Point firewall janvier 2023

Emmanuel Halbwachs

Réunion Castors/Milan, 09/01/2023

Observatoire de Paris, DIO

Rappel des fonctions initialement attendues

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

Jalons historiques

Année	Période	Activité
2020	mai-nov	Prospection, devis, recherche financement
	déc	Commande Fortinet, livraison, rackage
2021	jan-mar	Presta Nomios, travail pré-migration
	30 mars	Bascule Paris
	avr-oct	Refonte complète règles Paris
	juin-déc	Modif topologie Meudon pour double racc.
2022	jan	Souci licence expirée
	jan-juin	Install. Meudon depuis zéro, règles Meudon
	4 juil	Bascule Meudon
	juil-nov	Discussion politique avec ASR
	oct-déc	Recette Nomios, formation Nomios + Fortinet
	nov-déc	Duplication règles pour VPN
2023	jan-	Duplication règles pour VPN

Temps passé depuis le début (sans compter celui des collègues)

Firewall	795 :24	100.0
Firewalls : presta/migration	173 :08	21.8
Firewalls : Paris : implantation nouvelle politique filtrage	157 :29	19.8
Firewalls : Meudon : implantation nouvelle politique filtrage	106 :14	13.4
Firewalls : achat	101 :24	12.7
Firewalls : Meudon : configuration	57 :38	7.2
Firewalls : Meudon : bascule prod (pre, post, etc.)	55 :25	7.0
Firewalls : formation, transfert compétences	54 :39	6.9
Firewalls : réflexion archi/règles	28 :13	3.5
Firewalls : installation physique/câblage	18 :18	2.3
Firewalls : auto-formation, appropriation	14 :26	1.8
Firewalls : Paris : configuration	5 :15	0.7
Firewalls : VPN	4 :54	0.6
Firewalls : mise à jour	4 :17	0.5
Firewalls : incidents	3 :50	0.5
Firewalls : environnement système	3 :06	0.4
Firewalls : vérif/modif politique filtrage	3 :00	0.4
Firewalls : outillage supervision	2 :33	0.3

Enjeux, difficultés, remarques

- touche au centre névralgique du réseau
- firewall = objet complexe
- prestataire pas du tout à la hauteur, sauf à la toute fin
- politique de filtrage complexe → migration et refonte chronophages
- consensus politique filtrage : LERMA...
- filtrage évolué → interception SSL
- rendre l'ensemble maintenable par toute personne Castors, Milan, Suricate++
- inquiétudes VPN
  - gestion du parc de clients VPN (màj suite faille)
  - un seul facteur d'auth. (login/passwd) et phishing

Fonctions attendues vs implantées

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

Travail à venir

- polir la diodoc
- réunion DIO pour discuter bonnes pratiques
- VPN
  - créer règles (doublons)
  - rédaction doc VPN
  - tests VPN avec ASR labos
  - VPN en production
- généralisation graduelle filtrage évolué (App Control, IPS)
- implanter politique après consensus, cf. compte-rendu réunion dite « Cisco » [1]
- POP2025 : on casse tout et on recommence...

1. https://mdbook.obspm.fr/_MvWaTDvTMKF7gdwAH2jWg#

Merci

Merci pour votre attention