Sécurité et Surveillance des systèmes

Les moyens de sécurisation et de surveillance

Avec la démocratisation des outils informatiques, le besoin de sécurisé et monitorer notre cœur de réseaux s'est imposé.

Pour cela plusieurs moyen ont étais mis en place par les différentes sociétés du monde du numérique.

La sécurisation des système via la mise en place de Systèmes de détections d'intrusions (IDS: Intrusion detection system) dont le Pare-feu fait partie.

Le filtrage des navigation des utilisateurs d'une société grâce au Proxy.

L'observation en temps réel des hôte d'un réseau via les solution de Monitoring.

Systèmes de détections d'intrusions (IDS: Intrusion detection system)

Un IDS est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).

Il permet ainsi d'avoir connaissance des tentatives d'intrusions réussites ou échouées.

Il existe deux grandes catégories:

- Les SIDS (Signature-based intruction detection system) analysant les signatures des paquet

Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera detectée.

Cette signature peut référencer un seul paquet, ou un ensemble (dans le cas d'une attaque par déni de service). Cette méthodologie de détection se révèle être efficace uniquement si la base de signatures est maintenue à jour de manière régulière.

- Les AIDS (Anomaly-based Intrusion Detection System) identifie les anomalies de comportment

Lors de l'analyse du flux réseau les AIDS vont se charger de détecter des comportements anormaux. Pour cela, le système va reposer sur deux phases:

- Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau.

- Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances.

Source WIKIPEDIA

Pare-feu (Firewall)

Un pare-feu (de l'anglais firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique.

Il surveille et contrôle les applications et les flux de données (paquets).

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.

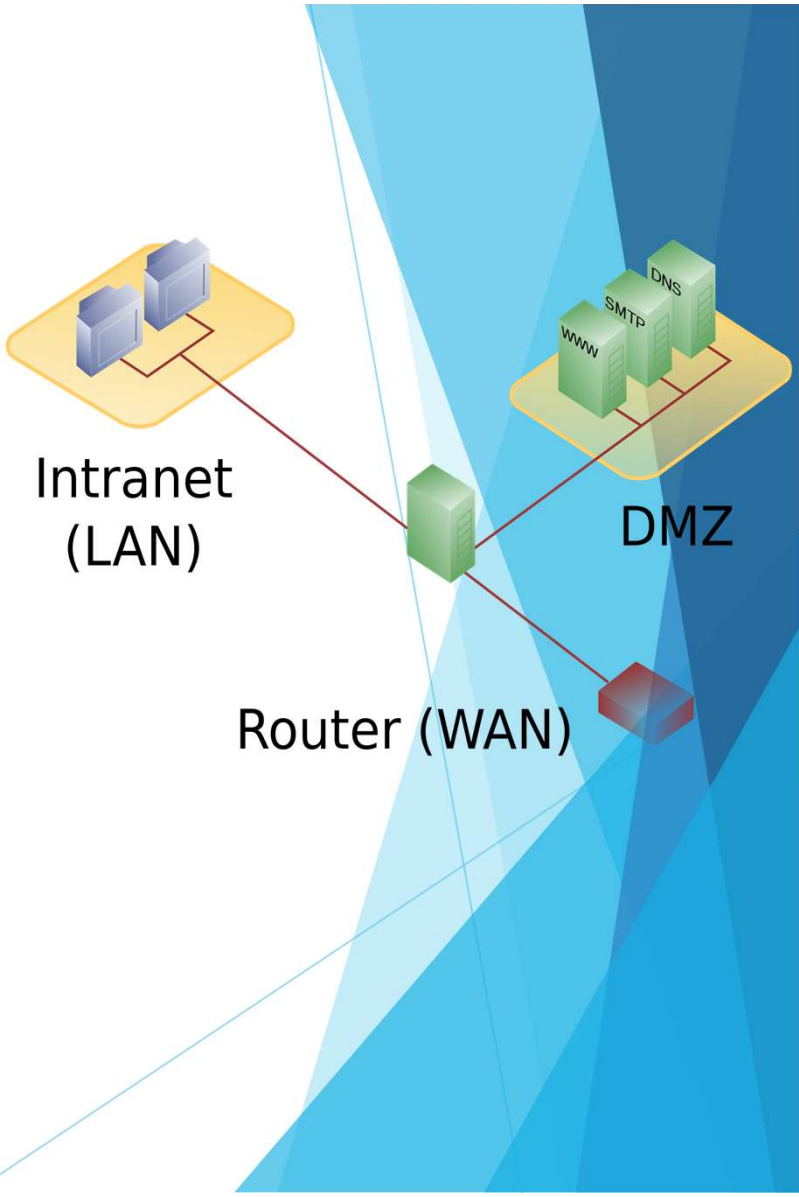
Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).

Le filtrage se fait selon divers critères. Les plus courants sont :

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;
- les options contenues dans les données (fragmentation, validité, etc.)
- les données elles-mêmes (taille, correspondance à un motif, etc.) ;
- les utilisateurs.

Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte.

Source WIKIPEDIA



Proxy

Un proxy est un composant logiciel informatique intervenant au niveau de la couche application (HTTP, FTP, SSH, etc.) qui joue le rôle d'intermédiaire pour accéder à un autre réseau, généralement Internet.

Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.

Un proxy permet:

- l'acceleration de la navigation grâce au a la mise cache, la compression des données, et le filtrage des publicités ou des contenus lourds (Java, Flash)
- la journalisation des requêtes
- le filtrage et l'anonymat

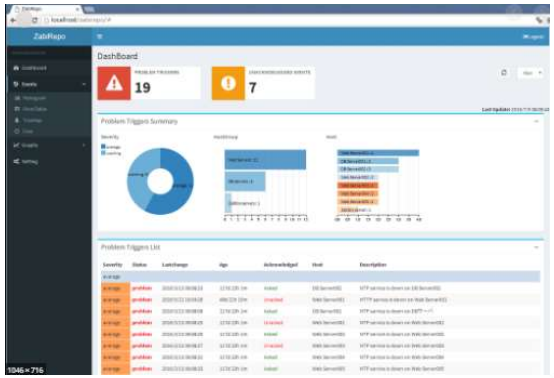
Monitoring ou Supervision

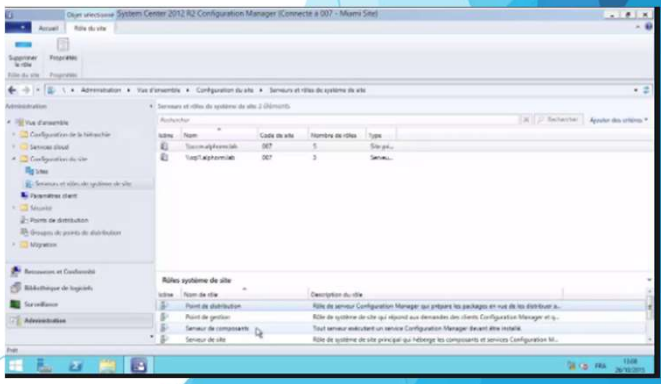
Le monitoring se définit par la vérification et la mesures statistiques de l'états des hôte d'un réseau permettant la mise en place d'alarme en cas d'anomalie ou absence d'une machine ou d'un services.

Les outils de supervision sont nombreux mais seulement trois types de solution existe:

- L'analyse serveur vers hotes
- L'analyse par remonter d'information des hotes vers le serveur (fonctionne généralement avec un agent sur les postes).
- L'analyse Hybride exécutant les deux solutions précédentes dans des cas conditionne par les administrateurs.

Les solutions les plus utiliser sont originaire du monde libre tel que Zabbix et Nagios s'installant sur un OS linux mais Microsoft a aussi une solution appelé SCCM System Client Center Manager integrer dans MECM depuis 2012 R2.





TP1 Installation système

- Installez un serveur 2019 DATACENTER (GUI) avec la configuration matériel ci-après, en vous aidant du lien suivant:

https://www.infonovice.fr/guide-dinstallation-de-windows-server-2019-avec-une-interface-graphique/

SDC0

HDD: 1 x 200 Go

RAM: 8 Go

PROCESSEUR: 1

CORE: 2

- Nommer le serveur SDC0 et modifier son adressage IP en vous référent spécificités.

Spécificité:

Nom:	SDC0
IP Statique:	@NAT .100
IP Statique DNS:	@NAT .100
IP Statique Passerelle:	@NAT

TP2 Installation ADDS

- Renommez le disque local C:\ en SYSTEM
- Installez ensuite le Rôle ADDS sur SDC0 et créez la forêt ECHO.com
- Créez les groupes IT, COMPTA et RH.
- Créez les utilisateurs IT1, COMPTA1, RH1 et ADMIN1.
- Ajoutez IT1 dans IT, COMPTA1 dans COMPTA, RH1 dans RH et ADMIN1 dans le groupe admins du domaines , Administrateurs du schéma et Administrateurs
- Ajouter la zone de recherche inverse a votre DNS en vous aidant du tutoriel suivant:

http://pbarth.fr/node/31

TP3 Installation DHCP

- Sur SDC0 activé le rôle DHCP
- Créez l'étendue DHCP entre @passerelle et @IP SDC0 (logiquement .100) en excluant les adresse IP de votre @passerelle et @SDC0.

https://www.pc2s.fr/installation-du-role-serveur-dhcp-sur-windows-serveur-2019-2016-ou-2012-r2/

TP4 P1 Installation système

- Installez un serveur 2019 DATACENTER (GUI) avec la configuration matériel ci-après, en vous aidant du lien suivant:

https://www.infonovice.fr/guide-dinstallation-de-windows-server-2019-avec-une-interface-graphique/

SDC1

HDD: 1 x 500 Go
RAM: 12 Go
PROCESSEUR: 2
CORE: 2

- Nommer le serveur SDC1 et modifier son adressage IP en vous référent spécificités.
- Ajoutez l'exception @nat.80 a votre étendue DHCP

Spécificité:

Nom:	SDC1
IP Statique:	@NAT .80
IP Statique DNS:	@NAT .100
IP Statique Passerelle:	@NAT

TP4 P2 Installation MECM

- Sur SDC1 installez SCCM en vous aidant tu tutoriel suivant:

https://www.it-connect.fr/modules/sccm-decouverte-prerequis-et-installation/

TP5 Installation client

- Creez une machine Windows 10 LPT001 avec la configuration matériel ci après:

LPT001

HDD: 1

1 x 60 Go

RAM: 2 Go

PROCESSEUR: 1

CORE: 2

- Ajoutez LPT001 dans le domaine ECHO.COM avec le compte ADMIN1
- Connectez l'utilisateur COMPTA1

TP6 Installation FSP (Federation Service Proxy)

- Sur SDC0 installez FSP en vous aidant tu tutoriel suivant:

https://docs.microsoft.com/fr-fr/windows-server/identity/ad-fs/deployment/install-the-federation-service-proxy-role-service

- [AUTONOMIE] Configurez LPT001 pour que COMPTA1 utilise le serveur proxy de SDC0