Actualités firewall à l'Observatoire juin 2021

Emmanuel Halbwachs

Observatoire de Paris, DIO

Réunion DIO/ASR labos, 14/06/2021

Depuis la dernière réunion 02/12/2020 (1)

- commande chez UGAP → Nomios → Fortinet
- réception/rackage en A-111 et 15/027 (fin 12/2020)
- prestation avec Nomios (11 j)

atelier compréhension contexte/besoins	4 j
rédaction dossier migration	2 j
config firewall Paris	2 j
transfert de compétence à la DIO	2 j
migration Paris	1 j

- gros travail d'accompagnement du prestataire
- firewall Paris en prod depuis le 30/03/2021
- refonte des règles de Paris pour être dans la logique du firewall

Depuis la dernière réunion (2)

- une statistique de temps à ce jour (uniquement E. Halbwachs, hormis le travail des collègues)

En-tête	Temps
Firewall	368 :13
Firewall : achat	93 :55
Firewall : presta/migration	164 :21
Firewall : réflexion archi/règles	17 :19
Firewall : implantation nouvelle...	57 :19
Firewall : installation physique/câblage	17 :57
Firewall : formation, transfert...	16 :12
Firewall : auto-formation, appropriation	1 :01
Firewall : outillage supervision	0 :09

(et ce n'est pas fini)

Difficultés rencontrées lors de la migration

- boucles réseau (VLAN tout-ou-rien sur interfaces actives)
- routage asymétrique sur serveurs hôtes Linux VServer

Ce qu'il reste à faire

- terminer la refonte des règles
- créer règles pour VPN
- modification d'architecture réseau Meudon (double attachement)
- bascule Meudon en production
- activation filtrage évolué
- rédaction doc VPN
- tests VPN avec vous ASR labos
- VPN en production
- recette Meudon avec prestataire (1 j)
- reliquat de prestation (3 j) : questions
- cible : sept-oct 2021 (ça glisse)

Rappel des fonctions attendues

- filtrage niv. 4 (addr. IP, services/ports)
- anti-virus (e-mail SMTP)
- App Control (ouverture de session)
- IPS (surveillance en continue)
- concentrateur VPN

Rappel : pas (peu) de filtrage en sortie

Filtrage : routeur vs firewall

- en commun
  - filtre = ensemble de règles (source, dest, services, actions)
  - first match wins
- routeur
  - filtre sur une interface, pour un sens donné
  - un flux = potentiellement 4 filtres traversés
  - par défaut, on laisse passer
- firewall
  - un seul gros filtre
  - règle s'applique sur une paire d'interface
  - par défaut, on bloque

VPN

- authentification « faible » (uniq. login/passwd)
- groupe LDAP *vpn-fw* dans chaque branche : comptes bénéficiants du VPN
- vous aurez le contrôle sur qui bénéficie du VPN

Questions pour ASR labos

Nouvelle politique de filtrage : compromis simplicité/sécurité raisonnable

- interdiction serveurs externes $\rightarrow$ intérieur ?
- filtrage inter-labos ?
- avez-vous du routage asymétrique ?

Rien d'urgent mais à réfléchir dès maintenant.

Démo de l'interface de gestion

- (s'il reste du temps)
- `https://fortimanager.obspm.fr/`
- vous aurez un accès read-only via LDAP

Questions ?

- (s'il reste du temps)
- merci pour votre attention