BTS INFORMATIQUE DE GESTION - ISE4R SESSION 2011

E4R - ÉTUDE DE CAS

Durée : 5 heures **Coefficient : 5**

CAS IMAGE'IN

Ce sujet comporte 15 pages dont 6 pages d'annexes.
Il est constitué de 5 dossiers qui peuvent être traités de façon indépendante.
Le candidat est invité à vérifier qu'il est en possession d'un sujet complet.

Matériels et documents autorisés :

- Lexique SQL sans commentaire ni exemple d'utilisation des instructions.
- Règle à dessiner les symboles informatiques.

Aucune calculatrice n'est autorisée

Liste des annexes

Barème

Dossier 1 : Sécurisation des réseaux	26	points
Dossier 2 : Configuration du réseau local	27	points
Dossier 3 : Affectation des ressources humaines	17	points
Dossier 4 : Supervision des connexions VPN	15	points
Dossier 5 : Coût et intégration d'une offre de service logiciel hébergé	15	points
Total	100	points

Présentation du contexte

La société IMAGE'IN est spécialisée dans la conception, le développement et la mise en réseau des applications nécessaires à la gestion des offres Internet des fournisseurs d'accès. Ses clients sont de grands opérateurs d'accès en Europe comme ORANGE, BOUYGUES Telecom, SFR, VODAFONE ou BELGACOM.

Comme fournisseur d'accès à Internet (FAI), les clients d'IMAGE'IN fournissent à leurs abonnés un boîtier de connexion Internet (*box*) qui est relié à leur réseau, par câble ou par ADSL. Chaque abonné peut choisir, en plus de l'accès Internet, un certain nombre de services (téléphonie fixe, téléphonie mobile, télévision, vidéo à la demande, etc.).

Dans ce cadre, la société IMAGE'IN intervient auprès d'eux à deux niveaux :

- elle conçoit et maintient les logiciels qui permettent le fonctionnement de ces services et qui sont embarqués dans les boîtiers de connexion internet,
- elle conçoit et maintient les logiciels qui assurent le fonctionnement du réseau chez l'opérateur pour permettre la bonne distribution de ces services.

Par exemple, si un abonné disposant de l'offre internet souhaite étendre son abonnement pour acquérir un bouquet de chaînes de télévision, il faudra modifier à distance la configuration de son boîtier ainsi que les éléments du réseau qui le relient au serveur distribuant ces chaînes. Ces modifications de configuration sont réalisées grâce à des logiciels conçus par IMAGE'IN et hébergés chez l'opérateur.

Le réseau interne de la société IMAGE'IN comporte 110 postes de travail et une dizaine de serveurs. Tous les serveurs sont regroupés physiquement dans une salle machine sécurisée et climatisée située dans les locaux du service informatique. Le cœur de réseau est un commutateur de niveau 3. Tous les commutateurs qui y sont connectés sont des commutateurs de niveau 2 possédant au moins deux modules de connexion fibre optique pour assurer la liaison avec le cœur de réseau par double lien agrégé.

Le réseau local de la société IMAGE'IN est découpé en VLAN, à raison d'un VLAN par service. La société dispose également d'une DMZ contenant :

- un serveur hébergeant les services suivants : un service *web* pour héberger le site de la société, un service de messagerie et un service FTP avec accès authentifié. Les clients peuvent déposer les cahiers des charges des applications à réaliser, leurs demandes de modification ou de correction, ainsi que des fichiers pouvant servir de jeu d'essai pour les tests de développement en laboratoire.
- un deuxième serveur « support » permet aux clients de télécharger par FTP les différents correctifs des applications réalisées, déposés après authentification par les salariés de IMAGE'IN.

L'entreprise IMAGE'IN est située à Sophia Antipolis (06), mais ses employés sont souvent en déplacement chez les clients pour des installations ou des configurations de produits. Ils ont un accès permanent au réseau interne de leur société via une liaison VPN (Réseau privé virtuel).

Un schéma complet du réseau de la société vous est proposé en **annexe 1**.

Dossier 1 - Sécurisation des réseaux

Documents à utiliser : annexes 1, 2 et 3

Le cœur de réseau, constitué d'un commutateur de niveau 3, permet d'assurer le routage entre les VLAN, la DMZ et Internet. Il a été paramétré pour répondre à ces objectifs.

TRAVAIL À FAIRE	
1.1	**Donner la route par défaut définie sur le cœur du réseau pour permettre la communication avec la DMZ et Internet.** ***Vous respecterez le formalisme suivant :***

Destination	Masque	Passerelle	Interface

Le responsable du service informatique désire également contrôler et sécuriser l'accès à la DMZ et à Internet. Il doit donc aussi paramétrer le pare-feu PIX. Avant de définir les règles de filtrage, l'administrateur réseau doit définir la table de routage de ce pare-feu PIX. Le routeur du FAI de la société IMAGINE'IN a pour adresse IPV4 : 213.30.180.108.

La répartition des VLAN avec leur adresse réseau IPV4 est donnée en **annexe 2**.

TRAVAIL À FAIRE	
1.2	**Donner la table de routage du pare-feu PIX en écrivant un minimum de routes.** ***Vous respecterez le même formalisme qu'à la question précédente.***

Pour le filtrage, sur le pare-feu PIX, les règles de retour (trafic établi) sont implicites. L'**annexe 3** présente les règles de redirection qui ont été paramétrées sur ce dernier. Par défaut, les seules règles définies sont les suivantes :

Sur l'interface extérieure 213.30.180.97 :

N°	action	Type protocole	IP source / masque	Port origine	IP dest. / masque	Port destination
1	*deny*	*any*	*any*	*any*	*any*	*any*

Sur l'interface interne 172.16.0.1 :

N°	action	Type protocole	IP source / masque	Port origine	IP dest. / masque	Port destination
1	*accept*	*any*	*any*	*any*	*any*	*any*

Sur l'interface de la DMZ 10.50.1.1 :

N°	action	Type protocole	IP source / masque	Port origine	IP dest. / masque	Port destination
1	*deny*	*any*	*any*	*any*	*any*	*any*

L'administrateur souhaite que :

1. seul le serveur de messagerie, sécurisé par un antivirus, puisse faire des requêtes SMTP (port 25) vers l'extérieur ;
2. toute requête SMTP provenant du réseau local ne soit autorisée que vers ce serveur ;
3. les requêtes POP3 (port 110) entrantes venant d'internet ne soient autorisées que vers ce serveur ;
4. seul le serveur Web ait le droit de faire des requêtes vers le serveur de données local situé à l'adresse 192.168.1.9 fonctionnant sur le port 5432 ;
5. depuis l'extérieur, seul le protocole FTP entrant soit autorisé sur le serveur FTP (port 21) qui est réservé aux échanges de fichiers entre la société et ses clients.

TRAVAIL À FAIRE	
1.3	**Pour chaque contrainte, donner l'interface concernée du pare-feu. *Justifier la réponse.***
1.4	**Donner les règles nécessaires pour répondre à ces objectifs.**

Jusqu'à présent le serveur « Support », situé dans la DMZ et fonctionnant avec authentification, possédait son propre fichier de comptes utilisateurs.

L'administrateur réseau souhaite maintenant permettre à tous les salariés de ne s'authentifier qu'une seule fois (authentification unique ; SSO – *Single Sign On*) sur le réseau et d'accéder à toutes les applications avec ce compte.

Il souhaite donc modifier le paramétrage de ce serveur FTP pour lui permettre d'accéder directement à l'annuaire de l'entreprise.

TRAVAIL À FAIRE	
1.5	**Indiquer quel protocole doit installer l'administrateur réseau sur le serveur FTP pour lui permettre d'accéder à l'annuaire de l'entreprise.**

Dossier 2 - Configuration du réseau local

Documents à utiliser : annexes 1, 2 et 4

L'entreprise dispose dans son VLAN Informatique (« Info ») de deux serveurs DHCP en grappe[1]. Tous les postes de travail des différents VLAN ont une adresse dynamique attribuée par les serveurs DHCP.

Un seul serveur de la grappe est actif à un moment donné. Si le serveur principal tombe en panne, automatiquement le serveur de secours prend la relève. Par souci de sécurité et pour éviter les conflits éventuels d'adresses IP lors de la reprise du serveur principal, les plages d'adresses sont distinctes pour ces deux serveurs sur un même réseau.

TRAVAIL À FAIRE	
2.1	**Donner la configuration complète des deux serveurs DHCP pour servir les adresses IPV4 du VLAN 2 « Admin », en précisant les plages d'adresses, la durée du bail, les passerelles à définir ainsi que les services ou options DHCP à activer.**

Après une étude approfondie, l'administrateur réseau s'aperçoit que le masque associé au VLAN 6 ne correspond pas au nombre strictement nécessaire d'adresses.

TRAVAIL À FAIRE	
2.2	**Indiquer le nombre d'adresses IPV4 possibles pour le VLAN 6 avec le masque actuel. *Justifier la réponse.***
2.3	**Proposer un masque plus adapté pour le VLAN 6 en tenant compte du schéma du réseau et expliquer les conséquences sur le plan d'adressage. *Argumenter la réponse.***

Il faut maintenant paramétrer l'interface du VLAN 3 sur le cœur de réseau.

Le troisième octet de l'adresse réseau 192.168.x.0 représente le numéro du VLAN.

L'interface de ce VLAN sur le cœur de réseau est identifiée par la dernière adresse IPV4 disponible selon le masque calculé pour le réseau du VLAN concerné.

Exemple : pour la salle de démonstration (VLAN 4, 10 postes, donc 20 adresses pour les plages des deux serveurs DHCP). Dans la table de routage du cœur de réseau, pour accéder au VLAN 4, il faut utiliser l'interface 192.168.4.30 avec pour passerelle 192.168.4.30.

TRAVAIL À FAIRE	
2.4	**Donner l'adresse IPV4 de l'interface du VLAN 3 « Dvlpt » sur le cœur de réseau. *Justifier la réponse.***

[1] Serveurs en grappe (*cluster* en anglais) : une grappe de serveurs est constituée de plusieurs serveurs capables de prendre le relais d'un serveur défaillant

Devant les demandes des opérateurs téléphoniques d'intégrer IPv6 dans leurs boîtiers Internet, l'administrateur réseau a décidé de se familiariser avec ce nouveau système d'adressage afin de l'intégrer à terme dans les logiciels que IMAGE'IN propose.

Il a donc décidé d'activer le protocole IPv6 sur sa machine (**annexe 4**). En regardant la configuration détaillée des paramètres réseau, il s'aperçoit que son ordinateur s'est vu attribuer l'adresse IPv6 suivante :

fe80::99b3:579:2b73:7c4c

TRAVAIL À FAIRE	
2.5	**Donner la forme étendue complète de cette adresse.**
2.6	**Indiquer la nature de l'adresse obtenue et préciser si elle est routable. *Justifier la réponse en utilisant l'annexe 4.***

Dossier 3 : Affectation des ressources humaines

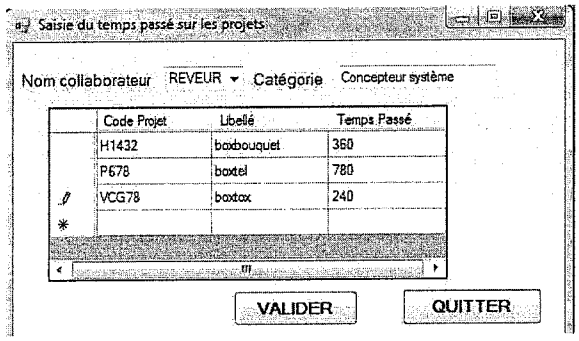
Document à utiliser : annexe 5

Dans la société IMAGE'IN, le service développement a en charge l'élaboration des applications qui seront implémentées dans les boîtiers de connexion à Internet. Ce service emploie des développeurs, des spécialistes système, mais aussi d'autres catégories de personnel.

Chacune des applications en développement fait l'objet d'un projet à budget indépendant. Une facturation entre les services de la société IMAGE'IN tient compte des prestations effectuées par chaque salarié sur chaque projet. Cette comptabilisation s'appuie sur une base de données dont le schéma relationnel vous est fourni en **annexe 5**. Un salarié peut être affecté sur plusieurs projets simultanément.

Chaque fin de semaine, les salariés se connectent à la base de données et remplissent un formulaire dans lequel ils indiquent le temps qu'ils ont passé sur chacun des projets pendant la semaine écoulée. Chaque salarié dispose d'un compte de connexion à la base.

Exemple :



TRAVAIL À FAIRE	
3.1	**Indiquer si la base de données permet d'enregistrer le fait qu'un salarié peut être responsable de plusieurs projets. *Justifier la réponse.***
3.2	**Rédiger en SQL les requêtes permettant d'obtenir les résultats suivants :** **A. Liste (nom et prénom) des employés de la catégorie dont le libellé est « Concepteur système ».** **B. Liste (matricule, nom, prénom et temps total passé sur le projet) des salariés intervenant sur le projet de code « H1432 ».**

Monsieur MARTINEZ, responsable du projet de code « H1432 », dont l'identifiant de connexion à la base est MARTINEZ, demande le droit de consulter les enregistrements de la table AFFECTATION qui concernent ce projet.

3.3	**A. Créer une vue, nommée AFFECTATIONH1432, qui regroupe les enregistrements du projet de code « H1432 » de la table AFFECTATION.** **B. Donner à Monsieur MARTINEZ le droit de consulter les enregistrements de la vue précédente.**

Dossier 4 - Supervision des connexions VPN

Document à utiliser : annexe 6

Le concentrateur VPN reçoit les demandes de connexion des utilisateurs distants. Seuls les utilisateurs authentifiés peuvent initier une connexion.

Depuis quelques temps, les utilisateurs se plaignent de difficultés de connexion et de délais de réponse trop longs. L'administrateur a décidé d'inspecter les fichiers de journalisation du concentrateur VPN pour comprendre la cause de ces dysfonctionnements.

Ces fichiers journaux étant nombreux et difficilement exploitables, l'administrateur a fait réaliser un petit utilitaire qui, à partir de ces fichiers, remplit un tableau correspondant à l'activité d'un mois donné. Seules les informations utiles ont été conservées dans ce tableau.

Ce tableau (nommé tabLog), conçu pour contenir 1000 lignes au maximum, a autant de lignes remplies que de connexions enregistrées pendant le mois étudié. Il est trié chronologiquement. Sa structure est donnée ci-dessous :

```
EnrConnexion : structure
        jour : date
        heure : date
        utilisateur : chaine
        iPSource : chaine
        statut : chaine          // pourra contenir les valeurs failed ou success
        durée : entier           // en minutes
        canal : entier           // contient une valeur de 0 à 127
Fin-structure

tabLog : tableau [1..1000] de EnrConnexion
```

Le nombre de lignes effectivement remplies dans le tableau est donné par la variable nbConnexions. *On considère que le tableau tabLog et la variable nbConnexions sont des variables globales déclarées et déjà renseignées.*

L'**annexe 6** présente le principe de fonctionnement du concentrateur VPN et le mode de calcul du nombre de canaux utilisés simultanément sur une journée.

TRAVAIL À FAIRE	
4.1	**Écrire une procédure Pourcentage() qui affiche le pourcentage de connexions ayant échoué durant le mois étudié.**
4.2	**Écrire la fonction *Charge*(unJour : date), de type entier, qui retourne le nombre maximum de connexions simultanées qui ont eu lieu pendant la journée dont la date est passée en paramètre.**

Dossier 5 - Coût et intégration d'une offre de service logiciel hébergé

Document à utiliser : annexe 7

La gestion des notes de frais de déplacement des employés d'IMAGE'IN relève actuellement d'un traitement lourd, sur une application réalisée à l'aide d'un tableur.

La transmission des données entre domaines de gestion multiplie les saisies. Les notes sont, en effet, saisies par les employés sur des feuilles de calcul, puis globalement reprises lors de l'établissement des fiches de paye et enfin intégrées dans le logiciel de gestion comptable.

Les éléments de contrôle de gestion permettent de déterminer que le traitement d'une note de frais coûte 50 € (coût complet).

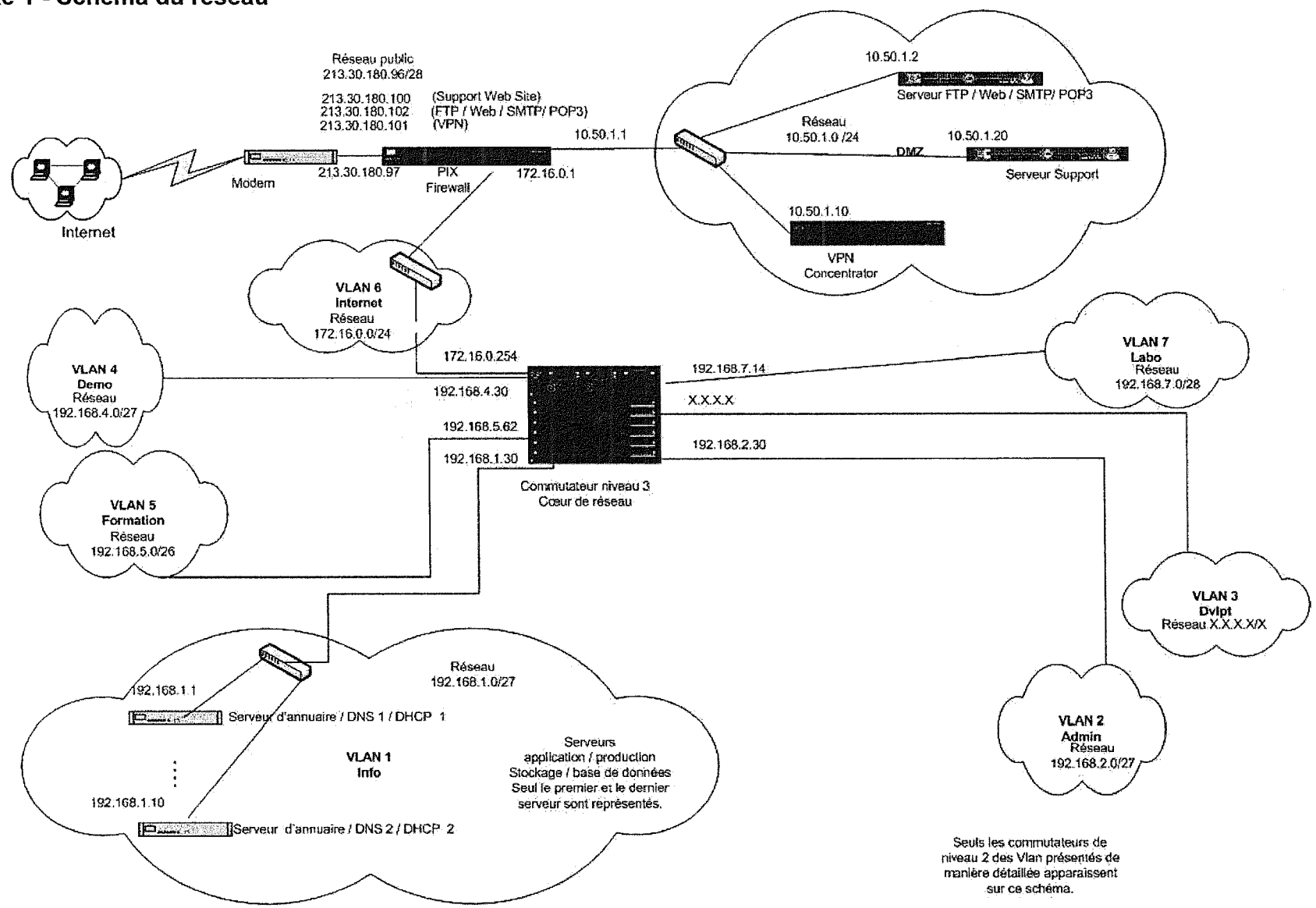
Une solution d'application de gestion des notes de frais en mode hébergé est envisagée. L'offre permet, outre la gestion des notes de frais, une intégration des données comptables dans l'application locale de gestion comptable par des transferts de fichiers.

	TRAVAIL À FAIRE
5.1	**Citer trois avantages pour la société IMAGE'IN de choisir une application en mode hébergé pour la gestion des notes de frais.**
5.2	**Calculer le coût de l'offre pour le volume observé en mai et juin et indiquer le gain réalisé en utilisant l'offre de traitement en mode Saas.**

Lors de la dernière réunion du groupe de pilotage des systèmes d'information, un participant a indiqué qu'il serait pertinent d'accroître le nombre de déplacements pour basculer vers la tarification à 30 €/note.

	TRAVAIL À FAIRE
5.3	**Indiquer quelle réponse apporter à cette affirmation si l'on tient compte du budget total prévisionnel des déplacements dans le service.**

Annexe 1 - Schéma du réseau



Annexe 2 - Répartition des VLAN

Chaque réseau virtuel (VLAN), sauf le VLAN 6, est associé à un service de l'entreprise et dispose d'une adresse de classe C privée. Le troisième octet de leur adresse représente le numéro du VLAN. Le masque associé à chacun de ces réseaux tient compte de l'existence de deux plages d'adresses IPV4 distribuées par les serveurs DHCP.

Service	Nombre d'hôtes	VLAN	Adresse réseau IPV4 du VLAN	Adresse IPV4 de la passerelle
Service informatique (Info)	10 serveurs	VLAN 1	192.168.1.0 /27	192.168.1.30
Service administratif (Admin)	12 postes	VLAN 2	192.168.2.0 /27	192.168.2.30
Service développement (Dvlpt)	58 postes	VLAN 3	X.X.X.X /X	X.X.X.X
Salle de démonstration (Demo)	10 postes	VLAN 4	192.168.4.0 /27	192.168.4.30
Salle de formation (Formation)	20 postes	VLAN 5	192.168.5.0 /26	192.168.5.62
Accès Internet et DMZ (Internet)		VLAN 6	172.16.0.0 /24	172.16.0.254
Laboratoire de test (Labo)	14 postes	VLAN 7	192.168.7.0 /28	192.168.7.14

Le VLAN 1 héberge tous les serveurs internes de la société (DNS, annuaire, base de données, application, production, stockage, DHCP, etc.) Les serveurs, au nombre de 10, disposent d'une adresse fixe. Ces adresses correspondent aux dix premières valeurs de la plage.

Annexe 3 - Fonctionnement du pare-feu

Le pare-feu qui permet l'accès à Internet et à la DMZ possède trois interfaces :

- Une interface connectée sur le VLAN 6 : 172.16.0.1/24,
- Une interface vers la DMZ : 10.50.1.1/24,
- Une interface vers Internet : 213.30.180.97/28.

La DMZ étant située sur un réseau local privé, le pare-feu doit obligatoirement faire de la translation d'adresse IP de type NAT-PAT. Sur ce pare-feu, les règles s'appliquent en entrée de l'interface et substituent l'adresse IP destination et le port destination public par une adresse privée et un port privé, de façon à transmettre la requête venant de l'extérieur au serveur destinataire de la DMZ.

Les règles de filtrage s'appliquent donc **après** la translation d'adresses.

N°	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
1	213.30.180.97	NP	TCP	213.30.180.102	21/80/25/110	10.50.1.2	21/80/25/110
3	213.30.180.97	NP	TCP	213.30.180.100	80/support	10.50.1.20	80/support
2	213.30.180.97	NP	TCP	213.30.180.101	VPN	10.50.1.10	VPN

Annexe 4 - Adressage IPv6

Le développement rapide d'Internet a conduit à la pénurie du nombre d'adresses IPv4 disponibles. Le protocole IPv6 a été principalement développé en réponse à la demande d'adresses Internet que le protocole IPv4 ne permet plus de satisfaire.

L'**adresse IPv6** est une adresse IP dans la version 6 du protocole IP (IPv6). Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits (4 octets) pour le protocole IPv4.

Notation d'une adresse IPv6

La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale dans laquelle 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points. Voici un exemple d'adresse IPv6 :

2001:0db8:0000:0000:0000:85a3:ac1f:8001

Il est permis d'omettre les zéros non significatifs situés à gauche de chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus peut être raccourcie en retirant les zéros situés à gauche dans les groupes :

2001:db8:0:0:0:85a3:ac1f:8001

De plus, une suite de un ou plusieurs groupes consécutifs valant zéro peut être omise (ceci une seule fois). Ainsi, l'adresse IPv6 ci-dessus peut être encore raccourcie en retirant la suite « 0:0:0 » pour obtenir :

2001:db8::85a3:ac1f:8001

Catégories d'adresses et préfixes associés

- **adresses globales point à point (unicast) ;** parmi ces adresses, on distingue :
  - les adresses globales point à point (préfixe 2001::/16) qui permettent de communiquer sur internet,
  - les adresses 6to4 (préfixe 2002::/16) qui permettent d'acheminer le trafic IPv6 via un ou plusieurs réseaux IPv4,

- **adresses locales uniques** (préfixe fc00::/7) ; elles sont utilisées pour les communications locales et ne sont routables que sur les sites qui le souhaitent. C'est l'équivalent des plages d'adresses privées de IPv4,

- **adresses de lien local** *(link-local,* préfixe fe80::/10) ; elles sont utilisables uniquement au sein d'un réseau local, elles ne sont pas routables,

- **adresses de multidiffusion** *(multicast,* préfixe ff00::/8) : IPv6 n'utilise pas d'adresse de diffusion (*broadcast*) ; elles sont remplacées par des adresses multi-adressées.

(Sources : texte adapté de Wikipédia, RFC 2373 , section 2.2, IPv6 Global Unicast Address Assignments)

Annexe 5 - Schéma relationnel de la base de suivi des affectations sur les projets de développement

PROJET (code, intitule, dateDebut, montant, responsable)
code : clé primaire
responsable : clé étrangère en référence à matricule de SALARIE

Remarque :
- *« responsable » désigne le matricule du salarié responsable du projet*

SALARIE (matricule, nom, prenom, categorie)
matricule : clé primaire
categorie : clé étrangère en référence à numero de CATEGORIE

CATEGORIE (numero, libelle)
numero : clé primaire

AFFECTATION (salarie, projet, semaine, tempsPasse)
salarie, projet, semaine : clé primaire
salarie : clé étrangère en référence à matricule de SALARIE
projet : clé étrangère en référence à code de PROJET

Remarque :
- *« tempsPasse » est exprimé en minutes*
- *« semaine » est un nombre entier indiquant le numéro de la semaine dans l'année ; par exemple, la semaine du 2 au 8 Mai 2011 est la 18° semaine de l'année 2011.*

Annexe 6 - Fonctionnement du concentrateur VPN

Le concentrateur VPN peut gérer jusqu'à 128 connexions simultanées et dispose donc de 128 canaux numérotés de 127 à 0.

À chaque connexion, le concentrateur attribue le premier canal libre.

Si aucune connexion n'est établie, la première demande se verra attribuer le canal 127.

Si la connexion 127 est toujours active, la demande suivante utilisera le canal 126 etc. Quand une connexion se termine, le canal est libéré. Il redevient disponible pour la connexion suivante.

Il arrive que certaines connexions échouent, elles apparaissent dans les fichiers de journalisation avec le statut *failed*.

Exemple de fonctionnement

jour	heure	utilisateur	IPSource	statut	durée	canal
....	....	....	....	....	....	....
5/04/2011	8:06	FIGAROL	88.167.96.83	*failed*		
5/04/2011	8:09	FIGAROL	88.167.96.83	*success*	**225**	**127**
6/04/2011	10:12	ERHART	121.17.23.48	*success*	**15**	**127**
6/04/2011	10:16	GASSER	206.11.45.121	*success*	**40**	**126**
6/04/2011	10:16	GODARD	90.105.91.20	*failed*		
6/04/2011	10:21	HALL	206.11.45.121	*success*	**11**	**125**
6/04/2011	10:30	GODARD	90.105.91.20	*success*	**18**	**127**
11/04/2011	10:12	FIGAROL	88.167.96.83	*success*	**33**	**127**
....	....	....	....	....	....	....

Le 6 Avril, ERHART se connecte à 10h12 et reste connecté jusqu'à 10h27 (15 minutes) ; le canal 127 lui est affecté.

GASSER se connecte à 10h16 ; le canal 127 étant occupé, le canal 126 lui est affecté jusqu'à sa libération à 10h56 (40 minutes).

La connexion suivante (pour GODARD) n'aboutit pas ; elle n'utilise donc pas de canal.

HALL se connecte ensuite à 10h21 ; les canaux 127 et 126 étant occupés, le canal 125 est affecté jusqu'à sa libération à 10h32 (11 minutes).

GODARD se connecte ensuite à 10h30 ; les canaux 126 et 125 sont toujours occupés mais le canal 127 est libre, c'est ce canal qui est affecté jusqu'à 10h48 (18 minutes).

Pour déterminer le nombre de canaux utilisés simultanément sur une journée, il faut donc :

- *sur cette journée, déterminer le plus petit numéro de canal affecté à une connexion,*
- *soustraire ce numéro au nombre de canaux du concentrateur.*

Ici, le plus petit canal attribué le 6 avril 2011 est le canal 125, le concentrateur VPN a donc eu besoin de 3 connexions simultanées(128-125).

Annexe 7 – Éléments du dossier de gestion de l'offre SaaS

Extrait du contrat de l'offre Saas (*software as a service*):

« *ARTICLE 10. FORMATION*

La formation des utilisateurs est prise en charge par le prestataire à raison d'une heure par personne. La formation à l'administration est prise en charge à raison de 3h par administrateur. (1 formation par an).

ARTICLE 13. CONDITIONS FINANCIÈRES

Le prix du service SaaS dépend du volume de notes de frais traitées. Un volume minimum d'utilisation du service de 150 notes de frais par mois est facturé.

13.1. REDEVANCES

Les conditions financières sont exposées ci-dessous :
Tarification mensuelle adaptable :

Volume total inférieur à 150 notes	*Volume total compris entre 151 et 200 notes*	*Volume total supérieur à 200 notes*
Forfait 7500€	*40 € / note*	*30 € / note*
Charges fixes liées à l'infrastructure		
200 €	*200 €*	*800 €*

Les redevances des Services sont indiquées en euros et s'entendent hors taxe et hors frais.
L'adresse de facturation est l'adresse du siège social du Client.
Il est expressément convenu que le montant des sommes facturées par le Prestataire sera révisé chaque année en fonction de l'indice du Coût Horaire du travail de tous les salariés des entreprises de la Fédération Syntec.

Sont exclues de la redevance et donnent lieu à facturation séparée les prestations suivantes :
- les prestations de formation non prévues dans l'article 10,
- les prestations d'assistance technique,
- et plus généralement toutes prestations n'entrant pas dans l'offre SaaS. »

Éléments de gestion prévisionnels

	Janvier	Février	Mars	Avril[2]	Mai	Juin
Nombre de notes de frais	152	123	158	250	200	300
Coût moyen d'un déplacement	200	200	200	350	250	400

Article de presse - Les écueils : attention aux problématiques d'intégration

« Pour l'ensemble des sociétés que nous avons interrogées, le risque de perte de connexion internet est un faux problème. Du moins au niveau de la ligne ADSL, dont on peut installer une ligne redondante à faible coût. " En six ans, le service du site de Meilleuregestion.com a été interrompu moins d'une heure au total ", témoigne MG chez Z. Et, " même sans parler de la connexion, nous ne pourrions pas assurer un taux de disponibilité aussi élevé de notre PGI, même installé en interne ", relativise SC. La partie la plus technique de la mise en œuvre reste l'intégration de l'application hébergée avec le reste du système d'information. " Parmi les entreprises qui utilisent un logiciel hébergé, 76 % sont confrontées à des difficultés d'intégration ", estime Markess International. Dans le cas de logiciels traditionnels, l'intégration s'effectue par un échange régulier de fichiers entre les progiciels. C'est la méthode – fastidieuse mais efficace – retenue par Z (entre la paie de meilleuregestion.com et sa comptabilité) et AX (entre son site internet et les logiciels de caisse des boutiques). » (Source : JournalSurLeNet.fr)

[2] L'augmentation du nombre de missions induit des déplacements de plus en plus coûteux (éloignement, nombre de nuits d'hôtel, usure des véhicules).