Fonctions Réseau et Télécom

Haute Disponibilité

FAST360®
Appliances

Sommaire

I. Performance et disponibilité

Résumé

- ✓ Qualité de Service : gestion du trafic et marquage « Diffserv »
- ✓ Equilibrage de charge et lien de secours
- ✓ Optimisation des ressources de télécommunication
- ✓ Haute disponibilité

1. Gestion de la bande passante et qualité de service (QoS)

A ce jour, les réseaux IP s'appuie sur des mécanismes de « Best Effort ».
La saturation des liens, l'augmentation de la latence des équipements sont à l'origine de nombreux problèmes (drop de paquets « imprédictibles », délai d'acheminement et gigue importante) et ne permettent plus un fonctionnement optimal d'un certain nombre d'applications critiques et stratégiques pour l'entreprise (streaming, VoIP, vidéo-conférence , application métier…).

FAST360 implémente un module de gestion du traffic (QoS), conforme à la norme « Diffserv » et permettant d'optimiser la bande passante.
Le modèle DiffServ consiste à classer le trafic grâce à un code présent dans le paquet IP (champ DSCP). On applique ensuite des traitements différenciés aux différentes classes de trafic.

Différents mécanismes sont implémentés :

- Dans le traitement des flux en entrée
  - Classification selon différents critères (source, destination, service, plage horaire, utilisateur, accès Internet)
  - Trafic Conditionner : Token Bucket (réservation dynamique de bande passante) et « Two Rates Three Color Marker » permettant des actions différentes (drop, marquage, accept packet) selon 2 seuils paramétrables.
- Dans le traitement des flux en sortie
  - Classification selon différents critères (source, destination, service, plage horaire, utilisateur, acces Internet, marquage DSCP)
  - Gestion des files d'attentes (queing et dequeing) avec 2 scheduler : CBQ et HTB (organisation hiérarchique des classes de trafic et gestion du débordement)
  - Gestion des congestions (dropper) avec 2 algorithmes : Taildrop (FIFO) et RED (drop avant saturation)
  - Marquage du champ DSCP (Classes de Service BE, EF, AF conforme au modèle Diffserv RFC2475) pour forcer les équipements à suivre une politique de QoS.
- Fonctions d'audit
  - Représentation graphique du trafic
  - Alertes

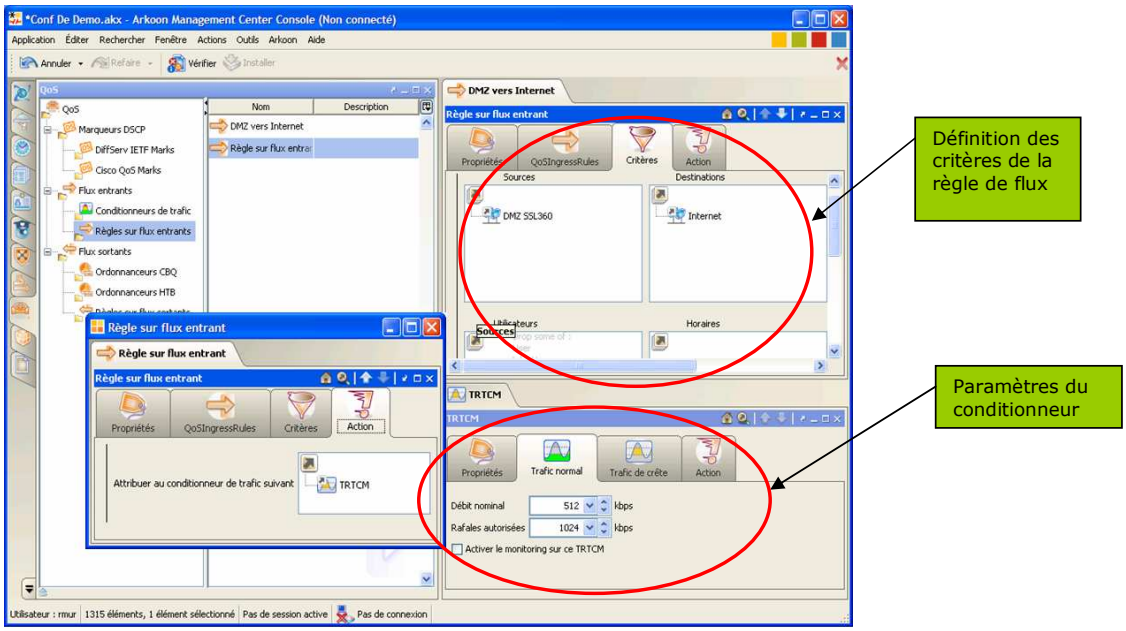


Fig 1 : Règle de flux en entrée - conditionneur TRTCM

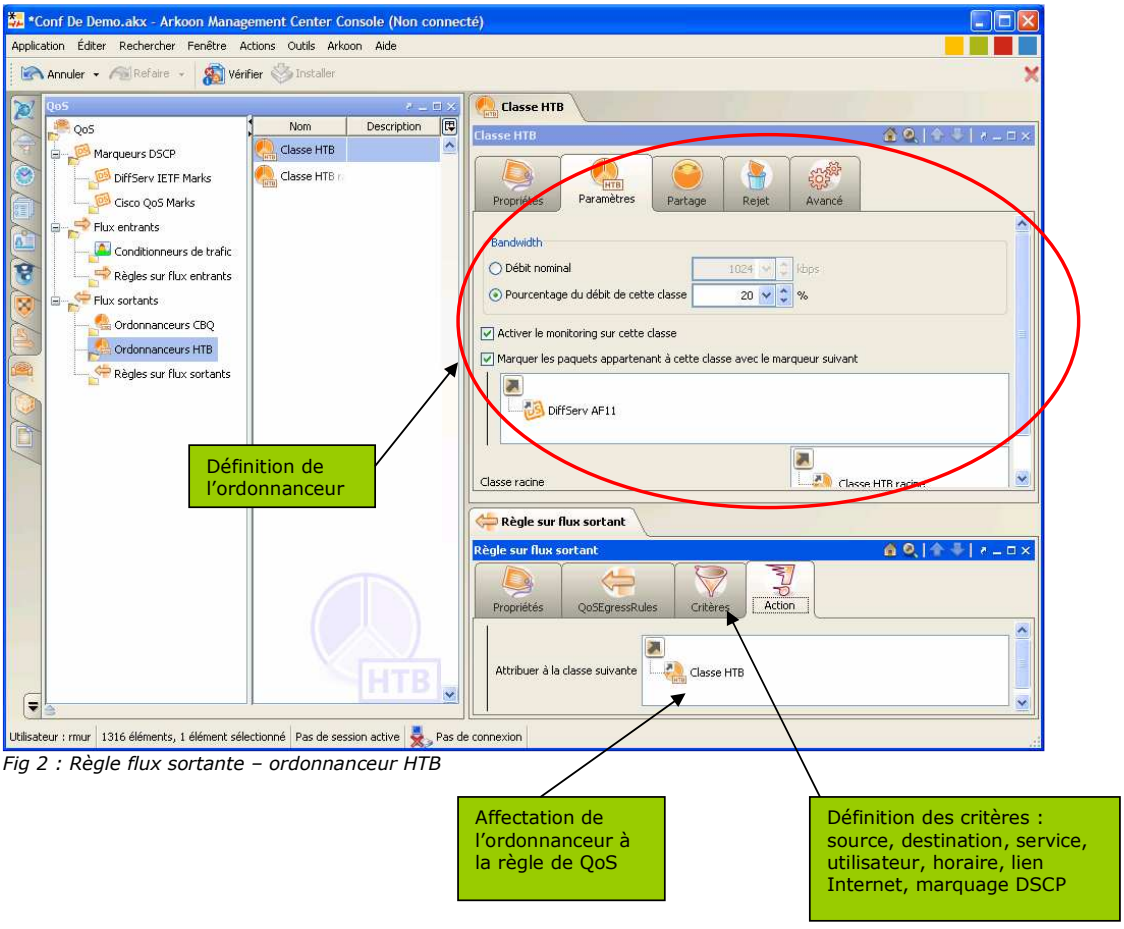


Fig 2 : Règle flux sortante – ordonnanceur HTB

2. *Équilibrage de charge*

Une appliance FAST360® peut gérer plusieurs accès Internet en simultané (par exemple ADSL ou ISDN et Ethernet). Il est alors possible de définir des règles d'équilibrage de charge de manière à gérer plus efficacement les types et les volumes de trafic sur des accès différents.

Les fonctionnalités disponibles sont les suivantes :

- Équilibrer la charge sur plusieurs accès
- Pour chaque protocole, définir un ou plusieurs accès principaux et un ou plusieurs accès secondaires (liaisons de secours)
- Forcer certains flux de données (définis par le protocole et par les adresses IP source/destination) à utiliser tel ou tel accès

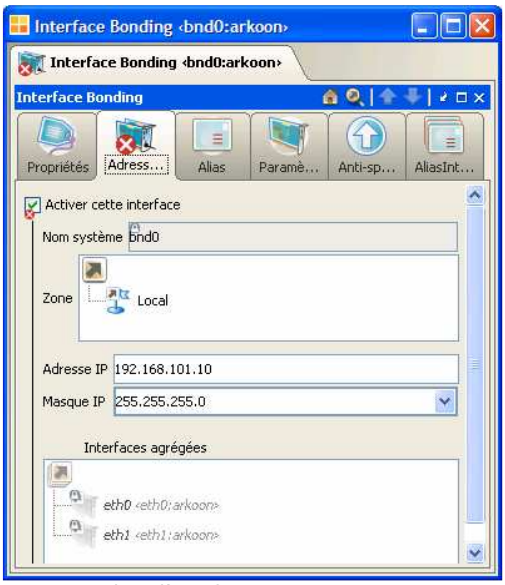


Fig 3 : Bonding d'interfaces

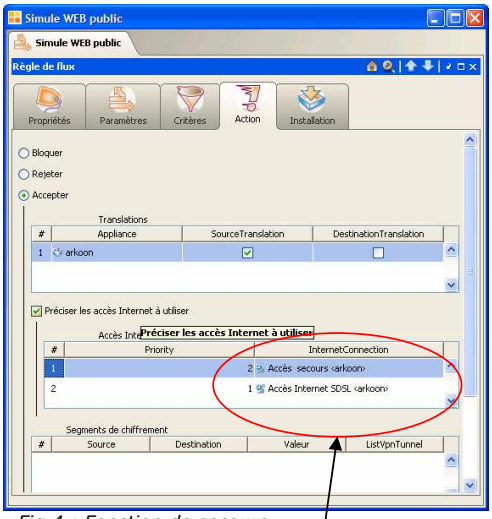


Fig 4 : Fonction de secours

Définition du lien principal (priorité 1) et du lien de secours (priorité 2)

3. *Agrégation de liens*

Les appliances FAST360® permettent de configurer l'agrégation de plusieurs interfaces physiques sous une seule interface logique afin d'optimiser la performance (et la bande passante) de la liaison.

4. Haute disponibilité (Gamme XPA sauf A2200 et A5200)

a. Introduction

La solution de haute disponibilité (HA, High Availabilty) proposée par ARKOON s'appuie sur deux machines qui se comportent comme une seule. Connectées en parallèle, ces machines garantissent que l'interruption de service ne dépassera pas quelques dixièmes de secondes en cas d'incident affectant la machine principale.

Une seule machine est active à la fois. La machine passive est chargée de détecter les incidents de la machine active via une liaison « heartbeat ». Si nécessaire, les machines sont interverties : la machine passive devient active à la place de la machine défectueuse.

Enfin, la possibilité de garder actives les connexions HA réduit la possibilité d'un changement d'état des connexions existantes et garantit une disponibilité encore plus élevée dans un environnement de sécurité optimal.

b. Heartbeat

Le « heartbeat » est une liaison redondante qui garantit des communications authentifiées entre deux machines HA. Cette liaison peut être définie sur différents supports :

- Sur une liaison série et une ou plusieurs liaisons Ethernet
- Sur plusieurs liaisons Ethernet

Dans leur liaison "heartbeat", les machines ARKOON HA transmettent les données suivantes :

- Communication continue pour vérifier l'activité de l'autre machine
- Données de configuration
- Logs
- Mises à jour
- E-mails disponibles dans la machine qui est devenue passive après inversion des rôles
- Indication des connexions actives (si cette option est sélectionnée)

c. Administration et supervision

La fonction est supervisée à l'aide de l'outil Minarkconf (interface accessible en mode console). L'administration de la politique de sécurité s'effectue en mode transparent, à l'aide de l'outil ARKOON Manager.

L'état HA des machines est supervisé à l'aide de l'outil ARKOON Monitoring, qui indique en permanence l'état de la configuration et qui avertit l'administrateur en cas d'interversion des appliances FAST360® active et passive.

d. Exemple d'architecture

Le schéma ci-dessous illustre une configuration réseau élémentaire qui utilise une solution ARKOON HA.

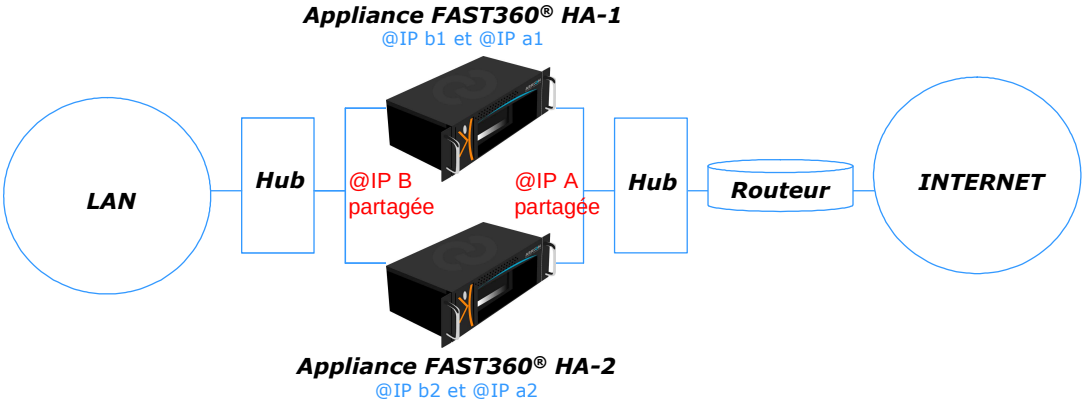
Trois interfaces Ethernet sont utilisées par machine :

- Une pour le heartbeat
- Une autre pour le réseau interne
- Une dernière pour le réseau externe sur chaque machine HA

Chaque interface réseau interne et externe des machines ARKOON HA doit être configurée avec une adresse (spécifique à chaque machine). Ces « adresses réelles » sont affectées de manière permanente à la machine active et à la machine passive). Les adresses réelles sont disponibles dans le menu de configuration HA de Minarkconf.

Les adresses fonctionnelles (ou « adresses virtuelles ») sont définies dans le fichier de configuration commun aux deux machines, à l'aide de l'outil ARKOON Manager.

La connexion série permet de doubler la liaison heartbeat entre les deux machines et d'éviter les inversions de rôle non justifiées entre machine passive et machine active. La machine passive devient active lorsqu'elle ne reçoit plus le heartbeat de la machine active (ni sur la liaison Ethernet dédiée ni sur la liaison série).



5. Clustering (Gamme NPA et A2200/A5200)

Le Clustering consiste à implémenter plusieurs appliances en parallèle. Ces appliances fournissent **des services identiques** et partagent un certain nombre d'éléments :

- La configuration de l'appliance
- Les logs
- La table des connexions actives

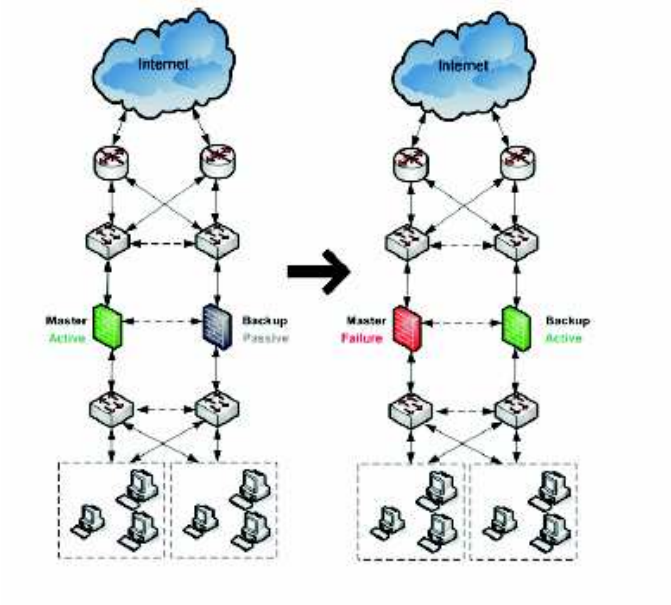
Le Clustering peut être configuré en mode Haute-Disponibilité ou en mode Haute-Performance.

a. Mode Haute-Disponibilité

Ce mode est souvent appelé « **Actif-Passif** » : dans ce mode, on a un nœud actif (il gère l'ensemble du trafic) et un nœud passif (sans activité) en attente de reprise des services dans le cas de rupture du nœud actif.
Dans ce mode, la performance globale est identique avant et après la bascule : si on l'estime à **100% d'un nœud simple avant la rupture de service**, elle reste à 100% après la rupture de service.

Ce mode est particulièrement adapté dans les cas de protection d'applications critiques où le besoin de continuité du service sans aucune dégradation de performance est impératif.

- ***Cas d'utilisation***



Dans ce mode, un nœud est **actif**, l'autre nœud est **passif**, en attente de défaillance du nœud actif.
Le **master** propage sa configuration et la table des connexions vers le **backup**.

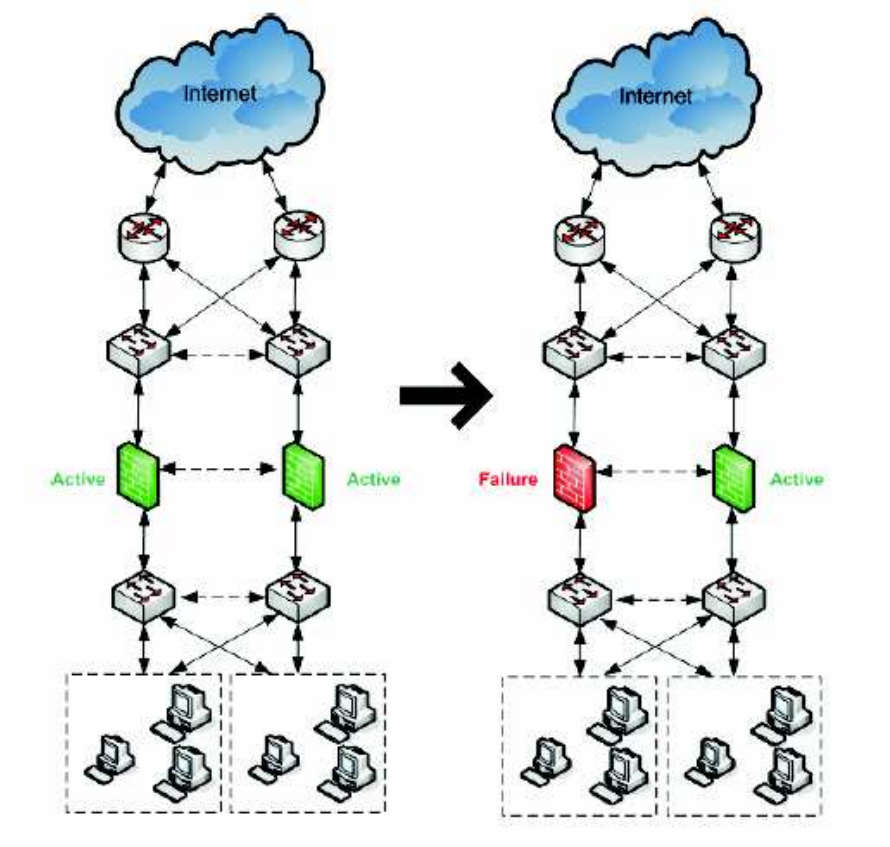
La performance est de 100% **avant et après** la bascule
En cas de bascule, le backup est promu actif et il prend en charge l'ensemble du trafic

b. Mode Haute-Performance

Ce mode est souvent appelé « **Actif-Actif** » : dans ce mode, les deux nœuds sont actifs simultanément, chacun gérant une partie du trafic.
En cas de rupture d'un nœud, le nœud restant reprend l'ensemble du trafic : si la performance globale est estimée à **200% d'un nœud simple avant la rupture de service**, elle passe à 100% après la rupture de service : il faudra donc s'assurer que ce niveau de performance dégradé est acceptable ponctuellement.

Ce mode est particulièrement adapté dans les cas de protection d'applications critiques où le besoin essentiel est de répartir les fortes charges sur 2 équipements en parallèle : en cas de rupture d'un nœud, le système doit rester globalement opérationnel pour absorber les pics de charge liés à la dégradation de performance (débit divisé par 2).

- ***Cas d'utilisation***



Dans ce mode, les 2 nœuds sont **actifs simultanément.** En cas de défaillance d'un nœud, le nœud restant reprend l'ensemble des connexions du nœud défaillant.
Si la performance est de **200% avant** la bascule, elle passe à **100% après** la bascule. (ie ce n'est donc pas du HA puisque le service est alors « dégradé »)
Chaque appliance prend en charge une partie du trafic. En cas de défaillance d'un nœud, le nœud restant gère l'ensemble du trafic.
La répartition de charge est à la charge de l'environnement : load-balancer externe, assignation statique ou dynamique (DHCP) des « default route », implémentation de routage dynamique, utilisation de DNS (passerelle Internet)…

c. Protocole VRRP

La fonction Clustering repose sur les concepts suivants :

- "State Protocol" : Protocole permettant de déterminer l'état d'une appliance (Active, Passive, en panne,…). Ce protocole pouvant être envoyé sur différents type de média (port série, Ethernet,…). Le protocole VRRP est utilisé pour assurer cette fonction ;

- "Data Synchronisation Protocol" : Protocole permettant de transmettre les données et les états des modules FAST entre les différents noeuds/appliances du cluster (protocole propriétaire).

Dans un réseau donné, l'ensemble des noeuds partagent un ou plusieurs Virtual Router Identifier (VRID). Un VRID est un entier compris entre 1 et 255. Chaque VRID représente un routeur virtuel, possédant une adresse IP virtuelle, et une adresse MAC virtuelle (00:00:5E:00:01:VRID). Dans ce réseau, pour un VRID donné, le routeur Maître a une priorité de 255, les autres routeurs ont une priorité comprise entre 1 et 254.

Un noeud peut être Routeur Maître pour un VRID donné, et Routeur Backup pour une autre VRID. Pour le protocole de synchronisation, il est important de connaître quel noeud est maître pour un VRID donné.

Pour implémenter les 2 modes de fonctionnement disponibles, VRRP est utilisé de manière différente en fonction de ce mode.

Utilisation de VRRP en mode Actif / Passif

Mise en forme : Puces et numéros

En mode Actif/Passif, l'appliance utilise VRRP avec seulement un seul VRID par interface. Un des 2 noeuds est Maître pour ce VRID, l'autre est le Backup.

Le protocole VRRP peut définir un noeud Maître ou Backup pour chaque VRID. Dans notre cas, il a été choisi d'avoir le même état pour tous les VRIDs. Donc, l'état VRRP d'un VRID associé à une interface est le même pour tous les VRID utilisés sur une appliance. On obtient donc un état de l'appliance au lieu d'un état d'un VRID.

Si l'état VRRP d'un des VRID devient Backup, tous les VRID VRRP deviennent alors "backup".

Utilisation de VRRP en mode Actif / Actif

Mise en forme : Puces et numéros

En mode Actif/Actif, l'appliance utilise 2 VRID par interface (dans le cas d'un cluster à 2 noeuds). Pour le premier VRID, une appliance est Maître. Pour l'autre VRID, l'autre appliance est également Maître.

d. Supervision de la fonctionnalité HA

Mise en forme : Puces et numéros

L'état du système en mode HA/Cluster est visible dans la fenêtre « Cluster » de l'outil Monitoring.

Cette fenêtre fournit les informations suivantes :

- Mode de Cluster (Actif/Passif ou Actif/Actif) ;
- Liste des noeuds du cluster ;

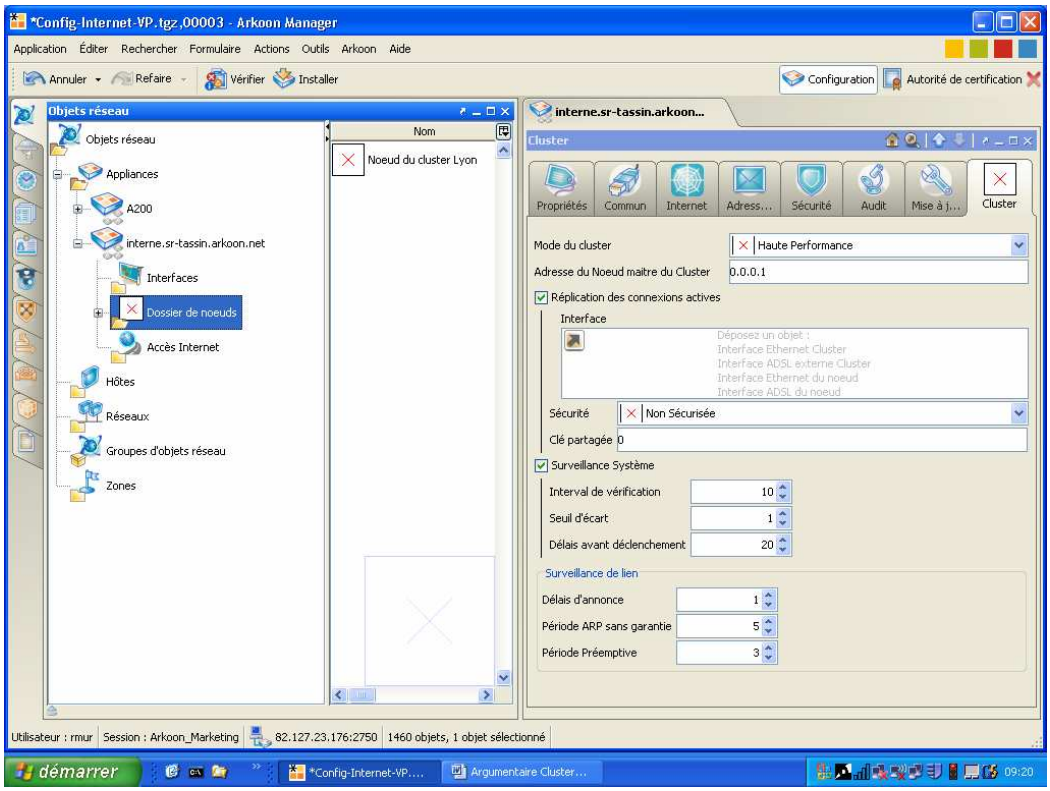
Pour chaque noeud, les informations suivantes :

- Etat : actif ou passif ;
- Etat du système (par sysmon) ;
- Les interfaces configurées ;

Pour chaque interface, les informations suivantes :

- Adresse IP statique ;
- Adresse IP virtuelle initiale ;
- Adresse(s) IP virtuelle(s) courante(s).

A tout moment, l'opérateur doit pouvoir mettre un ou plusieurs noeuds en mode Failure (panne).



II. Fonctions réseau et télécommunication

Résumé

Déployées en réseau, les appliances de sécurité FAST360® assurent des fonctions réseaux évoluées :

- ✓ Translation des adresses
- ✓ Mode transparent (ou bridge)
- ✓ Partitionnement de réseaux VLAN (802.1q)
- ✓ Interprétation des paquets ICMP
- ✓ Routage dynamique
- ✓ DHCP Relais et Serveur

1. Translation d'adresses

La translation d'adresses IP permet de masquer les adresses IP des hôtes d'un réseau privé aux hôtes d'un réseau public. Par ailleurs, la translation d'adresses IP simplifie les tables de routage des appliances en réseau.

Les appliances FAST360® supportent plusieurs types de translations d'adresses :

a. Translation statique, ou NAT statique

Translation symétrique 1-à-1 : un hôte du réseau à protéger est publié en externe et se voit affecter l'adresse externe correspondante.

L'appliance FAST360® applique la translation statique comme attribut d'un objet réseau « hôte ».

b. Translation Réseau à Réseau

La translation de réseau à réseau offre des fonctions similaires à celles fournies par la NAT statique mais appliquées à l'ensemble des hôtes du réseau. Il permet de translater l'adresse IP du réseau en conservant la partie de l'adresse spécifique à l'hôte. La translation de réseau à réseau nécessite que le réseau protégé et le réseau translaté aient le même masque de sous-réseau.

Exemple : Le LAN à protéger à l'adresse IP 192.168.0.0/24 et contient 3 hôtes : 192.168.0.12 ; 192.168.0.29 ; 192.168.0.121. Le réseau translaté (ou destination) est 2.21.0.0/24. Les adresses translatées des hôtes dans le réseau destination seront 2.21.0.12 ; 2.21.0.29 et 2.21.0.121.

c. Masquage

Le masquage correspond à la translation n-à-1 des adresses du réseau interne vers une seule Adresse IP externe. Il s'agit d'une translation asymétrique qui s'applique uniquement aux connexions de sortie.

Les appliances FAST360® appliquent le masquage des adresses IP comme caractéristique d'un objet « règle de flux ». Le masquage doit être activé flux par flux :

- Soit par défaut, avec l'adresse externe principale de l'appliance ARKOON
- Soit en spécifiant un alias d'adresse de translation dans l'interface externe de l'appliance ARKOON

d. PAT, ou redirection de port

La translation de ports PAT permet de publier dans un réseau non protégé un service (port TCP/UDP) qui est hébergé sur l'un des serveurs du réseau à protéger. Il s'agit d'une translation asymétrique qui s'applique uniquement aux connexions d'entrée.

PAT garantit un niveau de sécurité plus élevé que la translation statique, dans la mesure où seuls les services pertinents sont redirigés. En outre, la redirection de port permet à plusieurs services hébergés sur des serveurs distincts de partager la même adresse IP publique.

Les appliances FAST360® appliquent la translation PAT comme caractéristique d'un objet « règle de flux ».

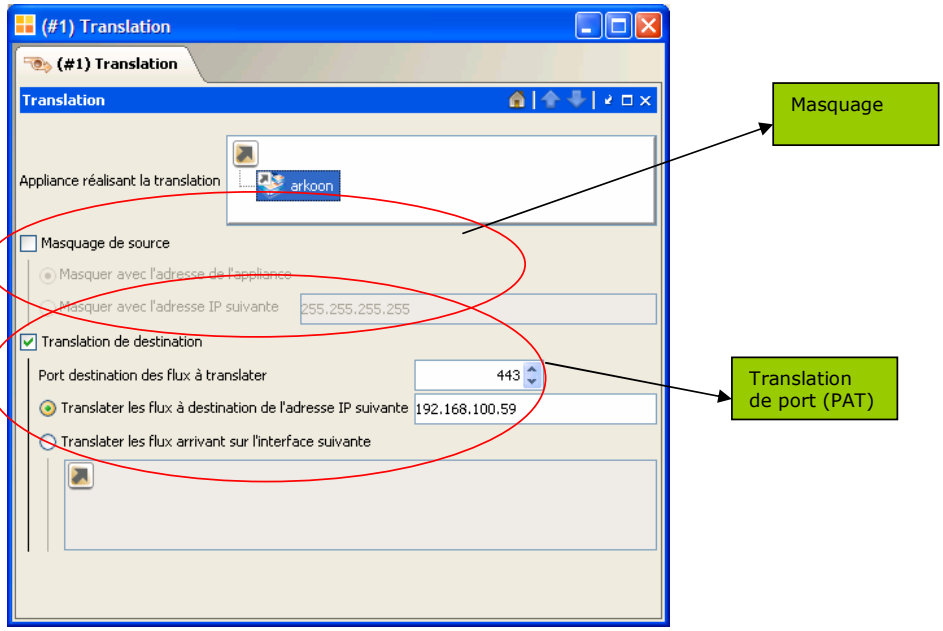


Fig 5 : Masquage et PAT

2. *Bridge, ou mode transparent*

Le mode transparent facilite le déploiement des appliances FAST360® sans impacter le niveau de sécurité. Le bridge établi entre plusieurs interfaces permet à une appliance FAST360® d'être intégrée dans un réseau sans avoir à modifier l'architecture de ce dernier.

Par exemple, vous pouvez déplacer un serveur dans une zone sécurisée (DMZ) sans modifier son adresse IP, c'est-à-dire sans aucun impact sur l'environnement du réseau. Une fois le serveur isolé dans la DMZ, tous les accès à ce serveur traversent l'appliance FAST360® pour plus de sécurité.

Pour une plus grande souplesse de déploiement, les appliances FAST360® proposent deux modes d'exploitation pour les bridges :

- *Mode furtif* – Le bridge ne dispose pas d'une adresse IP dans le réseau : il est complètement indétectable (même par une interrogation systématique/scan du réseau).
- *Mode non furtif* – Le bridge dispose de l'adresse IP commune à toutes les interfaces de bridge.

3. VLAN

En insérant une appliance FAST360® dans une architecture VLAN, vous pouvez envisager les actions suivantes :

- Partitionner les entités du réseau
- Implémenter un filtrage entre plusieurs VLAN

ARKOON implémente le standard VLAN le plus répandu : 802.1q dans ses appliances de sécurité. Les VLAN peuvent être définis par sous-réseaux, par adresses MAC ou par ports. Les appliances FAST360® peuvent uniquement être utilisées dans les architectures VLAN définies par sous-réseaux.

Dans les architectures de ce type, la communication entre commutateurs est assurée explicitement à l'aide de balises/tags qui permettent de spécifier l'affiliation à un VLAN spécifique.

Le système FAST360® peut être utilisé pour les fonctions suivantes :

- Filtrage entre plusieurs VLAN
- Filtrage entre commutateurs (liaison principale/trunk)

Pour le filtrage entre plusieurs VLAN, les appliances supportent toutes les fonctions de sécurité nécessaires.

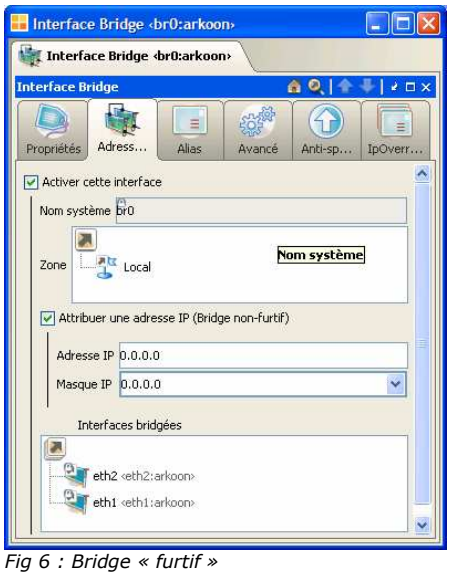


Fig 6 : Bridge « furtif »

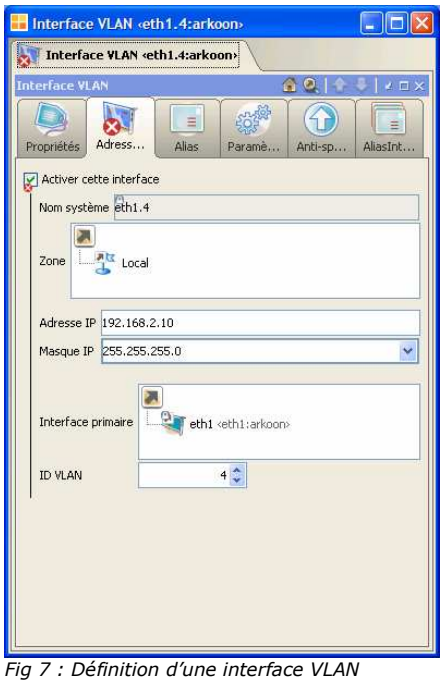


Fig 7 : Définition d'une interface VLAN

4. Routage dynamique

Les appliances FAST360® peuvent fonctionner comme des routeurs IP, intégrant la fonction de routage dynamique basée sur les principaux protocoles standard de l'industrie.

- *RIP :* Les équipements FAST360® intègrent aussi bien RIP que RIPv2. Notez cependant que la configuration de RIP nécessite que soit également configuré, sur l'appliance, des règles de filtrage qui autorisent les messages de broadcast, car RIP utilise le broadcast pour diffuser ses mises à jour de table de routage avec les autres équipements du réseau. RIP est généralement considéré comme le protocole de routage dynamique le plus simple, mais il est essentiellement adapté aux petits réseaux ou aux liaisons point à point.

- *OSPF :* Initialement développé pour parer à certaines limites de RIP, OSPF est le plus puissant et le plus sophistiqué des protocoles de routage dynamique. Cependant il nécessite une plus grande connaissance des réseaux, de leur plan de configuration et de leur implémentation. C'est le protocole le mieux adapté aux grands réseaux d'entreprise.

- *BGP :* BGP a été introduit pour faciliter le routage entre les opérateurs sur le backbone Internet. Il est principalement utilisé par les opérateurs et les grandes organisations qui ont besoin de routage sur des liens backbone.

Seule l'activation des protocoles se fait à travers l'interface graphique : la configuration et l'administration du routage dynamique se fait par une interface en lignes de commandes qui paraîtra familière aux ingénieurs réseaux qui ont l'expérience de la configuration de routeurs. Le guide d'administration fourni avec les appliances Arkoon FAST360® présente de façon complète comment administrer les appliances de sécurité comme des éléments de routage dynamique du réseau.

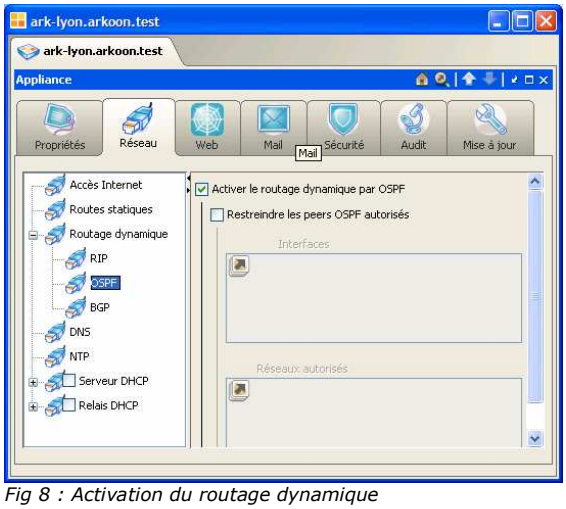


Fig 8 : Activation du routage dynamique

a. Contraintes imposées par le routage dynamique

Les contraintes ci-après sont imposées par les appliances Arkoon FAST360® sur lesquelles le routage dynamique a été activé :

- Dans une architecture avec plusieurs appliances, au moment de la configuration, il est difficile de déterminer quelles routes seront configurées sur chaque appliance. Pour éliminer cette ambiguïté, toutes les routes devront être configurées sur toutes les appliances qui ont du routage dynamique activé.

- Pour les appliances qui utilisent le routage dynamique, il n'est pas possible d'utiliser le système standard de contrôle de cohérence de la configuration. Par exemple, pour vérifier que les règles de flux et les VPN sont correctement configurés par rapport à la topologie du réseau.

- Il n'est pas possible de configurer les routes statiques de façon "classique", via le manager, lorsque le routage dynamique est activé. Si nécessaire, les routes statiques doivent être configurées en utilisant l'interface en lignes de commandes. Dans le cas d'une migration depuis une configuration qui utilise des routes statiques, pour installer la nouvelle configuration (avec routage dynamique) l'administrateur doit d'abord supprimer toutes les routes statiques puis re-configurer celles-ci en utilisant l'interface en lignes de commandes.

b. Routage Dynamique et Haute Disponibilité (HA)

Suivant le protocole utilisé, le routage dynamique est supporté différemment en haute disponibilité :

- *OSPF :* OSPF est activé sur les 2 équipements du système en HA (afin d'éliminer les problèmes liés à la latence lors du basculement HA). Le poids OSPF maximum est assigné aux routes qui passent par l'équipement passif pour éviter au réseau d'utiliser cette route. Ce poids est réajusté de façon appropriée au moment du basculement.

- *BGP :* Il s'agit d'un protocole point-à-point, donc BGP n'est activé que sur l'équipement actif.

- *RIP :* Ce protocole n'est pas supporté en configuration HA ARKOON.

5. Fonctions DHCP

DHCP est aujourd'hui un concept incontournable dans le réseau local (nombre croissant d'adresses IP, mobilité….) : FAST360 implémente deux mécanismes.

a. Relais DHCP

Les fonctionnalités suivantes sont intégrées :

- Forward des requêtes et/ou des réponses (broadcast et unicast) DHCP et BOOTP vers les serveurs et/ou les clients.
- Chaînage de relais
- Audit des évènements
- Support de DHCP Over Ipsec : forward des requêtes en provenance d'un tunnel VPN

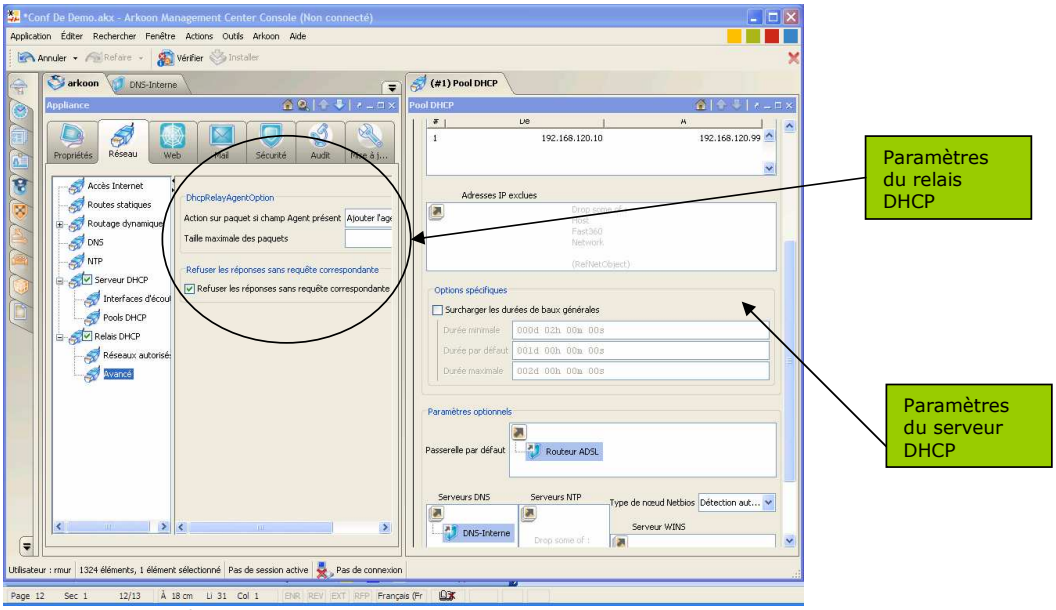


Fig 9 : Serveur et relais DHCP

b. Serveur DHCP

Les fonctionnalités suivantes sont intégrées :

- Traitement des requêtes DHCP et allocation d'in adresse IP
- Envoie d'information comme la « Gateway » le DNS, le Wins….
- Support de configuration par « pool » (1 pool unique par interface)
- Audit des évènements