SÉCURITÉ.ORG

# Flux Réseau et Sécurité

v1.01

**Yann BERTHIER**
Spécialiste Sécurité Systèmes et Réseaux
yb@bashibuzuk.net

**Nicolas FISCHBACH**
Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - http://www.securite.org/nico/

COLT

# Agenda

- Etat des lieux
- NetFlow 101
- Connaître son réseau
- Violation de la politique de sécurité
- Détection d'anomalies
- Scans
- Analyse post-mortem
- Conclusion

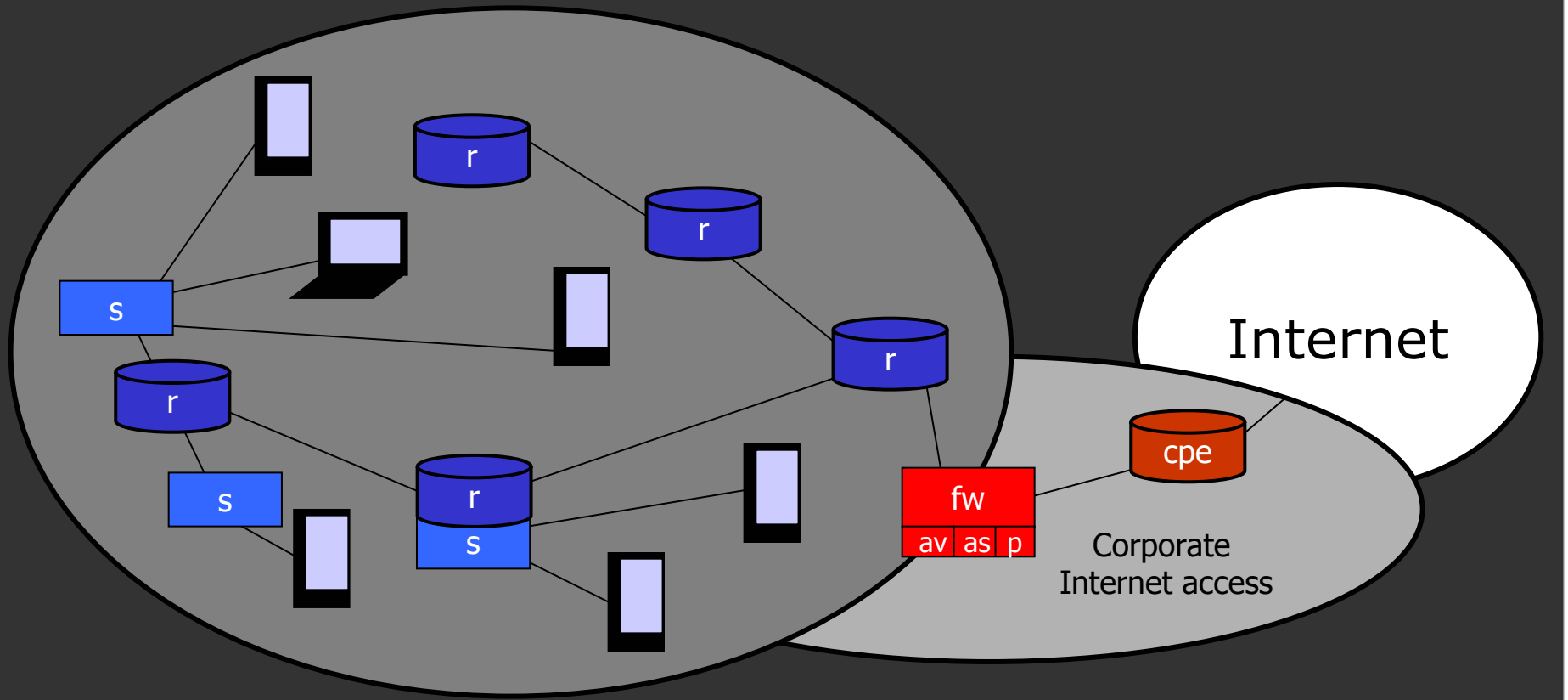
# Etat des lieux

- Porosité du périmètre
  - WiFi, 3G, RAS/VPN (employés, télémaintenance, etc)
- Opacité du réseau interne
  - Systèmes et applications non documentés
  - Réseau “plat” - pas de segmentation
- Vulnérabilité des ressources internes
  - Canaux cachés, chevaux de Troie, vers, virus, vulnérabilités clients (malware/spyware/navigateur)
  - De plus en plus de « wannabe power users »

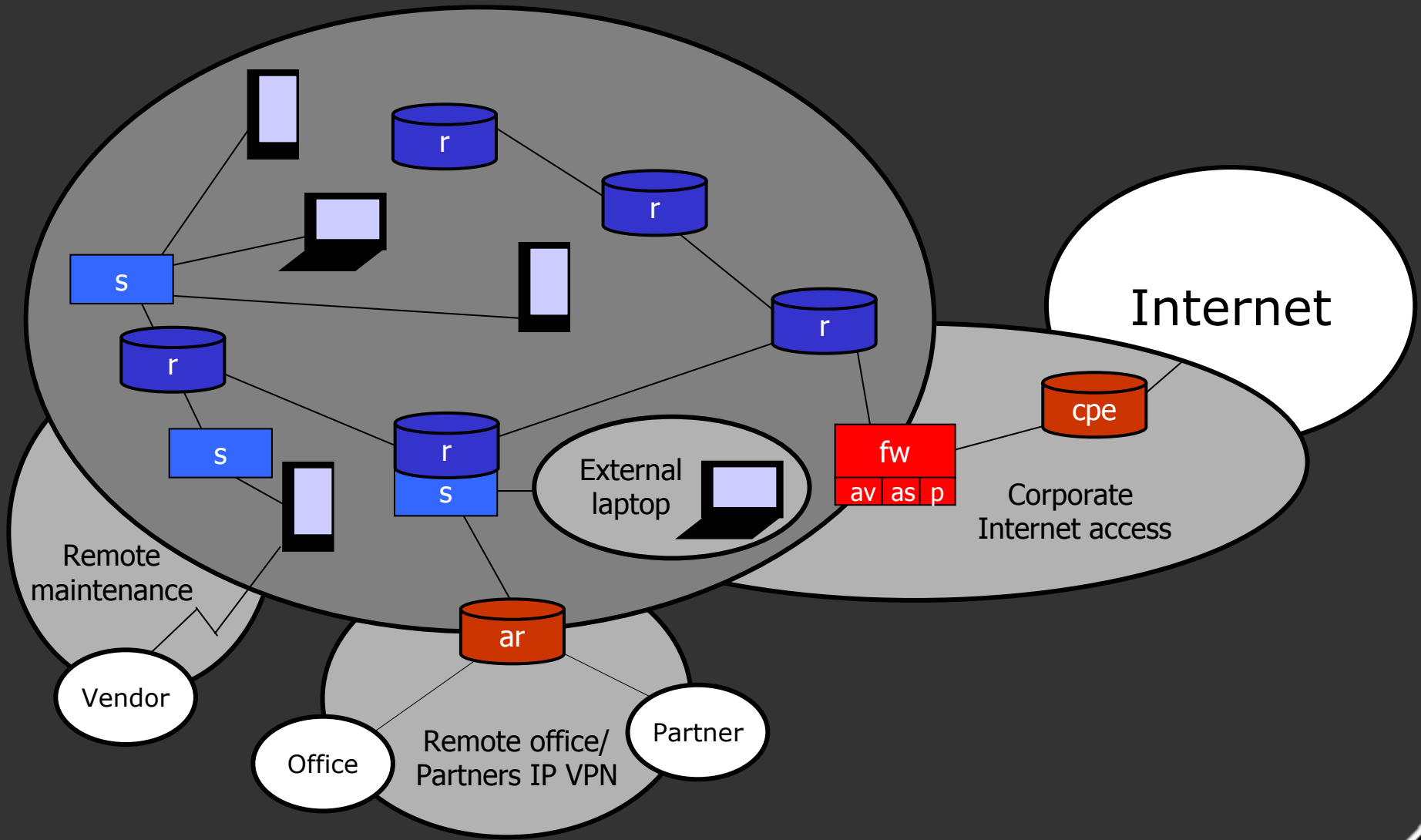
# Etat des lieux

- Limites des mesures de sécurité existantes
  - Les I{D,P}S n'ont pas tenu leurs promesses
  - De plus en plus de flux chiffrés : SSH, SSL, IPsec
  - Liens GE, 10GE

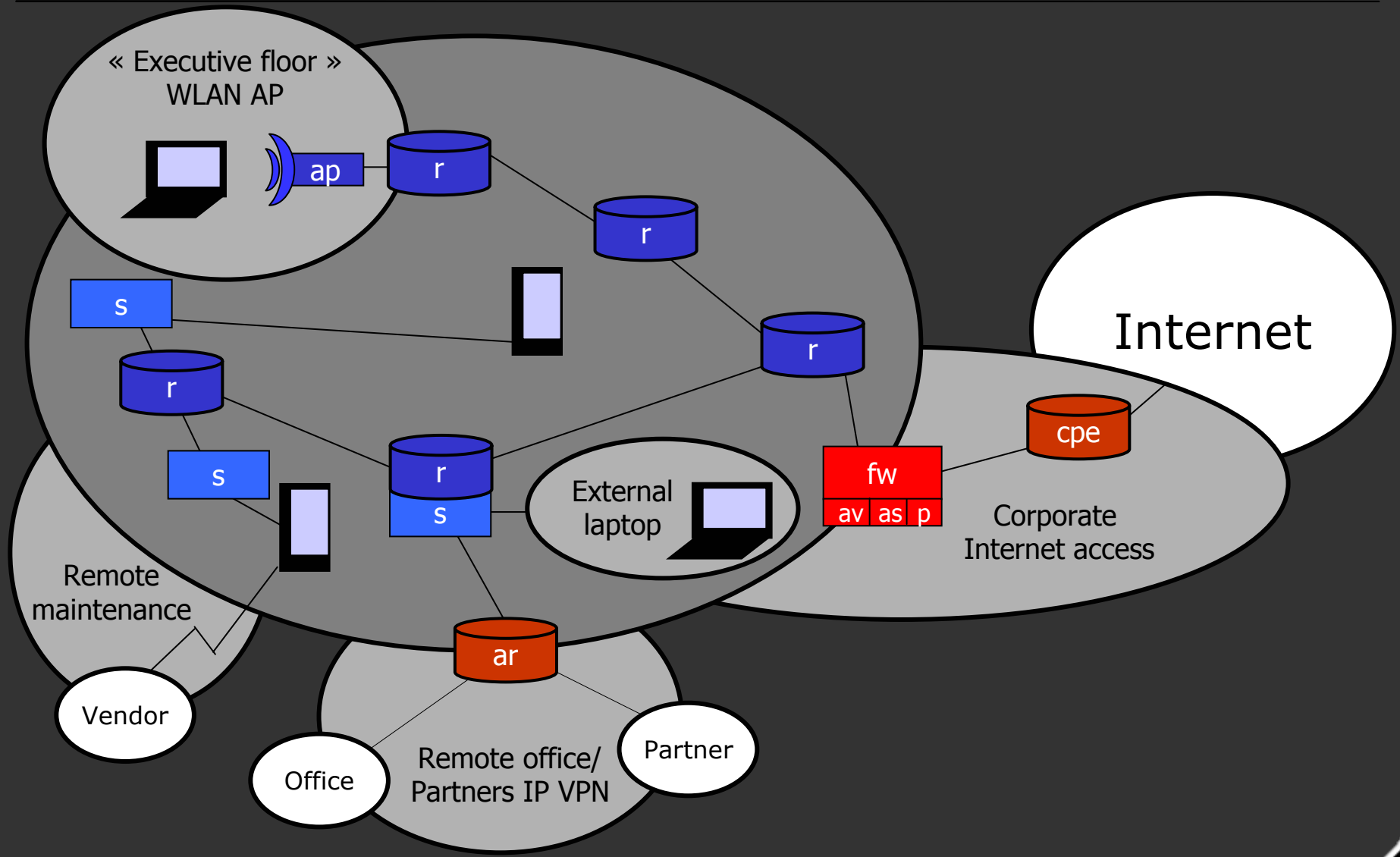
# La vision du responsable sécurité



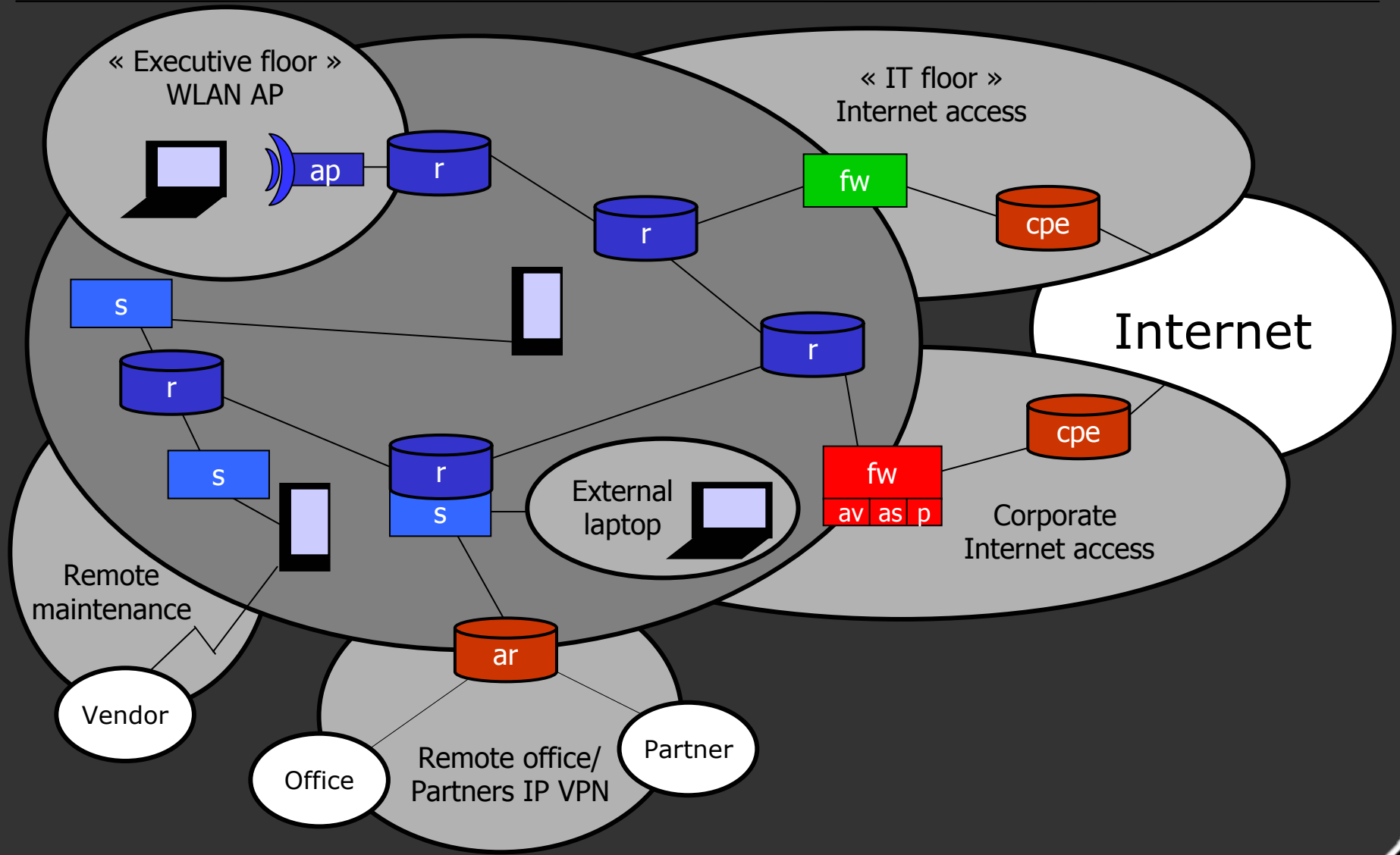
# La vision du RSSI



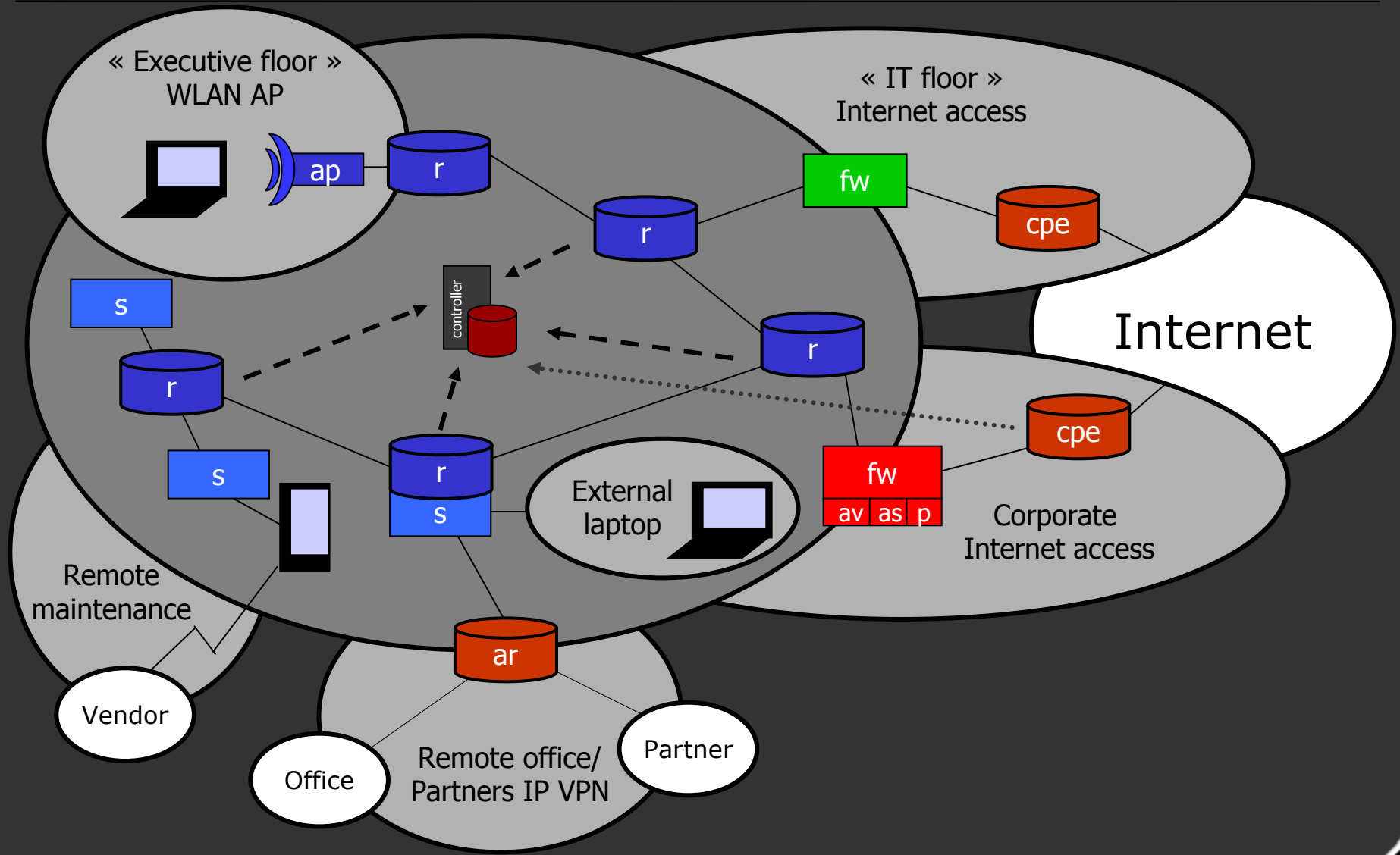
# L'étage de Direction



# La réalité


« Executive floor »
WLAN AP
ap
r
« IT floor »
Internet access
fw
cpe
Internet
r
s
r
r
cpe
s
r
s
External
laptop
fw
av
as
p
Corporate
Internet access
Remote
maintenance
ar
Vendor
Office
Remote office/
Partners IP VPN
Partner

# Collection des flux



# Flux réseaux

- Implémentation majoritaire : Cisco NetFlow
  - Plusieurs versions : v1 (ancienne), v5 (la plus fréquemment rencontrée), v7 (certains commutateurs, v8 (agrégation côté routeur), v9 (retenu par l'IETF comme base pour IPFIX)
- Nombreux autres formats
  - SFLOW, CRANE, LFAP, DIAMETER, Argus, …
  - Autres vendeurs

# NetFlow 101

- Exportés par les équipements de routage / commutation multi-niveaux
  - Historiquement pour améliorer le traitement des paquets (routage)
- Utilisés traditionnellement par le Billing/NetEng/NOC
  - Comptabilité / facturation des ressources, anticipation des besoins en BP, résolution de problèmes
  - Dénis de services
- Réutilisables par le SOC
  - Données, ressources, infrastructure
- OPEX / CAPEX

# NetFlow 101

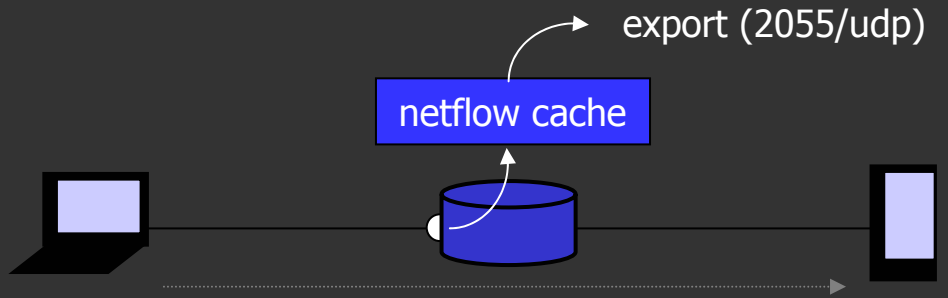
- Domestication du réseau
  - Topologie
  - Taxinomie des applications
- Détection d'anomalies
  - Ver, DoS, tunnels, scans lents
  - Compromission
- Analyse post-mortem

# Définition

- « Ensemble de paquets possédant des caractéristiques communes »
  - Champs clefs (7-tuple)
    - saddr, sport, daddr, dport, proto L3, ToS, input ifIndex
  - Autres champs exportés
    - Date de début, date de fin, nb d'octets, nb de paquets, output ifIndex, drapeaux TCP (sauf certaines combinaisons HW/SW), next hop
  - Champs optionnels (en fonction de la version)
    - Numéro d'AS, labels MPLS, ...

# Caractéristiques

- Unidirectionnel
- Ingress
- « Outrepasse » les ACL
- Flux stockés dans un cache mémoire
  - 64k entrées par défaut
  - Mis à jour à chaque paquet (tous les n si sampling)
    - Nouvelle entrée crée ou entrée existante mise à jour
    - Nb d'octets, nb de paquets (sommés), date de fin, drapeaux TCP (OR)



# Export des flux

- Mécanisme d'expiration
  - RST/FIN
  - 15 secondes (défaut) si flux inactif
  - 30 minutes (défaut) si flux actif
  - Cache plein
- A l'expiration, export vers un collecteur
  - UDP
  - En-tête suivie par 1 à 30 flux (48 octets)

# Echantillonnage

- Dépend de la combinaison SW/HW
- Déterministe (Sampled)
  - 1 paquet tous les n est passé au cache NetFlow
  - Rate tous les pics de trafic
- Aléatoire (Random Sampled)
  - Depuis la 12.3(2)T
  - Vue réaliste du trafic si le nombre d'échantillons est suffisant
- Solution « scalable »

# Considérations diverses

- Dédoublonnage
  - Flux exportés par plusieurs routeurs
- Agrégation
  - Flux longs
- Corrélation
  - Flux unidirectionnels
- Echantillonnage
  - Réduction de la charge CPU, mais “pertes”
    - OK: détection de DDoS
    - NOK: détection de la violation de politique

# Considérations de sécurité

- Pas de mécanisme de retransmission (sauf v9)
  - Mais numéro de séquence -> détection des pertes
- Pas de somme de contrôle, UDP
  - Protection du lien exporteur – collecteur
  - uRPF, ACL, TCP-Wrapper
- 48 octets pour un paquet de 24 octets
  - Opportunités de dénis de service

# Autres considérations

- Pas de charge utile – mais
  - Caractérisation du trafic (nb d'octets in/out, taille des paquets in/out, durée)
    - Trafic interactif vs trafic non interactif (eg HTTPS « régulier » vs tunnel SSL)
  - Flux chiffrés
  - Qui parle à qui
    - Combien de temps, a quelles heures
    - Volume de données échangées
    - Port + caractéristiques donne une bonne idée du type de données

# PCAP vs NetFlow

- Granularité maximale
- Charge utile
- Pas IP centrique
- Vue micro vs macro
  - Génération de flux à partir d'une trace
    - Argus, softflowd, « conversations » Ethereal
- Volume de données ...

# Configuration

- Export des flux

```
router (config-if)#  ip route-cache flow ! Par interface
router (config)# ip flow-export destination <addr>  <port>
router (config)# ip flow-export source loopback0
router (config)# ip flow-export version 5
```

- Configuration du cache

```
router (config)# ip flow-cache entries <1024-524288>
router (config)# ip flow-cache timeout active <1-60> (mn)
router (config)# ip flow-cache timeout inactive <10-600> (sec)
```

- Affichage du cache en temps réel

```
router # show ip cache flow
```

# Configuration

- Sampled

```
router (config)# ip flow-sampling-mode packet-interval 100
router (config-if)# ip route-cache flow sampled
```

- Random sampled

```
router (config)# flow-sampler-map RSN
router (config-sampler)# mode random one-out-of 100
router (config-if)# flow-sampler RSN
```

# Collecte, stockage & analyse des flux

- Collecte
  - Nombreux collecteurs : argus, flow-tools, nfdump/nfsen, nnfc, nfcd, netflow2mysql, flowc, flowd, netams
- Stockage
  - Fichiers plats vs base de données
- Analyse
  - Outils spécifiques + sort / awk / cut / head vs requêtes SQL

# Domestication du réseau interne (« connais ton réseau »)

- Serveurs, applications, utilisation du réseau
  - Segmentation
  - Validation de la politique de filtrage
    - Flux inattendus de chaque côté du firewall
  - Détermination d'une « baseline »
  - Détection d'anomalies

# Domestication du réseau

- 1) TopN, bottomN, averageN
  - Source, destination, port, durée, volume
- 2) Agrégation
- 3) Retour à 1)

| src_net | dst_net | sum_bytes | sum_packet | average_packet_size |
|---|---|---|---|---|
| 218.xxx.yyy.0/24 | 163.221.yyy.0/24 | 1207916 | 806 | 1498,66 |
| 163.221.yyy.0/24 | 216.xxx.yyy.0/24 | 520500 | 347 | 1500 |
| 64.xxx.yyy.0/24 | 163.221.yyy.0/24 | 439622 | 509 | 863,7 |
| 218.xxx.yyy.0/24 | 163.221.yyy.0/24 | 245748 | 171 | 1437,12 |
| 66.xxx.yyy.0/24 | 163.221.yyy.0/24 | 162572 | 114 | 1426,07 |
| 163.221.yyy.0/24 | 213.xxx.yyy.0/24 | 127877 | 86 | 1486,94 |
| 163.221.yyy.0/24 | 61.xxx.yyy.0/24 | 125312 | 90 | 1392,36 |
| 163.221.yyy.0/24 | 130.xxx.yyy.0/24 | 111888 | 78 | 1434,46 |
| 203.xxx.yyy.0/24 | 163.221.yyy.0/24 | 68024 | 48 | 1417,17 |

# Violations de la politique de sécurité

- Flux « inhabituels » (bottomN)
  - Nouvelles adresses IPs
  - Journaux DHCP, adresses MAC, port physique (SNMP)
  - Flux “liés” (auto-update et spyware)
    - Après allocation DHCP ou après authentification
    - Après la première communication réseau ou navigateur
- Horaires de bureau : poste de travail “actif” à 2h du mat’
- Flux depuis des serveurs non-liés aux applicatifs installés
- Flux vers des serveurs (ports non documentés)

# Détection d'anomalie

- Dénis de Service distribués
  - Augmentation massive de flux vers une destination (IP / port)
  - En fonction de l'environnement, pas besoin de baseline
  - Retour de flammes
- Chevaux de Troie
  - Ports identifiés, ports inattendus, flux longs, horaires inattendus

# Scans et vers

- Scans lents
- Scans distribués
- Vers
  - Scan du /24, /16, /8, BOGON, non-private
  - Propagation avec des IP sources forges
  - Identification: taille de la charge utile / port
- Difficile à mettre en évidence avec les moyens « classiques »
  - Evasion MS-RPC snort

# Ne pas confondre : scan et retour de flamme

- Où la victime n'est pas celle que l'on pense ...

| Date | Duration | Prot | Source | | Destination | | Pkt | Bytes | Flows |
|---|---|---|---|---|---|---|---|---|---|
| Dec 06 2004 16:11:20 | 38537 | TCP | aaa.bb.ccc.dd:80 | -> | www.xx.yyy.56:16250 | 2 | 80 | B | 2 |
| Dec 06 2004 16:12:11 | 38595 | TCP | aaa.bb.ccc.dd:80 | -> | www.xx.yyy.85:61504 | 4 | 160 | B | 2 |
| Dec 06 2004 16:42:27 | 40661 | TCP | aaa.bb.ccc.dd:80 | -> | www.xx.yyy.34:29441 | 3 | 120 | B | 2 |
| [...] | | | | | | | | | |
| Dec 08 2004 15:50:38 | 0 | TCP | aaa.bb.ccc.dd:80 | -> | www.xx.yyy.48:24378 | 1 | 40 | B | 1 |
| Dec 08 2004 16:17:11 | 0 | TCP | aaa.bb.ccc.dd:80 | -> | www.xx.yyy.78:12340 | 2 | 80 | B | 1 |

- 131 flux (après agrégation, 205 avant) sur un /24
- Drapeaux TCP
- www.xx.yyy.zz/24 est usurpé !

tcp_flags = 20 (RST-ACK)

# La durée importe

- Flux longs
  - Tunnels : HTTP(s), DNS, ICMP, etc.
  - Le ratio input/output (paquets, octets) est à surveiller
    - 10:1 pour une requête HTTP « classique » contre 1:1 pour une session interactive à travers un relais HTTP(s)
- Exercice : session HTTPS ou tunnel ?

| Date | Durée | Prot | Saddr:sport | | Daddr:dport | Paquets | taille |
|---|---|---|---|---|---|---|---|
| Nov 18 2004 14:53:10 | 9218 | TCP | 192.168.10.10:4822 | -> | 10.123.84.104:443 | 10299 | 1.4 MB |
| Nov 18 2004 14:53:10 | 9218 | TCP | 10.123.84.104:443 | -> | 192.168.10.10:4822 | 11547 | 3.7 MB |

# P2P

- Les protocoles « historiques » utilisent souvent des ports fixés (ou des plages de ports)
- Parfois : port de données == port de contrôle +/-1
  - Façon FTP
- Certains protocoles récents ont le détail de la session dans la charge utile
  - Surveiller la taille des flux, les topN (IP), le “comportement”

# Réponse et Analyse post-mortem

- Localisation
  - IP et source Netflow
  - Physique (MAC/port)
- Réponse
  - Désactivation du port
  - ACLs ou “trou noir”
- Analyse (une fois la problématique de stockage résolue)
  - On connait une des victimes (généralement)
  - Un historique des flux permet de connaître l'activité réseau vers et depuis cette adresse avant, pendant et après l'incident

# Conclusions

- Flux réseau et capture PCAP ne sont pas antinomiques
  - Stratégies complémentaires
  - Déploiement tactique / stratégique de sondes réseau
- Réutilisation des ressources (OPEX / CAPEX)
- Pas de solution clef en main pour l'analyse
  - (Hors solutions spécifiques)
  - Minimum syndical : on stocke, et on ressort les données lors d'un incident
    - Nombreuses heures de travail épargnées
- Preuve de concept: http://yeflow.rstack.org/

# Ressources

- Flow generators
  - NetFlow homepage <http://www.cisco.com/go/netflow>
  - Fprobe <http://fprobe.sourceforge.net/>
  - softflowd <http://www.mindrot.org/softflowd.html>
  - ng_netflow <http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netgraph/netflow>
  - Pfflowd <http://www.mindrot.org/pfflowd.html>

# Ressources

- Flow collectors
  - argus <http://qosient.com/argus/>
  - Cflowd <http://www.caida.org/tools/measurement/cflowd/>
  - Flow-tools <http://www.splintered.net/sw/flow-tools/>
  - Flowscan <http://www.caida.org/tools/utilities/flowscan/>
  - Nfdump <http://nfdump.sourceforge.net/>
  - Flowc <http://netacad.kiev.ua/flowc/>
  - Netams <http://www.netams.com/>

# Ressources

- Graphs
  - MTRG <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>
  - RRDTools <http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/>
- Network forensics
  - Smacq <http://smacq.sourceforge.net/>
- Misc
  - Glflow <http://freshmeat.net/projects/glflow/>
  - NetFlow v9 <http://www.ietf.org/rfc/rfc3954.txt>
  - Many more links here: http://www.switch.ch/tf-tant/floma/software.html