netMET – Network's METrology, De nouveaux besoins, de nouvelles fonctionnalités

Sébastien MOROSI
Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault - 54500 VANDOEUVRE-LÈS-NANCY - FRANCE
Sebastien.Morosi@ciril.fr

Alexandre SIMON
Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault - 54500 VANDOEUVRE-LÈS-NANCY - FRANCE
Alexandre.Simon@ciril.fr

Résumé

La mise en œuvre de l'outil de métrologie netMET par un nombre important d'utilisateurs a permis de mettre en avant de nouveaux besoins et de nouvelles utilisations de la métrologie. Ces utilisateurs sont à la recherche d'informations toujours plus concises et synthétiques, mais nécessitent également de pouvoir obtenir un niveau de détail important à la demande. La métrologie propose des informations permettant d'assister les administrateurs dans leur mission de sécurité quotidienne. Les fonctionnalités proposées par netMET ont évolué naturellement dans ce sens, suivant les demandes importantes des utilisateurs.
Nous verrons également que les technologies sur lesquelles reposent la métrologie doivent évoluer et s'adapter aux nouveaux réseaux et débits. Le Sampled NetFlow et IPFIX sont certainement les évolutions les plus marquantes, du moins ce sont celles que netMET intègre et intégrera pour proposer une métrologie aussi souple que possible.

Mots clefs

Métrologie, sécurité, netMET, NetFlow Cisco, Sampled NetFlow, IPFIX

1 Introduction

Lancé en 1999 pour répondre aux besoins émergents en terme de métrologie, netMET est en passe de réussir son pari, comme en témoigne le nombre grandissant de sites en production. Grâce à ses récentes évolutions, netMET s'ouvre à de nouveaux utilisateurs toujours à la recherche d'informations à forte valeur ajoutée.

Rappelons que netMET est une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus. netMET est composé d'un collecteur de datagrammes NetFlow Cisco ainsi que d'un ensemble de programmes et scripts permettant l'exploitation de cette collecte. Cette solution a été présentée lors des dernières JRES 2001 par Alexandre SIMON[1]. Pour mémoire, NetFlow Cisco est une technologie d'accélération de routage propriétaire proposant l'export d'informations de métrologie. Cette technologie est embarquée dans les matériels (routeurs et switchs/routeurs) du constructeur ainsi que dans certains équipements d'autres constructeurs.

Cet outil à vocation métrologique s'est rapidement avéré auprès des utilisateurs comme un outil de sécurité. De la mise en évidence de trafics importants (entendez inhabituels) à la traçabilité de flux spécifiques, netMET permet de réaliser une sécurité à plusieurs niveaux. Les fonctionnalités de netMET se sont donc étoffées dans ce sens, les "rapports de scan" en sont un exemple.

L'accès et la diffusion de l'information sont également des domaines dans lesquels netMET a dû évoluer. Une interface plus intuitive a été mise en place de façon à en faciliter l'utilisation. De plus, la publication cohérente et structurée des données permet aux "administrateurs netMET" d'ouvrir les informations à leurs utilisateurs. Cette fonctionnalité ne vient pas sans soulever des problèmes d'authentification et de droits d'accès aux informations. La solution a donc évolué dans ce sens et propose aujourd'hui une authentification et des permissions basées sur le serveur web Apache qui permet de contrôler l'accès aux informations en fonction des utilisateurs et de leurs droits.

Les débits réseaux et les flux routés devenant de plus en plus conséquents, la technologie NetFlow "Full Flow" est devenue pénalisante. Les plateformes traitant les hauts débits du cœur de l'Internet ont dû adopter la technologie "Sampled NetFlow",

et le collecteur de netMET a été adapté de façon à la prendre en compte. netMET a été validé sur les plateformes Cisco et Juniper, et il a été démontré qu'il est apte à réaliser une métrologie cohérente à partir de "Sampled NetFlow". La métrologie sur RAP[5] en est un bon exemple.

Comme nous l'avons mentionné, netMET s'appuie sur la technologie propriétaire NetFlow Cisco embarquée dans les routeurs. Cette technologie a pour inconvénient majeur d'être liée à un constructeur et à des spécifications matérielles. Cette contrainte, qui a freiné dans une certaine mesure la métrologie basée sur l'export d'information de flux, va disparaître avec les récents travaux du groupe de travail IPFIX de l'IETF. netMET entend bien s'adapter aux nouveaux standards et proposer une métrologie sans contrainte.

Ces évolutions ont été accompagnées d'un nombre croissant d'utilisateurs. A ce jour, 88 utilisateurs se sont inscrits au projet et 22 sites utilisent officiellement netMET. Ces quelques chiffres tendent à montrer que la solution apporte une réponse aux besoins identifiés il y a quelques années, mais également que netMET présente une faculté d'adaptation suffisante pour intégrer de nouveaux besoins.

Tout au long de cet article, nous ferons référence aux réponses des utilisateurs netMET collectées suite à un audit de satisfaction mené à la rentrée universitaire 2002[2]. Cet audit de satisfaction était composé de deux questionnaires destinés aux utilisateurs d'une part et aux administrateurs d'autre part. Sur la forme, les personnes auditées ont répondu via un formulaire sur le site Web de netMET, quant au fond, le but de cet audit était pour nous de connaître l'utilisation qui est faite de netMET, les attentes des utilisateurs et les conditions de mises en œuvre de la solution.

2 Les évolutions de l'exploitation netMET

Les évolutions de netMET ont toujours eu pour objectif de répondre aux demandes les plus pressantes des utilisateurs. Nous verrons ensemble que les récentes évolutions traduisent des besoins importants en terme de sécurité. A la question *"Quelle est la principale utilisation que vous faites de netMET ?"*, 53.2 % des utilisateurs répondent *"la sécurité"* [2]. netMET devient donc plus qu'un outil de métrologie : il accompagne les administrateurs de réseaux dans leur mission quotidienne de sécurité.

En plus de consulter les informations proposées par netMET, les administrateurs ont également éprouvé le besoin de les mettre à disposition de leurs utilisateurs. Cela supposait une interface plus intuitive, plus ergonomique, mais également sécurisée. C'est pourquoi, toute l'arborescence de l'exploitation netMET a été pensée de façon à permettre une authentification/autorisation basée sur les fichiers de configuration du serveur web Apache.

2.1 La sécurité avec netMET

2.1.1 Comment avoir une approche sécurité avec netMET ?

Nous avons constaté que les informations présentées dans les rapports de netMET sont de plus en plus utilisées pour détecter les problèmes de sécurité dans le réseau. Lorsqu'une faille a été utilisée ou bien qu'une machine est soumise à des virus ou des attaques, cela se traduit quasiment toujours par un comportement atypique. Ce comportement peut être détecté grâce à netMET. Une fois qu'un problème potentiel est identifié, netMET peut également être utilisé pour affiner les recherches et valider les soupçons.

La première démarche est l'identification d'un problème potentiel. Pour cela, plusieurs rapports sont utiles :

- Les Tops généraux et locaux permettant de rapidement identifier une machine ayant un trafic bien plus élevé que de coutume. Les comportements anormaux se traduisent souvent par une augmentation significative de la quantité d'octets envoyée ou reçue.
- Les "statistiques vers le réseau fédérateur" permettent de savoir si l'évolution du trafic dans la journée est normale ou non. Un pic de trafic en pleine nuit peut être le signe d'une attaque.
- Enfin, les rapports de scans permettent de déterminer si une machine, un sous réseau, a été victime ou est à l'origine d'attaque.

La deuxième démarche est une étude plus précise du problème. Cette étude peut-être menée en utilisant conjointement les Top N locaux et la section "détail" dont nous présentons les fonctionnalités ci-après.

L'approche de la sécurité à l'aide de netMET se fait donc à deux niveaux : la recherche des problèmes potentiels sur l'ensemble du réseau, et l'investigation détaillée pour une machine ou un organisme particulier.

2.1.2 Identification de flux

La sécurité a pris une place prépondérante dans l'utilisation de netMET. Le Top N s'est rapidement avéré un outil utile pour détecter des comportements "anormaux". Un *trafic atypique* en quantité est souvent le résultat d'un *comportement atypique*. Une fois une machine détectée, isolée, les questions des utilisateurs netMET étaient invariablement les mêmes : quel type de trafic était-ce ? Avec qui ? Quand a-t-il eu lieu ?

Pour répondre à ces questions, nous avons mis à disposition pour chaque machine des Top N journaliers un lien vers une nouvelle page web proposant une vue synthétique de son activité. La Figure 1 présente une vue d'un Top 10 proposant des liens vers la section "*détails*" de netMET.

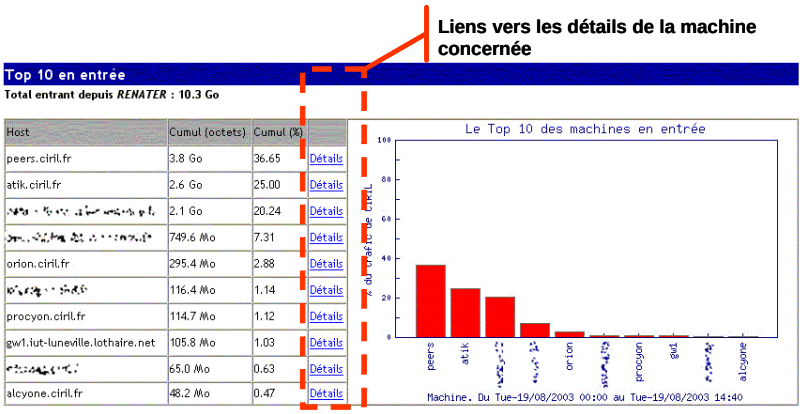

Figure 1 – Lien "Détails"

L'idée de cette page web "Détails" est de répondre aux trois questions énoncées ci-dessus, elle contient donc trois graphiques :

- La répartition temporelle du trafic en entrée et en sortie, permettant de déterminer les horaires du problème suspecté,
- la répartition par service/protocole en entrée et en sortie, permettant souvent de valider si oui on non nous faisons face à un problème,
- la répartition par source/destination, permettant le cas échéant de déterminer quelle est la source du problème.

Une capture de page "Détails" est donnée par la Figure 2. Elle met en évidence les trois graphiques fournis par la solution et le niveau de détail alors disponible.

L'interprétation de ces graphiques nous permet de déterminer aisément que le trafic envoyé par cette machine était relativement constant entre minuit et 15h00, et qu'il était généré à 60% par un logiciel de partage de fichiers de type "peer-to-peer" (le port 1214/tcp étant généralement utilisé par KaZaa). Dans l'exemple de la Figure 2, la liste des machines de destination n'est pas très significative, puisque ce type de trafic a généralement un nombre élevé de destinataires. Par contre il met en évidence un détail que nous supposions : toutes les destinataires sont des "particuliers" ayant un abonnement chez un fournisseur Internet.

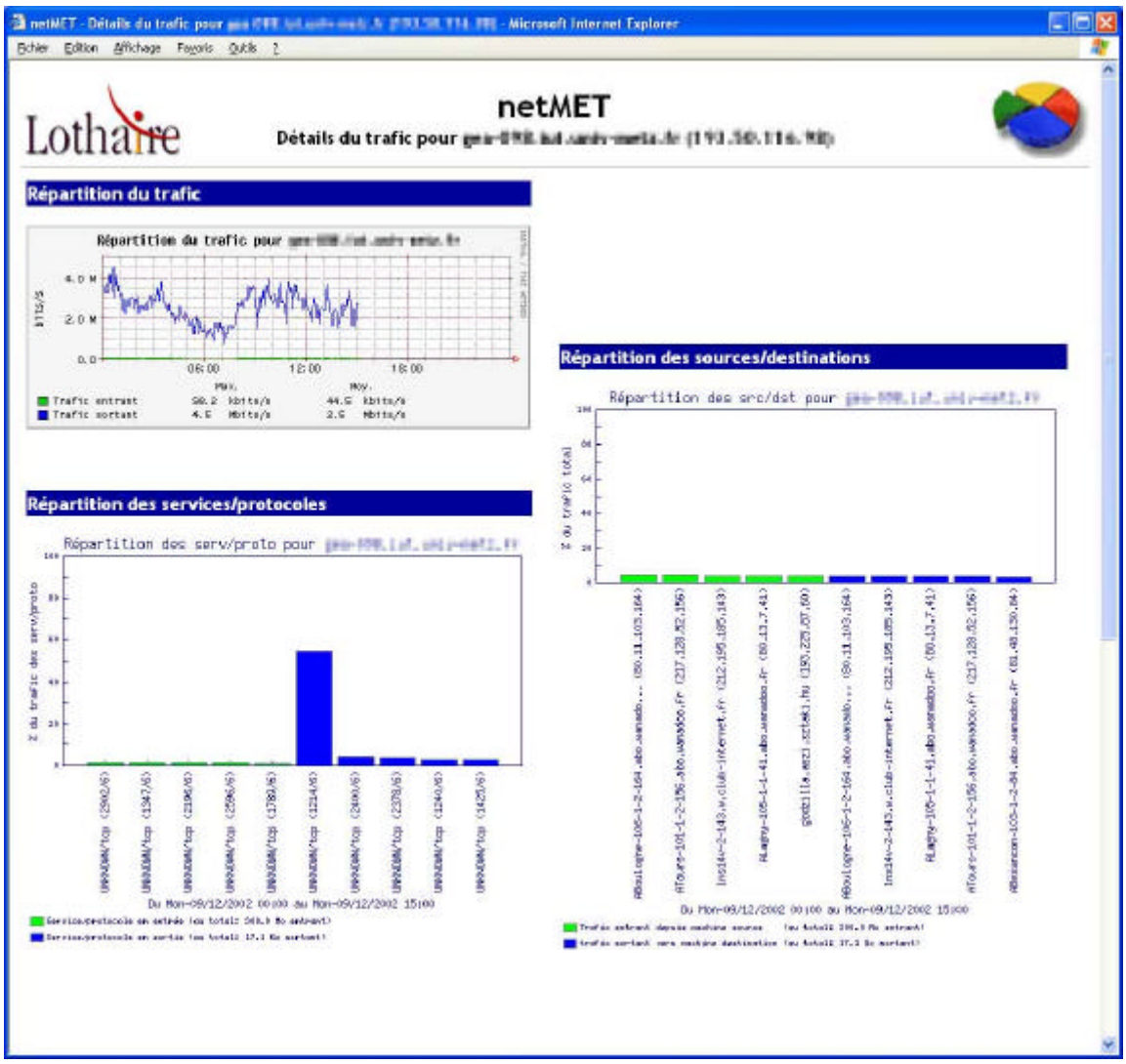

Figure 2 – La page "Détails"

Les trois graphiques de cette page permettent de répondre dans la majorité des cas à la question "*ce trafic était-il légitime ?*". Mais parfois, il est nécessaire de pouvoir tracer l'évolution individuelle des protocoles les plus utilisés pour trouver une réponse.
La dernière évolution en terme de métrologie a de ce fait concerné la répartition temporelle des protocoles. En effet, netMET était capable de vous dire que 50 % du trafic de la journée d'une machine était de type *http*, mais il ne vous disait pas quand avait eu lieu ce trafic spécifique. Cette nouvelle page Web (voir Figure 3) présente l'évolution temporelle des services/protocoles et permet de tracer encore plus finement les services utilisés.

Cette page présente l'évolution des cinq services les plus importants sur la journée et rappelle en filigrane le trafic de la machine concernée. Cette fonctionnalité sera mise à disposition dans la version 2.5 de l'exploitation de netMET, prévue avant la fin 2003. La Figure 3 est un exemple qui illustre bien la répartition des protocoles dans le temps. Il est possible de facilement identifier un pic de trafic http à 22h00 avec ce type de graphique, alors qu'avec la seule représentation globale (illustrée en gris) cela est impossible.

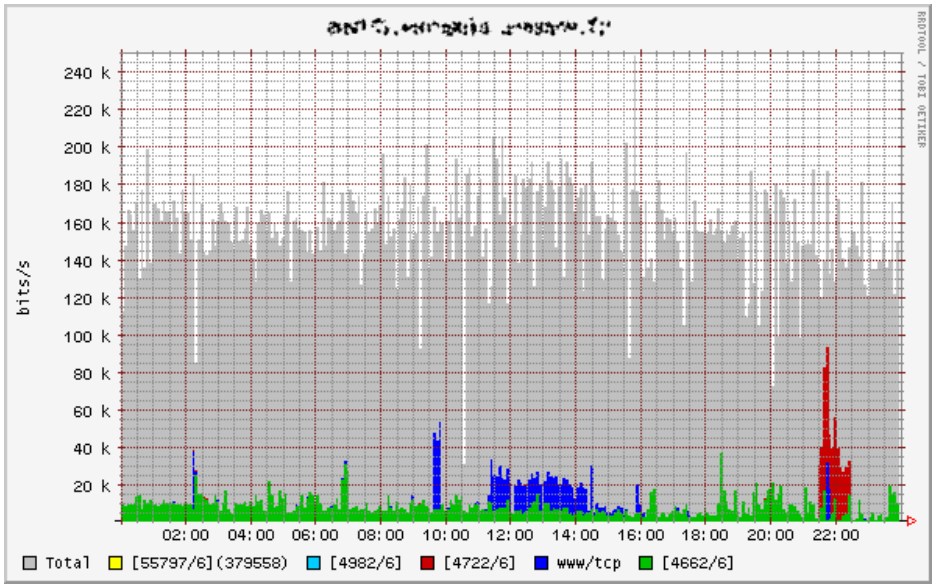

Figure 3 - Evolution temporelle des services/protocoles

Les deux pages de détails ajoutées à l'exploitation de netMET assistent les administrateurs dans leur mission de sécurité quotidienne. Ces pages leur permettent de "creuser" un problème lorsqu'il est détecté, la détection ayant été réalisée sur la quantité d'octets observée. Mais en évoquant la détection de problèmes de sécurité, nous avons soulevé un second enjeu : détecter les trafics anormaux sur d'autres critères que le volume d'octets.

L'autre solution retenue à ce jour pour identifier un trafic atypique en terme de sécurité, consiste à analyser les scans subis ainsi que les scans réalisés par notre réseau.

2.1.3 Qu'est-ce que le SCAN ?

Les réseaux de grande envergure offrant des débits importants sont régulièrement victimes de scans massifs. Le scan est une technique simple permettant à une personne malveillante de détecter sur un réseau les machines potentiellement vulnérables à des attaques plus élaborées. Plus le débit vers l'Internet est élevé, plus le nombre d'adresses IP gérées est important, et donc plus les scans sont volumineux. Les scans peuvent également mettre en évidence une machine infectée par un virus ou une machine utilisée comme rebond.

netMET disposant de toutes les informations nécessaires pour détecter ces scans, l'exploitation a rapidement été complétée par des scripts de détections de scan. Ces scripts permettent de fournir la liste des *scans en hauteur et en largeur* :

- il y a scan en "hauteur" lorsqu'une machine communique avec plus de n machines d'un même réseau.
- il y a scan en "largeur" lorsqu'une machine communique avec une seule machine destination mais sur un grand nombre de services.

Nous avons remanié les rapports de scan existants en essayant de cibler la problématique qu'ils avaient soulevée :

- leur volume : malgré la quantité d'information à présenter, ils doivent rester concis et simples,
- donner à chaque utilisateur un rapport les concernant,
- faire en sorte que ces rapports soient réellement exploitables.

2.1.4 Améliorations apportées aux rapports de SCAN

Le problème de ces rapports venait essentiellement de leur taille et du manque de synthèse. Un vieil adage nous avait pourtant prévenu : "trop d'information tue l'information". Ce besoin ressort très clairement dans les résultats au questionnaire des utilisateurs netMET [2]. A la question *"Que proposeriez-vous comme évolution et/ou nouvelles fonctionnalités ?"* les utilisateurs répondent :

- *"Si possible les rapports/scans juste pour les réseaux du site concerné"*
- *"Si possible une analyse scan en temps réel et un rapport de scan plus condensé"*

- *"Un rapport de scan réellement utilisable. La page actuelle est beaucoup trop longue ce qui la rend difficilement lisible. Ce qu'il serait bien, ça serait de classer les scans par organisme, voire par établissement. (et éventuellement classes réseau). "*
- …

Nous avons donc totalement remanié les rapports de scan pour les présenter de façon synthétique et exploitable. Tout d'abord, un résumé est maintenant disponible. Un exemple de résumé est donné par la Figure 4.
Il fournit les informations suivantes :

- le nombre de scans en hauteur et en largeur *vers votre* organisme : le nombre de scan ainsi que le nombre d'adresses IP scannées sont de bons indicateurs des attaques subies et de leur importance. Des valeurs numériques permettent en plus de comparer facilement les rapports entre eux. Le détail du rapport de scan permettra de déterminer quelles sont les machines de l'Internet qui ont attaqué notre réseau, et dans quelle mesure.

- le nombre de scan en hauteur et en largeur *depuis votre organisme*, avec en plus les adresses IP (et noms) des machines ayant réalisé ces scans. Cette liste permet de repérer efficacement des machines ayant un comportement suspect et d'agir en conséquence. Ce type d'information nous a permis par exemple de détecter très vite les machines infectées par des vers. Il faut toutefois faire attention car certaines machines peuvent avoir une activité tout à fait normale, mais s'apparentant à du scan (les serveurs DNS ou DHCP par exemple).

- La dernière partie du résumé vous prévient en cas de *spoofing* de vos adresses IP. Le spoofing est une technique qui consiste à forger l'adresse source d'un paquet IP pour faire croire que ce paquet provient d'une machine de votre réseau. Cela peut s'apparenter à de l'usurpation d'identité, et netMET détecte les éventuels paquets en provenance de l'Internet essayant d'utiliser des adresses de vos sous-réseaux.

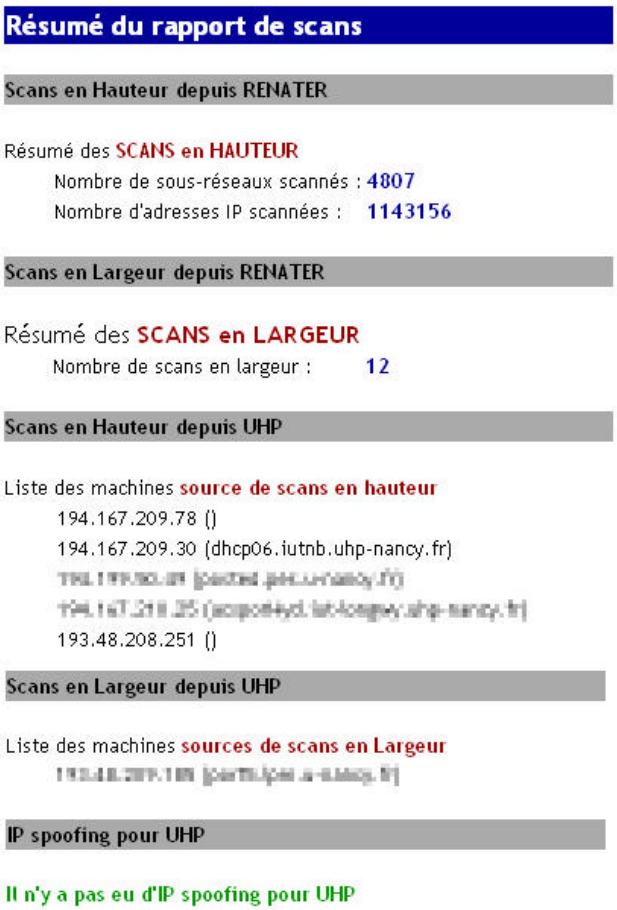

Figure 4 – Résumé de rapport de SCAN

La deuxième amélioration consistait à fournir des *rapports par organisme* contenant uniquement les scans des réseaux (ou sous-réseaux) le concernant. Cette amélioration a été mise en place en même temps que le résumé. Cela permet également de mettre à disposition des utilisateurs ou administrateurs d'un organisme le rapport de scan le concernant.

Mais cette amélioration des rapports de scan ne serait pas vraiment finalisée si le résultat de ces rapports n'est pas exploité comme il se doit. Quelle est la finalité d'un outil de détection de scan ?
La réflexion que nous avons menée nous a apporté deux orientations :
- protéger son réseau,
- faire "remonter" l'attaque aux autorités de façon à limiter ces agissements.

Pour la première orientation, netMET ne peut mettre en évidence que les risques réels, et c'est à vous de vous protéger en conséquence. Par contre, pour ce qui est de la remontée des informations vers les autorités compétentes, netMET pouvait vous aider. C'est pourquoi nous avons travaillé avec le CERT Renater de façon à générer automatiquement un rapport de scan au format texte. Ce rapport est pré-formaté, directement intégrable par les automates des bases du CERT.

2.2 Les évolutions de l'interface

Les résultats de l'exploitation de netMET sont consultables exclusivement via l'interface WEB. Cette interface WEB se devait d'être la plus intuitive et ergonomique possible. L'idée était donc la suivante : repenser l'interface netMET de façon à rendre toutes les informations accessibles en "1 clic".

2.2.1 Entête et charte graphique

L'interface a été totalement modifiée, le résultat étant représenté par la Figure 5. Toute page netMET se découpe en trois grandes sections :

- Le titre contenant toujours la période (mois, jour, année) et le type des statistiques affiché (Top, métrologie détaillée…),
- la barre de navigation netMET,
- les statistiques.

Un détail, peut-être plus esthétique que pratique, qui mérite d'être signalé : toutes les pages de netMET respectent à présent la même charte graphique.

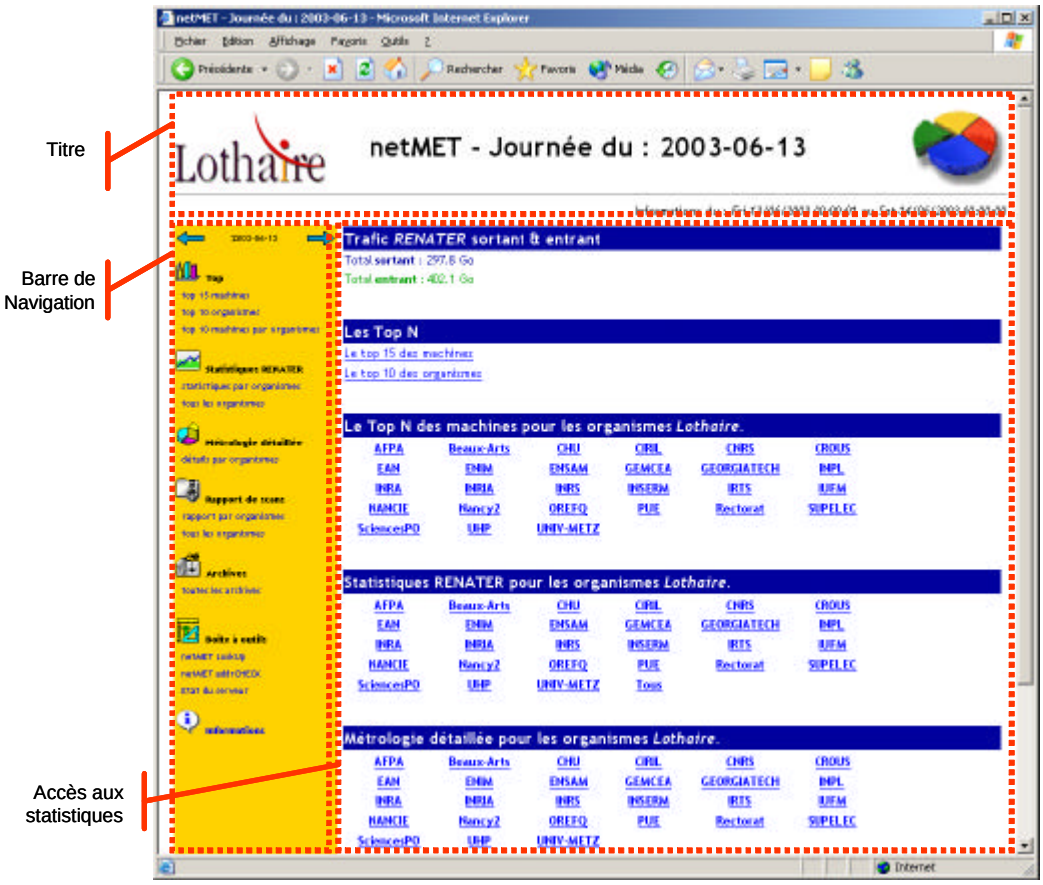

Figure 5 - Nouvelle interface netMET : page d'accueil

L'entête de toute page contient le type de statistiques affiché, l'organisme concerné, la périodicité (jour, semaine, mois) et la période concernée.

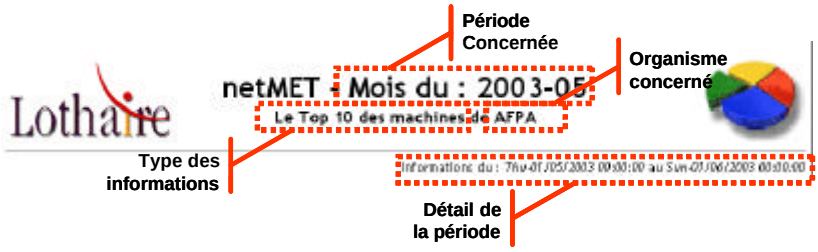

Figure 6 - Entête de page netMET

2.2.2 Barre de navigation

La barre de navigation représente certainement la plus grande avancée de l'interface netMET. Cette barre de navigation permet à l'utilisateur d'accéder à toutes les statistiques pour la période concernée, ainsi qu'aux outils et archives de netMET. Cette barre contient plusieurs parties pouvant être regroupées comme suit.

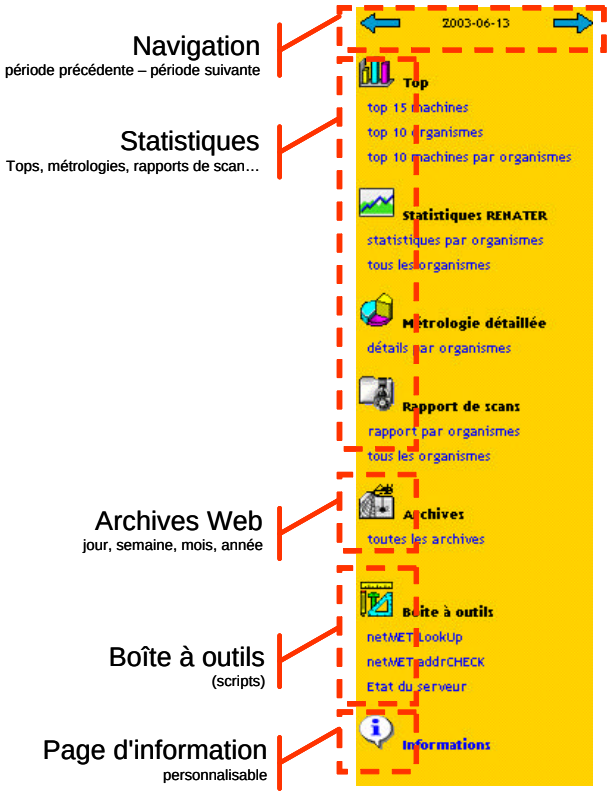

Figure 7 - Barre de navigation

Une section "**Navigation**" permet de passer à la période précédente ou suivante en cliquant sur les flèches. Entendez par là que si vous consultez des pages avec une périodicité journalière, en utilisant ces flèches, vous allez passez automatiquement à la journée suivante ou bien précédente. Si la périodicité est hebdomadaire, vous allez alors naviguer de semaine en semaine.

La section "**Statistiques**" permet d'accéder directement à toutes les informations concernant la période en cours :

- Les Tops,
- les statistiques vers/depuis le réseau fédérateur (Renater par exemple),
- la métrologie détaillée,
- et les rapports de scans.

La section "**archives**" donne accès aux archives journalières, hebdomadaires et mensuelles.

La section "**boîte à outils**" propose des liens vers les trois outils bien connus :

- netMET lookup : le moteur de recherche de netMET
- netMET addrCHECK, permettant de retrouver à quel organisme appartient une adresse IP
- et enfin l'état du serveur pour connaître la charge du serveur, les processus actifs et l'état des fichiers de log.

La dernière section ajoutée est la page "**Informations**". Cette page statique pouvant peut-être personnalisée selon vos besoins.

2.2.3 Menu contextuel

Pour rendre les informations des différents organismes directement accessibles depuis la barre de navigation, nous avons mis en place un menu contextuel (ou "pop up") s'affichant lorsque la souris passe au dessus des liens "Top N par organisme", "Top N machines par organisme", "statistiques par organismes", "détails par organisme". Nous avons préféré l'utilisation d'un menu contextuel à une sous-liste par catégorie qui aurait rendu la barre de navigation trop "longue" et peu pratique.

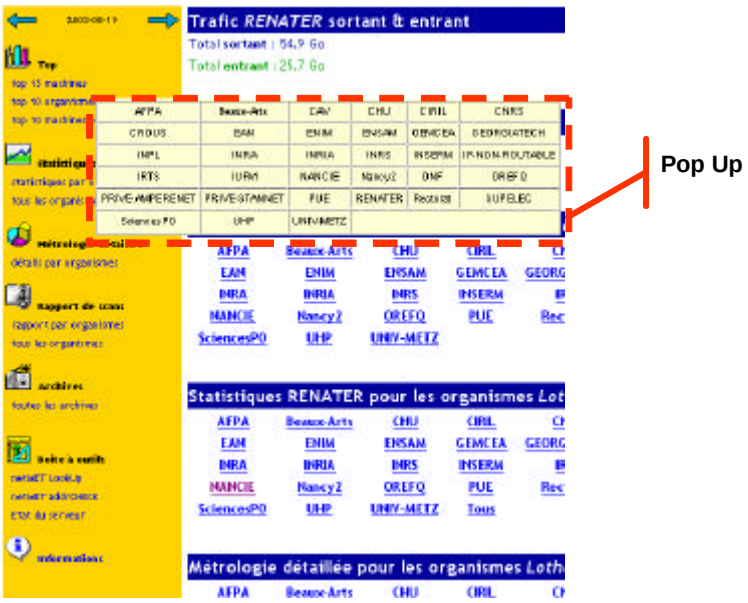

Figure 8 - Menu contextuel

Les liens de ce menu mènent directement à la catégorie de l'organisme sélectionné. C'est la conjonction de ce menu et de la barre de navigation qui permet d'accéder à toutes les informations en "1 clic".

2.3 Authentification et autorisation

Les administrateurs de netMET ont rapidement été confrontés au problème de la mise à disposition des informations issues de l'exploitation. Ils voulaient (ou devaient) donner aux utilisateurs un accès aux pages les concernant mais en revanche, l'utilisateur d'un organisme ne devait pas avoir connaissance des informations concernant un autre organisme.

L'idée fut donc d'associer plusieurs concepts :

- un espace de nommage complet et cohérent pour stocker tous les fichiers générés par l'exploitation. Le nouvel espace de nommage permet de retrouver dans l'URL de chaque page le nom de l'organisme concerné.
- utiliser l'authentification d'Apache en créant des utilisateurs et des groupes, chaque groupe correspondant à un organisme netMET,
- utiliser les autorisations Apache (via la clause "Location Match") pour autoriser chaque groupe à n'accéder qu'aux pages de son organisme.

La combinaison de ces trois éléments permet aujourd'hui à netMET de proposer une mise à disposition sécurisée des informations. Elle accorde aux administrateurs la possibilité d'ouvrir leur plateforme aux utilisateurs.

Plus d'informations peuvent être obtenues sur la façon de réaliser cette authentification en ce reportant au document "Exploiter & intégrer netMET" [3].

2.4 Conclusion

Nous avons vu que les informations extraites des fichiers de collecte de netMET sont aujourd'hui en constante évolution. Les besoins initiaux en terme de métrologie sont aujourd'hui couverts, et ne devraient plus évoluer de façon importante. Par contre, il reste encore beaucoup d'informations à retirer de ces fichiers pour en exploiter pleinement les possibilités en terme de sécurité. Les demandes des utilisateurs netMET sont quasiment toutes orientées dans cette direction.

L'exploitation de netMET a donc encore de nombreuses évolutions à venir, mais ne doit pas occulter les nouveautés concernant l'acquisition des données : la collecte. Cette collecte, même si elle n'a pas fondamentalement changé en quelques années, a été améliorée en permanence pour prendre en compte les différentes versions et évolutions de NetFlow.

3 Sampled NetFlow

3.1 Pourquoi le "Sampled NetFlow" ?

Il existe deux approches de mesure des flux en interne dans les matériels :

- l'approche "Full Flow" qui consiste à comptabiliser tous les paquets des flux qui transitent dans le matériel
- et l'approche "Sampled Flow" qui consiste à comptabiliser les paquets à un certain taux : ne compter qu'un paquet sur 10 par exemple.

L'approche "Sampled NetFlow" se justifie par plusieurs points :

- certains exploitants de réseaux ne s'intéressent pas forcément à une comptabilité au plus juste et l'approximation du trafic peut les satisfaire,
- les débits sur les artères fédératrices sont de plus en plus élevés (1Gb/s, 2.5Gb/s … 10Gb/s!) et ces débits ne permettent plus de faire de la comptabilité au flow près. En effet, le processus de comptabilité dans ce cas devient beaucoup trop gourmand et nécessite des temps de traitement qui nuiraient aux performances du matériel,
- et enfin la collecte d'informations "Full Flow" peut quelques fois être très contraignante car il n'est pas toujours facile de concevoir un collecteur capable de traiter et stocker des exportations "Full Flow" à débits très élevés… dans ce cas, l'approche peut être de soulager le collecteur en passant en "Sampled Flow".

Le "Sampled NetFlow" est un véritable challenge pour les constructeurs s'ils veulent proposer des solutions de métrologie intégrées dans les matériels de cœur, là où se trouvent les très Hauts Débits. A ce jour, Cisco avec son format NetFlow v9 et Juniper (compatibilité formats v1 et v5) proposent du "Sampled NetFlow".

3.2 netMET et "Sampled NetFlow"

Il était très important pour netMET de rendre le collecteur et l'exploitation compatibles avec l'approche "Sampled NetFlow". C'est au cours d'une étude de métrologie sur le réseau RAP [5] que l'équipe netMET a eu l'occasion de valider sa solution. Rappelons quelques points techniques :

- RAP est connecté sur Renater par un routeur de tête type Juniper M10,
- RAP souhaitait effectuer une métrologie fine entre son réseau et le réseau fédérateur Renater.

Dans ce cadre, l'équipe RAP a sollicité le CIRIL pour avoir une expertise sur la mise en place de la solution netMET sur leur réseau, et pour connaître les avantages et inconvénients d'un tel déploiement. En effet, il fallait valider les points suivants :

- quel est l'impact de l'activation du NetFlow sur le M10 ?
- le collecteur netMET saura-t-il décoder des NetFlow Juniper ?
- comment l'exploitation fera-t-elle pour réajuster les erreurs induites par l'échantillonnage ?

Pour répondre à toutes ces questions, le CIRIL a convenu d'un prêt de routeur Juniper M5 avec la société Juniper pour mettre en place une maquette d'expérimentation sur le réseau Lothaire.

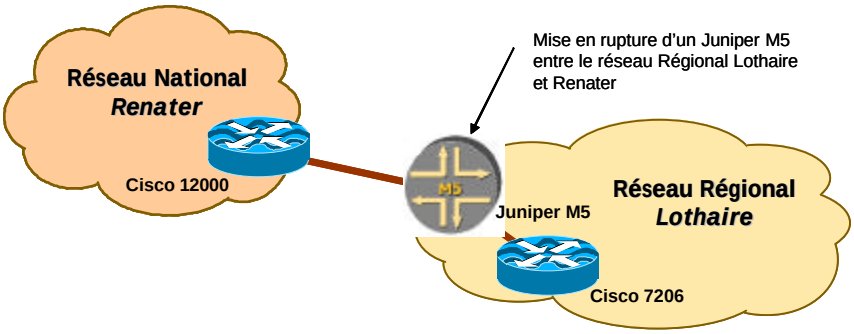

Figure 9 - Expérimention "Sampled NetFlow Juniper" sur Lothaire

La Figure 9 illustre la mise en place du routeur Juniper M5 sur le réseau Lothaire. Nous n'expliciterons pas ici tous les détails techniques de sa mise en place, mais nous insistons sur l'intérêt de mettre le M5 en rupture sur le réseau avec la présence d'un Cisco 7206 en amont. En effet, au delà de la validation du format d'exportation Juniper, il fallait valider et prouver que les informations collectées en "Sampled NetFlow" proposeraient les mêmes résultats que des informations collectées en "Full Flow". Ainsi comme l'illustre la Figure 10, nous avons mis en place deux serveurs netMET en parallèle, collectant du "Sampled NetFlow" en provenance du Juniper et du "Full Flow" en provenance du Cisco 7206.

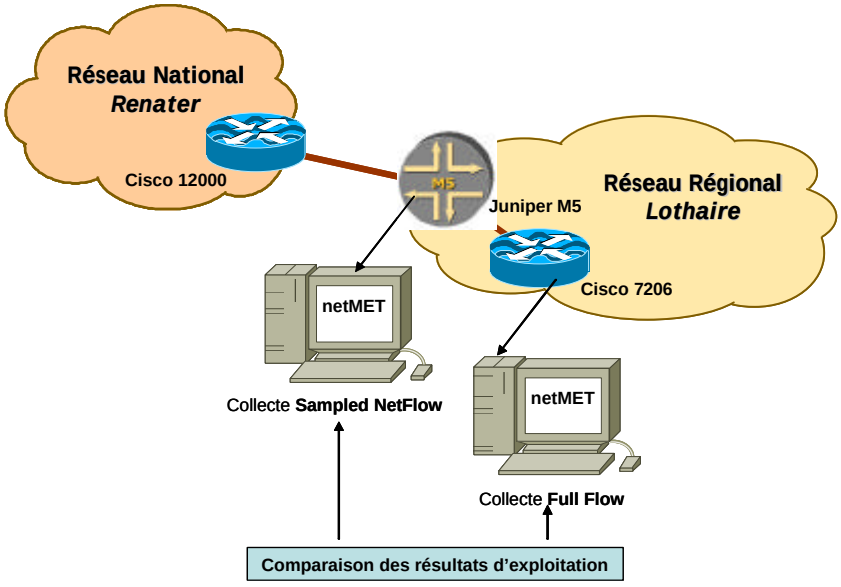

Figure 10 - Comparaison "Sampled NetFlow" et "Full Flow"

Dans cette architecture, il était donc très aisé pour nous de réaliser des comparaisons de résultats entre les deux approches et éventuellement de modifier le modèle de réajustement des valeurs dans le cas du "Sampled NetFlow".

3.3 Conclusion de l'étude et compatibilité "Sampled NetFlow"

La validation de l'impact d'activation du NetFlow sur un Juniper et la validation de la compatibilité du collecteur netMET par rapport aux exportations Juniper n'ont pas posé de problème majeur. Par contre, c'est la validation du modèle de réajustement des valeurs échantillonnées qui a pris le plus de temps. En effet, les flux transitant dans le Juniper sont échantillonnés puis comptabilisés : il manque donc des informations… et pour retrouver les quantités et débits réels, il faut

donc réajuster les résultats de la collecte. Ainsi, après la mise en place de plusieurs modèles de réévaluation et de comparaisons systématiques avec le "Full Flow", il s'est avéré qu'une simple multiplication des résultats collectés par le taux d'échantillonnage (si celui-ci est activé à 1/10 alors on multiple les compteurs de collecte par 10) suffit à réajuster les compteurs et induire une erreur tout à fait négligeable. L'erreur induite variait alors entre 0.09% et 0.17%, ce qui, sur les résultats synthétisés sur l'exploitation (HTML et images) passe totalement inaperçu. Ces résultats proviennent des observations de comparaison des deux approches et ne peuvent pas remplacer une étude théorique de ce problème. Il nous semblait toutefois très intéressant d'aborder ce problème d'une manière pratique puis théorique (l'auteur laissera le soin à des spécialistes du sujet de valider cette approche !).

Seul le collecteur netMET a été modifié pour prendre en compte le "Sampled NetFlow" et sera disponible en standard dans la distribution d'une prochaine version. En attendant, l'équipe reste bien entendu disponible pour fournir ce collecteur spécifique à ceux qui le souhaiteraient avant son officialisation.

Les résultats de cette étude ont bien entendu été remontés à l'équipe RAP, qui a immédiatement choisi netMET comme solution de métrologie et mis en production ce service à partir de Décembre 2002 / Janvier 2003. L'exploitation à long terme et la consultation des résultats a également permis de valider la compatibilité de la solution netMET dans un contexte "Sampled NetFlow".

A noter tout de même que l'approche "Sampled NetFlow" peut poser des problèmes en terme de détection de problème de sécurité, car en effet comment peut-on faire pour détecter des scans alors que l'on n'a plus tous les flows ? Non pas que cela soit impossible, mais il faut essayer de réajuster les seuils de détection pour que les rapports de sécurité restent cohérents. Par contre, la solution reste tout à fait valide concernant les détections à base de trafics et de quantités atypiques.

4 IPFIX

netMET est une solution bien souvent associée à un constructeur : Cisco. Même si d'autres industriels proposent une implémentation de NetFlow, et que Cisco est assez largement implanté dans le monde du routage, la métrologie via netMET reste tout de même limitée à un groupe d'utilisateurs. Cette restriction étant intrinsèque à l'implémentation de NetFlow - un mécanisme Cisco – la définition de nouveaux standards pourrait bien lever cette contrainte.

L'Internet Engineering Task Force (IETF) standardise actuellement un format d'export des informations de routage basé sur les flux de trafic. Le standard proposé, IP Flow Information Export (IPFIX) [6], sera "multi constructeur".

Les principaux objectifs de ce groupe de l'IETF sont de :

- définir ce qu'est un flux IP,
- suporter IPv4, IPv6, le multicast,
- prendre en compte l'échantillonnage",
- sécuriser l'export des informations de flux,
- définir le format d'export des informations,
- rendre le mécanisme d'export fiable.

L'IETF a choisi NetFlow version 9 comme base d'IPFIX.
Un flux IP sera identifié par :

- l'adresse IP source,
- l'adresse IP destination,
- le port source,
- le port destination,
- le protocole de niveau trois,
- les champs "type of service",
- l'interface logique d'entrée.

Toutes les informations nécessaires au collecteur netMET seront disponibles, et netMET devrait très logiquement intégrer le standard qui résultera de ce groupe de travail. netMET pourra bientôt proposer une métrologie sans contrainte !

L'équipe de netMET travaille actuellement avec un membre du groupe de travail de l'IPFIX sur le test des nouveaux formats, et participe à la validation du modèle d'échantillonnage.

5 Nouveaux utilisateurs

Le nombre des utilisateurs de netMET n'a cessé de croître depuis sa création en 1999. Le graphique Figure 11 illustre la croissance des utilisateurs de netMET : au cours de la dernière année, netMET a doublé le nombre de ces utilisateurs.

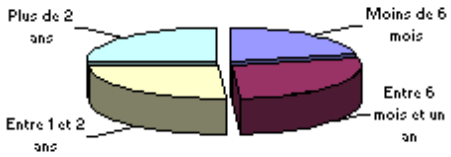

Figure 11 - évolution du nombre de sites netMET

Il est également intéressant de savoir que le problème auquel répond netMET est un problème rencontré par de nombreux gestionnaires de réseau. Plus le nombre et la diversité des utilisateurs netMET seront importants, plus le retour que nous pourrons avoir sera riche et intéressant. A ce jour, 22 sites netMET sont officiellement en production, principalement dans le domaine universitaire. La carte de France de la Figure 12 représente la répartition sur le territoire français des sites netMET.

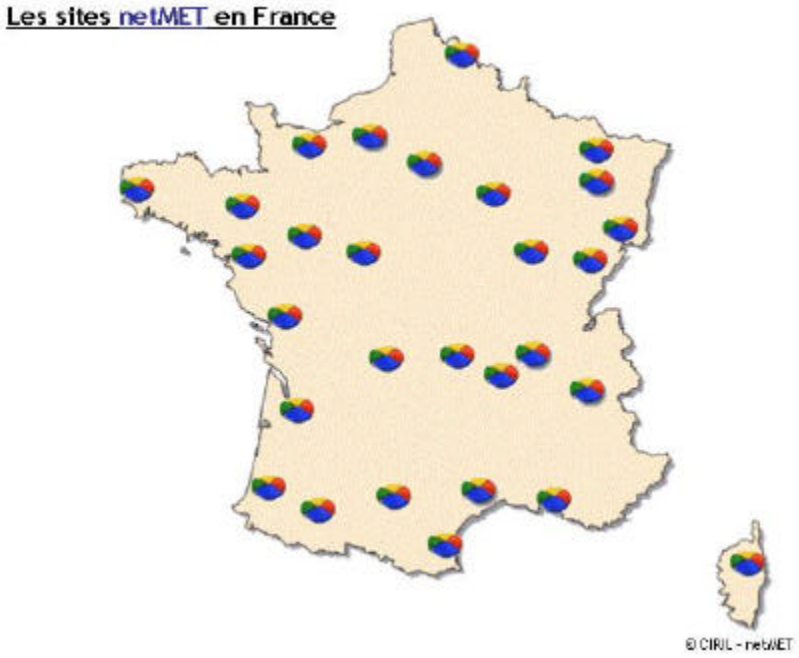

Figure 12 - La carte de France "netMET "

Le but de cette carte est de montrer que l'évolution des fonctionnalités de netMET s'est accompagnée d'une augmentation importante du nombre de ses utilisateurs ; ce qui tente également à prouver que les questions ciblées par netMET touchent une partie significative des gestionnaires de réseaux.

6 Conclusion

Les fonctionnalités mises en place récemment ne couvrent pas encore tous les besoins énoncés par les utilisateurs. Le récent audit de satisfaction fait émerger une demande grandissante : *"Avoir un aperçu global des problèmes"* [2]. netMET restera un outil de métrologie : il n'est pas prévu d'en faire un tableau de bord. Par contre, il est envisageable d'étoffer la détection de problèmes (comme les rapports de scan) et de donner à posteriori un résumé des évènements notables observés.

A la question *"Que proposeriez vous comme évolution et/ou nouvelles fonctionnalité ?"* les utilisateurs nous ont répondu :

- *"Amélioration de la navigation entre les pages : passer de jour en jour sans revenir au sommaire"*
- *"Si possible les rapports/scans juste pour les réseaux du site concerné"*
- *"Avoir les src/dst dans rapport détaillé d'une machine"*

A ces questions (et quelques autres) nous avons apporté des réponses et parfois des solutions. Par contre, les utilisateurs nous ont également répondu :

- *"J'aimerais avoir le Top 10 des ports les plus scannés de mon réseau"*
- *"Aperçu global des problèmes : si un trafic "bizarre" apparaît"*

Cela nous montre que nous avons encore beaucoup d'informations à extraire des fichiers de collecte de netMET. Les prochaines évolutions devraient donc principalement concerner l'exploitation et être centrées sur la sécurité. Mais n'oublions pas que les standards se mettant en place nous ouvrent de nouveaux horizons, et une fois encore, netMET ne manquera pas le tournant.

Références

[1] Alexandre SIMON, netMET - Network's METrology Une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus. Dans *Actes du congrès JRES2001,* pages 305-317 - Lyon, Décembre 2001

[2] Alexandre SIMON, Audit de satisfaction de la solution netMET - Novembre 2002 - Janvier 2003
http://www.netmet-solutions.org/documentation/wp/netMET-resultats-audit2003.pdf

[3] Sébastien MOROSI, Formations CiREN : Exploiter et intégrer netMET – Montpellier, Mars 2003
http://www.netmet-solutions.org/WWW/documentation/wp/netMET-20030324_CiRen-explt.pdf

[4] Alexandre SIMON, Formations CiREN : Mise en œuvre pratique de netMET – Montpellier, Mars 2003
http://www.netmet-solutions.org/WWW/documentation/wp/netMET-20030324_CiRen-general.pdf

[5] Réseau académique Parisien
http://www.rap.prd.fr

[6] IP Flow Information Export (IPFIX)
http://www.ietf.org/html.charters/ipfix-charter.html