Contrôle de l'utilisateur grâce au portail captif

Source d’identité du portail captif

Le portail captif est l’une des sources d’identité autorisées prises en charge par le système. Le portail captif est une méthode d’authentification active où les utilisateurs s’authentifient sur le réseau à l’aide d’un périphérique géré. (Le VPN d'accès à distance est un autre type d’authentification active.). L’authentification active diffère de l’authentification passive en ce que le périphérique géré présente une page de connexion à l’utilisateur, tandis que l’authentification passive interroge le domaine d’authentification (par exemple, Microsoft AD) pour authentifier l’utilisateur.

Vous utilisez généralement un portail captif pour exiger l’authentification pour accéder à Internet ou à des ressources internes restreintes; vous pouvez éventuellement configurer l’accès invité aux ressources. Une fois que le système a authentifié les utilisateurs du portail captif, il gère le trafic de ces utilisateurs conformément aux règles de contrôle d’accès. Le portail captif authentification sur le trafic HTTP et HTTPS uniquement.

Remarque Le trafic HTTPS doit être déchiffré avant que le portail captif puisse effectuer l’authentification.

Le portail captif enregistre également les tentatives d’authentification échouées. Un échec de tentative n’ajoute pas de nouvel utilisateur à la liste des utilisateurs dans la base de données. Le type d’activité de l’utilisateur pour l’échec de l’authentification signalé par le portail captif est **Failed Auth User**.

Les données d’authentification obtenues à partir du portail captif peuvent être utilisées pour la sensibilisation et le contrôle des utilisateurs.

Sujets connexes

Configurer le portail captif pour le contrôle utilisateur, à la page 5

À propos de la redirection de nom d'hôte

(Snort 3 uniquement.) Une règle d'identité d'authentification active redirige vers le port du portail captif à l'aide de son interface configurée. Comme la redirection s'effectue généralement vers une adresse IP, l'utilisateur obtient une erreur de certificat non fiable et, comme ce comportement est similaire à une attaque de l'homme du milieu, les utilisateurs peuvent être réticents à accepter le certificat non fiable.

Pour éviter ce problème, vous pouvez configurer le portail captif pour utiliser le nom de domaine complet (FQDN) du périphérique géré. Avec un certificat correctement configuré, les utilisateurs ne recevront pas d'erreur de certificat non fiable, et l'authentification sera plus transparente et semblera plus sécurisée.

Sujets connexes

Conditions de règles de réseau pour la redirection vers le nom d'hôte

Exigences de licence pour le portail captif

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et prérequis pour le portail captif

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices et limites relatives au portail captif

Lorsque vous configurez et déployez un portail captif dans une politique d'identité, les utilisateurs de domaines spécifiés s'authentifient à l'aide de défense contre les menaces pour accéder à votre réseau.

Remarque Lorsqu'un utilisateur VPN d'accès à distance s'est déjà authentifié activement au moyen d'un périphérique géré agissant comme passerelle sécurisée, l'authentification active sur portail captif ne se produira pas, même si elle est configurée dans une politique d'identité.

Portail captif et politiques

Vous configurez le portail captif dans votre politique d'identité et appelez l'authentification active dans vos règles d'identité. Les politiques d'identité sont associées aux politiques de contrôle d'accès, et celles-ci définissent l'accès aux ressources du réseau. Par exemple, vous pouvez empêcher les utilisateurs du groupe US-West/Finance d'accéder aux serveurs d'ingénierie ou vous pouvez interdire aux utilisateurs d'accéder aux applications non sécurisées sur le réseau.

Vous configurez certains paramètres de politique d'identité de portail captif dans la page à onglet **Active Authentication** (authentification active) de la politique d'identité et configurez le reste dans la règle d'identité associée à la politique de contrôle d'accès.

Une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée. Dans chaque cas, le système active ou désactive de manière transparente le déchiffrement TLS/SSL, qui redémarre le processus Snort.

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). u de déchiffrement) redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Lorsque le portail captif authentifie les utilisateurs qui correspondent à une règle d'identité, tout utilisateur de Microsoft Active Directory ou d'un groupe LDAP qui n'a pas été téléchargé est identifié comme étant inconnu. Pour éviter que les utilisateurs soient identifiés comme inconnus, configurez le domaine de domaine pour télécharger les utilisateurs de tous les groupes que vous souhaitez authentifier sur le portail captif. Les utilisateurs inconnus sont traités conformément à la politique de contrôle d'accès associée; si la politique de contrôle d'accès est configurée pour bloquer les utilisateurs inconnus, ces utilisateurs sont bloqués.

Pour vous assurer que le système télécharge tous les utilisateurs dans un domaine de domaine , vérifiez que les groupes figurent dans la liste Groupes disponibles dans la configuration du domaine.

Pour en savoir plus sur la synchronisation des utilisateurs et des groupes, consultez Synchroniser les utilisateurs et les groupes.

Interface routée nécessaire

L'authentification active du portail captif ne peut être effectuée que par un périphérique doté d'une interface de routage configurée. Si vous configurez une règle d'identité pour un portail captif et que votre périphérique de portail captif contient des interfaces en ligne et routées, vous devez configurer les conditions de règle d'interface dans la politique de contrôle d'accès pour cibler uniquement les interfaces routées sur le périphérique.

Si la politique d'identité associée à votre politique de contrôle d'accès contient une ou plusieurs règles d'identité de portail captif et que vous déployez la politique sur le centre de gestion qui gère un ou plusieurs périphériques avec des interfaces de routage configurées, le déploiement de la politique réussit et les interfaces de routage effectuent une authentification active.

Exigences et limites du portail captif

Notez les exigences et les limites suivantes :

- Le portail captif ne prend pas en charge les connexions HTTP/3 QUIC.
- Le système prend en charge jusqu'à 20 connexions à un portail captif par seconde.
- Il y a une limite maximale de cinq minutes entre les tentatives de connexion échouées pour qu'une tentative de connexion échouée soit prise en compte dans le décompte des tentatives de connexion maximales. La limite de cinq minutes n'est pas configurable.

  (Le nombre maximal de tentatives de connexion est affiché dans les événements de connexion : **Analysis** > **Connections** > **Events**(événements de connexion d'analyse).

  Si plus de cinq minutes s'écoulent entre deux échecs de connexion, l'utilisateur est redirigé vers le portail captif pour l'authentification et n'est pas désigné comme un utilisateur ayant échoué à la connexion ou comme un utilisateur invité, et n'est pas signalé au centre de gestion.
- Le portail captif ne négocie pas les connexions TLS v1.0.

  Seules les connexions TLS v1.1, v1.2et TLS 1.3 sont prises en charge.
- La seule façon d'être sûr qu'un utilisateur se déconnecte est de fermer et de rouvrir le navigateur. Si ce n'est pas le cas, dans certains cas, l'utilisateur peut se déconnecter du portail captif et accéder au réseau sans avoir à s'authentifier à nouveau en utilisant le même navigateur.
- Si un domaine est créé pour un domaine parent et que le périphérique géré détecte une connexion à un enfant de ce domaine parent, la déconnexion ultérieure de l'utilisateur n'est pas détectée par le périphérique géré.
- Si un domaine est créé pour un domaine parent et que le périphérique géré détecte une connexion à un enfant de ce domaine parent, la déconnexion ultérieure de l'utilisateur n'est pas détectée par le périphérique géré.
- Votre règle de contrôle d'accès doit autoriser le trafic destiné à l'adresse IP et au port du périphérique que vous prévoyez utiliser pour le portail captif.
- Pour effectuer une authentification active du portail captif sur le trafic HTTPS, vous devez utiliser u de déchiffrement pour déchiffrer le trafic des utilisateurs que vous souhaitez authentifier. Vous ne pouvez pas déchiffrer le trafic de la connexion entre le navigateur Web d'un utilisateur du portail captif et le daemon du portail captif sur le périphérique géré; cette connexion est utilisée pour authentifier l'utilisateur du portail captif.
- Pour limiter le volume de trafic non HTTP ou HTTPS autorisé par le périphérique géré, vous devez saisir les ports HTTP et HTTPS typiques dans la page à l'onglet **Ports** de la politique d'identité.

  Le périphérique géré fait passer un utilisateur jamais vu auparavant de **`En attente`** à **`Inconnu`** lorsqu'il détermine que la demande entrante n'utilise pas le protocole HTTP ou HTTPS. Dès que le périphérique géré fait passer un utilisateur de **`En attente`** à un autre état, le contrôle d'accès, la qualité de service et Politiques de déchiffrement peuvent être appliqués à ce trafic. Si vos autres politiques n'autorisent pas le trafic non-HTTP ou HTTPS, la configuration des ports sur la politique d'identité du portail captif peut empêcher le trafic indésirable d'être autorisé par le périphérique géré.

Conditions préalables à Kerberos

Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : Conventions

de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles.

Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans la section 6.2.5 de la RFC 6891.

Configurer le portail captif pour le contrôle utilisateur

Avant de commencer

Pour utiliser le portail captif pour l'authentification active, vous devez configurer un domaine LDAP; un domaine Microsoft AD; la politique de contrôle d'accès; une politique d'identité; u de déchiffrement; et associez l'identité et Politiques de déchiffrement à la même politique de contrôle d'accès. Enfin, vous devez déployer les politiques sur les périphériques gérés. Cette rubrique fournit un résumé général de ces tâches.

Effectuez les tâches suivantes d'abord :

- Confirmez que votre centre de gestion gère un ou plusieurs périphériques avec une interface de *routage* configurée.
- Pour utiliser l'authentification chiffrée avec le portail captif, créez un objet PKI pour le périphérique géré authentificateur ou assurez-vous que les données et la clé de votre certificat sont disponibles sur la machine à partir de laquelle vous accédez au centre de gestion. Pour créer un objet PKI, consultez ICP.

Procédure

Étape 1 Créez et activez un domaine LDAP; ou un domaine Microsoft AD comme indiqué dans les rubriques suivantes :

- Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine
- Synchroniser les utilisateurs et les groupes

Pour vous assurer que le système télécharge tous les utilisateurs dans un domaine de domaine , vérifiez que les groupes figurent dans la liste Groupes disponibles dans la configuration du domaine.

Pour en savoir plus, consultez Synchroniser les utilisateurs et les groupes.

Étape 2 Créez un objet réseau avec une autorité de certification approuvée.

Consultez Configurer le portail captif, partie 1 : créer un objet de réseau, à la page 6.

Étape 3 Créez un exemple de politique d'identité avec une règle d'authentification active

La politique d'identité permet aux utilisateurs sélectionnés de votre domaine d'accéder aux ressources après s'être authentifiés sur le portail captif.

Pour en savoir plus, consultez Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 8.

Étape 4 Configurez une règle de contrôle d'accès pour le portail captif qui autorise le trafic sur le port du portail captif (par défaut, TCP 885).

Vous pouvez choisir n'importe quel port TCP disponible pour le portail captif. Quel que soit votre choix, vous devez créer une règle qui autorise le trafic sur ce port.

Pour en savoir plus, consultez Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 9.

Étape 5 Ajoutez une autre règle de contrôle d'accès pour permettre aux utilisateurs du domaine de domaines sélectionnés d'accéder aux ressources à l'aide du portail captif.

Pour en savoir plus, consultez Configurer le portail captif Partie 4 : Créer une règle de contrôle d'accès utilisateur, à la page 11.

Étape 6 Configurez u de déchiffrement avec une règle **Decrypt – Resign** (Déchiffrer - Resigner) pour l'utilisateur **Inconnu** afin que les utilisateurs du portail captif puissent accéder aux pages Web à l'aide du protocole HTTPS.

Le portail captif ne peut authentifier les utilisateurs que si le trafic HTTPS est déchiffré avant d'être envoyé à celui-ci. Le portail captif lui-même est vu par le système comme un utilisateur **inconnu**.

Exemple de portail captif : créer une politique de déchiffrement avec une règle de trafic sortant, à la page 11

Étape 7 Associez l'identité et Politiques de déchiffrement à la politique de contrôle d'accès de l'étape 3.

Cette dernière étape permet au système d'authentifier les utilisateurs sur le portail captif.

Pour en savoir plus, consultez Configurer le portail captif, partie 6 : associer l'identité et les Politiques de déchiffrement à l'aide de la politique de contrôle d'accès, à la page 14.

Prochaine étape

Consultez Configurer le portail captif, partie 1 : créer un objet de réseau, à la page 6.

Sujets connexes

Exclure des applications du portail captif, à la page 15
ICP
Dépannage de la source d'identité du portail captif, à la page 16
Scénarios de redémarrage de Snort

Configurer le portail captif, partie 1 : créer un objet de réseau

Cette tâche explique comment commencer à configurer le portail captif en tant que source d'identité.

Avant de commencer

(Snort 3 uniquement.) Créez un nom d'hôte complet (FQDN) en utilisant votre serveur DNS et téléversez le certificat interne de Défense contre les menaces] sur centre de gestion. Vous pouvez consulter une ressource comme celle-ci si vous ne l'avez jamais fait auparavant. Précisez l'adresse IP d'une interface de routage sur l'un des périphériques gérés par votre centre de gestion.

Pour plus d'informations sur l'objet réseau, consultez Conditions de règles de réseau pour la redirection vers le nom d'hôte.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 3 Développez **PKI**.

Étape 4 Cliquez sur **Internal Certs** (Certificats internes).

Étape 5 Cliquez sur **Add Internal Certs** (Ajouter des certificats internes).

Étape 6 Dans le champ **Name**, saisissez un nom pour identifier le certificat interne (par exemple, **`MyCaptivePortal`**).

Étape 7 Dans le champ **Certificate Data**, collez le certificat ou utilisez le bouton **Parcourir** pour le trouver.

Le nom commun du certificat doit correspondre exactement au FDQN avec lequel vous souhaitez que les utilisateurs du portail captif s'authentifient.

Étape 8 Dans le champ **Key**, collez la clé privée du certificat ou utilisez le bouton **Parcourir** pour la localiser.

Étape 9 Si le certificat est chiffré, cochez la case **Encrypted** (chiffré) et saisissez le mot de passe dans le champ adjacent.

Étape 10 Cliquez sur **Save** (enregistrer).

Étape 11 Cliquez sur **« Network »** (réseau)

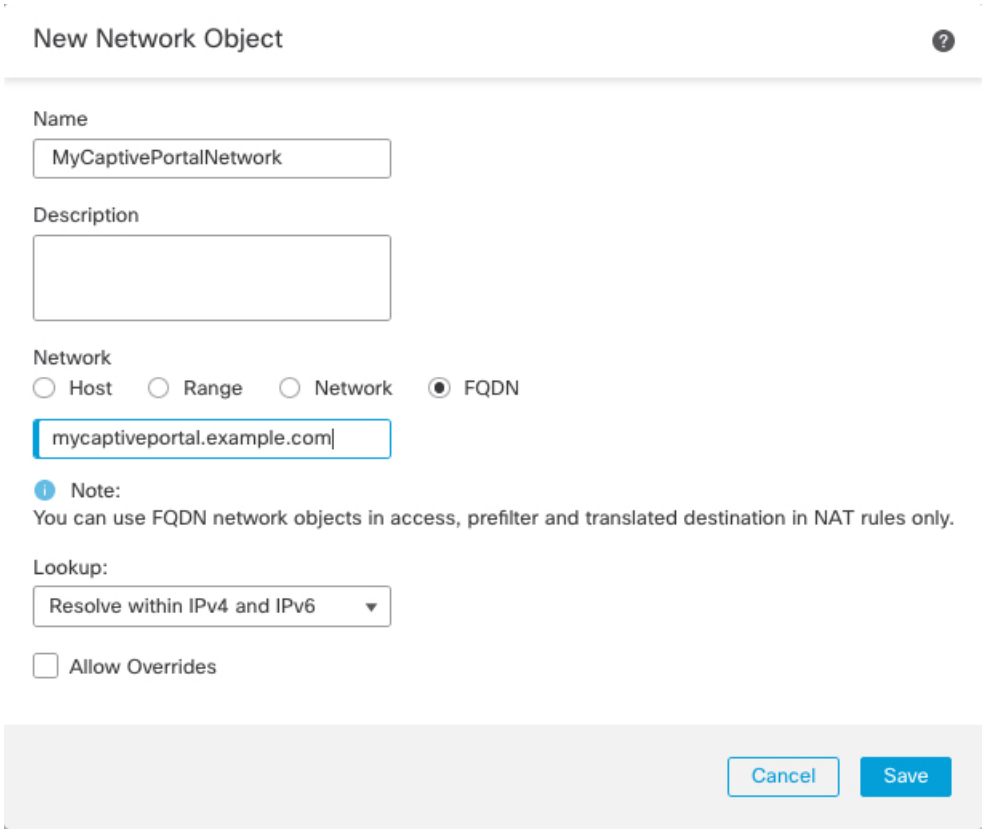
Étape 12 Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > Ajouter un objet).

Étape 13 Dans le champ **Name**, saisissez un nom pour identifier l'objet (par exemple, **`MyCaptivePortalNetwork`**).

Étape 14 Cliquez sur **FDQN** et, dans le champ, saisissez le nom du FDQN (nom de domaine complet) du portail captif.

Étape 15 Cliquez sur une option de **Recherche**.

La figure suivante présente un exemple.



Étape 16 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 8

Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active

Avant de commencer

Cette procédure en plusieurs parties montre comment configurer le portail captif en utilisant le port TCP 885 par défaut et en utilisant un certificat de serveur centre de gestion pour le portail captif et pour le déchiffrement TLS/SSL. Chaque partie de cet exemple explique une tâche requise pour permettre au portail captif d'effectuer l'authentification active.

Si vous suivez toutes les étapes de cette procédure, vous pouvez configurer le portail captif pour qu'il fonctionne pour les utilisateurs de vos domaines. Vous pouvez éventuellement effectuer des tâches supplémentaires, qui sont décrites dans chaque partie de la procédure.

Pour obtenir une présentation de l'ensemble de la procédure, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 5.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Cliquez sur **Policies** > **Access Control** > **Identity** (Politiques > Contrôle d'accès > Identité) et créez ou modifiez une politique d'identité.

Étape 3 (Facultatif) Cliquez sur **Add Catégorie** pour ajouter une catégorie aux règles d'identité du portail captif et saisissez un **nom** pour la catégorie.

Étape 4 Cliquez sur l'onglet **Active Authentication** (authentification active).

Étape 5 Choisissez le **certificat de serveur** approprié dans la liste ou cliquez sur **Ajouter** (+) pour en ajouter un.

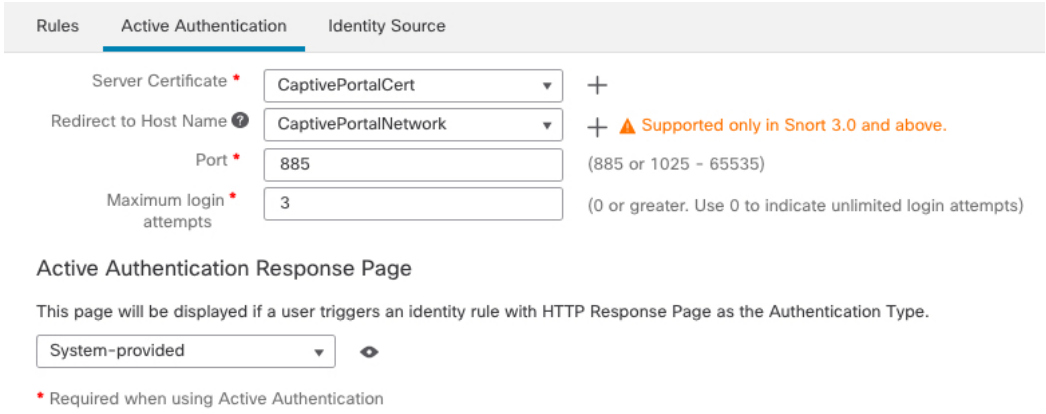
Remarque Le portail captif ne prend *pas* en charge l'utilisation des certificats de l'algorithme de signature numérique (DSA) ou de l'algorithme de signature numérique à courbe elliptique (ECDSA).

Étape 6 Dans le champ **Redirect to Host Name** (Rediriger vers le nom d'hôte), cliquez sur l'objet réseau que vous avez créé précédemment ou cliquez sur **Ajouter** (+).

Étape 7 Saisissez **885** dans le champ **Port** et précisez le **nombre maximal de tentatives de connexion**.

Étape 8 (Facultatif) Choisissez une **page de réponse d'authentification active** comme décrit dans Champs du portail captif, à la page 14.

La figure suivante présente un exemple.



Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Cliquez sur **Rules** (règles).

Étape 11 Cliquez sur **Add Rule** pour ajouter une nouvelle règle ou sur **Edit** ( ) pour modifier une règle existante.

Étape 12 Saisissez un **nom** pour la règle.

Étape 13 Dans la liste **Action**, choisissez **Active Authentication** (Authentification active).

Étape 14 Cliquez sur **Realm & Settings** (Domaine et paramètres).

Étape 15 Dans la liste **Realms** (domaines), choisissez un domaine ou une pour l'authentification de l'utilisateur.

Les séquences de domaine ne sont pas prises en charge.

Étape 16 (Facultatif) Cochez la case **Identifier comme invité si l'authentification ne permet pas d'identifier l'utilisateur**. Pour en savoir plus, consultez Champs du portail captif, à la page 14.

Étape 17 Choisissez un **protocole d'authentification** dans la liste déroulante.

Étape 18 (Facultatif) Pour exclure le trafic d'applications spécifiques du portail captif, consultez Exclure des applications du portail captif, à la page 15.

Étape 19 Ajoutez des conditions à la règle (port, réseau, etc.) comme indiqué dans Conditions des règles d'identité.

Étape 20 Cliquez sur **Add** (ajouter).

Étape 21 En haut de la page, cliquez sur **Save**(Enregistrer) .

Prochaine étape

Continuez avec Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 9.

Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP

Cette partie de la procédure montre comment créer une règle de contrôle d'accès qui permet au portail captif de communiquer avec les clients à l'aide du port TCP 885, qui est le port par défaut du portail captif. Vous pouvez choisir un autre port si vous le souhaitez, mais le port doit correspondre à celui que vous avez choisi dans Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 8.

Avant de commencer

Pour une présentation de la configuration complète du portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 5.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Si vous ne l'avez pas encore fait, créez un certificat pour le portail captif, comme indiqué dans ICP.

Étape 3 Cliquez sur **Policies** > **Access Control** > **Access Control** (Politiques > Contrôle d'accès) et créez ou modifiez une politique de contrôle d'accès.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Saisissez un **nom** pour la règle.

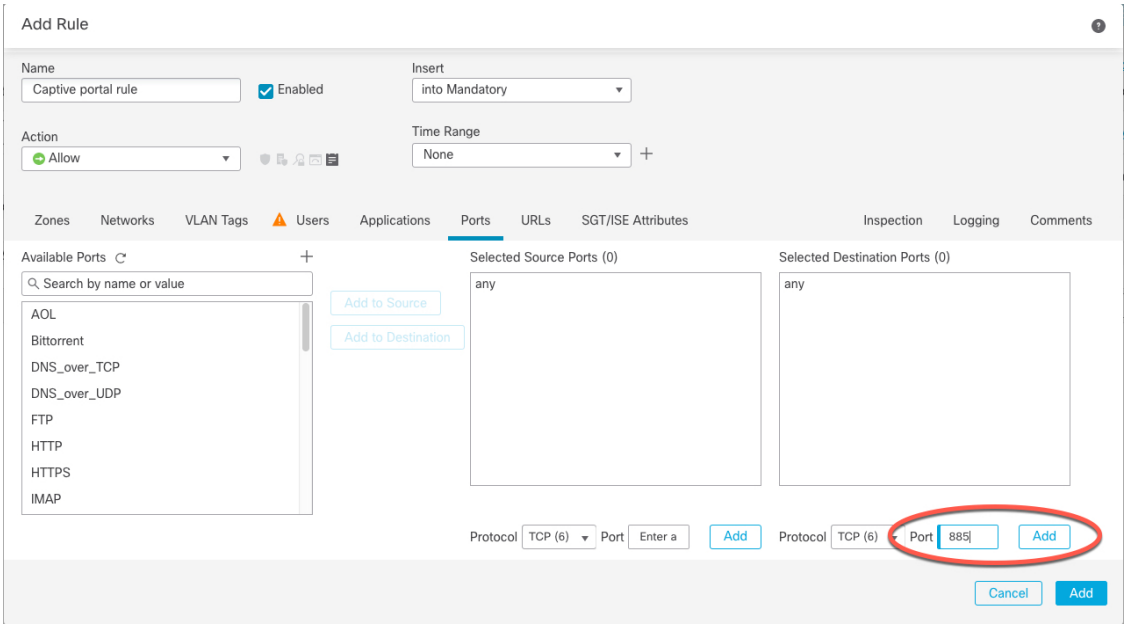
Étape 6 Choisissez **Autoriser** dans la liste **Action**.

Étape 7 Cliquez sur **Ports**.

Étape 8 Dans la liste **Protocol** (Protocole), sous le champ **Selected Destination Ports** (Ports de destination sélectionnés), choisissez **TCP**.

Étape 9 Dans le champ **Port**, saisissez **885**.

Étape 10 Cliquez sur **Add** (Ajouter) à côté du champ **Port**.
La figure suivante présente un exemple.



Étape 11 Cliquez sur **Add** (Ajouter) en bas de la page.

Prochaine étape

Continuez avec Configurer le portail captif Partie 4 : Créer une règle de contrôle d'accès utilisateur, à la page 11.

Configurer le portail captif Partie 4 : Créer une règle de contrôle d'accès utilisateur

Cette partie de la procédure explique comment ajouter une règle de contrôle d'accès qui permet aux utilisateurs d'un domaine de s'authentifier à l'aide d'un portail captif.

Avant de commencer

Pour une présentation de la configuration complète du portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 5.

Procédure

Étape 1 Dans l'éditeur de règles, cliquez sur **Add Rule** (ajouter une règle).

Étape 2 Saisissez un **nom** pour la règle.

Étape 3 Choisissez **Autoriser** dans la liste **Action**.

Étape 4 Cliquez sur **Users** (Utilisateurs).

Étape 5 Dans la liste des **domaines disponibles**, cliquez sur les domaines à autoriser.

Étape 6 Si aucun domaine ne s'affiche, cliquez sur **Actualisation** ( ).

Étape 7 Dans la liste des **utilisateurs disponibles**, choisissez les utilisateurs à ajouter à la règle et cliquez sur **Add to Rule** (ajouter à la règle).

Étape 8 (Facultatif) Ajoutez des conditions à la politique de contrôle d'accès comme indiqué dans Conditions des règles d'identité.

Étape 9 Cliquez sur **Add** (ajouter).

Étape 10 Dans la page des règles de contrôle d'accès, cliquez sur **Save** (Enregistrer).

Étape 11 Dans l'éditeur de politique, définissez la position de la règle. Cliquez dessus et faites-la glisser ou utilisez le menu contextuel pour la couper et la coller. Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic. Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.

Prochaine étape

Exemple de portail captif : créer une politique de déchiffrement avec une règle de trafic sortant, à la page 11

Exemple de portail captif : créer une politique de déchiffrement avec une règle de trafic sortant

Cette partie de la procédure explique comment créer des u de déchiffrement pour déchiffrer et resigner le trafic avant qu'il n'atteigne le portail captif. Le portail captif ne peut authentifier le trafic qu'après son déchiffrement.

Avant de commencer

Vous devez avoir une autorité de certification (CA) interne pour votre serveur de trafic sortant; en d'autres termes, le périphérique géré qui déchiffre le trafic à authentifier par les utilisateurs du portail captif.

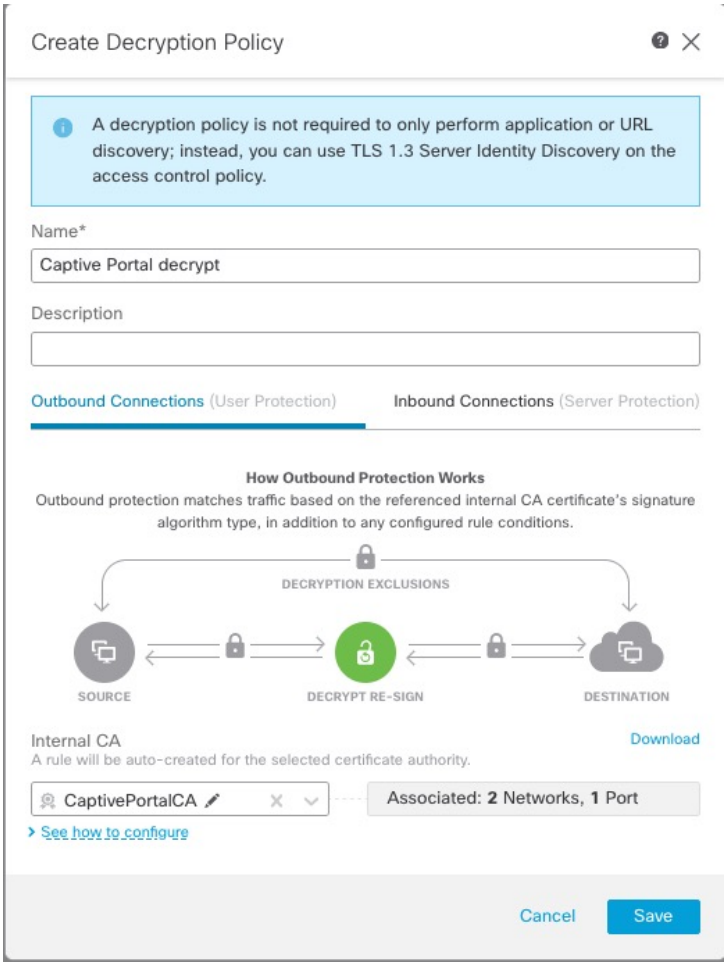
Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

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

Étape 4 Cliquez sur l'onglet **Outbound Connections** (Connexions sortantes).



Étape 5 Téléversez ou choisissez des certificats pour les règles.

Le système crée une règle par certificat.

Étape 6 (Facultatif) Choisissez des réseaux et des ports.

Pour en savoir plus :

- Conditions de la Règle de déchiffrement

- Conditions des règles de réseau
- Conditions de règle de port

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Cliquez sur **Edit** (✎) à côté de la politique de déchiffrement que vous venez de créer.

Étape 9 Cliquez sur **Edit** (✎) à côté de la règle de déchiffrement pour le portail captif.

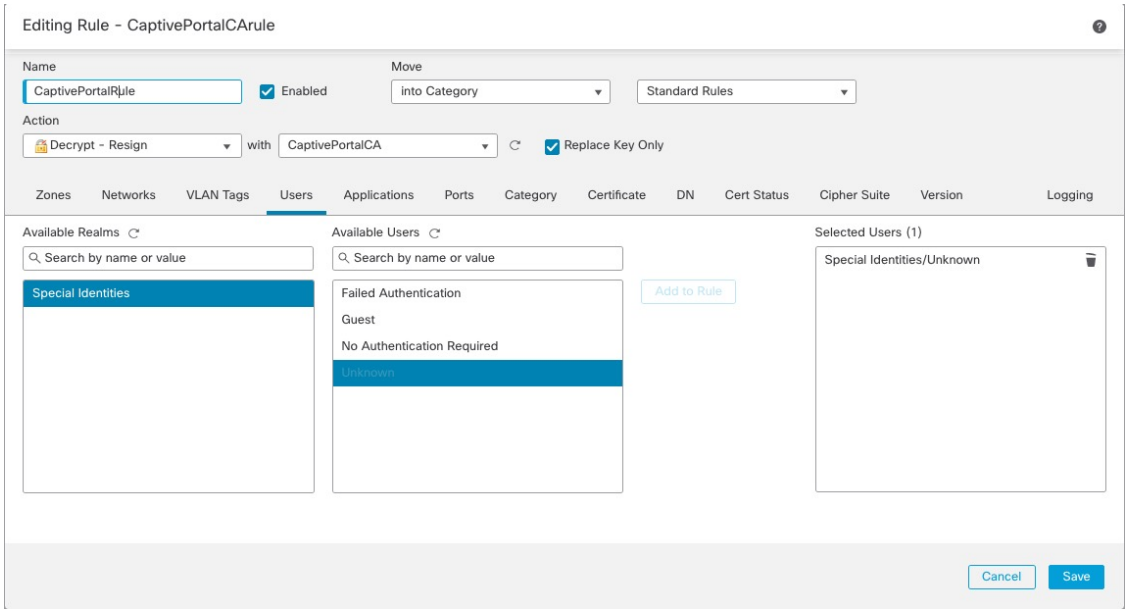
Étape 10 Cliquez sur **Users** (Utilisateurs).

Étape 11 Au-dessus de la liste des **domaines disponibles**, cliquez sur **Actualisation** (↻).

Étape 12 Dans la liste des **domaines disponibles**, cliquez sur **Identités spéciales**.

Étape 13 Dans la liste des **Utilisateurs disponibles**, cliquez sur **Unknown** (Inconnu).

Étape 14 Cliquez sur **Add Rule** (ajouter une règle).
La figure suivante présente un exemple.



Étape 15 (Facultatif) Définissez les autres options comme indiqué dans Conditions de la Règle de déchiffrement.

Étape 16 Cliquez sur **Add** (Ajouter).

Prochaine étape

Configurer le portail captif, partie 6 : associer l'identité et les Politiques de déchiffrement à l'aide de la politique de contrôle d'accès, à la page 14

Configurer le portail captif, partie 6 : associer l'identité et les Politiques de déchiffrement à l'aide de la politique de contrôle d'accès

Cette partie de la procédure explique comment associer la politique d'identité et la règle TLS/SSL **Déchiffrer - Resigner** à la politique de contrôle d'accès que vous avez créée plus tôt. Après cela, les utilisateurs peuvent s'authentifier en utilisant le portail captif.

Avant de commencer

Pour une présentation de la configuration complète du portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 5.

Procédure

Étape 1 Cliquez sur **Policies** > **Access Control** > **Access Control** (Politiques > Contrôle d'accès > Contrôle d'accès) et modifiez la politique de contrôle d'accès que vous avez créée, comme indiqué dans Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 9. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 2 Créer une nouvelle politique de contrôle d'accès ou modifier une politique existante.

Étape 3 En haut de la page, cliquez sur le mot **Identity** (Identité).

Étape 4 Dans la liste, choisissez le nom de votre politique d'identité et, en haut de la page, cliquez sur **Save** (Enregistrer).

Étape 5 Répétez les étapes précédentes pour associer votre portail captif politique de déchiffrement à la politique de contrôle d'accès.

Étape 6 Si vous ne l'avez pas encore fait, ciblez la politique sur les périphériques gérés, comme indiqué dans Définition des périphériques cibles pour une politique de contrôle d'accès.

Prochaine étape

- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration.
- Surveillez l'activité de l'utilisateur, .

Champs du portail captif

Utilisez les champs suivants pour configurer le portail captif dans la page à onglet **Active Authentication** (authentification active) de votre politique d'identité. Voir aussi Champs de la règle d'identité et Exclure des applications du portail captif, à la page 15.

Certificat du serveur

Un certificat interne présenté par le daemon du portail captif.

Remarque Le portail captif ne prend *pas* en charge l'utilisation des certificats de l'algorithme de signature numérique (DSA) ou de l'algorithme de signature numérique à courbe elliptique (ECDSA).

Port

Le numéro de port à utiliser pour la connexion au portail captif. Vous devez configurer votre règle de contrôle d'accès avec un port TCP à utiliser pour le portail captif, puis associer la politique d'identité à cette politique de contrôle d'accès. Pour en savoir plus, consultez Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 9.

Nombre maximal de tentatives de connexion

Le nombre maximal autorisé d'échecs de tentatives de connexion avant que le système rejette la demande de connexion d'un utilisateur.

Page de réponse d'authentification active

La page de réponse HTTP fournie par le système ou personnalisée que vous souhaitez afficher pour les utilisateurs du portail captif. Après avoir sélectionné une **page de réponse** d'authentification active dans les paramètres d'authentification active de votre politique d'identité, vous devez également configurer une ou plusieurs règles d'identité avec la **`page de réponse HTTP`** comme **protocole d'authentification**.

La page de réponse HTTP fournie par le système comprend les champs **Nom d'utilisateur** et **Mot de passe**, ainsi qu'un bouton **Se connecter en tant qu'invité** pour permettre aux utilisateurs d'accéder au réseau en tant qu'invités. Pour afficher une méthode de connexion unique, configurez une page de réponse HTTP personnalisée.

Choisissez les options suivantes :

- Pour utiliser une réponse générique, cliquez **sur**. Vous pouvez cliquer sur **Afficher** ( ) pour afficher le code HTML de cette page.
- Pour créer une réponse personnalisée, cliquez sur **Personnalisé**. Une fenêtre s'affiche avec le code fourni par le système que vous pouvez remplacer ou modifier. Lorsque vous avez terminé, enregistrez vos modifications. Vous pouvez modifier une page personnalisée en cliquant sur **Edit** ( ).

Sujets connexes

Objets de certificat interne

Exclure des applications du portail captif

Vous pouvez sélectionner des applications (identifiées par leurs chaînes `d'agent utilisateur` HTTP) et les exempter de l'authentification active sur le portail captif. Cela permet au trafic des applications sélectionnées de passer par la politique d'identité sans authentification.

Remarque Seules les applications avec la **`balise d'exclusion d'agent d'utilisateur`** **sont** affichées dans cette liste.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Modifiez la politique d'identité qui contient la règle de portail captif.

Étape 4 Dans la page à onglet **Realm and Settings** (domaine et paramètres), développez **HTTP User Agent Exclusions** (Exclusions de l'agent utilisateur HTTP).

- Dans la première colonne, cochez la case à côté de chaque élément pour filtrer les applications, puis sur une ou plusieurs applications, et cliquez sur **Add to Rule**.

  Les cases à cocher font l'objet d'une combinaison AND.

- Pour affiner les filtres affichés, saisissez une chaîne de recherche dans le champ **Rechercher par nom**; cela est particulièrement utile pour les catégories et les balises. Pour effacer la recherche, cliquez sur **Effacer** ( ).

- Pour actualiser la liste des filtres et effacer les filtres sélectionnés, cliquez sur **Recharger** ( ).

Remarque La liste affiche 100 applications à la fois.

Étape 5 Choisissez les applications que vous souhaitez ajouter au filtre dans la liste **Applications disponibles** :

- Pour restreindre les applications individuelles qui s'affichent, saisissez une chaîne de recherche dans le champ **Rechercher par nom**. Pour effacer la recherche, cliquez sur **Effacer** ( ).
- Utilisez la messagerie au bas de la liste pour parcourir la liste des applications disponibles individuelles.
- Pour actualiser la liste des applications et effacer les applications sélectionnées, cliquez sur **Recharger** ( ).

Étape 6 Ajouter les applications sélectionnées à exclure de l'authentification externe. Vous pouvez cliquer et faire glisser, ou vous pouvez cliquer sur **Add to Rule**. Le résultat correspond à la combinaison des filtres d'application que vous avez sélectionnés.

Prochaine étape

- Continuez à configurer la règle d'identité comme décrit dans Créer une règle d'identité.

Dépannage de la source d'identité du portail captif

Pour d'autres renseignements relatifs au dépannage, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs et Dépannage du contrôle d'utilisateur.

Si vous rencontrez des problèmes avec le portail captif, vérifiez les éléments suivants :

- L'heure de votre périphérique géré de portail captif doit être synchronisée avec l'heure affichée sur centre de gestion.

- Si la résolution DNS est configurée et que vous créez une règle d'identité pour effectuer une opération de portail captif **Kerberos** (ou **HTTP Negotiate**, si vous souhaitez Kerberos en option), vous devez configurer votre serveur DNS pour résoudre le nom de domaine complet (FQDN) du nom de domaine du périphérique du portail captif. Le nom de domaine complet (FQDN) doit correspondre au nom d'hôte que vous avez fourni lors de la configuration du DNS.

  Pour en savoir plus, consultez À propos de la redirection de nom d'hôte, à la page 2.

- Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : Conventions de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles.

- Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans la section 6.2.5 de la RFC 6891.

- Si le portail captif est configuré correctement, mais que la redirection vers une adresse IP ou un nom de domaine complet (FQDN) échoue, désactivez le logiciel de sécurité pour points terminaux. Ce type de logiciel peut interférer avec la redirection.

- Si vous sélectionnez **Kerberos** (ou **HTTP Negotiate**, si vous souhaitez que Kerberos soit l'option) comme **type d'authentification** dans une règle d'identité, le **domaine** que vous sélectionnez doit être configuré avec un nom d'**utilisateurAD Join et un mot de passe AD Join** pour effectuer l'authentification active du portail captif Kerberos.

- Si vous sélectionnez **HTTP de base** comme **type d'authentification** dans une règle d'identité, les utilisateurs de votre réseau pourraient ne pas remarquer que leurs sessions expirent. La plupart des navigateurs Web mettent en cache les informations d'authentification des connexions **HTTP de base** et utilisent les informations d'authentification pour commencer en toute transparence une nouvelle session après l'expiration d'une ancienne session.

- Si la connexion entre votre centre de gestion et un périphérique géré échoue, aucune connexion à un portail captif signalée par le périphérique ne peut être identifiée pendant le temps d'arrêt, sauf si les utilisateurs ont déjà été vus et téléchargés sur centre de gestion. Les utilisateurs non identifiés sont connectés en tant qu'utilisateurs inconnus sur centre de gestion. Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.

- Si le périphérique que vous souhaitez utiliser pour le portail captif contient des interfaces en ligne et des interfaces routées, vous devez configurer une condition de zone dans vos règles d'identité de portail captif pour cibler uniquement les interfaces routées sur le périphérique de portail captif.

- Le nom d'hôte du périphérique géré doit comporter moins de 15 caractères pour que l'authentification Kerberos réussisse.

- La seule façon d'être sûr qu'un utilisateur se déconnecte est de fermer et de rouvrir le navigateur. Si ce n'est pas le cas, dans certains cas, l'utilisateur peut se déconnecter du portail captif et accéder au réseau sans avoir à s'authentifier à nouveau en utilisant le même navigateur.

- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.

- Lorsque le portail captif authentifie les utilisateurs qui correspondent à une règle d'identité, tout utilisateur de Microsoft Active Directory ou d'un groupe LDAP qui n'a pas été téléchargé est identifié comme étant inconnu. Pour éviter que les utilisateurs soient identifiés comme inconnus, configurez le domaine de domaine pour télécharger les utilisateurs de tous les groupes que vous souhaitez authentifier sur le portail captif. Les utilisateurs inconnus sont traités conformément à la politique de contrôle d'accès associée; si la politique de contrôle d'accès est configurée pour bloquer les utilisateurs inconnus, ces utilisateurs sont bloqués.

  Pour vous assurer que le système télécharge tous les utilisateurs dans un domaine de domaine , vérifiez que les groupes figurent dans la liste Groupes disponibles dans la configuration du domaine.

  Pour en savoir plus, consultez Synchroniser les utilisateurs et les groupes.

Historique du portail captif

Fonctionnalités	Centre de gestion Minimum Centre de gestion	Défense contre les menaces Minimum	Détails
Redirection du nom d'hôte.	N'importe lequel	7.1.0 avec Snort 3	Vous pouvez utiliser un objet réseau qui contient le nom d'hôte complet (FQDN) de l'interface que le portail captif peut utiliser pour les demandes d'authentification actives.
Connexion invité.	N'importe lequel	6.1.0	Les utilisateurs peuvent se connecter en tant qu'invités en utilisant le portail captif.
portail captif	N'importe lequel	6.0.0	Fonctionnalité introduite. Vous pouvez utiliser le portail captif pour demander aux utilisateurs de saisir leurs informations d'authentification lorsque vous y êtes invité dans une fenêtre de navigateur. Le mappage permet également de fonder les politiques sur un utilisateur ou un groupe d'utilisateurs.

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.