ARKOON NETWORK SECURITY

Argumentaire
Arkoon Management Center

Arkoon
Management Center

1. **Qu'est-ce que l' AMC**
2. **A quel besoins répond l'AMC**
3. **A qui s'adresse l'AMC**
4. **La valeur ajoutée de l'AMC**
5. **Réponses aux objections type**

Copyright © 2008 ARKOON Network Security

1. Qu'est ce que l'Arkoon Management Center (AMC) ?

Avec les solutions d'administration standard ARKOON (Arkoon Tools), une architecture d'administration 3-tiers peut déjà être mise en place. C'est le mode de fonctionnement maître/esclaves (qui existe depuis 2000 chez ARKOON) dans lequel la centralisation de la configuration se fait sur l'appliance maître.

- L'AMC est un logiciel serveur qui s'installe sur un OS Linux.
- L'AMC sert à centraliser l'administration des appliances UTM FAST360 d'Arkoon.
- L'AMC apporte des fonctionnalités d'administration et de supervision avancée (notamment en matière de gestion des droits d'administration et de centralisation des logs).

2. A quels besoins répond l'AMC ?

1. *Besoin d'administration avancée*

Parce qu'elle est une plateforme centrale de l'architecture de management des appliances ARKOON, l'AMC offre des fonctionnalités d'administration avancées. Les entreprises qui souhaitent avoir une gestion centralisée plus poussée de leur politique de sécurité sont les principaux utilisateurs de l'AMC.
Cette notion d'administration avancée est dissociée du nombre d'appliances. Même avec 2 ou 3 appliances, un client peut souhaiter superviser en temps réel l'état de ses équipements ou bénéficier de fonctionnalités de mise à jour globale. C'est pour cela que l'AMC est disponible dans une version « de 2 à 5 appliances ».

2. *Besoin de soulager la base de données locale*

L'AMC permet de mettre à disposition une base de données (MySQL) dédiée et centralisée. Cette base de données peut d'ailleurs être installée sur un autre serveur physique que celui sur lequel se trouve le logiciel serveur AMC.
Cette base de données dédiée permet d'exporter les logs des appliances Arkoon et ainsi d'éviter le processus d'écriture dans la base de données locale de chaque appliance (processus gourmand en ressources, et impactant la performance de l'appliance et la charge du disque dur).
Les entreprises qui souhaitent optimiser la performance de leurs appliances et/ou qui constatent des ralentissements (voire des dysfonctionnements) liés à la charge de la base de données locale de chaque appliance, seront donc intéressées par l'AMC.
Il est à noter que l'utilisation d'une telle base de données centralisée et dédiée n'est pas une obligation mais peut toujours être mise en place, au besoin, avec un serveur AMC.

3. *Besoin de gérer des droits d'administration complexes*

L'AMC permet de gérer plusieurs « instances » d'administration centralisée. Cela signifie qu'un même serveur AMC gère plusieurs politiques de sécurité, correspondant à plusieurs groupes d'appliances.
L'ensemble des appliances de chaque groupe partage un fichier de configuration et peut être supervisé de façon centralisée. L'accès à l'administration d'un groupe se fait via un certificat X509 (utilisé par les tools ARKOON lors de la connexion sur le serveur AMC) qui confère des droits en lecture seule ou en lecture/écriture.

Copyright © 2008 ARKOON Network Security

L'AMC est donc adapté aux entreprises qui souhaitent créer une architecture d'administration avec plusieurs instances (plusieurs groupes indépendant en terme de politique de sécurité) administrables avec des droits différents depuis un même serveur central.

3. A qui s'adresse l'AMC ?

Cible	Apports fonctionnels	Bénéfices
Les clients qui utilisent le mode maître / esclaves	▪ Allègement de la base de données locale des appliances. ▪ Mise à jour centralisée ▪ Supervision avancée (états vert/orange/rouge).	▪ Gain de performance sur les appliances (car elles ne loguent plus en local) ▪ Optimisation de la supervision.
Les partenaires qui vendent du service autour de la sécurité	▪ Centralisation des connexions d'administration. ▪ Centralisation des logs. ▪ Cloisonnement des droits d'administration et des politiques de sécurité. ▪ Supervision avancée.	▪ Vente de nouveaux services liés à la supervision. ▪ Management multi clients plus simple.
Les clients Grands comptes	▪ Allègement de la base de données. ▪ Scalabilité du nombre d'équipements supervisés. ▪ Pérennité de notre choix d'architecture 3 tiers avec serveur central. ▪ Road map et pérennité de la solution.	▪ Augmentation du ROI de l'administration. ▪ Pérennité de l'investissement grâce à l'évolutivité de l'AMC (nouvelles fonctionnalités, scalabilité…)

4. La valeur ajoutée par l'AMC ?

Fonctionnalités avancées d'administration centralisée :

- Monitoring temps réel de l'état des appliances (états vert/orange/rouge) suivant des alertes prédéfinies
  Comme la charge CPU, la mauvaise installation d'une configuration, l'expiration prochaine d'une licence, etc…
- Mise à jour centralisée et simplifiée
  Il est possible de mettre à jour plusieurs appliances en même temps dans la même version système
- Regroupement des règles de flux
- Regroupement des appliances dans la configuration
  Afin de structurer l'affichage des appliances dans la configuration et dans le monitoring (notamment pour la supervision des états en temps réel) pour simplifier le travail de l'administrateur

Copyright © 2008 ARKOON Network Security

Stockage des logs sur un serveur dédié :

- Désengorgement de la base de données locale des appliances
  Il est possible de ne plus écrire les logs dans la base de données locale des appliances et d'exporter directement ces logs sur un serveur dédié contenant MySQL
- Archivage centralisé des logs
  Les logs d'un groupe d'appliances sont regroupés dans la même base afin de pouvoir les consulter de façon centralisée.

Gestion des droits d'administration par groupes d'équipement :

- Droits d'accès à la configuration et la supervision en mode *lecture/écriture* ou *lecture seule*
- Droits attribués sur une instance d'administration (correspondant à un groupe d'équipements)
- Supervision globale de l'ensemble des instances

5. Réponse aux objections types ?

Si ARKOON sort un nouvel outil d'administration, ça signifie que les outils standard ne vont plus évoluer, tout sera payant !	Il faut bien comprendre que l'AMC n'est pas un nouvel outil d'administration, c'est un outil qui vient compléter l'administration ARKOON. Un serveur central qui s'intercale entre les appliances ARKOON et les tools standards. Il est là pour apporter de nouvelles fonctionnalités qui ne seront jamais accessibles sans un serveur central. Mais l'AMC est complémentaire des tools et les 2 produits évoluent donc en parallèle. D'ailleurs dès la première version de l'AMC les fonctionnalités qui ne sont pas liées au serveur (comme les communautés VPN) sont incluses gratuitement dans les tools standard.
L'AMC ne fonctionne que sous Linux, mes postes d'administration sont sous Windows !	L'AMC est un serveur qui doit être installé sur un OS linux. Mais une fois son installation faite, seul l'administrateur du serveur est dans un environnement linux. Les administrateurs de la politique de sécurité utilisent les tools ARKOON qui sont eux sous Windows. Autrement dit, la partie linux de l'AMC est transparente pour l'administrateur de la sécurité qui utilisera toujours une console d'administration sous Windows.
Le serveur AMC ne peut pas être installé en haute disponibilité.	L'utilisation d'un serveur logiciel permet de bénéficier de toutes les fonctionnalités de haute dispo offertes par l'OS Linux. L'AMC peut profiter de toute la souplesse d'une architecture logicielle Linux (valeur ajoutée par le partenaire).
Une administration 2 tiers apporte autant de fonctionnalités.	Sans entrer dans le débat du détail de chaque fonctionnalité, il est intéressant de se pencher sur le choix d'architecture fait par ARKOON. ARKOON utilise une architecture 3 tiers et un serveur central, par opposition a des architectures 2 tiers et aucun serveur central. Le choix d'une architecture d'administration 2 tiers est extrêmement limitant car il ne permet pas de gérer la cohérence de la configuration et expose donc la politique de sécurité à des limites de centralisation. De même, l'absence de serveur central limite fortement les fonctionnalités actuelles et avenir de centralisation (fichiers de configuration, logs, alertes, droits d'accès, etc…). L'architecture ARKOON, avec les tools et leur combinaison à l'AMC offre une plus grande souplesse et une plus grande pérennité.

Copyright © 2008 ARKOON Network Security