Classifier les utilisateurs finaux pour l'application des politiques

Cette rubrique contient les sections suivantes :

Survol de la classification des utilisateurs et logiciels clients

Les profils d'identification vous permettent de classer les utilisateurs et les agents utilisateurs (logiciel client) aux fins suivantes :

- Demandes de transaction groupées pour l'application des politiques (sauf les logiciels-services)
- Spécification des exigences d'identification et d'authentification

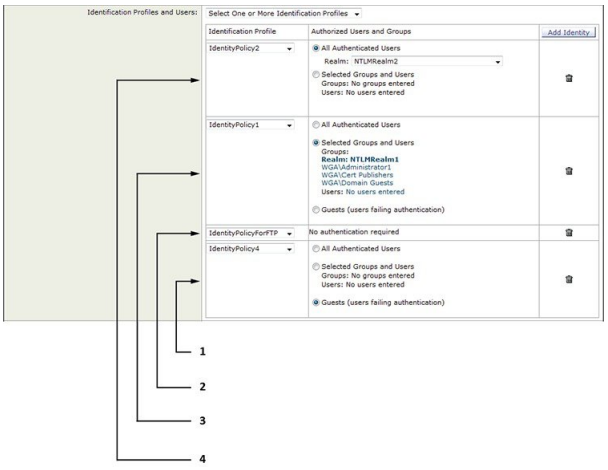
AsyncOS attribue un profil d'identification à chaque transaction :

- Profils d'identification personnalisés – AsyncOS attribue un profil personnalisé en fonction des critères de cette identité.
- Profil d'identification global – AsyncOS attribue le profil global aux transactions qui ne répondent aux critères d'aucun profil personnalisé. Par défaut, le profil global ne nécessite pas d'authentification.

AsyncOS traite les profils d'identification de manière séquence, en commençant par le premier. Le profil global est le dernier profil.

Un profil d'identification ne peut comprendre qu'un seul critère. Par ailleurs, les profils d'identification qui comprennent plusieurs critères exigent que tous les critères soient satisfaits.

Une politique peut faire appel à plusieurs profils d'identification :



1	Ce profil d'identification permet l'accès en tant qu'invité et s'applique aux utilisateurs dont l'authentification échoue.
2	L'authentification n'est pas utilisée pour ce profil d'identification.
3	Les groupes d'utilisateurs précisés dans ce profil d'identification sont autorisés pour cette politique.
4	Ce profil d'identification utilise une séquence d'authentification et cette politique s'applique à un domaine dans la séquence.

Classification des utilisateurs et des logiciels clients : bonnes pratiques

- Créez des profils d'identification moins nombreux et plus généraux qui s'appliquent à tous les utilisateurs ou à des groupes d'utilisateurs moins nombreux et plus importants. Utilisez des politiques plutôt que des profils pour une gestion plus granulaire.
- Créez des profils d'identification avec des critères uniques.
- S'il est déployé en mode transparent, créez un profil d'identification pour les sites qui ne prennent pas en charge l'authentification. Consultez Contournement de l'authentification.

Critères du profil d'identification

Ces caractéristiques de transaction sont disponibles pour définir un profil d'identification :

Option	Description
Subnet (Sous-réseau)	Le sous-réseau client doit correspondre à la liste des sous-réseaux dans une politique.
Protocole	Le protocole utilisé dans la transaction : HTTP, HTTPS, SOCKS ou FTP natif.

Option	Description
Port	Le port proxy de la demande doit se trouver dans la liste de ports du profil d'identification, le cas échéant. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination.
User Agent (Agent d'utilisateur)	L'agent utilisateur (application client) effectuant la demande doit figurer dans la liste des agents utilisateurs du profil d'identification, le cas échéant. Certains agents utilisateurs ne peuvent pas gérer l'authentification. Par conséquent, la création d'un profil qui n'exige pas d'authentification est nécessaire. Les agents utilisateurs comprennent des programmes comme les programmes de mise à jour et les navigateurs comme Internet Explorer et Mozilla Firefox.
URL Category (Catégorie URL)	La catégorie de l'URL de la demande doit faire partie de la liste des catégories d'URL du profil d'identification, le cas échéant.
Authentication requirements (Exigences relatives à l'authentification)	Si le profil d'identification nécessite une authentification, les justificatifs d'authentification du client doivent correspondre aux exigences d'authentification du profil d'identification.

Classification des utilisateurs et logiciels clients

Avant de commencer

- Créez des domaines d'authentification. Reportez-vous aux sections Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique) ou Création d'un domaine d'authentification LDAP.
- Sachez que lorsque vous validez des modifications aux profils d'identification, les utilisateurs finaux doivent s'authentifier de nouveau.
- Si vous êtes en mode Cloud Connector, sachez qu'une option supplémentaire de profil d'identification est offerte : l'ID de l'ordinateur. Consultez Identification des ordinateurs pour l'application des politiques.
- (Facultatif) Créez des séquences d'authentification. Voir la section Création de séquences d'authentification.
- (Facultatif) Activez Secure Mobility si le profil d'identification doit inclure des utilisateurs mobiles.
- (Facultatif) Découvrez les méthodes de substitution d'authentification. Voir Suivi des utilisateurs identifiés .

Étape 1 Choisissez **Web Security Manager** > **Identification Profiles** (Web Security Manager > Profils d'identification).

Étape 2 Cliquez sur **Add Profile** (Ajouter un profil) pour ajouter un profil.

Étape 3 Cochez la case **Enable Identification Profile** (Activer le profil d'identification) pour activer ce profil ou pour le désactiver rapidement sans le supprimer.

Étape 4 Attribuez un **nom** de profil unique.

Étape 5 La **description** est facultative.

Étape 6 Dans la liste déroulante **Insert Above** (Insérer au-dessus), choisissez l'endroit où ce profil doit apparaître dans le tableau.

Remarque Parmi les profils d'identification de poste qui ne nécessitent pas d'authentification figurent le premier profil d'identification qui nécessite une authentification.

Étape 7 Dans la section **User Identification Method** (Méthode d'identification de l'utilisateur), choisissez une méthode d'identification, puis définissez les paramètres connexes; les options affichées varient selon la méthode choisie.

a) Choisissez une méthode d'identification dans la liste déroulante **User Identification Method** (Méthode d'identification de l'utilisateur).

Option	Description
Exempt from authentication/ identification (Dispenser d'authentification et d'identification)	Les utilisateurs sont principalement identifiés par leur adresse IP. Aucun paramètre supplémentaire n'est requis.
Authenticate users (Authentifier les utilisateurs)	Les utilisateurs sont identifiés par les justificatifs d'authentification qu'ils ont saisis.
Transparently identify users with ISE (Identification transparente des utilisateurs avec ISE)	Disponible lorsque le service ISE est activé(Network > Identity Services Engine) (Réseau > Moteur ISE). Pour ces transactions, le nom d'utilisateur et les étiquettes Groupe sécurisé associées seront obtenus à partir du moteur ISE. Dans les déploiements ISE-PIC, les informations sur les groupes et les utilisateurs ISE sont reçues. Pour en savoir plus, consultez Tâches relatives à l'intégration du service ISE/ISE-PIC.
Transparently identify users with authentication realm (Identification transparente des utilisateurs à l'aide du domaine d'authentification)	Cette option est disponible si un ou plusieurs domaines d'authentification sont configurés pour prendre en charge l'identification transparente.

Remarque Lorsqu'au moins un profil d'identification avec authentification ou identification transparente est configuré, les tableaux de politiques prennent en charge la définition de l'appartenance à la politique à l'aide de noms d'utilisateur, de groupes de répertoires et d'étiquettes Groupe sécurisé.

Remarque L'agent CDA (Context Directory Agent) n'est plus pris en charge. Il est recommandé de configurer ISE/ISE-PIC pour une identification transparente de l'utilisateur afin d'obtenir la même fonctionnalité.

Les options de configuration de CDA ne seront plus disponibles dans les versions ultérieures.

Pour en savoir plus, consultez https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/bulletin-c25-2428601.html.

b) Fournissez les paramètres appropriés à la méthode choisie. Les sections décrites dans ce tableau ne sont pas toutes visibles pour chaque choix.

Option de rechange au domaine d'authentification ou aux privilèges invité	Si l'authentification de l'utilisateur n'est pas disponible dans ISE : • **Support Guest Privileges** (Privilèges d'assistance invité) : la transaction sera autorisée à se poursuivre et correspondra aux politiques ultérieures pour les utilisateurs invités de tous les profils d'identification. • **Block Transactions** (Bloquer les transactions) : l'accès à Internet n'est pas permis aux utilisateurs qui ne peuvent pas être identifiés par ISE. • **Support Guest privileges** (Privilèges d'assistance invité) : cochez cette case pour accorder l'accès invité aux utilisateurs qui échouent à l'authentification en raison d'informations d'authentification non valides.

Domaine d'authentification	

Select a Realm or Sequence (Sélectionner un domaine ou une séquence) : choisissez un domaine ou une séquence d'authentification défini.

Select a Scheme (Sélectionner un schéma) : choisissez un schéma d'authentification :

- **Kerberos** : le client est authentifié de manière transparente au moyen de tickets Kerberos.
- **Basic** (De base) : le client demande toujours aux utilisateurs des informations d'authentification. Une fois que l'utilisateur a saisi les informations d'authentification, les navigateurs proposent généralement une case à cocher pour se souvenir des informations d'authentification fournies. Chaque fois que l'utilisateur ouvre le navigateur, le client demande des informations d'authentification ou renvoie les informations d'authentification précédemment enregistrées.

  Les informations d'authentification sont envoyées non sécurisées en texte clair (Base64). Une capture de paquets entre le client et Secure Web Appliance peut révéler le nom d'utilisateur et la phrase secrète.
- **NTLMSSP** : le client s'authentifie de manière transparente à l'aide de ses coordonnées de connexion Windows. L'utilisateur n'est pas invité à saisir ses informations d'authentification.

  Cependant, le client l'invite à saisir ses informations d'authentification dans les circonstances suivantes :

  - Échec des informations d'authentification Windows.
  - Le client ne fait pas confiance au Secure Web Appliance en raison des paramètres de sécurité du navigateur.

  Les informations d'authentification sont envoyées de manière sécurisée à l'aide d'une liaison tridirectionnelle (authentification de style condensé). La phrase secrète n'est jamais envoyée sur la connexion.
- **Header Based Authentication** (Authentification par en-tête) : le client et Secure Web Appliance considèrent l'utilisateur comme authentifié et ne lui demandent plus son authentification ou ses identifiants. La fonctionnalité X-Authenticated est opérante lorsque Secure Web Appliance agit en tant que périphérique en amont.

  Une fois l'authentification réussie, le périphérique en aval envoie le nom d'utilisateur et les groupes d'utilisateurs (facultatif) à Secure Web Appliance par le biais des en-têtes HTTP étendus X-Authenticated-User et X-Authenticated-Groups (facultatif).

  L'en-tête X-Authenticated-Groups sera pris en compte uniquement si vous configurez l'option **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** (Utiliser des groupes dans l'en-tête X-Authenticate-Groups/l'en-tête personnel pour les politiques correspondantes) sur l'appliance [**Network** > **Authentication** > **Edit Global Settings** (Réseau > Authentification > Modifier les paramètres globaux)].

  Remarque Les en-têtes X-Authenticated ne s'appliquent qu'aux politiques d'accès ou de routage. Cependant, l'association à une politique de déchiffrement du profil d'identification pour lequel l'option **Header**

	Based Authentication (Authentification basée sur l'en-tête) est activée ne produira pas de correspondance. • **Support Guest privileges** (Privilèges d'assistance invité) : cochez cette case pour accorder l'accès invité aux utilisateurs qui échouent à l'authentification en raison d'informations d'authentification non valides.
Domaine pour l'authentification de groupe	• **Select a Realm or Sequence** (Sélectionner un domaine ou une séquence) : choisissez un domaine ou une séquence d'authentification défini.

Authentication Surrogates (Substitutions d'authentification)	Indiquez comment les transactions seront associées à un utilisateur une fois l'authentification réussie (les options varient en fonction du mode de déploiement du proxy Web) : • **IP Address (Adresse IP)** : le proxy Web suit un utilisateur authentifié à une adresse IP particulière. Pour une identification transparente de l'utilisateur, sélectionnez cette option. • **Persistent Cookie** (Témoin persistant) : le proxy Web suit un utilisateur authentifié sur une application particulière en générant un témoin persistant pour chaque utilisateur et par application. La fermeture de l'application ne supprime pas le témoin. • **Session Cookie** (Témoin de session) : le proxy Web suit un utilisateur authentifié sur une application particulière en générant un témoin de session pour chaque utilisateur, par domaine et par application. (Cependant, lorsqu'un utilisateur fournit différents identifiants pour le même domaine à partir de la même application, le témoin est remplacé.) La fermeture de l'application supprime le témoin. • **No Surrogate** (Pas de substitution) : le proxy Web n'utilise pas de substitution pour mettre en cache les informations d'authentification et il suit un utilisateur authentifié pour chaque nouvelle connexion TCP. Lorsque vous choisissez cette option, l'interface Web désactive les autres paramètres qui ne s'appliquent plus. Cette option est disponible uniquement en mode de transfert explicite et lorsque vous désactivez le chiffrement des informations d'authentification dans la page Network > Authentication. • **Apply same surrogate settings to explicit forward requests** (Appliquer les mêmes paramètres de substitution aux demandes de transfert explicites) : cochez cette case pour appliquer la substitution utilisée pour les demandes transparentes aux demandes explicites; active automatiquement le chiffrement des identifiants. Cette option ne s'affiche que lorsque le proxy Web est déployé en mode transparent. **Remarque** • Vous pouvez définir une limite de délai d'expiration pour le remplaçant d'authentification pour toutes les demandes dans les paramètres d'authentification globaux. • Si vous avez configuré les profils d'identification de manière à utiliser différentes substitutions d'authentification (adresse IP, témoin persistant, témoin de session, etc.), l'accès est authentifié à l'aide de la substitution d'adresse IP même si l'accès correspond aux profils d'identification avec d'autres substitutions.

Étape 8 Dans la section de **Membership Definition** (Définition de l'appartenance), indiquez les paramètres d'appartenance appropriés selon la méthode d'identification choisie. Notez que toutes les options décrites dans ce tableau ne sont pas disponibles pour toutes les méthodes d'identification de l'utilisateur.

Membership Definition (Définition de l'appartenance)

Define Members by User Location (Définir les membres par emplacement d'utilisateur)	Configurez ce profil d'identification de sorte qu'il s'applique aux utilisateurs suivants : **utilisateurs locaux uniquement**, **utilisateurs à distance uniquement** ou les **deux**. Cette sélection affecte les paramètres d'authentification disponibles pour ce profil d'identification.
Define Members by Subnet (Définir les membres par sous-réseau)	Saisissez les adresses auxquelles ce profil d'identification doit s'appliquer. Vous pouvez utiliser des adresses IP, des blocs d'CIDR et des sous-réseaux. **Remarque** Si aucune information n'est saisie, le profil d'identification s'applique à toutes les adresses IP.
Define Members by Protocol (Définir les membres par protocole)	Sélectionnez les protocoles auxquels ce profil d'identification doit s'appliquer; sélectionnez toutes les réponses qui s'appliquent : • **HTTP/HTTPS** : s'applique à toutes les demandes qui utilisent HTTP ou HTTPS comme protocole sous-jacent, y compris FTP sur HTTP et tout autre protocole tunnelisé à l'aide de HTTP CONNECT. • **FTP natif** : s'applique aux demandes FTP natives uniquement. • **SOCKS** : s'applique uniquement aux politiques SOCKS
Define Members by Machine ID (Définir les membres par ID d'ordinateur)	• **Do Not Use Machine ID in This Policy** (Ne pas utiliser l'ID d'ordinateur dans cette politique) : l'utilisateur n'est pas identifié par l'ID d'ordinateur. • **Define User Authentication Policy Based on Machine ID** (Définir la politique d'authentification des utilisateurs en fonction de l'ID de l'ordinateur) : l'utilisateur est identifié principalement par l'ID de l'ordinateur. Cliquez sur la zone Machine Groups (Groupes d'ordinateurs) pour afficher la page des groupes d'ordinateurs autorisés. Pour chaque groupe que vous souhaitez ajouter, dans le champ Directory Search (Recherche dans le répertoire), commencez à taper le nom du groupe à ajouter, puis cliquez sur Add (Ajouter). Vous pouvez sélectionner un groupe, et cliquer sur Delete (Supprimer) pour le retirer de la liste. Cliquez sur Done (Terminé) pour revenir à la page précédente. Cliquez dans la zone Machine IDs (ID d'ordinateur) pour afficher la page des ordinateurs autorisés. Dans le champ Authorized Machines (Ordinateurs autorisés), saisissez les ID des ordinateurs à associer à la politique, puis cliquez sur Done (Terminé). **Remarque** L'authentification à l'aide de l'ID d'ordinateur est prise en charge uniquement en mode Connector et nécessite Active Directory.

Advanced (Niveau avancé)	Développez cette section pour définir les exigences d'appartenance supplémentaires. • **Proxy Ports** (Ports proxy) : indiquez un ou plusieurs ports proxy utilisés pour accéder au proxy Web. Entrez les numéros de port séparés par des virgules. Pour les connexions de transfert explicite, le port proxy est configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. La définition des identités par port fonctionne mieux lorsque l'appliance est déployée en mode de transfert explicite ou lorsque les clients transfèrent explicitement les demandes à l'appliance. La définition des identités par port lorsque les demandes des clients sont redirigées de manière transparente vers l'appliance peut entraîner le refus de certaines demandes. • **URL Categories** (Catégories d'URL) : sélectionnez des catégories d'URL prédéfinies ou définies par l'utilisateur. L'appartenance pour les deux est exclue par défaut, ce qui signifie que le proxy Web ignore toutes les catégories, sauf si elles sont sélectionnées dans la colonne Add (ajouter). Si vous devez définir l'appartenance par catégorie d'URL, définissez-la uniquement dans le groupe Identity lorsque vous devez exclure des demandes d'authentification à cette catégorie. • **User Agents** (Agents utilisateurs) : définit l'appartenance au groupe de politiques des agents utilisateurs trouvés dans la demande du client. Vous pouvez sélectionner des agents généralement définis ou définir les vôtres à l'aide d'expressions régulières. Précisez également si ces spécifications d'agent utilisateur sont inclusives ou exclusives. Autrement dit, si la définition de l'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateurs sélectionnés

Étape 9 Envoyez et validez les modifications.

Prochaine étape

- Survol de l'acquisition des informations d'authentification de l'utilisateur final
- Présentation des tâches de gestion des demandes Web au moyen de politiques

Activer/désactiver une identité

Before you begin

- Sachez que la désactivation d'un profil d'identification entraîne la suppression de ce dernier des politiques associées.
- Sachez que la réactivation d'un profil d'identification ne le réassocie à aucune politique.

Étape 1 Choisissez **Web Security Manager** > **Identification Profiles** (Web Security Manager > Profils d'identification).

Étape 2 Cliquez sur un profil dans le tableau des profils d'identification pour ouvrir la page Identification Profile (Profil d'identification) pour ce profil.

Étape 3 Cochez ou décochez la case **Enable Identification Profile** (Activer le profil d'identification) immédiatement sous Client/User Identification Profile Settings (Paramètres du profil d'identification utilisateur/client).

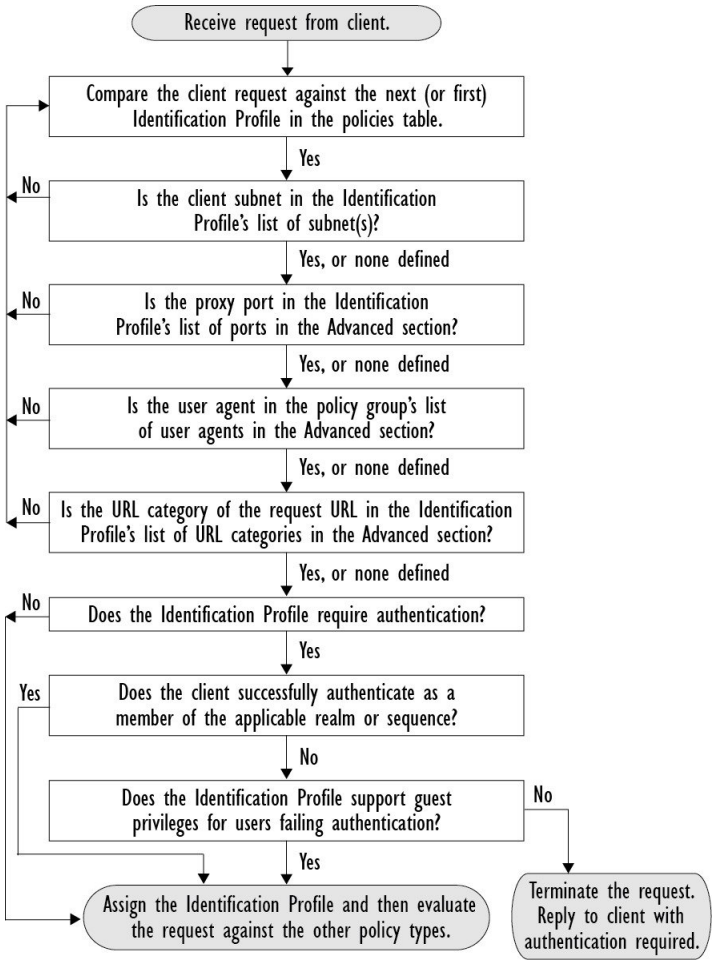
Étape 4 Envoyez et validez les modifications.

Profils d'identification et authentification

Le diagramme suivant montre comment le proxy Web évalue une demande d'un client par rapport à un profil d'identification lorsque ce dernier est configuré pour utiliser :

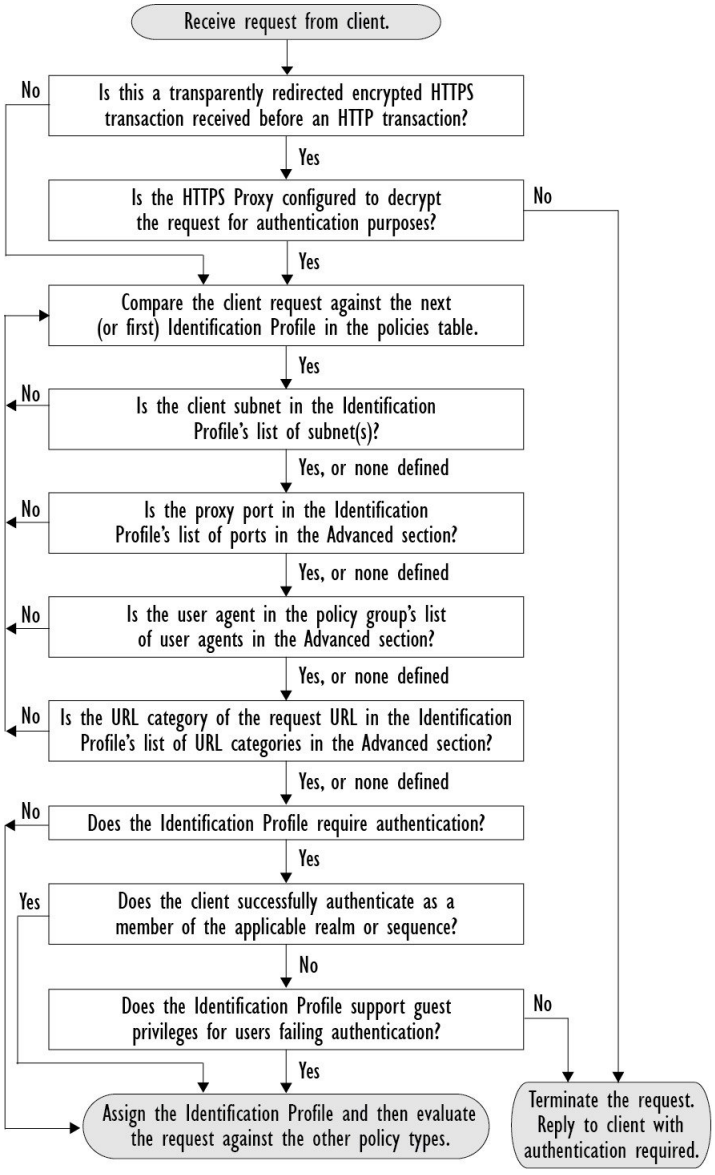
- Aucune substitution d'authentification
- Adresses IP comme substitutions d'authentification
- Témoins comme témoins d'authentification avec des demandes transparentes
- Les témoins comme substitutions d'authentification avec des demandes explicites et le chiffrement des identifiants sont activés

Figure 1: Profils d'identification et traitement d'authentification – Aucune substitution et substitutions basées sur IP



Le diagramme suivant montre comment le proxy Web évalue une demande d'un client par rapport à un profil d'identification lorsque le profil d'identification est configuré pour utiliser des témoins comme substitutions d'authentification, le chiffrement des informations d'identification est activé et la demande est explicitement transférée.

Figure 2: Profils d'identification et traitement d'authentification – Substitutions basées sur des témoins



Résolution de problèmes relatifs aux profils d'identification

- Problèmes d'authentification de base
- Problèmes de politique
- La politique n'est jamais appliquée
- Outil de résolution de problèmes liés aux politiques : Suivi des politiques

Résolution des problèmes relatifs aux types de substitution dans les profils d'identification

Lorsque l'appliance Cisco pour la sécurité du Web est configurée pour utiliser à la fois l'adresse IP et les substitutions d'authentification par témoin et que l'accès de l'utilisateur final correspond aux deux identités, l'adresse IP prévaut sur les substitutions d'authentification par témoin.

Dans un réseau comprenant des ordinateurs partagés et des ordinateurs individuels, il est recommandé de créer deux profils d'identification différents en fonction des adresses IP et des sous-réseaux, qui détermineront si des valeurs de substitution pour l'authentification par IP ou à l'aide de témoins sont utilisées.

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.