UTM : Fortigate

Le fabricant Fortinet commercialise les UTM **FortiGate** qui incluent des fonctionnalités de :

- Filtrage/firewall,
- monitoring,
- contrôle de bande passante (Qualité de Service / QOS)
- antivirus / anti spam

Accès de base

Après réinitialisation par le bouton ***reset***, les paramètres par défaut des Fortigate de la section sont :

- Fortigate 80c (plus maintenus depuis 2023) : IP : 192.168.0.1 / Compte **admin** sans mot de passe.

L'accès se fait en interface web (http://ip_fortigate) ou par port console (9600 bits/s).

Configurations

Définition de l'adressage

Adresses des interfaces et VLAN

Les FortiGate ont des ports sur 3 “zones” :

- Internal (1) : correspond à la partie LAN du réseau. Un switch permet de gérer plusieurs ports physiques ou des VLAN
  - Pour chaque interface définie en interne, on indique le/les port/s physique/s sur lesquels on l'applique
- DMZ (2) : zone dédié aux <wram em>équipements exposés</wrap> de l'entreprise
- WAN (2) : partie destinée aux accès extérieurs

Le paramétrage de l'adressage se passe dans le menu **Network/Interfaces ou Réseau/Interfaces** :

Illustration

⇒

Pour chaque interface, on peut paramétrer une **plage DHCP**.

Serveur DNS

On paramètrera le **DNS** dans le menu **Network/DNS**

Routes

On ajoute les routes statiques nécessaires au fonctionnement, notamment :

- La **route par défaut** 0.0.0.0/0.0.0.0 vers le prochain routeur de sortie ou le FAI
- Les routes vers les VLAN internes ou de DMZ le cas échéant

Illustration

⇒

Pour chaque **route** on précise :

- la destination (un réseau, une adresse ou une URL)
- la **passerelle (/gateway)**, soit le prochain routeur
- l'interface sur laquelle la route s'applique
- la **métrique**

Configuration du filtrage

Définition des objets

Avant de définir les règles que l'on souhaite appliquer, on nomme les **objets (plages, machines, services, etc)** que l'on veut manipuler, pour améliorer la lisibilité du paramétrage.

Illustration

Définition des règles

Les règles sont :

- appliquées sur des interfaces d'entrée (**incoming**) et de sortie (**outgoing**)
- pour des **IP** source et destination (machine, plage, réseau)
- pour des **services** définis (ports/protocoles)
- avec une action (autoriser/bloquer/apprendre)

Sur une règle, on peut choisir d'**activer le NAT**, masquant l'adressage interne (remplacé par l'IP de l'interface du Fortigate).

Illustration

⇒