heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2007

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

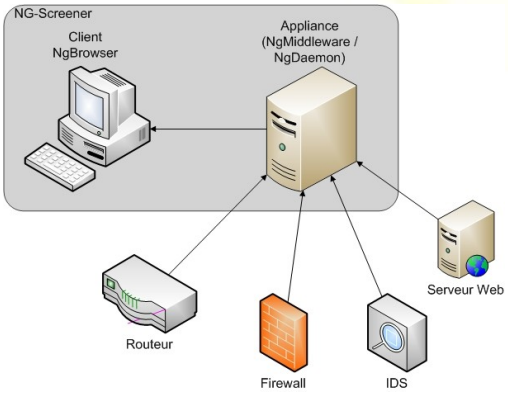
Visualisation et interprétation graphiques de données liées à la sécurité informatique

Contexte

Le domaine de la récolte et de l'analyse d'événements de type sécuritaire devient vite complexe avec le temps et l'augmentation de la taille des réseaux d'entreprises. C'est pour cette raison qu'un outil de gestion générale permettant la centralisation et la visualisation de ces événements dans des interfaces graphiques évoluées est devenu indispensable à la sécurité des entreprises. Cet outil permet également d'analyser et de corréler ces événements avec beaucoup plus de souplesse que les méthodes utilisées actuellement.

Architecture

La solution Ng-Screener a pour but de centraliser, stocker, normaliser, traiter, visualiser et enfin analyser les millions d'événements journaliers de type sécuritaires issus des réseaux d'entreprise. Le but premier du produit est de donner aux administrateurs réseaux, une suite d'outils permettant la détection d'intrusions et une aide à l'investigation. Un autre point essentiel du produit est la possibilité de produire des rapports d'audits sécuritaires permettant ainsi d'évaluer la politique de sécurité de l'entreprise en la comparant aux normes et standards actuels.



NG-Screener est composé de deux parties principales :

Une partie serveur (Appliance), basée sur une récupération, un stockage, une normalisation et un traitement des alertes provenant du réseau.

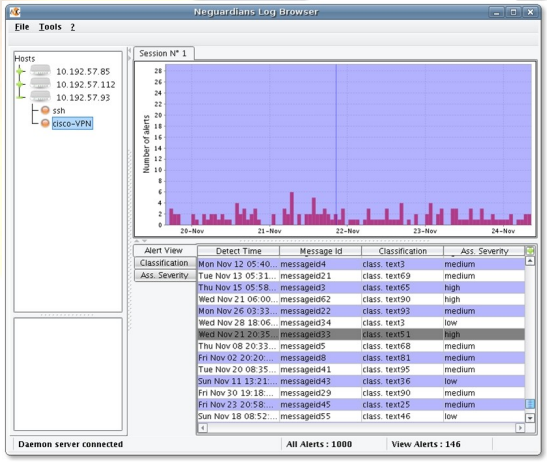
Une partie client, basée sur une interface de visualisation et d'interprétation graphiques d'événements de type sécuritaire.

Récolte des événements

L'Appliance s'occupe de récupérer et de stocker les événements envoyés par les différents éléments réseaux surveillés. Ces événements sont ensuite normalisés et traités à la demande de l'utilisateur.

Interface de visualisation

L'interface graphique du client propose plusieurs vues à l'utilisateur (statistiques, vue temporelle, liste d'évènements, etc.) lui permettant d'avoir une vue d'ensemble sur la situation de son réseau.



Technologies utilisées

Java 6, PostgreSQL, Hibernate, Serveur Linux et BTM Transaction.

Auteur: **SYDLER Gregory**
Répondant externe: **MAIO Raffael**
Prof. responsable: **FATEMI Nastaran**
Sujet proposé par: **NetGuardians SA**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale