Formation/discussion : utilisation et configuration des firewalls

Emmanuel Halbwachs

26/09/2023

Observatoire de Paris, DIO

But de cette visio

- à destination de toutes les personnes qui ont à agir sur le filtrage (permanence, activité système, RSSI)
- de l'interactivité
- le filtrage est un sujet complexe : pas de question idiote, ne pas hésiter
- que tout le monde ait à peu près tout compris et puisse pratiquer
- le tout dans le respect des bonnes pratiques (BP)...
- ... qui sont à débattre pour trouver un consensus DIO
- je fais ici des propositions de BP et nous en débattrons

Ordre du jour

- présentation éclair des différentes docs
- quelques rappels de contexte
- démos sur des cas pratiques de simulation de flux
- démos sur des cas pratiques de modification du filtrage
- au fil des démos (interactif)
  - discussion sur les bonnes pratiques
  - questions
- historique des modifs, sauvegarde
- s'il reste du temps
  - filtrage avancé avec inspection SSL/TLS
  - point d'avancement sur VPN

Présentation éclair des différentes docs

- Firewall Fortinet : utilisation
- Firewall Fortinet : utilisation en lecture seule (read-only)
- Firewall Fortinet : discussion et consensus vers une politique de filtrage commune
- Firewall Fortinet : organisation politique de filtrage
- Utilisation des firewalls Fortinet
- Mise à jour de FortiOS sur les firewalls Fortinet et de FortiManager

Un peu de vocabulaire

- FortiGate (FGT) : firewall physique (en cluster chez nous), un par campus
- FortiManager (FMG) : console d'administration, appli web dans une VM
- règle de filtrage (*policy*) : règle unitaire, ID unique
- politique de filtrage : ensemble de toutes les règles (*policy package*) qui s'applique sur un firewall
- section : « intercalaire » qui permet de séparer/replier une sequence de règles regroupées selon telle ou telle logique
- filtrage évolué : filtrage avec une inspection du contenu au-dessus de la couche 4 (au-dessus de TCP/UDP) qui nécessite une interception SSL (*man-in-the-middle*) et donc une gestion des certificats

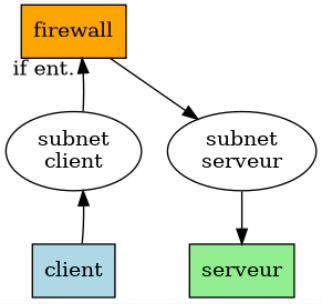
Règles d'or

- tout se fait sur le FMG
  - tout ce qui peut se faire sur le FMG doit se faire sur le FMG
  - si ça ne peut pas être fait sur le FMG, demander aux Pandas ◡̈
  - les exceptions existent, mais sont très rares et doivent être faites en connaissance de cause, avec les Pandas
- les netadmins n'ont pas accès au FMG
- les netadmins ont accès aux FGT en lecture seule pour
  - visualiser les règles
  - simuler des flux

Comment simuler un flux

- fonctionnalité : *policy lookup* (consultation de la politique)
  - se fait sur les FGT, qui seul à la conscience des interfaces physiques
  - mais peut se faire sur le FMG qui alors sous-traite au FGT
  - conseillé de le faire sur le FMG, plus pratique
- flux
  - source = IP client (FQDN impossible ∴)
  - destination = FQDN serveur
  - nécessité de bien comprendre la notion d'interface d'entrée de flux (`if ent.`)
  - protocole
  - port destination

À l'intérieur d'un campus

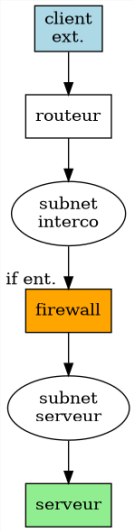


Exemples :

- de ma machine perso (Meudon) vers tycho.o.f en SSH
- de rubicon vers ma machine perso (Paris) en SSH

Comment simuler un flux, cas pratiques (2)

De l'extérieur vers un campus

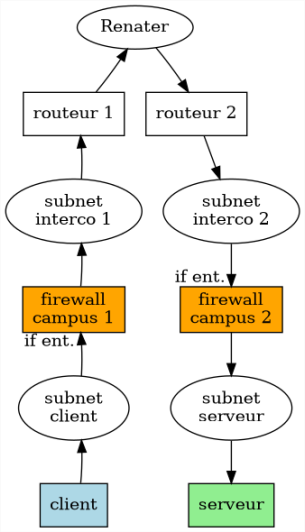


Exemples :

- de 1.1.1.1 vers www.o.f en HTTP
- de 1.1.1.1 vers tycho.o.f en SSH

Comment simuler un flux, cas pratiques (3)

D'un campus à l'autre



Il faut procéder à deux simulations, une par firewall

Exemple :

- de vpn.o.f (Meudon) vers hardy (Paris) en RDP

Anatomie d'une règle

Objets :

- *policy package* = {règles}
- règle = {objets} {interfaces, adresses, services}
- adresses, services : peuvent être groupées, poupées russes

Tour du propriétaire des règles existantes :

- conseil sur configuration des colonnes
- tour d'horizon rapide des sections : nommage, ordre
- visualisation de quelques règles en détail pour illustrer les concepts
- un mot sur les règles pour le VPN

Exemples de règles

- Meudon, BBB : ID 26
- Meudon, web externes DIO : ID 29, 30
- Meudon, serveurs internes DIO : ID 121
- Paris, windows Milans : ID 412
- Paris, labo (IMCCE) : ID 651
- Paris, flux sortant (sas SSH, serveurs d'impression) : ID 699, 700
- *Implicit Deny* final

Comment modifier une règle existante, cas pratique

- Meudon : ajouter un nouveau serveur web externe DIO foo.o.f
- suivons la doc Firewall Fortinet : utilisation

Comment créer une nouvelle règle, cas pratique

- Paris : ajouter un nouveau serveur foo.o.f avec un nouveau service (GRMBL TCP/UDP 6666)
- suivons la doc Firewall Fortinet : utilisation

Historique des modifications, sauvegarde, logs de flux

- historique des modifications
  - FMG
  - c'est le seul endroit où on a les logs (pas dans FGT et donc pas dans Oxidized)
  - c'est un tourniquet avec 250 positions seulement, donc on perd de l'info au fil du temps 😬
- sauvegarde
  - FMG (implicite, mais probablement pas complète)
  - Oxidized
- logs de flux, compteurs
  - sur le FGT

Bonnes pratiques pour les commit logs

Propositions

- commit logs parlant en une ligne (cf. git)
- le faire pour les collègues et les RSSI en particulier
- faciliter la revue rapide des modifs par une autre personne

Exemple :

- revue des commit logs réels

Bonus s'il reste du temps

- filtrage avancé avec inspection SSL/TLS
- point d'avancement sur VPN

C’est fini

Merci pour votre attention et votre participation ◡̈