

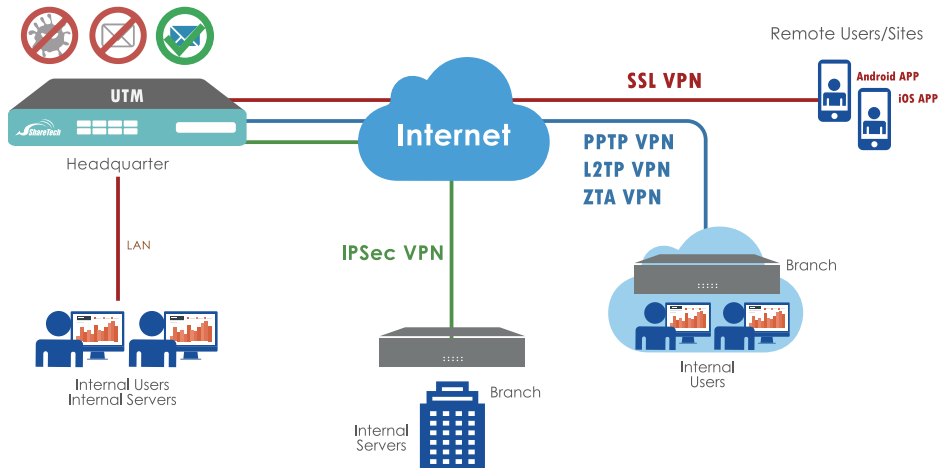
ShareTech’s next-generation UTM appliances deliver high performance, comprehensive multi-layer protection, and role-based management, making them ideal for SMB networks. NU-840H features advanced firewall capabilities, including DPI-based application control, IPS, SSL inspection, web filtering, antivirus, and spam filtering to prevent intrusions and unauthorized access. High Availability (HA) ensures uninterrupted operation. Equipped with flexible multi-Gigabit interfaces, integrated LAN security with APs and switches, USB connectivity, and cloud-based centralized monitoring, NU-840H enables secure, reliable, and easy network management from a single platform.

### High Performance with Advanced Protection

Built on an x86 architecture with a quad-core Intel processor, the NU-840H features six 1G network interface network interfaces, delivering firewall throughput of up to 4.2 Gbps and VPN throughput of up to 650 Mbps. Even under high traffic loads and deep inspection conditions, the system maintains stable performance, ensuring both robust security enforcement and reliable network connectivity.

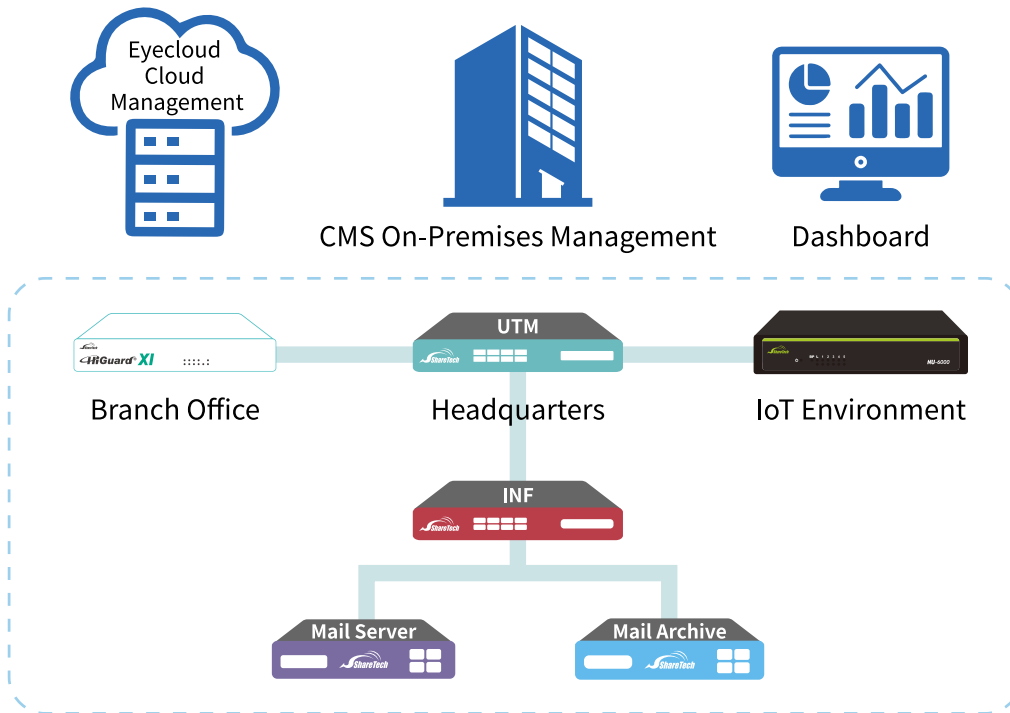
### Efficient Multi-Site Secure Connectivity

ShareTech provides secure, flexible VPN connectivity for remote users and distributed sites with centralized management and visibility. Supporting IPSec, PPTP, L2TP, SSL VPN, and ZTA VPN—with strong encryption, cross-platform clients, and Auto VPN for simplified deployment—NU-840H enables rapid and secure inter-site connectivity. Integrated SD-WAN over IPSec VPN further optimizes bandwidth, reduces latency, lowers connectivity costs, and ensures uninterrupted access to critical applications through intelligent multi-WAN traffic routing and automatic failover.



## Single Interface Management Across Cloud and On-Premises

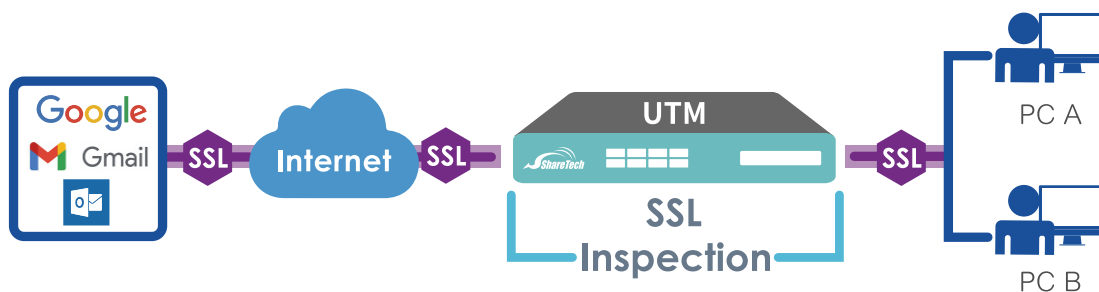
ShareTech provides centralized visibility and management through an intuitive dashboard accessible via GUI and cloud services. Administrators can monitor real-time system status, security events, connection activity, and device performance across all deployed appliances without logging into multiple devices. With integrated CMS, Eye Cloud, and AP management, administrators can remotely monitor, manage, and maintain UTM devices and wireless APs across multiple sites. Instant alerts and continuous monitoring enable rapid issue identification and streamlined network operations across both internal and external networks.



## I. Features

### 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, gateway anti-virus, web filtering, application control, and QoS.



### Anti-Virus

ClamAV 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-840H contains a 1-year ShareTech license. Customers may renew ShareTech protection for their security needs.

## AI AI IPS

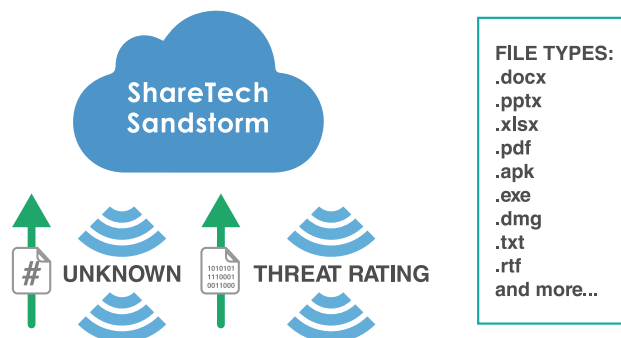
The built-in IPS performs deep inspection of network communications to identify attack behaviors and malicious signatures hidden within protocols and traffic. When anomalies are detected, threats are blocked in real time to prevent intrusion into the internal network.

The optional AI IPS enhances this capability through AI-driven behavioral analysis and threat learning, enabling detection of, zero-day exploits, and abnormal connection activities. By leveraging multi-source threat intelligence, it automatically evaluates risks and provides immediate protection, significantly strengthening overall intrusion defense.

## AI AI Sandstorm (Malicious Programs Filtering System)

The built-in Sandstorm engine provides baseline malware detection and analysis, identifying potential threats embedded in email attachments, compressed files, or web downloads.

The optional AI Sandstorm further enhances protection through advanced behavioral analysis and machine learning techniques, improving detection of unknown malware, phishing attacks, and zero-day threats, thereby elevating the overall security posture.



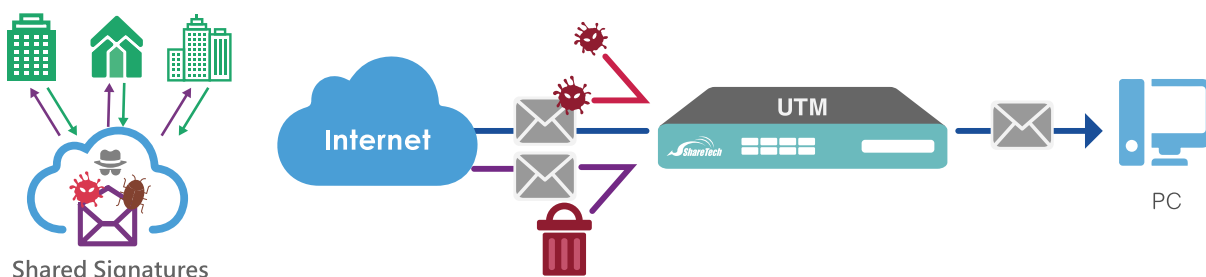
## WAF

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 (RCE) attacks, and webshell uploads to avoid severe consequences.

## Mail Gateway Protection with Advanced Anti-Spam

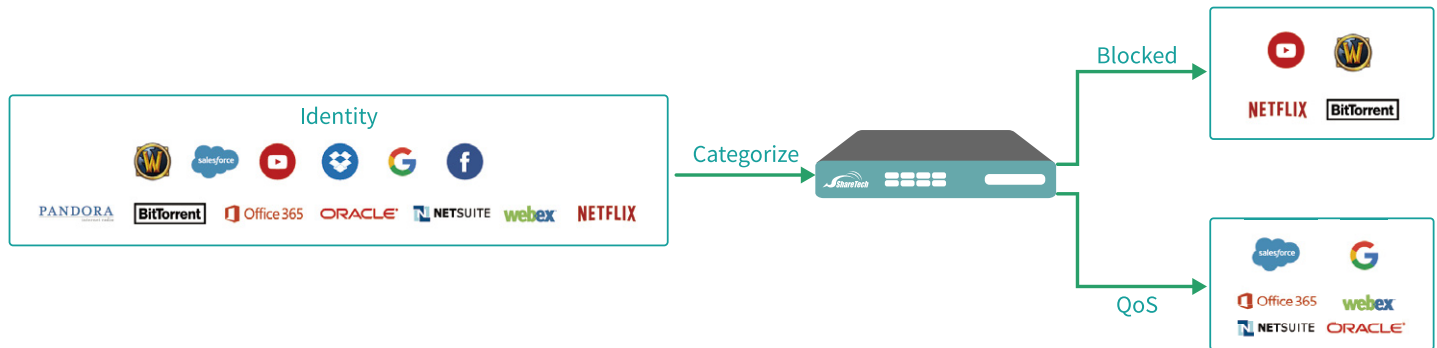
ShareTech NU Series can be deployed as a mail gateway to protect enterprise mail servers from spam, viruses, and malware. It utilizes multiple anti-spam technologies, including IP reputation (ST-IP network rating), Bayesian filtering, spam pattern analysis, fingerprinting, and auto-learning mechanisms. Administrators can define custom filtering policies with allowlist and blocklist controls to enhance filtering accuracy.

Through its shared signature mechanism, spam intelligence identified by one device is automatically shared across the group, improving detection rates and enabling faster response to emerging spam threats. Flexible actions such as forwarding, deletion, and quarantine can be applied to detected messages.



### Advanced Application Control and Database

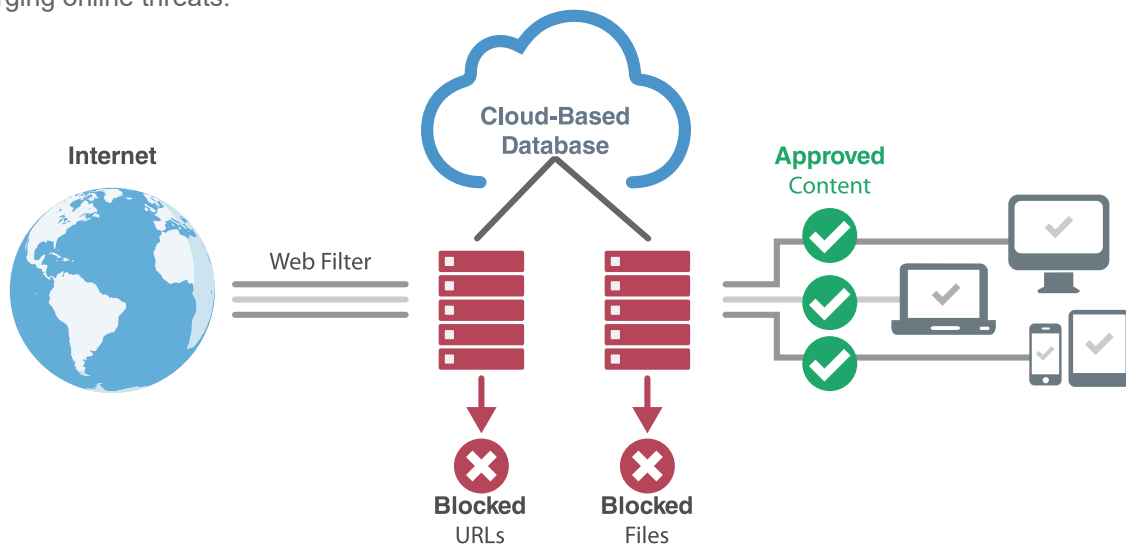
Advanced application visibility and control enable management of cloud services, remote access, messaging, file sharing, and streaming applications—reducing Shadow IT and data leakage risks. Granular policies and continuously updated application intelligence ensure real-time control over emerging applications and threats.



### Advanced URL Control and Database

Leveraging an extensive URL database, the system automatically categorizes websites and identifies associated risks, eliminating the need for administrators to configure rules individually. High-risk or malicious websites are blocked in real time when users attempt to access them.

With continuously updated threat intelligence, the URL database ensures protection remains effective against the latest emerging online threats.

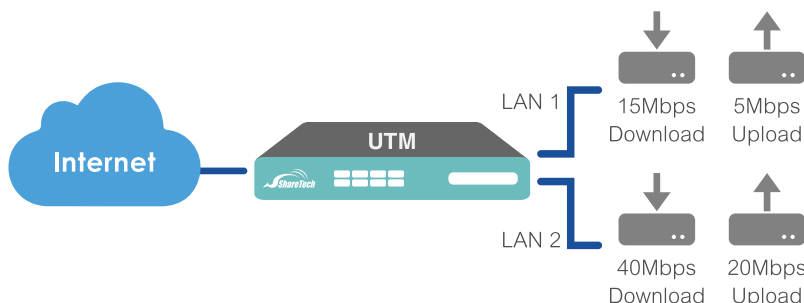


### Co-Defense

Through an intuitive network topology view, IT administrators can visualize the switch architecture and monitor the operational status of each node. The Co-Defense feature prevents attackers from accessing or spreading within the internal network by isolating compromised devices when security threats are detected. 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.

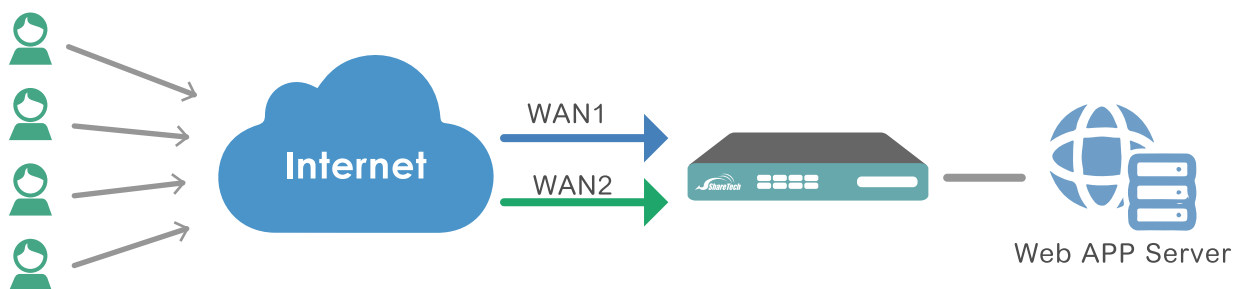
### QoS

QoS offers more flexible 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

NU-840H supports outbound and inbound load balancing, providing businesses with at least 2 WAN links. Multihoming load balancing distributes Internet traffic across multiple WAN links to increase aggregate bandwidth and automatically redirects traffic when a link fails. An additional 4G/5G USB can also be attached to one of the USB ports to add a backup wireless connectivity.



## II. SPECIFICATION

	NU-840	NU-840HH	NU-8060H	NU-8060T
<b>Hardware</b>				
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	4 x Gigabit 4 x 2.5 Gigabit	4 x Gigabit 4 x 2.5 Gigabit 2 x 10G SFP+
Custom ports	5	5	7	9
USB	3.0 x 2	3.0 x 2	2.0 x 2	2.0 x 2
LAN bypass	x	x	● (1 pair)	● (2 pair)
Power consumption	65W	65W	120W	120W
<b>Capacity</b>				
Max firewall throughput	4.2 Gbps	4.2 Gbps	13.8 Gbps	27.2 Gbps
Max. concurrent sessions	2,000,000	2,000,000	3,900,000	3,900,000
New sessions per second	65,000	65,000	100,000	100,000
Anti-virus throughput	750 Mbps	750 Mbps	2 Gbps	2.5 Gbps
IPS throughput	750 Mbps	750 Mbps	3 Gbps	5 Gbps
VPN throughput	650 Mbps	650 Mbps	1.5 Gbps	1.6 Gbps
<b>VPN Tunnels</b>				
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
<b>Network Protection</b>				
Anti-virus engine	ClamAV	ClamAV	ClamAV	ClamAV
ShareTech Anti-virus engine	Optional	Optional	1-Year Subscription Included	1-Year Subscription Included
AI IPS	Subscription	Subscription	1-Year Subscription Included	1-Year Subscription Included
AI Sandstorm	Subscription	Subscription	1-Year Subscription Included	1-Year Subscription Included
Spam filtering & shared signatures	●	●	●	●
Mail audit	Optional	Optional	Optional	●
URL control & database		1-Year Subscription Included		
APP control & database		1-Year Subscription Included		
WAF	●	●	●	●
Geo IP	●	●	●	●
Dashboard	x	Optional	Optional	●
Co-Defense (switch)	●	●	●	●
AP management	100 pcs	100 pcs	100 pcs	100 pcs
Load balance (Out/In)	● / ●	● / ●	● / ●	● / ●
Authentication		POP3, IMAP, RADIUS, Active Directory, LDAP		
2FA	●	●	●	●
High availability	●	●	●	●
VPN	●	●	●	●
SD-WAN	●	●	●	●
Wizard	●	●	●	●
CMS	●	●	●	●
Eye Cloud	●	●	●	●

## II. SPECIFICATION

	NU-8700C	NU-8700F	NU-8700T
<b>Hardware</b>			
Platform size	1U	1U	1U
Recommended users numbers	Under 400	Under 400	Under 400
Ethernet interfaces	14 x Gigabit	6 x Gigabit 8 x 1G SFP	6 x Gigabit 4 x 10G SFP+
Custom ports	13	5 / 8	5 / 4
USB	3.0 x 2	3.0 x 2	3.0 x 2
LAN bypass	•	•	•
Power consumption	220W	220W	220W
<b>Capacity</b>			
Max firewall throughput	18 Gbps	18 Gbps	25 Gbps
Max. concurrent sessions	3,500,000	5,000,000	5,000,000
New sessions per second	170,000	170,000	200,000
Anti-virus throughput	1.2 Gbps	1.2 Gbps	1.5 Gbps
IPS throughput	1.1 Gbps	1.1 Gbps	1.4 Gbps
VPN throughput	2.1 Gbps	2.1 Gbps	2.4 Gbps
<b>VPN Tunnels</b>			
IPSec VPN	6,000	6,000	8,000
PPTP/L2TP/SSL VPN	3,000	3,000	3,000
IP tunnel	1,500	1,500	1,750
<b>Network Protection</b>			
Anti-virus engine	ClamAV	ClamAV	ClamAV
ShareTech Anti-virus engine	1-Year Subscription Included	1-Year Subscription Included	1-Year Subscription Included
AI IPS		Subscription	
AI Sandstorm		Subscription	
Spam filtering & shared signatures	•	•	•
Mail audit	•	•	•
URL control & database		1-Year Subscription Included	
APP control & database		1-Year Subscription Included	
WAF	•	•	•
Geo IP	•	•	•
Dashboard	•	•	•
Co-Defense (switch)	•	•	•
AP management	300 pcs	300 pcs	300 pcs
Load balance (Out/In)	• / •	• / •	• / •
Authentication	POP3, IMAP, RADIUS, Active Directory, LDAP		
2FA	•	•	•
High availability	•	•	•
VPN	•	•	•
SD-WAN	•	•	•
Wizard	x	x	x
CMS	•	•	•
Eye Cloud	•	•	•

## Co-Defense Switch – Supported Models

Brand	Models	
ShareTech	ML-9324E	
Zyxel	GS2210-24	
	GS2210-24HP	
	GS2210-48	
	GS2220-28	
	GS2220-50	
	XGS2210-52	
	XGS3700-24	
	XGS3700-48	
	XGS2210-28	
	XS3800-28	
	GS2220-10HP	
	Cisco	C2960L-24TS-LL
		Cisco3560e
Cisco3750		
PROSCEND	850G-12I	
	850X-28	
Other	Juniper-EX2200	

## AP Management – Supported Models

Brand	Models
Zyxel	NWA50AX
	NWA50AX PRO
	NWA90AX
	NWA90AX PRO
	NWA110AX
	NWA110BE
	NWA130BE
	NWA210AX
	NWA210BE
	WAX510D
	WBE510D
	WBE530
	WAX610D
	WBE630S
	Netgear

## UPS Supported Models

Brand	Models
APC	Smart-UPS 3000
	Back-UPS Pro 700
	Back-UPS 1100
Flight Technic	FT-1000BS
EATON	5E 650

## 3G / 4G / 5G USB Modem – Supported Models

Brand	Models
DLINK	DWM-222 A1
HUAWEI	E3372h
	E161 ( 3G only )
APAL	5G Dongle