CAS XONI

Ce sujet comporte 12 pages dont 6 pages de documentation
Il est constitué de 3 parties qui peuvent être traités de façon indépendante.
Le candidat est invité à vérifier qu'il est en possession d'un sujet complet..

Aucune calculatrice n'est autorisée

Documentation fournie pour chaque partie :

Partie 1 :

- *Schéma du réseau de la société XONI*
- *Description de l'infrastructure réseau de XONI*
- *Configuration du service DNS*
- *Documentation technique de la plate-forme collaborative*
- *Configuration des routeurs ADSL*
- *Liste de numéros de ports standards*
- *Proposition de solution pour l'ouverture de la plate-forme collaborative*

Partie 2 :

- *Liste des VLAN du site de Dijon*
- *Réseau de Dijon après le remplacement du routeur R4*
- *Configuration partielle du commutateur SW1*

Partie 3 :

- *Offres de solutions de sauvegarde en ligne*

Barème

Partie 1 - Mise en place d'une plate-forme de travail collaboratif.		40 points
Partie 2 - Modification de l'infrastructure du site de Dijon		40 points
Partie 3 - La gestion des sauvegardes		20 points
	Total	100 points

Le contexte :

La société XONI est le leader dans la fabrication et la distribution de tubes en acier inoxydable sans soudure destinés à une industrie à forte contrainte de sécurité.
Elle utilise deux principes de fabrication :

- le filage,
- l'étirage.

La production est réalisée sur deux sites, l'un situé à Dijon et l'autre à Rouen. Le siège social situé à Paris gère toutes les transactions commerciales de la société.

Le site de Dijon

L'usine conçoit des tubes de diamètre compris entre 25 et 50 mm. De l'acier fondu dans des fourneaux à 1 000°C passe dans des filières de diamètre variable. À sa sortie, le tube est plongé dans un bain d'acide afin d'évacuer toute aspérité.

Le site de Rouen

L'usine est spécialisée dans la conception des tubes fins ayant un diamètre inférieur à 25 mm. Pour les réaliser, la technique de l'étirage est utilisée. Elle nécessite des tubes plus épais produits par le site de Dijon. Ces tubes sont tirés à froid et passent dans des goulottes de plus en plus étroites jusqu'à l'obtention du diamètre désiré.

Le contrôle qualité

Chaque tube doit être contrôlé minutieusement. Toute imperfection pourrait avoir des conséquences désastreuses. Ces vérifications sont effectuées par des scanners. Un tube ne correspondant pas aux critères de sélection est mis au rebut.

Le service commercial

Le service commercial est composé majoritairement d'ingénieurs spécialisés dans les transactions commerciales. Ces ingénieurs négocient aussi bien avec des compagnies françaises qu'étrangères.

Ils doivent à tout moment et en tout lieu pouvoir accéder aux informations commerciales des produits. Ces données étant sensibles, chaque ingénieur doit disposer d'une liaison sécurisée.

Le service informatique

Ce service est basé au siège social. Il est composé de cinq techniciens dont vous faites partie et d'un chef de service. Il est chargé de l'administration et de l'entretien technique de tout le réseau de l'entreprise. Les techniciens sont souvent amené à se déplacer sur les sites de Dijon ou de Rouen.

Partie 1 : Mise en place d'une plate-forme de travail collaboratif.

Une plate-forme de travail collaboratif vient d'être achetée. Cette plate-forme intègre un ensemble d'outils accessibles par une interface web et facilitant la communication et le travail en équipe. Une documentation technique est fournie avec la plate-forme.

L'objectif est de rendre cette plate-forme accessible à l'ensemble des employés de l'entreprise tout en assurant la confidentialité des données de l'entreprise circulant sur internet et la sécurité du réseau et des serveurs de l'entreprise.

Un projet a été mis en place pour répondre à cet objectif, projet qui va vous amener à assurer différentes mission au cours de sa réalisation, en vous appuyant sur la documentation mise à disposition de l'équipe.

Mission 1 : Analyse de la demande

1.1 Expliquer à l'aide d'un schéma légendé, le fonctionnement et le rôle des différents éléments de la plate-forme collaborative.

1.2 Inventorier en les expliquant les risques liés à l'ouverture de la plate-forme collaborative aux sites distants.

Mission 2 : Étude des solutions

Une solution a été proposée par l'équipe du projet. Cette solution, décrite dans la documentation, envisage deux possibilités pour l'accès des sites distants de Dijon et Rouen au portail collaboratif : une inter-connexion des sites par VPN, ou par ADSL/SDSL Vous êtes chargé de présenter cette solution au chef de service.

1.3 Justifier le choix d'une résolution de nom en interne pour le domaine intranet.xoni.com.

1.4 Pourquoi est-il nécessaire de mettre en place la réplication entre les annuaires des sites distants et celui du siège ?

1.5 Rédiger un dossier de choix permettant d'expliquer au chef de service par quel moyen chacune des deux solutions de connexion inter-site assure la confidentialité des données de l'entreprise et la sécurité des serveurs et présentant les avantages et inconvénients de chacune.

Mission 3 : Mise en production d'un service.

La proposition A (connexion ADSL/SDSL) a été choisie par le chef de service, essentiellement pour des raisons budgétaires. Vous êtes chargé de mettre en œuvre l'intégralité de la solution.

1.6 Proposer une configuration pour le routeur du siège social.

1.7 Lister les modifications à effectuer sur les serveurs DNS pour rendre la solution opérationnelle

Mission 4 : Assurer la continuité du service

1.8 Proposer une solution pour superviser et assurer la continuité du service de travail collaboratif. Vous détaillerez l'ensemble des éléments matériels et logiciels à mettre en place.

Partie 2 : Modification de l'infrastructure du site de Dijon

Le site de Dijon est composé de deux réseaux : un réseau administratif (172.16.32.0/20) et un réseau dédié à la production (192.168.32.0/24) pour son usine qui est composée de trois ateliers.
Le responsable informatique local souhaite réorganiser cette infrastructure pour des raisons de sécurité et de débit. Vous êtes chargé de le conseiller et de l'assister dans la mise en œuvre de ce projet.

Mission 1 : Proposer une solution d'infrastructure

Vous proposez dans un premier temps d'affecter un sous-réseau IP différent à chaque atelier. On dispose d'environ 50 postes par atelier. Vous êtes chargé de définir le nouveau plan d'adressage

2.1 Donner l'adresse de chaque sous-réseau et le masque correspondant. Justifier la réponse.

Le responsable informatique de Dijon réalise des tests de ce nouveau plan d'adressage dans chaque atelier. Pour chaque test, il conserve l'adresse IP du poste et ne change que le masque.

La plupart des machines testées n'ont plus accès aux ressources réseau telles que le service d'annuaire ou internet. Par exemple la machine d'adresse 192.168.32.110 ne peut plus accéder à Internet bien qu'elle possède comme adresse de passerelle : 192.168.32.1.

2.2 Expliquer la cause de ces dysfonctionnements.

Finalement, le responsable informatique décide de décomposer le réseau dédié à la production en cinq sous réseaux, en dotant les ateliers 1 et 3 de deux sous réseaux chacun. Il vous demande conseil pour l'implémentation de cette nouvelle infrastructure. Vous envisagez pour cela de remplacer le routeur R4 par un commutateur de niveau 3 (SW1) relié à trois nouveaux commutateurs de niveau 2 (SW2, SW3, SW4). Chaque sous-réseau se verra attribuer un VLAN différent. Vous définissez la liste des VLAN et le nouveau plan détaillé du réseau de production du site de Dijon (voir documentation de la partie 2). Lors d'un entretien, vous devez présenter et justifier votre solution au responsable.

2.3 Justifier le choix d'un commutateur de niveau 3.

2.4 Énumérer la liste des VLAN à définir sur chaque commutateur SW1, SW2, SW3 et SW4. La liste sera limitée au strict nécessaire.

Le responsable informatique a commencé à configurer le switch SW1 mais a été interrompu. Vous devez terminer le travail. La configuration partielle du switch est fournie dans la documentation

2.5 Donner la configuration des ports 2 à 4 du commutateur SW1.

2.6 Donner le nombre d'adresses IP disponibles pour les machines de production de l'atelier 1 (VLAN2) et pour les machines de l'atelier 2 du site de Dijon (VLAN4).

2.7 Donner la configuration des étendues du serveur DHCP de Dijon permettant d'attribuer des adresses aux machines des VLAN 2, 3 et 4 (étendues, masques, passerelles).

Mission 2 : Résoudre un problème

Le serveur DHCP doit distribuer des adresses à tous les réseaux du site de production. Suite à la mise en place du commutateur SW1 et des VLAN, les machines clientes du réseau 172.16.32.0 se voient attribuer des adresses IP, alors que les machines des ateliers ne reçoivent rien. Pourtant toutes les étendues nécessaires ont été définies sur le serveur DHCP.

2.8 Expliquer les raisons de ce dysfonctionnement.

Pour pallier à ce problème, vous proposez de tester une solution basée sur la compatibilité de la carte réseau du serveur DHCP avec les VLAN et le protocole 802.1Q.

Il faut pour cela définir sur le serveur une interface virtuelle pour chaque VLAN. Vous décidez d'utiliser la première adresse disponible sur chaque sous-réseau.

2.9 Décrire cette solution et définir les paramètres IP de la carte réseau du serveur DHCP.

Mission 3 : Améliorer la sécurité

Le responsable informatique vous demande d'étudier la documentation des commutateurs pour les configurer afin qu'ils interdisent que les employés se connectent sur le réseau de l'entreprise avec des ordinateurs personnels.

Les différentes procédures de contrôle d'accès des postes envisagées sont les suivantes :

a) règles de filtrage de niveau deux à partir des adresses MAC, à mettre en place sur les ports d'interconnexion des commutateurs, ou sur les ports d'accès aux serveurs ;
b) règles de filtrage de niveau trois sur le commutateur-routeur SW1, à partir des adresses IP ;
c) contrôle d'accès basé sur les adresses MAC autorisées à se connecter sur chaque port, fixées manuellement par l'administrateur ;
d) contrôle d'accès basé sur les adresses MAC autorisées à se connecter sur chaque port, apprises automatiquement à partir de la première trame qui traverse le port ;
e) limitation du nombre d'hôtes (adresses MAC) qui peuvent accéder sur chaque port ;
f) mise en place de VLAN privés qui interdisent la communication entre deux ports du même VLAN ;

2.10 Évaluer la pertinence de chaque solution et proposer celle qui est la plus appropriée en justifiant ce choix.

Partie 3 : La gestion des sauvegardes

La société XONI est soumise à une exigence de traçabilité et de sécurisation des données au regard du caractère particulier des usages des produits fabriqués.

Elle envisage de remplacer sa solution actuelle de sauvegarde par une solution en mode hébergé de type « As a Service ».

Pour l'entreprise, externaliser la sauvegarde permet de mieux estimer les coûts, à défaut de les faire baisser. Pour le personnel la charge de travail s'en trouve allégée.

Les données de la base, objet de la sauvegarde pour les deux sites, ont été estimées à 30 Go avec un accroissement en volume annuel de l’ordre de 5%.

Les offres de deux prestataires, BeNeo et Tecarch, ont été examinées et détaillées dans la documentation de la partie 3.

Mission 1 : Choix d'une solution

3.1 Déterminer le volume à sauvegarder à partir duquel l’offre BeNeo sera, d’un point de vue tarifaire, plus intéressante.

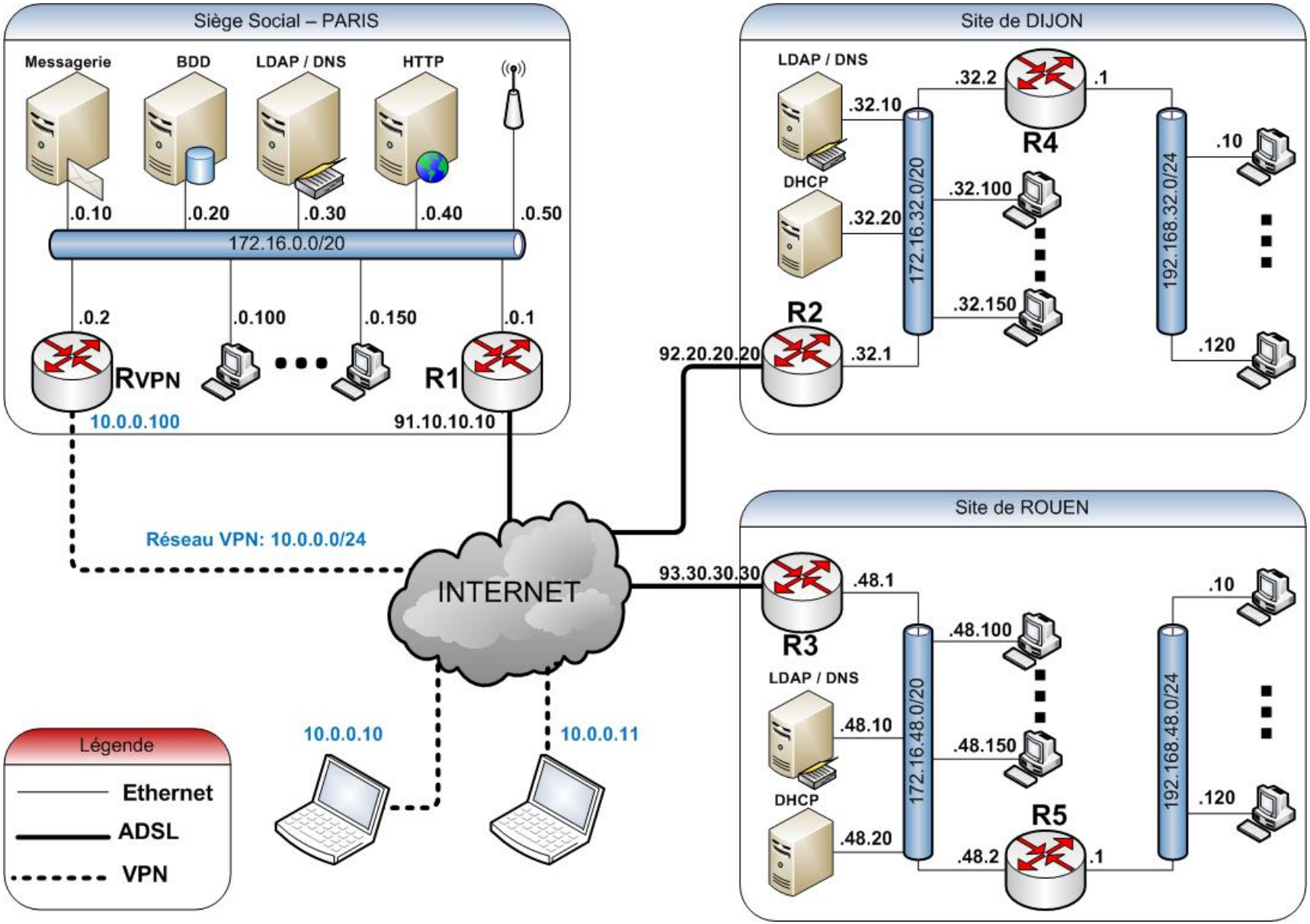
Le coût est un élément important mais pas l’unique déterminant pour arrêter le choix du prestataire.

3.2 Expliquer les réponses des deux prestataires sur le critère « Type de sauvegarde autorisée » et leur incidence sur une restauration complète en fin de période de sauvegarde.

3.3 Proposer un examen critique de chacun des critères chez les deux prestataires et préconiser le choix d’une solution.

Documentation de la partie 1

Schéma du réseau de la société XONI



page 7/12

Description de l'infrastructure réseau de XONI

Chaque site est actuellement géré par des serveurs autonomes : serveur DHCP, serveur DNS, Annuaire LDAP pour l'authentification des utilisateurs du site.

Chaque site possède son propre accès à Internet par ADSL. Les routeurs d'accès à internet sont loués au FAI. Ces routeurs sont configurables.

Un VPN SSL permet l'accès des employés nomades au réseau du siège social.

Le site web de l'entreprise est hébergé en externe chez un prestataire et accessible par l'url http://www.xoni.com. L'accès est ouvert au public. C'est une vitrine commerciale.

La zone xoni.com est gérée par un registrar externe (OVH).

Configuration du service DNS

Configuration de la zone DNS xoni.fr sur le registrar OVH (hébergeur web et DNS) :

```
$TTL 86400
xoni.com.       IN SOA dns103.ovh.net. tech.ovh.net. (2012120101 86400 3600 3600000 300)

                IN NS       ns103.ovh.net.
                IN NS       dns103.ovh.net.
                IN MX 1     mail.xoni.com.
mail            IN A        91.10.10.10
www             IN CNAME    web.ovh.net
```

Les serveurs DNS internes du réseau de XONI sont des serveurs DNS cache uniquement.

Configuration des routeurs ADSL

Les routeurs ADSL/SDSL intègrent une fonction de masquage IP activée automatiquement. La politique de filtrage par défaut est l'acceptation du paquet.

Configuration du routeur R1
Règles de redirection :

Interface d'arrivée	Adresse publique	Port public	Adresse privée	Port privé
91.10.10.10	91.10.10.10	53	172.16.0.30	53
91.10.10.10	91.10.10.10	25	172.16.0.10	25

Règles de filtrage en entrée de l'interface externe 91.10.10.10 :

No règle	Adresse Source	Port source	Adresse dest.	Port dest.	Protocole	Connexion TCP	Action
1	*	*	172.16.0.10/32	25	TCP	*	Accepte
2	*	*	172.16.0.30/32	53	*	*	Accepte
3	*	*	*	*	*	Etablie	Accepte
4	*	*	*	*	*	*	Refuse

Les routeurs R2 et R3 n'ont aucune règles de redirection ni de filtrage actives.

Liste de numéros de ports standards :

Protocole/application	Port utilisé	Protocole
SMTP	25	TCP
HTTP	80	TCP
HTTPS	443	TCP
DNS	53	TCP/UDP
Telnet	23	TCP
SSH	22	TCP
POP3	110	TCP
IMAP	143	TCP
LDAP	389	TCP
LDAPS (ldap over SSL)	636	TCP

Documentation technique de la plate-forme collaborative

La plate-forme collaborative est composée d'un portail, installé sur un serveur web qui donne accès à un espace dans lequel chaque utilisateur retrouve les applications nécessaires au travail collaboratif: webmail, gestion d'agenda, gestion documentaire, gestion de projet, catalogue des produits, base de connaissance des procédés industriels, actualités, contacts / annuaire d'entreprise...

Aucun logiciel client n'est nécessaire. Un simple navigateur compatible Java suffit pour accéder au portail et à l'ensemble des applications collaboratives.

Les données sont stockées dans une base de donnée SQL, soit interne à la plate-forme, soit hébergée sur un serveur SGBD externe.

Le portail utilise le protocole LDAP pour l'authentification des utilisateur, soit par un annuaire intégré à la plate-forme, soit sur l'annuaire de l'entreprise.

Le portail se connecte au serveur de messagerie de l'entreprise pour récupérer le courrier destiné à l'utilisateur et l'afficher dans une interface de type webmail.

Les applications du portail utilisent le serveur de messagerie pour la communication nécessaire aux travail collaboratif (par exemple envoyer un rappel par mail avant une réunion prévue sur l'agenda du projet).

Proposition de solution pour l'ouverture de la plate-forme collaborative

1. Configuration du serveur web du siège social (serveur nommé HTTP, 172.16.0.20) afin d'héberger le portail collaboratif et de le mettre disposition des utilisateurs par l'URL https://intranet.xoni.com

2. Hébergement de bases de données de la plate-forme sur le serveur SGBD de l'entreprise (serveur nommé BDD, 172.16.0.40)

3. Authentification du portail sur l'annuaire du siège social (serveur LDAP/DNS, 172.16.0.30)

4. Mise en place de la réplication entre les annuaires LDAP des sites distants et celui du siège sur une connexion sécurisée par certificat SSL, utilisant le protocole LDAPS (LDAP over SSL).

5. Configuration des serveurs DNS de l'entreprise pour assurer la résolution en interne du nom de domaine intranet.xoni.com.

6. Accès des sites distants au portail : deux possibilités :

A. Connexion inter-site par internet :

- Modification de l'abonnement du siège social : remplacement de l'accès ADSL par une connexion SDSL avec débit garanti 10Mb/s.
- Pour les sites de Dijon et Rouen : utilisation des connexion ADSL actuelles .
- Pour les employés nomades on conserve l'accès par VPN actuel.
- Configuration du routeur SDSL du siège afin de rediriger les connexions entrantes vers la plate-forme collaborative et en sécuriser l'accès (accès ouvert uniquement aux sites distants de l'entreprise).
- Solution réalisable en interne, à moindre coût.

B. Réseau privé virtuel

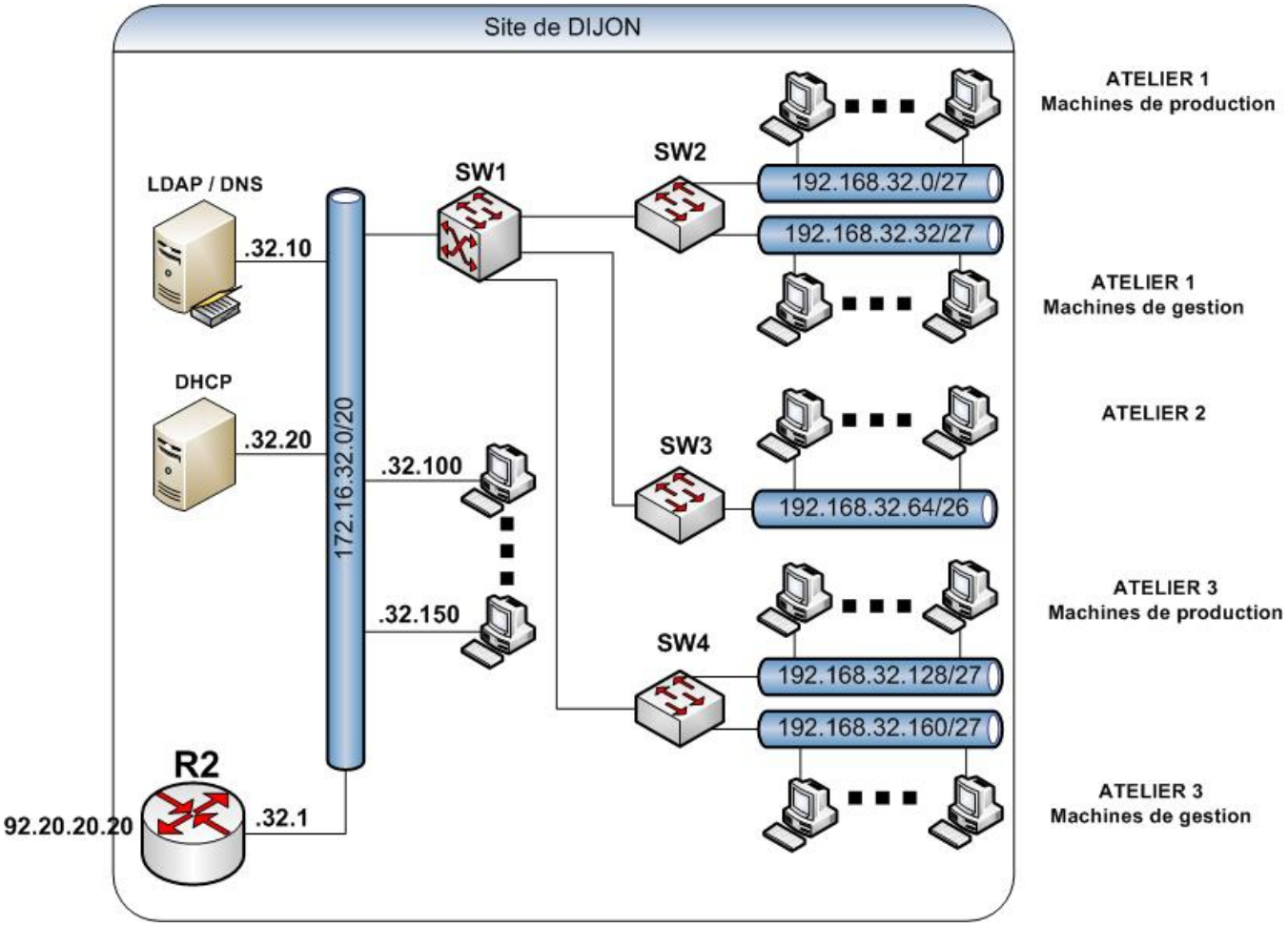
- VPN d'entreprise basé sur Ipsec et intégrant la priorisation des flux (QoS).
- Solution fournie par un opérateur, nécessitant d'importants frais de mise en service, et des coûts d'abonnement plus importants.
- Dans cette solution, les trois sites communiquent par le réseau privé de l'entreprise.

Documentation de la partie 2

Liste des VLAN du site de Dijon

VLAN	Adresse réseau	Adresse interface virtuelle du Vlan
Vlan 1 (Réseau administratif)	172.16.32.0/20	172.16.32.2
Vlan 2 (Atelier 1 - Machines de production)	192.168.32.0/27	192.168.32.1
Vlan 3 (Atelier 1 - Machines de gestion)	192.168.32.32/27	192.168.32.33
Vlan 4 (Atelier 2)	192.168.32.64/26	192.168.32.65
Vlan 5 (Atelier 3 - Machines de production)	192.168.32.160/27	192.168.32.161
Vlan 6 (Atelier 3 - Machines de gestion)	192.168.32.192/27	192.168.32.193

Réseau de Dijon après le remplacement du routeur R4



Configuration partielle du commutateur SW1

Port	VLAN	Port 802.1Q activé	Périphérique connecté
1	1	non	R2
2			SW2
3			SW3
4			SW4
Autres	1	non	…

Documentation de la partie 3

Offres de solutions de sauvegarde en ligne

Critères	Offre BeNeo	Offre Tecarch
Tarification	60 € par mois pour un volume autorisé de 50 Go sauvegardés	500 € par an pour un volume autorisé de 20 Go sauvegardés, puis 10 € par an par Go supplémentaire
Disponibilité du service	24/24 heures, 7/7 jours, 365/365 jours	24/24 heures, 7/7 jours, 365/365 jours
Conditions techniques de l'hébergement	Deux centres d'hébergement Tier3 reliés par fibre optique Caractéristiques : • Norme ISO 9001 • Sécurité d'accès physique 24x7x365 par du personnel présent sur site • Contrôle d'accès biométrique • Alimentation électrique, de grande capacité, stable et redondante • Double liaison télécoms et support de communication intégralement en fibre optique • Climatisations redondantes et protection anti-feu	Un centre de pilotage surveille l'environnement
Confidentialité	• Cryptage des données • Serveurs virtuellement « privés » permettant une administration personnalisée • Rapport quotidien de sauvegarde par courriel	• Cryptage des données • Serveurs mutualisés • Rapport quotidien de sauvegarde par courriel
Type de sauvegarde autorisée	• Totale en début de période de sauvegarde, différentielle ensuite • Période de sauvegarde modulable de 5 à 20 jours	• Totale en début de période de sauvegarde, incrémentielle ensuite • Période de sauvegarde hebdomadaire
Restauration	Complète ou partielle ; accès à distance aux données sauvegardées, avant restauration	Complète ou partielle ; accès à distance aux données sauvegardées avant restauration