ORSENNA
NMS SERVICES

SUPERVISION
NETFLOW SFLOW

ORSENNA
NMS SERVICES

Netflow

- Créé par Cisco en 1996, Netflow est le standard de fait pour collecter des données IP opérationnelles.
- C'est un protocole de niveau 3 (Couche réseau)
- La différence avec les autres analyseurs de trafic (MRTG…) est que Netflow est tourné vers le niveau application et pas seulement en SNMP. Grâce à Netflow on peut dire que 40% de l'utilisation de la bande passante est utilisé pour le http, 20% pour…
- IpFix ➔ standardisation de la version 9 de Netflow

ORSENNA
NMS SERVICES

Netflow

- Chaque constructeur utilise les même caractéristiques que Netflow en l'appelant différemment :
  - Jflow ou cflowd chez Juniper Networks
  - NetStream chez 3Com/HP
  - NetStream chez Huawei Technologies
  - Cflowd chez Alcatel-Lucent
  - Rflow chez Ericsson
  - AppFlow chez Citrix

- Le concept majeur de Netflow est la notion de flux:
  - Adresses IP source et destination,
  - Protocole (TCP, UDP, ICMP,…),
  - ToS (Type Of Service)
  - Ports applicatifs (HTTP, SMTP, DNS,…),
  - Interfaces d'entrée et de sortie du routeur.

- Permet de voir les évolutions des flux pour permettre d'adapter la politique de QOS (Quality Of Service).

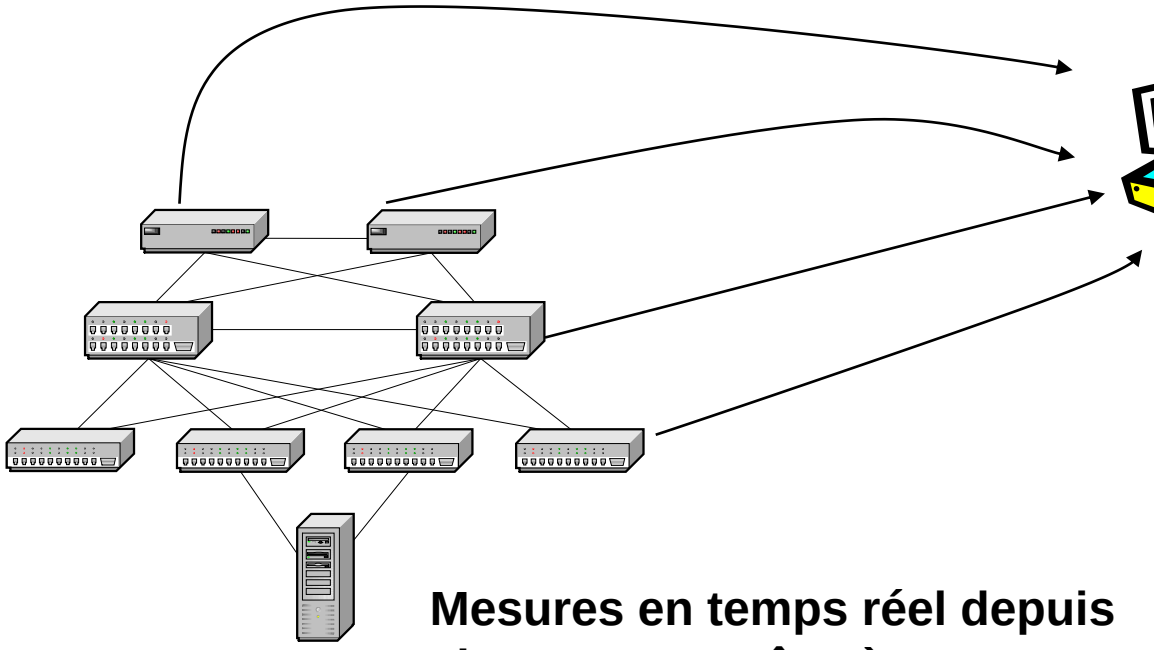
ORSENNA
NMS SERVICES

Netflow

- Netflow permet de :
  - Connaître l'utilisation du réseau par les applications
  - Comprendre par qui, quand, et où est utilisé le réseau
  - Mesurer l'efficacité du réseau et des ressources
  - Appréhender l'impact des changements au réseau
  - Détecter les anomalies et les vulnérabilités de sécurité de réseau
  - Auditer la conformité et les processus business
  - De répondre à des questions du genre:
    - Peut-on mettre en place la VOIP ?
    - Pourquoi mon application / serveur est lent ? …

- La technologie Netflow peut être utilisée dans une grande variété d'applications pour :
  - Surveillance en temps réel du réseau
  - Analyse des nouvelles applications et leur impact sur le réseau.
  - Capacity planning
  - Détection et classification d'incidents de sécurité
  - Accounting et facturation
  - Troubleshooting (lenteurs réseaux)

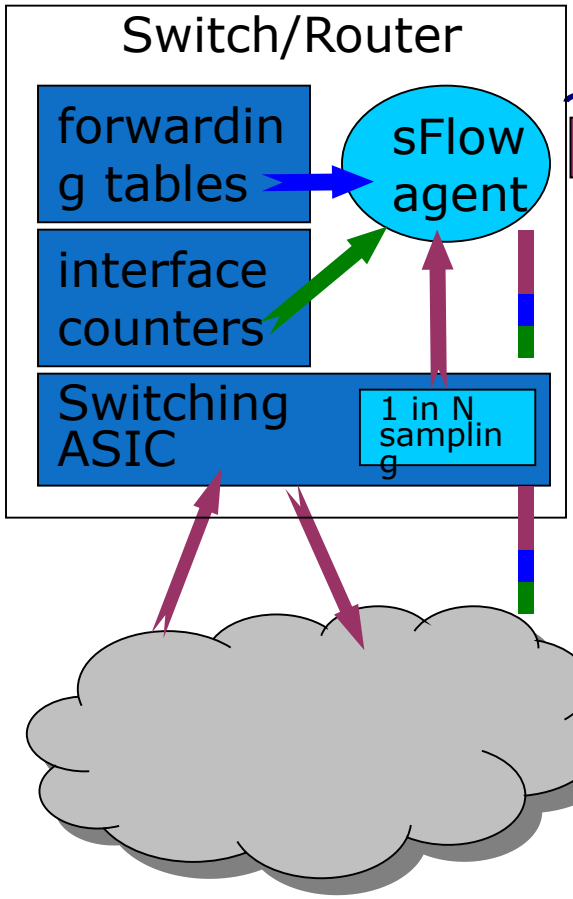
Netflow



Collecteur et analyseur NETFLOW

Mesures en temps réel depuis chaque port grâce à un agent présent sur l'équipement.

Netflow

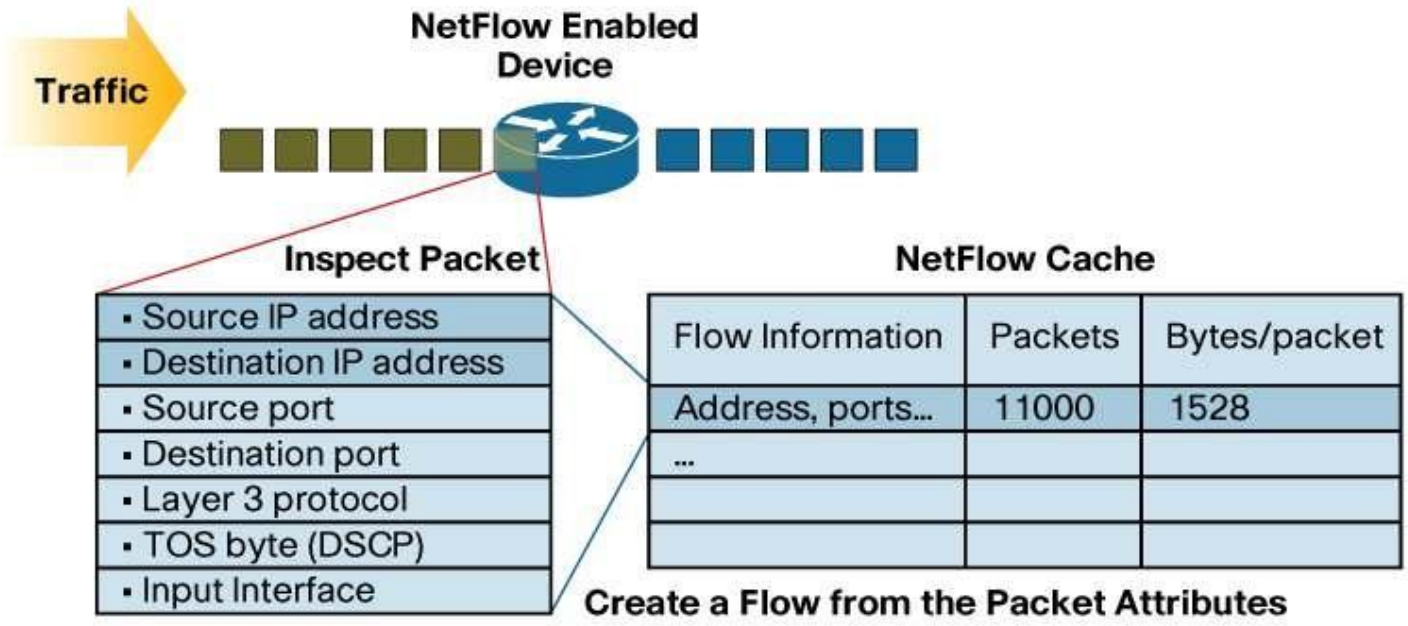


sFlow Datagram

packet header	src/dst i/f	sampling parms	forwarding	user ID	URL	i/f counters
eg 128B		rate pool	src 802.1p/Q dst 802.1p/Q next hop src/dst mask AS path communities localPref	src/dst Radius TACACS		

NetFlow / sFlow Collector & Analyzer

Netflow


Traffic
NetFlow Enabled Device
Inspect Packet
▪ Source IP address
▪ Destination IP address
▪ Source port
▪ Destination port
▪ Layer 3 protocol
▪ TOS byte (DSCP)
▪ Input Interface
NetFlow Cache
Flow Information
Packets
Bytes/packet
Address, ports...
11000
1528
...
Create a Flow from the Packet Attributes

Netflow

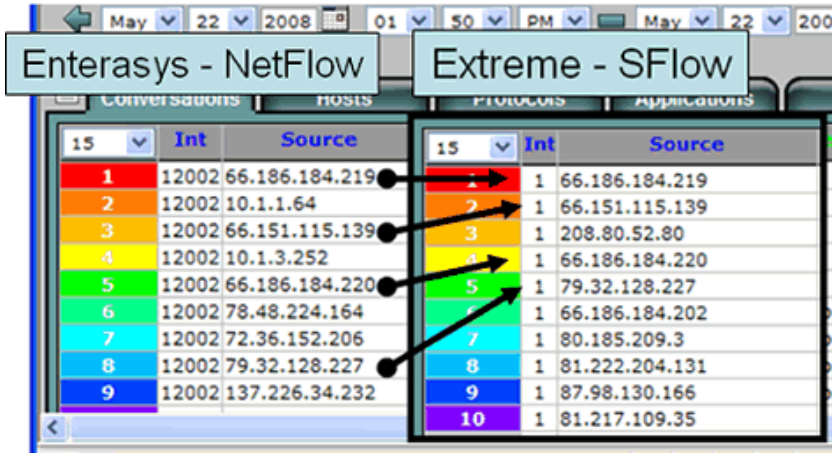
- Le routeur compte le nombre de paquets et d'octets reçus pour chaque flux
- Dès qu'il reçoit un paquet, le routeur créé une nouvelle entrée si le flux n'est pas connu ou bien incrémente le compteur du flux si il est déjà présent.
- La mémoire du routeur n'étant pas infinie, il faut faire le tri. Pour cela le routeur retire automatiquement du cache un flux lorsque celui-ci a été inactif pendant un certain temps (inactive timeout) et le supprime s'il a été actif trop longtemps (active timeout).
- Le routeur se sert de la date du dernier paquet reçu pour ce flux et la compare à la date actuelle pour connaître l'inactivité de celui-ci.
- Lorsqu'un flux a expiré et est supprimé du cache, il peut être exporté vers une machine de collecte.

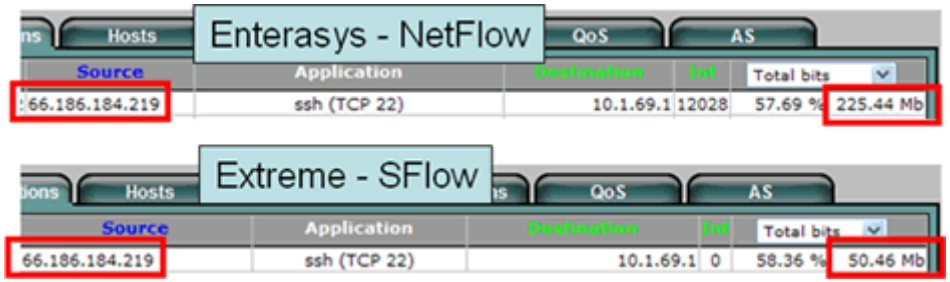
Netflow

- Il existe 10 versions du protocole Netflow.
- Les versions 2, 3, 4, 6 => pas sorties sur le marché (interne chez Cisco).
- La version 5 est la plus utilisée sur les routeurs (seulement pour IPv4)
- La version 7 est spécifique aux Switchs Catalyst.
- La version 9, elle supporte l'IPv6 ainsi que le MPLS.
- La dernière version la version 10: Connue comme IPFIX. Champs définis par les utilisateurs, champs en longueur variable

Netflow Vs Sflow

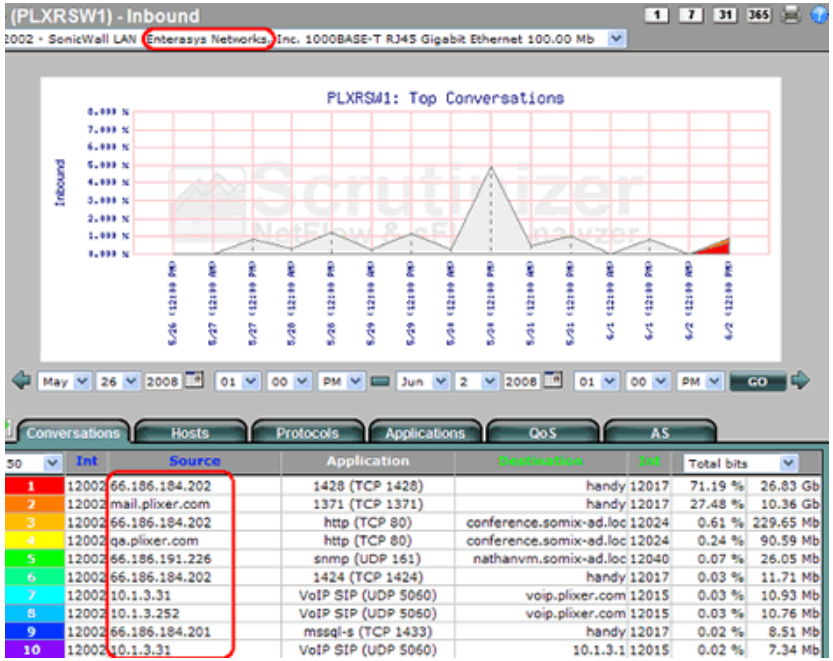
- Sflow réalise un échantillonnage (choix personnel => N paquet).
- Cela consomme donc moins de charge CPU sur les équipements.
- Moins de bande passante consommée.



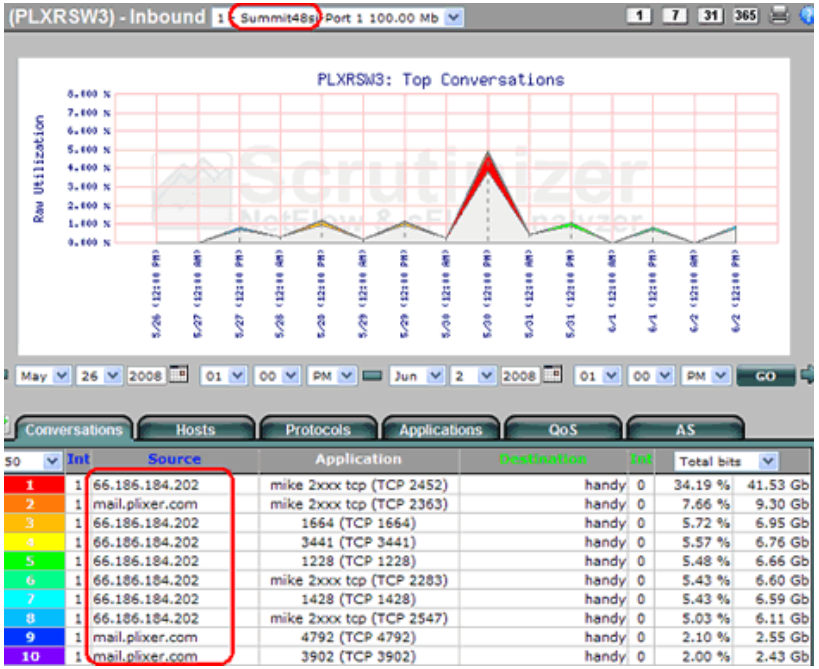


Netflow Vs Sflow

- Il est donc moins précis que NetFlow à court terme. Néanmoins sur une grande période, nous retrouverons les mêmes résultats.



NetFlow



SFlow

Netflow Vs Sflow

- Lequel faut-il utiliser et à quel moment ?
  - NetFlow : analyse précise du réseau => analyse de sécurité par exemple
  - Sflow : permet d'avoir une vue sur l'utilisation des ressources du réseau.

- Nous avons donc ensuite différents logiciels et équipements en fonction des besoins de chaque personne :
  - WUG NetFlow monitor et Orion Netflow Traffic Analyser : outils de reporting / statistiques.
  - Scrutinizer et flow analytics : logiciel dédié à l'analyse de flux réseau.
  - Fluke network : équipement dédié à l'analyse de flux réseau.
  - Observer : Analyzer réseau => capture le flux.

ORSENNA
NMS SERVICES

Equipements

- Equipements supportant NetFlow:
  - **Adtran** NetVanta 3200, 3305, 4305, 5305, 1524, 1624, 3430, 3448, 3130, 340, and 344
  - **Cisco** ASA Firewall (IOS version 8.2) ; Catalyst série 4000/4650/4500/ 6000/6500/7600/7000 NX-OS ; Cisco 800, 1700, 2600, 1800, 2800, 3660, 3800, 7200, 7300, 7500 ; Cisco 10000, 12000, CRS-1
  - **3Com** : 8800 Series Switches
  - **Enterasys** Router
  - **ESX Server** avec Wmware
  - **Extreme** Networks Router : Alpine 3800 series, BlackDiamond 6800 series, BlackDiamond 8800 series, BlackDiamond 10808, BlackDiamond 12804C , BlackDiamond 12804R ,Summit X450 Series , Summit i series
  - Juniper Router
  - Mikrotik Router
  - Riverbed Steelhead Appliance
  - Vyatta Core 6 software

- Equipements ne supportant pas NetFlow ➔ besoin d'un agent matériel ou logiciel:
  - Cisco 2900, 3500, 3660, 3750, Nexus 5000
  - Netgear
  - Bintec
- Pour la configuration: http://www.plixer.com/products/netflow-sflow/configure-netflow-sflow.php

ORSENNA
NMS SERVICES

Equipements

- Equipements supportant SFlow:
  - 3Com : 4800G Family
  - AlaxalA Networks : AX7800R ; AX7800S ; AX7700R ; AX5400S
  - Alcatel-Lucent : OmniSwitch 6850 ; OmniSwitch 9000 series
  - Allied Telesis : SwitchBlade 7800R series ; SwitchBlade 7800S series ; SwitchBlade 5400S series
  - Blade Network Technologies : HP 10Gb Ethernet BL-C Switch ; HP 1:10Gb Ethernet BL-C Switch ; HP GbE2c Layer2/3 Ethernet Blade Switch
  - Brocade : BigIron series ; FastIron series ; IronPoint series ; NetIron series ; SecureIron series ; ServerIron series
  - Comtec Systems : !-Rex 16Gi & 24Gi & 24Gi-Combo
  - Dell : PowerConnect 6200 series ; PowerConnect 8000 series
  - D-Link : DGS-3600 series
  - Enterasys : G-Series ; SecureStack B3 ; SecureStack C3
  - Extreme Networks : Alpine 3800 series ; BlackDiamond 6800 series ; BlackDiamond 8800 series ;BlackDiamond 10808 ; BlackDiamond 12804C ; BlackDiamond 12800R Series ; Summit X150 Series ; Summit_X250e Series ;

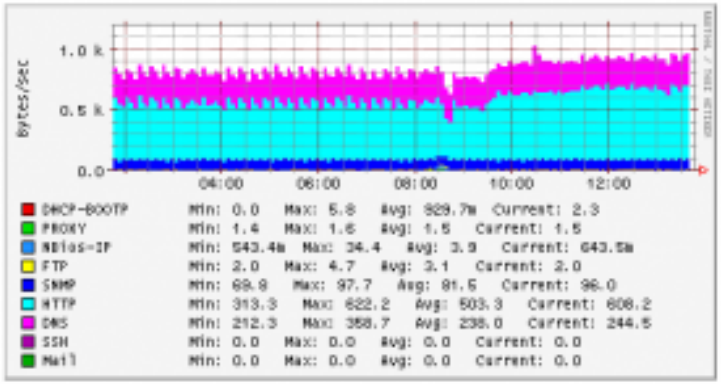
    Summit X450 Series ; Summit i series
  - Force10 Networks : C series ; E series
  - H3C : H3C S5800 Series ; H3C S5820X Series ; H3C S7500E Series Switches ; H3C S9500E Series Switches ; H3C S12500 Series Data Center Switches ; H3C MSR 20-1X Series Routers

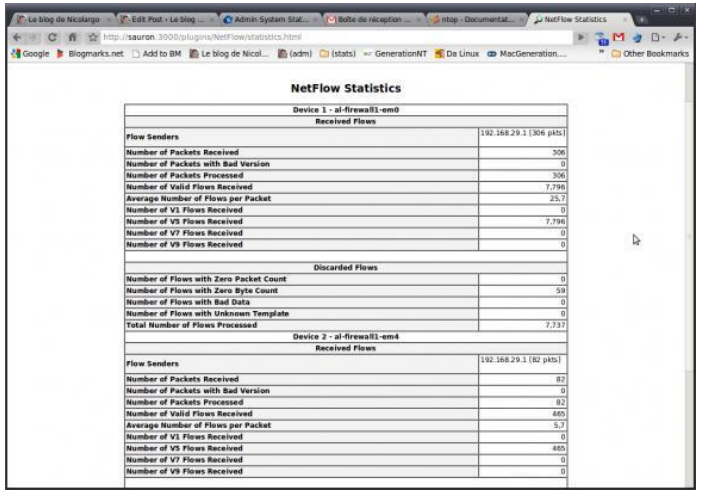
Equipements

- Equipements supportant SFlow:
  - Hewlett-Packard : ProCurve 2610 series ; ProCurve 2800 series ; ProCurve 2900 series ; ProCurve 2910al series ; ProCurve 3400cl series ; ProCurve 3500yl series ; ProCurve 4200vl series ; ProCurve 5300xl series ; ProCurve 5400zl series ; ProCurve 6200yl series ; ProCurve 6400cl series ; ProCurve 6600 series ; ProCurve 8212zl ; ProCurve 9300m series ; ProCurve Routing Switch 9408sl ; ProCurve Wireless Edge Services xl Module ; ProCurve Wireless Edge Services zl Module ; ProCurve Access Point 530
  - Hitachi : GR4000 ; GS4000 ; GS3000
  - IBM : c-series ; g-series ; m-series ; r-series ; s-series ; x-series ; J08E and J16E ; J48E
  - InMon Corp. : Virtual Probe
  - Juniper Networks : EX3200 series ; EX4200 series ; EX8200 series
  - MRV : OptiSwitch-MR series
  - NEC : IP8800/R400 series ; IP8800/S400 series ; IP8800/S300 series ; IP8800/S3640 series ; IP8800/S3640 ER series ; IP8800/S3630 series ; IP8800/S2400 series
  - NETGEAR : GSM7352S-200 ; GSM7328S-200
  - Open vSwitch : Open vSwitch
  - Vyatta : Vyatta 514 ; Vyatta 2500 series ; Vyatta 3500 series ; Vyatta Core (VC) Routing & Security Software ; Vyatta Virtual Router, Firewall, VPN
  - XRoads Networks : EdgeXOS

Ntop

- **Qu'est-ce que Ntop ?**
  - Ntop est un outil libre.
  - C’est un collecteur Nflow/IPfix
  - Il capture et analyse les trames d’une interface.
  - Il permet d’observer une majeure partie des caractéristiques du trafic entrant et sortant.
  - Stockage des statistiques au format RRD

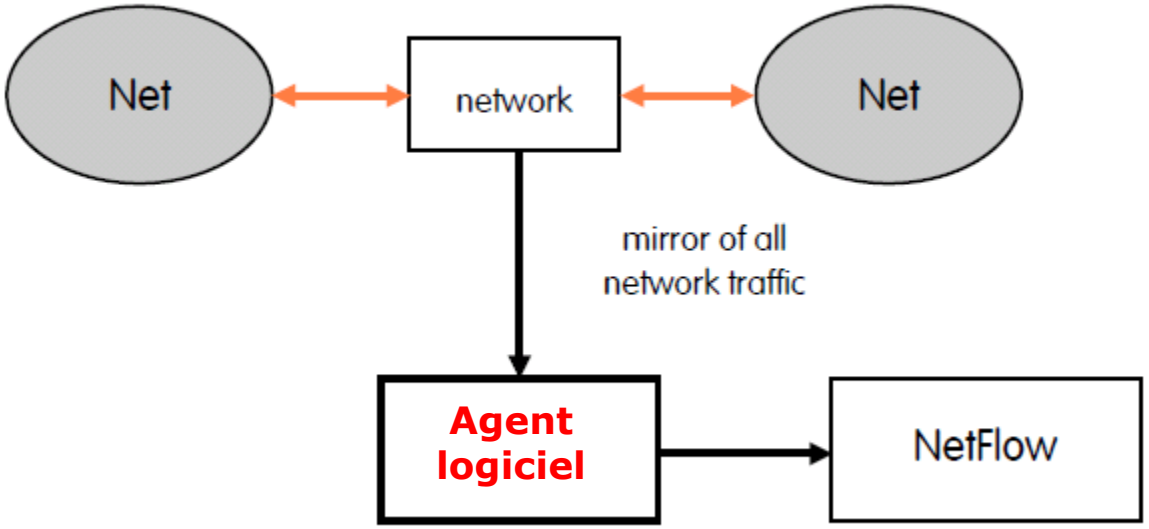




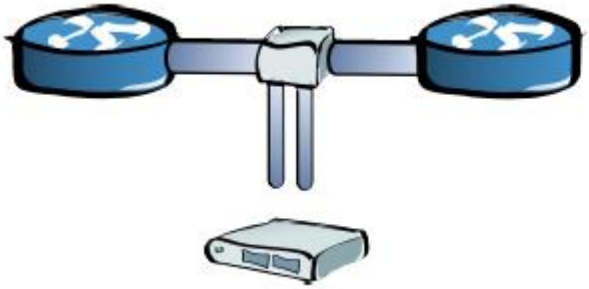
- **Logo :** ntop
- **Lien :** http://www.ntop.org/

Agent Logiciel / Matériel

- **Pourquoi prendre un agent matériel plutôt qu'un agent logiciel ?**
  - Un ordinateur peut souvent être déplacé, ce qui rendra l'agent indisponible.
  - Moins de maintenance à réaliser.
  - Besoin d'un PC dédié, ce qui implique un clavier, un écran…



Agent Logiciel / Matériel



- **TAP mode ➔ cela peut se représenter comme un Y, le flux arrive sur la branche du bas, puis se divise en deux, une partie reste sur le réseau tandis que l'autre va vers l'agent matériel.**
- **SPAN mode ➔ Mirroring d'un port vers un autre.**
- **RSPAN mode ➔ Mirroring d'un port du routeur vers un port d'un autre routeur.**

Nprobe

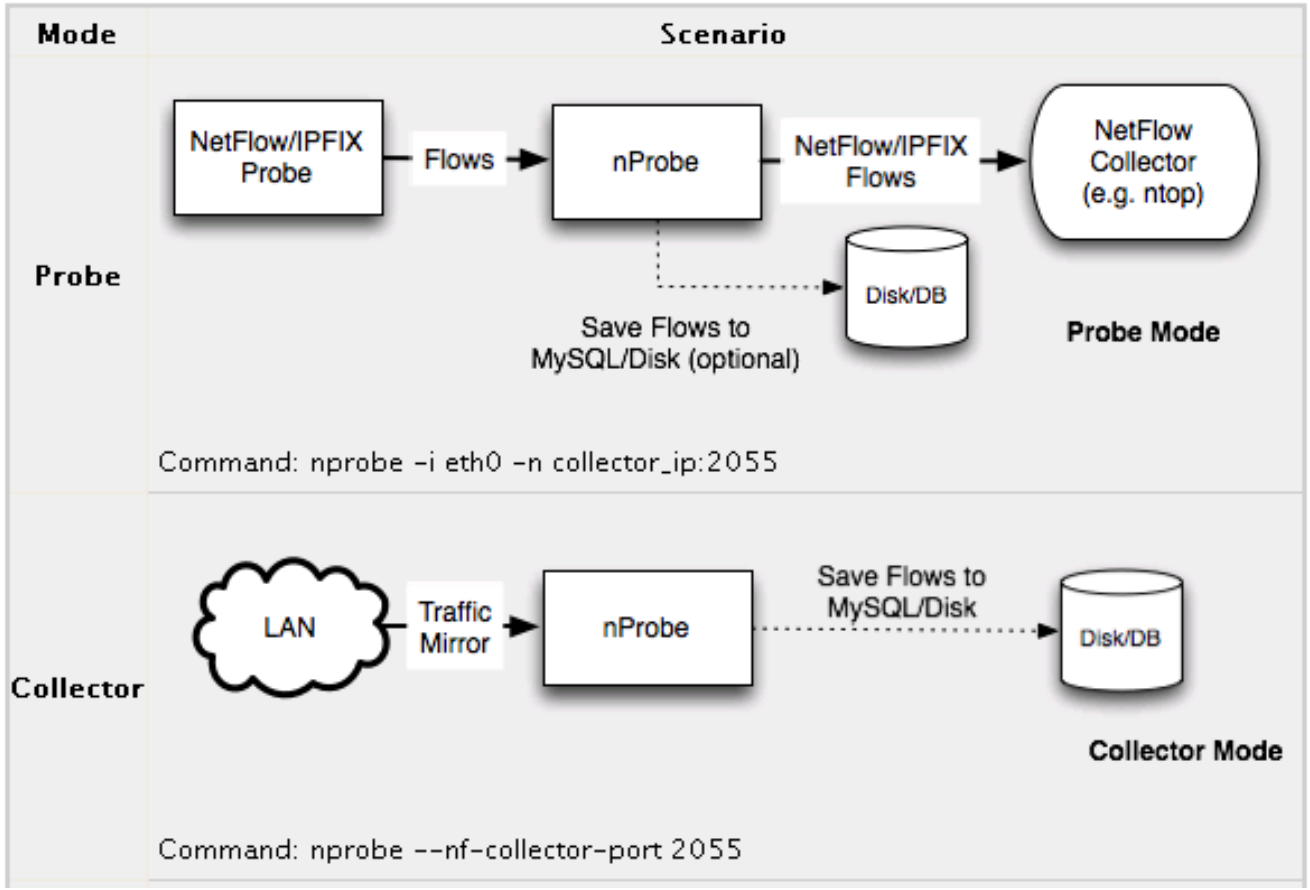
- **Qu'est-ce que Nprobe ?**
  - C’est un agent logiciel.
  - Idéal pour les devices qui n’incorporent pas de façon hardware une sonde Netflow.
  - Il peut analyser le trafic et générer un flux standard « Netflow ».
  - Disponible pour Windows, Unix et Mac.
  - Supporte IPv4 et Ipv6.
  - Possibilité d’être en mode collecteur de flux and en proxy.
  - Analyse de trafic VoIP.
  - Totalement configurable par l’utilisateur.
  - Compatible avec les collecteurs des constructeurs Fluke, Cisco, Dartware, AdventNet, Plixer, SolarWinds…

- **Logo :** ntop

- **Lien :** https://www.ntop.org/products/netflow/nprobe/

Nprobe

- **Qu'est-ce que Nprobe ?**



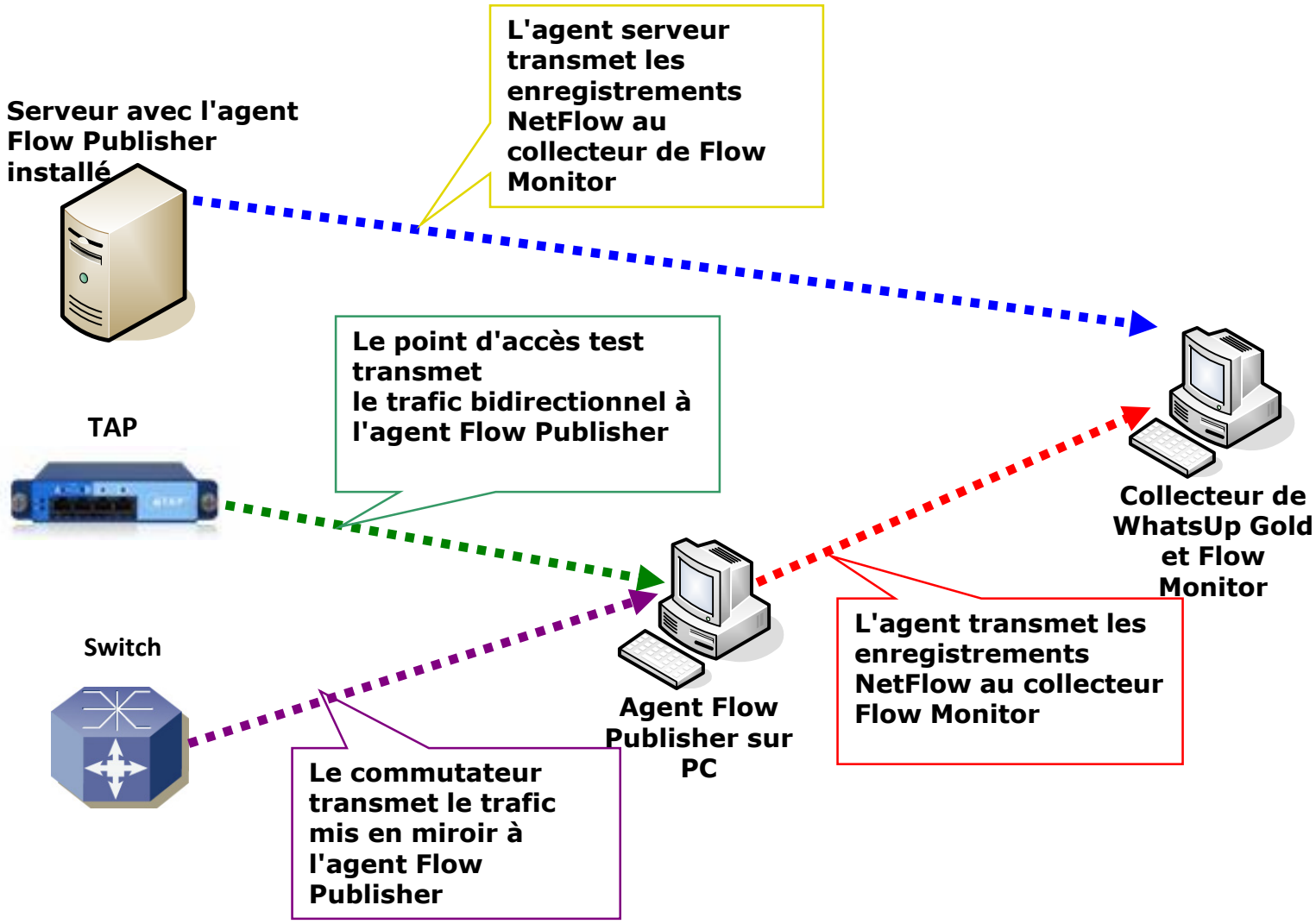
WhatsUP Flow Publisher

- **Qu'est-ce que Flow Publisher ?**
  - C’est un agent logiciel.
  - Il permet l'analyse du trafic réseau pour chaque périphérique et segment du réseau.
  - De déterminer les utilisateurs, applications ou sources de trafic qui consomment de la bande passante.
  - Recevoir des alertes en temps réel lorsque les paramètres de trafic surveillés dépassent des seuils définis.
  - Assurer que les applications de l'entreprise disposent de toute la bande passante nécessaire.
  - Accéder à plus de 40 rapports mobiles et Web pour l'établissement d'une base de référence et l'analyse.
  - Crée des enregistrements compatibles NetFlow v1, v5 ou v9 à partir du trafic brut

- **Logo :** WhatsUp Flow Publisher

- **Lien :** http://fr.whatsupgold.com/products/flow_publisher/

WhatsUP Flow Publisher



FlowMon

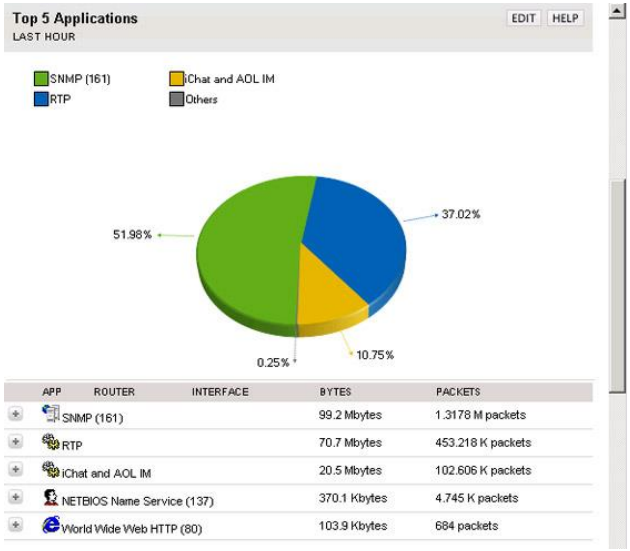
- **Qu'est-ce que FlowMon ?**
  - C’est un agent matériel.
  - Il est basé sur les technologies NetFlow V5/V9
  - Donne des informations sur qui communique avec qui ? Pendant combien de temps ? Quel protocol ? Combien cela prend de bande passante ?
  - Une solution pour tout types de réseau.

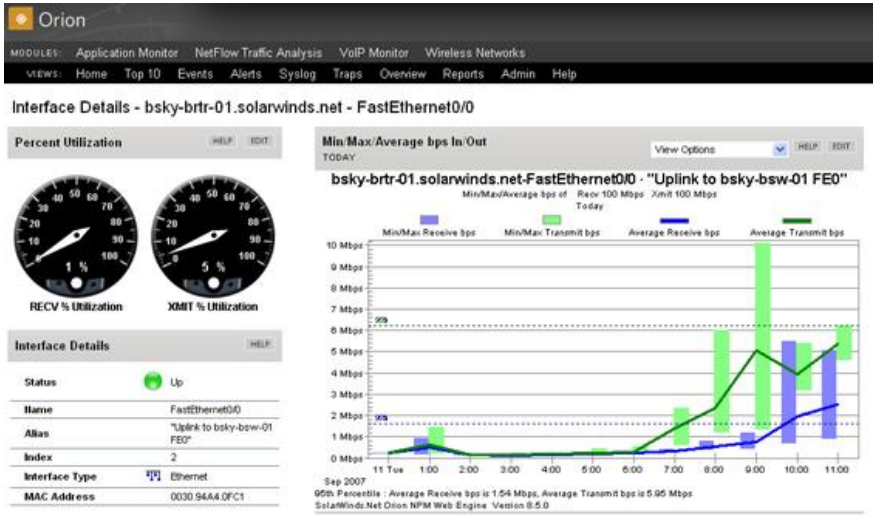
- **Logo :** inveaTECH
- **Lien :** https://www.flowmon.com/en/solutions/use-case

Solarwinds – Orion Netflow Traffic Analyser

- **Qu'est-ce que Netflow Traffic Analyser ?**

  C’est un outil de reporting / statistique.





- **Logo :**

- **Lien : http://www.solarwinds.com/products/orion/nta/**

PRTG - Traffic Grapher

- **Qu'est-ce que Traffic Grapher ?**

  Il est doté d'un serveur web intégré => permet d'accéder aux graphiques et aux tableaux à partir d'un navigateur web.

  Utilise trois méthodes de surveillance :

  - SNMP pour les compteur de trafic.
  - Analyse des paquets réseau entrants/sortants qui transitent sur la carte réseau d'un ordinateur => capture de paquets.
  - Analyse des paquets Cisco NetFlow

  Fiabilité de la surveillance du réseau (plus de 100 000 utilisateurs chaque jour)

  Classification du trafic réseau en fonction de l'adresse IP, du protocole et d'autres paramètres

  Fonctionne avec la plupart des commutateurs, routeurs, pare-feu et autres équipements réseau

  Poste de surveillance permettant la supervision de plusieurs milliers de sondes

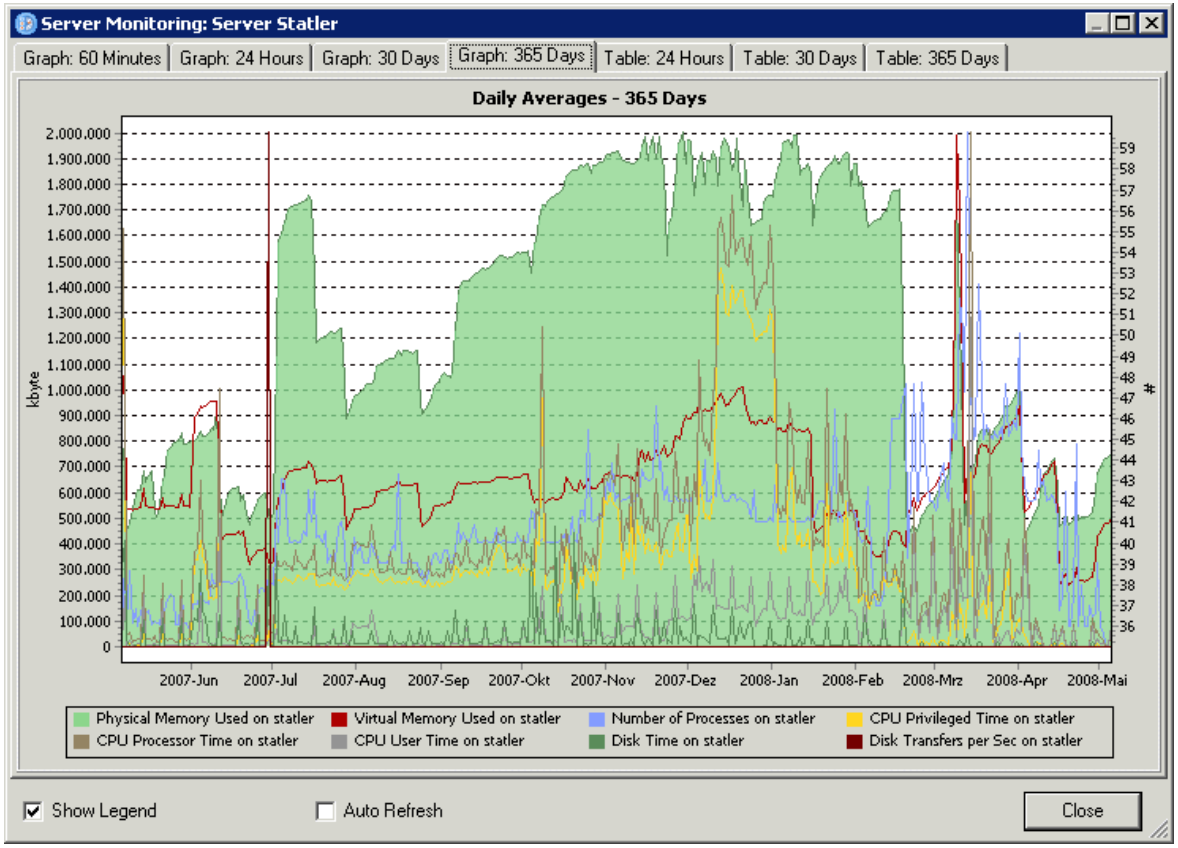
  Version Freeware disponible pour les petits réseaux

- **Logo :**

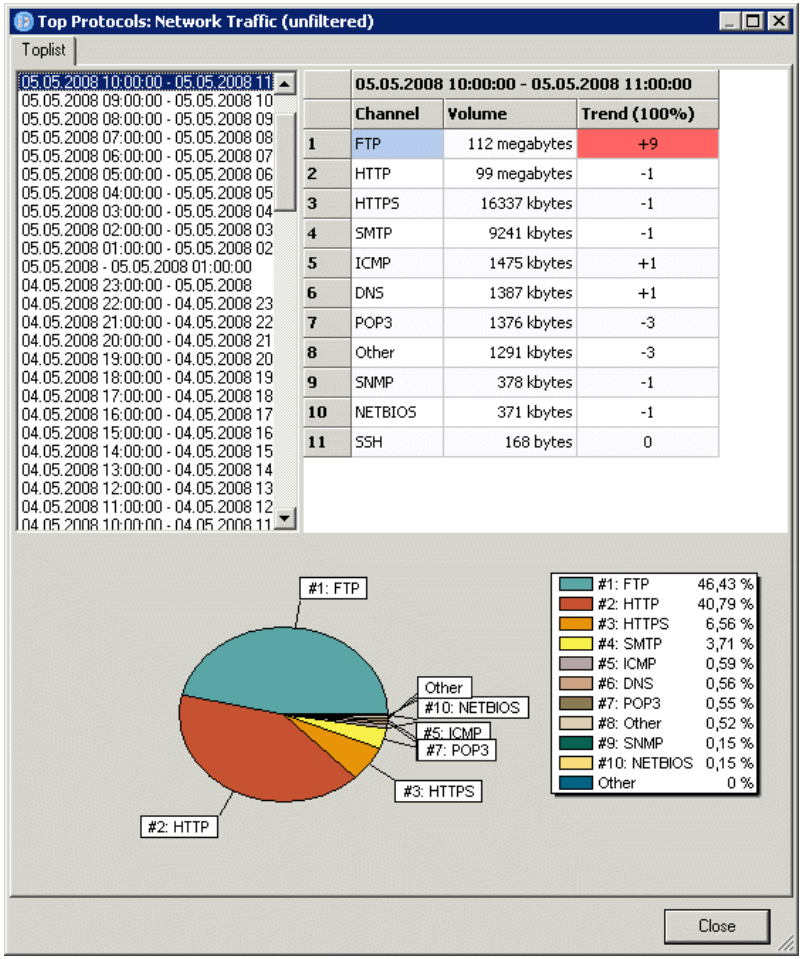
- **Lien : http://www.paessler.com/**

ORSENNA
NMS SERVICES

PRTG - Traffic Grapher



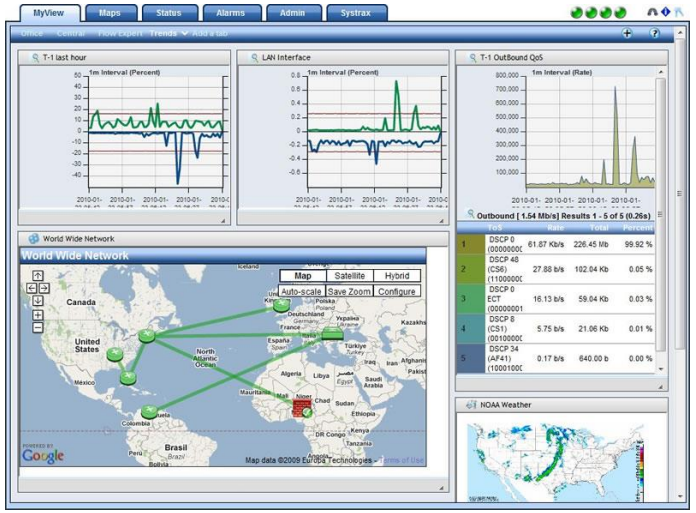
PRTG - Traffic Grapher



Plixer - Scrutinizer

- **Qu'est-ce que Srutinizer NetFlow & sFlow Analyser ?**

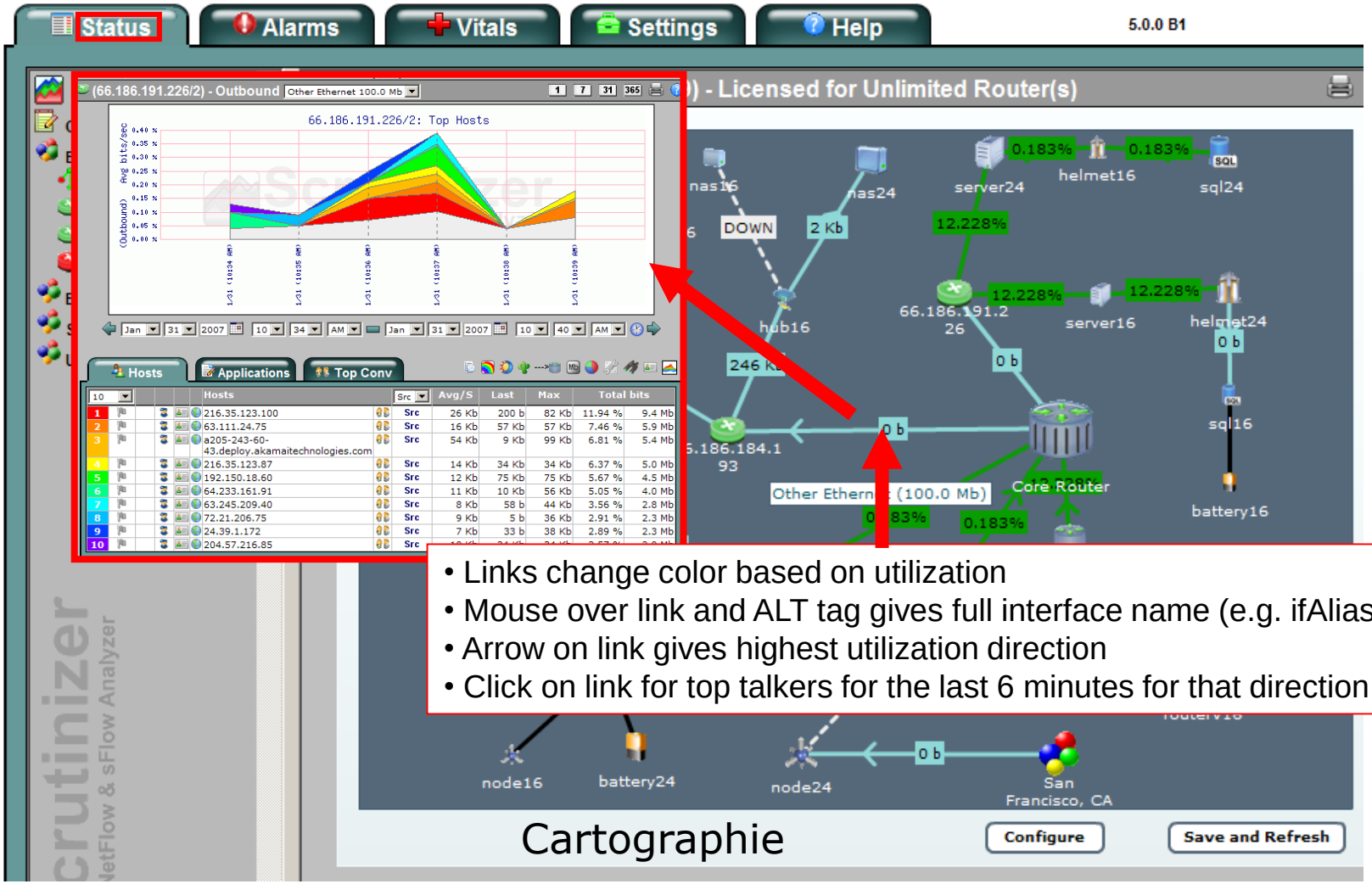
  - Logiciel dédié à l'analyse de flux (fonctions précises et poussées).
  - Logiciel permettant de fournir des informations concernant le réseau (bande passante, graphique, répartion des charges…).
  - Scrutinizer peut recevoir des flux d'un nombre illimité d'interfaces.
  - Scrutinizer s'intègre avec le logiciel WhatsUp Professional d'Ipswitch.



- **Logo :** Scrutinizer™ v7 NetFlow & sFlow Analyzer

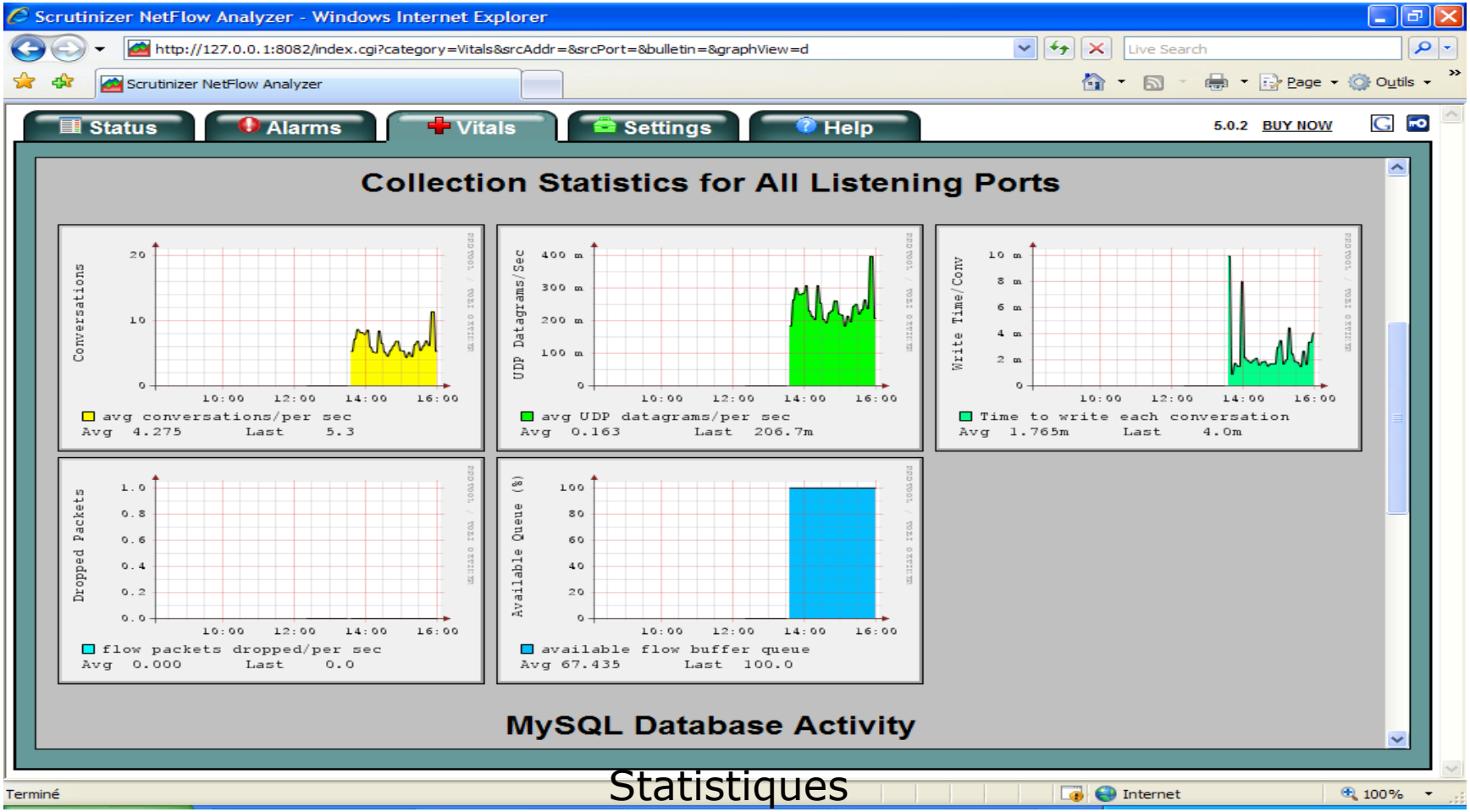
- **Lien :** http://www.plixer.com/products/scrutinizer.php

Plixer - Scrutinizer



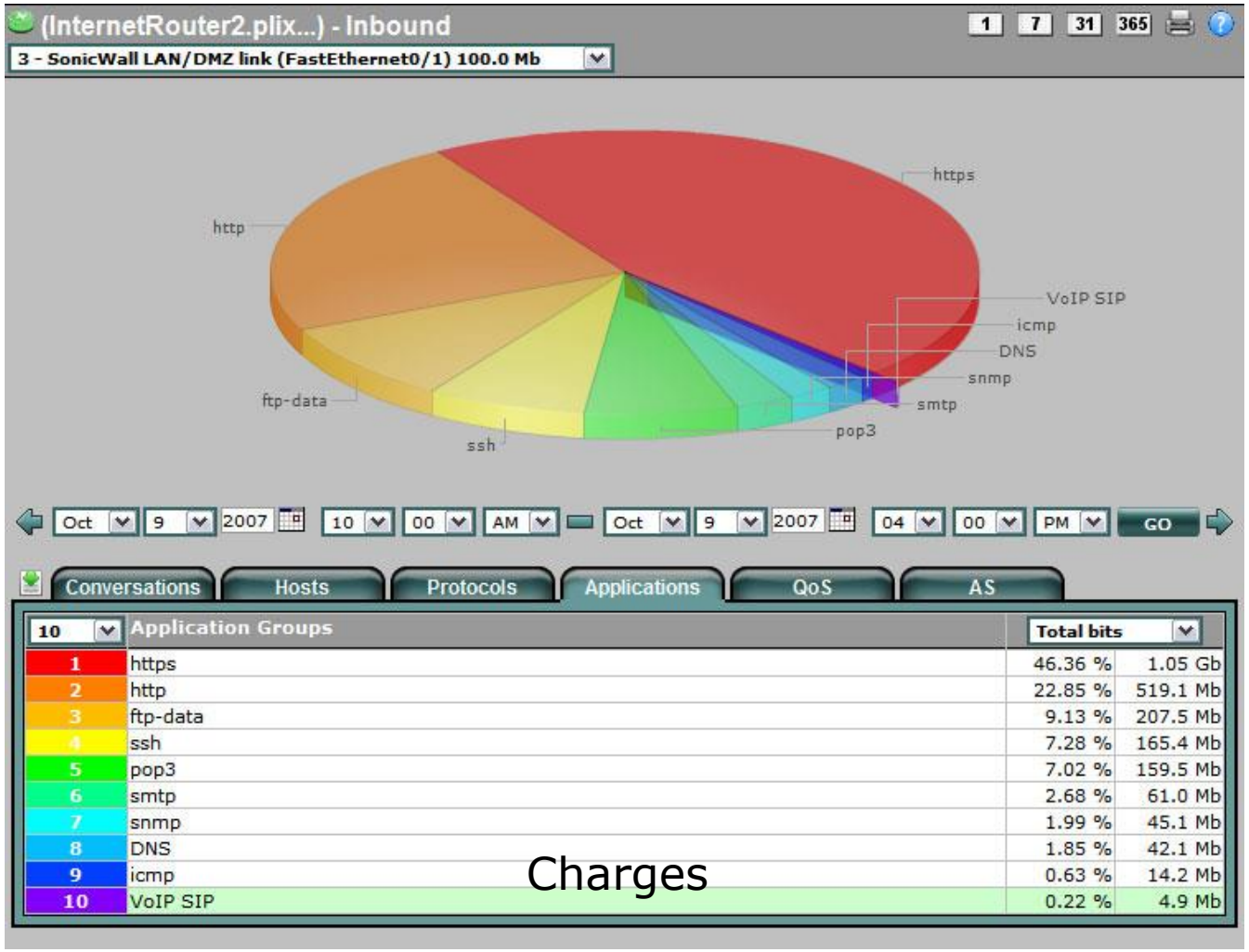
- Links change color based on utilization
- Mouse over link and ALT tag gives full interface name (e.g. ifAlias)
- Arrow on link gives highest utilization direction
- Click on link for top talkers for the last 6 minutes for that direction

Plixer - Scrutinizer



Statistiques

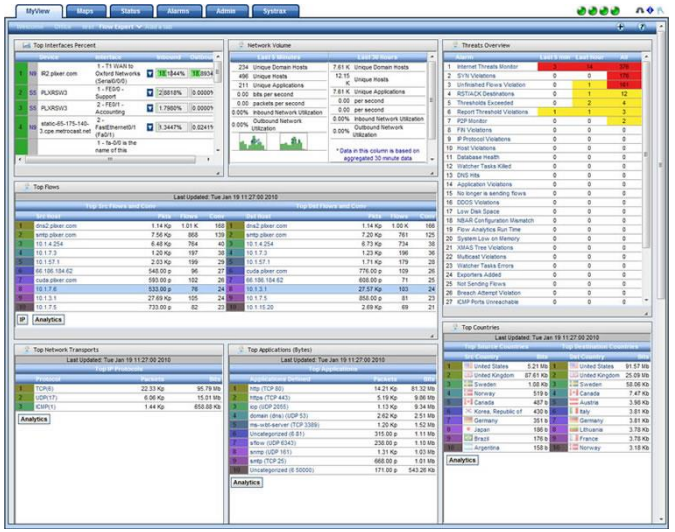
Plixer - Scrutinizer



Charges

Plixer – Flow Analytics

- **Qu'est-ce que Flow Analytics ?**
  - C'est un add-on pour Scrutinizer.
  - Permet d'archiver les données NetFlow après 24 heures.
  - Identification des applications, conversations, flux, protocoles plus facilement.
  - Déclencher des alarmes en fonction de seuils.
  - Possibilité de mettre des alarmes et de créer des rapports.
  - Nouvelle fenêtre pour voir directement les problèmes du réseau.

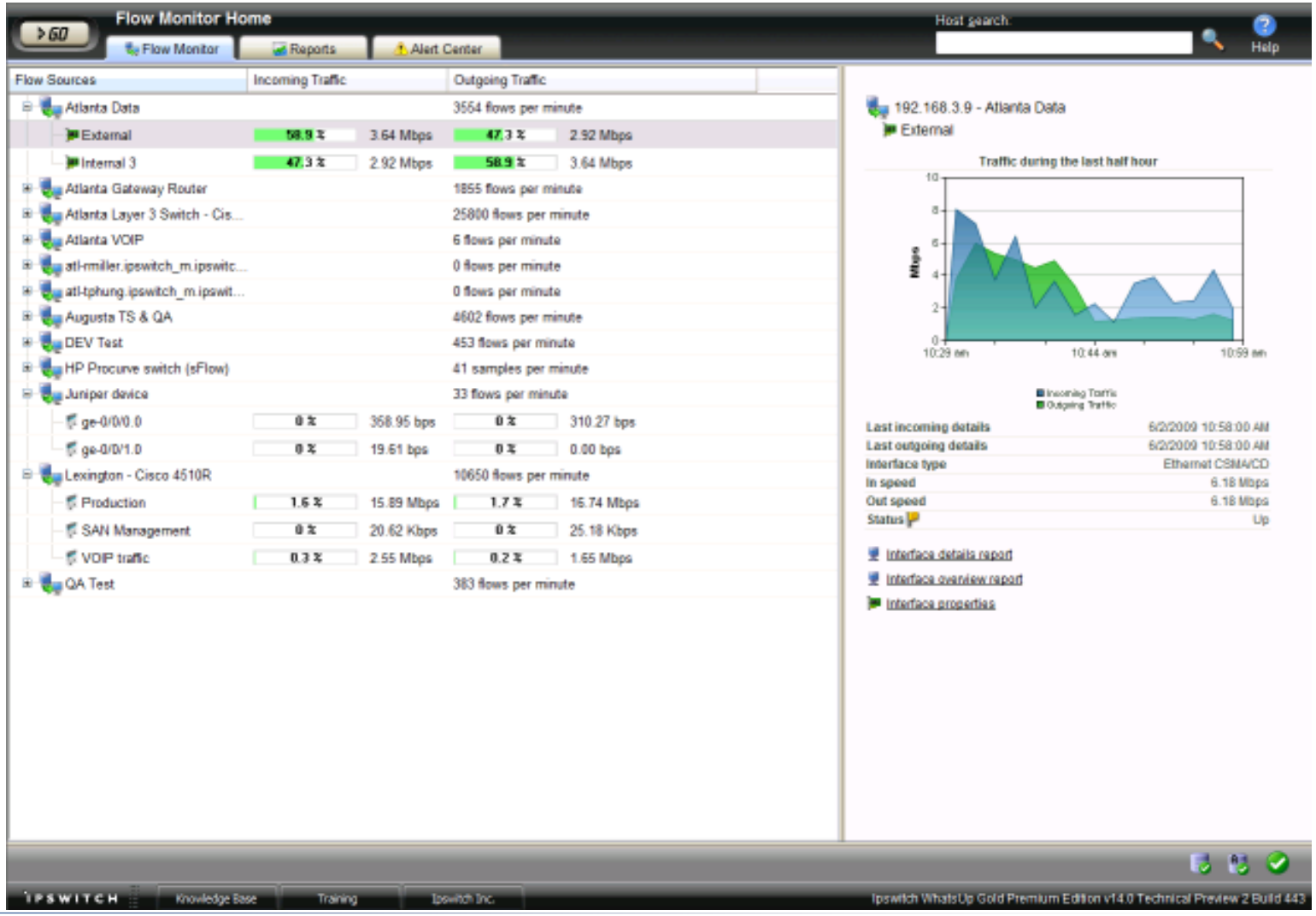


- **Logo :** Flow Analytics™
- **Lien :** http://www.plixer.com/products/netflow-sflow/flow-analytics.php

ORSENNA NMS SERVICES

IPSWITCH WhatsUpGold

WhatsUp – Flow Monitor



Network Supervision – Fluke Networks

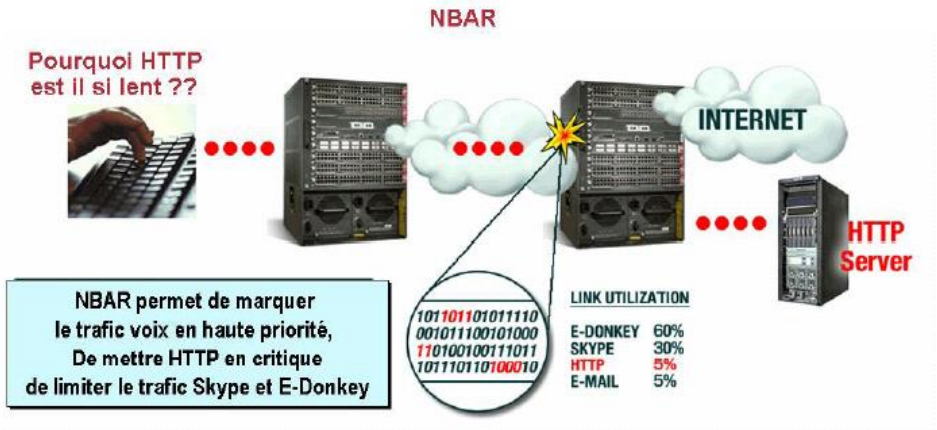
- **Qu'est-ce que Fluke Networks ?**

- **Logo :**

- **Lien :** http://www.flukenetworks.com/

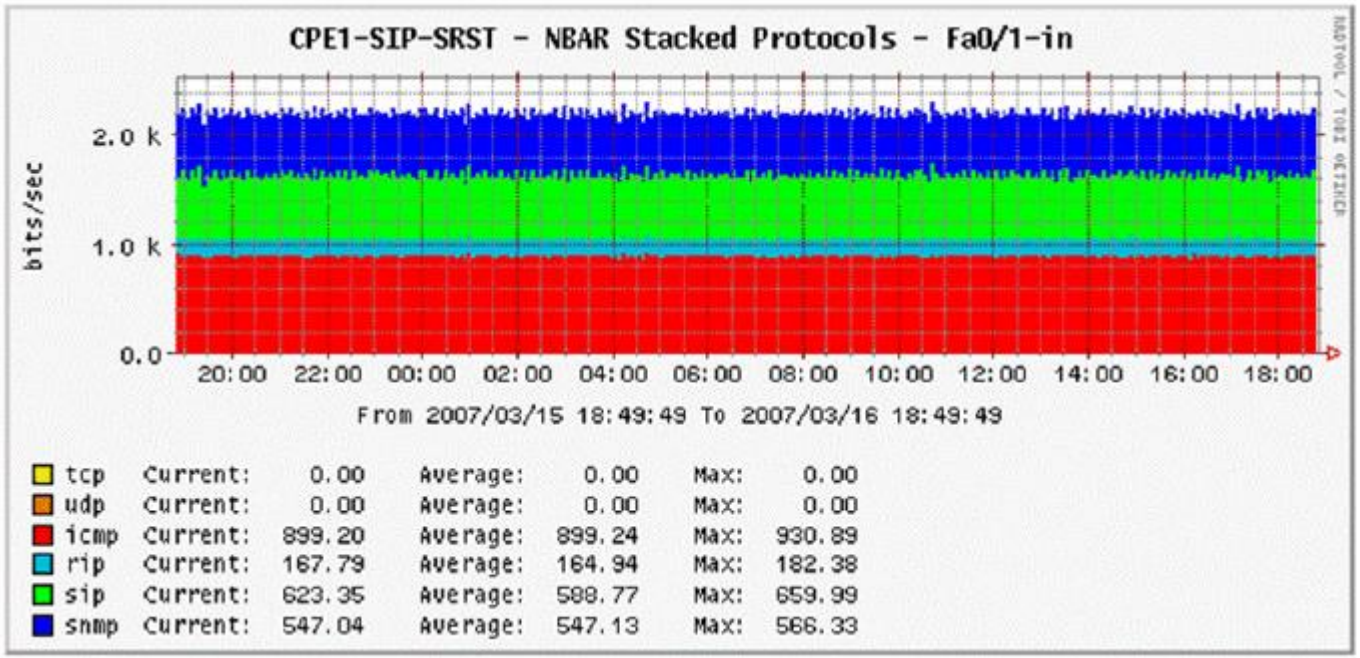
NBAR

- Nbar ➔ Network Based Application Recognition
- Permet de s'affranchir des limites des ACL ➔ peut identifier des applications ou des URLs.
- Nbar reconnait les applications utilisant les ports TCP et UDP.
- Classification approfondie : HTTP et ICA (Citrix applications).



NBAR

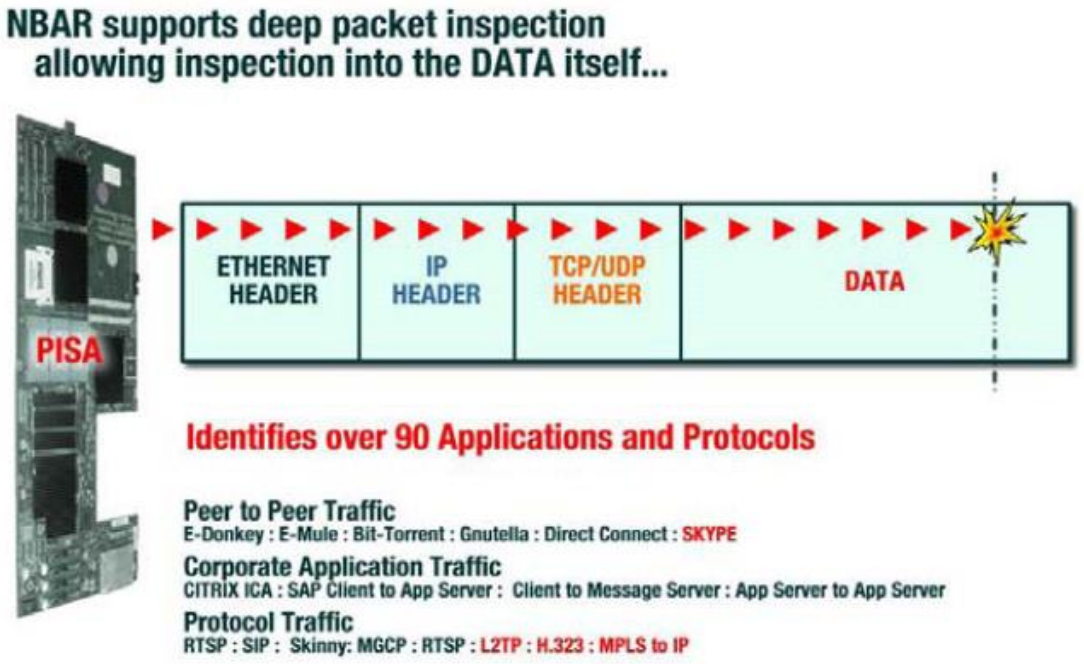
- La découverte d'applications et de protocoles est une fonction associée à NBAR.
- NBAR collecte les statistiques sur les applications présentes sur le réseau.



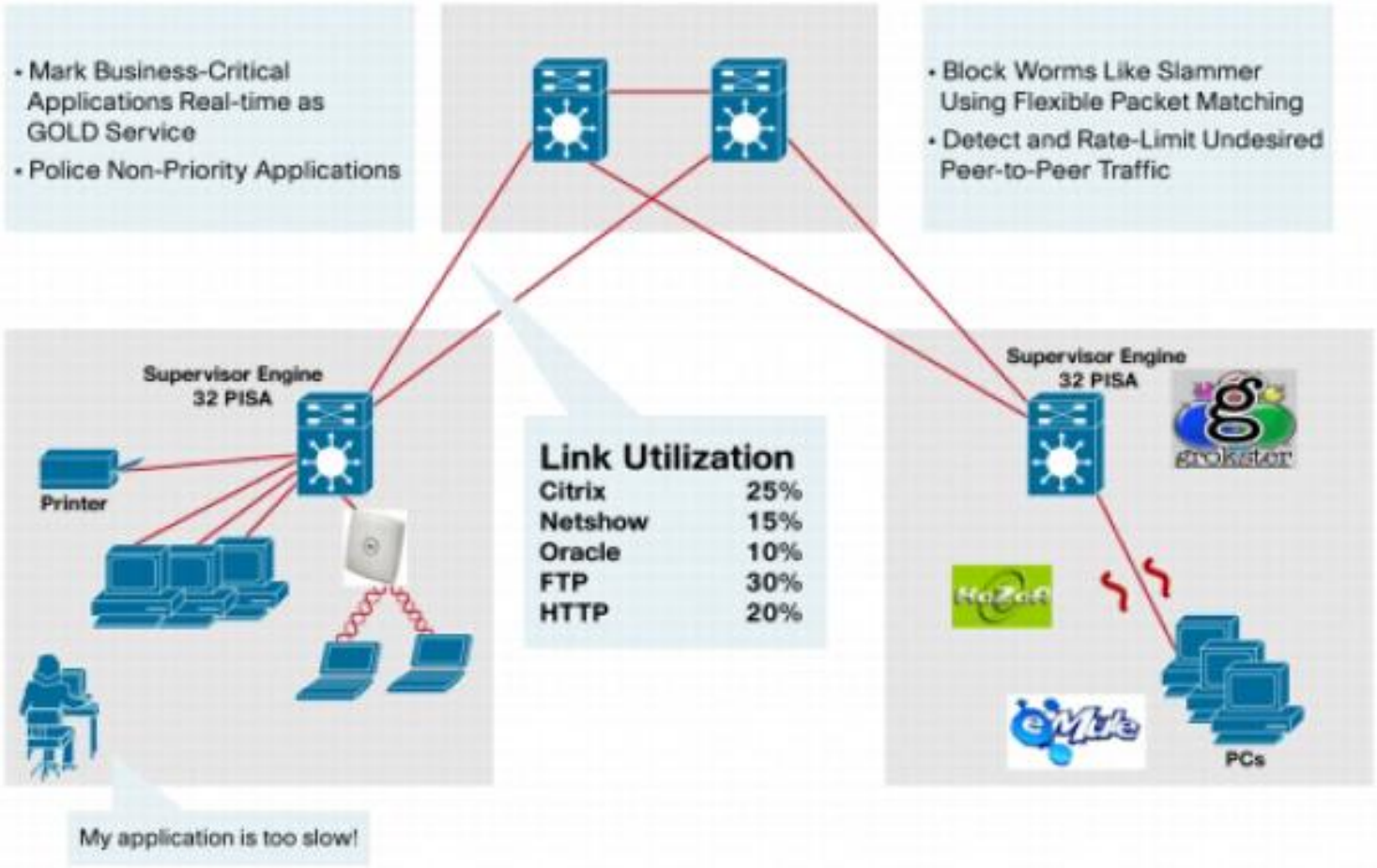
NBAR

- La technologie NBAR est apparue sur les routeurs 7200 et ensuite sur les Catalyst 6500.

- NBAR hardware est apparu sur le Catalyst 6500 sous la forme d'une carte supervisor (Engine 32 PISA) :



NBAR


• Mark Business-Critical Applications Real-time as GOLD Service
• Police Non-Priority Applications
• Block Worms Like Slammer Using Flexible Packet Matching
• Detect and Rate-Limit Undesired Peer-to-Peer Traffic
Supervisor Engine 32 PISA
Printer
Link Utilization
Citrix 25%
Netshow 15%
Oracle 10%
FTP 30%
HTTP 20%
Supervisor Engine 32 PISA
PCs
My application is too slow!

Exemple de configuration

- **Configuration de base CISCO**

Router> enable	➔ passer en mode enable
Router# configure terminal	➔ passer en mode configuration
Router(config)# ip flow-export destination 172.16.10.2 9996	➔ permet d'exporter le flux vers une adresse sur le port 9996 (port défaut)
Router(config)# ip flow-export version 9	➔ Utilisation de la version 9 de Netflow
Router(config)# interface ethernet 0/0	
Router(config-if)# ip flow ingress	➔ supervision du trafic allant dans l'interface
Router(config-if)# ip flow egress	➔ supervision du trafic sortant de l'interface
Router(config-if)# exit	
Router(config-if)# end	

- **Vérification**

1. show ip flow interface	➔ voir la configuration actuelle du NetFlow
2. show ip cache flow	➔ voir les flux en activités ainsi que la
3. show ip cache verbose flow	➔ ressource utilisée

Exemple de configuration

- **Configuration de base Mikrotik :**

This example shows how to configure Traffic-Flow on a router

1. Enable Traffic-Flow on the router:

```
[admin@MikroTik] ip traffic-flow> set enabled=yes
[admin@MikroTik] ip traffic-flow> print
                 enabled: yes
              interfaces: all
           cache-entries: 1k
     active-flow-timeout: 30m
   inactive-flow-timeout: 15s
[admin@MikroTik] ip traffic-flow>
```

2. Specify IP address and port of the host, which will receive Traffic-Flow packets:

```
[admin@MikroTik] ip traffic-flow target> add address=192.168.0.2:2055 \
\... version=9
[admin@MikroTik] ip traffic-flow target> print
Flags: X - disabled
 #   ADDRESS               VERSION
 0   192.168.0.2:2055      9
[admin@MikroTik] ip traffic-flow target>
```

Now the router starts to send packets with Traffic-Flow information.

Exemple de configuration

- **Configuration pour Alcatel Omniswitch (Sflow) :**

```
-> ip interface loopback0 10.10.10.1
-> sflow receiver 1 name sFlowTrend address 10.1.2.5 udp-port 6343
-> sflow sampler 1 1/1-24 receiver 1 rate 128
-> sflow poller 1 1/1-24 receiver 1 interval 30
```

- **Configuration pour Extreme Network (Sflow):**

```
enable sflow
configure sflow-agent 10.10.10.1
configure sflow-collector 10.1.2.5 port 6343
configure sflow sample-rate 128
configure sflow poll-interval 30
configure sflow backoff-threshold 50
enable sflow backoff-threshold
enable sflow ports all
```

- **Configuration pour HP (Sflow) :**

```
(config)# sflow 1 destination 10.1.2.5 6343
(config)# sflow 1 sampling ethernet A1-A24 128
(config)# sflow 1 polling ethernet A1-A24 30
```