Juniper : Capture Pcap

>>> Mise en place d’une capture de paquets de type Pcap.

Description :

Ce cours a pour but d’apprendre à mettre en place une capture de paquets, afin d’analyser ce qui transite sur une interface de votre équipement Juniper SRX.

Juniper : Capture Pcap

>>> Mise en place d'une capture de paquets de type Pcap.

Sommaire :

I) Introduction
II) Configuration
1) Partie Forwarding-options
2) Partie Firewall
3) Partie Interface
III) Fichiers Pcap

I) Introduction

Lors d'un dépannage, une capture de paquets est très utile. Pour ce faire, effectuez une capture de paquets en dehors du périphérique J-series ou SRX. Cependant, dans certains cas, il peut ne pas être possible d'avoir un PC ou un serveur en ligne pour les captures Ethereal / Wireshark ou tcpdump. Ainsi, les périphériques J-Series et SRX Branch (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX300 series, SRX1500) peuvent directement effectuer une capture de paquets. Les étapes pour ce faire sont documentées dans la solution ci-dessous.

Notes : 1. La capture de paquets PCAP ne peut capturer que le trafic du protocole IPv4.
Notes : 2. Si vous utilisez la capture de paquets sur les interfaces reth, deux fichiers sont créés, l'un pour les paquets d'entrée et l'autre pour les paquets de sortie en fonction du nom de l'interface reth. Ces fichiers peuvent être fusionnés en dehors de l'appareil à l'aide d'outils tels que Wireshark ou Mergecap.

II) Configuration

Pour obtenir la capture de paquets sur les périphériques SRX, suivez la procédure ci-dessous :

1) Partie Forwarding-options

Ajoutez les commandes suivantes, en définissant :
• Le nom du fichier
• La taille maximum d'un fichier
• Le nombre maximum de fichier

```
forwarding-options {
    packet-capture {
        file filename Capture_15022019 files 5 size 10m;
        maximum-capture-size 1500;
    }
}
```

2) Partie Firewall

Dans la partie Firewall du Juniper, ajoutez les lignes suivantes :

```
firewall {
    family inet {
        filter Capture {
            term TERM1 {
                from {
                    address {
                        0.0.0.0/0;
                    }
                }
                then {
                    sample;
                    accept;
                }
            }
            term DEFAULT {
                then accept;
            }
        }
    }
}
```

3) Partie Interface

Pour activer la capture ajoutez les lignes suivantes dans la partie interface :

```
    ge-0/0/5 {
        unit 0 {
            family inet {
                filter {
                    input Capture;
                    output Capture;
                }
            }
        }
```

III) Fichiers Pcap

Vous trouverez les fichiers générés par la capture dans le répertoire **"/var/tmp/"**.
Vous n'aurez plus qu'à récupérer les fichiers en vous connectant via WinSCP sur le routeur. Ou en utilisant un transfert FTP depuis le routeur SRX.