Sécurisation de réseaux : intégration d'un firewall ASA dans un réseau

Contexte :

L'entreprise toulousaine TOLOSA-AERO, sous-traitant dans l'aéronautique a son siège à Toulouse et des bureaux dans certaines grandes villes comme Paris.

Pour sécuriser le réseau du siège, il a été décidé de migrer progressivement certains serveurs, initialement situés dans le LAN, dans une DMZ. Pour commencer, le serveur Intranet sera le premier à être migré dans la DMZ.

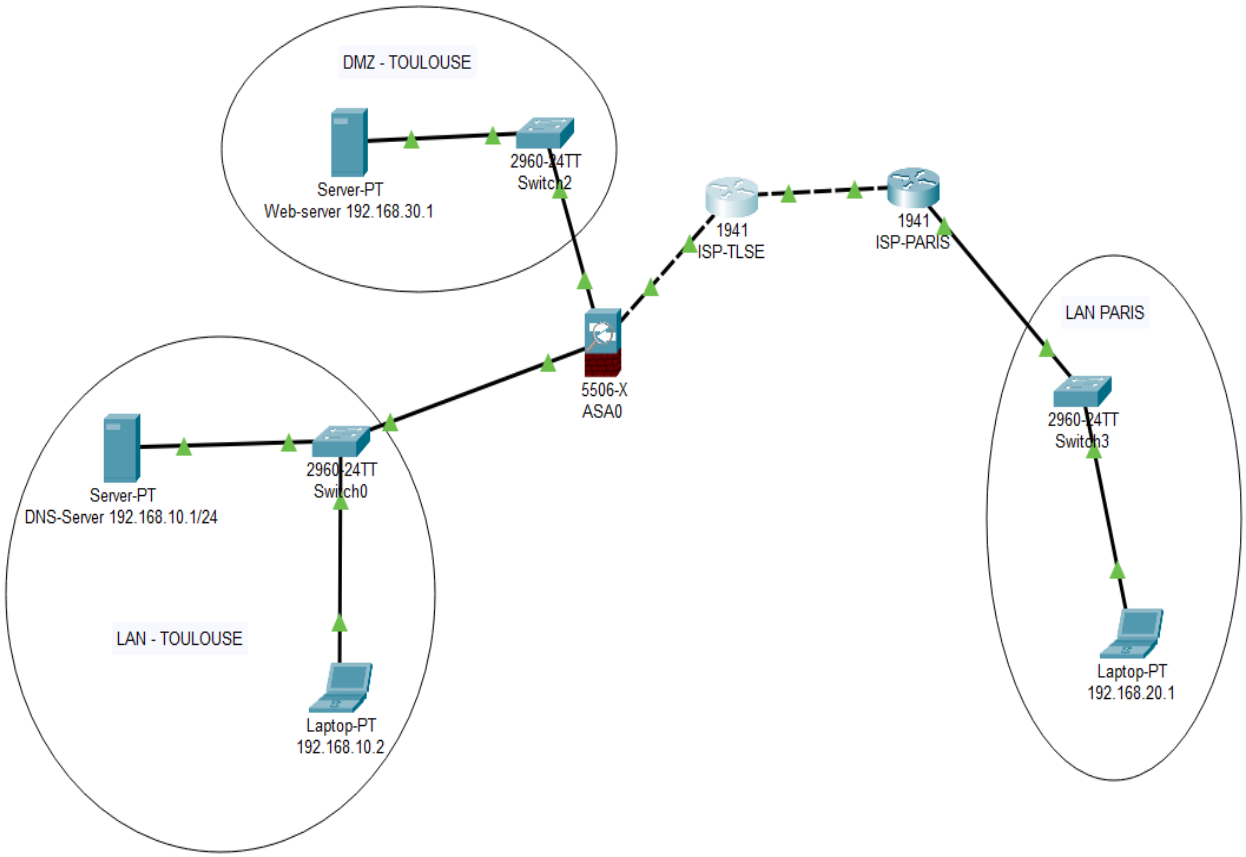
Vous venez d'intégrer le service informatique et il vous a été confié l'intégration du Firewall ASA dans le réseau.

Etape 1 : configuration des accès à une DMZ avec un FW ASA

Architecture étape 1 :

Les IP LAN sont les dernières IP valides de chaque sous-réseau.

Le choix des IP des routeurs et ASA reste à votre convenance.



Vous êtes chargé de configurer le FW ASA du site de Toulouse et les routeurs intermédiaires pour répondre aux objectifs ci-dessous. Dans toute l'étude, le ping devra être autorisé depuis n'importe quel site, pour faciliter les tests.

Depuis le LAN de Toulouse

- Chaque poste du LAN de Toulouse accède par la commande ping à l'interface WAN du routeur ISP-Paris
- Chaque poste du LAN de Toulouse doit accéder au serveur Web de la DMZ à la fois par la commande ping que par **http**.
- Depuis un poste de Toulouse, le ping vers un poste de Paris doit être fonctionnel

Depuis la DMZ

- Les serveurs de la DMZ accèdent par la commande **PING** à l'interface wan ISP-PARIS et à poste dans le LAN PARIS
- Les serveurs de la DMZ accèdent au LAN de Toulouse (Commande ping sur un poste dans le LAN de Toulouse)

Depuis le site de Paris

- Chaque poste du LAN de Paris accède par la commande **PING** à l'interface WAN du routeur ISP-TOULOUSE
- Chaque poste du LAN de Paris doit accéder au serveur Web de la DMZ à la fois par la commande **PING** et par **HTTP**.
- Depuis un poste de Paris, le ping vers un poste de Toulouse doit être fonctionnel

Résultat attendu :

Vous devez rendre votre un document .docx ou .odt contenant les preuves des résultats obtenus à chaque demande du CDC, les configurations effectuées sur les routeurs (extraits significatifs) et le fichier Packet Tracer associé de votre maquette.

Etape 2 : sécurisation de chaque site par un FW ASA

Après la première phase il a été décidé d'introduire un firewall dans chaque site pour mieux sécuriser les sites distants.

En prenant pour site pilote celui de Paris, configurer l'ASA de Paris de sorte à permettre toujours l'accès au serveur de la DMZ, à partir du poste 192.168.20.1.

a) Sans VPN mis en place entre le site de Paris et le site de Toulouse
b) Avec un VPN mis en place un VPN entre les sites de Paris et Toulouse