Fiche comparative pour appliances UTM Version 09.07/1

Protocoles of Invest 3, 4 1 1 1 1 1 1 1 1 1	Critères			ARKOON FAST360 [®]	WATCHGUARD
New Year Security			IP		Ø
CP	– 3 to 7		ICMP		
Cuels protocoles sont analyses en mode Fire Content of the protocoles and the protoco		,	TCP		Ø
Guels Techniques ? Securité de la VoIP Quels Techniques ? Securité de la VoIP Quels Techniques ? Contrôle des protocoles VoIP (H.323, SIP, MCCP, SDP, RTP, RTCP) SSL Additivirus & Antispyware Quel moteur est utilisé ? Quels son le protocoles voir étages connection, étaque protocoles analysés ? Antivirus & Antispyware Quel moteur est utilisé ? Quels son le protocoles nalysés son les protocoles analysés ? Antispyware inlegre Antispyware inlegre Antispyware inlegre Antispyware Analyse sur FITP Consolide inlegree, type genotype viral (cypesture) point inlegree, type genotype viral (cypesture) viral (cypesture) point inlegree, type genotype viral (cypesture) viral (cypesture) point inlegree, type genotype viral (cypesture) viral (cypesture) viral (cypesture) point inlegree, type genotype viral (cypesture) viral (cy			UDP		
protocoles sont analysés en mode applicatifs and the protocole analyses and test applications are statisfied as a possible applications and the protocole analyses are formed analyses are fairly applicatifs and the protocole analyses are formed analyses are fairly applicatifs and the protocole analyses are formed analyses are fairly analyses are fairly analyses are fairly analyses analyses. Analyses are fairly analyses are fairly analyses are fairly analyses analyses. Analyses are fairly analyses are fairly analyses analyses. Analyses are fairly analyses are fairly analyses analyses. Analyses are fairly analyses. Analyses are fairly analyses analyses. Analyses are fairly analyses are fairly analyses a	Ouels		HTTP		
Analyse serior mode	protocoles sont		FTP		
Securité de la VoIP Cuels Techniques ? Cuels Techniques ? Cuels techniques ? Cuel cest la technologie de détection d'intrusion ? Analyse sur Ports : Antivirus & Antispyware Antivirus & Antispyware Antivirus & Antispyware Quel moteur est utilise ? Quels and protection sanalysés and is protectioles analysés ? Comment fonctionnent les mises à jour ? Analyse sur HTTP Analyse sur FIPP Echno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virius) Cuels sur Fire Company (special per la contextue) Analyse sur FIPP Echno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virius) Analyse sur FIPP Echno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virius) Analyse sur FIPP Echno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virius) Coulement on the content of the		аррисаціз	DNS TCP		×
IMAP4			DNS UDP		☑ Gamme Peak et Edge
POP3			SMTP		V
NETBIOS Ports 137,138 et 139			IMAP4		×
SOLNet SMMP V1, V2 et V3 RTSP H323 SIP MGCP RTP-RTCP SSL Controle des protocoles V0IP (H.323, SIP, MCCP, SDP, RTP, RTCP) Founds Techniques? Adaptive Filtering (controle du flux media par rapport au flux Signalisation) Fireconverge, interface de communication entre une sonde Chekphone et l'appliance securité IP Mode alerte Utilisation de profits applicatifs (signatures dans la base son long dup protecoles analysés ? Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels son le signatures dans la base Antivirus intégré Editeur des moteurs antivirus et antispyware SOPHOS Wildist Nombre de signatures Antispyware intégré Editeur des moteurs antivirus et antispyware SOPHOS Wildist Analyse sur POP3 Analyse sur FIP Techno. Proactive intégrée, type genotype viral (signatures generiques pour anticiper les nouveaux virus)			POP3		
SIMP V1, V2 et V3			NETBIOS Ports 137,138 et 139		×
RTSP			SQLNet		×
H323			SNMP V1, V2 et V3		×
SiP			RTSP		\square
MGCP RTP-RTCP SSL Controlle des protocoles VollP (H. 323, SIP, MCP, SDP, RTP, RTCP) Adaptive Filtering (controle du flux media par rapport au flux Signalisation) Fireconverge, interface de communication entre une sonde Chekphone et l'appliance sécurité IP Intrusion Detection System — IDPS— Quelle est la technologie de détection d'intrusion? Mode alerte Utilisation de profis applicatifs (signatures adaptée à chaque connexion, chaque protocole) Mode alerte Utilisation de profis applicatifs (signatures darbies au systeme protégé, serveur, OS) Méthode de scoring (type Wheight Pattern Matching) dipondere la détection de chaque signatures Antivirus & Antispyware Quel moteur est utilise? Quels sont les protocoles analysés? Comment fonctionnent les mises à jour? Antivirus intégré Antivirus intégré Antivirus intégré Editeur des moteurs antivirus et antispyware Antivirus de signatures Antivirus et signatures Antivirus et antispyware Antivirus de signatures Antivirus et antispyware Antivirus de signatures Antivirus et antispyware Antivirus et antispyware Antivirus de signatures Antivirus et antispyware Antivirus et signatures Antivirus et antispyware Antivirus et signatures Antivirus et antispyware Ant			H323		×
Sécurité de la VoIP Quels Techniques ? Controle des protocoles VoIP (H.323, SIP, MGCP, SDP, RTP, RTCP) Adaptive Filtering (controle 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 - Quelle est la technologie de détection d'intrusion ? Mode alerte Utilisation de profils applicatifs (signatures adaptée a detection d'intrusion ? Mode alerte Utilisation de profils applicatifs (signatures adaptées au systeme protegé, serveur, OS) Methode de socring (type Wheight) Pattern Matching) qui pondère la détection de chaque signature) Logs sur des signatures identifiées Nombre de signatures dans la base Antivirus & Antispyware Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Antivirus intégré Antivirus intégré Antivirus intégré Antivirus intégré Editeur des moteurs antivirus et antispyware Nombre de signatures Analyse sur HTTP Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures genériques pour anticiper les nouveaux virus)			SIP		×
SSL Sécurité de la VoIP Quels Techniques ? Controle des protocoles VoIP (H.323, SIP, MGCP, SDP, RTP, RTCP) 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— Quelle est la technologie de détection d'intrusion ? Mode alerte Utilisation de profils applicatifs (Signatures adaptée a detection d'intrusion ?) Mode alerte Utilisation de profils applicatifs (Signatures adaptées au systeme protocole) Mode coupure Utilisation de profils applicatifs (Signatures adaptées au systeme protocée, 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 Intrusion Patricipal de protocoles analysés Antivirus & Antispyware Quel moteur est utilisé ? Quels sont les protocoles analysés ? Antivirus intégré Antivirus intégré Antivirus intégré Editeur des moteurs antivirus et antispyware Nombre de signatures Analyse sur HTTP Analyse sur SMTP Techno. Proactive intégrée, type genotype viral (Signatures génériques pour anticiper les nouveaux virus)			MGCP		×
Sécurité de la VoIP Quels Techniques ? Contrôle des protocoles VoIP (H.323, SIP, MGCP, SDP, RTP, RTCP) 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) Mode coupure Analyse contextuelle (base de signatures adaptée à chaque connexion, chaque protocole) Mode coupure Mode alerte Utilisation de profils applicatifs (signatures adaptées au système protoègé, serveur, OS) Méthode de scoring (type Wheight Pattern Matching) voil pondère la détection de chaque signature) Logs sur des signatures dans la base Nombre de signatures dans la base Nombre de protocoles analysés Antivirus & Antispyware Quel moteur est utilisé ? Quels sont les protocoles analysés ? Antivirus intégré Antispyware intégré Editeur des moteurs antivirus et antispyware SoPHOS Wildlist Nombre de signatures Nombre de signatures Analyse sur HTTP Analyse sur POP3 Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)			RTP-RTCP	V	×
Ouels Techniques ? MGCP, SDP, RTCP)			SSL	7	×
Adaptive Filtering (controle du flux média par rapport au flux Signalisation) Fireconverge, interface de communication entre une sonde Chekphone et l'appliance sécurité IP Analyse contextuelle (base de signatures adaptée à chaque connexion, chaque protocole) Mode coupure Duelle est la technologie de détection d'intrusion? Mode alerte Utilisation de profils applicatifs (signatures adaptées au système protégé, serveur, OS) Méthode de scoring (type Wheight Pattern Matching) qui pondere la détection de chaque signatures identifiées Nombre de signatures dans la base Antivirus & Antispyware Quel moteur est utilisé? Quels sont les protocoles analysés? Antivirus fronctionnent les mises à jour? Antivirus intégré Editeur des moteurs antivirus et antispyware Nombre de signatures Antivirus et antispyware Editeur des moteurs antivirus et antispyware Nombre de signatures Analyse sur HTTP Analyse sur SMTP Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)	Sécurité de la	VolP			×
Intrusion Detection System - IDPS - Quelle est la technologie de détection d'intrusion? Wode alerte Utilisation de profils applicatifs (signatures adaptée a us ystème protégé, serveur, OS) Méthode de scoring (type Wheight Pattern Matching) qui pondère la détection de signatures dans la base Nombre de signatures dans la base Antivirus & Antispyware Quel moteur est utilisé? Quels sont les protocoles analysés? Comment fonctionnent les mises à jour? Antivirus est moteure est utilisé? Antispyware et de signatures Antivirus et antispyware Editeur des moteurs antivirus et antispyware Nombre de signatures Antivirus et antispyware SOPHOS Wildlist Nombre de signatures Antivirus et antispyware SOPHOS Wildlist 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)	Quels Techniques	?	Adaptive Filtering (contrôle du flux média par rapport au flux Signalisation)		×
Cuelle est la technologie de détection d'intrusion? 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 dans la base Nombre de protocoles analysés Nombre de protocoles analysés Nombre de protocoles analysés Antivirus & Antispyware Quel moteur est utilise? Quels sont les protocoles analysés? Comment fonctionnent les mises à jour? Antivirus de signatures dens la base Antivirus et antispyware Editeur des moteurs antivirus et antispyware Nombre de signatures Antivirus et antispyware SOPHOS Wildlist Nombre de signatures Nombre de signatures Analyse sur HTTP Analyse sur SMTP Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)			Fireconverge, interface de communication entre		×
Ouelle est la technologie de détection d'intrusion? Mode alerte Utilisation de profils applicatifs (signatures adaptées au système protégé, serveur, OS) Méthode de scoring (type Wheight Pattern Matching) qui pondere la détection de chaque signature) Logs sur des signatures identifiées Nombre de signatures dans la base Nombre de protocoles analysés Nombre de protocoles analysés Nombre de protocoles analysés Antivirus & Antispyware Ouel moteur est utilisé? Ouels sont les protocoles analysés? Comment fonctionnent les mises à jour? Antivirus intégré Editeur des moteurs antivirus et antispyware Nombre de signatures Analyse sur HTTP Analyse sur SMTP Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)		ection System	chaque connexion, chaque protocole)		
détection d'intrusion? 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 Nombre de protocoles analysés Nombre de signatures Metivirus intégré Metivirus intégré Metivirus intégré Metivirus et antispyware SOPHOS Wildlist Nombre de signatures Nombre de	Ovalla ant la tanh				
Signatures adaptées au système protégé, serveur, OS) Méthode de scoring (type Wheight Pattern Matching) victorial qui pondère la détection de chaque signature) Logs sur des signatures identifiées victorial qui pondère la détection de chaque signatures victorial qui pondère la detection					
Méthode de scoring (type Wheight Pattern Matching) qui pondere la détection de chaque signature) ☑ ☑ Logs sur des signatures identifiées ☑ ☑ Nombre de signatures dans la base > 1 000 Nombre de protocoles analysés > 15 ☑ Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Antivirus intégré ☑ ☑ Editeur des moteurs antivirus et antispyware intégré ☑ ☑ ☑ Nombre de signatures > 95 000 22 000 Analyse sur HTTP ☑ ☑ Analyse sur SMTP ☑ ☑ Analyse sur FTP ☑ ☑ Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus) ☑ ☑			Utilisation de profils applicatifs (signatures adaptées au système protégé, serveur, OS)	lacksquare	×
Nombre de signatures dans la base > 1 000 Nombre de protocoles analysés > 15 Antivirus & Antispyware Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Antivirus intégré Antispyware intégré Editeur des moteurs antivirus et antispyware SOPHOS Wildlist Nombre de signatures > 95 000 22 000 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)			Méthode de scoring (type Wheight Pattern Matching) qui pondère la détection de chaque signature)		
Nombre de protocoles analysés Antivirus & Antispyware Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Antivirus intégré Antispyware intégré Editeur des moteurs antivirus et antispyware Nombre de signatures > 95 000 22 000 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)			Logs sur des signatures identifiées		×
Antivirus & Antispyware Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Antispyware intégré Editeur des moteurs antivirus et antispyware Nombre de signatures 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)			ŭ .		
Quel moteur est utilisé ? Quels sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Antispyware intégré Editeur des moteurs antivirus et antispyware Nombre de signatures > 95 000 22 000 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)			Nombre de protocoles analysés	> 15	×
Sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Editeur des moteurs antivirus et antispyware SOPHOS Wildlist Nombre de signatures > 95 000 22 000 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)	Antivirus & An	ntispyware	Antivirus intégré		✓
Sont les protocoles analysés ? Comment fonctionnent les mises à jour ? Editeur des moteurs antivirus et antispyware SOPHOS Wildlist Nombre de signatures > 95 000 22 000 Analyse sur HTTP	Quel moteur est u	ıtilisé ? Quels	Antispyware intégré		Ø
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)	sont les protocole Comment fonction	s analysés ?	Editeur des moteurs antivirus et antispyware	SOPHOS	Wildlist
Analyse sur SMTP Analyse sur POP3 Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)	jour ?		Nombre de signatures	> 95 000	22 000
Analyse sur POP3 Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)			-	V	Ø
Analyse sur FTP Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)			Analyse sur SMTP	$\overline{\square}$	$\overline{\square}$
Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)			Analyse sur POP3	\square	Ø
Techno. Proactive intégrée, type genotype viral (signatures génériques pour anticiper les nouveaux virus)			Analyse sur FTP	7	$\overline{\mathbf{Q}}$
			(signatures génériques pour anticiper les nouveaux		
					Ø

Fiche comparative pour appliances UTM Version 09.07/1

Antispam	Version 09.07/1 DNS BL	$\overline{m{arphi}}$	×
Antispani	Technologie du moteur filtrage de contenu	Temps réel	Temps réel
Quel moteur est utilisé ? Quels sont les protocoles analysés ?	(temps réel, heuristique, bayesien ou signatures, etc)		16πρ3166
	Editeur du moteur de filtrage de contenu	COMMTOUCH	COMMTOUCH
	Analyse sur SMTP	$\overline{\checkmark}$	Ø
	Analyse sur POP3	$\overline{\mathbf{V}}$	V
	Analyse des mails entrants	$ \overline{\checkmark} $	
	Analyse des mails sortants	$ \overline{\checkmark} $	V
	Bloque les spams images	$\overline{\checkmark}$	V
	Taux de faux positifs	< 0.001%	< 0.001%
	Gestion d'une quarantaine externe	$\overline{\mathbf{Q}}$	V
Filtrage d'URL	Nombre de catégories standard	15	×
3	Nombre de catégories en option	60	40 (option WebBlocker)
	ICAP Reg mode	$lue{oldsymbol{arDelta}}$	(Option Webblocker)
VPN IPSEC	Mode site à site et mode nomade	<u> </u>	<u> </u>
	Algorithmes de chiffrement : DES, 3DES et AES	<u> </u>	\square
	Authentification par certificat X509, clés	<u> </u>	\square
	partagées	<u></u>	V
	Support PKI interne et externe	$\overline{\mathbf{V}}$	(PKI externe)
	Mode hiérarchique et maillage complet	$\overline{\mathbf{V}}$	V
	Support de la répartition de charge et des liens de secours	Ø	\square
Routage dynamique	RIP	$\overline{\checkmark}$	☑ (Fireware Pro)
Quels protocoles ?	OSPF	$ \overline{\checkmark} $	(Fireware Pro)
Quels protocoles .	BGP	$ \overline{\checkmark} $	(Fireware Pro)
Support de VLAN	Nombre de VLAN supportés	illimité	Illimité (Fireware Pro)
	Filtrage par VLAN		(Fireware Pro)
Masquage	NAT		$\overline{\mathbf{Q}}$
	PAT	$\overline{\checkmark}$	\square
	Mode bridge	$\overline{\mathbf{V}}$	☑
QoS, Gestion de la bande	Dynamique	<u> </u>	(Fireware Pro)
passante &	Par interfaces physique	<u> </u>	(Fireware Pro)
Répartition de charge	Par services (par applications)	<u> </u>	(Fireware Pro)
	Par horaires Par utilisateurs	<u> </u>	(Fireware Pro)
	Pour chaque flux, accès Internet principal et	<u> </u>	(Fireware Pro)
	accès de secours		(Fireware Pro)
	Compatibilité Diffserv		(Fireware Pro)
	Haute disponibilité	☑ Actif-passif	Actif-passif (Fireware Pro)
	Conservation des connexions actives	abla	(Fireware Pro)
Administration standard	Administration via outils graphiques dédiés et sécurisés avec authentification forte et	Ø	✓
Quelles sont les caractéristiques des outils d'administration inclus en standard avec le produit (sans	chiffrement Configuration des équipements centralisée : mode « maître-esclave »	\square	
coût additionnel) ?	Nombre de rôle d'administrateurs pré définis (conformité au profil de protection DCSSI)	6	N/A
	Mise à jour automatisée.	$\overline{\mathbf{Q}}$	V
	Monitoring temps réel		<u> </u>
	Gestion des logs depuis l'outil « Monitoring » et depuis des outils externes	Ø	\square
	Compatibilité SNMP	$ \overline{\checkmark} $	