ConfIn : une gestion centralisée de niveau 3 pour une plaque régionale

Olivier Lacroix

ConfIn : une gestion centralisée de niveau 3 pour une plaque régionale

Olivier LACROIX
CIRIL – Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du doyen Marcel Roubault – 54500 Vandœuvre-lès-Nancy - France
olivier.lacroix@ciril.fr

Résumé

ConfIn (acronyme de CONFiguration des INterfaces) est un logiciel permettant aux différents correspondants des entités (établissements, ou EPST) de la plaque régionale de Lorraine, Lothaire, d'avoir accès aux configurations de leurs réseaux, de voir les filtres mis en place, de faire des modifications sur ceux-ci, d'identifier les dysfonctionnements ou attaques et de faire des recherches.

Les équipements réseaux sont mutualisés. Seule l'équipe réseau du CIRIL peut y accéder et effectuer des modifications. Pour permettre aux correspondants des sites de Lothaire d'accéder à diverses informations sur les réseaux qu'il gèrent, le projet ConfIn a démarré en 2000. Son objectif de départ était simplement de fournir, au travers d'une interface Web, la configuration des interfaces réseaux et leurs filtrages. Les modifications du filtrage sur les routeurs restaient à l'époque à la charge de l'équipe réseau du CIRIL via des fichiers texte et quelques scripts. Depuis 2006, le produit a pris une nouvelle dimension en offrant aux correspondants des réseaux la possibilité de modifier eux-mêmes les règles de filtrage, de mettre en place des filtres temporaires et de faire des recherches dans les filtres. Il inclut aussi le support d'IPv6 pour toutes ses fonctionnalités.

Mots clefs

sécurité, filtrage, routeur, mutualisation

1 Préambule

Pour comprendre les origines de ConfIn et différents termes utilisés par la suite, il est nécessaire de présenter la façon dont est géré le réseau de la plaque régionale Lorraine, Lothaire.

Le réseau régional Lothaire est mutualisé, tant au niveau financier, que des équipements. De cette mutualisation découle le fait que tous les routeurs, souvent partagés entre plusieurs entités différentes (établissements ou EPST), sont gérés exclusivement par l'équipe réseau du CIRIL. Chaque entité reste cependant maître de sa politique de sécurité, ce qui inclut la définition des filtres positionnés sur les routeurs.

Pour gérer ses réseaux, chaque entité dispose de personnel que nous appellerons « correspondants » dans la suite de cet article.

Les correspondants sont des informaticiens (ou des personnes faisant fonction) désignés par les responsables des entités. Ils sont les interlocuteurs de l'équipe réseau du CIRIL dans la gestion quotidienne de leurs réseaux. Plus particulièrement pour cet article, ils sont en charge du suivi et des demandes de modification du filtrage.

2 Les origines de ConfIn

Le mode de fonctionnement de Lothaire (équipements mutualisés et gérés par le CIRIL, politique de sécurité définie par les entités) permet une gestion cohérente, mais il pose le problème du suivi et de la modification du filtrage de leurs réseaux par les correspondants des entités. Une mise à disposition de ces informations est donc nécessaire. Le projet ConfIn est né de ce besoin en 2000. Au départ, son but était simplement de proposer une interface Web permettant d'afficher et d'archiver les configurations des interfaces réseaux. Les modifications restaient à la charge de l'équipe réseau qui « traduisait » en langage de routeur (des « access-list ») les demandes de filtrage faites par les correspondants via des courriers électroniques. Bien que satisfaisante, cette méthode de modification avait des inconvénients :

- une demande pouvait être mal interprétée et la modification ne pas être celle souhaitée ;
- si une demande n'était pas assez claire (notamment si elle n'indiquait pas l'équipement et l'interface concernée parmi les 50 routeurs et les quelques 700 interfaces gérées), les demandes de précision pouvaient générer des délais ;
- les correspondants ne maîtrisaient pas du tout le filtrage de leurs réseaux.

Le produit a donc évolué pour pallier à ces difficultés.

3 L'évolution

3.1 Les choix réalisés

Depuis longtemps de nombreuses informations étaient stockées :

- les configurations des routeurs dans des fichiers texte ;
- les logs des transgressions des règles de filtrage ;
- des fichiers textes contenant les filtres de chacune des interfaces.

Cependant il n'existait rien pour les lier entre elles.

Chaque type d'information était transmis aux correspondants des sites ou utilisé localement via des logiciels indépendants. L'envoi des informations se faisait uniquement par courrier électronique automatisé ce qui ne permettait pas aux correspondants de choisir eux-mêmes les informations qu'ils désiraient récupérer. De plus, il n'y avait pas de point d'entrée unique pour accéder à celles-ci. Devant l'augmentation des besoins d'accès à ces informations et les demandes des correspondants, le choix a été fait d'offrir progressivement un moyen unique d'accès aux informations des interfaces des routeurs : configurations, filtres, violations des filtres, définition de ceux-ci, ...

Pour réaliser le logiciel, l'ensemble des informations disponibles a été centralisé et structuré. Suite à une phase d'analyse des besoins, des choix ont été réalisés.

Coté structuration du logiciel, cela se traduit par :

- le stockage des informations brutes au format texte (configurations des routeurs et logs) afin d'être facilement utilisables par toute application ;
- l'utilisation d'un SGBD[1] pour toutes les informations propres à l'application ;
- la fusion des applications autonomes dans un même produit.

Coté fonctionnalité, le produit répond aux principaux besoins suivants :

- associer les correspondants aux interfaces ;
- regrouper en une seule vue toutes les informations d'une interface ;
- donner des informations claires en restant le plus proche possible de la configuration des routeurs ;
- permettre à des correspondants « privilégiés » de modifier les filtres de façon simple ;
- prévenir les correspondants lors d'un changement de la configuration d'une interface gérée ;
- permettre des recherches dans les filtres et les violations de ceux-ci ;
- gérer la redondance d'interfaces ;
- être compatible IPv4 et Ipv6.

3.2 Les différentes versions

Trois versions majeures se sont succédées depuis 2000. Le changement de version majeure correspond à l'inclusion dans le produit d'un nouveau groupe de fonctionnalités, qui étaient jusqu'à lors traitées par des programmes indépendants.

La première version ne permettait que la consultation des configurations des interfaces et de leurs archives.

Dans la version suivante, tous les outils concernant les transgressions des filtres mis en place ont été intégrés : affichage de ceux-ci, recherche, génération par interface d'un résumé chaque nuit et archivage de celui-ci.

Enfin la troisième version majeure est apparue courant 2006. Elle a offert aux correspondants la possibilité de modifier eux-même les filtres des interfaces (c.f. 4.3) et a apporté le support d'IPv6.

4 Le produit actuel

4.1 Le principe de fonctionnement

Les correspondants accèdent au logiciel via une interface Web personnalisée en fonction de leurs droits. Le point d'entrée est la liste des interfaces pour lesquelles la personne a été définie correspondante.

Par interface, il existe deux niveaux de droits :

- les correspondants « simples » avec uniquement un droit de lecture ;
- les correspondants avec des droits de modifications.

Pour chaque interface, tout correspondant peut :

- consulter la configuration actuelle, les archives des configurations ou obtenir les différences entre deux configurations ;
- obtenir les logs du filtrage du jour ou des jours précédents (avec possibilité de lancer des recherches) ou une synthèse de ceux-ci ;
- voir tous les filtres du réseau Lothaire dans lesquels une machine de ses réseaux apparaît (très utile lors du déplacement d'un service d'une machine à une autre) ;
- activer ou désactiver des filtres temporaires préalablement définis. Ces filtres viennent s'ajouter aux filtres en cours et sont automatiquement désactivés toutes les nuits ;
- consulter les modifications de filtrage.

Le correspond ayant un droit de modification sur l'interface aura accès à une option supplémentaire lui permettant de

[1] Système de Gestion de Bases de Données

faire des demandes de modification du filtrage. Il ne s'agit que d'une demande. Les ajouts, les modifications ou les suppressions de règles sont enregistrées, puis la demande de changement est notifiée aux administrateurs (l'équipe réseau du CIRIL), catégorie particulière de correspondants. Ceux-ci, via la même interface Web peuvent visualiser toutes les demandes en attente et peuvent pour chacune d'entre elles accepter, modifier ou rejeter chaque changement. Ce n'est qu'après la validation de la demande par un administrateur que celle-ci est effectivement appliquée sur le routeur. Cette fonction assez complexe fait l'objet d'un paragraphe spécifique.

Enfin le correspondant dispose d'un menu contrôlant ses options de notification par courrier électronique :

- recevoir ou non chaque nuit un résumé, pour chaque interface, des transgressions des filtres de la veille ;
- être ou non prévenu lorsque la configuration d'une interface gérée a été modifié. Cette notification peut se faire à chaque changement ou une seule fois par jour. Le correspondant peut également demander à recevoir en pièce jointe la configuration de l'interface, la différence avec la configuration précédente ou les deux.

4.2 La structure actuelle du logiciel

Pour réaliser l'ensemble de ces fonctions, ConfIn est composé d'une base de données MySQL pour tous les paramètres (en dehors de l'identification des correspondants qui est séparée) et de différents programmes écrits en PERL pour l'interface Web et les divers traitements.

Les modules sont au nombre de quatre :

- **confingen** analyse les sauvegardes au format texte des routeurs et extrait les configurations des différentes interfaces en incluant la définition de l'interface, ses filtres, le routage statique, les « route map », ... Il se charge également de l'archivage des configurations et de la notification des changements aux correspondants en ayant fait la demande.
- **confintache** est le gestionnaire de tâches du logiciel. Certaines actions, telles que les demandes de recherches ou les mises à jour du filtrage, peuvent demander un certain temps. Pour éviter un dépassement du délai d'expiration dans le navigateur et une surcharge ponctuelle du serveur hébergeant la plate-forme, toutes les requêtes longues font l'objet de création d'une tâche. Les tâches sont traitées séquentiellement. Suivant la tâche, un ou plusieurs correspondants de l'interface à laquelle elle s'adresse, sont notifiés de sa réalisation par courrier électronique.
- **confinjour** est lancé automatiquement une fois par jour, comme son nom l'indique, et s'occupe principalement de l'analyse des violations des filtrages en générant des rapports synthétiques. Ceux-ci sont envoyés par courrier aux correspondants qui en ont fait la demande et archivés durant 60 jours.
- **confin** est le programme qui gère l'interface Web. Suivant le type de correspondant (simple, privilégié ou administrateur) il affiche différentes options.

4.3 La modification du filtrage

Cette fonction mérite un paragraphe à elle seule, car elle a apportée une grande souplesse aux correspondants, mais elle a aussi été la plus complexe à mettre en place et elle sera certainement celle qui évoluera le plus dans les futures versions du produit.

Jusqu'à sa mise en oeuvre, les filtres étaient gérés dans des fichiers texte. Ils étaient écrits en langage « routeur »., préfixés par le nom du filtre et un script permettait de les positionner sur le routeur avec un minimum de contrôle, à savoir que ce qui avait été envoyé avait été correctement reçu. La volonté d'ouvrir la modification aux correspondants ne permettait plus de conserver ce mode de fonctionnement. S'il y avait eu un accès simple, au travers d'une interface Web, à ces filtres, le risque d'erreurs (fautes de frappe, oubli d'un mot-clé, adresses IP n'étant pas dans les plages des réseaux de l'interface, etc.) aurait été trop important.

Avec l'aide d'une stagiaire de DESS[2], une étude des besoins et de la meilleure façon de les réaliser a été menée en tenant compte de l'existant.

Il y avait trois contraintes fortes vis à vis de l'existant :

- chaque règle ou groupe de règles d'un filtre était précédé d'un commentaire qui n'était pas visible sur le routeur, mais transmis aux correspondants ;
- un mécanisme de filtres temporaires existait (les filtres mis en place auxquels s'ajoutaient temporairement des filtres permettant la maintenance ponctuelle d'applications, du style de celles de gestion) et devait être conservé, voire simplifié ;
- pour palier à toute évolution n'étant pas encore prévue, l'équipe réseau devait pouvoir modifier simplement l'existant sans perturber ou rendre impossible l'utilisation de l'interface.

Après analyse, il a été décidé que :

- dans la page de modification, les correspondants verraient les filtres dans le langage natif du routeur ;
- dans un soucis de facilité pour tous, il faudrait que l'interface soit la plus proche possible du langage du routeur (des sessions de formation étant

[2]Diplôme d'Etudes Supérieures Scientifiques

programmées pour former les correspondants à ce langage). L'interface devrait toutefois permettre une saisie simplifiée et un minimum d'erreur (donc incluant des contrôles sur les adresses IP saisies, les protocoles et les ports spécifiés, en permettant des saisies par menu, etc.) ;

- la possibilité de commentaires serait reprise (et même incitée) pour permettre à plusieurs correspondants d'une même interface de suivre les changements ;
- pour faciliter l'écriture des filtres, des modèles contenant une ou plusieurs règles seraient disponibles ;
- les filtres temporaires seraient prédéfinis et facilement activables ;
- toute demande serait soumise à un administrateur pour validation ou refus des modifications, son rôle étant principalement de contrôler la cohérence avec la politique de sécurité des réseaux et le bon positionnement des règles (un pseudo-standard ayant été établi pour une bonne lisibilité) ;
- en cas de soucis sur une demande, l'administrateur devrait pouvoir facilement intervenir ;
- il ne devrait pas y avoir de modification de filtres venant se chevaucher, mais tout filtre non validé devrait pouvoir être modifiable.

Afin de mettre en oeuvre toutes ces décisions, les filtres ont été stockés dans le SGBD dans leur format brut. Lors d'une demande de modification pour une interface, les filtres de celle-ci sont recopiés dans une table des modifications (1). Le demandeur dispose d'une seconde table temporaire pour proposer ses changements durant une période donnée (2). Il peut apporter plusieurs changements et doit valider ensuite l'ensemble de sa demande ou l'annuler. S'il les valide, ceux-ci seront recopiés dans la table des modifications et soumises aux administrateurs. Tant que les administrateurs n'ont pas validé la demande, le mécanisme peut se répéter en partant de la table des modifications (donc en tenant compte des propositions précédentes).

Lors de l'étape de validation (3), l'administrateur peut, pour chaque proposition, rejeter ou modifier la demande. Lorsqu'il valide la demande, l'ensemble des règles est envoyé sur le routeur, la table des modifications devient la table de référence et les personnes, qui le désirent, sont informées du changement. Un contrôle de l'envoi est fait. S'il y a des différences entre l'envoi et ce qui a été mis en place sur le routeur, les administrateurs reçoivent une notification d'échec. Ils doivent alors modifier le filtre dans sa version « brute ». Cette option de modification des filtres « bruts » est toujours disponibles pour les administrateurs afin de leur permettre d'effectuer facilement et rapidement de nombreux changements.

Les différentes étapes décrites ci-dessus sont schématisées par la figure suivante.

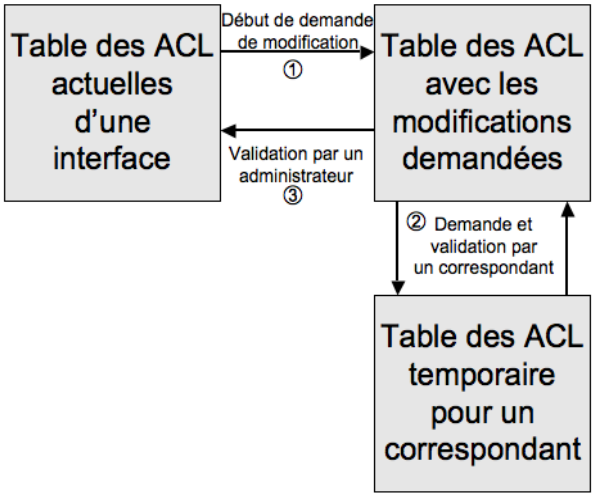

Figure 1: *mécanisme de modification des ACL*

Pour permettre de simplifier les demandes répétitives, les correspondants peuvent demander (par courriel) la création de modèles spécifiques aux interfaces, qu'ils gèrent, à l'équipe réseau du CIRIL. Celle-ci les intègre via un menu spécifique de ConfIn.

5 Limites et avantages

5.1 Les limites

Plusieurs types de limitation existent actuellement.

D'un coté, il y a des limites techniques. ConfIn a été développé pour répondre aux besoins de la plaque régionale Lothaire qui ne possède pour l'instant que des routeurs Cisco. Si des équipements d'autres constructeurs devaient être acquis, il serait nécessaire de réécrire une grande partie du logiciel notamment pour tout ce qui concerne le filtrage. De plus, les routeurs comportent d'innombrables options, certaines variant en fonction de la version du système : il est donc difficile d'offrir aux correspondants l'utilisation des dernières fonctionnalités (sauf à avoir un parc d'équipements identiques, ce qui n'est pas possible financièrement et ne se justifie pas). Enfin, nous rencontrons des soucis dans la récupération des logs des filtres[3] : il n'est actuellement plus possible de les obtenir toutes, ce qui pénalise la détection des problèmes de filtrage.

Il existe également des limites logicielles. Certaines peuvent faire l'objet d'évolution du produit, d'autres sont plus complexes à traiter. La principale concerne l'authentification des correspondants. ConfIn utilise actuellement un système d'informations (S.I.) propre au CIRIL (S.I. utilisé pour tous les services offerts). Il serait idéal que le produit puisse utiliser les S.I. des entités utilisatrices. Mais si les établissements universitaires ont

[3]Ce sujet a fait l'objet d'un débat sur la liste cisco-fr@cru.fr début 2007

tous un S.I., ce n'est pas le cas pour toutes les entités utilisatrices. Il est donc difficile de franchir cette étape.

5.2 Les avantages

L'avantage offert par les options de consultation et de recherche est de permettre aux correspondants d'accéder quand ils le désirent à diverses informations bien qu'ils ne puissent pas accéder au routeur et cela sans avoir besoin de passer par l'équipe réseau du CIRIL.

Au niveau de la possibilité de modifier les filtres, divers avantages sont apparus pour les utilisateurs de ConfIn (correspondants des entités et équipe réseau du CIRIL) :

- moins d'erreur dans les modifications des filtres ;
- pour les correspondants, une meilleure connaissance des possibilités de filtrage et un gain d'autonomie ;
- un meilleur suivi de ceux-ci avec plus de suppression de règles devenues inutiles ;
- un peu plus de travail pour les correspondants, mais une mise en place beaucoup plus rapide ;
- un gain de travail et de temps pour l'équipe réseau.

6 L'avenir du produit

Les fonctionnalités principales du produit satisfont actuellement la majorité des demandes des correspondants du réseau Lothaire. Ceci ne veut pas dire que le produit est figé.

Différentes évolutions sont déjà prévues :

- amélioration de l'ergonomie et du visuel de l'application Web ;
- de nouvelles possibilités dans l'écriture du filtrage
- des procédures de contrôle automatique des filtres mis en place (cohérence, doublons, filtres inutiles).

Les autres changements se feront au fur et à mesure des demandes des correspondants ou des décideurs des entités et en fonction des possibilités de leur intégration.

Une piste d'évolution est de proposer une coopération, dans un premier temps, avec d'autres établissements sur RENATER. Cette première expérience permettrait de voir si l'ouverture du produit est viable. Le produit a un module spécifique d'accès aux informations des correspondants et un fichier de paramètres, mais il reste pour l'instant très ciblé sur les besoins du réseau Lothaire. Quelques changements devront donc y être apportés pour correspondre aux fonctionnements d'autres réseaux.