ARKOON
NETWORK SECURITY

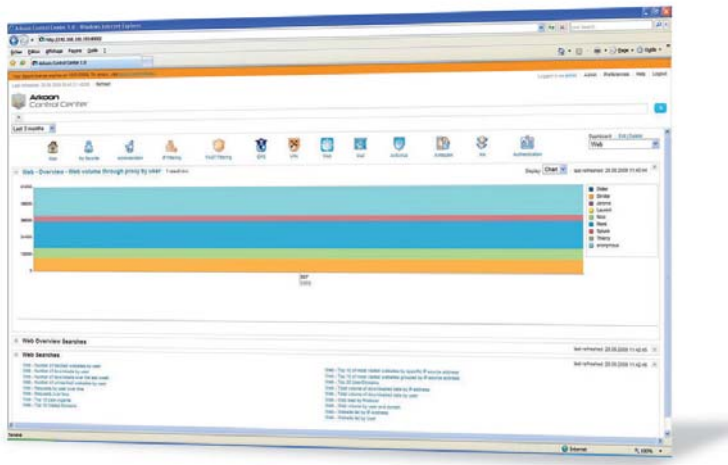
Arkoon Control Center

Bâtir de l'information pratique, compréhensible et accessible

Les équipements UTM FAST360 sont de formidables points de contrôle pour les exploitants (Trafic Web et Messagerie, Trafic Nomade via VPNs, Authentification, Détection d'intrusion, Infection virales…). Ces équipements produisent quotidiennement des volumes de logs très importants. Ces données, indispensables pour les opérations de diagnostics, d'audit et de mesures sont très souvent sous exploitées par les outils classiques de part la faiblesse de l'expression des requêtes et la présentation des résultats.

Il est donc indispensable de fournir aux différents acteurs de l'entreprise (de l'administrateur exploitant au contrôleur de gestion), une plateforme de gestion des logs permettant de répondre aux besoins d'une sécurité mesurable et compréhensible de tous tout en réduisant les temps d'investigation.

Arkoon Control Center



Outil convivial et simple à mettre en œuvre, accessible depuis une interface Web, Arkoon Control Center répond aux besoins des exploitants techniques ou des contrôleurs de gestion : production et partage de rapports d'audit et d'aide à la décision, génération d'alertes et corrélation d'événements.
Véritable "Wiki" de l'exploitant, basé sur un moteur de recherche très performant, ACC propose des rapports précis et des capacités de recherche extrêmement rapides.

ACC est fourni avec plus de 50 rapports prédéfinis (graphiques, tableaux) et avec un langage de requête évolué permettant de personnaliser tout type de requêtes en temps réel.
Disponible en version multi-utilisateurs, ACC s'adresse aussi bien au clients finaux qu'aux fournisseurs de services de sécurité managés (MSSP) désirant compléter et valoriser leur offre.

Points Clés

- Stockage et indexation des logs en temps réel sans limitation de volume
- Moteur de recherche optimisé
- Plus de 50 rapports prédéfinis et classés par thème
- Langage de requête multi-critères évolué
- Interface d'accès très conviviale
- Plateforme multi-utilisateurs, multi-clients

Descriptif technique

Stockage – Indexation

- Indexation et stockage des logs FAST360 transmis via Syslog ou depuis des fichiers d'archives
- Très haute performance : traitement jusqu'à 150 000 évènements / sec.
- Taux de compression de 12 à 48 %
- Scalabilité de traitement (plusieurs téraoctets / jour en architecture distribuée)
- Politique d'archivage et de restauration configurable

Recherche, extraction et rapport

- Langage de requête évolué permettant des tris et des extractions instantanés et interactifs sur tous les champs et plages de dates.
- Opérateurs pour analyse statistique et corrélation d'évènements
- Création et sauvegarde de requêtes et rapports personnalisés pour réutilisation et partage
- Vue sous forme de graphiques (lignes, histogrammes, camenberts…) et/ou de tableaux
- Plus de 50 rapports prédéfinis classés dans des "dashboard" personnalisables (Administration, Réseau, IP Filtering, FAST Filtering, IDPS, VPN, Web, Mail, Antivirus, Antispam, Cluster, QoS, Authentification)
- Planification des requêtes et des rapports pour envoi via e-mail ou flux RSS
- Modules d'impression paramétrable des rapports[1]
- Alertes (via e-mail, RSS, SNMP ou scripts personnalisés) basées sur le résultats des requêtes.

Authentification utilisateur

- Authentification utilisateur basée sur annuaire AD ou LDAP
- Gestion des rôles granulaire pour l'accès discrétionnaire aux données sources, aux requêtes et aux rapports (mode multi-utilisateurs et/ou MSS)

Interface

- Interface Web pour l'accès aux modules de recherche / rapport
- Personnalisation de l'interface pour une utilisation en mode MSS

Plateforme système

- Distribution Linux Red Hat 32 et 64 bits
- Distribution Linux Debian 32 et 64 bits
- Windows XP, Windows Server 2000, 2003 et 2008 (32 bits)[2]

Note : Les environnements Virtuels (VMWare, Xen, HyperV…) sont supportés.

(1) Disponible en V2.0
(2) Version US en V1.0

Système exploitation Client / Navigateur

- AIX, BSD et Linux: Firefox 1.5 or 2.0; Adobe Flash 9 ou supérieur
- Mac OS X : Firefox 1.5 or 2.0; Adobe Flash 9 ou supérieur
- Windows : Internet Explorer 6 ou 7, Firefox 1.5 ou 2.0; Adobe Flash 9 ou +

Références produits

Référence	Libellé
020-ACC-ACC200	Licence ACC 200 Mbs / jour
020-ACC-ACC500	Licence ACC 500 Mbs / jour
020-ACC-ACC1000	Licence ACC 1 Gb / jour
020-ACC-ACC2000	Licence ACC 2 Gb / jour
020-ACC-ACC5000	Licence ACC 5 Gbs / jour
020-ACC-ACC10000	Licence ACC 10 Gbs / jour
032-ALS-ACC200	Contrat Serenium ACC 200 Mbs / jour - 3 ans
032-ALS-ACC500	Contrat Serenium ACC 500 Mbs / jour - 3 ans
032-ALS-ACC1000	Contrat Serenium ACC 1 Gb / jour - 3 ans
032-ALS-ACC2000	Contrat Serenium ACC 2 Gb / jour – 3 ans
032-ALS-ACC5000	Contrat Serenium ACC 5 Gbs / jour - 3 ans
032-ALS-ACC10000	Contrat Serenium ACC 10 Gbs / jour - 3 ans

Plateforme hardware minimum et recommandée

Système	Plateforme Hardware recommandée	Plateforme Hardware minimum
Non Windows	2x3.4 GHz CPU, 4 GB RAM	1x1.4 GHz CPU, 1 GB RAM
Windows	Multi-core Xeon ou equivalent at 3Ghz, 4GB RAM	Pentium 4 or equivalent at 2Ghz, 2GB RAM

ARKOON
1, Place Verrazzano
69009 Lyon - France
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60
www.arkoon.net

Arkoon Control Center