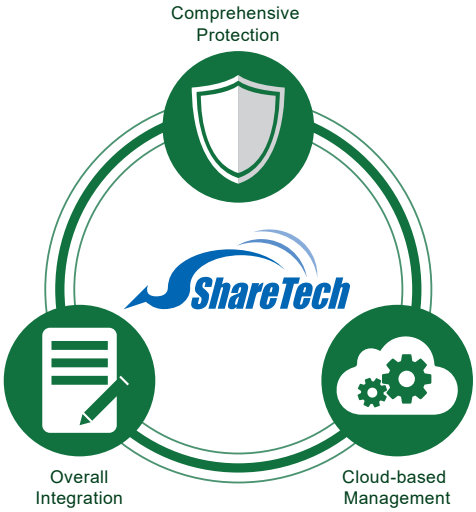
Middle-Size Business
Multi-Function Firewall
UR-960/UR-960H/UR-960C

Next-gen ShareTech UTM with extraordinary performance and deployment flexibility is designed for business to secure highly demanding network environments. UTM is an all-in-one appliance that carries a variety of security and networking features: Anti-Virus, Anti-Spam, authentication, content record, QoS, online behavior management, anomaly IP analysis, Co-Defense (switch), APP access control, Load Balance, content filtering, CMS, VPN, etc. Additional features (Kaspersky, IDP and BotNet Defense, reports, mail audit and SSL VPN) are available through add-on modules. Moreover, web-based interface provides friendly and consistent user experience, auto firmware update, and multi-languages supported. Configuration files can be imported and exported directly to and from UTM. UR-960, UR-960H, and UR-960C provide a wide variety of choices and flexibility to fit into any budget for middle-size companies.



Security
- Anti-Hacker/Malware
- Anti-Virus(WEB/FTP/Mail)
- Spam Filtering
- Co-Defense
- HTTPS/SSL Encryption
- IDP/Botnet Detection

Control
- QoS
- Web Filtering
- Flow Monitoring
- App Access Control
- VPN/SSL VPN
- Network Access Auth.

Record
- Anomaly IP Analysis Log
- Firewall Protection Log
- ARP Spoofing Log
- Event Log
- Auth. Log

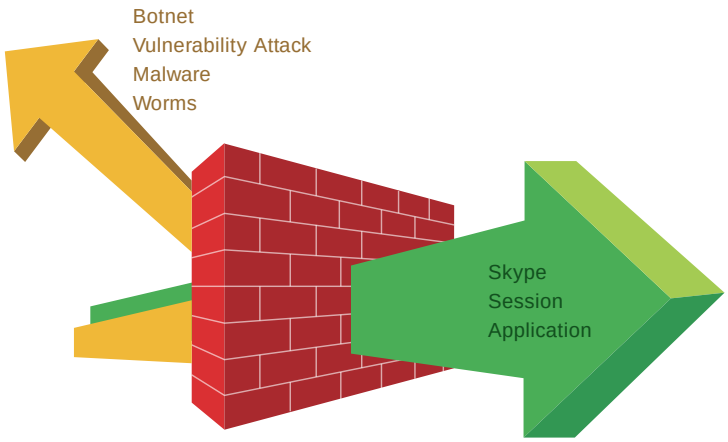
I. Functions Description

Perfect Balance of Features and Performance

ShareTech UTM adapts next–gen platform which brings up to 50% performance boost in throughput and connection. Higher security modules are provided to meet growing demands for more connection usage. Moreover, IT administrators can easily set up backup schedule and use the USB port as the disaster recovery key.

Firewall

Built-in SPI (Stateful Packet Inspection) provides DoS detection and prevention against some popular attack modes, such as SYN flooding, port scans, and packet injection. When the unusually high rates of new connection are detected, the firewall system will issue an alert notification or block anomalous session.

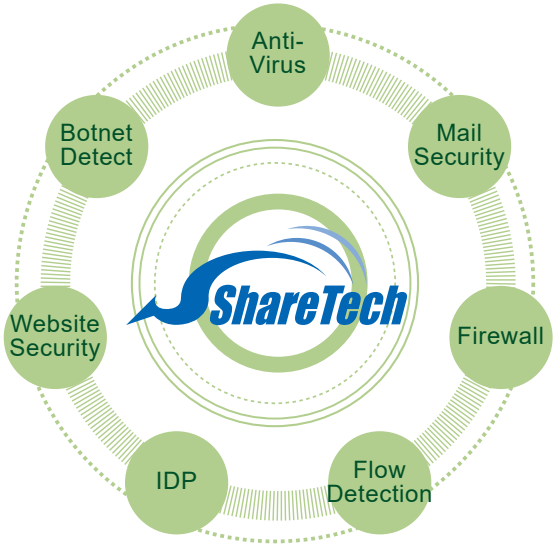


IPv4 / IPv6 Dual Mode

Native dual-stack supported. To cope with IPv4 depletion, ShareTech provides a solution that covers both IPv4 and IPv6 network and can be configured for IPv4 only, IPv6 only, or to support both protocols simultaneously. Furthermore, all ShareTech appliances have been certificated with “IPv6 Ready” logo.

Content Filtering

IT administrator can remove specific undesirable objects from HTTP traffic, such as ActiveX objects or Java applets that may pose a security threat in certain situations. According to the blacklist, vicious websites which may cause damage to PCs can be blocked. IT administrator can add both keywords and URLs of specified websites or webpages to Blacklist and Whitelist.



Load Balance

Outbound/inbound load balancing are provided for distributing the traffic across available links. When one of the links is down, the other link will take over the work and handle the traffic until troubled link returns to normal, in manual or auto mode.

QoS

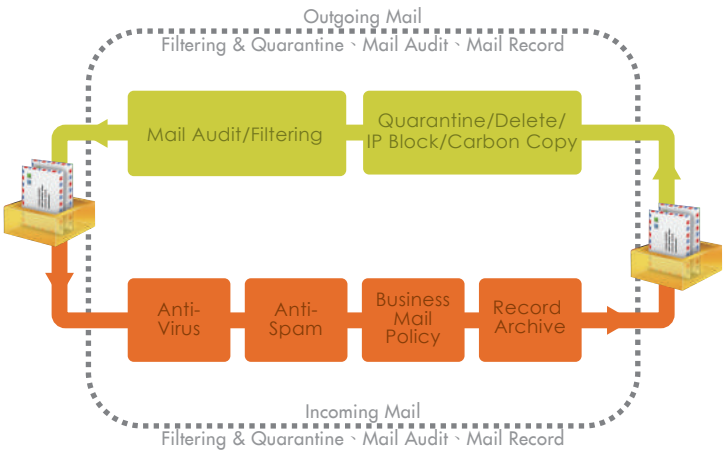
Smart QoS offers more agile bandwidth management for industries and organizations. All the servers and users can be configured their minimum and maximum bandwidth; the remaining bandwidth will be allotted to the other users according to their configuration.

Application Access Control

To prevent data leakage and ensure regulatory compliance, the access to applications which are unrelated to work should be controlled during working hours. ShareTech UTM can block file sharing via P2P, control access to IM/web/entertainment applications, and help industries meet their requirements.

Authentication

In most industries and organizations, internet access control is indispensable for defending network security. ShareTech UTM offers three authentication methods: Active Directive (AD), POP3, and Radius. When a user first opens a web browser and begins to access an internet site, they will be



Anti-Virus

ShareTech UTM for middle-size business offers Clam AV for virus scanning which can detect over 800,000 kinds of viruses, worms, and Trojans. Once suspicious emails are detected, the administrator can decide to delete or block them. Moreover, websites and FTP will be scanned once the function of anti-virus is enabled in policy. Customers may choose to purchase a Kaspersky module to UR-960H or UR-960C for their security needs.

Anti-Spam

ShareTech UTM for middle-size business 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 own database by importing the latest spam update. Following actions like forward, delete, quarantine can be taken on the mail identified as the spam.

Intrusion Detection and Prevention (IDP) & Signature Database

Built-in IDP (IDS+IPS) inspects the packets from OSI layer 4-7 (transport to application layer) and block concealed malicious code and worms delivered in TCP/IP protocols. As soon as an attack is suspected, UR-960H and UR-960C will immediately notify the IT administrator 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 IDP security package.

Botnet Co-Defense

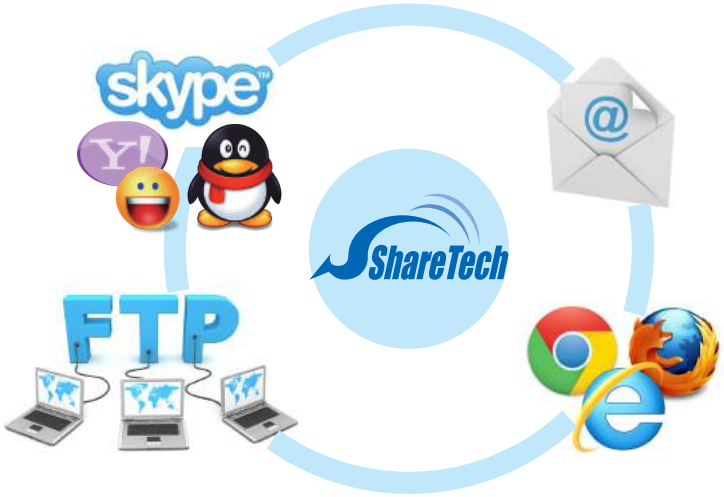
UR-960H and UR-960C can efficiently block botnets using RBL list, C&C mechanism, and malicious URL filtering. In combination of IDP, they protect a company against both external and internal threats. To ensure CPU recourse not being wasted on the same matter, administrator can enable BotNet Co-Defense and directly shut down switch port of infected computers. It not only saves recourses but also suspends malicious software spreading in the internal network.

Anomalous IP Analysis

ShareTech UTM provides the excellent function of anomaly traffic detection because the appliances can detect outgoing/incoming concurrent sessions, upload flow and download flow. If employees are violating the rules and exceeding more downloading flow, they will be logged and blocked. In addition, IT administrator is allowed to define the trusted IP list. If an IP address is added to the trusted IP list, then it will not be detected, and the selected actions will not be implemented to that IP address as well.

Mail Audit (Optional)

ShareTech mail audit offers powerful filtering, multi-layer scanning on mail content and subject, and analysis on outgoing/incoming mail. IT administrators are allowed to create and prioritize policies based on a user-defined events and attributes. Auditing rules handle mail in a variety of actions: auto quarantine, delete, block source IP address, carbon copy, and forward to the supervisor to prevent data leakage. Customers may choose to purchase the module to UR-960H or UR-960C for their security needs.



WEB, FTP, Instant Messaging, Mail Records

UR-960H, UR-960C, and UR-955 can monitor HTTP, FTP, IM (Yahoo, ICQ, ICR, and Google), etc. It records browsed websites: contents (with HTTP) and attachments, files transferred by FTP, and IM chatting contents.

Capture & Log Encrypted Skype

Profound Skype content record is to prevent future disasters and minimize privacy risk. UR-960H, UR-960C, and UR-955 records the full content of all text-based messages, along with voice message and transferred files.

VPN

VPN supplies private connectivity over public lines. Deploying VPNs enables businesses of any size to deliver secured connectivity for mobile employees, branch offices, and clients.

1. IPSec VPN

IPsec VPN securing the site-to-site connections allows a headquarter and its branch offices to be on the same network and sharing resources among offices. For indus tries, IPSec is the best way to connect for transmitting encrypted data over the network.

2. L2TP VPN

L2TP VPN offers point to point connection for employees working at home. Employees can get access to industry's network securely and easily.

3. SSL VPN

SSL VPN offers you an easy VPN access to your head quarters simply through a web browser. Offsite users may create VPN connections at anytime from anywhere with ease.

LAN Bypass

LAN Bypass, a fault-tolerance feature is supported to protect essential business communications in the event of power outage. Bypass ports will be bridged together when the power runs out. When used with Drop-in Mode, such failure would be completely transparent
to the network. Therefore, a business' network connectivity can be fully protected.

Diagnostic Tool

ShareTech UTM provides diagnostic tools such Ping, Traceroute, DNS Query, Server link and so on. They make fault isolation and troubleshooting easy for administrators.

Log

ShareTech UTM records mail with attachments through mail server and gateway. The server supports EML file format for storage which is easier to be read or searched in any operating system.

Graphical Reports

ShareTech reporting allows administrators to custom how the chart types (bar, pie, line, and table) or texts will be displayed at the top of the report. ShareTech UTM displays operation status for the time frame specified (day, week, month), including CPU, RAM, modification times, security level and flow monitor reports.

Unified Device Management Platform

Built-in CMS (Central Management System) provides a useful management platform which allows industries to manage distributed UTM appliances across remote offices and clients. Moreover, ShareTech network peripherals such as Wireless Access Points and switch can also be integrated into device management control and visibility which allows business to be potentially efficient.

Support USB Backup & Restore

It is available to back up the appliance configuration 24/7 by connecting a USB flash drive to one of the UTM appliance's USB ports. Users can restore the configuration from the USB flash drive as needed.

II. Key Features of ShareTech UTM

Features	Description
Threat Defense (Anti-Virus / IDP / Botnet)	1. Uses open source Clam AV engine with huge database includes more than 200,000 unique signatures 2. Kaspersky module (Optional) 3. Clam AV team has fast response time, updates signature regularly and requires no yearly subscription fees. 4. Provides IDP and Botnet attack-signature database 5. IDP risk management is divided into 3 levels (High, Medium, and Low) 6. IDP and BotNet database require no subscription fees.
Malicious URL Filtering (URL & Databases)	1. URL conditions allow to perform URL filtering 2. URL filtering can be configured on UTM 3. IT administrator can add keywords and URLs to B/W list.
Firewall Protection	1. Coordinated DoS/DDOS attacks and UDP Flood performed by hackers can be blocked automatically. 2. Smart QoS provides bandwidth guarantees and a priority command can be given for min/man bandwidth guarantee. 3. Supports IPv4, IPv6, and Dual Stack 4. Supports load balancing and failover for both outbound and inbound traffics 5. Provides DNS service and Dynamic DNS services
Potential Risk Detection (Flow Analysis)	1. Flow/behavior based anomaly detection allows all sessions (up/down) to be analyzed and see if a performance problem exists 2. Following actions can be taken when an anomaly occurs. An anomaly can be recorded, blocked, and notify subscribers. 3. Integrated with advanced switching technology, Co-Defense can be applied to protect the internal network. 4. Prevents ARP spoofing 5. Manages switch port mapping that gives an instant view into the operational status and speed of each port.
Mail Security (Anti-Spam, Mail Filtering)	1. Employs multiple spam mechanisms: ST-IP network rating, Fingerprinting, Bayesian Filtering, Auto learning, Auto-whitelist, system and personal Blacklist/Whitelist and Spam characteristics filtering. 2. Offers Email virus scanning 3. Offers Email auditing, advanced filtering and quarantine 4. Client-side spam mail search is available on web-based interface 5. Additional actions such as quarantine, delete, blocking IP, and carbon copies can be performed to all mail. 6. Searching recorded email are available
Application Access Control (Applications Control)	1. Multiple application categories e.g. P2P, IM, VOIP, Web, WebMail, Game, and others. 2. Free schedule updates 3. Administrators can use policies to prohibit their users from accessing to applications

Features	Description
Content Record	1. Logs all incoming/outgoing emails with delivering date and time 2. Records FTP Server transfers 3. Records browsing history 4. Records instant messaging eg. Skype (limited to models with record-level features)
User Identity (Radius)	1. The host computers are established to ensure user identity and also supports the use of LDAP, RADIUS, AD or POP3 servers for authentication. 2. Desired user groups can be customized 3. Supports Radius services 4. Provides authentication record and connection status
VPNs Connection	1. IPSec and Site-to-Site PPTP VPN 2. Reliable SSL VPN connection 3. Users can create, edit, and control over VPN connections.
Qos	1. Supports Smart QoS 2. Supports bandwidth guarantee, max/min-limit, and priority commands 3. Bandwidth usage from the internal/external source IP can be limited 4. Efficient priority scheme is available
Operation Modes	Transparent, Bridge mode, NAT, Routing
Log & Report	1. Multiple event logs can be centrally logged and monitored. And it includes configuration, networking and route, objects, services, advanced protection, mail security, VPN, etc. 2. A report includes a statistic table, ranking grid and charts & graphs.
Virtual Server	Supports virtual server that data flows can be transmitted to any of the other ports without using any switch or router
High Availability	Building a cluster and hot standby of two or more ShareTech devices is available
CMS	1. Manages multiple UTMs and wireless access points 2. Provides real-time monitoring and proactive management 3. Cloud-based integration can be led to ShareTech Cloud service system
Bulletin Board	Announcement can be made to employees in a very effective and proper way
Diagnostic Tool	1. Standard net tools such as Ping, Traceroute, DNS lookup, and port scanner are available to help users identify and fix connection problems. 2. Test widgets like IP Route, Wake Up, SNMP, IPv6 tool are provided to test your connec tion and readiness as well.
Others	1. Supports transparent bridge mode, routing, and URL redirection 2. Administrators can select authorized users and assign access conditions 3. Automatic disk check is scheduled 4. Supports 802.1Q 5. Data backup and mount (UR-960H/UR-960C) 6. Autonomous management based on a user-friendly interface 7. LCM display

III. Feature Specification

Stateful Inspection Firewall
- User Authentication
- Multiple Security Zones
- Access Control Criteria (ACC) - User-Identity, Source &Destination Zone, MAC and IP address, Service
- UTM policies : IDP, Web Filtering, Application Filtering, Anti-virus, Anti-spam and Bandwidth Management
- Layer 7 (Application) Control & Visibility
- Access Scheduling
- Policy based Source & Destination NAT
- H.323, SIP NAT Traversal
- 802.1q VLAN Support
- DoS & DDoS attack prevention
- MAC & IP-MAC filtering and Spoof prevention
- SSL-Encrypted Connections Test

Administration & System Management
- Role-based Access control
- Firmware Upgrades via Web UI
- Web 2.0 compliant UI (HTTPS)
- Commandline interface (Serial)
- SNMP(v1, v2c, v3)
- Multi-lingual support: Simplified Chinese, Traditional Chinese, English
- NTP Support
- Management: sub-administrator
- HA
- Bulletin Board
- Configuration Backup/ Recovery
- LAN Bypass
- Custom Ports

Gateway Anti-spam
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- IP address Black/ White list
- Spam Notification
- IP Reputation-based spam filtering

User Identity & Group Based Controls
- Access time restriction
- Time and Data Quota restriction
- Schedule based Committed

Log
- Syslog support
- Log Viewer

Networking
- Automated Failover/Failback, Multi-WAN failover
- WRR based Load balancing
- IP Address Assignment: Static, PPPoE, PPTP & DDNS, Client, Proxy ARP, DHCP server
- Dynamic Routing: RIP v1&v2

Gateway Anti-Virus & Anti-Spyware
- Virus, Worm, Trojan Detection & Removal, Malware protection
- Automatic virus signature database update
- Scans HTTP, FTP, SMTP, POP3 Tunnels
- Scan and deliver by file size
- Self Service Quarantine area (BotNet)
- Bayesian filtering
- Graylist filtering
- Personal and System Black/White List

Codefense
- Anomaly IP Analysis (block/notify)
- Switch ports monitor
- Co-defense with Botnet

VPN (Virtual Private Network)
- IPSec, PPTP, L2TP
- Encryption: 3DES, DES, AES
- Hash Algorithms: MD5, SHA-1
- Authentication: Preshared key
- Dead peer detection and PFS support
- Diffie Hellman Groups: 1,2,5
- Overlapping Network support
- Hub & Spoke VPN support

SSL VPN
- TCP & UDP Tunneling
- Authentication: Active Directory, LDAP, RADIUS
- Multi-layered Client Authentication: Certificate, Username/Password
- User & Group policy enforcement
- Lightweight SSL VPN Tunneling Client

Recorder
- WEB/ FTP/ IM/ Mail
- Remote Backup: Flow Analysis/ WEB/ FTP/ Mail

Mail Audit
- Email Notification
- Audit rule setting: sender, recipient, attach ments, etc.
- Action: Quarantine, Delay, and Block.

Intrusion Detection and Prevention
- Signatures: Default (2397), Custom
- IDP Policies: Multiple, Custom
- Protocol Anomaly Detection
- DDoS attack prevention

Reports
- Username, IP, Email ID specific Monitoring Dashboard
- Reports: CPU/RAM system load, network flow, Outgoing ranking, and Incoming ranking
- Mixed format reports: tabular and graphical
- Automated Report Scheduling
- Reports sent via Email

Web Filtering
- Inbuilt Web category database
- URL, keyword, File type block
- Web Categories: Default &Custom
- Protocols supported: HTTP
- Block Malware
- Data leakage control via HTTP upload
- Schedule-based access control
- Custom block messages per category

IM (Instant Messaging) Management
- ICQ/AIM/Google Talk/ QQ/ Yahoo
- Web IM/ LINE
- Allow/Block Login

HA (High Availability)
- Active-Standby
- Active-Passive with state synchronization
- Stateful Failover
- Alerts on Appliance status change

Bandwidth Management
- IP Identity based Bandwidth Management
- Guaranteed & max/ min bandwidth
- Multi WAN bandwidth reporting
- Smart QoS
- Session Control by IP or Service
- Scheduling

Application Filtering
- Inbuilt App Category Database
- Application Categories e.g. File Sharing,IM,VOIP,Web,Web Mail,Game
- Schedule: access control
- Block
- File Sharing: e.g. Foxy
- IM: e.g. Skype
- VOIP Application: e.g. SIP
- Game: e.g. PPStream

User Authentication
- Internal database
- Active Directory Integration
- External LDAP/RADIUS database Integration
- External Authentication: Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

Botnet
- Signature: Default (5432), custom
- Mode: Sniffer, Inline

Certification
- IPv6 Ready Gold Logo

Compliance
- CE
- FCC

IV. Product Comparison

Models	UR-960	UR-960H	UR-960C
Performance			
Giga Port	6	6	14
Fiber Port	-	-	-
UTM Throughput	5.5Gbps	5.5Gbps	5.5Gbps
VPN Throughput	460Mbps	500Mbps	560Mbps
Anti-Virus Throughput	500Mbps	650Mbps	650Mbps
Max. Connections	2 Million	3.3 Million	3.3 Million
Mail Scan/Day	2,600,000	4,280,000	4,280,000
VPN Tunneling			
IPSec VPN Tunnels	4,000	4,000	4,000
PPTP Tunnels	500	500	500
L2TP Tunnels	500	500	500
SSL VPN Tunnels	500	500	500
Features			
Anti-Virus	•	•	•
Anti.Spam	•	•	•
IDP Defense	Optional	•	•
Botnet Defense	Optional	•	•
APP Control	•	•	•
URL Database		•	•
Reports	Optional	•	•
Mail Audit		Optional	Optional
Online Behavior Record		•	•
Anomaly IP Analysis	•	•	•
Co-Defense(Switch)	•	•	•
Load Balance(Outbound/Inbound)	•	•	•
QoS	•	•	•
Bulletin	•	•	•
Authentication	•	•	•
AP Control	•(100)	•(100)	•(100)
CMS	•	•	•
High Availability	•	•	•
VPN (IPSec / PPTP)	•	•	•
L2TP VPN	•	•	•
SSL VPN	•	•	•
Role-based System Administration	•	•	•