Politiques de déchiffrement

Les rubriques suivantes donnent un aperçu de la création, de la configuration, de la gestion et de la journalisation des politiques de déchiffrement.

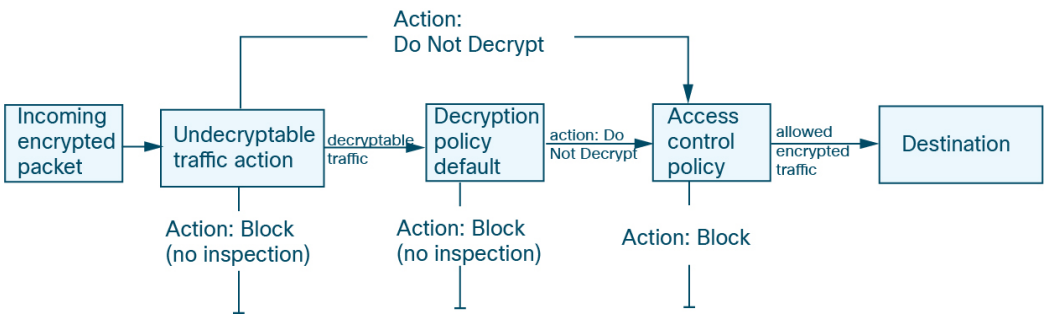
À propos des politiques de déchiffrement

U de déchiffrement détermine comment le système gère le trafic chiffré sur votre réseau. Vous pouvez configurer un ou plusieurs Politiques de déchiffrement, associer u de déchiffrement à une politique de contrôle d'accès, puis déployer la politique de contrôle d'accès sur un périphérique géré. Lorsque le périphérique détecte une prise de contact TCP, la politique de contrôle d'accès gère et inspecte d'abord le trafic. S'il identifie par la suite une session chiffrée TLS/SSLsur la connexion TCP, le politique de déchiffrement prend le relais, gère et déchiffre le trafic chiffré.

Vous pouvez créer plusieurs règles en même temps, y compris des règles pour déchiffrer le trafic entrant (action de règle **déchiffrer - clé connue**) et le trafic sortant (action de règle **Déchiffrer - Resigner**). Pour créer une règle **Ne pas déchiffrer** ou une autre action de règle (comme **Bloquer** ou **Surveiller**), créez une politique de déchiffrement vide et ajoutez la règle ensuite.

Pour commencer, consultez Créer une politique de déchiffrement, à la page 2.

Voici un exemple de politique de déchiffrement avec une action de règle **Ne pas déchiffrer** :



Le politique de déchiffrement le plus simple, comme le montre le diagramme suivant, dirige le périphérique là où il est déployé pour gérer le trafic chiffré avec une seule action par défaut. Vous pouvez définir l'action par défaut pour bloquer le trafic déchiffrable sans autre inspection, ou pour inspecter le trafic déchiffrable non déchiffré avec le contrôle d'accès. Le système peut alors autoriser ou bloquer le trafic chiffré. Si le périphérique détecte du trafic non déchiffrable, il bloque le trafic sans autre inspection ou ne le déchiffre pas, en l'inspectant avec le contrôle d'accès.

Exigences et conditions préalables pour les Politiques de déchiffrement

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Créer une politique de déchiffrement

Cette rubrique explique comment créer une politique de déchiffrement et, éventuellement, une ou plusieurs règles pour protéger les serveurs internes ou externes. Vous pouvez également créer une politique de déchiffrement sans règles et ajouter les règles ultérieurement. La création d'une politique vide est un bon choix pour créer des règles avec des actions de règle **Ne pas déchiffrer**, **Bloquer**, **Bloquer avec réinitialisation** ou **Surveiller**.

Avant de commencer

Passez en revue vos besoins en matière de déchiffrement:

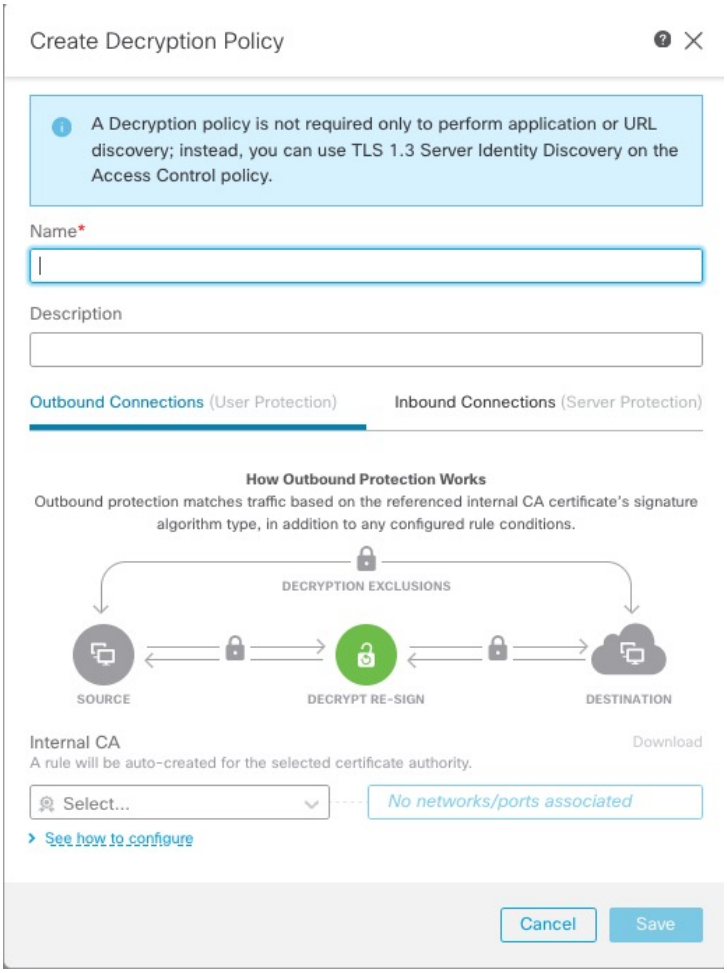
- Le déchiffrement est un moyen d'exposer le trafic réseau à une inspection approfondie; cependant, il y a des cas où vous ne devez *pas* déchiffrer le trafic : Quand déchiffrer le trafic et quand ne pas le déchiffrer.
- Pour protéger les serveurs *internes* en déchiffrant et en inspectant éventuellement le trafic, vous devez avoir le certificat interne pour votre serveur interne : ICP.
- Pour protéger les serveurs *externes* en déchiffrant et éventuellement en inspectant le trafic, vous devez téléverser un objet autorité de certification interne qui sera utilisé pour déchiffrer et démissionner du trafic : ICP.

Procédure

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

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

Étape 3 Saisissez un nom pour la politique dans le champ **Name** (nom) et une description facultative dans le champ **Description**.



La page à onglet **Outbound Connections** (connexions sortantes) vous permet de créer des règles **Déchiffrer - Resigner**. Ces règles nécessitent un certificat interne. Vous pouvez soit créer au préalable (à l'aide de **Objets** > **Gestion des objets** > **PKI** > **Autorités de certification internes**) ou les créer dans le cadre de la règle de connexion sortante.

la page à onglet **Inbound Connections (connexions entrantes)** vous permet de créer des règles **Déchiffrer - Clé connue**. Ces règles nécessitent un certificat interne que vous pouvez créer au préalable (à l'aide d'un **Objets** > **Gestion des objets** > **PKI** > **Certifications internes**) ou que vous pouvez créer dans le cadre de la règle de connexion entrante.

Étape 4 Associer la règle de déchiffrement à une règle de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès.

Étape 5 Poursuivre avec l'une des sections suivantes.

Prochaines étapes

Créer une politique de déchiffrement avec protection de la connexion sortante

Cette tâche explique comment créer une politique de déchiffrement avec une règle qui protège les connexions sortantes. c'est-à-dire que le serveur de destination se trouve à l'extérieur de votre réseau protégé. Ce type de règle possède une action de règle **Déchiffrer – Resigner**.

Lorsque vous créez une politique de déchiffrement, vous pouvez créer plusieurs règles en même temps, y compris plusieurs règles **Déchiffrer - Clé connue** et plusieurs règles **Déchiffrer - Resigner**.

Avant de commencer

Vous devez téléverser une autorité de certification (CA) interne pour votre serveur sortant avant de pouvoir créer une politique de déchiffrement qui protège les connexions sortantes. Vous pouvez le faire de l'une des manières suivantes :

- Créer un objet autorité de certification interne en accédant à **Objets** > **Gestion des objets** > **PKI** > **Autorités de certification internes** et en vous reportant à ICP.
- Lorsque vous créez la politique de déchiffrement.

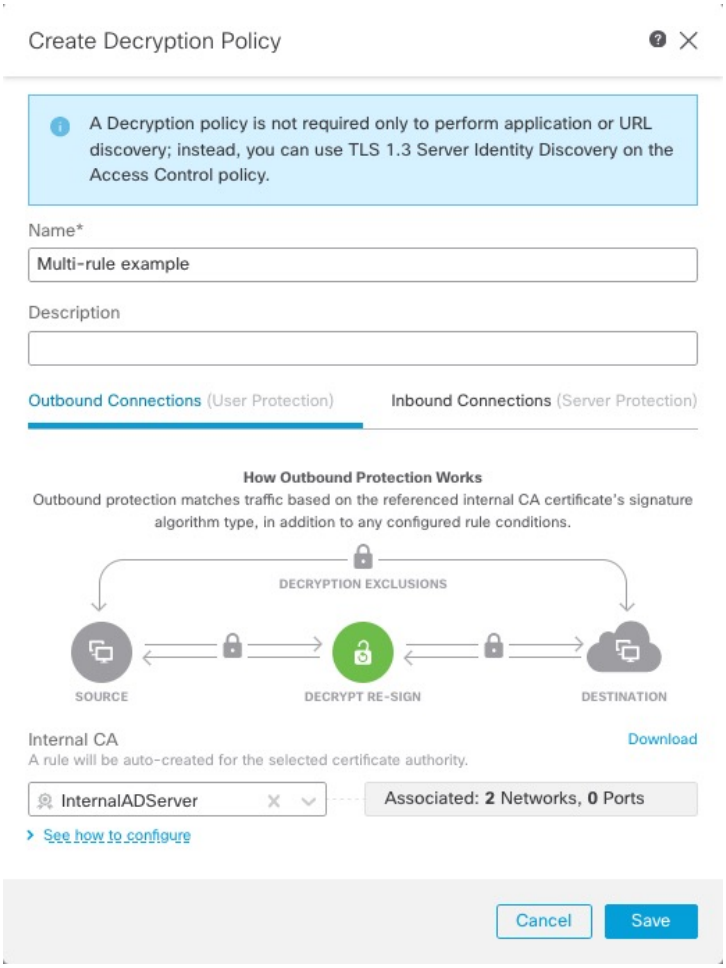
Procédure

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

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

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

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



Étape 5 Téléversez ou choisissez des certificats pour les règles.

Le système crée une règle par certificat.

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

Pour en savoir plus :

- Conditions de la Règle de déchiffrement
- Conditions des règles de réseau
- Conditions de règle de port

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

Prochaine étape

- Ajouter des conditions de règles Conditions de la Règle de déchiffrement
- Ajouter une action de politique par défaut : Actions par défaut Politique de déchiffrement, à la page 10

- Configurez les options de journalisation pour l'action par défaut, .
- Définissez les propriétés de politique avancées : Options avancées de Politique de déchiffrement, à la page 13.
- Associer politique de déchiffrement à une politique de contrôle d'accès, comme décrit dans Association d'autres politiques au contrôle d'accès.
- Déployer les changements de configuration.

Téléverser une autorité de certification interne pour la protection du trafic sortant

Cette tâche explique comment télécharger une autorité de certification interne lorsque vous créez une règle de déchiffrement qui protège les connexions sortantes. Vous pouvez également télécharger l'autorité de certification interne en utilisant **Objects (objets)** > **Object Management (gestion des objets)**, comme indiqué dans Importation d'un certificat d'autorité de certification et d'une clé privée.

Avant de commencer

Assurez-vous de disposer d'une autorité de certification interne dans l'un des formats décrits dans Objets Autorité de certification interne.

Procédure

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

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

Étape 3 Saisissez un nom pour la politique dans le champ **Name** (nom) et une description facultative dans le champ **Description**.

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

Étape 5 Dans la liste **Internal CA** (autorité de certification interne), cliquez sur **Create New** > **Upload CA** (créer une nouvelle autorité de certification, la téléverser).

Étape 6 Attribuez un **Nom** à l'autorité de certification interne.

Étape 7 Collez ou recherchez le certificat et sa clé privée dans les champs prévus à cet effet.

Étape 8 Si l'autorité de certification possède un mot de passe, cochez la case **Encrypted** (chiffré) et saisissez le mot de passe dans le champ adjacent.

Générer une autorité de certification interne pour la protection du trafic sortant

Cette tâche explique comment vous pouvez générer facultativement une autorité de certification interne lorsque vous créez une règle de déchiffrement qui protège les connexions sortantes. Vous pouvez également effectuer ces tâches à l'aide de **Objects (objets)** > **Object Management (gestion des objets)**, comme indiqué dans Téléversement d'un certificat signé émis en réponse à une requête de signature de certificat (CSR).

Avant de commencer

Assurez-vous de comprendre les exigences de génération d'un objet d'autorité de certification interne, comme indiqué dans le Objets Autorité de certification interne.

Procédure

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

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

Étape 3 Saisissez un nom pour la politique dans le champ **Name** (nom) et une description facultative dans le champ **Description**.

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

Étape 5 Dans la liste **Internal CA** (autorité de certification interne), cliquez sur **Create New** > **Generate CA** (générer une nouvelle autorité de certification).

Étape 6 Attribuez un **nom** à l'autorité de certification interne et indiquez un **nom de pays** à deux lettres.

Étape 7 Cliquez sur **Self-Signed** (Auto-signé) ou **CSR**.

Pour en savoir plus sur ces options, consultez Objets Autorité de certification interne.

Étape 8 Saisissez les renseignements demandés dans les champs prévus à cet effet.

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

Étape 10 Si vous avez choisi **CSR**, une fois la demande de signature terminée, cliquez sur **Install Certificate** (Installer le certificat) comme suit :

a) Répétez les étapes précédentes de cette procédure.

b) Modifiez l'autorité de certification dans la liste des **autorités de certification interne** comme suit.

c) Cliquez sur **Install Certificate** (Installer le certificat).

d) Suivez les instructions à l'écran pour terminer la tâche.

Créer une politique de déchiffrement avec protection de connexion entrante

Cette tâche explique comment créer une politique de déchiffrement avec une règle qui protège les connexions entrantes. c'est-à-dire que le serveur de destination se trouve dans votre réseau protégé. Ce type de règle possède une action de règle **Déchiffrer – Clé connue**.

Lorsque vous créez une politique de déchiffrement, vous pouvez créer plusieurs règles en même temps, y compris plusieurs règles **Déchiffrer - Clé connue** et plusieurs règles **Déchiffrer - Resigner**.

Avant de commencer

Vous devez télécharger un certificat interne pour votre serveur interne avant de pouvoir créer une politique de déchiffrement qui protège les connexions entrantes. Vous pouvez le faire de l'une des manières suivantes :

- Créez un objet de certificat interne en accédant à **Objets** > **Gestion des objets** > **PKI** > **Certifications internes** et en vous référant à ICP.

- Lorsque vous créez la politique de déchiffrement.

Procédure

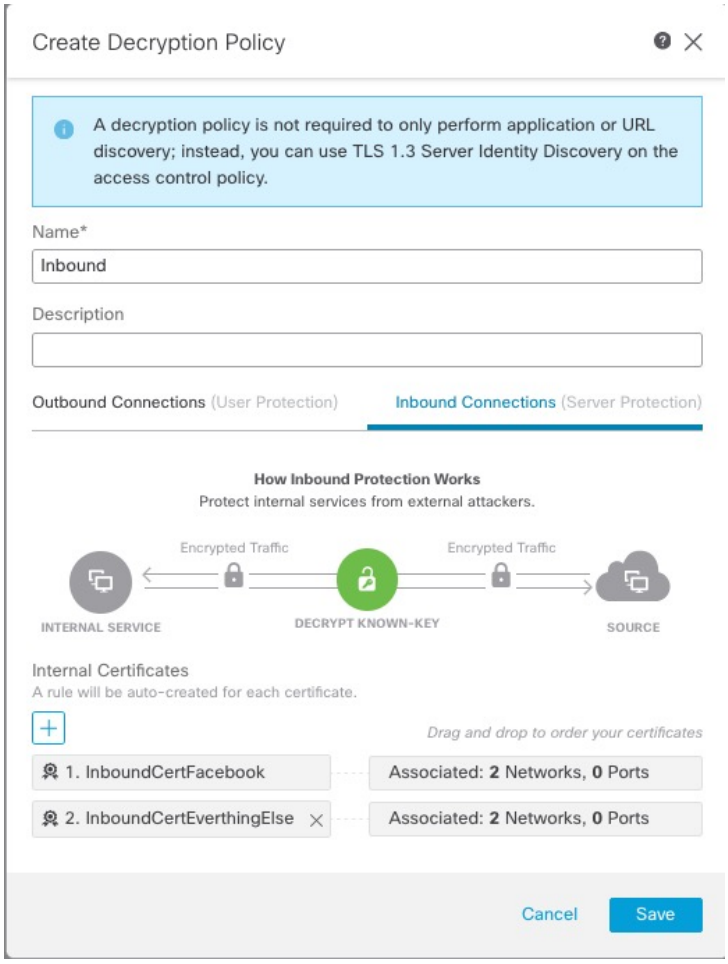
Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Firewall Management Center** > **Politiques** > **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 3 Cliquez sur **New Policy** (Nouvelle politique).

Étape 4 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 5 Cliquez sur l'onglet **Inbound Connections** (Connexions entrantes).



Étape 6 Téléversez ou choisissez des certificats pour les règles.

Le système crée une règle par certificat.

Étape 7 (Facultatif) Choisissez des réseaux et des ports.

Pour en savoir plus :

- Conditions de la Règle de déchiffrement

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

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Ajouter des conditions de règles Conditions de la Règle de déchiffrement
- Ajouter une action de politique par défaut : Actions par défaut Politique de déchiffrement, à la page 10
- Configurez les options de journalisation pour l'action par défaut,.
- Définissez les propriétés de politique avancées : Options avancées de Politique de déchiffrement, à la page 13.
- Associer politique de déchiffrement à une politique de contrôle d'accès, comme décrit dans Association d'autres politiques au contrôle d'accès.
- Déployer les changements de configuration.

Créer une politique de déchiffrement avec d'autres actions de règles

Pour créer une règle de déchiffrement avec une action de règle **Ne pas déchiffrer**, **Bloquer**, **Bloquer avec réinitialisation** ou **Surveiller**, créez une politique de déchiffrement et modifiez la politique pour ajouter la règle.

Lorsque vous créez une politique de déchiffrement, vous pouvez créer plusieurs règles en même temps, y compris plusieurs règles **Déchiffrer - Clé connue** et plusieurs règles **Déchiffrer - Resigner**.

Procédure

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

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

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

Étape 4 Cliquez sur **Edit** () à côté du nom de la politique de déchiffrement.

Étape 5 Cliquez sur **Add Rule** (ajouter une règle).

Étape 6 Attribuez un nom à la règle.

Étape 7 Dans la liste **Action**, cliquez sur une action de règle et consultez l'une des sections suivantes pour obtenir plus d'informations :

- Action Ne pas déchiffrer de la Règle de déchiffrement
- Actions de blocage de Règle de déchiffrement
- Action Monitor (Surveiller) de Règle de déchiffrement

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Ajouter des conditions de règles Conditions de la Règle de déchiffrement
- Ajouter une action de politique par défaut : Actions par défaut Politique de déchiffrement, à la page 10
- Configurez les options de journalisation pour l'action par défaut, .
- Définissez les propriétés de politique avancées : Options avancées de Politique de déchiffrement, à la page 13.
- Associer politique de déchiffrement à une politique de contrôle d'accès, comme décrit dans Association d'autres politiques au contrôle d'accès.
- Déployer les changements de configuration.

Actions par défaut Politique de déchiffrement

L'action par défaut de u de déchiffrement détermine la façon dont le système gère le trafic chiffré déchiffrable qui ne correspond à aucune règle sans surveillance dans la politique. Lorsque vous déployez un u de déchiffrement qui ne contient aucun règles de déchiffrement, l'action par défaut détermine la façon dont tout le trafic déchiffrable est géré sur votre réseau. Notez que le système n'effectue aucun type d'inspection sur le trafic chiffré bloqué par l'action par défaut.

Pour définir l'action par défaut politique de déchiffrement :

1. Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.
2. Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.
3. Cliquez sur **Edit** (✎) à côté de politique de déchiffrement.
4. Sur la ligne Default Action (action par défaut), cliquez sur l'une des actions suivantes dans la liste.

Tableau 1 : Actions par défaut Politique de déchiffrement

Action par défaut	Incidence sur le trafic chiffré
Bloquer	Bloquer la session TLS/SSL sans autre inspection.
Bloc avec action de réinitialisation	Bloquez la session TLS/SSL sans autre inspection et réinitialisez la connexion TCP. Choisissez cette option si le trafic utilise un protocole sans connexion comme UDP. Dans ce cas, le protocole sans connexion tente de rétablir la connexion jusqu'à ce qu'il soit réinitialisé. Cette action affiche également une erreur de réinitialisation de connexion dans le navigateur pour informer l'utilisateur que la connexion est bloquée.
Ne pas déchiffrer	Inspecter le trafic chiffré à l'aide du contrôle d'accès.

Options de traitement par défaut du trafic non déchiffrable

Tableau 2 : Types de trafic non déchiffrables

Type	Description	Action par défaut	Action disponible
Session compressée	La session TLS/SSL applique une méthode de compactage de données.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Session SSLv2	La session est chiffrée avec SSL version 2. Notez que le trafic est déchiffrable si le message ClientHello est SSL 2.0 et si le reste du trafic transmis est en SSL 3.0.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Suite de chiffrement inconnue	Le système ne reconnaît pas la suite de chiffrement.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Suite de chiffrement non prise en charge	Le système ne prend pas en charge le déchiffrement basé sur la suite de chiffrement détectée.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Session non mise en mémoire cache	La session TLS/SSL a activé la réutilisation de session, 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.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut

Type	Description	Action par défaut	Action disponible
Erreurs de connexion	Une erreur s'est produite lors de la négociation de l'établissement de liaison TLS/SSL.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Erreurs de déchiffrement	Une erreur est survenue lors du déchiffrement du trafic.	Bloquer	Bloquer Bloquer avec réinitialisation

Lorsque vous créez u de déchiffrement pour la première fois, la journalisation des connexions gérées par l'action par défaut est désactivée par défaut. Comme les paramètres de journalisation pour l'action par défaut s'appliquent également à la gestion du trafic non déchiffrable, la journalisation des connexions gérées par les actions de trafic non déchiffrable est désactivée par défaut.

Notez que si votre navigateur utilise l'épinglage de certificat pour vérifier un certificat de serveur, vous ne pouvez pas déchiffrer ce trafic en signant de nouveau le certificat de serveur. Pour obtenir plus de renseignements, consultez Lignes directrices et limites relatives à Règle de déchiffrement.

Sujets connexes

Définir le traitement par défaut pour le trafic non déchiffrable, à la page 12

Définir le traitement par défaut pour le trafic non déchiffrable

Vous pouvez définir des actions de trafic non déchiffrable au niveau politique de déchiffrement pour gérer certains types de trafic chiffré que le système ne peut pas déchiffrer ou inspecter. Lorsque vous déployez un u de déchiffrement qui ne contient pas de règles de déchiffrement, les actions relatives au trafic indéchiffrable déterminent la façon dont tout le trafic chiffré non déchiffrable est géré sur votre réseau.

Selon le type de trafic déchiffrable, vous pouvez choisir de :

- Bloquer la connexion.
- Bloquez la connexion, puis réinitialisez-la. Cette option est préférable pour les protocoles sans connexion comme UDP, qui continuent d'essayer de se connecter jusqu'à ce que la connexion soit bloquée.
- Inspecter le trafic chiffré à l'aide du contrôle d'accès.
- Héritage de l'action par défaut de politique de déchiffrement.

Procédure

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

Étape 2 Cliquez sur **Edit** (✎) à côté de politique de déchiffrement.

Étape 3 Dans l'éditeur politique de déchiffrement, cliquez sur **Undecryptable Actions**(Actions indéchiffrables).

Étape 4 Pour chaque champ, choisissez l'action par défaut de politique de déchiffrement ou une autre action que vous souhaitez appliquer au type de trafic déchiffrable. Reportez-vous à Options de traitement par défaut du trafic non déchiffrable, à la page 11 et à Actions par défaut Politique de déchiffrement, à la page 10 pour en savoir davantage.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- configurer la journalisation par défaut pour les connexions gérées par les actions de trafic non déchiffrable.
- Déployer les changements de configuration.

Options avancées de Politique de déchiffrement

La page **Paramètres avancés** de U de déchiffrement contient des paramètres globaux qui sont appliqués à tous les périphériques gérés configurés pour Snort 3 auxquels la politique est appliquée.

Les paramètres avancés U de déchiffrement sont tous ignorés sur tout périphérique géré qui exécute :

- Toute version antérieure à la 7.1.
- Snort 2

Bloquer les flux demandant ESNI

L'indication du nom de serveur chiffré (ESNI (lien vers le projet de proposition)) est un moyen pour un client d'indiquer à un serveur TLS 1.3 ce que le client demande. Comme le SNI est chiffré, vous pouvez éventuellement bloquer ces connexions, car le système ne peut pas déterminer le serveur.

Désactiver les annonces HTTP/3

Cette option supprime HTTP/3 (RFC 9114) de ClientHello dans les connexions TCP. HTTP/3 fait partie du protocole de transport QUIC, et non du protocole de transport TCP. Empêcher les clients de faire de la publicité HTTP/3 offre une protection contre les attaques et les tentatives d'évitement potentiellement englouties dans les connexions QUIC.

Propager les certificats de serveur non sécurisé aux clients

Cela s'applique uniquement au trafic correspondant à une action de règle **Déchiffrer - Resigner**.

Activez cette option pour remplacer le certificat du serveur par l'autorité de certification (CA) sur le périphérique géré dans les cas où le certificat du serveur n'est pas fiable. Un *certificat* de serveur non fiable n'est pas répertorié comme autorité de certification de confiance dans Cisco Secure Firewall Management Center. (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**).

Activer le déchiffrement TLS 1.3

Indiquer s'il faut appliquer les règles de déchiffrement aux connexions TLS 1.3. Si vous n'activez pas cette option, les règles de déchiffrement s'appliquent uniquement au trafic TLS 1.2 ou de version inférieure. Consultez Bonnes pratiques de déchiffrement TLS 1.3, à la page 14.

Activer la sonde d'identité du serveur TLS adaptatif

Activé automatiquement lorsque le déchiffrement TLS 1.3 est activé. Une *sonde* est une connexion partielle de TLS avec le serveur, dont le but est d'obtenir le certificat du serveur et de le mettre en cache. (Si le certificat est déjà en cache, la sonde n'est jamais établie.)

Si la découverte de l'identité du serveur TLS 1.3 est désactivée sur la politique de contrôle d'accès à laquelle la politique de déchiffrement est associée, nous tentons d'utiliser l'indication du nom du serveur (SNI), qui n'est pas aussi fiable.

La sonde d'identité du serveur TLS adaptatif se produit dans l'une des conditions suivantes, et non à chaque connexion comme dans les versions précédentes :

- Émetteur du certificat : correspond lorsque la valeur **DN de l'émetteur** dans la condition de règle de DN d'une règle de déchiffrement est mise en correspondance.

  Pour en savoir plus, consultez Conditions de règles de noms distinctifs (DN).

- État du certificat : correspond lorsque l'une des conditions **d'état du certificat** est satisfaite dans une règle de déchiffrement.

  Pour en savoir plus, consultez Conditions de Règle de déchiffrement d'état du certificat.

- Certificat interne/externe : les certificats internes peuvent correspondre au certificat utilisé dans les actions de règle **Déchiffrer - Clé connue** ; les certificats externes peuvent être mis en correspondance dans les conditions de règle **Certificats**.

  Pour plus de renseignements, consultez les sections Déchiffrement par clé connue (trafic entrant) et Conditions de Règle de déchiffrement du certificat.

- ID d'application : peut correspondre aux conditions de règle des **applications** dans une politique de contrôle d'accès ou une politique de déchiffrement.

  Pour en savoir plus, consultez Conditions des règles d'application.

- Catégorie d'URL : Peut correspondre aux conditions de règle d'**URL** dans une politique de contrôle d'accès.

  Pour en savoir plus, consultez Conditions de règle d'URL.

Remarque **L'activation du mode de découverte de serveur TLS adaptatif** n'est prise en charge sur aucun Cisco Secure Firewall Threat Defense Virtual déployé sur AWS. Si de tels périphériques gérés sont gérés par Cisco Secure Firewall Management Center, l'événement de connexion **PROBE_FLOW_DROP_BYPASS_PROXY** est incrémenté chaque fois que le périphérique tente d'extraire le certificat du serveur.

Bonnes pratiques de déchiffrement TLS 1.3

Recommandation : Quand activer les options avancées?

decryption policy (politique de déchiffrement) et la politique de contrôle d'accès comportent tous deux des options avancées qui affectent la façon dont le trafic est géré, qu'il soit déchiffré ou non.

Les options avancées sont les suivantes :

- Politique de déchiffrement :

- Déchiffrement TLS 1.3
- Sonde d'identité du serveur TLS adaptatif

- Politique de contrôle d'accès : découverte de l'identité du serveur TLS 1.3

  Le paramètre de politique de contrôle d'accès est prioritaire sur le paramètre de politique de déchiffrement.

Utilisez le tableau suivant pour décider quelle option activer :

Paramètre de la sonde d'identité du serveur adaptatif TLS (politique de déchiffrement)	Paramètre de découverte de l'identité du serveur TLS 1.3 (politique de contrôle d'accès)	Résultat	Recommandé quand
Activé	Désactivé	La sonde adaptative est envoyée si la politique de déchiffrement contient *des* conditions de règle spécifiées dans Options avancées de Politique de déchiffrement, à la page 13 *et* si le certificat de serveur n'est pas mis en cache.	• Vous n'utilisez pas les conditions d'application ou d'URL dans les règles de contrôle d'accès • Vous déchiffrez le trafic
Activé	Activé	La sonde est toujours envoyée si le certificat du serveur n'est pas mis en cache.	À utiliser uniquement si vos règles de contrôle d'accès ont des conditions d'URL ou d'application
Désactivé	Activé	La sonde est toujours envoyée si le certificat du serveur n'est pas mis en cache.	non recommandée
Désactivé	Désactivé	La sonde n'est jamais envoyée.	Utilité très limitée; à utiliser uniquement si le trafic n'est pas déchiffré et si les conditions d'application ou d'URL ne sont pas utilisées dans la règle de contrôle d'accès

Remarque Un certificat de serveur TLS en cache est disponible pour toutes les instances Snort sur un défense contre les menaces spécifique. Le cache peut être effacé à l'aide d'une commande CLI et est automatiquement effacé au redémarrage du périphérique.

Numéro de référence

Pour en savoir plus, consultez l'explication de la découverte d'identité du serveur TLS sur secure.cisco.com.

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.