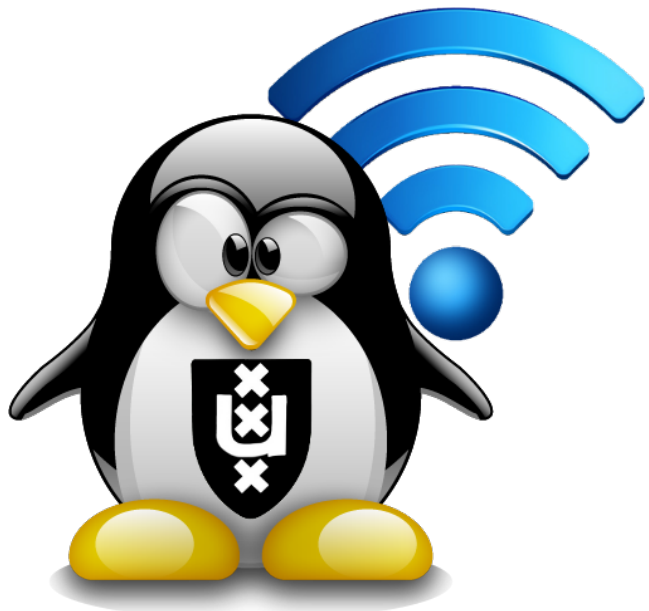
Les Réseaux

Éric BERTHOMIER
eric.berthomier@free.fr

March 16, 2022



Version 1.0 - Version Stagiaire

Warriors of the Net (1999)

Écoutez, regardez, prenez des notes . . .

Warriors of the Net - Vocabulaire

IP packet	Paquet IP (Internet Protocol)
Proxy Server	Serveur Proxy ou Mandataire
LAN	Local Area Network - Réseau Local
Novell packets	- Paquet Novell IPX/SPX
Apple Talk packets	- Paquet Apple Talk (Mac)
Router	- Routeur
Router Switch	- Switch
Firewall	- Firewall
Ping Of Death	- Ping de la Mort
Ports	- Port d'écoute

Serveur Mandataire ou Proxy

Un serveur proxy (serveur mandataire en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

Serveur Mandataire ou Proxy

Un serveur proxy (serveur mandataire en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (java, flash);

Serveur Mandataire ou Proxy

Un serveur proxy (serveur mandataire en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (java, flash);
- journalisation des requêtes (logging) ;

Serveur Mandataire ou Proxy

Un serveur proxy (serveur mandataire en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (java, flash);
- journalisation des requêtes (logging) ;
- sécurité du réseau local ;

Serveur Mandataire ou Proxy

Un serveur proxy (serveur mandataire en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (java, flash);
- journalisation des requêtes (logging) ;
- sécurité du réseau local ;
- filtrage et l'anonymat.

Serveur Mandataire ou Proxy

Un serveur proxy (serveur mandataire en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (java, flash);
- journalisation des requêtes (logging) ;
- sécurité du réseau local ;
- filtrage et l'anonymat.

Source Wikipédia : `http://fr.wikipedia.org/wiki/Proxy`

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 communication autorisés sur ce réseau informatique.
Le filtrage se fait selon divers critères.

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 communication autorisés sur ce réseau informatique.
Le filtrage se fait selon divers critères.

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;

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 communication autorisés sur ce réseau informatique.
Le filtrage se fait selon divers critères.

- 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.) ;

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 communication autorisés sur ce réseau informatique.
Le filtrage se fait selon divers critères.

- 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.) ;

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 communication autorisés sur ce réseau informatique.
Le filtrage se fait selon divers critères.

- 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 pour les plus récents.

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 communication autorisés sur ce réseau informatique.
Le filtrage se fait selon divers critères.

- 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 pour les plus récents.

Source Wikipédia :
`http://fr.wikipedia.org/wiki/Pare-feu_(informatique)`

Ping de la Mort

Le ping de la mort (en anglais ping of death ou PoD) est une attaque historique de type déni de service réalisé par l'envoi de paquet ping **malformé**.

Ping de la Mort

Le ping de la mort (en anglais ping of death ou PoD) est une attaque historique de type déni de service réalisé par l'envoi de paquet ping **malformé**.
Un ping a normalement une taille de 56 octets (soit 84 octets avec l'entête IP), or certains systèmes n'étaient pas en mesure de traiter correctement les paquets plus gros que la taille maximale (65 535 octets) pouvant provoquer un crash de la machine cible.

Ping de la Mort

Le ping de la mort (en anglais ping of death ou PoD) est une attaque historique de type déni de service réalisé par l'envoi de paquet ping **malformé**.
Un ping a normalement une taille de 56 octets (soit 84 octets avec l'entête IP), or certains systèmes n'étaient pas en mesure de traiter correctement les paquets plus gros que la taille maximale (65 535 octets) pouvant provoquer un crash de la machine cible.

Source Wikipédia :
`http://fr.wikipedia.org/wiki/Ping_de_la_mort`

Déni de Service (DOS)

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

Déni de Service (DOS)

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- linondation dun réseau afin d'empêcher son fonctionnement ;

Déni de Service (DOS)

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- linondation dun réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;

Déni de Service (DOS)

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- linondation dun réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier.

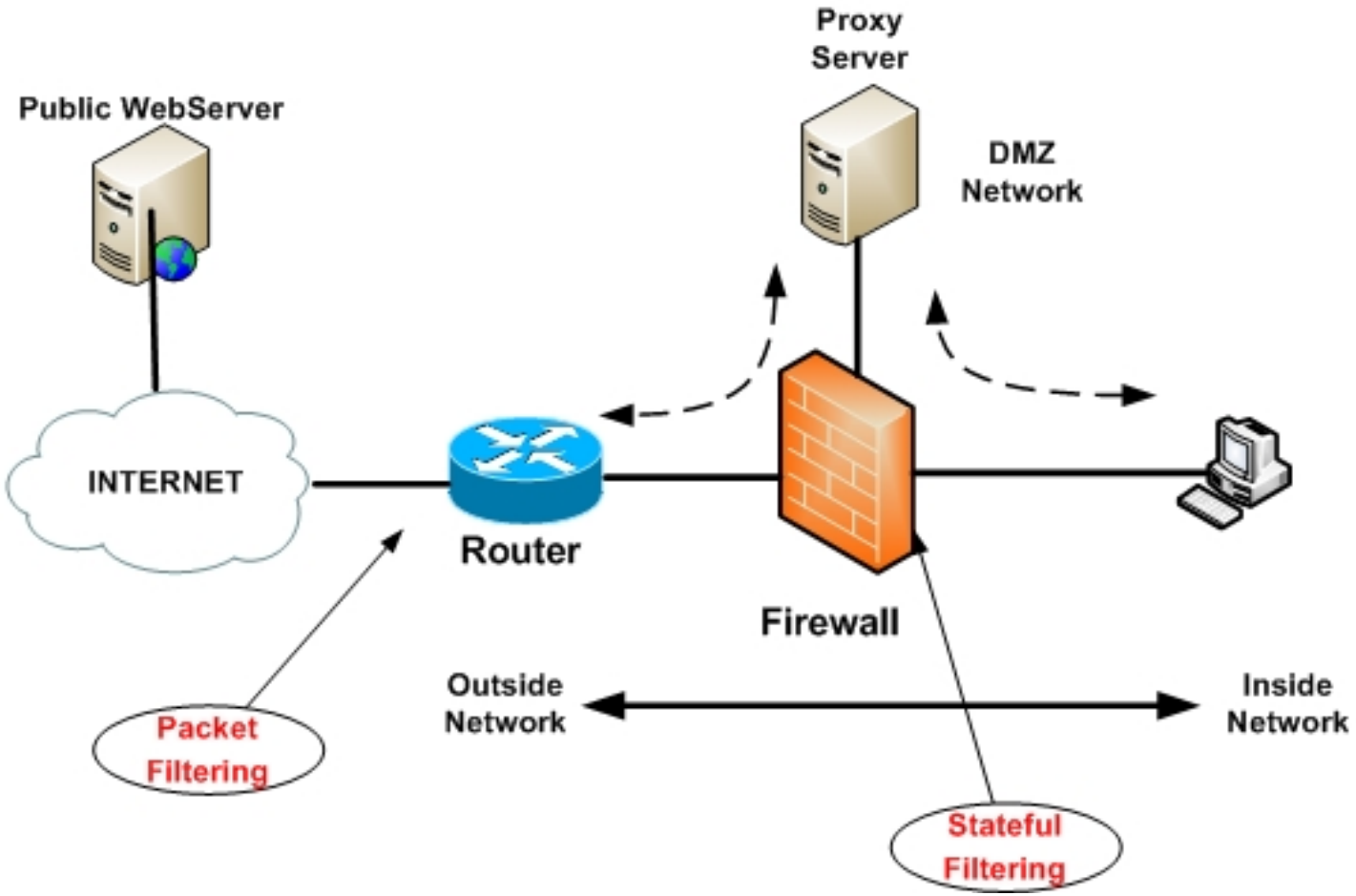
Déni de Service (DOS)

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- linondation dun réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier.

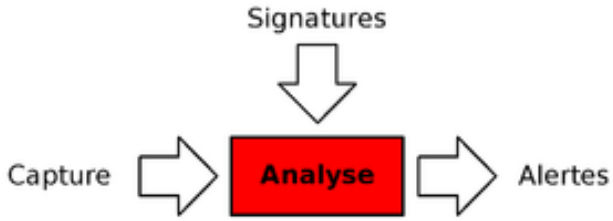
Source Wikipédia : `http://fr.wikipedia.org/wiki/Attaque_par_déni_de_service`

Schéma simple d'un réseau d'entreprise



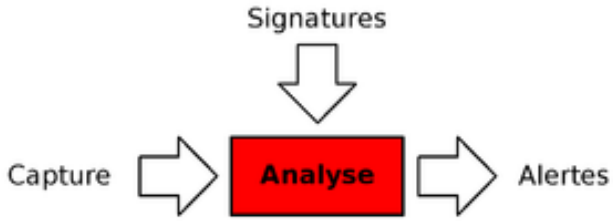
Mieux protéger : IDS

Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).



Mieux protéger : IDS

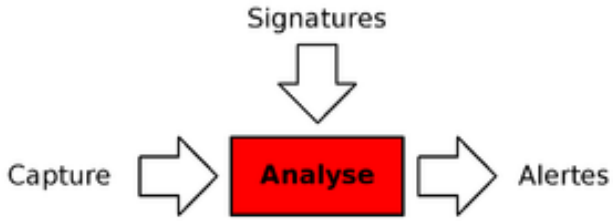
Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).



1. La **capture** sert à la récupération de trafic réseau.

Mieux protéger : IDS

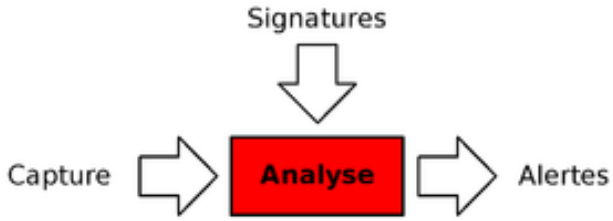
Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).



1. La **capture** sert à la récupération de trafic réseau.
2. Les **bibliothèques de signatures** (approche par scénario) rendent la démarche d'analyse similaire à celle des antivirus.

Mieux protéger : IDS

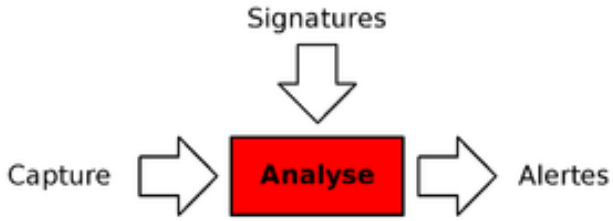
Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).



1. La **capture** sert à la récupération de trafic réseau.
2. Les **bibliothèques de signatures** (approche par scénario) rendent la démarche d'analyse similaire à celle des antivirus.
3. Les **alertes** sont généralement stockées dans les journaux du système.

Mieux protéger : IDS

Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).



1. La **capture** sert à la récupération de trafic réseau.
2. Les **bibliothèques de signatures** (approche par scénario) rendent la démarche d'analyse similaire à celle des antivirus.
3. Les **alertes** sont généralement stockées dans les journaux du système.

Source Wikipédia : `http://fr.wikipedia.org/wiki/Système_de_détection_d'intrusion`

Exemple d'une signature d'IDS : ShellShock

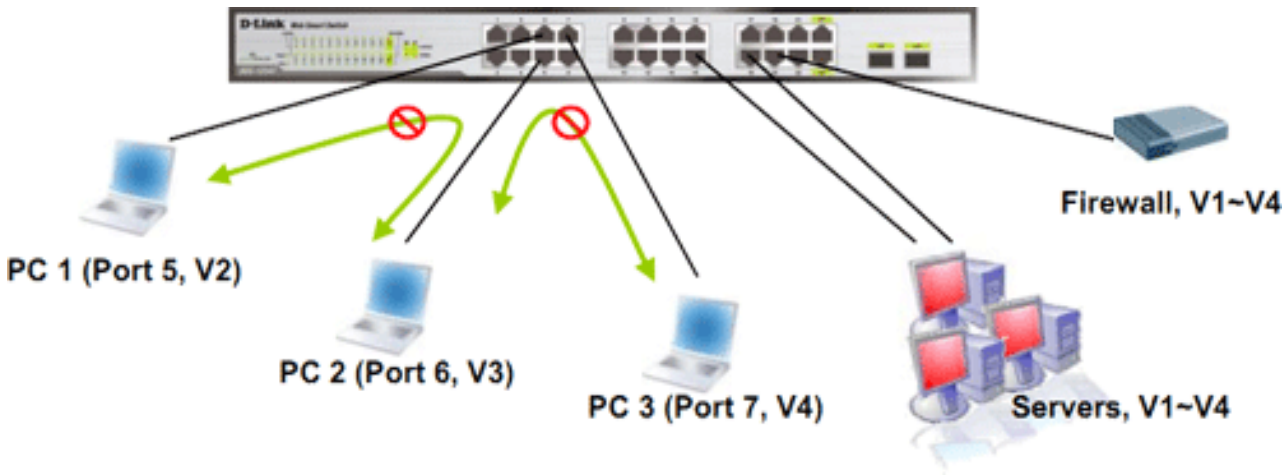
Signatures

Rule sets have now been released for the majority of common IDS systems, although the false positive rate appears to be high on many of the rules.

Vendor	Signatures
Cisco	31975-31978 and 31985
Sourcefire	4689-0, 4689-1,4689-2 and 4689-3
Emerging Threats	2019234, 2019236-2019239, 2019241, 2019244-2019273
Palo Alto	https://threatvault.paloaltonetworks.com/Home/ThreatDetail/36729
F5	https://devcentral.f5.com/articles/shellshock-mitigation-with-big-ip-irules

Protéger son réseau local

Les VLANs (vidéo)



Notre nouveau réseau d'Entreprise

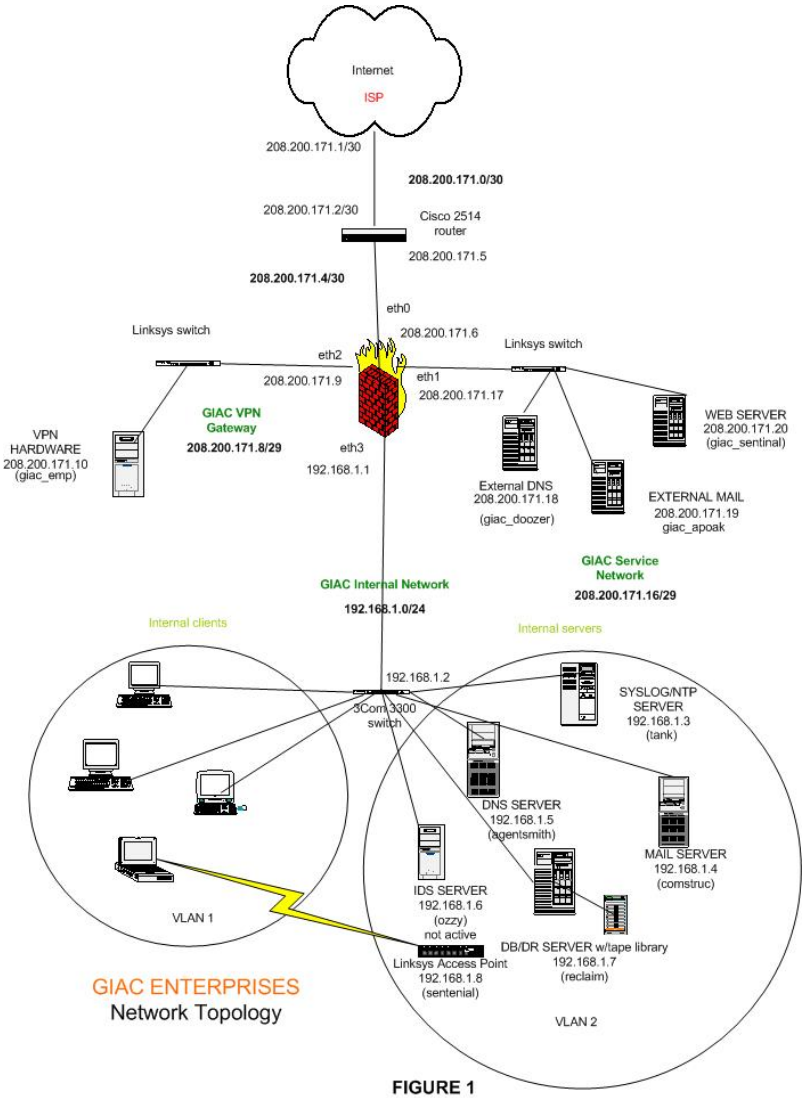
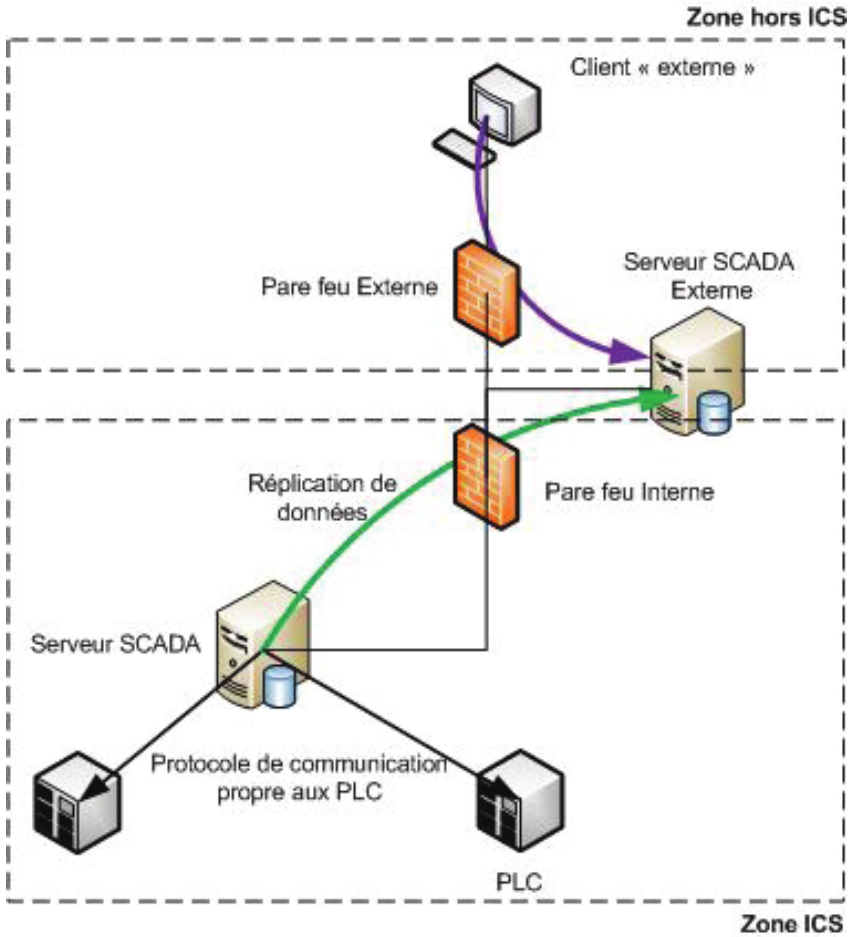


FIGURE 1

Notre nouveau réseau d'Entreprise Industrielle



PLC : Programmable Logic Controller
Source ANSSI : `http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-systemes-industriels/la-cybersecurite-des-systemes-industriels.html`

Analyse d'une faille de sécurité - TA14-353A

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

par contre celui-ci induit des coûts :

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

par contre celui-ci induit des coûts :

- Paramétrage, mise à jour et suivi des éléments actifs, du proxy, du firewall, de l'IDS ...

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

par contre celui-ci induit des coûts :

- Paramétrage, mise à jour et suivi des éléments actifs, du proxy, du firewall, de l'IDS ...

Et du décisionnel

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

par contre celui-ci induit des coûts :

- Paramétrage, mise à jour et suivi des éléments actifs, du proxy, du firewall, de l'IDS ...

Et du décisionnel

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

par contre celui-ci induit des coûts :

- Paramétrage, mise à jour et suivi des éléments actifs, du proxy, du firewall, de l'IDS ...

Et du décisionnel

Conclusion

L'ensemble des éléments mis sur notre réseau nous permettent de :

- Protéger notre réseau de l'extérieur
- Identifier des comportements réseaux suspects.
- Cloisonner nos différents réseaux.

par contre celui-ci induit des coûts :

- Paramétrage, mise à jour et suivi des éléments actifs, du proxy, du firewall, de l'IDS ...

Et du décisionnel

Alerte Firewall, alerte IDS, alerte Proxy ...
Que faire ? Qui fait ? Qui décide ?