



netMET Network's METrology



De nouveaux besoins,
de nouvelles fonctionnalités

Lille, 20 novembre 2003

netMET
Sébastien MOROSI
Alexandre SIMON

*netmet@netmet-solutions.org
Sebastien.Morosi@ciril.fr
Alexandre.Simon@ciril.fr*

- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : Sampled NetFlow
- Standardisation NetFlow : IPFIX
- Conclusion

De nouveaux besoins : les utilisateurs

- Audit netMET en décembre 2002
- Question : "*Que proposeriez vous comme évolution et/ou nouvelles fonctionnalités ?*"
 - Améliorer la navigation sur les pages html générées
 - Avoir le TOP 10 des ports les plus scannés de mon réseau
 - Avoir un rapport de scan réellement utilisable
 - Avoir les src/dst dans le rapport détaillé d'une machine
 - (...)

- Evolutions de NetFlow Cisco
 - version 9
 - échantillonnage de flux : Sampled NetFlow
 - IPv6

- Standardisation
 - IPFIX
 - support de NetFlow par de nouveaux constructeurs

- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : Sampled NetFlow
- Standardisation NetFlow : IPFIX
- Conclusion

- Passage à la version 2 de l'exploitation : avril 2003
- Mise à jour de l'exploitation de netMET
 - nouvelle interface
 - nouvelles fonctionnalités
 - diffusion de l'information

Une nouvelle exploitation : interface

- Version 1 axée
 - sur la faisabilité
 - sur la mise à disposition de contenu
 - pas sur le design
 - pas sur la convivialité

- Nouvelle interface : version 2
 - charte graphique homogénéisée et plus agréable
 - navigation améliorée
 - réponses aux besoins exprimés par les utilisateurs

Une nouvelle exploitation : interface

- Charte graphique homogène
- Trois sections
 - titre : type des données et période
 - barre de navigation
 - les données de la page

The screenshot shows the netMET web interface in Microsoft Internet Explorer. The browser title is "netMET - Journée du : 2003-06-13". The page features a header with the "Lothaire" logo and the date "netMET - Journée du : 2003-06-13". A navigation bar on the left contains links for "Top", "Statistiques RENATER", "Métrologie détaillée", "Rapport de scans", "Archives", "Outils", and "Informations". The main content area is divided into several sections: "Trafic RENATER sortant & entrant" (Total sortant: 297.8 Go, Total entrant: 402.1 Go), "Les Top N" (Le top 15 des machines, Le top 10 des organismes), "Le Top N des machines pour les organismes Lothaire" (listing organizations like ATPA, ERM, INRA, etc.), "Statistiques RENATER pour les organismes Lothaire" (listing organizations like ATPA, ERM, INRA, etc.), and "Métrologie détaillée pour les organismes Lothaire" (listing organizations like ATPA, ERM, INRA, etc.). Red annotations with arrows point to the "Titre" (Title), "Barre de Navigation" (Navigation Bar), and "Accès aux statistiques" (Access to statistics) sections.

Une nouvelle exploitation : interface

Navigation, jour suivant – jour précédent

Accès aux informations "en 1 clic"

Archives Web

Boîte à outils (scripts)

Page d'informations personnalisée

Microsoft Internet Explorer

2002-12-08

netMET - Journée du : 2002-12-08

Informations du : Sam-08/12/2002 00:00:01 au Mon-09/12/2002 00:00:00

MATER sortant & entrant

179.1 Go
63.7 Go

Statistiques RENATER

statistiques par organismes
tous les organismes

Métrologie détaillée

détail par organismes

Rapport de scans

rapport par organismes
tous les organismes

Archives

toutes les archives

Boîte à outils

netMET LookUp
netMET addrCHECK
État du serveur

Informations

Les machines pour les organismes Lothaire.

Beaux-Arts	CHU	CIRIL	CNRS	CROUS
ENIM	ENSAM	GEMCEA	GEORGIA TECH	INPL
INRIA	INRS	INSERM	IRTS	IJFM
Nancy2	PUE	Rectorat	SUPELEC	SciencesPO
UNIV-METZ				

Les machines RENATER pour les organismes Lothaire.

Beaux-Arts	CHU	CIRIL	CNRS	CROUS
ENIM	ENSAM	GEMCEA	GEORGIA TECH	INPL
INRIA	INRS	INSERM	IRTS	IJFM
Nancy2	PUE	Rectorat	SUPELEC	SciencesPO
UNIV-METZ	Tous			

détaillée pour les organismes Lothaire.

Beaux-Arts	CHU	CIRIL	CNRS	CROUS
ENIM	ENSAM	GEMCEA	GEORGIA TECH	INPL
INRIA	INRS	INSERM	IRTS	IJFM
Nancy2	PUE	Rectorat	SUPELEC	SciencesPO
UNIV-METZ				

Rapport sur les scans du jour.

Rapport SCANS

Une nouvelle exploitation : interface

Menu popup

Menu popup,
pour accès "en 1 clic" aux informations
déclinées par organismes

The screenshot shows the netMET web interface in Microsoft Internet Explorer. The page title is "netMET - Journée du : 2002-12-08". The main content area displays "Trafic RENATER sortant & entrant" with statistics: "Total sortant : 179.1 Go" and "Total entrant : 163.7 Go". Below this is a table of links for various organizations, which is circled in red. The table has columns for different organizations and rows for different categories. The circled area highlights the table structure.

AFFA	Beaux-Arts	CAV	CHU	CIRIL	CNRS
CROUS	EAM	ENIM	ENSAM	GEMCEA	GEORGIA TECH
INPL	INRA	INRIA	INRS	INSERM	IP-NDH-ROUTABLE
IRTS	IUFM	NANCIE	Nancy2	ONF	PRIVE-AMPERENET
PRIVE-STANNET	PUE	RENATER	Reborat	SUPELEC	SciencesPO
UHP	UNIV-METZ				

Below the table, there are sections for "Top N des machines pour les organismes Lorraine.", "Statistiques RENATER pour les organismes Lorraine.", "Météologie détaillée pour les organismes Lorraine.", and "Rapport sur les scans du jour." Each section contains a grid of links to specific reports or data for the same set of organizations.

Une nouvelle exploitation : interface

Répartitions des trafics par protocoles et services/protocoles pour l'organisme CIRIL en entrée et en sortie

Répartition par protocoles

Répartition par services/protocoles

netMET - Journée du : 2002-12-08 - Métrologie détaillée pour CIRIL - Microsoft Internet Explorer

Favorites - Quête : 2

netMET - Journée du : 2002-12-08
Métrologie détaillée pour CIRIL

Informations du : Sun-08/12/2002 00:00:01 au Mon-09/12/2002 00:00:00

Métrologie détaillée pour RENATER vers CIRIL
Total de RENATER vers CIRIL : 8.1 Go

Répartition par protocoles

Protocole	Cumul (octets)	Cumul (%)
tcp (6)	7.4 Go	91.72
udp (17)	656.3 Mo	8.15
icmp (1)	10.8 Mo	0.13

Répartition par services/protocoles

Service/protocoles	Cumul (octets)	Cumul (%)
ntp/tcp (119/6)	6.1 Go	75.69
UNKNOWN/udp (65535/17)	540.4 Mo	6.71
www/tcp (80/6)	430.4 Mo	5.34
UNKNOWN/tcp (65535/6)	395.2 Mo	4.91
ftp-data/tcp (20/6)	293.5 Mo	3.64
domain/udp (53/17)	110.7 Mo	1.37
domain/tcp (53/6)	73.9 Mo	0.92
smtp/tcp (25/6)	61.9 Mo	0.77

Métrologie détaillée pour CIRIL vers RENATER
Total de CIRIL vers RENATER : 28.9 Go

Répartition par protocoles

Protocole	Cumul (octets)	Cumul (%)
tcp (6)	28.2 Go	97.53
udp (17)	675.6 Mo	2.34
icmp (1)	39.1 Mo	0.14

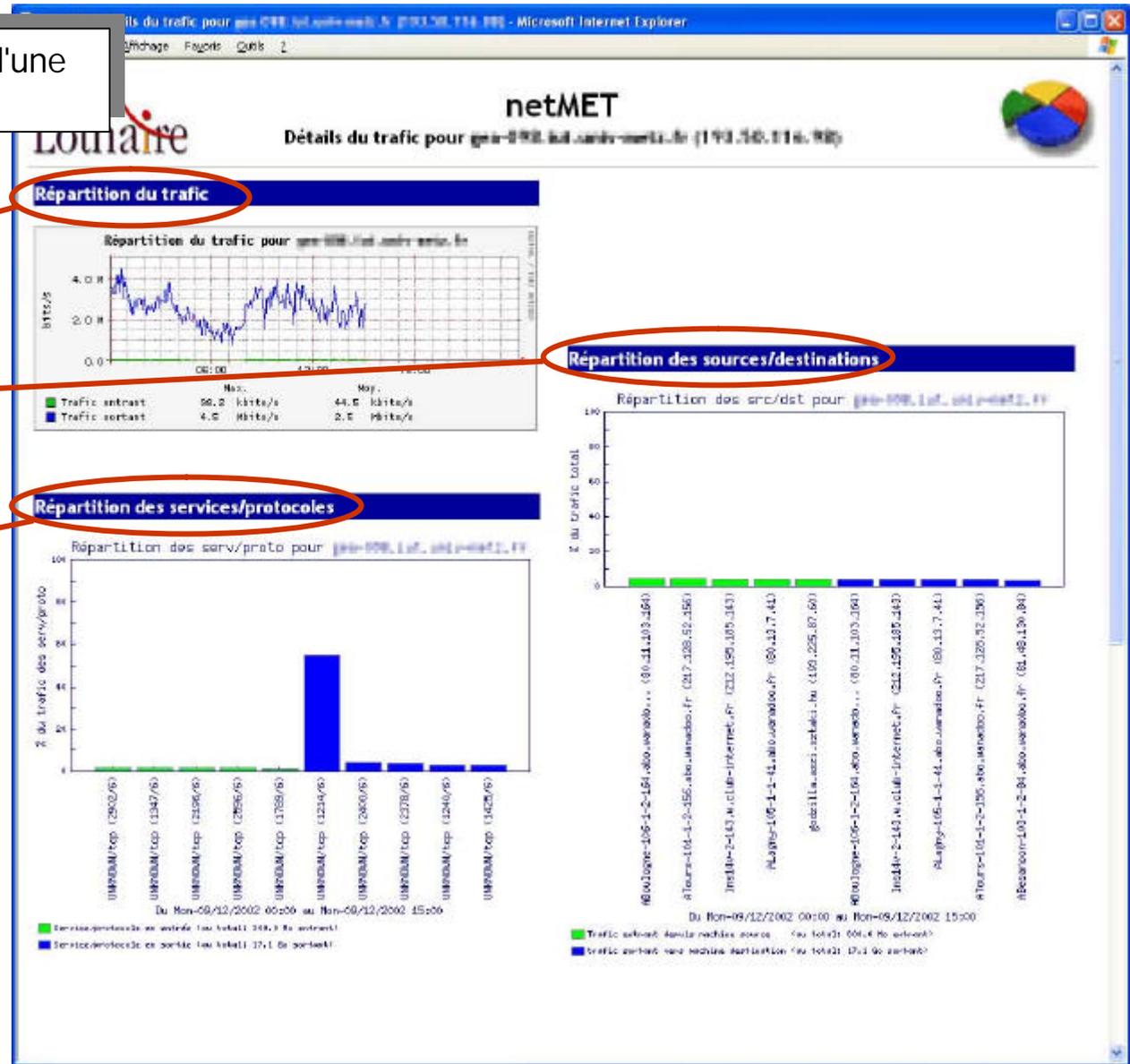
Une nouvelle exploitation : informations

Tous les détails de trafic d'une machine particulière

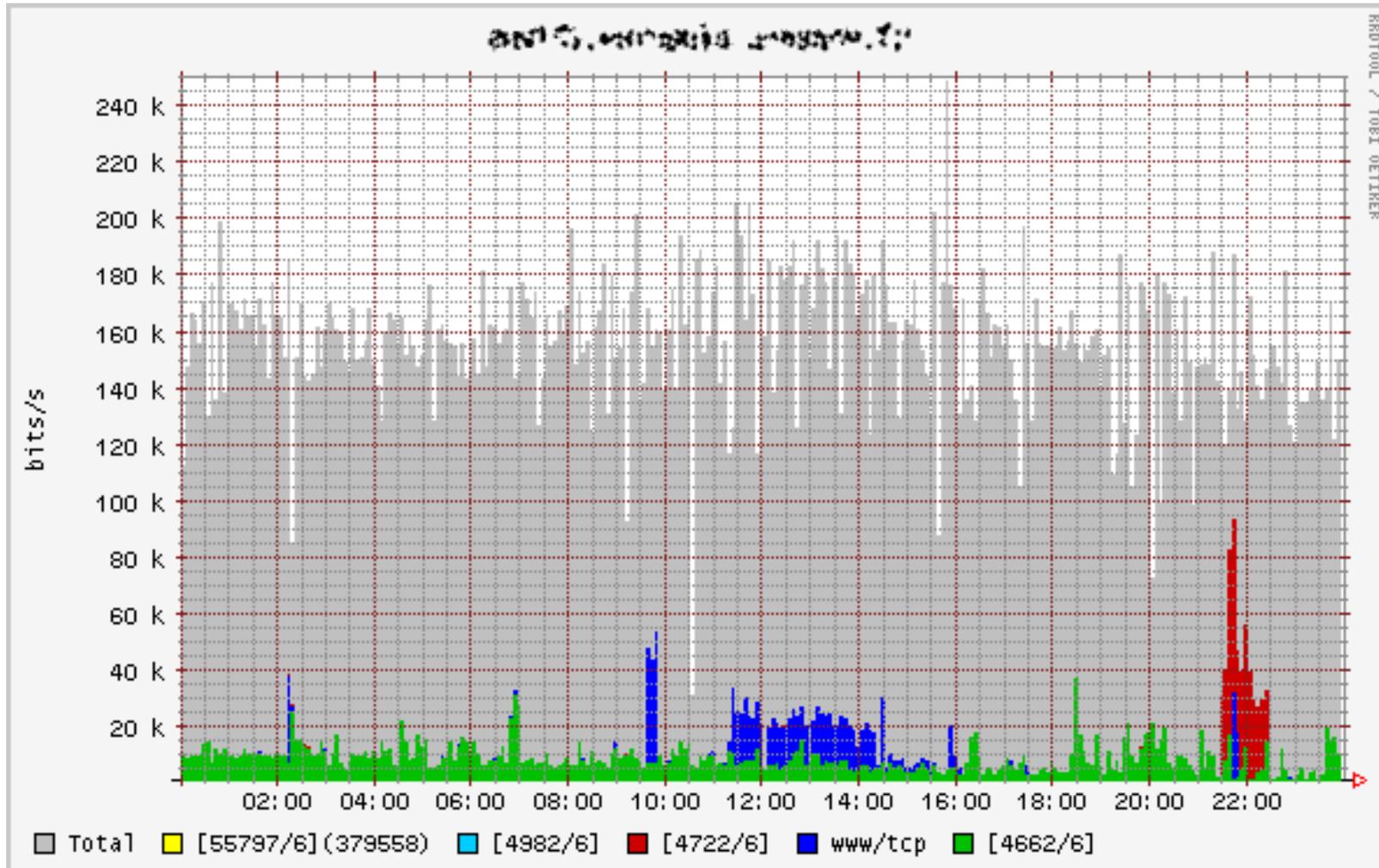
Répartition du trafic dans le temps
Quand ?

Répartition du trafic par sources/destinations
Avec Qui ?

Répartition du trafic par services/protocoles
Quoi ?



Une nouvelle exploitation : informations



Une nouvelle exploitation : informations

- Problèmes des rapports de scan de la version 1
 - non disponibles par organisme
 - très volumineux et par conséquent peu exploitables
- Apports de la nouvelle exploitation
 - génération de rapport de scan pour chaque établissement
 - synthèse des points importants en tête de rapport
 - mise à disposition de rapports pré-formatés pour le CERT Renater

Une nouvelle exploitation : informations

Liste des scans en hauteur et largeur pour l'organisme CIRIL

Résumé synthétique des scans

Rapport au format texte conforme aux traitements automatiques du CERT

Scans en HAUTEUR
1 machine vers n machines sur 1 port

Scans en LARGEUR
1 machine vers 1 machine sur n ports

netMET - Journée du : 2002-12-08 - Les scans détectés pour CIRIL - Microsoft Internet Explorer

netMET - Journée du : 2002-12-08
Les scans détectés pour CIRIL

Informations du : Sun-08/12/2002 00:00:09 au Mon-09/12/2002 00:00:00

Les scans détectés pour CIRIL
2002-12-08

Liens vers :
[Résumé](#)
[Scans en hauteur depuis CIRIL](#)
[Scans en largeur depuis CIRIL](#)
[Scans en hauteur depuis RENATER](#)
[Scans en largeur depuis RENATER](#)

Statistiques RENATER
[Lien vers le rapport au format texte, pdf-formaté pour le CERT](#)
[Liste des scans en HAUTEUR depuis RENATER](#)

Machine source : 192.168.0.2

Réseaux	Organismes	Horaires	Nb machines scannées	Services scannés	Nb réponses
1 192.168.209.0	*ORGA1*	06:40-7:00	255	[22/6]	0
2 192.168.210.0	*ORGA2*	06:50-7:00	255	[22/6]	1
3 192.168.213.0	*ORGA1* *ORGA2*	06:50-7:00	192	[22/6]	4
4 192.168.222.0	*ORGA3*	06:50-7:00	255	[22/6]	18
5 192.169.1.0		06:50-7:00	240	[22/6]	15
6 192.169.2.0	*ORGA3*	06:50-7:00	255	[22/6]	6
7 192.169.3.0	*ORGA4*	06:50-7:00	255	[22/6]	6
8 192.170.200.0	*ORGA5*	06:50-7:00	255	[22/6]	7

[Liste des scans en LARGEUR depuis RENATER](#)

Machine source	Machine destination	Horaires	Nb services
1 toto.org1.fr (192.168.200.1)	61.103.90.22	06:00	681
2 61.103.90.22	toto.org1.fr [192.168.200.1]	06:00	814
3 toto.org2.fr (192.168.202.1)	suspect.mal.intentionna.fr [122.203.45.21]	09:20	534
4 machine.quelque.peu.bizarre.fr [172.10.2.3]	192.168.222.3	11:10	584
5 suspect.mal.intentionna.fr [122.203.45.21]	toto.org1.fr [192.168.200.1]	12:10	1524
6 62.0.0.1	192.169.200.5	12:10	1521

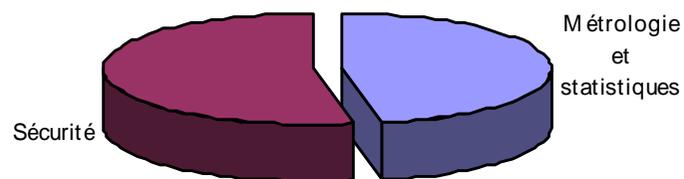
- Besoin des administrateurs réseau
 - fournir l'information netMET aux utilisateurs
- Problématique
 - confidentialité
 - accès aux données les concernant uniquement
- Solution netMET
 - authentification/permissions gérées par le serveur web Apache
 - authentification par login/password
 - permissions en fonction du document consulté
 - toutes les pages HTML contiennent le nom de l'organisme
 - chaque organisme correspond à un groupe Apache

- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : Sampled NetFlow
- Standardisation NetFlow : IPFIX

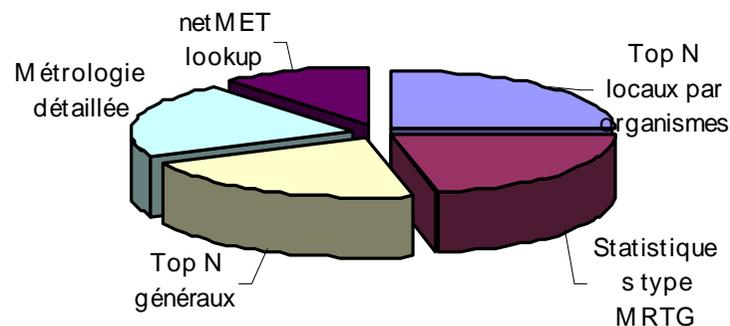
- Conclusion

La métrologie au service de la sécurité

- Résultats de l'audit netMET auprès des utilisateurs
 - Quelle est la principale utilisation que vous faites de netMET ?



- Dans l'utilisation pour la sécurité, classez les fonctionnalités netMET par ordre d'importance



- Avoir une approche sécurité avec netMET
 - détection des comportements atypiques
 - utilisation des Tops généraux et locaux
 - utilisation des statistiques vers le réseau fédérateur
 - utilisation des rapports de scan
 - investigation détaillée pour une machine ou un organisme
 - utilisation de la page détails
 - utilisation de l'outil de recherche multi-critères : netMET Lookup
 - utilisation des Tops locaux

Résumé du rapport de scans

Scans en Hauteur depuis RENATER

Résumé des SCANS en HAUTEUR

Nombre de sous-réseaux scannés : **4807**
 Nombre d'adresses IP scannées : **1143156**

Scans en Largeur depuis RENATER

Résumé des SCANS en LARGEUR

Nombre de scans en largeur : **12**

Scans en Hauteur depuis UHP

Liste des machines source de scans en hauteur

194.167.209.78 ()
 194.167.209.30 (dhcp06.iutnb.uhp-nancy.fr)
 194.167.209.29 (dhcp06.iutnb.uhp-nancy.fr)
 194.167.211.25 (dhcp06.iutnb.uhp-nancy.fr)
 193.48.208.251 ()

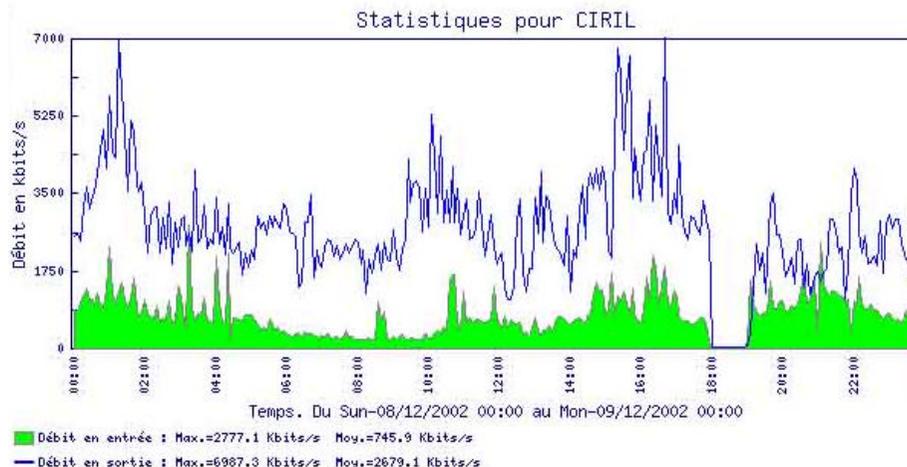
Scans en Largeur depuis UHP

Liste des machines sources de scans en Largeur

193.48.208.188 (participa.uhp-nancy.fr)

IP spoofing pour UHP

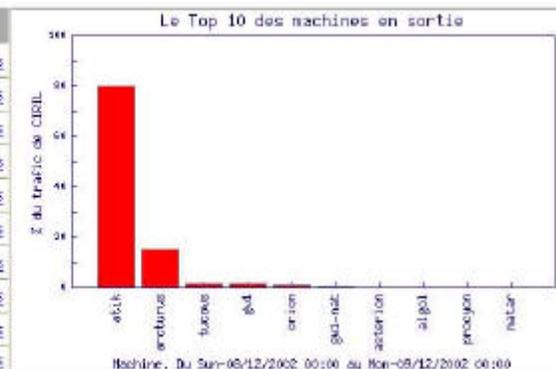
Il n'y a pas eu d'IP spoofing pour UHP

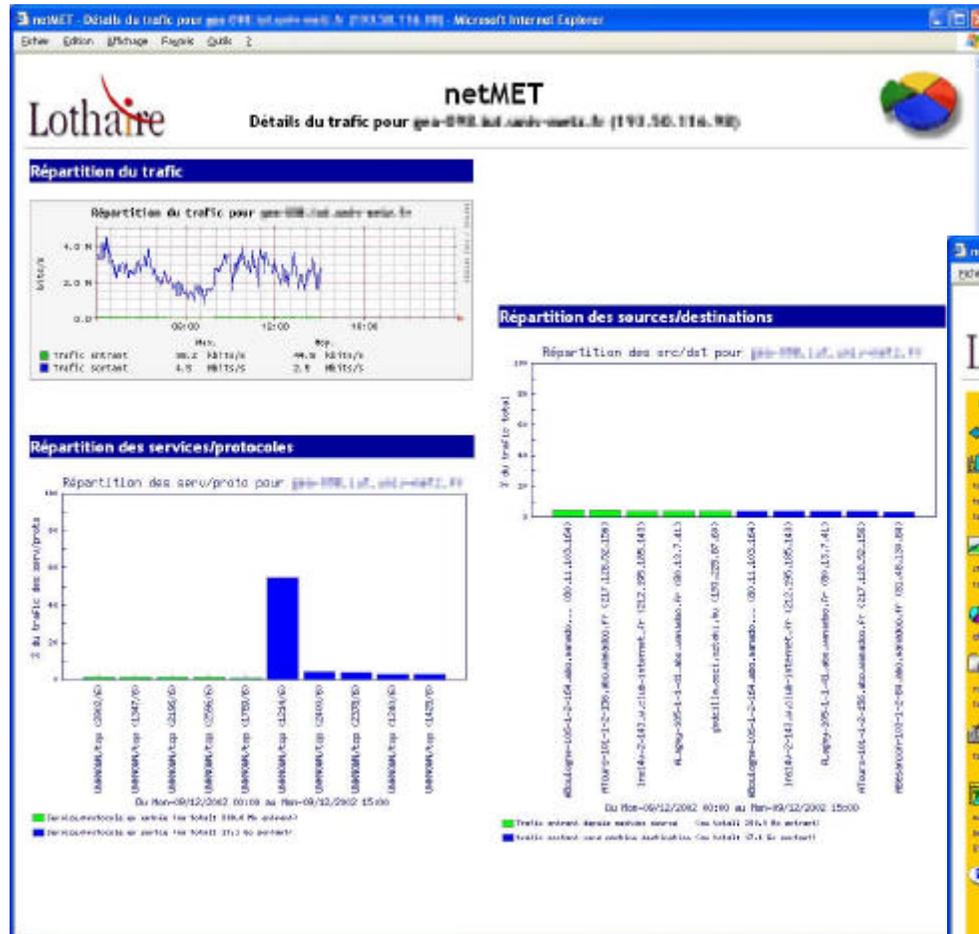


Top 10 en sortie

Total sortant vers RENATER : 20.9 Go

Host	Cumul [octets]	Cumul [%]	
atik.ciril.fr	29.1 Go	79.81	Détails
areturns.ciril.fr	4.5 Go	15.43	Détails
tucoys.ciril.fr	429.0 Mo	1.48	Détails
gpi-143-korner.fr.localhost	412.6 Mo	1.43	Détails
arles.ciril.fr	294.0 Mo	0.88	Détails
gpi-143-143.ciril.fr	123.7 Mo	0.43	Détails
action.ciril.fr	51.3 Mo	0.18	Détails
algot.ciril.fr	34.1 Mo	0.12	Détails
projet.ciril.fr	9.3 Mo	0.03	Détails
natun.ciril.fr	8.9 Mo	0.03	Détails





netMET LookUp - Le moteur de recherche de netMET - Microsoft Internet Explorer

Lothaire netMET LookUp
Le moteur de recherche de netMET

Sélection des adresses IP

Machine / Subnet n°1 :

ou Organisme n°1 :

Machine / Subnet n°2 :

ou Organisme n°2 :

La Machine n°1 est la source.
 La Machine n°1 est la destination.
 La Machine n°1 est la source ou la destination.
 La Machine n°1 est la source, La Machine n°2 est la destination.

Sélection d'un service et/ou d'une quantité de service

Service : [Jdbc/service]

Quantité entrée : [Octets] et [Octets]

Les machines distantes sont considérées dans leur globalité

Sélection d'une quantité pour le trafic total

Trafic entre : [Octets] et [Octets]

Les machines distantes sont considérées dans leur globalité

Options d'affichage

Faire la résolution DNS

Valider

- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : **Sampled NetFlow**
- Standardisation NetFlow : IPFIX

- Conclusion

Echantillonnage des flux : Problématique

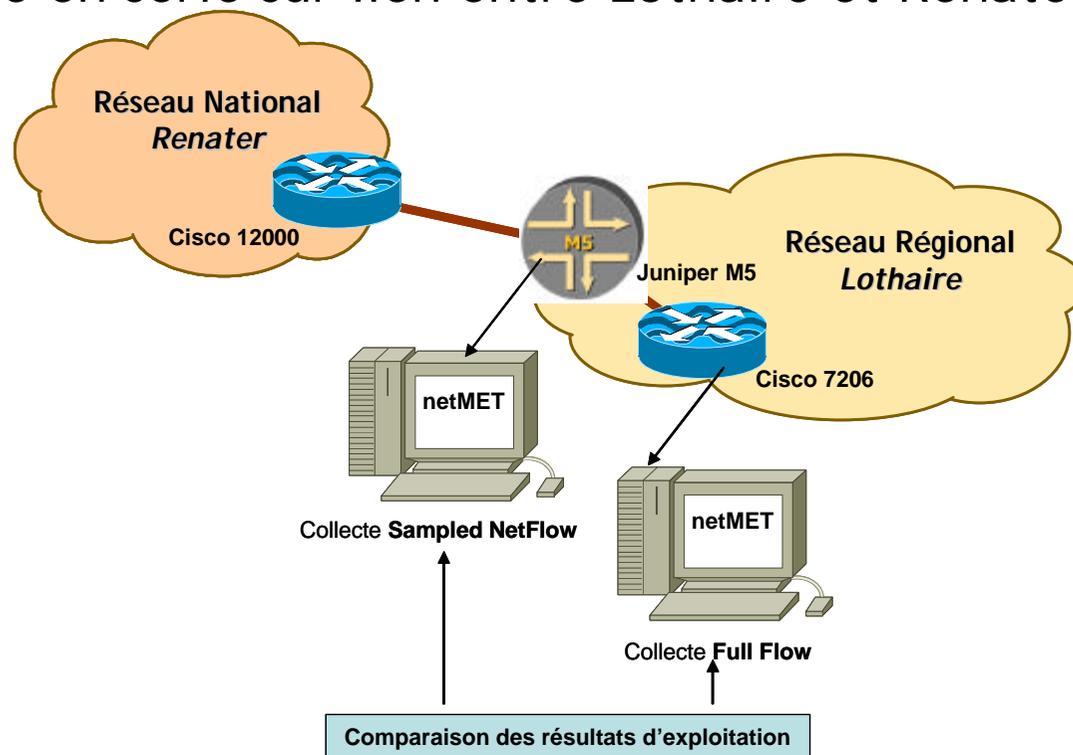
- Dans le cadre des liaisons à hauts débits
 - problématique
 - gestion du NetFlow sur les routeurs très consommateurs de CPU
 - collecteurs submergés d'informations
 - question subsidiaire
 - est-il nécessaire de traiter de tels volumes d'information ?
 - "mesures au bit près" vs "mesures de tendances"

- Solution
 - échantillonnage des flux
 - exportation des informations de métrologie pour 1 flux sur n

- Expertise métrologie pour RAP (Réseau Académique Parisien)
 - possibilité de faire fonctionner netMET sur RAP ?
 - sur plate-forme Juniper M5 ?

- Support de Sampled NetFlow par netMET
 - modification apportée au collecteur
 - simple multiplication par le facteur n
 - la loi des grands nombres fait le reste
 - disponible depuis janvier 2003
 - version spécifique
 - non fournie en standard
 - peut-être obtenue sur demande

- Validation pour RAP sur Lothaire
- Plateforme : Juniper M5
 - en prêt au CIRIL
 - inséré en série sur lien entre Lothaire et Renater



- Etude et résultats pratiques (non théoriques)
 - erreur induite par la fonction de réévaluation (multiplication) comprise entre 0.09% et 0.17%
 - acceptable pour réaliser la métrologie

- Utilisation "sécurité" toujours possible
 - détection des comportements atypiques sur type et quantité de trafic
 - les rapports de scan nécessitent un réajustement des seuils de détection

- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : Sampled NetFlow
- **Standardisation NetFlow : IPFIX**
- Conclusion

- *IP Flow Information eXport*
www.ietf.org/html.charters/ipfix-charter.html
- Groupe de l'IETF dont le but est de standardiser l'exportation des informations de routage
- Objectifs
 - définir ce qu'est un flux IP
 - supporter IPv4, IPv6 et le multicast
 - prendre en compte l'échantillonnage
 - sécuriser l'exportation des informations de flux
 - définir le format d'exportation des informations
 - rendre le mécanisme d'exportation fiable

- D'après les discussions actuelles :
 - les premiers documents décrivent un standard proche de NetFlow Cisco version 9
 - un flux « IPFIX » contiendra toutes les informations nécessaires à netMET
- netMET saura exploiter ce standard
- IPFIX permettra de faire de la métrologie standardisée sur tous types d'équipement l'implémentant

- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : Sampled NetFlow
- Standardisation NetFlow : IPFIX
- Conclusion

- Les choix réalisés à l'origine du projet permettent aujourd'hui une évolution de la solution ainsi que le support de nouvelles fonctionnalités
- netMET s'adapte continuellement
 - aux besoins exprimés par les utilisateurs
 - aux évolutions des protocoles et des standards
- Les récentes évolutions sont très orientées "sécurité"
 - la majorité des demandes vont dans ce sens
 - les informations associées contiennent le plus de valeur ajoutée
 - c'est dans ce domaine que nous travaillons le plus et qu'il y a encore beaucoup à faire
- netMET fait toujours l'unanimité auprès des utilisateurs, ceux-ci étant de plus en plus nombreux à adhérer au projet



e-mail : netmet@netmet-solutions.org

web : <http://www.netmet-solutions.org>

mailing-list : netmet-list@netmet-solutions.org