

Sécurisation du Réseau Local

Europea Consulting



Sommaire :

I. La mission	3
II. Comment sécuriser un réseau	4
III. Les équipements utilisés	4
IV. Les programmes utilisées	5
V. Schéma globale de l'installation	8

I. La mission

Notre mission avec mes collègues était de configurer un switch et un pare-feu dont l'objectif cible était :

- d'améliorer la sécurisation des flux,
- d'améliorer les performances
- et avoir une meilleure gestion des PC utilisateurs et équipements serveurs, téléphones IP et imprimantes.

Pour cela, nous avons envisager :

- de configurer des VLANs sur switch administrable de marque HP ARUBA pour avoir un réseau segmenté par type d'équipements (PC Utilisateurs, Serveurs et Téléphones IP)
- et d'ajouter un véritable pare-feu de marque Fortinet pour pallier à l'insuffisance technique du routeur opérateur en place (Box Internet).

Nota: nous avons fait le choix d'intégrer l'imprimante-scanner dans le réseau serveur.

L'ensemble Switch Aruba + Pare-feu Fortinet permet un contrôle complet du trafic entre les différents sous-réseaux IP (VLANs IP) internes et l'Internet.

Une politique de sécurité minimale a été mise en place à travers des règles de filtrage paramétrées sur le pare-feu.

II. Comment sécuriser un réseau

Pour avoir un réseau privé protégé, il faut prendre des mesures de sécurisation afin d'éviter toute attaque, ou acte malveillant.

On peut par exemple citer la démarche et les moyens de protection ci-dessous :



- Identifier les sous-réseaux internes à protéger
- installer un switch permettant la segmentation des sous-réseaux via l'implémentation de Vlans par type d'équipements.
- Installer un pare feu (firewall) connecté au réseau interne (LAN) et externe (Internet)
- Utiliser un VPN pour chiffrer les données si nécessaire
- Sensibiliser et former les utilisateurs à la protection de leur données
- Assurer une surveillance et analyse du trafic réseau via des outils de Supervision en temps réels (ex: PRTG, Centreon, et autres)

Une fois ces mesures de sécurité mises en place, il est important d'adopter une politique stricte de gestion des accès et des identités pour limiter les risques d'intrusion.

En combinant ces pratiques, un réseau privé peut être efficacement protégé contre les attaques et les actes malveillants.

III. Les équipements utilisés

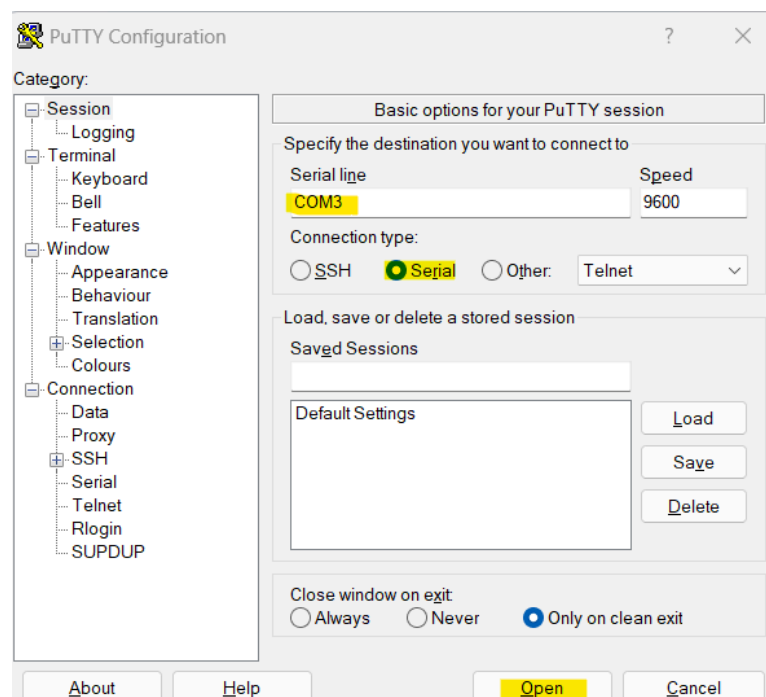
Nous avons utilisé un switch de la marque Aruba et un pare-feu de la marque Fortinet.

	Switch (Commutateur) HP ARUBA - 48 ports Gigabit - POE (pour alimentation des téléphones IP).
	Fortinet 50E avec 2 ports Wan et 5 ports Lan.

IV. Les programmes utilisées

Pour accéder à la configuration du Switch HP ARUBA, nous avons eu besoin d'utiliser le logiciel Putty qui combine un émulateur de terminal avec un client prenant en charge les protocoles SSH, Telnet, rlogin et TCP brut.

Nous avons relié le port Console du Switch au port USB de notre PC via une liaison série RS-232, et paramétrer Putty avec le bon port COM3 détecté par le gestionnaire de périphérique du PC.



En lançant le terminal, nous avons pu ainsi avoir accès au Switch pour amorcer les configurations en ligne de commande (appelé aussi en mode CLI - Command Line Interface).

Ci-dessous l'accès en CLI avec l'exécution de la commande : show version.

```
Aruba-2930F-48G-PoEP-4SFPP# show version

Image stamp:
 /ws/swbuildm/rel_ajanta_qaoff/code/build/lvm(swbuildm_rel_ajanta_qaoff_rel_ajanta)
      Oct 27 2022 21:05:50
      WC.16.10.0011
      215
Boot Image:      Primary

Boot ROM Version:  WC.16.01.0008
Active Boot ROM:   Primary
```

Nous avons manuellement configuré chacun des Vlan à la fois sur le Switch et le Firewall Fortinet.

- PC Utilisateur => sur les ports 1 à 12 => Vlan 10 => Name DATA
- Serveurs => sur les ports 13 à 24 => Vlan 20 => Name SERVER
- Téléphonie => sur les ports 25 à 36 => Vlan 30 => Name VoIP

● Côté Switch

Switch#configure terminal (ou conf t)

Switch(conf)#

vlan 10

name "Data"

untagged 1-12

no ip address

vlan 20

name "Server"

untagged 13-24

no ip address

vlan 30

name "VoIP"

untagged 25-36

no ip address

Switch(conf)#write terminal (ou wr mem); pour la sauvegarde de la configuration.

- **Côté Pare-Feu (Firewall Fortinet)**

Nous avons utilisé 1 port par Sous-réseaux interne ou externe en déclarant respectivement le bon numéro de Vlans :

- Interface Lan port 1 = Vlan Data, connecté au port 1 du Switch
- Interface Lan port 2 = Vlan Server, connecté au port 13 du Switch
- Interface Lan port 3 = Vlan Data, connecté au port 25 du Switch et enfin
- Interface Wan 1 sans Vlan connecté directement à la Box Internet Europea Consulting.

Voici un exemple avec le Vlan "Data".

The screenshot shows the 'New Interface' configuration page in Fortinet's web interface. The interface is named 'Data' and is configured as a VLAN. The 'Type' is set to 'VLAN'. The 'VLAN protocol' is set to '802.1Q'. The 'Interface' is set to 'InternalLANSwitch (internal1)'. The 'VLAN ID' is set to '10'. The 'VRF ID' is set to '0'. The 'Role' is set to 'LAN'. The 'Address' section shows the 'Addressing mode' set to 'Manual' and the 'IP/Netmask' set to '192.168.10.1 /24'. The 'Administrative Access' section shows 'IPv4' with 'HTTPS', 'HTTP', 'SSH', 'PING', 'FMG-Access', 'FTM', 'RADIUS Accounting', 'SNMP', and 'Security Fabric Connection' all checked. The 'DHCP Server' section is unchecked. The 'Network' section shows 'Device detection', 'Explicit web proxy', and 'Security mode' all unchecked. The 'Traffic Shaping' section shows 'Outbound shaping profile' unchecked.

V. Schéma globale de l'installation



Vision globale de l'Architecture Réseau IP réalisée

