

Appliances UTM FAST360



Le A5200 est un équipement permettant, non seulement d'offrir une grande modularité dans sa connectivité grâce à ses modules d'extension, mais aussi de soutenir les hautes performances des réseaux les plus exigeants (4Gbps de débit Firewall). Le A5200 propose en standard 8 interfaces gigabit cuivre et 2 ports 10/100 et peut évoluer vers des configurations nécessitant jusqu'à 16 interfaces Giga et 2 interfaces 10/100. Cette appliance haut de gamme est leader sur son segment de marché car elle garantit des performances hors du commun dans tous les domaines de protection et d'analyse (aussi bien Firewall, qu'IDPS, VPN IPSEC, filtrage de contenu, antivirus, antispam...).



Principales fonctionnalités



Firewall, prévention et détection d'intrusions

Moteur d'analyse applicative basé sur la technologie brevetée FAST – Fast Applicative Shield Technology. Analyse en temps réel des protocoles réseau, transport et applicatifs. FAST in line IDPS : sonde de prévention et de détection d'intrusion pour se protéger des attaques 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 d'implémenter 2 appliances en parallèle qui fournissent 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 plus de 60 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



	A5200
Performance	
Débit Firewall (Mb/s)	4 000
Débit VPN 3DES (Mb/s)	200
Débit VPN AES (Mb/s)	500
Débit du filtrage applicatif (Mb/s)	2 800
Connexions simultanées	1 000 000
Nouvelles connexions / seconde	40 000
Nombre de tunnels VPN	illimités
Interfaces	
Port console	1
Ports FastEthernet 10/100	2
Ports Gigabit Ethernet Cuivre 10/100/1000	8
Slots optionnels d'extension du nombre d'interfaces	
Nombre de slots optionnels	2
Type de modules optionnels d'extension de nombre de ports (fourni sans Gbic)	4 ports SFP Ports 10/100/1000 fibre pour slots optionnels 4 ports cuivre Ports 10/100/1000 cuivre pour slots optionnels
Routage et mode de fonctionnement	
Routage statique	oui
Routage dynamique	RIP, OSPF, BGP
Mode transparent (niveau 2)	oui
NAT / PAT	oui
PPTP, PPPoE, PPPoA, IP over ATM	oui
Filtrage par VLAN	oui
Nombre de VLAN supportés	illimité
Firewall - 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, h323, SQLNet, snmp, flux netbios, imap4, sip, mgcp, sdp, rtp, rtcp, ssl/tls
Protection contre DOS et DDOS	oui
Protection applicative contre les violations de protocoles	oui
Intrusions Detection System - FAST in line IDPS	
Base d'analyse contextuelle	oui
Fonctionnement en coupure	oui
Fonctionnement alerte seulement	oui
Mise à jour automatique de la base de signatures	oui
Possibilité de créer ses propres signatures IDPS	oui
VoIP Security	
Contrôle de la signalisation (SIP/MGCP/H.323/SDP)	oui
Contrôle des flux média (RTP/RTCP)	oui
Corrélation entre l'analyse du flux média et du flux signalisation	oui
VPN IPSEC	
Algorithme de chiffrement	DES, 3DES, AES, Blowfish, SHA-1 / MD5
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

	A5200
Filtrage URL et Filtrage Web	
Filtrage d'URL	oui
M-à-J automatique des bases d'URL	oui
Support ICAP pour filtrage URL	oui
Blocage applets Java, Activ X	oui
Antispam et filtrage Mail	
Filtrage mail	par mots clés, émetteurs, destinataires, pièces jointes
Antispam DNS BL	oui
Antispam « Temps réel »	pop3, smtp, mails entrants et sortants
Quarantaine externe	oui
Fonctions Réseau et Disponibilité	
DHCP	Relais et Serveur
Secours sur lien	oui : WAN et VPN
Répartition de charge	par accès WAN et VPN
Qualité de Service – Limitation, réservation, priorisation des flux, gestion des files d'attente et marquage	Diffserv
Agrégation de liens	oui
Haute disponibilité	oui : actif-passif ou : actif-actif
Authentification	
Par flux avec agent d'authentification Arkoon	oui
Compatible avec les serveurs d'authentification : NT, Act. Directory, Radius, LDAP	oui
Par certificats numériques (PKI interne appliance)	oui
Par certificats numériques (PKI externe)	oui
Authentification forte (Token, carte à puce...)	oui
Administration	
Configuration via Arkoon Manager (Windows et linux)	oui
Supervision via Arkoon Monitoring (Windows et linux)	oui
Gestion des rôles d'administration	oui : 6 rôles prédéfinis
Administration centralisée	oui
Connexions sécurisées (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 ACC	oui
Compatibilité Arkoon Management Center (AMC)	oui
Compatibilité Arkoon Virtual Edition	oui
Dimensions	
Format	Rack 2U
L / l / H (mm)	429 / 382 / 88
Poids	11 Kg
Environnement	
Température de fonctionnement	5 à 40°C
Humidité de fonctionnement	20 à 90%
Température de stockage	0 à 70°C
Humidité de stockage	5 à 90%
Alimentation	100/240V
Alimentation Redondante	oui
Redondance disque	RAID1
Capacité Disque	2 disques SATA, 80Go
Fréquence	48 – 63Hz
Puissance électrique max	2 x 460W
Certifications	CE/FCC/UL/cUL