Journée « Sécu »

9ème Journée Thématique du Réseau MIn2RIEN

Retour d'expérience sur la mise en place d'un parefeu NG

Mickaël MASQUELIN (**IEMN**)

http://www.min2rien.fr/

Université de Lille — UNR Universités Numériques en Région Nord-Pas de Calais — Min2RIEN — iemn

Villeneuve d'Ascq, France

10 Novembre 2015

Plan

- Introduction
- Contexte
- Premières mesures
- Pare-feu nouvelle génération ?
- Cahier des charges
- Solution retenue
- Questions

1 Introduction

Introduction

- Laboratoire Central de l'Institut (LCI) : site principal de l'Institut d'Electronique, de Microélectronique et de Nanotechnologie (IEMN) ;
- Héberge 21 groupes de recherches, 2 start ups ;
- Un peu plus de 450 personnes (chercheurs, administratifs, …) y travaillent ;
- De nombreux invités (27 nationalités différentes représentées) ;
- 3 plans IPv4 publics, 6 plans IPv4 privés ;
- 29 serveurs (physiques et virtuels) ;
- Plus de 1 150 objets connectés au LAN (ordinateurs, imprimantes, ordiphones, tablettes, …)

2 Contexte

Contexte

Contexte

- Constat (fin 2012) :
  - Parc de machines très hétérogènes ;
  - Postes de travail administrés à la “ va comme j'te pousse ” ;
  - Infogérance réseau ;
  - Très peu de documentation.

- Sécurité du réseau local :
  - Des redondances, inutiles en termes d’ACLs sur :
    - les serveurs (iptables) ;
    - les commutateurs de périphérie ;
    - le controleur Wi-Fi ;
    - les pare-feux (cluster de NetAsq F1000 en HA).
  - De nombreux problèmes de fiabilité liés aux pare-feux NetAsq :
    - Tampon Anti-Virus ou filtrage URL souvent saturé ;
    - Problèmes de HA (problème de négociation maitre/esclave) ;
    - Composants intégrés tels que DHCPd qui dysfonctionnait.

Contexte

- Nouvelles problématiques :
  - BYOD, encapsulation du traffic, …

  - Evolution du contexte réglementaire :
    - Corpus PGSI du CNRS mis à jour, définition de ZRRs, … ;
    - Circulaire du Premier ministre du 17 juillet 2014 qui porte sur la PSSIE.
- Des points positifs malgré tout :
  - Première ligne de sécurité : pare-feux du Campus de l'Université Lille1.

3 Mesures

Mesures

- Modernisation et rationalisation de l'infrastructure :
  - Travail sur la mise en place d'une gestion de parc "efficace" :
    - Serveur AD/DS sous MS Windows Server pour les postes clients ;
    - Déploiement de logiciels pour clients MS Windows.
  - Supervision : utilisation de sondes pour surveiller les services
  - Anti-Virus centralisé, …

Nagios® WAPT

- D'un point de vue réseau :
  - Routage descendu sur le coeur de réseau (en lieu et place des pare-feux) ;
  - Mise en place de VLANs (DMZ, VLAN de management, wireless, …) ;
  - Remplacement des pare-feux (fin de vie des Netasq F1000).

4 Pare-feu nouvelle génération ?

Pare-feu nouvelle génération ?

- Historique :
  - Au commencement :
    - ACL (*non-stateful*) sur les routeurs
  - Années 90 :
    - Premiers pare-feux dits « *stateful* »
    - Filtrage basé sur l'adressage IP et les ports/protocoles (TCP/UDP)
  - Année 2004 :
    - Nouveau concept, les UTM (*Unified Threat Management*)
    - Fonctions de base : Filtrage niveau 4, IPSec, NAT, …
    - + Fonctions ajoutées : Filtrage URL par catégories, IPS, Anti-Virus, …
  - Année 2007 :
    - Commercialisation des 1er pare-feux NG aux Etats-Unis
    - Caractéristiques :
      - Reconnaissance des applications quels que soient les ports utilisés ;
      - Reconnaissance des utilisateurs, quels que soient les IPs utilisées ;
      - Scan des flux pour proposer des fonctions IPS, Anti-Virus, DLP, … ;
      - Déchiffrement des flux SSL.

5 Cahier des charges / spécifications

Cahier des charges / spécifications [extrait]

- Identifier et contrôler les applications, quels que soient les ports, pas seulement les ports standard (y compris http(s)) ;
- Identifier les techniques d'évasion et de contournement (proxy, accès distant, applications dans les tunnels chiffrés, …) ;
- Permettre un contrôle des différentes fonctions d'une même application (ex : autoriser Google Chat mais pas Google Docs) ;
- Détecter les menaces dans une application collaborative autorisée (ex : bloquer les fichiers vérolés en provenance d'un espace collaboratif Sharepoint) ;
- Gérer le traffic inconnu avec des règles (pas seulement le laisser passer) ;
- Identifier et contrôler les applications partageant une même connexion ;
- Disposer du même contrôle et de la même visibilité sur les utilisateurs distants que sur les utilisateurs internes ;
- Simplifier la sécurité réseau : contrôler les applications, sans contrôler la sécurité ;
- Fournir les mêmes débits sans dégrader les performances avec les fonctions de contrôle activées ;
- Déchiffrer le traffic SSL sortant ;

6 Solution retenue

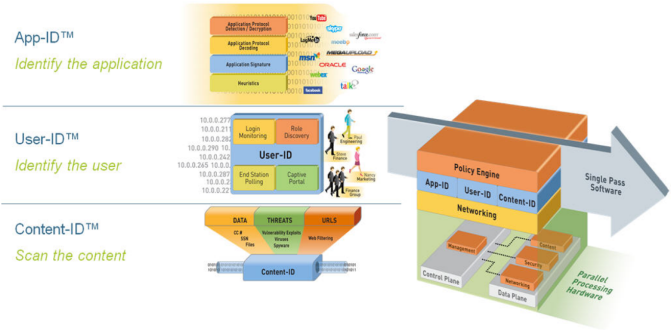
Solution retenue (hardware)

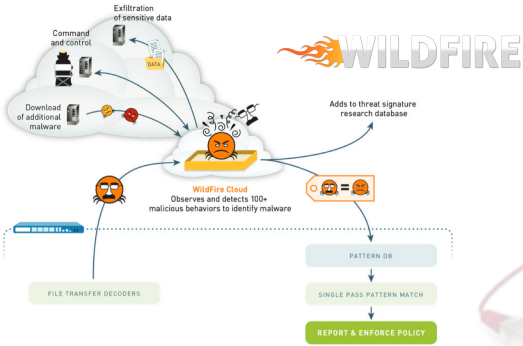
PA-3020

- Pare-feu série PA-3000 (modèle PA-3020)
- Quelques caractéristiques techniques :
  - Cluster haute disponibilité (actif-passif)
  - Débit pare-feu (avec App-ID activé) : 2 Gbit/s
  - Débit pare-feu (avec threat prenvention) : 1 Gbit/s
  - Débit VPN IPSec : 500 Mbit/s
  - Utilisateurs simultanés en VPN SSL : 1 000
  - Sessions de déchiffrement SSL : 1 000

Solution retenue (software)

- Threat prevention :
  - prévention des menaces,
  - exploits, CnC, … ;
- PANDB URL filtering :
  - filtrage URL selon BDD





Pourquoi ? (1/5)

- Une valeur sûre dans le domaine de la sécurité, avec de très bonnes performances :
  - Leader du Magic Quadrant Gartner depuis 4 ans

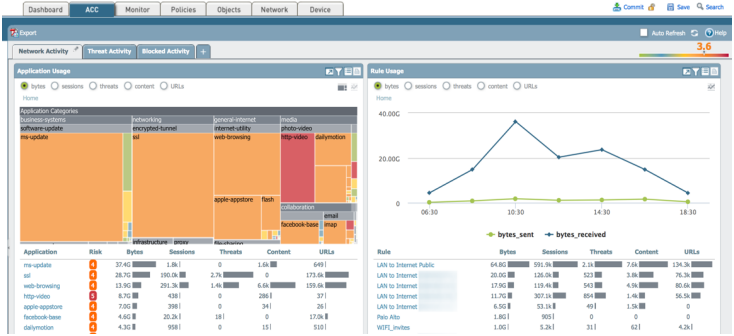
  - Très bons résultats aux tests effectués par NSS Labs :

NSS LABS
SECURITY RECOMMENDED

    - 100% d'efficacité sur les tests d'évasion effectués
    - Taux de blocage à 98,8% sur les exploits testés

Pourquoi ? (2/5)

- Console d'administration full web :
  - HTML5 avec widgets (personnalisable), exports possibles, API XML, …

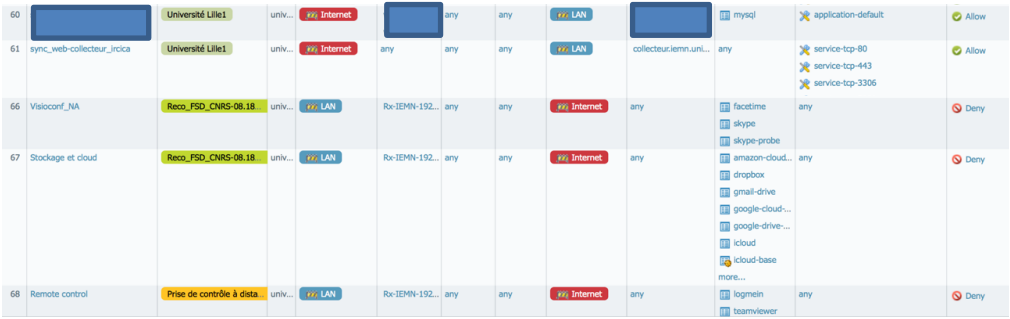


- Gestion possible par CLI (via ssh)

```
Time                    App             From            Src Port        Source
Rule                    Action          To              Dst Port        Destination
                        Src User        Dst User        End Reason
================================================================================
2015/08/28 14:41:51 not-applicable  Corp_SSL        123             192.168.98.6
Deny All            deny            LAN             123             192.168.103.5
                    masqueli                        policy-deny
2015/08/31 19:11:04 ssl             Corp_SSL        64583           192.168.98.6
GlobalProtect__mgmt allow           LAN             443             172.20.1.10
                    masqueli                        tcp-fin
2015/08/31 19:11:18 ssl             Corp_SSL        64589           192.168.98.6
GlobalProtect__mgmt allow           LAN             443             172.20.1.10
                    masqueli                        tcp-fin
masqueli@PA-3020-1(active)> show log traffic srcuser equal masqueli
[base] 1:zsh- 2:ssh*
```

Pourquoi ? (3/5)

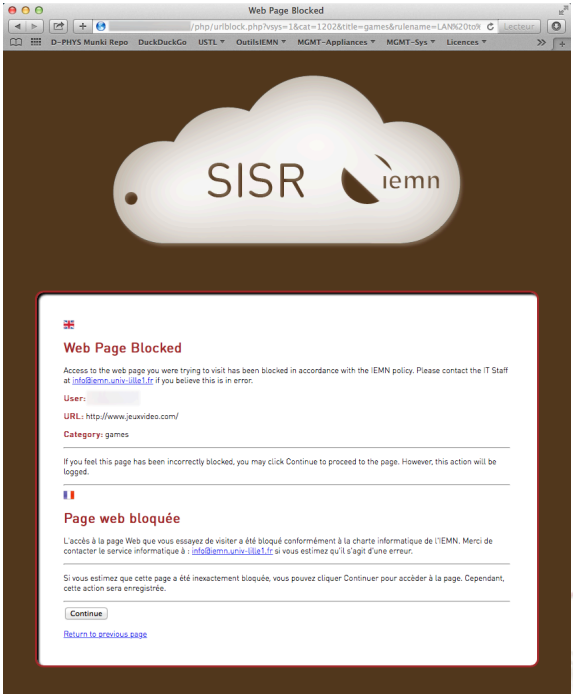
- Ecriture des règles différentes, plus complète :



60	[redacted]	Université Lille1	univ...	Internet	[redacted]	any	any	LAN	[redacted]	mysql	application-default	Allow
61	sync_web-collecteur_ircica	Université Lille1	univ...	Internet	any	any	any	LAN	collecteur.iemn.uni...	any	service-tcp-80 service-tcp-443 service-tcp-3306	Allow
66	Visioconf_NA	Reco_FSD_CNRS-08.18...	univ...	LAN	Rx-IEMN-192...	any	any	Internet	any	facetime skype skype-probe	any	Deny
67	Stockage et cloud	Reco_FSD_CNRS-08.18...	univ...	LAN	Rx-IEMN-192...	any	any	Internet	any	amazon-cloud... dropbox gmail-drive google-cloud-... google-drive-... icloud icloud-base more...	any	Deny
68	Remote control	Prise de contrôle à dista...	univ...	LAN	Rx-IEMN-192...	any	any	Internet	any	logmein teamviewer	any	Deny

- Avant :
  - [Adresse IP A] peut accéder à [Adresse IP B] sur le [port Y]
- Aujourd'hui :
  - [Utilisateur] du [Service Financiers] peut accéder à [SAP] (*Geslab*) de [7:30 à 19:00]
  - [Etudiants] peuvent accéder aux [Réseaux sociaux] de [17:00 à 9:00]
  - [Tout le monde] peut [uploader] à [5 ko/s] pour [bittorrent]
  - [Tout le monde] peut faire du [www] s'il est [authentifié]

Pourquoi ? (4/5)

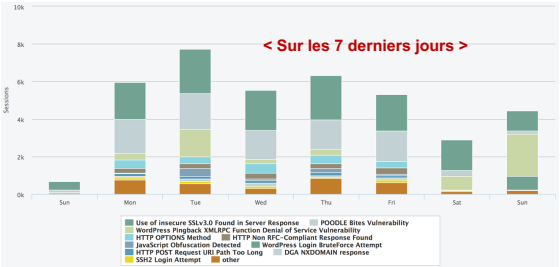


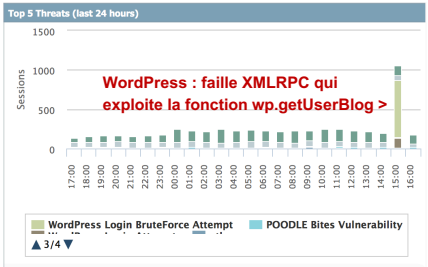
< Filtrage URL

Action : block & continue

Pourquoi ? (5/5)

- Redonne une vraie visibilité de ce qui se passe sur LAN et WAN :





- Un reporting assez complet :

< Top 50 des applications les plus gourmandes en BP au mois d'Octobre 2015

- **Finalité >>> mesures adaptées :**
  - **Correctifs sur serveurs,**
  - **QoS sur sites web ou applis, …**

7 Conclusion

Conclusion

- J'aime :
  - Meilleure gestion de l'IDS/IPS ;
  - Compteur des sessions qui passent dans les règles ;
  - Export des logs (traités bientôt avec ELK ☺) ;
  - Beaucoup de ressources en ligne :
    - Applipedia PaloAlto Networks ;
    - KB très complète et concrète.
  - Meilleure gestion des tunnels VPN IPsec ;
  - Liste de filtrage web (catégories) ;
  - Redonne une vraie visibilité sur son infrastructure réseau ;
  - Reporting des communications sans-fil (API avec IAP Aruba Networks) ;
  - La communauté d'utilisateurs régionaux.

- Je n'aime pas :
  - Le coût ;
  - Le commit des règles, un chouilla long ;
  - Le coût ☺

Questions