ZneTS v1.2 « The NEtwork Trafic Supervisor »

Ismael ZAKARI TOURE
LPSC IN2P3
53, rue des Martyrs, 38026 Grenoble Cedex

Thierry DESCOMBES
LPSC IN2P3
53, rue des Martyrs, 38026 Grenoble Cedex

contact: info@znets.net

Résumé

ZNeTS, "The Network Traffic Supervisor", est un outil de surveillance des machines d'un ou plusieurs LANs, développé pour l'IN2P3.

Ses fonctions sont :
- la conservation de plusieurs mois de données de trafic en base de données ;
- la recherche et l'extraction de données, grâce à son moteur de recherche intégré ;
- la détection d'anomalies provoquant la génération d'alerte et l'envoi éventuel de email ;
- le calcul et la visualisation des statistiques horaires et journalières du trafic global et individuel (pour chaque sous-réseau, et machine du LAN).

ZNeTS s'adapte à toutes les architectures réseau. Il est capable d'acquérir ses données non seulement à partir des NetFlow (mode netflow), mais aussi directement depuis une interface physique (mode sniffer). Il est capable de décoder la plupart des versions de NetFlow et l'IPFIX. Il est compatible IPv4 et IPv6. Des packages ont été construit pour la plupart des distributions Linux.

Mots clefs

Supervision, surveillance, réseau, LAN, traces, analyse trame, métrologie, détection anomalies, sniffer, NetFlow, IPFIX, sonde, collecteur

1 Généralités

ZNeTS, est l'acronyme de "The Network Traffic Supervisor". C'est un outil de surveillance des machines d'un ou plusieurs LANs.

Il a été conçu pour satisfaire 4 objectifs :

- fournir des traces des flux réseaux entrants et sortants
- offrir des outils permettant une analyse fine de ces données
- détecter certaines anomalies et lever des alertes
- être un outil de métrologie pertinent et fiable

ZNeTS est simple à déployer. Il a été développé en C++ et intègre un serveur web implémentant la norme HTTP/1.1(RFC2616). Une authentification par identifiant et mot de passe, ou par certificats X509 est possible.

Une interface web est disponible. Basée sur le framework Dojo1.6, elle est particulièrement ergonomique et permet l'interprétation et la visualisation des données.

ZNeTS fonctionne au choix, en mode collecteur de NetFlow (IPFIX), ou capture (sniffer). Dans le premier cas, il reçoit et traite des données de trafic agrégées des routeurs, pare feux, ou d'une sonde logicielle (ZNeTS ou toute autre sonde logicielle capable d'envoyer des NetFlow).

En mode sniffer, la sonde acquiert ses données directement d'une de ses cartes réseau.

ZNeTS peut fonctionner sur des réseaux IPv4 et Ipv6.

Ce logiciel a été développé avec l'objectif d'être à la fois très modulaire et très simple à déployer. Des *packages* ont été construits pour la plupart des distributions Linux.

2 Les flux réseaux de ZneTS

ZNeTS gère une liste de flux bidirectionnels ordonnés chronologiquement.

Ces flux sont caractérisés par 1 clé (unique) composée de 5 données :

- IP local (V4 ou V6)
- IP externe (V4 ou V6)
- Protocole de niveau 3
- Port Local
- Port Externe

Ils contiennent également :

- le sens d'établissement de la connexion
- le nombre de paquets entrants et sortants
- le nombre d'octets de trafic entrant et sortant
- un masque des éventuels *flags* TCP
- une date de début
- une date de fin
- le pays relatif à l'IP externe
- le numéro de l'AS [1] de l'IP externe

Tous les flux de ZNeTS sont donc intrinsèquement entrants ou sortants. (Les flux internes sont ignorés)

Toutes les dates sont au format UTC, afin de faciliter la gestion des changements d'horaire. L'application web applique le décalage correspondant à la zone géographique dans laquelle est situé votre navigateur.

Ce schéma de données offre 2 avantages, par rapport à des flux unidirectionnels classiques. Tout d'abord, ils sont moins nombreux (1 flux bidirectionnel correspond à 2 flux unidirectionnels) et ils sont donc moins volumineux. De plus, ils permettent une indexation facile et naturelle des flux par IP locale.

[1] Autonomous System

3. Agrégation des flux

ZNeTS agrège ses flux au cours d'un cycle ou « période d'agrégation », dont la durée est paramétrable [2]. Plus cette période est longue, moins il y a de flux enregistrés par heure.

À la fin de cette période, les flux sont réinitialisés. Les compteurs sont remis à zéro. Les autres paramètres sont conservés.

Les flux dont les compteurs étaient déjà à zéro, sont considérés comme terminés et sont supprimés.

Ainsi, un flux qui s'étend sur plusieurs cycles aura une entrée par cycle. Les quantités de trafic et de paquets seront propre à un cycle donné. En plus des 5 champs composant la clé (voir ci-dessus), la date de début sera également conservée d'un cycle à l'autre.

L'agrégation des ports clients est également possible [3] , ce qui permet d'ignorer les ports client. Cette option permet de diminuer, en moyenne, d'un facteur 3 à 4, le nombre de flux.

4. L'acquisition des données

L'acquisition des données se fait soit à travers la réception de NetFlow, soit en décodant les trames d'une interface dédiée (mode *sniffer*).

4.1 Utilisation de la technologie NetFlow

ZNeTS est compatible avec la technologie NetFlow, qui est la plus répandue pour l'analyse réseau (notamment supportée par tous les systèmes basés sur l'IOS Cisco). Elle est basée sur un algorithme qui agrège, pendant une durée paramétrable, une liste de flux unidirectionnels ordonnés chronologiquement. Les données sont envoyées vers un collecteur selon un modèle « *push* » (Par défaut, le port 2055 du protocole UDP est utilisé)

10 versions de ce protocole existent. ZNeTS supporte les versions les plus répandues : 1, 3, 5, 6, 7, 9 et IPFIX.

Les versions 9 et IPFIX sont basées sur un mécanisme de *template*, c'est à dire la définition dynamique des modèles de données, par la sonde. Pour que ZNeTS puissent interpréter les NetFlow V9 et IPFIX, les *templates* doivent contenir les données suivantes :

Données indispensables pour les NetFlow V9:

- (IPV4_SRC_ADDR ET IPV4_DST_ADDR) OU (IPV6_SRC_ADDR ET IPV6_DST_ADDR)
- PROTOCOL
- IN_BYTES
- IN_PKTS
- L4_SRC_PORT
- L4_DST_PORT
- FIRST_SWITCHED
- LAST_SWITCHED

Données facultatives pour les NetFlow V9:

- TCP_FLAGS
- OUT_BYTES
- OUT_PKTS

[2] voir man znets.conf - paramètre « nbCollectCyclePerHour »

[3] voir man znets.conf - paramètres « aggregateTcpClientPorts » et « aggregateUdpClientPorts »

- IN_SRC_MAC
- OUT_DST_MAC

Données indispensables pour IPFIX :

- (sourceIPv4Address ET destinationIPv4Address) OU (sourceIPv6Address ET destinationIPv6Address)
- protocolIdentifier
- octetDeltaCount
- packetDeltaCount
- sourceTransportPort
- destinationTransportPort
- (systemInitTimeMilliseconds ET flowStartSysUpTime ET flowEndSysUpTime)
  OU (flowStartMilliseconds ET flowEndMilliseconds)
  OU (flowStartSeconds ET flowEndSeconds)

Données facultatives pour IPFIX :

- tcpControlBits
- postOctetDeltaCount
- postPacketDeltaCount
- sourceMacAddress
- postDestinationMacAddress

Les NetFlow V9 et IPFIX reçus incomplets sont ignorés.

À chaque fin de cycle, un message de statistique informe du nombre de flux reçus, et ignorés (au total, ainsi que pour chaque version du protocole)

4.2 Utilisation d'une interface dédiée (IpSniff)

ZNeTS peut aussi acquérir des trames directement depuis une interface dédiée. Ces trames sont alors analysées, et les informations de flux en sont extraites. Actuellement, ZNeTS n'analyse que les entêtes. Le contenu des trames est ignoré.

Certaines anomalies des datagrammes sont détectées et génèrent des messages d'information. Les paquets erronés ou incomplets sont ignorés.

ZNeTS peut éventuellement être raccordé à un lien *vlan trunk.* La détection est automatique.

À la fin des cycles, un message de statistique informe du nombre de paquets reçus et perdus.

NB : L'utilisation d'une interface dédiée sollicite beaucoup plus le CPU et l'utilisation de la mémoire. Son utilisation n'est pas conseillée sur des réseaux très haut débit (plusieurs Gb/s).

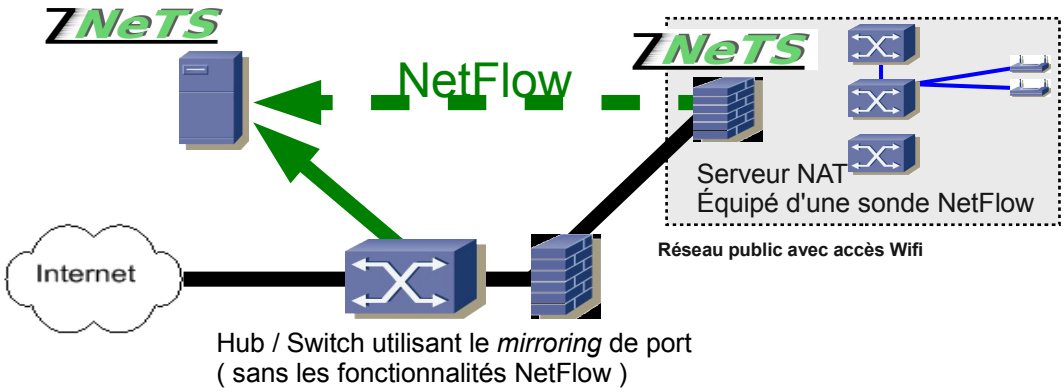
4.3 Exporter des NetFlow

ZNeTS peut également être configuré pour se comporter comme une simple sonde NetFlow. Ainsi, il est tout à fait envisageable de faire communiquer 2 instances de ZNeTS (pour déporter l'acquisition des données, par exemple), sans qu'aucun autre logiciel ne soit requis.

5. Déploiement

ZNeTS a été conçu pour s'adapter à la plupart des architectures réseaux.

- Avec un routeur compatible NetFlow, le déploiement est simple. ZNeTS devra alors être configuré en mode collecteur de NetFlow[4].
- Avec un routeur ne supportant pas les NetFlow mais disposant des fonctionnalités de *mirroring* de ports, ZNeTS pourra être configuré en mode *sniffer*[5].
- Si vous ne disposez ni des fonctionalités de NetFlow ni de *mirroring*, d'autres solutions peuvent encore être envisagées : installation d'un *hub*, mise en place d'un PC agissant comme un pont transparent, équipé d'une sonde ZNeTS, ...
- Avec un ou plusieurs réseaux NATés dans votre LAN, en visualisant les machines avec leurs adresses privées.



Une solution est de démarrer une Instance ZNeTS en mode sonde NetFlow qui enverra ses données à l'instance ZNeTS principale (sur laquelle, cette nouvelle source de NetFlow, et ce nouveau réseau local auront été déclarés).

Il pourra être utile également d'ignorer le trafic du serveur de NAT, afin de ne pas prendre 2 fois en compte le trafic vers ce réseau[6].

NB : La technologie Netflow repose sur l'utilisation systématique du protocole UDP pour l'envoi des données. Ce protocole est sensible aux congestions, pertes de paquets, désynchronisations... Il est donc recommandé de mettre le collecteur et le ou les sondes de NetFlow sur un lien dédié suffisamment rapide et non routé.

6. Traitements périodiques

ZNeTS effectue, de manière cyclique, plusieurs types de traitement.

1) Le « cyclic collector processing » a lieu à chaque fin de cycle. Au cours de celui-ci, les flux de ZNeTS sont enregistrés (en base de données et sous forme de fichiers). Les alertes sont générées. Éventuellement, si le mode sonde est activé, ZNeTS envoie ses flux vers son collecteur. Une entrée dans les logs est ajoutée à la fin du traitement. Elle précise le nombre de flux ZNeTS, ainsi que

---

[4] voir znets.conf - « useNetFlow »

[5] voir znets.conf - « usePcap »

[6] voir znets.conf - « AddLocalHostToIgnore »

la durée du traitement (total, nécessaire à l'enregistrement en base de données : « recDB », à l'écriture des fichiers« wrFile », à l'envoie sous forme de Netflow « sndNF », et au processing en mémoire « procLH »)

2) Le « hourly stats processing» démarre à chaque changement d'heure. Les statistiques pour la métrologie sont calculées et enregistrées en base de données. Une entrée dans les logs est ajoutée à la fin du traitement avec la durée du traitement (total, et nécessaire à l'insertion en base de données « recDB »)

3) De manière analogue, un « daily stats processing» démarre à chaque fin de journée (à minuit UTC).

4) Lorsqu'il est activé le « databaseDataflowAutovacuum» démarre à 4h du matin UTC. Sa fonction est de supprimer les flux, datant de plus d'un nombre paramétrable de jours, puis de mettre à jour les index des tables du SGBD.

7. Détection d'anomalies

À chaque fin de cycle, ZNeTS analyse le trafic collecté par machine locale, et génère une alerte dès qu'un comportement anormal est détecté. Une étape d'ajustement des seuils peut parfois être nécessaire (en fonction de la durée des cycles, du type de trafic, …)

Les alertes sont relatives au dernier cycle écoulé et sont actuellement de 7 types distincts :

- une machine locale a communiqué avec plus de X machines externes : permet de repérer l'utilisation de logiciels de type *Peer to Peer*.
- une machine locale a scanné une machine externe: suite à plusieurs tentatives de connexions infructueuses sur des ports distincts et éventuellement des protocoles différents.
- une machine externe a scanné une machine interne : idem
- une machine locale a eu du trafic SMTP sortant de plus Y KB
- une machine locale a eu du trafic avec une machine externe définie comme compromise.
- Le logiciel « znetsSuspiciousDL » fait parti de ZNeTS et permet le téléchargement ainsi que la mise à jour de listes de machines suspectes.(serveur botnets, vers, virus, …)
- une machine locale interroge un serveur DNS externe inconnu.
- une adresse IP locale est dupliquée

Les alertes peuvent être envoyées par mail. Elles sont stockées en base de données. Elles sont activables et désactivables. Il est possible définir des exceptions et des seuils spécifiques.

La simplicité de ces algorithmes de détection les rend particulièrement efficaces.

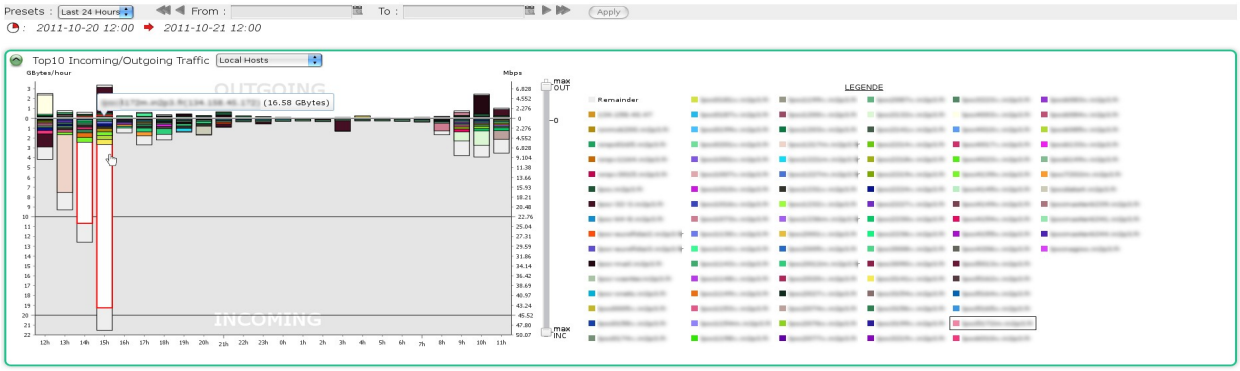
8. Métrologie

ZNeTS est un puissant outil de métrologie, permettant de visualiser les statistiques horaires et journalières. Potentiellement, plusieurs mois et années de statistiques sont disponibles et peuvent être consultés.

La plupart des statistiques se présente sous forme de graphiques empilés, représentant pour chaque heure ou chaque jour, les 10 plus gros consommateurs (machine locale, service, ...) d'une ressource.

33 types de graphique sont disponibles pour l'ensemble du réseau et pour chaque sous-réseau, et 7 types pour chaque machine du réseau local.

Les nombreuses interactions Javascript sur les graphiques aident à suivre les évolutions, et à bien interpréter les données. Les clics sur les graphiques pré-remplissent les formulaires de recherche de flux et d'analyse de machines locales.

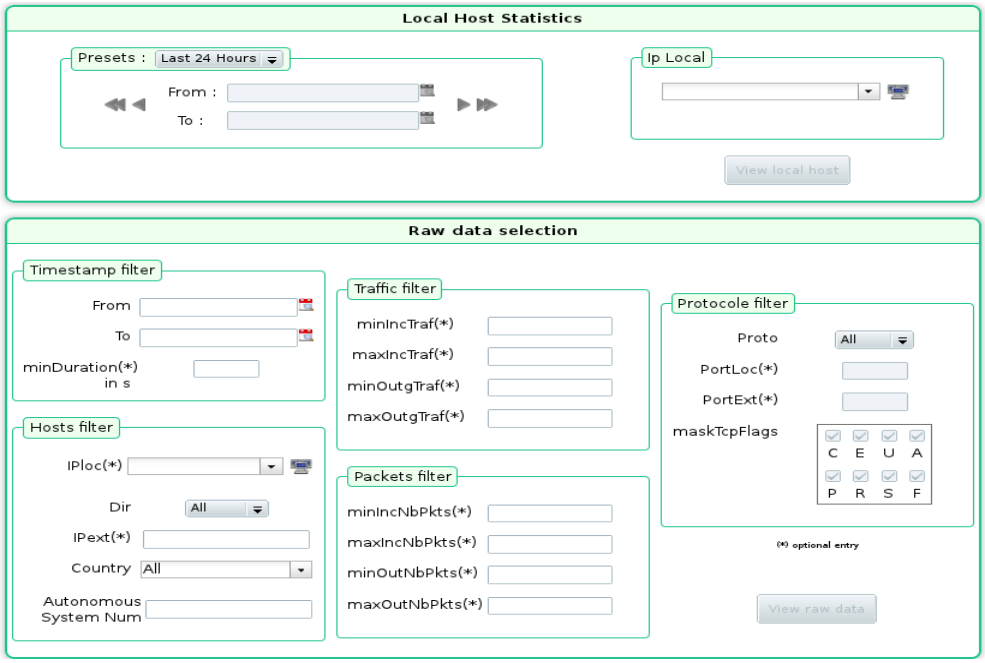


Exemple d'un graphique de trafic réseau

Ces données statistiques (utilisées pour générer tous les graphiques, à l'exception des camemberts), sont stockées indépendamment des données. Les options de nettoyage automatique[7] ne les suppriment pas. (L'espace qu'elles occupent dans la base de données étant insignifiant).

9. Analyse détaillée

ZNeTS possède un formulaire de recherche assez complet, qui permet la sélection puis la visualisation des données brutes enregistrées.



Les exports au format CSV sont possibles.

Les IPs externes sont automatiquement résolues (lorsqu'elles sont survolées par le curseur de la souris) et recopiées (lors d'un clic).

De plus, ZNeTS s'interface facilement avec l'utilitaire « whois » [8], et facilite ainsi l'interrogation des registres Internet.

[7] Voir man znets.conf – paramètres « databaseDataflowAutovacuum » et « databaseDataflowAutovacuumSize=NB_DAYS »

10. Performance

Le tableau ci-dessous résume les performances de ZNeTS sur 3 sites. Les résultats sont indicatifs et issus de moyennes. Les 3 instances fonctionnent avec des cycles d'un quart d'heure. L'IPNL a fait le choix de ne pas utiliser l'agrégation de port, ce qui explique son nombre de *flows* plus important..

Site	*Type de serveur*	*Débit moyen entrant/sortant*	*Nb machines locales*	*Nb Flows par ¼ d'heure*	*Durée d'un « Cycle processing »*	*Durée d'un « Hourly Stats processing »*	*Taille de la BD sur le disque*
LPSC	Dell PE1950 (age > 5ans)	25Mbps / 19Mbps	2530	10900	3s	10s	7Go/mois
IPNL	Dell PE1950 (age > 5ans)	31Mbps / 26Mbps	2760	24340	1s	12s	15Go/mois
Centre Calcul	Dell R610 avec 2 disques SSD en stripping	1.3 Gbps / 2.4 Gbps	10430	320000	10s	17s	6Go/jours

Plusieurs années de trafic peuvent être stockées en base sans problème (à condition que l'espace disque soit suffisant), mais à l'usage, l'intérêt peut sembler limité. En effet, ces données sont principalement utilisées pour l'analyse fine d'une anomalie, à laquelle on procède généralement, peu de temps après qu'elle se soit produite.

L'utilisation de fichiers, pour le stockage, est donc à privilégier [9], conjointement au nettoyage automatique des données en base (dont l'"âge maximum est à déterminer à l'usage et en fonction du trafic).

11. Conclusion

ZNeTS est un outil complet, fiable et abouti. Il est simple à déployer, et complètement transparent pour le réseau et les machines clientes.

Il permet de conserver les traces de tous les flux entrants et sortants, pendant plusieurs mois. Les graphiques de métrologie sont pertinents, interactifs, et facilement interprétables. La sélection et la consultation des trames est aisée : les formulaires sont pré-remplis automatiquement.

Après un incident de sécurité, ou un dysfonctionnement, ZNeTS est l'outil idéal pour visualiser rapidement l'état du réseau, analyser précisément les conséquences d'une attaque, d'un virus, ou de mettre en évidence un vol d'informations. En outre, il permet d'identifier, d'une manière fiable et préventive, des machines locales compromises.*

[8] voir man znets.conf - paramètre « whoisCmd»

[9] Voir znets.conf - paramètre « saveDataflowToFile » , qui permet la création de fichier journalier de données au format CSV

12.Bibliographie

[1] RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1

[2] *RFC2720 - Traffic Flow Measurement: Meter MIB*

[3] RFC3917 - Requirements for IP Flow Information Export (IPFIX)

[4] RFC3954 - Cisco Systems NetFlow Services Export Version 9

[5] RFC3955 - Candidate Protocols for IP Flow Information Export (IPFIX)

[6] RFC5101 – Specification of the IP Flow Information Export (IPFIX)

[7] RFC5102 – IPFIX Information Model

[8] RFC5470 – Architectures for IP Flow Information Export

[9] RFC5472 – Flow Information Export (IPFIX) Applicability

[10] RFC5655 – Specification of the IP Flow Information Export (IPFIX) File Format