SYSTROME

ASG-8600

Cumilon Series Firewall

Product Overview

Systrome's Next Generation Firewalls provides comprehensive security protection from layer 2 to layer 7 for the mobile Internet era. The new next generation security gateway is using x86 multi-core CPU architecture, combined with single path parallel processing mechanism to achieve user identification, application identification and other security detection. Systrome NGF can achieve in-depth analysis of users, applications and content to provide users high performance, visualization, accurate and effective integration of application layer security protection system.

Systrome next generation firewall support pipe based 4-level nested bandwidth management, in addition the firewall support link load balance technology to achieve comprehensive intelligent network management, combined with hot standby and VRRP technology to ensure high reliability. Systrome firewall can be flexibly deployed in transparent, NAT, VPN, multi-Link and other network environments, helping users conduct business and simplifying network security architecture.

High Performance: Systrome next generation firewall is using x86 multi-core architecture that expertise in complex business computing, combined with proprietary SystromeOS professional operating system to deliver high-speed, low-latency security system. Technologies like attack signatures, virus database storage tree, stream scanning process, zero copy parallel streams processing efficiency defence are using in SystromeOS, the whole resolution process only unpack once, ensure the effectiveness even after deploying multiple protective function.



Flexible virtualization extension: Systrome next generation firewall support virtualization technology, SystromeOS can be implemented in different virtual OS such as KVM, XEN, VMware, which realizes independent CPU, memory, interface, storage in the virtualization system achieving resource isolation and management isolation, the resource can be flexibly allocated according to resources to achieve performance improvements and platform extensions, which is the best security practices virtualization and cloud systems.

Unified security engine: Systrome next generation firewall provide customer user and application based unified security protection, providing user authentication and L4-L7 parallel processing engine to achieve multidimension, no-dead angle protection. Customer can setup IPS, anti-virus, web guard and content filter feature to prevent the Trojans, worms, SQL injection, XSS attacks and overflow attack to secure file transfer security, block bad sites and illegal links.

Accurate Internet behavior management and audit: Systrome next generation firewall takes user and application as core considerations of security protection utilizing advanced user and application identification technology to realize accurate management and audit of users and applications.

The system supports multiple identification modes such as IP/MAC binding, Radius, LDAP, Portal, SMS gateway. The system support almost 1000 Internet application identification and accurate control including major application, high-risk application and mobile applications, by application behaviour and content in-depth analysis, customer can refine and precisely control network making network management closer to user expectations.

Comprehensive Intrusion Protection: After 10 years network security and accumulated precipitation in the field, Systrome team built up senior attack signatures and security service team, always concerned about the industry's latest discovered security vulnerabilities and attack signatures received from users worldwide, and provide updates in real time to improve the attack signature database, provide the timely, comprehensive intrusion prevention. The system supports more than 3000 kinds of predefined attack signatures that can be real-time updated online, which provide effectively protection for worms, SQL injection, overflow and other attacks to ensure network security, besides the system can provide hierarchical events management and configurations management delivering user-oriented network.

Intelligent Bandwidth Management: Systrome next generation firewall can fully identify common Internet applications, such as P2P download, IM instant messaging, online video, stocks, games and so on, which often

results in Internet bandwidth abuse. By deploying firewall in the Internet, users can effectively curb various applications snatch valuable bandwidth and IT resources, thereby ensuring the rational allocation and quality of business-critical network resources, and significantly improve the overall performance of the network.

Independent VPN Module: Systrome firewall has built-in dedicated hardware VPN module that supports GRE, IPSec VPN and other business models. It supports multiple platforms mobile terminal VPN access. The firewall support VPN tunnel traffic management, which regulates online behaviour in the VPN tunnel management and eliminate blind spots. By configuring our cloud management software, VPN on scattered branches can be centralized managed, which achieves a unified configuration management, centralized alarm processing, unified log reporting, which reduced administrator workload.

Flexible Network Deploying: Systrome next generation firewall supports MCE\IPSEC, 802.1Q, GRE, VPN track and other network features, and support PPPoE, DHCP, VLAN, Trunk and other access methods. The firewall can be flexibly deployed in routing, transparent and mixed mode in network. The system supports IPv4/IPv6 dual stack to support NAT64, NAT66, NAT66 and other NAT technology, which can be easily deployed in v6, v4 network boundaries to upgrade network security.

Simple Configuration & Management: Systrome next generation firewall supports security policies centralized display, stand-alone configuration, integration testing tool, which provides users clear and visible policy and greatly improves user configuration and viewing experience. Users can control according to different needs for different users to customize different management strategies, flexible convenient, simple maintenance, and clear, with good results, such as Forwarding, application control policies, audit policies, intrusion detection strategies, antivirus policy, VPN policy, traffic control policies showcase, and stand-alone configuration.

High Availability: Systrome next generation firewall supports stateful failover, VRRP and hardware by-pass function, which prevents network bottleneck and failure point to ensure high network reliability. When the device CPU, memory and other parameters is above a certain threshold, the system will turn to automatic bypass mode, as a result the device becomes pure transparent forwarding without service interruption.

Hardware Specifications

| Hardware specifications | ASG 8600 |
|-------------------------|----------|
| Memory | 4 GB |



| MGT | 1MGT,1 HA |
|--|--|
| Fixed Port | 2GE |
| Expansion card/interface | 8* Slot |
| Dimension | - |
| Line Cards | 4GE 4SFP 8GE 8SFP 4GE+4SFP 2SFP+ 4SFP+ 2QSFP+ (2*40G) |
| Power | 2U, Redundant power |
| NGFW Throughput | 55G |
| Advanced Throughput (APP/IPS/AV) is ON | 32G |
| Throughput (1518 bytes) | 100G |
| Throughput (512 bytes) | 52G |
| Throughput (64 bytes) | 8.1G |
| New TCP Sessions | 13,00,000 |
| New HTTP Sessions | 11,00,000 |
| Maximum Concurrent sessions | 2,00,00,000 |
| NGFW Maximum Concurrent sessions | 1,00,00,000 |
| Ipsec Tunnels | 40,000 |
| Ipsec VPN Throughput | 12 G |
| Operating temperature | 0~40°C |
| Operating Humidity | 5%~95% |

Features

| Feature | Description |
|---------|---|
| Network | Support transparent, routing and mix mode |
| | Support physical, BVI, VLAN, port aggregation, tunnel, loopback interface |
| | Support GRE interface |
| | Support security domain |
| | Support PPPoE Client |
| | Support DHCP server and relay |
| | Support Static ARP, IP-MAC binding |
| | Support DNS client, server |
| | Support DNS proxy and intelligent DNS |
| | Support static routing, dynamic routing (RIP, OSPF, BGP4) |
| | Support applications and users based policy routing |



| Support ISP routing Support a variety of application protocols NAT Traversal Support TPTP, TFTP protocol non-standard ports ALG Frewall Support inverface / security domain/addresses/users/vervices/ applications and time based frewall policy Support TPTP, TFTP protocol non-standard ports ALG Support Step applications set as control Supports the applications set as control Support at a variety of applications set as control Support at a variety of applications set as control Support TOV DOS stack protection Support and tARP attacks and ARPFlood attack protection Support flow-based and packet count based TCP Flood, UDP Flood, ICMP Flood attack protection Support per IP based sessions blocking Support source based destination based and rule set based intrusion detection Support source Vased count based and rule set based intrusion detection Support To could be attack tog and alurn. Support CC attack detense Support TPTP, PDP, PDP3, SMTP, IMAP protocols viras remeval Ytrea detection on mailbody / attachments, web pages and download files included Support TAR file and other packaged viras detection Support TAR file and other packaged viras detection Support TAR file and other packaged viras detection | | |
|---|-----------------|--|
| Support a variety of apflication protocols NAT Traversal Support FTP, TTP protocol non-standard ports A1.6 Firewall Support interface / security domain/addresse/users/services/ applications and time based firewall policy Supports the applications of the source based of firewall policy Supports the applications of the source base control of Dievy real IM, streaming modia, P29 applications such as control Support attri-RTP TOP and ICCMP scanning protection Support attri-RTP info/addresse Support anti-RTP field defense Support anti-RTP field defense Support servicin Support assion blocking Support servicin Support servicin Support record the attack tog and alarm. Support record the attack tog and alarm. Support record the attack tog and alarm. Support servicin Support record the attack tog and alarm. Suppo | | Support ISP routing |
| Support FPP, TPTP protocol non-standard ports ALG Frewall Support interface / security domain/addressev/users/ services/ applications and time based firewall policy Support Support interface / security domain/addressev/users/ services/ support DOS attack, Protocola access control policy can IM, streaming media, P2P applications such as control Support SUP protection Support STCP, UDP and ICMP seaming protection Support anti-ARP attacks and ARPFlood attack protection Support anti-ARP attacks and ARPFlood attack protection Support support flow-based and packet count based TCP Flood, UDP Flood, ICMP Flood attack prevention Support source based, destination based and rule set based intrusion detection Support source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support Source based, destintation based based based based based dots, in: p.2p. vulnerabit | | Support source NAT, Destination NAT, static NAT |
| Firewall Support interface / security domain/addresses/users/ services/ applications and time based firewall policy Support Site application protocol access control policy can IM, streaming media, P2P applications such as control Support DOS attack protection Support TCP, UDP and ICMP scanning protection Support flow-based and packet count based TCP Flood, UDP Flood, ICMP Flood attack protection asset (Count based TCP Flood, UDP Flood, ICMP Flood attack protection asset (Count based TCP Flood, UDP Flood, ICMP Flood attack protection asset (Count based and rule set based intrusion detection Support Suid Support S kinds of sclf-define actions Support S inds of sclf-define actions Support Rough and Janual/automatic signulare upgrade Support S inds of sclf-define actions Support SUI injection, XSS attack defense Support SUI injection, SSS attack defense Support SUI injection, SSS attack defense Support SUI injection of unknown viruses Support SUI injection of unknown viruses Support SUI interface desed files such as virus detection Support SUI | | Support a variety of application protocols NAT Traversal |
| applications and time based freewall policy Supports the applications such as control Supports the applications such as control Support DOS attack protection Support STCP, UDP and ICMP scanning protection Support flow-based and packet count based TCP Flood, UDP Flood, ICMP Flood attack protections restrictions Support flow-based and packet count based TCP Flood, UDP Flood, ICMP Flood attack protections restrictions Support protocol-based long connection management Support protocol-based long connection management Support Skinds of self-define actions Support Skinds of self-define actions Support Skinds of self-define actions Support SQL injection, XSS attack defense Support SQL injection, XSS attack defense Support SQL injection or mail body / attachments, web pages and download files included files included Support Support source has acted chains detection Support SQL injection or mail body / attachments, web pages and download files included file included Support source has acted chains and integement Support Tark file and oher packaged virus detection <td></td> <td>Support FTP, TFTP protocol non-standard ports ALG</td> | | Support FTP, TFTP protocol non-standard ports ALG |
| Image: streaming media, P2P applications such as control Support DOS attack protection Support DOS attack protection Support SDC, UDP and ICMP scanning protection Support struct UDP and ICMP scanning protection Support anti-ARP attacks and ARPFlood attack protection Support anti-ARP attacks and ARPFlood attack protection Support part P4 tacks and ARPFlood attack protections Support source have and packet count based TCP Flood, UDP Flood, ICMP Flood attack prevention Support per IP based sessions and new connections restrictions Support source have, destination based and rule set based intrusion Support source have, destination based and rule set based intrusion Support Source have, destination based and rule set based intrusion Support Tocol-based long and atro. Support Source inclusion, pagenet Support CC attack log and atro. Support CC attack defense Support CC attack defense Support SDL injection, XSS attack defense Support SDL injection, XST attack defense Support theuristics detection of malibody / attachments, web pages and download Support interristics detection of unknown viruses Support TSDP (FDAR attack and and online tabatifies actions Support four injection of unknown viruses Support Interristics detection of unknown viruses Support four injection of unknown viruses Support Inter Atta Atta Read online | Firewall | applications and time based firewall policy |
| First Carter of the server of the s | | streaming media, P2P applications such as control |
| Average of the second | | Supports TCP, UDP and ICMP scanning protection |
| Av Support flow-based and packet count based TCP Flood, UDP Flood, ICMP Flood attack prevention Support per IP based sessions and new connections restrictions Support protocol-based long connection management Support source based, destination based and rule set based intrusion detection Support source based, destination based and rule set based intrusion detection Support source based, destination based and rule set based intrusion detection Support Skinds of self-define actions Support Skinds of self-define actions Support Skinds of self-define actions Support Skinds of self-define actions Support Skinds of self-define actions Support Skinds of self-define actions Support Cort attack log and alarm. Support Skinds of self-define actions Support Deter TSK Statesk defense Support CC attack defense Support CC attack defense Support CC attack defense Support Skinds detection on mail body / attachments, web pages and download files included Support surgive self set such as virus database updated regularly with timely Support TAR file and other packaged virus detection Support interface based uplink and downlink bandwidth management Support shifty, medium and low priority channel settings Support aptification/supers/source address/ service/ time based channel matching Support apprit application/supers/source address/ service/ time based channel matching | | Support smart TCP Flood defense |
| ICMP Flood attack prevention Support per IP based sessions and new connections restrictions Support session blocking Support source based, destination based and rule set based intrusion detection Support rotocol-based long connection management Support rotocol-based destination based and rule set based intrusion detections Support rocord the attack log and alarm. Support record the attack log and alarm. Support Cattack define actions Support Cattack defense Support Cattack defense Support Cattack defense Support Suita Statack defense Support Suita Statack defense Support Apri IPT, FTP, POP3, SMTP, IMAP protocols virus removal Yirus detection on mail body / attachments, web pages and download files included Support TAR file and other packaged virus detection Support TAR file and other packaged virus detection Support sprities detection of unknown viruses Support sprities bandwidth Support priper bigh, medium and low priority channel settings Support priper bigh, medium and low priority channel settings Support priper bandwidth Support sprities onclusions, sendvidth guarantees and elastic banativity Suport aprication/viers/source address/ serv | | Support anti-ARP attacks and ARPFlood attack protection |
| Support session blocking Support protocol-based long connection management Support source based, destination based and rule set based intrusion detection Support source based, destination based and rule set based intrusion Support scinds of self-define actions Support record the attack log and alarm. Support record the attack log and alarm. Support record the attack log and alarm. Support Cattack defonse Support Cattack defense Support Cattack defense Support HTTP, FTP, POPS, SMTP, IMAP protocols virus removal Yirus detection on mail body / attachments, web pages and download files included Support METTP, FTP, POPS, SMTP, IMAP protocols virus removal Yirus detection on mail body / attachments, web pages and download files included Supports ZIP / RAR compressed files such as virus detection Support Interface based uplink and downlink bandwidth management Support appritations/suers/source address/ service/ time based channel matching Support appritations/suers/source address/ service/ time based channel matching Support appritations/suers/source address/ service/ time based channel matching Support automatic traffic shaping Support automatic traffic shaping Suport uutomatic traffic shaping | | ICMP Flood attack prevention |
| Support protocol-based long connection management Support source based, destination based and rule set based intrusion detection Support 5 kinds of self-define actions Support 7 binds of self-define actions Support annual/automatic signature upgrade System-defined over 3000 rules, including Backdoor, buffer overflow, dosddos, im, p2p, vulnerability, scan, worm, game. Support CC attack defense Support CC attack defense Support HTTP, FTP, POP3, SMTP, IMAP protocols virus removal Virus detection on mail body / attachments, web pages and download files included Support AR file and other packaged virus detection Support TAR file and other packaged virus detection Support high, medium and low priority channel settings Support purphications/users/source address/ service/ time based channel matching Support purphications/users/source address/ service/ time based channel matching Support high, medium and low priority channel settings Support purphications/users/source address/ service/ time based channel matching Support paplications/users/source address/ service/ time based channel matching Support high, medium and low priority channel settings Support paplications/users/source address/ service/ time based channel matching Suport paplications/users/source address/ service/ time based channe | | |
| AV Support source based, destination based and rule set based intrusion detection Support Source based, destination based and rule set based intrusion detection Support 5 kinds of self-define actions Support manual/automatic signature upgrade Support manual/automatic signature upgrade System-defined over 3000 rules, including Backdoor, buffer overflow, dosddos, im, p2p, vulnerability, scan, worm, game. Support SQL injection, XSS attack defense Support CC attack defense Support BOU injection on mail body / attachments, web pages and download files included Supports Nore than 3 million virus detection, virus database updated regularly with timely Support SUP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support budwidth limitations, bandwidth management Support bindwidth limitations, bandwidth management Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per P based speed control Support per P based speed control Support automatic traffic shaping Support automatic traffic shaping | | |
| detection Support 5 kinds of self-define actions Support 7 kinds of self-define actions Support record the attack log and alarm. Support manual/automatic signature upgrade Support manual/automatic signature upgrade Support SUL injection, XSS attack defense Support CC attack defense Support CC attack defense Support MTTP, FTP, POP3, SMTP, IMAP protocols virus removal Virus detection on mail body / attachments, web pages and download files included Support SUP race than 3 million virus detection, virus database updated regularly with timely Support TAR file and other packaged virus detection Support TAR file and other packaged virus detection Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support high, medium and low priority channel settings Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support per IP based speed control Support automatic traffic shaping Support automatic traffic shaping | | Support protocol-based long connection management |
| HPS Support record the attack log and alarm. Support manual/automatic signature upgrade System-defined over 3000 rules, including Backdoor, buffer overflow, dosddos, im, p2p, vulnerability, scan, worm, game. Support SQL injection, XSS attack defense Support CC attack defense Support CC attack defense Support CC attack defense Av Support HTTP, FTP, POP3, SMTP, IMAP protocols virus removal Virus detection on mail body / attachments, web pages and download files included Supports more than 3 million virus detection, virus database updated regularly with timely Support supports ZIP / RAR compressed files such as virus detection Support interface based uplink and downlink bandwidth management Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support high, medium and low priority channel settings Support high, medium and low priority channel settings Support per H based speed control Support per IP based speed control Support per IP based speed control Support user-based, address exclusion policy | | detection |
| IPS Support manual/automatic signature upgrade System-defined over 3000 rules, including Backdoor, buffer overflow, dosddos, im, p2p, vulnerability, scan, worm, game. Support SQL injection, XSS attack defense Support CC attack defense Support CC attack defense Support SQL injection, XSS MTP, IMAP protocols virus removal Virus detection on mail body / attachments, web pages and download files included AV Support Band Support SZIP / RAR compressed files such as virus database updated regularly with timely Support SZIP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support Interface based uplink and downlink bandwidth management Support interface based uplink and downlink bandwidth management Support applications/users/source address/ service/ time based channel matching Support applications/users/source address/ service/ time based channel matching Support automatic traffic shaping Support automatic traffic shaping Support automatic traffic shaping Support suce-based, address exclusion policy | | |
| Av System-defined over 3000 rules, including Backdoor, buffer overflow, dosddos, im, p2p, vulnerability, scan, worm, game. Support SQL injection, XSS attack defense Support CC attack defense Support CC attack defense Support CC attack defense Virus detection on mail body / attachments, web pages and download files included Supports more than 3 million virus detection, virus database updated regularly with timely Support SUP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support Ine and nested channel based bandwidth management Support interface based uplink and downlink bandwidth management Support applications/users/source address/ service/ time based channel matching Support applications/users/source address/ service/ time based channel matching Support per IP based speed control Support per IP based speed control Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy Support user-based, address exclusion policy | IPS | |
| Support CC attack defenseSupport HTTP, FTP, POP3, SMTP, IMAP protocols virus removalVirus detection on mail body / attachments, web pages and download files includedSupports more than 3 million virus detection, virus database updated regularly with timely Support heuristics detection of unknown virusesSupports ZIP / RAR compressed files such as virus detection Support TAR file and other packaged virus detectionSupport interface based uplink and downlink bandwidth management Support high, medium and low priority channel settingsSupport applications/users/source address/ service/ time based channel matchingSupport per IP based speed control Support per IP based speed controlSupport automatic traffic shaping Support user-based, address exclusion policy | 11.5 | dosddos, im, p2p, vulnerability, scan, worm, game. |
| AV Support HTTP, FTP, POP3, SMTP, IMAP protocols virus removal Virus detection on mail body / attachments, web pages and download files included Supports more than 3 million virus detection, virus database updated regularly with timely Support heuristics detection of unknown viruses Support SZIP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support interface based uplink and downlink bandwidth management Support line and nested channel based bandwidth management Support pupications/users/source address/ service/ time based channel matching Support paper and downlink bandwidth management Support pupications/users/source address/ service/ time based channel Support port port pipications/users/source address/ service/ time based channel matching Support port part IP based speed control Support port per IP based speed control Support user-based, address exclusion policy | | |
| AV Virus detection on mail body / attachments, web pages and download files included Supports more than 3 million virus detection, virus database updated regularly with timely Supports more than 3 million virus detection, virus database updated regularly with timely Support heuristics detection of unknown viruses Support heuristics detection of unknown viruses Support TAR file and other packaged virus detection Support TAR file and other packaged virus detection Support line and nested channel based bandwidth management Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy Support user-based, address exclusion policy | | |
| AV files included Supports more than 3 million virus detection, virus database updated regularly with timely Support heuristics detection of unknown viruses Support SZIP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support TAR file and other packaged virus detection Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | | |
| AV regularly with timely Support heuristics detection of unknown viruses Supports ZIP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support line and nested channel based bandwidth management Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support bandwidth limitations/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support automatic traffic shaping Support automatic traffic shaping | | • |
| Supports ZIP / RAR compressed files such as virus detection Support TAR file and other packaged virus detection Support Iine and nested channel based bandwidth management Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | AV | regularly with timely |
| Traffic Control Support TAR file and other packaged virus detection Support line and nested channel based bandwidth management Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | | |
| Traffic Control Support line and nested channel based bandwidth management Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | | Supports ZIP / RAR compressed files such as virus detection |
| Traffic Control Support interface based uplink and downlink bandwidth management Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | | Support TAR file and other packaged virus detection |
| Traffic Control Support high, medium and low priority channel settings Support applications/users/source address/ service/ time based channel matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | Traffic Control | Support line and nested channel based bandwidth management |
| Traffic ControlSupport applications/users/source address/ service/ time based channel matchingSupport bandwidth limitations, bandwidth guarantees and elastic bandwidthSupport per IP based speed controlSupport automatic traffic shapingSupport user-based, address exclusion policy | | Support interface based uplink and downlink bandwidth management |
| Traffic Control matching Support bandwidth limitations, bandwidth guarantees and elastic bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | | Support high, medium and low priority channel settings |
| bandwidth Support per IP based speed control Support automatic traffic shaping Support user-based, address exclusion policy | | matching |
| Support automatic traffic shaping Support user-based, address exclusion policy | | |
| Support user-based, address exclusion policy | | Support per IP based speed control |
| | | Support automatic traffic shaping |
| IPv6 Support IPv4 / IPv6 dual stack | | Support user-based, address exclusion policy |
| | IPv6 | Support IPv4 / IPv6 dual stack |



| | Supports routing, transparent, mixed-mode deployment |
|--------------------|---|
| VPN | Support NAT66, NAT64 support cross-protocol conversion and NAT46 |
| | Support DNSv6 |
| | Support for IPv6 Static Routing |
| | Support device management and maintenance protocol: PING, HTTP, HTTPS, SSH, TELNET Support IPSecVPN |
| | Support shared key / certificate authentication negotiation |
| | Support gateway-to-gateway and remote access deployment models |
| Object Management | Support addresses, services, time, object-oriented program |
| | Support more than 1000 kinds of applications and regularly updated |
| | Support for user objects, user static binding |
| | Support for third-party user authentication servers: LDAP, RADIUS |
| | Support for local and user certificates issued by the CA centre, maintenance |
| | Support ISP address database |
| | Support 2000+ default IPS Event |
| | Support network health check template |
| System Management | Support WEB (HTTP / HTTPS), Command Line, Console to manage the configuration |
| | Support division administrator privileges, customize the administrator role |
| | Support SNMP v1, v2, v3 |
| | SNMP trap support configuration change |
| | Support local multi-configuration files store up to 10 files |
| | Support system resource usage monitoring abnormal, and saved as a file locally on the device and support to export |
| | Support web graphical network debugging, diagnostic commands and packet capture |
| Virtual Firewall | Support L2-L7 business full virtualization, each virtual system run independently, and have independent administrator to configure |
| | Support allot CPU, memory, network I / O resources on demand |
| High Available | Support Active-Active and Active-Standby Mode |
| | Transparent mode |
| | Backup machine can be managed by configuring out-band IP management |
| | Supports VRRP protocol |
| | Supports heartbeat signal lost, the link disconnecting, the remote service not reachable, and other means of switching conditions and logic HA Support automatic synchronization session in HA devices, to ensure that any service interruption occurs when switching HA |
| | Support pre-emptive priority, high priority device can automatically seize master status |
| Log and Monitoring | Support streaming log, NAT conversion log, real-time attacks log, flow alarm logs, Internet behaviour management logs, network intrusion detection logs, virus protection logs |
| | Support local log save and send syslog |



| | Support mail alert |
|--|--|
| | Support real-time traffic statistics and analysis functions |
| | Support online user monitoring, query, freeze |
| | Session system state monitoring |
| | Support Interface status monitoring, interface packet transceiver, interface forwarding rate, etc. |
| | Top10 application supports traffic statistics and trends chart |
| | Support Top10 user traffic statistics and trends chart |
| | |
| | |
| | |
| | |
| | |
| | |



Copyright 2022 Systrome Networks Limited. All rights reserved. Systrome, the Systrome logo are registered trademarks of Systrome Networks Limited.

All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Systrome Networks assumes no responsibility for any inaccuracies in this document. Systrome Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. www.systrome.com info@systrome.com