gbps
VPN Tunnels					
IPSec VPN	3,000	6,000	6,000	8,000	10,000
PPTP/L2TP/SSL VPN	1,200	3,000	3,000	3,000	4,000
IP tunnel	600	1,500	1,500	1,750	2,000
Network Protection					
Anti-virus engine	Clam AV	Clam AV	Clam AV	Clam AV	Clam AV
Kaspersky	1-year	1-year	1-year	1-year	1-year
IPS database	•	•	•	•	•
Sandstorm	•	•	•	•	•
Spam filtering & shared signatures	•	•	•	•	•
Mail audit	•	•	•	•	•
URL control & database	1-year	1-year	1-year	1-year	1-year
APP control & database	1-year	1-year	1-year	1-year	1-year
WAF	•	•	•	•	•
Geo IP	•	•	•	•	•
Dashboard	•	•	•	•	•
Co-Defense (switch)	•	•	•	•	•
Switch compatibility	ML-9324E | GS2220-28 | GS2220-50 | XGS2210-52 | XGS2210-28 | XS3800-28				
AP management	100 pcs	300 pcs	300 pcs	300 pcs	Unrestricted
AP compatibility	NWA50-AX | NWA90-AX | NWA110-AX | NWA210-AX | NWA1123-ACv3 | NWA90AX PRO				
Load balance (Out/In)	• / •	• / •	• / •	• / •	• / •
Virtual server	•	•	•	•	•
Authentication	•	•	•	•	•
2FA	•	•	•	•	•
High availiability	•	•	•	•	•
VPN	•	•	•	•	•
IPSec Tunnel	•	•	•	•	•
SD-WAN	•	•	•	•	•
Wizard	•	X	X	X	X
CMS	•	•	•	•	•
Eye Cloud	•	•	•	•	•