PROJET DMZ

Définition du besoin

La maison des ligues de Lorraine (M2L) fait héberger depuis plusieurs années ses services extranet hébergés par un prestataire. Afin de mieux maîtriser les risques, il a été décidé d'internaliser l'hébergement des services ouverts à l'ensemble des associations partenaires. L'application de gestion de parc et d'incidents GLPI sera la première à basculer en interne.
Il est donc demandé au département IT de la M2L d'adapter l'infrastructure actuelle à ce nouveau besoin, en la cloisonnant et en la sécurisant pour des accès distants.
La solution retenue sera un GLPI sécurisé par TLS en architecture trois-tiers dans une DMZ hiérarchisée, avec administration distante sécurisée par VPN avec certificats clients.

Mission

La mission de votre équipe sera de :
- Construire une infrastructure sécurisée de type DMZ hiérarchique
- Offrir un service sécurisé d'administration à distance
- Déployer un service Web sécurisé et réparti sur les deux DMZ
- Migrer l'application `GLPI` existante et la sécuriser
- Mettre en place de la supervision et de la robustesse sur le service `GLPI`
- Respecter les contraintes de maquettage en labo SISR

Projet : **AP 4.1**	Contexte : **M2L**	Mode : **projet**	Équipe : **4 étudiants**	Durée : **20 heures (5 séances)**

Cahier des charges

Vue d'ensemble et contraintes de maquettage :

- **Nommage**
  - Les réseaux seront nommés `WAN`, `Pub<eq>`, `Priv<eq>` , `Adm<eq>`, `Dev<eq>` et `Usr<eq>`, où `<eq>` correspond à votre numéro d'équipe [1 à 8].
  - De même, les passerelles seront nommées `Fgtw<eq>` (pour la passerelle frontale) et `Bgtw<eq>` (pour la passerelle dorsale), dans le domaine `m2l.fr`.
  - Les serveurs seront nommés `WebR<eq>`, `Bdd<eq>` et `Sav<eq>`.
  - Les pattes des hôtes seront nommées `wan`, `pub`, `priv`, `adm`, `dev` ou `usr` selon leur emplacement.
- **STA et utilisateurs**
  Il y aura 3 profils d'utilisateurs et donc de STA, utilisées depuis le LAN ou le WAN :
  - Postes `usr.usr` et `usr.wan` de Otto LISATER (`olisater`) → Win10 avec firefox.https (ou edge.https) pour accéder à l'application Web depuis le LAN ou le WAN.
  - Postes `dev.dev` et `dev.vpn` de Dave LOPPER (`dlopper`) → Win10 avec firefox.https (ou edge.https) et winscp.sftp (ou explorer.sftp) pour accéder aux serveurs `WebR` et `Bdd`.
  - Postes `adm.adm` et `adm.vpn` de Amine YSTRATER (`aystrater`) → Kali avec firefox.https (ou chromium.https), ssh, scp et filezilla.sftp (ou thunar.sftp) pour accéder à l'ensemble des machines de l'infrastructure.

  `Otto`, `Dave` et `Amine` seront vos utilisateurs pour les tests et vous pourrez en créer d'autres de votre choix si besoin. Pour des questions de simplification, nous n'implanterons pas de service d'annuaire centralisé de type LDAP. Les comptes seront donc créés sur chaque machine administrée.
- **Câblage**
  - Fgtw aura 2 pattes { LAN → pub ; WAN → WAN } …
  - Bgtw aura 5 pattes { LAN → adm ; WAN → pub ; OPT1..OPT3 → usr/dev/priv }. Le script de création de la 5e patte est fourni en ressource.

- Le réseau SIO sera utilisé comme accès au WAN – APP(#0).
- Le switch 1 sera utilisé comme domaine de diffusion pour le réseau Pub – APP(#1).
- Le switch 2 sera utilisé comme domaine de diffusion pour le réseau Priv – APP(#2).
- Des hubs virtuels seront utilisés comme domaine de diffusion pour les 3 réseaux restants – RI(Usr ; Adm ; Dev).
- Aucune reconfiguration virtuelle de l'infrastructure OSI1+2 ne sera donc nécessaire dans ce projet. Ainsi, vous aurez uniquement besoin d'une STA infra pour vérifier que les matériels d'interconnexion sont dans leur état par défaut en début de séance.
- Les switches NG de l'armoire de plot seront déconnectés l'un de l'autre par le prof. durant le temps des AP.

- **Règles de bonne pratique**
  - Les VM nécessaires seront implantées sous VirtualBox sur vos HM de plot.
  - Pour des questions d'hygiène de sûreté et d'efficacité dans votre travail de réalisation, vous commenterez systématiquement vos paramètres en relation avec le contexte et sauvegarderez systématiquement les fichiers de configuration originaux ainsi qu'une version par action de configuration validée par des tests réussis, et au 'pire' au moins une version par séance…
  - Pour avoir une chance de finir le projet dans les temps impartis, vous validerez systématiquement chaque tâche passée de ***WIP*** à ***Done*** par un test unitaire.
  - Afin que chaque séance d'AP soit un jalon documenté, vous penserez à tenir à jour votre trello et à en faire une copie d'écran en fin de séance.

Réseaux et cloisonnement des accès (routage et filtrage) :

- **LAN** → Subdivisé en 5 sous-réseaux, tous reliés, routés et filtrés par **Bgtw**.
  - Toutes les machines du LAN bénéficieront d'un accès à Internet par passerelle, ainsi que des services centralisés de Bgtw.adm.dns et Fgtw.pub.ntp.
  - `Usr<eq> 172.16+<eq>.0.0/16`, réseau hébergeant la majeure partie du parc informatique de la M2L dont les postes `usr.usr`, les imprimantes `prn.usr`. En dehors de leur réseau et d'Internet, les utilisateurs pourront uniquement accéder à l'application Web en mode sécurisé sur l'intranet.
  - `Dev<eq> 192.168.<eq>.0/24`, réseau où l'on trouve uniquement les postes des développeurs en présentiel `dev.dev`, En plus des droits de base des utilisateurs, les développeurs sont autorisés à développer en accès sécurisés sur les serveurs WebR et Bdd.
  - `Adm<eq> 192.168.100+<eq>.0/24`, réseau duquel les administrateurs en présentiel sont autorisés à accéder à tous éléments de l'infrastructure qu'ils administrent à distance en mode sécurisé depuis leur poste `adm.adm`. On y trouve aussi le serveur Sav, qui lui ne peut converser qu'avec le serveur Bdd.
  - `Pub<eq> 10.54.<eq>.0/24`, réseau frontal de DMZ "publique" qui héberge le serveur Web sécurisé (2e tiers de l'application `GLPI`). Ce serveur peut uniquement converser avec le serveur Bdd.
  - `Priv<eq> 172.31.<eq>.224/27`, réseau qui héberge le serveur de base de données sécurisé (3e tiers de l'application `GLPI`). Ce serveur recevra uniquement des requêtes de WebR, Adm, Dev, VpnA et VpnD.
- **WAN** → Constitué du réseau `SIO 192.168.51.0/24` faisant office de FAI local avec service DHCP complet, relié au LAN par **Fgtw**.pub qui assure le routage et le filtrage.
  Depuis le WAN, les utilisateurs distants `usr.wan` comme les membres de bureaux de clubs ou salariés de la ligue en télétravail accèderont aux services de la M2L, en particulier l'application sécurisée GLPI dans le cadre de ce projet.
  Depuis le WAN, les membres de la DSI autorisés `adm.vpn` et `dev.vpn`, en télétravail ou lors de leurs astreintes, pourront se connecter en VPN routé pour accéder à distance de manière sécurisée aux machines ou services qu'ils administrent avec les protocoles https, ssh, sftp, scp.
- **VPN** → Constitué de 2 sous-réseaux dédiés :
  - Toutes les machines du VPN bénéficieront d'un accès à Internet par passerelle, ainsi que des services centralisés de Bgtw.adm.dns et Fgtw.pub.ntp.
  - `VpnA<eq> 10.7.<eq>.0/28`, réseau OpenVPN routé servi, routé et filtré par Fgtw.wan et dédié aux administrateurs en accès depuis le WAN `adm.vpn`, qui bénéficient des mêmes privilèges que les `adm.adm`.
  - `VpnD<eq> 10.6.<eq>.0/28`, réseau OpenVPN routé servi, routé et filtré par Fgtw.wan et dédié aux développeurs en accès depuis le WAN `dev.vpn`, qui bénéficient des mêmes privilèges que les `dev.dev`.
- Les passerelles seront aux adresses IP les plus hautes. Les serveurs aux adresses en dessous.
- Tous les hôtes auront comme passerelle par défaut celle qui est la plus proche d'Internet.

- Pour des besoins de supervision, toutes les pattes devront répondre aux requêtes ping.

Serveurs et services :

- Toutes les pattes de serveur ou passerelle seront en configuration IP statique à l'exception de Fgtw.wan qui sera en configuration IP dynamique.
- Les accès WAN des utilisateurs se feront en https, mais les développeurs et les administrateurs devront se connecter en VPN depuis le WAN pour pouvoir travailler sur les machines du LAN.
- Tous les accès seront sécurisés :
  - Les accès SSH et VPN seront authentifiés par certificat client et login et mot de passe.
  - Les accès HTTPS aux services seront authentifiés par login et mot de passe.
- **WebR**
  - Les utilisateurs de l'application Web GLPI devront pouvoir y accéder depuis Internet et depuis le LAN, de manière sécurisée (HTTPS).
  - Une page Web statique personnalisée pour identifier votre équipe sera déposée sur le serveur Web.
  - La base existante GLPI sera reprise pour assurer la migration de l'existant.
  - Le nouveau serveur Web (`WebR<eq>`) basé sur Apache2, PHP, et Debian12, sera placé dans le nouveau réseau DMZ publique.
- **Bdd**
  - Le nouveau serveur de base de données basés sur MySQL ou MariaDB et Windows 2016 (serveur WAMP), sera placé dans le nouveau réseau DMZ privée.
- **Sav**
  - Les utilisateurs métier ont rempli une backlog avec la liste des besoins, leurs priorités, et les résultats attendus : https://trello.com/b/I0FETurc/migration-glpi-m2l
- **Fgtw**
  - Services DNAT et VPN côté wan
  - Services admin GUI, relai/cache de résolution de noms, synchro horloges et SNAT côté pub
    - Fgtw.wan → { dnat tcp 443 → WebR }
    - Fgtw.pub → { https tcp 443 admin ; dnsmask udp/tcp 53 ; ntp udp 123 ; snat auto }
    - Fgtw.vpna → { openvpn udp 1199 }
    - Fgtw.vpnd → { openvpn udp 1200 }
  - Initialement, le routage devra être assuré et validé et le filtrage annulé par des règles "TOUT PASSE". À terme, toute autre flux requête que ceux listés devra être bloqué.
- **Bgtw**
  - Service DHCP côté usr, dev et adm
  - Services admin GUI et résolution de noms complète (zone directe, zone inverse, relai, cache, hôtes dynamiques) côté adm
    - Bgtw.usr → { kea-dhcp4 udp 67 }
    - Bgtw.dev → { kea-dhcp4 udp 67 }
    - Bgtw.adm → { https tcp 443 admin ; unbound udp/tcp 53 ; pki ; kea-dhcp4 udp 67 ; snat disable }
    - Bgtw.priv → { }
  - Initialement, le routage devra être assuré et validé et le filtrage annulé par des règles "TOUT PASSE". À terme, toute autre flux requête que ceux listés devra être bloqué.
    - DHCP → { IP ; mask ; gtw ; dns ; domain ; search ; ntp ; dns-registration }
    - DNS → { forwarding(Fgtw.pub) ; host overrides }
    - PKI → { 1 CA } { 5 SC : WebR.https Bdd.https Fgtw.pub.https Bgtw.adm.https Fgtw.vpna Fgtw.vpnd } { 2 CC : adm.vpna(Amine) dev.vpnd(Dave) }

Tâches et livrables

Afin de réaliser ce projet, vous devrez, au sein de l'équipe, planifier et distribuer les **tâches** telles que, par exemple :

- la spécification de l'infrastructure de maquettage dans le cadre de votre plot de Labo SISR, sous formes d'un schéma réseau logique et d'un schéma réseau physique ;
- l'identification et la validation des US auprès du directeur de projet ;
- le découpage des US en tâches d'une durée de **1h max chacune** (méthode agile) ;
- l'utilisation de **Trello** comme outil de gestion **agile** du projet ;
- la spécification d'un **plan de tests** de validation (US) ;
- la spécification d'un plan de tests unitaires (tâche) et d'intégration (tâche spécifique) ;

- la configuration du réseau, des systèmes et des services ;
- les **preuves** de résultats des **tests unitaires, d'intégration et de validation** ;
- tout autre documentation spécifiquement requise par le client.

Les **livrables** attendus par le client sont :

PARTIE GESTION DE PROJET

◦ vos 5 screenshots Trello de fin de chaque séance ;
◦ vos journaux de bord ;
◦ vos fiches de réalisation professionnelle ;
◦ votre onglet d'équipe du fichier Livraison par équipe ap4.1 ;
◦ **une fiche recette** sous forme de grille synthétique, recensant :
  ▪ pour chaque US du projet si la solution apportée est totalement fonctionnelle (vert), partiellement fonctionnelle (orange) ou non livrée (rouge) ;
  ▪ pour chaque US orange ou rouge (**réserves**), les problèmes rencontrés (techniques, humains, temporels, organisationnels) et les solutions tentées ou envisagées.
◦ un bilan d'équipe avec 1 à 5 points clés sur ce que vous avez appris et ce que vous feriez différemment si c'était à refaire.

PARTIE TECHNOLOGIQUE

- votre plan de tests (unitaires, d'intégrations) basé sur les tâches de votre Trello ;
- votre plan de tests de validation, basé sur vos US et cas d'utilisations (fournis en ressource) ;
  (→ qui seront pour moitié évalués en Labo avec vous)

- une documentation technique de conception avec : = { la table des systèmes ; vos schémas réseaux logique et physique ; les 2 tables de routage ; la liste des 8 (1+5+2) certificats ; la table de translation dnat ; les 7 (2+5) tables de filtrage ;
- une documentation technique simple mais structurée de la configuration de Fgtw, avec les screenshots { dashboard ; status.interfaces ; status.services ; services.ntp ; services.dns-forwarder ; system.routing.gateway ; system.routing.static-routes ; diagnostics.routes ; diagnostics.sockets ; vpn.openvpn (2S+2C) ; firewall.nat.port-forward ; firewall.nat.outbound ; firewall.rules (2) } ;
- une documentation technique simple mais structurée de la configuration de Bgtw, avec les screenshots { dashboard ; status.interfaces ; status.services ; services.dns-resolver ; services.dhcp-server (3) ; system.certificates (1A+5S+2C) ; system.routing.gateway ; diagnostics.routes ; diagnostics.sockets ; firewall.nat.outbound ; firewall.rules (5) } ;
- les paires de clés bien nommées de l'organisation (1), des serveurs (5) et des clients (2) ;
- les fichiers de configuration des 2 passerelles ;

- vos procédures de migration et de tests pour la reprise de GLPI ;
- les différents livrables correspondants à chaque besoin dans la backlog.

Le chef d'équipe rassemble les livrables de ses coéquipiers pour livraison à l'échéance. *Les livrables contribuent conséquemment à la note d'AP. Le récapitulatif des répartitions par livrable fera foi.*

Ressources

Vous avez à votre disposition les ressources suivantes, sur le partage Commun :

- Dossier AP/ap4.1/ avec énoncé, fichier d'analyse et ressources, dont documents de contexte M2L ; schéma réseau de la M2L ; wampserver3.2.6_x64 ; documentation de consignes et d'aide diverses dont les fichiers { table-des-systèmes ; conception-initiale ; plan-de-tests ; livraison-par-équipe }
- Les OVA { pfSense-2.81 ; debian-12 ; Kali ; Win10 ; Win2016 } ; le dossier AP contextes.
- L'application GLPI à migrer se trouve actuellement sur le serveur web en 192.168.51.234, accessible en SSH (id *sisr* ; mdp *P@55aran*, le prestataire ne vous a PAS donné les identifiants GLPI). Il est possible que cela évolue au cours du projet !