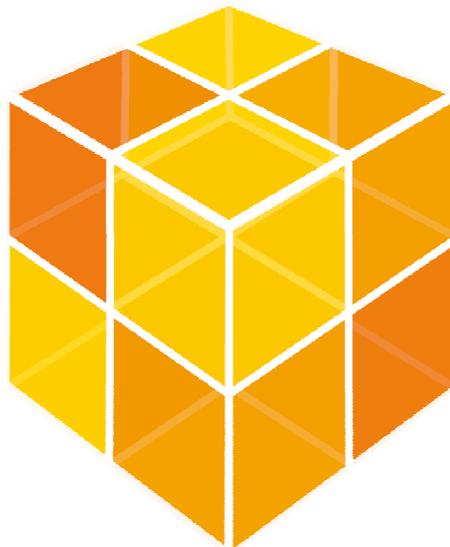


Outils d'administration

Arkoon Manager
Arkoon Monitoring
Arkoon Reporting



FAST360®
Appliances



Sommaire

I. Administration de la sécurité	3
1. Introduction.....	3
2. Architecture.....	3
a. Mode « Stand Alone »	3
b. Mode « maître-Esclave »	4
c. Mode « plateforme AMC »	4
3. Sécurisation de l'accès	5
a. Authentification multiple et mutuelle	5
b. Protocole de communication.....	5
c. Gestion des rôles d'administration	5
II. Arkoon Manager.....	<i>Erreur ! Signet non défini.</i>
1. Opérations Arkoon Manager.....	7
2. Principes de l'interface utilisateur	9
a. Présentation de l'interface.....	9
b. Création et organisation des configurations.....	10
c. Fonctions de recherche.....	11
d. Personnalisation de l'interface	12
e. Aides diverses	12
3. Utilisation de l'interface.....	13
a. Fonctions de configuration et de déploiement.....	13
b. Fonctions de maintenance	14
III. Supervision	15
1. ARKOON Monitoring	15
a. Les journaux de logs	15
b. Supervision de l'état des appliances en temps réel.....	19
c. Gestion des appliances	21
d. Mises à jour	21
2. Intégration avec des solutions tierces	23
IV. ARKOON Reporting.....	24

I. Administration de la sécurité

1. Introduction

Arkoon offre une suite d'outils logiciels reposant sur une interface utilisateur graphique, "Arkoon Tools", en vue de faciliter la gestion, le suivi et la maintenance des appliances FAST360®. Arkoon Tools comprend trois modules destinés à la gestion de FAST360

- Arkoon Manager est l'interface de configuration de l'appliance FAST360®. Elle comprend également les modules de gestion des sessions, de gestion des rôles et de gestion de l'autorité de certification
- Arkoon Monitoring est l'interface de suivi quotidien des activités de FAST360. Elle a recours à des journaux ainsi qu'à des alertes, et elle applique un suivi de l'état de l'appliance en temps réel (charge, performance, etc.)
- Arkoon Reporting sert à consolider les rapports d'activité de l'appliance FAST360®. De nombreuses options sont disponibles pour filtrer les données et générer des résumés et indicateurs graphiques des activités réseau à des fins de rapport et de planification.

2. Architecture

Les trois modules constituent une suite d'outils autonomes qui communiquent avec des périphériques FAST360® en mode « client-serveur ».

La suite logicielle Arkoon Tools a été conçue pour prendre en charge des opérations de gestion de réseau allant de déploiements autonomes simples de FAST360® à des réseaux multisites étendus. L'architecture de gestion repose sur un modèle à trois niveaux :

- une interface utilisateur → *fonction de présentation*
- un serveur de déploiement de politique → *fonction moteur*
- une ou plusieurs appliances individuelles → *fonction utilisation*

L'interface utilisateur est fournie par la suite Arkoon Tools et peut être installée sur un PC à n'importe quel emplacement du réseau. Des protocoles de communication sécurisés SSLV3 garantissent que seules les consoles Arkoon Tools identifiées peuvent communiquer avec le serveur de déploiement de politique et assurent l'intégrité et la confidentialité des flux d'administration.

Trois cas de figures distincts sont possibles

a. Mode « Stand Alone »

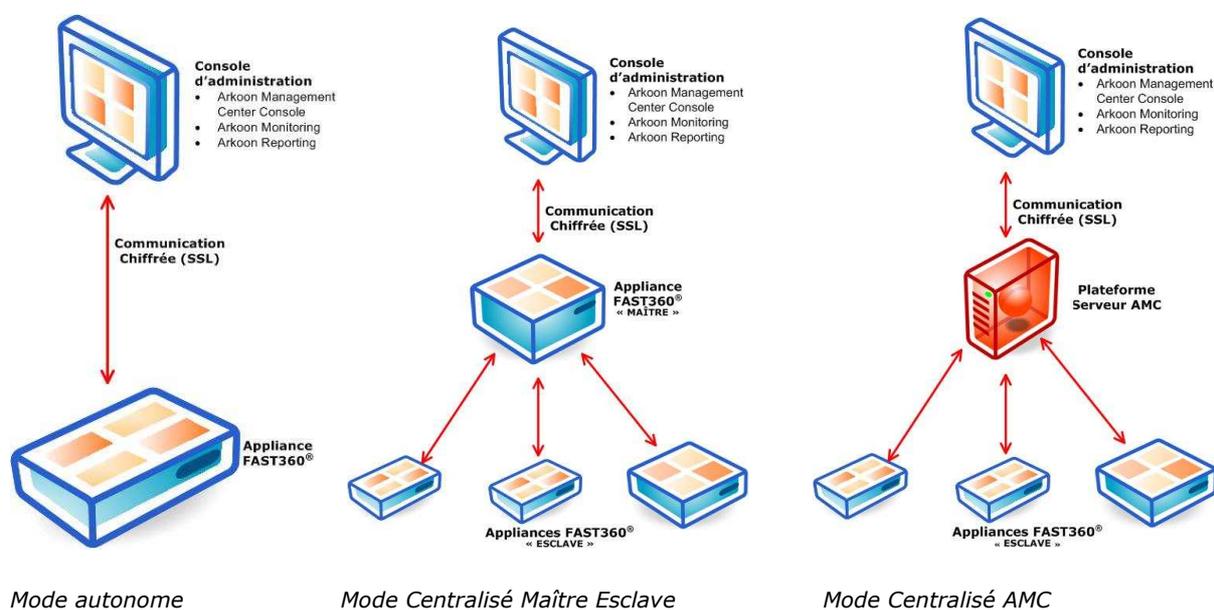
Ce mode est principalement utilisé pour le déploiement d'appliance unique (monosite). Le déploiement des appliances est autonome, chaque appliance gérant de manière indépendante sa politique de sécurité. Dans ce cas, l'appliance FAST360® est également son propre serveur de déploiement. On a une architecture dans laquelle les fonctions *moteur et utilisation* sont confondues.

b. Mode « Maître-Esclave »

Les politiques de sécurité sont centralisées. Le serveur de déploiement de politique (*fonction moteur*) est joué par une appliance FAST360® identifiée dite « appliance Maître ». Ce mode d'administration centralisée est fourni en standard.

c. Mode « plateforme AMC »

Ici aussi, les politiques de sécurité sont centralisées. Le serveur de déploiement de politique est une plateforme d'administration dédiée, Arkoon Management Center. Ce package logiciel est un produit logiciel Arkoon complémentaire qui s'installe sur un serveur dédié.



Le mode centralisé (Maître-esclave ou AMC) apporte plusieurs bénéfices par rapport au mode stand alone :

- Garantir une configuration cohérente des politiques de sécurité pour les mises en oeuvre sur des réseaux important. L'appliance FAST360® maître (ou le serveur AMC) diffuse les règles de sécurité à un ensemble d'appliances esclaves. Toutes les appliances de l'entreprise sont intégrés et gérés dans le cadre d'une seule politique de sécurité et dispose du même fichier de configuration.
- Assurer la cohérence des règles. L'administrateur définit ses règles de sécurité sans se soucier des appliances FAST360® sur lesquelles elles devront être installées. En effet, une technologie exclusive ARKOON permet à chaque appliance de déterminer, parmi l'ensemble des règles de flux, celles qui la concerne et qu'elle doit par conséquent installer et utiliser. La gestion automatique de la cohérence des règles de sécurité se base sur la topologie de l'architecture et sur les règles de routage.

- Centraliser les logs : les appliances esclaves peuvent communiquer leurs logs à l'appliance maître en temps réel. L'affichage des informations (logs IP, alertes, logs HTTP et logs SMTP) est entièrement centralisé.
- Simplifier et automatiser les mises à jour : chaque appliance FAST360® peut jouer le rôle de serveur de mises à jour pour les autres appliances

3. Sécurisation de l'accès

Une appliance FAST360® est un élément de sécurité, et l'intégrité de l'appliance est essentielle pour optimiser le niveau de la sécurité des systèmes d'information. Par conséquent, il est crucial de s'assurer que seul le personnel autorisé peut se connecter à l'appliance et en modifier la configuration, ou même seulement superviser et/ou télécharger des informations relatives à l'appliance et au(x) réseau(x) qu'elle protège.

a. Authentification multiple et mutuelle

L'identité du poste d'administration ARKOON est filtrée en fonction de son adresse IP et de son interface d'accès à l'équipement (ou à la plateforme d'administration dans une architecture AMC). L'identité de l'administrateur est validée en fournissant un certificat numérique X509 protégé par un mot de passe et fourni par ARKOON CA. Cette triple vérification signifie que seuls les administrateurs autorisés peuvent administrer l'appliance. En symétrique, le poste d'administration ARKOON utilise un certificat pour valider l'identité de l'appliance FAST360® qu'il administre (ou le serveur AMC).

b. Protocole de communication

Les communications échangées entre l'appliance FAST360® (ou le serveur AMC) et le poste d'administration distant sont chiffrées en utilisant le protocole SSLv3 (clé de chiffrement de 168 bits). Cette configuration assure l'intégrité et la confidentialité des données : il est impossible d'intercepter ou de modifier les flux d'administration.

c. Gestion des rôles d'administration

Une infrastructure de sécurité peut renfermer plusieurs appliances FAST360® pouvant requérir différents administrateurs qui disposent de rôles différents et interviennent sur ces appliances. Les outils d'administration de l'appliance FAST360® permettent à un responsable sécurité de distribuer les responsabilités d'administration en fonction de sept rôles définis. Un administrateur peut combiner plusieurs de ces rôles.

Nom du rôle	Description du rôle
Responsable sécurité	Ce rôle est assigné à la personne qui crée les nouveaux administrateurs. Par conséquent, cette personne n'a aucune responsabilité d'administration ou de supervision. Elle fait uniquement le lien entre les certificats SSL et un ou plusieurs rôles d'administration
Administrateur système et réseau	Ce rôle est attribué à la personne en charge des paramètres système et réseau. Elle peut lire la politique de sécurité et gérer les journaux système. Responsable de la gestion des systèmes, elle peut mettre à jour la version logicielle et l'attribution de licence FAST360®
Superviseur système et réseau	Ce rôle est attribué à une personne qui vérifie

	l'état du système et les événements de réseau.
Administrateur sécurité	Ce rôle est attribué à la personne responsable de la sécurité. Elle peut définir tous les paramètres de configuration liés à la sécurité et suivre les journaux de sécurité.
Superviseur sécurité	Ce rôle est attribué à la personne qui suit les événements de sécurité et vérifie/supprime les alertes de sécurité.
Auditeur	Rôle auditeur
Rôle toutes autorisations	Ce rôle sera utilisé dans les organisations au sein desquelles une seule personne est responsable de l'appliance FAST360®

Tableau 1 : Description des rôles

II. Arkoon Manager

1. Opérations Arkoon Manager

Les opérations possibles d'un administrateur dépendent des facteurs suivants :

- le mode de travail de l'administrateur (à savoir, connecté ou déconnecté) ;
- les droits d'administrateur, ou rôles, qui lui ont été attribués.

Mode déconnecté

En mode déconnecté, seuls les menus Session Manager et Offline Security Policy Manager sont disponibles.

- Session Manager : Le menu Session Manager permet l'accès au gestionnaire de session. Depuis ce gestionnaire, en cas de connexion valide, l'administrateur accède au menu Connected.
- Offline Security Policy Manager : Une nouvelle configuration peut être créée, ou une configuration locale peut être téléchargée à l'aide du menu Offline Security Policy Manager.

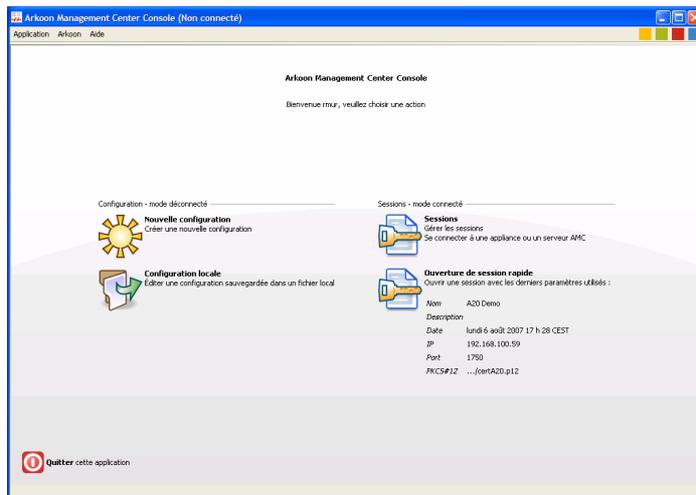


Fig 1 Accueil Mode Déconnecté

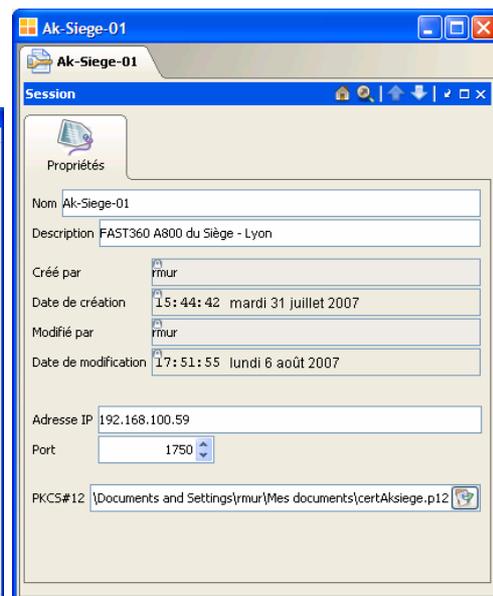


Fig 2 Gestion d'une session

Mode connecté

En mode connecté, les menus Online Security Policy Manager, Online Access Control Manager et Certificate Authority Manager sont disponibles, tandis que le menu Session Manager ne l'est pas. Il est possible que l'administrateur ne soit pas autorisé à accéder à toutes les applications en fonction du rôle dont il dispose.

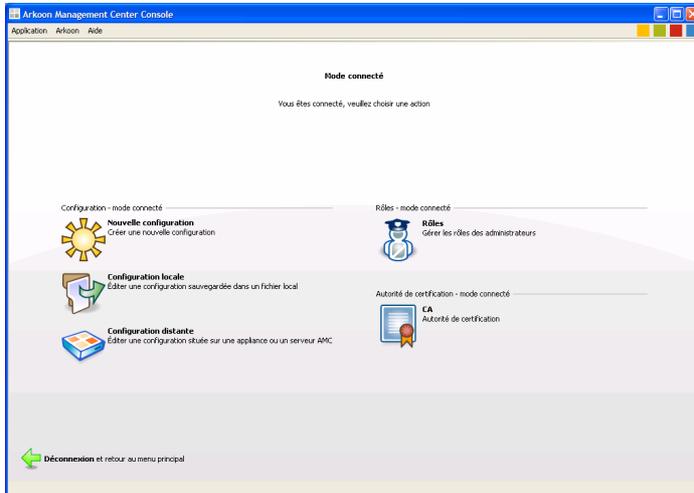


Fig 3 Accueil Mode déconnecté

- Online Security Policy Manager Une politique de sécurité est chargée à partir de l'appliance/du serveur AMC. Seul un responsable sécurité authentifié peut charger une politique de sécurité locale.
- Rôles Manager : c'est l'application de gestion des politiques de contrôle d'accès d'administration. Rôles Manager n'est accessible que si l'administrateur authentifié est un responsable sécurité.

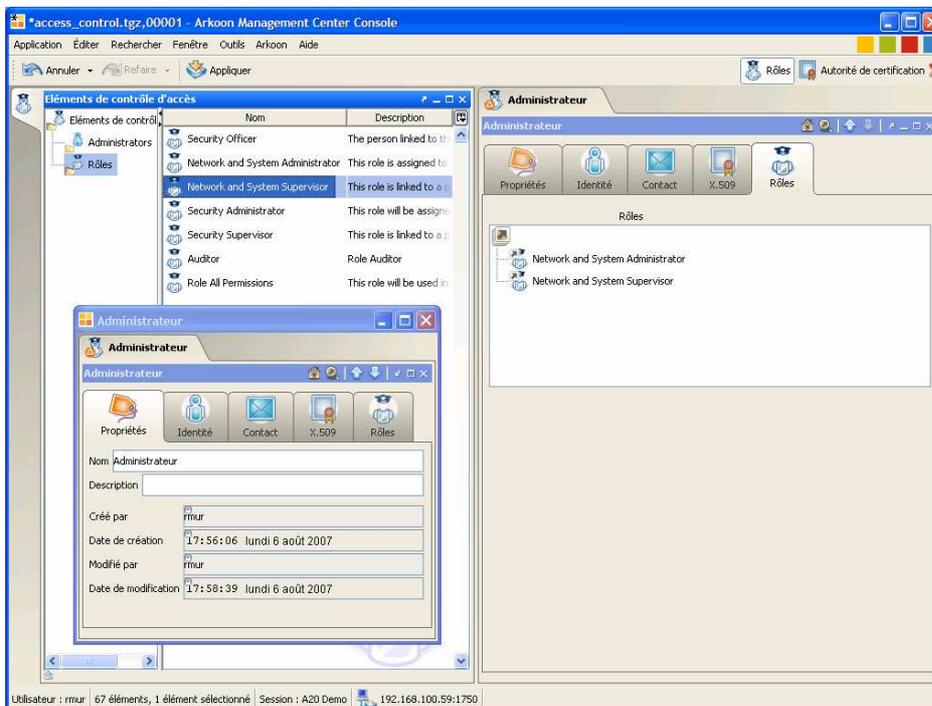


Fig 4 Application « Gestion des Rôles »

- Certificate Authority Manager : c'est l'application de gestion de l'autorité de certification Arkoon (création, révocation des certificats). L'application Certificate Authority Manager n'est accessible que si l'administrateur authentifié est un responsable sécurité.

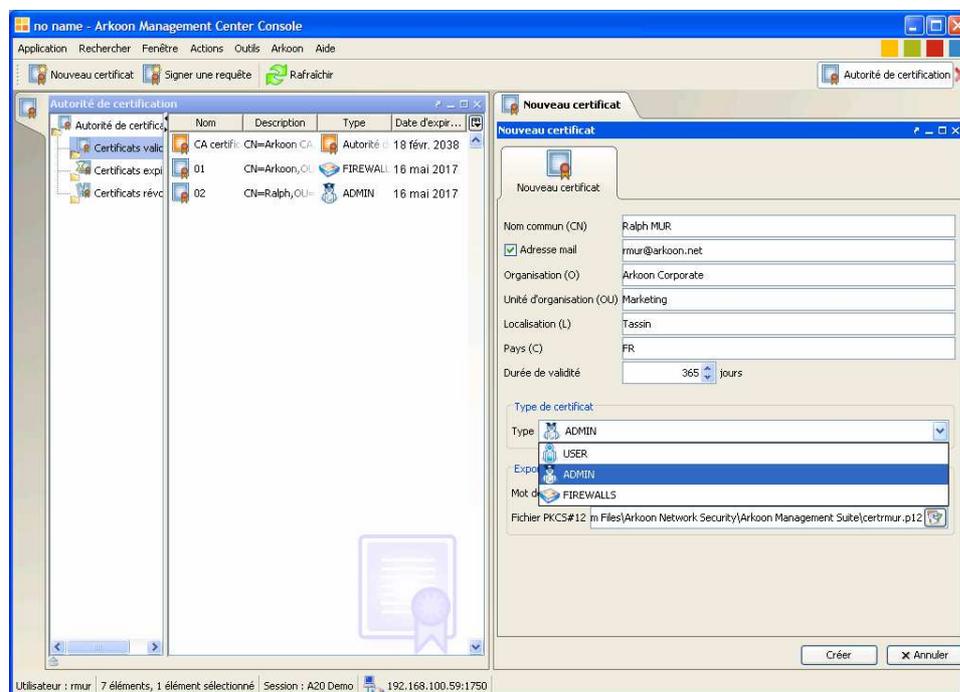


Fig 5 Application « Autorité de Certification »

2. Principes de l'interface utilisateur

a. Présentation de l'interface

Chaque application permet d'éditer en continu une configuration donnée. C'est une interface non modale : plusieurs vues peuvent exister de manière concurrente fournissant ainsi une lisibilité optimale des données manipulées.

Outre les barres d'outils, barres de menu, et autres barres d'état, l'interface propose à l'administrateur un ensemble de fenêtres dédiées à chacune de ses activités spécifiques. Ces fenêtres sont **non modales**, elles peuvent donc coexister sur un ou **plusieurs écrans** et être organisées de manière personnalisée.

Onglets, arborescences, tableaux et formulaires

- Sur la gauche de l'écran, une série d'onglets permettent d'accéder aux différents services et éléments (ou objets) disponibles.
- La partie gauche de chaque onglet est la vue d'explorateur, une arborescence des divers éléments que renferme l'onglet sélectionné. Vous pouvez y trouver des objets configurables ou des dossiers contenant des groupes d'objets. Les dossiers peuvent être développés dans cette arborescence pour accéder aux objets individuels.
- La partie droite de l'onglet est occupée par une vue développée de l'objet sélectionné dans la vue d'explorateur, appelée la vue descriptive.

- Sur la droite de l'écran sont présents l'onglet de configuration et les formulaires de configuration de l'objet sélectionné pour être modifié.

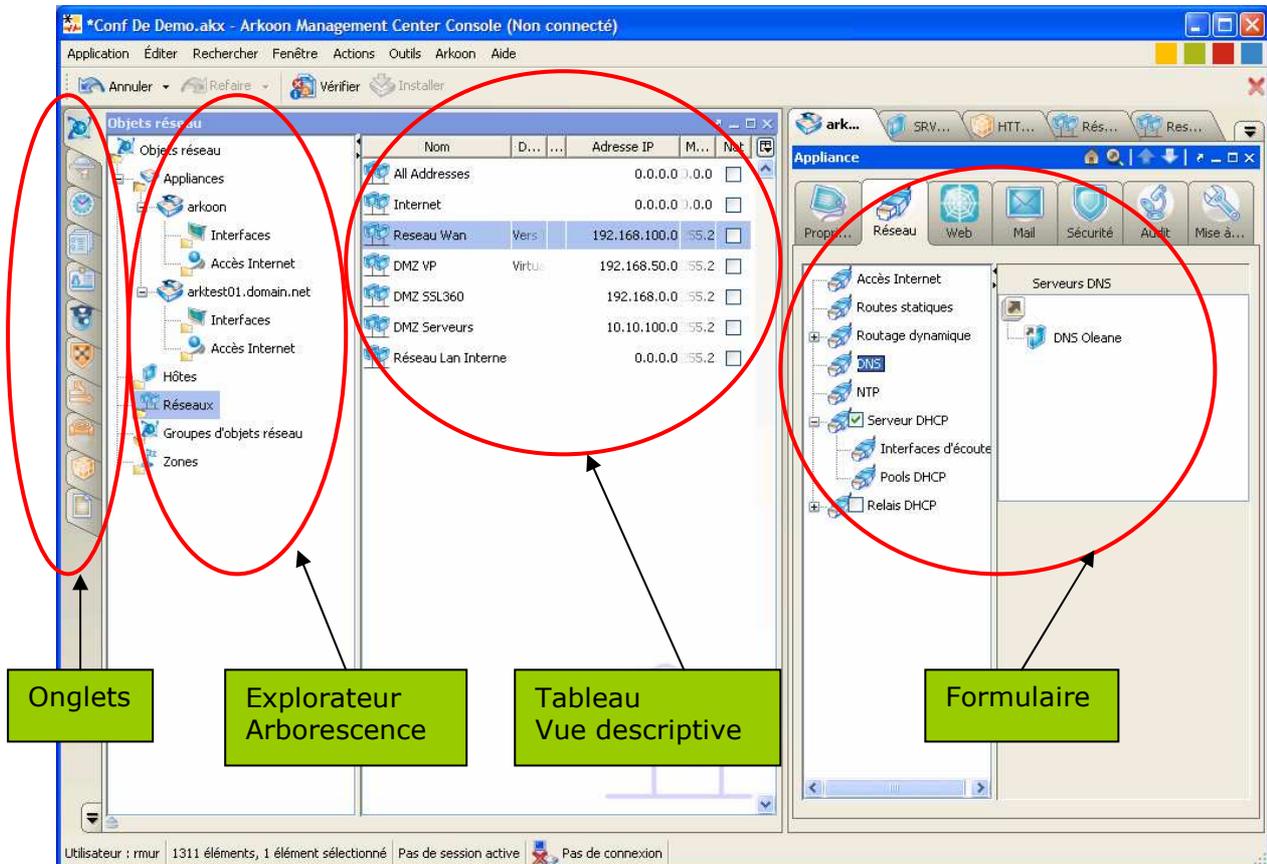


Fig 6 Onglets, arborescences, tableaux et formulaires

b. Création et organisation des configurations

La configuration de l'appliance FAST360® repose sur des objets. Au lieu de saisir un nombre élevé de paramètres pour configurer une appliance, vous créez des objets que vous faites glisser dans la configuration.

Par exemple, au lieu de saisir les paramètres d'un serveur DNS directement dans chaque configuration d'appliance FAST360®, vous créez un objet « hôte » avec une **capacité** « DNS », son adresse IP et d'autres paramètres adéquats. Cet objet DNS peut maintenant être ajouté à la configuration de plusieurs appliances par un simple **glisser-déposer**.

Dossiers

Arkoon Manager vous permet d'arranger les objets dans une hiérarchie à nombre indéterminé de niveaux dans des dossiers. Ces derniers peuvent servir à l'organisation des objets du même type uniquement.

Groupes d'objets

Arkoon Manager vous permet de grouper des objets de différents types à utiliser dans des objets de politique de sécurité.

Cette possibilité contraste avec les dossiers dans lesquels un objet n'apparaît qu'une fois dans la hiérarchie de dossiers, puisque cette hiérarchie de dossiers sert à stocker les définitions d'objet. Un objet, ou plus précisément une référence à un objet, peut ici au contraire apparaître plusieurs fois dans une hiérarchie de groupes pour pouvoir appliquer les politiques.

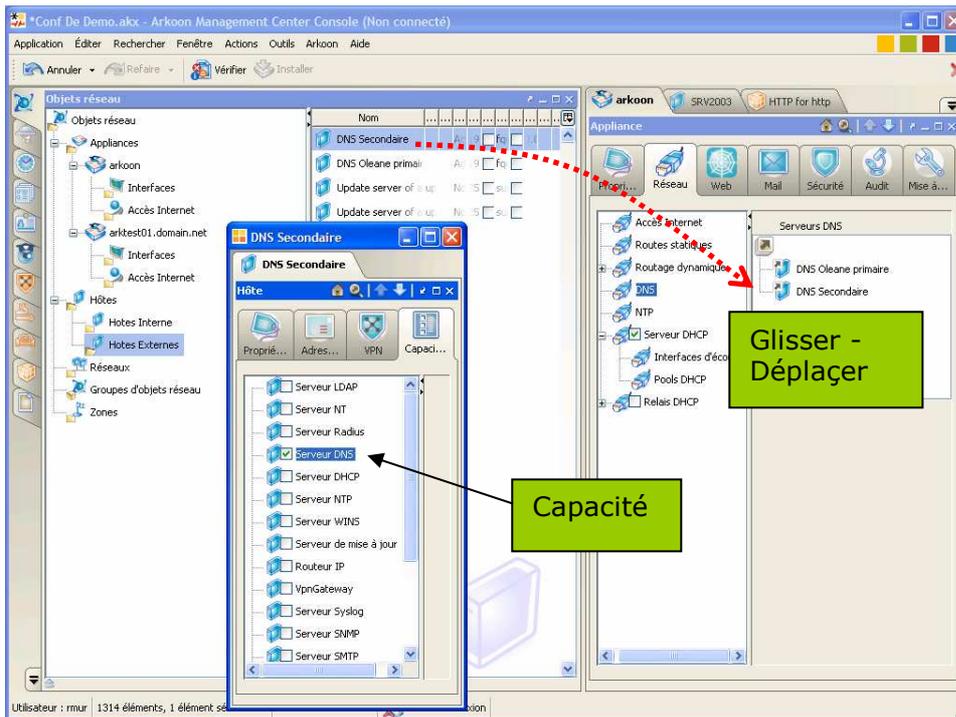


Fig 7 Hôtes et capacités

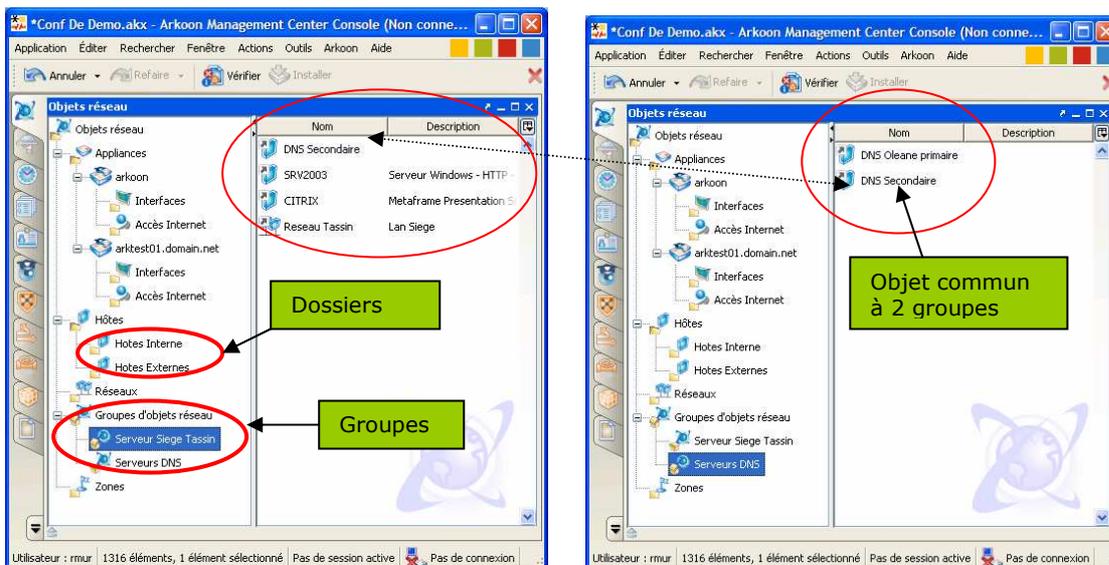


Fig 8 et 9 Dossiers et Groupes d'objets

c. Fonctions de recherche

L'interface propose plusieurs méthodes de recherche :

- Mise en surbrillance d'objets : Arkoon Manager vous permet de mettre en surbrillance des objets importants et d'améliorer la lisibilité de votre configuration.
- Barre de recherche de l'explorateur
- Recherche d'un élément d'origine : Arkoon Manager vous permet de trouver un objet dans la configuration afin de déterminer à quel service ou élément l'objet appartient.
- Recherche de références : Arkoon Manager vous permet de rechercher quels objets sont référencés par quels objets dans la configuration

- Recherche avancée : La fonction de recherche avancée permet de rechercher par type d'objet, nom, description, etc.
- Fonction de recherche intelligente : Lors de la configuration d'objets, vous pouvez utiliser la fonction de recherche intelligente pour trouver les objets qui correspondent à l'élément en cours de configuration

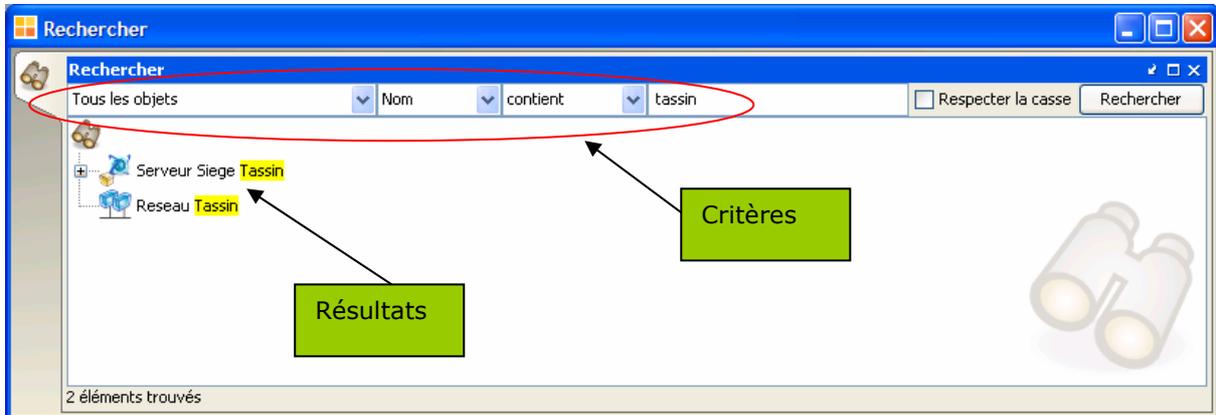


Fig 10 Recherche avancée

d. Personnalisation de l'interface

Les aspects personnalisables de l'interface d'Arkoon Manager ne se limitent pas à la présentation des éléments de fenêtre. Les cinq aspects clés de l'interface qui peuvent être modifiés sont les suivants :

- Apparence : langue, taille, alignement
- Edition : paramètres de définition de modification de nouveaux objets
- Fenêtres : Aspects des fenêtres et des onglets
- Messages : paramètres d'affichage des messages d'avertissement, des info-bulles et des astuces du jour.
- Réseau

e. Aides diverses

- Visuelles : Info-bulles, astuces, message

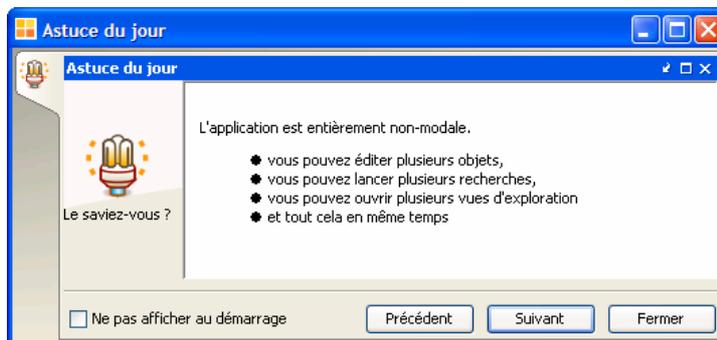


Fig 11 Tooltip

- Fonction undo-redo avec profondeur paramétrable

3. Utilisation de l'interface

a. Fonctions de configuration et de déploiement

Onglets de configuration

Les onglets de configuration, alignés verticalement sur la partie gauche de la fenêtre de configuration par défaut permettent d'accéder à différents groupes ou classes d'objets de configuration. Les objets de configuration sont regroupés et portent les noms d'onglet suivants :

- Objets réseaux : Renferme des dossiers d'appliances FAST360®, de systèmes hôtes et de réseaux de votre déploiement.
- Services : Permet de configurer les services de protocole utilisés dans les règles de filtrage du trafic.
- Horaires : Permet de définir les règles de programmation utilisées dans la configuration des règles de filtrage du trafic.
- Catégories : Permet d'entrer des URL ou des mots clés pour un filtrage Web.
- Authentification : Permet de définir et de configurer les différentes méthodes d'authentification utilisées dans votre déploiement.
- IDPS : Permet de configurer et de gérer le système facultatif FAST IDPS (Intrusion Detection and Prevention).
- VPNs : Permet de configurer les tunnels VPN IPsec sur l'appliance FAST360®.
- Règles de flux : Permet de créer et de gérer des règles de filtrage de trafic.
- QoS : Comprend des dossiers pour gérer et configurer les paramètres de qualité de service
- Politiques FAST : Comprend des dossiers pour les politiques FAST définies par l'utilisateur et par le système.
- Politiques : Comprend des dossiers pour définir des politiques de gestion diverses pour les appliances FAST360® sur le réseau : politiques ICMP, de journal, de reporting, de mise à jour et antispam.

Chargement de politiques de sécurité

Lors du chargement d'une politique de sécurité en mode connecté, la configuration est synchronisée à la configuration matérielle de l'appliance. Deux cas sont possibles :

- Ouverture d'une configuration enregistrée localement : L'ouverture d'une configuration enregistrée localement implique le chargement du fichier de configuration depuis le poste d'administration.
- Téléchargement d'une configuration enregistrée sur l'appliance FAST360® ou sur un serveur AMC .

Enregistrement d'une configuration localement

L'enregistrement d'une configuration localement revient à l'enregistrer sur le poste d'administration. Deux options sont disponibles pour enregistrer une configuration localement :

- Enregistrer : Cette option permet d'enregistrer instantanément les changements effectués sur la configuration en cours.
- Enregistrer sous : Cette option permet d'enregistrer localement le fichier de configuration actif dans un autre répertoire et/ou sous un autre nom que l'original, puis de le chiffrer le cas échéant.

Enregistrement d'une configuration sur l'appliance FAST360

Cet enregistrement revient à enregistrer la configuration sur l'appliance FAST360® à laquelle vous êtes connectée. Enregistrer la configuration sur l'appliance FAST360® ne signifie pas que l'appliance FAST360® la prend en compte. Il faut en effet déployer la configuration pour que celle-ci soit prise en compte.

Vérification de la cohérence d'une configuration

Il est essentiel de vérifier la cohérence de la configuration avant de la déployer. Arkoon Manager recherche automatiquement les erreurs de cohérence avant le déploiement d'une configuration.

La fenêtre « Vérification de Cohérence » affiche trois types de message différents :

- Erreurs
- Avertissements
- Messages d'information

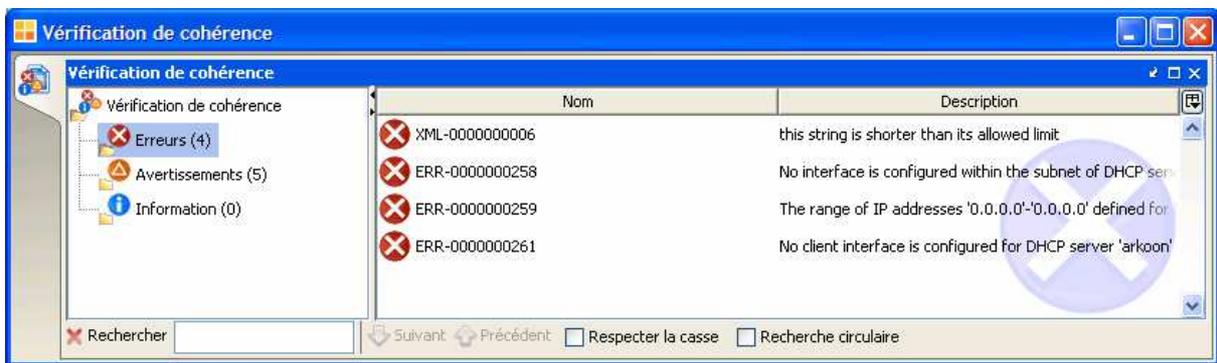
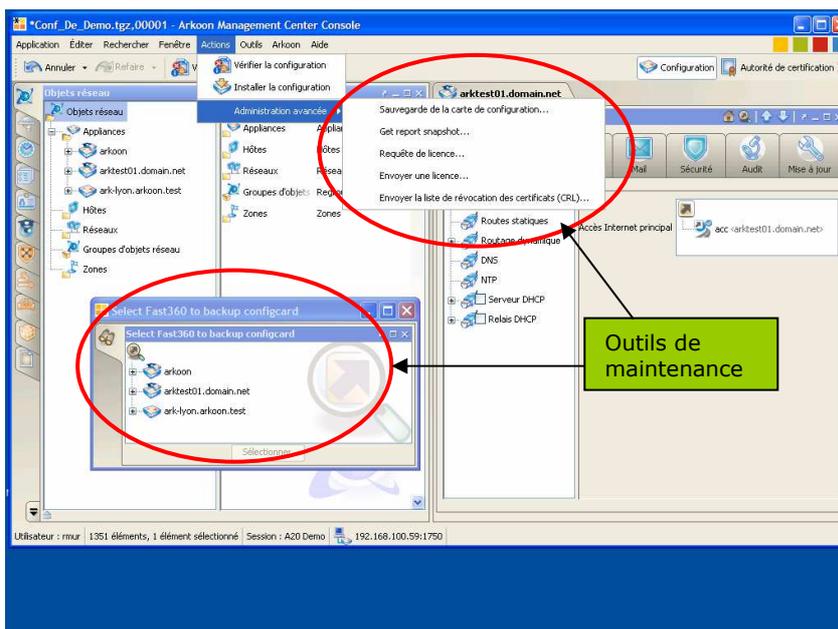


Fig 11 : Vérification de cohérence

b. Fonctions de maintenance

Arkoon Manager fournit aux administrateurs un ensemble de fonctionnalités facilitant la maintenance des appliances. Ces fonctionnalités sont accessibles à partir du menu Actions dans le cadre de la modification d'une configuration de politique de sécurité en mode connecté.



- Sauvegarde de configuration système
- Obtention d'un instantané d'état
- Obtention d'une requête de licence depuis l'appliance FAST360®
- Installation d'une licence sur une appliance FAST360®
- Déploiement de listes de révocation de certificat (CRL)

Fig 12 Fonctions de maintenance

III. Supervision

1. ARKOON Monitoring

ARKOON Monitoring est une application « temps réel » qui permet de superviser et de piloter l'activité des appliances FAST360®. Les fonctions principales suivantes sont accessibles depuis l'interface :

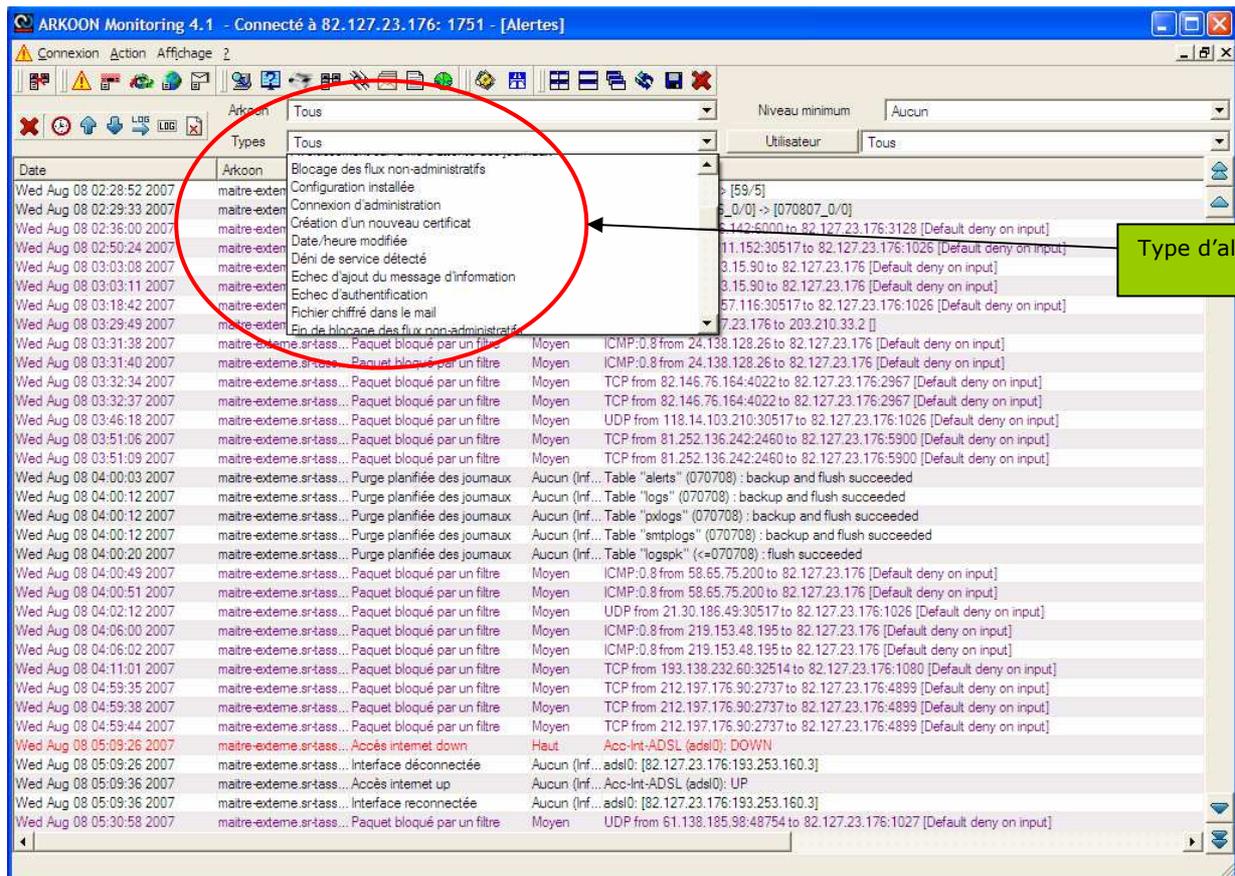
- Consultation/Supervision des journaux (logs)
- Supervision de l'état des appliances en temps réel
- Gestion des appliances
- Mise à jour les appliances

L'accès à ces différentes fonctions est soumis à la gestion des politiques de contrôle d'accès (gestion des rôles)

a. Les journaux de logs

Les logs sont classifiés dans cinq catégories différentes :

- **Alertes** : attaques applicatives, virus, scan de ports, incidents réseau, etc....



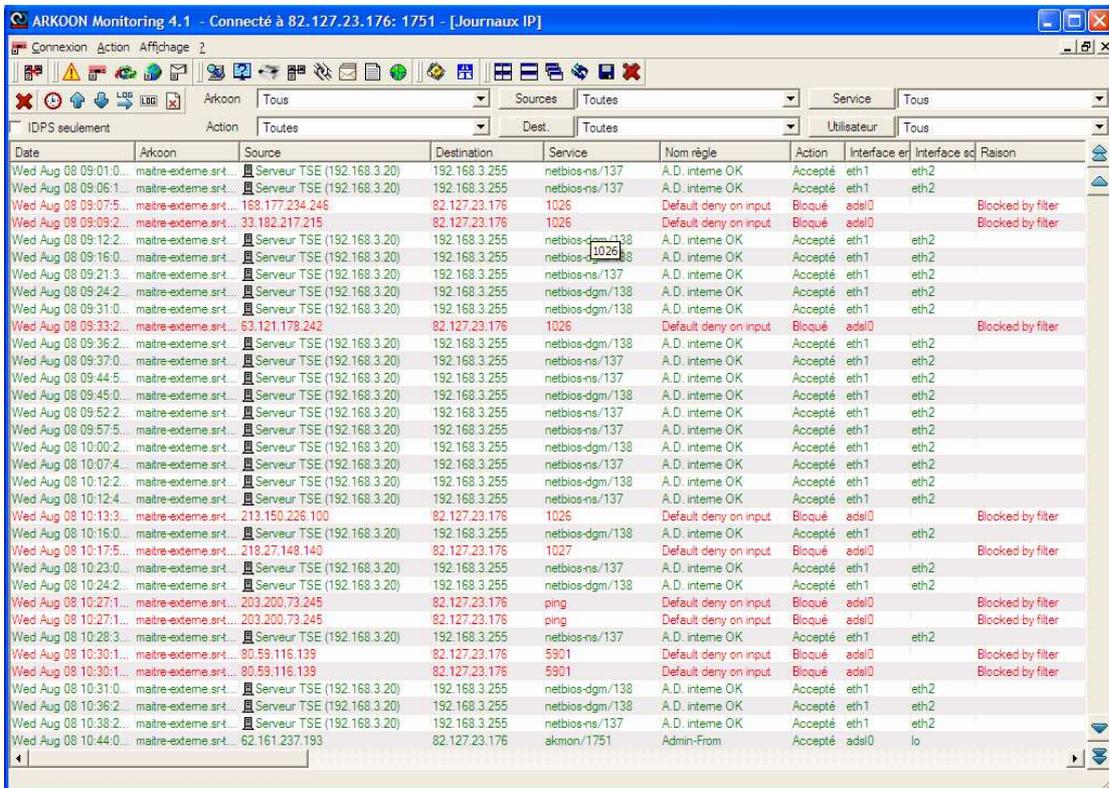
The screenshot shows the ARKOON Monitoring 4.1 interface. The main window displays a list of alerts with columns for Date, Type, and Description. A red circle highlights the 'Types' column, and a green box labeled 'Type d'alertes' points to the 'Alertes' category in the dropdown menu. The list includes various system events and network-related alerts.

Date	Type	Description
Wed Aug 08 02:28:52 2007	Arkoon	Blocage des flux non-administratifs
Wed Aug 08 02:29:33 2007	maître-exter	Configuration installée
Wed Aug 08 02:36:00 2007	maître-exter	Connexion d'administration
Wed Aug 08 02:50:24 2007	maître-exter	Création d'un nouveau certificat
Wed Aug 08 03:03:08 2007	maître-exter	Date/heure modifiée
Wed Aug 08 03:03:11 2007	maître-exter	Déni de service détecté
Wed Aug 08 03:18:42 2007	maître-exter	Echec d'ajout du message d'information
Wed Aug 08 03:29:49 2007	maître-exter	Echec d'authentification
Wed Aug 08 03:31:38 2007	maître-exter	Fichier chiffré dans le mail
Wed Aug 08 03:31:40 2007	maître-exter	Fin de blocage des flux non-administratifs
Wed Aug 08 03:32:34 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 03:32:37 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 03:46:18 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 03:51:06 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 03:51:09 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:00:03 2007	maître-exter.srtass...	Purge planifiée des journaux
Wed Aug 08 04:00:12 2007	maître-exter.srtass...	Purge planifiée des journaux
Wed Aug 08 04:00:12 2007	maître-exter.srtass...	Purge planifiée des journaux
Wed Aug 08 04:00:20 2007	maître-exter.srtass...	Purge planifiée des journaux
Wed Aug 08 04:00:49 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:00:51 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:02:12 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:06:00 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:06:02 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:06:02 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:11:01 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:59:35 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:59:38 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 04:59:44 2007	maître-exter.srtass...	Paquet bloqué par un filtre
Wed Aug 08 05:09:26 2007	maître-exter.srtass...	Accès internet down
Wed Aug 08 05:09:26 2007	maître-exter.srtass...	Interface déconnectée
Wed Aug 08 05:09:36 2007	maître-exter.srtass...	Accès internet up
Wed Aug 08 05:09:36 2007	maître-exter.srtass...	Interface reconnectée
Wed Aug 08 05:30:58 2007	maître-exter.srtass...	Paquet bloqué par un filtre

Fig 13 : Logs Alertes

Les alertes sont regroupées par niveau :

- Niveau Aucun : il s'agit d'une simple information, il n'y a pas eu de comportement anormal ;
 - Niveau Bas : il s'agit d'une information ayant trait à un événement pouvant avoir un impact sur la sécurité ;
 - Niveau Moyen : l'alerte signale un événement méritant une analyse par l'administrateur ;
 - Niveau Haut : l'alerte remonte un problème qui mérite d'être rapidement diagnostiqué (une action devra probablement être réalisée par l'administrateur).
- **Logs IP** : ils permettent de visualiser les informations relatives aux paquets acceptés, bloqués ou rejetés lorsque leur journalisation est paramétrée dans la politique de sécurité installée sur l'Arkoon. Les journaux IP permettent de visualiser l'ensemble des informations de l'entête du paquet IP. On affichera notamment (liste non exhaustive)
 - Date : date et heure de l'Arkoon à l'arrivée du paquet ;
 - Arkoon : nom de l'Arkoon qui journalise le paquet ;
 - Source : adresse IP source ;
 - Destination : adresse IP destination ;
 - Service : nom du service et port destination associé ;
 - Utilisateur : nom de l'utilisateur de l'Arkoon.
 - Action : action effectuée sur le paquet (ce champ peut prendre les caractéristiques Accepté, Bloqué, Rejeté).
 - Protocole : nom du protocole ;
 - Interface d'entrée : nom de l'interface d'entrée ;
 - Interface de sortie : nom de l'interface de sortie.
 - Translation
 - N° séquence, fenêtre TCP, etc.....



Date	Arkoon	Source	Destination	Service	Nom règle	Action	Interface en	Interface sd	Raison
Wed Aug 08 09:01:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:06:1...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:07:5...	maitre-externe.srt...	168.177.234.246	82.127.23.176	1026	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 09:09:2...	maitre-externe.srt...	33.182.217.215	82.127.23.176	1026	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 09:12:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:16:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:21:3...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:24:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:31:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:33:2...	maitre-externe.srt...	63.121.178.242	82.127.23.176	1026	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 09:36:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:37:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:44:5...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:45:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:52:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 09:57:5...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:00:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:07:4...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:12:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:12:4...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:13:3...	maitre-externe.srt...	213.150.226.100	82.127.23.176	1026	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 10:16:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:17:5...	maitre-externe.srt...	218.27.148.140	82.127.23.176	1027	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 10:23:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:24:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:27:1...	maitre-externe.srt...	203.200.73.245	82.127.23.176	ping	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 10:27:1...	maitre-externe.srt...	203.200.73.245	82.127.23.176	ping	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 10:28:3...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:30:1...	maitre-externe.srt...	90.59.116.139	82.127.23.176	5901	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 10:30:1...	maitre-externe.srt...	90.59.116.139	82.127.23.176	5901	Default deny on input	Bloqué	ads10		Blocked by filter
Wed Aug 08 10:31:0...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:36:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-dgm/138	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:38:2...	maitre-externe.srt...	192.168.3.20	192.168.3.255	netbios-ns/137	A.D. interne OK	Accepté	eth1	eth2	
Wed Aug 08 10:44:0...	maitre-externe.srt...	62.161.237.193	82.127.23.176	akmon/1751	Admin-From	Accepté	ads10	lo	

Fig 14 : Logs « IP »

Il est par ailleurs possible de visualiser le contenu d'un paquet bloqué en sélectionnant « Détail du paquet ».

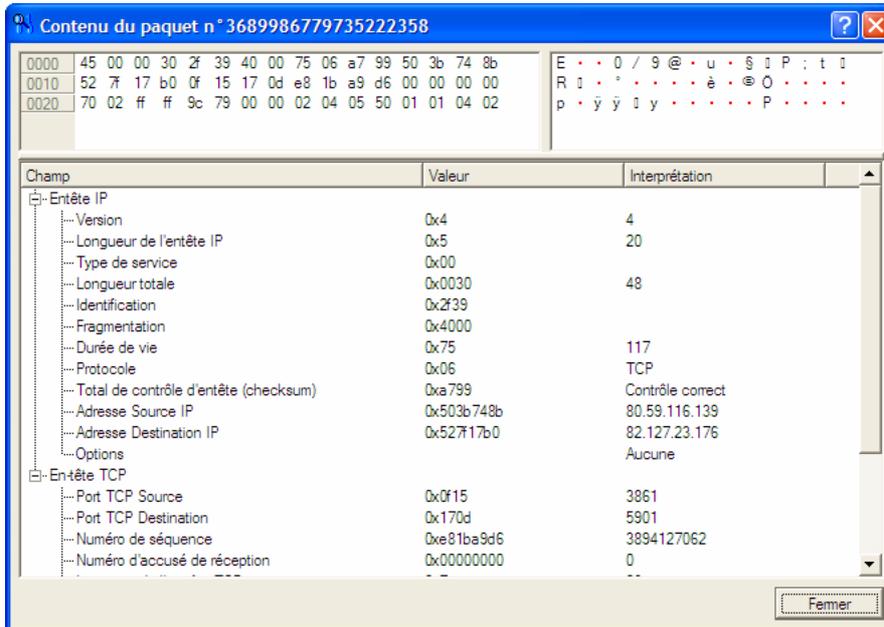


Fig 14 : Détail d'un paquet

- **Logs IDPS** : permet de visualiser les principales caractéristiques de la connexion qui a déclenché l'alerte IDPS. Cette fenêtre ne liste que les connexions qui ont été coupées par l'IDPS. Elle permet de suivre l'activité IDPS en mode Coupure.

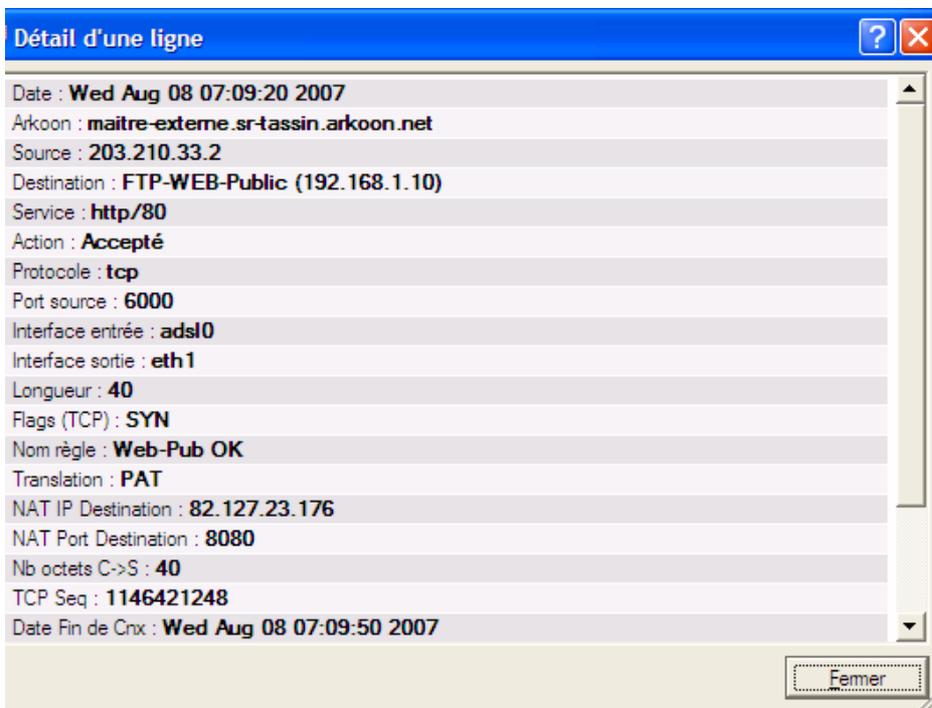
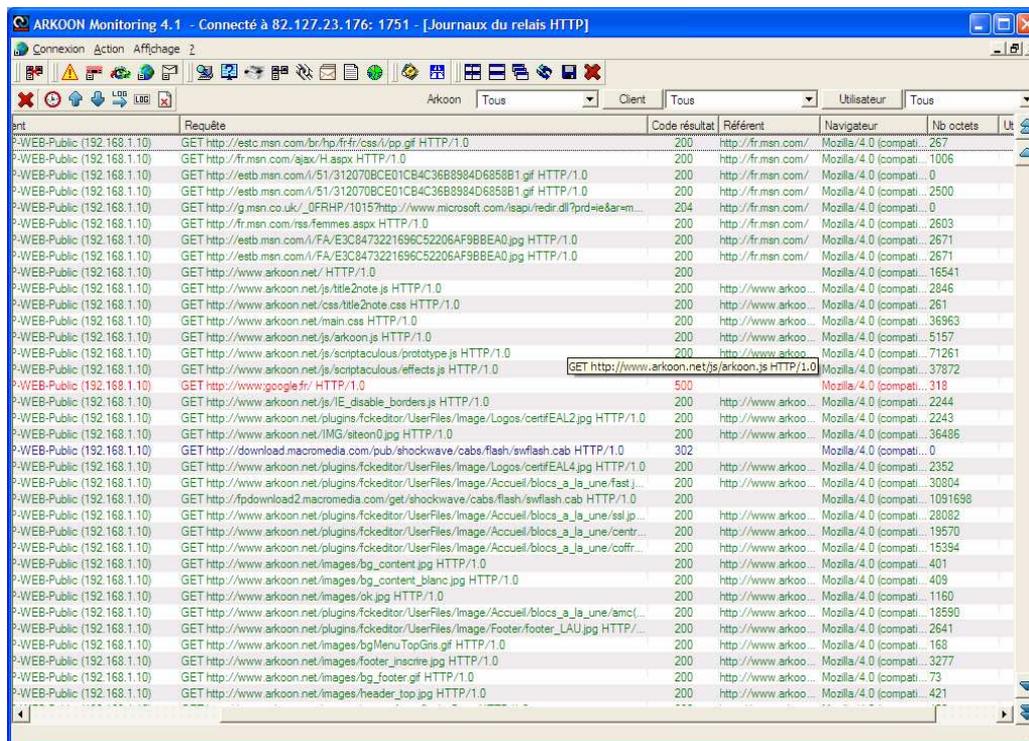


Fig 15 : Détail IDPS

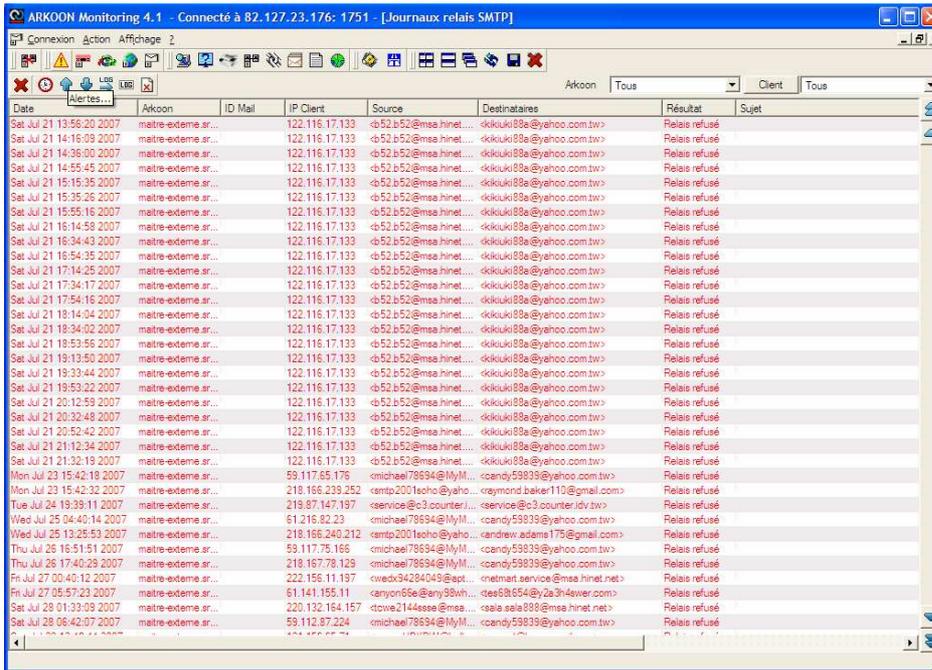
- Logs HTTP : Les journaux du relais HTTP permettent de visualiser les détails des requêtes HTTP, FTP, HTTPS et Gopher qui sont relayées par le relais http. Les journaux du relais HTTP permettent de visualiser les informations suivantes :
 - Date : date et heure de l'Arkoon à l'arrivée de la requête ;
 - Arkoon : nom de l'Arkoon journalisant le paquet ;
 - IP Client : adresse IP source du client émettant la requête ;
 - Utilisateur : nom de l'utilisateur, s'il s'est authentifié ;
 - Requête : contenu de la requête ;
 - Code résultat : code résultat de la requête.
 - Référent : contenu de l'en-tête Referer du paquet HTTP ;
 - Navigateur : navigateur utilisé par le client, comme spécifié dans l'en-tête User-Agent du paquet HTTP ;
 - Nb octets : taille des données reçues en réponse à la requête en octets.



Requête	Code résultat	Référent	Navigateur	Nb octets
GET http://estc.msn.com/br/hp/fr/fr/css/v/p/gf HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	267
GET http://fr.msn.com/ajax/H.aspx HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	1006
GET http://estb.msn.com/i/51/312070BCED1C84C368B984D6858B1.gif HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	0
GET http://estb.msn.com/i/51/312070BCED1C84C368B984D6858B1.gif HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	2500
GET http://g.msn.co.uk/_9FRHP/1015?http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=...	204	http://fr.msn.com/	Mozilla/4.0 (compati...	0
GET http://fr.msn.com/rss/femmes.aspx HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	2603
GET http://estb.msn.com/i/FA/E3C8473221696C52206AF98BEA0.jpg HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	2671
GET http://estb.msn.com/i/FA/E3C8473221696C52206AF98BEA0.jpg HTTP/1.0	200	http://fr.msn.com/	Mozilla/4.0 (compati...	2671
GET http://www.arkoon.net/ HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	16541
GET http://www.arkoon.net/js/title2note.js HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	2846
GET http://www.arkoon.net/css/title2note.css HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	261
GET http://www.arkoon.net/main.css HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	36963
GET http://www.arkoon.net/js/arkoon.js HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	5157
GET http://www.arkoon.net/js/scriptaculous/prototype.js HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	71261
GET http://www.arkoon.net/js/scriptaculous/effects.js HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	37872
GET http://www.google.fr/ HTTP/1.0	500	http://www.arkoo...	Mozilla/4.0 (compati...	318
GET http://www.arkoon.net/js/IE_disable_borders.js HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	2244
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Logos/centfEAL2.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	2243
GET http://www.arkoon.net/IMG/siteon0.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	36496
GET http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab HTTP/1.0	302	http://www.arkoo...	Mozilla/4.0 (compati...	0
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Logos/centfEAL4.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	2352
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Accueil/blocs_a_la_une_fast.j...	200	http://www.arkoo...	Mozilla/4.0 (compati...	30804
GET http://download2.macromedia.com/get/shockwave/cabs/flash/swflash.cab HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	1091698
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Accueil/blocs_a_la_une/ssl.jp...	200	http://www.arkoo...	Mozilla/4.0 (compati...	28082
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Accueil/blocs_a_la_une/centr...	200	http://www.arkoo...	Mozilla/4.0 (compati...	19570
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Accueil/blocs_a_la_une/coffr...	200	http://www.arkoo...	Mozilla/4.0 (compati...	15394
GET http://www.arkoon.net/images/bg_content.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	401
GET http://www.arkoon.net/images/bg_content.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	409
GET http://www.arkoon.net/images/ok.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	1160
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Accueil/blocs_a_la_une/amc(...	200	http://www.arkoo...	Mozilla/4.0 (compati...	18590
GET http://www.arkoon.net/plugins/fckeditor/UserFiles/Image/Footer/footer_LAU.jpg HTTP/...	200	http://www.arkoo...	Mozilla/4.0 (compati...	2641
GET http://www.arkoon.net/images/bg_MenuTopGns.gif HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	168
GET http://www.arkoon.net/images/footer_inscrite.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	3277
GET http://www.arkoon.net/images/bg_footer.gif HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	73
GET http://www.arkoon.net/images/header_top.jpg HTTP/1.0	200	http://www.arkoo...	Mozilla/4.0 (compati...	421

Fig 16 Journal relais HTTP

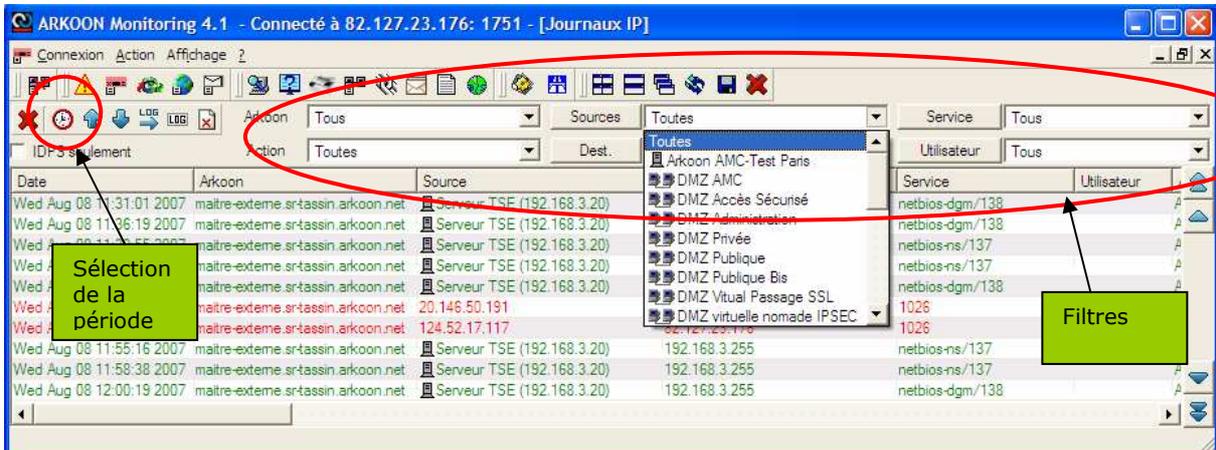
- Les journaux du relais SMTP permettent de visualiser le détail des mails qui sont relayés par le relais SMTP. Les journaux du relais SMTP permettent de visualiser les informations suivantes :
 - Date : date et heure de l'Arkoon à l'arrivée de la requête ;
 - Arkoon : nom de l'Arkoon journalisant le paquet ;
 - ID Mail : identifiant associé au mail (généralisé de façon aléatoire) ;
 - IP Client : adresse IP du client SMTP qui a émis le mail ;
 - Origine : adresse email de l'émetteur ;
 - Destinataires : adresse(s) email du/des destinataire(s) ;
 - Sujet : objet du mail ;
 - Nb octets : taille du mail en octets ;
 - Résultat : résultat du traitement du mail. (Réception OK, Contenu OK, Relais refusé, Virus détecté dans le message, Message refusé par la règle, Message placé en quarantaine



Date	Arkoon	ID Mail	IP Client	Source	Destinataires	Résultat	Sujet
Sat Jul 21 13:56:20 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 14:16:09 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 14:36:00 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 14:55:45 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 15:15:35 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 15:35:26 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 15:55:16 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 16:14:58 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 16:34:43 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 16:54:35 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 17:14:25 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 17:34:17 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 17:54:16 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 18:14:04 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 18:34:02 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 18:53:56 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 19:13:50 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 19:33:44 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 19:53:22 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 20:12:59 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 20:32:48 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 20:52:42 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 21:12:34 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Sat Jul 21 21:32:19 2007	maitre-externe.ar...		122.116.17.133	<52.b52@msa.hinet...	<kikuiki88a@yahoo.com.tw>	Relais refusé	
Mon Jul 23 15:42:18 2007	maitre-externe.ar...		59.117.85.178	<michael78694@MyM...	<candy59839@yahoo.com.tw>	Relais refusé	
Mon Jul 23 15:42:32 2007	maitre-externe.ar...		218.166.239.252	<cento2001teho@yaho...	<ojymont.parker113@gmail.com>	Relais refusé	
Tue Jul 24 19:39:11 2007	maitre-externe.ar...		219.87.147.197	<service@3.counter.i...	<service@3.counter.idv.tw>	Relais refusé	
Wed Jul 25 04:40:14 2007	maitre-externe.ar...		61.216.82.23	<michael78694@MyM...	<candy59839@yahoo.com.tw>	Relais refusé	
Wed Jul 25 13:25:53 2007	maitre-externe.ar...		218.166.240.212	<cento2001teho@yaho...	<sandrew.adame175@gmail.com>	Relais refusé	
Thu Jul 26 15:51:51 2007	maitre-externe.ar...		59.117.75.166	<michael78694@MyM...	<candy59839@yahoo.com.tw>	Relais refusé	
Thu Jul 26 17:40:29 2007	maitre-externe.ar...		218.167.78.129	<michael78694@MyM...	<candy59839@yahoo.com.tw>	Relais refusé	
Fr Jul 27 00:40:12 2007	maitre-externe.ar...		222.156.11.197	<wcdx34284049@ept...	<netmart.service@msa.hinet.net>	Relais refusé	
Fr Jul 27 05:57:23 2007	maitre-externe.ar...		61.141.155.11	<canyon66a@any98wh...	<des68654@za3h4ever.com>	Relais refusé	
Sat Jul 28 01:33:09 2007	maitre-externe.ar...		220.132.164.157	<stove214asse@msa...	<caia.sala898@msa.hinet.net>	Relais refusé	
Sat Jul 28 06:42:07 2007	maitre-externe.ar...		59.112.87.224	<michael78694@MyM...	<candy59839@yahoo.com.tw>	Relais refusé	

Fig 17 : journal relais SMTP

Pour augmenter la précision, ARKOON Monitoring permet d'appliquer des filtres aux requêtes pour chaque type de log et permet de sélectionner et ordonner les colonnes à afficher



Date	Arkoon	ID Mail	IP Client	Source	Destinataires	Résultat	Sujet
Wed Aug 08 11:31:01 2007	maitre-externe.sr-tassin.arkoon.net			Serveur TSE (192.168.3.20)			
Wed Aug 08 11:36:19 2007	maitre-externe.sr-tassin.arkoon.net			Serveur TSE (192.168.3.20)			
Wed Aug 08 11:55:09 2007	maitre-externe.sr-tassin.arkoon.net			Serveur TSE (192.168.3.20)			
Wed Aug 08 12:00:12 2007	maitre-externe.sr-tassin.arkoon.net			Serveur TSE (192.168.3.20)			
Wed Aug 08 11:55:53 2007	maitre-externe.sr-tassin.arkoon.net			20.146.50.191			
Wed Aug 08 12:00:19 2007	maitre-externe.sr-tassin.arkoon.net			124.52.17.117			
Wed Aug 08 11:55:16 2007	maitre-externe.sr-tassin.arkoon.net			192.168.3.255			
Wed Aug 08 11:58:38 2007	maitre-externe.sr-tassin.arkoon.net			192.168.3.255			
Wed Aug 08 12:00:19 2007	maitre-externe.sr-tassin.arkoon.net			192.168.3.255			

Fig 18 : Critères de sélections

Les logs sont stockés soit directement sur l'apppliance, soit remontés sur l'apppliance Maître ou sur le serveur AMC. Les bases de données de logs sont archivées automatiquement (avec une fréquence configurable). Cette gestion dynamique de l'archivage limite l'augmentation de taille des bases de données de logs.

b. Supervision de l'état des appliances en temps réel

L'administrateur dispose de différents indicateurs lui permettant de surveiller l'état de l'apppliance en temps réel

- Etat CPU, Disque, Mémoire
- Connexions actives
- Etat des tunnels VPN : possibilité de monter ou démonter un tunnel manuellement
- Etat des interfaces

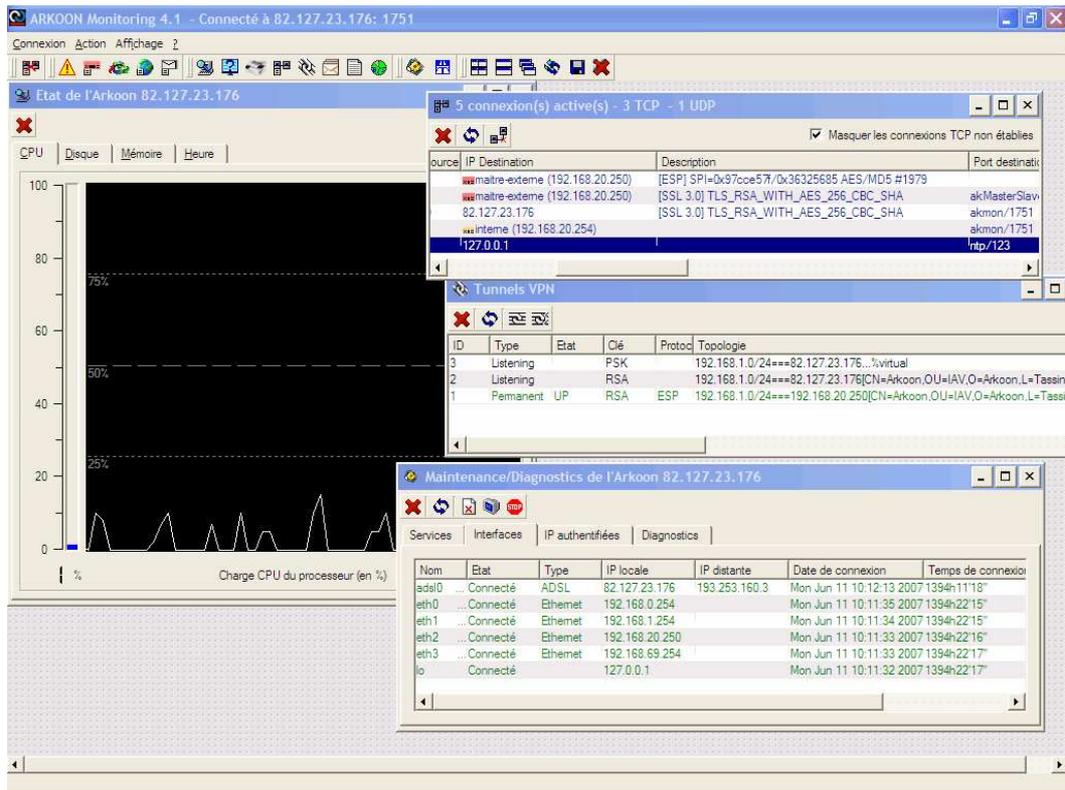


Fig 19 Etat de l'appliance

- Etat des services
- Etat de la bande passante : optimisation de la politique de gestion dynamique de la bande passante en fonction des règles de QoS

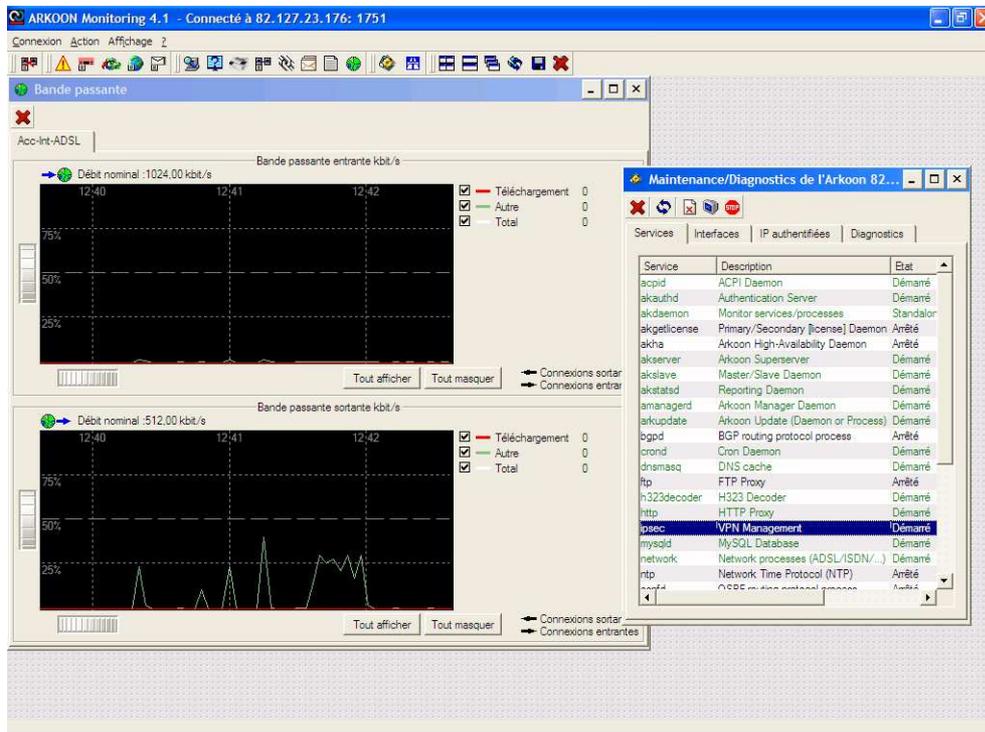


Fig 20 : Bande passante

c. Gestion des appliances

Arkoon Monitoring permet également des opérations de gestion

- archives de logs
- mises en quarantaine des mails
- Diagnostics

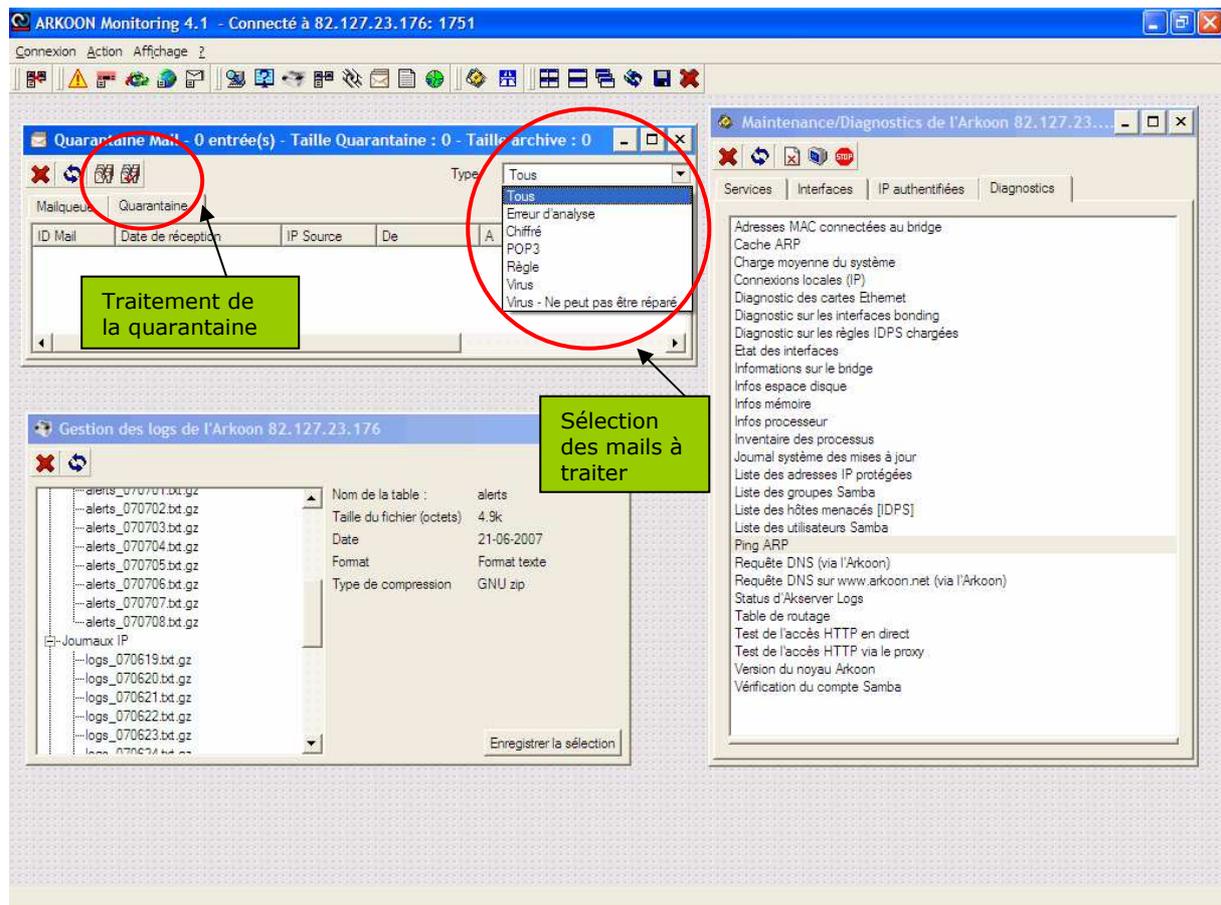


Fig 21 : Gestion des appliances

d. Mises à jour

Pour augmenter l'efficacité des appliances FAST360®, des mises à jour automatiques programmables sont disponibles sur les serveurs dédiés hébergés par ARKOON. Les connexions pour mise à jour sont sécurisées :

- Authentification de l'appliance par son certificat (lié à sa licence)
- Chiffrement des flux (SSL, 168 bits)

Les appliances peuvent télécharger les mises à jour de type suivant (mode de téléchargement « pull »):

- Signatures antivirus/antispymware
- Signatures d'attaques (FAST in line IDPS)
- Listes noires pour filtrage des URL (relais HTTP)
- Règles heuristiques d'antispam
- Système ARKOON AKS des appliances FAST360®

La fréquence de mise à jour (15 minutes minimum) est définie par l'administrateur.

Il s'agit de mises à jour différentielles. Une fréquence de mise à jour élevée est donc sans impact sur le fonctionnement de l'apppliance ou sur la bande passante mise à sa disposition.

La mise à jour s'effectue dans un contexte hautement sécurisé :

- Disponibilité totale des serveurs de mise à jour, qui sont hébergés dans des locaux sécurisés
- Connexions authentifiées par certificats X509 (liés à la licence de chaque machine)
- Téléchargements chiffrés en SSLv3
- Action Undo/Défaire disponible en cas d'échec de la mise à jour

Arkoon Monitoring permet de contrôler les MAJ, de lancer manuellement les téléchargements des MAJ et de procéder à la mise à jour du système.

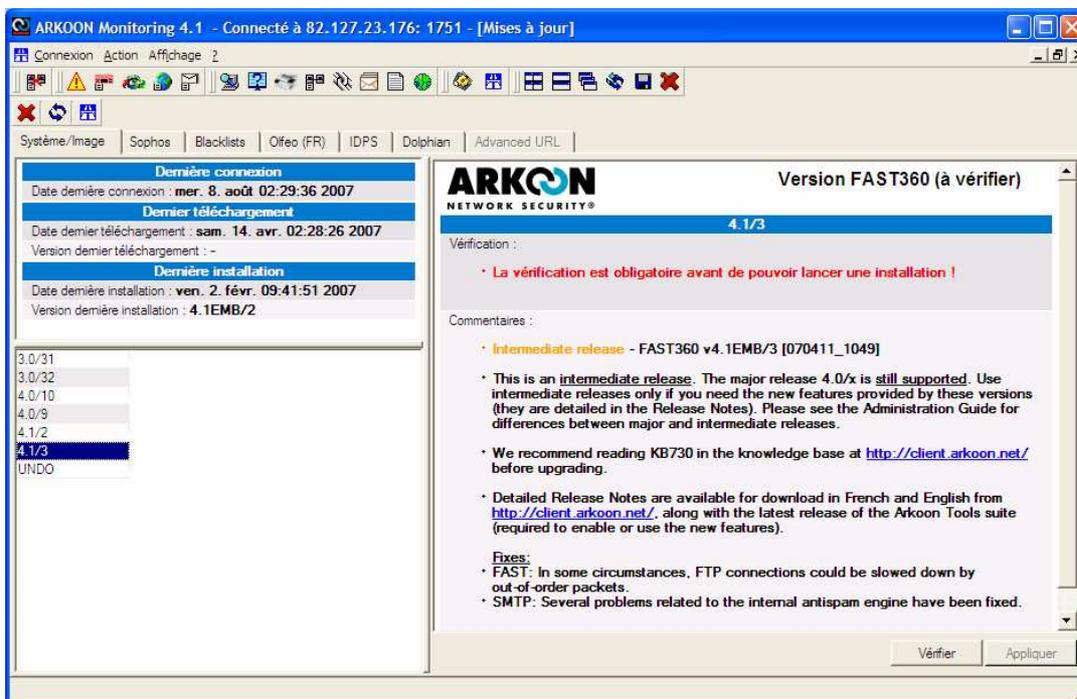


Fig 22 Mise à jour système

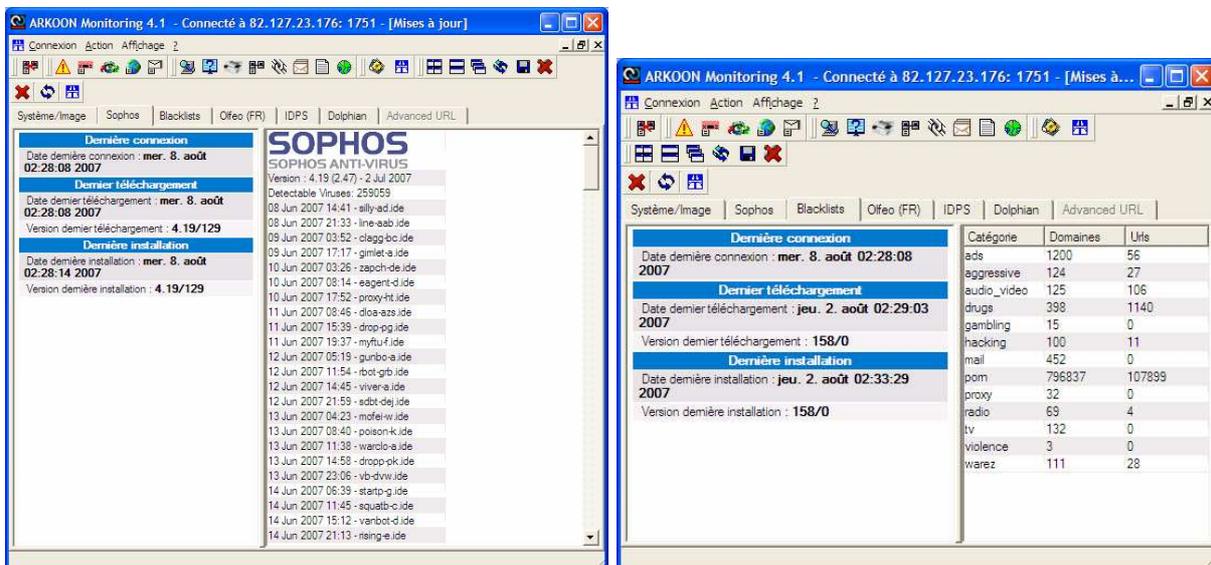


Fig 23 Mise à jour Antivirus et Blacklists

2. *Intégration avec des solutions tierces*

L'environnement d'administration complet des appliances ARKOON garantit l'efficacité de leur implémentation et de leur exploitation.

ARKOON intègre les mécanismes de communication avec des solutions externes de supervision :

- Envoi des Alertes par Email ou par traps SNMP
- Déport des logs en temps réel sur des serveurs Syslog
- Exportation des logs au format Texte ou WELF : dans ce cadre, des solutions spécialisées de traitement et d'analyse des logs son compatibles avec les systèmes Arkoon :
 - Webtrends
 - Net Report
- Supervision SNMP

L'objectif de la supervision SNMP est de permettre le suivi de la « bonne santé » de l'appliance (états de la mémoire, des interfaces, des disques, du processeur...) et de récupérer des données brutes sur le comportement de l'appliance (comme le trafic réseau par interfaces) pour analyser les tendances et conserver un historique. Dans ce cadre, la totalité des superviseurs SNMP sont ainsi supportés : HP Openview, Tivoli.....

L'agent SNMP intégré aux appliances FAST360® fonctionne en mode « read only » ce qui interdit la configuration SNMP (qui constituerait une limite de sécurité sur l'appliance, la configuration de la politique de sécurité nécessitant systématiquement une authentification forte de l'administrateur).

La configuration de la supervision SNMP se fait depuis l'outil de configuration Arkoon Manager et permet d'activer des sous-ensembles de la MIB-II et UC DAVIS.

Liste des MIB supportés :

system	RFC1213
interfaces (ifaces)	RFC1213
IP	RFC1213
TCP	RFC1213
UDP	RFC1213
SNMP	RFC1213
mem	UCD SNMP MIB
proc	UCD SNMP MIB
disk	UCD SNMP MIB
load	UCD SNMP MIB
sysstats	UCD SNMP MIB
perf	RFC 1514

IV. ARKOON Reporting

Destiné aux sites gérant jusqu'à une centaine d'utilisateur, l'outil ARKOON Reporting réduit considérablement les coûts liés à la gestion de la sécurité. Vous contrôlez directement l'activité de votre réseau et vous analysez les attaques et les comportements à caractère intrusif qui menacent votre système d'information.

ARKOON Reporting collecte les rapports d'activité générés quotidiennement par les appliances FAST360®. Il est ainsi possible de générer les rapports concernant une certaine période. En général, les rapports graphiques affichent le résumé des logs d'activité :

Activité Internet (avec relais HTTP) :

- 10 URL les plus visitées (volume, nombre de requêtes, etc.)
- 10 utilisateurs les plus actifs (volume de téléchargement, durée de connexion, etc.)
- Résumé des alertes HTTP

Activité de messagerie (avec proxy SMTP) :

- Résumé par expéditeur ou par destinataire
- Alertes de sécurité (virus, spam, tentatives de mise en relais, etc.)

Alertes de sécurité :

- Tri par type d'alerte (scan des ports, virus, infractions au protocole, etc.)
- Tri par niveau d'alerte
- Tri par calendrier/timetable

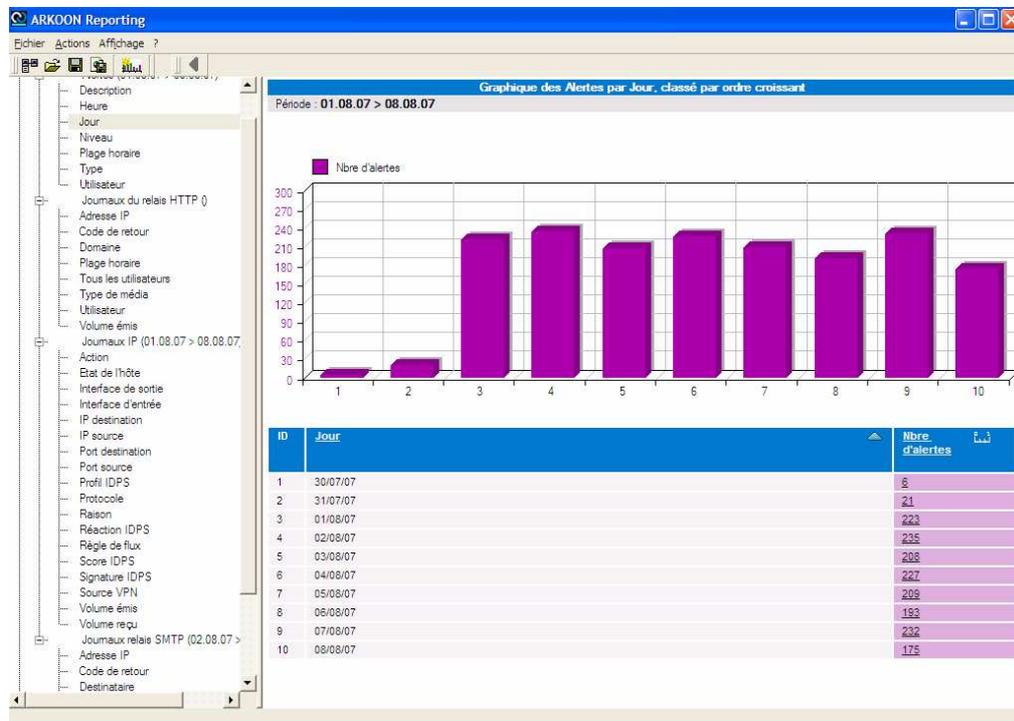


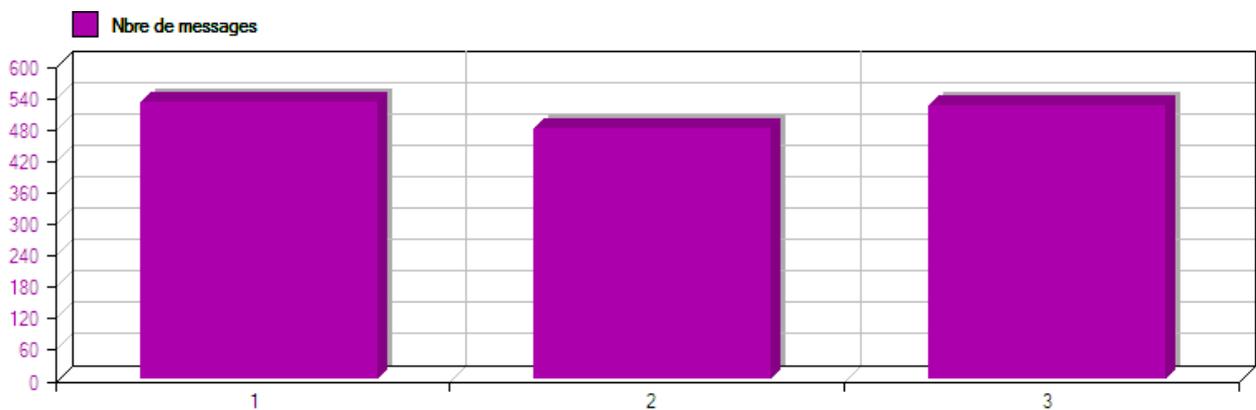
Fig 24 Graphique « Nombre alertes / jour »

Publication automatique des rapports d'activité

ARKOON Reporting génère automatiquement des rapports d'activité sous forme graphique (HTML). Vous pouvez ainsi distribuer à vos responsables ou à vos collaborateurs les résumés et les indicateurs graphiques décrivant les performances globales de votre système d'information. ARKOON Reporting supporte vos décisions stratégiques en vous aidant à anticiper vos besoins futurs

Graphique des Journaux IP par Protocole, classé par ordre croissant

Période : 01.08.07 > 08.08.07



ID	Protocole	Nbre de messages
1	icmp	529
2	tcp	479
3	udp	523