Firewall et VLAN

Damien Gros

CEA

11 mars 2019

Plan du cours

NAT

- NAT Statique
- NAT Dynamique
- Port forwarding et Port mapping

Firewall

Plan du cours

NAT
- NAT Statique
- NAT Dynamique
- Port forwarding et Port mapping

Firewall

L'histoire du NAT

- Manque d'adresses IPv4 public ;
- Introduction des adresses dites **privée**
  - Adresses non-routées : si un routeur (autre que votre box/passerelle) voit une adresse IP, il droppe le paquet.
  - Une seule adresse publique `héberge` des milliers de machines derrière un équipement réseau.
- RFC 1918
- Network Address Translation

L'histoire du NAT

Adresses privées (non routées)

- $10.0.0.0_{/8}$
- $192.168.0.0_{/16}$
- $172.16.0.0_{/12}$

L'histoire du NAT

- Que se passe-t'il si on utilise une autre plage d'adresse pour le NAT ?
- Rien : si ce n'est que vous ne pourrez plus aller sur certains sites.

NAT Statique

- Association entre une adresse public (celle du routeur) et une adresse privée
- Tout se fait au niveau du routeur
- Remplacement dans l'entête IP de l'adresse source (adresse privée) par l'adresse publique (paquets sortant)
- Remplacement dans l'entête IP de l'adresse destination (adresse publique) par l'adresse privée (paquets entrant)
- Utilisation d'ARP pour renvoyer le paquet à la bonne personne sur le réseau privée.

NAT Dynamique

- Aussi appelé IP masquerading
- Association entre : 1 adresse publique et N adresses privées
- Modification par le routeur
  - Adresse IP des entêtes (comme pour le NAT statique)
  - Modification des ports ! : PAT Port Address Translation
- Utilisation des ports (attribution de ses ports par le routeur, donc différents de ceux utiliser par les clients/serveurs) pour se souvenir de qui a fait la demande de connexion

Port forwarding et Port mapping

- Port forwarding :
  - Redirige un paquet vers une machine en fonction du port de destination
- Port mapping
  - Procédé similaire que le port forwarding
  - Redirige en plus vers un nouveau port (80 vers 8080 par exemple)

Plan du cours

NAT
- NAT Statique
- NAT Dynamique
- Port forwarding et Port mapping

Firewall

Firewall

- Les pare-feux !
- C'est un concept (et non un logiciel ou un matériel)
- Définit une politique d'accès aux ressources sur le réseau
- Un vrai pare-feu agit sur les couches 2, 3 et 4 du modèle OSI.
- Pour les autres couches : pare-feu applicatif, socks, de proxy, etc.

Portée

- Évolution des pare-feux dans le temps :
  - Stateless firewall : pare-feu sans état, analyse les paquets indépendamment les uns des autres ;
  - Statefull firewall : pare-feu avec état, prend en compte les séquences de paquets (communication TCP)
  - Pare-feu Applicatif : filtre les couches de 5 à 7.
  - Pare-feu identifiant : filtre en fonction de l'utilisateur.
- On s'intéresse aux pare-feux de couches 2, 3 et 4.

Pare-feux de couche 2 à 4

- Versions libres :
  - NetFilter/Iptables : pare-feu libre des noyaux linux 2.4 et 2.6 et 3.X
  - Packet Filter (PF) : pare-feu libre OpenBSD ;
  - IPFilter (IPF) : pare-feu libre BSD et Solaris 10.
- Versions propriétaires :
  - Checkpoint Firewall
  - Cisco Pix
  - Juniper Screen OS

Pare-feu et routeur

- Un pare-feu peut diviser un réseau en plusieurs sous-réseaux et y appliquer des politiques de sécurité différentes :
  - Il est donc capable de **router** les paquets entre différentes parties du réseau
- Il dessine des zones différentes
- Zones sécurisées complètement protégées
  - Zones privées, intranet
- Zones hébergeant des serveurs accessibles depuis Internet
  - Protection différente d'un réseau local, exposition aux attaques extérieures
  - Zones démilitarisées (DMZ) : zones entre Internet et le réseau local, où sont hébergés les services exposés à Internet.

Architecture réseau

schéma PF 1

Les rôles d'un pare-feu

- Être un point de passage obligatoire pour :
  - vérifier si les règles de sécurité spécifiées sont appliquées ;
  - contrôler le trafic entre deux zones du réseau
  - auditer/traçer de façon centrale ce trafic ;

Politique de sécurité

La seule politique de sécurité viable :
On interdit tout et on autorise aux coups par coups

Politique de sécurité

Tout ce qui n'est pas explicitement autorisé dans la politique est donc interdit

Filtrage des paquets

- Chaque paquet IP contient des informations que le pare-feu va extraire et traiter :
  - Adresse de l'expéditeur
  - Adresse du destinataire
  - Port TCP/UDP du service demandé
  - Port TCP/UDP du poste demandeur
  - le FLAGS (pour TCP) : qui précise su le paquet est une initialisation de connexion, un ACK, ou tout autre chose.

Netfilter/iptables

Netfilter :

- Mécanisme du noyau Linux ;
- Ensemble de 5 **crochets** (ou chaines) ;
- Utilisation des informations lorsqu'un paquet traverse la pile réseau

iptables :

- Interface de commande
- Permet la communication avec le module Netfilter ;
- Mais ce n'est pas le seul, il existe aussi nufw par exemple.

Vue de netfilter

schéma PF 2

Types de tables

- Iptables utilise des tables pour gérer les connexions ;
- 3 grandes tables :
  - Filter
  - NAT
  - MANGLE
- Ces tables définissent les crochets utilisables dans les scripts iptables

Table filter

- 3 chaînes :
  - INPUT : paquets rentrant vers des processus locaux ;
  - OUTPUT : paquets sortants des processus locaux
  - FORWARD : paquets passant d'une interface à une autre

schéma PF 3

Table NAT

- 3 chaînes :
  - PREROUTING : paquets rentrants dans la couche réseau
  - POSTROUTING : paquets sortants de la couche réseau
  - OUTPUT : paquets sortants des processus locaux

schéma PF 4

Table MANGLE

- Mangle : Mutilation des paquets...
- Application : Qualité de service (par exemple)

Iptables

toutes les lignes commences par la commande **iptables**

- Manipulation des tables : -t nom_table
- Cible (ou action) : DROP, ACCEPT, REJECT
- Manipulation des chaines : -F (flush), -X (eXtra), -P (policy), -N new, -A Append, -D delete, -L liste
- Critères : -i input, -o output, -d destination, -p protocole, -sport source port

Exemples

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
iptables -A OUTPUT -p udp -o eth1 –sport 69 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 –dport 22 -j ACCEPT
```

Suivi de connexion

- Module noyau nommé conntrack ;
- Connexions :
  - NEW : premier paquet d'une nouvelle connexion pas encore établie
  - ESTABLISHED : connexion déjà enregistré dans le noyau
  - RELATED (exemple FTP) : pour une nouvelle connexion créée par une connexion plus ancienne et déjà établie
  - INVALID

IP masquerading

- Table NAT
- Voie montante
- Voie descendante
- Modules NAT
- Nécessite l'activation de l'ip forward dans le noyau

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

IP masquerading

- La commande qui suit active le NAT pour toutes les machines situées derrière l'interface ethernet eth0 et leur attribue l'adresse IP de la passerelle pour toute connexion sortante :
- iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
- La commande qui suit active le NAT pour toutes les machines situées derrière l'interface ethernet eth0 et leur attribue l'adresse IP routable 192.168.0.1 pour toute connexion sortante :
- iptables -t nat -A POSTROUTING -o eth0 -j SNAT –to 192.168.0.1
- But du TP : vous faire comprendre cette notion de masquerading !