

PROJET Navajo



Définition du besoin

Le département IT de GSB fait face à de nombreuses demandes de la part des départements Métier de l'entreprise. Différents projets à venir vont nécessiter une infrastructure de test et de validation.

En effet, la solution *Navajo*, consistant à fournir un service Web extranet aux visiteurs médicaux, qui sera aussi accessible aux développeurs, doit être validée en maquette avant d'être intégrée à l'environnement de production. Un système de noms de domaines local ainsi qu'une gestion déportée de configurations dynamiques IPv4, vont être redéployées en intranet.

Navajo sera basé sur des technologies autour d'Apache2, hébergée sur le nouveau serveur EXTRALAB.

Les autres services seront fournis par le serveur REZOLAB.

Mission



La mission de votre équipe sera de :

- Fournir une maquette partielle de test de l'infrastructure, administrable à distance de manière sécurisée ;
- Respecter les contraintes de maquettage imposées par le labo SISR ;
- Valider le bon fonctionnement, du point de vue des utilisateurs, des trois services fournis, et en particulier de la solution *Navajo*, qui devra être sécurisée.

Projet : AP 3.1	Contexte : GSB	Mode : projet	Équipe : 4 étudiants	Durée : 20 heures (5 séances)
------------------------	-----------------------	----------------------	-----------------------------	--------------------------------------

Cahier des charges

• Interconnexion réseau :

- Etant donné que vous n'êtes pas les seuls usagers du labo SISR, vos configurations de matériel d'armoire de plot devront être restaurées en début et sauvegardées en fin de chaque séance d'AP ; Les configurations par défaut devront être restaurées et les armoires débranchées avant de quitter la salle – vous prévoirez du temps à cet effet.
- Le câblage existant dans le labo SISR ne devra pas être modifié – vous devrez donc implanter une infrastructure virtuelle au sein de l'infrastructure réelle pré-câblée, au niveau OSI1+2 !
- Les serveurs et STA nécessaires seront implantés sous VirtualBox sur les machines hôtes de plot, en accès par pont vers les commutateurs de niveau 2 NG gs108tv3.
- Le **routing Inter-VLAN** sera assuré par MUTLAB, commutateur de niveau 3 HP 2615. A la livraison, MUTLAB devra être administrable à distance via **SSH**, depuis une STA Infra (Kali). Les commutateurs de sous-répartition de niveau 2 NG gs108tv3 seront administrés à distance via **HTTPS**.
- Le **routing LAN-WAN** sera assuré par PROXYLAB, passerelle de sécurité pfSense.
- Le réseau Dev<eq> est en { VLAN 150+<eq>; 192.168.150+<eq>.0/24 } et contient les terminaux des développeurs.
- Le réseau Srv<eq> est en { VLAN 300+<eq>; 172.16.0.0/17 } et contient les services intranet .
- Le nouveau réseau DMZ<eq> est en { VLAN 400+<eq>; 172.18.<eq>.0/27 } et contient les services extranet.
- Le réseau Internet et notre FAI seront émulés par le réseau privé SIO en 192.168.51.0/24 avec services DHCP, DNS (relais) et de passerelle en .254.
- Le réseau Infra est en { VLAN 1; 10.s.p.0/24 } et permet l'administration de l'infrastructure – s correspond au numéro de salle 0 (b100) ou 1 (b101) et p au numéro de plot 1, 2, 3 ou 4.
- Vous documenterez la table des systèmes selon le format { hostname+OS | fonctions | protocoles | hostname+OS+app STA admin | hostname+OS+app STA test } - fait avec les profs au moment de la présentation du projet.

- La documentation du plan d'adressage/routage et du plan de câblage sous forme de schémas réseaux logique et physique devra être complétée (un squelette vous est fourni en ressource). Auquel il faudra ajouter les tables de routage de MUTLAB et de PROXYLAB (modèle fourni en ressource).

• Serveurs et services :

- Les serveurs seront administrés à distance (**SSH**, **HTTPS**) depuis une STA Admin (Kali). Les développeurs accèderont en Intranet à leurs services depuis des terminaux soit sous W10 avec vscode et winscp, soit sous Kali avec vscode et thunar ou filezilla client. Ils pourront ainsi déposer leur code sur EXTRALAB. Ils utiliseront Firefox pour tester leurs applications. Les visiteurs médicaux accèderont en Extranet à l'application Navajo.
- Le serveur REZOLAB, (debian-12 ; cf. SR de contexte) est dans le réseau Srv. Il offre un service DHCP déporté pour le réseau Dev, et un service DNS pour le domaine local galaxy-swiss<eq>.lan.
- Le service **DHCP** devra fournir les options globales ou d'étendue : domaine, passerelle, serveur de noms.
- Les développeurs partagent une imprimante HP LaserJet, en .2, qui devra toujours recevoir la même configuration IP.
- Le service **DNS** devra fournir une zone d'autorité locale (rôle Master) avec enregistrements d'adresses d'hôtes (mutlab, rezolab, extralab, ...), un alias www pour EXTRALAB, une zone de recherche inversée pour le réseau Srv, et une redirection (rôle Relais) vers le DNS du FAI pour les autres zones, notamment globales.
- Les STA du réseau déporté Dev devront pouvoir être jointes grâce à leur nom (dyndns).
- Le nouveau serveur EXTRALAB (debian-12 ; .<eq>.2) sera placé dans le nouveau réseau DMZ.
- Le **service Web** (apache2) devra être accessible depuis une STA de visiteur médical (VisiteurM) en tournée (accès Extranet), mais aussi par les développeurs (Dev) afin qu'ils puissent tester leur code (accès Intranet).
- Une page Web statique mais personnalisée pour identifier votre équipe sera déposée sur le serveur Web, qui sera sécurisé en **HTTPS**.
- Les utilisateurs devront s'authentifier pour être autorisés à accéder au site Web. Voici quelques comptes utilisateurs : Gérard Mansoif, Denis De Pool, Aïcha Fémal (développeurs) ; Sarah Tiboise, Henri Golan, Geoffrey Décado (visiteurs médicaux) ; sisr (administrateurs).
- Le mode d'authentification visé à terme s'appuiera sur le protocole **LDAPS**. L'annuaire sécurisé est disponible à l'adresse 192.168.51.247 (dans la ferme de virtualisation). Les comptes utilisateurs y sont actifs, tous avec le mot de passe P@55aran.
- Le serveur CERTILAB (pfSense ; .0.40) fournira le service de **PKI** permettant d'administrer les différents certificats (auto-signés) de l'organisation, dans le réseau Srv.
- Les services de pare-feu, **reverse-proxy** et service local de **synchronisation d'horloges** seront fournis par le serveur PROXYLAB (pfSense avec paquetage haproxy ; .30 ; cf. SR de contexte), en interface entre MUTLAB et Internet.
- Le service de temps sera référencé par tous les serveurs (statique) et postes utilisateurs (dhcp).

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 en ligne Livraison par équipe ap3.1 ;
- **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 ;
(→ qui seront pour moitié évalués en Labo avec vous)
- un dossier technique de conception réseau avec : { la table des systèmes ; le schéma logique complété pour correspondre à votre équipe ; le schéma réseau physique (avec numéros de ports et de VLAN en formalisme U/T) correspondant à votre équipe et votre plot ; les tables de routage prévues pour mutlab et proxylab ; la liste des certificats } → cf. ressource *Conception initiale - infos.txt* ;
- un dossier technique de configuration de mutlab avec les commandes : { show vlan 1/50/300/400 ; show ip ; show ip route ; show dhcp-relay ; show ip helper-address } ;
- les fichiers de configuration effectifs des switches NG et MUTLAB ;
- les fichiers de configuration et journaux DNS avec : { 6 named.conf named.conf.local named.conf.options named.conf.default-zones db.galaxy-swiss.local db....in-addr-arpa + 1 bind9.log } ;
- les fichiers de configuration et journaux DHCP avec : { 1 dhcpd.conf + 2 dhcpd.log dhcpd.leases } ;
- les fichiers de configuration et journaux HTTPS avec : { 5 apache2.conf ports.conf extralab<eqX>.conf,-default-ssl index.html + 2 access.log error.log } ;
- un dossier technique de configuration de certilab avec les screenshots de : { dashboard services status.interfaces firewall.rules routing-table pki } ;
- les certificats de certilab avec : { 1 CA [crt] + 3 CS [key,crt] } ;
- un dossier technique de configuration de proxylab avec les screenshots de : { dashboard services status.interfaces firewall.rules routing-table ha-proxy } ;
- les fichiers de configuration de certilab et de proxylab ;

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 du temps passé par tâche fera foi.

Ressources



Ressources à disposition sur le Commun :

- Contexte GSB, dont schéma logique de GSB ;
- Schéma réseau logique de maquette – à compléter ;
- docs Labo SISR ;
- docs matériel d'interconnexion (SW NG 108gstv2, SW HP 2615) ;
- fichiers de configuration par défaut des matériels d'armoire technique ; docs VLAN et PVID ;
- docs serveurs/passerelle Debian, pfSense ;
- docs services Apache2, DNS, DHCP, LDAP, PKI, NTP, HA-Proxy
- Rappels Trello Agile ;

Et dans le dossier MVOrg :

- OVA des VM serveur Deb12 ; passerelle et serveur pfSense 2.80 ; STA W10 et Kali incluant les applications ssh, firefox, thunar/filezilla, scp/winscp, vscode ...