BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2017

E5SR : PRODUCTION ET FOURNITURE DE SERVICES

Durée : 4 heures	Coefficient : 5

UNIVERSITÉ OUEST

Ce sujet comporte 15 pages dont un dossier documentaire de 9 pages.
Il est constitué de deux dossiers, qui peuvent être traités de façon indépendante.
Le candidat ou la candidate est invité.e à vérifier qu'il est en possession d'un sujet complet.

Aucune calculatrice n'est autorisée

Barème

Dossier A	Spécifications des accès réseaux sur le site de Belle-Beille	60 pts
Dossier B	Maintenance des accès réseaux	40 pts
	Total	100 pts

Dossier documentaire

Documents spécifiques au dossier A	*Document 1: extrait du schéma directeur du système d'information de l'université Ouest* *Document 2: infrastructure générale de l'université Ouest* *Document 3: matériel actif utilisé* *Document 4: préparation de la réunion de travail sur la prise en charge sécurisée du BYOD* *Document 5: principes retenus pour le contrôle des accès au réseau informatique*
Documents spécifiques au dossier B	*Document 6 : extrait de la liste des VLAN de l'université Ouest* *Document 7 : configuration DHCP du VLAN Étudiants* *Document 8 : extrait du fichier de zone univ-ouest.fr* *Document 9 : extrait de la configuration du commutateur de niveau 3* *Document 10: attribution des blocs d'adresses IPv6 par RENATER* *Document 11: règles de filtrage du commutateur de niveau 3 pour le VLAN Labo-info* *Document 12 : liste de ports courants* *Document 13 : extrait du fichier de configuration du client VPN* *Document 14 : accès réseau des résidences universitaires*

Présentation du contexte

L'université Ouest possède un centre de ressources informatiques (CRI) destiné à coordonner les projets. Le Schéma Directeur du Système d'information défini par la Direction du Numérique de l'université a permis de dresser les grandes lignes de l'évolution de son système d'information, en se fixant trois objectifs :

- ✓ faire un état des lieux de la situation de tous les éléments liés au système d'information de l'université (ressources humaines, équipements, infrastructures, circuits de décisions, organisation, marchés publics) ;
- ✓ faire apparaître, après consultation des utilisateurs, les besoins non-résolus ;
- ✓ définir les projets à mettre en place pour améliorer le service à l'utilisateur.

Le centre de ressources informatiques (CRI) est le prestataire de services informatiques de tous les acteurs de l'Université : étudiants, personnels et enseignants-chercheurs.
Le CRI intervient autour de 4 axes de service : Réseau et téléphonie, Système et Support, Applications de gestion.
Ses missions prioritaires sont les suivantes :

- le fonctionnement technique et l'évolution du système d'information de l'établissement ;
- le maintien de l'infrastructure réseaux et serveurs ;
- la gestion du parc informatique ;
- l'assistance aux usagers ;
- la conception, le développement et le déploiement de logiciels ;
- l'intégration de nouveaux services dans le système d'information ;
- la veille technologique ;
- la mise à disposition de services dédiés aux étudiants, aux enseignants-chercheurs et aux personnels administratifs et techniques.

L'université ouvre une nouvelle formation à la rentrée 2017, il s'agit d'une licence professionnelle intitulée « objets connectés ». Cette nouvelle formation a conclu des partenariats avec la « cité des Objets connectés » qui a ouvert ses portes dans l'agglomération en mai 2016.

Un nouveau bâtiment situé sur le site de Belle-Beille, destiné à regrouper les formations informatiques de l'université, vient d'être livré. Nommé « pôle informatique », Il hébergera la nouvelle licence « objets connectés », ainsi que la licence « Réseaux & Télécommunications » déjà existante, qui la rejoindra dans le nouveau bâtiment dédié.

Vous êtes accueilli au sein du CRI afin de participer à la mise en place du système informatique de ce nouveau secteur. Il vous est précisé que votre domaine d'intervention concernera les fonctions liées à la gestion et à l'évolution de l'infrastructure système et réseau.

Vos différentes missions consistent à participer dans un premier temps aux choix des solutions techniques et à la rédaction de la réponse à un appel à projet, avec pour objectif la mise en œuvre de l'infrastructure réseau. Dans un second temps, vous participerez au maintien en fonctionnement de l'infrastructure mise en place.

Vous vous appuierez sur les deux dossiers documentaires mis à votre disposition.

Dossier A – Spécifications des accès réseaux sur le site de Belle-Beille

Mission A.1 – Étude des commutateurs d'accès

Les matériels d'interconnexion ont été prévus pour équiper le local technique desservant Belle-Beille. Le responsable du CRI vous demande de rédiger une note démontrant à la direction du numérique que les matériels choisis respectent les préconisations du schéma directeur.

Question A.1.1

Relever au moins trois caractéristiques du commutateur SW-48T-L2 qui favorisent la haute disponibilité, en expliquant brièvement en quoi ces caractéristiques contribuent à éviter des interruptions de services.

Question A.1.2

Justifier dans une note adressée à la direction :

a. Le choix d'un empilement des commutateurs par rapport à une liaison des commutateurs par câble cuivre sur port Ethernet.

b. La présence d'un commutateur de type SW-48TE-L2 dans la pile de commutateurs SW-48T-L2.

Mission A.2 – Politique des accès aux ressources informatiques

Depuis quelques années, de nombreux enseignants ont peu à peu pris l'habitude d'utiliser leurs outils informatiques et téléphoniques personnels (PC, tablettes, smartphones…) pour se connecter au système informatique de l'université. Cette pratique, de plus en plus répandue dans les entreprises, est connue sous le nom de *BYOD* (*Bring Your Own Device*).

Vous participez à la réflexion sur la sécurisation de ces solutions techniques d'accès (STA) diverses et non gérées directement par la Direction du Numérique.

Deux solutions sont particulièrement envisagées :

- mise en place d'une solution de gestion de flotte mobile (*Mobile Device Management* ou *MDM*) qui vise à installer sur la STA personnelle de l'utilisateur les composants logiciels permettant l'accès aux ressources ;
- virtualisation du poste de travail qui vise à permettre un accès distant à un poste de travail virtualisé à partir de la STA personnelle de l'utilisateur.

Votre responsable vous demande de rédiger deux documents pour préparer une réunion de travail sur ce sujet. Le premier document devra traiter les problèmes de sécurité. Le deuxième document présentera les avantages et inconvénients de ces solutions pour les utilisateurs et la direction du numérique.

Il vous a fourni pour cela une compilation de documents traitant du sujet.

Question A.2.1

Rédiger une note répondant aux questions suivantes :

a) quels sont les risques liés à l'utilisation de postes personnels aussi bien pour l'utilisateur que pour l'université ?
b) comment sont-ils pris en charge par une solution *MDM* ?
c) comment sont-ils pris en charge par une solution de virtualisation du poste de travail ?

Question A.2.2
Établir un tableau comparatif des deux solutions envisagées présentant l'impact en matière de configuration et de coût pour la direction du numérique.

Question A.2.3
Présenter votre opinion argumentée sur le choix d'une des deux solutions pour préparer votre participation active à la réunion.

Mission A.3 – Authentification des accès aux ressources informatiques

Les professeurs et les étudiants étant de plus en plus « connectés » (smartphones, tablettes, ordinateurs portables) avec leur propre matériel, il faut faire évoluer la politique d'accès au système d'information de l'université Ouest tout en la contrôlant.

Les accès filaires et *Wi-Fi* seront nécessairement authentifiés et chaque catégorie d'accès bénéficiera d'autorisations différentes. Un suivi des activités de chacun.e sera aussi mis en place.

Votre responsable vous a fourni une note exposant les principes retenus pour le contrôle des accès.

Pour empêcher les connexions filaires non autorisées dans les salles en libre-service, les ports des commutateurs d'accès seront contrôlés par le protocole 802.1X.

Des scripts de configuration pour les commutateurs d'accès ont été définis. Vous êtes chargé.e d'en vérifier les effets avant d'implanter les commutateurs.

Question A.3.1
Expliquer les tests que vous effectuez en connexion filaire pour une salle d'accès libre-service et les résultats attendus.

Les étudiants, utilisant leur matériel, auront un accès internet via le *Wi-Fi* contrôlé par un portail captif. Le responsable vous demande de rédiger une note à leur destination sur la configuration réseau des postes étudiants.

Question A.3.2
Donner les éléments de configuration que les étudiants auront à effectuer sur leur poste pour accéder à internet en passant par le portail captif.

Les accès *Wi-Fi* des personnels enseignants seront contrôlés via le protocole *WPA2-Entreprise* (802.1X-PEAP). Vous devez expliquer aux enseignants la nécessité d'installer le certificat de l'autorité de certification de l'université pour accéder au réseau *Wi-Fi*.

Question A.3.3
Préciser quelles seraient les conséquences si le certificat de l'autorité de certification de l'université n'était pas installé sur le poste des enseignants.

Dossier B – Maintenance des accès réseaux

Mission B.1 – Mise à jour de la configuration *DHCP*

On s'intéresse à la configuration automatique des postes des étudiants : ces postes clients obtiennent la configuration IP nécessaire à l'utilisation d'internet à partir des 2 serveurs *DHCP* (SRV_Dhcp1, SRV_Dhcp2) montés en grappe (*cluster*).

De nouveaux serveurs *DNS* secondaires ont été ajoutés. Pour les prendre en compte, on vous demande de mettre à jour la configuration *DHCP* du *VLAN* étudiant à partir d'un extrait du fichier *DNS*.

Question B.1.1

a) Compléter le fichier de configuration du serveur *DHCP* pour prendre en compte les nouveaux serveurs *DNS*.

b) Détailler les étapes d'obtention de l'adresse IP dans le *VLAN* étudiant en précisant les unités de données de protocole et les matériels et logiciels impliqués.

c) Indiquer la démarche permettant de valider tous les éléments de configuration transmis par le service *DHCP*, en testant pas à pas la bonne configuration d'un client.

Pour permettre des tests sur le *VLAN* Étudiants des adresses ne sont pas distribuées par le serveur *DHCP*.

Question B.1.2

Préciser la plage d'adresses utilisables pour les tests dans le *VLAN* Étudiants. *Justifier le résultat.*

Mission B.2 – Mise à jour IPv6 de la configuration *DNS*

Afin de préparer au mieux la migration vers IPv6, la direction du numérique souhaite rendre compatible dès maintenant l'ensemble de ses services.
Un des premiers services réseaux concernés est le *DNS*.

Question B.2.1

Vérifier la validité des adresses IPv6 utilisées dans le fichier de configuration *DNS* par rapport au bloc fourni par RENATER. Pour cela :

a) Expliquer le lien entre le bloc des adresses RENATER et le bloc des adresses de l'université Ouest.
b) Donner la notation complète (avec les zéros) des adresses IPv6 présentes dans le fichier de configuration du *DNS*.
c) Conclure sur la validité de ces adresses.

Mission B.3 – Dépannage des accès réseaux

Un étudiant utilise un poste fixe de la salle libre-service (*VLAN* Labo-info) et ne parvient pas à accéder à internet alors qu'il dispose d'une passerelle et d'un *DNS* obtenus par *DHCP*. Il a comparé ces éléments de configuration à partir d'un autre poste fixe de la même salle fonctionnant normalement et pouvant accéder à internet.

Question B.3.1
a) Expliquer l'objectif des règles de filtrage actuelles.
b) Expliquer pourquoi l'accès n'est pas possible malgré la bonne configuration IP apparente de son poste.
c) Donner une solution.

Afin de rendre compte d'un stage qu'elle a suivi, une étudiante a besoin d'accéder aux fichiers de l'entreprise dans laquelle elle avait été accueillie. L'entreprise lui a ouvert à cet effet un accès réseau privé virtuel (*VPN*) et son ordinateur portable personnel a été configuré pour en permettre l'usage.
L'étudiante vous contacte et vous explique qu'elle peut accéder normalement aux ressources de l'entreprise à partir du domicile de ses parents avec son ordinateur portable, mais que la connexion au *VPN* avec le même poste lui est refusée à partir de sa chambre universitaire, ce qui la handicape fortement pour la rédaction de son mémoire.

Question B.3.2
Indiquer quelle intervention effectuer pour autoriser l'accès des clients extérieurs au serveur *VPN* à partir de la résidence universitaire.

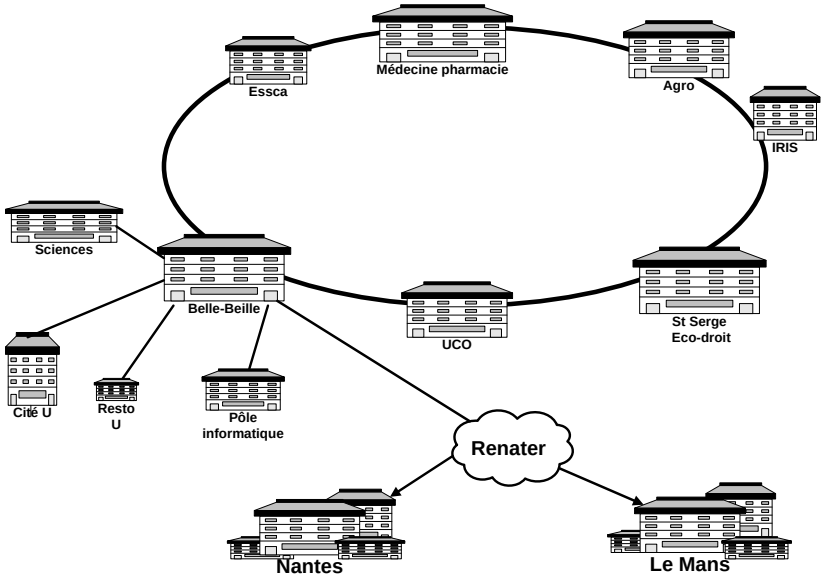
Documents spécifiques au dossier A

DOCUMENT 1 : extrait du schéma directeur du système d'information de l'université Ouest

« **Haute disponibilité de l'infrastructure réseau**
Il est indispensable de garantir la haute disponibilité sur l'ensemble du réseau. Il convient que l'ensemble des commutateurs du réseau intègre l'ensemble des fonctionnalités nécessaires. Notamment, dans certains cas, il faut assurer l'alimentation électrique d'éléments réseau installés dans des zones non-alimentées et il faut également éviter que les équipements d'interconnexion soient générateurs de latence. Enfin, de manière générale, ces améliorations ne doivent pas augmenter la difficulté d'administration de l'ensemble. »

DOCUMENT 2 : infrastructure générale de l'université Ouest

Les instituts de formation supérieure sont structurés autour d'une boucle à 10 Gbits/s fédérant les sept grands sites. Cette boucle est elle-même reliée à deux autres pôles universitaires (Le Mans et Nantes) via le réseau RENATER, réseau national reliant les différentes universités et les différents centres de recherche français entre eux.



Les points centraux du réseau sont situés à Belle-Beille, à St Serge et à l'UFR de médecine. À Belle-Beille, où est implanté le nouveau pôle informatique, la tête de réseau est bâtie autour de deux commutateurs redondants SW-24T-L3 de niveau 3 qui assure la liaison avec les différents pôles du site. Le local technique principal (LTP) du pôle de Belle-Beille est situé dans l'UFR sciences, il dessert le pôle informatique grâce à une artère à 1 Gbit/s. Cette liaison est réalisée avec une fibre optique connectée à un émetteur-récepteur (*transceiver*) SFP+.

Le matériel actif choisi pour équiper le local technique du pôle informatique est composé d'une pile (*stack*) de 6 commutateurs SW-48T-L2 et d'un SW-48TE-L2. La connectivité des équipements terminaux des utilisateurs est assurée grâce à un câblage cuivre de catégorie 6. Le standard 1000Base-T a été retenu pour relier les commutateurs aux équipements terminaux. Des bornes *Wi-Fi* couvrent le bâtiment et permettent à chaque étudiant.e d'utiliser un équipement mobile de son choix. La connectivité *Wi*-Fi est possible pour les étudiants grâce à un portail captif donnant accès à un VLAN dédié.

À compter du 1er septembre 2016, l'accès Internet dans les logements universitaires (Cité U) sera assuré par la société WifUni.

DOCUMENT 3 : matériel actif utilisé

Commutateur
SW-48T-L2

Connectivité	
48 ports RJ-45 de commutation de base Ethernet, Fast Ethernet, Gigabit Ethernet	
4 ports SFP/SFP+	
Empilable (Stackable) par connecteur dédié en face arrière	
Réseau	
Full duplex	Serveur DHCP
Agrégation de lien	Contrôle Broadcast Storm
Auto MDI/MDI-X	Filtrage IGMP
Protocole Spanning Tree (STP)	Client DHCP
Transmission des données	
Capacité de commutation : 160 Gbit/s	
Protocoles	
RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, SSH/SSL	
Caractéristiques	
Remplacement de module à chaud, Layer 2 switching, affectation dynamique des adresses IP, auto-négociation, prise en charge d'ARP, liaisons, prise en charge du réseau local (LAN) virtuel, auto-uplink (MDI/MDI-X auto), *IGMP snooping*, prise en charge de Syslog, régulation de trafic, contrôle de la tempête de Broadcast, Multicast et Unicast Storm Control, STP (*Spanning Tree Protocol*), assistance *Trivial File Transfer Protocol* (TFTP), assistance *Access Control List* (ACL), qualité de service (QoS), support d'images étendues, MLD, *Dynamic ARP Inspection* (DAI), *Link Aggregation Control Protocol* (LACP), alimentation redondante	
Conformité aux normes	
IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1X, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1s, IEEE 802.1ae	

Commutateur SW-48TE-L2

Caractéristiques identiques au SW-48T-L2 avec en plus, option connexion Ethernet supportant l'alimentation via port *PoE* (*Power over Ethernet*) sur les 48 ports.

Commutateur SW-24T-L3

Caractéristiques identiques au SW-48T-L2 24 ports, supporte la commutation de niveau 3.

DOCUMENT 4 : préparation de la réunion de travail sur la prise en charge sécurisée du BYOD

4.1 BYOD : les bonnes pratiques

Source CNIL

L'employeur est responsable de la sécurité des données personnelles (nominatives) de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.

Les risques contre lesquels il est indispensable de se prémunir sont : l'atteinte ponctuelle à la disponibilité, l'intégrité et la confidentialité des données, enfin la compromission générale du système d'information de l'entreprise (intrusion, virus, chevaux de Troie, etc.).

4.2 Virtualisation du poste de travail

On appelle virtualisation du poste de travail le fait d'héberger et de gérer de manière centralisée un environnement de travail dans un *datacenter*. Les utilisateurs accèdent à distance à ce poste de travail virtualisé depuis n'importe quelle solution technique d'accès (ordinateur portable, tablette, mobile…).

Une technologie envisagée à l'université Ouest pour la virtualisation des postes de travail est l'**infrastructure de bureau virtuel (*VDI Virtual Desktop Infrastructure*)**. Chaque utilisateur a accès à son propre poste de travail sous forme d'une machine virtuelle qui dispose des capacités du matériel informatique et des logiciels du serveur informatique utilisé.

Une plateforme de virtualisation nécessite donc sur le matériel de l'utilisateur un bureau distant permettant l'accès au poste virtualisé et sur le serveur de virtualisation des ressources suffisamment importantes pour permettre l'exécution des différentes images des postes virtualisés.

4.3 Gestion de terminaux mobiles

Une solution de type **Gestion de Terminaux Mobiles (*MDM Mobile Device Management*)** permet la gestion d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes, de smartphones, voire d'ordinateurs hybrides au format tablette ou d'ordinateurs portables.

Cette gestion est effectuée au niveau du service informatique de l'organisation (entreprise, association ou collectivité), elle permet aux administrateurs réseaux d'appliquer des contrôles précis, basés sur divers paramètres tels que le type d'appareil, le rôle de l'employé.e et le cas échant, leurs mises à jour et l'installation automatique d'applications sécurisées et obligatoires pour accéder aux ressources informatiques. Si la solution technique d'accès (STA) de l'utilisateur ne peut être configurée par la solution *MDM* il ne pourra pas se connecter aux ressources.

Une telle solution se compose généralement, coté client d'un logiciel installé sur la solution technique d'accès, coté serveur d'un logiciel chargé de contrôler et de configurer la STA.

DOCUMENT 5: principes retenus pour le contrôle des accès au réseau informatique

5.1 Protocole 802.1X (source wikipedia)

802.1X est un standard lié à la sécurité des réseaux informatiques.
Il permet de contrôler l'accès aux équipements d'infrastructure réseau.
En s'appuyant sur le protocole *EAP* (*Extensible Authentication Protocol*) pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que *Radius* par exemple), le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.
Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne *Wi-Fi* est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (*Port Access Entity PAE*).
Indépendamment du type de connexion, chaque port sous contrôle du protocole 802.1X se comporte comme une bascule à deux états :

- un état « connexion non contrôlée » permettant uniquement l'accès au serveur d'authentification.
- un état « connexion contrôlée » en cas de succès d'identification permettant l'accès aux ressources.

La mise en œuvre d'un contrôle d'accès par port 802.1X nécessite l'activation du standard IEEE 802.1X sur :

- les commutateurs réseau ou les points d'accès sans fil (clients d'identification) ;
- chaque point terminal (ordinateur hôte, équipement voix sur IP (*VOIP)*, etc.) ;
- le serveur d'identification chargé de valider l'identité de l'utilisateur du port.

5.2 Extrait du script de configuration du contrôle des accès filaires (cet extrait montre entre autre la configuration du port 10)

```
configure terminal
# configuration de l'authentification et des autorisations gérées par Radius
aaa new-model
aaa authentication dot1x default group RADIUS
aaa authorization network default group RADIUS
# activation de 802.1X
dot1x system-auth-control
# accès radius
RADIUS-server host 192.168.33.100 auth-port 1812 acct-port 1813 key Univ&Ouest
# Configuration des ports avec affectation dynamique du VLAN 130 par Radius si
# l'authentification a réussi
# Configuration du port gigabit 10
interface gi0/10
switchport mode access
authentication port-control auto
dot1x pae authenticator
# Affectation du port au VLAN 99 si le poste ne supporte pas le 802.1X
authentication event no-response action authorize VLAN 99
# Affectation du port au VLAN 99 si l'authentification 802.1X a échoué
authentication event fail action authorize VLAN 99
# Le VLAN 99 est un VLAN d'isolement qui ne donne accès ni aux ressources informatiques
# ni à internet.
```

5.3 Processus d'authentification 802.1X PEAP

PEAP (*Protected EAP*) permet de sécuriser l'échange *EAP* (*Extensible Authentication Protocol*) en créant un tunnel crypté de type *SSL/TLS* (*Secure Sockets Layer* / *Transport Layer Security*).
Le processus d'authentification *PEAP* se décompose en deux phases principales :

1. **Authentification du serveur et création d'un canal de cryptage *TLS***. Le serveur d'authentification s'identifie auprès du client en lui présentant son certificat. Dès que le client a vérifié l'identité du serveur, une clé secrète principale est générée. Les clés de session dérivées de cette clé principale sont ensuite utilisées pour créer un canal de cryptage *TLS* chargé de crypter toute communication ultérieure entre le serveur et le client sans fil.

2. **Conversation *EAP* et authentification de l'utilisateur et de l'ordinateur client**. Une conversation *EAP* complète établie entre le client et le serveur est encapsulée dans le canal de cryptage *TLS*. *PEAP* permet d'utiliser n'importe quelle méthode d'authentification *EAP* (telle que les mots de passe, les cartes à puce et les certificats) pour authentifier l'ordinateur client et l'utilisateur.

5.4 Autorité de certification de l'université

L'université utilise des certificats auto-signés, c'est-à-dire signés par une autorité de certification sous sa responsabilité et non par un organisme de certification reconnu par les éditeurs courants de logiciels.

5.5 Portail captif

Lorsque les étudiants se connecteront au point d'accès via le *SSID* **univOuestBeille**, le portail captif de l'université leur affectera dynamiquement une adresse IP.
Cette adresse IP ne leur fournira aucun accès au réseau de l'université mais leur permettra d'accéder à internet où ils pourront utiliser les différents services *web* mis à leur disposition.
Pour cela le portail captif forcera le client *HTTP* (navigateur) de l'étudiant.e à afficher une page d'authentification avant d'accéder à internet normalement. Cela est obtenu en bloquant tous les paquets liés aux protocoles *HTTP* ou *HTTPS* quelles que soient leurs destinations jusqu'à ce que l'utilisateur s'authentifie. Une fois l'authentification approuvée, l'accès à internet devient possible mais reste sous contrôle d'un serveur mandataire (*Proxy*).

Documents spécifiques au dossier B

DOCUMENT 6 : extrait de la liste des VLAN de l'université Ouest

VLAN	Nom	Adresse réseau	Commentaires
-	Rocade	2001:660:7201:709::72/64	Liaison fibre avec le cœur de réseau
2	Enseignants	192.168.2.0/23	Non commenté
4	Personnel	192.168.4.0/23	Plage 192.168.4.0/29 non distribuée réservée aux postes des administrateurs
12	Serveurs Publics	192.168.12.0/24	192.168.12.1 Messagerie 192.168.12.2 Serveur de fichiers (Accès *SSH* possible sur tous les serveurs)
13	Services réseau	192.168.13.0/24	192.168.13.1 SRV_Proxy 192.168.13.2 SRV_Dhcp1 192.168.13.3 SRV_Dhcp2 192.168.13.4 SRV_Dns (cache DNS du LAN) 192.168.13.5 SRV_SuperV (supervision) 192.168.13.10 SRV_DhcpG (cluster)
16	Résidences universitaires	192.168.16.0/22	Plage d'adresses réservée aux chambres universitaires
20	*VOIP*	192.168.20.0/23	Système de téléphonie IP
24	Wi-Fi	192.168.24.0/22	Non commenté
33	Admin	192.168.33.0/24	administration du matériel actif
64	Étudiants	192.168.64.0/20	Une plage non distribuée est réservée pour les tests
99	Isolement	N/A	Isolement des clients non authentifiés. Aucun accès aux ressources (internes ou externes)
130	Labo-info	192.168.130.0/24	Salle libre-service nouvellement créée dans le pôle informatique

- La passerelle de chaque *VLAN* correspond à la dernière adresse IP de la plage réseau
- Tous les *VLAN* sont routés entre eux, des règles de filtrage appliquées aux interfaces assurent la sécurité.
- L'accès *SSH* est possible sur tous les serveurs

DOCUMENT 7 : configuration DHCP du VLAN Étudiants

```
subnet 192.168.64.0 netmask 255.255.240.0 {
    # Plage d'adresses distribuée aux clients
    range 192.168.64.8 192.168.79.253;
    # Passerelle par défaut du VLAN étudiants
    option routers    192.168.79.254;
    # Serveur DNS. On peut renseigner en DNS primaire le serveur cache local,
    # puis les serveurs DNS publics de l'université par ordre de préférence
    option domain-name-servers   192.168.13.4  193.49.144.1;
    # Nom du domaine
    option domain-name   "univ-ouest.fr";
    # Bail d'une durée de 86400 s, soit 24 h
    default-lease-time  86400;
}
```

DOCUMENT 8 : extrait du fichier de zone univ-ouest.fr

univ-ouest.fr.	IN	SOA	ns.univ-ouest.fr. hostmaster.univ-ouest.fr. 2016050300 7200 21600 3542400 3600	
univ-ouest.fr.	IN	NS	ns.univ-rouen.fr.	
univ-ouest.fr.	IN	NS	ns.univ-rennes1.fr.	
univ-ouest.fr.	IN	NS	ns.univ-ouest.fr.	
univ-ouest.fr.	IN	MX	100 mxd.relay.renater.fr.	
univ-ouest.fr.	IN	MX	100 mxa.relay.renater.fr.	
univ-ouest.fr.	IN	MX	100 mxb.relay.renater.fr.	
univ-ouest.fr.	IN	MX	100 mxc.relay.renater.fr.	
univ-ouest.fr.	IN	MX	20 smtp.univ-ouest.fr.	
ns.univ-ouest.fr.		IN	A	193.49.144.1
ns.univ-ouest.fr.		IN	AAAA	2001:660:7201:709::10
ns.univ-rouen.fr.		IN	A	193.52.152.15
ns.univ-rennes1.fr.		IN	A	129.20.254.1
ametys-fo.univ-ouest.fr.		IN	A	193.49.144.40
frontal1.univ-ouest.fr.		IN	A	193.49.144.31
frontal1.univ-ouest.fr.		IN	AAAA	2001:66:7201:709::30
www.univ-ouest.fr.		IN	CNAME	ametys-fo.univ-ouest.fr.
smtp.univ-ouest.fr.		IN	A	193.49.144.100
smtp.univ-ouest.fr.		IN	AAAA	2001:660:7201:709::20
pop.univ-ouest.fr.		IN	CNAME	frontal1.univ-ouest.fr.

DOCUMENT 9 : extrait de la configuration du commutateur de niveau 3

```
# Configuration du relais : adresses des serveurs DHCP auxquels seront transmises les
# demandes de configuration IP dynamique du vlan
interface  vlan64
ip  address  192.168.79.254  255.255.240.0
ip  helper-address  192.168.13.10
```

DOCUMENT 10 : attribution des blocs d'adresses IPv6 par RENATER

10.1 RENATER et l'université Ouest.

Le réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER) est le réseau informatique français reliant les différentes universités et les différents centres de recherche entre eux en France métropolitaine et dans les départements d'outre-mer.

Il s'agit d'un réseau reliant plus de 1000 sites via une liaison très haut débit (liaisons jusqu'à 10 Gbit/s, cœur de réseau à 80 Gbit/s en Île-de-France) et en IPv4 et IPv6 natifs.
RENATER est connecté au réseau pan-européen GÉANT2 (via deux liaisons à 20 Gbit/s). Il est également relié à internet, en France via SFINX (à 2x10 Gbit/s), et dans le monde via 2 liaisons IP Transit à 20 Gbit/s de Paris et de Marseille.

RENATER dispose du bloc d'adresses IPv6 2001:0660::/32 dont il redistribue des plages à ses différents membres. Conscient de l'importance du déploiement rapide d'IPv6, il encourage ses membres à l'implanter, afin de diminuer le trafic IPv4 sur ses réseaux.

L'université Ouest dispose ainsi du bloc 2001:0660:7201::/48.

10.2 Rappels sur l'adressage IPv6

Une adresse IPv6 est notée en hexadécimal et comporte 16 octets, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points comme dans l'exemple suivant : 2001:0db8:0000:0853:0000:0000:ac1f:8001. Ceci est la notation complète et comporte 39 caractères soit 32 caractères hexadécimaux et 7 séparateurs.
Une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls et les 0 en tête de bloc peuvent être omis.
La même adresse peut donc s'écrire : 2001:db8:0:853::ac1f:8001. Ceci est la notation abrégée.

DOCUMENT 11: règles de filtrage du commutateur de niveau 3 pour le VLAN Labo-info

Note : Si une règle autorise un paquet caractérisé par un quadruplet (ip_src, port_src, ip_dst, port_dst) à passer, la réponse caractérisée par le quadruplet inversé sera autorisée automatiquement.
Extrait concernant l'interface 192.168.130.254 (VLAN 130 Labo-info)

N°	Protocole	IP source	Port source	IP destination	Port destination	action
1	tous	192.168.130.0/24	tous	192.168.13.1	3128	autorise
2	UDP	toutes	tous	toutes	67	autorise
3	tous	192.168.130.0/24	tous	192.168.13.4	53	autorise
4	ICMP	192.168.130.0/24		toutes		autorise
5	tous	toutes	tous	toutes	tous	bloque

DOCUMENT 12 : liste de ports courants

N°	type	description
20	tcp	ftp-data - File Transfer Protocol [flux de données]
21	tcp	ftp - File Transfer Protocol - commandes
22	tcp	SSH - Secure Shell
23	tcp	telnet
25	tcp	smtp - Simple Mail Transfer Protocol RFC 5321
53	udp/tcp	domain - Domain Name Service (DNS)
67	udp	bootps - DHCP, pour la recherche d'un serveur DHCP
69	udp	tftp - Trivial File Transfer
80	tcp	www-http - World Wide Web HTTP
88	tcp	kerberos
110	tcp	pop3 - Post Office Protocol - Version 3 RFC 1939
123	udp	ntp - Network Time Protocol RFC 5905
143	tcp	imap4 - Internet Message Access Protocol - RFC 3501
161	udp	SNMP - Simple Network Management Protocol
443	tcp	https
587	tcp	message submission agent (serveur de messagerie sortant sécurisé)
993	tcp	imap4-ssl IMAP4+SSL
995	tcp	POP3 protocol over TLS SSL
1194	tcp/udp	openvpn
1863	tcp	msn - Windows Live Messenger
3128	udp/tcp	Proxy Server Squid

DOCUMENT 13 : extrait du fichier de configuration du client VPN

```
dev tun
proto udp
comp-lzo
// adresse du serveur VPN, port d'écoute
remote   193.49.144.31   1194
//certificats
ca ca.crt
cert certificat-vpn-client1.crt
key certificat-vpn-client1.key
```

DOCUMENT 14 : accès réseau des résidences universitaires