Politiques DNS

Les rubriques suivantes expliquent les politiques DNS, les règles DNS et comment déployer les politiques DNS sur les périphériques gérés.

Aperçu de la politique DNS

La Security Intelligence basée sur DNS vous permet de bloquer le trafic en fonction du nom de domaine demandé par un client, à l'aide d'une liste de blocage de Security Intelligence. Cisco fournit des renseignements sur les noms de domaine que vous pouvez utiliser pour filtrer votre trafic; vous pouvez également configurer des listes et des flux de noms de domaines personnalisés selon votre déploiement.

Le trafic sur une liste de blocage de politique DNS est immédiatement bloqué et n'est donc soumis à aucune inspection supplémentaire, que ce soit pour les intrusions, les exploits, les programmes malveillants, etc., mais aussi pour la découverte de réseau. Vous pouvez utiliser une liste Ne pas bloquer Security Intelligence pour remplacer une liste de blocage et forcer l'évaluation des règles de contrôle d'accès, et, ce qui est recommandé dans les déploiements passifs, vous pouvez utiliser un paramètre de « surveillance seulement » pour le filtrage Security Intelligence. Cela permet au système d'analyser les connexions qui auraient été bloquées par une liste de blocage, mais enregistre également la correspondance avec la liste de blocage et génère un événement Security Intelligence de fin de connexion.

Remarque Les renseignements sur la sécurité basés sur le DNS peuvent ne pas fonctionner comme prévu pour un nom de domaine, à moins que le serveur DNS supprime une entrée du cache de domaine en raison de son expiration, ou que le cache DNS d'un client ou le cache du serveur DNS local soit effacé ou expire.

Vous configurez les renseignements sur la sécurité basés sur DNS à l'aide d'une politique DNS et des règles DNS associées. Pour la déployer sur vos périphériques, vous devez associer votre politique DNS à une politique de contrôle d'accès, puis déployer votre configuration sur les périphériques gérés.

Politiques DNS de Cisco Umbrella

Cisco Umbrella DNS Connection dans le centre de gestion permet de rediriger les requêtes DNS vers Cisco Umbrella. Cela permet à Cisco Umbrella de valider les demandes, de les autoriser ou de les bloquer en fonction des noms de domaine et d'appliquer une politique de sécurité basée sur le DNS à la demande. Si vous utilisez Cisco Umbrella, vous devez configurer Cisco Umbrella Connection (**Intégration > Autres intégrations > Services en nuage > Cisco Umbrella Connection**) pour rediriger les requêtes DNS vers Cisco Umbrella.

Le connecteur Cisco Umbrella fait partie de l'inspection DNS du système. Si votre liste de politiques d'inspection DNS existante décide de bloquer ou d'abandonner une demande en fonction de vos paramètres d'inspection DNS, la demande n'est pas transmise à Cisco Umbrella. Vous disposez ainsi de deux lignes de protection :

- Votre politique d'inspection DNS locale
- Votre politique en nuage de Cisco Umbrella

Lors de la redirection des demandes de recherche DNS vers Cisco Umbrella, le connecteur Cisco Umbrella ajoute un enregistrement EDNS (Extension mécanismes for DNS). Un enregistrement EDNS comprend les renseignements sur l'identifiant du périphérique , l'ID de l'organisation et l'adresse IP du client. Votre politique en nuage peut utiliser ces critères pour contrôler l'accès en plus de la réputation du nom de domaine complet. Vous pouvez également choisir de chiffrer la requête DNS à l'aide de DNSCrypt pour assurer la confidentialité des noms d'utilisateurs et des adresses IP internes.

Pour rediriger les requêtes DNS du centre de gestion vers Cisco Umbrella :

1. Configurez les paramètres de connexion de Cisco Umbrella.
2. Créer et configurer une politique Cisco Umbrella DNS
3. Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès.
4. Déployez les modifications.

Pour des renseignements détaillés sur la configuration de Umbrella DNS Connector dans le centre de gestion, consultez Configurer le connecteur DNS Umbrella pour Cisco Secure Firewall Management Center.

Composants de la politique DNS

Une politique DNS vous permet de bloquer les connexions en fonction d'un nom de domaine, à l'aide d'une liste de blocage, ou d'exempter ces connexions de ce type de blocage à l'aide d'une liste Ne pas bloquer. La liste suivante décrit les configurations que vous pouvez modifier après la création d'une politique DNS.

Nom et description

Chaque politique DNS doit avoir un nom unique. La description est facultative.

Dans un déploiement multidomaine, les noms de politique doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'une politique que vous ne pouvez pas voir dans votre domaine actuel.

Règles

Les règles fournissent une méthode fine de gestion du trafic réseau en fonction du nom de domaine. Les règles d'une politique DNS sont numérotées, en commençant par 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant.

Lorsque vous créez une politique DNS, le système la remplit avec une liste globaleNe pas bloquer pour la règle DNS et une liste de blocage globale par défaut pour cette dernière. Les deux règles sont définies en première position dans leurs catégories respectives. Vous ne pouvez pas modifier ces règles, mais vous pouvez les désactiver.

Dans un déploiement multidomaine, le système ajoute également les listes descendantes DNS et Ne pas bloquer et de blocage DNS aux politiques DNS dans les domaines ancêtres. Ces règles sont définies en deuxième position dans leurs catégories respectives.

Remarque Si l'architecture multi-détenteur est activée pour votre centre de gestion, le système est organisé en une hiérarchie de domaines, y compris les domaines ascendants et descendants. Ces domaines sont distincts et distincts des noms de domaine utilisés dans la gestion du DNS.

Une liste descendante contient les domaines sur les listes Bloquer ou Ne pas bloquer des utilisateurs du sous-domaine du système. À partir d'un domaine ascendant, vous ne pouvez pas afficher le contenu des listes descendantes. Si vous ne voulez pas que les utilisateurs de sous-domaine ajoutent des domaines à une liste de blocage ou Ne pas bloquer :

- désactivez les règles de liste descendante, et
- appliquez les renseignements sur la sécurité à l'aide des paramètres hérités de la politique de contrôle d'accès;

Le système évalue les règles dans l'ordre suivant :

- Liste globale Ne pas bloquer pour la règle DNS (si activée)
- Règle des listes descendantes DNS Ne pas bloquer (si activée)
- Règles avec une action Ne pas bloquer
- Liste de blocage globale pour la règle DNS (si activée)
- Règle de listes de blocage DNS descendantes (si activée)
- Règles avec une action autre que Ne pas bloquer

Habituellement, le système gère le trafic réseau basé sur le nom distinctif (DN) en fonction de la *première* règle DNS, où *toutes* les conditions de la règle correspondent au trafic. Si aucune règle DNS ne correspond au trafic, le système continue d'évaluer le trafic en fonction des règles de la politique de contrôle d'accès associée. Les conditions des règles du DNS peuvent être simples ou complexes.

Licences requises pour les politiques DNS

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques DNS

Prise en charge des modèles

N’importe lequel

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’accès
- Administrateur de réseau

Important Vous devez appliquer la politique de découverte de réseau sur le périphérique pour réussir la validation DNS du trafic.

Gestion des politiques DNS et Cisco Umbrella DNS

Utilisez la page de politique DNS (**Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**) pour gérer les politiques DNS personnalisées et Cisco Umbrella.

En plus des politiques personnalisées que vous créez, le système fournit la politique DNS par défaut et la politique Cisco Umbrella DNS par défaut. La politique DNS par défaut utilise la liste de blocage et la liste Ne pas bloquer par défaut. Vous pouvez modifier et utiliser ces politiques personnalisées fournies par le système. Dans un déploiement multidomaine, cette politique DNS par défaut utilise la liste de blocage DNS globale, la liste Ne pas bloquer DNS globale, les listes de blocage DNS descendantes et les listes Ne pas bloquer DNS descendantes par défaut, et ne peut être modifiée que dans le domaine global.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez

pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Gérez votre politique DNS :

- Comparer : pour comparer les politiques DNS, cliquez sur **Compare Policies** (Comparer les politiques) et procédez comme décrit dans Comparer les stratégies.
- Copier : pour copier une politique DNS, cliquez sur **Copier** ( ) et procédez comme décrit dans Modification des politiques DNS, à la page 5.
- Créer : pour créer une nouvelle politique Cisco Umbrella DNS, cliquez sur **New Policy** > **Umbrella DNS Policy** (Nouvelle politique > Politique DNS Umbrella) et procédez comme décrit dans Créer une politique Cisco Umbrella DNS, à la page 19.
- Supprimer : pour supprimer une politique DNS ou Cisco Umbrella DNS, cliquez sur **Supprimer** ( ), puis confirmez que vous souhaitez supprimer la politique.
- Modifier : pour modifier une politique DNS existante, cliquez sur **Edit** ( )) et procédez comme décrit dans Modification des politiques DNS, à la page 5. Pour modifier une politique Cisco Umbrella DNS existante, cliquez sur **Edit** ( )) et procédez comme décrit dans Modifier les politiques et les règles de Cisco Umbrella DNS, à la page 19.

Création de politiques DNS de base

Lorsque vous créez une nouvelle politique DNS, elle contient les paramètres par défaut. Vous devez ensuite le modifier pour personnaliser le comportement.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Cliquez sur **Add DNS Policy (ajouter une politique DNS) Add DNS Policy** > **DNS Policy)**.

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurer la politique. Consultez Modification des politiques DNS, à la page 5.

Modification des politiques DNS

Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées.

Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Cliquez sur **Edit** (✎) à côté de la politique DNS que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Modifier votre politique DNS

- Name and Description (nom et description) : pour modifier le nom ou la description, cliquez dans le champ et saisissez les nouvelles informations.
- Rules (règles) : pour ajouter, classer, activer, désactiver ou gérer des règles DNS, cliquez sur **Rules** (règles) et procédez comme décrit dans Création et modification des règles DNS, à la page 7.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Vous pouvez également configurer davantage la nouvelle politique comme décrit dans *Journalisation des connexions avec Security Intelligence* dans Guide d'administration Cisco Secure Firewall Management Center.
- Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Règles DNS

Les règles DNS gèrent le trafic en fonction du nom de domaine demandé par un hôte. Dans le cadre des renseignements sur la sécurité, cette évaluation a lieu après tout déchiffrement du trafic et avant l'évaluation du contrôle d'accès.

Le système fait correspondre le trafic aux règles DNS dans l'ordre que vous spécifiez. Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle DNS où *toutes* les conditions de la règle correspondent au trafic.

En plus d'avoir un nom unique, chaque règle DNS comporte les composants de base suivants :

État

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles d'une politique DNS sont numérotées, en commençant par 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. À l'exception des règles de surveillance, la première règle à laquelle le trafic correspond est celle qui gère ce trafic.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Une règle DNS doit contenir un flux DNS ou une condition de liste, et peut également mettre en correspondance le trafic par zone de sécurité, réseau ou VLAN.

Action

L'action découlant d'une règle détermine comment le système traite le trafic correspondant.

- Le trafic avec une action **Ne pas bloquer** sur la est autorisé, sous réserve d'une inspection de contrôle d'accès plus approfondie.
- Le trafic surveillé est soumis à une évaluation plus approfondie selon les règles restantes dans la liste de blocage DNS. Si le trafic ne correspond pas à une règle de liste de blocage du DNS, il est inspecté par les règles de contrôle d'accès. Le système consigne un événement Security Intelligence pour le trafic.
- Le trafic sur une liste de blocage est abandonné sans autre inspection. Vous pouvez également renvoyer une réponse Domain Not Found (domaine introuvable) ou rediriger la requête DNS vers un serveur « sinkhole » (gouffre).

Sujets connexes

À propos des renseignements sur la sécurité

Création et modification des règles DNS

Dans une politique DNS, vous pouvez ajouter jusqu'à 32 767 listes DNS aux règles de liste de blocage (Block List) et Ne pas bloquer; c'est-à-dire que le nombre de listes de la politique DNS ne peut pas dépasser 32 767.

Procédure

Étape 1 Dans l'éditeur de politiques DNS, vous avez les options suivantes :

- Pour ajouter une nouvelle règle, cliquez sur **Add DNS Rule** (Ajouter une règle DNS).
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Étape 2 Saisissez un **Nom**.

Étape 3 Configurez les composants de la règle ou acceptez les valeurs par défaut :

- Action : sélectionnez une **Action** de règle; voir Actions découlant d'une règle DNS, à la page 9.
- Conditions (conditions) : configurez les conditions de la règle. voir Conditions des règles DNS, à la page 10.
- Enabled (activer) : spécifiez si la règle est activée (**Enabled)**.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Gestion des règles DNS

L'onglet **Rules** (Règles) de l'éditeur de politique DNS vous permet d'ajouter, de modifier, de déplacer, d'activer, de désactiver, de supprimer et de gérer les règles DNS de votre politique.

Pour chaque règle, l'éditeur de politiques affiche son nom, un résumé de ses conditions et l'action liée à la règle. Les autres icônes représentent **Avertissement** ( ), **Erreur** ( )et d'autres **Information** ( ) importants. Les règles désactivées sont grisées et marquées `(désactivées)` sous le nom de la règle.

Activation et désactivation des règles DNS

Lorsque vous créez une règle DNS, elle est activée par défaut. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle. Lors de l'affichage de la liste des règles dans une politique DNS, les règles désactivées sont grisées, bien que vous puissiez toujours les modifier. Notez que vous pouvez également activer ou désactiver une règle DNS à l'aide de l'éditeur de règles DNS.

Procédure

Étape 1 Dans l'éditeur de politiques DNS, effectuez un clic droit sur la règle et choisissez un état de règle.

Étape 2 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Évaluation de l'ordre des règles DNS

Les règles d'une politique DNS sont numérotées, en commençant par 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle DNS, pour laquelle *toutes* les conditions de la règle correspondent au trafic :

- Pour les règles Monitor (Surveiller), le système journalise le trafic, puis continue à évaluer le trafic par rapport aux règles de la liste de blocage du DNS de priorité inférieure.
- Pour les règles **non** liées au moniteur, le système interrompt l'évaluation du trafic par rapport à d'autres règles DNS de priorité inférieure une fois que le trafic correspond à une règle.

Notez les éléments suivants concernant l'ordre des règles :

- La liste blanche globale des à ne pas bloquer pour le DNS vient toujours en premier et a préséance sur toutes les autres règles.

- La règle d'interdiction de blocage des listes blanches du DNS ne s'affiche que dans les déploiements multidomaine, dans les domaines non terminaux. Elle vient toujours en deuxième position et a préséance sur toutes les autres règles, à l'exception de la globale des règles à ne pas bloquer pour le DNS.
- La section de la liste Ne pas bloquer précède la section de la liste de blocage; Les règles de la liste d'autorisation ont toujours priorité sur les autres règles.
- La liste de blocage globale pour le DNS figure toujours en premier dans la section de liste de blocage et a priorité sur toutes les autres règles de surveillance et de liste de blocage.
- La règle des listes d'interdiction DNS descendantes ne s'affiche que dans les déploiements multidomaine, dans les domaines non terminaux. Elle figure toujours en deuxième position dans la section de la liste de blocage et a préséance sur toutes les autres règles de surveillance et de liste de blocage, à l'exception de celle de la liste de blocage globale.
- La section de liste de blocage contient les règles de surveillance et de liste de blocage.
- Lorsque vous créez une règle DNS pour la première fois, le système la positionne en dernier dans la section de la liste à ne pas bloquer si vous affectez une action **Ne pas bloquer** ou en dernier dans la section de la liste de blocage si vous affectez une autre action.

Vous pouvez faire glisser et déposer des règles pour les réorganiser.

Actions découlant d'une règle DNS

Chaque règle DNS a une *action* qui détermine les éléments suivants pour la correspondance du trafic :

- traitement : avant tout, l'action de la règle régit si le système bloque, ne bloque pas ou surveille le trafic qui correspond aux conditions de la règle, en fonction d'une liste de blocage ou Ne pas bloquer
- journalisation : l'action de règle détermine quand et comment vous pouvez consigner les détails sur le trafic correspondant.

ActionNe pas bloquer

L'action **Ne pas bloquer** permet au trafic de passer à la phase suivante d'inspection, c'est-à-dire les règles de contrôle d'accès.

Le système ne consigne pas les correspondances dans la liste Ne pas bloquer. L'enregistrement de ces connexions dépend de leur disposition finale.

Action Surveiller

L'action **Monitor** (surveiller) est conçue pour forcer la journalisation de la connexion; le trafic correspondant n'est ni immédiatement autorisé ni bloqué. Au contraire, le trafic est comparé à des règles supplémentaires afin de déterminer s'il faut l'autoriser ou le refuser. La première règle DNS non liée au moniteur mise en correspondance détermine si le système bloque le trafic. S'il n'y a pas de règles de correspondance supplémentaires, le trafic est soumis à une évaluation de contrôle d'accès.

Pour les connexions surveillées par une politique DNS, le système consigne les renseignements sur la sécurité de fin de connexion et les événements de connexion dans la base de données centre de gestion.

Actions Bloquer

Ces actions bloquent le trafic sans autre inspection d'aucune sorte :

- L'action **Drop** (Abandonner) supprime le trafic.
- L'action **Domain Not Found** (Domaine non trouvé) renvoie une réponse de domaine Internet inexistante à la requête DNS, ce qui empêche le client de résoudre la requête DNS.
- L'action **Sinkhole** (gouffre) renvoie l'adresse IPv4 ou IPv6 d'un objet en aval en réponse à la requête DNS (enregistrements A et AAAA uniquement). Le serveur snkhole peut journaliser, ou journaliser et bloquer, les connexions de suivi à l'adresse IP. Si vous configurez une action **Sinkhole**, vous devez également configurer un objet « Sinkhole » (Gouffre).

Pour une connexion bloquée en fonction des actions **Abandon** ou **Domaine introuvable**, le système consigne les renseignements sur la sécurité et les événements de connexion de début de connexion. Comme le trafic bloqué est immédiatement refusé sans inspection supplémentaire, il n'y a pas de fin de connexion unique à consigner.

Pour une connexion bloquée en fonction de l'action **Sinkhole**, la journalisation dépend de la configuration de l'objet sinkhole. Si vous configurez votre objet Sinkhole pour ne consigner que les connexions Sinkhole, le système consigne les événements de connexion de fin de connexion pour la connexion de suivi. Si vous configurez votre Sinkhole doline pour qu'il journalise et bloque les connexionsSinkhole, le système consigne les événements de début de connexion pour la connexion de suivi, puis bloque cette connexion.

Conditions des règles DNS

Les conditions d'une règle DNS identifient le type de trafic géré par la règle. Les conditions peuvent être simples ou complexes. Vous devez définir un flux DNS ou une condition de liste dans une règle DNS. Vous pouvez également contrôler le trafic par zone de sécurité, réseau ou VLAN.

Lors de l'ajout de conditions à une règle DNS :

- Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère.
- Vous pouvez configurer plusieurs conditions par règle. Le trafic doit correspondre à **toutes** les conditions de la règle pour que celle-ci s'applique au trafic. Par exemple, une règle avec une condition de flux DNS ou de liste et une condition de réseau, mais sans condition de balise VLAN, évalue le trafic en fonction du nom de domaine et de la source ou de la destination, indépendamment de tout balisage VLAN dans la session.
- Pour chaque condition d'une règle, vous pouvez ajouter jusqu'à 50 critères. Le trafic qui correspond à **l'un** quelconque des critères d'une condition satisfait à la condition. Par exemple, vous pouvez utiliser une seule règle pour bloquer le trafic en fonction d'un maximum de 50 listes DNS et flux.

Sujets connexes

Conditions des règles de zone de sécurité, à la page 10
Conditions des règles de réseau
Conditions de règle des balises VLAN
Conditions des règles DNS, à la page 12

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions des règles DNS

Les conditions DNS dans les règles DNS vous permettent de contrôler le trafic si une liste, un flux ou une catégorie DNS contient le nom de domaine demandé par le client. Vous devez définir une condition DNS dans une règle DNS.

Que vous ajoutiez une liste de blocage ou de ne pas bloquer globale ou personnalisée à une condition DNS, le système applique l'action de règle configurée au trafic. Par exemple, si vous ajoutez la liste globale des exclusions à une règle et configurez une action **Abandon**, le système bloque tout le trafic qui aurait dû être autorisé à passer à la prochaine phase d'inspection.

Comment créer des règles DNS

Les rubriques suivantes expliquent comment créer des règles DNS.

Sujets connexes

Contrôle du trafic en fonction du DNS et de la zone de sécurité, à la page 13
Contrôle du trafic en fonction du DNS et du réseau, à la page 13
Contrôle du trafic en fonction du DNS et du VLAN, à la page 14
Contrôle du trafic en fonction d'une liste ou d'un flux DNS, à la page 15

Contrôle du trafic en fonction du DNS et de la zone de sécurité

Les conditions de zone dans les règles DNS vous permettent de contrôler le trafic en fonction de sa zone de sécurité source. Une *zone de sécurité* est un ensemble d'une ou de plusieurs interfaces, qui peuvent être situées sur plusieurs périphériques.

Procédure

Étape 1 Dans l'éditeur de règles DNS, cliquez sur **Zones**.

Étape 2 Recherchez et sélectionnez les zones que vous souhaitez ajouter dans les **zones disponibles**. Pour rechercher des zones à ajouter, cliquez sur le bouton **Rechercher par nom** au-dessus de la liste **Zones disponibles**, puis saisissez un nom de zone. La liste est mise à jour à mesure que vous saisissez pour afficher les zones correspondantes.

Étape 3 Cliquez pour sélectionner une zone, ou cliquez avec le bouton droit et sélectionnez **Sélectionner tout**.

Étape 4 Cliquez sur **Add to Source** (ajouter à la source) ou faites un glisser-déposer.

Étape 5 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Contrôle du trafic en fonction du DNS et du réseau

Les conditions de réseau dans les règles DNS vous permettent de contrôler le trafic en fonction de son adresse IP source. Vous pouvez spécifier explicitement les adresses IP source pour le trafic que vous souhaitez contrôler.

Procédure

Étape 1 Dans l'éditeur de règles DNS, cliquez sur **Networks** (réseaux).

Étape 2 Recherchez et sélectionnez les réseaux que vous souhaitez ajouter dans la liste des **réseaux disponibles**, comme suit :

- Pour ajouter un objet réseau à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des **réseaux disponibles** et procédez comme décrit dans Création d'objets réseau.

- Pour rechercher des objets de réseau à ajouter, cliquez sur l'invite **Search by Name or value** (Rechercher par nom ou par valeur) au-dessus de la liste des **réseaux disponibles**, puis saisissez un nom d'objet ou la valeur de l'un des composants de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 3 Cliquez sur **Add to Source** (ajouter à la source) ou faites un glisser-déposer.

Étape 4 Ajoutez les adresses IP source ou les blocs d'adresses que vous souhaitez définir manuellement. Cliquez sur le bouton **Enter an IP address** (Saisissez une adresse IP) sous la liste des **réseaux source**; saisissez une adresse IP ou un bloc d'adresses et cliquez sur **Add** (Ajouter).

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 5 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Contrôle du trafic en fonction du DNS et du VLAN

Les conditions VLAN dans les règles DNS vous permettent de contrôler le trafic balisé VLAN. Le système utilise la balise VLAN la plus à l'intérieur pour identifier un paquet par VLAN.

Lorsque vous créez une condition de règle DNS basée sur VLAN, vous pouvez spécifier manuellement les balises VLAN. Par ailleurs, vous pouvez configurer les conditions VLAN avec des *objets* de balise VLAN, qui sont réutilisables et associent un nom à une ou plusieurs balises VLAN.

Procédure

Étape 1 Dans l'éditeur de règles DNS, sélectionnez **Balises VLAN**.

Étape 2 Recherchez et sélectionnez les VLAN que vous souhaitez ajouter à partir des **balises VLAN disponibles**, comme suit :

- Pour ajouter un objet de balise VLAN à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des balises VLAN disponibles et procédez comme décrit dans Création d'objets de balise VLAN.
- Pour rechercher des objets de balise VLAN et des groupes à ajouter, cliquez sur l'invite **Search by Name or value** (rechercher par nom ou par valeur) au-dessus de la liste des **balises VLAN disponibles** , puis saisissez le nom de l'objet ou la valeur d'une balise VLAN dans l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 3 Cliquez sur **Add to Rule** (ajouter à la règle) ou faites un glisser-déposer.

Étape 4 Ajoutez les balises VLAN que vous souhaitez définir manuellement. Cliquez sur le lien **Saisissez une balise VLAN** sous la liste des **balises VLAN sélectionnées**; Saisissez ensuite une balise ou une plage VLAN et

cliquez sur **Add** (Ajouter). Vous pouvez spécifier n'importe quelle balise VLAN, entre 1 et 4094; Utilisez un tiret pour spécifier une plage de balises VLAN.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 5 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Contrôle du trafic en fonction d'une liste ou d'un flux DNS

Procédure

Étape 1 Dans l'éditeur de règles DNS, cliquez sur **DNS**.

Étape 2 Recherchez et sélectionnez les listes DNS et les flux que vous souhaitez ajouter parmi les **listes et les flux DNS**, comme suit :

- Pour ajouter une liste ou un flux DNS à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la **liste et flux DNS** et procédez comme décrit dans Création de flux de renseignements sur la sécurité.
- Pour rechercher des listes DNS, des flux ou des catégories à ajouter, cliquez sur l'invite **Rechercher par nom ou par valeur** au-dessus de la liste **Listes et flux DNS**, puis saisissez un nom d'objet ou la valeur de l'un des composants de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.
- Pour obtenir une description des catégories de menaces fournies par le système, utilisez Catégorie de renseignements sur la sécurité.

Étape 3 Cliquez sur **Add to Rule** (ajouter à la règle) ou faites un glisser-déposer.

Étape 4 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Déploiement de politique DNS

Après avoir terminé la mise à jour de la configuration de votre politique DNS, vous devez la déployer dans le cadre de la configuration du contrôle d'accès.

- Associez votre politique DNS à une politique de contrôle d'accès, comme décrit en Configurer les renseignements sur la sécurité.
- Déployer les changements de configuration.

Politiques DNS de Cisco Umbrella

Cisco Umbrella DNS Connection dans le centre de gestion permet de rediriger les requêtes DNS vers Cisco Umbrella. Cela permet à Cisco Umbrella de valider les demandes, de les autoriser ou de les bloquer en fonction des noms de domaine et d'appliquer une politique de sécurité basée sur le DNS à la demande. Si vous utilisez Cisco Umbrella, vous devez configurer Cisco Umbrella Connection (**Intégration > Autres intégrations > Services en nuage > Cisco Umbrella Connection**) pour rediriger les requêtes DNS vers Cisco Umbrella.

Le connecteur Cisco Umbrella fait partie de l'inspection DNS du système. Si votre liste de politiques d'inspection DNS existante décide de bloquer ou d'abandonner une demande en fonction de vos paramètres d'inspection DNS, la demande n'est pas transmise à Cisco Umbrella. Vous disposez ainsi de deux lignes de protection :

- Votre politique d'inspection DNS locale
- Votre politique en nuage de Cisco Umbrella

Lors de la redirection des demandes de recherche DNS vers Cisco Umbrella, le connecteur Cisco Umbrella ajoute un enregistrement EDNS (Extension mécanismes for DNS). Un enregistrement EDNS comprend les renseignements sur l'identifiant du périphérique , l'ID de l'organisation et l'adresse IP du client. Votre politique en nuage peut utiliser ces critères pour contrôler l'accès en plus de la réputation du nom de domaine complet. Vous pouvez également choisir de chiffrer la requête DNS à l'aide de DNSCrypt pour assurer la confidentialité des noms d'utilisateurs et des adresses IP internes.

Pour rediriger les requêtes DNS du centre de gestion vers Cisco Umbrella :

1. Configurez les paramètres de connexion de Cisco Umbrella.
2. Créer et configurer une politique Cisco Umbrella DNS
3. Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès.
4. Déployez les modifications.

Pour des renseignements détaillés sur la configuration de Umbrella DNS Connector dans le centre de gestion, consultez Configurer le connecteur DNS Umbrella pour Cisco Secure Firewall Management Center.

Rediriger les requêtes DNS vers Cisco Umbrella

Cette section fournit des instructions pour rediriger les requêtes DNS du périphérique vers Cisco Umbrella en utilisant la touche centre de gestion.

Étape	Faire ceci	Plus d'informations
1	Assurez-vous de remplir les conditions préalables.	Conditions préalables à la configuration du connecteur Cisco Umbrella DNS, à la page 17

Étape	Faire ceci	Plus d'informations
2	Configurez les paramètres de connexion de Cisco Umbrella.	Configurer les paramètres de connexion Cisco Umbrella, à la page 18
3	Créer une politique Cisco Umbrella DNS	Créer une politique Cisco Umbrella DNS, à la page 19
4	Configurer la politique Cisco Umbrella DNS	Modifier les politiques et les règles de Cisco Umbrella DNS, à la page 19
5	Associer la politique de Cisco Umbrella DNS à une politique de contrôle d'accès	Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès, à la page 20

Conditions préalables à la configuration du connecteur Cisco Umbrella DNS

Tableau 1 : Plateformes minimales prises en charge

Produit	Version
Cisco Secure Firewall Threat Defense	6.6 ou ultérieure
Cisco Secure Firewall Management Center	7.2 ou ultérieure

- Créez un compte auprès de Cisco Umbrella à l'adresse https://umbrella.cisco.com et connectez-vous à Umbrella à l'adresse http://login.umbrella.com.
- Importez le certificat de l'autorité de certification du serveur Cisco Umbrella dans centre de gestion. Dans Cisco Umbrella, choisissez **Deployments > Configuration > Root Certificate** (Déploiements > Configuration > Certificat racine) et téléchargez le certificat.

  Vous devez importer le certificat racine pour établir la connexion HTTPS avec le serveur d'enregistrement de Cisco Umbrella. Le certificat doit être fiable pour la validation du serveur SSL, qui n'est pas une option par défaut dans centre de gestion. Copiez et collez le certificat suivant pour le périphérique dans centre de gestion(**Device > Certificates**) (Périphériques > Certificats).

```
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
```

```
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=
```

Lorsque vous ajoutez le certificat dans le centre de gestion, assurez-vous de cocher la case **CA Only** (autorité de certification uniquement).

- Installez le certificat sur le périphérique.
- Obtenez les données suivantes d'Umbrella:
  - Identifiant de l'entreprise ou ou de l'organisme
  - Clé de l'appareil réseau
  - Secret de l'appareil réseau
  - Jeton d'appareil réseau existant
- Assurez-vous que le centre de gestion est connecté à Internet.
- Assurez-vous que l'option de licence de base avec l'option de fonctionnalités d'exportation contrôlée est activée dans centre de gestion.
- Assurez-vous que le serveur DNS est configuré pour résoudre api.opendns.com.
- Vérifiez que centre de gestion peut résoudre management.api.umbrella.com pour la configuration de la politique.
- Configurez la route défense contre les menaces vers api.opendns.com.

Configurer les paramètres de connexion Cisco Umbrella

Les paramètres de Cisco Umbrella Connection définissent le jeton nécessaire pour enregistrer le périphérique auprès de Cisco Umbrella.

Avant de commencer

Créez un compte auprès de Cisco Umbrella https://umbrella.cisco.com, puis connectez-vous à Umbrella à l'adresse https://dashboard.umbrella.com et obtenez les informations nécessaires pour établir la connexion à Cisco Umbrella.

Procédure

Étape 1 Choisissez **Integration** > **Autres intégrations** > **Services en nuage** > **Cisco Umbrella Connection**.

Étape 2 Obtenez les renseignements suivants et ajoutez-les aux paramètres **généraux** :

- **ID d'organisation** : numéro unique qui identifie votre organisation sur Cisco Umbrella. Chaque organisation Umbrella est une instance distincte de Umbrella et possède son propre tableau de bord. Les organisations sont identifiées par leur nom et par l'identifiant de leur organisation (Org ID).
- **Clé de périphérique réseau** : clé pour récupérer la politique Umbrella de Cisco Umbrella.
- **Secret de périphérique réseau** : code secret pour récupérer la politique Umbrella de Cisco Umbrella.

- **Jeton d'appareil réseau existant** : un jeton d'API pour les périphériques réseau existants est émis par le tableau de bord de Cisco Umbrella. Umbrella a besoin du jeton d'API pour enregistrer un périphérique réseau.

Étape 3 (Facultatif) Sous **Advanced** (Options avancées), configurez les éléments suivants :

- **Clé publique DNSCrypt** : DNSCrypt authentifie et chiffre les requêtes DNS entre le point terminal et le serveur DNS. Pour activer DNScrypt, vous pouvez configurer la clé publique DNScrypt pour la vérification de certificat. La clé est une valeur hexadécimale de 32 octets et est préconfigurée sur B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79, qui est la clé publique des serveurs Umbrella Anycast.
- **Clé de gestion** : clé permettant de récupérer les détails du centre de données dans le nuage Umbrella pour la politique VPN.
- **Code secret de gestion** : code secret utilisé pour récupérer les centres de données du nuage Umbrella pour VPN.

Étape 4 Cliquez sur **Tester la connexion** : Tester si le nuage Cisco Umbrella est accessible à partir de centre de gestion. Lorsque vous fournissez l'ID d'organisation et les détails du périphérique réseau requis, la connexion Umbrella est créée.

Étape 5 Cliquez sur **Save** (enregistrer).

Créer une politique Cisco Umbrella DNS

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Cliquez sur **Add DNS Policy** > **Umbrella DNS Policy** (ajouter une politique DNS > Politique Cisco Umbrella DNS).

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurer la politique. Consultez Modifier les politiques et les règles de Cisco Umbrella DNS, à la page 19.

Modifier les politiques et les règles de Cisco Umbrella DNS

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Dans la page DNS Policy, sélectionnez la politique Cisco Umbrella DNS que vous souhaitez modifier, puis cliquez sur **Edit** ( ).

Actualiser la politique de protection Cisco Umbrella

Si vous souhaitez obtenir la dernière politique de protection de Cisco Umbrella, cliquez sur l'icône **Actualiser** à côté de **Dernière mise à jour de la politique de protection de Cisco Umbrella**.

Pour configurer ou modifier les paramètres de connexion d'Umbrella pour le centre de gestion, accédez à **Intégration** > **Autres intégrations** > **services en nuage** > **Connexion Cisco Umbrella**.

Étape 3 Dans l'éditeur de politique Umbrella DNS, sélectionnez la règle Umbrella DNS et cliquez sur **Edit** ( ).

Étape 4 Configurez les composants de la règle ou acceptez les valeurs par défaut :

- **Umbrella Protection Policy** : précisez le nom de la politique de Cisco Umbrella à appliquer au périphérique.
- **Bypass Domain**(contourner le domaine) spécifiez le nom des domaines locaux pour lesquels les demandes DNS doivent contourner Cisco Umbrella et aller directement aux serveurs DNS configurés.

  Par exemple, vous pouvez demander à votre serveur DNS interne de résoudre tous les noms pour le nom de domaine de l'organisation en supposant que toutes les connexions internes sont autorisées.
- **DNSCrypt** : activez DNSCrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella.

  L'activation de DNScrypt démarre le fil d'échange de clés avec le résolveur Umbrella. Le fil d'échange de clés effectue l'établissement de liaison avec le résolveur toutes les heures et met à jour le périphérique avec une nouvelle clé secrète. Comme DNScrypt utilise UDP/443, vous devez vous assurer que la carte de trafic utilisée pour l'inspection DNS comprend ce port. Notez que la classe d'inspection par défaut comprend déjà UDP/443 pour l'inspection DNS.
- **Idle Timeout**(Délai d'inactivité) : configurez le délai d'inactivité après lequel une connexion d'un client au serveur Umbrella sera supprimée s'il n'y a pas de réponse du serveur.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès. Pour en savoir plus, consultez Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès, à la page 20.

Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès

Avant de déployer la politique de Cisco Umbrella DNS sur le périphérique, vous devez l'associer à une politique de contrôle d'accès.

Procédure

Étape 1 Choisissez **Policies > Access Control** (Politiques > Contrôle d'accès), puis sélectionnez la politique d'accès à modifier.

Étape 2 Sélectionnez **Security Intelligence** (Renseignements sur la sécurité)

Étape 3 Dans la liste déroulante **Umbrella DNS Policy** (politique DNS Cisco Umbrella), sélectionnez la politique Umbrella DNS.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.