

Concevoir une architecture segmentée

Tout ce dont vous avez besoin pour ce module, dans un seul document. Cochez au fur et à mesure.

U4-S2-M3

module

Élève

document

TechnoVert

scénario 2

B · 3 h

format et durée

Ce qu'il faut savoir avant de commencer	3
C'est quoi un sous-réseau ?	3
C'est quoi un VLAN ?	3
C'est quoi un service et un port ?	3
C'est quoi un pare-feu ?	3
Vérifiez-vous	4
Segmenter et cloisonner	5
Capsule 1 sur 3 Découper le réseau en zones	5
Capsule 2 sur 3 Décider qui peut joindre quoi	7
Capsule 3 sur 3 Contrôler au point de passage	10
Ce qu'on retient	12
Segmenter et cloisonner	13
L'essentiel	13
Les mots à connaître	13
La méthode	13
Un exemple concret	14
Les pièges	14
Trois architectures pour un même besoin	15
PARTIE A — Comprendre le besoin	16
PARTIE B — Comparer trois architectures	19
PARTIE C — Trouver les points faibles	23
PARTIE D — Proposer une segmentation pour TechnoVert	25
POUR ALLER PLUS LOIN	31
CE QU'IL FAUT RETENIR	31
Tous les documents du module	32
A1 — Le constat d'audit de TechnoVert et les demandes des interlocuteurs	32
A2 — Trois architectures pour le même besoin	33
A3 — La grille d'analyse et ses critères	35

Ce qu'il faut savoir avant de commencer

Ce qu'il faut savoir avant de commencer. Lisez-le si vous avez un doute.

C'est quoi un sous-réseau ?

Un sous-réseau est un groupe d'adresses IP qui se suivent, défini par une adresse et un masque. Par exemple 192.168.1.0/24.

Deux machines du même sous-réseau se parlent directement. Pour joindre un autre sous-réseau, elles passent par un routeur.

C'est quoi un VLAN ?

Un **VLAN** est un réseau séparé, créé à l'intérieur d'un même switch. Deux postes branchés sur le même switch, mais dans deux VLAN différents, ne se voient pas.

En général, on donne un sous-réseau à chaque VLAN. Pour passer d'un VLAN à l'autre, il faut un routeur ou un switch de niveau 3.

C'est quoi un service et un port ?

Un service est ce qu'une machine offre aux autres : un site web, des fichiers partagés, une base de données.

Chaque service écoute sur un numéro de port. Exemples : 443 pour un site web sécurisé en HTTPS, 445 pour le partage de fichiers en SMB, 22 pour l'administration à distance en SSH.

C'est quoi un pare-feu ?

Un **pare-feu**, ou firewall, est un équipement ou un logiciel qui laisse passer ou bloque les échanges. Il décide selon des règles : d'où vient l'échange, où il va, et pour quel service.

Vérifiez-vous

☐ 1. Deux postes sont dans deux VLAN différents du même switch. Se voient-ils directement ?

☐ 2. Sur quel port écoute un site web en HTTPS ?

☐ 3. Un pare-feu décide selon trois informations. Lesquelles ?

Réponses

1. Non. Il faut passer par un routeur ou un switch de niveau 3.

2. Le port 443.

3. La source, la destination et le service.

Segmenter et cloisonner

COURS-U4-S2-03

Sophie Lemarchand est comptable chez TechnoVert. Un lundi matin, ses fichiers ne s'ouvrent plus.

Un poste de l'atelier a été infecté par une clé USB. Le virus a traversé tout le réseau et chiffré une partie du serveur de fichiers, comptabilité comprise. Chiffrés, les fichiers sont verrouillés par un code secret : plus personne ne peut les ouvrir.

Sophie demande : « Pourquoi un poste de l'atelier peut-il toucher à mes fichiers ? »

À la fin de la séance, vous saurez découper un réseau en zones. Vous saurez décider ce qui passe d'une zone à l'autre, et où le contrôler.

LE PLAN DE LA SÉANCE

- 1 Découper le réseau en zones.
- 2 Décider qui peut joindre quoi.
- 3 Contrôler au point de passage.

LA QUESTION DE DÉPART

Dans les couloirs du lycée, il y a des portes coupe-feu. À quoi servent-elles ?

CAPSULE 1 SUR 3

Découper le réseau en zones

Chez TechnoVert, le réseau est plat : un seul grand réseau, sans aucune séparation, comme une cour de récré sans barrière. Toutes les machines se voient, et rien n'arrête un virus.

Comment couper le réseau en parties séparées ?

C'est ce qu'on appelle **SEGMENTER** un réseau : le découper en zones séparées, pour contrôler ce qui passe de l'une à l'autre.

Au lycée, c'est pareil. Les élèves n'entrent pas dans la salle des profs, et les visiteurs passent par l'accueil. Chaque espace a ses règles, et un réseau segmenté fonctionne de la même façon.

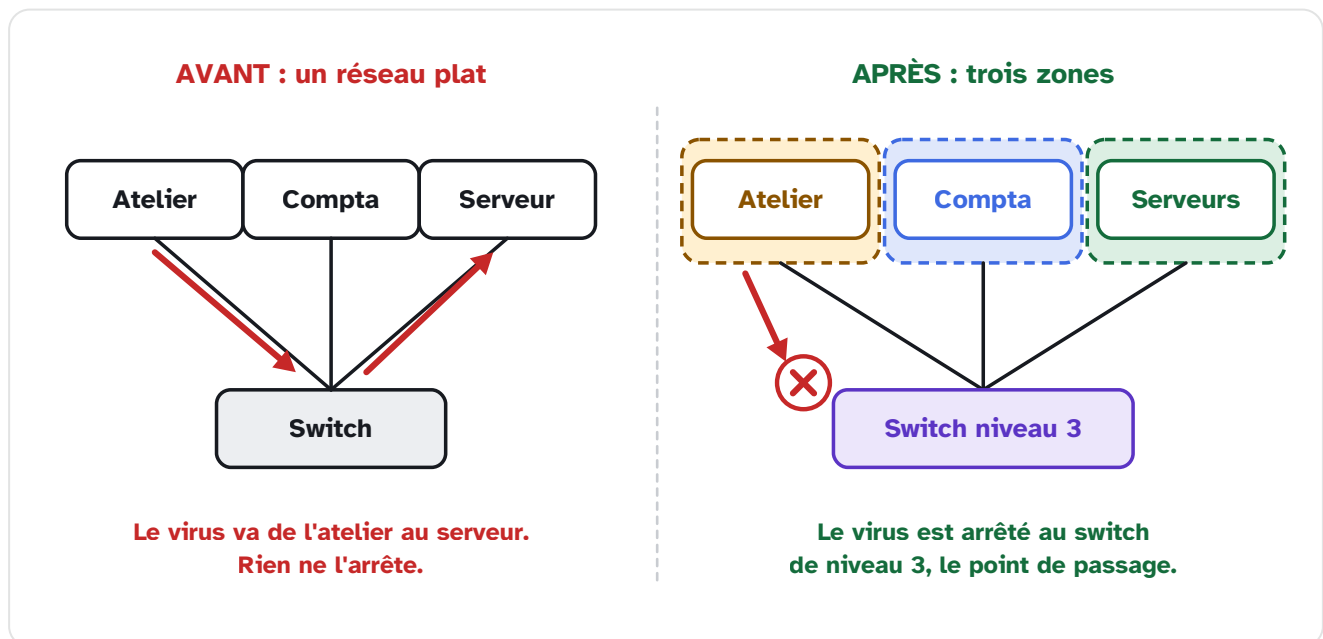


Schéma • Avant, le virus traverse le réseau plat ; après, il est arrêté au switch de niveau 3

Pour découper, on choisit un critère. Il y en a trois :

- 1 **Le métier.** On regroupe les machines d'un même service. Elles ont les mêmes besoins et les mêmes droits.
- 2 **La sécurité.** On regroupe les machines selon leur sensibilité : ce qu'on perd si elles sont attaquées. Les serveurs d'un côté, les appareils inconnus de l'autre.
- 3 **La performance.** On isole ce qui produit beaucoup de trafic, pour ne pas gêner les autres. Par exemple les caméras ou les sauvegardes.

Dans une vraie entreprise, on combine. On découpe d'abord par métier, puis on ajoute des zones de sécurité : les serveurs, les invités, l'administration du réseau.

ON LE FAIT ENSEMBLE — UNE ÉCOLE DE MUSIQUE

1. Le poste du secrétariat, avec les inscriptions : quelle zone, quel critère ?
2. Le Wi-Fi des parents qui attendent ?
3. Le serveur qui garde les fiches des élèves et les plannings de cours ?
4. La caméra du hall, qui filme toute la journée ?

Exemple	Pourquoi
✓ La comptabilité séparée de l'atelier	Les métiers sont différents, et les données de la comptabilité sont sensibles : secrètes et importantes, comme les salaires.
✗ Une zone par étage du bâtiment	L'étage ne dit rien des besoins. Deux services différents se retrouvent ensemble.
✗ Une zone par poste	Chaque zone demande des règles. Avec une zone par poste, plus personne ne peut les tenir à jour.

CHECKPOINT

À l'oral, 3 minutes. Chacun note sa réponse sur sa feuille, puis on corrige.

1. Donnez les trois critères de segmentation.
2. Pourquoi le réseau plat de TechnoVert a-t-il laissé passer le virus ?

CAPSULE 2 SUR 3

Décider qui peut joindre quoi

Le réseau est découpé en zones. Mais qui a le droit de parler à qui ?

Chaque zone est une **ZONE DE CONFIANCE** : un groupe de machines qui suivent les mêmes règles, parce qu'on leur fait la même confiance.

Ce qui définit une zone, ce n'est pas le câble. C'est la règle qu'on lui applique : qui peut y entrer, et ce qu'elle a le droit de joindre.

On range les zones en trois niveaux. Le plus bas s'appelle « exposé » : la zone est ouverte à des appareils inconnus, donc en danger.

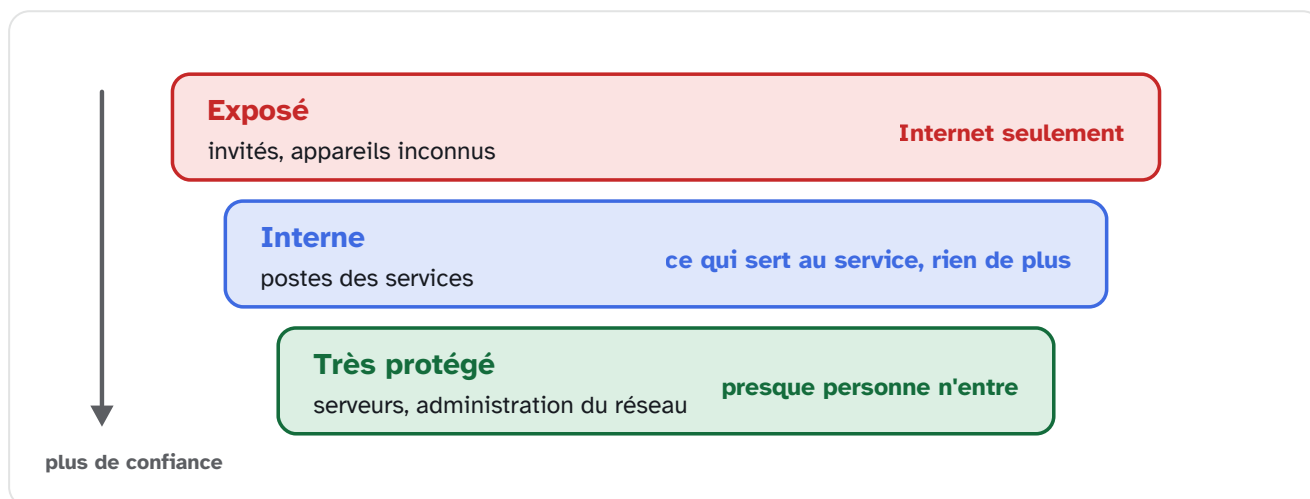


Schéma • Trois niveaux de confiance : exposé, interne, très protégé

Pour choisir le niveau d'une zone, posez-vous une question : que se passe-t-il si une machine de cette zone est infectée ? Plus la réponse est grave, plus la zone doit être protégée.

Une règle guide tous ces choix : le **MOINDRE PRIVILÈGE**. Chaque zone reçoit les accès utiles, et rien d'autre. On ferme tout, puis on ouvre au cas par cas.

Pensez à un badge d'entreprise. Il ouvre certaines portes, pas toutes : le badge d'un stagiaire n'ouvre pas la salle des serveurs. Une zone, c'est pareil : elle n'ouvre que les portes dont elle a besoin.

INSTANT HISTOIRE — 2013 : TARGET PIRATÉ PAR L'ACCÈS DE SON CHAUFFAGISTE

Fin 2013, des pirates volent les données d'environ 40 millions de cartes bancaires chez Target, une grande chaîne de supermarchés américaine, comme Carrefour chez nous.

Ils sont entrés avec le compte d'un prestataire de chauffage et de climatisation. Ce prestataire avait un accès au réseau de l'entreprise.

Pourquoi le compte du chauffagiste n'aurait-il jamais dû mener aux caisses des magasins ?

Ces règles, on les écrit dans un tableau.

Ce tableau s'appelle une **MATRICE DE FLUX** : il dit quelle zone peut joindre quelle zone, et pour quel service. C'est la liste des portes que chaque badge ouvre.

Un flux, c'est un échange entre deux machines pour un service : ouvrir un site web, lire un fichier partagé, imprimer. Tout ce qui n'est pas dans la matrice est interdit.

Pour la construire :

- 1 **Listez** les zones, en ligne et en colonne.
- 2 **Demandez** à chaque service ce qu'il doit joindre, et pour quoi faire.
- 3 **Remplissez** chaque case : « non », « oui », ou le service précis.
- 4 **Placez** chaque serveur dans une zone à part, jamais avec les postes.

ON LE FAIT ENSEMBLE — TROIS CASES POUR UNE CLINIQUE VÉTÉRINAIRE

1. Les invités de la salle d'attente vers les serveurs ?
2. L'accueil vers les serveurs ?
3. Les salles de soins vers l'accueil ?

Voici la matrice complète de la clinique :

De ↓ vers

Accueil	—	non	agenda et facturation seulement	non	oui
Soins	non	—	dossiers des animaux seulement	non	oui
Serveurs	non	non	—	non	mise à jour seulement
Invités	non	non	non	—	oui

Exemple

Pourquoi



« Soins vers Serveurs : dossiers des animaux seulement »

Le service est précis. Le pare-feu pourra l'appliquer tel quel.



« Accueil vers Serveurs : oui, tout »

L'accueil peut alors administrer les serveurs. Personne ne l'a demandé.



« On ouvre tout, et on fermera ce qui pose problème »

C'est l'inverse du moindre privilège. Le problème arrive avant la fermeture.

CHECKPOINT

À l'oral, 3 minutes. Chacun note sa réponse sur sa feuille, puis on corrige.

1. Dans quel niveau placez-vous le Wi-Fi des visiteurs ?
2. Un flux n'apparaît pas dans la matrice. Est-il permis ?

CAPSULE 3 SUR 3

Contrôler au point de passage

La matrice dit ce qui est permis. Mais qui l'applique, et à quel endroit du réseau ?

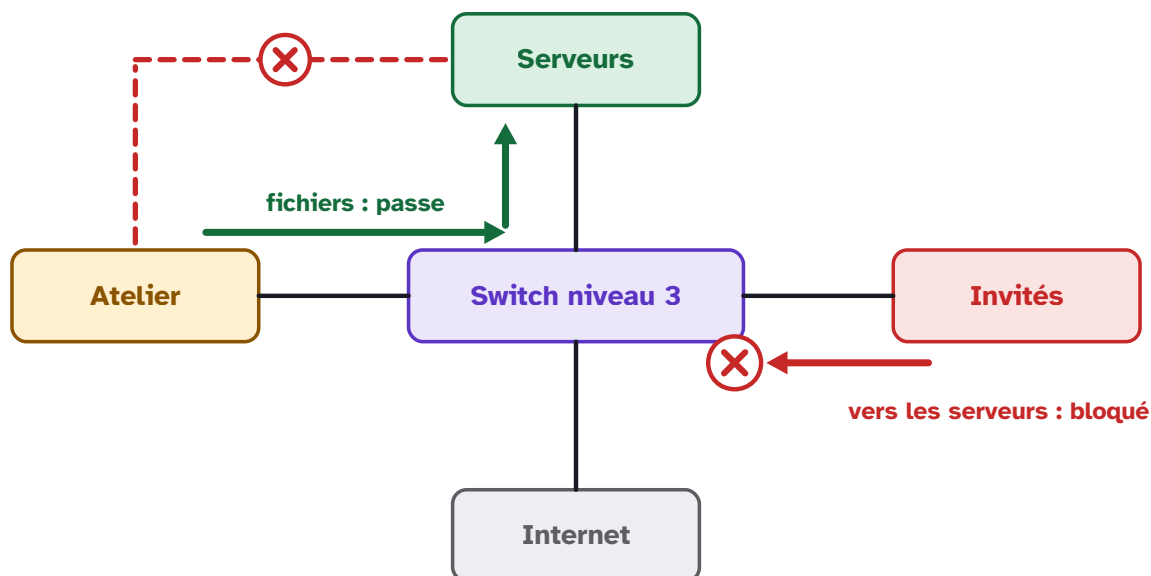
Cet endroit s'appelle un **POINT DE PASSAGE OBLIGÉ** : l'équipement que traverse tout échange entre deux zones.

C'est comme le portique à l'entrée du lycée. Tout le monde passe par là, et c'est là qu'on contrôle les badges. Si une porte de derrière reste ouverte, le portique ne sert plus à rien.

Ce peut être un routeur, un switch de niveau 3 qui relie les zones, ou un pare-feu. Chaque flux entre deux zones le traverse.

C'est donc là qu'on contrôle. On peut y :

- 1 **Autoriser ou refuser** un flux, selon sa source, sa destination et son service.
- 2 **Enregistrer** les passages, pour savoir ce qui s'est passé après un incident.
- 3 **Couper** une zone infectée, sans arrêter les autres.



Un chemin de côté, en pointillé, contourne le contrôle : on l'interdit.

Schéma • Tout passe par le switch de niveau 3 : l'atelier passe, l'invité est bloqué, le chemin de côté est interdit

Le point de passage ne sert à rien s'il existe un autre chemin. Un poste branché sur deux zones à la fois ouvre une porte de côté. Un point d'accès Wi-Fi branché dans la mauvaise zone aussi.

ON LE FAIT ENSEMBLE — UN POSTE DE L'ATELIER EST INFECTÉ

1. Le virus veut joindre un poste de la comptabilité. Par où passe-t-il ?
2. Que fait le switch ?
3. Le virus veut ouvrir un fichier sur le serveur. Que se passe-t-il ?
4. Que fait le technicien ?

Et si l'entreprise grandit, et qu'il faut une zone de plus ? Chaque zone ajoutée demande une ligne et une colonne de plus dans la matrice, et de nouvelles règles.

Changer une segmentation plus tard coûte cher : nouvelles adresses, nouvelles règles, interventions sur chaque switch. On choisit donc le nombre de zones avec soin, et on garde de la place pour la zone de demain.

Exemple	Pourquoi
✓ Tous les flux entre zones passent par le switch de niveau 3	Un seul endroit à surveiller et à régler.
✗ Un serveur branché à la fois dans la zone serveurs et dans la zone atelier	Il crée un chemin qui ne passe par aucun contrôle.
✗ Découper en vingt zones « pour être tranquille »	20 zones, c'est 20 lignes sur 20 colonnes : 400 cases à tenir à jour. Personne n'y arrivera.

CHECKPOINT

À l'oral, 3 minutes. Chacun note sa réponse sur sa feuille, puis on corrige.

1. Donnez deux choses qu'on peut faire à un point de passage.
2. Pourquoi un poste branché sur deux zones est-il dangereux ?

Ce qu'on retient

SI VOUS NE DEVEZ RETENIR QUE TROIS CHOSES

1. Découpez d'abord par métier, puis ajoutez des zones pour les serveurs, les invités et l'administration du réseau.
2. Écrivez la matrice de flux avec le moindre privilège : tout est fermé, sauf ce qui est utile.
3. Faites passer tous les flux entre zones par un point de passage obligé, sans aucun chemin de côté.

Revenons à Sophie Lemarchand. Avec une zone pour l'atelier, une pour l'administration et une pour les serveurs, le virus n'aurait plus atteint les postes des autres services.

Au point de passage, l'atelier n'aurait joint le serveur que pour l'intranet, le site web interne de l'entreprise, et pour les fichiers. Avec des droits réglés sur le dossier de la comptabilité, celle-ci aurait continué de travailler.

Segmenter et cloisonner

COURS-U4-S2-03

L'essentiel

- **Segmenter** : découper le réseau en zones séparées, pour contrôler ce qui passe.
- **Trois critères** : le métier, la sécurité, la performance. On les combine.
- **Zone de confiance** : des machines qui suivent les mêmes règles.
- **Moindre privilège** : chaque zone reçoit les accès utiles, rien de plus.
- **Point de passage obligé** : l'endroit où tous les flux entre zones sont contrôlés.

Les mots à connaître

Mot	En clair
Segmentation	Le découpage du réseau en zones.
Zone de confiance	Un groupe de machines avec le même niveau de confiance.
Moindre privilège	On ferme tout, puis on ouvre seulement ce qui sert.
Matrice de flux	Le tableau qui dit qui peut joindre quoi, et pour quel service.
Point de passage obligé	Routeur, switch de niveau 3 ou pare-feu entre deux zones.

La méthode

1. **Listez** les services et les machines.
2. **Découpez** par métier, puis ajoutez les zones serveurs, invités et administration du réseau.
3. **Classez** chaque zone : très protégée, interne ou exposée.
4. **Remplissez** la matrice de flux, case par case.
5. **Vérifiez** que chaque flux passe par un point de passage, sans chemin de côté.

Un exemple concret

Une clinique vétérinaire a un accueil, des salles de soins, un serveur et une salle d'attente avec Wi-Fi.

Étape	Ce qu'on fait	Résultat
1	Découper par métier	Accueil, Soins
2	Ajouter les zones de sécurité	Serveurs, Invités
3	Classer	Serveurs très protégés, Accueil et Soins internes, Invités exposés
4	Remplir la matrice	Accueil vers Serveurs : agenda et facturation. Invités : Internet seulement.
5	Placer le point de passage	Tous les flux passent par le routeur de la clinique.

Conclusion : un Wi-Fi de visiteur infecté ne peut plus toucher aux dossiers des animaux.

Les pièges

- **✗ Découper par étage** → découpez selon les besoins, pas selon le bâtiment.
- **✗ Écrire « oui, tout »** → précisez le service utile.
- **✗ Mettre les serveurs avec les postes** → donnez-leur une zone à part.
- **✗ Brancher une machine sur deux zones** → tout flux passe par le point de passage.

Trois architectures pour un même besoin

LABO-U4-S2-03

Contexte — Vous travaillez pour la société qui reprend le réseau de TechnoVert. Après l'incident de la clé USB, la dirigeante veut séparer les services.

Trois architectures sont sur la table. Aucune n'est parfaite. Votre travail : les comparer avec méthode, puis proposer la vôtre.

RÈGLE 1A DE LA SÉANCE

Scénario 2 : l'IA peut vous expliquer une notion, par exemple le moindre privilège. Elle ne remplit pas vos grilles et ne propose pas votre segmentation.

Si vous lui posez une question, notez-la en bas de votre feuille.

À la fin de ce labo, vous saurez comparer des architectures avec une grille et trouver leur point faible. Vous saurez proposer une segmentation pour un vrai besoin.

Ce que vous rendez — les grilles remplies et votre proposition de segmentation, avec son schéma et sa matrice de flux. Retour oral en fin de séance. Pas de note.

Les mots de la séance

Mot	Ce que ça veut dire
Zone	Un groupe de machines qui suivent les mêmes règles.
Point de passage	L'équipement que traverse tout flux entre deux zones.
Flux	Un échange entre deux machines, pour un service : web, fichiers, impression.
Matrice de flux	Le tableau qui dit quelle zone peut joindre quelle zone, et pour quel service.
Moindre privilège	Chaque zone reçoit les accès utiles, rien de plus.
Rédhibitoire	Un défaut si grave qu'il suffit à refuser la solution.
Réseau plat	Un seul grand réseau, sans aucune séparation : toutes les machines se voient.

Mot	Ce que ça veut dire
Intranet	Le site web interne de l'entreprise, comme l'ENT du lycée.
Télémaintenance	Réparer une machine à distance, par le réseau, sans se déplacer.
Sous-traitant	Une entreprise extérieure qui fait une partie du travail. Ici, l'entretien de la machine de découpe.

Ce dont vous avez besoin

- [Annexe A1](#) : le constat d'audit de TechnoVert et les demandes des interlocuteurs.
- [Annexe A2](#) : les trois architectures.
- [Annexe A3](#) : la grille d'analyse et ses critères.
- Une feuille et un crayon pour le schéma. Si vous préférez l'écran : diagrams.net, dans le navigateur, sans inscription.

En binôme — le pilote écrit, le lecteur lit les consignes et les annexes à voix haute. On inverse à la partie C.

Le plan du labo

Partie	Étapes	Ce que vous obtenez
A — Comprendre le besoin	1 à 5	la liste de ce qui doit changer
B — Comparer trois architectures	6 à 10	la grille remplie
C — Trouver les points faibles	11 à 14	le point faible et le flux difficile de chacune
D — Proposer une segmentation	15 à 21	vos zones, votre schéma, votre matrice

PARTIE A — Comprendre le besoin

Étapes 1 à 5. À la fin, vous savez ce que la nouvelle architecture doit empêcher.

Besoin d'un rappel ? Revoir le cours : [« Découper le réseau en zones »](#).

01 Lire le constat d'audit

Le constat d'audit décrit le réseau tel qu'il est, mesuré sur place.

☐ Ouvrez l'[annexe A1](#) et lisez la partie « Le réseau aujourd'hui ».

☐ Notez le nombre de machines trouvées, et le type de réseau :

Vous devez avoir : un nombre proche de 35, et un mot qui dit que toutes les machines se voient.

02 Trouver dans la doc

Deux équipements n'ont été cités par personne pendant les entretiens. Le balayage du réseau les a trouvés : un logiciel a interrogé toutes les adresses, une par une.

☐ Dans l'[annexe A1](#), trouvez ces deux équipements. Remplissez la grille :

Adresse	Équipement	Service ouvert	Qui doit décider

Vous devez avoir : deux adresses qui finissent par .201 et .202. Deux personnes différentes décident.

03 Lire les demandes

- ☐ Lisez la partie « Ce que demandent les interlocuteurs » de l'[annexe A1](#).
- ☐ Remplissez la grille. Pour chaque demande, choisissez le critère de découpage : métier, sécurité ou performance. Si aucun ne convient, écrivez « aucun, c'est une contrainte ». La première ligne est faite pour vous.

Personne	Ce qu'elle demande	Critère
Sophie Lemarchand	Ses données ne doivent plus être accessibles à toute l'entreprise.	sécurité
Karim Benali		
Ludivine Marchetti		
Hélène Vasseur, sa demande sur les visiteurs		

Vous devez avoir : quatre lignes. Au moins deux critères différents.

04 Comparer ce qui est dit et ce qui est mesuré

Sophie Lemarchand affirme : « L'atelier n'a pas accès à la compta. »

- ☐ Trouvez dans l'[annexe A1](#) la ligne qui contredit Sophie. Recopiez-la :

Vous devez avoir : une ligne sur le partage du serveur de fichiers.

Pourquoi ? Pourquoi un technicien vérifie-t-il par un balayage ce qu'on lui a dit en entretien ?

Votre réponse :

05 Lister ce qui doit devenir impossible

- ☐ Écrivez trois flux qui existent aujourd'hui et qui doivent devenir impossibles. Exemple de forme : « Un poste de l'atelier se connecte à un poste de la comptabilité. »

1. _____
2. _____
3. _____

Vous devez avoir : trois flux différents. Au moins un concerne les invités ou les deux équipements oubliés.

POINT DE CONTRÔLE A

- ☐ Montrez au formateur vos grilles des étapes 2 et 3, et vos trois flux.
- ☐ Le formateur a validé. Passez à la partie B.

PARTIE B — Comparer trois architectures

Étapes 6 à 10. À la fin, la grille de comparaison est remplie.

Besoin d'un rappel ? Revoir le cours : « [Contrôler au point de passage](#) ».

06 Lire une colonne résolue

☐ Ouvrez l'[annexe A2](#) et lisez l'architecture A.

☐ Ouvrez l'[annexe A3](#) et lisez les cinq critères.

Voici la colonne de l'architecture A, remplie en entier. Suivez ce modèle pour les deux autres.

Critère	Architecture A	Pourquoi
1. Une infection de l'atelier atteint-elle la comptabilité ?	oui	Tout le réseau interne est une seule zone.
2. Un invité atteint-il le serveur de fichiers ?	oui	Les invités sont dans la même zone que le serveur.
3. Combien de points de passage entre zones internes ?	0	Le pare-feu ne contrôle que la sortie vers Internet.
4. Peut-on limiter l'atelier à l'intranet et aux fichiers ?	non	Aucun équipement ne voit passer ces flux.
5. Combien de règles à tenir à jour ?	peu	Seulement les règles vers Internet.

Vous devez voir : une architecture simple, mais qui ne répond à aucune demande de sécurité.

07 Remplir la colonne de l'architecture B

☐ Lisez l'architecture B dans l'[annexe A2](#).

☐

Remplissez la grille :

Critère	Architecture B	Pourquoi
1. Infection de l'atelier vers la comptabilité ?		
2. Invité vers le serveur de fichiers ?		
3. Points de passage entre zones internes ?		
4. Atelier limité à l'intranet et aux fichiers ?		
5. Règles à tenir à jour ?		

Vous devez avoir : au moins une réponse différente de l'architecture A, sur les invités.

08 Remplir la colonne de l'architecture C

☐ Lisez l'architecture C dans l'[annexe A2](#).

☐ Remplissez la grille :

Critère	Architecture C	Pourquoi
1. Infection de l'atelier vers la comptabilité ?		
2. Invité vers le serveur de fichiers ?		
3. Points de passage entre zones internes ?		
4. Atelier limité à l'intranet et aux fichiers ?		
5. Règles à tenir à jour ?		

Vous devez avoir : la seule architecture où le critère 4 est possible.

09 Compter les points de passage

☐ Sur chaque schéma de l'[annexe A2](#), entourez l'équipement que traversent les flux entre deux zones internes.

☐ Notez pour chaque architecture l'équipement entouré, ou « aucun » :

Vous devez avoir : « aucun » pour deux architectures.

10 Relier la grille à la demande

☐ Relisez la demande de Sophie Lemarchand dans l'[annexe A1](#), puis votre grille complète.

Vous devez avoir : une seule ligne de la grille qui parle de la comptabilité.

Pourquoi ? Sophie Lemarchand a fait la demande la plus urgente. Quelle ligne de la grille y répond ? Quelle architecture y répond ?

Votre réponse :

POINT DE CONTRÔLE B

☐ Montrez au formateur la grille complète des trois architectures.

☐ Le formateur a validé. Passez à la partie C.

PARTIE C — Trouver les points faibles

Étapes 11 à 14. À la fin, vous connaissez le point faible et le flux difficile de chaque architecture.

Besoin d'un rappel ? Revoir le cours : [« Décider qui peut joindre quoi »](#).

11 Le point faible de chaque architecture

☐ Pour chaque architecture, écrivez le critère où elle est la plus faible. La première ligne est faite pour vous.

Architecture	Critère le plus faible	En une phrase
A	1	Une infection de l'atelier atteint toute l'entreprise.
B		
C		

Vous devez avoir : un critère différent pour l'architecture C.

12 Réhibitoire ou non ?

- ☐ Pour chaque point faible, dites s'il est réhibitoire pour TechnoVert. Justifiez avec une demande de l'[annexe A1](#).

Architecture	Réhibitoire ?	Quelle demande le prouve
A		
B		
C		

Vous devez avoir : une seule architecture dont le point faible n'est pas réhibitoire.

13 Le flux difficile à contrôler

- ☐ Pour chaque architecture, écrivez un flux qu'elle ne permet pas de contrôler, ou qu'elle rend difficile : _____

Vous devez avoir : pour A et B, un flux interne. Pour C, une phrase qui dit ce que ça coûte de tout contrôler.

14 Tirer la leçon

- ☐ Comparez la ligne 5 de la grille avec les lignes 1, 2 et 4, pour l'architecture A.

Vous devez avoir : une architecture qui gagne sur le coût, et perd sur toute la sécurité.

Pourquoi ? L'architecture A est la plus simple. Pourquoi n'est-elle pas la meilleure pour TechnoVert ?

Votre réponse :

POINT DE CONTRÔLE C

☐ Montrez au formateur vos tableaux des étapes 11 et 12.

☐ Le formateur a validé. Passez à la partie D.

PARTIE D — Proposer une segmentation pour TechnoVert

Étapes 15 à 21. À la fin, vous avez vos zones, votre schéma et votre matrice de flux.

Besoin d'un rappel ? Revoir le cours : [« Décider qui peut joindre quoi »](#).

15 Choisir les zones

☐ Listez vos zones. Pour chacune, donnez son critère et son niveau : très protégé, interne ou exposé. La première ligne est faite pour vous.

Zone	Critère	Niveau	Pourquoi cette zone
Invités	sécurité	exposé	Leurs appareils sont inconnus.

Zone	Critère	Niveau	Pourquoi cette zone

Vous devez avoir : entre cinq et sept zones. Les serveurs ont leur propre zone.

16 Placer les machines

☐ Pour chaque machine, écrivez sa zone :

Machine	Zone
Poste de Sophie Lemarchand, comptable	
Poste de Ludivine Marchetti, chargée d'études	
Poste de montage de l'atelier	
Serveur de fichiers TV-SRV-FIC	
Portable d'un client en visite	
Switch de niveau 3 à administrer	

Vous devez avoir : six machines dans au moins cinq zones différentes.

17 Les deux équipements oubliés

☐ Relisez votre grille de l'étape 2.

☐ Proposez une zone pour la caméra et pour le boîtier de télémaintenance. Écrivez aussi qui doit valider votre choix : _____

Vous devez avoir : aucun des deux dans une zone de postes. Un nom de personne ou d'entreprise pour chacun.

Pourquoi ? Pourquoi le technicien ne coupe-t-il pas tout seul le boîtier de télémaintenance ?

Votre réponse :

18 Dessiner le schéma

- ☐ Dessinez votre architecture, sur papier ou dans diagrams.net. Montrez chaque zone, le point de passage et la sortie vers Internet.

Pour démarrer, vous pouvez partir de ce modèle :

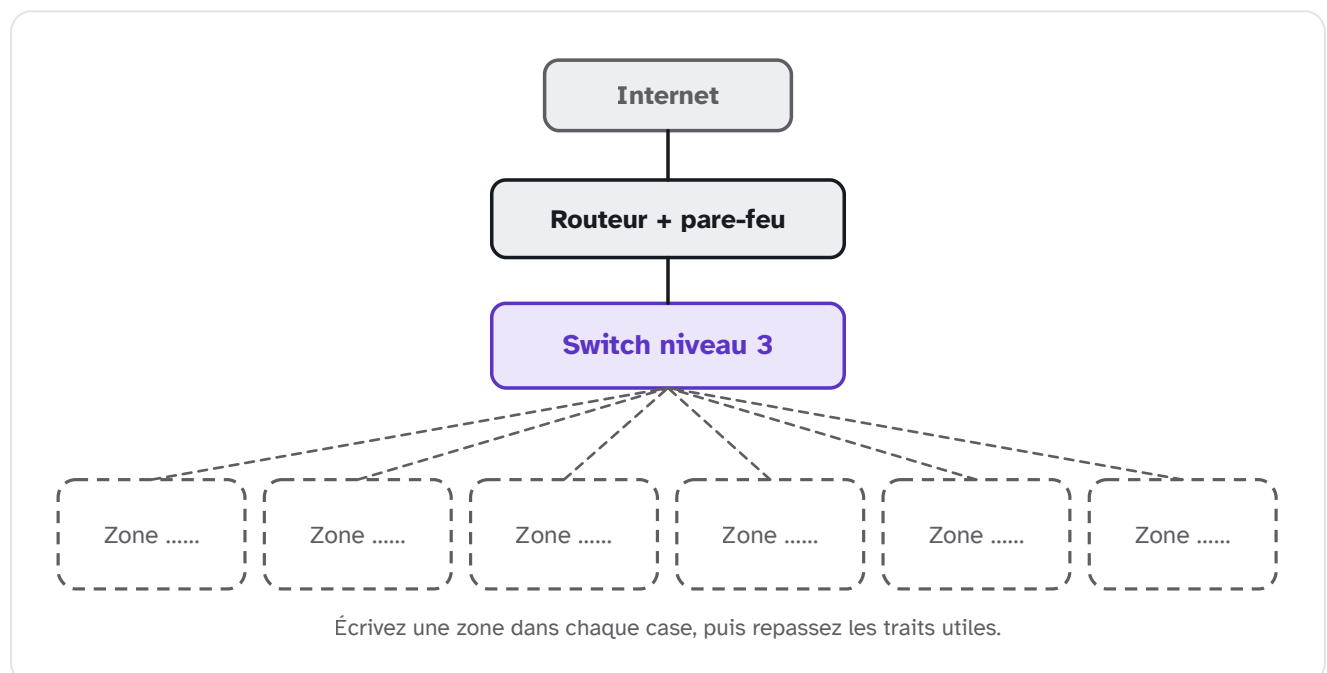


Schéma • Modèle à compléter : vos zones autour du switch de niveau 3

Vous devez avoir : un seul point de passage entre les zones internes. Aucun trait qui relie deux zones sans passer par lui.

19 Écrire la matrice de flux

- ☐
- Remplissez la matrice avec vos zones. Dans chaque case : « non », « oui », ou le service précis. Laissez vides les lignes et les colonnes en trop.

De ↓ vers →	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5	Zone 6	Zone 7	Internet

De ↓ vers →	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5	Zone 6	Zone 7	Internet

Vous devez avoir : une ligne des invités avec « non » partout, sauf vers Internet. Une ligne de l'atelier avec un service précis vers les serveurs.

20 Vérifier contre les demandes

☐ Reprenez vos trois flux de l'étape 5. Pour chacun, montrez la case « non » de votre matrice qui le bloque : _____

☐ Un flux passe par un service autorisé, comme les fichiers ? La matrice ne peut pas le bloquer. Notez ce qu'il faut régler sur le serveur, par exemple les droits d'un dossier :

Vous devez avoir : pour chaque flux, une case « non » ou un droit à régler. Si un flux n'est ni bloqué ni réglé, corrigez la matrice.

21 Comparer avec un autre binôme

☐ Échangez votre proposition avec un autre binôme. Relisez la sienne avec ces quatre questions :

- Chaque zone est-elle justifiée par une demande ?
- Les serveurs ont-ils leur propre zone ?
- Les invités sont-ils isolés de tout, sauf d'Internet ?
- Les trois flux de l'étape 5 sont-ils bloqués ?

☐ Notez une différence entre vos deux propositions, et la demande qui la justifie :

Vous devez avoir : une différence expliquée par un besoin, pas par un goût.

POINT DE CONTRÔLE D

☐ Montrez au formateur votre schéma et votre matrice de flux.

☐ Le formateur a validé. Rendez votre travail.

POUR ALLER PLUS LOIN

Un collègue a demandé une matrice de flux à une IA pour TechnoVert. Voici trois lignes de sa réponse. Elles contiennent trois erreurs.

- « Atelier vers Serveurs : oui, tous services, pour simplifier la maintenance. »
- « Invités vers Serveurs : HTTPS autorisé, pour qu'ils consultent l'intranet. »
- « Serveurs vers Internet : oui, tous services. »

☐

Pour chaque ligne, écrivez l'erreur et la bonne case : _____

CE QU'IL FAUT RETENIR

1. On compare des architectures avec une grille et des critères, pas au goût.
2. La plus simple n'est pas la meilleure : elle doit d'abord répondre aux demandes de sécurité.
3. Une segmentation se prouve avec sa matrice de flux : chaque flux dangereux y trouve sa case « non ».

Tous les documents du module

A1 — Le constat d'audit de TechnoVert et les demandes des interlocuteurs

Source : document de scénario, § 2 « Le client », § 3 « Les interlocuteurs », § 5 « L'existant avant refonte ». Utilisée dans : LABO étapes 1 à 5 et 12.

L'entreprise

TechnoVert installe et entretient des systèmes d'arrosage automatique et d'éclairage extérieur. Elle emploie 45 salariés.

Elle occupe deux bâtiments sur le même terrain, reliés par une seule fibre. Le bâtiment A abrite l'administration, la direction, le commercial et le bureau d'études. Le bâtiment B est l'atelier : assemblage, préparation du matériel, stockage.

L'incident. Un poste de l'atelier a été infecté par une clé USB. Il a chiffré, c'est-à-dire verrouillé par un code secret, une partie du serveur de fichiers, dossier de la comptabilité compris. La dernière sauvegarde avait été faite onze jours avant : onze jours de travail perdus.

Le réseau aujourd'hui

Constat mesuré sur place, par un balayage du réseau. Un logiciel a interrogé toutes les adresses, une par une. Voici ce qu'il a trouvé :

- Un seul réseau plat, 192.168.0.0/24. Toutes les machines se voient.
- Environ 35 machines actives.
- Le routeur de l'opérateur en 192.168.0.1. Il distribue les adresses de 192.168.0.50 à 192.168.0.250.
- Le serveur de fichiers TV-SRV-FIC en 192.168.0.10. Partage SMB ouvert en lecture et en écriture à tous les postes, dossier de la comptabilité compris.
- Deux switchs de 24 ports non administrables, un par bâtiment.
- Un point d'accès Wi-Fi. Son mot de passe est affiché au mur de l'atelier.

- Aucune documentation. Le prestataire qui a installé le réseau a fermé.

Deux équipements que personne n'a cités en entretien

Adresse	Équipement	Service ouvert	Qui doit décider
192.168.0.201	caméra IP de l'atelier, posée par l'ancien prestataire	flux vidéo non protégé, RTSP, port 554	Hélène Vasseur, la dirigeante : c'est une décision de sécurité, et la loi encadre le fait de filmer des salariés
192.168.0.202	boîtier de télémaintenance de la machine de découpe	Telnet ouvert, port 23, joignable de tout le réseau	le sous-traitant qui entretient la machine : lui seul sait ce qui casse si on le coupe

Ce qui a été dit en entretien. Sophie Lemarchand affirme : « L'atelier n'a pas accès à la compta. »

Ce que demandent les interlocuteurs

Personne	Fonction	Ce qu'elle demande
Hélène Vasseur	Dirigeante	Que les services soient séparés après l'incident. Un accès pour les visiteurs qui ne touche à rien d'interne. Un devis et un délai.
Karim Benali	Responsable d'atelier	Que l'atelier ne s'arrête jamais. Aucune intervention pendant les heures de production.
Sophie Lemarchand	Comptable	Que ses données ne soient plus accessibles à toute l'entreprise.
Yann Ropars	Commercial	Accéder à l'intranet depuis chez les clients.
Ludivine Marchetti	Chargée d'études	Un espace de travail pour les plans, séparé de l'atelier.

La fenêtre d'intervention, ce sont les horaires où l'on a le droit de travailler sur le réseau. C'est après 17 h ou le samedi, jamais pendant les heures de l'atelier.

A2 — Trois architectures pour le même besoin

Source : architectures écrites pour l'exercice. Utilisée dans : LABO étapes 6 à 9.

Les trois architectures servent le même parc : administration, bureau d'études, atelier, serveurs, invités.

Architecture A : le réseau plat, avec un pare-feu en sortie

Un seul réseau interne. Le pare-feu filtre seulement ce qui entre et sort vers Internet. À l'intérieur, tout le monde se voit.

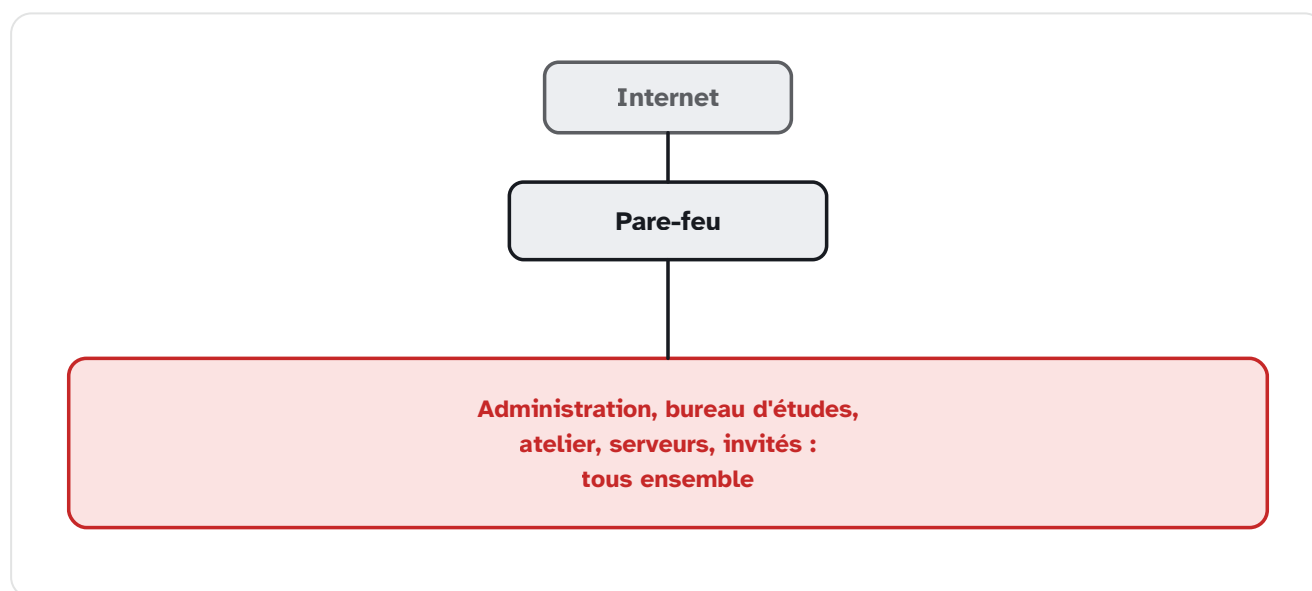


Schéma • Architecture A : le réseau plat, avec un pare-feu en sortie

Architecture B : deux zones, interne et invités

Une zone pour tous les postes et serveurs de l'entreprise. Une zone à part pour les invités.

Les deux zones ne communiquent pas. Chacune sort vers Internet.

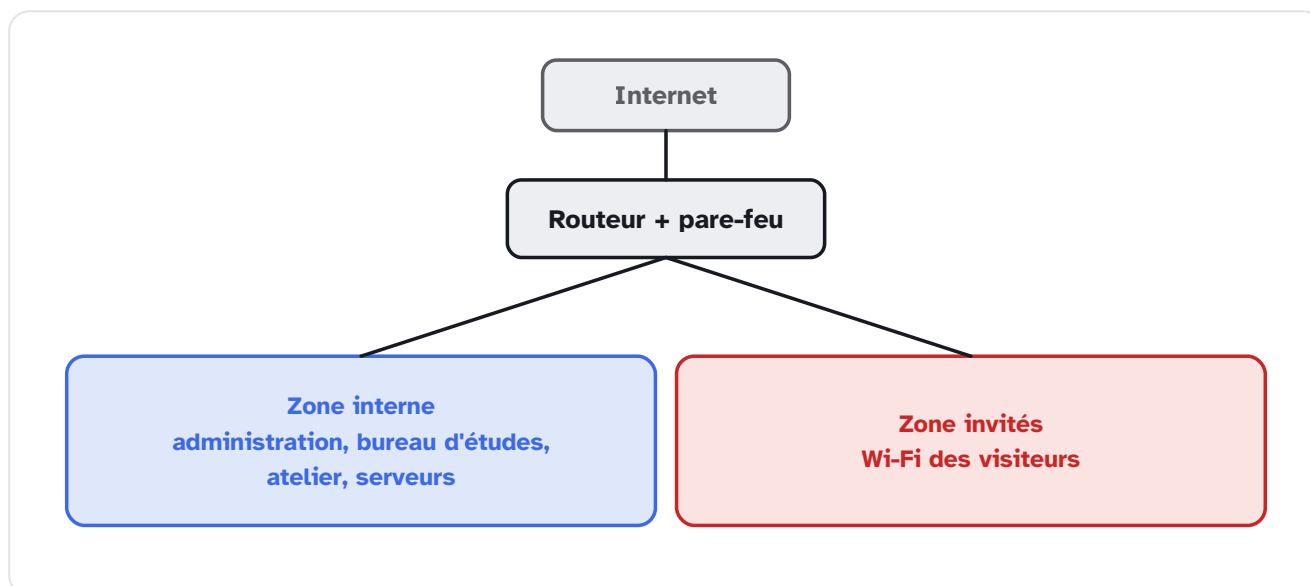


Schéma • Architecture B : deux zones, interne et invités

Architecture C : une zone par service, plus une zone serveurs et une zone invités

Cinq zones. Elles ne communiquent qu'à travers le switch de niveau 3, qui applique des règles.

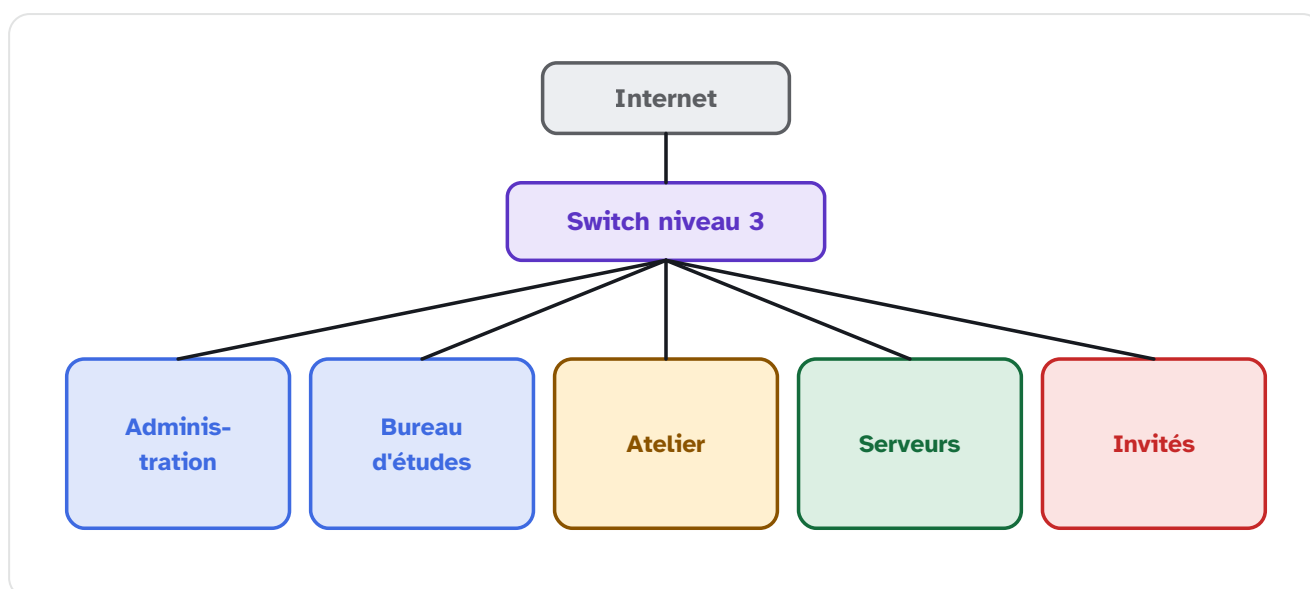


Schéma • Architecture C : une zone par service, plus une zone serveurs et une zone invités

A3 — La grille d'analyse et ses critères

Source : grille écrite pour l'exercice. Utilisée dans : LABO étapes 6 à 8.

Pour chaque architecture, répondez aux cinq critères. Chaque réponse est courte : oui, non, un nombre, ou peu, moyen, beaucoup.

N°	Critère	Ce qu'il faut regarder
1	Une infection de l'atelier atteint-elle la comptabilité ?	L'atelier et l'administration sont-ils dans la même zone ?
2	Un invité atteint-il le serveur de fichiers ?	Les invités et les serveurs sont-ils séparés ?
3	Combien de points de passage entre zones internes ?	Quel équipement voit passer les flux entre deux services ?
4	Peut-on limiter l'atelier à l'intranet et aux fichiers ?	Existe-t-il un endroit où écrire cette règle ?
5	Combien de règles à tenir à jour ?	Plus il y a de zones et de flux, plus il y a de règles.

Rappel pour lire la grille. Une bonne architecture doit d'abord répondre au besoin de sécurité, critères 1, 2 et 4. Le critère 5 dit ce qu'elle coûte à exploiter.