**Cahier des charges**

1. Définition du besoin/objectifs

Actuellement la sécurité réseau contre les cyber-attaques est confiée au serveur Linux Pfsens

Or, ce dernier s’est révélé inefficace face à des attaques récentes plus élaborées et sophistiquées. Car ce commutateur de niveau 3 se limite à filtrer les flux de données en fonction des critères IP et TCP sans aucune analyse du comportement des trames transitant entre les zones internet, LAN et DMZ.

La DSI (Direction des Systèmes Informatiques) réfléchit à une solution d’évolution du système actuel de protection contre les cyber-attaques.

Il a été décidé qu’il faut remplacer le Firewall existant par un Firewall Nouvelle Génération de chez Storm Shield avec redondance (c’est-à-dire 2 Firewall).

Pour éviter une perturbation du réseau, des tests seront faits au préalable sur une infrastructure réduite de celle qui est actuellement utilisée.

Ces tests nous permettront de créer de la documentation pour créer un « kit » qui sera utilisé une fois les tests terminés pour, cette fois-ci, faire l’installation sur la véritable infrastructure de CUB.

1. Environnement

* Les tests de préproduction doivent être réalisés sur une infrastructure Sandbox (c’est-à-dire que les composants logiciels sont séparés du système d’exploitation)
* Ces modifications ne doivent pas perturber les habitudes de travail des employés.
* Le plan d’adressage IPv4 opérationnel doit rester inchangé.
* Un renforcement des contrôles de navigation sur internet est nécessaire. (Prévoir une sécurité supplémentaire)
* Il faudra également prévoir une charte d’information à destination des usagers des ressources internet.

1. Utilisation

• Une évolution transparente pour les usagers à l’exception de la charte informatique (les employés ne doivent pas être au courant des modifications)

• Management de la solution de sécurité via une interface WEB sécurisée

• Gestion des logs (fichier historique des évènements)

• Supervision des interfaces d’entrée/sortie (Gestion des alertes)

1. Sécurité

• Définir la stratégie d’accès au firewall ainsi que les outils utilisés

• Définir les règles de sécurité en entrée et en sortie des zones LAN/DMZ/Internet (Prévoir un tableau).

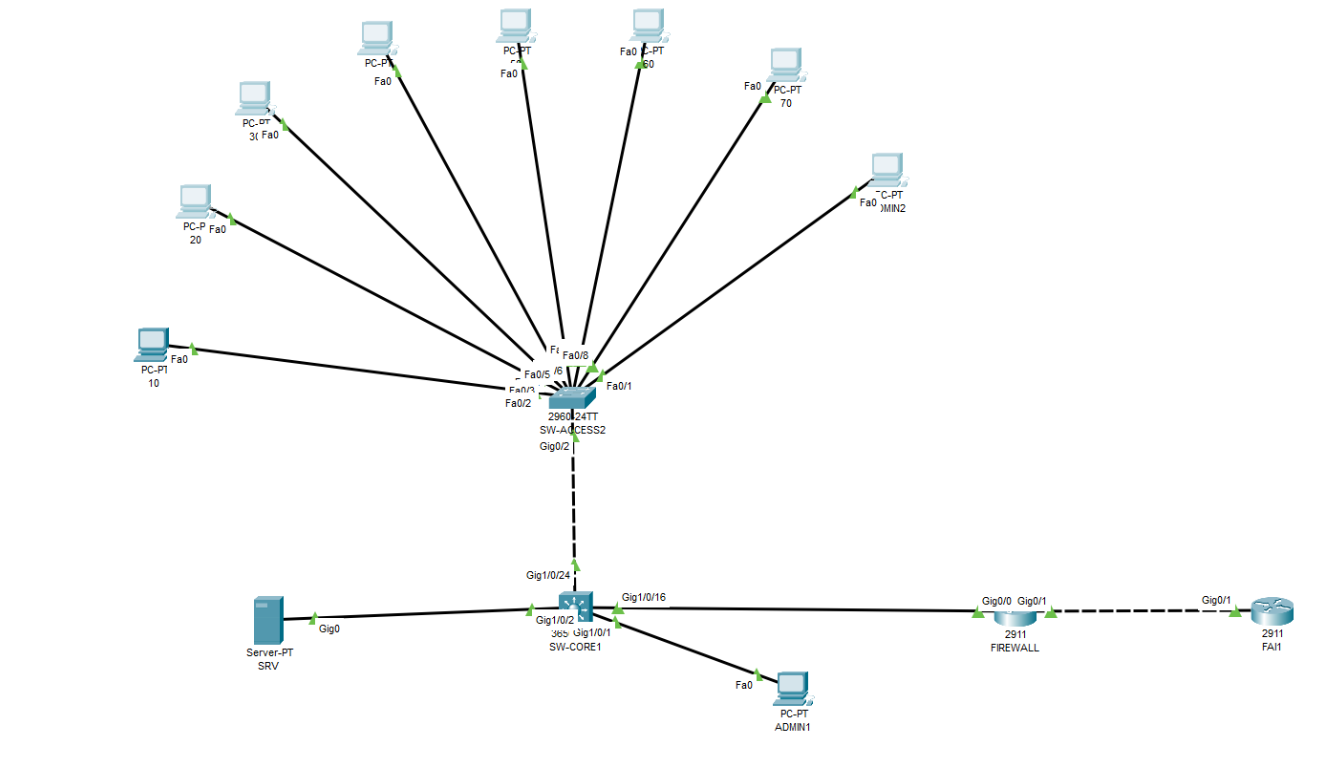
• Définir la stratégie de filtrage du contenu internet (La stratégie PROXY)

1. Coût

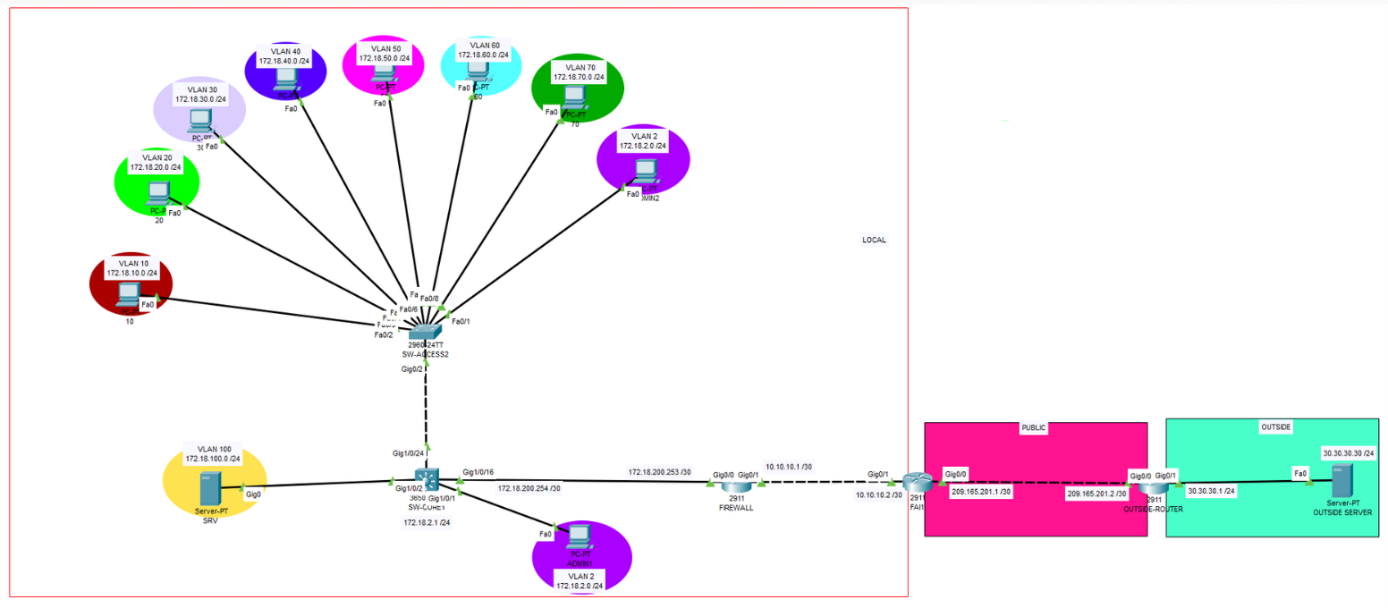
Switch SN2100 de chez Storm Shield avec redondance = 8 424,20 € HT // 10 109,04 € TTC

**Mise en place de la solution technique**

Schéma physique :



Schema logique

Plan d’adressage et de VLAN

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N° VLAN | VLAN | Service(s) | Adressage IP | Pools d’adressage | Passerelle par défaut |
| 2 | MANAGEMENT | Gestion des commutateurs et AP (WIFI), (Statique)  Sw-CORE1 : a.b.c.1  Sw-CORE2 : a.b.c.2  SwA-1 : a.b.c.11  SwA-2 : a.b.c.12  … | 172.18.2.0/24 | Aucun | 172.18.2.254 |
| 10 | DIR | Direction | 172.18.10.0/24 | 172.18.10.01/24À  172.18.10.150/24 | 172.18.10.254 |
| 20 | ADM | RH - Comptabilité - Juridique | 172.18.20.0/24 | 172.18.20.01/24  A  172.18.20.150./24 | 172.18.20.254 |
| 30 | COMMU | Communication | 172.18.30.0/24 | 172.18.30.01 /24  A  172.18.30.150 | 172.18.30.254 |
| 40 | MARKET | Marketing | 172.18.40.0/24 | 172.18.40.01 /24  A  172.18.40.150/24 | 172.18.40.254 |
| 50 | RDEV | Recherche et développement des solutions applicatives | 172.18.50.0/24 | 172.18.50.01 /24  A  172.18.50.150/24 | 172.18.50.254 |
| 60 | INFRASYS | Infrastructure & Système  ESXi-1 : 172.Y.60.1 | 172.18.60.0/24 | 172.18.60.01 /24  A  172.18.60.150/24 | 172.18.60.254 |
| 70 | VOIP | Téléphonie | 172.18.70.0/24 | 172.18.70.01 /24  A  172.18.70.150/24 | 172.18.70.254 |
| 100 | SRV | Serveurs  SRV-AD1 : 172.Y.100.1  SRV-AD2 : 172.Y.100.2  SRV-DHCP1 : 172.Y.100.3  SRV-DHCP2 : 172.Y.100.4 | 172.18.100.0/25 | 172.18.100.01 /25  A  172.18.100.150/25 | 172.18.100.126 |
| 200 | EXIT | Sortie (réseau d'accès à la sortie sur internet) | 172.18.200.0/30 | 172.18.200.01 /30  A  172.18.200.02/30 | 172.18.200.02 |

Configuration de base de l’élément de sécurité :

**Stratégie AD :**

Nous allons mettre en place une stratégie par groupe d’utilisateurs/VLAN + règle générale

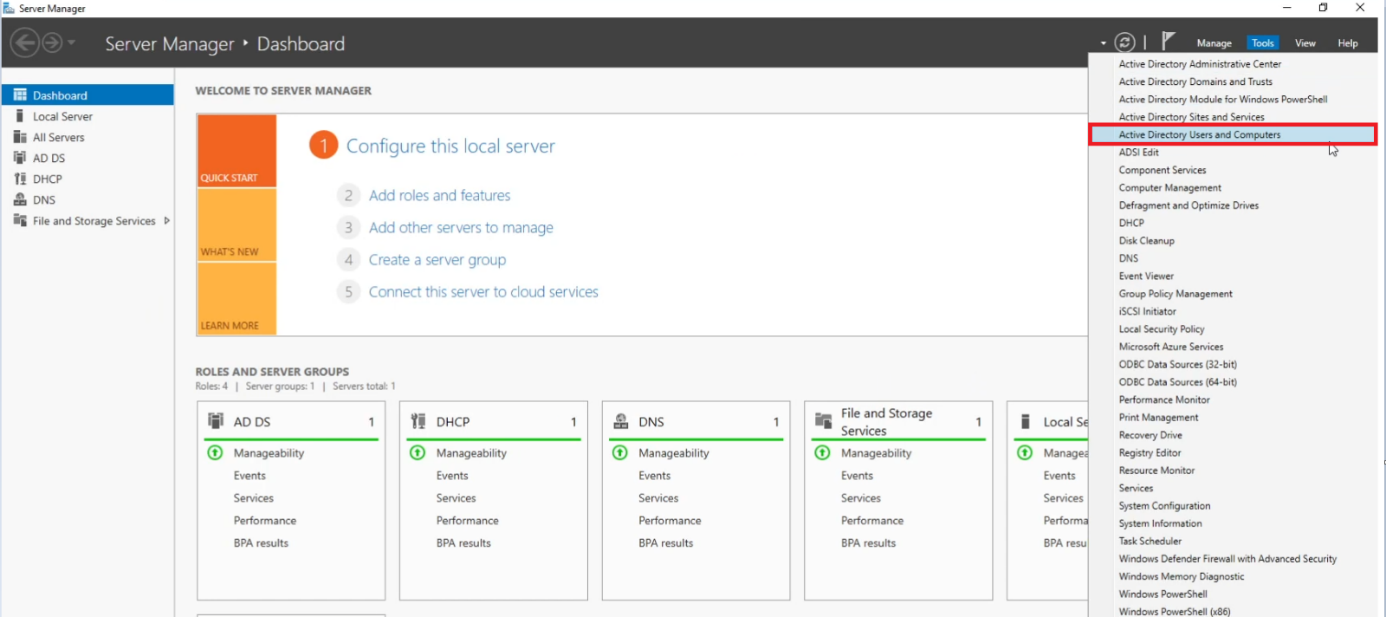
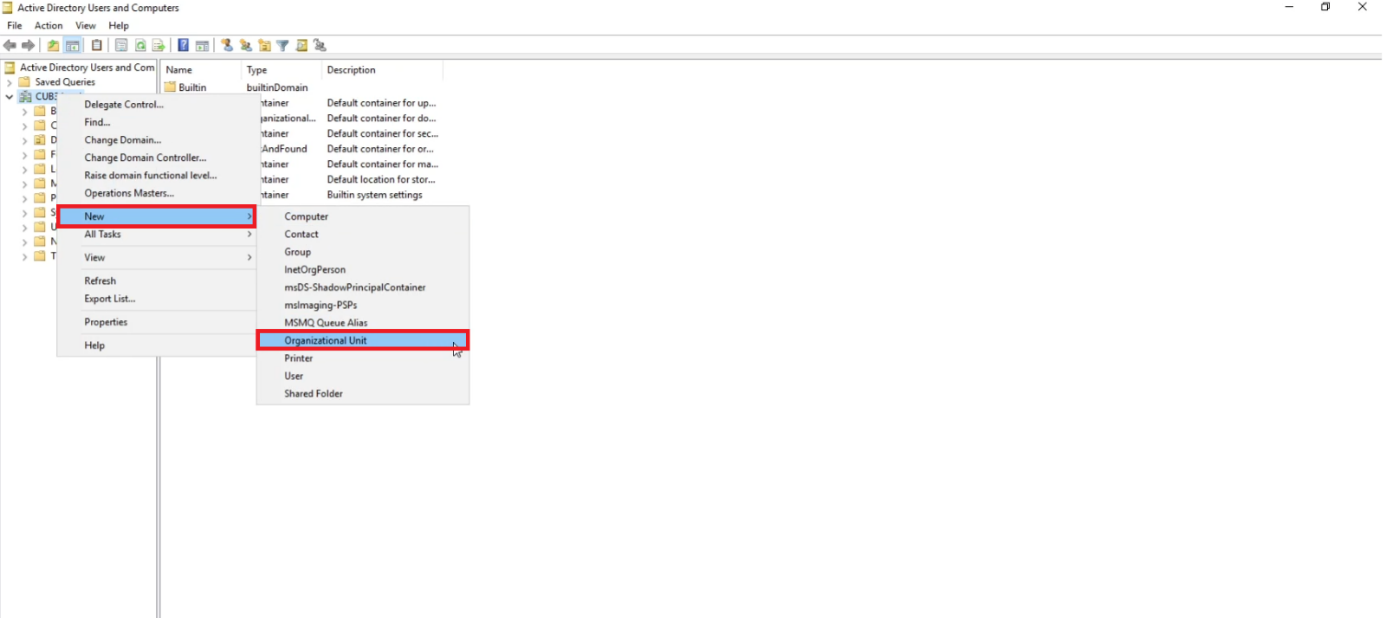
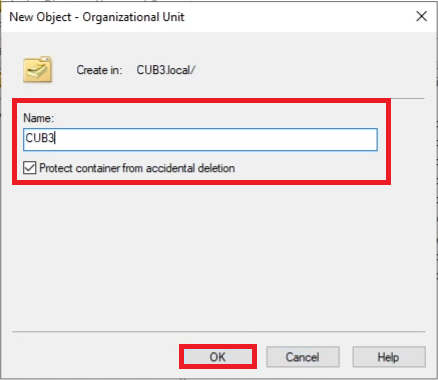
Règle générale :

-Avoir un mot de passe fort qui doit se composer d’un minimum de 16 caractères, le mot de passe devra également se composer d’au moins d’un des caractères suivants : une majuscule, une minuscule et un caractère spécial

|  |  |
| --- | --- |
| Groupe d’utilisateurs/VLAN | Règle mise en place |
| Administrateur/Vlan 2, Management | Droit de lecture et d’écriture - Accès au serveur depuis une zone défini |
| Vlan 10, Direction | Droit de lecture et d’écriture - Pas accès aux serveurs |
| Vlan 20, RH - Comptabilité - Juridique | Droit de lecture - Pas accès aux serveurs |
| Vlan 30 | Droit de lecture - Pas accès aux serveurs |
| Vlan 40 | Droit de lecture - Pas accès aux serveurs |
| Vlan 50 | Droit de lecture - Pas accès aux serveurs |
| Vlan 60 | Droit de lecture - Pas accès aux serveurs |
| Vlan 70 | Droit de lecture - Pas accès aux serveurs |
| Vlan 100 | Droit de lecture - Pas accès aux serveurs |
| Vlan 200 | Aucun droit |

**Création des unités d’organisation, des groupes et des utilisateurs ainsi que l’attribution de leur droit selon leurs groupes**

**F1.**Cliquer sur « Active Directory Users and Computers ».

Faites un clic droit sur le nom de votre domaine ici « CUB3.local » puis, cliquer sur « New » et enfin « Organizational Unit ». **Choissiser un nom pour votre unité d’organisation ici « CUB3 » puis, cliquer sur « OK ».** Faites un clic droit sur l’unité d’organisation que vous venez de créer puis, cliquer sur « New » enfin, cliquer sur « Organizational Unit » 