Déchiffrement SSL

Certains protocoles, comme HTTPS, utilisent Secure Sockets Layer (SSL) ou son successeur, Transport Layer Security (TLS), pour chiffrer le trafic en vue d'une transmission sécurisée. Comme le système ne peut pas inspecter les connexions chiffrées, vous devez les déchiffrer si vous souhaitez appliquer des règles d'accès qui tiennent compte des caractéristiques de trafic de couche supérieure pour prendre des décisions en matière d'accès.

À propos du déchiffrement SSL

Normalement, les connexions passent par la politique de contrôle d'accès pour déterminer si elles sont autorisées ou bloquées. Toutefois, si vous activez la politique de déchiffrement SSL, les connexions chiffrées sont d'abord envoyées par l'intermédiaire de la politique de déchiffrement SSL pour déterminer si elles doivent être déchiffrées ou bloquées. Toute connexion qui n'a pas été bloquée, qu'elle soit déchiffrée ou non, est ensuite soumise à la politique de contrôle d'accès pour une décision finale d'autorisation ou de blocage.

Remarque Vous devez activer la politique de déchiffrement SSL pour mettre en œuvre les règles d'authentification active dans la politique d'identité. Si vous activez le déchiffrement SSL pour activer les politiques d'identité, mais que vous ne souhaitez pas autrement mettre en œuvre le déchiffrement SSL, sélectionnez Do Not Decrypt (Ne pas déchiffrer) pour l'action par défaut et ne créez pas de règles de déchiffrement SSL supplémentaires. La politique d'identité génère automatiquement les règles dont elle a besoin.

Les rubriques suivantes expliquent plus en détail la gestion et le déchiffrement du flux de trafic chiffré.

Pourquoi mettre en œuvre le déchiffrement SSL?

Le trafic chiffré, comme les connexions HTTPS, ne peut pas être inspecté.

De nombreuses connexions sont légitimement chiffrées, notamment les connexions aux banques et à d'autres établissements financiers. De nombreux sites Web utilisent le chiffrement pour protéger la confidentialité ou les données sensibles. Par exemple, votre connexion au Firepower Device Manager est chiffrée.

Cependant, les utilisateurs peuvent également masquer le trafic indésirable dans les connexions chiffrées.

En mettant en œuvre le déchiffrement SSL, vous pouvez déchiffrer les connexions, les inspecter pour vérifier qu'elles ne contiennent pas de menaces ou d'autre trafic indésirable, puis les chiffrer à nouveau avant de poursuivre la connexion. (Le trafic déchiffré passe par votre politique de contrôle d'accès et correspond aux règles en fonction des caractéristiques inspectées de la connexion déchiffrée, et non des caractéristiques chiffrées.) Cela équilibre votre besoin d'appliquer des politiques de contrôle d'accès avec le besoin de l'utilisateur de protéger les informations sensibles.

Vous pouvez également configurer des règles de déchiffrement SSL pour bloquer le trafic chiffré des types que vous savez ne pas vouloir sur votre réseau.

Gardez à l'esprit que le déchiffrement puis le rechiffrement du trafic ajoute une charge de traitement sur le périphérique, ce qui réduira les performances globales du système.

Actions que vous pouvez appliquer au trafic chiffré

Lors de la configuration des règles de déchiffrement SSL, vous pouvez appliquer les actions décrites dans les rubriques suivantes. Ces actions sont également disponibles pour l'action par défaut, qui s'applique à tout trafic qui ne correspond pas à une règle explicite.

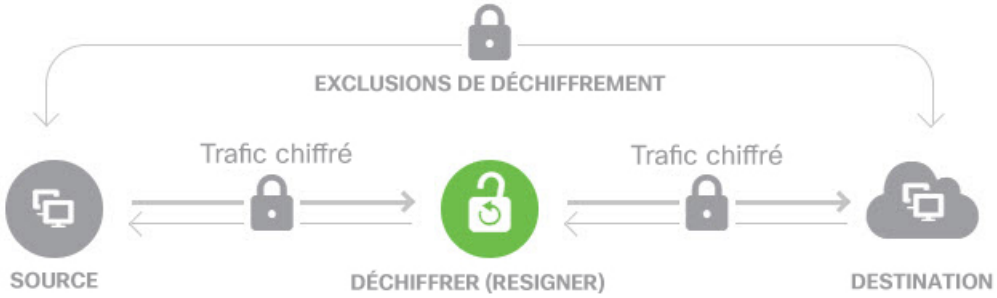
Remarque Tout trafic qui passe par la politique de déchiffrement SSL doit ensuite passer par la stratégie de contrôle d'accès. À l'exception du trafic que vous abandonnez dans la politique de déchiffrement SSL, la décision finale d'autorisation ou d'abandon dépend de la stratégie de contrôle d'accès.

Déchiffrer - Resigner

Si vous choisissez de déchiffrer et de signer le trafic de nouveau, le système agit comme un intermédiaire.

Par exemple, l'utilisateur saisit https://www.cisco.com dans un navigateur. Le trafic atteint le périphérique Cisco Firewall Threat Defense, le périphérique négocie ensuite avec l'utilisateur à l'aide du certificat d'autorité de certification spécifié dans la règle et crée un tunnel SSL entre l'utilisateur et le périphérique Cisco Firewall Threat Defense. En même temps, le périphérique se connecte à https://www.cisco.com et crée un tunnel SSL entre le serveur et le périphérique Cisco Firewall Threat Defense.

Ainsi, le client voit le certificat de l'autorité de certification configuré pour la règle de déchiffrement SSL au lieu du certificat de www.cisco.com. Le client doit faire confiance au certificat pour terminer la connexion. Le périphérique Cisco Firewall Threat Defense effectue ensuite le déchiffrement/rechiffrement dans les deux sens du trafic entre le client et le serveur de destination.



Remarque Si le client ne fait pas confiance à l'autorité de certification (CA) utilisée pour signer de nouveau le certificat du serveur, il avertit l'utilisateur que le certificat ne doit pas être approuvé. Pour éviter cela, importez le certificat d'autorité de certification dans le magasin d'autorités de certification de confiance du client. Sinon, si votre entreprise dispose d'une PKI privée, vous pouvez émettre un certificat d'autorité de certification intermédiaire signé par l'autorité de certification racine et qui est automatiquement approuvé par tous les clients de l'organisation, puis téléverser ce certificat d'autorité de certification sur le périphérique.

Si vous configurez une règle avec l'action Decrypt Re-Sign (Déchiffrer et resigner), la règle correspond au trafic en fonction du type d'algorithme de signature du certificat interne de l'autorité de certification référencé, en plus des conditions de la règle configurée. Comme vous pouvez sélectionner un seul certificat de resignature pour la politique de déchiffrement SSL, cela peut limiter le trafic correspondant pour les règles de resignature.

Par exemple, le trafic sortant chiffré à l'aide d'un algorithme de courbe elliptique (EC) correspond à une règle Déchiffrer - Resigner uniquement si le certificat de resignature est un certificat d'autorité de certification basé sur EC. De même, une règle Decrypt Re-Sign (Déchiffrer et resigner) qui fait référence à un certificat d'autorité de certification basé sur RSA correspond uniquement au trafic sortant chiffré avec un algorithme RSA; le trafic sortant chiffré avec un algorithme EC ne correspond pas à la règle, même si toutes les autres conditions de règle configurées correspondent.

Déchiffrer à l'aide d'une clé connue

Si vous êtes propriétaire du serveur de destination, vous pouvez mettre en œuvre le déchiffrement avec une clé connue. Dans ce cas, lorsque l'utilisateur ouvre une connexion à https://www.cisco.com, l'utilisateur voit le certificat réel pour www.cisco.com, même si c'est le périphérique Cisco Firewall Threat Defense qui présente le certificat.

Votre entreprise doit être le propriétaire du domaine et du certificat. Pour l'exemple de cisco.com, la seule façon possible de faire en sorte que l'utilisateur final voie le certificat de Cisco serait si vous êtes propriétaire du domaine cisco.com (c'est-à-dire que vous êtes Cisco Systems) et que vous êtes propriétaire du certificat cisco.com signé par une autorité de certification publique (CA). Vous ne pouvez déchiffrer qu'avec des clés connues pour les sites appartenant à votre organisation.

L'objectif principal du déchiffrement avec une clé connue est de déchiffrer le trafic dirigé vers votre serveur HTTPS pour protéger vos serveurs contre les attaques externes. Pour inspecter le trafic côté client vers des

sites HTTPS externes, vous devez utiliser la re-signature du déchiffrement, car vous n'êtes pas propriétaire des serveurs.

Remarque Pour utiliser le déchiffrement par clé connue, vous devez charger le certificat et la clé du serveur en tant que certificat d'identité interne, puis l'ajouter à la liste des certificats de clé connue dans les paramètres de la politique de déchiffrement SSL. Vous pouvez ensuite écrire la règle de déchiffrement par clé connue en utilisant l'adresse du serveur comme adresse de destination. Pour en savoir plus sur l'ajout du certificat à la politique de déchiffrement SSL, consultez Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 19.

Ne pas déchiffrer

Si vous choisissez de contourner le déchiffrement pour certains types de trafic, aucun traitement n'est effectué sur le trafic. Le trafic chiffré est dirigé vers la stratégie de contrôle d'accès, où il est autorisé ou abandonné en fonction de la règle de contrôle d'accès à laquelle il correspond.

Bloquer

Vous pouvez simplement bloquer le trafic chiffré qui correspond à une règle de déchiffrement SSL. Le blocage dans la politique de déchiffrement SSL empêche la connexion d'atteindre la politique de contrôle d'accès.

Lorsque vous bloquez une connexion HTTPS, l'utilisateur ne voit pas la page de réponse de blocage par défaut du système. Au lieu de cela, l'utilisateur voit la page par défaut du navigateur pour un échec de connexion sécurisée. Le message d'erreur n'indique pas que le site a été bloqué en raison de la politique. Au lieu de cela, des erreurs peuvent indiquer qu'il n'y a pas d'algorithmes de chiffrement communs. Ce message n'indique pas clairement que la connexion a été bloquée intentionnellement.

Règles de déchiffrement SSL générées automatiquement

Que vous activiez ou non la politique de déchiffrement SSL, le système génère automatiquement des règles de re-signature de déchiffrement pour chaque règle de politique d'identité qui met en œuvre l'authentification active. Cela est nécessaire pour activer l'authentification active pour les connexions HTTPS.

Lorsque vous activez la politique de déchiffrement SSL, ces règles s'affichent sous l'en-tête Règles d'authentification actives de la politique d'identité. Ces règles sont regroupées en haut de la politique de déchiffrement SSL. Les règles sont en lecture seule. Vous pouvez les modifier uniquement en modifiant votre politique d'identité.

Gestion du trafic non déchiffrable

Plusieurs caractéristiques rendent une connexion indéchiffrable. Si une connexion possède l'une des caractéristiques suivantes, l'action par défaut est appliquée à la connexion, quelle que soit la règle à laquelle la connexion correspondrait. Si vous sélectionnez Bloquer comme action par défaut (plutôt que Ne pas déchiffrer), vous pourriez rencontrer des problèmes, notamment des pertes excessives de trafic légitime. Vous pouvez modifier le comportement par défaut, comme expliqué dans Configurer les paramètres de trafic avancé et non déchiffrable, à la page 21.

- Session compressée : une compression de données a été appliquée à la connexion.
- Session SSLv2 : la version minimale de SSL prise en charge est SSLv3.

- Unknown cipher suite (suite de chiffrement inconnu) : le système ne reconnaît pas la suite de chiffrement pour la connexion.
- Unsupported cipher suite : le système ne prend pas en charge le déchiffrement selon la suite de chiffrement détectée.
- Session not cached (session non mise en cache) : la session SSL a la réutilisation de session activée, le client et le serveur ont rétabli la session avec l'identifiant de session et le système n'a pas mis en cache cet identifiant de session.
- Handshake errors (Erreurs d'établissement de liaison) : une erreur s'est produite lors de la négociation d'établissement de liaison SSL.
- Decryption error (erreurs de déchiffrement) : une erreur s'est produite lors de l'opération de déchiffrement.
- Passive interface traffic (trafic d'interface passive) : tout le trafic sur les interfaces passives (zones de sécurité passives) est non déchiffrable.

Exigences de licence pour le déchiffrement SSL

Vous n'avez pas besoin de licence particulière pour utiliser la politique de déchiffrement SSL.

Cependant, vous avez besoin de la licence **URL** pour créer des règles qui utilisent les catégories et la réputation d'URL comme critères de correspondance. Pour en savoir plus sur la configuration des licences, consultez Activation ou désactivation des licences facultatives.

Directives pour l'utilisation du déchiffrement

Gardez les éléments suivants à l'esprit lors de la configuration et de la surveillance des politiques de déchiffrement SSL :

- La politique de déchiffrement SSL est contournée pour toutes les connexions qui correspondent aux règles de contrôle d'accès avec des actions Trust (Confiance), Block (Blocage) ou Block with reset (Blocage avec réinitialisation) si ces règles :
  - Utilisez la zone de sécurité, le réseau, la géolocalisation et le port uniquement comme critères de correspondance de trafic.
  - précède d'autres règles qui nécessitent une inspection, telles que les règles qui font correspondre les connexions en fonction de l'application ou de l'URL, ou les règles d'autorisation qui appliquent l'inspection des intrusions ou des fichiers.
- Lors de l'utilisation de la mise en correspondance de catégorie d'URL, notez qu'il existe des cas où la page de connexion d'un site se trouve dans une catégorie différente de celle du site lui-même. Par exemple, Gmail se trouve dans la catégorie « Courriels sur le Web », alors que la page de connexion se trouve dans la catégorie « Portails Internet ». Pour faire déchiffrer les connexions à ces sites, vous devez inclure les deux catégories dans la règle.
- Si une mise à jour de la base de données des vulnérabilités (VDB) supprime (abandonne) les applications, vous devez apporter des modifications aux règles de déchiffrement SSL ou aux filtres d'application qui utilisent l'application supprimée. Vous ne pouvez pas déployer les modifications avant d'avoir corrigé ces règles. En outre, vous ne pouvez pas installer les mises à jour du logiciel système avant de résoudre

le problème. Dans la page d'objet des filtres d'application ou dans l'onglet Application de la règle, ces applications indiquent « (Deprecated) » (Obsolète) après le nom de l'application.

- Vous ne pouvez pas désactiver la politique de déchiffrement SSL si vous avez des règles d'authentification actives. Pour désactiver la politique de déchiffrement SSL, vous devez soit désactiver la politique d'identité, soit supprimer toutes les règles d'identité qui utilisent l'authentification active.

Comment mettre en œuvre et maintenir la politique de déchiffrement SSL

Vous pouvez utiliser les politiques de déchiffrement SSL pour convertir le trafic chiffré en trafic de texte brut, afin de pouvoir ensuite appliquer le filtrage d'URL, la prévention des intrusions et des programmes malveillants, ainsi que d'autres services nécessitant une inspection approfondie des paquets. Si vos politiques le permettent, le trafic est rechiffré avant de quitter le périphérique.

La politique de déchiffrement SSL s'applique uniquement au trafic chiffré. Aucune connexion non chiffrée n'est évaluée par rapport aux règles de déchiffrement SSL.

Contrairement à certaines autres politiques de sécurité, vous devez surveiller et maintenir activement la politique de déchiffrement SSL, car les certificats peuvent expirer ou même être modifiés sur les serveurs de destination. En outre, les modifications apportées au logiciel client peuvent altérer votre capacité à déchiffrer certaines connexions, car l'action de re-signer le déchiffrement est impossible à distinguer d'une attaque de type Man-in-the-middle (d'intermédiaire).

La procédure suivante explique le processus de bout en bout de mise en œuvre et de maintenance de la politique de déchiffrement SSL.

Procédure

Étape 1 Si vous mettez en œuvre les règles de déchiffrement et de réauthentification, créez le certificat d'autorité de certification interne requis.

Vous devez utiliser un certificat d'autorité de certification (CA) interne. Vous avez les options suivantes. Étant donné que les utilisateurs doivent faire confiance au certificat, téléversez soit un certificat déjà approuvé par les navigateurs clients, soit assurez-vous que le certificat téléversé est ajouté aux magasins de certificats de confiance des navigateurs.

- Créez un certificat d'autorité de certification interne autosigné, qui est signé par le périphérique lui-même. Consultez Génération de certificats internes autosignés et de certificats d'autorité de certification internes.
- Chargez un certificat d'autorité de certification interne et une clé signée par une autorité de certification externe de confiance ou par une autorité de certification de votre organisation. Consultez Charger les certificats d'identité interne et d'autorité de certification interne.

Étape 2 Si vous mettez en œuvre les règles de déchiffrement de la clé connue, collectez le certificat et la clé sur chacun des serveurs internes.

Vous ne pouvez utiliser le déchiffrement de la clé connue qu'avec les serveurs que vous contrôlez, car vous devez obtenir le certificat et la clé du serveur. Chargez ces certificats et clés en tant que certificats internes

(et non en tant que certificats d'autorité de certification interne). Consultez Charger les certificats d'identité interne et d'autorité de certification interne.

Étape 3 Activez la politique de déchiffrement SSL., à la page 9.

Lorsque vous activez la politique, vous configurez également certains paramètres de base.

Étape 4 Configurer l'action de déchiffrement SSL par défaut, à la page 11.

En cas de doute, sélectionnez **Do Not Decrypt (Ne pas déchiffrer)** comme action par défaut. Votre stratégie de contrôle d'accès peut tout de même abandonner le trafic qui correspond à la règle de déchiffrement SSL par défaut, au besoin.

Étape 5 Configurer les règles de déchiffrement SSL, à la page 11.

Déterminez le trafic à déchiffrer et le type de déchiffrement à appliquer.

Étape 6 Si vous configurez le déchiffrement par clé connue, modifiez les paramètres de la politique de déchiffrement SSL pour inclure ces certificats. Consultez Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 19.

Étape 7 Si nécessaire, téléchargez le certificat d'autorité de certification utilisé pour les règles de déchiffrement et de réauthentification et chargez-le dans le navigateur sur les postes de travail clients.

Pour en savoir plus sur le téléchargement du certificat et sa distribution aux clients, consultez Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 21.

Étape 8 Périodiquement, mettez à jour les certificats de réauthentification et de clé connue.

- Certificat de réauthentification : mettez à jour ce certificat avant son expiration. Si vous générez le certificat par le biais de Firepower Device Manager, il est valide pendant 5 ans. Pour vérifier la période de validité d'un certificat, sélectionnez **Objects (Objets)** > **Certificates (Certificats)**, repérez le certificat dans la liste, puis cliquez sur l'icône d'information ( ) correspondante dans la colonne Actions. La boîte de dialogue d'information affiche la période de validité et certaines autres caractéristiques. Vous pouvez également téléverser un certificat de remplacement à partir de cette page.
- Certificat de clé connue : pour toute règle de déchiffrement de clé connue, vous devez vous assurer d'avoir chargé le certificat et la clé actuels du serveur de destination. Chaque fois que le certificat et la clé changent sur les serveurs pris en charge, vous devez également charger le nouveau certificat et la clé (en tant que certificat interne) et mettre à jour les paramètres de déchiffrement SSL pour utiliser le nouveau certificat.

Étape 9 Chargez les certificats d'autorité de certification de confiance manquants pour les serveurs externes.

Le système comprend un large éventail de certificats racine d'autorité de certification et intermédiaires de confiance émis par des tiers. Ceux-ci sont nécessaires lors de la négociation de la connexion entre le Cisco Firewall Threat Defense et les serveurs de destination pour les règles de déchiffrement et de réauthentification.

Chargez tous les certificats de la chaîne de confiance d'une autorité de certification racine dans la liste des certificats d'autorités de certification de confiance, y compris le certificat de l'autorité de certification racine et tous les certificats d'autorités de certification intermédiaires. Sinon, il est plus difficile de détecter les certificats de confiance émis par des autorités de certification intermédiaires. Chargez les certificats sur la page **Objects (Objets)** > **Certificates (Certificats)**. Consultez Téléchargement des certificats de l'autorité de certification de confiance.

Configuration des politiques de déchiffrement SSL

Vous pouvez utiliser les politiques de déchiffrement SSL pour convertir le trafic chiffré en trafic de texte brut, afin de pouvoir ensuite appliquer le filtrage d'URL, la prévention des intrusions et des programmes malveillants, ainsi que d'autres services nécessitant une inspection approfondie des paquets. Si vos politiques le permettent, le trafic est rechiffré avant de quitter le périphérique.

La politique de déchiffrement SSL s'applique uniquement au trafic chiffré. Aucune connexion non chiffrée n'est évaluée par rapport aux règles de déchiffrement SSL.

Remarque Les tunnels VPN sont déchiffrés avant l'évaluation de la politique de déchiffrement SSL, de sorte que la politique ne s'applique jamais au tunnel lui-même. Cependant, toute connexion chiffrée dans le tunnel est soumise à une évaluation par la politique de déchiffrement SSL.

La procédure suivante explique comment configurer la politique de déchiffrement SSL. Pour une explication du processus de bout en bout de création et de gestion du déchiffrement SSL, voir Comment mettre en œuvre et maintenir la politique de déchiffrement SSL, à la page 6.

Avant de commencer

Le tableau des règles de déchiffrement SSL contient deux sections :

- **Règles d'authentification active de la politique d'identité** : si vous activez la politique d'identité et créez des règles qui utilisent l'authentification active, le système crée automatiquement les règles de déchiffrement SSL nécessaires pour faire fonctionner ces politiques. Ces règles sont toujours évaluées avant les règles de déchiffrement SSL que vous créez vous-même. Vous ne pouvez modifier ces règles qu'indirectement, en modifiant la politique d'identité.
- **Règles natives SSL** : il s'agit de règles que vous avez configurées. Vous ne pouvez ajouter de règles qu'à cette section.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Si vous n'avez pas encore activé la politique, cliquez sur **Enable SSL Decryption** (Activer le déchiffrement SSL) et configurez les paramètres de la politique, comme décrit dans Activez la politique de déchiffrement SSL., à la page 9.

Étape 2 Configurez l'action par défaut pour la politique.

Le choix le plus sûr est **Do Not Decrypt** (Ne pas déchiffrer). Pour en savoir plus, consultez Configurer l'action de déchiffrement SSL par défaut, à la page 11.

Étape 3 Gérez la politique de déchiffrement SSL.

Après avoir configuré les paramètres de déchiffrement SSL, 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 désactiver la politique, cliquez sur le bouton de bascule **SSL Decryption Policy** (politique de déchiffrement SSL). Vous pouvez la réactiver en cliquant sur **Enable SSL Decryption** (Activer le déchiffrement SSL).
- Pour modifier les paramètres de la politique, y compris la liste des certificats utilisés dans la politique, cliquez sur le bouton **SSL Decryption Settings** (Paramètres de déchiffrement SSL) (); voir Configurer les paramètres de déchiffrement SSL, à la page 19. Vous pouvez également télécharger le certificat utilisé avec les règles de reconnexion de déchiffrement afin de pouvoir le distribuer aux clients. Consultez les rubriques suivantes:
  - Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 19
  - Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 21
- Pour configurer des règles :
  - Pour créer une nouvelle règle, cliquez sur le bouton +. Consultez Configurer les règles de déchiffrement SSL, à la page 11.
  - 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 déplacer une règle, modifiez-la et sélectionnez le nouvel emplacement dans la liste déroulante **Order** (Ordre).
- Si des règles rencontrent des problèmes, par exemple en raison de catégories d'URL supprimées ou modifiées, cliquez sur le lien **See Problem Rules** (voir les règles pour lesquelles il y a des problèmes) à côté de la zone de recherche pour filtrer le tableau afin d'afficher uniquement ces règles. Veuillez modifier et corriger (ou supprimer) ces règles afin qu'elles fournissent le service dont vous avez besoin.

Activez la politique de déchiffrement SSL.

Avant de pouvoir configurer les règles de déchiffrement SSL, vous devez activer la politique et configurer certains paramètres de base. La procédure suivante explique comment activer la politique directement. Vous pouvez également l'activer lorsque vous activez les politiques d'identité. Les politiques d'identité nécessitent que vous activiez la politique de déchiffrement SSL.

Avant de commencer

Si vous avez effectué la mise à niveau à partir d'une version qui n'avait pas de politiques de déchiffrement SSL, mais que vous aviez configuré la politique d'identité avec des règles d'authentification actives, la politique de déchiffrement SSL est déjà activée. Assurez-vous de sélectionner le certificat de déchiffrement Re-Sign que vous souhaitez utiliser et activez éventuellement les règles prédéfinies.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez sur **Enable SSL Decryption** (activer le déchiffrement SSL) pour configurer les paramètres de la politique.

- S'il s'agit de la première fois que vous avez activé la politique, la boîte de dialogue SSL Decryption Configuration (Configuration du déchiffrement SSL) s'ouvre. Passez à l'étape suivante.
- Si vous avez déjà configuré la politique une fois, puis l'avez désactivée, la politique est simplement réactivée avec vos paramètres et règles précédents. Vous pouvez cliquer sur le bouton **SSL Decryption Settings** (Paramètres de déchiffrement SSL) () et configurer les paramètres comme décrit dans Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 19.

Étape 3 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, à la page 21.

Étape 4 (Facultatif) Cliquez sur le signe **plus (+)** sous **Trusted CA Certificates** (Certificats d'autorité de certification approuvés) et sélectionnez les certificats ou les groupes de certificats auxquels vous souhaitez que la politique fasse confiance.

Le groupe par défaut, Cisco-Trusted-Authorities, comprend tous les certificats d'autorité de certification de confiance définis par le système. Si vous avez chargé des certificats supplémentaires, vous pouvez les ajouter ici ou les collecter dans votre propre groupe et sélectionner le groupe ici. Vous pouvez soit remplacer le groupe Cisco-Trusted-Authorities, soit simplement ajouter votre groupe. Les utilisateurs seront invités à accepter le certificat pour tout site dont l'autorité de signature du certificat n'est pas représentée dans cette liste : l'accès au site n'est pas bloqué simplement parce que le certificat n'est pas fiable.

Si vous laissez la liste vide ou ne sélectionnez que des groupes de certificats vides, la politique de déchiffrement SSL fera confiance à n'importe quel certificat.

Étape 5 Sélectionnez les règles de déchiffrement SSL initiales.

Le système comprend la règle prédéfinie suivante que vous pourriez trouver utile :

- **Sensitive_Data** (Données_sensibles) : cette règle ne déchiffre pas le trafic qui correspond aux sites Web dans les catégories d'URL Services financiers ou d'URL de santé et de médecine, qui comprennent les banques, les services de santé, etc. Vous devez activer la licence d'URL pour mettre en œuvre cette règle.

Étape 6 Cliquez sur **Enable** (activer).

Configurer l'action de déchiffrement SSL par défaut

Si une connexion chiffrée ne correspond pas à une règle de déchiffrement SSL spécifique, elle est gérée par l'action par défaut de la politique de déchiffrement SSL.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez n'importe où dans le champ **Default Action** (action par défaut).

Étape 3 Sélectionnez l'action à appliquer au trafic correspondant.

- **Do Not Decrypt** (Ne pas déchiffrer) : autorise la connexion chiffrée. La stratégie de contrôle d'accès évalue ensuite la connexion chiffrée et l'abandonne ou l'autorise en fonction des règles de contrôle d'accès.
- **Block** (Bloquer) : interrompt la connexion immédiatement. La connexion n'est pas transmise à la stratégie de contrôle d'accès.

Étape 4 (Facultatif) Configurez la journalisation pour l'action par défaut.

Vous devez activer la journalisation du trafic correspondant à la règle pour qu'elle soit incluse dans les données du tableau de bord ou le visualisateur d'événements. Sélectionnez parmi les options suivantes :

- **At End of Connection** (À la fin de la connexion) : génère un événement à la fin de la connexion.
  - **Send Connection Events To** (Envoyer les événements de connexion à) : si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Create New Syslog Server** (Créer un nouveau serveur syslog) et créez-le. (Pour désactiver la journalisation sur un serveur syslog, sélectionnez **Any** (N'importe lequel) dans la liste des serveurs.)

    Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.
- **No Logging** (Aucune journalisation) : ne génère aucun événement.

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

Configurer les règles de déchiffrement SSL

Utilisez les règles de déchiffrement SSL pour déterminer comment gérer les connexions chiffrées. Les règles de la politique de déchiffrement SSL sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic.

Vous pouvez créer et modifier des règles uniquement dans la section SSL Native Rules (Règles SSL natives).

Remarque Le trafic pour vos connexions VPN (de site à site et d'accès à distance) est déchiffré avant que la politique de déchiffrement SSL n'évalue les connexions. Ainsi, les règles de déchiffrement SSL ne sont jamais appliquées aux connexions VPN, et vous n'avez pas besoin de prendre en compte les connexions VPN lors de la création de ces règles. Cependant, toute utilisation de connexions chiffrées dans un tunnel VPN est évaluée. Par exemple, une connexion HTTPS à un serveur interne par l'intermédiaire d'une connexion VPN d'accès à distance est évaluée par les règles de déchiffrement SSL, même si le tunnel VPN d'accès à distance lui-même ne l'est pas (car il est déjà déchiffré).

Avant de commencer

Si vous créez une règle de déchiffrement de clé connue, veillez à charger le certificat et la clé pour le serveur de destination (en tant que certificat interne) et à modifier les paramètres de la politique de déchiffrement SSL pour utiliser le certificat. Les règles de clé connue précisent généralement le serveur de destination dans les critères de réseau de destination de la règle. Pour en savoir plus, consultez Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 19.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Si vous n'avez configuré aucune règle de déchiffrement SSL (hormis celles générées automatiquement pour les règles d'identité d'authentification actives), vous pouvez ajouter des règles prédéfinies en cliquant sur **Add Pre-Defined Rules** (Ajouter des règles prédéfinies). Vous êtes invité à sélectionner les règles que vous souhaitez.

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.

Vous ne pouvez insérer des règles que dans la section **SSL Native Rules** (Règles SSL natives). Les Identity Policy Active Authentication Rules (Règles d'authentification active de la politique d'identité) sont automatiquement générées à partir de votre politique d'identité et sont en lecture seule.

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.

Le nom ne peut pas contenir d'espaces. Vous pouvez utiliser des caractères alphanumériques et les caractères spéciaux suivants : + . _ -

Étape 5 Sélectionnez l'action à appliquer au trafic correspondant.

Pour une description détaillée de chaque option, consultez les éléments suivants :

- Déchiffrer - Resigner, à la page 2
- Déchiffrer à l'aide d'une clé connue, à la page 3
- Ne pas déchiffrer, à la page 4
- Bloquer, à la page 4

Étape 6 Définissez les critères de correspondance du trafic en utilisant n'importe quelle combinaison des onglets suivants :

- **Source/Destination** : les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) de l'adresse IP, ou les ports TCP utilisés dans le trafic. La valeur par défaut est toute zone, adresse, emplacement géographique et port TCP. Consultez Critères de source/destination pour les règles de déchiffrement SSL, à la page 14.
- **Application** : l'application ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est n'importe quelle application chiffrée. Consultez Critères d'application pour les règles de déchiffrement SSL, à la page 15.
- **URL** : la catégorie d'URL d'une requête Web. Par défaut, la catégorie d'URL et la réputation ne sont pas prises en compte à des fins de correspondance. Consultez Critères d'URL pour les règles de déchiffrement SSL, à la page 16.
- **Users** (Utilisateurs) : la source d'identité, l'utilisateur ou le groupe d'utilisateurs. Vos politiques d'identité déterminent si les informations d'utilisateur et de groupe sont disponibles pour la correspondance du trafic. Vous devez configurer les politiques d'identité pour utiliser ce critère. Consultez Critères d'utilisateur pour les règles de déchiffrement SSL, à la page 17.
- **Advanced** (Avancé) : caractéristiques dérivées des certificats utilisés dans la connexion, telles que la version SSL/TLS et l'état du certificat. Consultez Critères avancés pour les règles de déchiffrement SSL, à la page 18.

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.

Lorsque vous ajoutez des conditions aux règles de déchiffrement SSL, tenez compte des conseils suivants :

- Vous pouvez configurer plusieurs conditions par règle. Le trafic doit correspondre à toutes les conditions de la règle pour que celle-ci s'applique au trafic. Par exemple, vous pouvez utiliser une règle unique pour déchiffrer le trafic en fonction de la catégorie d'URL.
- Pour chaque condition d'une règle, vous pouvez ajouter jusqu'à 50 critères. Le trafic qui correspond à l'un des critères d'une condition satisfait à la condition. Par exemple, vous pouvez utiliser une règle unique pour appliquer le contrôle d'application à 50 applications ou filtres d'application. Ainsi, il existe une relation OU entre les éléments d'une condition unique, mais une relation ET entre les types de condition (par exemple, entre la source ou destination et l'application).
- La mise en correspondance de la catégorie d'URL nécessite la licence de filtrage d'URL.

Étape 7 (Facultatif) Configurez la journalisation pour la règle.

Vous devez activer la journalisation du trafic correspondant à la règle pour qu'elle soit incluse dans les données du tableau de bord ou le visualisateur d'événements. Sélectionnez parmi les options suivantes :

- **At End of Connection** (À la fin de la connexion) : génère un événement à la fin de la connexion.
  - **Send Connection Events To** (Envoyer les événements de connexion à) : si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Create New Syslog Server** (Créer un nouveau serveur syslog) et créez-le. (Pour désactiver la journalisation sur un serveur syslog, sélectionnez Any (N'importe lequel) dans la liste des serveurs.)

    Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.

- **No Logging** (Aucune journalisation) : ne génère aucun événement.

Étape 8 Cliquez sur **OK**.

Critères de source/destination pour les règles de déchiffrement SSL

Les critères Source/Destination d'une règle de déchiffrement SSL 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 ports TCP utilisés dans le trafic. La valeur par défaut englobe toute zone, adresse, emplacement géographique et tout port TCP. TCP est le seul protocole correspondant aux règles de déchiffrement SSL.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK**. 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 utiliser les critères suivants pour identifier la source et la destination à mettre en correspondance dans la règle.

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 tout le trafic allant des hôtes externes vers les hôtes internes est déchiffré, vous devez sélectionner votre zone externe comme **Source Zones** (Zones source) et votre zone interne comme **Destination Zones** (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.

Remarque Pour les règles de déchiffrement de clé connue, sélectionnez un objet avec l'adresse IP du serveur de destination qui utilise le certificat et la clé que vous avez chargés.

- **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.

Ports source, ports/protocoles de destination

Les objets de port qui définissent les protocoles utilisés dans le trafic. Vous pouvez spécifier le protocole TCP et les ports uniquement pour les règles de déchiffrement SSL.

- Pour faire correspondre le trafic d'un port TCP, configurez les **Source Ports** (Ports source).
- Pour faire correspondre le trafic à un port TCP, configurez les **Destination Ports/Protocols** (Ports/Protocoles de destination).
- Pour faire correspondre le trafic provenant de ports TCP spécifiques et destiné à des ports TCP spécifiques, configurez les deux. Par exemple, vous pouvez cibler le trafic du port TCP/80 au port TCP/8080.

Critères d'application pour les règles de déchiffrement SSL

Les critères d'application d'une règle de déchiffrement SSL définissent l'application utilisée dans une connexion IP, ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est toute application qui a la balise SSL Protocol. Vous ne pouvez pas faire correspondre les règles de déchiffrement SSL à une application non chiffrée.

Bien que vous puissiez spécifier des applications individuelles dans la règle, les filtres d'applications simplifient la création et l'administration des politiques. Par exemple, vous pouvez créer une règle de déchiffrement SSL qui déchiffre ou bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est déchiffrée ou bloquée.

De plus, Cisco met fréquemment à jour et ajoute des détecteurs d'applications supplémentaires par l'intermédiaire des mises à jour du système et de la base de données des vulnérabilités (VDB). Ainsi, une règle pour les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Vous pouvez spécifier des applications et des filtres directement dans la règle, ou créer des objets de filtre d'application qui définissent ces caractéristiques. Les spécifications sont équivalentes, bien que l'utilisation d'objets puisse permettre de respecter plus facilement la limite du système de 50 éléments par critère si vous créez une règle complexe.

Pour modifier la liste des applications et des filtres, vous cliquez sur le bouton **+** dans la condition, sélectionnez les applications ou les objets de filtre d'application souhaités, qui sont répertoriés sur des onglets distincts, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Dans l'un ou l'autre des onglets, vous pouvez cliquer sur **Advanced Filter** (Filtres avancés) pour sélectionner des critères de filtre ou pour vous aider à rechercher des applications spécifiques. Cliquez sur le **x** pour une application, un filtre ou un objet pour le supprimer de la politique. Cliquez sur le lien **Save As Filter** (Enregistrer en tant que filtre) pour enregistrer les critères combinés qui ne sont pas déjà un objet en tant que nouvel objet de filtre d'application.

Pour en savoir plus sur les critères d'application et comment configurer les filtres avancés et sélectionner des applications, consultez Configuration des objets de filtre d'application.

Tenez compte des conseils suivants lors de l'utilisation des critères d'application dans les règles de déchiffrement SSL.

- Le système peut identifier les applications non chiffrées qui deviennent chiffrées à l'aide de StartTLS. Cela inclut des applications telles que SMTPS, POPS, FTPS, TelnetS et IMAPS. En outre, il peut identifier certaines applications chiffrées en fonction de l'indication du nom du serveur dans le message TLS ClientHello ou de la valeur du nom distinctif du sujet provenant du certificat du serveur.
- Le système peut identifier l'application uniquement après l'échange du certificat du serveur. Si le trafic échangé pendant l'établissement de liaison SSL correspond à toutes les autres conditions dans une règle SSL contenant une condition d'application, mais que l'identification n'est pas terminée, la politique SSL permet au paquet de passer. Ce comportement permet à l'établissement de liaison de se faire afin que les applications puissent être identifiées. Une fois que le système a terminé son identification, il applique la règle d'action appropriée au trafic de session restant.
- Si une application sélectionnée a été supprimée par une mise à jour de VDB, « (Deprecated) » s'affiche après le nom de l'application. Vous devez supprimer ces applications du filtre, sinon les déploiements et les mises à niveau logicielles du système suivants seront bloqués.

Critères d'URL pour les règles de déchiffrement SSL

Les critères d'URL d'une règle de déchiffrement SSL définissent la catégorie à laquelle appartient l'URL dans une requête Web. Vous pouvez également préciser la réputation relative des sites à déchiffrer, à bloquer ou à autoriser sans déchiffrement. La valeur par défaut est de ne pas mettre en correspondance les connexions selon les catégories d'URL.

Par exemple, vous pourriez bloquer tous les sites de jeux chiffrés ou déchiffrer les sites de réseaux sociaux non fiables. Si un utilisateur tente d'accéder à une URL avec cette catégorie et ce niveau de réputation, la

session est bloquée ou déchiffrée. Pour en savoir plus sur la mise en correspondance des catégories d'URL, consultez Filtrage des URL par catégorie et par réputation.

Onglet Catégories

Cliquez sur **+**, sélectionnez les catégories souhaitées, puis cliquez sur **OK**. Cliquez sur le **x** pour supprimer une catégorie de la politique.

La valeur par défaut est d'appliquer la règle à toutes les URL de chaque catégorie sélectionnée, quelle que soit leur réputation. Pour limiter la règle en fonction de la réputation, cliquez sur la flèche vers le bas pour chaque catégorie, désélectionnez la case **Any** (Tout), puis utilisez le curseur **Reputation** (Réputation) pour choisir le niveau de réputation. La partie gauche du curseur de réputation indique les sites autorisés sans déchiffrement, tandis que la partie droite regroupe les sites qui seront déchiffrés ou bloqués. La façon dont la réputation est utilisée dépend de l'action de la règle :

- Si la règle déchiffre ou bloque les connexions, la sélection d'un niveau de réputation sélectionne également toutes les réputations plus graves que ce niveau. Par exemple, si vous configurez une règle pour déchiffrer ou bloquer les sites (Suspects) et **Questionable** (Discutables) (niveau 2), elle déchiffre ou bloque également automatiquement les sites (À risque élevé) et **Untrusted** (Non fiables) (niveau 1).
- Si la règle autorise les connexions sans déchiffrement (ne pas déchiffrer), la sélection d'un niveau de réputation sélectionne également toutes les réputations moins graves que ce niveau. Par exemple, si vous configurez une règle pour ne pas déchiffrer les site (Suspects) et **Questionable** (Discutables) (niveau 4), elle ne déchiffre également pas automatiquement les sites (Bien connus) et **Trusted (de confiance)** (niveau 5).

Sélectionnez l'option **Include Sites with Unknown Reputation** (inclure les sites avec une réputation inconnue) pour inclure les URL de réputation inconnue dans la correspondance de réputation. Les nouveaux sites ne sont généralement pas classés, et il peut y avoir d'autres raisons pour lesquelles la réputation d'un site est inconnue ou ne peut être déterminée.

Vérifier la catégorie d'une URL

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Saisissez l'URL dans le champ **URL to Check** (URL à vérifier), puis cliquez sur **Go** (Lancer). Vous serez redirigé vers un site Web externe pour consulter les résultats. Si vous êtes en désaccord avec une catégorisation, cliquez sur le lien **Submit a URL Category** Dispute (Soumettre une contestation de catégorie d'URL) et faites-le-nous savoir.

Critères d'utilisateur pour les règles de déchiffrement SSL

Les critères d'utilisateur d'une règle de déchiffrement SSL définissent l'utilisateur ou le groupe d'utilisateurs pour une connexion IP. Vous devez configurer les politiques d'identité et le serveur de répertoire associé pour inclure les critères d'utilisateur ou de groupe d'utilisateurs dans une règle.

Vos politiques d'identité déterminent si l'identité de l'utilisateur est collectée pour une connexion particulière. Si l'identité est établie, l'adresse IP de l'hôte est associée à l'utilisateur identifié. Ainsi, le trafic dont l'adresse IP source est mappée à un utilisateur est considéré comme provenant de cet utilisateur. Les paquets IP en eux-mêmes ne comprennent pas d'informations sur l'identité de l'utilisateur, de sorte que ce mappage adresse IP-utilisateur est la meilleure approximation disponible.

Étant donné que vous pouvez ajouter un maximum de 50 utilisateurs ou groupes à une règle, il est généralement plus logique de sélectionner des groupes que de sélectionner des utilisateurs individuels. Par exemple, vous pouvez créer une règle qui déchiffre le trafic vers le groupe d'ingénierie qui provient du réseau externe, et créer une règle distincte qui ne déchiffre pas le trafic sortant de ce groupe. Ensuite, pour que la règle s'applique

aux nouveaux ingénieurs, il vous suffit d'ajouter le spécialiste en ingénierie au groupe Engineering dans le serveur d'annuaire.

Vous pouvez également sélectionner les sources d'identité à appliquer à tous les utilisateurs de cette source. Ainsi, si vous prenez en charge plusieurs domaines Active Directory, vous pouvez fournir un déchiffrement différentiel en fonction du domaine.

Pour modifier la liste des utilisateurs, vous cliquez sur le bouton **+** dans la condition et sélectionnez les utilisateurs ou les groupes d'utilisateurs souhaités en utilisant l'une des techniques suivantes. Cliquez sur le **x** pour un utilisateur ou un groupe pour le supprimer de la politique.

- **Sources d'identité** : sélectionnez une source d'identité, telle qu'un domaine AD ou la base de données d'utilisateurs locaux, pour appliquer la règle à tous les utilisateurs obtenus à partir des sources sélectionnées. Si le domaine dont vous avez besoin n'existe pas encore, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité) et créez-le maintenant.
- **Groupes** : sélectionnez les groupes d'utilisateurs souhaités. Les groupes sont disponibles uniquement si vous les configurez dans le serveur de répertoire. Si vous sélectionnez un groupe, la règle s'applique à tous les membres du groupe, y compris les sous-groupes. Si vous souhaitez traiter un sous-groupe différemment, vous devez créer une règle d'accès distincte pour le sous-groupe et la placer au-dessus de la règle pour le groupe parent dans la stratégie de contrôle d'accès.
- **Utilisateurs** : sélectionnez des utilisateurs individuels. Le nom d'utilisateur est précédé de la source d'identité, par exemple Realm\username (domaine\nom_utilisateur).

  Il existe certains utilisateurs intégrés dans le domaine Special-Identities-Realm (domaine d'identités spéciales) :

  - **Failed Authentication** (Échec de l'authentification) : l'utilisateur a été invité à s'authentifier, mais n'a pas réussi à saisir une paire nom d'utilisateur/mot de passe valide dans le nombre maximal de tentatives autorisées. L'échec de l'authentification n'empêche pas l'utilisateur d'accéder au réseau, mais vous pouvez écrire une règle d'accès pour limiter l'accès au réseau pour ces utilisateurs.
  - **Guest** (Invité) : les utilisateurs invités sont similaires aux utilisateurs en Failed Authentication (Échec de l'authentification), sauf que votre règle d'identité est configurée pour identifier ces utilisateurs comme Guest (Invité). Les utilisateurs invités ont été invités à s'authentifier et n'ont pas réussi à le faire dans les limites du nombre maximal de tentatives.
  - **No Authentication Required** (Aucune authentification requise) : l'utilisateur n'a pas été invité à s'authentifier, car ses connexions correspondaient à des règles d'identité ne spécifiant aucune authentification.
  - **Unknown** (Inconnu) : aucun mappage d'utilisateur n'existe pour l'adresse IP et aucun échec d'authentification n'a encore été enregistré. En règle générale, cela signifie qu'aucun trafic HTTP n'a encore été vu à partir de cette adresse.

Critères avancés pour les règles de déchiffrement SSL

Les critères de correspondance de trafic avancé sont liés aux caractéristiques dérivées des certificats utilisés dans la connexion. Vous pouvez configurer les options suivantes :

Options des propriétés du certificat

Le trafic correspond à l'option des propriétés du certificat de la règle s'il correspond à l'une des propriétés sélectionnées. Vous pouvez configurer les éléments suivants :

État du certificat

Si le certificat est **Valid** (valide) ou **Invalid** (non valide). Sélectionnez **Any** (tout) (par défaut) si l'état du certificat n'a pas d'importance.

Un certificat est considéré comme valide si toutes les conditions suivantes sont remplies, sinon il n'est pas valide :

- La politique fait confiance à l'autorité de certification qui a émis le certificat.
- La signature du certificat peut être correctement validée par rapport au contenu du certificat.
- Le certificat de l'autorité de certification émettrice est stocké dans la liste des certificats d'autorités de certification de confiance de la politique.
- Aucune des autorités de certification de confiance de la politique n'a révoqué le certificat.
- La date actuelle est comprise entre la date de début de validité du certificat et la date de fin de validité du certificat.

Autosigné

Le certificat de serveur détecté contient le même nom distinctif d'émetteur et de sujet. Sélectionnez l'une des options suivantes :

- **Self-Signing** (Auto-signature) : le certificat du serveur est autosigné.
- **CA-Signing** (Signature par une autorité de certification) : le certificat du serveur est signé par une autorité de certification. C'est-à-dire que l'émetteur et le sujet ne sont pas la même chose.
- **Any** (Tout) : ne tient pas compte du fait que le certificat est autosigné comme critère de correspondance.

Version prise en charge

La version SSL/TLS à mettre en correspondance. La règle s'applique au trafic qui utilise uniquement les versions sélectionnées. Toutes les versions sont sélectionnées par défaut. Sélectionnez parmi : **SSL 3.0**, **TLS 1.0**, **TLS 1.1**, **TLS 1.2**, **TLS 1.3**.

Par exemple, si vous souhaitez autoriser uniquement les connexions TLSv1.2/3, vous pouvez créer une règle de blocage pour les versions antérieures.

Vous devez utiliser Snort 3 pour faire correspondre les connexions TLS 1.3.

Le trafic qui utilise une version non répertoriée, comme SSL v2.0, est géré par l'action par défaut de la politique de déchiffrement SSL.

Configurer les paramètres de déchiffrement SSL

Vous devez configurer les paramètres de certificat si vous avez des règles qui déchiffrent le trafic. Vous pouvez également modifier les paramètres pour changer la façon dont le déchiffrement est appliqué au trafic chiffré. Les rubriques suivantes expliquent les options disponibles.

Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement

Si vous mettez en œuvre le déchiffrement, soit par nouvelle signature ou par utilisation de clés connues, vous devez identifier les certificats que les règles de déchiffrement SSL peuvent utiliser. Assurez-vous que tous les certificats sont valides et n'ont pas encore expiré.

Surtout pour le déchiffrement par clé connue, vous devez vous assurer que le système dispose du certificat et de la clé actuels pour chaque serveur de destination dont vous déchiffrez les connexions. Avec une règle de déchiffrement de clé connue, vous utilisez le certificat et la clé réels du serveur de destination pour le déchiffrement. Ainsi, vous devez vous assurer que le périphérique Cisco Firewall Threat Defense dispose du certificat et de la clé actuels à tout moment, sinon le déchiffrement échouera.

Chargez un nouveau certificat interne et une nouvelle clé chaque fois que vous modifiez le certificat ou la clé sur le serveur de destination dans une règle de clé connue. Chargez-les en tant que certificat interne (et non en tant que certificat d'autorité de certification interne). Vous pouvez téléverser le certificat au cours de la procédure suivante, ou aller à la page **Objects (Objets)** > **Certificates (Certificats)** et le charger à cet endroit.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez sur le bouton **SSL Decryption Settings** ( ).

Si nécessaire, sélectionnez l'onglet **Basic** (Base).

Étape 3 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, à la page 21.

Étape 4 Pour chaque règle qui déchiffre à l'aide d'une clé connue, téléversez le certificat interne et la clé du serveur de destination.

a) Cliquez sur + sous **Decrypt Known-Key Certificates** (Déchiffrer les certificats à clé connue).
b) Sélectionnez le certificat d'identité interne ou cliquez sur **Create New Internal Certificate** (créer un nouveau certificat interne) pour le téléverser maintenant.
c) Cliquez sur **OK**.

Étape 5 (Facultatif) Cliquez sur le signe **plus (+)** sous **Trusted CA Certificates** (Certificats d'autorité de certification approuvés) et sélectionnez les certificats ou les groupes de certificats auxquels vous souhaitez que la politique fasse confiance.

Le groupe par défaut, Cisco-Trusted-Authorities, comprend tous les certificats d'autorité de certification de confiance définis par le système. Voici les principaux cas dans lesquels vous pourriez modifier ce paramètre :

- Vous souhaitez utiliser des certificats d'autorité de certification de confiance qui ne sont pas dans le groupe par défaut. Vous devez ensuite sélectionner le groupe par défaut et votre nouveau groupe dans les paramètres de la politique de déchiffrement SSL. Vous pouvez le faire si vous avez chargé des certificats d'autorité de certification de confiance supplémentaires.
- Vous souhaitez utiliser une liste plus limitée de certificats d'autorité de certification de confiance que celle du groupe par défaut. Vous devez ensuite créer un groupe qui a une liste complète de certificats de

confiance, pas seulement votre delta, et le sélectionner comme seul groupe dans les paramètres de la politique de déchiffrement SSL.

Les utilisateurs seront invités à accepter le certificat pour tout site dont l'autorité de signature du certificat n'est pas représentée dans cette liste : l'accès au site n'est pas bloqué simplement parce que le certificat n'est pas fiable.

Si vous laissez la liste vide ou ne sélectionnez que des groupes de certificats vides, la politique de déchiffrement SSL fera confiance à n'importe quel certificat.

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

Configurer les paramètres de trafic avancé et non déchiffrable

Vous pouvez configurer les paramètres de déchiffrement avancé et les paramètres du trafic non déchiffrable si vous ne souhaitez pas utiliser le comportement par défaut.

Procédure

Étape 1 Select **Policies (politiques)** > **SSL Decryption**.

Étape 2 Cliquez sur le bouton **SSL Decryption Settings** ( ).

Étape 3 Dans l'onglet **Advanced** (Avancé), choisissez d'activer ou non **TLS 1.3 Decryption (déchiffrement TLS 1.3)**.

Si vous activez le déchiffrement TLS 1.3, vous devez également sélectionner l'option TLS 1.3 sous l'onglet Advanced (Avancé) de chaque règle qui doit s'appliquer à TLS 1.3. Vous devez exécuter Snort 3 pour déchiffrer TLS 1.3.

Étape 4 Dans l'onglet **Undecryptable Actions** (Actions indéchiffrables), modifiez la façon dont le système gère les connexions qui correspondent aux règles qui mettent en œuvre le déchiffrement, dans les cas où la connexion ne peut pas être déchiffrée.

La valeur par défaut est d'appliquer la même action que l'action par défaut à ces connexions. L'exception est les erreurs de déchiffrement, pour lesquelles vos options sont de bloquer ou de bloquer avec réinitialisation uniquement.

Pour obtenir une description des catégories de menaces fournies par le système, utilisez Gestion du trafic non déchiffrable, à la page 4.

Étape 5 Cliquez sur **OK**.

Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature

Si vous décidez de déchiffrer le trafic, les utilisateurs doivent avoir le certificat d'autorité de certification interne qui est utilisé dans le processus de chiffrement défini comme une autorité de certification racine de confiance dans leurs applications utilisant TLS/SSL. Généralement, si vous générez un certificat, ou parfois même si vous en importez un, le certificat n'est pas déjà défini comme un certificat de confiance dans ces

applications. Par défaut, dans la plupart des navigateurs Web, lorsque les utilisateurs envoient des requêtes HTTPS, un message d'avertissement de l'application client leur indique qu'il existe un problème avec le certificat de sécurité du site Web. Habituellement, le message d'erreur indique que le certificat de sécurité du site Web n'a pas été émis par une autorité de certification approuvée ou que le site Web a été certifié par une autorité inconnue, mais l'avertissement peut également indiquer qu'il y a une possible attaque de l'homme du milieu en cours. Certaines autres applications client ne présentent pas ce message d'avertissement aux utilisateurs et ne permettent pas aux utilisateurs d'accepter le certificat non reconnu.

Vous disposez des options suivantes pour fournir aux utilisateurs le certificat requis :

Informer les utilisateurs d'accepter le certificat racine

Vous pouvez informer les utilisateurs de votre organisation des nouvelles politiques de l'entreprise et leur dire d'accepter le certificat racine fourni par l'entreprise en tant que source de confiance. Les utilisateurs doivent accepter le certificat et l'enregistrer dans la zone de stockage de l'autorité de certification racine de confiance pour qu'ils ne soient plus invités à le faire lorsqu'ils accèdent au site.

Remarque L'utilisateur doit accepter et faire confiance au certificat d'autorité de certification qui a créé le certificat de remplacement. S'ils font plutôt confiance au certificat du serveur de remplacement, ils continueront à voir des avertissements pour chaque site HTTPS qu'ils visitent.

Ajouter le certificat racine aux périphériques clients

Vous pouvez ajouter le certificat racine à tous les périphériques clients du réseau en tant qu'autorité de certification racine de confiance. De cette façon, les applications client acceptent automatiquement les transactions avec le certificat racine.

Vous pouvez soit rendre le certificat accessible aux utilisateurs en l'envoyant par courriel ou en le plaçant sur un site partagé, soit l'intégrer à l'image de votre poste de travail d'entreprise et utiliser les fonctions de mise à jour de votre application pour le distribuer automatiquement aux utilisateurs.

La procédure suivante explique comment télécharger le certificat d'autorité de certification interne et l'installer sur les clients Windows.

Procédure

Étape 1 Téléchargez le certificat à partir de Firepower Device Manager.

a) Select **Policies (politiques)** > **SSL Decryption**.

b) Cliquez sur le bouton **SSL Decryption Settings** ( ).

c) Cliquez maintenant sur le bouton **Download** pour procédez au téléchargement ( ).

d) Sélectionnez un emplacement de téléchargement, modifiez éventuellement le nom du fichier (mais pas l'extension), puis cliquez sur **Save** (enregistrer).

Vous pouvez maintenant annuler la boîte de dialogue SSL Decryption Settings (paramètres de déchiffrement SSL).

Étape 2 Installez le certificat dans la zone de stockage de l'autorité de certification racine de confiance dans les navigateurs Web sur les systèmes clients, ou mettez-le à la disposition des clients pour qu'ils l'installent eux-mêmes.

Le processus varie selon le système d'exploitation et le type de navigateur. Par exemple, vous pouvez utiliser le processus suivant pour Internet Explorer et Chrome fonctionnant sous Windows. (Pour Firefox, faites l'installation dans la page **Tools (outils)** > **Options (options)** > **Advanced (avancées)**.)

a) Dans le menu **Start** (démarrer), sélectionnez **Control Panel (panneau de configuration)** > **Internet Options (options Internet)**.
b) Sélectionnez l'onglet **Content** (contenu).
c) Cliquez sur le bouton **Certificates** pour ouvrir la boîte de dialogue des certificats.
d) Sélectionnez l'onglet **Trusted Root Certificate Authorities** (autorités de certification racine de confiance).
e) Cliquez sur **Import** (importer), puis suivez l'assistant pour localiser et sélectionner le fichier téléchargé (<uuid> _internalCA.crt) et ajoutez-le au magasin des autorités de certification racine de confiance (Trusted Root Certificate Authorities).
f) Cliquez sur **Finish** (Terminer).

   Les messages doivent indiquer que l'importation a réussi. Vous pourriez voir une boîte de dialogue intermédiaire vous avertir que Windows ne pourrait pas valider le certificat si vous avez généré un certificat autosigné plutôt que de l'obtenir auprès d'une autorité de certification tierce bien connue.

   Vous pouvez maintenant fermer les boîtes de dialogue Certificate et Internet Options.

Exemple : blocage des anciennes versions SSL/TLS du réseau

Certaines entreprises sont tenues d'empêcher l'utilisation d'anciennes versions de SSL ou de TLS en raison de la réglementation gouvernementale ou de la politique de l'entreprise. Vous pouvez utiliser la politique de déchiffrement SSL pour bloquer le trafic qui utilise une version SSL/TLS que vous interdisez. Il est conseillé de placer cette règle en haut de la politique de déchiffrement SSL pour vous assurer de détecter immédiatement le trafic interdit.

L'exemple suivant bloque toutes les connexions SSL 3.0 et TLS 1.0.

Avant de commencer

Cette procédure suppose que vous ayez déjà activé la politique de déchiffrement SSL, comme expliqué dans la section Activez la politique de déchiffrement SSL., à la page 9.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez sur le bouton **+** pour créer une nouvelle règle.

Étape 3 Dans Order (Ordre), sélectionnez **1** pour placer la règle en haut de la politique, ou sélectionnez le numéro le plus adapté à votre réseau.

La valeur par défaut consiste à ajouter la règle à la fin de la politique.

Étape 4 Dans **Title (Titre)**, saisissez un nom pour la règle, par exemple, Block_SSL3.0_and_TLS1.0.

Étape 5 Dans **Action**, sélectionnez **Block** (Bloquer). Cela abandonnera immédiatement tout trafic qui correspond à la règle.

Étape 6 Laissez les valeurs par défaut pour toutes les options sous les onglets suivants : **Source/Destination**, **Applications**, **URLs**, **Users** (utilisateurs).

Étape 7 Cliquez sur l'onglet **Advanced** (Avancé) et sous **Supported Versions** (Versions prises en charge), laissez SSL 3.0 et TLS 1.0 sélectionnés, mais décochez TLS 1.1, TLS 1.2, TLS 1.3.

Étape 8 (Facultatif) Cliquez sur l'onglet **Logging** (Journalisation) et sélectionnez **At End of Connection** (Événements de fin de connexion) si vous souhaitez que les tableaux de bord et les événements reflètent les connexions bloquées. Vous pouvez également sélectionner un serveur syslog externe si vous en utilisez un.

Étape 9 Cliquez sur **OK**.

Vous pouvez maintenant déployer la politique. Une fois déployée, toute connexion SSL 3.0 ou TLS 1.0 qui passe par le système sera abandonnée.

Remarque
Les connexions SSL 2.0 sont gérées par l'action par défaut pour la politique. Si vous souhaitez vous assurer qu'elles sont également abandonnées, modifiez l'action par défaut pour Block (Bloquer).

Prochaine étape

Si vous mettez en œuvre cette règle, nous avons les recommandations suivantes :

- Pour tout type de règle de déchiffrement, laissez les paramètres par défaut sous l'onglet Advanced (Avancé), où toutes les options SSL/TLS sont sélectionnées. En s'appliquant à toutes les versions, le processus d'établissement de liaison est simplifié. Cependant, votre règle de blocage initiale empêchera toujours les connexions SSL 3.0 et TLS 1.0.
- Nous vous recommandons normalement d'utiliser Ne pas déchiffrer comme action par défaut pour la politique. Cependant, comme les connexions SSL 2.0 sont toujours gérées par l'action par défaut, vous pouvez utiliser Block (Bloquer) à la place. Toutefois, si vous souhaitez appliquer la règle Ne pas déchiffrer comme action par défaut à tout le trafic déchiffrable, créez une règle Do Not Decrypt (Ne pas déchiffrer) à la fin de la politique où vous acceptez toutes les valeurs par défaut pour les critères de correspondance du trafic. Cette règle correspondrait à toute connexion TLS prise en charge qui ne correspond pas à une règle antérieure dans le tableau et servirait de règle par défaut pour ces versions TLS.

Surveillance et dépannage du déchiffrement SSL

Les rubriques suivantes expliquent comment surveiller et résoudre les politiques de déchiffrement SSL.

Surveillance du déchiffrement SSL

Vous pouvez afficher les renseignements sur le déchiffrement dans les tableaux de bord et les événements pour le trafic qui correspond aux règles (ou à l'action par défaut) pour lesquelles vous avez activé la journalisation.

Tableau de bord du déchiffrement SSL

Pour évaluer les statistiques globales de déchiffrement, consultez le tableau de bord **Monitoring (Surveillance)** > **SSL Decryption (Déchiffrement SSL)**. Le tableau de bord affiche les informations suivantes :

- Pourcentage du trafic chiffré par rapport au trafic en texte brut.
- La quantité du trafic chiffré est déchiffrée par les règles SSL.

Événements

En plus du tableau de bord, la visionneuse d'événements (**Monitoring (Surveillance)** > **Events (Événements)**) comprend des informations SSL pour le trafic chiffré. Voici quelques conseils pour évaluer les événements :

- Pour les connexions qui ont été abandonnées parce qu'elles correspondaient à une règle SSL (ou à une action par défaut) qui a bloqué le trafic correspondant, le champ **Action** doit être « Block » (Blocage) et le **Reason** (Motif) doit indiquer « SSL Block » (Blocage SSL).
- Le champ **SSL Actual Action (Action réelle SSL)** (Syslog : SSLActualAction) indique l'action réelle que le système a appliquée à la connexion. Cette valeur peut différer de **SSL Expected Action (Action SSL attendue)** (Syslog : SSLExpectedAction), qui indique l'action définie dans la règle de correspondance. Par exemple, une connexion peut correspondre à une règle qui applique le déchiffrement, mais qui n'a pas pu être déchiffrée pour une raison quelconque.

Gestion des sites Web où la règle Decrypt Re-sign (Déchiffrer-Resigner) fonctionne pour un navigateur mais pas pour une application (SSL ou épinglage d'autorité de certification)

Certaines applications pour téléphones intelligents et autres périphériques utilisent une technique appelée épinglage SSL (Autorité de certification). La technique d'épinglage SSL intègre le hachage du certificat de serveur d'origine dans l'application elle-même. Par conséquent, lorsque l'application reçoit le certificat résigné du périphérique Cisco Firewall Threat Defense, la validation du hachage échoue et la connexion est abandonnée.

Le principal signe est que les utilisateurs ne peuvent pas se connecter au site Web à l'aide de l'application du site, mais qu'ils peuvent se connecter à l'aide du navigateur Web, même s'ils utilisent le navigateur sur le même périphérique sur lequel l'application échoue. Par exemple, les utilisateurs ne peuvent pas utiliser l'application Facebook iOS ou Android, mais ils peuvent pointer Safari ou Chrome vers https://www.facebook.com et établir une connexion avec succès.

Comme l'épinglage SSL est spécifiquement utilisé pour éviter les attaques de l'homme du milieu, il n'y a pas de solution de contournement. Vous devez choisir entre les options suivantes :

- Prenez en charge les utilisateurs de l'application, auquel cas vous ne pouvez pas déchiffrer le trafic vers le site. Créez une règle Do Not Decrypt (Ne pas déchiffrer) pour l'application du site (sous l'onglet Application de la règle de déchiffrement SSL) et assurez-vous que la règle précède toute règle Decrypt Re-sign (Déchiffrer-resigner) qui s'appliquerait aux connexions.
- Forcez les utilisateurs à utiliser uniquement les navigateurs. Si vous devez déchiffrer le trafic vers le site, vous devrez informer les utilisateurs qu'ils ne peuvent pas utiliser l'application du site lorsqu'ils se connectent sur votre réseau et qu'ils doivent utiliser uniquement leur navigateur.

Renseignements complémentaires

Si un site fonctionne dans un navigateur mais pas dans une application sur le même périphérique, il s'agit presque certainement d'une instance d'épinglage SSL. Toutefois, si vous souhaitez approfondir la recherche

de la cause, vous pouvez utiliser des événements de connexion pour identifier l'épinglage SSL en plus du test du navigateur.

Une application peut gérer les échecs de validation du hachage de deux manières :

- Les applications du groupe 1, telles que Facebook, envoient un message d'alerte SSL dès qu'elles reçoivent le message CH, CERT ou SHD du serveur. L'alerte est généralement une alerte « Autorité de certification inconnue (48) » indiquant un épinglage SSL. Une réinitialisation TCP est envoyée après le message d'alerte. Vous devriez voir les symptômes suivants dans les détails de l'événement :
  - Les indicateurs de flux SSL incluent ALERT_SEEN.
  - Les indicateurs de flux SSL n'incluent pas APP_DATA_C2S ni APP_DATA_S2C.
  - Les messages de flux SSL sont généralement les suivants : CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.
- Les applications du groupe 2, comme Dropbox, n'envoient aucune alerte. Au lieu de cela, ils attendent la fin de la prise de contact, puis envoient une réinitialisation TCP. Vous devriez voir les symptômes suivants :
  - Les indicateurs de flux SSL n'incluent pas ALERT_SEEN, APP_DATA_C2S ou APP_DATA_S2C.
  - Les messages de flux SSL sont généralement les suivants : CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.

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.