EdgeWave™

MILITARY-GRADE CYBER SECURITY

EdgeWave EPIC USG6300 Series Next-Generation Firewall

Enterprise networks are evolving into next-generation networks that feature mobile broadband, big data, social networking and cloud services. Yet, mobile applications, Web2.0 and social media expose enterprise networks to the risks on the open Internet. Cybercriminals can easily penetrate a traditional firewall by spoofing or using Trojan horses, malware or botnets.

EdgeWave EPIC USG6300 series is designed to address these challenges and provide a reliable and secure network for small and medium-sized enterprises. It analyzes intranet service traffic from six dimensions, including application, content, time, user, attack, and location and then automatically generates security policies as suggestions to optimize the security management and provide high-performance application-layer protection for enterprise networks.

Product Features

Granular Application Access Control

- Identifies the application-layer attacks and their application, content, time, user, and location information.
- Provides all-round visibility into service status, network environment, security postures, and user behaviors.
- Provides an analysis engine that integrates application identification and security functions, such as IPS, AV, and data leak prevention, to prevent application-based malicious code injections, network intrusions, and data interceptions.

Excellent Performance

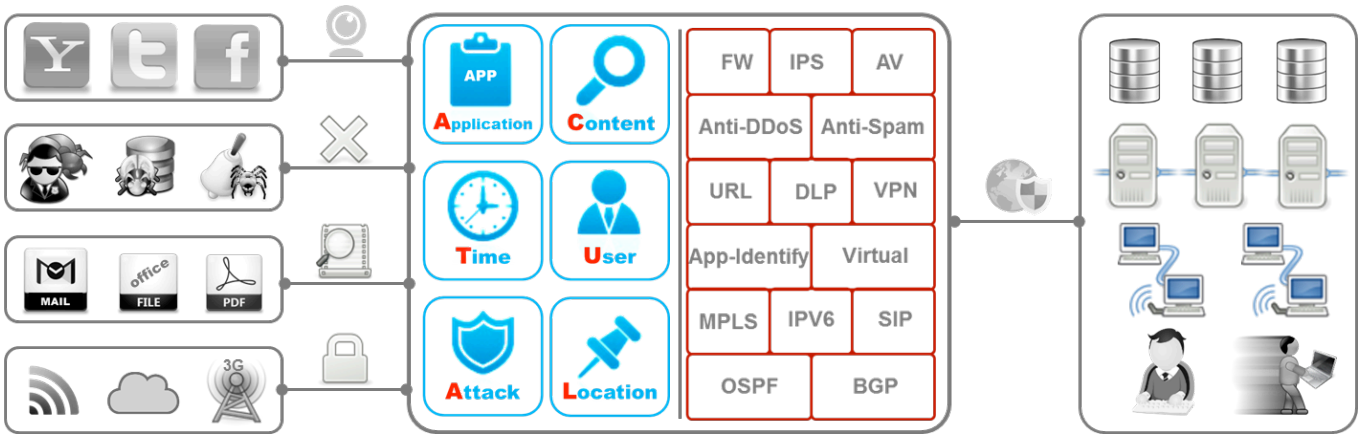
- Provides an Intelligent Awareness Engine (IAE) capable of parallel processing with all security functions enabled after intelligent application identification.
- Improves application-layer protection efficiency and ensures the 10G+ performance with all security functions enabled.

Easy Security Management

- Complies with the minimum permission control principle and automatically generates policy tuning suggestions based on network traffic and application risks.
- Analyzes the policy matching ratio and discovers redundant and invalid policies to remove policies and simplify policy management.

Prevention of Unknown Threats

- Prevent Advanced Persistent Threat (APT) attacks using a reputation system.



EdgeWave™

MILITARY-GRADE CYBER SECURITY

EdgeWave EPIC USG6300 Series Next-Generation Firewall

Specifications				
Model	**USG6320**	**USG6330**	**USG6350**	**USG6370**
Firewall throughput	2 Gbit/s	1 Gbit/s	2 Gbit/s	4 Gbit/s
IPS throughput	700 Mbit/s	500 Mbit/s	1 Gbit/s	2 Gbit/s
IPS+AV throughput				
Concurrent sessions	50,000	1,500,000	2,000,000	4,000,000
New sessions per second	20,000	30,000		60,000
VPN Throughput (IPSec, 3DES)	400Mbit/s			3 Bbit/s
Virtual firewalls	20	50		100
Fixed port	4GE+2Combo			8GE+4SFP
Expansion Slots	2 x WSIC			
Interface module	-	2 x 10GE (SFP+)+8 x GE (RJ45), 8 x GE (RJ45), 8 x GE (SFP), 4 x GE (RJ45) BYPASS		
Height	1U			
Dimensions (H x W x D)	442*421*43.6			
Weight (full configuration)	10 Kg			
HDD	Optional. Supports single 300 GB hard disks (hot swappable).			
Redundant power supply	Optional			
AC power supply	100 V - 240V			
DC power supply	-			
Maximum power	170W			
Operating environment: (Temperature/ Humidity)	Temperature: 0°C to 40°C/5°C to 40°C (with optional HDD) Humidity: 10% to 90%			
Non-operating environment	Temperature: -40°C to 70°C/Humidity: 5% to 95%			

EdgeWave™

MILITARY-GRADE CYBER SECURITY

EdgeWave EPIC USG6300 Series Next-Generation Firewall

Functions	
Context awareness	ACTUAL (Application, Content, Time, User, Attack, Location)–based awareness capabilities
	Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security)
Application security	Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases
	Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications
	Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks
Intrusion prevention	Provides over 3500 signatures for attack identification.
	Provides protocol identification to defend against abnormal protocol behaviors.
	Supports user-defined IPS signatures.
Web security	Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 80 categories
	Defense against web application attacks, such as cross-site scripting and SQL injection attacks
	HTTP/HTTPS/FTP-based content awareness to defend against web viruses
	URL blacklist and whitelist and keyword filtering
Security virtualization	Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)
Network security	Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks
	VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE
Routing	IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6
Intelligent management	Evaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy matching ratio analysis and the detection of conflict and redundant policies to remove them, simplifying policy management.
	Provides a global configuration view and integrated policy management. The configurations can be completed in one page.
	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.

15333 Avenue of Science, Suite 100
San Diego, CA 92128

Give us a call
1-855-881-2004

Send us an email:
info@edgewave.com

For more info, visit us at:
www.EdgeWave.com