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

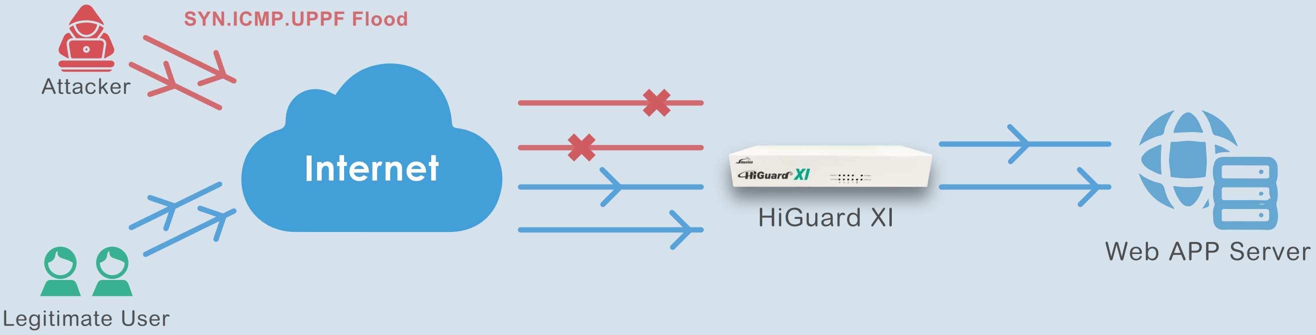
ShareTech HiGuard Series offers an all-around security appliance best suited to deployments in retail stores, branch offices, and smaller business environments. 4 Gigabit ports provide Gigabit Ethernet connectivity for users under 50. The desktop security solution has high-reliability storage and memory 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.

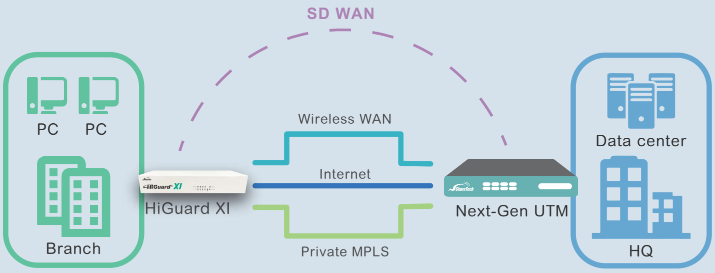


QoS

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.

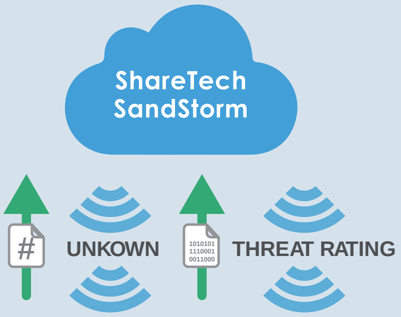
SD WAN

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

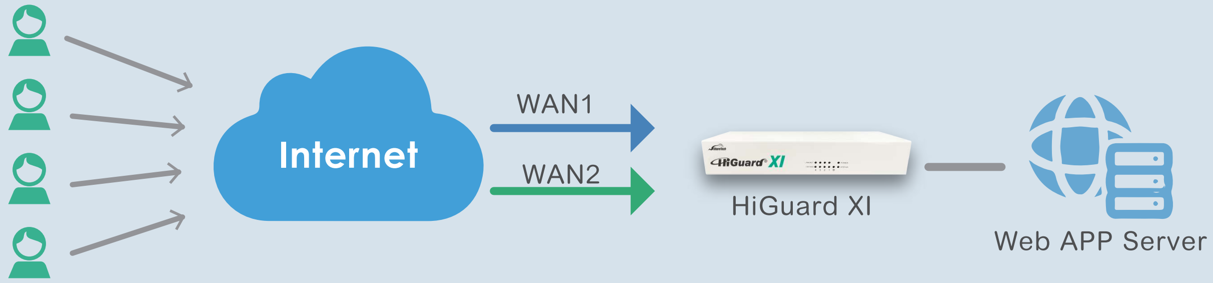
To detect unknown attached files, such as Word, Excel, PowerPoint, PDF, ZIP or RAR format. Threatening emails will be quarantined and will not have the opportunity to affect the operation of the email system. HiGuard Series supports Sandstorm IP that compares suspicious files with our database.



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)

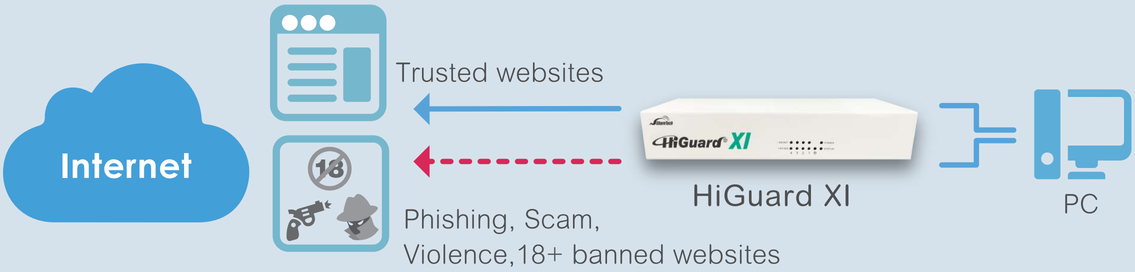
- Supports IPSec, PPTP, L2TP, SSL, and GRE Tunnel
- Supports DES, 3DES, AES, AES128, AES192, and AES256 encryption and SHA-1, SHA256, SHA512, and MD5 authentication algorithms
- SSL VPN mobility client for Android and Apple iOS
- Controls connectivity of remote sites from the central site

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)

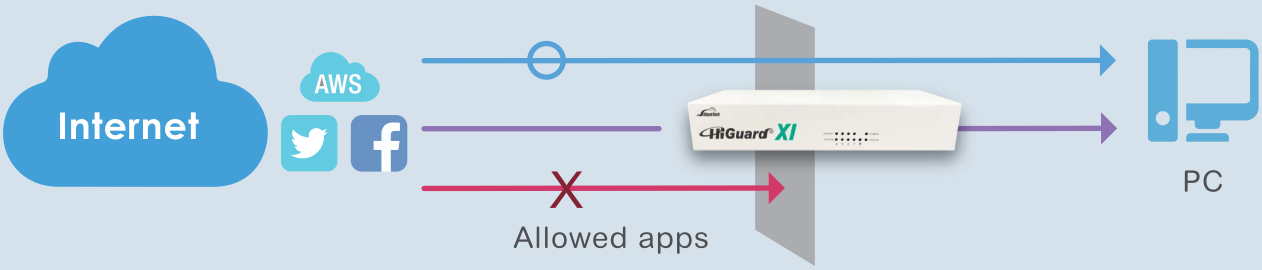
URL Database (1-year license)

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.



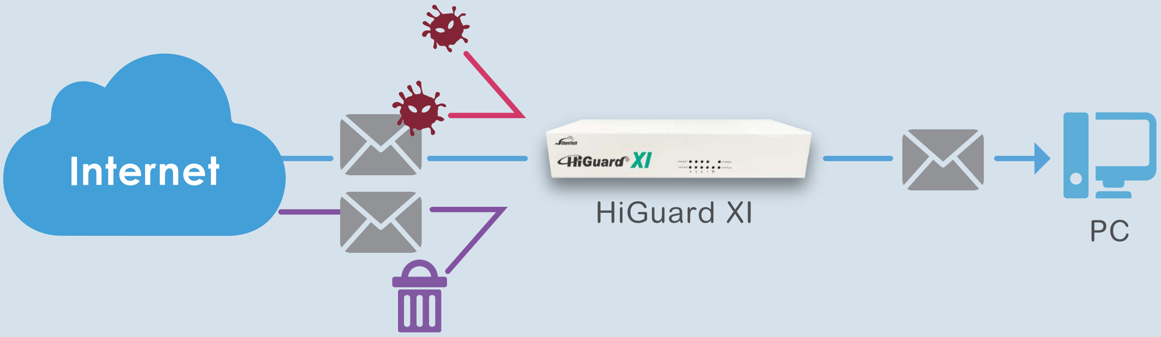
Application Control (1-year license)

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.



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.



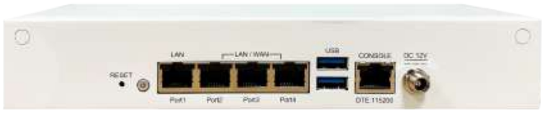
Intrusion Prevention System (IPS) HiGuard XI Security Solutions

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

Back View



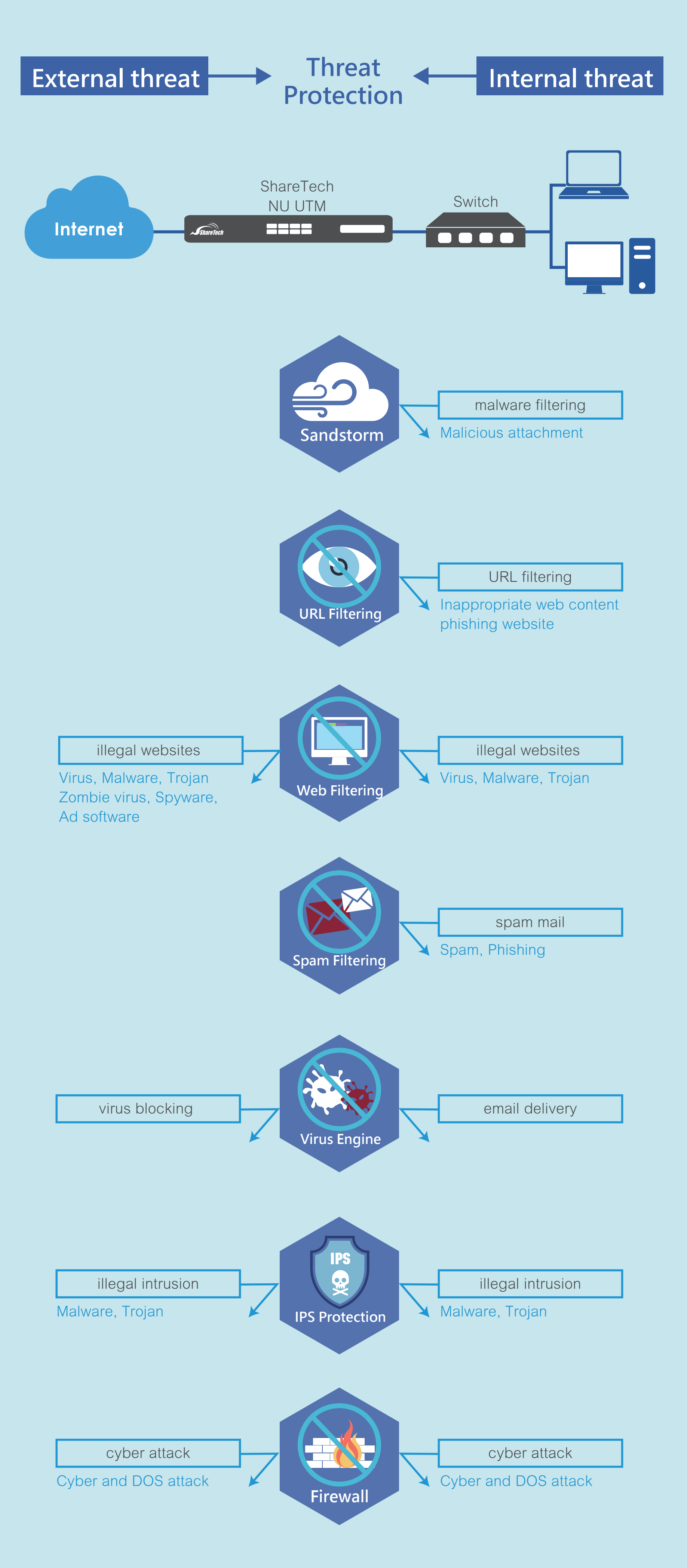
Physical specifications

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

Performance

Performance	
Firewall throughput	1.9 Gbps
Concurrent connections	200,000
New connections/sec	49
VPN throughput	380 Mbps
Anti-virus 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



External threat → Threat Protection ← Internal threat

Internet — ShareTech NU UTM — Switch

Sandstorm: malware filtering — Malicious attachment

URL Filtering: URL filtering — Inappropriate web content phishing website

Web Filtering: illegal websites — Virus, Malware, Trojan Zombie virus, Spyware, Ad software | illegal websites — Virus, Malware, Trojan

Spam Filtering: spam mail — Spam, Phishing

Virus Engine: virus blocking | email delivery

IPS Protection: illegal intrusion — Malware, Trojan | illegal intrusion — Malware, Trojan

Firewall: cyber attack — Cyber and DOS attack | cyber attack — Cyber and DOS attack

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.

Malicious Traffic Protection

NU Series protects business against Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, and ICMP Fragment.

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

A UTM unit can operate in one of two modes: Transparent or NAT/Route mode. Moreover, Port Address Translation (PAT) is supported to conserve IP addresses.

ShareTech

NEXT-GEN UTM

Exceptional Performance and Consolidated Security Features

DASHBOARD AND REPORTS

CLOUD MANAGEMENT

DATA LOSS PREVENTION

ClamAV KASPERSKY lab ANTI-VIRUS

SANDSTORM

L2 / L3 SWITCHING

Internet VPN

IPS AND RANSOMWARE

APP WWW ADVANCED URL/APP DATABASE

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-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	•	•	•	•

	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	•	•	•	•	•

✱ NU-8800T supports Power Supply Redundant.

V2024.02

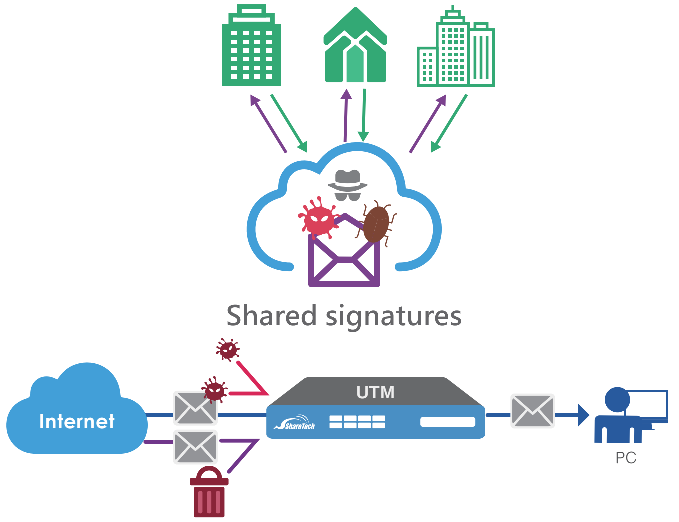
NEXT-GEN UTM FEATURES

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.

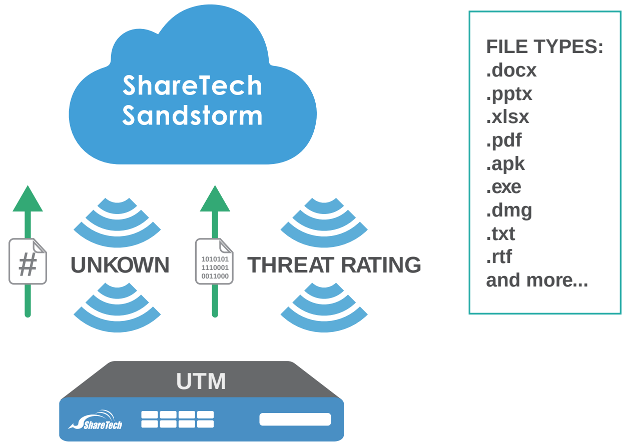


Intrusion Prevention System (IPS)

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.

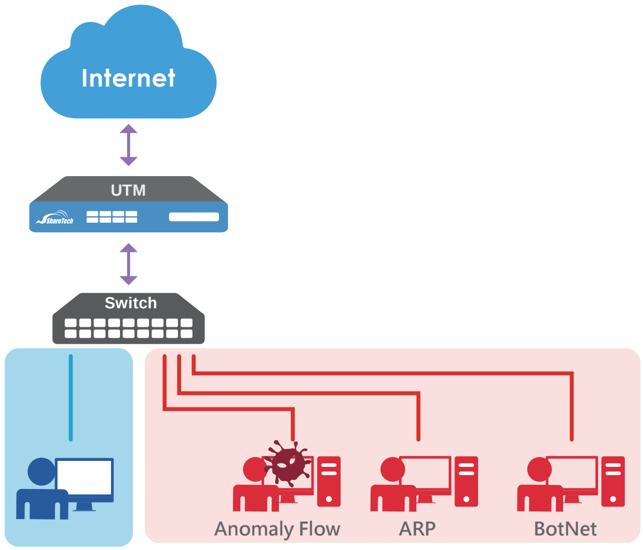
ShareTech Sandstorm
Malicious Programs Filtering System

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.



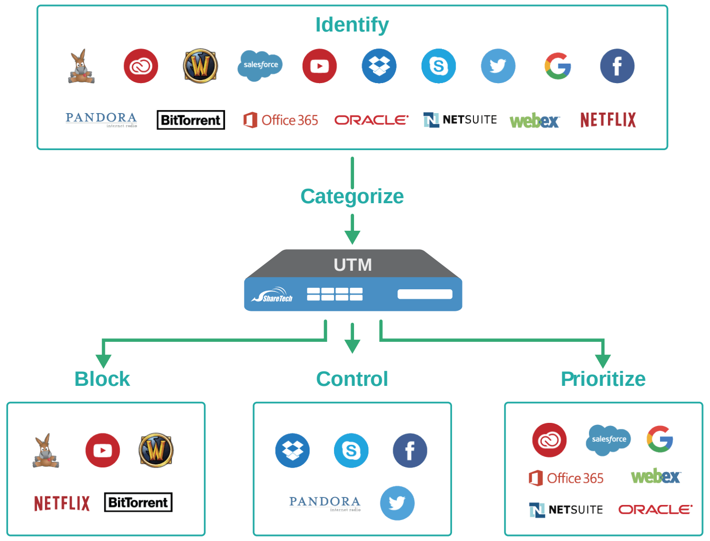
Co-Defense

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.



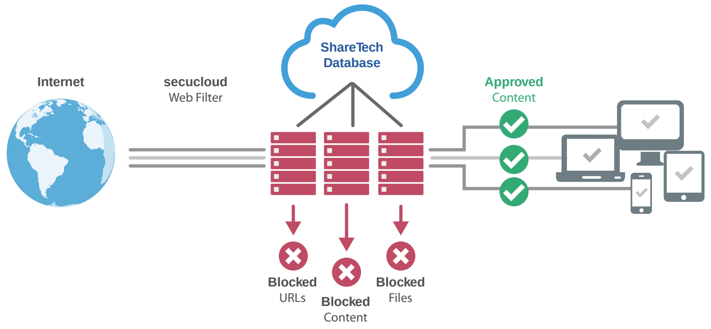
Advanced Application Control and Database

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.



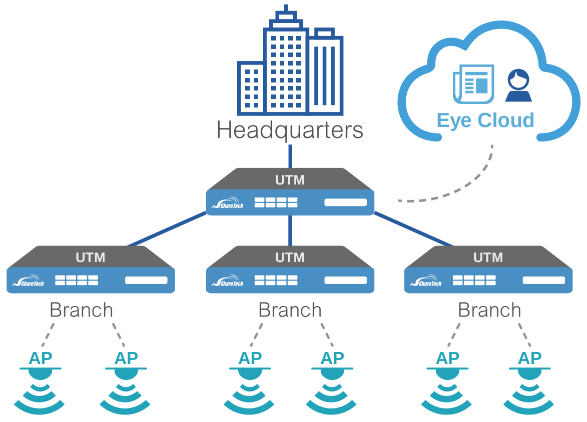
Advanced URL Control and Database

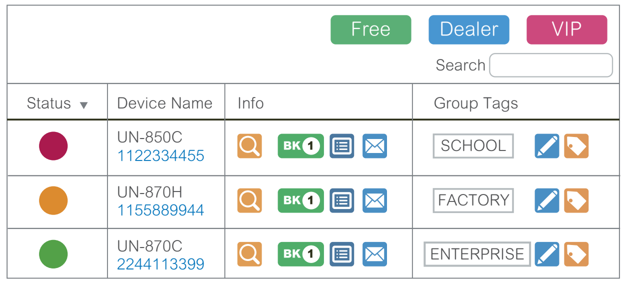
Advanced URL database collects millions of URLs and updates every period. All these URLs and their contents were analyzed and classified, including Pornography & Violence, Network & Cloud Service, Organizations & Education, Security Risks & Criminal, Life Information, and Others. IT administrators can 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.

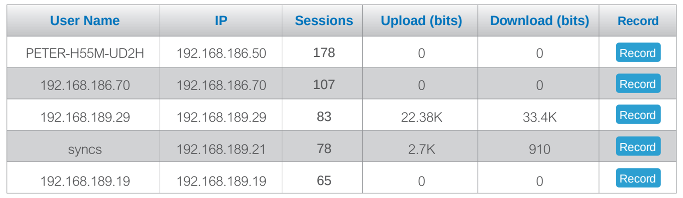




Status ▾	Device Name	Info	Group Tags
●	UN-850C 1122334455	BK 1	SCHOOL
●	UN-870H 1155889944	BK 1	FACTORY
●	UN-870C 2244113399	BK 1	ENTERPRISE

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

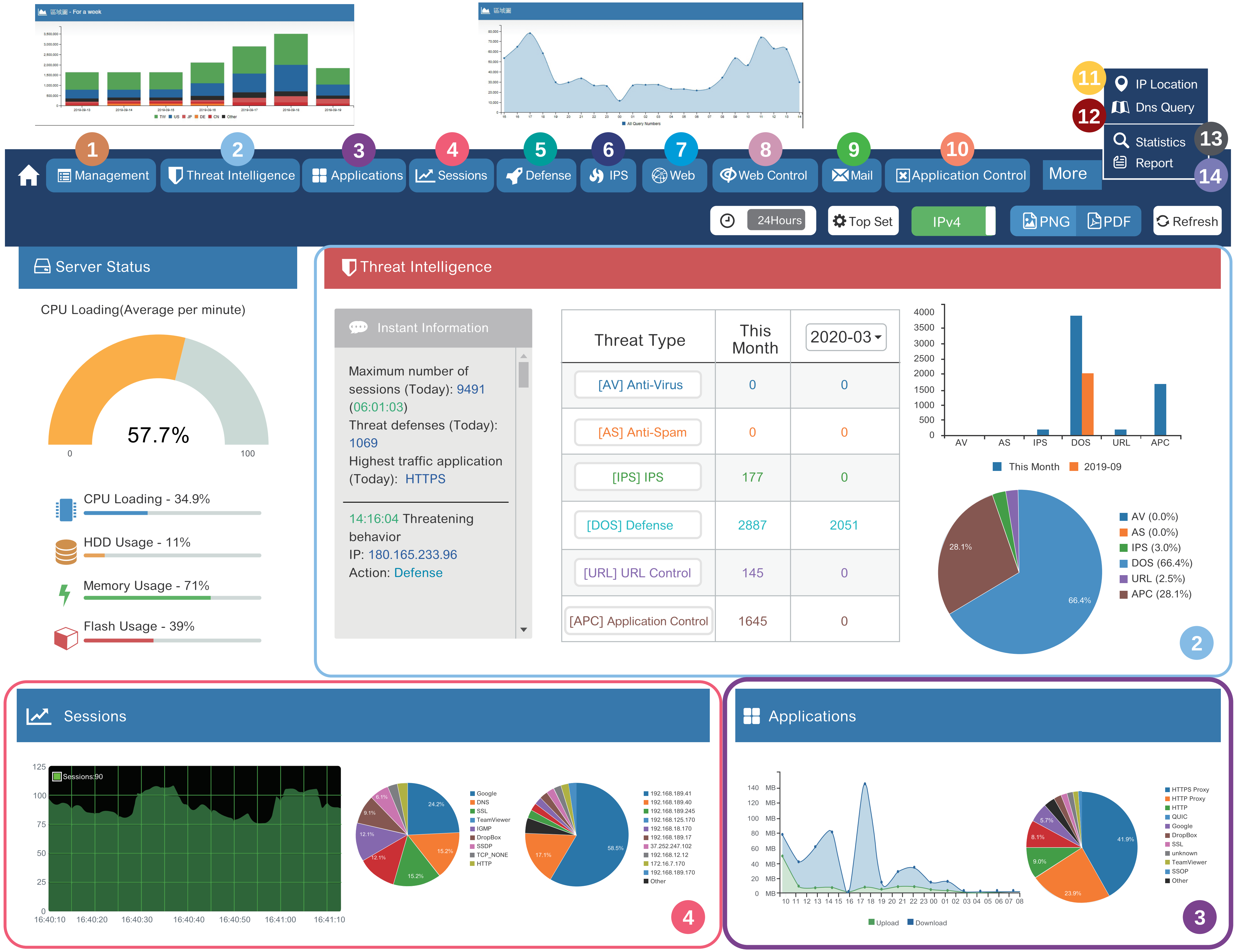
The bar chart indicates the amount of IP from different locations at the designated. Admins can view the IP location arranged in rank order according incoming and outgoing directions.

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.



Maximum number of sessions (Today): 9491 (06:01:03)
Threat defenses (Today): 1069
Highest traffic application (Today): HTTPS

14:16:04 Threatening behavior
IP: 180.165.233.96
Action: Defense

Threat Type	This Month	2020-03
[AV] Anti-Virus	0	0
[AS] Anti-Spam	0	0
[IPS] IPS	177	0
[DOS] Defense	2887	2051
[URL] URL Control	145	0
[APC] Application Control	1645	0

Specifications

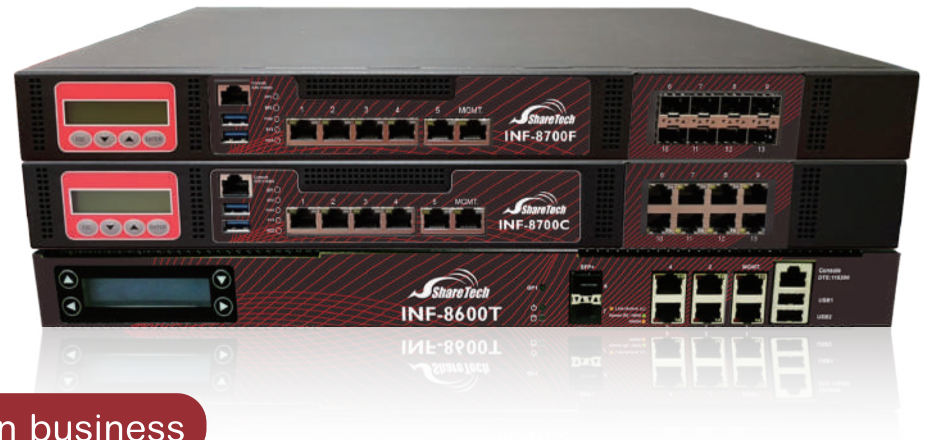
Model	INF-8400H	INF-8600T	INF-8700C	INF-8700F
Interfaces				
Form Factor	1U	1U	1U	1U
Memory	4G RAM	8G RAM	8G RAM	8G RAM
HD	240G SSD	480G SSD	480G SSD	480G SSD
I/O Ports	6 x Giga Ports	6 x Giga Ports 2 x 10G Fiber Ports	14 x Giga Ports	6 x Giga Ports 8 x 1G Fiber Ports
Watchdog Bypass	O	O	O	O
LAN Bypass	1 pair	1 pair	2 pairs	2 pairs
Supported Mode	Bridge	Bridge	Bridge	Bridge
Applicable Environment	Under 50	Under 100	Under 200-300	Under 200-300
System Performance				
Firewall Throughput	4.2 Gbps	9 Gbps	13 Gbps	13 Gbps
Concurrent Sessions	2,000,000	2,000,000	3,000,000	3,000,000
New Sessions/Second	65,000	120,000	350,000	350,000
Threat Protection Throughput (IPS, Anti-Virus, and Web Filtering)	900 Mbps	900 Mbps	1,200 Mbps	1,200 Mbps
Anti-Virus Throughput (bidirectional)	750 Mbps	1,300 Mbps	1,600 Mbps	1,600 Mbps
IPS Throughput	600 Mbps	1,000 Mbps	1,200 Mbps	1,200 Mbps
Software Security				
Virus Engine(s)	ClamAV & Optional Kaspersky	ClamAV & 1-year Kaspersky	ClamAV & 1-year Kaspersky	ClamAV & 1-year Kaspersky
FTP Virus Scan	O	O	O	O
Spam Filtering	O	O	O	O
Mail Audit	O	O	O	O
IPS	O	O	O	O
WAF	O	O	O	O
Sandstorm	O	O	O	O
Application Control	1-year	1-year	1-year	1-year
URL Database	1-year	1-year	1-year	1-year
Anomaly Flow Analysis	O	O	O	O
Co-Defense (Switch)	O	O	O	O
AP Management	O	O	O	O
Intranet Protection	O	O	O	O
Geo IP	O	O	O	O
Network Testing Tools	O	O	O	O
Logging	O	O	O	O
QoS	O	O	O	O
Offline Update	O	O	O	O
Dashboard	Optional	O	O	O
UPS	O	O	O	O
Eye Cloud/CMS (Client)	O	O	O	O

2023.04

ShareTech

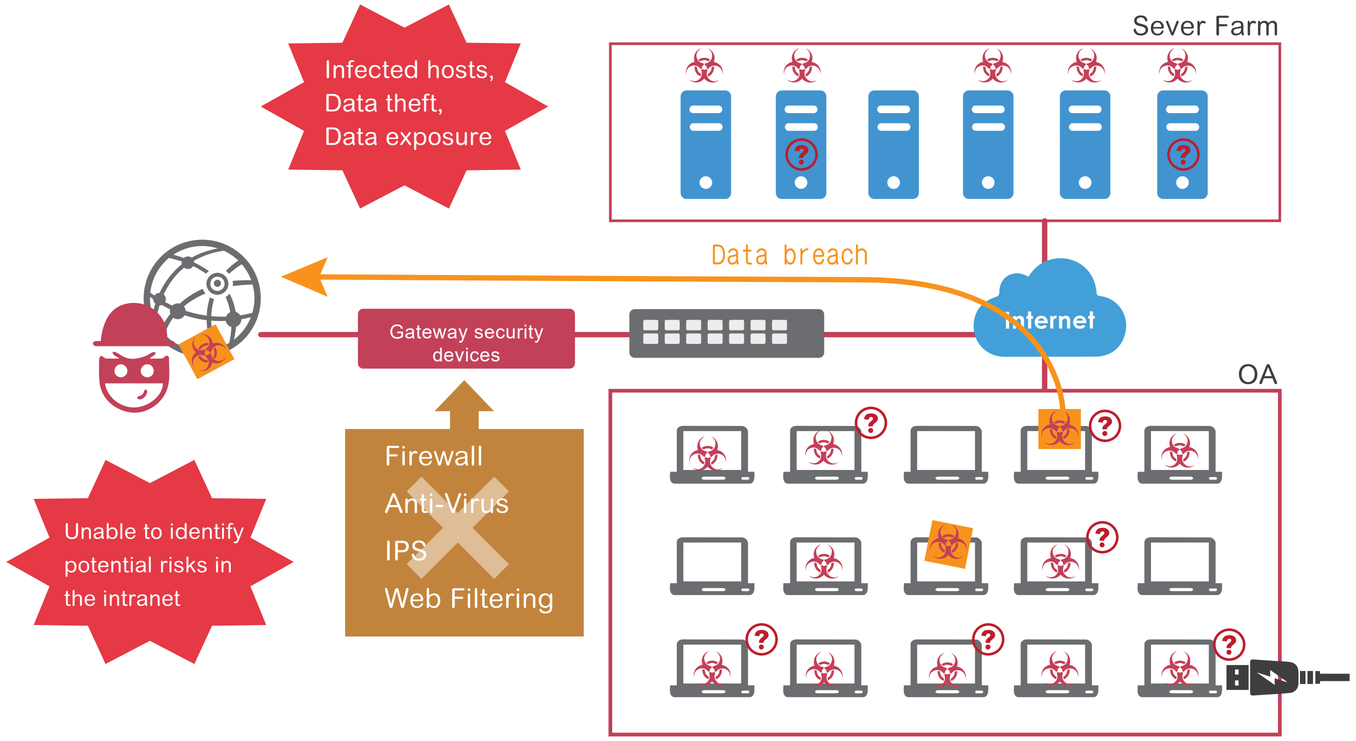
Internal Firewall

INF Series



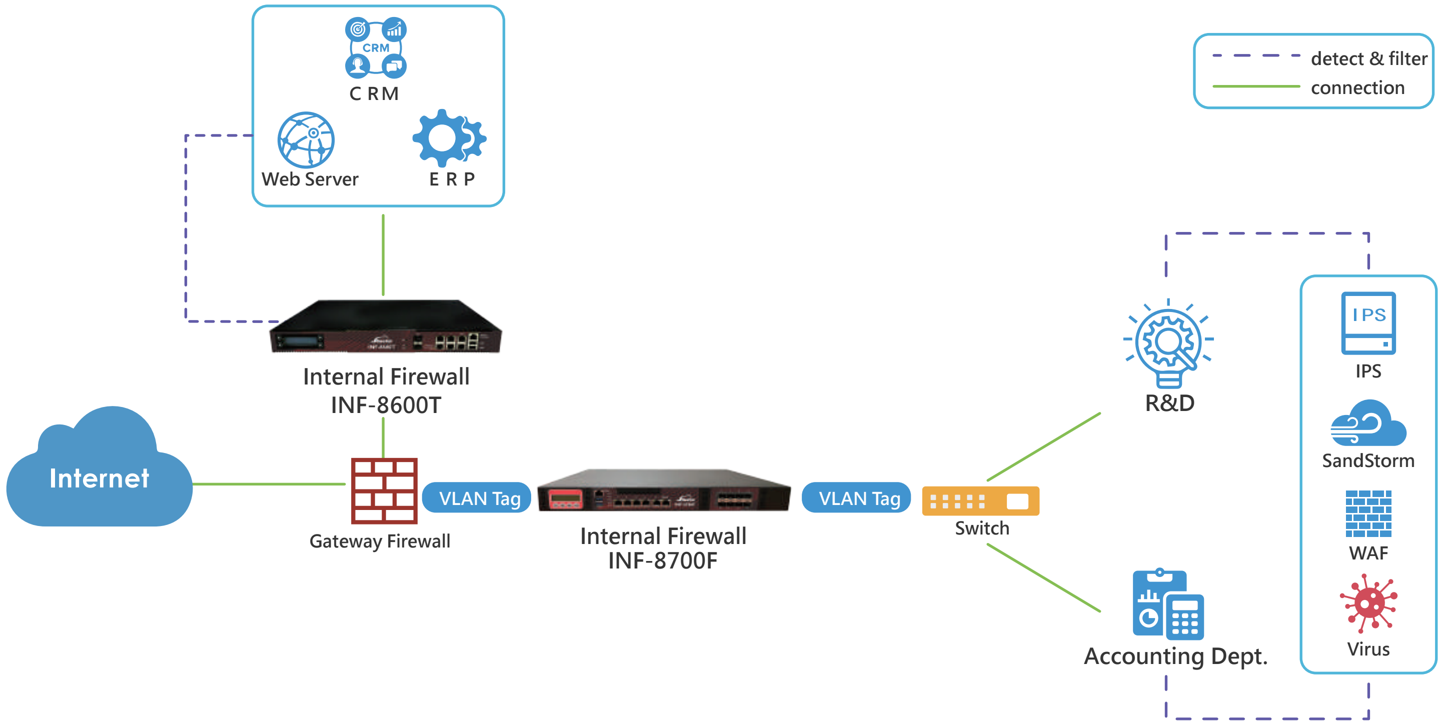
Various intranet security threats in business

- The intranet would never be 100% safe, and your network might have been hacked
- Ineffective response to any cyber incidents
- Malware-Infected Servers
- Lack of network segmentation
- Relatively less secure wireless network
- Weaker integration within collaborating and sharing
- Failure to patch the vulnerability
- Lack of visibility into processes and applications



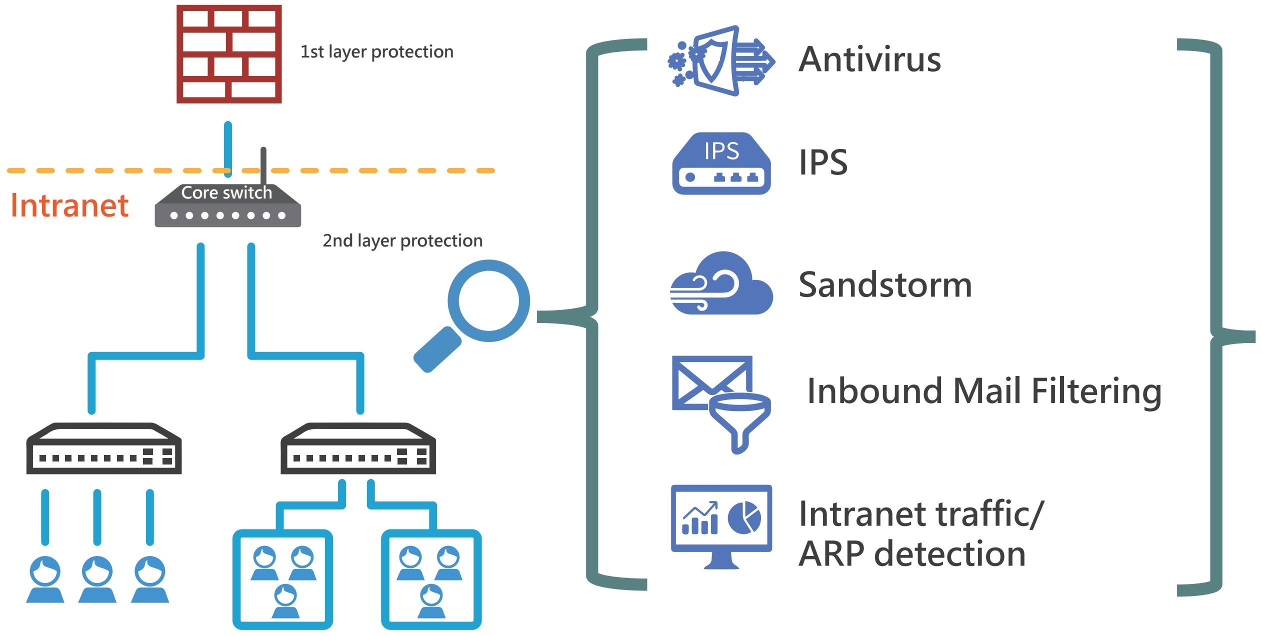
ShareTech internal firewall decreased intranet security risks.

ShareTech intranet firewall (INF Series) has a unique combination that allows businesses to stay ahead of intranet attacks, detect-and-response to threats, and collaborate effectively in other networking peripherals. Aside from regular next-generation firewalls designed to detect and combat attacks across the entire network, ShareTech INF Series ensures a network is protected from the inside out, providing higher visibility, spotting relevant attacks, and collecting all suspicious security events.



I. Minimize the possibility of a zero-day attack

Most network appliances are used as a border defense that analyzes packets, isolates an organization's internal network, and assumes nothing got past the firewall. However, infections in the intranet may not be detectable, so that malware might have been spreading throughout an organization. ShareTech INF Series can detect anomaly-based behaviors in the internal network environment. By using anti-virus engines, IPS, WAF, and Sandstorm, malicious activities can either get responded to appropriately or banned proactively.

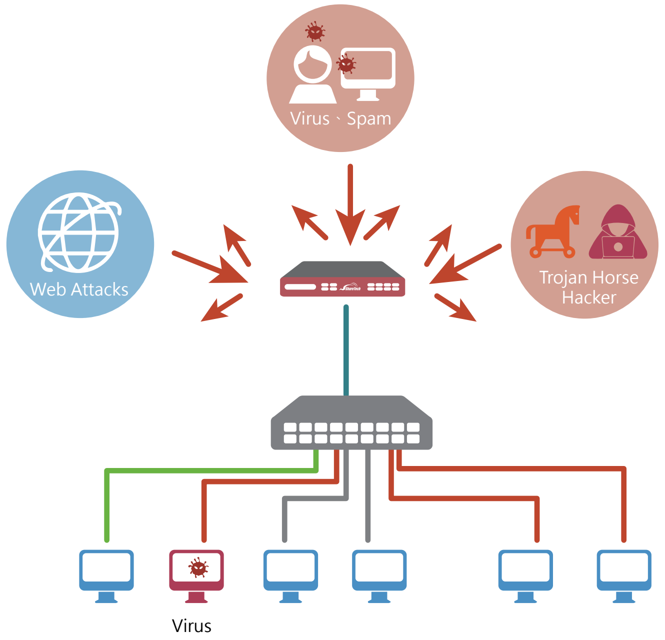


II. Secure vitally important and dedicated servers

ShareTech INF Series can perform scans and detect many security vulnerabilities in web applications, such as cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection, among others. To perform in-depth detection, ShareTech INF Series has a built-in web application firewall (WAF), a protocol layer 7 defense, is a type of reverse proxy that protects critical servers from exposure. It operates through policies that aim to protect against vulnerabilities in the application by filtering out malicious traffic. Meanwhile, users can maintain speed and ease.

III. Guard intranet security with switches

Once any abnormal behavior gets detected in protected segments, ShareTech INF Series will actively block all packets to/from the source of infection and isolate associated traffics going through the network segment. At the same time, collected data will be displayed and expressed visually, allowing IT administrators to analyze the data further and see if it is a malicious hacking attack. Moreover, by integrating with switches, IT administrators can clearly understand the switch architecture deployment and the usage status of each node via the network topology.



IV. Gain a comprehensive overview of dashboard reporting

Built-in ShareTech Dashboard is specially designed for intranet security. Loggings and event data of the device can be simplified and centralized for analysis, collection, storage, query, and reporting. IT administrators can inspect and search all traffics for enhanced security and define possible risk sources or suspicious activities through event correlation.

Important Dashboard Features

- ■ Monitor network traffics and analyzes threats
- ■ Support flow-generated Syslog
- ■ Track events
- ■ Collect and correlate logs for queries
- ■ Gain complete visibility of the whole system

SPECIFICATIONS

產品型號		MS-6400X	MS-6410X	MS-6420X	MS-6430X	MS-6440L
Hardware						
RAM		4G	4G	4G	8G	16G
HD Space		500G	1TB	1TB	2TB	2TB*3
Mounting		1U	1U	1U	1U	1U
LCM			•	•	•	
Network Interface		LAN/HA	LAN/HA	LAN/HA/iSCSI 2*10G	LAN/HA/iSCSI	LAN/HA
Capacity						
Max. Licensed Users		Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Max. Email Delivery		2,100,000	4,500,000	5,800,000	9,200,000	12,400,000
Recommended Number of Users		Under 100	Under 200	Under 200	Under 400	600 - 1,000
Software						
Basic Setup	Multiple Domains	•(5)	•	•	•	•
	Email Migration	•	•	•	•	•
	Send Large Files with Hyperlinks	•	•	•	•	•
	SMTP Proxy	X	X	•	•	•
	Email Encryption	X	X	PDF/ZIP	PDF/ZIP	PDF/ZIP
	Mail Gateway	X	•	•	•	•
	Email Auth.	X	•	•	•	•
	POP3 Proxy (Admin./Users)	(•/X)	(•/X)	(•/5)	(•/10)	(• /Unrestricted)
	Firewall	•	•	•	•	•
Anti-Virus	Clam AV	•	•	•	•	•
	Kaspersky	Optional	Optional	Optional	Optional	1-year license
Spam Filtering	Greylisting	•	•	•	•	•
	IP Reverse	•	•	•	•	•
	URL Filtering	•	•	•	•	•
	Auto-Learning	•	•	•	•	•
	Shared signatures	•	•	•	•	•
	DKIM&SPF Auth.	•	•	•	•	•
	Sandstorm	X	X	•	•	•
Mail Audit	Mail Record	•	•	•	•	•
	Content Filtering	•	•	•	•	•
	Audit Setting	Optional	•	•	•	•
	Personal Information Filtering	Optional	Optional	•	•	•
	Pre-and-Post Auditing	•	•	•	•	•
Account	Application & Group Management	•	•	•	•	•
	Role-Based Management	•	•	•	•	•
	Create Email Accounts (Host/AD/LDAP)	•	•	•	•	•
Backup	FTP/Samba/USB	•	•	•	•	•
	iSCSI	X	X	•	•	X
Log		•	•	•	•	•
Statistical Report		Optional	•	•	•	•
Management	SSL Certificates	•	•	•	•	•
	Disaster Recovery	•	•	•	•	•
	UPS	•	•	•	•	•
	HA / Off-Site Backup	(•/X)	(•/Optional)	•/•	•/•	•/ •
	Hard Disk Health Check	•	•	•	•	•
	Web Server	X	•	•	•	•
	Distributed Architecture	Sub only	Sub only	Core & Sub	Core & Sub	Core & Sub
	E-paper	Optional	•	•	•	•
Webmail	Quota (Max. 100G)	10GB	10GB	30GB	30GB	100GB
	2-Step Verification (Line & Email)	X	•	•	•	•
	Auto-Reply/Forward/ Delayed Delivery	•	•	•	•	•
	Google Calendar Sync.	Optional	Optional	•	•	•
	Cloud HDD	•	•	•	•	•
	Shared File Links	•	•	•	•	•
	Bulletin Board/Calendar	•	•	•	•	•
	Personal Mail Rules	•	•	•	•	•
	Mail Retrieve	•	•	•	•	•
	Mail APP(iOS&Android)	•	•	•	•	•

ShareTech

SHARETECH HARDWARE-BASED MAIL SERVER

INCREASED EFFECTIVENESS OF MAIL SECURITY

- Supports on 64-bit OS 3.0, x86 server platform
- Employs multi-layered spam filtering
- Clam AV and additional Kaspersky
- Shared spam signature
- Email encryption and certified email

RECORD-BASED MAIL BACKUP AND RESTORE

- Supports POP3 and IMAP protocols
- External USB hard drives backup
- Distributed architecture
- Disaster recovery system
- HA and Offsite Backup
- UPS graceful shutdown

COMPLETE SEAMLESS SOLUTIONS

- Mail APP available on iOS and Android
- Easy access to Cloud HDD
- Sync contacts and calendar with Outlook and iPhone
- Marketing digital e-paper

MAIL TRAFFIC AUDITING AND MONITORING

- Content-level filtering
- Specific group policies for departments
- Multiple filtering mechanisms
- Policy-based email auditing for in/outbound email

COMPETENT SYSTEM MANAGEMENT

- Automatic backup and fast lookup
- Scheduled statistic report
- Easy access to Cloud HDD
- Role-based administration
- Cloud-based service system (Eye Cloud)

KEY FEATURES & BENEFITS

I. SYSTEM MANAGEMENT

Mail Firewall

Inbuilt firewall manages and filters all inbound and outbound email traffic to protect organizations from email-based threats. Added detections such as anomaly flow, authentication failures, and sender confirmation deliver deeper levels of protection for defeating today's increasingly complex attacks.

Hassle-Free Mail Migration

Existing user accounts and email can be imported within a few minutes without worries of message loss due to human errors or domain migration. Administrators can create users accounts automatically, manually or integration with AD servers.

POP3 Proxy

ShareTech mail server acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP, and Webmail access.

Statistics Reports

A scheduled statistic report can include Top N traffics, POP3 traffic, personal information, mail distribution, quarantined messages, worst passwords ranking, sources of spam mail, etc. Administrators can modify reporting properties and customize display of reports for your business requirements.

Signature Line (Email Disclaimer)

Automatically add company signature line and email disclaimer on outgoing email. Different domains can set up different content. Besides, administrator can also set up the accounts and IPs that do not follow the setting.

II. BACKUP AND RECOVERY

System Backup and Disaster Recovery

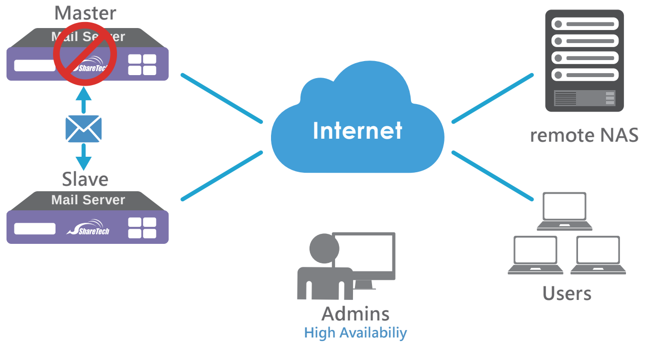
Users can restore the configuration files to a USB drive. When regular operations are interrupted, a disaster recovery operation can be performed. If the mail server does not boot from the installed image, it can be booted using a USB drive. Moreover, when the mail server is operating normally, the installed image can be upgraded by performing a USB boot operation.

Mail Record and Backup

Incoming and outgoing mail including attachments will be automatically and timely backed up to a local disk, the network neighborhoods or a remote FTP server. Administrators can easily monitor email traffics by searching for keywords and reasons behind blocking.

High Availability (HA)
Off-site/Cloud Backup

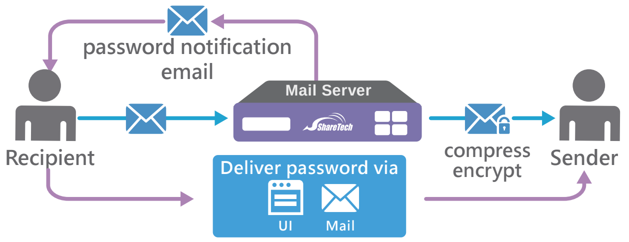
ShareTech mail server offers additional survivability-never-fail network. Off-site backup is also available to store backup data external to the core IT environment. The slave server will take over the master server to ensure email service continuity once device failure occurs. Overall, three backup options are provided to maintain the smooth email delivery process.



III. MAIL SECURITY AND FILTERING

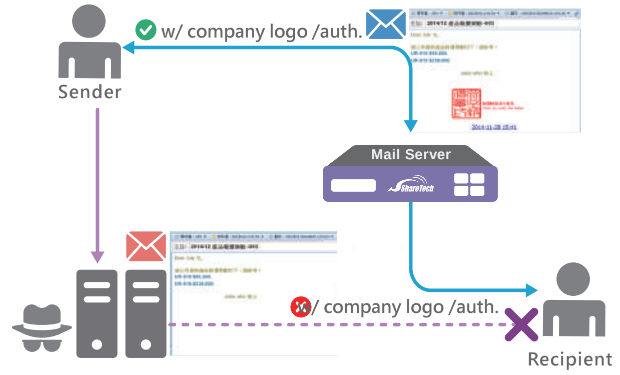
Email Compression and Encryption

Administrators may select users to convert .eml mail messages to PDF files or simply encrypt and compress email attachments to protect sending sensitive data over email. Recipients can use a permissions password to access the file and view the original email and its attachment(s) in PDF Reader.



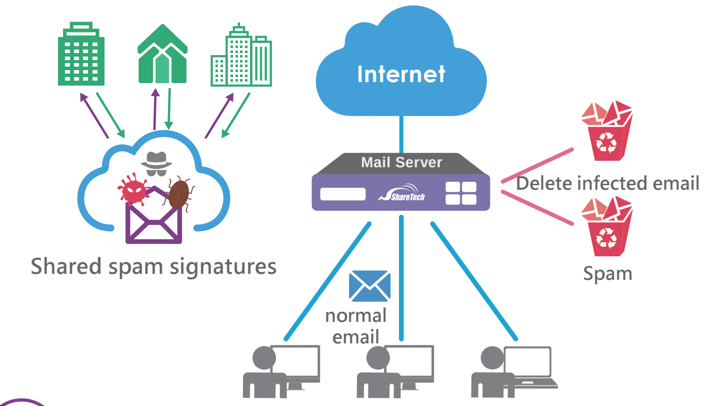
Certified Mail

Users' email can be digitally signed with an electronic stamp. Should you need to prove at some later stage that you sent your email, the attached signatures provide admissible certifiable proof that your email was posted on the date and time specified.



Anti-Virus and Spam Filtering 3.0

Clam AV is provided for virus scanning which can detect over millions of viruses, worms, and Trojans. Customers may choose to purchase a Kaspersky module for their security needs. ShareTech spam filtering 3.0 includes 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.

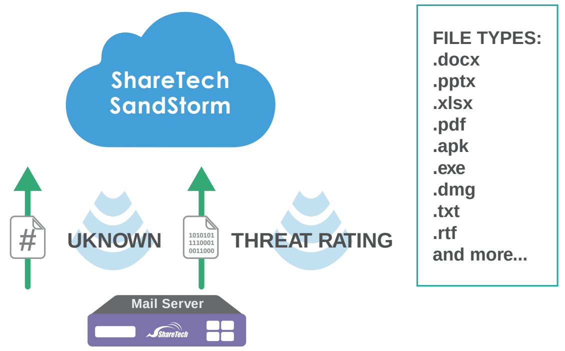


Protection against Ransomware

Transport rules provide the ability to examine email subjects, attachments (zip/rar), and file extension as a defense against the ransomware attack. Additionally, a built-in URL database is provided to block fast-spreading ransomware threats delivered through malicious attachments and URLs.

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 email system.



SPF / DKIM / DMARC Authentication

SPF defines a process to validate an email message that has been sent from an authorized mail server to detect forgery and to prevent spam. DKIM allows an organization to claim responsibility for a message in a way that can be validated by the recipient. Moreover, DMARC is added to allow a sender's domain to indicate that their emails are protected by SPF and/or DKIM, and to tell a receiver what to do if neither of those authentication methods passes.

IV. WEBMAIL AND OTHERS

Personal Data Protection

ShareTech mail server protects personally identifiable information such as ID number, credit card number, phone number, mobile number, and date of birth. Whether it is employee data or customer data, companies have an obligation to protect the personal information they stored on their network.

Eye Cloud

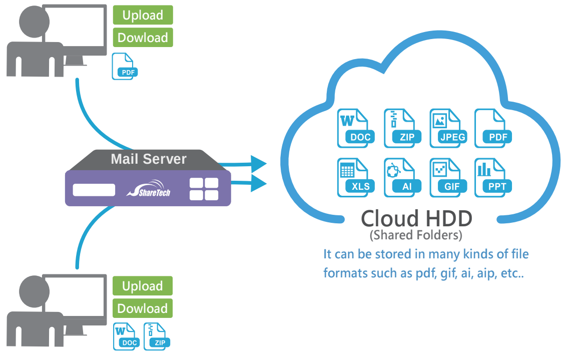
A cloud service platform provides users friendly interface to support instant equipment maintenance and management. It is an all-inclusive solution to monitor various networking appliances deployed in either external or internal networks. When an anomaly occurs, administrators will be notified of the problem.

Webmail Two-Step Verification

People used to set the same password for different websites. However, once clicking phishing URL or downloading malicious files, the password can easily be snatched. ShareTech Webmail now equips with two-step verification. User can set up LINE notification or backup email account to secure your webmail. You can still keep your account safety even if the password has been exposed.

Cloud HDD

ShareTech mail server supports web disk-like platform which gives users the ability to store, synchronize, and share content on a relative core and assign access permission from any device. Users have an individual storage space to create folders, download/upload files and categorize data into preferred management. Moreover, users can set up a password, dates and download times to share large files outside of your organization with a shared link.



Calendar Integration and Sync

Webmail calendar allows you to manage your appointments via drag & drop and inline editing. It also supports calendar overlays to allow simultaneous viewing (side-by-side) of shared calendars. ShareTech provides APP to sync Webmail with smart devices. Moreover, ShareTech provides Outlook Connector that can integrate with Outlook contacts (included contact group). Webmail Calendar also combines with Google Calendar. In one single page, user can check personal and business schedule at the same time and can arrange events easily.

ShareTech

ShareTech Mail Archive

Mail Archive

Mail Data Analytics

Cloud-Based Backup

Mail Security

Security Features

• Multiple Domains & Servers Support

ShareTech MA Series supports multiple domains and mail servers. For example, sharetech.com.tw and tpsharetech.com.tw. Email with its attachments will be transferred and archived based on administrator defined policies.

• Mail Gateway

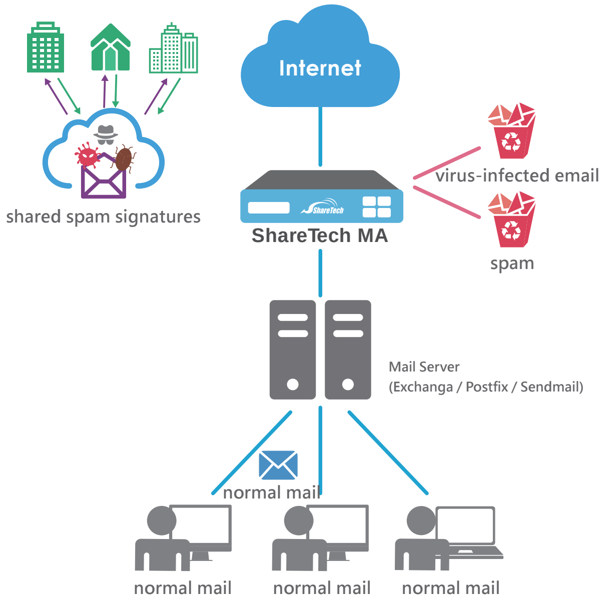
ShareTech MA Series provides fast and accurate email security that does not affect end users or delay their communications. Appliances can be deployed on premises and gateway to defend your mission-critical email systems.

• Dual Anti-Virus Engines

Built-in Clam AV can detect over 5,000,000 kinds of Trojans, viruses, malware & other malicious threats. Moreover, clients can purchase Kaspersky module which ensures a rapid response to new attacks. Legitimate email will be quarantined as virus-infected email, and the system can keep logs, create reports, or issue an alert notification.

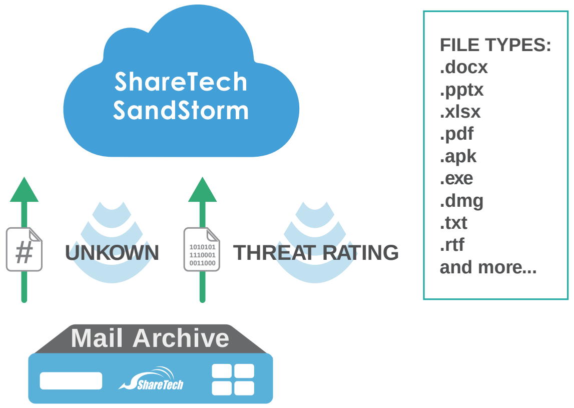
• Anti-Spam and Shared Signatures

The MA 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. 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.



• 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 email will be quarantined and will not have the opportunity to affect the operation of the email system.



• Email & Personal Data Auditing

Security policies can be created and prioritized by the system administrator in the user interface based on governmental regulations or internal business processes. Both incoming and outgoing mails are handled according to recipients, senders, subjects, size, attachments, etc. Moreover, protection for personally identifiable information are provided such as ID number, credit card number, phone number, mobile number, and date of birth.

• Mail Archive Retrieval & Inspection

MA Series protects organizations’ email from accidental deletion, provides email resume, and allows for quick searching and data retrieval in the email archive. This system allows users to enter a keyword search query on web-based interfaces to search through all fields. Users can either read or retrieve crucial documents for investigations.

• Securely Backup Office 365 & Gmail

MA Series backup solution supports cloud-based storage platform by creating hybrids clouds which gives businesses greater flexibility. MA Series can integrate with Google and Microsoft Office 365. Data can be securely stored in different geographically locations as off-site backup.

- **Email Record, Archive & Backup**

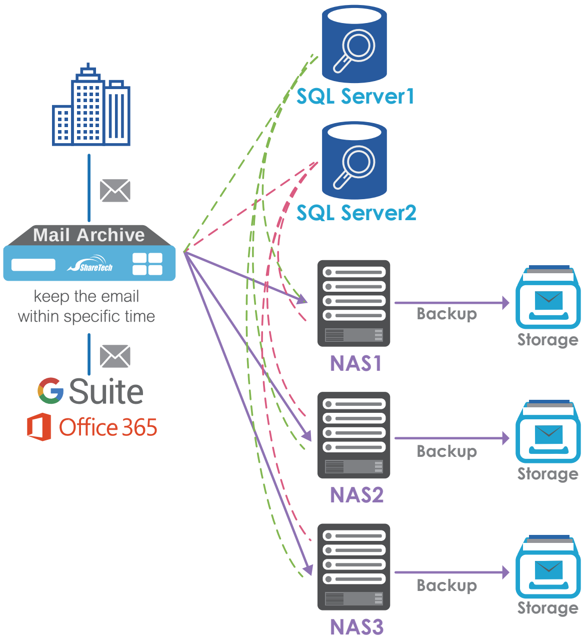
  Storage can be divided into two main types:

  A. Localhost Storage

  By default, archiving policies can be applied to move email messages automatically to archive database.

  B. Remote Storage

  USB flash drive, FTP, SAMBA are supported for users to retrieve individual messages through Network Neighborhood in a failover. Administrators can search for archived messages, inspect its contents and retrieve them easily from within their archive database.



- **Multiple Server-Based Password Authentications**

  ShareTech MA Series supports the use of RADIUS, AD, POP3, IMAP, LDAP servers and Google oAuth for authentication. A valid user name, password and full email address are required to connect to these authentication servers.

- **Role-based System Administration**

  After securely assigning different levels of initial accesses, users have fully integrated functionality to grant, manage, and revoke items such as system management, SMTP server, bridge mode, domain management, and authentication across internal and external organizations.

- **Event Logs Analyzer**

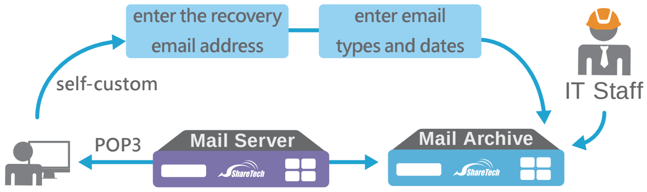
  MA Series provides a solution to handle complete network fault management from one window. Administrators are capable of searching through events logs efficiently for evidence of a particular event.

- **Personal Archive Interface**

  For a better experience, ShareTech recommends using the Outlook Plug-in that users can access archived email from Outlook on the web. Individual users are allowed searching over fields in domain, department, and personal email usage, and further perform searches for any words in the sender name, recipient, subject, body, date, etc.

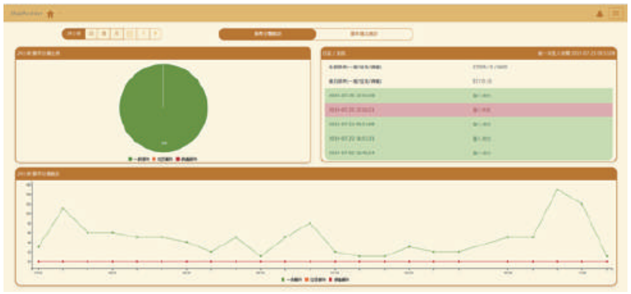
- **Individual Mailbox Backup & Restore**

  ShareTech MA Series provides an easier way to perform individual mailbox backup and restore. When hard drive failure or unforeseen circumstances occurs, the system allows users to directly resend email stored on the MA appliances to designated accounts.



- **Personal Dashboard**

  MA series provides personal dynamic dashboard in the web user interface presenting a graphic view of personal email statistics. Users can specify a date range to analyze their ordinary email, spam email, and virus -infected email activities. In this way, users are given more visibility into their email flow statistics.



SPECIFICATIONS

			MA-200	MA-400	MA-600
Hardware & Capacity					
RAM			4GB	4GB	16GB
HD Space			1TB	2TB	6TB*4
Mounting			1U	1U	1U
LCM			●	●	x
User Accounts			Unrestricted	Unrestricted	Unrestricted
Virus Signature Updates			ClamAV Auto Update(Kaspersky Optional)		
Spam Signature Updates			●	●	●
Recommended Number of Users			Under 200	Under 500	Under 2000
Email Processing/per day (100kb per mail)			60,000 (6GB)	120,000 (12GB)	2,000,000 (15GB)
Software					
Mail Gateway			●	●	●
System Management	Network Setup	IPV4 / IPV6	●	●	●
	Multiple Domains		●	●	●
	Role-Based Management		●	●	●
	Backup Management	Remote Backup(NAS/Samba/FTP/USB)	●	●	●
		Browse/Search	●	●	●
		Disaster Recovery	●	●	●
	Basic Setup	Bridge Mode	●	●	●
		POP3 Proxy (Journaling)	●	●	●
Architecture	Permission	Admin./Querior/User	●	●	●
Authentication & Permissions	Oauth Auth	Google oAuth 2.0	●	●	●
		Office 365 oAuth 2.0	●	●	●
	Account Integration	LDAP	●	●	●
		Active Directory (AD)	●	●	●
Auditing & Protection	Audit Filtering		●	●	●
	Mail Firewall		●	●	●
	IP Blocking		●	●	●
Anti-Virus	Clam AV		●	●	●
	Kaspersky		Optional	1-year license	1-year license
Spam Filtering	Database	IST-IP Networking Rating	●	●	●
		Bayesian Filtering	●	●	●
		URL Filtering	●	●	●
		Auto Learning &Shared Signatures	●	●	●
		System/Personal B/W Listing	●	●	●
Email Archiving	Mail Transfering	POP3	●	●	●
		IMAP	●	●	●
		Cloud HDD	●	●	●
	Pre-and-Post Auditing		●	●	●
	Online Browse/Search		●	●	●
	Personal Email Archiving		●	●	●
	Email Query/Forward		●	●	●
	Attachments/Contents Search		●	●	●
	Audit Filtering		●	●	●
User Archive Interface	Email Query		●	●	●
	Email Auditing		●	●	●
	Email Quarantine/Deletion		●	●	●
	Mail Behavior Analytics	Association Graph	Optional	Optional	Optional
		Statistics	Optional	Optional	Optional
		Working Hours Graph	Optional	Optional	Optional
		Mail Resume	Optional	●	●
Others	Personal Dashboard		●	●	●
	UTF-8 Encoding		●	●	●
	TLS Encryption		●	●	●
	High Availability (HA)		●	●	●
	WEB UI		Traditional/Simplified Chinese and English		
	Max. Number of Users		Unrestricted	Unrestricted	Unrestricted

ShareTech
ShareTech Information Co., LTD.

www.sharetech.com.tw | sales@sharetech.com.tw | help@sharetech.com.tw

V. 2021.08