Supervision des flux Netflow

Eléments à surveiller : flux provenant de la carte NAM, CISCO Routeur, Enterasys

Il est souhaitable de paramétrer les équipements réseaux pour renvoyer les flux Netflow sur le collecteur Netflow Analyser.

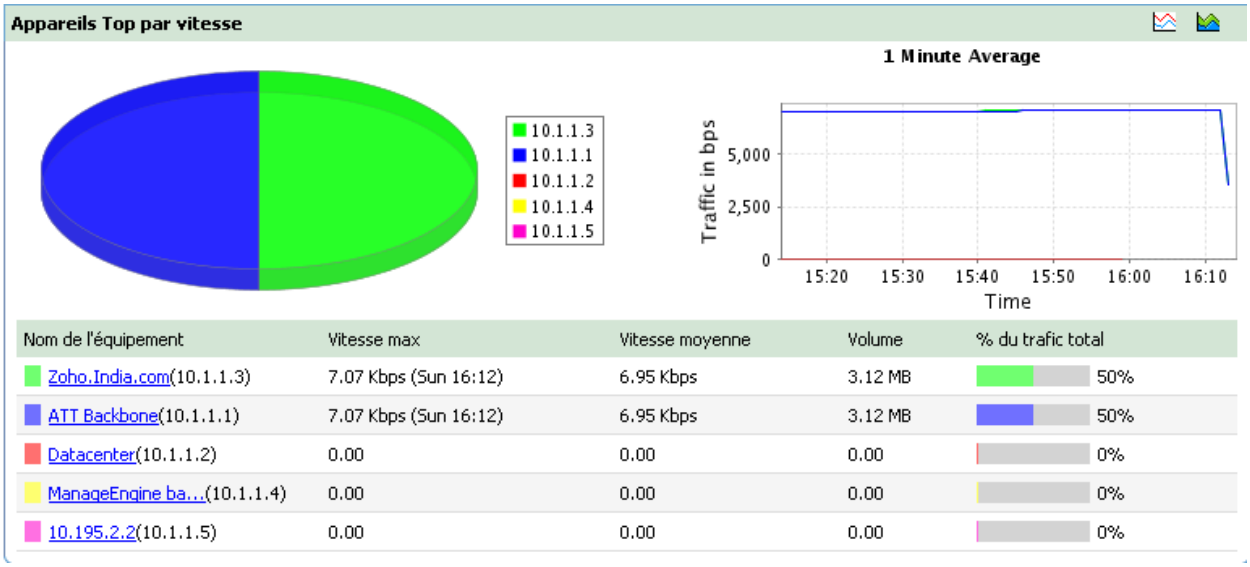
L'outil Netflow Analyser est capable d'analyser simultanément les flows de plusieurs routeurs.

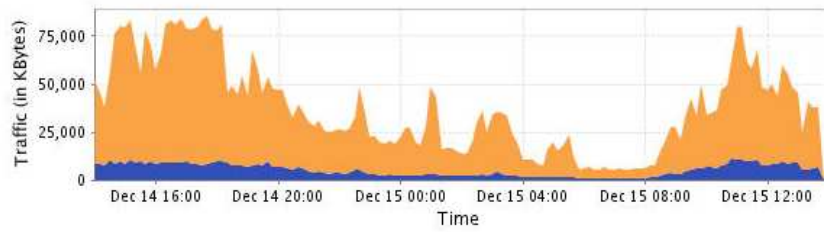
Les informations Netflow sont consolidées sur le serveur Netflow Analyser pour analyser, **sur le plan historique,** l'état des flows sur chaque routeur, avec une vision de l'état de la qualité de service sur chacun des sites ou les flows sont collectés.

Les flows sont stockés dans une base de données Mysql permettant d'avoir une vision en temps réel des flux qui transitent sur votre réseau ; une Agrégation des IPDR par période est réalisée pour conserver un maximum de détails et réduire le volume de données

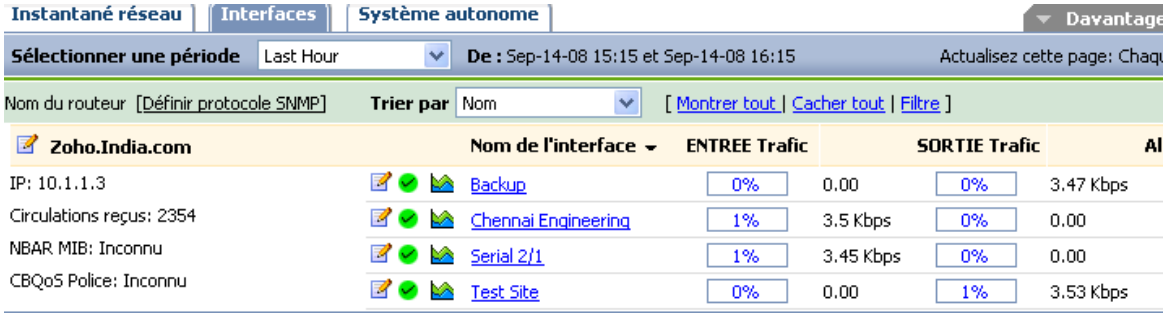
L'agent netflow activé sur l'équipement réseau de niveau 3 et le collecteur Netflow Analyser seront configurés afin de prendre en compte ces flux et d'offrir aux utilisateurs de la solution un reporting en fonction des sites géographiques qui les concernent.

Les rapports fournis offrent une granularité concernant la consultation des données:
On commence par une analyse globale des flux en termes de trafic de performances sur ce segment réseau,





Category	Total	Max	Min	Avg
Traffic IN	722.9 MB	11.1 MB	766.18 KB	5.02 MB
Traffic OUT	4649.23 MB	76.66 MB	4.23 MB	32.28 MB



puis on s'intéresse aux informations suivantes :

- le volume de trafic global sur le réseau
- les N protocoles les plus consommateurs
- les volumes émis pour chacun des couples d'adresses IP
- la répartition de l'utilisation de la bande passante en émission pour chaque couple d'adresse IP
- Top N par application
- Top N trafic par protocole
- Top N par trafic par Adresse IP Serveur/client
- Top N par TOS

- Filtrage avancé :
- Par TOS
- Par Application
- Par adresse IP
- Par interface…

ApplicationIN [2609.03 MB]

Application	Traffic	Traffic Percentage
http	2200.41 MB	84%
https	119.96 MB	5%
ESP_App	111.92 MB	4%

SourceIN [2609.03 MB]

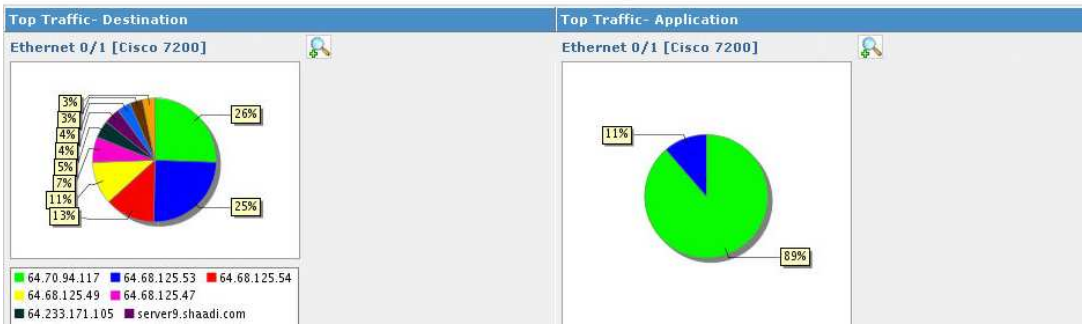
Source	Traffic	Traffic Percentage
192.168.1.76	98.02 MB	4%
192.168.1.67	55.5 MB	2%
192.168.1.86	50.35 MB	2%

On commence à analyser qui consomme un trafic important pour ce protocole donné, puis par la suite on descend d'un autre niveau pour identifier quelle machine ip source est responsable de ce fort trafic et avec qui elle communique.

Les Top talkers

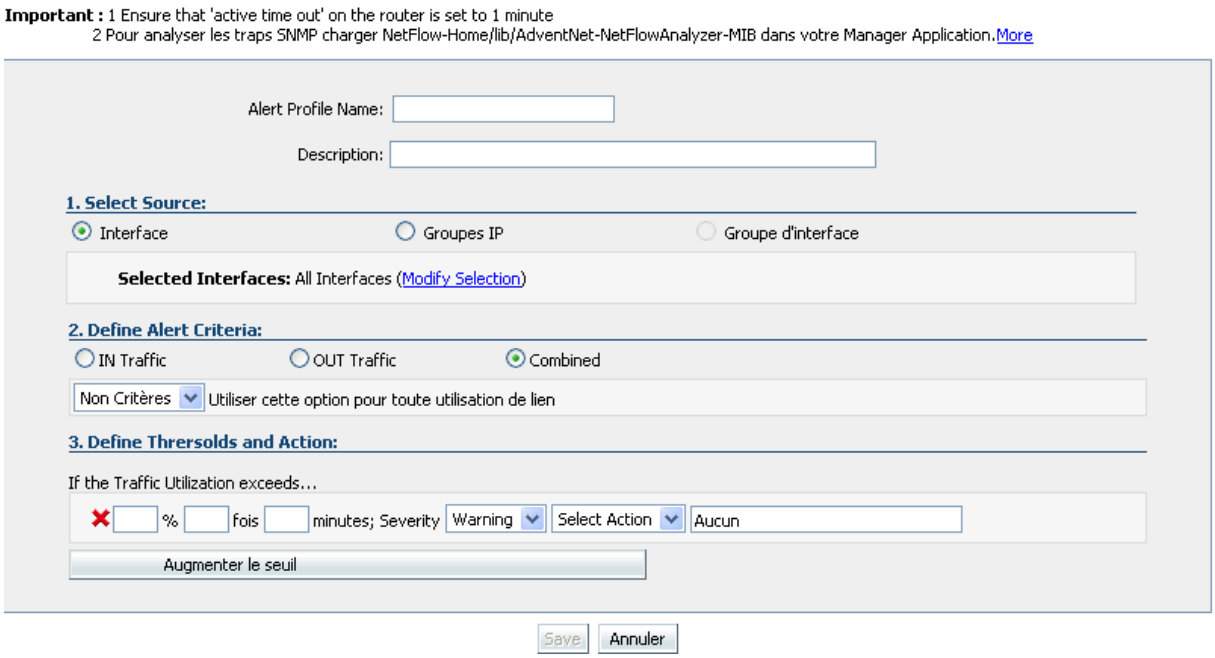
Show IP — Group by | None — Show | Top 10 Resu

Source IP	Destination IP	Application	Port	Protocol	Traffic (143.51 MB)	% of Traffic
kevin.adventnet.com	u716.hotmail.com	http	80	TCP	22.48 MB	16%
gary.adventnet.com	f417.mail.yahoo.com	http	80	TCP	21.71 MB	15%
winnt3.adventnet.com	192.168.2.54	http	80	TCP	11.58 MB	8%
plgroup3.adventnet.com	192.168.1.49	http	80	TCP	9.87 MB	7%
donald.adventnet.com	192.168.2.54	http	80	TCP	5.79 MB	4%
web-proxy.india.adventnet.com	adventnet.info	https	443	TCP	4.01 MB	3%
narmada.adventnet.co.in	gallys.nastydollars.com	http	80	TCP	3.87 MB	3%
phillip.adventnet.com	ns3.vtitan.com	https	443	TCP	3.1 MB	2%
alex.adventnet.com	up1.ph.vip.scd.yahoo.com	https	443	TCP	2.87 MB	2%
aditya.adventnet.com	server9.shaadi.com	http	80	TCP	2.78 MB	2%

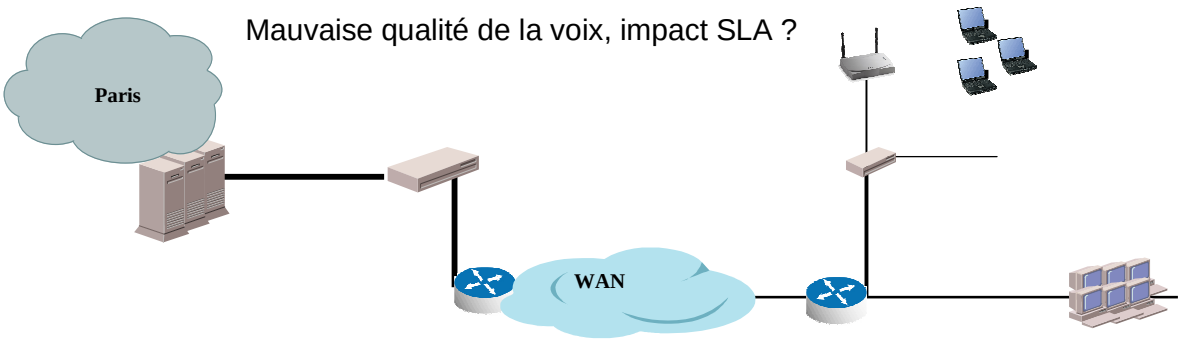


Notification

- Notification à l'utilisateur admin par mail des alarmes sur les l'interfaces.
- Notification immédiate à l'utilisateur admin par mail ou SMS dès que la charge d'un équipement dépasse 80 %
- Notification immédiate à l'utilisateur admin par mail ou SMS dès que le volume protocolaire dépasse un volume défini dans un seuil de référence.
- Notification à l'admin par mail ou SMS dès que le volume protocolaire dépasse un volume défini dans un seuil de référence.
- Notification à l'admin par mail ou SMS dès que le débit d'une classe de service dépasse un volume défini dans un seuil de référence.



Exemple d'un cas concret d'analyse d'une dégradation de la qualité de service



Show Applications | View DSCP Group Showing 1 to 3 View per page 100

DSCP	Traffic(Total: 2.25 GB)	Percentage of total traffic
Best Effort	1.86 GB	83%
000010	29.3 MB	1%
000100	4.86 MB	<1%

Au travers des rapports fournis par Netflow Analyser on remarque qu'une file d'attente Best effort est très représenté sur l'accès au site de Paris, ce qui dégrade fortement les flux voix et les autres flux prioritaires ; d'autres part on constate un mécontentement des utilisateurs finaux qui plaignent des lenteurs pour accéder à l'application métier, de plus les appels voix sont dégradés.

Ceci nous amène à dire qu'il est souhaitable de revoir la configuration de la qualité de service déployé, car pour les flux voix il est recommandé d'avoir une classe de service qui dispose d'un canal prioritaire quelque soit la charge du trafic. Dans notre cas la voix est prioritaire sur toutes les autres classes, elle doit être configurée dans une "Classe EF dscp 46"

Application	Traffic	% Utilization
https	553.2 MB	30%
voice	510.64 MB	27%
ESP_App	336.95 MB	18%
TCP_App	252.13 MB	14%
smtp	179.39 MB	10%