Next-Generation UTM
NU-6000

NU-6000 is the optimal network security and management solution for small and medium-sized enterprises. It boasts high-performance operation, robust multi-layered security mechanisms, and hierarchical authorization management. Built-in functionalities include Deep Packet Inspection (DPI), application identification and control, Intrusion Prevention System (IPS), SSL decryption and blocking, web filtering, bandwidth management, antivirus, spam filtering, and support for external authentication integration. Moreover, NU-6000 supports industrial control protocols, delivering comprehensive security protection for industrial system environments by effectively detecting hacker attacks and unauthorized access to internal network resources.

Designed in desktop form, equipped with 6 Gigabit ports (1 management port included), NU-6000 contains 5 ports for administrators freely configured as WAN, LAN, or DMZ, and support with a pair of LAN BYPASS. To enhance internal network security, it offers internal network protocol defense, integrating wireless access points (APs) and managed switches to create a unified wired and wireless security protection. This allows administrators to comprehensively manage both internal and external networks, providing thorough threat management solution. With a simplified management interface and comprehensive reporting capabilities, it is suitable for various scenarios including enterprise LANs and small SOHO studios.

Guardian of Gateway Security

Stateful packet inspection (SPI) firewall technology examines the packet header and destination port for authentication and checks the entire packet’ s content before determining whether to allow its passage into the network. SPI firewalls can drop any packet that is identified as potentially dangerous and automatically blocks DoS, DDOS, and UDP Flood attacks.

- Web filtering to block HTTP/HTTPS access
- Intrusion prevention system (IPS)
- Application control
- Virus scanning and spam filtering
- Network traffic monitoring and Co-Defense

Support Industrial Control Protocols

NU-6000 supports industrial control protocols including MODBUS, BACNet, LonWorks, and other related protocols, effectively safeguarding the security of different communication ports within various TCP/UDP protocols. This ensures the stable operation and reliability of industrial systems. It also features BYPASS functionality, automatically switching traffic to a backup channel in case of firewall malfunction, preventing operational disruptions to machines.

Deep Packet Inspection (DPI) and Application Control

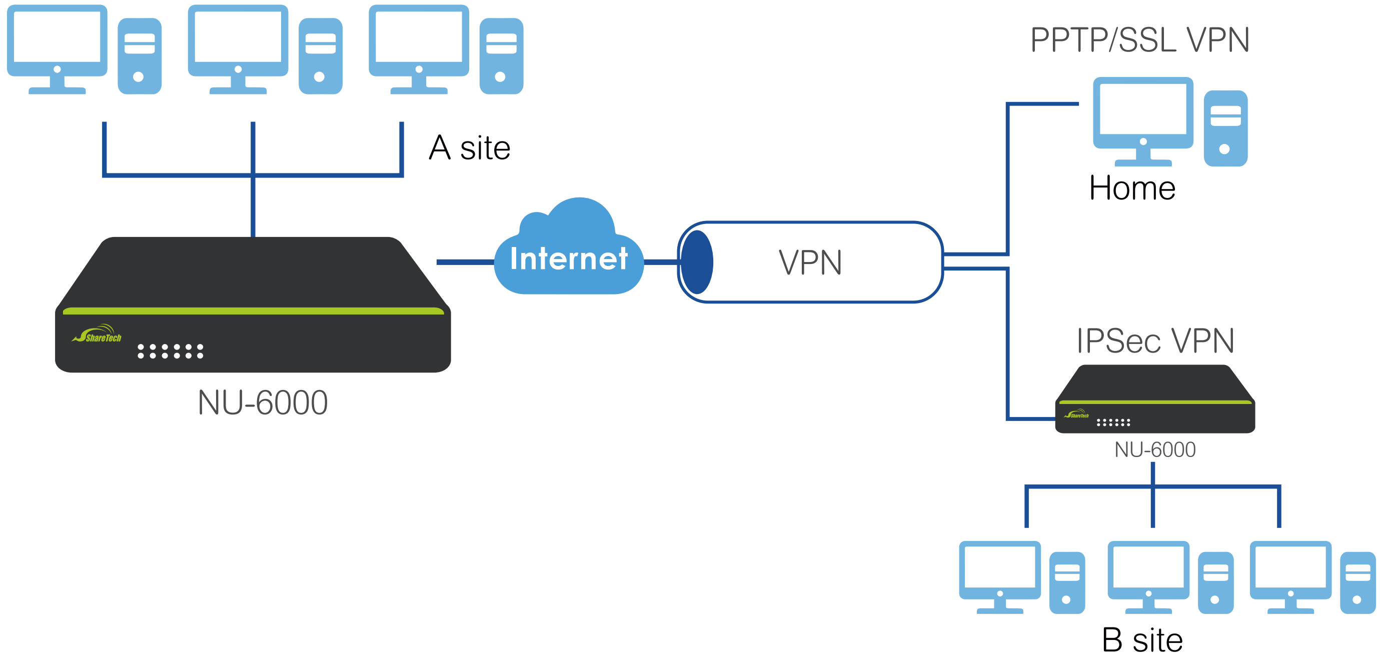
Unique DPI performs traffic signature analysis by inspecting all packets for new application signatures, scoring up the signatures, and appending them to the relevant database. More importantly, having recorded these collected data will be available for future audits.

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

Complete VPN Solutions

VPN connections provide data confidentiality, data integrity, and data authentication. At the same time, popular protocols such as web, SMTP, and POP3 that contain packets transmitting within tunnels can be controlled.

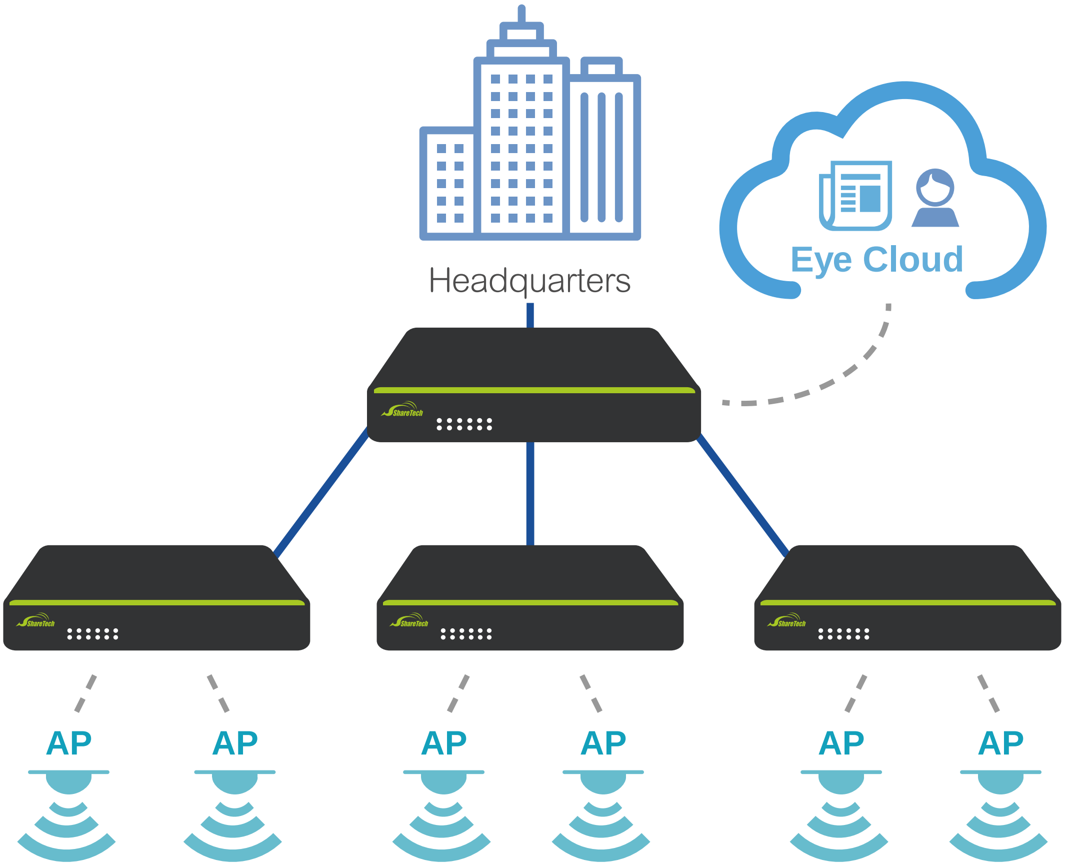
- Supports IPSec, PPTP, L2TP, SSL, and GRE Tunnels
- Supports DES, 3DES, and AES encryption and SHA-1/MD5 authentication algorithms
- SSL VPN mobility client for Android and Apple iOS
- Supports Auto VPN (Server & Client)
- Controls connectivity of remote sites from the central site



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

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

- Eye Cloud is a cloud service platform which can manage and monitoring firewall devices across multiple locations. IT administrators can simply log into the cloud management platform to centrally monitor all ShareTech firewall devices, including real-time status updates of internal wireless access points and switches. This centralized management greatly simplifies operations and significantly reduces enterprise operating costs.
- CMS, on the other hand, is a local management solution designed for managing all firewall devices within a single location. Through CMS, administrators can monitor and manage these devices from a control platform, enhancing management efficiency.



I. Features

Intel Central Processing Unit Reinforces Internal Management

Embedded with strong Intel hardware platform and built-in 4G RAM provide outstanding security protection and high performance to meet demanding requirements. Also, the X86 hardware design eliminates concerns about performance limitations, enabling enterprises to fully leverage UTM functionalities to safeguard network stability and security against complex cybersecurity challenges.

Intrusion Prevention System (IPS)

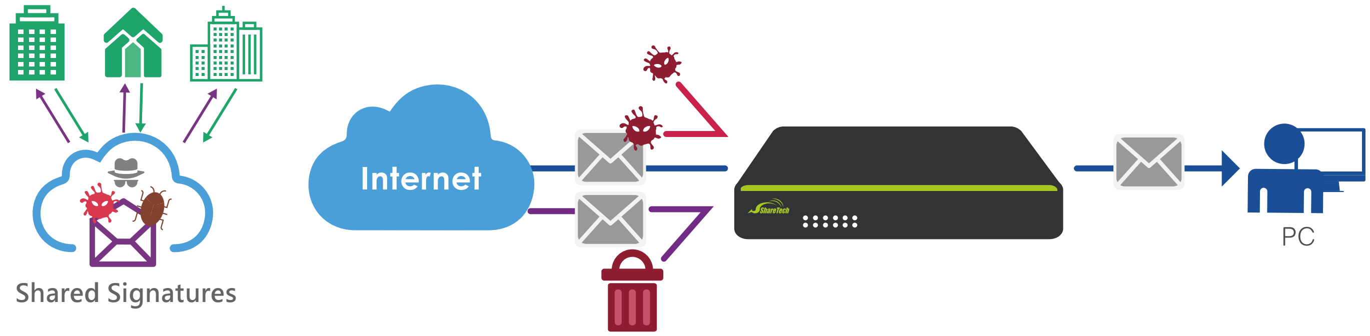
Built-in IPS inspects the packets from OSI layers 4-7 (transport to application layer) and blocks concealed malicious code and worms delivered in TCP/IP protocols. As soon as an attack is suspected, IT administrators will be notified immediately, and later an extensive range of reports will be available for analysis. The predefined attack signature database is regularly updated which makes it available as an IPS security package.

Anti-Virus

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

Anti-Spam

Multi-spam filters such as ST-IP network rating, Bayesian filtering, spam characteristics filtering, fingerprinting, auto-learning, and personal B/W list are crucial for strengthening the security of mail transportation. Also, administrators are flexible to enforce custom filtering. These help industries create their database by importing the latest spam updates. Following actions like forward, delete, and quarantine can be taken on the mail identified as spam. Moreover, the shared signatures mechanism shares the signature of an early receiver with the rest of the group so that higher spam detection accuracy can be obtained.



Sandstorm

Sandstorm protection mechanism effectively detects unknown advanced malware attachments (such as common Microsoft Word, Excel, PowerPoint, or PDF files), targeted phishing emails, and compressed files (commonly ZIP and RAR). If users accidentally click on a malicious URL or open a malicious attachment in an email, Sandstorm will automatically compare and block them. Moreover, it offers four types for checking: File Hash, Web URL, Domain, and IP. With cloud-based test scanning analysis, hidden malicious links and attachments in emails can be exposed.

WAF

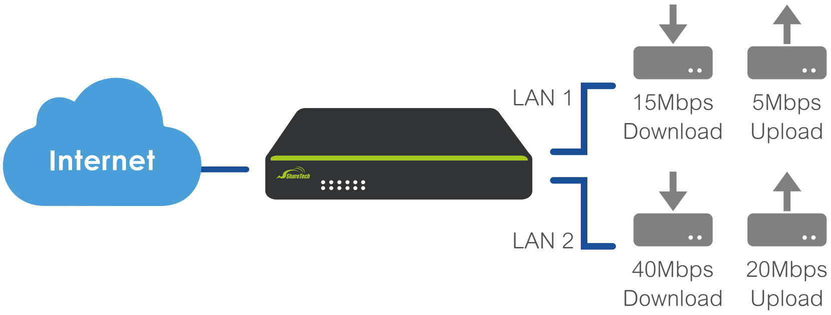
WAF (Web Application Firewall) specifically manages traffic on web pages, enhancing HTTP/HTTPS protocol security and filtering abnormal connections. Before enterprises confirm or improve website security, WAF acts as a protective barrier to safeguard internal hosts. It shields web servers from common website attacks such as XSS (Cross-Site Scripting), SQL injection, Remote Command Execution, and other prevalent forms of website intrusion.

Inbound/Outbound Load Balance

Support inbound and outbound load balancing, providing businesses with at least 2 WAN links. Multi-homing load balancing is supported to spread a business's Internet traffic among multiple access links to increase the aggregate throughput and to divert traffic away from non-functional links when they fail.

QoS

QoS offers more agile bandwidth management for industries and organizations. Since bandwidth can be limited using source IP in both directions, all the servers and users can be configured with their minimum and maximum bandwidth. The remaining bandwidth will be allotted to the other users according to their configuration. Moreover, an efficient priority scheme can be available for minimum/maximum bandwidth guarantee.

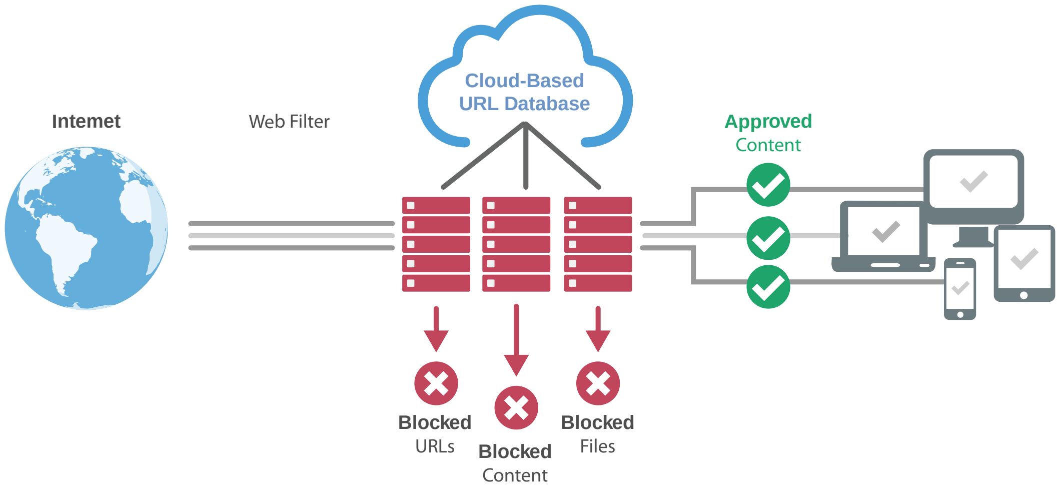


Content Filtering

Provide Web Filter functionality to block access to inappropriate websites (such as pornography, violence) and malicious websites (such as hackers, viruses) from endpoints. It allows customization of filtering criteria to block inappropriate sites.

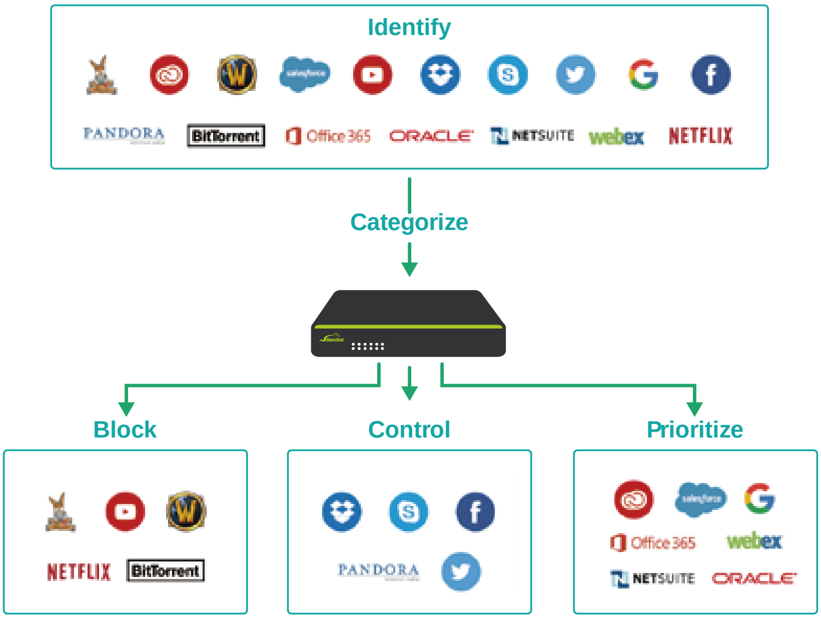
Advanced URL Control and Database

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



Advanced Application Control and Database

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



Abnormal IP Analysis

Regardless of which software users are running, from the perspective of network packets, connections are broadly categorized into upload and download quantities, flow (Flow), and duration (Time). When abnormal behavior by internal users is detected, administrators can implement various strategies such as blocking internet access, immediately limiting maximum bandwidth, activating collaborative defense mechanisms to notify switches for blocking, or simply notifying administrators.

Authentication

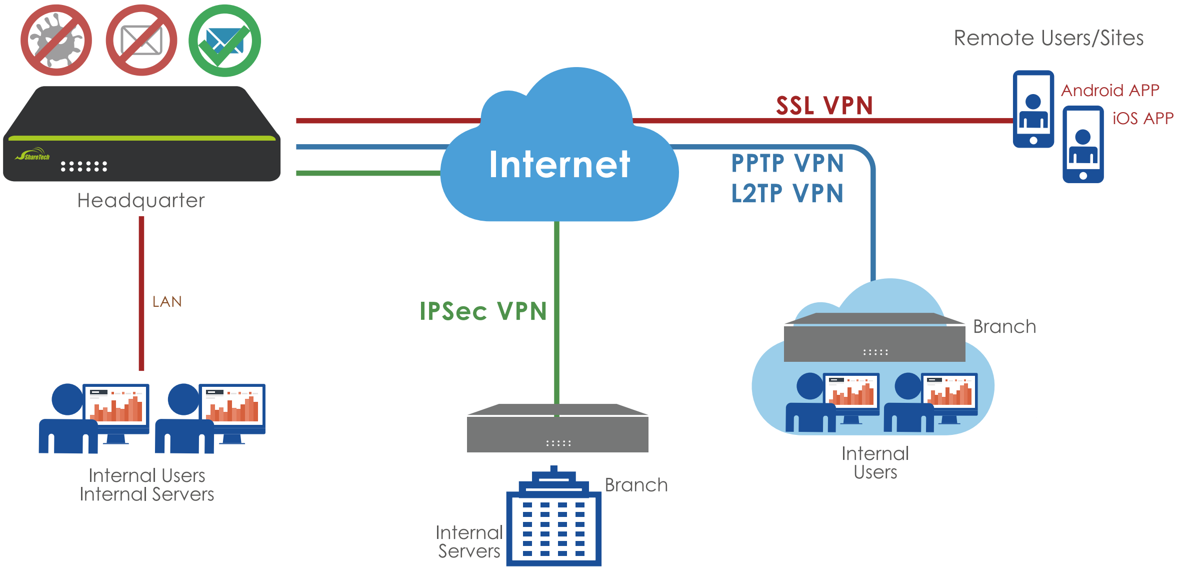
Multiple authentication mechanisms such as local user authentication, Active Directory (AD), POP3, Radius, and others assist network administrators in monitoring all user accounts within the enterprise. These authentication mechanisms ensure that users are granted access to network resources only after their IDs are verified to have valid authorization, effectively managing the use of enterprise network resources. To sum up, the authentication mechanisms not only offer flexibility and choice but also adapt to different enterprise needs and environments.

Multi-factor Authentication Mechanism

The multi-factor authentication methods such as Google/Microsoft Authenticator can ensure robust user identity verification and enhance account security. This feature is primarily applied to administrator login interfaces and user SSL VPN login interfaces. Multi-factor authentication is a security enhancement method that requires users not only to enter a password but also another factor. For example, a temporary password generated by Google Authenticator is valid for 30 seconds. Users must input this verification code during login to gain access.

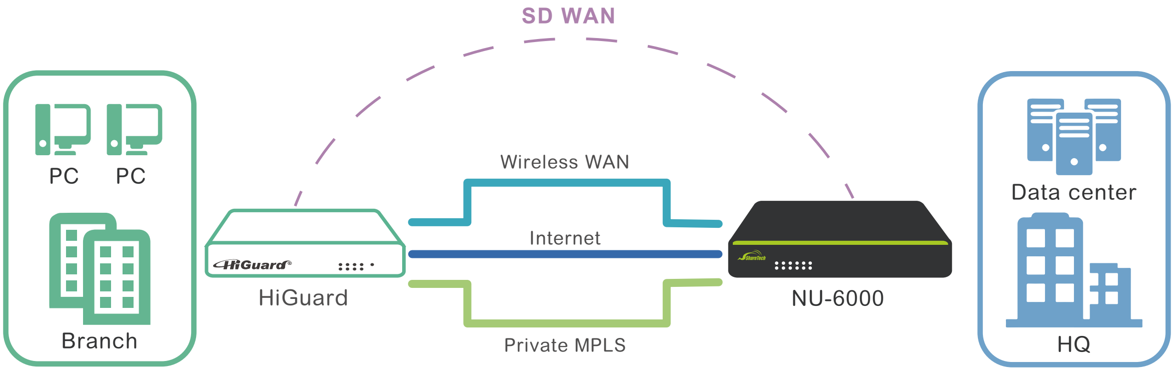
VPN

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



SD WAN

The primary advantage of ShareTech SD-WAN lies in effectively reducing MPLS cost by utilizing multiple VPNs connected into a single tunnel for redundancy, significantly enhancing network performance and stability. This design not only saves on expensive MPLS expenses but also leverages multiple WAN connections. It dynamically selects the optimal path based on network conditions changes, ensuring stable operation of critical business applications.



Threat Intelligence Center Dashboard (Optional Purchase)

The Threat Intelligence Center Dashboard provides real-time reflection of network status through a Dashboard, including common network threats, real-time connection numbers, application categorization, top users of network resources, HTTP and HTTPS traffic, and firewall offense and defense information. Using application layer DPI technology, it gathers enterprise device, user, and application data to simplify troubleshooting processes through a unified interface, enhancing user experience, and gaining network visibility to monitor real-time connections, applications, emails, defenses, and web usage. By integrating and analyzing real-time and historical data, it assists enterprises to select suitable solutions.

II. Protection

FIREWALL

- **Routing：**
  Supports static/dynamic route, designated gateway group, and default gateway.
- **IPv4/v6：**
  Supports IPv4, IPv6, and IPv4/IPv6 dual-stack. Admins can quickly swap between at the click of a button.
- **IEEE VLAN 802.1Q：**
  The Intranet can be divided into multiple segments, isolating different traffic logically.
- **GEO IP：**
  Geo IP restriction allows admins to configure a geolocation-based policy by specifying source and destination locations.
- **Network Services：**
  Support Client/Server DHCP, DDNS, SNMP, and DNS Server and Proxy.
- **VPN：**
  Supports IPSec, PPTP, L2TP VPN, SSL VPN, and IP Tunnel.
- **SD-WAN：**
  SD-WAN can combine from the designated gateway or VPN tunnels, enable optimized traffic routing over multiple transport links, and select a route for applications based upon configured policies and priorities.
- **IP Tunnel：**
  A secure VPN can be created via IP Tunnel between two ShareTech UTMs, and traffic passed through the VPN can be monitored.
- **Auto IPSec VPN：**
  To create an IPSec VPN between two sites having massive/dynamic IP addresses, Auto VPN can reduce the complexity of deployment and increase stability.
- **Log：**
  Include logging for system operation and status, wizard, login/logout, system anomaly & control, configuration, networking, policies, objects, services, advanced protection, IPS, WAF, email security, content record, VPN, etc.

NETWORK & EMAIL PROTECTION

- **Anti-Virus Engine：**
  Support ClamAV, an open-source anti-virus engine that detects millions of trojans, viruses, malware, and other malicious threats. Kaspersky is also available for optional purchase.
- **Intrusion Prevention System (IPS) & Signature Database：**
  Supports IPS that proactively detects intrusion behaviors and matches the signature database. IPS Protection’ s severity level is defined as LOW, MEDIUM, and HIGH.
- **Sandstorm：**
  Support four types of security inspection: file hash, Web URL, domain, and IP.
- **WAF：**
  Cyberattacks are classified into 19 categories by WAF. A host-based WAF sets between external users and web applications to block and log requests.
- **Anomaly IP Analysis：**
  Flow/behavior-based anomaly detection allows both up and down sessions to be analyzed. An anomaly can be blocked, recorded, and notified to subscribers.

WEB PROTECTION

- **Transport Layer Security (TLS)：**
  TLSv1.3 inspection on IPv4 and IPv6
- **Deep packet inspection (DPI)：**
  DPI is a form of packet filtering that locates, classifies, and reroutes packets. It has higher detection accuracy than ort-based TCP/UDP.

- **WEB Service：**
  Supports HTTPS scanning in anti-virus, SSL certificate installation, loggings for HTTPS proxy action, and certificate allowlist.
- **URL Filtering：**
  A third-party database sorts malicious URLs into six categories. Users can renew the license to get real-time updates or periodically apply firmware upgrades for free updates.
- **Application Control：**
  A third-party database sorts applications into 17 categories. Users can renew the license to get real-time updates or periodically apply firmware upgrades for free updates.

ACCESS CONTROLS & FLOW MANAGEMENT

- **Authentication：**
  The system can authenticate users with accounts on hosts, POP3/IMAP, Radius, and AD servers. Admins can add users to groups, view logs, and get status information.
- **Multi-factor Authentication：**
  The multi-factor authentication can add an additional layer of login security to user accounts, authentication, and SSL VPN access. Users can download mobile security apps (Google/Microsoft authenticator) to generate codes and use the codes to log in.
- **Load Balance：**
  Inbound and outbound flow can be reviewed to make sure traffic patterns are expected. Administrators can set up traffic rules in priority order so that all traffic can be evenly distributed among multiple WAN links.
- **QoS：**
  Ensure an adequate bandwidth for high-priority tasks and applications, maximum bandwidth limits, and priority levels.

INTRANET PROTECTION

- **Switch Co-Defense：**
  Common SNMP switches and advanced L2/L3 switches (a topology included that gives an instant view of the operational status and speed of each port) can be centrally managed. Zyxel switches support IP Source Guard (static IP-MAC-Port binding) to perform DHCP Snooping. Moreover, the PoE schedule can be configured via UTM to manage power consumption.
- **AP Management：**
  It displays the status of AP and online users. Quick deployment (config. files) can be delivered for large numbers of access points.
- **Intranet Protection：**
  ARP spoofing prevention, IP & MAC spoofing prevention, notification, and block status.

CENTRAL ORCHESTRATION

- **Cloud-Based service system (Eye Cloud)：**
  ShareTech-branded devices can be remotely monitored and efficiently maintained. Multi-region Wireless APs and switches can be accessed via UTMs as well. Flexible options (Free, VIP, and Distributor) are offered to match requirements. Administrators 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.
- **Server-Side and Client-Side CMS：**
  Support regularly passing data from the client side to the server side. The system makes periodic backups (config. file) automatically.
- **Dashboard：**
  A real-time Dashboard that shows a graphical presentation of the current status.

OTHERS

- **Industrial Control Protocols：**
  Support multiple industrial control protocols include EtherCAT, Ethernet/IP, MODBUS, DNP3, DNP3-Secure, IEC-104, IEC-104-SEC, IEC-61850, MMS, AXView2.0, BACNet, LonWorks, LonWorks2, PROFINET, Citrix, MQTT, MQTT over SSL, Siemens OPC-UA, Kepware OPC-UA. This function enables enterprise to implement in manufacture fields.
- **Operation Management Interface：**
  Management interface and Dashboard GUI.
- **Diagnostic Tools：**
  Standard net tools such as Ping, Traceroute, DNS lookup, and port scanners are available to help users identify and fix connection problems. Test widgets like IP Route, Wake Up, SNMP, and IPv6 tools can test your connection and readiness.
- **Remote Log Server：**
  Log data can be forwarded in the Syslog format to a remote Syslog server that receives, categorizes and stores log messages for advanced analysis.
- **Distributed administration：**
  Authority can be delegated to one or more administrators, such as Admins and assistant admins. Admins can assign three types of privileges (READ, WRITE, and ALL privileges).
- **Custom Password Policy：**
  Password length and complexity requirements, unable to reuse old passwords, and change passwords at regular intervals.
- **Interrupt：**
  Hardware interrupts (via CPU) and software interrupts (via ZONE) are supported, allowing the CPU to perform specific tasks. IT administrators can optimize system performance and troubleshoot issues more effectively.
- **Offline Signature Update via USB drives：**
  Support the following items: IPS, the default APP Blocklist, anti-virus (ClamAV & Kaspersky), and Sandstorm.
- **Backup & Restore：**
  Offer USB system backup. A system recovery can be ready to minimize the damage imposed by an incident.
- **UPS：**
  Provide backup power as quickly as possible in the event of data loss and some protection from power quality issues.
- **LAN Bypass：**
  Support 1 pair of LAN bypass as a fault-tolerance to protect business communication in the event of a power outage.
- **High Availability (HA)：**
  Supports Hot-Standy (Active-Passive) mode.
- **Warranty ：**
  Warranty terms vary by region. Please contact our local distributor for specific details.

III. SPECIFICATION

	NU-6000
Hardware	
Appearance	Desktop
Suggested User	~50
Network Interface	6 x Gigabit
Custom Port	5
USB	3.0 x 2
LAN Bypass	1
Power Consumption	24 W
Performance	
Firewall Operating Speed (MAX)	4 Gbps
MAX Concurrent Session	1,500,000
New Session per Second	65,000
Mail Scan per Day	2,000,000
Anti-Virus	720 Mbps
IPS	500 Mbps
VPN	260 Mbps
VPN	
IPSec VPN Tunnels	2,000
PPTP/L2TP/SSL VPN Tunnels	600
IP Tunnels	300
Network Security	
Anti-Virus Engine	Clam AV/Kaspersky(Optional Purchase)
IPS Defense and Database	•
Sandstorm	•
Spam Filter & Spam Learning Share	•
Mail Audit	Optional Purchase
Advanced URL Management and Database	1 year built-in
Advanced APP Management and Database	1 year built-in
WAF	•
Geo IP	•
Switch Co-management	•
Switch Support List	ML-9324E、GS2220-28、GS2220-50、XGS2210-52、XGS2210-28、XS3800-28
AP Management(MAX Quantity)	50
AP Support List	NWA50-AX、NWA90-AX、NWA110-AX、NWA210-AX、NWA1123-ACv3、NWA90AX PRO
Load Balance(Inbound/Outbound)	• / •
Virtual Server	•
Authemtication	•
2FA	•
High Availability	•
VPN	•
IPSec Tunnel	•
SD-WAN	•
Wizard	•
CMS	•
Eye Cloud	•
Others	
Industrial Contrtol Protocols Support	EtherCAT, Ethernet/IP, MODBUS, DNP3, DNP3-Secure, IEC-104, IEC-104-SEC, IEC-61850,MMS, AXView2.0, BACNet, LonWorks, LonWors2, PROFINET, Citrix
Dashboard	Optional Purchase