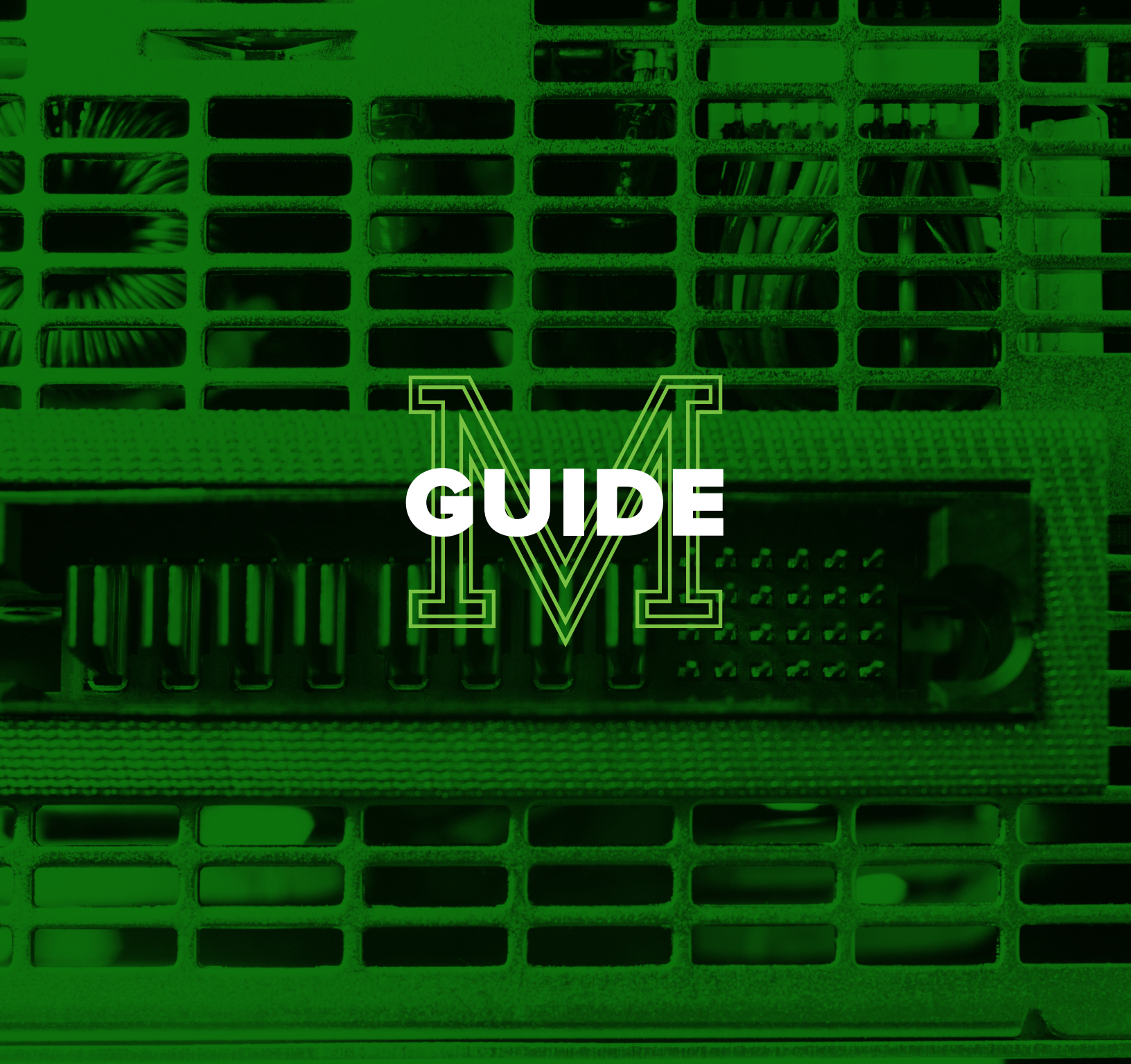


GUIDE

LA SÉCURITÉ SIMPLIFIÉE

Sommaire

Présentation générale

La tâche des administrateurs informatiques n'est pas simple : ils doivent non seulement installer les équipements réseau, mais aussi les mettre à jour et tout administrer, des clients aux applications. Et comme si cela ne suffisait pas, ils doivent aussi gérer la sécurité. En raison des différents types d'utilisateurs (collaborateurs, invités, sous-traitants) et des différents types d'appareils (ordinateurs portables appartenant à l'entreprise, smartphones appartenant aux collaborateurs, objets connectés) qui tentent d'accéder au réseau, les administrateurs ont besoin d'une solution évolutive pour gérer la sécurité et l'accès réseau des utilisateurs et des équipements.

Pour sécuriser leur réseau, les équipes IT utilisent les solutions de différents fournisseurs, avec des tableaux de bord disparates, des intégrations manuelles et plusieurs systèmes matériels. En effet, plus de 25 % des entreprises utilisent les solutions de 1 à 20 fournisseurs pour tenter de sécuriser leurs réseaux.[1] Cette grande variété de solutions est loin de simplifier la sécurité. Au contraire, elle la complique. Les administrateurs finissent par renoncer et installer un pare-feu de base. Bien qu'ils comprennent l'intérêt de la mise en œuvre d'une infrastructure de sécurité couvrant toutes les couches du réseau, ils ne disposent pas des ressources ni du temps nécessaires à sa réalisation. Les hackers profitent de ces vulnérabilités. Plus de 43 % des attaques ciblent[2] les PME ayant des équipes informatiques restreintes et plus de 74 % de ces attaques exploitent des politiques de sécurité et d'accès réseau inadaptées.[3]

Meraki arrive à la rescousse ! Avec son tableau de bord unique, il vous permet non seulement de gérer l'ensemble de votre réseau, mais également d'appliquer des politiques de sécurité et d'accès sophistiquées. Basé dans le cloud, le tableau de bord Meraki garantit que tous les produits sont constamment corrigés et mis à jour. La solution Meraki est également ouverte et offre des API extensibles pour étendre l'intégration avec la gamme de solutions de sécurité Cisco.

1 Rapport annuel Cisco 2018 sur la cybersécurité
2 Rapport annuel Cisco 2018 sur la cybersécurité
3 Rapport annuel Cisco 2018 sur la cybersécurité

Mises à jour matérielles

PRÉSENTATION

Le MS390 combine la puissance de la technologie ASIC UADP 2.0 de Cisco avec la simplicité du tableau de bord de Meraki pour micro-segmenter les différents utilisateurs et équipements d'un réseau. En appliquant des politiques efficaces de sécurité et d'accès, il évite à l'entreprise du client de subir une violation de ses données personnelles et de faire la une des journaux. Avec ses liaisons ascendantes modulables, ses blocs d'alimentation et son circuit ASIC personnalisé, le MS390 est le commutateur d'accès le plus performant de la gamme Meraki. Il résout de nombreux problèmes pour les administrateurs informatiques.

ANNONCE

Le MS390 est le commutateur d'accès le plus performant jamais produit par Meraki. Il combine la simplicité de l'IT gérée dans le cloud avec la puissance des circuits spécialement conçus par Cisco. En plus de fournir des fonctions classiques de commutation, le MS390 offre la possibilité d'activer des politiques de sécurité et d'accès sophistiquées basées sur la micro-segmentation des groupes d'utilisateurs au lieu d'adresses IP individuelles difficiles à déchiffrer. Il propose également d'autres fonctionnalités clés :

- Il aide les clients à se conformer aux exigences élevées de qualité de service à l'aide du circuit ASIC UADP 2.0
- Il multiplie le débit par 3 (480 Gbit/s) par rapport à son prédécesseur (le MS350) et offre une interface mGig 48 ports avec liaisons ascendantes modulables remplaçables à chaud permettant aux clients de choisir entre des liaisons ascendantes 1/10/40 Gbit/s à mesure que les besoins du réseau évoluent
- Il bénéficie d'un empilage physique amélioré qui réduit la latence à moins d'une seconde pour accélérer la convergence des équipements en cas de panne du commutateur, ce qui est essentiel dans les déploiements d'entreprise
- Il inclut StackPower, qui regroupe toute l'alimentation disponible pour fournir une redondance d'alimentation supplémentaire

PRINCIPAUX POINTS À RETENIR

Le circuit ASIC UADP 2.0 intégré sur la gamme de commutateurs MS390 facilite la mise en œuvre de réseaux intent-based en tout lieu. Les clients peuvent micro-segmenter les utilisateurs en fonction de leur identité et non de l'endroit où ils se trouvent pour appliquer des politiques de sécurité et d'accès sophistiquées. Riche en fonctionnalités, le MS390 facilite la gestion des équipements et optimise la gestion de l'alimentation grâce à la simplicité inédite du tableau de bord Meraki.

Mises à jour des composants logiciels et des fonctionnalités

Politique adaptative

PRÉSENTATION

À mesure qu'une entreprise se développe et ajoute des appareils, des utilisateurs et des applications, la collecte d'adresses IP sur le réseau en utilisant la méthode classique se complique. En outre, les adresses IP ne fournissent pas d'informations sur les utilisateurs, les appareils et les applications. La fonctionnalité de politique adaptative donne la priorité à la sécurité en ajoutant toutes ces informations à chacune des liaisons de communication vers les adresses IP, sans compromettre les ressources et la capacité du matériel de commutation.

ANNONCE

La fonctionnalité de politique adaptative est intégrée au commutateur MS390 pour fournir une couche supplémentaire de sécurité en fonction de l'objectif de l'utilisateur, de l'appareil et de l'application. Elle met en œuvre des politiques réseau qui s'adaptent automatiquement à l'environnement de l'entreprise en fonction de l'objectif du client, de l'application de l'utilisateur ou de l'appareil.

PRINCIPAUX POINTS À RETENIR

La fonctionnalité de politique adaptative résout les problèmes actuels des réseaux en assurant une sécurité efficace, une réduction des coûts d'exploitation, une automatisation puissante, une meilleure visibilité, une efficacité matérielle accrue et une hausse de la productivité de l'entreprise.

SecureConnect

PRÉSENTATION

Le matériel réseau est vulnérable aux menaces potentielles. SecureConnect est la solution la plus simple et la plus efficace pour sécuriser les ports de commutation et automatiser les configurations des appareils. Aucun autre fournisseur ne fournit ce niveau de sécurité en seulement quelques clics.

ANNONCE

SecureConnect est une fonctionnalité logicielle disponible pour tous les modèles MS à partir du MS210, ainsi que tous les modèles MR 802.11ac et 802.11ax. SecureConnect permet au commutateur MS de détecter et de vérifier que le point d'accès MR connecté au port appartient à la même organisation, puis transmet automatiquement les configurations au MR connecté.

PRINCIPAUX POINTS À RETENIR

SecureConnect offre aux clients une sécurité fiable, une automatisation évolutive et une productivité accrue, et élimine les erreurs potentielles de configuration. Il fournit les avantages du modèle de licence Meraki et permet de bénéficier du cloud de Meraki qui inclut les fonctionnalités logicielles évolutives dont nos clients ont besoin. Meraki continue à résoudre les besoins en matière de sécurité avec des fonctionnalités s'adaptant à plusieurs produits pour permettre aux clients ayant investi dans Meraki de continuer à tirer parti de cette solution

Trusted Access

PRÉSENTATION

Les administrateurs informatiques n'ont pas la possibilité de contrôler précisément à tout moment les utilisateurs et les appareils qui se connectent au réseau. Meraki Trusted Access fournit une visibilité sur les utilisateurs et les appareils et offre un accès sécurisé et transparent au réseau.

ANNONCE

Meraki Trusted Access est une fonctionnalité logicielle qui permet aux organisations de créer une connexion réseau sécurisée entre les ressources de l'entreprise et les appareils personnels sans avoir à installer un agent/profil MDM. Trusted Access nécessite l'activation de MR + SM. Cette fonctionnalité est disponible pour les appareils iOS, macOS et Android.

PRINCIPAUX POINTS À RETENIR

Meraki Trusted Access offre aux clients des méthodes d'authentification flexibles combinées à une sécurité avancée. Cette fonctionnalité améliore l'expérience utilisateur et fournit une visibilité sur les utilisateurs et les appareils. Elle automatise également l'intégration des appareils et l'application des politiques de sécurité. Meraki Trusted Access permet en outre des intégrations personnalisées grâce à l'utilisation d'API.

Systèmes fiables

PRÉSENTATION

Cisco Meraki est un facteur de différenciation sur le marché avec ses gammes complètes de produits (points d'accès MR, commutateurs MS et appliances de sécurité MX SD-WAN) prenant en charge les systèmes fiables de Cisco.

ANNONCE

Les systèmes fiables sont une suite de solutions Cisco qui vérifient que le code exécuté sur ses plates-formes matérielles est authentique, non modifié et fonctionne comme prévu. Sont incluses des technologies comme la signature d'image, Secure Boot et le module Cisco Trust Anchor (TAm). L'approche multicouche, incluant une racine de confiance au niveau du matériel, une identité d'appareil unique et la validation de tous les niveaux de logiciels pendant le démarrage, établit une chaîne de confiance pour le système. Les produits matériels Cisco Meraki prennent maintenant tous en charge les systèmes fiables de Cisco.

PRINCIPAUX POINTS À RETENIR

Les systèmes fiables de Cisco promettent d'assurer la sécurité et la fiabilité des produits matériels Cisco pour éviter les menaces telles que les produits contrefaits et les cyberattaques. La pile complète Meraki est une solution d'entreprise dont la fiabilité peut désormais être garantie par une infrastructure réseau de systèmes fiables.

Licence Umbrella + MR

PRÉSENTATION

Les clients peuvent désormais sécuriser leurs réseaux en combinant la puissance de la solution de sécurité DNS de Cisco Umbrella et la simplicité du tableau de bord Meraki. Les nouvelles licences MR Advanced et MR Upgrade activent automatiquement les politiques définies par Meraki au niveau de la couche DNS de votre réseau. Avec la nouvelle licence, les clients bénéficient également d'un gain de visibilité sur les événements DNS bloqués depuis le tableau de bord Meraki. Les administrateurs informatiques n'ont plus besoin d'intégrer manuellement Umbrella avec leurs points d'accès MR et peuvent faire évoluer les déploiements de sécurité sur plusieurs sites en quelques minutes.

ANNONCE

Meraki lance une nouvelle licence qui fournit aux clients une visibilité granulaire sur les événements DNS bloqués à l'aide de la console de sécurité du tableau de bord Meraki. Les clients peuvent également déployer des politiques prédéfinies sans intégration manuelle. Avec l'ajout de la console de sécurité au tableau de bord Meraki, les clients peuvent également surveiller, protéger et dépanner leurs réseaux sans fil au niveau DNS. Les nouveaux clients peuvent acheter la référence de licence Advanced pour accéder à ces fonctionnalités communes et les clients existants de solutions sans fil peuvent acheter la référence de licence Upgrade pour activer la sécurité DNS optimisée par Umbrella sur leur réseau Meraki.

PRINCIPAUX POINTS À RETENIR

La nouvelle licence qui combine Umbrella et MR offre aux clients une simplicité et une centralisation inégalées. Ils peuvent déployer une sécurité au niveau de la couche DNS sur tous les points d'accès Meraki dans le cloud sans avoir à utiliser de matériel ou de machines virtuelles supplémentaires. Meraki a également créé des terminaux d'API pour extraire et déployer des politiques prédéfinies qui protègent les utilisateurs contre la plupart des menaces Internet. Les administrateurs informatiques peuvent maintenant déployer une sécurité au niveau de la couche DNS à grande échelle sur plusieurs réseaux pour créer un espace de travail numérique simple et sécurisé.

API d'intégration de MX avec Cisco Defense Orchestrator (CDO)

PRÉSENTATION

Cisco Defense Orchestrator (CDO) est une solution de gestion dans le cloud qui vous permet de gérer les configurations et les politiques de sécurité en toute simplicité sur l'ensemble de vos produits de sécurité Cisco, y compris Meraki MX.

ANNONCE

CDO prend maintenant en charge Meraki MX. Cette solution renforce la sécurité en coordonnant les politiques dans l'ensemble de l'entreprise, quel que soit le produit de sécurité Cisco. Elle permet de gérer facilement les politiques de sécurité sur plusieurs produits de sécurité Cisco afin d'éviter les incohérences et les lacunes. Les clients disposant d'une combinaison de produits de sécurité Cisco, notamment Meraki MX, apprécieront l'intérêt d'utiliser CDO pour unifier, gérer et mettre à jour les politiques sur tous les sites de leur entreprise.

PRINCIPAUX POINTS À RETENIR

CDO est une solution performante qui unifie la gestion de la sécurité dans une infrastructure hybride Cisco et Meraki.

Clé d'identité prépartagée (iPSK)

PRÉSENTATION

Avec la prolifération des objets connectés, les administrateurs font face à une croissance exponentielle du nombre d'équipements connectés aux réseaux sans fil. Tous ces appareils ne prennent pas en charge l'authentification 802.1X, ce qui complique l'authentification. Le WPA-PSK utilisé aujourd'hui ne permet pas toujours d'éviter qu'une clé soit partagée avec des utilisateurs non autorisés. La fonctionnalité iPSK (clé d'identité pré-partagée) va considérablement simplifier la sécurisation du réseau sans fil.

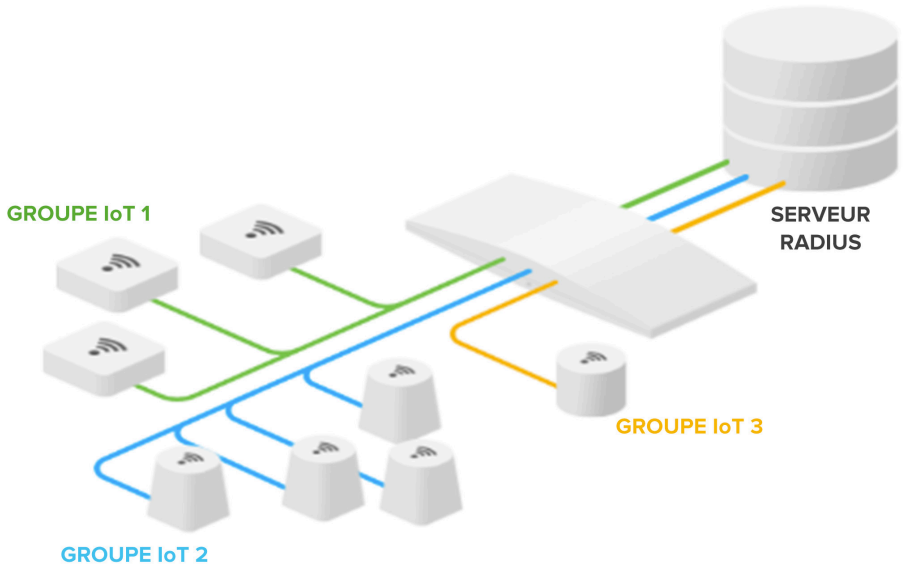
ANNONCE

iPSK est une nouvelle fonctionnalité MR qui authentifie les appareils sans fil de façon plus sécurisée que les méthodes précédentes comme WPA-PSK. Elle ne nécessite pas de certificats ni d'authentification 802.1X supplémentaires. Au lieu de prépartager une clé avec les équipements se connectant à un SSID, elle met en corrélation une clé PSK unique avec l'adresse MAC de chaque équipement et l'authentifie via un serveur RADIUS. Cette fonctionnalité autorise également l'assignation de politiques de groupe distinctes au sein d'un même SSID, en fonction de la clé PSK utilisée. Par exemple, tous les appareils utilisant la clé PSK « Meraki123 » reçoivent automatiquement la politique de groupe 1, et ceux utilisant la clé PSK « Meraki456 » reçoivent automatiquement la politique de groupe 2.

PRINCIPAUX POINTS À RETENIR

Cette fonctionnalité permet aux entreprises de sécuriser leurs réseaux sans créer plusieurs SSID, qui diminueraient les performances du réseau sans fil. Elle fournit une sécurité supplémentaire aux entreprises qui ont entamé leur transformation numérique.

.



Groupes d'objets de pare-feu

PRÉSENTATION

Les groupes d'objets de pare-feu permettent de mapper des entités du réseau telles que la téléphonie, les imprimantes, etc., vers un sous-réseau ou une adresse IP. Vous pouvez ensuite regrouper ces objets réseau pour simplifier les règles de pare-feu sur le MX.

ANNONCE

Les groupes d'objets de pare-feu sont une nouvelle fonctionnalité MX qui simplifie le processus de création et de gestion de plusieurs règles de pare-feu.

PRINCIPAUX POINTS À RETENIR

Il n'a jamais été aussi facile de créer et de gérer des règles de pare-feu. Ce nouveau processus améliore les performances de MX et, par conséquent, la simplicité de gestion du réseau.

cisco Meraki