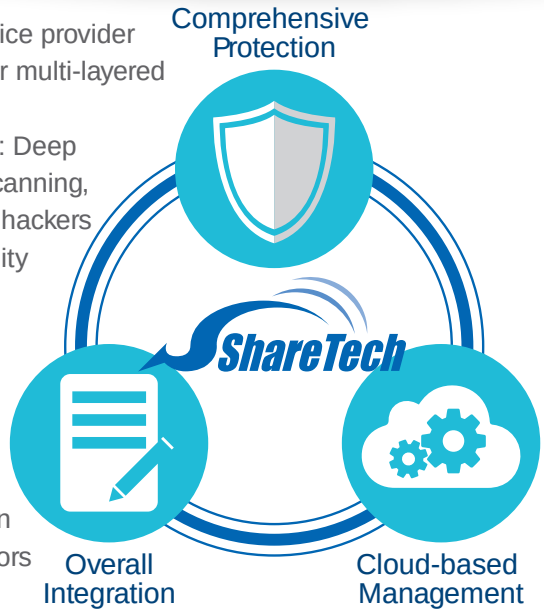
Medium / Large Enterprises
Next-Generation UTM
NU-880H

ShareTech NU-880H is the next phase of technology change which will help service provider to launch the services in single click, delivering exceptional performance, superior multi-layered threat protection, and role-based administration to medium and large businesses.
NU-880H carries advanced protection across your network security deployments: Deep Packet Inspection (DPI), In-Line IPS, SSL Inspection, Web Filtering, QoS, virus scanning, spam filtering and external authentication to prevent potential attack launched by hackers and legitimate authorized users from accessing network. Moreover, High Availability (HA) is supported to ensure smooth network operation.
As with NG-UTMs offering future-ready security, NU-880H delivers a full range of Layer 2-7 switching which can be a great replacement for a L3 core switch. Furthermore, it unifies and deploys consistent security policies across both wired and wireless networks, centrally manage and monitor internal wireless APs and switches. ShareTech also introduces a cloud-based service system providing a new way to deploy, operate, and manage distributed networking appliances. When anomalies occur in network traffic, the system sends notification to IT administrators and help them to resolve issues quickly.



Protection

- Firewall
- IPS
- Anti-Virus (Kaspersky)
- Anomaly Flow Analysis
- Wireless Security
- URL Database

Detection

- Malware
- Persistent Threat
- Ransomeware
- DPI
- APP Analysis
- SSL Decryption

Integration

- L2/L3 Switch
- AP Control
- Dashboard
- SDN Controller
- Cloud Management (Eye-Cloud)

Guardian of Gateway Security

NU-880H fully integrates firewall, Deep Packet Inspection (DPI), virus scanning, ISP, SSL Inspection and blocking, moreover, extended APT prevention is provided to stay one step ahead for improved compliance and security.

- Stateful packet inspection (SPI) firewall technology exams 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 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

Integrated NG UTM & Layer 3-7 Switching into One Single Appliance

NU-880H is an integrated appliance that combines the security features of NG-UTM and layer 3 core switch, upgrading management from Layer 3 routing capability to the higher application layer. It is a real-world firewall based on 8 Core Xeon-branded Processor, with 18 gigabit Ethernet ports, firewall throughput up to 14 Gbps, and improved VPN throughput of 2.2 Gbps.

- ShareTech NG-UTM differs from other competitors in multiple physical Gigabit Ethernet interfaces, allowing IT administrators to bind ports into port groups.
- Going beyond the traditional Layer 3 routing mechanism among port groups, DPI is embedded as an advanced method to filter packets functioning at the application layer and allows business to be much more precise in their control of what enters or exits the network.

Supports SDN Controller

SDN controller is designed to be in charge of translating the requirements from the SDN application layer down to the SDN data paths and provides the SDN applications with an abstract view of the network.

- While the traffic is sent from the underlying systems to the selected destination, application-layer (Layer 7) management can be applied for higher-level functionality.
- Transferring traditional UTM to SDN structure delivers a seamless, hassle free experience to medium and large businesses.

Data Loss Prevention (DLP) & Application Control

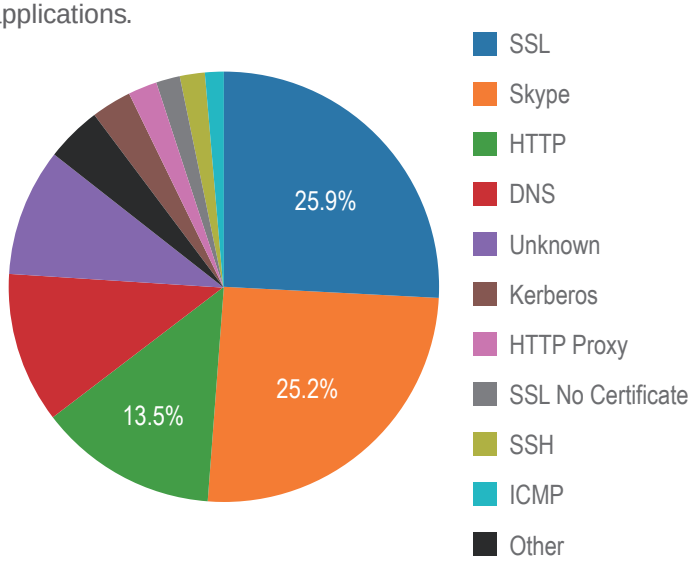
DLP detects potential data breaches / data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data. Having application layer firewall technology, NU-880H is able to inspect both HTTP and HTTPS packets and prevents losing sensitive information or subsequently acquired by unauthorized party.

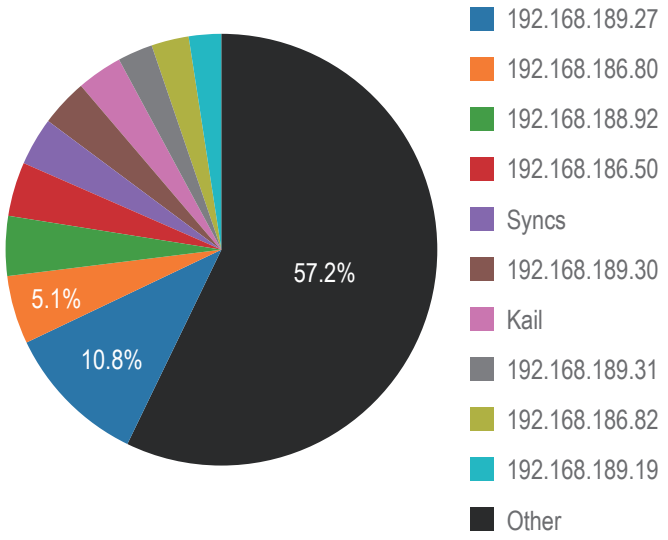
Unique DPI performs traffic signature analysis by inspecting all packets for new application signatures, score up the signatures, and append them to the relevant database. More importantly, having recorded these collected data will be available for future audits.

- 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

Single-Pane-of-Glass Dashboard

NU-880H dynamic dashboard in the web user interface (web UI) presents a graphic view of the system status including concurrent connections, application classification, network resource usage, HTTP or HTTPS traffics and intrusion defense to help in tracking and diagnosis. IT administrators are given visibility into the network users, their devices, and their applications.





Complete VPN Solutions

Using IPsec, PPTP, L2TP, SSL VPN connections, NU-880H provides data confidentiality, data integrity, and data authentication. At the same time, popular protocols such as web, SMTP, and POP3 that contains packets transmitting within tunnels are able to be controlled.

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

Cloud-based Management

Eye Cloud is a next-gen cloud service platform providing 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 anomaly occurs, administrators will be notified of the problem.

- Central management system designed for multi-site network security appliances deployments.

I. FUNCTIONS DESCRIPTION

Exceptional Performance & Consolidated Security Features

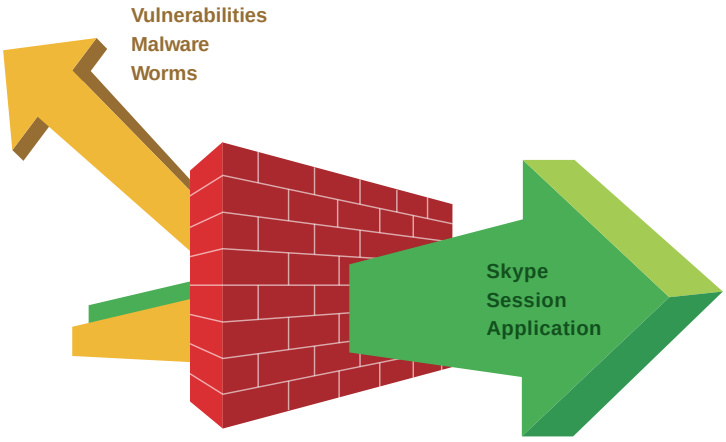
NU-880H adopts best-on-class multi-core x86 CPU platform to deliver exceptional performance and intelligent network security features. ShareTech develops high-performance security modules and delivers enterprise-class security modules, high connection capacity connectivity, and supports USB instant recovery.

Supports SDN Controller

Being the core of an SDN network, SDN controller is designed to manage flow control to enable intelligent networking. Based on protocols, the controller configures network devices and chooses the optimal network path for application traffic. IEEE 802.1Q VLAN is supported to provide a degree of isolation by dividing the network into isolated islands as if provided by separate physical networks.

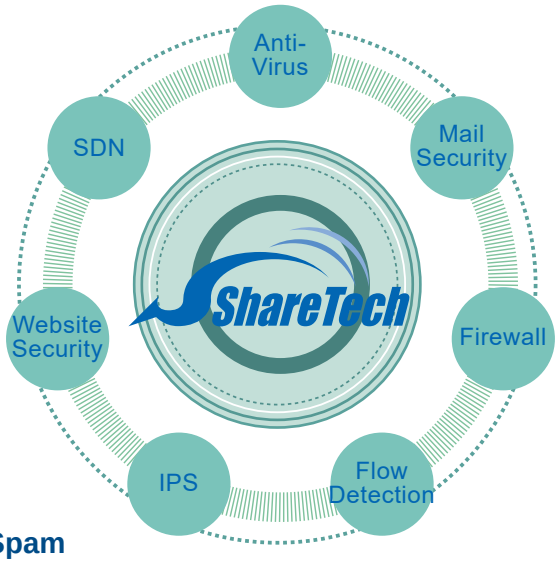
Intrusion Prevention System (IPS)

Built-in 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, IT administrator 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.



SSL Inspection

To protect your network from network threats, SSL inspection is the key used to unlock encrypted sessions, see into encrypted packets, find threats, and block them. Several security features that can be applied using SSL certificate inspection are ISP, gateway anti-virus, web filtering, application control, and QoS.



Anti-Spam

NU-880H 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. Email accessed by users from LAN to DMZ can be especially filtered and logged.

Gateway

For companies that have deployed mail servers in their network environments but lacking of advanced filtering, NU-880H can be placed at gateway to secure your email and get simple and powerful protection from spam, virus and malware.

IP Traffic Streams Analysis

Outgoing/incoming concurrent sessions, upload/download flow, and time duration are flow parameters collected for packet-based traffic analysis. Using a combination of pattern matching can determine whether an activity is performing normally or abnormally. If employee are violating the rules and exceeding more downloading flow, IT administrators are allowed to define the trusted IP list and take appropriate actions to block network access, limit maximum bandwidth, blocking ports on switches (Co-Defense), or simply receive notification.

WEB & Email Records

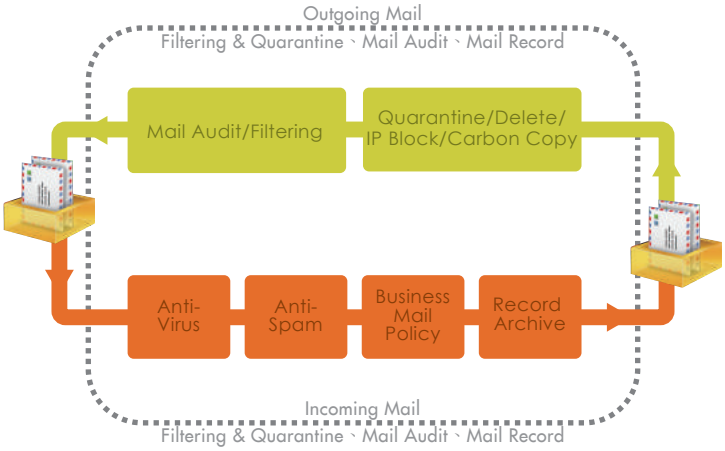
Record each user online behavior (computer name, IP address, MAC address, and traffics) time stamps, items and locations.

Record incoming and outgoing mail (Webmail) and their attachments pass through the mail gateway.

Email is saved in an .eml format that can easily be viewed and searched.

Anti-Virus

NU-880H for large enterprises offer 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 will be scanned once the function of anti-virus is enabled in policy. Customers may choose to purchase a Kaspersky module for their security needs. (NU-880H contains 1-year Kaspersky license.)



Advanced Threat Defense

In addition to firewall, Intrusion Prevention System (IPS), and virus scanning, NU-880H can monitor malware or threats within traffics based on analyzing flows, webpages, and email. By performing different security mechanisms, business network is given more effective and profound protection against active cyberattacks, targeted attacks, and sophisticated malware.

Content Filtering

IT administrators can configure Web filtering profiles that block URLs to inappropriate webpages like violence and pornography and hacking attacks like malware and virus. Moreover, UTM filters out ActiveX objects, Cookies or Java applets that may pose a security threat in certain situations. Both keywords and URLs of specified websites can be added to Blacklist and Whitelist.

Application Control

In order to prevent data leakage and ensure regulatory compliance, the access to applications which unrelated to work should be controlled during working hours. NU-880H can enforce policy for applications like P2P, VOIP, GoToMyPc, Webpages, Games, Media Player, Bit Torrent, Foxy (Gnutrlla), stock market, Instant Messaging, Xunlei, Gator, Yahoo Manager, Virus and Malware, filename extension, Kazaa, Facebook, etc.

URL Database

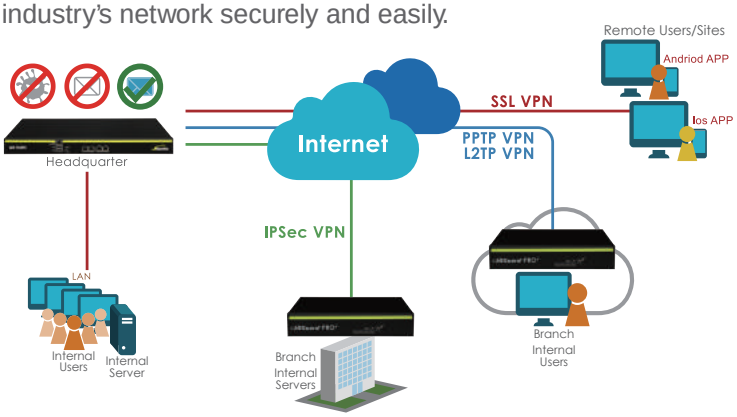
Built-in URL database collects almost 1,000,000 URLs and updates every period of time without additional charge. All these URLs and their contents were analyzed and classified into 12 categories, including Aggressive, Audio-Video, Drugs, Gambling, Hacking, Porn, Proxy, Redirector, Spyware, Suspect, Violence, and Warez. IT administrator is able to block any category in the database with ease without entering keywords or desired URL addresses one by one.

SSL VPN

SSL-based VPNs provide remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. It does not require any special-purpose client software to be pre-installed on the system. For remote clients, there are two different types of access. One is access to the internal network and the other is access to the Internet over VPN server. Administrators can control over bandwidth usage, VPN service and time from both accesses.

Remote-Access VPN

Remote-access VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to anyone, anyplace, anytime. ShareTech offers both IPSec VPN and PPTP VPN technologies on a single platform with unified management. IPsec VPN securing the site-to-site connections allows headquarters and their branch offices to be on the same network and sharing resources among offices. Moreover, PPTP VPN offers point to point connection for employees working at home. Employees can get access to industry's network securely and easily.



Flow Analysis

No matter whether internal users' computers are on or off, flow analysis tools can display real-time statistics, protocol distribution list, and rankings of traffic flows.

II. KEY FEATURES

Features	Description
Threats Defense **(Anti-Virus/IPS/SSL Inspection)**	1. Uses open source Clam AV engine with huge database includes more than 400,000 unique signatures 2. Kaspersky module (Optional); built-in 1 your for NU-880H 3. Clam AV team has fast response time, updates signature regularly and requires no yearly subscription fees 4. Provides IPS attack-signature database 5. IPS risk management is divided into 3 levels (high, medium, and low) 6. Provides scalable SSL inspection
Malicious URL Filtering **(URL & Databases)**	1. Provides URL filtering and database 2. URL filtering policies are allowed to be configured by administrators 3. IT administrator can add keywords or URLs to Black/White lists
Firewall Security	1. Coordinated DoS/DDOS attacks and UDP Flood performed by hackers can be blocked automatically. 2. QoS provides bandwidth guarantees and a priority command can be given for min/man bandwidth guarantee. 3. Limit the bandwidth using source IP in both directions 4. Supports IPv4, IPv6, and Dual Stack 5. Supports load balancing and failover for both outbound and inbound traffics 6. Provides DNS service and Dynamic DNS services
Potential Risks Detection **(Flow Analysis)**	1. Flow/behavior-based anomaly detection allows both up and down sessions 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 characteris tics 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	1. Multiple application categories e.g. P2P, IM, VOIP, Web, WebMail, game, video, spyware, stock and others. 2. Administrators can use policies to prohibit their users from accessing to applications
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. Applies access control methods 4. Provides authentication record and connection status

Features	Description
Content Record	1. Logs all incoming/outgoing emails with delivering date and time 2. Archived email is exported in. eml format 3. Records browsing history
Load Balance	1. Ensuring the network is never disconnected 2. Provides inbound & outbound load balancing 3. Users can assign load balancing automatically, manually, or by source-destination IP 4. Built-in Smart DNS Server
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 4. Supports IP Tunneling and definable policy control
QoS	1. Supports 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	NAT, Routing
Logging & Reports	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, bar/line graphs, and pie charts. 3. Provides analysis of debug, system performance, intrusion attempts, and tracking.
Virtual Server	IP 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
Eye Cloud	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 Eye Cloud service system
Bulletin Board	Announcement can be made to employees in a very effective and proper way
Diagnostic Tools	Standard net tools such as Ping, Traceroute, DNS lookup, and port scanner are available to help users identify and fix connection problems.
Others	1. The network is divided in zones and a zone can by managed by SDN 2. Administrators can select authorized users and assign access conditions 3. Automatic disk check can be scheduled 4. Supports SNMP 5. Supports VLAN 802.1Q 6. LCM display 7. Data backup and mount

III. SPECIFICATION

	NU-850C	NU-870H	NU-870C	NU-880H
Hardware				
Dimensions W*H*D(mm)	430*250*44	438*292*44	438*292*44	430*550*88
Platform Size	1U	1U	1U	2U
Recommended Users numbers	Under 200	Under 400	Under 400	1,000-2,000
LAN Bypass	•	•	•	•
Reset Button		•	•	•
USB	2.0	3.0	3.0	3.0
Capacity				
Ethernet Interfaces	14xGigabit	10xGigabit	18xGigabit	18xGigabit
UTM Throughput	6 Gbps	8 Gbps	9.6 Gbps	16.5 Gbps
VPN Throughput	0.8 Gbps	2 Gbps	2 Gbps	2.5 Gbps
IPS Throughput	0.65 Gbps	1 Gbps	1.2 Gbps	2 Gbps
Anti-Virus Throughput	0.7 Gbps	0.9 Gbps	0.9 Gbps	1.4 Gbps
Max. Concurrent Sessions	3,000,000	4,000,000	5,000,000	6,000,000
Mail Scan/Day	4,800,000	5,000,000	5,500,000	6,000,000
VPN Tunnels				
IPSec VPN Tunnels	3,000	6,000	8,000	12,000
PPTP Tunnels	1,200	2,000	3,000	4,000
SSL VPN Tunnels	1,200	2,000	3,000	4,000
IP Tunnel Tunnels	600	1,000	1,500	2,000
Network Protection				
Security Gateway	•	•	•	•
Kaspersky	1-year	1-year	1-year	1-year
HTTPS Filtering	•	•	•	•
Spam Filtering	•	•	•	•
IPS	•	•	•	•
IPS Signature Database	•	•	•	•
APP Access Control	Add network configuration, video, file transfer, remote control, browser, software update			
URL Database	•	•	•	•
Dashboard	APP, Mail, IPS, Web, Defense, Dynamic Sessions Analysis			
Reports	•	•	•	•
Mail Audit	•	•	•	•
Behavior Management	•	•	•	•
Anomaly IP Analysis	•	•	•	•
Co-Defense (Switch)	•	•	•	•
Load Balance (Outbound/Inbound)	•	•	•	•
QoS	•	•	•	•
Bulletin Board	•	•	•	•
Authentication	•	•	•	•
AP Management	• (100pcs)	• (300pcs)	• (300pcs)	• (Unrestricted)
Eye Cloud	•	•	•	•
High Availability	•	•	•	•
IPS Signatures	4,020	4,020	4,020	4,020
IPSec VPN	•	•	•	•
PPTP VPN	•	•	•	•
SSL VPN	•	•	•	•
Encrypted IP Tunnel Mode	•	•	•	•