Stratégies d'identité

Vous pouvez utiliser des politiques d'identité pour collecter des renseignements sur l'identité des utilisateurs à partir des connexions. Vous pouvez ensuite afficher l'utilisation en fonction de l'identité de l'utilisateur dans les tableaux de bord et configurer le contrôle d'accès en fonction de l'utilisateur ou du groupe d'utilisateurs.

Aperçu de la politique d'identité

Vous pouvez utiliser les politiques d'identité pour détecter l'utilisateur associé à une connexion. En identifiant l'utilisateur, vous pouvez corréler les informations sur les menaces, les points terminaux et le réseau avec les informations d'identité de l'utilisateur. En associant le comportement, le trafic et les événements du réseau directement à chaque utilisateur, le système peut vous aider à déterminer la source des violations des politiques, des attaques ou des vulnérabilités du réseau.

Par exemple, vous pouvez identifier à qui appartient l'hôte ciblé par un incident d'intrusion et qui a lancé une attaque interne ou un balayage de port. Vous pouvez également identifier les utilisateurs à bande passante élevée et les utilisateurs qui accèdent à des sites Web ou à des applications indésirables.

La détection des utilisateurs va au-delà de la collecte de données pour l'analyse. Vous pouvez également définir des critères d'accès en fonction du nom d'utilisateur ou du nom de groupe d'utilisateurs, afin d'autoriser ou de bloquer sélectivement l'accès aux ressources selon l'identité de l'utilisateur.

Vous pouvez obtenir l'identité de l'utilisateur à l'aide des méthodes suivantes :

- Authentification passive—Pour tous les types de connexions, obtenez l'identité de l'utilisateur à partir d'autres services d'authentification sans demander le nom d'utilisateur et le mot de passe.
- Authentification active : pour les connexions HTTP uniquement, demandez le nom d'utilisateur et le mot de passe et authentifiez-vous auprès de la source d'identité indiquée afin d'obtenir l'identité de l'utilisateur pour l'adresse IP source.

Pour plus d'informations, consultez les rubriques suivantes.

Établissement de l'identité de l'utilisateur par l'authentification passive

L'authentification passive recueille l'identité de l'utilisateur sans lui demander son nom d'utilisateur et son mot de passe. Le système obtient les mappages à partir des sources d'identité que vous indiquez.

Vous pouvez obtenir de manière passive des mappages utilisateur-adresse IP à partir des sources suivantes :

- Connexions VPN d'accès à distance. Les types d'utilisateurs suivants sont pris en charge pour l'identité passive :
  - Comptes d'utilisateur définis dans un serveur d'authentification externe.
  - Les comptes d'utilisateurs locaux qui sont définis dans le Firepower Device Manager.
- Cisco Identity Services Engine (ISE) ; Cisco Identity Services Engine Passive Identity Connector (ISE PIC).

Si un utilisateur donné est identifié par plusieurs sources, l'identité du VPN d'accès à distance prévaut.

Établissement de l'identité de l'utilisateur par l'authentification active

L'authentification est l'action de confirmer l'identité d'un utilisateur.

Avec l'authentification active, lorsqu'un flux de trafic HTTP provient d'une adresse IP pour laquelle le système ne dispose d'aucun mappage d'identité d'utilisateur, vous pouvez décider d'authentifier ou non l'utilisateur à l'origine du flux de trafic auprès du répertoire configuré pour le système. Si l'utilisateur s'authentifie avec succès, l'adresse IP est considérée comme ayant l'identité de l'utilisateur authentifié.

L'échec de l'authentification n'affecte pas l'accès au réseau pour l'utilisateur. Ce sont vos critères d'accès qui déterminent en dernier ressort le niveau d'accès accordé à ces utilisateurs.

Traiter avec des utilisateurs inconnus

Lorsque vous configurez le serveur de répertoire pour la politique d'identité, le système télécharge les informations d'appartenance des utilisateurs et des groupes à partir du serveur de répertoire. Ces informations sont actualisées toutes les 24 heures à zéro, ou chaque fois que vous modifiez et enregistrez la configuration du répertoire (même si vous n'apportez aucune modification).

Si un utilisateur réussit à s'authentifier lorsqu'il est invité par une règle d'identité d'authentification active, mais que le nom de l'utilisateur ne figure pas dans les informations d'identité de l'utilisateur téléchargées, l'utilisateur est marqué comme Inconnu. Vous ne verrez pas l'ID de l'utilisateur dans les tableaux de bord liés à l'identité, et l'utilisateur ne correspondra pas aux règles de groupe.

Cependant, toutes les règles de contrôle d'accès pour l'utilisateur inconnu s'appliqueront. Par exemple, si vous bloquez les connexions pour les utilisateurs inconnus, ces utilisateurs sont bloqués même s'ils ont réussi à s'authentifier (ce qui signifie que le serveur de répertoire reconnaît l'utilisateur et que le mot de passe est valide).

Ainsi, lorsque vous apportez des modifications au serveur de répertoire, comme l'ajout ou la suppression d'utilisateurs, ou la modification de l'appartenance à un groupe, ces modifications ne sont pas répercutées dans l'application des politiques tant que le système n'a pas téléchargé les mises à jour à partir du répertoire.

Si vous ne souhaitez pas attendre la mise à jour quotidienne de minuit, vous pouvez forcer une mise à jour en modifiant les informations de domaine du répertoire (à partir de **Objects (Objets)** > **Identity Sources (Sources**

d'identité), puis modifiez le domaine). Cliquez sur **Save** (Enregistrer), puis déployez les modifications. Le système téléchargera immédiatement les mises à jour.

Remarque Vous pouvez vérifier si des informations d'utilisateur nouvelles ou supprimées se trouvent sur le système en vous rendant dans **Policies (Politiques)** > **Access Control (Contrôle d'accès)**, en cliquant sur le bouton **Add Rule (Ajouter une règle) (+)**, puis en consultant la liste des utilisateurs sous l'onglet **Users (Utilisateurs)**. Si vous ne trouvez pas un nouvel utilisateur ou si vous trouvez un utilisateur supprimé, le système dispose d'informations obsolètes.

Comment mettre en œuvre la politique d'identité

Pour activer l'acquisition de l'identité de l'utilisateur, afin que l'utilisateur associé à une adresse IP soit connu, vous devez configurer plusieurs éléments. Lorsqu'il est configuré correctement, vous pourrez voir les noms d'utilisateur dans les tableaux de bord et les événements de surveillance. Vous pourrez également utiliser l'identité de l'utilisateur dans les règles de contrôle d'accès et de déchiffrement SSL comme critère de correspondance du trafic.

La procédure suivante fournit un aperçu de ce que vous devez configurer pour que les politiques d'identité fonctionnent.

Procédure

Étape 1 Configurez le domaine d'identité AD.

Que vous collectiez l'identité de l'utilisateur de manière active (en invitant à l'authentification de l'utilisateur) ou passive, vous devez configurer le serveur Active Directory (AD) qui dispose des informations d'identité de l'utilisateur. Consultez Configuration des domaines d'identité AD.

Si vous configurez l'identité passive, vous pouvez créer des séquences de domaine AD qui permettent au système d'extraire les identités de plusieurs domaines AD. Cette fonction est utile si vous avez plusieurs domaines AD dans votre réseau.

Étape 2 Si vous souhaitez utiliser des règles d'identité d'authentification passive, configurez les sources d'identité passive.

Vous pouvez configurer l'un des éléments suivants, en fonction des services que vous mettez en œuvre dans le périphérique et des services disponibles dans votre réseau.

- VPN d'accès à distance : si vous avez l'intention de prendre en charge les connexions VPN d'accès à distance sur le périphérique, les connexions d'utilisateur peuvent fournir l'identité en fonction du serveur AD ou des utilisateurs locaux (ceux définis dans Firepower Device Manager). Pour en savoir plus sur la configuration du VPN d'accès à distance, consultez Configuration du VPN d'accès à distance.
- Cisco Identity Services Engine (ISE) ou Cisco Identity Services Engine Passive Identity Connector (ISE PIC) : si vous utilisez ces produits, vous pouvez configurer l'appareil en tant qu'abonné pxGrid et obtenir l'identité de l'utilisateur auprès d'ISE. Consultez Configurer Identity Services Engine (ISE).

Étape 3 Choisissez **Policies (Politiques)** > **Identity (Identité)**, et activez la politique d'identité. Consultez Configuration des politiques d'identité, à la page 5.

Étape 4 Configurer les paramètres de la politique d'identité, à la page 6.

Les sources d'identité passives sont automatiquement sélectionnées en fonction des sources que vous avez configurées dans le système. Si vous souhaitez configurer l'authentification active, vous devez configurer les certificats pour le portail captif et le déchiffrement avec nouvelle signature SSL (si vous n'avez pas encore activé la politique de déchiffrement SSL).

Étape 5 Configurer l'action par défaut de la politique d'identité, à la page 8.

Si votre intention est d'utiliser uniquement l'authentification passive, vous pouvez définir l'action par défaut sur l'authentification passive et il n'est pas nécessaire de créer des règles spécifiques.

Étape 6 Configurer les règles d'identité, à la page 8.

Créez des règles qui collecteront les identités d'utilisateurs passives ou actives à partir des réseaux concernés.

Bonnes pratiques pour Active Authentication (Authentification active)

Lorsqu'une règle d'identité requiert une authentification active pour un utilisateur, l'utilisateur est redirigé vers le port du portail captif de l'interface par laquelle il est connecté, puis il est invité à s'authentifier.

Comme cette redirection se fait vers l'adresse IP de l'interface, le certificat Identity Policy (Politique d'identité) ne correspond pas exactement et les utilisateurs reçoivent une erreur de certificat non fiable. L'utilisateur doit accepter le certificat pour continuer et s'authentifier sur le périphérique. Comme ce comportement est similaire à une attaque de l'homme du milieu, les utilisateurs sont réticents à accepter le certificat non fiable.

Pour éviter ce problème, vous pouvez configurer l'authentification active pour utiliser le nom de domaine complet (FQDN) d'une interface sur le périphérique. 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.

Avant de commencer

La fonctionnalité Active Authentication (Authentification active) s'applique uniquement au trafic HTTP et perturbe l'utilisateur final chaque fois que le périphérique n'a pas de mappage d'utilisateur à jour pour le poste de travail de l'utilisateur ou un autre périphérique client. Vous pouvez éviter ces perturbations en mettant plutôt en œuvre l'authentification passive.

Procédure

Étape 1 Dans le serveur DNS, définissez un nom de domaine complet (FQDN) pour l'adresse IP de l'interface que vous souhaitez utiliser pour recueillir l'authentification active.

Également appelée Captive Portal (portail captif), il doit s'agir d'une interface routée.

Étape 2 À l'aide d'une Certificate Authority (CA) (autorité de certification), obtenez un certificat pour ce nom de domaine complet.

Vous pouvez créer un certificat pour le nom de domaine complet spécifique, par exemple ftd1.captive-port.example.com. Vous pouvez également :

- Obtenir un certificat générique qui peut s'appliquer aux interfaces de Captive Portal (portail captif) sur de nombreux périphériques différents, par exemple : *.captive-port.example.com. Le caractère générique peut aussi être plus large et s'appliquer à une vaste classe de points d'accès, par exemple : *.eng.example.com ou même *.example.com.
- Inclure plusieurs Subject Alternate Names (SAN) (noms alternatifs du sujet) dans le certificat.

Étape 3 Sélectionner **Objects (Objets)** > **Certificates (Certificats)** et charger le certificat.

Étape 4 Sélectionner **Objects (Objets)** > **réseau d'objets** et créez un objet de réseau FQDN pour le nom DNS.

Étape 5 Sur la page **Policies (Politiques)** > **Identity (Identité)**, mettre à jour les paramètres de la politique d'identité avec le certificat et l'objet FQDN.

Étape 6 Créer des règles dans la politique d'identité qui utilisent Active Authentication (authentification active).

Configuration des politiques d'identité

Vous pouvez utiliser des politiques d'identité pour collecter des renseignements sur l'identité des utilisateurs à partir des connexions. Vous pouvez ensuite afficher l'utilisation en fonction de l'identité de l'utilisateur dans les tableaux de bord et configurer le contrôle d'accès en fonction de l'utilisateur ou du groupe d'utilisateurs.

Voici un aperçu de la configuration des éléments requis pour obtenir l'identité de l'utilisateur au moyen des politiques d'identité.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Si vous n'avez pas encore défini de politique d'identité, cliquez sur **Enable Identity Policy** (Activer la politique d'identité) et configurez les paramètres comme décrit dans Configurer les paramètres de la politique d'identité, à la page 6.

Étape 2 Gérer la politique d'identité.

Une fois que vous avez configuré les paramètres d'identité, cette page répertorie toutes les règles dans l'ordre. Les règles sont comparées au trafic du haut vers le bas, la première correspondance détermine l'action à appliquer. Vous pouvez effectuer ce qui suit à partir de cette page :

- Pour activer ou désactiver la politique d'identité, cliquez sur le bouton à bascule **Identity Policy** (Politique d'identité).
- Pour modifier les paramètres de la politique d'identité, cliquez sur le bouton **Identity Policy Configuration** (Configuration de la politique d'identité) ().
- Pour modifier **Default Action** (Action par défaut), cliquez sur l'action et sélectionnez l'action souhaitée. Consultez Configurer l'action par défaut de la politique d'identité, à la page 8.

- Pour déplacer une règle, modifiez-la et sélectionnez le nouvel emplacement dans la liste déroulante **Order** (Ordre).
- Pour configurer des règles :
  - Pour créer une nouvelle règle, cliquez sur le bouton +.
  - Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle (dans la colonne Actions). Vous pouvez également modifier de manière sélective une propriété de règle en cliquant sur la propriété dans le tableau.
  - Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle (dans la colonne Actions).

Pour plus d'informations sur la création et la modification des règles d'identité, consultez Configurer les règles d'identité, à la page 8.

Configurer les paramètres de la politique d'identité

Pour que les politiques d'identité fonctionnent, vous devez configurer les sources qui fournissent des informations sur l'identité de l'utilisateur. Les paramètres que vous devez configurer varient selon le type de règles que vous configurez : passives, actives ou les deux.

La boîte de dialogue des paramètres affiche ces paramètres dans des sections distinctes. Selon la façon dont vous accédez à la boîte de dialogue, vous verrez les deux sections ou une seule section. La boîte de dialogue s'affiche automatiquement si vous essayez de créer une règle pour un type d'authentification sans avoir déjà configuré les paramètres requis.

La procédure suivante couvre la boîte de dialogue complète.

Avant de commencer

Vérifiez que les paramètres d'horloge sont uniformes pour les serveurs d'annuaire, le périphérique Firewall Threat Defense et les clients. Un décalage temporel entre ces périphériques peut empêcher l'authentification de l'utilisateur réussie. « cohérence » signifie que vous pouvez utiliser différents fuseaux horaires, mais que l'heure doit être la même pour ces fuseaux horaires; par exemple, 10 h HNP = 13 h HNE.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Étape 2 Cliquez sur le bouton **Identity Policy Configuration** ( ).

Étape 3 Configurez les options **d'authentification passive**.

La boîte de dialogue vous affiche les sources d'authentification passive que vous avez déjà configurées.

Si nécessaire, vous pouvez configurer ISE à partir de cette boîte de dialogue. Si vous n'avez pas encore configuré d'objet ISE, vous pouvez cliquer sur le lien **Integrate ISE** (intégrer ISE) et le créer maintenant. Si l'objet existe, il est répertorié avec son état : Enabled (activé) ou Disabled (désactivé).

Vous devez avoir configuré au moins une source d'identité passive pour créer des règles d'authentification passive.

Étape 4 Configurez les options **d'authentification active**.

Lorsqu'une règle d'identité requiert une authentification active pour un utilisateur, l'utilisateur est redirigé vers le port portail captif, puis il est invité à s'authentifier. Avant de configurer ces paramètres, lisez Bonnes pratiques pour Active Authentication (Authentification active), à la page 4.

- **Server Certificate** (certificat de serveur) : Sélectionnez le certificat interne à présenter aux utilisateurs lors de l'authentification active. Si vous n'avez pas encore créé le certificat requis, cliquez sur **Create New Internal Certificate** (créer un nouveau certificat interne) dans la partie inférieure de la liste déroulante.

  Les utilisateurs devront accepter le certificat si vous ne téléchargez pas un certificat déjà réputé fiable pour leurs navigateurs.

- **Redirect to Host Name** (rediriger vers le nom d'hôte) : sélectionnez l'objet réseau qui définit le nom d'hôte pleinement qualifié de l'interface devant être utilisée comme portail captif pour les demandes d'authentification active. Cliquez sur **Create New Network** (créer un nouveau réseau) si l'objet n'existe pas.

  Le nom de domaine complet doit mener à l'adresse IP de l'une des interfaces du périphérique. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP. Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat.

  Si une règle d'identité requiert une authentification active pour un utilisateur, mais que vous ne précisez pas de nom de domaine complet de redirection, l'utilisateur sera redirigé vers le port du portail captif de l'interface de connexion.

- **Port** : le port du portail captif. La valeur par défaut est 885 (TCP). Si vous configurez un autre port, il doit être compris entre 1025 et 65535.

  Remarque
  Si vous ne pouvez pas fournir un nom de domaine complet **Redirect to Host Name** (Redirection vers le nom d'hôte), les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM redirigent l'utilisateur vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.AD-domain-name*. Si vous souhaitez utiliser la négociation HTTP sans nom de domaine complet de redirection vers l'hôte (**Redirect to Host Name**), vous devez également mettre à jour votre serveur DNS pour mapper ce nom avec les adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier. Nous vous recommandons de toujours fournir un nom de domaine complet de redirection vers le nom d'hôte (**Redirect to Host Name**) pour assurer un comportement cohérent, quelle que soit la méthode d'authentification.

Étape 5 (Authentification active seulement) Dans **Decrypt Re-Sign Certificate** (Déchiffrer le certificat re-signé), sélectionnez le certificat d'autorité de certification interne à utiliser pour les règles mettant en œuvre le déchiffrement avec des certificats re-signés.

Vous pouvez utiliser le certificat NGFW-Default-InternalCA prédéfini ou celui que vous avez créé ou téléversé. Si le certificat n'existe pas encore, cliquez sur **Create Internal CA** (créer une autorité de certification interne) pour le créer.

Si vous n'avez pas encore installé le certificat dans les navigateurs clients, cliquez sur le bouton de téléchargement () pour en obtenir une copie. Consultez la documentation de chaque navigateur afin de savoir comment installer le certificat. Voir aussi Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature.

Remarque
Vous êtes invité à saisir les paramètres de déchiffrement SSL uniquement si vous n'avez pas encore configuré la politique de déchiffrement SSL. Pour modifier ces paramètres après avoir activé la politique d'identité, modifiez les paramètres de politique de déchiffrement SSL.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer l'action par défaut de la politique d'identité

La politique d'identité a une action par défaut, qui est mise en œuvre pour les connexions qui ne correspondent à aucune règle d'identité individuelle.

En fait, l'absence de règle est une configuration valide pour votre politique. Si vous avez l'intention d'utiliser l'authentification passive sur toutes les sources de trafic, configurez simplement l'authentification passive comme action par défaut.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Étape 2 Cliquez dans **Default Action** (Action par défaut) et choisissez l'une des options suivantes :

- **Passive Auth** (Any Identity Source) (toute source d'identité) : l'identité de l'utilisateur est déterminée à l'aide de toutes les sources d'identité passive configurées pour les connexions qui ne correspondent à aucune règle d'identité. Si vous ne configurez aucune source d'identité passive, l'utilisation de Passive Auth comme action par défaut équivaut à l'utilisation de No Auth.
- **No Auth** (No Authentication Required) : l'identité de l'utilisateur n'est pas déterminée pour les connexions qui ne correspondent à aucune règle d'identité.

Configurer les règles d'identité

Les règles d'identité déterminent si les informations d'identité d'utilisateur doivent être recueillies pour le trafic correspondant. Vous pouvez configurer No Authentication (aucune authentification) si vous ne souhaitez pas obtenir les informations d'identité de l'utilisateur pour le trafic correspondant.

N'oubliez pas que quelle que soit la configuration de votre règle, l'authentification active est effectuée uniquement sur le trafic HTTP. Ainsi, vous n'avez pas besoin de créer des règles pour exclure de

l'authentification active le trafic ne relevant pas de HTTP. Vous pouvez simplement appliquer une règle d'authentification active à toutes les sources et destinations si vous souhaitez obtenir des informations d'identité utilisateur pour tout le trafic HTTP.

Remarque Gardez également à l'esprit qu'un échec de l'authentification n'a aucune incidence sur l'accès au réseau. Les politiques d'identité recueillent uniquement les informations d'identité de l'utilisateur. Vous devez utiliser des règles d'accès si vous souhaitez empêcher les utilisateurs qui n'ont pas pu s'authentifier d'accéder au réseau.

Avant de commencer

Les règles sont évaluées de haut en bas. Pour une connexion qui correspond aux critères de réseau spécifiés d'une règle donnée, l'utilisateur est évalué par rapport au domaine d'identité spécifié dans la règle. Si l'utilisateur ne fait pas partie de ce domaine, il sera marqué comme inconnu et aucune autre règle de la politique d'identité ne sera évaluée. Par conséquent, si vous avez plusieurs domaines qui doivent être évalués, assurez-vous d'utiliser des séquences de domaines au lieu d'un seul domaine.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle.

Étape 3 Sous **Order**, sélectionnez l'endroit où vous souhaitez insérer la règle dans la liste ordonnée des règles.

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant.

La valeur par défaut consiste à ajouter la règle à la fin de la liste. Si vous souhaitez modifier l'emplacement d'une règle ultérieurement, modifiez cette option.

Étape 4 Dans **Title** (titre), entrez un nom pour la règle.

Étape 5 Sélectionnez **Action** et, si nécessaire, la source d'identité AD (**AD Identity Source**)..

Vous devez sélectionner le domaine d'identité AD qui comprend les comptes d'utilisateur pour les règles d'authentification passive et active. Si le domaine n'existe pas encore, cliquez sur **Create New Identity Realm** (créer un nouveau domaine d'identité) pour le créer maintenant. Pour l'authentification passive, vous pouvez sélectionner une séquence de domaine AD plutôt qu'un seul objet de domaine AD.

- **Passive Auth** : Utilisez l'authentification passive pour déterminer l'identité de l'utilisateur. Toutes les sources d'identité configurées sont affichées. La règle utilise automatiquement toutes les sources configurées.

- **Active Auth** : Utilisez l'authentification active pour déterminer l'identité de l'utilisateur. L'authentification active est appliquée uniquement au trafic HTTP de . Si un autre type de trafic correspond à une politique d'identité nécessitant ou autorisant une authentification active, l'authentification active ne sera pas tentée.
- **No Auth** : N'obtient pas d'information sur l'identité de l'utilisateur. Les règles d'accès basées sur l'identité ne seront pas appliquées à ce trafic. Ces utilisateurs sont marqués comme **No Authentication Required** (aucune authentification requise).

Étape 6 (Authentification active seulement) Sélectionnez la méthode d'authentification (**Type**) prise en charge par votre serveur d'annuaire.

- **HTTP de base** : Authentifiez les utilisateurs qui utilisent une connexion d'authentification de base HTTP non chiffrée. Les utilisateurs se connectent au réseau en utilisant la fenêtre contextuelle d'authentification par défaut de leur navigateur. Il s'agit du paramètre par défaut.
- **NTLM** : Authentifiez les utilisateurs qui utilisent une connexion NT LAN Manager (NTLM). Cette sélection est uniquement disponible lorsque vous sélectionnez un domaine AD. Les utilisateurs se connectent au réseau à l'aide de la fenêtre contextuelle d'authentification par défaut de leur navigateur. Vous pouvez aussi configurer les navigateurs IE et Firefox pour l'authentification transparente à l'aide du nom de domaine Windows (voir Activation de l'authentification transparente de l'utilisateur, à la page 12).
- **Négociation HTTP** : Permet au périphérique de négocier la méthode entre l'agent utilisateur (l'application utilisée par l'utilisateur pour lancer le flux de trafic) et le serveur Active Directory. La négociation donne lieu à l'utilisation de la méthode la plus efficace communément prise en charge, dans l'ordre suivant : NTLM, puis la méthode de base. Les utilisateurs se connectent au réseau en utilisant la fenêtre contextuelle d'authentification par défaut de leur navigateur.
- **Page de réponse HTTP** : Invite les utilisateurs à s'authentifier à l'aide d'une page Web fournie par le système. Il s'agit d'une forme d'authentification HTTP de base.

Remarque
Si vous ne pouvez pas fournir un nom de domaine complet **Redirect to Host Name** (Redirection vers le nom d'hôte), les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM redirigent l'utilisateur vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.AD-domain-name*. Si vous souhaitez utiliser la négociation HTTP sans nom de domaine complet de redirection vers l'hôte (**Redirect to Host Name**), vous devez également mettre à jour votre serveur DNS pour mapper ce nom avec les adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier. Nous vous recommandons de toujours fournir un nom de domaine complet de redirection vers le nom d'hôte (**Redirect to Host Name**) pour assurer un comportement cohérent, quelle que soit la méthode d'authentification.

Étape 7 (Authentification active seulement) Sélectionnez **Fall Back as Guest** > **On/Off** (activer/désactiver le mode Invité) pour déterminer si les utilisateurs qui échouent à l'authentification active sont étiquetés comme des utilisateurs invités.

Les utilisateurs ont trois chances de s'authentifier. Si elles échouent, votre sélection pour cette option détermine la façon dont l'utilisateur est marqué. Vous pouvez écrire des règles d'accès en fonction de ces valeurs.

- **Fall Back as Guest (basculement au mode d'invité)** > **On (activé)** Les utilisateurs sont marqués en tant qu'invité (**Guest**).
- **Fall Back as Guest (basculement au mode d'invité)** > **Off (désactivé)** Les utilisateurs sont marqués en tant qu'authentification échouée (**Failed Authentication**).

Étape 8 Définissez les critères de correspondance du trafic sous l'onglet **Source/Destination**.

N'oubliez pas que l'authentification active sera tentée uniquement avec le trafic HTTP. Par conséquent, il n'est pas nécessaire de configurer des règles entraînant la non-authentification pour le trafic en dehors du HTTP, et il est inutile de créer des règles d'authentification active pour tout trafic en dehors du HTTP. Cependant, l'authentification passive est valide pour tout type de trafic.

Les critères Source/Destination d'une règle d'identité définissent les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) pour l'adresse IP, ou les protocoles et les ports utilisés dans le trafic. La valeur par défaut englobe toute zone ou adresse et tout emplacement géographique, protocole et port.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Vous pouvez configurer les critères de correspondance de trafic suivants.

Zones source, zones de destination

Les objets de la zone de sécurité qui définissent les interfaces par lesquelles passe le trafic. Vous pouvez définir un critère, les deux critères ou aucun critère : tout critère non spécifié s'applique au trafic sur n'importe quelle interface.

- Pour faire correspondre le trafic sortant de l'appareil depuis une interface dans la zone, ajoutez cette zone aux **zones de destination**.
- Pour faire correspondre le trafic entrant dans l'appareil depuis une interface dans la zone, ajoutez cette zone aux zones source (**Source Zones**).
- Si vous ajoutez des conditions de zone source et de zone de destination à une règle, le trafic correspondant doit provenir de l'une des zones source spécifiées et sortir par l'une des zones de destination.

Utilisez ces critères lorsque la règle doit être appliquée en fonction de l'entrée ou de la sortie du trafic sur l'appareil. Par exemple, si vous voulez vous assurer que l'information sur l'identité de l'utilisateur soit collectée à partir de tout le trafic provenant des réseaux internes, sélectionnez une zone interne comme zones source (**Source Zones**) tout en laissant la zone de destination vide.

Remarque
Vous ne pouvez pas combiner des zones de sécurité passives et routées dans une seule règle. En outre, vous pouvez spécifier des zones de sécurité passives comme zones source uniquement, vous ne pouvez pas les spécifier comme zones de destination.

Réseaux sources, réseaux de destination

Les objets réseau ou les emplacements géographiques qui définissent les adresses réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic d'une adresse IP ou d'un emplacement géographique, configurez les réseaux sources (**Source Networks**).
- Pour faire correspondre le trafic à une adresse IP ou à un emplacement géographique, configurez les réseaux de destination (**Source Networks**).
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler.
- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

  Remarque
  Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Ports source, ports/protocoles de destination

Les objets de port qui définissent les protocoles utilisés dans le trafic. Pour TCP/UDP, cela peut inclure les ports.

- Pour faire correspondre le trafic d'un protocole ou d'un port, configurez les ports source (**Source Ports**). Les ports source peuvent uniquement être TCP/UDP.
- Pour faire correspondre le trafic à un protocole ou à un port, configurez les protocoles/ports de destination (**Destination Ports/Protocols**).
- Pour faire correspondre le trafic provenant de ports TCP/UDP spécifiques et destiné à des ports TCP/UDP spécifiques, configurez les deux. Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP. Par exemple, vous pouvez cibler le trafic du port TCP/80 au port TCP/8080.

Étape 9 Cliquez sur **OK**.

Activation de l'authentification transparente de l'utilisateur

Si vous configurez la politique d'identité pour permettre l'authentification active, vous pouvez utiliser les méthodes d'authentification suivantes pour obtenir l'identité de l'utilisateur :

HTTP de base

Avec l'authentification de base HTTP, les utilisateurs sont toujours invités à s'authentifier avec leur nom d'utilisateur et leur mot de passe de répertoire. Le mot de passe est transmis en texte clair. Pour cette raison, l'authentification de base n'est pas considérée comme une forme d'authentification sécurisée.

L'authentification de base est le mécanisme d'authentification par défaut.

Page de réponse HTTP

C'est un type d'authentification HTTP de base, suivant lequel l'utilisateur se voit présenter une page de navigateur de connexion.

NTLM, HTTP Negotiate (authentification Windows intégrée pour Active Directory)

Grâce à l'authentification Windows intégrée, vous profitez du fait que les utilisateurs se connectent à un domaine pour utiliser leur poste de travail. Le navigateur tente d'utiliser cette connexion de domaine lors

de l'accès à un serveur, y compris au portail captif de Cisco Firewall Threat Defense lors de l'authentification active. Le mot de passe n'est pas transmis. Si l'authentification réussit, l'utilisateur est authentifié de manière transparente; l'utilisateur n'est au courant d'aucun défi d'authentification.

Si le navigateur ne peut pas répondre à une demande d'authentification à l'aide des identifiants de connexion au domaine, l'utilisateur est invité à entrer son nom d'utilisateur et son mot de passe, ce qui correspond à l'expérience utilisateur de l'authentification de base. Ainsi, si vous configurez l'authentification Windows intégrée, cela peut réduire le besoin pour les utilisateurs de fournir des identifiants lors de l'accès au réseau ou aux serveurs dans le même domaine.

Il convient de signaler que HTTP Negotiate choisit la méthode la plus efficace prise en charge par le serveur Active Directory et l'agent utilisateur. Si la négociation sélectionne HTTP de base comme méthode d'authentification, vous n'obtiendrez pas une authentification transparente. L'ordre de priorité va comme suit : NTLM, puis authentification de base. La négociation doit sélectionner NTLM pour que l'authentification transparente soit possible.

Vous devez configurer les navigateurs clients pour prendre en charge l'authentification Windows intégrée afin de permettre une authentification transparente. Les sections suivantes expliquent les exigences générales et la configuration de base de l'authentification Windows intégrée pour certains navigateurs couramment utilisés qui la prennent en charge. Les utilisateurs doivent consulter les rubriques d'aide de leur navigateur (ou d'un autre agent utilisateur) pour obtenir des renseignements plus détaillés, car les techniques peuvent changer selon les versions de logiciels.

Astuces Tous les navigateurs ne prennent pas en charge l'authentification Windows intégrée, par exemple, Chrome et Safari (selon les versions disponibles au moment de la rédaction). Un nom d'utilisateur et un mot de passe seront demandés aux utilisateurs. Consultez la documentation du navigateur pour déterminer si une assistance est disponible dans la version que vous utilisez.

Exigences pour l'authentification transparente

Les utilisateurs doivent configurer leur navigateur ou leur agent utilisateur pour mettre en œuvre l'authentification transparente. Ils peuvent le faire individuellement ou vous pouvez le configurer pour eux et envoyer la configuration aux postes de travail clients à l'aide de vos outils de distribution de logiciels. Si vous décidez de laisser les utilisateurs le faire eux-mêmes, veillez à fournir les paramètres de configuration spécifiques qui fonctionnent pour votre réseau.

Quels que soient le navigateur ou l'agent utilisateur, vous devez mettre en œuvre la configuration générale suivante :

- Ajoutez le nom d'hôte de redirection Cisco Firewall Threat Defense, ou l'interface par laquelle les utilisateurs se connectent au réseau, à la liste des sites de confiance. Si vous n'utilisez pas de nom d'hôte de redirection, vous pouvez utiliser l'adresse IP ou, le cas échéant, le nom de domaine complet (par exemple : interne.exemple.com). Vous pouvez également utiliser des caractères génériques ou des adresses partielles pour créer un site de confiance généralisé. Par exemple, vous pouvez généralement couvrir tous les sites internes en utilisant *.example.com ou simplement exemple.com, en faisant confiance à tous les serveurs de votre réseau (utilisez votre propre nom de domaine). Si vous ajoutez l'adresse spécifique de l'interface, vous devrez peut-être ajouter plusieurs adresses aux sites de confiance pour prendre en compte tous les points d'accès des utilisateurs au réseau.
- L'authentification Windows intégrée ne fonctionne pas par l'intermédiaire d'un serveur mandataire. Par conséquent, vous devez soit ne pas utiliser de serveur mandataire, soit ajouter le nom d'hôte ou l'interface

de redirection Cisco Firewall Threat Defenseaux adresses exclues du passage par le serveur mandataire. Si vous décidez que vous devez utiliser un serveur mandataire, les utilisateurs seront invités à s'authentifier même si vous utilisez NTLM.

Astuces La configuration de l'authentification transparente n'est pas une exigence, mais une commodité pour les utilisateurs finaux. Si vous ne configurez pas l'authentification transparente, les utilisateurs reçoivent un défi de connexion pour toutes les méthodes d'authentification.

Configuration d'Internet Explorer pour l'authentification transparente

Pour configurer Internet Explorer pour l'authentification transparente NTLM :

Procédure

Étape 1 Sélectionnez **Tools (Outils) > Internet Options (Options Internet)**.

Étape 2 Sélectionnez l'onglet **Security** (Sécurité), sélectionnez la zone **Local Intranet** (Intranet local), puis procédez comme suit :

a) Cliquez sur le bouton **Sites** pour ouvrir la liste des sites de confiance.

b) Assurez-vous qu'au moins une des options suivantes est sélectionnée :

- **Automatically detect intranet network** (Détecter automatiquement le réseau intranet). Si vous sélectionnez cette option, toutes les autres options sont désactivées.
- **Include all sites that bypass the proxy** (Inclure tous les sites qui contournent le serveur mandataire).

c) Cliquez sur **Advanced (Avancé)** pour ouvrir la boîte de dialogue Sites intranet locaux, puis collez l'URL à approuver dans la zone **Add Site (Ajouter un site)** et cliquez sur **Add (Ajouter)**.

Répétez le processus si vous avez plusieurs URL. Utilisez des caractères génériques pour spécifier une URL partielle, comme `http://*.exemple.com` ou simplement `*.exemple.com`.

Fermez les boîtes de dialogue pour revenir à la boîte de dialogue des options Internet.

d) Avec **Local Intranet** (Intranet local) toujours sélectionné, cliquez sur **Custom Level** (Niveau personnalisé) pour ouvrir la boîte de dialogue Security Settings (Paramètres de sécurité). Recherchez le paramètre **User Authentication (Authentification utilisateur)** > **Logon (Connexion)** et sélectionnez **Automatic logon only in Intranet zone** (Connexion automatique uniquement dans la zone Intranet). Cliquez sur **OK**.

Étape 3 Dans la boîte de dialogue Internet Options, cliquez sur l'onglet **Connections** (Connexions), puis sur **LAN Settings** (Paramètres réseau local).

Si **Use a proxy server for your LAN** (Utiliser un serveur mandataire pour votre réseau local) est sélectionné, vous devez vous assurer que l'interface Cisco Firewall Threat Defense contourne le proxy. Effectuez l'une des actions suivantes, le cas échéant :

- Sélectionnez **Bypass proxy server for local addresses (Contourner le serveur proxy pour les adresses locales)**.

- Cliquez sur **Advanced** (Avancé) et saisissez l'adresse dans la zone **Do not use proxy server for addresses beginning with** (Ne pas utiliser de serveur proxy pour les adresses commençant par). Vous pouvez utiliser des caractères génériques, par exemple, **`*.exemple.com`**.

Configuration de Firefox pour l'authentification transparente

Configurer Firefox pour l'authentification transparente NTLM :

Procédure

Étape 1 Ouvrez **about:config**. Utilisez la barre de filtres pour vous aider à localiser les préférences que vous devez modifier.

Étape 2 Pour prendre en charge NTLM, modifiez les préférences suivantes (filtre sur network.automatic) :

- **network.automatic-ntlm-auth.trusted-uris** : double-cliquez sur la préférence, saisissez l'URL et cliquez sur **OK**. Vous pouvez saisir plusieurs URL en les séparant par des virgules ; le protocole peut être omis. Par exemple :

  ```
  http://host.example.com, http://hostname, myhost.example.com
  ```

  Vous pouvez également utiliser des URL partielles. Firefox correspond à la fin de la chaîne, et non à une sous-chaîne aléatoire. Ainsi, vous pouvez inclure l'ensemble de votre réseau interne en précisant uniquement votre nom de domaine. Par exemple :

  ```
  example.com
  ```

- **network.automatic-ntlm-auth.allow-proxies** : vérifiez que la valeur est **true**, qui est la valeur par défaut. Double-cliquez pour modifier la valeur si elle est actuellement false.

Étape 3 Vérifiez les paramètres du serveur mandataire HTTP. Vous pouvez les trouver en sélectionnant **Tools (Outils)** > **Options**, puis en cliquant sur l'onglet **Network** (Réseau) dans la boîte de dialogue des options. Cliquez sur le bouton **Settings** (paramètres) dans le groupe Connection (connexion).

- Si **No Proxy** (Aucun mandataire) est sélectionné, il n'y a rien à configurer.
- Si **Use System Proxy Settings** (Utiliser les paramètres de mandataire du système) est sélectionné, vous devez modifier la propriété **network.proxy.no_proxies_on** dans about:config pour ajouter les URI de confiance que vous avez inclus dans **network.automatic-ntlm-auth.trusted-uris**.
- Si **Manual Proxy Configuration** (Configuration manuelle du serveur mandataire) est sélectionnée, mettez à jour la liste **No Proxy For** (Aucun mandataire pour) pour inclure ces URI de confiance.
- Si l'une des autres options est sélectionnée, assurez-vous que les propriétés utilisées pour ces configurations excluent les mêmes URI de confiance.

Politiques d'identité de surveillance

Si les politiques d'identité qui nécessitent l'authentification fonctionnent correctement, vous devriez voir les informations sur les utilisateurs dans le tableau de bord **Monitoring (Surveillance)** > **Users (Utilisateurs)** ainsi que dans d'autres tableaux de bord qui incluent des informations utilisateur.

En outre, les événements affichés dans **Monitoring (Surveillance)** > **Events (Événements)** devraient inclure des informations utilisateur.

Si vous ne voyez aucune information d'utilisateur, vérifiez que le serveur de répertoire fonctionne correctement. Utilisez le bouton **Test** (Tester) dans la boîte de dialogue de configuration du serveur de répertoire pour vérifier la connectivité.

Si le serveur de répertoire fonctionne et est utilisable, vérifiez que les critères de correspondance du trafic dans les règles d'identité qui nécessitent une authentification active sont rédigés de manière à correspondre à vos utilisateurs. Par exemple, assurez-vous que la zone source contient les interfaces par lesquelles le trafic utilisateur entrera dans le périphérique. Les règles d'identité d'authentification active ne correspondent qu'au trafic HTTP; les utilisateurs doivent donc envoyer ce type de trafic par l'intermédiaire du périphérique.

Pour l'authentification passive, utilisez le bouton **Test** (Tester) dans l'objet ISE si vous utilisez cette source. Si vous utilisez le VPN d'accès à distance, vérifiez que le service fonctionne correctement et que les utilisateurs peuvent établir des connexions VPN. Consultez les rubriques de dépannage de ces fonctionnalités pour obtenir des renseignements plus détaillés sur l'identification et la résolution des problèmes.

Exemples de politiques d'identité

Le chapitre sur les cas d'utilisation comprend un exemple de mise en œuvre des politiques d'identité. Veuillez consulter Comment mieux comprendre le trafic de votre réseau.

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.