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 multi-dimension, 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, NAT46, 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 source NAT, Destination NAT, static NAT
	Support a variety of application protocols NAT Traversal
	Support FTP, TFTP protocol non-standard ports ALG
Firewall	Support interface / security domain/addresses/users/ services/ applications and time based firewall policy
	Supports the application protocol access control policy can IM, streaming media, P2P applications such as control
	Support DOS attack protection
	Supports TCP, UDP and ICMP scanning protection
	Support smart TCP Flood defense
	Support anti-ARP attacks and ARPFlood attack protection
	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 session blocking
	Support protocol-based long connection management
IPS	Support source based, destination based and rule set based intrusion detection
	Support 5 kinds of self-define actions
	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
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
	Supports ZIP / RAR compressed files such as virus detection
	Support TAR file and other packaged virus detection
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
IPv6	Support IPv4 / IPv6 dual stack

	Supports routing, transparent, mixed-mode deployment
	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
VPN	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

www.systrome.com
info@systrome.com