Configurer le client d’itinérance Umbrella sur un réseau d’entreprise

Table des matières

Introduction

Ce document décrit la configuration du client d'itinérance Umbrella sur le réseau de votre entreprise.

Aperçu

Le client d'itinérance Umbrella est un excellent outil de protection des utilisateurs distants, mais il peut également protéger les utilisateurs de votre réseau d'entreprise, ajoutant ainsi une couche de sécurité supplémentaire. En fonction des besoins de l'entreprise, certains administrateurs souhaitent que le client Umbrella roaming continue à être protégé sur le réseau de l'entreprise, tandis que d'autres préfèrent que le client Umbrella roaming soit « retiré » au profit d'autres politiques Umbrella.

Umbrella offre une grande souplesse quant au fonctionnement du client d'itinérance Umbrella lorsqu'il entre dans votre réseau. Cet article présente ces différentes approches.

Objectifs

Q). Pourquoi désactiver le client d'itinérance Umbrella sur le réseau de mon entreprise ?

Il n’est normalement pas nécessaire de désactiver le client d’itinérance Umbrella pour que le DNS interne et externe fonctionne. Le client d'itinérance Umbrella utilise la fonctionnalité Domain Management pour diriger votre trafic DNS interne vers vos serveurs DNS normaux. Cela vous permet de conserver à la fois la protection et la connectivité pendant que le client d'itinérance Umbrella s'exécute sur vos terminaux sur le réseau.

Cependant, il y a parfois des raisons d'envisager de désactiver la protection du client d'itinérance...

- Fournir une stratégie « *sur réseau* » et « *hors réseau* » différente aux utilisateurs itinérants qui quittent le réseau.
- L'utilisation d'un serveur DNS interne sur un réseau d'entreprise offre certains avantages en termes de mise en cache et de réduction du trafic DNS sortant.
- Le client d'itinérance Umbrella envoie régulièrement des messages d'analyse pour vérifier la connexion à Umbrella. Ce trafic supplémentaire peut être indésirable lorsque vous avez un très grand nombre de clients.

Q) Pourquoi voudrais-je que le client d'itinérance Umbrella reste activé sur le réseau de mon entreprise ?

D'un autre côté, il y a de très bonnes raisons de maintenir le client d'itinérance activé à tout moment :

- Assurez-vous que l'ordinateur client d'itinérance Umbrella utilise la même stratégie à tout moment.
- Toujours avoir le nom d'hôte du client d'itinérance Umbrella identifiable dans les rapports (au lieu de l'identité réseau) - pour un rapport granulaire.
- Le client d'itinérance utilise le trafic « DNS chiffré » pour une confidentialité améliorée
- Pour les utilisateurs de la passerelle Web sécurisée (utilisant AnyConnect), le client doit rester activé pour fournir le filtrage Web SWG.

Modes de fonctionnement

Toujours actif

Le client d'itinérance Umbrella peut rester actif même s'il est utilisé sur le réseau de l'entreprise. Dans ce mode, les stratégies sont configurées à l'aide de l'identité du client d'itinérance Umbrella, et cette identité apparaît dans les rapports.

Policy (politique)	L'identité du client d'itinérance Umbrella est toujours utilisée.
Rapports	L'identité du client d'itinérance Umbrella apparaît toujours dans les rapports offrant une granularité par machine
Trafic DNS	• Le client d'itinérance Umbrella continue d'envoyer des requêtes DNS

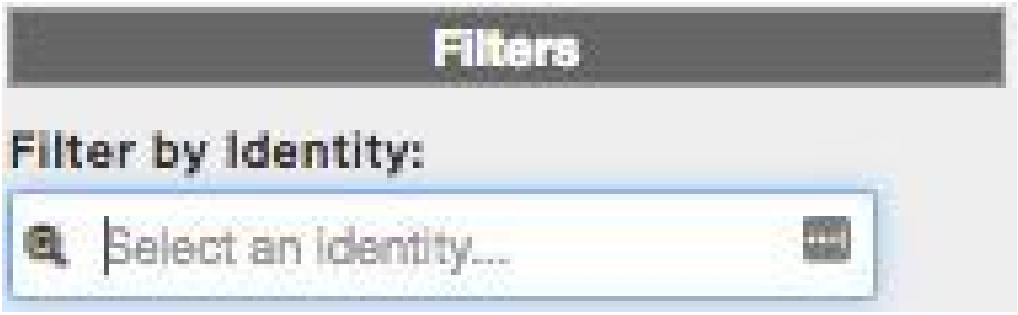
	directement à Umbrella, même sur un réseau d'entreprise. • Les requêtes envoyées à Umbrella sont chiffrées, ce qui renforce la sécurité. • Les requêtes pour les « domaines internes » sont acheminées vers vos serveurs DNS normaux et ne sont pas envoyées à Umbrella.
Messages de sondage	Le client d'itinérance Umbrella continue d'envoyer des messages d'analyse pour déterminer la disponibilité d'Umbrella.

Comment configurer le mode 'Always ON' :

1. Accédez à Identités > Ordinateurs itinérants.
2. Cliquez sur l'icône (Paramètres du client d'itinérance).
3. Effacez Désactiver la redirection DNS sur un réseau protégé par Umbrella et cliquez sur Enregistrer.
4. Créez une politique distincte pour vos clients Umbrella roaming et assurez-vous qu'elle est la priorité la plus élevée (tout en haut de la liste). Votre politique de client d'itinérance Umbrella doit avoir une priorité plus élevée que toute autre politique basée sur les identités réseau.

Utiliser une politique de réseau normale
Le client d'itinérance Umbrella est activé et continue à parler directement à Umbrella. Toutefois, l'identité réseau est utilisée à des fins de stratégie et de création de rapports. Ce mode est activé simplement en plaçant la stratégie réseau à une priorité plus élevée que la stratégie client d'itinérance Umbrella.

Policy (politique)	La stratégie réseau est utilisée sur le réseau protégé. Cela permet différentes politiques de réseau en marche/arrêt.
Rapports	• La création de rapports est associée à l'identité réseau en tant qu'identité principale. • La création de rapports vous permet toujours d'effectuer une recherche via le nom d'hôte du client d'itinérance Umbrella pour filtrer les résultats pour ce client uniquement.

	
Trafic DNS	• Le client d'itinérance Umbrella continue d'envoyer des requêtes DNS directement à Umbrella, même sur un réseau d'entreprise. • Les requêtes envoyées à Umbrella sont chiffrées, ce qui renforce la sécurité. • Les requêtes pour les « domaines internes » sont acheminées vers vos serveurs DNS normaux et ne sont pas envoyées à Umbrella.
Messages de sondage	Le client d'itinérance Umbrella continue d'envoyer des messages d'analyse pour déterminer la disponibilité d'Umbrella.

Comment « utiliser une politique de réseau standard » :

1. Accédez à Identités > Ordinateurs itinérants.
2. Cliquez sur l'icône (Paramètres du client d'itinérance).
3. Effacez Désactiver la redirection DNS sur un réseau protégé par Umbrella et cliquez sur Enregistrer.
4. Créez une stratégie distincte pour votre ou vos réseaux. Assurez-vous que la stratégie de votre ou vos réseaux a une priorité plus élevée que toute stratégie basée sur le client d'itinérance.

Désactiver derrière les réseaux protégés (idéal pour les réseaux plus petits)
Le client d'itinérance Umbrella peut « se désactiver » lorsqu'il détecte qu'il se trouve sur un réseau protégé. Cela signifie que l'identité réseau est utilisée à des fins de politique et de création de rapports.

Ce mode a un comportement similaire à celui du mode « Use Regular Network Policy », à ceci près que le client d'itinérance Umbrella se désactive lui-même et n'interfère pas avec le trafic DNS.

Policy (politique)	La stratégie réseau est utilisée sur le réseau protégé. Cela permet différentes politiques de réseau en marche/arrêt.

Rapports	Lorsque le réseau protégé n'offre aucune granularité par machine pour le rapport. La création de rapports est associée à l'identité réseau uniquement.
Trafic DNS	Lorsque le client d'itinérance Umbrella se trouve sur le réseau protégé, il n'interfère pas avec les requêtes DNS et se connecte au serveur DNS interne normal.
Messages de sondage	Le client d'itinérance Umbrella continue d'envoyer des messages d'analyse pour déterminer qu'il se trouve sur un réseau protégé.

Comment configurer la désactivation derrière les réseaux protégés :

1. Accédez à Identités > Ordinateurs itinérants.
2. Cliquez sur l'icône (Paramètres du client d'itinérance).
3. Sélectionnez Disable DNS redirection while on an Umbrella Protected Network et cliquez sur Save.
4. Accédez à Policies > Policies List.
5. Créez une stratégie distincte pour votre ou vos réseaux. Assurez-vous que la stratégie de votre ou vos réseaux est prioritaire par rapport à toutes les stratégies basées sur le client d'itinérance Umbrella.
6. Vos serveurs DNS locaux doivent être transférés vers les résolveurs Umbrella et doivent être correctement enregistrés dans le tableau de bord Umbrella.
7. Pour que cette fonctionnalité fonctionne, l'adresse IP de sortie utilisée par la station de travail cliente doit être enregistrée sur la même identité réseau que l'adresse IP de sortie utilisée par vos serveurs DNS internes. Pour plus de détails, consultez cet article.

Désactiver derrière le domaine de réseau approuvé (idéal pour les grands réseaux)

Il est désormais possible de choisir un « domaine de réseau approuvé » configuré par le client. Le client tente de résoudre ce domaine DNS (enregistrement A) et de désactiver la protection lorsque le domaine est résolu. Il s'agit d'un enregistrement DNS interne uniquement qui se résout uniquement lorsque le client se trouve sur le réseau de l'entreprise.

Policy (politique)	Le client se désactive chaque fois que le domaine approuvé est détecté et ne reçoit pas nécessairement la stratégie Umbrella ou le filtrage. Nous vous recommandons d'ajouter d'autres fonctions de parapluie (par ex. protection du réseau) pour garantir que la stratégie est toujours appliquée sur le réseau de l'entreprise.

Rapports	Le client se désactive chaque fois que le domaine approuvé est détecté et ne reçoit pas nécessairement la stratégie Umbrella ou le filtrage. Si le réseau est protégé par d'autres fonctionnalités Umbrella (par ex. Protection du réseau), le trafic apparaît dans les rapports sous l'identité du réseau.
Trafic DNS	Lorsque le client d'itinérance Umbrella se trouve sur le réseau approuvé, il n'interfère pas avec les requêtes DNS et il se connecte au serveur DNS interne normal.
Messages de sondage	Le client d'itinérance Umbrella désactive la majorité de ses tests de « sonde » DNS dans cet état, réduisant ainsi considérablement la quantité de trafic générée par les clients d'itinérance.

Comment configurer le domaine de réseau approuvé :

1. Créez un enregistrement DNS A sur vos serveurs DNS internes (par ex. magic.mondomaine.tld).
    1. L'enregistrement doit être un « sous-domaine » (3 étiquettes DNS minimum)
    2. L'enregistrement doit être résolu en une adresse RFC-1918 interne
    3. Veillez à ce que le dossier n'existe pas publiquement
2. Accédez à Identités > Ordinateurs itinérants.
3. Cliquez sur l'icône (Paramètres du client d'itinérance).
4. Sélectionnez l'option Trusted Network Domain et entrez le nom de domaine (par ex. magic.mondomaine.tld). Cliquez sur Save.

Utilisation du client d'itinérance Umbrella avec un appareil virtuel Umbrella

Dans le cadre du produit Umbrella « Insights » (dans les packages Platform et Insights), nous fournissons un appareil virtuel (VA) qui agit comme un redirecteur DNS au sein de votre réseau. Cette VA est la clé pour obtenir une visibilité sur la source des requêtes DNS sur votre réseau et est également requise pour notre intégration Active Directory.

Par défaut, le client d'itinérance Umbrella se désactive s'il détecte qu'une adresse virtuelle est utilisée pour le transfert DNS. Si l'appliance virtuelle a été attribuée en tant que serveur DNS (à l'aide de paramètres DHCP ou statiques), le client d'itinérance Umbrella le détecte et se désactive.

Désactivation VA

Policy (politique)	Lorsque la fonction VA Backoff est activée, l'identité VA est utilisée pour décider de la stratégie choisie. Les politiques peuvent être créées en fonction des identités suivantes : • Utilisateur AD (uniquement si l'intégration AD est activée) • Ordinateur AD (uniquement si l'intégration AD est activée) • Réseau interne • Nom du site parapluie. Cliquez ici pour plus d'informations sur la priorité des stratégies.
Rapports	Lorsque la fonction VA Backoff est activée, le client d'itinérance Umbrella est désactivé lorsqu'il se trouve derrière une VA et n'est pas affiché dans les rapports. Le rapport est consigné comme suit : • Utilisateur AD (uniquement si l'intégration AD est activée) • Ordinateur AD (uniquement si l'intégration AD est activée) • Réseau interne • Nom du site parapluie. En outre, l'adresse IP du client interne est consignée pour chaque requête. 
Trafic DNS	• Le client d'itinérance Umbrella n'interfère pas avec les requêtes DNS et elles accèdent à l'appliance virtuelle. • L'appliance virtuelle transfère les requêtes DNS externes à Umbrella (chiffrées). • L'appliance virtuelle achemine les requêtes DNS internes selon les besoins et les transfère aux serveurs DNS internes configurés.
Messages de sondage	Le client d'itinérance Umbrella envoie toujours des messages d'analyse à Umbrella, mais à un tarif réduit.

Configuration de la désactivation VA :

1. Cette fonctionnalité est activée par défaut, mais vous pouvez vérifier son état (et éventuellement la désactiver)
2. Accédez à Identités > Ordinateurs itinérants.
3. Cliquez sur l'icône (Paramètres du client d'itinérance).

4. Sélectionnez l'option VA Backoff

Module de sécurité d'itinérance Cisco Umbrella AnyConnect

Le module Umbrella pour Cisco AnyConnect prend en charge tous les modes de fonctionnement décrits ci-dessus. Deux autres modes spécifiques à AnyConnect sont également disponibles. Ces deux modes peuvent être activés dans votre tableau de bord Umbrella sur la page Identities > Roaming Computers, cependant, une configuration supplémentaire est requise dans le profil VPN AnyConnect.

- Respectez la détection de réseau sécurisé AnyConnect.
  Cette fonctionnalité entraîne la désactivation du module Umbrella Security lorsque Cisco AnyConnect détermine qu'il se trouve sur un réseau de confiance. Pour cela, la fonctionnalité Trusted Network Detection d'AnyConnect permet d'identifier le réseau. Les domaines approuvés, les serveurs DNS et les URL peuvent être utilisés pour identifier le réseau de votre entreprise. Pour plus d'informations, consultez la documentation AnyConnect.
- Désactiver le client d'itinérance lorsque les sessions VPN de tunnel complet sont actives
  Lorsque cette fonction est activée, le module Umbrella est désactivé lorsqu'AnyConnect est connecté à un VPN Full Tunnel (ou Tunnel All DNS).

Lorsqu'il est désactivé, le client d'itinérance ne filtre pas le trafic DNS. Il est donc important de s'assurer que votre réseau est couvert par d'autres mesures de sécurité, telles que notre fonction de protection du réseau.

Plus d'informations

Si vous souhaitez désactiver le client d'itinérance sur le réseau de votre entreprise, mais que vous avez besoin de plus de contrôle, ou si vous souhaitez discuter d'autres options, contactez l'assistance Cisco Umbrella.

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.