TP08 – Évolution d'une infrastructure

Changements au niveau de l'infrastructure :

Dans le cadre de l'évolution de notre infrastructure existante, certaines modifications seront nécesaires :

Tout d'abord, le serveur DNS2 est retiré et supprimé.

Ensuite, un nouveau sous-réseau en 172.17.0.0 /24 est créé avec un serveur nommé « srv-dmz » qui assure la fonction de PROXY et de serveur DNS.

La machine srv-service devient exclusivement dédiée au service DHCP.

La machine srv-admin reçoit une troisième carte réseau avec l'addresse 172.17.0.254.

La NAT reste établie pour le DNS, et la machine admin devient une machine de firewall, ce qui miroite un peu le TP07 en termes d'infrastructure.

Dans la nouvelle infrastructure, les machines *pc-cli, pc-desk et pc-secure* passent par le proxy pour un accès à internet filtré. Pour la résolution de nom, les nameservers de srv-dmz seront ceux du lycée (10.121.38.7 et 10.121.38.8 dans resolv.conf).

Services déployés à l'issue du TP06 :

Après la fin du TP numéro 6, les services déployés et actifs sont les suivants : *isc-dhcp-server* pour le DHCP, *bind9* pour les services DNS, et *squid* pour le proxy. De plus, un service nommé *dnsfwd.service* associé à un fichier bash du même nom se charge de router les requêtes DNS via la NAT.

Un ancien service de NAT, qui était un set de commandes *nftables*, a été supprimé pour la mise en place du proxy, lors du TP06.

Tableau des services :

Service	Localisation avant changement	Localisation après changement	Impacts prévus
Routage	srv-admin	srv-admin	Modification du simple routage en un pare-feu *statefull*. Impact important sur toutes les communications réseau ; filtrages et NAT à mettre en place pour les services adéquats
DHCP	srv-service	srv-service	Aucun changement visible au niveau des configurations DHCP, donc aucun impact sur les communications réseau/les adresses IP déjà définies. La plage DHCP ne change pas. Changer l'IP donnée du serveur DNS.
DNS	srv-service, srv-dns2	srv-dmz	Suppression d'une des deux machines DNS et déplacement total du service, vers une machine sur un autre réseau : il faudra changer les adresses IP qui pointaient vers les anciens DNS, et vérifier l'impact sur la résolution de nom. Il faudra aussi rajouter des alias dans les fichiers et d'autres adresses IP.
Proxy	srv-admin-ge	srv-dmz	Le proxy était installé d'abord sur srv-admin, le proxy devra donc être supprimé de la machine admin, et installé puis configuré sur la machine DMZ. Il faudra donc revoir toutes les configurations effectuées dans squid. Il faudra aussi changer les adresses dans les machines qui utilisent le proxy pour pointer au bon endroit. Mettre règles de redirection pour le proxy dans le firewall.

À rajouter dans tableau : ~~manque dans DHCP~~, ~~manque dans proxy~~.

Configurations de base à changer/préparer :

Rajouter une carte réseau à la machine admin qui pointe vers la future DMZ.

Créer la machine DMZ et y mettre les paquets ssh, bind9, git, tcpdump et squid en plus de debian, en CLI, pas besoin d'interface graphique.

Suppression du paquet squid sur la machine admin. (backup des fichiers de conf)

Supprimer les paquets bind9 de la machine srv-service. (idem)

Supprimer la machine DNS2.

Services à changer :

Retirer chaque référence à dns2 dans les fichiers de bind.

Changer les règles dans le pare-feu (ajouter règles de redirection pour le proxy).

Mettre la NAT et le filtrage du proxy en place dans squid.

Dans les fichiers de configuration du DHCP, changer l'adresse du serveur DNS.

Faire de même dans les fichiers resolv.conf.

Reprendre les fichiers DNS de srv-service et les adapter à la nouvelle situation.

Concernant la migration des services :

Pour migrer les services, je pense installer et configurer les nouveaux services d'abord, puis modifier les fichiers de configuration de chaque service (s'il est sur la bonne machine), modifier les fichiers de configuration des machines pour qu'ils pointent aux nouvelles adresses IP des services, puis supprimer les paquets des machines qui assumaient le rôle des services une fois l'infrastructure fonctionnelle et déployée dans son état final.

Configuration progressive du pare-feu :

Voir fichier *firewall_regles.txt* sur le Gitea.

Lien direct au fichier sur le Gitea.