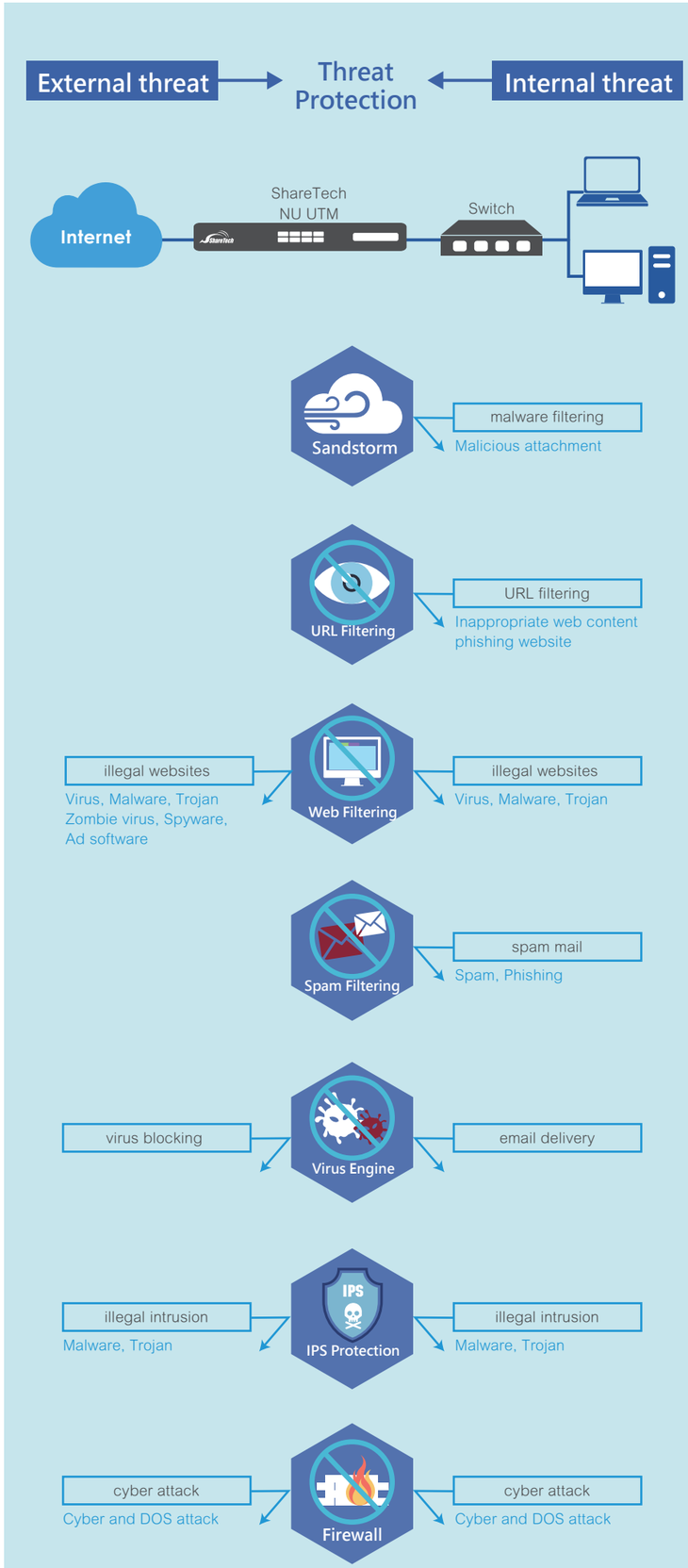


P2P

Files transferred via peer to peer (P2P) can be filtered to detect hidden malware. Administrators can select authorized users and assign their maximum bandwidth and connection sessions.

URL Filtering

Advanced URL database collects millions of URLs and updates every period. All URLs are classified into categories, including Pornography & Violence, Network & Cloud Service, Organizations & Education, Security Risks & Criminal, Life Information, and Others.

Virus Engine

Clam AV is included by default for virus scanning which can detect over millions of viruses, worms, and Trojans. Customers may purchase Kaspersky protection for their security needs.

Anti-Spam

ShareTech Anti-Spam 3.0 integrates a shared signatures mechanism that shares a signature of an early receiver with the rest of the group so that higher spam detection accuracy can be obtained.

IPS Protection

Built-in IPS (intrusion prevention system) inspects the packets from transport to application layer. The security levels (high, medium, or low) combine signature classification.

Firewall

Firewalls ensure legitimate content can pass through while blocking out potential hackers threatening to corrupt business devices.

ShareTech

NEXT-GEN UTM

Exceptional Performance and Consolidated Security Features

The ShareTech NU Series provides simplified security in one box which reduces the risk of cyber threats, enables early detection, and achieves satisfactory recovery. Moreover, ShareTech cloud-based management allows business leaders to focus on business growth and profit maximization.

NU系列規格表

	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	4.8 Gbps	15 Gbps
UTM Throughput	2 Gbps	2 Gbps	3.3 Gbps	10 Gbps
VPN Throughput	650 Mbps	650 Mbps	800 Mbps	850 Mbps
Anti-Virus Throughput	750 Mbps	750 Mbps	600 Mbps	700 Mbps
IPS Throughput	750 Mbps	750 Mbps	650 Mbps	700 Mbps
Max. Concurrent Sessions	2,000,000	2,000,000	3,000,000	3,000,000
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
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				
Gateway security	•	•	•	•
Anti-virus engine	Clam AV	Clam AV	Clam AV	Clam AV
Kaspersky	Optional	Optional	1-year license	1-year license
HTTPS Filtering	•	•	•	•
Spam filtering & shared signatures	•	•	•	•
IPS Database	•	•	•	•
Anomaly IP and flow analysis	•	•	•	•
Sandstorm	•	•	•	•
Mail Audit	Optional	Optional	Optional	•
Advanced URL control & database	1-year license	1-year license	1-year license	1-year license
Advanced APP control & database	1-year license	1-year license	1-year license	1-year license
WAF	•	•	•	•
Geo IP	•	•	•	•
Dashboard		Optional	Optional	•
Remote log server	•	•	•	•
Co-Defense (switch)	•	•	•	•
Load balance (Out/In)	•/•	•/•	•/•	•/•
Virtual server	•	•	•	•
Authentication	•	•	•	•
Firmware update record	x	•	•	•
Auto update & storage status	x	•	•	•
AP Management	100 pcs	100 pcs	100 pcs	100 pcs
High Availability	•	•	•	•
VPN	•	•	•	•
IPSec Tunnel	•	•	•	•
IP Tunnel	•	•	•	•
SD-WAN	•	•	•	•
Wizard	•	•	•	•
CMS	•	•	•	•
Eye Cloud	•	•	•	•

NU系列規格表

	NU-860C	NU-8700C	NU-8700F	NU-8700T	NU-880H
Hardware					
Platform size	1U	1U	1U	1U	2U
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+	18 x Gigabit
Custom ports	13	13	5 / 8	5 / 4	17
USB	2.0 x 2	3.0 x 2	3.0 x 2	3.0 x 2	3.0 x 2
LAN Bypass	•	•	•	•	•
Power Consumption	120W	220W	220W	220W	650W
Capacity					
Max Firewall Throughput	12 Gbps	18 Gbps	18 Gbps	25 Gbps	16.5 Gbps
UTM Throughput	8.4 Gbps	12.6 Gbps	12.6 Gbps	17.5 Gbps	11.5 Gbps
VPN Throughput	850 Mbps	2.1 Gbps	2.1 Gbps	2.4 Gbps	2.5 Gbps
Anti-Virus Throughput	700 Mbps	1.2 Gbps	1.2 Gbps	1.5 Gbps	1.4 Gbps
IPS Throughput	700 Mbps	1.1 Gbps	1.1 Gbps	1.4 Gbps	1.3 Gbps
Max. Concurrent Sessions	3,000,000	3,000,000	5,000,000	5,000,000	6,000,000
New sessions per second	120,000	170,000	170,000	200,000	285,000
Mail scan per day	5,200,000	5,200,000	5,200,000	5,200,000	6,000,000
VPN Tunnels					
IPSec VPN	3,000	6,000	6,000	8,000	10,000
PPTP/L2TP/SSL VPN	1,200	3,000	3,000	3,500	4,000
IP Tunnel	600	1,500	1,500	1,750	2,000
Network Protection					
Gateway security	•	•	•	•	•
Anti-virus engine	Clam AV	Clam AV	Clam AV	Clam AV	Clam AV
Kaspersky	1-year license	1-year license	1-year license	1-year license	1-year license
HTTPS Filtering	•	•	•	•	•
Spam filtering & shared signatures	•	•	•	•	•
IPS Database	•	•	•	•	•
Anomaly IP and flow analysis	•	•	•	•	•
Sandstorm	•	•	•	•	•
Mail Audit	•	•	•	•	•
Advanced URL control & database	1-year license	1-year license	1-year license	1-year license	1-year license
Advanced APP control & database	1-year license	1-year license	1-year license	1-year license	1-year license
WAF	•	•	•	•	•
Geo IP	•	•	•	•	•
Dashboard	•	•	•	•	•
Remote log server	•	•	•	•	•
Co-Defense (switch)	•	•	•	•	•
Load balance (Out/In)	•/•	•/•	•/•	•/•	•/•
Virtual server	•	•	•	•	•
Authentication	•	•	•	•	•
Firmware update record	•	•	•	•	•
Auto update & storage status	•	•	•	•	•
AP Management	100 pcs	300 pcs	300 pcs	300 pcs	Unrestricted
High Availability	•	•	•	•	•
VPN	•	•	•	•	•
IPSec Tunnel	•	•	•	•	•
IP Tunnel	•	•	•	•	•
SD-WAN	•	•	•	•	•
Wizard	•	x	x	x	x
CMS	•	•	•	•	•
Eye Cloud	•	•	•	•	•

ShareTech Information Co., LTD. www.sharetech.com.tw | sales@sharetech.com.tw | help@sharetech.com.tw

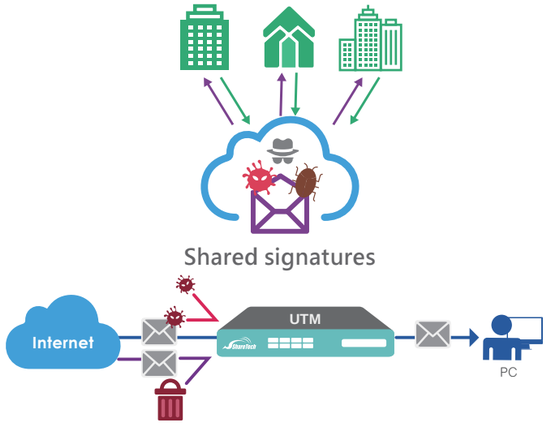
NEXT-GEN UTM FEATURES

Anti-Virus

Clam AV, a built-in a cross-platform anti-virus engine, can detect over 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. The NU Series contains 1-year Kaspersky license. Customers may renew the accurate and reliable Kaspersky anti-virus engine for their security needs.

Anti-Spam and Shared Signatures

The 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 update. Following actions like forward, delete, quarantine can be taken on the mail identified as the spam. Moreover, the shared signatures mechanism shares a signature of an early receiver with the rest of the group so that higher spam detection accuracy can be obtained.

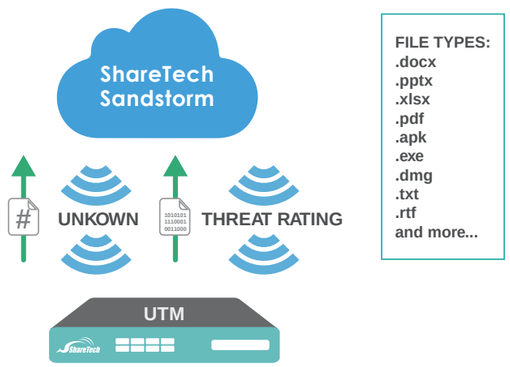


Intrusion Prevention System (IPS)

Built-in IPS inspects the packets from OSI layer 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 IPS security package.

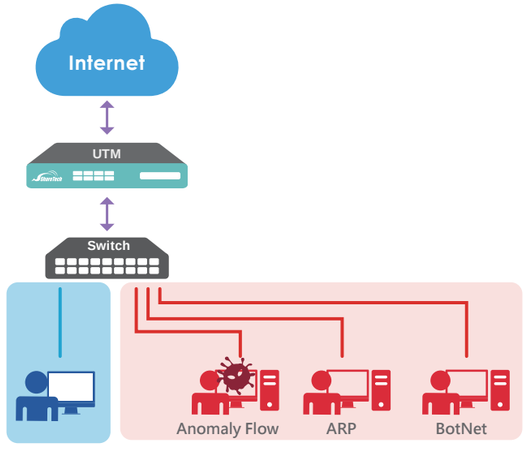
ShareTech Sandstorm Malicious Programs Filtering System

To detect unknown attached files, such as file in Word, Excel, PowerPoint, PDF, ZIP or RAR format, ShareTech Sandstorm system will compare the suspicious files with our database. Threatening emails will be quarantined and will not have the opportunity to affect the operation of the email system.



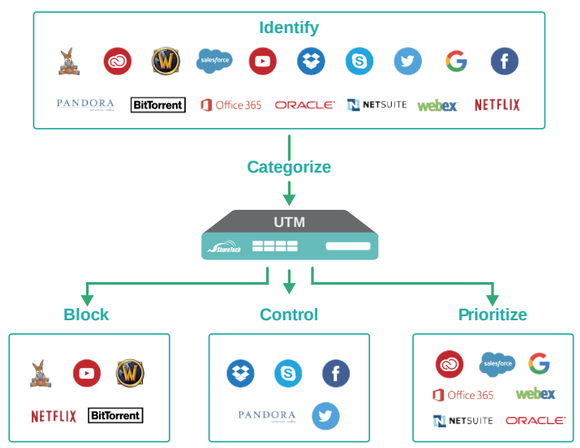
Co-Defense

The NU Series can integrate switches into Co-Defense. The mechanism directly shuts down switch port of infected devices which will slow down internet traffics and helps administrators identify real-time problems, save recourses, and suspend malicious software spreading in the intranet via devices used at work and for other. By using TCP/IP packets capture, infected devices are efficiently located and their paths will be blocked until they return to normal.



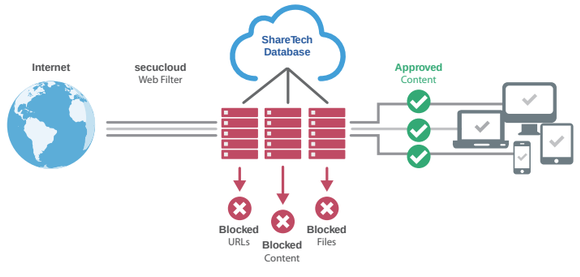
Advanced Application Control and Database

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. The NU Series contains 1-year application license. Customers may renew the license for an instantly updated database.



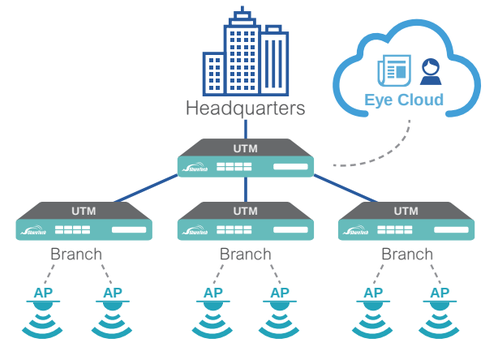
Advanced URL Control and Database

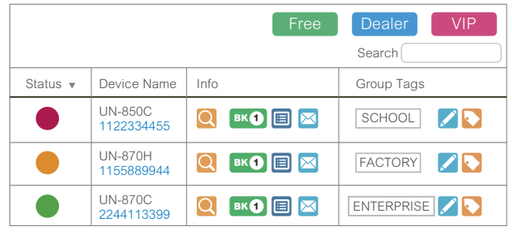
Advanced URL database collects millions of URLs and updates every period. All these URLs and their contents were analyzed and classified, including Pornography & Violence, Network & Cloud Service, Organizations & Education, Security Risks & Criminal, Life Information, and Others. IT administrators can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



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

CMS designed for multi-site network security appliances deployments allows administrators to remotely restart, reboot, and monitor devices. Moreover, Eye Cloud, a cloud service platform, provides users 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. When an anomaly occurs, administrators will be notified of the problem.





Log Analysis and CEF format

Most organizations and businesses are required to do data logging and log analysis as part of their security and compliance regulations.The NU Series provides log analysis that helps in reducing problem diagnosis, resolution time and ineffective management of applications and infrastructure. Common Event Format (CEF) format is supported and administrators can view the logging using a log management solution like Graylog.

User Name	IP	Sessions	Upload (bits)	Download (bits)	Record
PETER-H55M-UD2H	192.168.186.50	178	0	0	Record
192.168.186.70	192.168.186.70	107	0	0	Record
192.168.189.29	192.168.189.29	83	22.38K	33.4K	Record
syncs	192.168.189.21	78	2.7K	910	Record
192.168.189.19	192.168.189.19	65	0	0	Record

The Threat Intelligence Center

1 Management
An easy way to switch back to the management GUI.

2 Threat Intelligence
The bar chart indicates the amount of different threats at the designated time, while the pie chart illustrates the proportion. Admins can view the most common 6 types of threats arranged in rank order according to amount.

3 Applications
The line chart compares uploading and downloading flows over the last 24 hours, while the pie chart illustrates the proportion. Admins can view flows arranged in rank order according to application type and IP address.

4 Sessions
The chart shows total numbers of active user sessions, while the pie chart illustrates the proportion. Admins can view sessions arranged in rank order according to application and IP address.

5 Defense
The line chart compares defense between recent 2 weeks at the designated time, while the pie chart illustrates the proportion. Admins can view defense arranged in rank order according to defense type and IP address.

6 IPS
The bar chart indicates the amount of IPS protection in 3 different security levels at the designated time, while the pie chart illustrates the proportion. Admins can view the IPS protection arranged in rank order according to security level, IP address, and event.

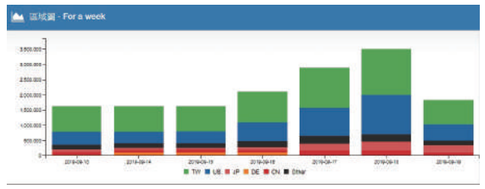
7 Web
The bar chart indicates the amount of HTTP and HTTPS flows at the designated time, while the pie chart illustrates the proportion. Admins can view the flows arranged in rank order according to domain and IP address.

8 Web Control
The bar chart indicates the amount of virus and URL listing at the designated time, while the pie chart illustrates the proportion. Admins can view the web control arranged in rank order according to virus, URL type, and IP address.

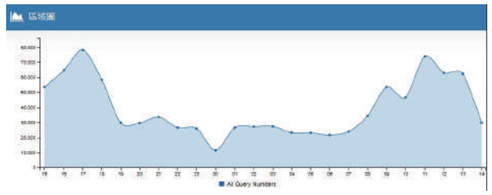
9 Mail
The line chart indicates the amount of email delivery at the designated time, while the pie chart illustrates the proportion. Admins can view email delivery arranged in rank order according to mail/IP address, domain, spam, virus, etc.

10 Application Control
The line chart indicates the amount of applications at the designated time, while the pie chart illustrates the proportion. Admins can view application control arranged in rank order according to type, IP address, and group.

11 IP Location
The bar chart indicates the amount of IP from different locations at the designated. Admins can view the IP location arranged in rank order according incoming and outgoing directions.



12 DNS Query
The line chart indicates the amount of DNS query at the designated time. Admins can view DNS query arranged in rank order according to domain and IP address.



13 Statistics 14 Reports
Admins can create custom statistics and generate reports based on their needs.