FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Cisco Meraki — Réseau managé dans le cloud

Guide Meraki / Multi-sites

Cisco Meraki pour les organisations multi-sites : MX (sécurité), MS (switching), MR (Wi-Fi), MV (caméras). Modèle de licence, dashboard cloud, SD-WAN, supervision centralisée.

Scannez pour acceder a la version en ligne

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

https://flashmodz.be

L'essentiel en 5 minutes

Cisco Meraki est l'écosystème de référence pour le multi-sites distribué. Pertinent à 5+ sites ou en secteur critique. Cher mais justifié da

1 Le bon choix dépend du nombre de sites et de la criticité

Meraki devient pertinent à 5-8 sites. En dessous, UniFi (Site Magic) ou pfSense + Auto VPN suffisent à 1/4 du prix. Au-dessus, ou en secteur 24/7 critique, le différentiel coût Meraki se justifie par le SD-WAN avancé, le dashboard, et le SLA Cisco.

2 Le SD-WAN Meraki est une vraie révolution multi-sites

Auto VPN, sélection de chemin automatique et optimisation dynamique remplacent avantageusement les MPLS coûteux. Pour 8-30 sites : facture WAN en forte baisse, meilleure disponibilité grâce au multi-WAN, et nouveaux sites déployés en quelques jours au lieu de quelques semaines.

3 Les licences obligatoires sont la clé du modèle

Chaque équipement Meraki exige une licence annuelle, facturée selon le modèle et la suite choisie. Si elle expire, l'équipement cesse de fonctionner après 30 jours de grâce. C'est un modèle SaaS strict. Avantage : MAJ + support 24/7 inclus, dashboard constamment amélioré. Inconvénient : pas de "matériel libre", jamais.

4 Le dashboard Meraki est un avantage concurrentiel reconnu

L'ergonomie du dashboard fait référence sur le marché du cloud-managed : recherche puissante, troubleshooting visuel, MAJ automatiques, API complète. Pour une équipe IT qui gère du multi-sites au quotidien, c'est un vrai différenciateur, pas un argument marketing.

5 L'écosystème Cisco étend les possibilités

Meraki s'intègre avec : Cisco Umbrella (sécurité DNS), ThousandEyes (visibilité Internet, racheté par Cisco en 2020), Cisco XDR, Cisco Secure Firewall. Pour une organisation qui veut une stack Cisco cohérente, c'est déterminant.

Et maintenant ?

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

Document conçu pour PME / ETI multi-sites — Cisco Meraki · 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

2012

rachat de Meraki par Cisco, pour environ 1,2 milliard de dollars

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

100%

du matériel Meraki exige une licence active : sans elle, l'équipement cesse de fonctionner

30 jours

de délai de grâce après expiration de licence, avant l'arrêt des équipements

Zero-touch

déploiement : le site distant branche le boîtier, la configuration descend du cloud

Contexte & enjeux

Cisco Meraki s'est imposé comme la référence du réseau cloud-managed pour les organisations multi-sites. Racheté par Cisco en 2012, Meraki a apporté au groupe ce qui lui manquait : une expérience cloud unifiée, simple à exploiter, taillée pour les organisations distribuées (retail, finance, hôtellerie, santé, services publics).

Concrètement, Meraki c'est : MX (security appliance, firewall + SD-WAN), MS (switches managés cloud), MR (AP Wi-Fi enterprise), MV (caméras IP), MT (capteurs environnementaux). Tout se pilote depuis le **Meraki Dashboard**, une console cloud dont l'ergonomie fait référence dans l'industrie.

Forces de Meraki : SD-WAN Auto VPN d'une simplicité remarquable (tunnels multi-sites en quelques minutes), dashboard cloud très soigné, déploiement zero-touch (le site distant reçoit le boîtier, le branche, la configuration descend du cloud), mises à jour automatiques, support Cisco 24/7 inclus dans la licence, SD-WAN avancé (sélection de chemin par application, optimisation dynamique), grande base installée multi-sites.

Limites, à connaître avant de signer : chaque équipement exige une licence active. Si elle expire, l'équipement cesse de fonctionner après un délai de grâce de 30 jours. Pas de licence, pas de réseau : c'est un modèle d'abonnement strict, assumé par Cisco, à budgéter en pluriannuel. Le coût total (matériel + licences) est plusieurs fois supérieur à un équivalent UniFi en mono-site. Et la dépendance au cloud est réelle : dashboard indisponible = pas de modification possible, même si le réseau local continue de fonctionner.

Quand choisir Meraki : (1) multi-sites > 5 avec exigences SD-WAN avancées, (2) secteur critique 24/7

> *"Meraki n'est pas le choix par défaut. C'est le bon choix dans des contextes précis : multi-sites distribué, secteur critique 24/7, groupe déjà standardisé Cisco. Hors de ces contextes, UniFi suffit largement."*
>
> — Jérémy Manet, FlashModz Enterprise

Quand Meraki est le bon choix (et quand ce ne l'est pas)

Chapitre 2

Le marketing Meraki est partout. Voici les vrais critères de pertinence.

Vous avez 8 sites mal connectés en MPLS coûteux

Les liens MPLS opérateur multi-sites coûtent souvent plusieurs centaines d'euros par mois et par site, avec des SLA décevants en pratique. Meraki SD-WAN les remplace par de la fibre ou de la 4G/5G locale + tunnels Auto VPN : facture WAN nettement réduite, meilleure résilience (multi-WAN), pilotage central simplifié.

Votre infogérant voyage entre sites pour chaque incident

Sans cloud-managed, chaque modification réseau (ajout VLAN, règle firewall, AP) demande déplacement ou intervention SSH. Avec Meraki, tout se fait depuis le dashboard cloud, en quelques minutes, sans déplacement. Pour 5+ sites, c'est l'argument décisif.

Le déploiement d'un nouveau site prend 2 semaines

Sans Meraki : technicien sur site, configuration locale, tests, formation utilisateurs locaux. Avec Meraki zero-touch : commande équipement > pré-config dashboard > expédition site > branchement par utilisateur final > ça marche. 3 jours au lieu de 2 semaines.

Vous n'avez pas de visibilité multi-sites consolidée

Sans dashboard centralisé, vous voyez chaque site indépendamment. Difficile de comparer, d'identifier des tendances, de troubleshooter à distance. Meraki Dashboard donne une vue consolidée temps réel sur tous vos sites : trafic, qualité Wi-Fi, équipements offline, anomalies.

Votre staff IT n'a pas la compétence Cisco CLI

Configurer du Cisco Catalyst classique en CLI (IOS) demande compétences CCNA/CCNP, formation, certifications. Meraki est conçu pour être opérable par un IT généraliste : pas de CLI obligatoire, interface web intuitive, courbe d'apprentissage bien plus courte que Catalyst.

Le SLA support Cisco vaut sa différence de prix

Pour un secteur critique (banque, hôpital, retail en haute saison), le support Cisco direct 24/7 et la base de connaissance massive du constructeur sont précieux. Meraki inclut ce niveau de support dans la licence. Côté UniFi, l'équivalent passe par un intégrateur, avec un engagement contractuel moindre.

Mythes vs Réalité

Chapitre 3

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

01

ON ENTEND SOUVENT

Meraki c'est juste du marketing premium pour vendre cher.

EN RÉALITÉ — *Pertinent à 5+ sites*

Le surcoût Meraki vs UniFi est réel, plusieurs fois le prix une fois les licences comptées. Mais pour 5+ sites ou un secteur critique, il est justifié par : SD-WAN avancé, dashboard cloud, SLA Cisco, audit logs centralisés. Pour 1-3 sites mono-usage, c'est probablement excessif.

02

ON ENTEND SOUVENT

Meraki c'est du Cisco, il faut un CCNA pour exploiter.

EN RÉALITÉ — *Meraki ≠ Catalyst classique*

Au contraire. Meraki est conçu pour être exploitable par un IT généraliste sans CCNA. Pas de CLI obligatoire, dashboard intuitif, MAJ auto. C'est précisément ce qui le différencie de Cisco Catalyst classique.

03

ON ENTEND SOUVENT

Si le cloud Cisco tombe, on perd notre réseau.

EN RÉALITÉ — *Cloud down ≠ réseau down*

Si le dashboard cloud est down (rare), vous ne pouvez plus modifier les configs, MAIS le réseau continue à fonctionner avec sa dernière configuration. Pas de coupure de service. Cisco s'engage contractuellement sur une disponibilité du dashboard de 99,99%.

04

ON ENTEND SOUVENT

Une fois Meraki acheté, on est libre.

EN RÉALITÉ — *Modèle subscription strict*

Faux. Sans licence active, l'équipement Meraki cesse de fonctionner après un délai de grâce de 30 jours. C'est un modèle subscription strict, assumé par Cisco. Renouvellements obligatoires, avec des durées de 1 à 10 ans. Budget pluriannuel à anticiper dès le départ.

05

ON ENTEND SOUVENT

Migrer de Meraki vers autre chose si besoin, c'est facile.

EN RÉALITÉ — *Verrouillage écosystème*

Migrer Meraki vers UniFi ou Catalyst classique = remplacer tout le matériel (pas de cohabitation simple). C'est un projet à part entière. Le verrouillage écosystème est réel. À considérer avant de s'engager 5 ans.

06

ON ENTEND SOUVENT

Meraki c'est uniquement pour les grands comptes.

EN RÉALITÉ — *Multi-sites = critère, pas taille*

Meraki couvre la PME (10-200 collab) jusqu'à l'ETI (1000+). La gamme MX (Z4, MX67/68, MX85/95/105, MX250/450) couvre toutes les tailles. Le seuil de pertinence est plus le nombre de sites que l'effectif.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

Chaîne de magasins (12 boutiques en Wallonie + Bruxelles)

Contexte: Réseau historique : routeurs grand public + Wi-Fi consumer dans chaque magasin. Aucune supervision centrale. Connexions internet asymétriques. Caisses lentes en heure de pointe.

Impact: Migration Meraki : MX67 (security + SD-WAN) + MS120 (switch) + MR42 (AP Wi-Fi) par magasin. Auto VPN site-à-site, QoS pour la caisse, Wi-Fi clients sur SSID dédié. Coût matériel : 30 K€. Licences : 8 K€/an. Bénéfices constatés : nette baisse des incidents, déploiement d'un nouveau magasin en 3 jours, visibilité centralisée.

Leçon: Pour une enseigne multi-sites distribuée, Meraki devient pertinent dès 8-10 sites. Le différentiel SD-WAN + dashboard centralisé compense largement le surcoût licence.

Cabinet d'avocats multi-sites (3 sites : Bruxelles, Liège, Namur)

Contexte: Cabinet 35 collaborateurs sur 3 sites historiques. Connexions VPN IPsec manuelles. Bases de données partagées entre sites. Configuration disparate.

Impact: Évaluation Meraki vs UniFi multi-sites. Décision : UniFi avec Site Magic suffit. 3 UDM Pro + 6 switches + 9 AP, total 9 K€ matériel + 3 jours intervention/site. vs Meraki estimé à 25 K€ matériel + 3 K€/an. Économie 60%.

Leçon: À 3 sites simples, UniFi avec Site Magic suffit dans la grande majorité des cas. Meraki devient pertinent à 5+ sites OU avec des exigences SD-WAN avancées (path selection, routage par application).

Groupe industriel régulé secteur santé (5 sites + 2 entrepôts)

Contexte: Hôpital privé sur 7 sites en Belgique. Données santé = catégorie particulière RGPD. Audit NIS2 imminent. Cisco déjà en groupe.

Impact: Choix Cisco Meraki pour la cohérence groupe et les exigences de support. MX85 par site + switches MS + AP MR + caméras MV. Architecture SD-WAN avec dual-WAN et failover automatique. Conformité NIS2 facilitée par les audit logs centralisés, filtrage DNS Cisco Umbrella en option.

Leçon: Pour un secteur très critique avec multi-sites et exigences NIS2/RGPD strictes, Meraki est défendable malgré le coût. SLA Cisco + audit logs + intégrations SOC valent leur prix dans ces contextes.

Avant / Après — la différence concrète

Chapitre 5

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

	Multi-sites avant Meraki	Multi-sites avec Meraki
01	**WAN**	
	MPLS coûteux, facturé au mois par site, avec SLA décevants.	SD-WAN Internet 4G/fibre, multi-WAN failover, facture en nette baisse.
02	**DÉPLOIEMENT NOUVEAU SITE**	
	Technicien sur place, 2 semaines, formation locale.	Zero-touch : équipement expédié, branché, ça marche en 3 jours.
03	**CONFIGURATIONS**	
	Disparates par site, divergence inévitable.	Cohérence globale : templates appliqués à tous les sites.
04	**VISIBILITÉ**	
	Site par site, pas de vue consolidée.	Dashboard cloud temps réel, drill-down par site.
05	**SUPPORT**	
	Variable selon prestataires multi-sites.	Cisco direct 24/7, base de connaissance massive.
06	**MAJ FIRMWARE**	
	Risquées, étalées sur semaines, parfois oubliées.	Automatiques, transparentes, planifiées par fenêtres.
07	**SÉCURITÉ**	
	Hétérogène par site, audit logs dispersés.	Politiques centralisées, audit logs cloud, intégrations SOC.

08 COÛT TOTAL 5 ANS

- Souvent comparable mais + risques + temps interne.
- Plus cher en facture, mais opérations simplifiées.

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 choix Meraki a été comparé objectivement à UniFi et Cisco Catalyst (TCO 5 ans).	☐	☐	☐
2. Toutes les licences Meraki sont actives et leur renouvellement est planifié.	☐	☐	☐
3. Auto VPN est configuré entre tous les sites (full mesh ou hub-spoke selon topologie).	☐	☐	☐
4. SD-WAN policies sont définies par application (voix prioritaire, etc.).	☐	☐	☐
5. Multi-WAN avec failover automatique est en place sur les sites critiques.	☐	☐	☐
6. Les configurations sont cohérentes entre sites (templates appliqués).	☐	☐	☐
7. IDS/IPS est activé sur les MX (suite Advanced Security ou Secure SD-WAN Plus).	☐	☐	☐
8. Les audit logs sont centralisés et conservés selon politique de rétention.	☐	☐	☐
9. Une intégration SOC existe (Cisco Umbrella, ThousandEyes ou SIEM tiers).	☐	☐	☐
10. Le staff IT est formé au dashboard Meraki (1 jour minimum).	☐	☐	☐
11. Un partenaire Meraki Gold/Platinum est identifié pour escalade.	☐	☐	☐
12. Documentation : topologie globale, exceptions par site, plan VLAN cohérent.	☐	☐	☐

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 indépendant, déploiement, optimisation des licences. Sans biais commercial.

Évaluation Meraki vs alternatives

Analyse indépendante de votre contexte. Comparaison Meraki vs UniFi vs Cisco Catalyst sur vos critères réels. Livrable : matrice de décision avec coût total propriété 5 ans, ROI, recommandation. Sans biais commercial.

Cadrage architecture Meraki

Si Meraki retenu : design détaillé. Modèles MX/MS/MR par site selon volumétrie, plan de licences (Enterprise, Advanced Security ou Secure SD-WAN Plus), topologie Auto VPN, plan VLAN multi-sites cohérent.

Déploiement Meraki multi-sites

Configuration complète depuis le dashboard, pré-provisioning des équipements, expédition zero-touch vers les sites, validation, formation locale minimale. Pour 3-30 sites.

Auto VPN & SD-WAN

Mise en place Auto VPN entre sites, configuration des SD-WAN policies (path selection par application : VoIP via fibre, autres via 4G secondaire), failover automatique, optimisation continue.

Optimisation des licences

Audit des licences Meraki existantes : adéquation entre les suites Enterprise, Advanced Security et Secure SD-WAN Plus, durée optimale (de 1 à 10 ans, remise croissante avec l'engagement), co-termination des dates de renouvellement. Objectif : ne payer que ce qui sert vraiment.

Migration depuis Cisco Catalyst ou autre

Phase de cohabitation, bascule par site (un weekend par site), validation applicative, plan de rollback. Inclut formation IT interne sur le dashboard Meraki.

Intégration SOC (Cisco Umbrella, ThousandEyes)

Pour les organisations matures : intégration Meraki avec Cisco Umbrella (DNS security cloud), ThousandEyes (visibilité internet), Cisco Secure Firewall en complément. Stack Cisco cohérente.

Run & gestion des licences

Veille sur les MAJ dashboard, gestion des renouvellements de licences (anticipation 90 jours), optimisation continue, accompagnement nouveaux sites. Forfait 1-3 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.

1	2	3	4	5
SEMAINE 1-2	SEMAINE 3-4	SEMAINE 5-7	SEMAINE 8-16	CONTINU
Évaluation	**Conception**	**Pré-déploiement**	**Déploiement**	**Run**
• Comparaison Meraki vs alternatives • TCO 5 ans • Décision matricielle • Choix partenaire	• Architecture multi-sites • Plan licences • BOM complet • Approche déploiement	• Achat matériel • Pré-config dashboard • Templates par type de site • Lab test	• Bascule par site (1 site/sem) • Auto VPN activé • SD-WAN policies • Formation IT	• Optimisation • Renouvellement licences • Nouveaux sites • Évolution écosystème Cisco

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 Meraki / NIS2 / ISO 27001

Chapitre 9

Comment l'écosystème Meraki s'intègre dans une démarche de conformité.

Conformité réseau multi-sites

NIS2 art. 21

Pour une entité essentielle ou importante NIS2 multi-sites, le dashboard Meraki centralise les preuves : audit logs, conformité des configurations, supervision, alertes incidents. Autant d'éléments attendus par les inspecteurs.

BÉNÉFICE CACHÉ :

Préparer un audit NIS2 sur 8 sites avec Meraki = consultation dashboard. Sans Meraki = compilation manuelle laborieuse.

Sécurité des réseaux

ISO 27001 A.8.20

Annex A 8.20-8.22 (sécurité réseau, segregation, security of network services) sont directement servies par Meraki : VLAN, ACL, IDS/IPS, audit logs centralisés, gestion des accès.

BÉNÉFICE CACHÉ :

Auditeurs ISO 27001 connaissent très bien Meraki. Démonstration rapide et efficace lors d'audits.

Conformité paiement carte

PCI-DSS retail

Pour le retail : PCI-DSS exige la segmentation des points de vente (CDE, Cardholder Data Environment). Meraki facilite cette conformité avec des VLANs dédiés CDE et des audit logs centralisés.

BÉNÉFICE CACHÉ :

Une chaîne retail Meraki a une longueur d'avance sur la conformité PCI-DSS comparée à un patchwork équipements.

Résilience multi-sites

DORA secteur financier

DORA exige résilience opérationnelle, dont la couche réseau. Meraki SD-WAN avec multi-WAN failover et supervision 24/7 répond directement à ces exigences.

BÉNÉFICE CACHÉ :

Pour un acteur financier multi-sites, Meraki est une réponse architecturale alignée avec DORA.

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
☐ Évaluation comparative Meraki vs UniFi vs Catalyst sur votre cas spécifique.	🟢🟢⚪⚪⚪	🟢🟢🟠🔴🔴	3 semaines
☐ Calculer le TCO 5 ans précisément (matériel + licences + intervention).	🟢🟢⚪⚪⚪	🟢🟢🟠🔴🔴	3 semaines
☐ Si Meraki retenu : choix des modèles MX/MS/MR/MV par site.	🟢🟢⚪⚪⚪	🟢🟢🟠🔴🔴	5 semaines
☐ Décider la durée de licence (de 1 à 10 ans).	🟢⚪⚪⚪⚪	🟢🟢🟠🔴⚪	5 semaines
☐ Identifier un partenaire Meraki Gold/Platinum.	🟢⚪⚪⚪⚪	🟢🟢🟠🔴⚪	4 semaines
☐ Commander matériel + licences (parfois délais 4-8 semaines).	🟢⚪⚪⚪⚪	🟢🟢🟠🔴🔴	6 semaines
☐ Pré-configurer le dashboard et créer les templates par type de site.	🟢🟢🟠🔴⚪	🟢🟢🟠🔴🔴	8 semaines
☐ Lab test : valider topologie sur 1-2 équipements.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	9 semaines
☐ Bascule progressive par site (1 site / semaine).	🟢🟢🟠🔴🔴	🟢🟢🟠🔴🔴	12 semaines
☐ Configurer Auto VPN entre tous les sites.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	14 semaines
☐ Configurer SD-WAN policies par application.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	14 semaines

		EFFORT	IMPACT	DÉLAI
☐	Activer IDS/IPS et content filtering (selon licence).	●●○○○	●●●●○	15 semaines
☐	Former les équipes IT internes au dashboard (1-2 jours).	●●○○○	●●●●○	16 semaines
☐	Programmer alertes renouvellement licences (90 jours avant échéance).	●○○○○	●●●●○	Continu
☐	Évaluer intégrations SOC (Umbrella, ThousandEyes).	●●●○○	●●●○○	18 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. Quand Meraki vs UniFi ?

Meraki devient pertinent à : (1) 5+ sites avec besoin SD-WAN avancé, (2) secteur critique 24/7 nécessitant SLA Cisco, (3) déjà standardisé Cisco au niveau groupe, (4) retail/franchises distribuées zero-touch indispensable. UniFi suffit pour : 1-4 sites simples, budget contraint, mono-secteur, équipe IT capable de monter en compétence.

Q2. Quel modèle MX choisir ?

Z4 : télétravail (1-5 users). MX67 / MX68 : petit site (5-50 users). MX85 / MX95 / MX105 : site moyen (50-500 users). MX250 / MX450 : grand site ou datacenter (500-5000 users). Les variantes C/CW intègrent le cellulaire pour le failover WAN. Choisissez selon le volume utilisateur ET le débit Internet : l'IDS/IPS actif réduit le throughput réel, vérifiez les fiches techniques.

Q3. Quelle suite de licence MX choisir ?

Trois suites. Enterprise : firewalling de base, Auto VPN. Advanced Security : ajoute IDS/IPS, AMP (anti-malware) et le filtrage de contenu. Secure SD-WAN Plus : ajoute le SD-WAN avancé et l'intégration ThousandEyes. Le tarif dépend du modèle MX et de la durée d'engagement : de quelques dizaines à plusieurs centaines d'euros par équipement et par an. Recommandation PME standard : Advanced Security. Multi-sites avec WAN critique : Secure SD-WAN Plus.

Q4. Combien de temps pour déployer Meraki sur 10 sites ?

10-12 semaines si bien cadré. Phase 1 : conception + achat matériel (4 sem). Phase 2 : pré-config dashboard + lab (1 sem). Phase 3 : déploiement progressif (1 site / semaine = 8-10 sem). Variabilité selon : qualité documentation existante, fenêtres de bascule disponibles, complexité applicative locale.

Q5. Que se passe-t-il si une licence expire ?

Le dashboard vous alerte bien avant l'échéance. Après expiration, Cisco accorde un délai de grâce de 30 jours pour régulariser. Passé ce délai, les équipements cessent de fonctionner : le réseau tombe. La politique est stricte et assumée. En pratique : programmez des alertes 90 jours avant chaque échéance, budgétez en pluriannuel, et utilisez la co-termination pour aligner toutes les dates de renouvellement.

Q6. Peut-on mixer Meraki et UniFi ?

Oui techniquement, dans des sites différents (Meraki sur les sites multi-distribués, UniFi sur le siège unique par exemple). Mais la simplicité opérationnelle de Meraki vient de l'unicité dashboard. Mixer divise cet avantage. Pertinent uniquement si justifications techniques fortes.

Q7. Comment renouveler les licences sans être pris au piège ?

Meraki vend des licences de 1 à 10 ans : plus l'engagement est long, plus la remise est forte. Recommandation : 3 ou 5 ans, bon équilibre entre économie et flexibilité. Anticiper systématiquement 90 jours avant expiration, négocier au global avec votre partenaire Meraki Gold/Platinum, et co-terminer les dates pour ne gérer qu'une seule échéance.

Q8. Cisco Catalyst (non Meraki) vs Meraki ?

Catalyst : enterprise classique, CLI IOS, fonctionnalités très avancées, pour très grands comptes ou secteurs très spécifiques (industriel, gov). Meraki : simplifié, cloud-managed, plus orienté PME/ETI. Peuvent cohabiter (Catalyst au cœur datacenter, Meraki en branches). Pour PME multi-sites : Meraki est généralement plus adapté.

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

Évaluons Meraki pour votre contexte

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