FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Réseau d'entreprise — VLAN & segmentation

Guide VLAN / Segmentation

Concevoir un réseau d'entreprise segmenté : VLAN, ACL, Zero Trust, QoS pour la voix/vidéo, isolation IoT, DMZ, réseau invités. Le passage du réseau plat au réseau structuré.

Scannez pour acceder a la version en ligne

contact@flashmodz.be | +32 471 87 87 07

https://flashmodz.be

FlashModz

L'essentiel en 5 minutes

En 2026, un réseau plat est devenu inacceptable. La segmentation par VLAN est une exigence cyber et réglementaire de base, pas un

1

La segmentation freine la propagation latérale

Un ransomware sur un réseau plat atteint tout ce qui répond au scan. Sur un réseau segmenté avec ACL inter-VLAN, chaque frontière de zone est un obstacle que l'attaquant doit franchir, et chaque tentative laisse des traces. Vous gagnez ce qui compte le plus en incident : du temps pour détecter, isoler et restaurer sélectivement.

2

Le design 6-10 VLANs couvre la quasi-totalité des cas PME

Pas besoin de design exotique. Découpage standard : Users (PC), Servers, Voice (VoIP), IoT (alarme, climatisation, badgeuse), Cameras, Printers, Guest (invités), DMZ (services exposés), Management (admin équipements). Optionnellement : VLAN spécifique production industrielle (OT) ou workloads critiques.

3

Le projet typique est de 4-8 semaines pour 50-200 utilisateurs

Audit (1 semaine) + Design (1 semaine) + Achat matériel (2 semaines) + Bascule (2-4 semaines) + Documentation (continu). Budget matériel + intervention : 15-30 K€ pour cette taille. Ce budget se relativise vite face au coût d'un seul incident sérieux : arrêt de production, restauration, notification, réputation.

4

Le matériel s'amortit sur 5-7 ans

Switches managés UniFi 24 ports à partir de ~250 €, AP Wi-Fi 6 UniFi à partir de ~150 €, firewall tout-en-un (UDM Pro) ~500 €. Chez Meraki, comptez plusieurs fois ces montants, licence annuelle obligatoire en plus, mais avec gestion cloud et support Cisco inclus. Le bon choix dépend du contexte, pas du catalogue. UniFi reste la référence prix/performance en PME.

5

Le Wi-Fi multi-SSID + 802.1X est le pendant essentiel

Un réseau filaire segmenté + Wi-Fi grand public sur tout le bâtiment = travail à moitié fait. Wi-Fi pro avec : SSID employés en WPA3-Enterprise (auth Entra ID/AD) sur VLAN Users, SSID invités captive portal sur VLAN Guest, SSID IoT en PSK sur VLAN IoT. Cohérence d'ensemble.

Et maintenant ?

Les pages qui suivent détaillent chacun de ces points avec exemples, chiffres et actions concrètes.

Document conçu pour PME — Réseau & Segmentation · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

802.1Q

le standard IEEE qui tague chaque trame avec son VLAN : supporté par tout switch managé du marché

Sources : textes officiels (NIS2, RGPD, DORA) et publications des éditeurs cités

Art. 21

de NIS2 : la segmentation réseau fait partie des mesures de gestion des risques attendues

4-8 semaines

durée typique d'un projet de segmentation pour PME 50-200 utilisateurs

15-30 K€

budget typique d'une refonte réseau PME (audit + design + bascule)

Contexte & enjeux

En 2026, le réseau plat est devenu une faute professionnelle. Pourtant, en auditant les réseaux PME en Belgique, on retrouve la même réalité partout : un seul VLAN (souvent VLAN 1 par défaut), une seule plage IP (typiquement 192.168.1.0/24), où cohabitent les PC utilisateurs, les serveurs, les imprimantes, les caméras IP, les téléphones VoIP, les éventuels objets IoT, et parfois même les invités. Aucune isolation, aucun filtrage, aucune segmentation.

Conséquence : quand un poste utilisateur est compromis (ransomware via phishing, par exemple), l'attaquant a accès à TOUT votre réseau. Il peut scanner les serveurs, exploiter une vulnérabilité Active Directory, atteindre les sauvegardes, exfiltrer des données. La propagation latérale d'un ransomware sur un réseau plat est inévitable et rapide. Sur un réseau segmenté, chaque frontière de zone devient un obstacle à franchir : l'attaque ralentit, laisse des traces, et vos équipes gagnent le temps de détecter et de réagir.

La segmentation n'a rien d'abstrait. Techniquement, un VLAN est un tag 802.1Q posé sur les trames Ethernet : un switch managé transporte plusieurs réseaux logiques isolés sur les mêmes câbles, avec des ports "access" (un seul VLAN, pour les équipements) et des ports "trunk" (plusieurs VLANs tagués, entre switches). Le routage inter-VLAN se fait sur un switch L3 ou un firewall, et c'est précisément là qu'on filtre : qui a le droit de parler à qui, sur quel port. Pour une PME wallonne typique, un design fonctionnel comprend 6 à 10 VLANs : utilisateurs, serveurs, voix, IoT, caméras, imprimantes, invités, DMZ, management, et parfois un VLAN spécifique pour les workloads critiques (BDD, AD, sauvegardes).

Ce guide vous donne les principes du design réseau segmenté, les pièges classiques (VLAN purement nominal sans filtrage, oubli de la voix, gestion mal faite des invités), les outils nécessaires (switches

> *"Un réseau plat en 2026, c'est ouvrir grand la porte du coffre-fort. La segmentation n'est pas un luxe : c'est l'hygiène cyber de base, exigée par NIS2."*
>
> — Jérémy Manet, FlashModz Enterprise

Pourquoi votre réseau plat est un danger

Chapitre 2

En 2026, un réseau non segmenté est une cible facile pour ransomware et exfiltration.

Un seul VLAN, toute la surface attaquable depuis n'importe où

Sur un réseau plat, le PC du commercial qui lit ses emails est sur le même réseau que le serveur de fichiers comptables et les sauvegardes. Si ce PC est compromis (phishing > trojan), l'attaquant scanne immédiatement toute la plage 192.168.1.0/24, identifie les serveurs, exploite SMB/NetBIOS/RPC, et chiffre tout, souvent en quelques heures à peine. Le scénario revient dans les rapports d'incident, en Belgique comme ailleurs.

Vos imprimantes et caméras sont des bombes à retardement

Imprimantes, caméras IP, contrôles d'accès, capteurs IoT industriels : ces équipements ont des firmwares rarement patchés, des CVE publiques pendant des années, des passwords par défaut souvent inchangés. Sur un réseau plat, ils sont accessibles depuis n'importe quel PC utilisateur. Cible de choix pour les attaquants : ils prennent le contrôle d'une caméra et l'utilisent comme pivot vers le LAN.

Les invités passent par votre réseau interne

Vos visiteurs (fournisseurs, clients, candidats) demandent souvent le Wi-Fi. Sans VLAN invités dédié, ils se retrouvent sur votre LAN avec accès aux serveurs, partages, imprimantes. Intentionnellement ou non, c'est un risque énorme. Un VLAN invités isolé, avec accès Internet seulement et bande passante limitée, est une mesure d'hygiène basique en 2026.

La voix VoIP n'est pas priorisée : qualité dégradée en heure de pointe

Sans VLAN voix dédié et sans QoS, vos appels téléphoniques se dégradent quand le réseau est chargé (sauvegarde nocturne décalée, gros téléchargement, visioconférence). Hachages, latence, coupures. La VoIP demande une bande passante très faible mais une priorisation forte (QoS DSCP 46). C'est trivial avec un design segmenté.

Aucune visibilité sur le trafic interne

Sur un réseau plat, vous ne pouvez pas savoir qui parle à qui. Sans monitoring (NetFlow, sFlow, IPFIX) ou switches managés, le trafic interne est une boîte noire. Si une exfiltration se prépare, vous ne le voyez pas. La segmentation oblige à passer par des points de contrôle (firewall inter-VLAN), où la supervision devient possible.

Les fournisseurs IoT vous demandent un VLAN dédié, et vous n'en avez pas

Climatisation connectée, badgeuse, alarme, vidéosurveillance, machines industrielles connectées : tous les fournisseurs sérieux demandent en 2026 "un VLAN dédié pour notre matériel". Sans architecture VLAN, vous improvisez ou refusez. Vous accumulez de l'IoT non isolé qui devient ingérable.

Mythes vs Réalité

Chapitre 3

Six idées reçues qui empêchent d'agir — et ce qu'en disent les chiffres.

01

ON ENTEND SOUVENT

On est 30 personnes, pas besoin de VLAN.

EN RÉALITÉ — *Segmentation = pertinente dès 20 users*

À 30 personnes, vous avez probablement 50-80 équipements connectés (PC, smartphones, imprimantes, caméras, alarme, IoT). La segmentation est PERTINENTE dès 20 utilisateurs si vous avez du sensible (cabinet juridique, médical, comptable). À 50+ utilisateurs : c'est obligatoire.

02

ON ENTEND SOUVENT

On a un firewall en bordure, le LAN interne est de confiance.

EN RÉALITÉ — *Defense in depth = firewall + segmentation*

Le firewall en bordure protège du trafic Internet > LAN. Mais une fois qu'un attaquant est entré (phishing, exploit RDP exposé, USB malveillante, BYOD compromis), le firewall ne protège plus. La segmentation interne est la 2e ligne de défense critique.

03

ON ENTEND SOUVENT

On a déjà des VLANs configurés sur les switches.

EN RÉALITÉ — *VLAN sans ACL = VLAN cosmétique*

Avoir des VLANs n'est pas suffisant si TOUS les VLANs peuvent communiquer librement entre eux (ce qui est souvent le cas par défaut sur les routeurs L3). La segmentation efficace = VLAN + ACL inter-VLAN restrictive (whitelist : seuls les flux autorisés passent).

04

ON ENTEND SOUVENT

Le matériel pro coûte une fortune, on garde notre Linksys.

EN RÉALITÉ

UniFi rapport qualité/prix imbattable

Switches managés UniFi : 250-500 € pour 24 ports. AP UniFi Wi-Fi 6 : 150 € l'unité. UDM Pro (firewall + contrôleur tout-en-un) : 500 €. Pour une PME de 50 personnes : ~3-5 K€ de matériel. Cisco Meraki ou Aruba coûtent plusieurs fois plus, mais avec gestion cloud et support. Le vrai "trop cher", c'est l'incident qu'on aurait pu éviter.

05

ON ENTEND SOUVENT

Une refonte réseau va casser les apps métier pendant des semaines.

EN RÉALITÉ

Bascule progressive = pas d'interruption

Avec un plan de bascule par lots et un environnement de test, une refonte se fait sans interruption de service significative. Bascule progressive : un VLAN à la fois, un soir ou un weekend par lot. Avec un rollback prêt à chaque étape, le pire scénario est un retour arrière d'une heure, pas une production à l'arrêt.

06

ON ENTEND SOUVENT

Notre infogérant gère le réseau, on est tranquilles.

EN RÉALITÉ

Tester la maturité réseau de son prestataire

Beaucoup d'infogérants PME ont des compétences réseau modestes (config Linksys de base). Demander : "pouvez-vous me montrer le diagramme VLAN, les ACL inter-VLAN, le plan QoS ?". Si la réponse est embarrassée, c'est qu'il n'y a probablement pas grand chose à montrer.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

Cabinet médical wallon (12 collaborateurs)

Contexte: Réseau plat 192.168.1.0/24. Un seul switch non managé. PC des médecins, PC des secrétaires, dossiers patients sur serveur partagé, caméras IP, imprimante. Aucune segmentation.

Impact: Phishing sur la secrétaire, ransomware, propagation latérale en moins d'une heure. Toute la base patients chiffrée. Sauvegardes externes intactes mais 3 jours d'arrêt pour restauration. Notification APD obligatoire (données santé). Coût total : 35 K€ + atteinte réputation.

Leçon: Pour un cabinet médical (donnée santé = catégorie particulière RGPD), un réseau plat est devenu inacceptable. Refonte post-incident : 3 VLANs (PC, serveurs, imprimantes/caméras), firewall inter-VLAN, segmentation Wi-Fi. 8 K€ de matériel + 4 jours d'intervention.

PME industrielle namuroise (85 collaborateurs)

Contexte: Réseau plat historique. 1 switch L2 non managé, 2 switches plus petits chaînés. WiFi grand public commerce. Atelier production avec 12 machines connectées. Dossier "industrie 4.0" en cours.

Impact: Audit cyber préalable au projet IoT industriel : refonte réseau préalable indispensable. Design 8 VLANs : Bureau (users), Serveurs (AD, fileshare), VoIP, Production (machines), IoT (capteurs), Invités, Caméras, Management. Switches L3 managés, firewall central. Budget 28 K€. Industrie 4.0 lancée en confiance.

Leçon: L'IoT industriel exige une segmentation propre. Tenter d'ajouter de l'OT sur un réseau IT plat est une catastrophe annoncée. La refonte réseau est un préalable, pas une option.

Hôtel de charme bruxellois (40 chambres + 18 employés)

Contexte: Wi-Fi clients (40 chambres) sur le même réseau que la facturation (PMS), la caisse, les caméras de sécurité, les badges des chambres. "Ça a toujours fonctionné comme ça."

Impact: Intrusion via un client malveillant qui scanne le réseau hôtel depuis sa chambre. Accès au PMS, exfiltration des données clients (noms, CB, numéros de chambre), tentative de cryptolocker. Détection précoce mais 2 jours de fonctionnement dégradé. Refonte radicale en 2 semaines : 5 VLANs distincts, contrôleur Wi-Fi pro, isolation client/back-office stricte.

Leçon: Dans l'hôtellerie, la confiance client est primordiale. Un Wi-Fi mutualisé avec le back-office est inacceptable depuis 2018. C'est aussi un sujet RGPD (données CB, données personnelles clients).

Avant / Après — la différence concrète

Chapitre 5

Ce qui change quand on passe d'une posture artisanale à une posture maîtrisée.

	Réseau plat	Réseau segmenté
01 ARCHITECTURE	1 VLAN, 1 plage IP. Toutes les machines se voient.	6-10 VLANs avec rôles distincts. Communications filtrées.
02 PROPAGATION RANSOMWARE	Toute l'entreprise touchée en 30-60 min.	Bloquée aux frontières VLAN. Impact limité.
03 IOT & CAMÉRAS	Sur le même réseau que les PC. Cibles faciles.	VLAN dédié, isolé, ACL spécifiques.
04 WI-FI INVITÉS	Soit pas de Wi-Fi invités, soit Wi-Fi mutualisé avec le LAN.	SSID Guest dédié, VLAN Guest isolé, captive portal.
05 VOIP QUALITÉ	Aléatoire. Hachages en heure de pointe.	VLAN voix dédié, QoS DSCP 46, qualité garantie.
06 VISIBILITÉ TRAFIC	Aucune. Boîte noire.	NetFlow, supervision, dashboard. Visibilité complète.
07 AUDIT CYBER/NIS2	Échec sur la segmentation, mesures à prendre.	Exigence couverte, démontrée par diagramme + configs.

08 ÉVOLUTION

- Nouvelle catégorie d'équipement = chaos ad-hoc.
- Nouveau VLAN ajouté proprement. Architecture extensible.

Auto-évaluation de maturité

Chapitre 6

Faites le point en 5 minutes : où en êtes-vous vraiment ?

Pour chaque question, cochez la case qui correspond le mieux à votre situation actuelle.

SITUATION	NON	PARTIEL	OUI
1. Le réseau est segmenté en au moins 5-6 VLANs distincts (Users, Servers, Voice, IoT, Guest, Management).	☐	☐	☐
2. Les communications inter-VLAN sont filtrées par ACL ou firewall (whitelist).	☐	☐	☐
3. Le Wi-Fi invités est sur un VLAN isolé, sans accès au LAN interne.	☐	☐	☐
4. Les imprimantes, caméras et IoT sont sur des VLANs distincts du VLAN Users.	☐	☐	☐
5. La voix VoIP a un VLAN dédié avec QoS DSCP 46.	☐	☐	☐
6. Le management des équipements (switches, firewall) est sur un VLAN isolé, accessible uniquement depuis l'IT.	☐	☐	☐
7. Les switches sont managés (Ubiquiti, Cisco, Aruba, Mikrotik), pas du matériel non managé.	☐	☐	☐
8. Le firewall a des règles inter-VLAN documentées, revues au moins annuellement.	☐	☐	☐
9. La supervision réseau (SNMP, NetFlow ou équivalent) est en place.	☐	☐	☐
10. Le diagramme physique et logique du réseau est à jour et accessible.	☐	☐	☐
11. Les configurations équipements sont sauvegardées automatiquement.	☐	☐	☐
12. Une procédure de gestion des changements réseau est appliquée.	☐	☐	☐

SCORING : Non = 0 pt • Partiel = 1 pt • Oui = 2 pts

< 40% : Critique • 40-70% : À renforcer • > 70% : Bonne posture

Ce qu'on met en place avec vous

Chapitre 7

Audit, design, bascule progressive, sans interrompre la production.

Audit réseau & cartographie

Inventaire des équipements (switches, AP, firewall), analyse des flux, identification des risques de propagation latérale. Outils : Wireshark, NetFlow, scanners. Livrable : rapport audit + design cible. 5 jours.

Design segmentation cible

Conception de l'architecture VLAN adaptée à votre taille et vos usages. Découpage typique : 6-10 VLANs (Users, Servers, Voice, IoT, Cameras, Printers, Guest, DMZ, Management). Plan d'adressage IP, ACL inter-VLAN, plan de QoS.

Choix du matériel réseau

Recommandation matériel selon votre taille et budget : switches L2/L3 managés (Ubiquiti UniFi, Cisco Meraki, HPE Aruba, Mikrotik), AP Wi-Fi pro, firewall (Fortinet, pfSense, OPNsense, Watchguard, MX Meraki). Cahier des charges achat.

Bascule réseau plat > segmenté

Mise en œuvre progressive (par lots fonctionnels) pour ne pas interrompre la production : configuration équipements, basculement utilisateurs, activation ACL, tests applicatifs. Plan de rollback en cas de problème. Pour 50-200 collaborateurs.

Wi-Fi entreprise multi-VLAN

Conception et déploiement Wi-Fi pro avec : SSID employés sur VLAN Users (auth WPA3-Enterprise/802.1X), SSID invités sur VLAN Guest (captive portal), SSID IoT sur VLAN dédié (PSK fort). Contrôleur (UniFi, Meraki, Aruba) inclus.

QoS voix/vidéo/temps-réel

Mise en place QoS sur les switches et le WAN : marquage DSCP de la voix (46) et vidéo (34), priorisation upstream, queues policing. Garantit la qualité des appels et visios même sous charge.

Supervision réseau (option)

Mise en place supervision : SNMP, NetFlow, syslog centralisé, dashboard (Grafana, PRTG, LibreNMS, contrôleur UniFi/Meraki). Visibilité du trafic, alertes sur anomalies, capacité planning.

Documentation & transfert de compétences

Documentation complète : diagramme physique, diagramme logique L2/L3, plan IP, plan VLAN, ACL inter-VLAN, configurations sauvegardées. Formation IT interne sur l'exploitation. Indispensable pour la pérennité.

Notre façon de travailler

Une méthode en 4 étapes, progressive, pensée pour votre réalité. Pas de slides : des livrables concrets à chaque étape.

1

VOIR CLAIR

AUDIT

On commence par comprendre votre contexte : cartographie de l'existant, entretiens avec les équipes, identification des vrais risques. Pas de diagnostic à distance, pas d'hypothèses. On part de ce qui existe chez vous.

2

PRIORISER ENSEMBLE

PLAN

Qu'est-ce qui est urgent, qu'est-ce qui peut attendre ? On construit le plan avec vous, pas à votre place. Chaque action est pondérée par son impact, son effort et votre budget. Vous gardez la main sur les décisions.

3

STABILISER

ACTION

On corrige, on durcit, on protège. Des actions concrètes et mesurables, livrées par jalons. À chaque étape, vous validez avant qu'on avance. Pas de surprise, pas de dérive budgétaire.

4

TRANSMETTRE

AUTONOMIE

On documente tout ce qu'on fait, on forme vos équipes, on vous laisse les clés. Notre succès se mesure à votre capacité à continuer sans nous. Pas de dépendance, du transfert de compétences.

Feuille de route en phases

Chapitre 8

Un chemin balisé, du diagnostic à la maturité — étape par étape.

1	2	3	4	5
SEMAINE 1	SEMAINE 1-2	SEMAINE 2-4	SEMAINE 4-8	CONTINU
Audit	**Design**	**Achat**	**Bascule**	**Run**
• Inventaire équipements • Cartographie flux • Analyse risques • Architecture cible	• Plan VLAN • Plan IP • ACL inter-VLAN • QoS plan	• Cahier des charges • Sélection matériel • Commande • Réception	• Lab test • Bascule par lots • Validation applicative • Wi-Fi pro	• Supervision • Documentation • Optimisation • Évolution

! **Conseil méthodo**

Chaque phase est un livrable autonome. Vous pouvez vous arrêter à n'importe quelle étape ou ralentir le rythme selon votre budget et votre charge interne. L'important n'est pas la vitesse — c'est de ne pas reculer.

Articulation segmentation / NIS2 / ISO 27001

Chapitre 9

Comment la segmentation devient une exigence réglementaire en 2026.

Mesures techniques de sécurité

NIS2 art. 21

NIS2 exige des mesures techniques proportionnées : segmentation, contrôle des accès, gestion des incidents. Un réseau segmenté avec ACL inter-VLAN coche directement les exigences article 21.

BÉNÉFICE CACHÉ :

Lors d'un audit NIS2, montrer un diagramme VLAN clair et des configurations ACL est un argument concret immédiatement reconnu.

Réduction propagation latérale

NIS2 — gestion incidents

Les inspecteurs NIS2 demandent : "comment limitez-vous la propagation d'un incident ?". La segmentation est la réponse #1, attendue et structurelle.

BÉNÉFICE CACHÉ :

Une PME segmentée réduit son risque NIS2 (et l'amende potentielle) en démontrant proactivement des mesures de réduction d'impact.

Sécurité des réseaux

ISO 27001 A.8.20

Annex A 8.20 (sécurité réseaux) et 8.22 (segregation in networks) sont directement servies par une architecture VLAN propre avec ACL inter-VLAN. Norme reconnue, contrôles vérifiables.

BÉNÉFICE CACHÉ :

Audit ISO 27001 sur le périmètre réseau : démonstration en 30 min par schéma + extraits de configuration.

Sécurité du traitement

RGPD art. 32

RGPD impose des mesures techniques pour protéger les données personnelles. La segmentation réseau, en réduisant la surface d'attaque et en isolant les zones sensibles, est une mesure proportionnée évidente.

BÉNÉFICE CACHÉ :

En cas d'incident, prouver une segmentation propre montre une démarche RGPD active. Réduit l'amende potentielle (proportionnalité art. 83).

Checklist détachable — vos actions prioritaires

Imprimez cette page, cochez au fur et à mesure. Les colonnes EFFORT et IMPACT vous aident à séquencer.

		EFFORT	IMPACT	DÉLAI
☐	Audit du réseau existant : équipements, VLANs, flux, points faibles.	2/5	4/5	2 semaines
☐	Concevoir l'architecture cible : 6-10 VLANs, plan IP, ACL.	3/5	5/5	4 semaines
☐	Choisir le matériel (UniFi vs Meraki vs Aruba selon budget).	2/5	4/5	5 semaines
☐	Acheter et préparer le matériel en lab.	2/5	3/5	7 semaines
☐	Créer un VLAN Guest dédié (premier gain rapide, peu risqué).	2/5	4/5	8 semaines
☐	Isoler les caméras et l'IoT sur des VLANs dédiés.	3/5	5/5	8 semaines
☐	Créer un VLAN Voice avec QoS pour la VoIP.	2/5	4/5	9 semaines
☐	Basculer les utilisateurs vers le VLAN Users dédié.	4/5	5/5	10 semaines
☐	Isoler les serveurs sur le VLAN Servers avec ACL strictes.	4/5	5/5	11 semaines
☐	Mettre en place le Wi-Fi pro multi-SSID + 802.1X pour les employés.	4/5	5/5	12 semaines
☐	Activer la supervision SNMP + NetFlow + dashboard.	3/5	4/5	12 semaines

		EFFORT	IMPACT	DÉLAI
☐	Documenter le réseau : diagrammes physique/logique, plans IP/VLAN, ACL.	●●	●●●●	12 semaines
☐	Formation IT interne sur l'exploitation et le troubleshooting.	●●	●●●	14 semaines

CONSEIL : Commencez par les actions à fort impact ET faible effort (les "quick wins").

Si vous bloquez sur une action, contactez-nous : on vous oriente gratuitement.

Questions fréquentes

Chapitre 10

Les questions que nos clients posent le plus souvent — et nos réponses sans détour.

Q1. Combien de VLANs faut-il pour une PME ?

Découpage type pour 50-200 utilisateurs : 1) Users (PC, smartphones), 2) Servers (AD, fileshare, BDD), 3) Voice (téléphones VoIP), 4) IoT (alarme, badgeuse, capteurs), 5) Cameras (vidéosurveillance), 6) Printers (imprimantes), 7) Guest (invités), 8) Management (admin équipements). Optionnel : 9) DMZ (services exposés), 10) Production (OT industriel). 6-8 VLANs couvrent la quasi-totalité des cas.

Q2. Switches L2 ou L3 ?

Switches L2 si vous avez un firewall qui fait le routage inter-VLAN (typique pfSense, OPNsense, UDM Pro, MX Meraki). Switches L3 si vous voulez router à la couche switch (perf supérieure, ACL distribuées). Pour PME : généralement L2 + firewall central. Pour ETI / multi-sites : L3 distribué.

Q3. Quelles sont les erreurs classiques d'un projet VLAN ?

Toujours les mêmes : 1) des VLANs créés mais un routage inter-VLAN ouvert, donc une segmentation cosmétique. 2) Le VLAN 1 laissé en native VLAN partout, avec le management dessus. 3) Des trunks configurés en mode « tous VLANs » au lieu d'être limités aux VLANs nécessaires. 4) Le DHCP oublié sur les nouveaux VLANs le jour de la bascule. 5) Les imprimantes isolées mais les flux d'impression non autorisés dans les ACL. 6) Le VLAN de management accessible depuis le VLAN Users. 7) Zéro documentation, donc un an plus tard personne n'ose plus toucher aux règles.

Q4. Combien coûte une refonte réseau pour 50 personnes ?

Matériel UniFi (switch L3 24 ports + 4 AP Wi-Fi 6 + UDM Pro) : ~3-4 K€. Matériel Meraki équivalent : ~6-10 K€ + licences ~1 500 €/an. Intervention (audit + design + bascule + doc) : 12-18 K€. Total UniFi : 15-22 K€. Total Meraki : 20-30 K€ initial + 1,5 K€/an.

Q5. Faut-il garder un firewall séparé ou tout-en-un (UDM, MX) ?

Tout-en-un (UDM Pro, MX Meraki) : avantages = simplicité, console unifiée, prix. Inconvénients = single point of failure, fonctionnalités firewall parfois plus limitées. Firewall dédié (Fortinet, pfSense, Watchguard) : meilleure profondeur sécurité, mais 2 consoles à gérer. Pour PME 30-150 users : tout-en-un est généralement le bon choix.

Q6. WPA3-Enterprise vs WPA2-Personal pour le Wi-Fi entreprise ?

WPA3-Enterprise (auth 802.1X via RADIUS, intégré Entra ID/AD) est l'idéal pour le SSID employés : chaque utilisateur s'authentifie avec son compte personnel, pas un PSK partagé. Permet révocation par utilisateur (départ collaborateur), audit individuel. WPA3-Personal (PSK) suffit pour Guest et IoT. WPA2 reste acceptable mais en fin de vie.

Q7. Comment gérer le BYOD (smartphones perso) en VLAN ?

Trois options : 1) BYOD interdit (politique stricte), 2) BYOD sur VLAN Guest (accès Internet seulement, pas LAN), 3) BYOD sur VLAN BYOD dédié avec accès limité aux services cloud (M365, Slack) via firewall, mais pas aux serveurs internes. Option 3 est la plus utilisée en 2026.

Q8. Faut-il chiffrer le trafic interne entre VLANs ?

Pour la majorité des PME, non. Les VLANs sont isolés physiquement (switches managés), le trafic ne sort pas du LAN. Le chiffrement applicatif (HTTPS, SMB encrypted, RDP TLS) protège les flux sensibles. Chiffrement L2 (MACsec) ou L3 (IPsec interne) pertinent pour secteurs très sensibles (défense, secret professionnel niveau APD), pas pour PME standard.

Q9. Comment basculer sans perturbation production ?

Méthodologie en 4 phases : 1) lab + test, 2) bascule des VLANs non critiques d'abord (Guest, IoT, Caméras), là où le risque est faible, 3) bascule du VLAN Users le soir ou le weekend avec retour arrière prévu, 4) bascule des serveurs en dernier (le plus critique). Le plan de rollback documenté à chaque étape est ce qui rend la bascule sereine : au pire, on revient en arrière en une heure.

Glossaire

Chapitre 11

Tous les termes techniques de ce guide, expliqués en français clair.

802.1X

Standard IEEE d'authentification à l'accès réseau, filaire ou Wi-Fi. Chaque utilisateur ou machine s'authentifie auprès d'un serveur RADIUS avant d'obtenir un port ou un SSID. Base du Wi-Fi WPA-Enterprise.

Ansible

Outil d'automatisation IT par Red Hat. Configuration, déploiement et orchestration en playbooks YAML, sans agent. Standard de fait pour automatiser RHEL.

Auto VPN

Technologie Meraki MX qui établit automatiquement des tunnels VPN entre sites avec un clic. Simplifie radicalement le SD-WAN multi-sites.

DMZ

DeMilitarized Zone. Zone réseau intermédiaire entre Internet et le LAN, hébergeant les services exposés (web, mail). Réduit la surface d'attaque sur le LAN.

DPI

Deep Packet Inspection. Analyse du contenu des paquets réseau (pas juste les headers) pour identifier applications, malware, contenus inappropriés.

IdM (Identity Management)

Annuaire d'identités open source intégré à RHEL (basé sur FreeIPA). Gestion centralisée des comptes, certificats, politiques sudo. Alternative AD pour les flottes Linux.

Insights

Service Red Hat (cloud) d'analyse continue de la conformité, sécurité et performance de votre parc RHEL. Recommandations automatisées.

IPS/IDS

Intrusion Prevention/Detection System. Détection (IDS) ou blocage (IPS) en ligne d'attaques connues sur le trafic réseau. Souvent intégré dans firewalls modernes.

Meraki Dashboard

Console cloud Cisco Meraki pour piloter switches (MS), security appliances (MX), AP (MR), caméras (MV). Interface unifiée, configuration centralisée, multi-sites.

NSG / ACL

Network Security Group / Access Control List. Règles de filtrage trafic (source/destination/port/protocole). Pierre de base de toute segmentation réseau.

OpenShift

Plateforme Kubernetes entreprise de Red Hat. Conteneurisation, orchestration, CI/CD, supervision intégrés. Disponible on-prem, cloud, hybride.

PoE / PoE+

Power over Ethernet. Alimentation des AP, caméras, téléphones via le câble réseau. PoE (15W), PoE+ (30W), PoE++ (60-90W). Indispensable en infrastructure pro.

QoS

Quality of Service. Priorisation du trafic réseau (voix > vidéo > data > web) pour garantir l'expérience des apps temps réel sur des liens partagés.

RHEL

Red Hat Enterprise Linux. Distribution Linux entreprise de référence, modèle de souscription avec support 10 ans par version majeure, écosystème complet (Satellite, Insights, IdM, OpenShift).

Rocky Linux / AlmaLinux

Distributions communautaires basées sur RHEL, gratuites, créées après la fin de CentOS Linux 8 en 2021. Compatibilité binaire avec RHEL.

Satellite

Plateforme Red Hat de gestion centralisée de parcs RHEL : patches, déploiements, configurations, conformité, life-cycle. Équivalent Microsoft SCCM pour Linux.

SD-WAN

Software-Defined WAN. Pilotage centralisé du WAN multi-sites avec choix dynamique de chemin (MPLS, fibre, 4G/5G) selon la qualité et l'application.

SELinux

Security-Enhanced Linux. Contrôle d'accès obligatoire intégré au noyau, activé par défaut sur RHEL. Confine chaque processus à ce qu'il a le droit de faire, même si le service est compromis.

SNMP

Simple Network Management Protocol. Standard de supervision des équipements réseau (routeurs, switches, AP). v3 chiffrée recommandée.

UDM Pro

UniFi Dream Machine Pro. Appareil tout-en-un Ubiquiti : router/firewall + contrôleur UniFi + IDS/IPS + VPN. Recommandé pour PME 10-100 utilisateurs.

UniFi OS

OS Ubiquiti pour les contrôleurs UniFi (UDM, Cloud Key) qui héberge les apps UniFi Network, Protect (caméras), Talk (téléphonie), Access (contrôle d'accès).

VLAN

Virtual LAN. Découpage logique d'un réseau physique en plusieurs réseaux isolés (par tag 802.1Q). Permet d'isoler trafic voix/data/IoT/invités sans multiplier les câbles.

Wi-Fi 6 / 6E / 7

Normes Wi-Fi 802.11ax (Wi-Fi 6, 2019), 802.11ax 6GHz (Wi-Fi 6E, 2021), 802.11be (Wi-Fi 7, 2024). Wi-Fi 6E ouvre la bande 6 GHz, Wi-Fi 7 introduit MLO et 320 MHz.

Zero Trust Network

Modèle où aucune connexion n'est implicitement de confiance, même au sein du réseau interne. Vérification continue, micro-segmentation, accès minimal.

Ressources externes

Chapitre 12

Sites officiels, outils gratuits et lectures recommandées pour aller plus loin.

CIS Benchmarks

cisecurity.org/benchmarks

Référentiels gratuits de durcissement pour Cisco IOS, Juniper, RHEL, Ubuntu, Windows, etc. Versions niveau 1 (essentiel) et niveau 2 (avancé).

Red Hat Customer Portal

access.redhat.com

Portail Red Hat : documentation, knowledge base, errata sécurité, support. Accès complet avec souscription RHEL.

Ubiquiti Help Center

help.ui.com

Documentation officielle UniFi : guides d'installation, configurations type, scripts. Communauté très active sur le forum.

Cisco Meraki Documentation

documentation.meraki.com

Documentation officielle Meraki : architecture, déploiements, intégrations. Tutoriels vidéo, best practices, designs de référence.

NIST SP 800-115

csrc.nist.gov/publications/detail/sp/800-115/final

Guide NIST de tests sécurité réseau. Référentiel public pour les pentests et audits réseau.

CCB / CERT.be

ccb.belgium.be

Recommandations CCB sur la sécurité réseau, segmentation, gestion des accès. Alertes CERT.be sur les CVE actives.

Wireshark

wireshark.org

Analyseur réseau de référence, gratuit, open source. Pour diagnostiquer, dépanner, analyser le trafic en profondeur.

Ansible Galaxy

galaxy.ansible.com

Hub communautaire Ansible : milliers de rôles prêts à l'emploi pour déployer RHEL, configurer du réseau, automatiser.

CIS Red Hat Enterprise Linux Benchmark

cisecurity.org/benchmark/red_hat_linux

Référentiel de durcissement RHEL gratuit. Niveau 1 (essentiel) et niveau 2 (avancé). Aligné NIS2/ISO 27001.

BNB / FSMA / CCB ccb.belgium.be

Pour les secteurs régulés en Belgique : alertes spécifiques sur menaces réseau, recommandations sectorielles, partage d'incidents anonymisés.

À propos de FlashModz Enterprise

FlashModz Enterprise est un cabinet d'expertise IT opérationnelle, fondé par Jérémy Manet et basé à Farciennes, dans la région de Charleroi. Conseil et mise en œuvre concrète : sécurité, audit et pentest, automatisation Linux/DevOps et formations — pour les particuliers comme pour les entreprises, en Belgique et à l'international. Notre conviction : les ressources, les connaissances pointues et les outils des grandes entreprises doivent être accessibles aux PME et aux indépendants. À leur échelle. À leur budget. Avec la même rigueur.

CE QUE NOUS FAISONS

- Audit sécurité
- Pentest & rapport
- Sprint de stabilisation
- Team Lead fractionnel
- Formations Linux / DevOps

CERTIFICATIONS & RÉFÉRENTIELS

- CWNA · Ruckus
- Cisco Meraki
- Fortinet NSE
- Veeam
- Jamf · Apple
- OWASP / PTES
- NIS2
- ISO 27001
- RGPD

Jérémy Manet

Fondateur · Ingénieur & architecte système/réseau

Plus de 15 ans en architecture et ingénierie système/réseau : infrastructure, Wi-Fi d'entreprise, sécurité et virtualisation. Également management (people & technique) et gouvernance IT en tant que Process Owner COBIT, DORA et NIS2. Certifié CWNA, Cisco Meraki, Fortinet, Veeam, Jamf, Apple. Technologies : Aruba, HPE, Cisco, FortiGate, Nutanix.

Spécialités : Architecture · Réseau · Wi-Fi · Sécurité · Virtualisation · Gouvernance · NIS2 · DORA

De l’expertise IT pour ce qui compte vraiment.

contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

LinkedIn Facebook TikTok Avis Google

IDENTITÉ LÉGALE

FlashModz Enterprise

DÉNOMINATION	FlashModz Enterprise
FONDATEUR	Jérémy Manet
SIÈGE SOCIAL	Rue du Wainage 18, 6240 Farciennes (Belgique)
BCE / TVA	1035.510.038 · BE 1035.510.038
EU VAT	2.386.268.987
ZONES DESSERVIES	Charleroi et alentours (B2C) · Belgique & international (B2B)
CONTACT	contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

FlashModz

Cadrons votre architecture réseau

Chaque entreprise est unique. Chaque idée a ses contraintes,
son contexte et ses priorités.

C'est pourquoi nous ne proposons pas de grille tarifaire figée.
Nous préférons échanger avec vous, comprendre votre situation
et construire une réponse adaptée à vos vrais besoins.

Parlons de votre situation

EMAIL

contact@flashmodz.be

TELEPHONE

+32 471 87 87 07

WEB

flashmodz.be

RETROUVEZ-NOUS

LinkedIn · Facebook · TikTok · Avis Google

Scannez pour accéder
à ce document

BCE 1035.510.038 | Charleroi · Belgique & international