TP *firewall* : lecture des règles, simulation des flux

Emmanuel Halbwachs

24,26/01/2024

Observatoire de Paris, DIO

But du TP

- à destination de toutes les personnes des services informatiques des laboratoires (ou de la DIO) qui administrent des services
- 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

Ordre du jour

- présentation éclair des différentes documentations
- quelques rappels de contexte
- lecture des règles
- démos sur des cas pratiques de simulation de flux
- questions au fil des démos (interactif)

Présentation éclair des différentes documentations

- dans Diodoc, rechercher « *Firewall* »
- documentation utiles
  - *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

Rappel de l'architecture réseau

- l'architecture réseau est schématisée dans une page diodoc

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

FortiManager (FMG) vs FortiGate (FGT)

- tout se fait sur le FMG (DIO uniquement)
- mais les netadmins n'ont pas accès au FMG
- les netadmins ont accès aux FGT en lecture seule pour
  - visualiser les règles
  - simuler des flux
  - visualiser les *logs*

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

TP 1 : visualiser les règles

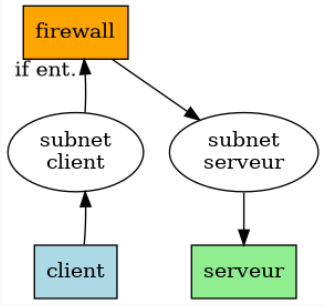
- ouvrir une session web sur le *firewall* de votre campus
- Policy & Objects → Firewall Policy
- organiser les colonnes selon le conseil de la doc
- déplier/replier les sections
- à l'aide de la boîte de recherche
  - chercher votre laboratoire
  - chercher votre serveur web

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 (DIO uniquement)
  - conseillé de le faire sur le FMG, plus pratique (DIO uniquement)
- description du flux
  - source = IP client (FQDN impossible ⌒̈)
  - destination = FQDN serveur
  - nécessité de bien comprendre la notion d'interface d'entrée de flux (`if ent.`)[1]
  - protocole
  - port destination
- conseil pour les netadmins
  - noter les paramètres de la simulation dans un fichier texte
  - puis copier-coller dans l'interface web
  - car les paramètres sont effacés à chaque simulation ⌒̈

1. s'aider du référentiel des sous-réseaux/VLAN dans Diodoc

À l'intérieur d'un campus



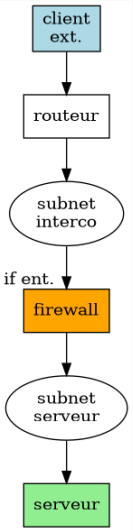
Si Paris, simuler :

- de votre poste de travail vers inrow-p-a111-4.o.f en SSH
- de votre poste de travail vers boite-cles-ba-p.o.f en HTTP
- de rubicon vers votre poste de travail en SSH

Si Meudon, simuler :

- de votre poste de travail vers video-m-b15b.o.f en HTTPS
- de votre poste de travail vers boite-cles-b04b.o.f en HTTP
- de styx vers votre poste de travail en SSH

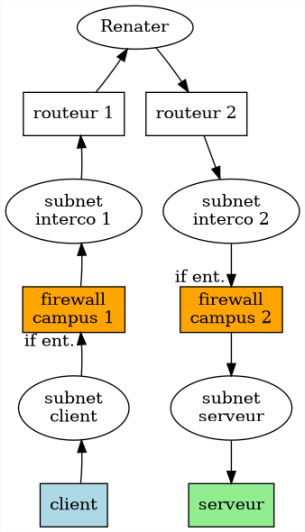
De l'extérieur vers un campus



Simuler :

- de 1.1.1.1 vers le serveur www de votre entité en HTTP
- de 1.1.1.1 vers tycho.o.f en SSH

D'un campus à l'autre



Il faut procéder à deux simulations, une par *firewall*

Simuler :

- du sas SSH du campus d'en face (rubicon, styx) vers un de vos serveur sur ce campus, en SSH

TP 4 : Simuler un flux de votre choix, pertinent dans votre cas

Essayer de trouver un flux qui a du sens dans votre contexte

TP 5 et 6 : Visualisation des *logs*

- certaines règles activent le *log* du trafic pour lequel elles correspondent
- TP 5 : trouver lesquelles ! (sur le *firewall* de notre site)
  - conseil : utiliser un filtre de colonne
- TP 6 : visualiser un *log* d'une règle qui vous intéresse ou vous concerne
  - clic droit → Show Matching Logs

Règles attrape-tout qui vont être désactivées

Des règles temporaires « attrape-tout » on été installées pour identifier du trafic qui ne serait pas explicitement autorisé :

- Paris
  - règles ID 814-815 et 817
- Meudon
  - règles ID 202-207

Ces règles ont le *logging* actif. Je vous demande svp d'y jeter un coup d'œil avant suppression de ces règles et donc interdiction du trafic qui y correspondrait. Nous nous sychroniserons sur la liste `netadmin@obspm.fr`.

Nota Bene : dans une règle très large qui se trouve avant le *deny* implicite final et qui *loggue*, on peut trouver du trafic retour à un trafic aller permis plus haut. Ce trafic sera implicitement autorisé. Exemple : les réponses DHCP des serveurs DHCP de la DIO.

C’est fini

Merci pour votre attention et votre participation ◡̈