Configurer les stratégies SIG pour l'accès à distance pour les utilisateurs Secure Connect

Table des matières

Introduction

Aperçu

Stratégies DNS

Stratégies de pare-feu

Stratégies Web

- Identification des utilisateurs Web

Stratégies DLP

- Identification utilisateur DLP

Introduction

Ce document décrit comment créer des stratégies SIG pour l'accès à distance pour les utilisateurs Secure Connect.

Aperçu

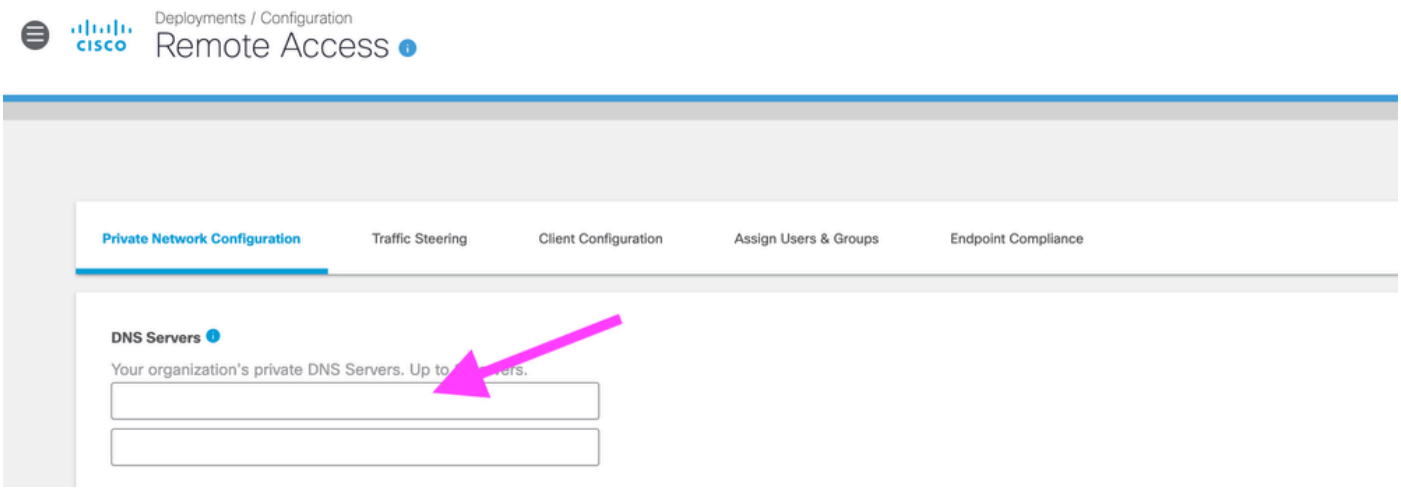
Cet article de la base de connaissances s'applique aux clients utilisant le package Secure Connect qui inclut la fonctionnalité d'accès à distance (VPNaaS) dans Umbrella.

Les administrateurs peuvent configurer les politiques Umbrella Firewall, Web et Data Loss pour les appliquer aux utilisateurs itinérants connectés à l'accès à distance via AnyConnect.

Stratégies DNS

Il est possible d'envoyer des requêtes DNS aux résolveurs Umbrella (par ex. 208.67.222.222) via la connexion VPN AnyConnect Remote Access. Cependant, cela n'active pas l'identification, la stratégie ou la création de rapports du trafic DNS sur le tableau de bord Umbrella.

- Cette option fournit uniquement la résolution DNS et n’est donc généralement pas recommandée.
- L'utilisation de résolveurs DNS externes dans votre configuration DNS VPN empêche la résolution des zones DNS internes.

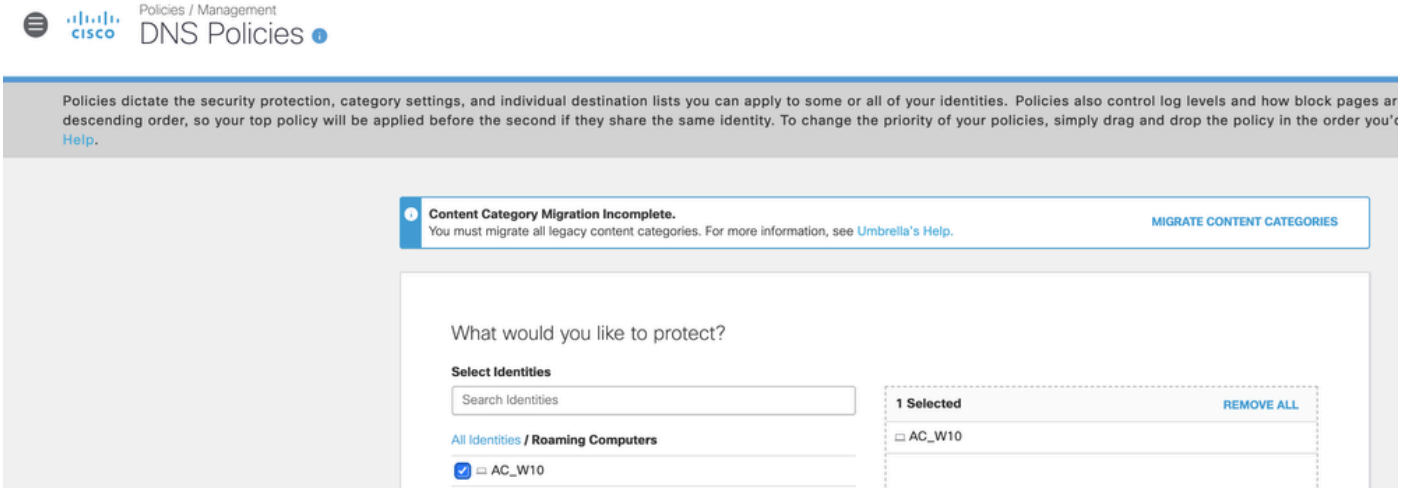


4410210378004

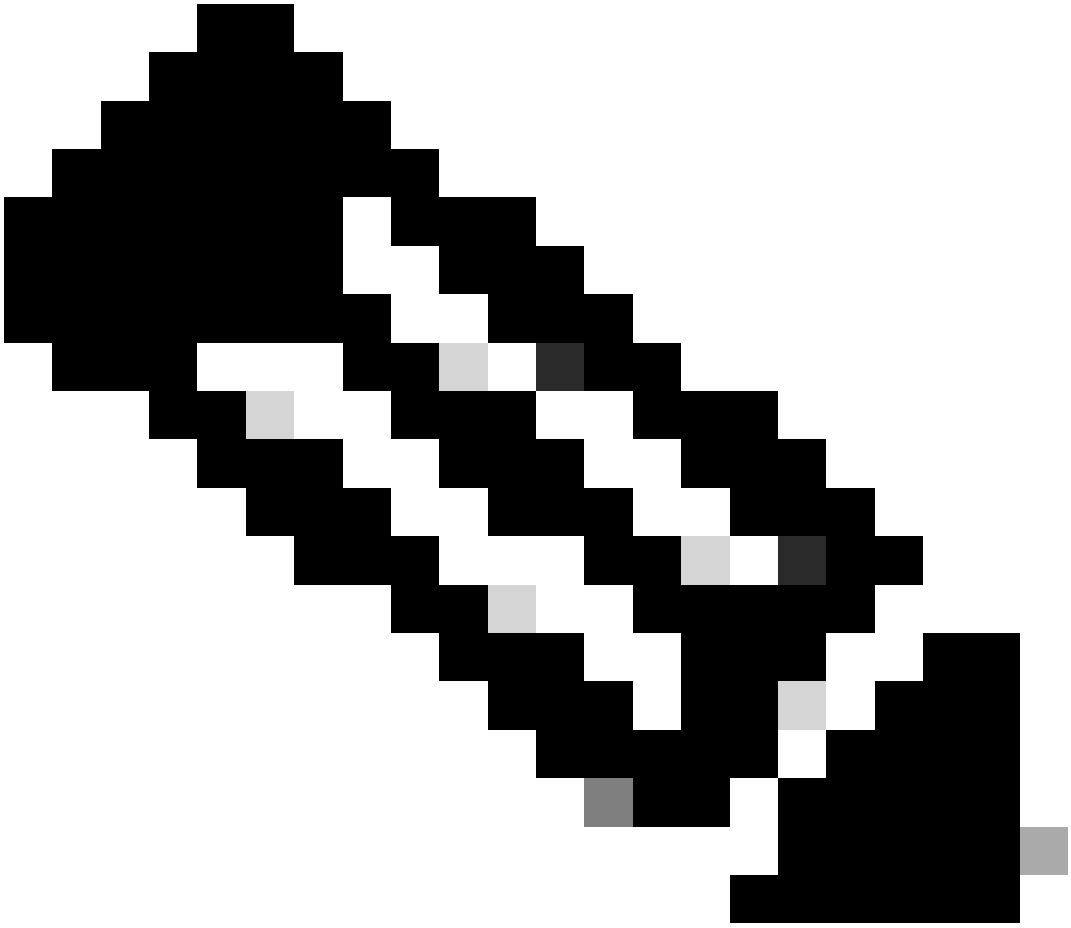
Pour ajouter des identités, des stratégies et des rapports pour les requêtes DNS, l'une des trois méthodes suivantes doit être prise en compte :

- (Recommandé) - Déployez le module d'itinérance Umbrella AnyConnect (dans Déploiements > Ordinateurs itinérants). Le trafic DNS externe est envoyé directement à Umbrella avec l'identité « Ordinateur itinérant » appliquée. Ce module prend également en charge l'identification utilisateur AD facultative.
- Transférez le trafic de votre serveur DNS sur site vers Umbrella et identifiez le trafic à l'aide d'une identité réseau. Tous les utilisateurs reçoivent la même stratégie/identité et il n'y a pas de rapport d'utilisateur granulaire.
- Utilisez un appareil virtuel Umbrella sur votre réseau sur site pour transférer le trafic vers Umbrella. Les requêtes DNS peuvent être identifiées par leur adresse IP interne (pool VPN). L'intégration AD peut être ajoutée - nécessite l'installation de composants sur site supplémentaires.

Cet exemple montre comment une stratégie DNS peut être configurée (Policies > DNS Policies) pour un client AnyConnect individuel. Cela n'est possible que lorsque le module d'itinérance AnyConnect Umbrella est déployé :



4410210455444



Remarque : Lorsque vous utilisez le module Umbrella pour AnyConnect, le trafic DNS peut être envoyé à l'intérieur ou à l'extérieur du tunnel, en fonction de votre configuration de transmission tunnel partagée.

Stratégies de pare-feu

Les stratégies de pare-feu s'appliquent au trafic entre les clients d'accès à distance (AnyConnect) et Internet. Configurez les règles dans 'Déploiements > Politique de pare-feu' conformément à la documentation disponible ici : Gérer le pare-feu.

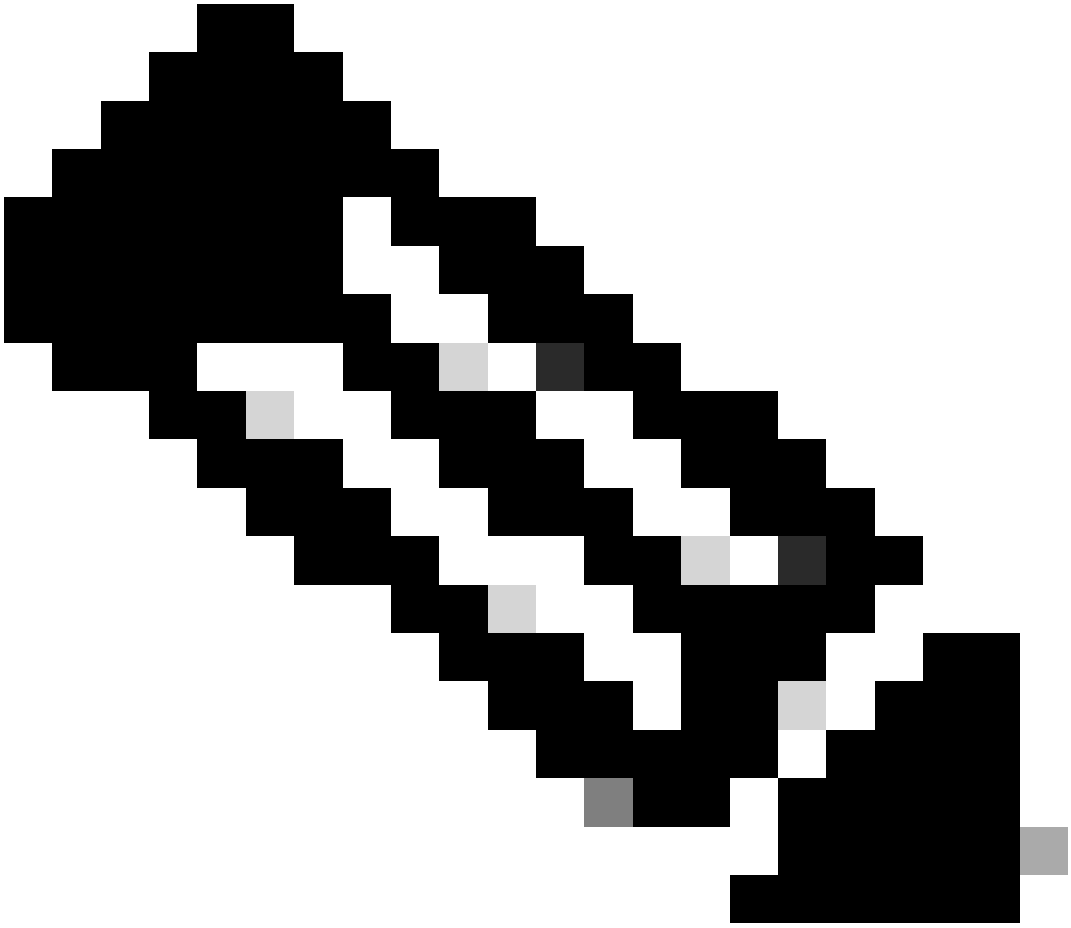
La règle de pare-feu par défaut s'applique aux clients d'accès distant. Si vous créez une stratégie spécifique pour les utilisateurs d'accès à distance, vous pouvez éventuellement choisir de créer une nouvelle stratégie de pare-feu et sélectionner « Remote Access Orgid:<ID> » comme identité de tunnel source.
La même stratégie de pare-feu s'applique à tous les utilisateurs d'accès distant.

- Les stratégies de pare-feu ne sont pas utilisées pour contrôler l'accès entre les clients RA et

les réseaux privés/de filiale. Cela doit être contrôlé par des pare-feu sur site.

- Comme toutes les règles de pare-feu Umbrella, ces règles contrôlent les connexions sortantes pour les clients d'accès à distance. Les connexions entrantes ne sont jamais autorisées.
- L'adresse IP source des clients d'accès à distance est toujours attribuée dynamiquement à partir du pool VPN.
    - Il n'est pas recommandé de créer des règles pour un ordinateur spécifique à l'aide de l'adresse IP source, car l'adresse IP est réattribuée dynamiquement
    - La création de règles affectant les utilisateurs d'un data center d'accès à distance spécifique est possible à l'aide d'une plage « Source CIDR ». Chaque data center fournit une plage de pools VPN différente qui est configurée sur la page « Déploiements > Accès à distance ».

4409322341524



Remarque : L'identification par utilisateur n'est pas disponible pour les stratégies de pare-feu.

Stratégies Web

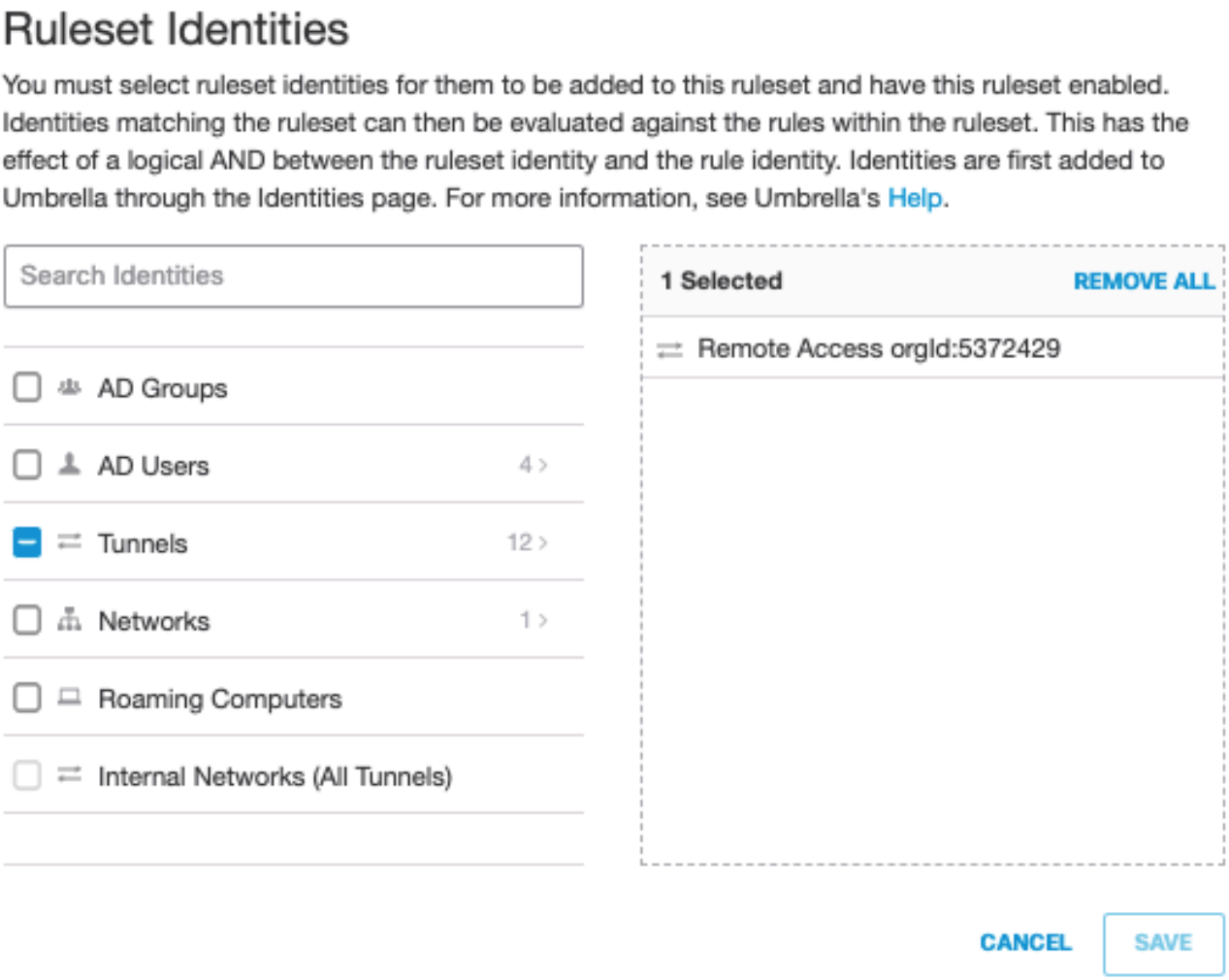
Les stratégies Web s'appliquent au trafic entre les clients d'accès à distance (AnyConnect) et Internet. Configurez les règles dans 'Déploiements > Stratégies Web' conformément à la documentation disponible ici : Gérer les stratégies Web.

- Les stratégies Web ne sont pas utilisées pour contrôler l'accès entre les clients RA et les serveurs Web privés/de filiale. Les stratégies Web s'appliquent uniquement aux sites Web externes.

La stratégie Web par défaut s'applique aux clients d'accès à distance. Toutefois, nous vous recommandons de créer un nouvel ensemble de règles pour définir les paramètres de sécurité spécifiquement pour les clients d'accès distant. Lors de la définition des identités de l'ensemble de règles, choisissez Remote Access orgid:<ID> dans la liste des tunnels. La même stratégie

Web s'applique à tous les utilisateurs d'accès à distance.

Après avoir créé un jeu de règles, il est possible d'ajouter une règle Web à laquelle sont définis le filtrage des catégories de contenu et les paramètres d'application.

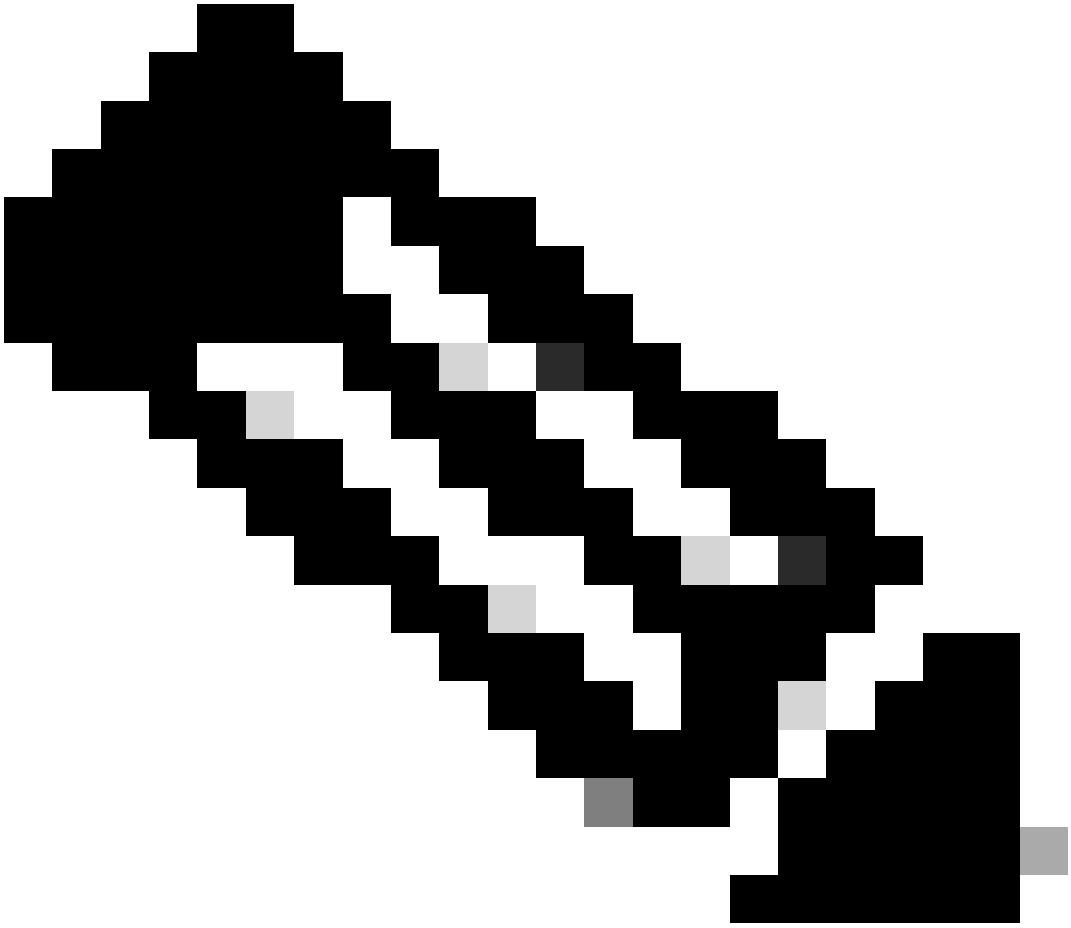


4409322363924

Identification des utilisateurs Web

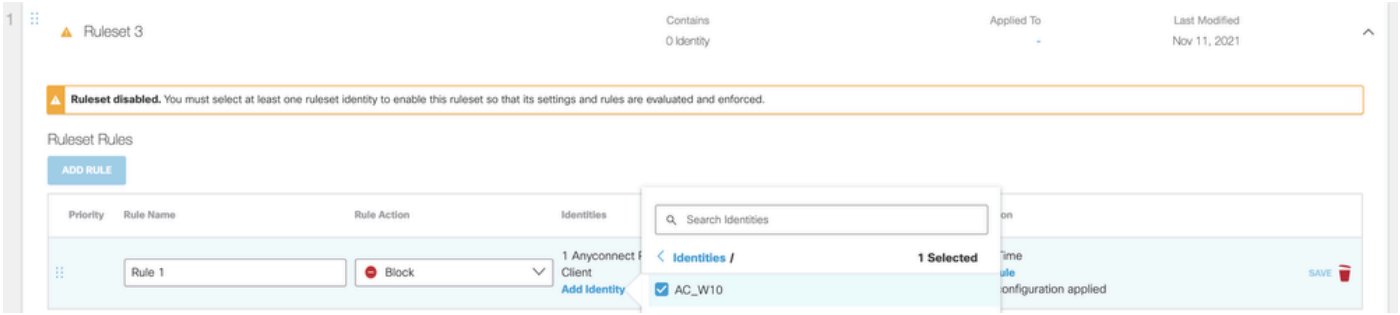
Par défaut, le trafic d'accès à distance ne peut pas être contrôlé par utilisateur ou par groupe. La même stratégie s'applique à tout le trafic RA basé sur l'identité « Remote Access Orgid ». Pour ajouter une identification d'utilisateur/de groupe, vous avez deux options :

- Installez le module AnyConnect Umbrella Roaming Security et activez la fonction d'agent SWG. L'agent envoie le trafic Web directement à Umbrella SWG avec l'identité « Ordinateur itinérant » appliquée. Ce module prend également en charge l'identification utilisateur AD facultative.
- Activez SAML dans le jeu de règles Web qui affecte votre identité « Remote Access Orgid ». Après la connexion à l'accès à distance, les utilisateurs RA sont invités à s'authentifier via SAML une seconde fois lors de la génération du trafic du navigateur Web.



Remarque : Lors de l'utilisation du module Umbrella pour AnyConnect, le trafic SWG peut éventuellement être envoyé à l'intérieur ou à l'extérieur du tunnel, en fonction de votre configuration de transmission tunnel partagée.

Cet exemple montre comment une stratégie DNS peut être configurée (Stratégies > Stratégies DNS) pour un client AnyConnect individuel. Cela n'est possible que lorsque le module d'itinérance Umbrella AnyConnect est déployé :

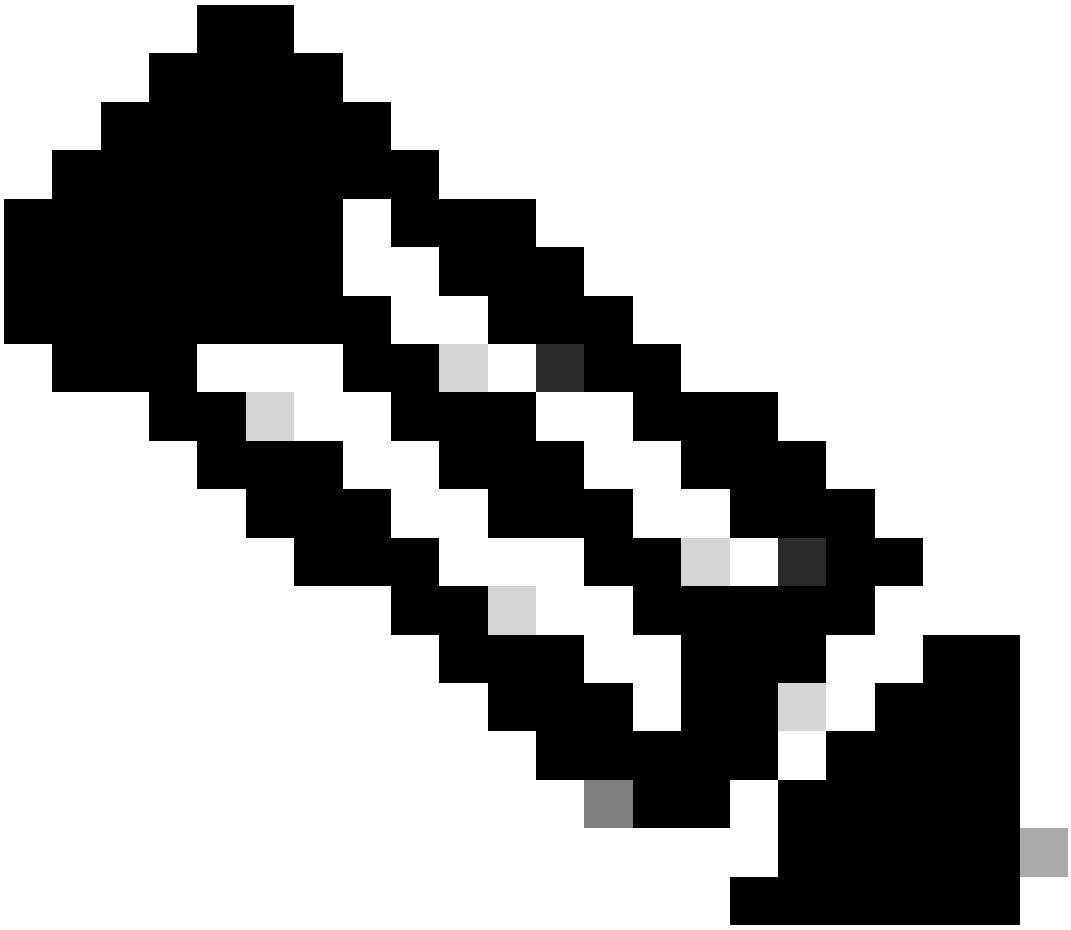


4410210499476

Stratégies DLP

Les stratégies de perte de données s'appliquent au trafic entre les clients d'accès à distance (AnyConnect) et Internet. Configurez les règles dans « Déploiements > Stratégies de prévention contre la perte de données » conformément à la documentation disponible ici : Gérer les politiques de protection des données.

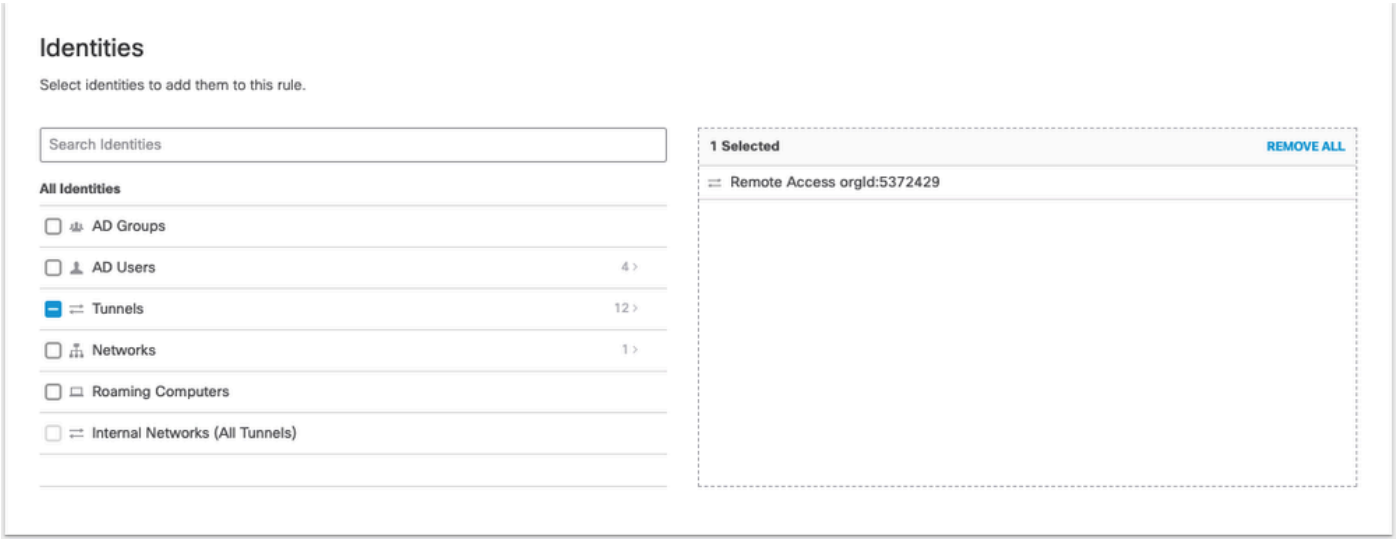
- Les stratégies DLP ne sont pas utilisées pour contrôler l'accès entre les clients RA et les serveurs Web privés/de filiale. Les stratégies DLP s'appliquent uniquement au trafic des sites Web externes.



Remarque : Pour que les stratégies DLP s'appliquent, vous devez d'abord avoir créé un ensemble de règles Web pour les utilisateurs d'accès à distance. Le décodage HTTPS doit être activé pour le jeu de règles Web.

Lorsque vous sélectionnez des identités pour une règle de protection des données, choisissez Remote Access orgid:<ID>. La même stratégie de protection des données s'applique à tous les

utilisateurs. Pour compléter la règle DLP, vous devez également sélectionner ou définir des classificateurs DLP.



4409322428820

Identification utilisateur DLP

DLP obtient l'identité de l'utilisateur de la passerelle Web sécurisée (stratégies Web). Reportez-vous à la section Stratégies Web pour obtenir des instructions sur l'ajout de l'identification utilisateur.

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.