Actualités firewall à l'Observatoire juin 2022

Emmanuel Halbwachs

Réunion DIO/ASR labos « Cisco », 07/06/2022

Observatoire de Paris, DIO

Point d'avancement

Rappel des fonctions attendues

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

Temps passé depuis la dernière réunion 01/12/2021 (1)

Headline	Time		%
Firewall	154 :43		100.0
Firewall : Meudon : implantation nouvelle politique filtrage		94 :33	61.1
Firewall : Meudon : configuration		29 :31	19.1
Firewall : Paris : implantation nouvelle politique filtrage		13 :27	8.7
Firewall : achat		6 :05	3.9
Firewall : réflexion archi/règles		4 :49	3.1
Firewall : auto-formation, appropriation		1 :54	1.2
Firewall : presta/migration		1 :15	0.8
Firewall : Paris : configuration		1 :05	0.7
Firewall : environnement système		0 :47	0.5
Firewall : communication vers netadmin/obs		0 :44	0.5
Firewall : mise à jour		0 :33	0.4

Nota : le temps passé sur la modification de l'architecture réseau Meudon n'est pas comptabilisé ici.

Temps passé depuis le début

Headline	Time	%
Firewall	634 :19	100.0
Firewall : presta/migration	165 :36	26.1
Firewall : Paris : implantation nouvelle politique filtrage	146 :21	23.1
Firewall : achat	100 :10	15.8
Firewall : Meudon : implantation nouvelle politique filtrage	94 :33	14.9
Firewall : Meudon : configuration	52 :33	8.3
Firewall : réflexion archi/règles	22 :09	3.5
Firewall : installation physique/câblage	18 :18	2.9
Firewall : formation, transfert compétences	16 :12	2.6
Firewall : auto-formation, appropriation	13 :13	2.1
Firewall : outillage supervision	2 :05	0.3
Firewall : Paris : configuration	1 :05	0.2
Firewall : environnement système	0 :47	0.1
Firewall : communication vers netadmin/obs	0 :44	0.1
Firewall : mise à jour	0 :33	0.1

Nota : le temps passé sur la modification de l'architecture réseau Paris/Meudon n'est pas comptabilisé

Fait depuis la dernière réunion 01/12/2021 (2)

- Paris
  - finalisation implantation nouvelle politique de filtrage
- Meudon
  - connexion 10 G à Rubis
  - modif archi LAN pour double attachement
  - cluster firewall monté depuis zéro
  - création nouvelle politique de filtrage (s'inspirant de Paris)

Ce qu'il reste à faire

- terminer la refonte des règles
- bascule Meudon en production
- VPN
  - créer règles
  - rédaction doc VPN
  - tests VPN avec vous ASR labos
  - VPN en production
- activation filtrage évolué (AV, App Control, IPS)
- recette Meudon avec prestataire (1 j)
- reliquat de prestation (3 j) : questions
- cible (ça continue de glisser)
  - bascule Meudon : avant fin juin 2022
  - VPN : je ne me hasarde plus à donner de dates, meilleur effort

Discussion : politique de filtrage

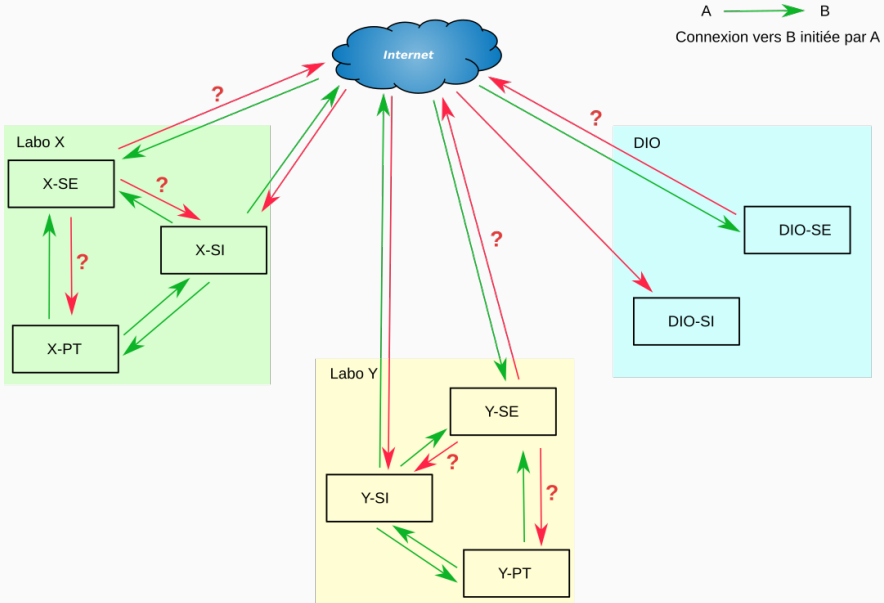
Rappels des concepts pour les sous-réseaux

- serveurs externes (X-SE)
  - fournissent services à l'extérieur (intérieur OK)
  - exposés sur l'Internet
- serveurs internes (X-SI)
  - fournissent services uniquement à l'intérieur (VPN/proxy/tunnel OK)
  - pas exposés sur l'Internet
- poste de travail
  - ne fournit aucun service
  - pas accessible de l'extérieur directement (VPN/tunnel OK selon politique du labo)
  - pas exposés sur l'Internet

Buts

- même politique pour tous les labos
- compromis sécurité/ergonomie
- besoin d'atteindre un consensus
  - présentation des bases : aujourd'hui
  - réflexion/discussion sur liste `netadmin@o.f`
  - on entérine lors de la prochaine réunion : 14/11
    - voire avant si le consensus est atteint

Graphiquement



Flux à laisser passer

- supervision poussée par les SE ?
- config Puppet/etc. tirée par les SE ?
- SSH ?