



Appliances UTM FAST360

Network Processor Appliance (NPA)



Les équipements de la série Medium sont des appliances de sécurité qui répondent aux exigences des moyennes et grandes entreprises qui souhaitent disposer d'une solution combinant sécurité périmétrique multi-fonctions, performance et haute connectivité. Les dispositifs de détection et de neutralisation d'attaques applicatives permettent une protection sans faille de l'ensemble du système d'information (VoIP, Messagerie, Intranet...) sans concession de performance. Autant de caractéristiques qui font des appliances Medium Series, les équipements de sécurité offrant à ce jour le meilleur rapport "fonctionnalités/performance/prix" sur son segment de marché.

Principales fonctionnalités



Firewall, prévention et détection d'intrusions

Moteur firewall basé sur la technologie brevetée FAST – Fast Applicative Shield Technology
Analyse en temps réel des protocoles réseau, transport et applicatifs.
IDS en coupure, FAST in line IDPS : détection des attaques applicatives à partir d'une base de signatures "contextuelle".
Technologie certifiée Critères Communs EAL2+.

- BÉNÉFICES** //
- Haute performance d'une analyse en temps réel sans impact sur le réseau.
 - Contrôle de plus de 20 protocoles applicatifs.
 - Base contextuelle garantissant la neutralisation des attaques sans violation protocolaire et l'élimination des faux positifs
 - Capacité à interdire les flux non productifs ou malicieux (Peer to Peer, messageries instantanées, Skype, Malware, phishing...)

Cluster

Le Service Clustering permet à 2 appliances en parallèle de fournir des services identiques

- BÉNÉFICES** //
- Mode "Haute-Disponibilité" (actif-passif) continuité du service sans aucune dégradation de performance.
 - Mode "Haute-Performance" (actif-actif) : répartition des fortes charges sur 2 équipements en parallèle

Protection de la voix

Sécurisation & Isolation des flux VoIP au travers de l'analyse des protocoles de signalisation et de transport de la voix, SIP, MGCP, SDP, H323, RTP/RTCP

(analyse FAST et IDPS). La sécurisation de la VoIP bénéficie de l'ADAPTIVE FILTERING qui permet de contrôler le flux de données en fonction du flux de signalisation.

- BÉNÉFICES** //
- Protection des applications VoIP, des IP PBX, des serveurs et terminaux de téléphonie
 - Détections et/ou isolation d'appels non conformes ou non désirés, en entrée et en sortie
 - Protection de la confidentialité des appels
 - Blocage du call spamming et IM spamming

Filtrage de contenu

Antivirus et antispyware sur les protocoles smtp, pop3, http, ftp.

Moteur antivirus et antispyware intégré, développé par SOPHOS. Il bénéficie de la technique de génotype viral (signatures génériques pour des familles de virus).

Antispam « Temps réel » et Filtrage mail

Issue d'un partenariat avec COMMTOUCH, cette technologie consiste à confronter une empreinte du message à une base de données centralisée.

Filtrage d'URL et filtrage web

Les appliances bénéficient nativement d'un moteur de filtrage Web qui permet de bloquer les applets hostiles et des URL classées dans près de 50 catégories mises à jour automatiquement.

- BÉNÉFICES** //
- Blocage des contenus indésirables et dangereux
 - Technologie Antispam, offrant les meilleurs ratios taux de détection et taux de faux positifs (moins de 0,001%)
 - Complémentarité et interaction entre les différentes analyses de contenu

VPN IPSEC

La fonctionnalité de passerelle VPN IPSEC intégrée dans toutes les appliances FAST360 permet de créer simplement des tunnels chiffrés site à site ou nomades.

- BÉNÉFICES** //
- Interconnexion sécurisée de sites au travers

d'Internet avec gestion des liens de secours et de la répartition de charge

Services Réseaux et QoS

Les appliances FAST360 proposent nativement le routage dynamique (protocoles RIP, OSPF et BGP), la gestion de VLAN, le mode bridge et un module DHCP (relais et serveur). Elles offrent également des fonctions d'agrégation de liens, de répartition de charge et un module de Qualité de Service (QoS) conforme à la norme Diffserv.

- BÉNÉFICES** //
- Intégration dans tout type d'architecture existante
 - Optimisation du trafic par priorisation des flux, gestion des files d'attente et répartition de la charge

Authentification

Les appliances UTM FAST360 sont compatibles avec les technologies d'authentification LDAP, Radius, NT et les systèmes d'authentification forte à base de certificats.

- BÉNÉFICES** //
- Contrôle de l'accès aux applications
 - Adaptabilité à la politique d'authentification existante

Administration centralisée

Les outils graphiques Arkoon Tools permettent nativement la conception, le déploiement et la supervision de la politique de sécurité de façon centralisée et sécurisée.

Six profils différents permettant de répartir les tâches d'administration sont disponibles.

Les équipements de sécurité Arkoon sont compatibles avec AMC (Arkoon Management Center) la plateforme dédiée d'administration centralisée pour la gestion des architectures complexes.

- BÉNÉFICES** //
- Optimisation et simplification des opérations d'administration et de maintenance et des coûts liés à celles-ci
 - Adaptation à l'organisation de l'entreprise



Processeurs Multicoeur Cavium Octeon

Les appliances de la gamme "Network Processor Appliance" intègrent les processeurs de dernière génération "Multicoeur Cavium Octeon".

Cette technologie, particulièrement optimisée pour les traitements réseau, permet de :

- Diminuer très fortement la latence dans le traitement des flux pour atteindre des débits exceptionnellement élevés quelle que soit la taille des paquets transportés.

- Supprimer les goulots d'étranglement en dédiant un ou plusieurs cœurs du processeur Cavium à des traitements particuliers*

- Optimiser certains traitements lourds (routage, chiffrement...) en les exécutant au plus près du Hardware*.

* Version FAST360 PostV5.0

	Medium-500	Medium-1000
Performance		
Débit Firewall (Mbps)	500	1020
Débit VPN (Mbps)	150	300
Débit Filtrage applicatif (FAST+IDPS) (Mbps)	130	250
Connexions simultanées	120 000	120 000
Nouvelles connexions / seconde	5 850	11 500
Nombre d'utilisateurs	illimité	illimité
Caractéristiques Hardware		
Processeur / Nombre de cœurs	Cavium Octeon / 1 cœur	Cavium Octeon / 2 cœur
Port console	1 (RJ45)	
Port USB *	-	
Switch Gigabit	-	
Ports FastEthernet 10/100	2	
Ports Gigabit cuivre 10/100/1000	3	
Capacité disque	SATA 80 GO	
Firewall VPN		
Filtrage Applicatif FAST – Intrusions Prevention System		
Filtrage temps réel (mode noyau)	oui	
Protocoles analysés niveau 3, 4	IP, TCP, UDP, ICMP	
Protocoles applicatifs analysés	http, ftp, smtp, pop3, nntp, dns, dns udp, SQLNet, snmp, flux netbios, imap4, H323, sip, mgcp, SSL/TLS	
Protection contre DOS et DDOS	oui	
Protection contre les violations de protocoles	oui	
VoIP Security		
Contrôle de la signalisation (SIP/MGCP/H.323/SDP)	oui	
Contrôle des flux média (RTP/RTCP)	oui	
Adaptive Filtering : Corrélation entre l'analyse des flux média et signalisation	oui	
Intrusions Detection System FAST IDPS		
Base d'analyse contextuelle	oui	
Fonctionnement en coupure ou en mode alerte	oui	
Mise à jour automatique de la base de signatures	oui	
VPN IPSEC		
Authentification	Certificat X509, clés partagés, clés RSA	
Algorithmes de chiffrement	DES, 3DES, AES, Blowfish	
Fonctions avancées	Traversal NAT, Dead Peer Detection	



	Medium-500	Medium-1000
Authentification		
Par flux avec agent d'authentification Arkoon		oui
Annuaire supportés		NT, Act. Directory, Radius, LDAP
Par certificats numériques (PKI interne appliance et externe)		oui
Authentification forte (Token, carte à puce, RSA Secure ID...)		oui
Analyse de contenu		
Antivirus et Antispyware		
Antispyware intégré		oui
Génotype viral (détection proactive des virus)		oui
Flux analysés		HTTP, SMTP, POP3, FTP
Nombre de virus détectés		> 100 000
M-à-j automatique et centralisée		oui
Filtrage URL et Filtrage Web		
Filtrage d'URL		oui
Mise-à-Jour automatique des bases d'URL		oui
Support ICAP pour filtrage URL		oui
Blocage applets Java, Activ X		oui
Filtrage Mail et Antispam		
Filtrage mail		par mots clés, émetteurs, destinataires, pièces jointes
Méthode d'analyse Antispam		DNSBL et "Recurrent Pattern Detection (CommTouch)" pour les mails entrants et sortants (pop3 et SMTP)
Quarantaine externe		oui
Fonction réseaux		
Routage - mode de fonctionnement		
Routage statique et dynamique		RIP, OSPF, BGP
Mode transparent (niveau 2)		oui
NAT / PAT		oui
PPTP, PPPoE, PPPoA, IP over ATM		oui
Filtrage par VLAN		Mode 802.1q
Nombre de VLAN supportés		4095
DHCP		Relai et Serveur
Répartition de charge - Qos		
Secours sur lien		Oui : WAN et VPN
Répartition de charge		Oui : WAN et VPN
Agrégation de liens		oui
Qualité de Service - priorisation des flux, gestion des files d'attente et marquage		Conformité Diffserv
Disponibilité		
Modes supportés		Haute disponibilité (Actif-Passif) et Haute Performance (Actif-Actif)
Nombre de noeuds		2
Reprise des connexions actives		Oui



	Medium-500	Medium-1000
Administration		
Configuration via Arkoon Manager (Windows et linux)		oui
Monitoring et Supervision via Arkoon Monitoring (Windows et linux)		oui
Gestion des rôles		Oui (6 rôles prédéfinis)
Administration centralisée et sécurisée (SSL)		oui
Connexions à distance LAN/WAN		oui
Mode console et ligne de commandes		oui
Mise à jour à distance du système		oui
Remontées d'alertes		par Email, console, traps SNMP
Supervision SNMP (MIB standard)		oui
Compatibilité Syslog		oui
Compatibilité WebTrend		oui
Compatibilité Arkoon Management Center (AMC)		oui
Dimension / Environnement		
Format		Rack 1U
L / l / H (mm)		429 / 260 / 44
Poids		3,2 Kg
Température de fonctionnement		0 à 40°C
Humidité de fonctionnement		20 à 90%
Température de stockage		0 à 75°C
Humidité de stockage		5 à 95%
Alimentation		100/ 240 Vac
Fréquence		48 – 63 Hz
Puissance électrique max		65 W
Certifications		CE, FCC, ROHS, UL

Retrouvez l'ensemble de la gamme FAST360 et leurs fiches détaillées sur : www.arkoon.net



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.net

