**Configuration de l’infrastructure réseau**

1. **Routeurs Cisco :**
   * Dans l'hôpital A, vous avez un routeur Cisco avec l'adresse IP 11.0.0.1/30
   * Dans l'hôpital B, un autre routeur Cisco est configuré avec l'adresse IP 12.0.0.1/30.
   * Ces routeurs servent de passerelle pour les données entre les deux hôpitaux.
2. **Firewall Stormshield :**
   * Chaque routeur Cisco est connecté à un firewall Stormshield.
   * Le firewall est chargé de sécuriser le trafic entre les routeurs et les réseaux locaux de chaque hôpital.
   * Il joue également de rôle de DHCP
3. **Switchs :**
   * Les firewalls Stormshield sont connectés aux switchs.
   * Les switchs permettent de connecter les serveurs et les PC de chaque hôpital.
4. **Adressage IP :**
   * L'hôpital A a un réseau local avec l'adresse IP 192.168.1.0/24.
   * L'hôpital B a un réseau local avec l'adresse IP 192.168.2.0/24.
   * Chaque serveur et PC dans ces réseaux utilisent des adresses IP de ces plages.
5. **VPN :**
   * Pour permettre la communication sécurisée entre les deux hôpitaux, un VPN est configuré.
   * Le VPN permet un échange sécurisé des procédures de consultation des données médicales entre les hôpitaux A et B.
   * Les firewalls Stormshield jouent un rôle essentiel dans la mise en place du VPN, assurant la confidentialité des données échangées.

Voici une description détaillée :

**Hôpital A :**

* Routeur Cisco A : Adresse IP 11.0.0.1/30
* Firewall Stormshield A : DMZ 10.0.0.0/24 - LAN 192.168.1.0/24 - WAN 11.0.0.0/30
* Switch A
* Réseau local : 192.168.1.0/24
* Serveurs et PC connectés au Switch A

**Hôpital B :**

* Routeur Cisco B : Adresse IP 12.0.0.1/30
* Firewall Stormshield B : DMZ 10.0.0.0/24 - LAN 192.168.2.0/24 - WAN 12.0.0.0/30
* Switch B
* Réseau local : 192.168.2.0/24
* Serveurs et PC connectés au Switch B

**VPN :**

* Configuration d'un tunnel VPN entre les deux firewalls Stormshield (A et B) pour permettre la communication sécurisée entre les deux hôpitaux.