

Ubiquiti UniFi — Réseau pro pour PME

Guide UniFi / PME

UniFi : choix du contrôleur (Cloud Key, UDM, hébergé), switches L2/L3, AP Wi-Fi 6/6E/7, gestion VLAN, VPN site-à-site, supervision. Excellent rapport qualité-prix pour PME et indépendants.



Scannez pour accéder
à la version en ligne

L'essentiel en 5 minutes

UniFi est devenu le choix par défaut pour les PME en 2026 : matériel pro à prix grand public, écosystème complet, sans abonnement.

1

Un TCO 5 ans nettement inférieur aux écosystèmes à licence

Pour une PME de 50 utilisateurs, comptez de l'ordre de 8-12 K€ sur 5 ans en UniFi (matériel + intervention + remplacement), sans aucune licence récurrente. Un équivalent Meraki se chiffre en dizaines de milliers d'euros une fois les licences annuelles obligatoires additionnées. L'écart vient surtout de là : pas d'abonnement.

2

L'écosystème dépasse le réseau

UniFi Network (LAN/Wi-Fi) + Protect (caméras IP) + Access (contrôle d'accès physique) + Talk (téléphonie) sont pilotés depuis la même console. Pour une PME, c'est une simplification opérationnelle majeure (1 outil au lieu de 4).

3

Wi-Fi 6/6E/7 démocratisé

Des AP UniFi entre 150 et 300 € mettent le Wi-Fi moderne à portée de toutes les PME. Sur le papier, débits et fonctionnalités radio rivalisent avec des AP entreprise vendus plusieurs fois plus cher. Ce que les gammes entreprise gardent : l'outillage RF avancé, le support constructeur, certaines intégrations. Pour un bureau PME classique, la différence ne se voit pas.

4

Auto-VPN simplifie le multi-sites

Site Magic (UniFi) ou Auto VPN (Meraki) configurent les tunnels VPN entre sites en 1 clic. Pour PME 2-10 sites : différence majeure vs IPsec manuel. UniFi propose Site Magic gratuit ; Meraki Auto VPN demande la licence Meraki.

5

Limites à connaître : support, SD-WAN avancé

Support Ubiquiti = essentiellement communautaire (forum très actif), pas de SLA contractuel. Pour une PME standard, suffisant. Pour secteurs critiques 24/7 : ajouter un partenaire UniFi pro avec engagement de service. Et le SD-WAN UniFi reste basique face à Meraki (pas de pilotage par application aussi fin).

Et maintenant ?

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

Document conçu pour PME — Ubiquiti UniFi · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

1	Chiffres clés & contexte	4
	Le panorama actuel en Belgique	
2	Menaces & risques	6
	Les vraies menaces, documentées	
3	Mythes vs Réalité	8
	Les idées reçues déconstruites	
4	Cas concrets	10
	Trois scénarios types en Belgique	
5	Avant / Après	11
	Ce qui change concrètement	
6	Auto-évaluation	13
	Où en êtes-vous vraiment ?	
7	Services & accompagnement	14
	Ce que l'on met en place pour vous	
8	Feuille de route	17
	Du diagnostic à la maturité	
9	Cadre réglementaire	18
	Obligations oubliées & bénéfices cachés	
10	Checklist actions	20
	Vos actions prioritaires (page détachable)	
11	Questions fréquentes	21
	Les questions qu'on nous pose le plus	
12	Glossaire	23
	Tous les termes techniques expliqués	
13	Ressources externes	26
	Pour aller plus loin	
14	À propos	29
	FlashModz Enterprise & Jérémy Manet	

Le marché belge en chiffres

Chapitre 1

0 €

de licence obligatoire : contrôleur inclus, auto-hébergeable,
mises à jour gratuites

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

2005

création d'Ubiquiti ; entreprise cotée au
NYSE depuis 2011

~200 €

prix public d'un AP Wi-Fi 6 professionnel
UniFi (U6 Pro), sans frais récurrents

2-4 semaines

durée typique de déploiement complet pour
PME 50-100 collaborateurs

Contexte & enjeux

Ubiquiti UniFi a profondément transformé le marché du réseau professionnel pour PME. Avant, un réseau pro signifiait Cisco Catalyst ou HPE Aruba, chers et complexes, ou alors du Linksys/Netgear qui n'a de pro que l'étiquette. Ubiquiti a comblé ce vide : du matériel professionnel à une fraction du prix, un contrôleur unifié pour tout l'écosystème, et surtout aucune licence obligatoire.

Concrètement, UniFi propose une gamme complète : switches L2 et L3 managés, AP Wi-Fi 6/6E/7, gateway/firewall (UDR, UDM, UDM Pro, UDM SE, UXG), caméras IP (Protect), contrôle d'accès (Access), téléphonie (Talk). Le tout piloté depuis une console unique, hébergée au choix sur un équipement dédié (Cloud Key Gen2+, UDM), auto-hébergée (UniFi Network Application sur Linux ou Docker) ou via l'offre d'hébergement cloud officielle d'Ubiquiti. Vous choisissez où vivent vos données de management.

Avantages : prix sans équivalent à ce niveau de fonctionnalités (UDM Pro ~500 €, AP Wi-Fi 6 dès ~150 €), VLAN, RADIUS/802.1X, VPN, IDS/IPS et VPN inter-sites inclus, interface soignée, mises à jour gratuites, communauté énorme. Limites, et il faut les dire : support constructeur essentiellement communautaire, sans SLA contractuel ; pas de remplacement matériel J+1 garanti ; des mises à jour majeures qui méritent un passage en lab avant la production ; haute disponibilité firewall limitée face aux gammes entreprise.

Pour la grande majorité des PME (5 à 200 collaborateurs, mono-site ou quelques sites simples), UniFi est le choix rationnel en 2026 : le coût total sur 5 ans est nettement inférieur aux écosystèmes à licence, essentiellement parce qu'il n'y a pas de licence. Si vous êtes en secteur très critique (banque, santé) ou en multi-sites complexe avec SD-WAN avancé, Cisco Meraki ou Aruba restent pertinents. Ce guide vous

"

"UniFi a démocratisé le réseau professionnel pour les PME. Pour la plupart d'entre elles, c'est le choix rationnel : des fonctions de niveau entreprise au prix du grand public, sans abonnement."

— Jérémy Manet, FlashModz Enterprise

Pourquoi UniFi s'est imposé sur le segment PME

Chapitre 2

Un rapport qualité/prix qui a changé la donne du réseau professionnel.



Vous payez trop cher pour Cisco ou HPE Aruba

Beaucoup de PME ont hérité d'un parc Cisco Catalyst ou Aruba acheté il y a 5-8 ans. À renouvellement, le devis Cisco/Aruba équivalent est plusieurs fois plus cher qu'UniFi, sans bénéfice fonctionnel proportionnel pour vos usages PME. C'est le moment de challenger.



Votre matériel grand public ne tient pas la charge

Linksys, Netgear, TP-Link grand public sur 30+ utilisateurs : Wi-Fi qui décroche, switches qui buffer overflow, fonctionnalités VLAN incomplètes ou bugées, pas de contrôleur centralisé. UniFi fournit le saut qualitatif vers le pro pour un budget juste au-dessus du grand public.



Vous voulez du Wi-Fi 6/6E/7 sans abonnement

Le Wi-Fi 6 s'est généralisé, le Wi-Fi 7 arrive dans les PME. Chez les acteurs à licence, chaque AP coûte cher à l'achat et impose un abonnement annuel pour rester géré. Un U7 Pro UniFi coûte de l'ordre de 200-300 € et ne coûtera plus rien ensuite. Sur un parc de 8 AP et 5 ans, l'écart se chiffre en milliers d'euros.



Vous voulez piloter caméras + Wi-Fi + LAN dans une console unique

UniFi Protect (caméras), UniFi Network (Wi-Fi/LAN), UniFi Access (contrôle physique), UniFi Talk (téléphonie) sont pilotés depuis une seule console. Pour une PME qui cherche la simplicité opérationnelle, c'est précieux. Compétiteur direct : Cisco Meraki, nettement plus cher une fois les licences comptées.



Vos sites distants sont mal connectés

Sans Auto-VPN UniFi (ou Auto VPN Meraki), connecter plusieurs sites en VPN demande de la configuration manuelle (IPsec point-à-point), du tuning, de la maintenance. UniFi Auto-VPN configure les tunnels en 1 clic entre sites UniFi (Site Magic). SD-WAN simplifié pour PME multi-sites.



Votre infogérant vous facture la "config réseau" très cher

Le coût de configuration de switches Cisco/Aruba est élevé (compétences spécifiques, interfaces CLI complexes). UniFi a une courbe d'apprentissage bien plus courte : un IT généraliste se forme en quelques jours et configure un réseau complet. Économie durable sur la facture infogérant.

Mythes vs Réalité

Chapitre 3

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

01

ON ENTEND SOUVENT

Ubiquiti c'est pour les particuliers passionnés, pas pour l'entreprise.

EN RÉALITÉ

UniFi = gamme pro Ubiquiti

Ubiquiti vend du matériel professionnel depuis les années 2000, d'abord pour les opérateurs sans fil, puis en entreprise avec UniFi. Le segment "amateur éclairé" existe (AmpliFi) mais UniFi est bien la gamme professionnelle, déployée dans des entreprises, hôtels, écoles et chez des FAI partout dans le monde.

02

ON ENTEND SOUVENT

Cisco reste le standard pro, UniFi est un compromis.

EN RÉALITÉ

Le contexte décide, pas la marque

Cisco reste leader entreprise grand compte, oui. Mais pour la plupart des PME (50-200 utilisateurs, 1-5 sites), UniFi atteint les mêmes objectifs fonctionnels pour une fraction du budget. La supériorité Cisco se mesure sur des cas spécifiques (multi-sites complexes, 24/7 critique), pas en absolu.

03

ON ENTEND SOUVENT

Sans support pro, on est seuls en cas de problème.

EN RÉALITÉ

Partenaire UniFi pro = SLA possible

Support Ubiquiti = forum communautaire très actif (réponses qualité en heures), tickets directs sur problèmes hardware (RMA). Pour SLA strict : passer par un partenaire UniFi pro qui contractualise un engagement de service. Pour PME standard, c'est suffisant en pratique.

04

ON ENTEND SOUVENT

Les MAJ UniFi sont régulièrement cassantes.

EN RÉALITÉ*Lab + tests = pas de surprise*

Les MAJ majeures UniFi ont eu des bugs en 2018-2020 (rare aujourd'hui). Depuis 2022, qualité fortement améliorée. Best practice : tester les MAJ en lab 1-2 semaines avant prod, garder un firmware N-1 stable. Comme avec tout vendor (y compris Cisco).

05

ON ENTEND SOUVENT

UniFi manque des fonctionnalités pro essentielles.

EN RÉALITÉ*L'essentiel des fonctions pro est là*

UniFi propose : VLAN, ACL, RADIUS, 802.1X, IDS/IPS, VPN, VPN inter-sites, QoS, multi-WAN, IPv6, routage dynamique sur les gateways récentes, syslog, SNMP, captive portal, RBAC, audit logs. L'essentiel des fonctions attendues en PME y est. Manquent : SD-WAN très avancé, micro-segmentation cloud-managed, certaines intégrations entreprise très spécifiques.

06

ON ENTEND SOUVENT

Pas de haute dispo, on est cuit en cas de panne.

EN RÉALITÉ*HA limitée mais souvent suffisante*

UniFi propose : redondance switches (LAG), Wi-Fi roaming entre AP, multi-WAN avec failover (UDM Pro), réplication des configs vers le cloud Ubiquiti. Pour HA firewall actif/actif : limité (vs Meraki Warm Spare). Pour PME standard : pas un sujet bloquant.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

Cabinet d'architecture wallon (40 collab, 2 sites)

- Contexte:** Cisco Catalyst 2960 + Linksys WiFi en fin de vie. Devis Cisco renouvellement : 18 K€. Devis HPE Aruba : 14 K€. Recherche d'alternative.
- Impact:** Architecture UniFi : 2 UDM Pro (1 par site), 4 switches L3 (USW Pro 24 PoE), 6 AP Wi-Fi 6 (U6-LR), Auto-VPN entre sites, VLAN Users/Servers/Voice/Guest. Matériel total : 5 200 €. Intervention 6 jours : 5 400 €. Budget total 10,6 K€ vs 18 K€ Cisco. Économie 7,4 K€.
- Leçon:** Pour un cabinet PME multi-sites, l'écart UniFi vs Cisco se mesure en milliers d'euros à fonctionnalités équivalentes, pas en pourcentage marginal. Faites chiffrer les deux avant de signer.

PME industrielle namuroise (90 collab, 1 site)

- Contexte:** Mix Linksys/Netgear pas managé. Wi-Fi qui décroche en heure de pointe. Pas de VLAN. Atelier production avec 15 IoT machines.
- Impact:** Refonte UniFi complète : 1 UDM Pro, 3 switches L3 (USW Pro 24 PoE + USW 16), 6 AP Wi-Fi 6 (U6-LR), 8 VLANs (Users, Servers, Voice, Production OT, IoT, Cameras, Guest, Mgmt). Budget matériel : 4 800 €. Intervention 8 jours : 7 200 €. Total 12 K€. Wi-Fi stable, segmentation propre.
- Leçon:** UniFi est devenu suffisamment mature pour gérer de l'industriel léger. Pour de l'industriel critique avec exigences temps réel strictes, les gammes durcies type Cisco IE restent pertinentes. Mais pour l'atelier connecté d'une PME, UniFi tient la route.

École privée bruxelloise (300 élèves, 50 profs)

- Contexte:** Wi-Fi grand public 8 routeurs en parallèle, ingérable. Pas de SSID dédié élèves vs profs. Filtrage contenu inexistant.
- Impact:** Architecture UniFi : 1 UDM Pro avec IDS/IPS, 4 switches PoE (USW Pro 24), 12 AP Wi-Fi 6 mesh (U6-Pro), VLAN Élèves / Profs / Admin / Invités, captive portal pour les invités. Filtrage DNS via NextDNS sur le VLAN Élèves. Budget matériel : 8 500 €. Total projet 18 K€.
- Leçon:** Pour une école, UniFi offre l'écosystème complet (réseau + caméras Protect + contrôle accès Access) à un budget compatible avec le secteur éducatif. Un équivalent Meraki aurait coûté plusieurs fois plus, licences annuelles comprises.

Avant / Après — la différence concrète

Chapitre 5

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

**UniFi pour PME 50 collab****Cisco Meraki pour PME 50 collab**

01 MATÉRIEL TOTAL (YEAR 1)

● ~3-5 K€ (UDM Pro + 2 switches + 4 AP)

● ~10-15 K€ (MX67 + MS120 + MR36)

02 LICENCES ANNUELLES

● 0 € (sauf cloud hosting optionnel ~10€/mois)

● ~1 500-3 000 €/an (obligatoires)

03 TCO 5 ANS

● ~8-12 K€ (matériel + intervention)

● ~25-40 K€ (matériel + licences + intervention)

04 SUPPORT

● Communautaire + RMA hardware. Partenaire UniFi pro pour SLA.

● Support Cisco direct 24/7 inclus avec licence.

05 MAJ FIRMWARE

● Auto, généralement stables. Lab recommandé.

● Auto, très stables (gérées en cloud).

06 MULTI-SITES

● Site Magic gratuit, simple à utiliser.

● Auto VPN, plus mature en SD-WAN avancé.

07 WI-FI 7

● Disponible (U7 Pro Max ~250 €).

● Disponible (gamme CW, nettement plus chère, licence en plus).

08 **CONSOLE**

- | | |
|--|--|
| <ul style="list-style-type: none">● Web UI moderne, mobile app native. | <ul style="list-style-type: none">● Web dashboard cloud (inégalé). |
|--|--|

09 **CAS D'USAGE IDÉAL**

- | | |
|--|---|
| <ul style="list-style-type: none">● PME 5-200 collab, 1-5 sites, budget contraint. | <ul style="list-style-type: none">● PME 50-500 collab, 5-50 sites, secteur critique 24/7. |
|--|---|

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 contrôleur UniFi (UDM Pro, Cloud Key ou auto-hébergé) est sécurisé : MFA admin, IP whitelist, MAJ régulières.	☐	☐	☐
2. Tous les équipements UniFi sont à jour (firmware stable testé en lab).	☐	☐	☐
3. La configuration est sauvegardée automatiquement (cloud UI Ubiquiti ou export local).	☐	☐	☐
4. Le Wi-Fi entreprise utilise WPA3-Enterprise (802.1X) ou au minimum WPA3-Personal pour les PSK.	☐	☐	☐
5. Au moins 5-6 VLANs sont configurés (Users, Servers, Voice, IoT, Guest, Mgmt).	☐	☐	☐
6. Les ACL inter-VLAN sont configurées sur le UDM/UDR (whitelist).	☐	☐	☐
7. IDS/IPS est activé sur le UDM Pro (latency vérifiée acceptable).	☐	☐	☐
8. Les logs syslog sont envoyés vers un serveur centralisé (ou conservés localement).	☐	☐	☐
9. Si multi-sites : Site Magic / Auto-VPN configuré et testé.	☐	☐	☐
10. Le Wi-Fi est dimensionné correctement : 1 AP par 25-30 utilisateurs Wi-Fi 6 (ou 1/40 en 6E).	☐	☐	☐
11. Le budget PoE est dimensionné (switches PoE+ selon AP et caméras ; attention, l'UDM Pro n'a pas de ports PoE, contrairement à l'UDM SE).	☐	☐	☐
12. La documentation topologie UniFi est à jour (export Network plan).	☐	☐	☐

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

Cadrage, déploiement et exploitation. Avec ou sans contrôleur cloud.

Cadrage architecture UniFi

Analyse de votre contexte (taille, sites, exigences), design UniFi cible, choix du matériel (gateway, switches, AP, caméras éventuelles). Livrable : architecture, BOM matériel, budget total. 3 jours.

Déploiement réseau UniFi

Installation et configuration du contrôleur (UDM Pro, Cloud Key, ou auto-hébergé), des switches L2/L3, des AP Wi-Fi, des VLANs, des ACL inter-VLAN, du Wi-Fi multi-SSID. Pour 30-150 collaborateurs.

Wi-Fi pro multi-SSID + 802.1X

Configuration Wi-Fi entreprise : SSID Employés en WPA3-Enterprise (auth via RADIUS, intégration Active Directory ou Entra ID), SSID Guest avec captive portal, SSID IoT en WPA3-PSK fort. AP Wi-Fi 6 ou 6E/7 selon besoins.

Multi-sites avec Auto-VPN (Site Magic)

Pour plusieurs sites UniFi : configuration des tunnels VPN automatiques entre sites avec routage cohérent, failover internet, priorisation. Idéal PME multi-agences (2-10 sites).

Intégration UniFi Protect (caméras)

Si remplacement parc caméras : déploiement UniFi Protect (NVR intégré au UDM Pro ou NVR dédié, caméras G4/G5), enregistrement local, accès distant sécurisé, RGPD-compliant.

Migration depuis Cisco/Aruba/Netgear

Migration progressive depuis un parc existant vers UniFi. Phase de cohabitation pour limiter le risque, bascule par lots, validation applicative. Plan de rollback systématique.

Supervision & alerting

Configuration des alertes UniFi : équipements offline, Wi-Fi dégradé, anomalies trafic. Intégration syslog vers SIEM si besoin. Dashboard sur mesure (Grafana possible).

Run & accompagnement (option mensuelle)

Veille sur les MAJ UniFi (parfois cassantes, à valider en lab), intervention sur incidents, ajustements de configuration, formation IT continue. Forfait 1-2 jours/mois.

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.



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 UniFi avec NIS2, ISO 27001

Chapitre 9

UniFi peut-il atteindre les exigences entreprise ? Ce qui marche, ce qui demande de l'attention.

UniFi peut-il atteindre NIS2 ?

NIS2 art. 21

UniFi fournit techniquement tout le nécessaire : VLANs, ACL, IDS/IPS, audit logs, RADIUS, supervision. Le défi est plutôt opérationnel : maintenir la rigueur de configuration et la documentation au niveau attendu par NIS2.

BÉNÉFICE CACHÉ :

Une PME UniFi correctement configurée et documentée passe les audits NIS2 sans difficulté. Le coût matériel n'est pas un critère d'audit.

Conformité ISO/RGPD avec UniFi

ISO 27001 / RGPD

L'audit ISO 27001 ou RGPD ne juge pas la marque, mais le résultat : segmentation, contrôle des accès, chiffrement des flux sensibles, audit logs. UniFi atteint ces exigences techniquement.

BÉNÉFICE CACHÉ :

Aucun frein réglementaire à utiliser UniFi en PME de 50-200 utilisateurs. Les vrais sujets restent organisationnels : politiques, formation, gouvernance.

Quand préférer Cisco Meraki

Limites entreprise

Cisco Meraki ou Aruba restent pertinents si : (1) > 10 sites avec SD-WAN avancé requis, (2) secteur critique exigeant SLA support strict (banque tier-1, hôpital), (3) déjà standardisé sur Cisco/Aruba en groupe, (4) besoin de fonctionnalités entreprise très spécifiques (DPI L7 fin, micro-segmentation cloud-managed).

BÉNÉFICE CACHÉ :

Pas de honte à choisir Cisco Meraki pour un cas où c'est justifié. Mais pour la grande majorité des PME, UniFi est le choix rationnel.

Hardening UniFi

CIS Benchmarks

CIS publie un Benchmark générique réseau qui s'applique à UniFi : changement passwords par défaut, désactivation services inutilisés (Telnet, SNMP v1/v2c, HTTP), TLS pour toute admin, journalisation centralisée.

BÉNÉFICE CACHÉ :

Une configuration UniFi durcie selon CIS répond aux mêmes exigences qu'un Cisco Catalyst durci. Le sujet n'est pas la marque, c'est la rigueur de configuration.

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 |
|--|--|--|-------------|
| ☐ Évaluer votre parc actuel et le besoin de remplacement. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 2 semaines |
| ☐ Choisir l'architecture UniFi cible (gateway, switches, AP, contrôleur). | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 3 semaines |
| ☐ Établir le BOM matériel et le budget total. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 3 semaines |
| ☐ Identifier un partenaire UniFi pro pour l'intégration et le run. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 4 semaines |
| ☐ Commander le matériel (délai 2-6 semaines selon modèles). | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 4 semaines |
| ☐ Configuration initiale en lab : valider tous les flux applicatifs. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 6 semaines |
| ☐ Bascule par lots : commencer par le moins critique (Guest, IoT, Caméras). | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 8 semaines |
| ☐ Configurer Wi-Fi multi-SSID + 802.1X RADIUS pour les employés. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 9 semaines |
| ☐ Mettre en place les VLANs et ACL inter-VLAN. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 9 semaines |
| ☐ Activer IDS/IPS sur le UDM Pro. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 10 semaines |
| ☐ Si multi-sites : configurer Site Magic / Auto-VPN. | <div><div></div><div></div><div></div><div></div><div></div></div> | <div><div></div><div></div><div></div><div></div><div></div></div> | 11 semaines |



Activer la supervision et les alertes critiques.

EFFORT



IMPACT



DÉLAI

10 semaines



Documenter la topologie UniFi et les configurations.

EFFORT



IMPACT



DÉLAI

12 semaines



Tester les MAJ firmware en lab avant rollout production.

EFFORT



IMPACT



DÉLAI

Continu

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. Quelle gateway choisir : UDM, UDR, UDM Pro, UDM SE ?

UDR (Dream Router, ~250 €) : compact, avec PoE, idéal indépendant ou TPE. UDM Pro (~500 €) : 8 ports + 2× SFP+, IDS/IPS, NVR Protect intégré, recommandé PME 30-100 ; attention, pas de ports PoE. UDM SE (~600 €) : même base avec ports PoE intégrés et plus de stockage pour Protect, pour PME 100+ ou parc caméras. UXG (~selon modèle) : gateway pure, sans contrôleur, pour les installations avec contrôleur dédié ou auto-hébergé.

Q2. Combien d'AP Wi-Fi pour combien d'utilisateurs ?

Wi-Fi 6 (U6-Lite/LR/Pro) : 1 AP couvre 25-30 utilisateurs simultanés en usage standard. Wi-Fi 6E (U6-Enterprise) : 1 AP couvre 35-40 utilisateurs. Wi-Fi 7 (U7 Pro/Max) : 1 AP couvre 50+ utilisateurs. Pour 50 collab : 2-3 AP Wi-Fi 6 ou 2 AP Wi-Fi 6E. Pour 100 collab : 4-5 AP Wi-Fi 6 ou 3-4 AP Wi-Fi 6E.

Q3. Auto-hébergé ou Cloud Key ou UDM ?

UDM/UDM Pro : tout-en-un, simple, recommandé PME standard. Cloud Key Gen2+ : contrôleur dédié si vous avez déjà un firewall non-UniFi. Auto-hébergé Linux : si vous avez la compétence Linux et voulez la flexibilité maximale (UniFi Network App sur Linux ou Docker). Hébergement cloud officiel Ubiquiti (payant) : si vous voulez une console externe gérée par le constructeur.

Q4. UniFi vs Cisco Meraki : critères de choix ?

UniFi si : budget contraint, < 200 collab, < 10 sites, IT généraliste capable de monter en compétence, secteur non critique 24/7. Meraki si : budget OK, > 100 collab + multi-sites, secteur critique, exigence support 24/7 SLA, déjà standardisé Cisco en groupe. Pour la plupart des PME, UniFi est le bon choix.

Q5. Faut-il un partenaire UniFi pro ?

Pour le déploiement initial : OUI, sauf si vous avez une compétence réseau interne. Le partenaire pro apporte expertise, choix matériel, méthodologie déploiement, suivi. Pour le run : option ou en interne selon compétence. Pour secteur critique : indispensable (SLA contractualisé).

Q6. Combien de temps pour un déploiement UniFi ?

50 collab mono-site : 4-6 jours intervention (1 IT pro). 100 collab : 8-12 jours. 200 collab multi-sites : 15-20 jours. Le facteur principal n'est pas la taille mais : (1) qualité de la cartographie existante, (2) complexité applicative (apps métier sensibles aux changements réseau), (3) fenêtres de bascule disponibles.

Q7. UniFi Protect (caméras) : pertinent ?

Excellent rapport qualité/prix pour la vidéosurveillance interne PME. Caméras G4/G5 robustes, NVR intégré au UDM Pro (suffisant pour 10-15 caméras) ou NVR dédié (UNVR/UNVR Pro pour 15-50 caméras). Console intégrée à UniFi Network. Limites : moins d'analytique vidéo embarquée que les acteurs spécialisés haut de gamme, et les fonctions IA les plus poussées demandent du matériel dédié supplémentaire.

Q8. Et le support 24/7 si on est en PME critique ?

Solution : passer par un partenaire UniFi pro qui contractualise un SLA (intervention en heures ouvrées ou 24/7 selon contrat). Coût : 200-800 €/mois selon profondeur. C'est l'équivalent d'un contrat de support Cisco mais via un intégrateur, pas le constructeur.

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. Confiner 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 / CCBccb.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



Cadrons votre projet UniFi

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