
NET REPORT

Présentation Société

DATASET / NETREPORT, propose une offre complète de solutions dans les domaines suivants:

- Outils d'aide à la décision
  - Gamme DATASET

- Solutions de gestion temps réel du système d'information (analyse de logs et gestion proactive des incidents)
  - Gamme NETREPORT

Problématique rencontrée…

- Toutes les sociétés possèdent des équipements réseau & sécurité
- Ils génèrent des logs … et ces logs sont stockés ..au mieux ?
- Ces logs sont ils analysés ?
- Si oui, les rapports sont-ils pertinents et adaptés aux besoins ?
- Sont-ils générés avec un seul outil ?
- Sont-ils centralisés en un seul point ?
- Peut-on répondre avec les outils actuels aux questions suivantes :
  - ★ Quel % de bande passante occupe le trafic mail ?
  - ★ Combien de rejets génère leFirewall par jour ?
  - ★ Combien d'attaques surviennent par mois ?
    - De quel type sont-elles ?
    - Quels sont les services / machines visés ?

- Existe t-il une méthode d'alerte sur les événements critiques de votre système d'information ?

- En fonction d'événements ou d'une suite d'événements, est-il possible générer une action adaptée à l'architecture ?

NET REPORT
Solution Suite

- Net Report propose des solutions de gestion temps réel du système d'information de l'entreprise permettant :

  ★ Une meilleure analyse de vos Log grâce a des rapports adaptés et personnalisable

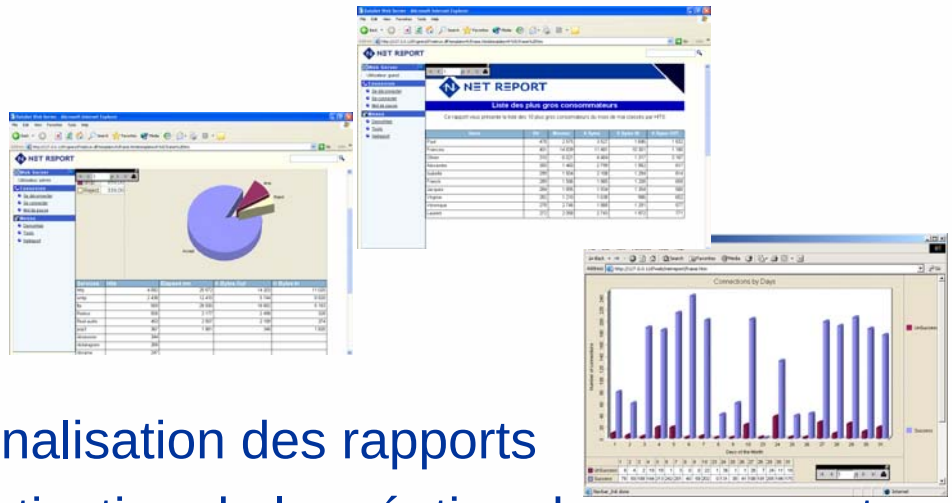
  ★Une gestion temps réel des événements pour être pro-actif sur les éventuels incidents.

NET REPORT LOG ANALYSER SUITE

NET REPORT MONITORING CENTER

NET REPORT
LOG ANALYSER SUITE

- Puissant outil de reporting, Log Analyser fournit :
  - Des rapports statiques planifiés
  - Des rapports dynamiques temps réels consultables à la demande
  - Le support de nombreux équipements tels que :
    - ★ Firewalls
    - ★ Proxy
    - ★ Web
    - ★ Détection d'Intrusion
    - ★ Serveur Radius
    - ★ Autres (wmi, routeurs…)



  - La customisation et la personnalisation des rapports
  - Un planificateur pour l'automatisation de la création de vos rapports
  - Un Portail Web sécurisé pour la consultation et la génération des rapports

NET REPORT LOG ANALYSER
Rapports

- Les rapports statiques automatisés de manière journalière, hebdomadaire ou mensuelle, permettent d'obtenir des informations pertinentes sans configuration additionnelle.

- Les rapports dynamiques permettent la consultation des données en temps réel et la génération de rapports à la demande entièrement paramétrables.

- Ces différents rapports peuvent être générés aux formats suivants :
  - Html
  - Excel
  - Pdf

- Collectés à partir de nombreux formats : WELF, W3C, LEA (Check Point), Syslog, Fichiers à plat, Radius, Microsoft WMI, ils supportent de nombreux équipements du marché …

NET REPORT LOG ANALYSER
Equipements leaders supportés

Firewalls / VPNs

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

NetScreen

Cisco Systems

NOKIA Connecting People

SONICWALL

NETASQ Firewall & VPN Solutions

symantec.

...

Proxy / Web

Microsoft

BlueCoat Systems

SQUID

Netscape

...

Intrusion Détection Serveur Radius

Internet Security Systems

ActivCard

SNORT

RSA SECURITY

...

Anti-Virus et autres

TREND MICRO

symantec.

CLEARSWIFT

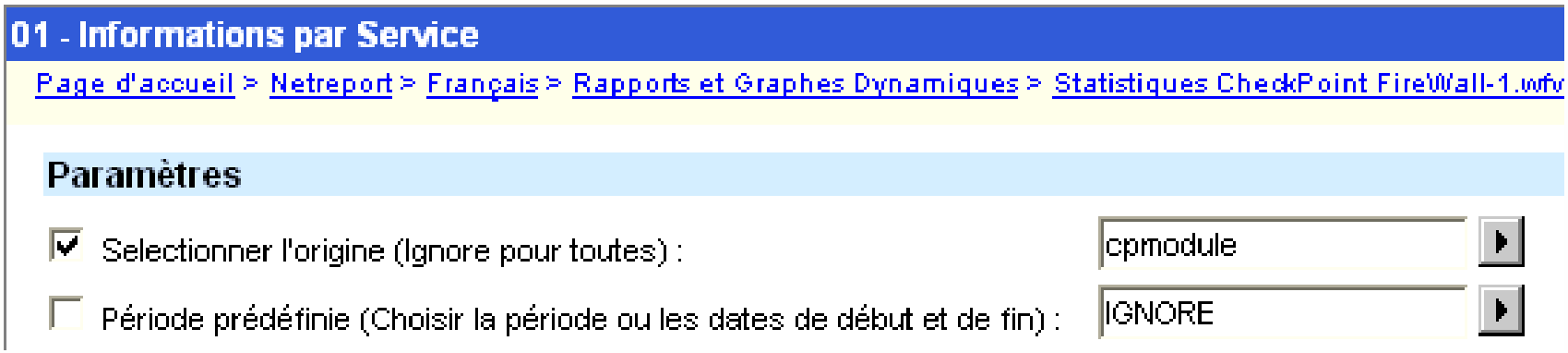
radware get certain

WEBSENSE.

...

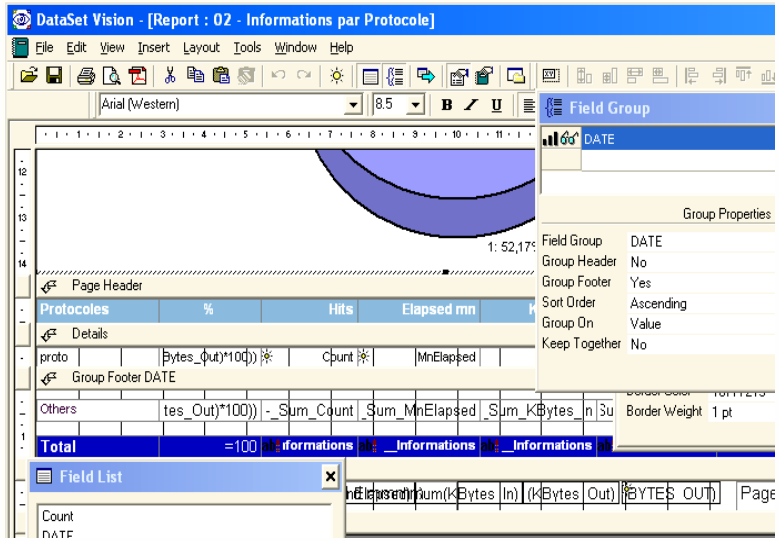
NET REPORT LOG ANALYSER : Web PORTAL

- Portail de consultation des rapports statiques et dynamiques
- Gestions de différents profils utilisateurs
- Notions de paramètres pour la génération de rapports dynamiques par type d'équipements
  - ✓ Services
  - ✓ Type d'attaque
  - ✓ Priorité
  - ✓ Date / Heure



Customisation

- Un Toolkit en option permet de :
  - Modifier les rapports existants
  - Créer de nouveaux rapports
  - Personnaliser les rapports aux couleur de la société

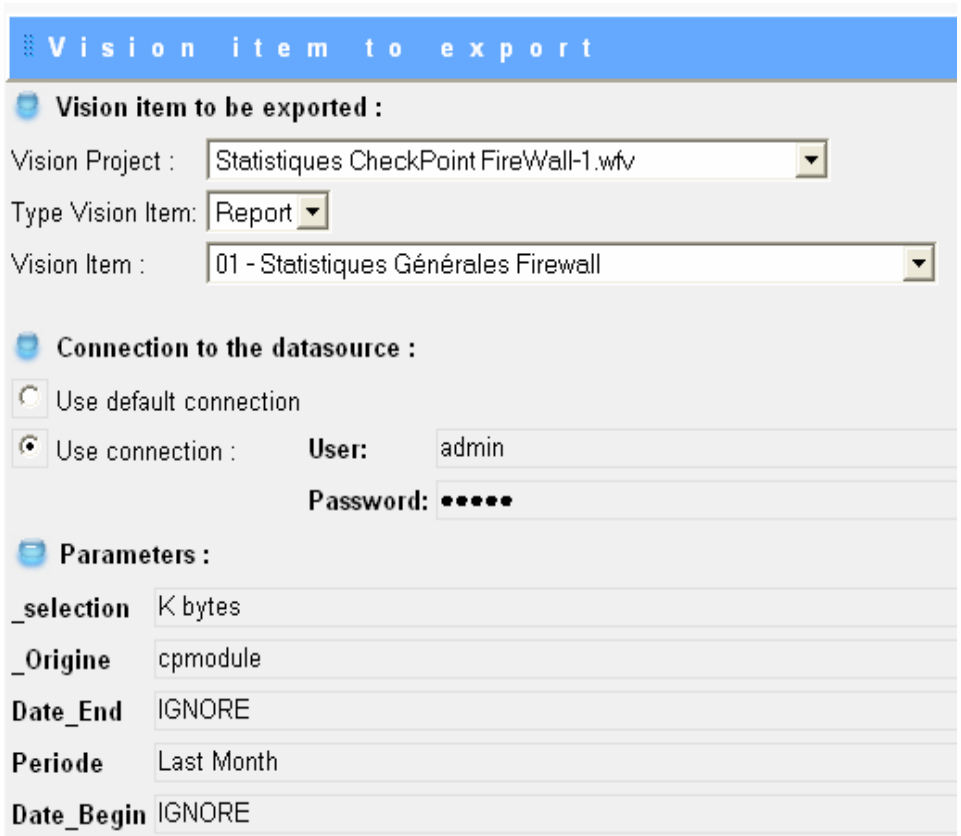


Scheduler

- Permet de mettre en place la génération des rapports récurrents à dates et heures fixes.

- Envoi automatique d'un Email dès mise à disposition du rapport

- Souplesse de paramétrage (ex : 3eme jour de chaque mois, 1 mois sur 2 etc …)



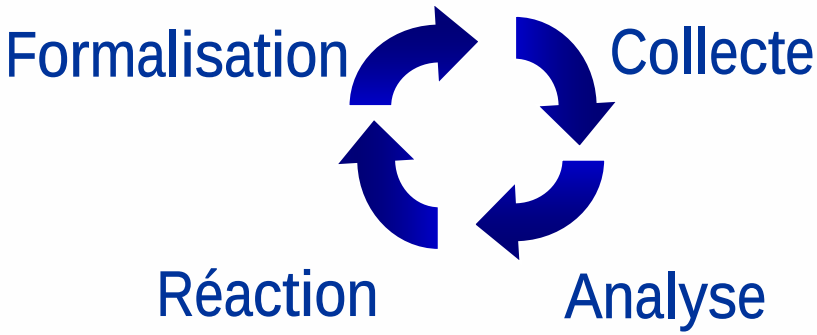
NET REPORT MONITORING CENTER

- Net Report Monitoring Center permet une gestion temps réel du système d'information de l'entreprise sur des attaques,alertes ou incidents de manière à garantir et améliorer les performances et la disponibilité du système d information

Principe

NetReport
Log Analyzer

✓Logs génériques
✓Logs spécifiques



✓Actions déclenchées sur événements par équipements (FW, Sonde, Serveurs ..)
✓Type Actions infini
✓Temps réel

✓Agrège les données
✓Complète à partir différentes sources
✓Filtre les événements sensibles

NET REPORT MONITORING CENTER

- Alerting multi équipements
- Possibilité de créer ses propres alertes et actions
- Filtre configurable
- Compteurs de Sessions / Seuil

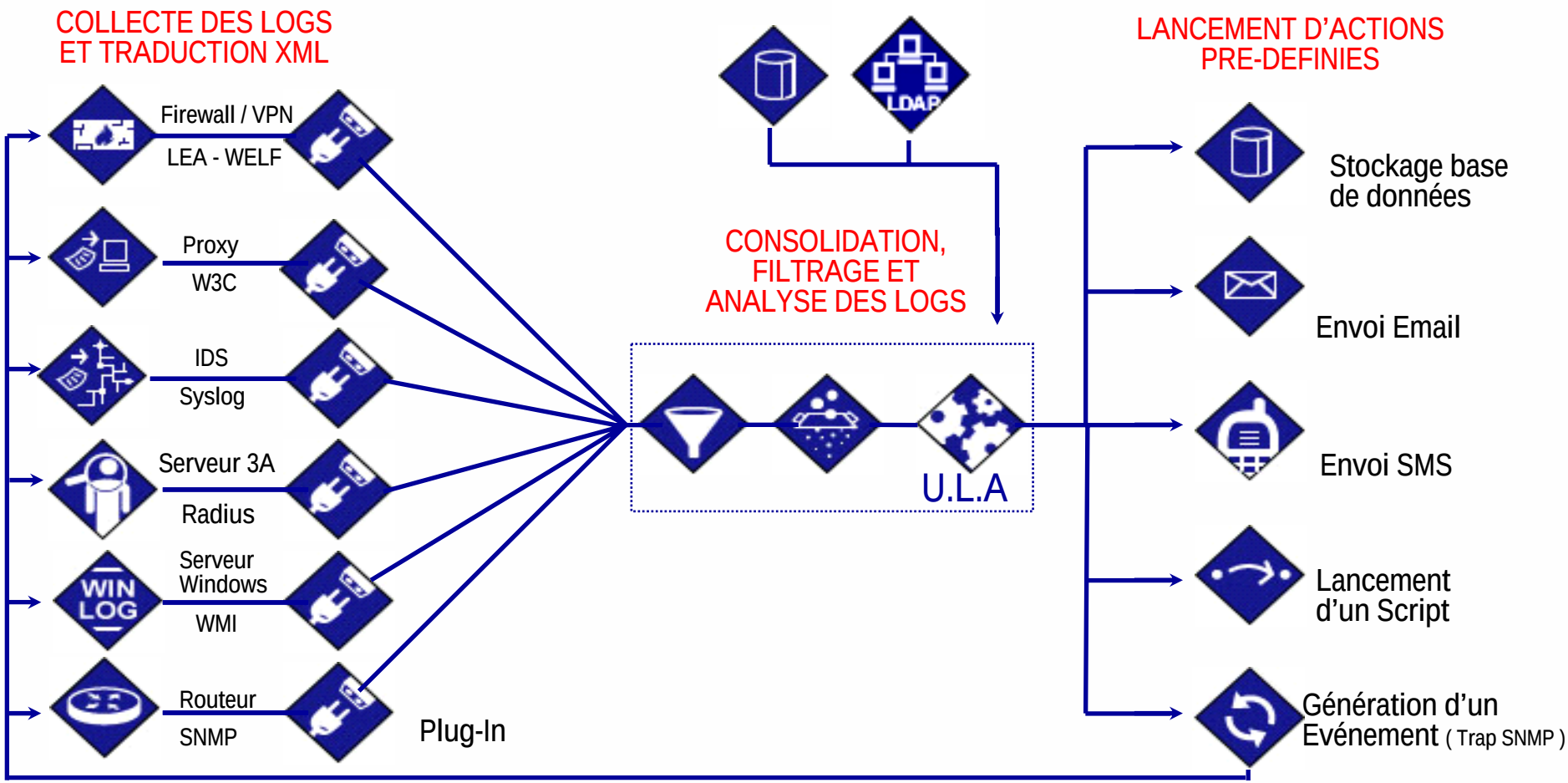
Syslog Main Rule Group

>NetReport/Local/ULA/Filters/syslogagent/Rules/Syslog Main Rule Group<

#	Action	Active	Critical		level		facility		SessionCoun
1	Send E-Mail Priority	yes	no	=	3 Error			>	5
2	Debug Message Box	no	no						
3	Send to SNORT	no	no			=	16 Local0		
4	Stop All	yes	no						

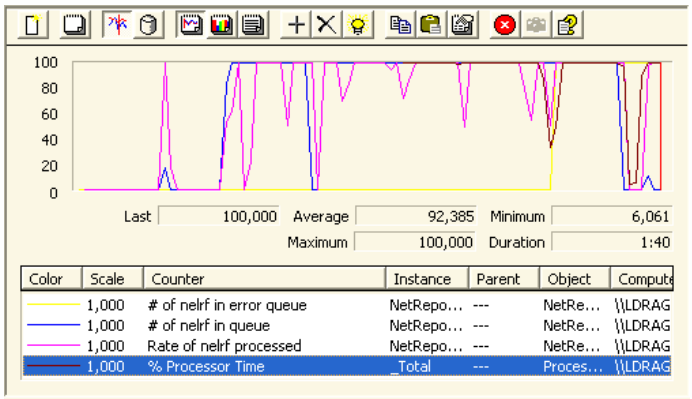
- Méthode d'alertes multiples (SMTP, SNMP, GUI)
- Agent de collecte transparents
- Monitoring Center inclus Log Analyzer

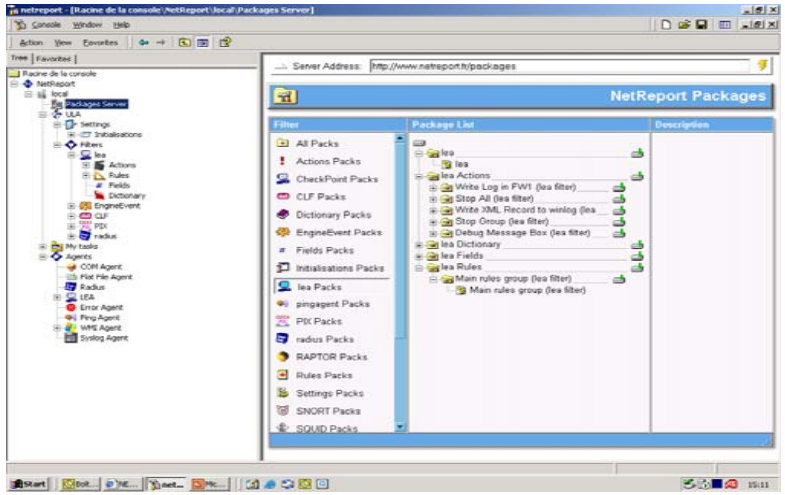
NET REPORT MONITORING CENTER : Architecture



NET REPORT MONITORING CENTER : Administration simple et efficace

- Administration d'un nombre illimité de moteurs d'analyses centralisé à partir d'une Microsoft Management Console (MMC)





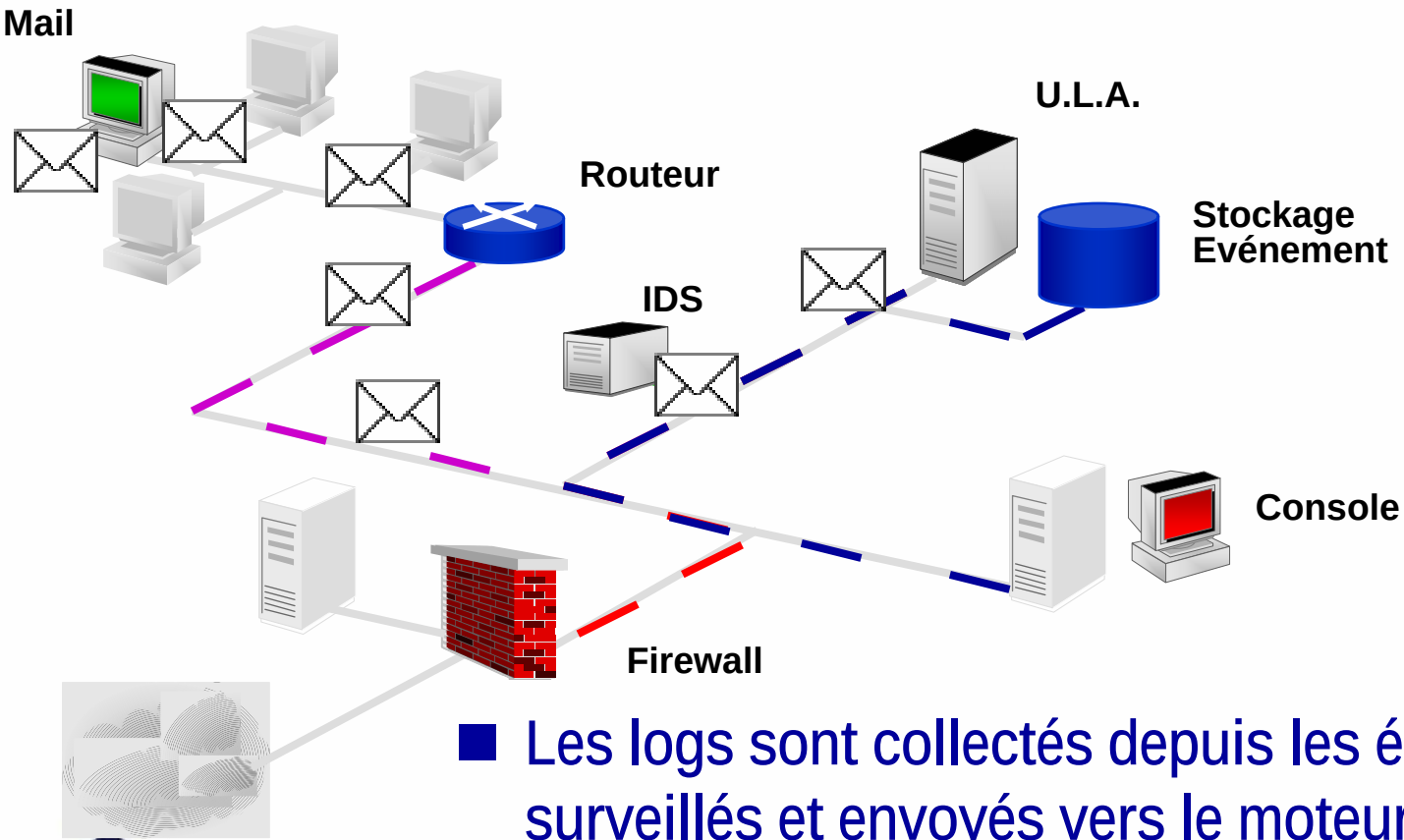
- Solution de micro-updates via le site Web de NetReport des Packages/ Actions/ Filtres/ Champs/ Dictionnaires
- Moniteur de performances temps réel

Microsoft WMI (Windows Management Instrumentation)

- Monitoring complet d’un système Windows
  - Plus qu’un simple analyseur de journaux d’événements
  - Permet d’accéder a toutes les fonctions de monitoring du système et interagir avec:
    - Utilisateurs en session
    - État des services
    - Charge processeur
    - Espace disque
    - Etc…

NET REPORT MONITORING CENTER :
Actions Pro actives mono-équipements

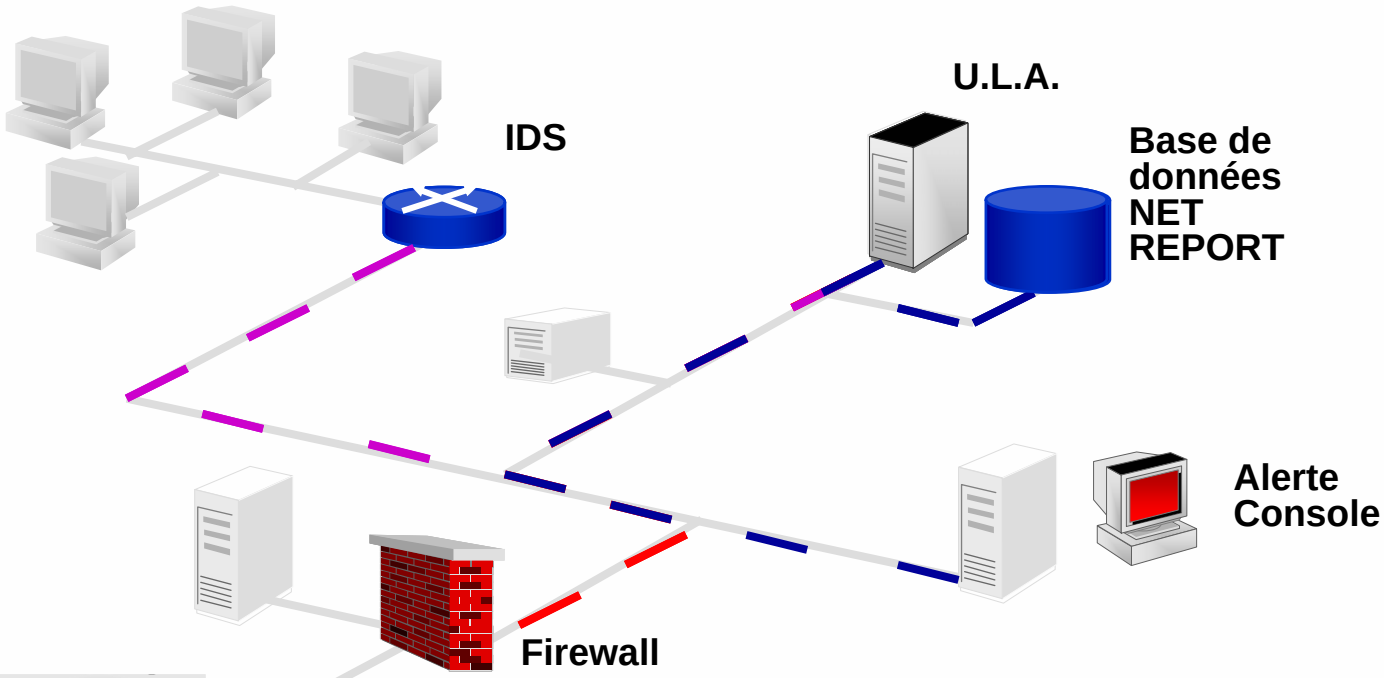
- Les événements sont traités grâce à un set de règles qui déclenche les actions appropriées



- Les logs sont collectés depuis les équipements surveillés et envoyés vers le moteur d'analyse

NET REPORT MONITORING CENTER :
Actions Pro actives multi-équipements

Un événement survient sur la sonde, l'information est stockée dans la base NetReport



Un événement survient sur le firewall ET sur la sonde , alors une alerte est générée sur la console

Un événement survient sur le firewall, l'information est stockée dans la base NetReport

Merci de votre attention

Infos@NetReport.fr

http://www.NetReport.fr