

Fiche comparative pour appliances UTM

Version 09.07/1

Critères			ARKOON FAST360®	CISCO ASA
Real time firewall – 3 to 7 layers (OSI model) – Quels protocoles sont analysés en mode « stateful » ?	Protocoles de niveau 3, 4	IP	✓	✓
		ICMP	✓	✓
		TCP	✓	✓
		UDP	✓	✓
	Protocoles applicatifs	HTTP	✓	✓
		FTP	✓	✓
		DNS TCP	✓	✓
		DNS UDP	✓	✓
		SMTP	✓	✓
		IMAP4	✓	✗
		POP3	✓	✗
		NETBIOS Ports 137,138 et 139	✓	✗
		SQLNet	✓	✗
		SNMP V1, V2 et V3	✓	✓
		RTSP	✓	✓
		H323	✓	✓
		SIP	✓	✓
		MGCP	✓	✓
		RTP-RTCP	✓	✗
		SSL	✓	✗
Sécurité de la VoIP		Contrôle des protocoles VoIP (H.323, SIP, MGCP, SDP, RTP, RTCP)	✓	✓ Gestion NAT/PAT principalement
Quels Techniques ?	Adaptive Filtering (contrôle du flux média par rapport au flux Signalisation)		✓	✗
	Fireconverge, interface de communication entre une sonde Chekphone et l'appliance sécurité IP		✓	✗
Intrusion Detection System – IDPS –		Analyse contextuelle (base de signatures adaptée à chaque connexion, chaque protocole)	✓	✓ option AIP-SSM
Quelle est la technologie de détection d'intrusion ?	Mode coupure		✓	✓
	Mode alerte		✓	✓
	Utilisation de profils applicatifs (signatures adaptées au système protégé, serveur, OS)		✓	✓
	Méthode de scoring (type Wheight Pattern Matching) qui pondère la détection de chaque signature)		✓	✓
	Logs sur des signatures identifiées		✓	✓
	Nombre de signatures dans la base		> 1 000	N/A
	Nombre de protocoles analysés		> 15	>15
Antivirus & Antispyware		Antivirus intégré	✓	✓ option CSC-SSM
Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ?	Antispyware intégré		✓	✓
	Editeur des moteurs antivirus et antispyware		SOPHOS	TREND MICRO
	Nombre de signatures		> 95 000	N/A
	Analyse sur HTTP		✓	✓
	Analyse sur SMTP		✓	✓
	Analyse sur POP3		✓	✓
	Analyse sur FTP		✓	✓
	Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)		✓	N/A
	Mise à jour automatique des signatures AV		✓	✓

Fiche comparative pour appliances UTM

Version 09.07/1

Antispam Quel moteur est utilisé ? Quels sont les protocoles analysés ?	DNS BL	☒	☒
	Technologie du moteur filtrage de contenu (temps réel, heuristique, bayésien ou signatures, etc...)	Temps réel	IP REPUTATION <i>option CSC-SSM premium</i>
	Editeur du moteur de filtrage de contenu	COMMTOUCH	TREND MICRO
	Analyse sur SMTP	☒	☒
	Analyse sur POP3	☒	☒
	Analyse des mails entrants	☒	☒
	Analyse des mails sortants	☒	☒
	Bloque les spams images	☒	☒
	Taux de faux positifs	< 0.001%	Non communiqué
	Gestion d'une quarantaine externe	☒	☒
Filtrage d'URL	Nombre de catégories standard	15	☒
	Nombre de catégories en option	60	☒ <i>option CSC-SSM premium</i>
	ICAP Req mode	☒	☒
VPN IPSEC	Mode site à site et mode nomade	☒	☒
	Algorithmes de chiffrement : DES, 3DES et AES	☒	☒
	Authentification par certificat X509, clés partagées	☒	☒
	Support PKI interne et externe	☒	☒ <i>Externe</i>
	Mode hiérarchique et maillage complet	☒	☒
	Support de la répartition de charge et des liens de secours	☒	☒
Routage dynamique Quels protocoles ?	RIP	☒	☒
	OSPF	☒	☒
	BGP	☒	☒
Support de VLAN	Nombre de VLAN supportés	illimité	100 maxi
	Filtrage par VLAN	☒	☒
Masquage	NAT	☒	☒
	PAT	☒	☒
	Mode bridge	☒	☒
QoS, Gestion de la bande passante & Répartition de charge	Dynamique	☒	☒
	Par interfaces physique	☒	☒
	Par services (par applications)	☒	☒
	Par horaires	☒	☒
	Par utilisateurs	☒	☒
	Pour chaque flux, accès Internet principal et accès de secours	☒	☒
	Compatibilité Diffserv	☒	☒
	Haute disponibilité	☒ Actif-passif	☒ Actif-actif
	Conservation des connexions actives	☒	☒
Administration standard Quelles sont les caractéristiques des outils d'administration inclus en standard avec le produit (sans coût additionnel) ?	Administration via outils graphiques dédiés et sécurisés avec authentification forte et chiffrement	☒	☒ <i>ASDM : interface Web</i>
	Configuration des équipements centralisée : mode « maître-esclave »	☒	☒
	Nombre de rôle d'administrateurs pré définis (conformité au profil de protection DCSSI)	6	16
	Mise à jour automatisée	☒	☒
	Monitoring temps réel	☒	☒
	Gestion des logs depuis l'outil « Monitoring » et depuis des outils externes	☒	☒
	Compatibilité SNMP	☒	☒