ARKOON NETWORK SECURITY

Medium Series

Medium-500 / Medium-1000

Appliances UTM FAST360

Network Processor Appliance (NPA)

Common Criteria EAL2+ CERTIFIED

Medium-series devices are security appliances meeting the requirements of large to midsize companies looking for a solution combining multi-functional security, performance, and a high level of connectivity. The neutralization and detection measures deployed in the event of an attack on applications provide a faultless level of protection for the entire information system (VoIP, e-mail client, Intranet, etc.) without compromising on performance. The winning combination of these characteristics means that the Arkoon Medium Series appliances offer the best "functionality/performance/price" ratio in its market segment.

Key Features

Firewall, intrusion prevention and detection

Firewall engine based on patented FAST – Fast Applicative Shield Technology.
Real-time analysis of network layer, transport layer and application layer protocols.
FAST in line IDPS using an intelligent signature-based approach to detect and block attacks.
Common Criteria EAL2+ certified.

BENEFITS ////////////////////////////

- High performance of real-time analysis
- Durability of an engine that is regularly updated with new application modules (more than 20 application layer protocols)
- Prevention of attacks which do not break protocol rules and elimination of false positives
- Blocking of P2P (peer-to-peer) and instant messaging traffic

Cluster

The Clustering service is used to implement two appliances in parallel, providing identical services.

BÉNÉFICES ////////////////////////////

- High Availability mode (active/passive) => service continuity without any reduction in performance
- High Performance mode (active/active) => distribution of heavy workloads over 2 appliances connected in parallel.

VoIP Security

Segmentation and security of VoIP traffic through adaptive synchronised analysis and filtering by the FAST and IDPS engines of voice signalling (SIP, MGCP, SDP, H323) and data (RTP/RTCP) protocols.

BENEFITS ////////////////////////////

- Protect VoIP applications, IP PBXs, telephone system servers and terminals
- Detect and respond to unwanted, unauthorized or illicit incoming and outgoing calls
- Protect call confidentiality
- Protect against DOS (Denial of Service) attacks
- Block SPIT (Spam over IP Telephony), call spamming, IM spamming

Content Filtering

Antivirus and antispyware protection on smtp, pop3, http, ftp.

Integrated antivirus and antispyware engine developed by Sophos and incorporating Sophos Genotype™ technology.

Heuristic Antispam and E-mail filtering

Integrated advanced heuristic spam analysis engine, filters incoming and outgoing email (smtp and pop3).
Additionally email can be filtered on the basis of key words, white/blacklist entries, file attachments, time of day…

URL and Web filtering

Integrated web filtering engine allows blocking of javascript, activX and other applets/embeds, and filters URLs in 50 categories regularly updated and customisable to adapt to business localisation and activity.

BENEFITS ////////////////////////////

- The only UTM appliances integrating genuine heuristic antispam filtering
- Improve web and email performance
- Protect against dangerous or undesirable content
- Enhanced protection through mutliple complementary filtering techniques

IPSEC VPN

Integrated IPSec VPN functionality supports encrytped tunnels for secure site-to-site, remote office or road-warrior interconnectivity.

BENEFITS ////////////////////////////

- Secure site-to-site interconnection over non-secure networks with support for backup link configurations and multi-link load balancing
- Encryption of confidential data exchanges
- Easy, automated configuration simplified with VPN community management

Dynamic Routing and QoS

FAST360 appliances incorporate support for dynamic routing (RIP, OSPF and BGP), VLAN management and bridge mode operation.
Port trunking, bandwidth management and load sharing features facilitate QoS management.

BENEFITS ////////////////////////////

- VLAN-based traffic filtering
- Network traffic optimisation and load sharing

Authentication

FAST360 UTM appliances are compatible with LDAP, Radius, AD (including Windows 2003) and NT authentication servers and support certificate-based strong authentication. Capable of interfacing with external PKI servers, FAST360 appliances easily integrate into enterprise certificate architectures, allowing user-based traffic filtering.

BENEFITS ////////////////////////////

- Manage and filter traffic and access to resources
- Compatible with pre-existing authentication architectures

Centralized Management

FAST360 appliances are delivered with Arkoon Tools, a software suite allowing for centralized GUI-based configuration, deployment and monitoring of consistent entreprise-wide security policies across multiple FAST360 appliances. FAST360 appliances can also be managed through Arkoon Management Center, a server-based solution ideal for larger networks.

BENEFITS ////////////////////////////

- Optimized management, reduced cost of ownership

Specifications

Medium Series

Medium-500 / Medium-1000

Cavium Octeon Multicore Processors

The Network Processor Appliances are fitted with the latest Cavium Octeon multicore technology.

This technology, optimized for network processing, brings the following advantages:

- Very significant reduction in latency in the processing of flows so as to reach very high speeds regardless of the size of the packets transported.
- Remove bottlenecks by reserving (for example) one or more cores of the Cavium processor for special processing operations.*
- Optimize some intensive processing operations (routing, encryption, etc.) by executing them closer to the hardware.*

* Version FAST360 PostV5.0

	Medium-500	Medium-1000
Performance		
Firewall rate (Mbps)	500	1020
VPN rate (Mbps)	150	300
Application Filtering rate (FAST+IDPS) (Mbps)	130	250
Simultaneous connections	120 000	120 000
New connections / second	5 850	11 500
Number of Users	unlimited	unlimited
Hardware characteristics		
Processor / Number of cores	Cavium Octeon / 1 core	Cavium Octeon / 2 cores
Console port	1 (RJ45)	
USB Port *	-	
Gigabit switch	-	
Fast Ethernet 10/100 ports	2	
Gigabit copper 10/100/1000 ports	3	
Hard Disk Capacity	SATA 80 GO	
Firewall VPN		
FAST Application Filtering – Intrusion Prevention System		
Real-time filtering (hub mode)	yes	
Protocols analyzed– levels 3,4	IP, TCP, UDP, ICMP	
Application protocols analyzed	http, ftp, smtp, pop3, nntp, dns, dns udp, SQLNet, snmp, flux netbios, imap4, H323, sip, mgcp, SSL/TLS	
Protection against DOS and DDOS	yes	
Protection against protocol violations	yes	
VoIP Security		
Checking signaling (SIP/MGCP/H.323/SDP)	yes	
Checking media flows (RTP/RTCP)	yes	
Adaptive Filtering: Correlation between the analysis of media flows and signaling	yes	
FAST Intrusions Detection System (IDPS)		
Contextual analysis base	yes	
Operation in the event of failure or in alert mode	yes	
Automatic updating of the signature base	yes	
IPSEC VPN		
Authentication	X509 Certificate, shared keys, RSA keys	
Encryption algorithms	DES, 3DES, AES, Blowfish	
Advanced functions	Traversal NAT, Dead Peer Detection	

* Future utilization

Specifications

Medium Series

Medium-500 / Medium-1000

	Medium-500	Medium-1000
Authentication		
By flow with Arkoon authentication agent	yes	
Directories supported	NT, Act. Directory, Radius, LDAP	
By digital certificates (external and internal appliance PKI)	yes	
Strong authentication (Token, smartcard, RSA Secure ID…)	yes	
Content analysis		
Antivirus & Antispyware		
Antispyware integrated	yes	
Viral genotype viral (proactive detection of viruses)	yes	
Flows analyzed	HTTP, SMTP, POP3, FTP	
Number of viruses detected	> 100 000	
Automatic, centralized updating	yes	
URL filtering and Web filtering		
URL filtering	yes	
Automatic updating of URL bases	yes	
ICAP support for URL filtering	yes	
Blocking of Java, Activ X applets	yes	
E-mail filtering and anti-spam		
E-mail filtering	By keywords, senders, recipients, attachments	
Antispam analysis method	DNSBL and "Recurring Pattern Detection" for incoming and outgoing e-mails" (pop3 et SMTP)	
External quarantine	yes	
Network functions		
Routing - Mode of operation		
Static and Dynamic Routing	RIP, OSPF, BGP	
Transparent Mode (Level 2)	yes	
NAT / PAT	yes	
PPTP, PPPoE, PPPoA, IP over ATM	yes	
Filtering via VLAN	802.1q mode	
Number of VLAN supported	4095	
DHCP	Relay & Server	
Load allocation - Quality of Service		
Link backup	Yes: WAN & VPN	
Load allocation	Yes: WAN & VPN	
Aggregation of links	yes	
Quality of Service: prioritization of flows, queue management and marking	Diffserv compliancy	
Availability		
Supported modes	High-availability (Active/Passive) and High-Performance (Active/Active)	
Number of nodes	2	
Restart of active connections	Yes	

Specifications

Medium Series

Medium-500 / Medium-1000

	Medium-500	Medium-1000
Administration		
Configuration via Arkoon Manager (Windows and Linux)	yes	
Monitoring & Supervision via Arkoon Monitoring (Windows & Linux)	yes	
Role Management	Yes (6 predefined roles)	
Centralized, Secure Administration (SSL)	yes	
LAN/WAN remote connections	yes	
Console mode and command line mode	yes	
Remote updating of system	yes	
Alarm reporting	By email, console, SNMP traps	
SNMP supervision (MIB standard)	yes	
Syslog compatibility	yes	
WebTrend compatibility	yes	
Arkoon Management Center (AMC) compatibility	yes	
Dimension / Environment		
Format	Rack 1U	
L / W / H (mm)	429 / 260 / 44	
Weight	3,2 Kg	
Operating temperature	0 to 40°C	
Operating humidity	20 to 90%	
Storage temperature	0 to 75°C	
Storage humidity	5 to 95%	
Power Supply	100/ 240 Vac	
Frequency of Supply	48 – 63 Hz	
Max. Elect Power	65 W	
Certifications	CE, FCC, ROHs, UL	

See all our products and their detailed datasheets on: www.arkoon.com

ARKOON

1, Place Verrazzano - CS 30603
69258 Lyon Cedex 09 - France
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60
www.arkoon.com

ADAPTIVE SECURITY
FAST360 Appliances
Arkoon Management Center