netMET Network's METrology

De nouveaux besoins, de nouvelles fonctionnalités

Lille, 20 novembre 2003

netMET — *netmet@netmet-solutions.org*
Sébastien MOROSI — *Sebastien.Morosi@ciril.fr*
Alexandre SIMON — *Alexandre.Simon@ciril.fr*

Plan

- 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
  - (...)

De nouveaux besoins : les protocoles

- Evolutions de NetFlow Cisco
  - version 9
  - échantillonnage de flux : Sampled NetFlow
  - IPv6
- Standardisation
  - IPFIX
  - support de NetFlow par de nouveaux constructeurs

netMET
Network's METrology

Plan

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

Une nouvelle exploitation

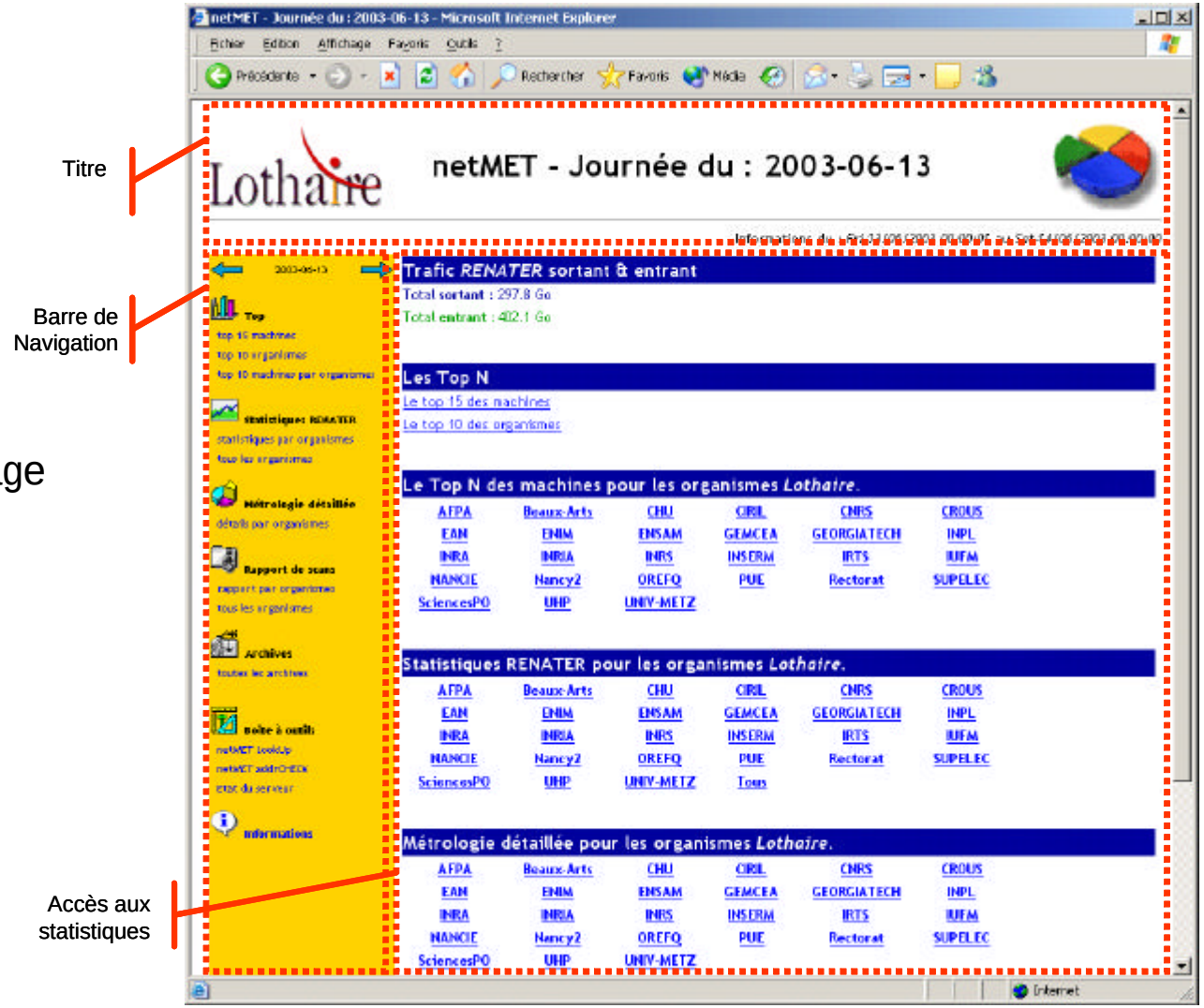
- Passage à la version 2 de l'exploitation : avril 2003
- Mise à jour de l'exploitation de netMET
  - nouvelle interface
  - nouvelles fonctionnalités
  - diffusion de l'information

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



Une nouvelle exploitation : interface

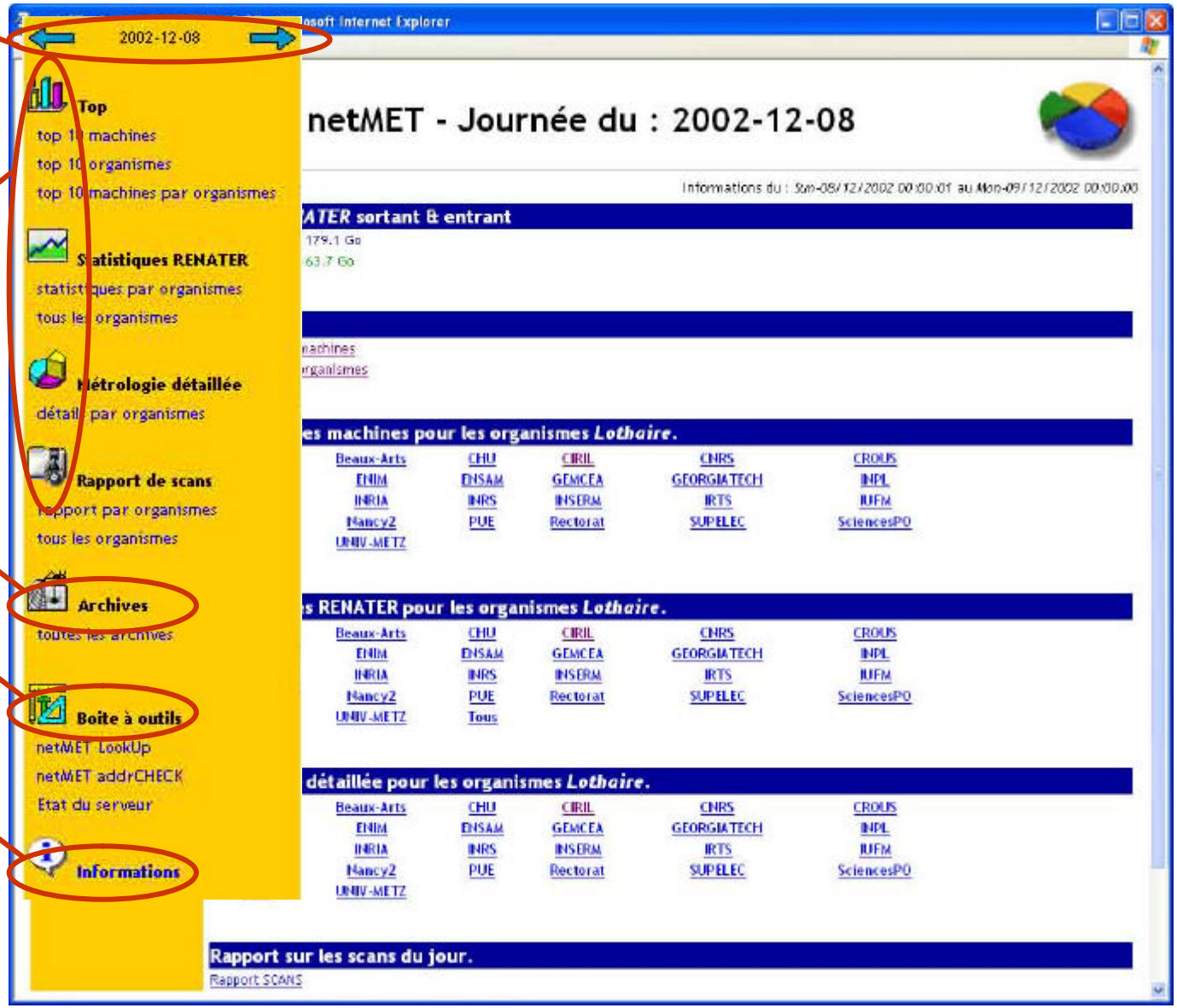
Navigation,
jour suivant – jour précédent

Accès aux informations "en 1 clic"

Archives Web

Boite à outils (scripts)

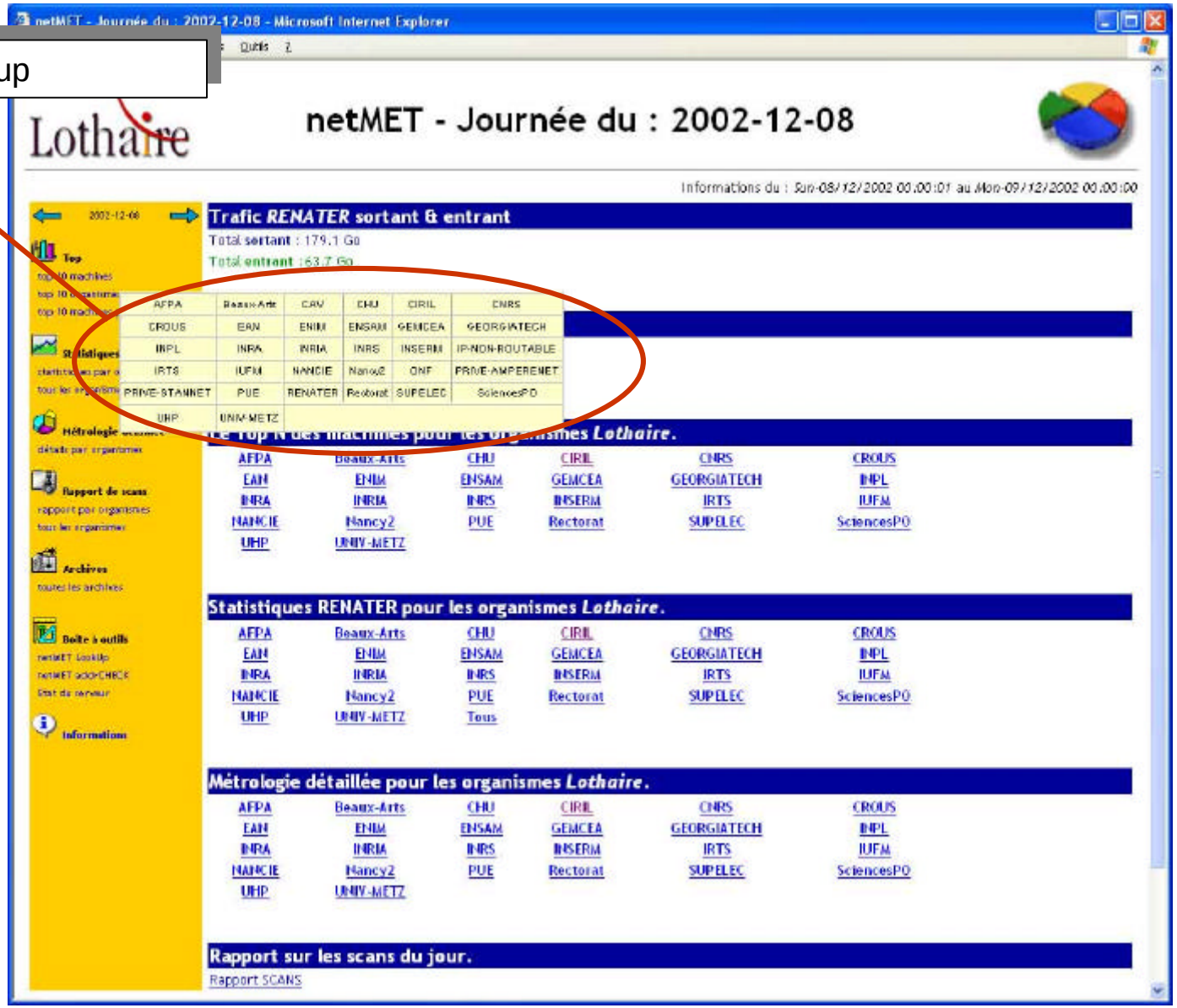
Page d'informations personnalisée



Une nouvelle exploitation : interface

Menu popup

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

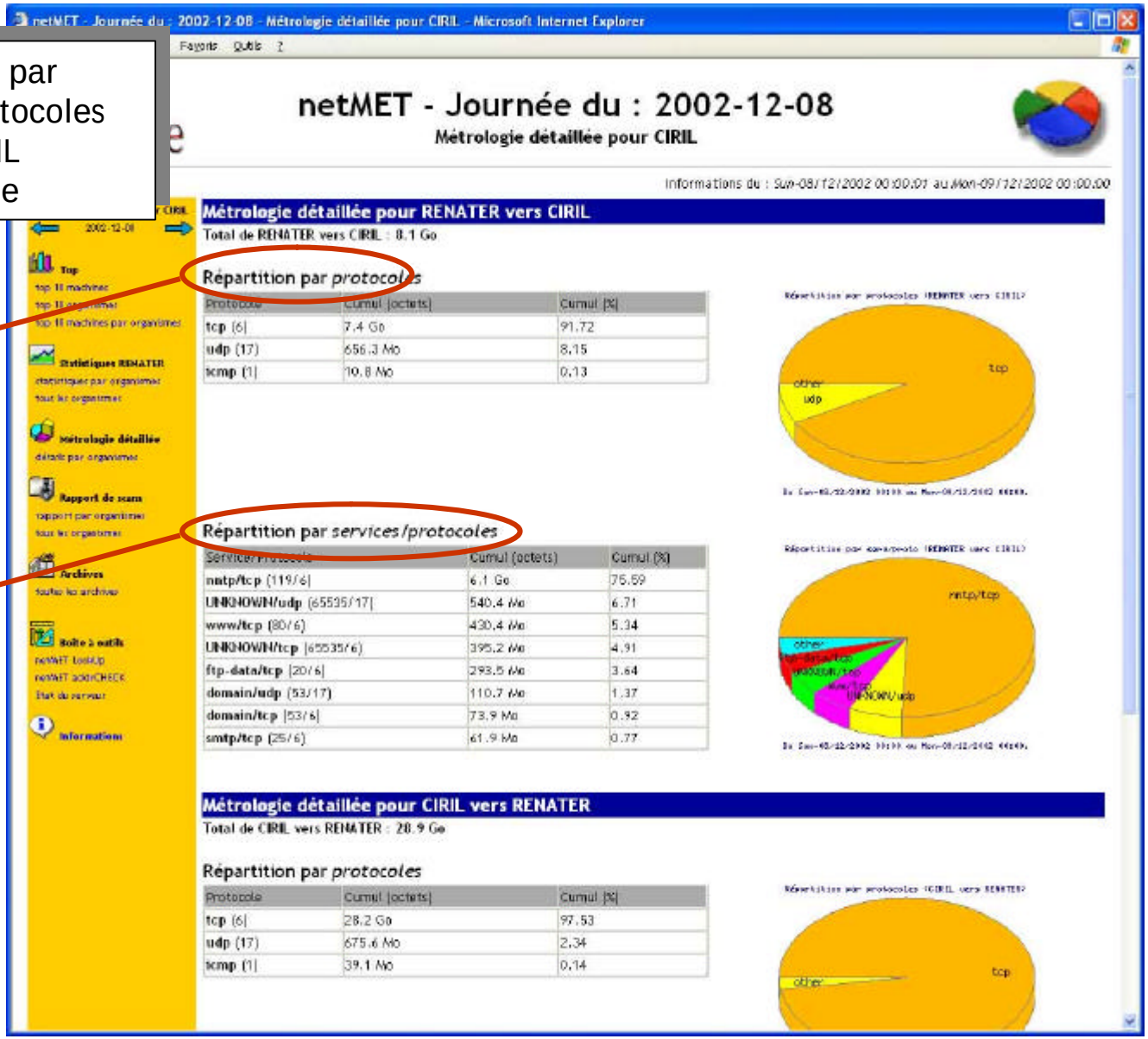


Une nouvelle exploitation : interface

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

Répartition par protocoles

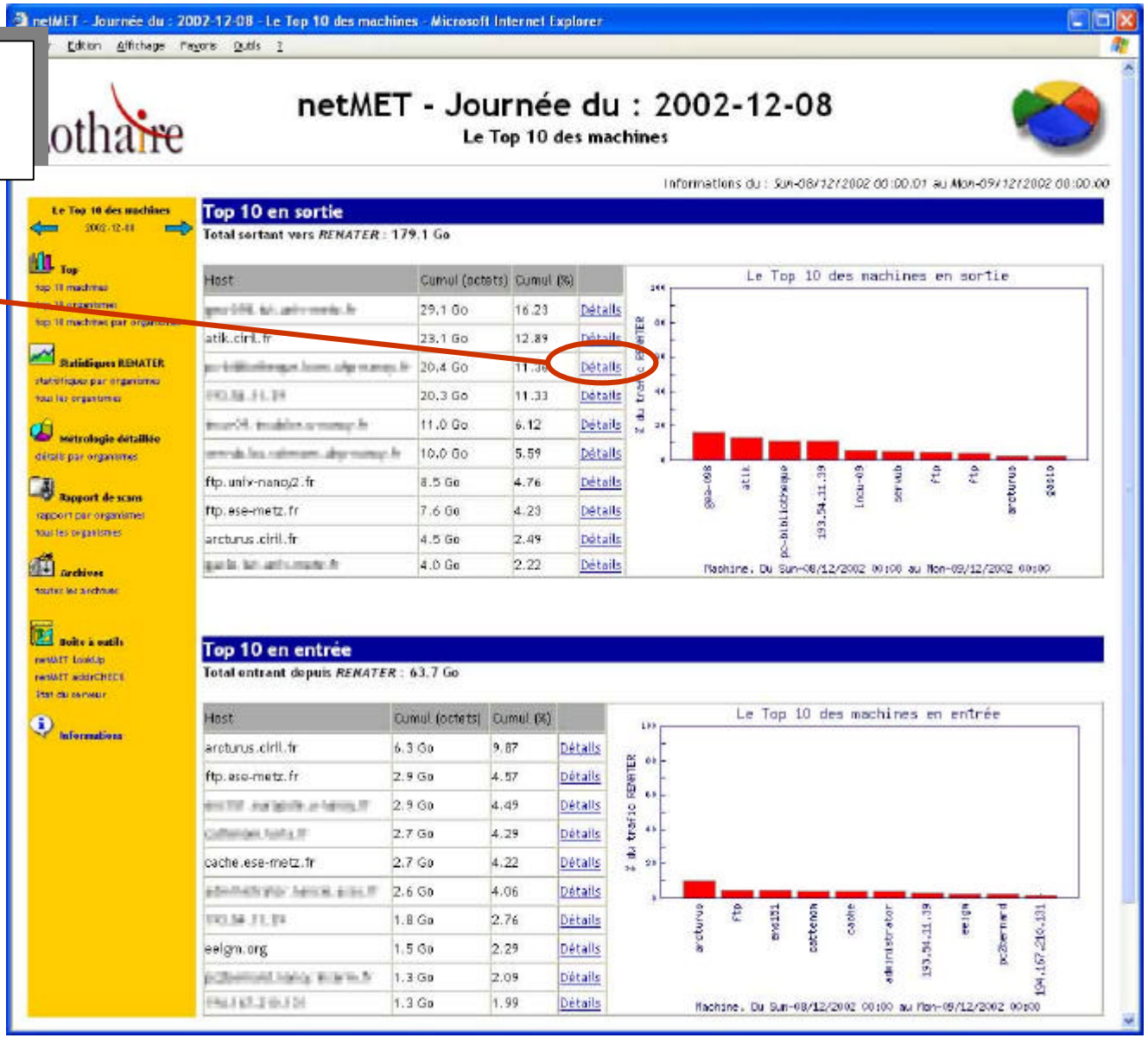
Répartition par services/protocoles



Une nouvelle exploitation : informations

Les TOPs 10 généraux des machines en entrée et en sortie

Accès aux détails de trafic
Quand ? Quoi ? Avec Qui ?



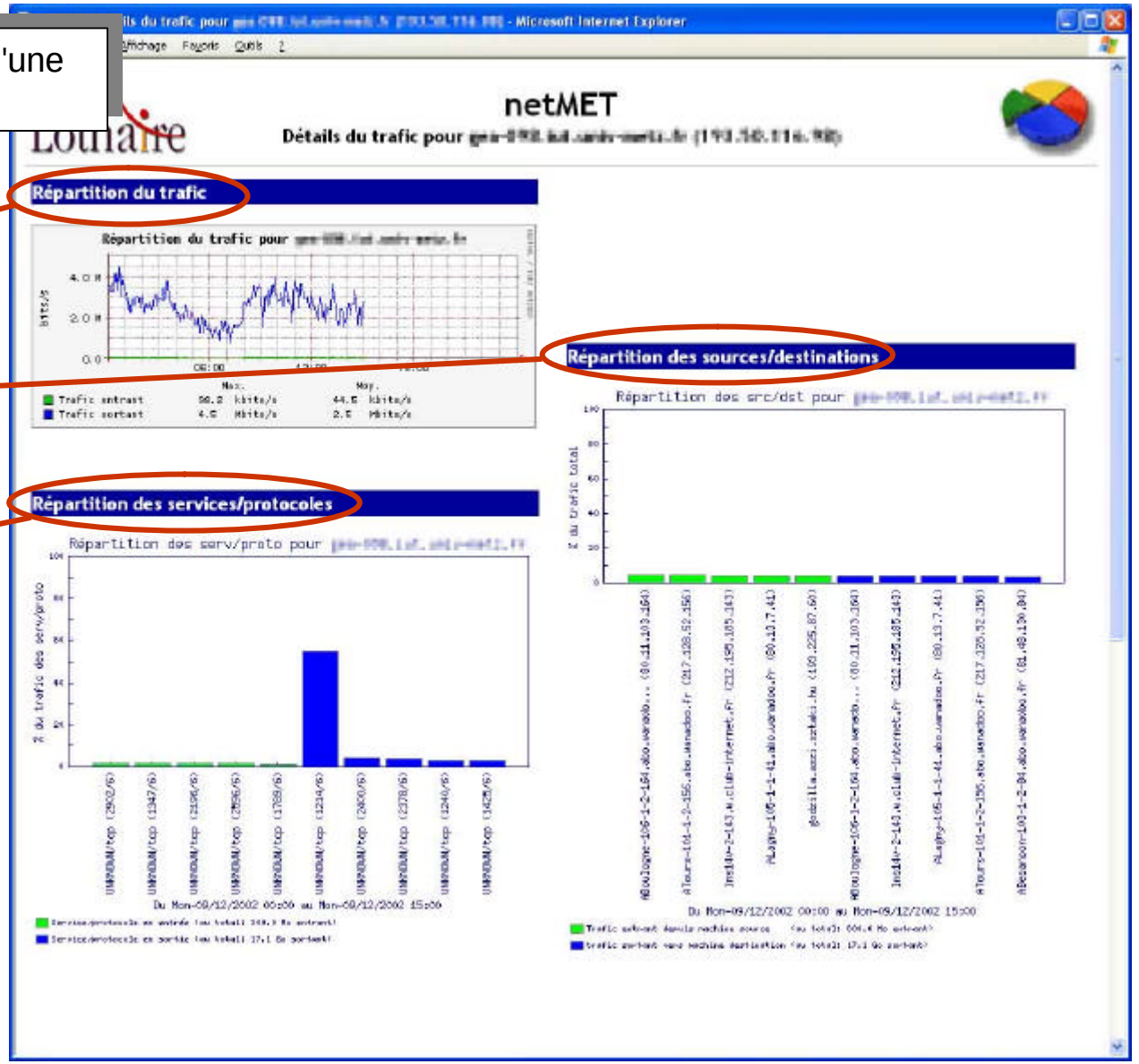
Une nouvelle exploitation : informations

Tous les détails de trafic d'une machine particulière

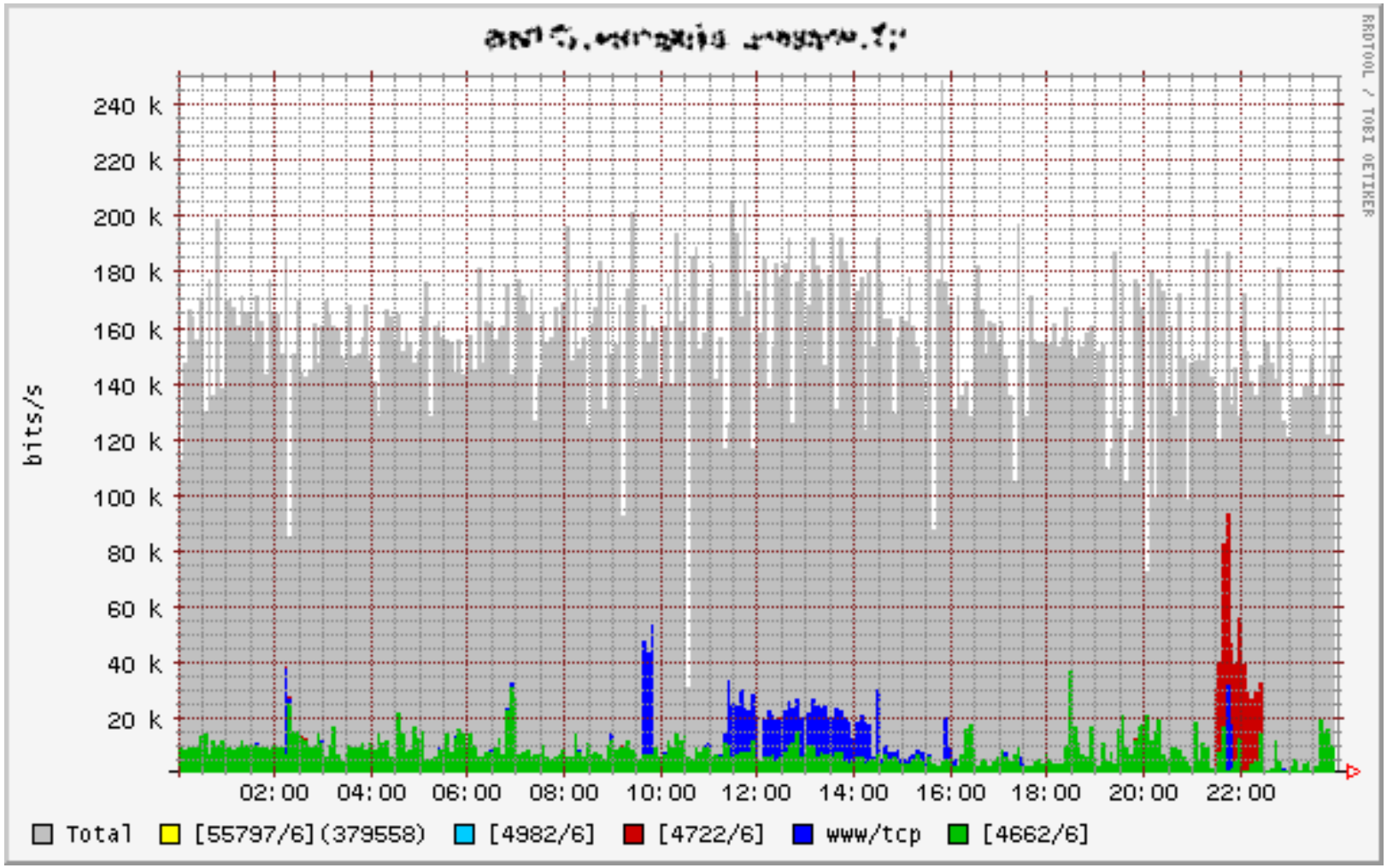
Répartition du trafic dans le temps
Quand ?

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

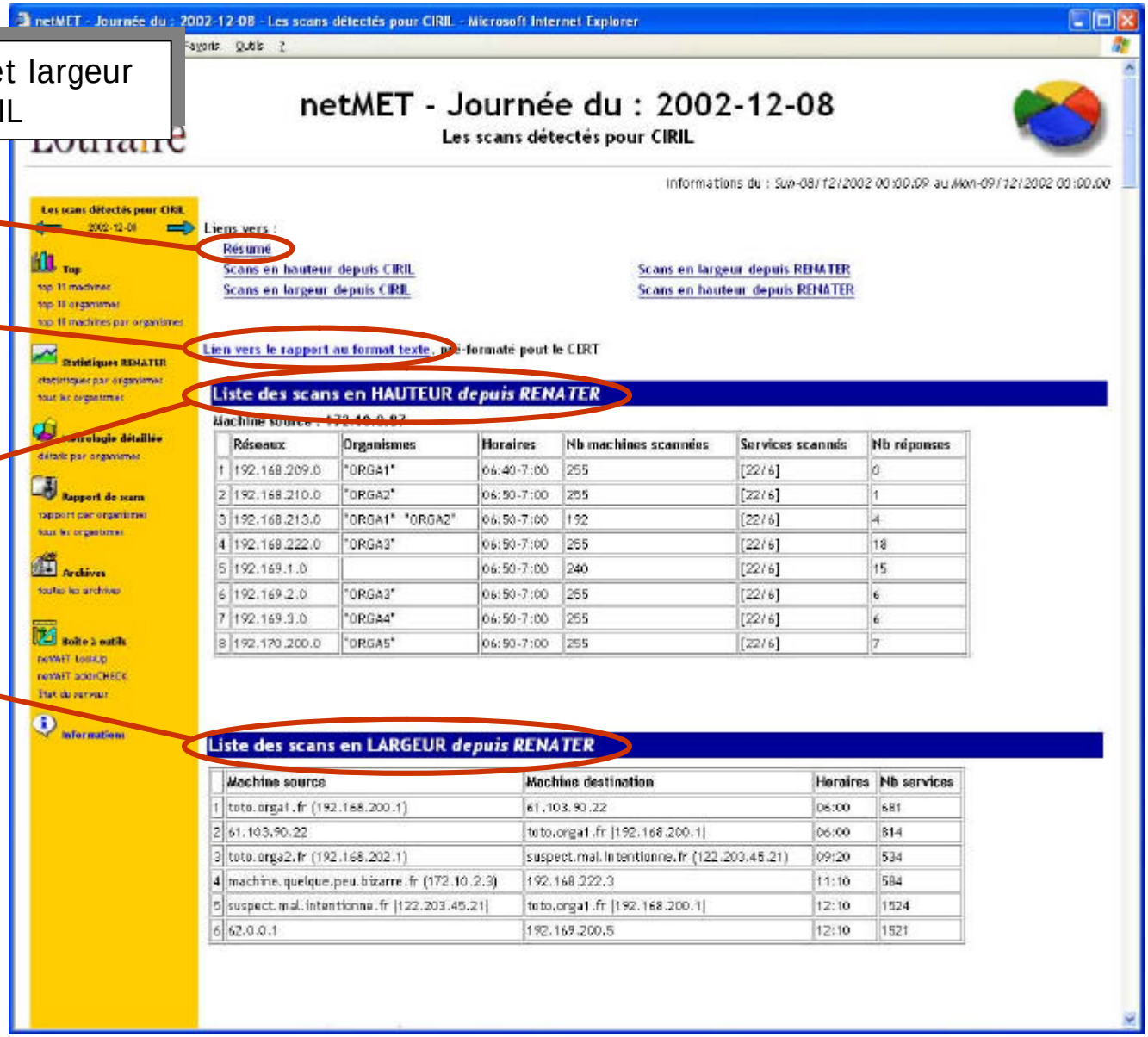
Liste des scans en hauteur et largeur pour l'organisme CIRIL

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



	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

	Machine source	Machine destination	Horaires	Nb services
1	toto.orga1.fr (192.168.200.1)	61.103.90.22	06:00	681
2	61.103.90.22	toto.orga1.fr (192.168.200.1)	06:00	814
3	toto.orga2.fr (192.168.202.1)	suspect.mal.intentionne.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.intentionne.fr (122.203.45.21)	toto.orga1.fr (192.168.200.1)	12:10	1524
6	62.0.0.1	192.169.200.5	12:10	1521

Diffusion de l'information

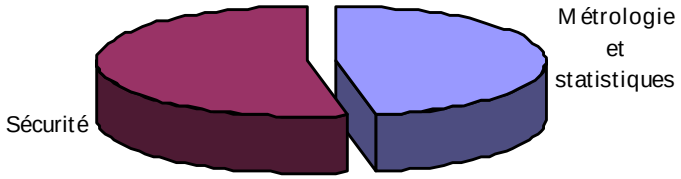
- Besoin des administrateurs réseau
  - fournir l'information netMET aux utilisateurs
- Problématique
  - confidentialité
  - accès aux données les concernant uniquement
- Solution netMET
  - authentification/permissions gérées par le serveur web Apache
    - authentification par login/password
    -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

Plan

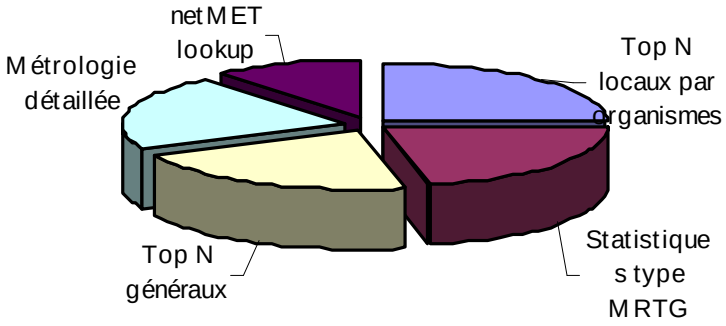
- De nouveaux besoins
- Une nouvelle exploitation
- La métrologie au service de la sécurité
- Echantillonnage des flux : Sampled NetFlow
- Standardisation NetFlow : IPFIX
- Conclusion

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



La métrologie au service de la sécurité

- 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

Détection des comportements anormaux

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)

[redacted]

193.48.208.251 ()

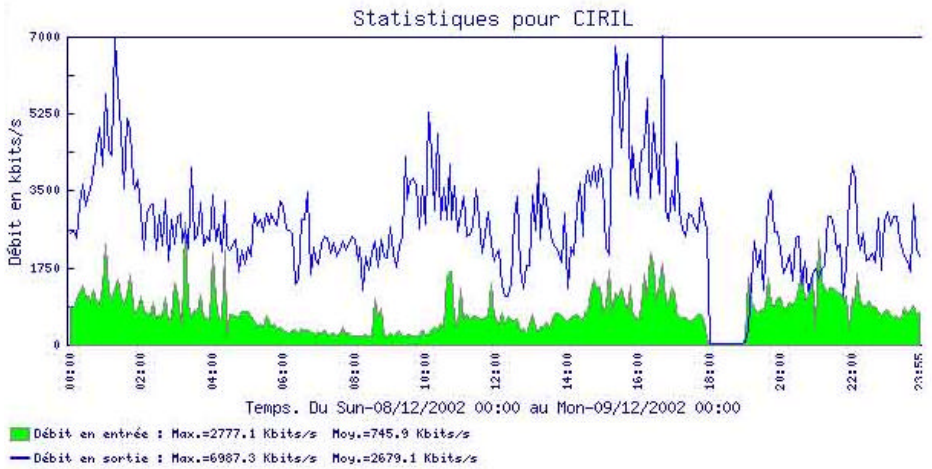
Scans en Largeur depuis UHP

Liste des machines sources de scans en Largeur

[redacted]

IP spoofing pour UHP

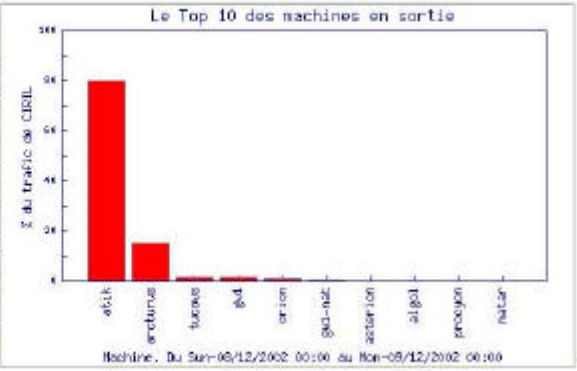
Il n'y a pas eu d'IP spoofing pour UHP



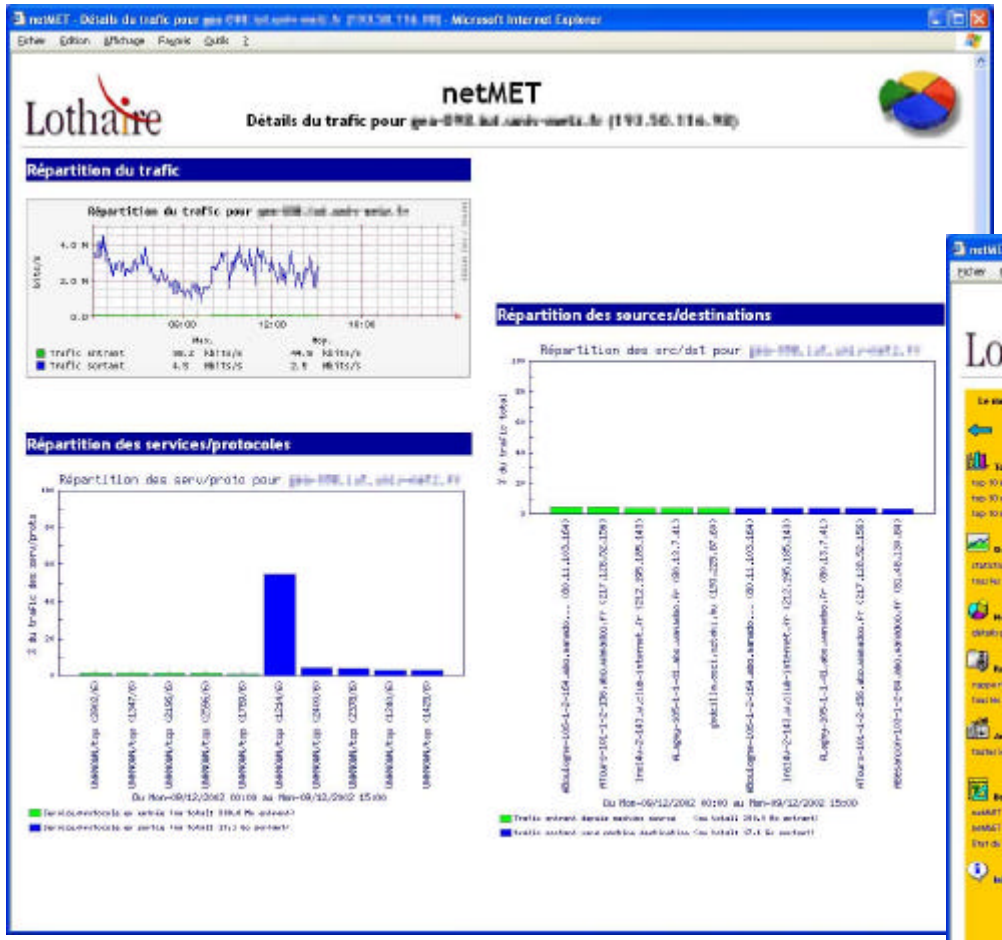
Top 10 en sortie

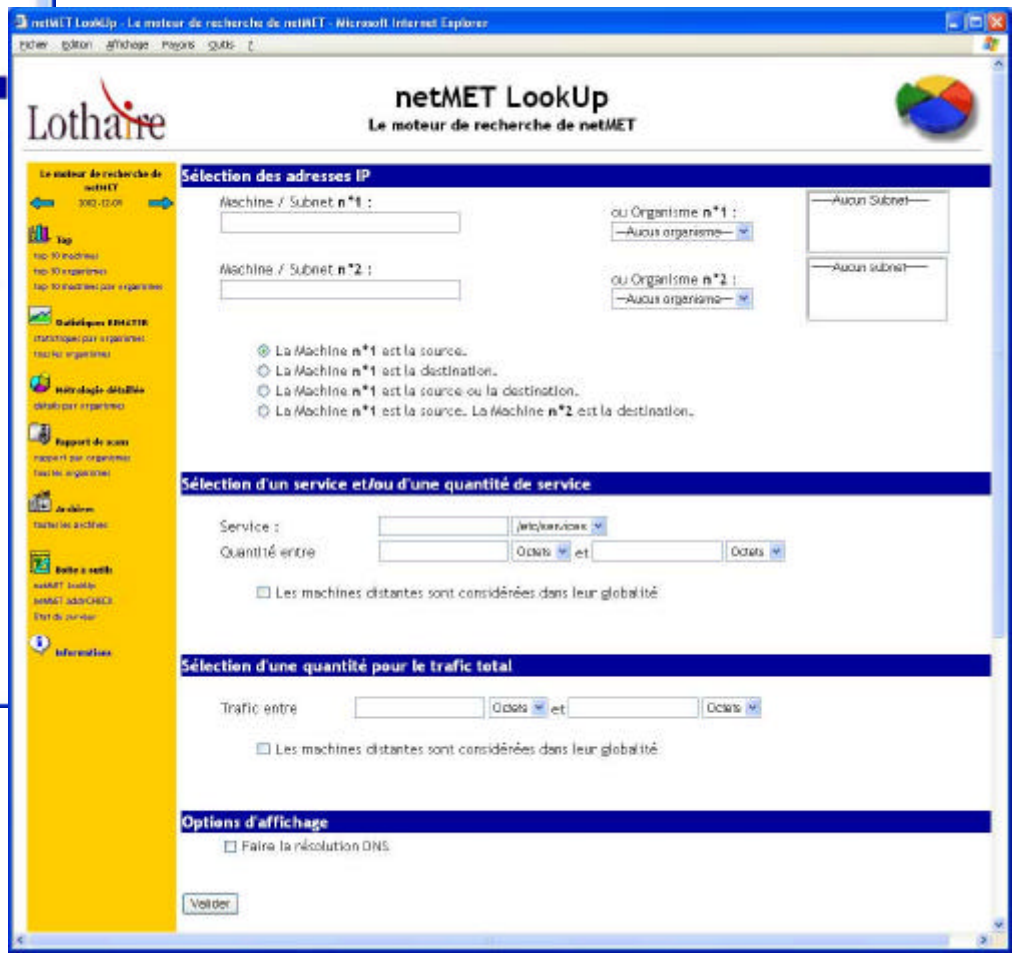
Total sortant vers *RENATER* : 28.9 Go

Host	Cumul (octets)	Cumul (%)	
atik.ciril.fr	23.1 Go	79.81	Détails
arcturus.ciril.fr	4.5 Go	15.43	Détails
tucows.ciril.fr	429.0 Mo	1.48	Détails
[redacted]	412.6 Mo	1.43	Détails
[redacted]	254.0 Mo	0.88	Détails
[redacted]	123.7 Mo	0.43	Détails
[redacted]	51.3 Mo	0.18	Détails
[redacted]	34.1 Mo	0.12	Détails
[redacted]	9.3 Mo	0.03	Détails
[redacted]	8.9 Mo	0.03	Détails



Investigation détaillée





netMET
Network's METrology

Plan

- 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"

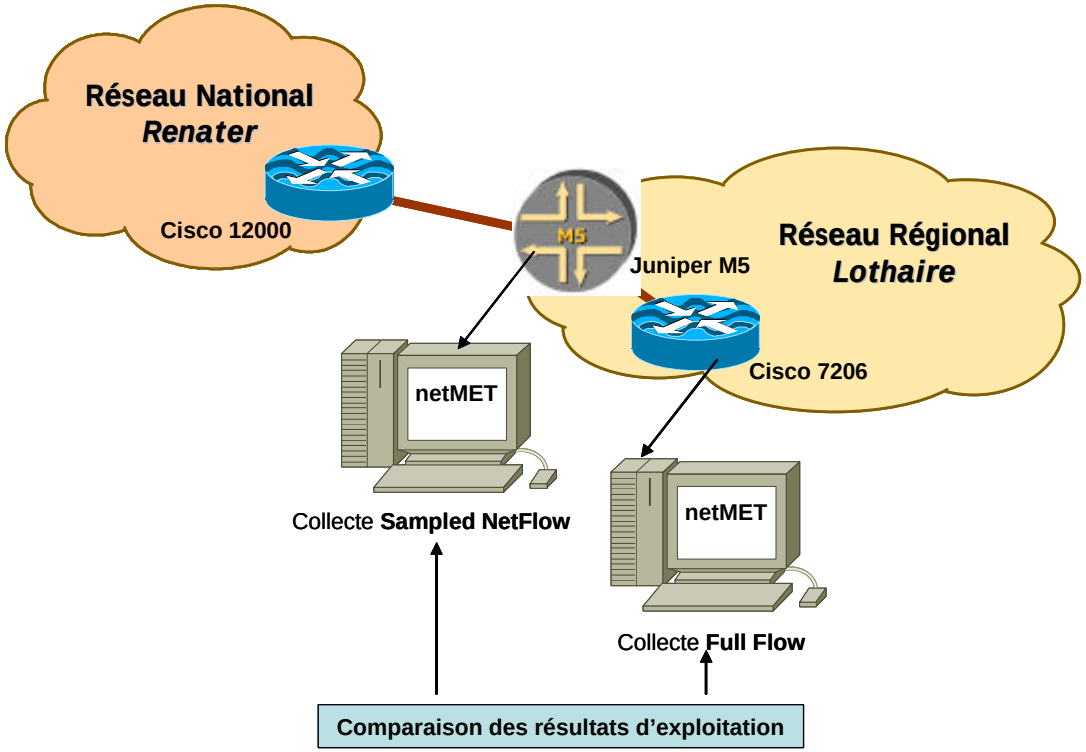
- Solution
  - échantillonnage des flux
  - exportation des informations de métrologie pour 1 flux sur n

Echantillonnage des flux : netMET

- 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

Echantillonnage des flux : validation

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



Echantillonnage des flux : conclusion

- 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

Plan

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

Standardisation NetFlow : IPFIX

- *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

Standardisation NetFlow : IPFIX

- 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

Plan

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

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**