

# Appliances UTM FAST360



Le A2200 est un équipement de type système de nouvelle génération. À ce titre, il bénéficie de nombreuses options matérielles (carte quad gigabits cuivre, carte quad gigabit SFP, carte accélératrices ASIC VPN) qui lui garantissent une grande adaptabilité et évolutivité. En outre, son châssis 2U, sa robustesse et ses performances exceptionnelles sur l'ensemble des fonctions de sécurité (performance réseau, performance VPN, performance de filtrage de contenu...) font du A2200 une parfaite solution pour la sécurisation UTM des réseaux de plusieurs centaines à plusieurs milliers de machines.



## 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 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 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

# Descriptif technique



# A2200 - A2200X

A2000 Series

Firewall, VPN, Prévention d'intrusion temps réel

	A2200	A2200X
<b>Performance</b>		
Débit Firewall (Mbps)	2 500	2500
Débit VPN 3DES (Mbps)	200	1 000
Débit VPN AES (Mbps)	500	1 000
Connexions simultanées	1 000 000	1 000 000
Nouvelles connexions / seconde	25 000	25 000
Tunnels simultanés	20 000	20 000
<b>Interfaces</b>		
Port console		1
Ports FastEthernet 10/100		2
Ports Gigabit Ethernet Cuivre 10/100/1000 (standard/ max)		6 / 10
Ports Gigabit SFP		4 (option)
Modules Gigabit optionnels	4 ports SFP / 4 Ports cuivre	
<b>Routage et mode de fonctionnement</b>		
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
<b>Firewall - Intrusions Prevention System</b>		
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, smtp, flux netbios, imap4, sip, mgcp, sdp, rtp, rtcp, ssl/tls
Protection contre DOS et DDOS		oui
Protection contre les violations de protocoles		oui
<b>Intrusions Detection System - FAST in line IDPS</b>		
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
<b>VoIP Security</b>		
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
Interface FIRECONVERGE		oui
<b>VPN IPSEC</b>		
ASIC VPN	-	oui
Algorithme de chiffrement		DES, 3DES, AES, Blowfish, SHA-1 / MD5
<b>Antivirus et Antispyware</b>		
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

	A2200	A2200X
<b>Filtrage Web</b>		
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
<b>Antispam et filtrage Mail</b>		
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
<b>Fonctions Réseau et disponibilité</b>		
DHCP		Relais et Serveur
Secours sur lien		oui : WAN et VPN
Répartition de charge		par accès WAN et VPN
Qualité de Service – priorisation des flux, gestion des files d'attente et marquage		Conformité Diffserv
Agrégation de liens		oui
Haute disponibilité		oui : actif-passif
<b>Authentification</b>		
Par flux avec agent d'authentification Arkoon		oui
NT, Act. Directory, Radius, LDAP		oui
Par certificats numérique (PKI interne appliance)		oui
Par certificats numérique (PKI externe)		oui
Authentification forte (Token, carte à puce...)		oui
<b>Administration</b>		
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
Analyses et stats via Arkoon Reporting (Windows et linux)		oui
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 WebTrend		oui
Compatibilité Arkoon Management Center (AMC)		oui
<b>Dimensions</b>		
Format		Rack 2U
L / l / H (mm)		429 / 382 / 88
Poids		11 Kg
<b>Environnement</b>		
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
Fréquence		48 – 63Hz
Puissance électrique max		2 x 460W
Certifications		CE/FCC/UL/cUL

**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](http://www.arkoon.net)

