Supervision de réseaux avec ZNeTS

Ismael Zakari Touré

Thierry Descombes

ZNeTS :
«The Network Traffic Supervisor»

Objectifs :

1) Traçabilité de la matrice des flux réseaux.

2) Analyse fine (Moteur de recherche de trames brutes)

3) Détection d'anomalies et levée d'alertes

4) Métrologie: visualisation de statistiques horaires et journalières (Top10)

ZNeTS

Ergonomique :

- HTML 2.0 (Dojo, Ajax, formulaires pré-remplis..)

Simple à déployer :

- Tout en un : unique binaire (serveur web + appli cliente JS)
- Adaptable (acquisition interface ou Netflow)
- Simple à configurer : 1 seul fichier ZNeTS.conf
- Librairies très répandues et portables (sous licence BSD)
- Packages Linux disponibles pour RHEL/CentOS/SL 6, Fedora, Mandriva 2010.2, Debian 6, Ubuntu (version Windows ?)

Compatible NetFlow

- Technologie la plus répandue pour l'analyse réseau
- Inventée par Cisco en 1996
- Supportée par tous les systèmes Cisco IOS (existence de sondes logicielles)
- Liste de Flux unidirectionnels ordonnés chronologiquement
- Agrégation de flux
- Protocole UDP (push model)
- Version 1 à 8 => IPv4 + types prédéfinis.
  Version 9 => définition dynamique de templates (compatible Ipv6, MPLS, BGP...)
  IPFIX = V9 standardisée par l'IETF

ZNeTS collecteur et sonde

- Collecteur, acquisition
- - à partir d'une interface dédiée (support 802.1Q)
- - à partir de données Netflow v1, 3, 5, 6, 7, 9 et IPFIX

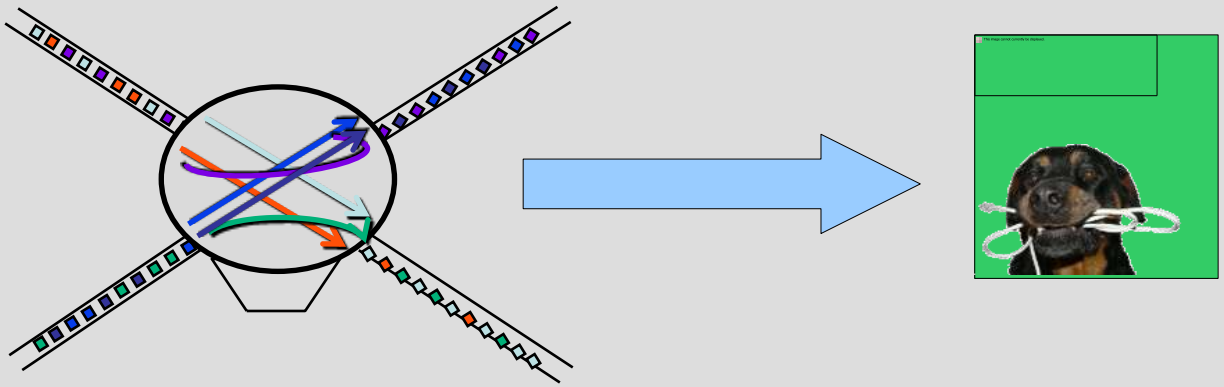
- Mode Sonde (option)
- - Envoi des flux collectés (en NetFlow V9)

Compatible : IPv4, IPv6

Flux bidirectionnelles de ZNeTS

Définit par 5 clés uniques:

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



Et contenant :

- Sens d'établissement connexion
- Nb Packets entrants/sortants
- Nb octets entrants/sortants
- Flags TCP
- Timestamps (2)
- Pays

=> ***Avantages :***

- 2 fois moins de flux qu'avec des flux unidirectionnels
- Indexation par IP locales

Acquisition des données

Traitements de fond de l'acquisition:

- Réception de NetFlow
- Capture du trafic d'une interface
- Discrimination des flux
- Calcul statistique par réseau, sous-réseau et machines locales
- Agrégation

Traitements périodiques

Interruption de acquisition : Bufferisation

1) Traitement périodique : fin d'une période d'agrégation (plusieurs fois par heure – fréquence configurable)

=> Enregistrement du trafic (fichier et SGBD)
=> Envoi du trafic sous forme de NetFlow
=> Levée des alertes
=> Ré-initialisation des flux : remise à zéro des compteurs, autres paramètres (dont sens d'établissement de la connexion) conservés, suppression des flux terminés.

2)Traitement cyclique horaire & journalier

=> Calcul et enregistrement des statistiques

ZNeTS - Configuration

/etc/ZNeTS.conf (cf : man ZneTS.conf)

=> 2 types de paramètres requis :

- Mode d'acquisition : « usePcap » et/ou « useNetFlow »
- Liste des LANs / sous LANs (nommés ou pas) : « localNetwork »

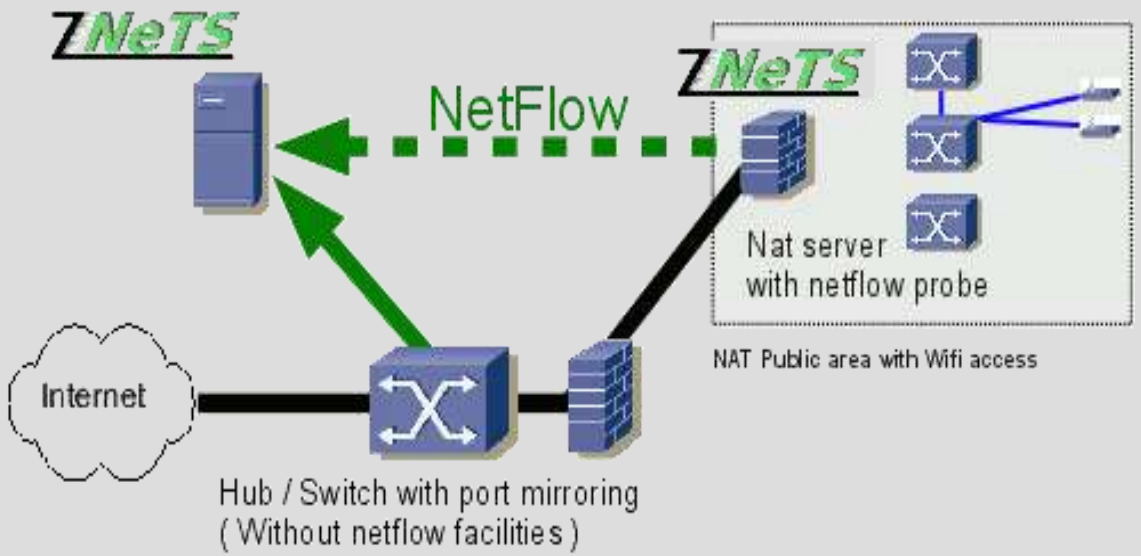
- + environ 60 paramètres optionnels :
- Agrégation des ports clients
- nb de périodes d'agrégation par heure : nbCollectCyclePerHour
- Mode sonde : sendNflowToHost
- Seuils d'alertes & machine suspecte (suspiciousHost)
- Exceptions (Whitelist)

Déploiement ZNeTS au LPSC

Port Mirroring

Machines « Visiteur » sur réseau natés

=> 2 instances de ZNeTS et ignorer le trafic du serveur de NAT.



ZNeTS – Configuration LPSC

Sonde sur notre serveur NAT « visiteur »

usePcap
pcapDevice="eth1.2"
sendNflowToHost="lpsc-znets"
nbCollectCyclePerHour=59
DBMS=NONE
disableHttpdServer
localNetwork=192.168.2.0/24
alertMaxDest=0
alertMaxInFlowByDest=0
alertMaxOutFlowByDest=0
alertMaxExtSMTPtraffic=0
aggragateTcpClientPorts
aggragateUdpClientPorts

ZNeTS – Configuration LPSC

Collecteur sur lpsc-znets

```
pcapBufferSize=16 // 16Mo
pcapFilter="icmp or tcp or udp"
pcapDevice="eth1"
databaseUser="znets"
databaseName="znets2"
saveDataflowToFile
dataflowFileRotateHourly

localNetwork=134.158.40.9/32,
"sauvegarde"
localNetwork=134.158.40.0/21, "labo"
localNetwork=193.48.83.0/24, "grille"
localNetwork=192.168.2.0/24, "visiteur"

usePcap
useNetFlow
netFlowIpDataSources=134.158.40.24/32

aggragateTcpClientPorts
aggragateUdpClientPorts
suspiciousHost=99.237.220.123/32,
```

```
whitelistLHostOut=134.158.40.8/32 25/tcp
whitelistLHostOut=134.158.40.199/32 53/*
whitelistLHostOut=134.158.40.21/32 25/tcp

nbCollectCyclePerHour=4
localHostToIgnore=193.48.83.24/32

sendMailOnAlert
mailDst="descombes@lpsc.in2p3.fr, meyrand..."
mailServer="lpsc-mail.in2p3.fr"

#httpdIpAllowed=134.158.40.0/21
httpdPort=8443
httpdAuthLoginPwd="admin:admin"
httpdUseSSL
#httpdAuthPeerSSL
httpdSSLcertFile="lpsc-test.in2p3.fr.pem2"
httpdSSLCaFile="ca-chain.crt"

#httpdAuthorizedPeerDN="/C=FR/O=CNRS/OU
=UMR5821/CN=Thierry Descombes/..."
```

Types d'alerte :

- 1 machine locale a communiqué (connexion établie) avec + de X machines externes

  => *connexion type « **peer to peer** » (emule, skype mode router...)*

- 1 machine locale a scanné une machine externe (connexions non établies)

- 1 machine locale a scanné plusieurs machines externes

- 1 machine externe a scanné une machine interne

- 1 machine locale a eu du trafic vers une machine externe définie comme compromise

  => liste dans la configuration (utilisation des alertes grilles et des alertes du CERT, hub dc++, serveurs eMule, sites de téléchargements, serveurs VPN anonyme...)

  => Mutualiser la gestion des listes ?

Types d'alerte

- 1 machine locale interroge un serveur DNS externe inconnu.
- Adresse IP locale dupliquée
- 1 machine locale a eu du trafic SMTP sortant de plus Y KB

  => trafic important vers un serveur SMTP inconnu => SPAM

=> Alertes envoyées par mail et stockées en base

=> Activables et désactivables

=> Seuils et exceptions configurables

=> Alertes pertinentes

Exemple d'alerte Mail

- ***ALERT OUTGOING SCAN, IPloc: 192.168.2.115***
- Outgoing Scan Detection: The host has probably scanned host 85.1.48.148 (148-48.1-85.cust.bluewin.ch) - 102 flows in 15 mn
- Ports used: 41046/Udp 63976/Udp 63977/Udp 63979/Udp 63980/Udp 63981/Udp 64115/Udp 64116/Udp 64117/Udp …

- ***ALERT SUSPICIOUS HOST, IPloc: 192.168.2.80***
- Host has communicated with suspicious host:
- IP address: 199.7.177.236
- hostname: w15.hotfile.com type: www.hotfile.com
- details(in GMT time) : '09/02/11 06:55:40' 192.168.2.80(*/TCP) > 199.7.177.236(80/TCP) Flg=APSF Inc=57835 Out=6754 PkInc=58 PkOut=44 Dur='29s'

Exemple d'alerte Mail

- ***ALERT MULTIPLE DEST SCAN, IPloc: 192.168.2.217***
- Host has scan 214 different hosts (in 15 mn)
- List of hosts: 111.2.231.0(8090/TCP), 218.90.3.1(8090/TCP), 116.9.101.2(8090/TCP), 115.199.211.2(8090/TCP), 114.235.225.2(8090/TCP), 123.185.131.3(8090/TCP), …
- => Trojan, Virus ?

- ***ALERT MANY EXTERNAL RECIPIENTS, IPloc: 192.168.2.43***
- Host has communicated with 383 different hosts (in 15 mn)
- List of hosts: 193.51.224.6(80/TCP), 195.10.18.9(80/TCP), 193.51.224.9(80/TCP), 66.220.158.11(80/TCP), 69.171.242.13(80/TCP), 66.220.147.14(80/TCP), ...
- => Skype, eDonkey, ...

Performance

- Bonne tenue en charge.

Interface graphique

- Objectifs de l'interface graphique
- - l'ergonomie
- - la simplicité
- - la performance

- => ***DEMO***

Etat actuel

- Déploiement dans tout l'IN2P3 mi-septembre. 5 mois de CDD pour Ismaël financé par l'IN2P3
- Une 10aine de labos impliqués (bug reports, suggestion d'évolution, …)
- Version 1.1 : finalisée et complètement debuguée. Prochainement en ligne sur www.znets.net
- Version 1.2 en développement. Nouveaux graphs, Top10 par FAI, moteur de recherche d'alerte, présélection... pour la fin de l'année
- => Après... Valorisation CNRS ?

Conclusion

- ZNeTS ne remplace pas IDS et monitoring SNMP
- 1 outil complet, simple, fiable et abouti pour:
- - la traçabilité (savoir qui a fait quoi, quand, comment et pouvoir remonter plusieurs mois en arrière)
- - la supervision (transparent pour les clients, facile à déployer)
- - la détection d'anomalie avec seuils adaptables (alertes & analyse grâce aux traces)