



Appliances UTM FAST360®

Le A20 est une appliance de sécurité qui embarque toutes les fonctions de sécurité, firewall, IDPS, Antivirus, VPN, indispensables à la sécurisation d'un réseau de petite taille. Le A20 s'adapte parfaitement aux besoins de sécurité et de performances des sites distants (agences) des moyennes et grandes entreprises ou des sites principaux de petites entreprises. Disponible dans une version équipée d'un modem ADSL A20a, cette appliance permet d'être indépendante du modem opérateur ou d'assurer la haute disponibilité de l'accès internet.



Principales fonctionnalités

Firewall et Prévention d'intrusion

Moteur firewall basé sur la technologie brevetée FAST - Fast Applicative Shield Technology. Analyse en temps réel des protocoles réseau, transport et applicatifs. Technologie certifiée Critères Communs EAL2+ **Protection des flux SSL**

Le module FAST SSL/TLS s'assure de la conformité protocolaire des échanges chiffrés et de la validité de la chaîne de confiance.

BÉNÉFICES

- Haute performance d'une analyse en temps réel
- Pérennité du moteur qui bénéficie régulièrement de nouveaux modules applicatifs
- Protection contre le "phishing", les malware et l'utilisation abusive d'outils comme Skype (canaux cachés)

Détection d'intrusions

FAST in line IDPS détecte les attaques applicatives à partir d'une base de signatures qui s'adapte dynamiquement à l'application contrôlée et aux systèmes protégés. La base de signatures est mise à jour automatiquement et permet d'ajouter des signatures personnalisées.

BÉNÉFICES

- Optimisation de la performance et élimination des détections à tort (faux positifs)
- Neutralisation des attaques qui agissent sans violation protocolaire
- Capacité à interdire les flux Peer to Peer et messageries instantanées

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



A20 - A20X

A20 Series

Firewall, VPN, Prévention d'intrusion temps réel

| | A20 | A20X |
|--|--------|--|
| Performance | | |
| Débit Firewall (Mbps) | 100 | 100 |
| Débit VPN 3DES (Mbps) | 10 | 50 |
| Débit VPN AES (Mbps) | 20 | 50 |
| Connexions simultanées | 30 000 | 30 000 |
| Nouvelles connexions / seconde | 2 000 | 2 000 |
| Tunnels simultanés | 100 | 100 |
| Interfaces | | |
| Port console | 1 | 1 |
| Interface modem ADSL intégrée | A20a | - |
| Ports FastEthernet 10/100 | 3 | 3 |
| Routing et mode de fonctionnement | | |
| Routing statique | | oui |
| Routing 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 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 |
| Interface FIRECONVERGE | | oui |
| VPN IPSEC | | |
| ASIC VPN | - | oui |
| 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 |

| | A20 | A20X |
|---|-----|---|
| 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 - priorisation des flux, gestion des files d'attente et marquage | | Conformité Diffserv |
| Agrégation de liens | | oui |
| Haute disponibilité | | - |
| Authentification | | |
| 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 |
| 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 |
| 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 |
| Dimensions | | |
| Format | | Slim Desktop |
| L / l / H (mm) | | 252 / 152 / 33 |
| Poids | | 1 Kg |
| Environnement | | |
| Température de fonctionnement | | 5 à 40°C |
| Humidité de fonctionnement | | 20 à 90% |
| Température de stockage | | 0 à 75°C |
| Humidité de stockage | | 5 à 95% |
| Alimentation | | 100/240V |
| Fréquence | | 48 – 63Hz |
| Puissance électrique max | | 15W |
| Certifications | | CE |

ARKOON

13 A, avenue Victor Hugo
69160 Tassin - France
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60
www.arkoon.net

