Configuration de Cisco Umbrella sur votre réseau via les routeurs de la gamme RV34x

Introduction

Depuis la version 1.0.0.2.16 du micrologiciel, les routeurs de la gamme RV34x prennent désormais en charge Cisco Umbrella. Umbrella utilise le DNS comme vecteur de défense ou bouclier contre les programmes malveillants et les intrusions de données.

Périphériques pertinents

- Routeur de la gamme RV34x

Version du logiciel

- 1.0.02.16

Exigences

- Un compte parapluie actif (vous n'en avez pas ? Demandez un devis ou commencez un essai gratuit)

Objectif

Ce guide vous présente les étapes à suivre pour intégrer la plate-forme de sécurité d'Umbrella à votre réseau. Avant d'entrer dans les détails, nous répondrons à quelques questions que vous pourriez vous poser sur Umbrella.

C'est quoi un parapluie ?

Umbrella est une plate-forme de sécurité cloud simple mais très efficace de Cisco. Umbrella opère dans le cloud et fournit de nombreux services liés à la sécurité. De la menace émergente à l'enquête post-événement. Umbrella détecte et empêche les attaques sur tous les ports et protocoles.

Comment cela fonctionne-t-il?

Umbrella utilise le DNS comme principal vecteur de défense. Lorsque les utilisateurs entrent une URL dans leur barre de navigateur et cliquent sur Entrée, Umbrella participe au transfert. Cette URL est transmise au résolveur DNS d'Umbrella et si un avertissement de sécurité est associé au domaine, la requête est bloquée. Ces données télémétriques sont transférées et analysées en microsecondes, ce qui n'ajoute pratiquement aucune latence. Les données de télémétrie utilisent des journaux et des instruments pour suivre des milliards de requêtes DNS dans le monde entier. Lorsque ces données sont omniprésentes, les

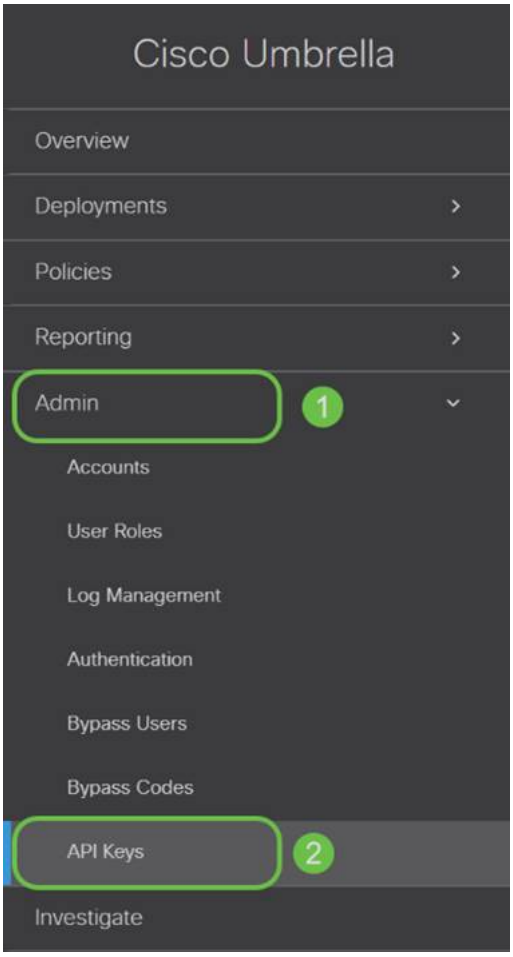
corréler dans le monde entier permet de réagir rapidement aux attaques dès leur apparition. Consultez la politique de confidentialité de Cisco ici pour plus d'informations - politique complète, version récapitulative. Considérez les données de télémétrie comme des données provenant d'outils et de journaux.

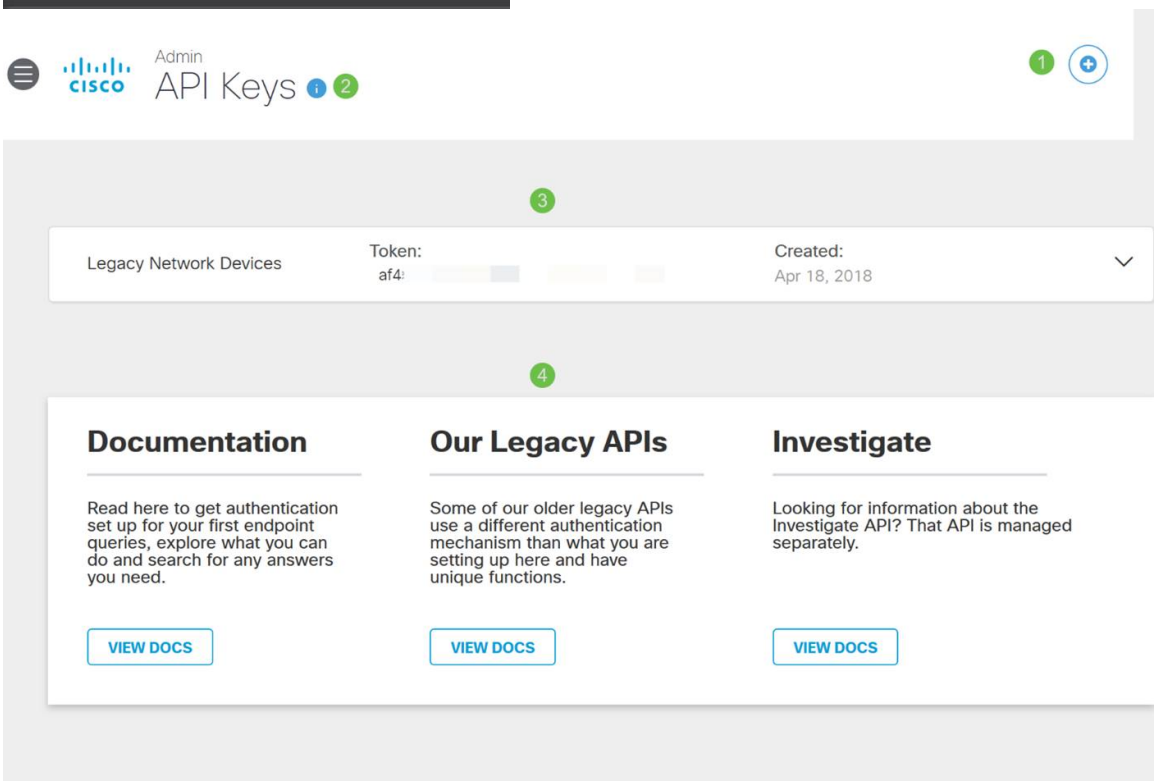
Pour résumer en une métaphore, imaginez que vous êtes à une fête. A cette fête, tout le monde est sur son téléphone et surfe sur le web. Le silence tranquille du groupe est ponctué par les fêtards qui tapent sur leurs écrans. Ce n'est pas une super fête, mais alors que sur votre propre téléphone vous voyez un lien hypertexte vers un GIF chaton qui semble irrésistible. Cependant, l'URL semble douteuse et vous ne savez pas si vous devez taper ou non. Avant d'appuyer sur le lien hypertexte, vous criez au reste de la personne : « Ce lien est-il incorrect ? » Si une autre personne à la fête a été sur le lien et a découvert qu'il s'agissait d'une arnaque, ils crieraient : « Oui, je l'ai fait et c'est une arnaque ! » Vous remerciez cette personne de vous avoir sauvé, continuant votre noble quête de photos d'animaux mignons. Bien sûr, à l'échelle de Cisco, ce type de vérification de la sécurité des demandes et des rappels se produit des millions de fois par seconde, ce qui profite à la sécurité de votre réseau.

Ça a l'air bien, comment on fait pour démarrer ça ?

Lorsque vous parcourez ce guide, commencez par saisir la clé API et la clé secrète dans le tableau de bord de votre compte Umbrella. Ensuite, nous nous connecterons à votre routeur pour ajouter l'API et la clé secrète. Si vous rencontrez des problèmes, consultez ici la documentation, et ici les options d'assistance Umbrella.

Étape 1. Après vous être connecté à votre compte Umbrella, à partir de l'écran *Tableau de bord*, cliquez sur **Admin > API Keys**.



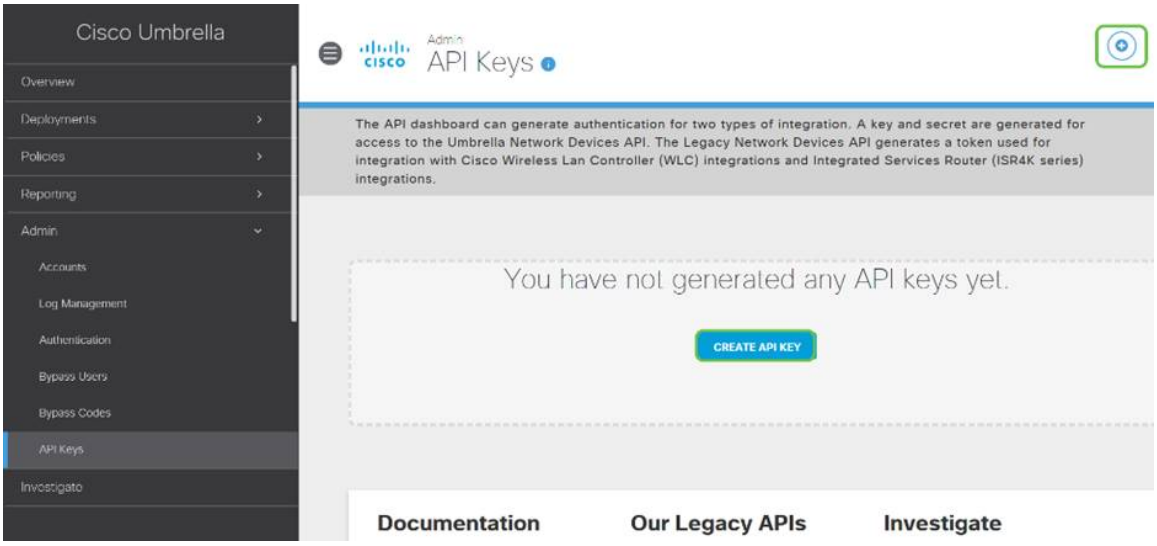


Écran Anatomie des clés API (avec clé API préexistante) -

1. Add API Key : lance la création d'une nouvelle clé à utiliser avec l'API Umbrella.
2. Informations supplémentaires : glisse vers le bas/haut avec un explicateur pour cet écran.
3. Puits de jeton : contient toutes les clés et tous les jetons créés par ce compte. (Remplit une fois qu'une clé a été créée)
4. Documents de support - Liens vers la documentation du site Umbrella relative aux sujets de

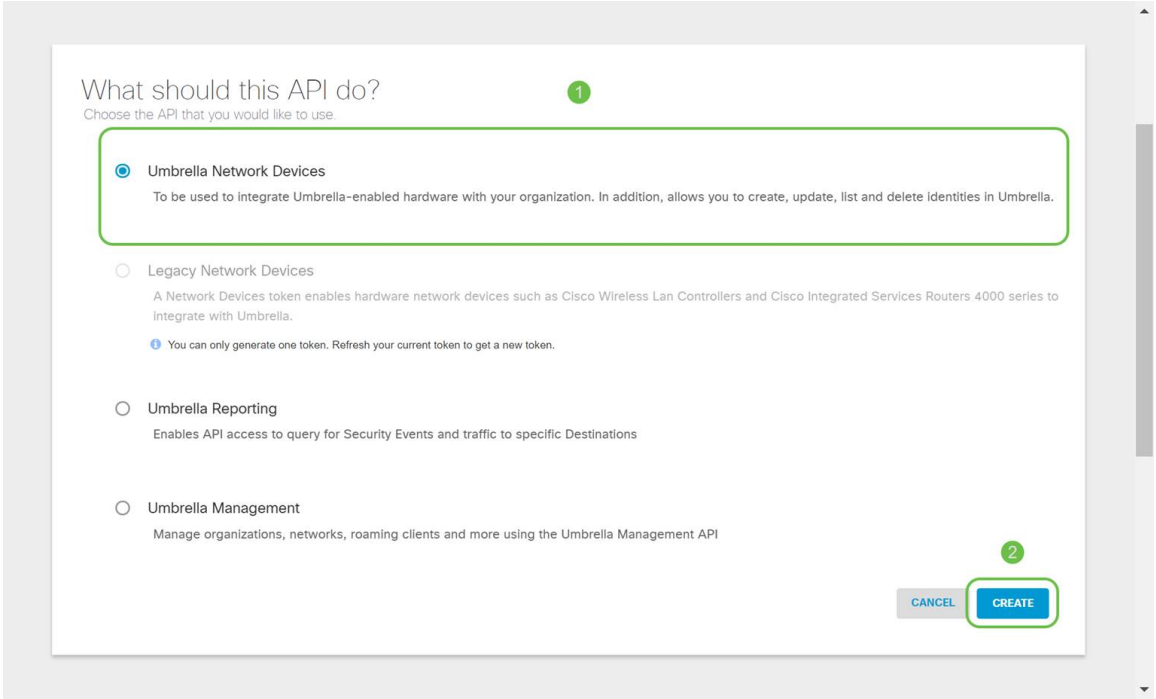
chaque section.

Étape 2. Cliquez sur le bouton **Add API Key** dans le coin supérieur droit, ou cliquez sur le bouton **Create API Key**. Ils fonctionnent tous les deux de la même manière.

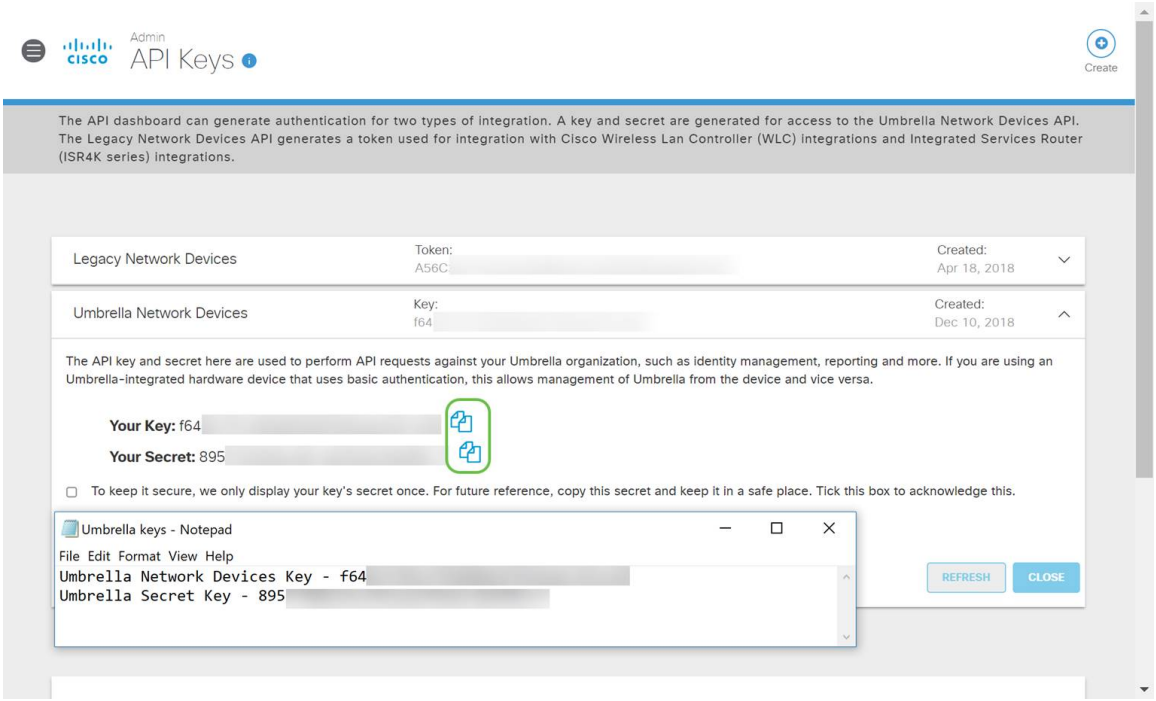


Note: la capture d'écran ci-dessus serait similaire à ce que vous verriez en ouvrant ce menu pour la première fois.

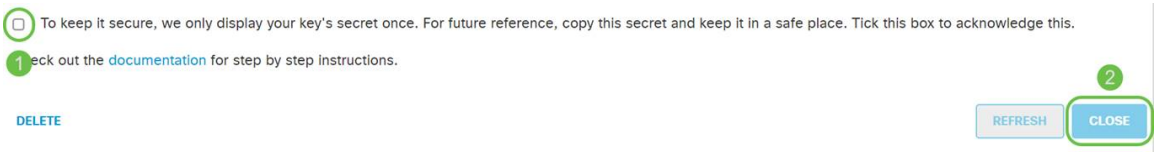
Étape 3. Sélectionnez **Umbrella Network Devices**, puis cliquez sur le bouton **Create**.



Étape 4. Ouvrez un éditeur de texte tel que le bloc-notes, puis cliquez sur le bouton **Copier** à droite de votre API et API *Secret Key.* Une notification contextuelle confirmera que la clé est copiée dans votre Presse-papiers. Une par une, collez votre clé secrète et votre clé API dans le document, en les étiquetant pour référence ultérieure. Dans ce cas, son étiquette est « clé de périphériques réseau parapluie ». Enregistrez ensuite le fichier texte dans un emplacement sécurisé auquel vous pourrez accéder facilement ultérieurement.



Étape 5. Après avoir copié la clé et la clé secrète vers un emplacement sûr, dans l'*écran de l'API Umbrella*, cochez la **case** pour confirmer l'accusé de réception de l'affichage temporaire de la clé secrète, puis cliquez sur le bouton **Close**.



Remarque importante : si vous perdez ou supprimez accidentellement la clé secrète, il n'y a aucune fonction ou numéro de support à appeler pour récupérer cette clé. Garde-le secret, garde-le en sécurité. En cas de perte, vous devrez supprimer la clé et réautoriser la nouvelle clé API avec chaque périphérique que vous souhaitez protéger avec Umbrella.

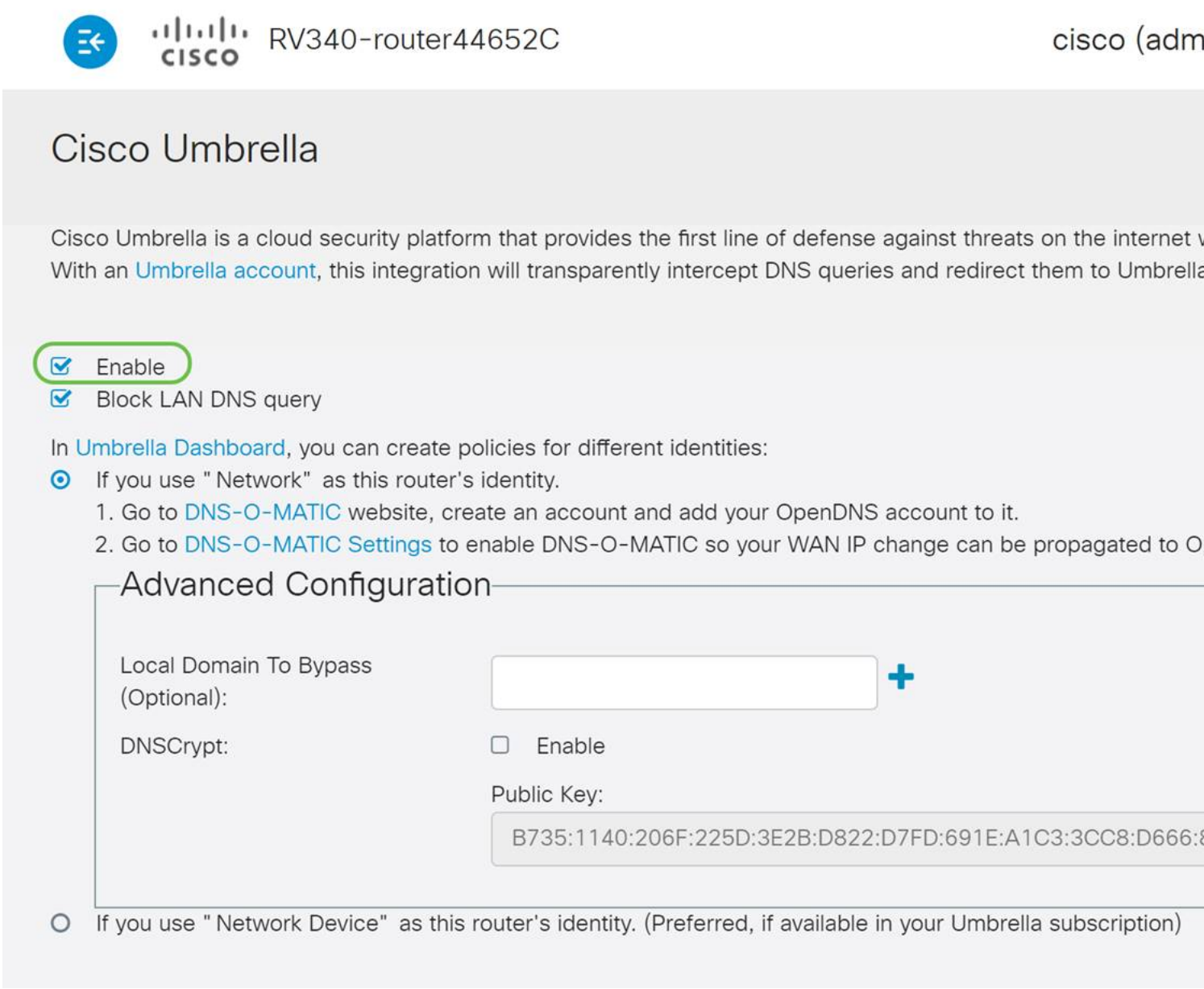
Meilleure pratique : Conservez une *seule* copie de ce document sur un périphérique, comme une clé USB, inaccessible depuis n'importe quel réseau.

Configuration de Umbrella sur votre périphérique RV34x

Maintenant que nous avons créé les clés API dans Umbrella, nous allons les prendre et les installer sur nos périphériques RV34x. Dans notre cas, nous utilisons un RV340.

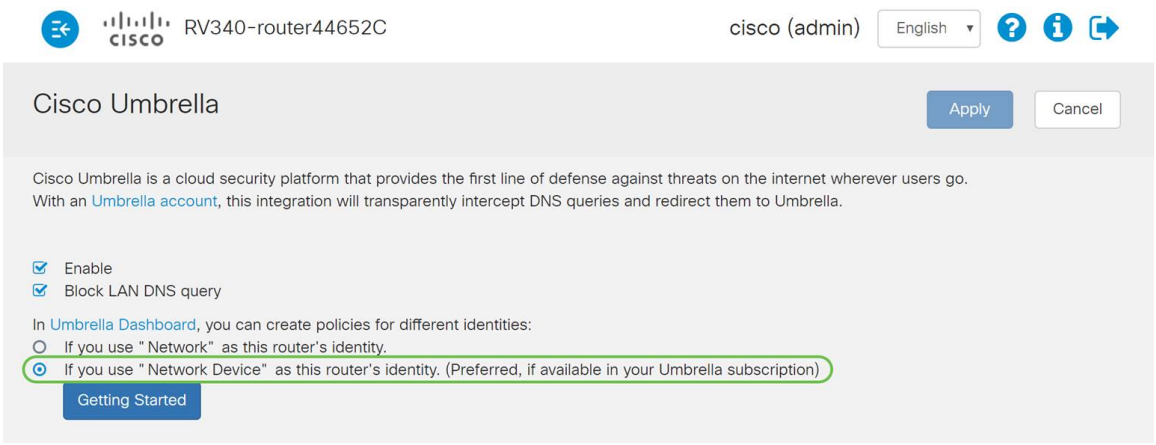
Étape 1. Après vous être connecté à votre périphérique RV34x, cliquez sur **Security > Umbrella** dans le menu de la barre latérale.

Étape 2. L'écran de l'API Umbrella propose une série d'options. Activez Umbrella en cochant la case **Enable (Activer)**.

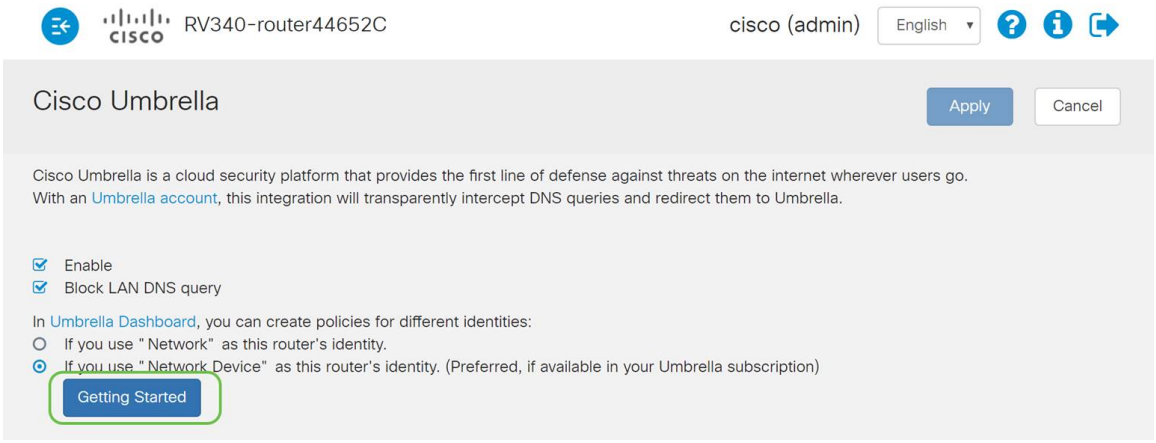


Étape 3. (Facultatif) Par défaut, la case Bloquer les requêtes DNS du réseau local est cochée. Cette fonctionnalité soignée crée automatiquement des listes de contrôle d'accès sur votre routeur, ce qui empêche le trafic DNS d'accéder à Internet. Cette fonctionnalité force toutes les requêtes de traduction de domaine à être dirigées par le RV34x et est une bonne idée pour la plupart des utilisateurs.

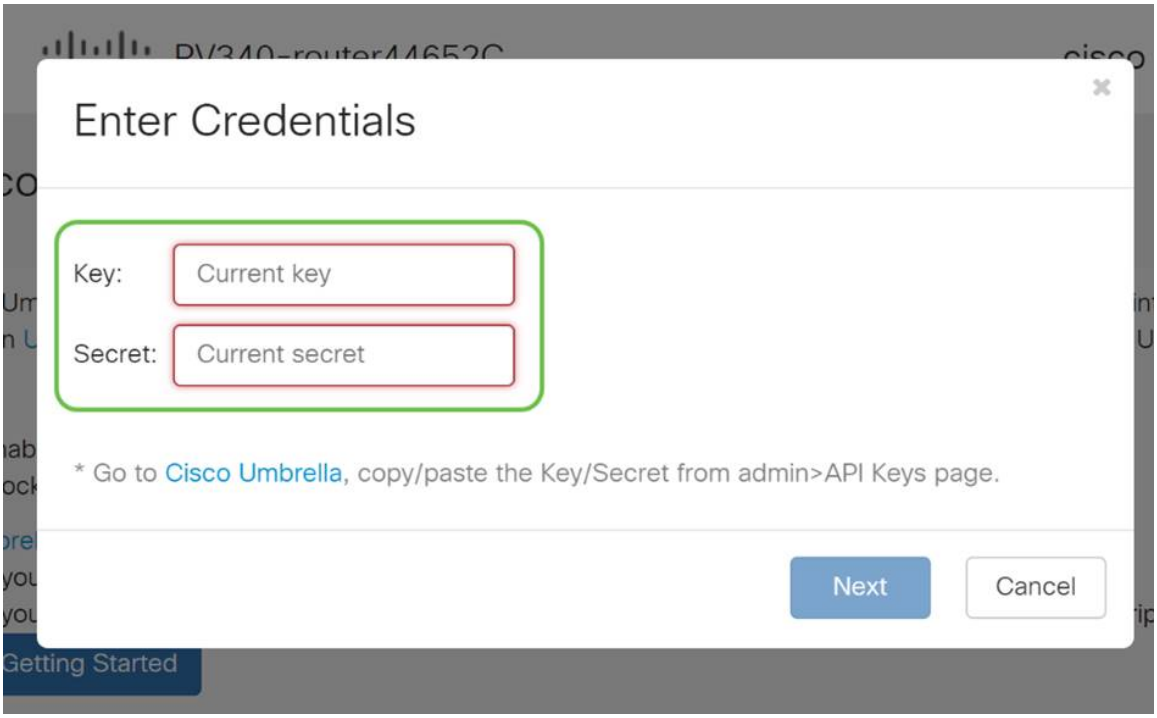
Étape 4. L'étape suivante se déroule de deux façons différentes. Ils dépendent tous deux de la configuration de votre réseau. Si vous utilisez un service tel que DynDNS ou NoIP, vous conserverez le schéma d'attribution de noms par défaut « Réseau ». Ensuite, vous devrez vous connecter à ces comptes pour assurer l'interface d'Umbrella avec ces services, car ils offrent une protection. Pour nos besoins, nous nous appuyons sur « Network Device » (Périphérique réseau), cliquez sur le bouton radial inférieur.



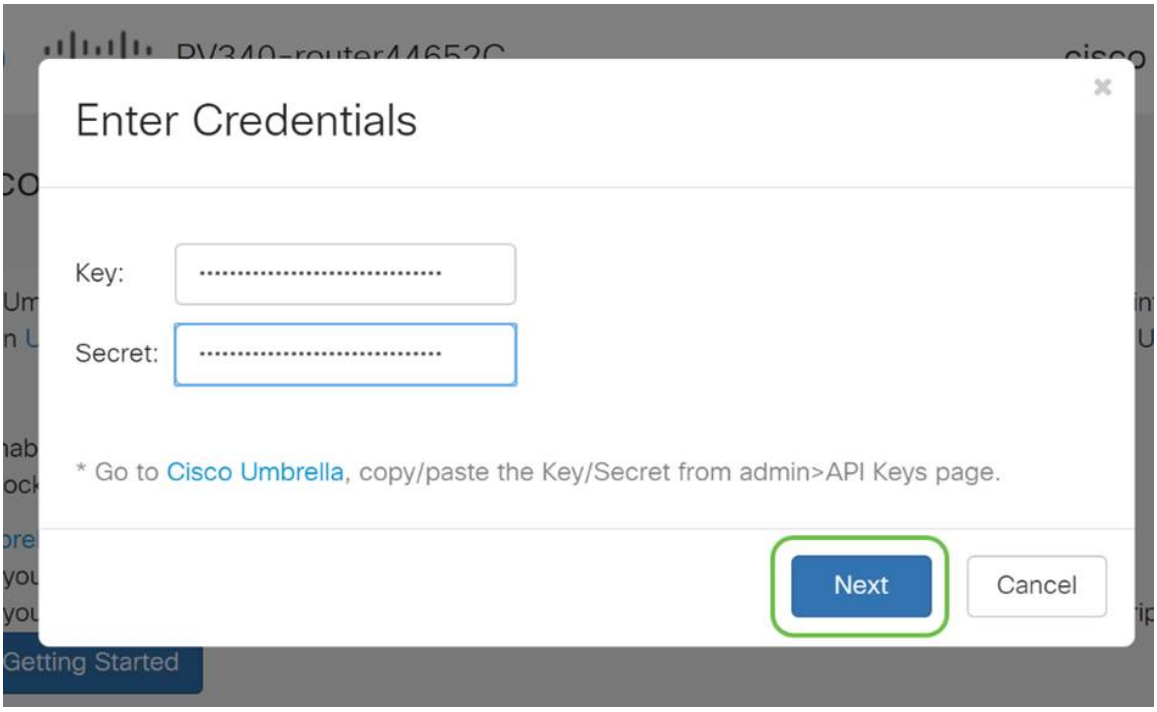
Étape 5. Cliquez maintenant sur **Getting Started** pour lancer le mini-assistant.



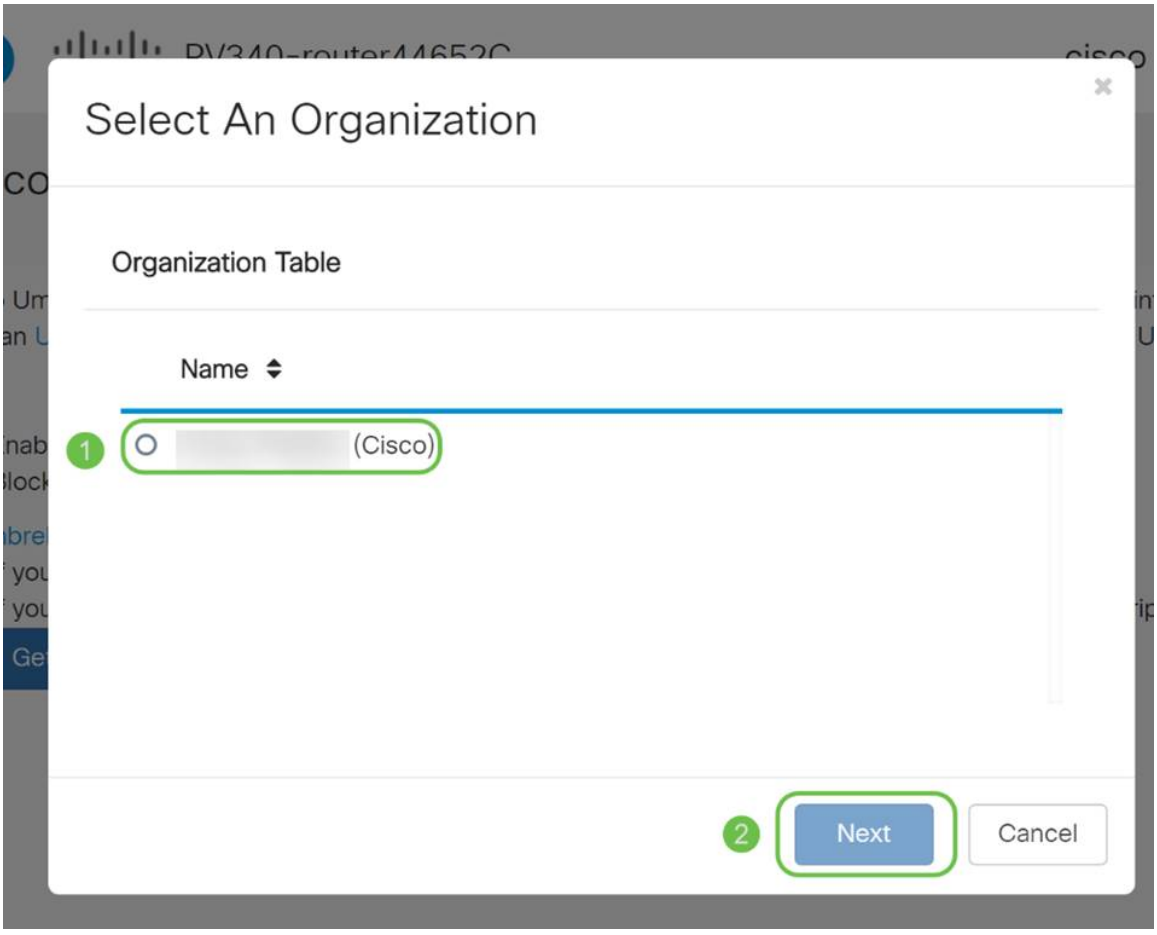
Étape 6. Entrez maintenant la **clé API** et la **clé secrète** dans les zones de texte.



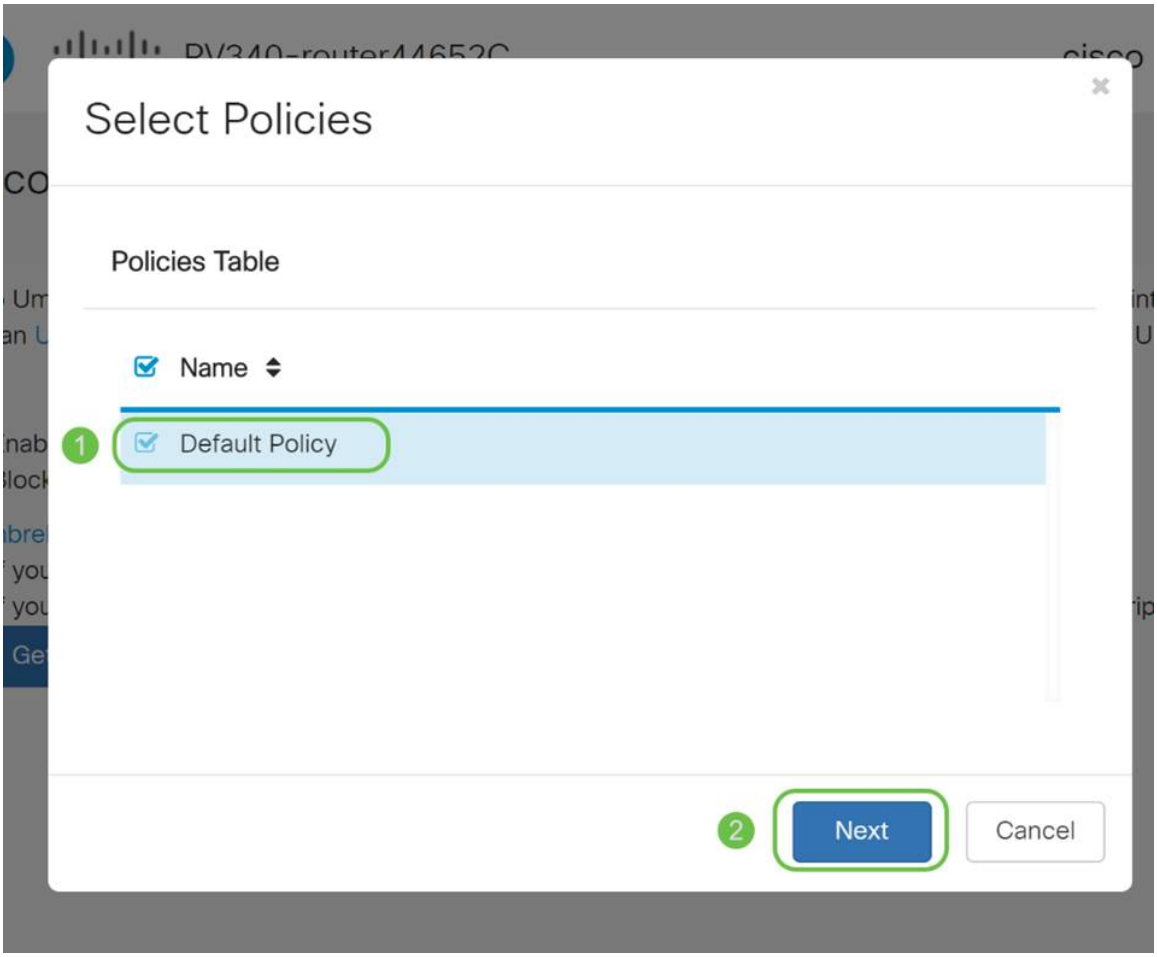
Étape 7. Après avoir saisi votre API et votre clé secrète, cliquez sur le bouton **Next**.



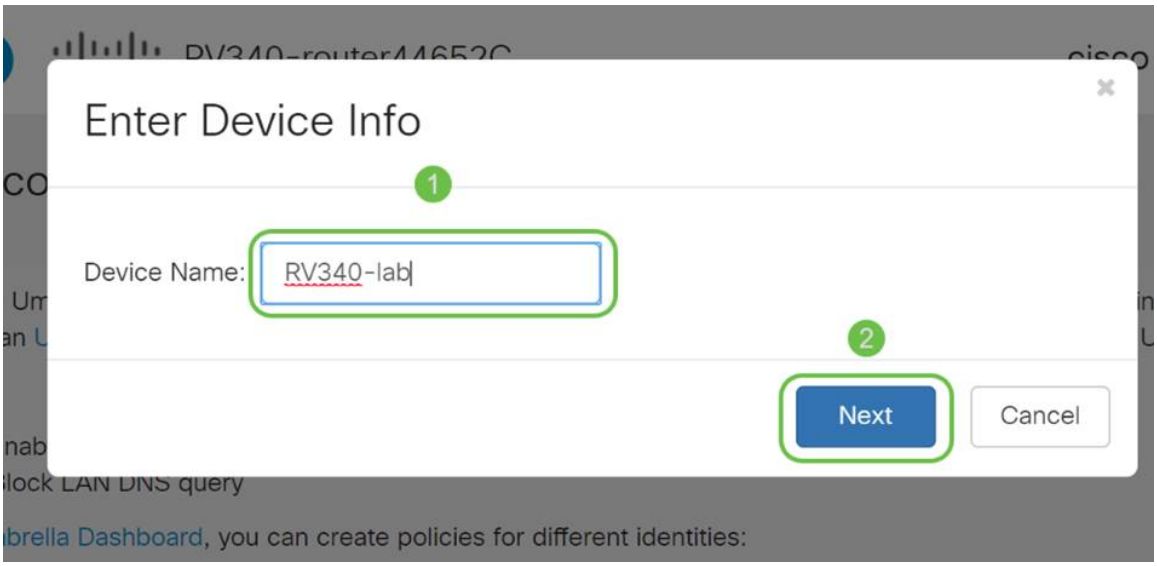
Étape 8. Dans l'écran suivant, sélectionnez l'**organisation** que vous souhaitez associer au routeur, puis cliquez sur **Next**.



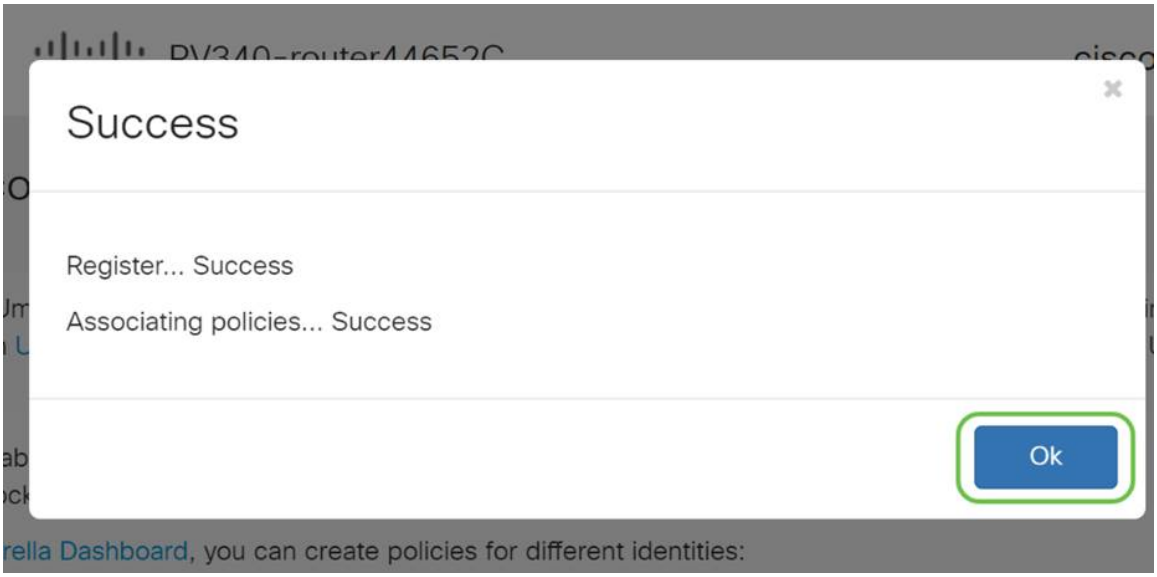
Étape 9. Sélectionnez maintenant la stratégie à appliquer au trafic routé par le RV34x. Pour la plupart des utilisateurs, la stratégie par défaut fournit une couverture suffisante.



Étape 10. **Attribuez un nom** au périphérique afin qu'il puisse être désigné dans le rapport Umbrella. Dans notre configuration, nous avons attribué « RV340-lab ».



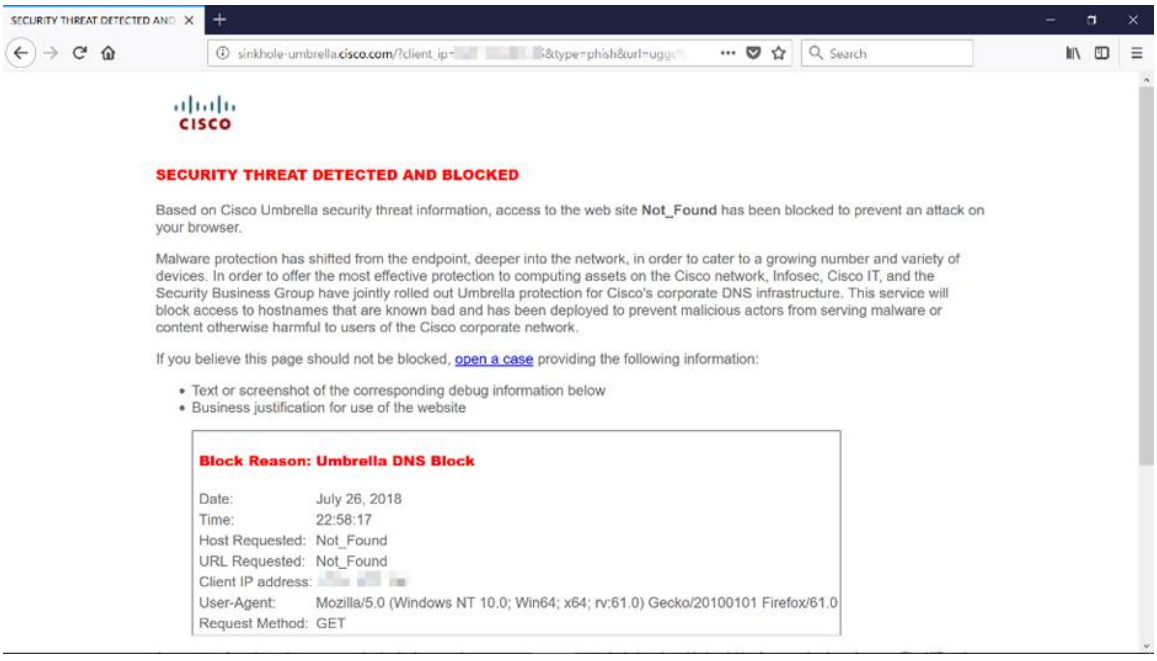
Étape 11. L'écran suivant valide les paramètres que vous avez choisis et fournit une mise à jour. Une fois associé, cliquez sur **OK**.



Confirmer que tout est à sa place

Félicitations, vous êtes désormais protégé par Cisco Umbrella. Ou vous êtes ? Assurez-vous qu'en vérifiant à nouveau avec un exemple en direct, Cisco a créé un site Web dédié à la détermination de ce problème dès que la page se charge. Cliquez ici ou tapez https://InternetBadGuys.com dans la barre du navigateur.

Si Umbrella est configuré correctement, vous serez accueilli par un écran similaire à celui-ci !



Voir une vidéo liée à cet article...

Cliquez ici pour afficher d'autres présentations techniques de Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.