SURVEILLANCE DU RÉSEAU DE L'ENTREPRISE

Enjeu majeur de la sécurité: comprendre/détecter rapidement la nature et des trafic

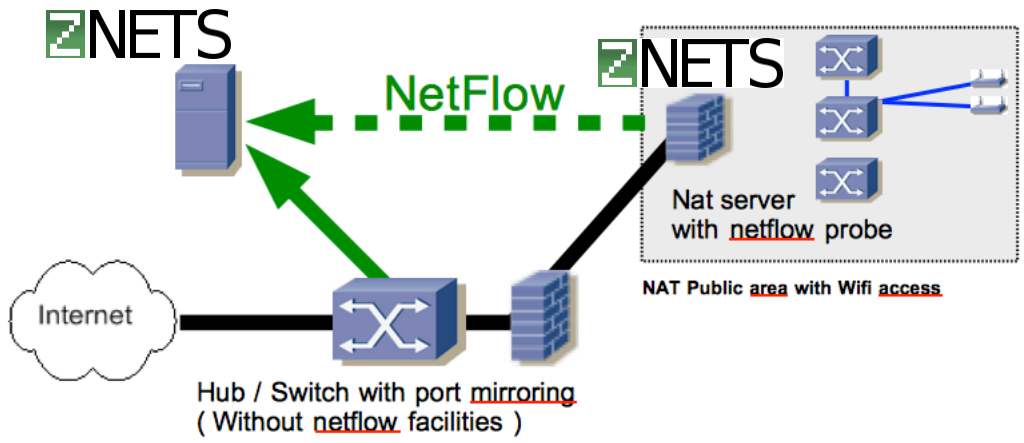
- Interprétation des flux réseau
- Etude de la métrologie

PRESENTATION

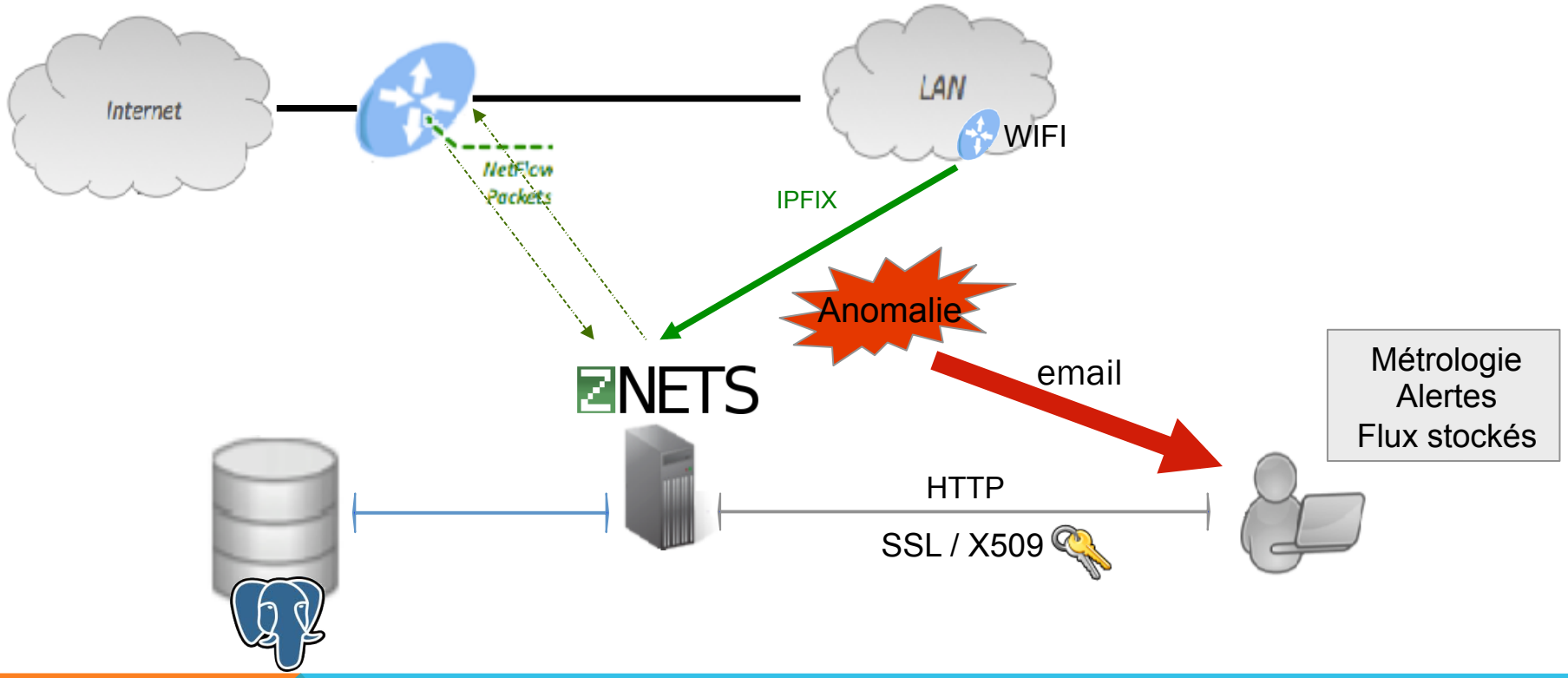
- Collecteur de flux
- Acquisition: capture directe, flux IPFIX ou netflow
- IPv4 ou IPv6
- Mode sonde IPFIX pour réseaux internes (remontée liste LH / applications, pays / asn…)
- Adaptable
- Facile à configurer:
  - 1 seul fichier de configuration, listes centralisées, mises à jour
  - 1 seul exécutable (serveur/repo HTTP, sonde, collecteur…)
- performance: limite pcap env. 5Gbps avec des équipements standards et détection applicative.
- V1.29 déployée en production: +100 labos

DÉPLOIEMENT

Possibilité d'avoir des sondes ZNeTS et d'ignorer le trafic du serveur NAT.



SCHEMA DE PRINCIPE



PRESENTATION

Installation:

- Package EL6 / Fedora / Debian / Ubuntu LTS / Mint (Windows&Mac… si demande)
- Simple et automatisée (scripts)

Dépendances:

- Postgresql
- Librairies Open Source (portables et répandues):

LA TRAÇABILITÉ DES FLUX

“flux réseaux” = informations importantes des datagrammes IP.

Ces flux sont:

- Incontestables
- Incorruptibles
- Inaltérables

Flux znets :

- Bidirectionnels
- Réagrégés pendant 1 heure: pas de perte
  et nb Flux < nb Paquet / 800

Champs:

début/fin, IP IN/OUT, sens, volume trafic in/out, nb paquets in/out, protocole IP, ports in/out, masques tcp in/out, asn, pays, application

LA TRAÇABILITÉ DES FLUX

Détermination du sens / capture: maintenant fiable > 99% des cas

180 applications détectées (même sur des ports non standard, et même encapsulé dans du ssl !): *Skype, Tor, Bittorent, openVPN, ciscoVPN, dropBox, Teamviewer, MySQL, PostgreSQL, Oracle*…

Flux sortant: Décodage/Stockage URLs HTTP + autres info de niveau applicatif (DNS)

Plusieurs mois (base de données postgresql partitionnée / insertions asynchrones)

Possibilité de consulter les flux en cours de réagrégation (mergés à la volée avec ceux stockés)

LA TRAÇABILITÉ DES FLUX

Cycle														
IpLocal	Dir	IpExtern	ASNum	Proto	PtLoc	PtExt	TcpFlg	IncTraf	OutgTraf	IncPkts	OutgPkts	Application	FirstTime	LastTime	Duration
134.158.47.197	<	193.48.244.139	2200	6	445	49373	APS	0	236258664	0	5359614	SMB	10:16:22	23:00:01	12:43:39
134.158.47.197	>	193.48.244.253	2200	6	50258	22	APS	0	191023960	0	3532465	SSH	10:00:10	23:00:01	12:59:51
193.48.83.164	>	128.142.144.62	513	6	43552	25085	APS	216280	1508	38	29	HTTP	22:00:00	22:00:01	00:00:01
193.48.83.97	<	194.80.35.59	786	6	4823	33552	APSF	376	688	6	4		22:00:00	22:00:16	00:00:16
193.48.83.60	<	193.48.99.161	789	6	24385	43816	APSF	322928281	1219920	23889	30498		21:59:40	22:00:42	00:01:02
193.48.83.96	>	193.206.93.38	137	6	36273	1094	APSF	140463298	1876512	51379	33158		21:57:26	22:03:36	00:06:10
193.48.83.165	<	134.158.103.10	789	17	9532	8833		42	0	1	0		21:59:31	22:00:01	00:00:30
193.48.83.165	>	200.130.35.232	1916	6	46442	8090	ASF	104	52	2	1		22:00:00	22:00:01	00:00:01
193.48.83.61	<	206.12.1.40	36391	6	24384	60817	APSF	226514910	718680	36008	17967		21:59:44	22:00:48	00:01:04
193.48.83.165	<	81.180.86.38	2614	6	861	0	APRSF	393880	1238032	5252	4744	H323	18:26:43	22:59:54	14 days 04:33:11
193.48.83.68	>	128.142.38.80	513	6	44840	1094	APS	112	1817	2	4		22:00:01	22:00:01	00:00:00
193.48.83.165	>	134.158.159.85	2200	17	8842	9545		0	15942	0	351		21:59:43	22:00:13	00:00:30
193.48.83.165	>	134.158.20.192	789	6	0	861	APRSF	1232920	391936	4646	5214	H323	18:26:41	22:59:58	14 days 04:33:17
193.48.83.97	>	62.40.120.52	20965	6	49882	8090	ASF	104	52	2	1		22:00:01	22:00:01	00:00:00
193.48.83.97	<	188.184.161.86	513	1	8	0		28512	0	297	0	ICMP	03:09:53	23:00:00	1 day 19:50:07
193.48.83.97	>	188.184.161.86	513	1	0	0		0	28512	0	297	ICMP	03:09:53	23:00:00	1 day 19:50:07
193.48.83.97	>	62.40.120.52	20965	6	49883	8090	APS	60	317	1	2	HTTP	22:00:01	22:00:01	00:00:00
193.48.83.165	>	134.158.73.243	2200	17	8911	9305		0	16362	0	361		21:59:43	22:00:15	00:00:32

MÉTROLOGIE AVANCÉE

2 niveaux de détail & 80 graphs environ

Mise en corrélation :

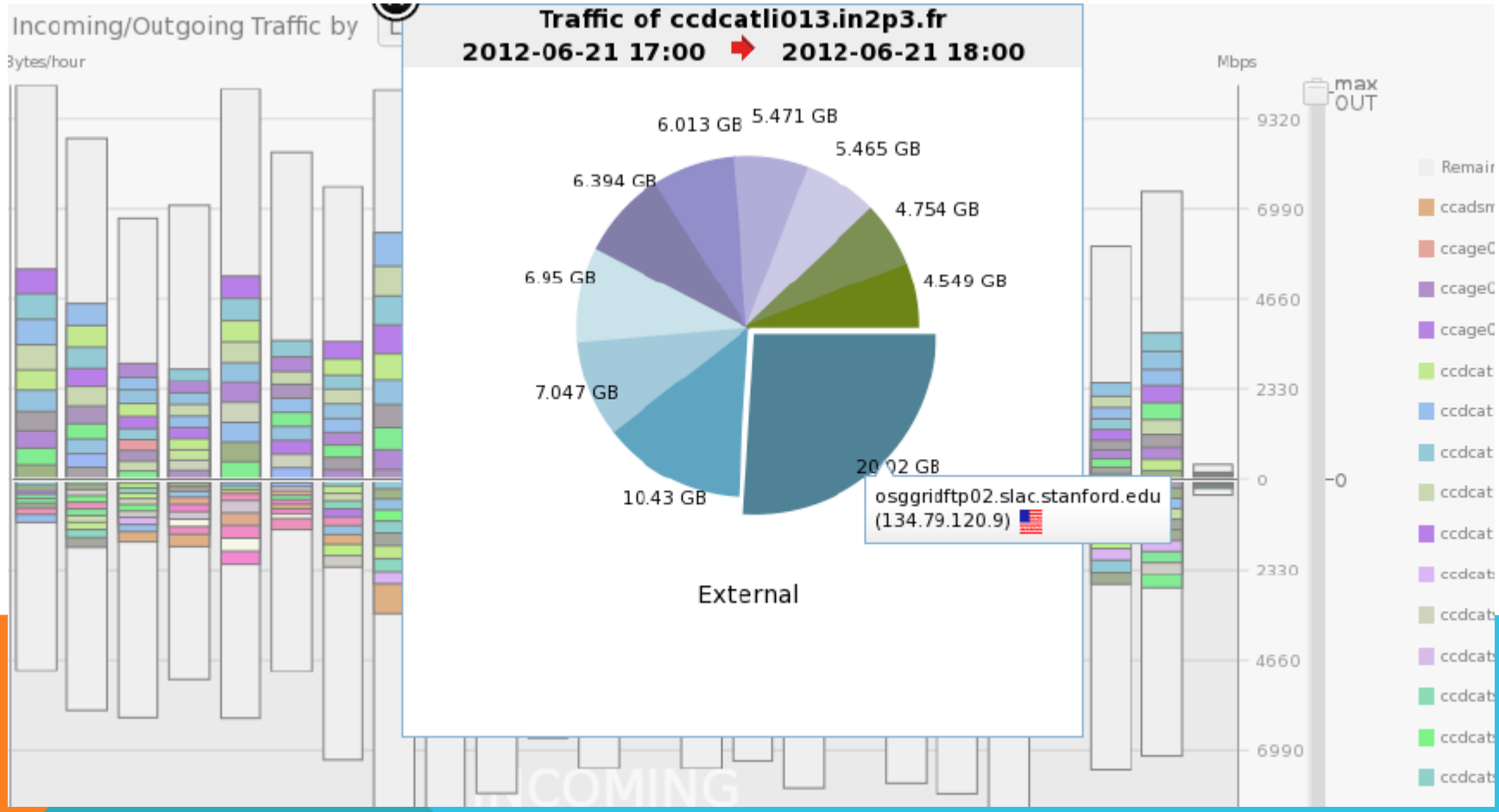
- chaque graphique de métrologie ⇔ flux

3 Types de graphique

- Temps réel (camemberts) de la dernière heure
- Horaire sur 24h
- Journalier sur 1 mois

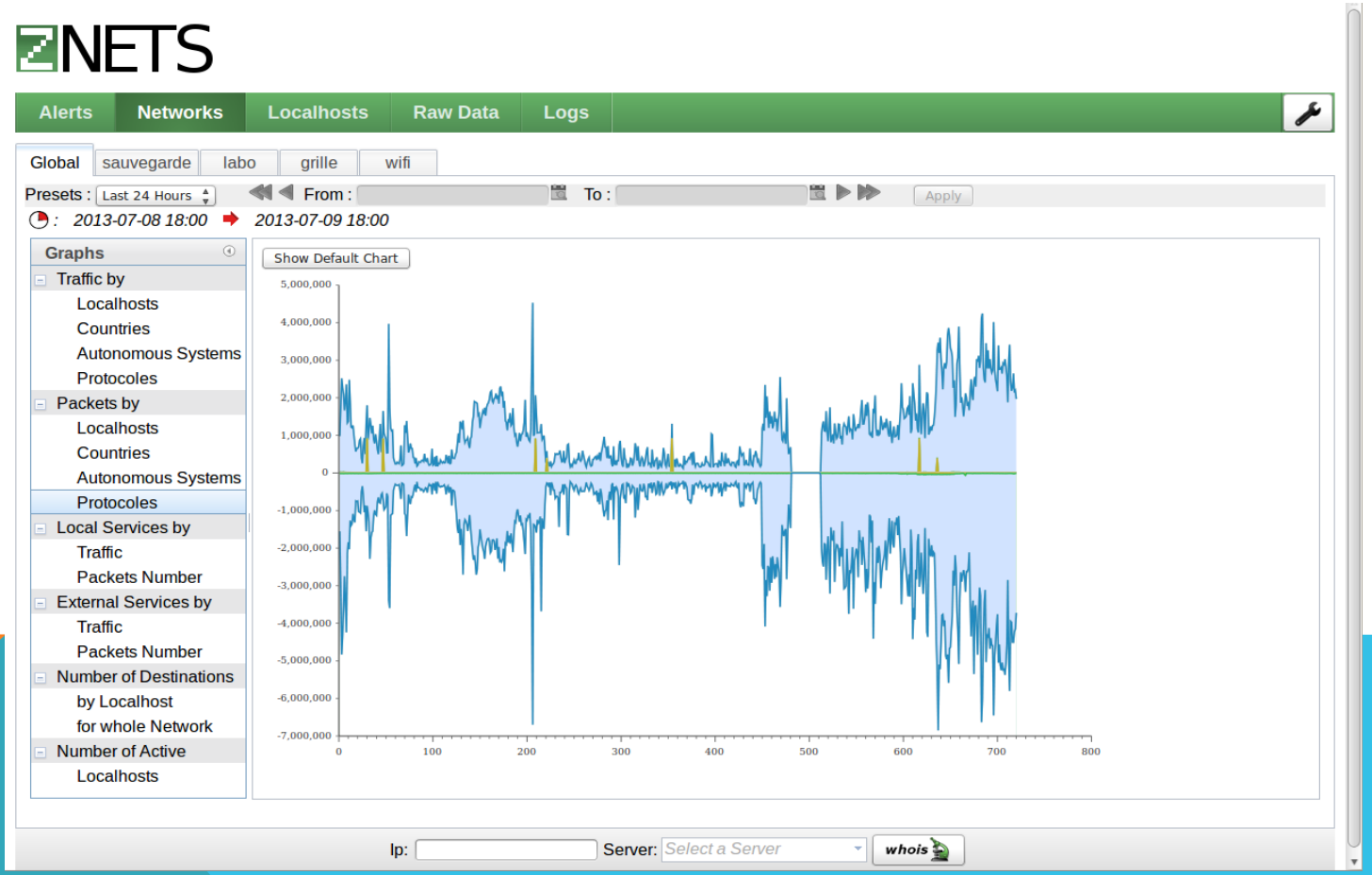
MÉTROLOGIE AVANCÉE

Sélection d'un trafic => 2è niveau de détail avec camembert



MÉTROLOGIE AVANCÉE

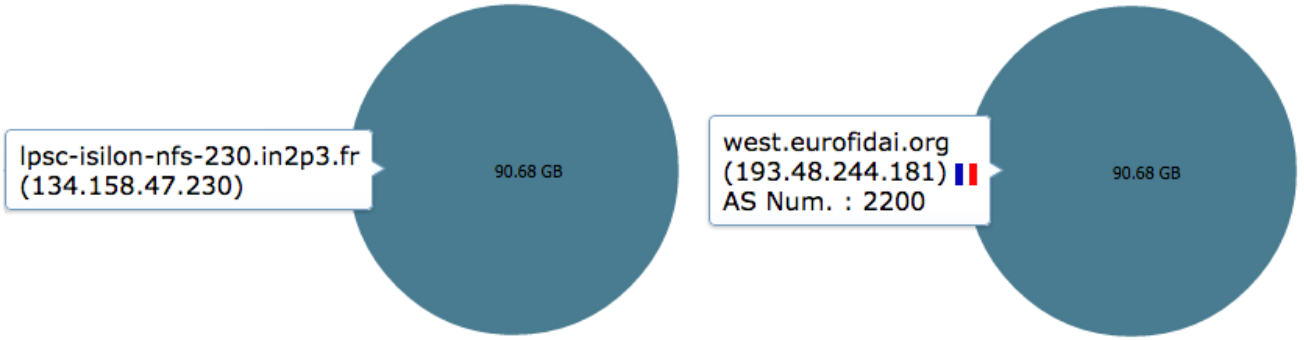
Nouveaux types de graphique: résolution 2 minutes

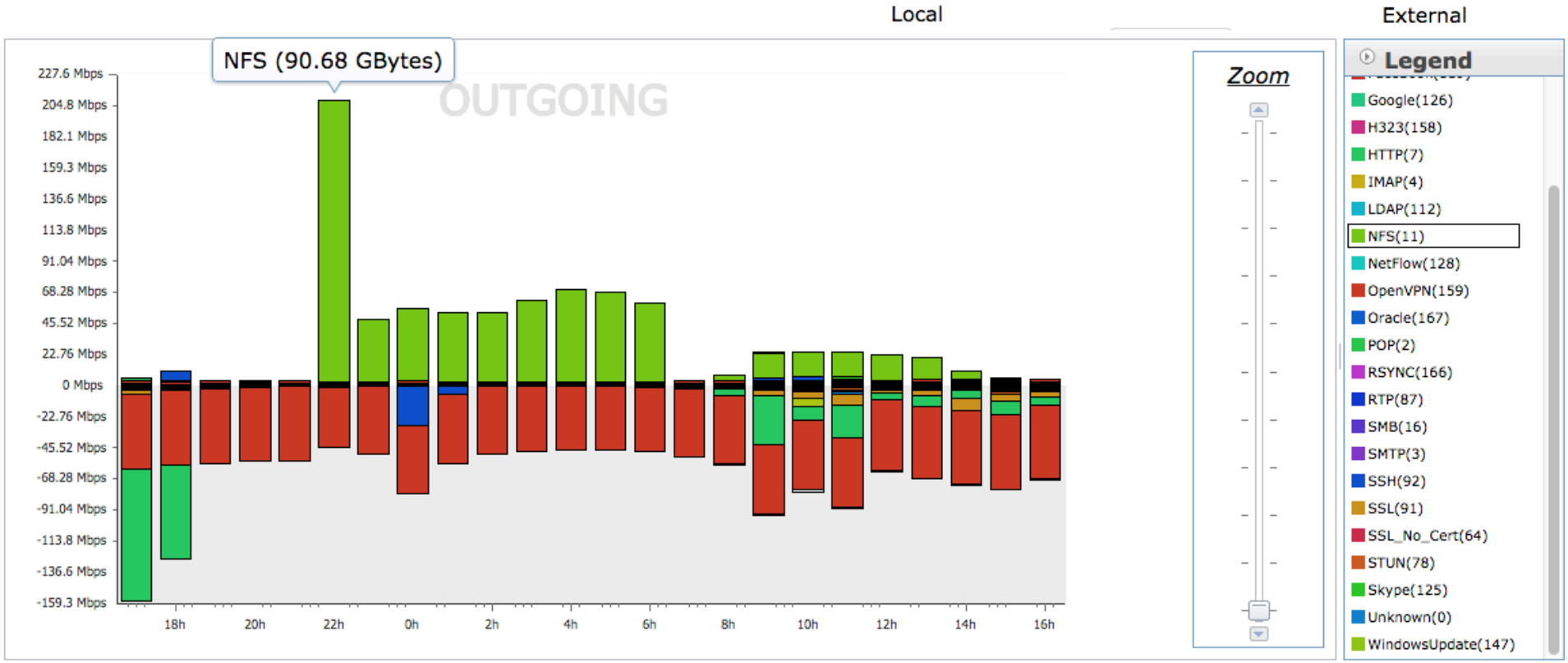


MÉTROLOGIE AVANCÉE

Nouveaux graphiques:

Par application détectée





INVENTAIRE DES ÉQUIPEMENTS COMMUNICANTS

Inventaire, détection d'OS, périodes de présence, dernier échange enregistré

Stockage des périodes de présence (résolution seconde)

Inventory

Ip Address	Name	Network	Last Activity	Mac Address	OS Name
... Aucun filtre appliqué					
192.168.20.21		eduroam	> 1 minute	6c:40:08:ae:e3:86	Mac OS X Mavericks64
192.168.20.22		eduroam	> 6 days 23 hours 43 minutes	f4:f5:a5:82:7c:66	
192.168.20.23		eduroam	> 1 day 5 hours 19 minutes	8c:3a:e3:19:7c:19	
192.168.20.24		eduroam	> 4 hours 42 minutes	b4:0b:44:0c:5f:a6	Android 5.0 Lollipop
192.168.20.25		eduroam	> 2 days 35 minutes	5c:51:4f:73:b7:34	Linux64
192.168.20.26		eduroam	> 1 week 3 days 9 hours 25 minutes	8c:3a:e3:19:7c:19	
192.168.20.27		eduroam	> 3 hours 13 minutes	84:db:ac:a6:b2:c0	
192.168.20.28		eduroam	> 1 week 33 minutes	34:bb:26:80:00:b9	Android 4.2 Jellybean
192.168.20.29		eduroam	> 2 days 22 hours 29 minutes	b4:07:f9:08:cd:6f	
192.168.20.30		eduroam	> 2 days 8 hours 24 minutes	04:e5:36:4f:de:e8	iPad
192.168.20.32		eduroam	> 22 hours 55 minutes	dc:9b:9c:22:0f:95	
192.168.20.33		eduroam	> 5 hours 22 minutes	2c:8a:72:5e:c2:9a	Windows 7 / Server 2008R264
192.168.20.34		eduroam	> 6 hours 18 minutes	ac:7b:a1:a3:ee:9f	Windows 7 / Server 2008R264
192.168.20.35		eduroam	> 6 hours	a4:17:31:1c:ab:ec	Windows 7 / Server 2008R2
192.168.20.36		eduroam	> 3 days 23 hours 35 minutes	68:94:23:8e:6d:31	Windows NT
192.168.20.37		eduroam	> 23 hours 5 minutes	9c:c1:72:91:9d:b8	Android 4.2 Jellybean
192.168.20.38		eduroam	> 21 hours 50 minutes	60:03:08:99:05:78	Mac OS X Mavericks64
192.168.20.39		eduroam	> 8 hours 32 minutes	00:73:8d:72:0c:ee	
192.168.20.40		eduroam	> 6 days 22 hours 49 minutes	1c:99:4c:f5:08:97	Android 3.x Honeycomb

DÉTECTION D'ANOMALIES

Outil pour la métrologie appliquée à la sécurité informatique

+

Process d'analyse des flux automatique => détecter compromissions

(=> assainir le réseau / sensibiliser les utilisateurs)

- logiciel malveillant (malware, virus…)
- vol d'information
- détournement de la ressource informatique intentionnelle ou pas (téléchargements, P2P, réseau Tor, utilisation d'un VPN)
- *attaques Ddos*
- *dysfonctionnements*

=> Liste d'heuristiques

DÉTECTION D'ANOMALIES

Alertes et Heuristiques:

- MAC SPOOFING ! DUPLICATED IP (pb de configuration ou… attaque sur le LAN!)
  Plusieurs Mac address, 1 seule IP

- MANY EXTERNAL RECIPIENTS (P2P, malware, virus)
  nb connections établies > seuil

- INCOMING SCAN (attaque à venir ? => ACL de routeur)
  Sens: de l'extérieur vers le LAN
  Des packets entrent, aucune réponse ou réponse TCP avec flag Reset / ICMP port unreachable

- OUTGOING SCAN (virus, nmap, …)
  Sens: du LAN vers l'extérieur
  Idem

- MULTIPLE HOSTS SCAN (virus, nmap, P2P…)
  Scan sortant vers plusieurs hôtes

DÉTECTION D'ANOMALIES

- OUTGOING TCP SYN FLOOD : (machine(s) locale(s) compromise(s) - DDOS)
  Nb flux TCP <= 2 paquets (1 envoyé, 0 ou 1 reçu sans Rst)

- INCOMING TCP SYN FLOOD (DDOS => filtrage ?)
  idem

- SUSPICIOUS DNS QUERY (compromission type DNSchanger)
  Requête envoyé à un serveur DNS qui n'appartient à la liste

- SUSPICIOUS HOSTS (malware, virus, streaming)
  Listes de réseaux suspects configurables/uploadable/…

- MAIL SPAM (Spam Bot)
  Nb connections SMTP(s) sortantes > seuil

DÉTECTION D'ANOMALIES

En mode sniffer (libpcap) uniquement :

- Malware URL Detected (malware/virus)
  Liste URL configurables/uploadable/…

- Fragmented header (Fragmented packet port scan attack …)
  Taille du paquet < taille de ses entêtes

- Recursive DNS server (pb configuration, DDoS)
  Réponse: Sens = OUTGOING
  standard Response && server is not authority for domain
  && server can do recursive queries

- Forbidden Application

DÉTECTION D'ANOMALIES

- Détection en Temps Réel
- Notification par Email / consultable (stockée DB)
- Exécution d'une commande externe possible
- Chaque alerte : activables / désactivables
- Seuils et exceptions configurables

- Alertes sont pertinentes (peu de faux positif)

- Amélioration à venir:
  - pour certains réseaux, extrapolation possible des seuils en fonction du trafic analysé au cours de la période écoulée

INFORMATION LIEN / LICENCE

Appel à contribution

Gratuit pour les établissements d'enseignement et de recherche

Période d'essai de 15 jours => numéro de série

Téléchargement:

www.znets.net

Disponibilité de la nouvelle version : mai 2015