Présentation du déchiffrement du trafic

Les rubriques suivantes fournissent une présentation de l'inspection de Transport Layer Security/Secure sockets (TLS/SSL), traitent des conditions préalables à la configuration de l'inspection TLS/SSL et détaillent les scénarios de déploiement.

Remarque Comme TLS et SSL sont souvent utilisés de manière interchangeable, nous utilisons l'expression *TLS/SSL* pour indiquer que l'un ou l'autre des protocoles est l'objet de la discussion. Le protocole SSL a été déconseillé par l'IETF au profit du protocole TLS plus sécurisé. Vous pouvez donc interpréter le protocole *TLS/SSL* comme faisant uniquement référence à TLS.

Pour en savoir plus sur les protocoles SSL et TLS, consultez une ressource comme SSL ou TLS - What's the Difference?

Explication du déchiffrement du trafic

La majeure partie du trafic Internet est chiffrée et, dans la plupart des cas, vous ne souhaitez pas le déchiffrer; Même si vous ne le faites pas, vous pouvez toujours obtenir des informations à ce sujet et les bloquer de votre réseau si nécessaire.

Les options sont :

- Déchiffrez le trafic et soumettez-le à tout l'éventail d'inspections approfondies :
  - protection améliorée contre les logiciels malveillants
  - Renseignements de sécurité
  - Threat Intelligence Director (directeur des informations sur les menaces)
  - Détecteurs d'applications

- Filtrage par URL et par catégories

- Laissez le trafic chiffré et configurez votre contrôle d'accès et politique de déchiffrement pour rechercher et éventuellement bloquer :
  - Des anciennes versions de protocole (comme le protocole SSL)
  - Des suites de chiffrement non sécurisées
  - Des applications présentant un risque élevé et une faible pertinence commerciale
  - Des noms distinctifs d'émetteur non fiable

Une politique de contrôle d'accès est la configuration principale qui appelle les sous-politiques et d'autres configurations, y compris un politique de déchiffrement. Si vous associez un politique de déchiffrement au contrôle d'accès, le système utilise ce politique de déchiffrement pour gérer les sessions chiffrées avant d'évaluer les sessions avec des règles de contrôle d'accès. Si vous ne configurez pas l'inspection TLS/SSL, ou si vos périphériques ne la prennent pas en charge, les règles de contrôle d'accès gèrent tout le trafic chiffré.

Les règles de contrôle d'accès gèrent également le trafic chiffré lorsque votre configuration d'inspection TLS/SSL permet au trafic de passer. Cependant, certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, de sorte que le trafic chiffré peut correspondre à moins de règles. En outre, par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès configurée pour l'inspection des intrusions et des fichiers.

Même si vos politiques n'exigent pas le déchiffrement du trafic, nous recommandons le *déchiffrement sélectif* comme bonne pratique. En d'autres termes, vous devez configurer certains règles de déchiffrement pour rechercher les applications, les suites de chiffrement et les protocoles non sécurisés indésirables. Ces types de règles n'exigent pas le déchiffrement des données du trafic, seulement assez pour déterminer si le trafic comporte ces caractéristiques indésirables.

Notes

Configurez des règles de déchiffrement *uniquement* si votre périphérique géré gère le trafic chiffré. Les Règles de déchiffrement nécessitent une surcharge de traitement qui peut avoir un impact sur les performances.

Tant que Snort 3 est activé sur vos périphériques gérés, le système prend en charge le déchiffrement du trafic TLS 1.3. Vous pouvez activer le déchiffrement TLS 1.3 dans les options avancées de politique de déchiffrement. pour en savoir plus, consultez Options avancées de Politique de déchiffrement.

Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 11 et Déchiffrement par clé connue (trafic entrant), à la page 12.

Si vous définissez la valeur de la taille de segment maximale (MSS) TCP à l'aide de FlexConfig, la MMS observée pourrait être inférieure à votre paramètre. Pour en savoir plus, consultez À propos de TCP MSS.

Sujets connexes

Traitement d'établissement de liaison TLS/SSL, à la page 3
Bonnes pratiques de TLS/SSL, à la page 8

Traitement d'établissement de liaison TLS/SSL

Dans cette documentation, le terme « établissement de *liaison TLS/SSL* » représente l'établissement de liaison bidirectionnelle qui lance les sessions chiffrées dans le protocole SSL et dans le protocole qui lui succède, TLS.

Dans un déploiement en ligne, le système Firepower traite l'établissement de liaison TLS/SSL, ce qui modifie potentiellement le message ClientHello et agit comme un serveur mandataire TCP pour la session.

La figure suivante montre un déploiement en ligne.

Une fois que le client a établi une connexion TCP avec le serveur (après avoir terminé avec succès l'établissement de la liaison TCP tridirectionnelle), le périphérique géré surveille la session TCP à la recherche de toute tentative d'ouverture d'une session chiffrée. L'établissement de liaison TLS/SSL établit une session chiffrée à l'aide de l'échange de paquets spécialisés entre le client et le serveur. Dans les protocoles SSL et TLS, ces paquets spécialisés sont appelés *messages d'établissement de liaison*. Les messages d'établissement de liaison communiquent les attributs de chiffrement pris en charge par le client et le serveur:

- ClientHello : le client spécifie plusieurs valeurs prises en charge pour chaque attribut de chiffrement.
- ServerHello : le serveur spécifie une valeur unique prise en charge pour chaque attribut de chiffrement, et la réponse de ServerHello détermine la méthode de chiffrement utilisée par le système pendant la session sécurisée.

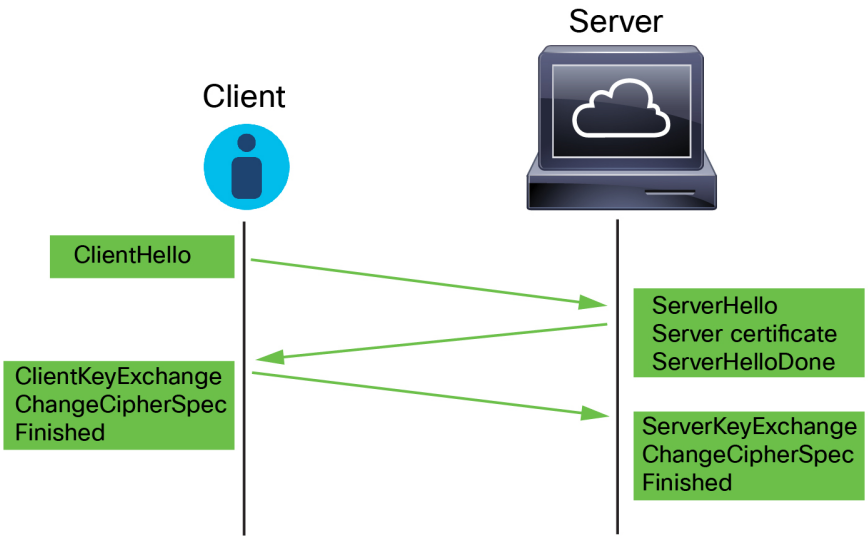
À la fin de l'établissement d'une liaison TLS/SSL, le périphérique géré met en cache les données de session chiffrées, ce qui permet la reprise de la session sans nécessiter l'établissement d'une liaison complète. Le périphérique géré met également en cache les données de certificat du serveur, ce qui accélère le traitement de l'établissement de liaison lors des sessions suivantes qui utilisent le même certificat.

Gestion des messages ClientHello

Le client envoie le message ClientHello au serveur qui sert de destination des paquets si une connexion sécurisée peut être établie. Le client envoie le message pour initier l'établissement de liaison TLS/SSL ou en réponse à un message ServerHello du serveur de destination.

Aperçu

La figure suivante présente un exemple. Voir également RFC 8446, sec. 4 . Vous pouvez également consulter une ressource comme Que se passe-t-il lors de l'établissement de liaison TLS? sur cloudflare.com.



Le processus peut être résumé comme suit :

1. ClientHello lance le processus.

   Le message ClientHello contient l'indicateur du nom du serveur (SNI), qui comporte le nom de domaine complet du serveur.

2. Lorsqu'un périphérique géré a traité un message ClientHello et l'a transmis au serveur de destination, ce dernier détermine s'il prend en charge les attributs de déchiffrement spécifiés dans le message. S'il ne prend pas en charge ces attributs, le serveur envoie une alerte d'échec d'établissement de liaison au client. S'il prend en charge ces attributs, le serveur envoie le message ServerHello. Si la méthode d'échange de clés convenue utilise des certificats pour l'authentification, le message de certificat du serveur suit immédiatement le message ServerHello.

   Le certificat du serveur contient le Subject Alternative Name (SAN), qui peut avoir des noms de domaine et des adresses IP complets. Pour plus d'informations sur SAN, consultez Nom distinctif.

3. Lorsque le périphérique géré reçoit ces messages, il tente de les mettre en correspondance avec les règles de déchiffrement configurés sur le système. Ces messages contiennent des informations qui étaient absentes du message ClientHello ou du cache de données de session. Plus précisément, le système peut mettre en correspondance ces messages aux conditions de règles de déchiffrement, état du certificat, suites de chiffrement et versions.

L'ensemble du processus est chiffré.

Échange de données

Si vous configurez le déchiffrement de TLS/SSL, lorsqu'un périphérique géré reçoit un message ClientHello, le système tente de faire correspondre le message à règles de déchiffrement qui a l'action **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue**. La correspondance repose sur les données du message ClientHello et des données de certificat du serveur en cache. Les données possibles comprennent :

Tableau 1 : Disponibilité des données pour les conditions Règle de déchiffrement

Condition Règle de déchiffrement	Données présentes
Zones	ClientHello

Condition Règle de déchiffrement	Données présentes
Réseaux	ClientHello
Balises VLAN	ClientHello
Ports	ClientHello
Utilisateurs	ClientHello
Applications	ClientHello (extension de l'indicateur de nom de serveur)
Catégories	ClientHello (extension de l'indicateur de nom de serveur)
Certificate (certificat)	Certificat du serveur (éventuellement en cache)
Noms distinctifs	Certificat du serveur (éventuellement en cache)
État du certificat	Certificat du serveur (éventuellement en cache)
Suites de chiffrement	ServerHello
Versions	ServerHello

Remarque Utilisez les conditions de règle **Suite de chiffrement** et **version** *uniquement* dans les règles avec l'action de règle **Bloquer** ou **Bloquer avec réinitialisation**. L'utilisation de ces conditions dans des règles avec d'autres actions liées à des règles peut interférer avec le traitement ClientHello du système, ce qui entraîne un rendement imprévisible.

Modifications de ClientHello

Si le message ClientHello correspond à une règle **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue** , le système modifie le message ClientHello comme suit :

- (TLS 1.2 uniquement; TLS 1.3 ne prend pas en charge la compression.) Compression méthodes : supprime l'élément `compression_methods`, qui spécifie les méthodes de compression prises en charge par le client. Le système ne peut pas déchiffrer les sessions compressées.
- Suites de chiffrement :: supprime les suites de chiffrement de l'élément `cipher_suites` si le système ne les prend pas en charge. S'il ne prend en charge aucune des suites de chiffrement précisées, le système transmet l'élément d'origine non modifié. Cette modification réduit les types de trafic non déchiffrable de la Suite de chiffrement inconnue et de la Suite de chiffrement non prise en charge.
- Identifiants de session : supprime toute valeur de l'élément `Session Identifier` et de l'extension SessionTicket (RFC 5077, sec 3.2) qui ne correspond pas aux données de session mises en cache. Si une valeur ClientHello correspond aux données en cache, une session interrompue peut reprendre sans que le client et le serveur effectuent l'établissement de liaison TLS/SSL complet. Cette modification augmente les chances de reprise de session et réduit le trafic non déchiffrable de type Session non mise en cache.

- Courbes elliptiques : supprime les courbes elliptiques de l'extension Courbes elliptiques prises en charge si le système ne les prend pas en charge. Si le système ne prend en charge aucune des courbes elliptiques spécifiées, le périphérique géré supprime l'extension et élimine toutes les suites de chiffrement connexes de l'élément `cipher_suites`.
- Extensions ALPN : supprime toute valeur de l'extension ALPN (Application-Layer Protocol Negotiation) qui n'est pas prise en charge dans le système (par exemple, le protocole HTTP/2).
- Autres extensions : supprime les extensions Next Protocol Negotiation (NPN) et les ID de canal TLS.

  Les règles de déchiffrement avec une action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** prennent désormais en charge de manière native l'extension SME (Extended Master Secret) lors de la négociation ClientHello, permettant des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627.

Une fois que le système a modifié le message ClientHello, il détermine si le message réussit l'évaluation de contrôle d'accès (qui peut inclure une inspection approfondie). Si le message passe cette évaluation avec succès, le système le transmet au serveur de destination.

Si le message ClientHello ne correspond *pas* à une règle **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue** , le système ne modifie pas le message. Il détermine ensuite si le message réussit l'évaluation de contrôle d'accès (qui peut inclure une inspection approfondie). Si le message réussit l'inspection, le système le transmet au serveur de destination.

ClientHello n'est *pas* modifié si le trafic correspond à une condition de règle **Monitor** (Surveiller).

Intermédiaire (Man-in-the-middle)

La communication directe entre le client et le serveur n'est plus possible pendant l'établissement de liaison TLS/SSL, car après la modification du message, les codes d'authentification de message (MAC) calculés par le client et le serveur ne correspondent plus. Pour tous les messages d'établissement de liaison suivants (et pour la session chiffrée une fois établie), le périphérique géré agit comme un intermédiaire. Cela crée deux sessions TLS/SSL, une entre le client et le périphérique géré, et une entre le périphérique géré et le serveur. Par conséquent, chaque session contient des détails de session cryptographiques différents.

Remarque Les suites de chiffrement que le système peut déchiffrer sont fréquemment mises à jour et ne correspondent pas directement aux suites de chiffrement que vous pouvez utiliser dans les conditions règle de déchiffrement. Pour obtenir la liste actuelle des suites de chiffrement déchiffrables, communiquez avec le TAC de Cisco.

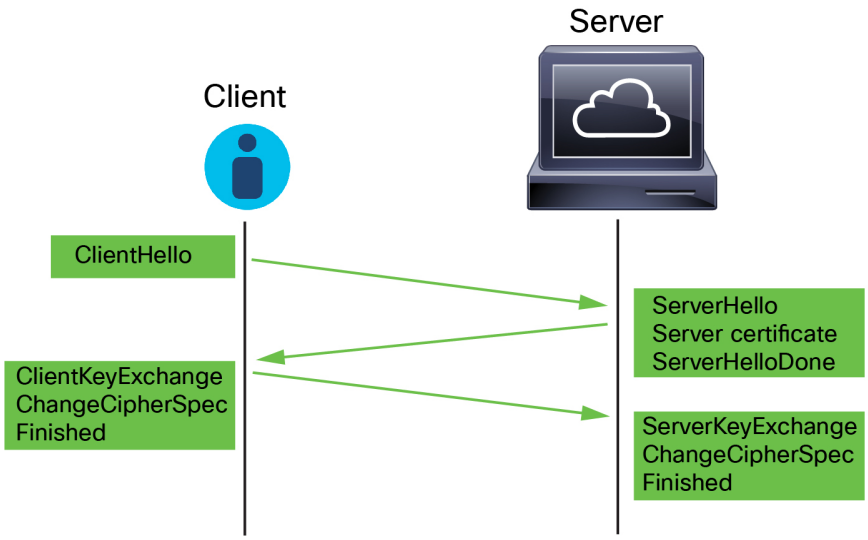
Sujets connexes

Options de traitement par défaut du trafic non déchiffrable
Gestion des messages de ServerHello et du certificat du serveur, à la page 6

Gestion des messages de ServerHello et du certificat du serveur

Aperçu

La figure suivante présente un exemple. Voir également RFC 8446, sec. 4 . Vous pouvez également consulter une ressource comme Que se passe-t-il lors de l'établissement de liaison TLS? sur cloudflare.com.



Le processus peut être résumé comme suit :

1. ClientHello lance le processus.

   Le message ClientHello contient l'indicateur du nom du serveur (SNI), qui comporte le nom de domaine complet du serveur.

2. Lorsqu'un périphérique géré a traité un message ClientHello et l'a transmis au serveur de destination, ce dernier détermine s'il prend en charge les attributs de déchiffrement spécifiés dans le message. S'il ne prend pas en charge ces attributs, le serveur envoie une alerte d'échec d'établissement de liaison au client. S'il prend en charge ces attributs, le serveur envoie le message ServerHello. Si la méthode d'échange de clés convenue utilise des certificats pour l'authentification, le message de certificat du serveur suit immédiatement le message ServerHello.

   Le certificat du serveur contient le Subject Alternative Name (SAN), qui peut avoir des noms de domaine et des adresses IP complets. Pour plus d'informations sur SAN, consultez Nom distinctif.

3. Lorsque le périphérique géré reçoit ces messages, il tente de les mettre en correspondance avec les règles de déchiffrement configurés sur le système. Ces messages contiennent des informations qui étaient absentes du message ClientHello ou du cache de données de session. Plus précisément, le système peut mettre en correspondance ces messages aux conditions de règles de déchiffrement, état du certificat, suites de chiffrement et versions.

L'ensemble du processus est chiffré.

Actions Règle de déchiffrement

Si les messages ne correspondent à aucun règles de déchiffrement, le périphérique géré exécute Actions par défaut Politique de déchiffrement.

Si les messages correspondent à une règle qui appartient à un politique de déchiffrement associé à une politique de contrôle d'accès, le périphérique géré continue comme approprié :

Action : Surveiller
L'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré suit et enregistre le trafic, mais ne le déchiffre pas.

Action : Bloquer ou Bloquer avec réinitialisation

Le périphérique géré bloque la session TLS/SSL et, si elle est configurée, réinitialise la connexion TCP.

Action : Ne pas déchiffrer

L'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré ne déchiffre pas les données d'application échangées pendant la session TLS/SSL.

Action : Déchiffrer - clé connue

Le périphérique géré tente de faire correspondre les données du certificat du serveur à un objet de certificat interne précédemment importé dans centre de gestion. Comme vous ne pouvez pas générer d'objet certificat interne, et que vous devez posséder sa clé privée, nous supposons que vous êtes propriétaire du serveur sur lequel vous utilisez le déchiffrement par clé connue.

Si le certificat correspond à un certificat connu, l'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré utilise la clé privée téléchargée pour déchiffrer et rechiffrer les données d'application échangées pendant la session TLS/SSL.

Si le serveur modifie son certificat entre la connexion initiale avec le client et les connexions ultérieures, vous devez importer le nouveau certificat de serveur dans le centre de gestion champ pour que les connexions futures soient déchiffrées.

Action : Déchiffrer - Resigner

Le périphérique géré traite le message du certificat de serveur et signe de nouveau le certificat de serveur avec l'autorité de certification (CA) importée ou générée précédemment. L'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré utilise ensuite la clé privée téléchargée pour déchiffrer et rechiffrer les données d'application échangées pendant la session TLS/SSL.

Remarque Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 11 et Déchiffrement par clé connue (trafic entrant), à la page 12.

Sujets connexes

Gestion des messages ClientHello, à la page 3

Bonnes pratiques de TLS/SSL

Cette section traite des informations que vous devez garder à l'esprit lors de la création de vos règles Politiques de déchiffrement.

Remarque Comme TLS et SSL sont souvent utilisés de manière interchangeable, nous utilisons l'expression *TLS/SSL* pour indiquer que l'un ou l'autre des protocoles est l'objet de la discussion. Le protocole SSL a été déconseillé par l'IETF au profit du protocole TLS plus sécurisé. Vous pouvez donc interpréter le protocole *TLS/SSL* comme faisant uniquement référence à TLS.

Pour en savoir plus sur les protocoles SSL et TLS, consultez une ressource comme SSL ou TLS - What's the Difference?

Sujets connexes

Les arguments en faveur du déchiffrement, à la page 9
Quand déchiffrer le trafic et quand ne pas le déchiffrer, à la page 10
Autres actions Règle de déchiffrement, à la page 12
Composants Règle de déchiffrement, à la page 12
Évaluation de l'ordre d'une Règle de déchiffrement, à la page 13
Bonnes pratiques de déchiffrement TLS 1.3

Les arguments en faveur du déchiffrement

Le trafic chiffré lorsqu'il passe dans le système peut être autorisé ou bloqué uniquement, mais il *ne peut pas* être soumis à une inspection approfondie ou à l'ensemble des mesures d'application des politiques (comme la prévention des intrusions).

Toutes les connexions chiffrées :

- Sont envoyés par le biais du politique de déchiffrement pour déterminer si elles doivent être déchiffrées ou bloquées.

  Vous pouvez également configurer règles de déchiffrement pour bloquer le trafic chiffré dont vous savez que vous ne voulez pas sur votre réseau, comme le trafic qui utilise le protocole SSL non sécurisé ou le trafic avec un certificat expiré ou non valide.

- S'il est débloqué, déchiffré ou non, le trafic passe par la politique de contrôle d'accès pour une décision finale d'autorisation ou de blocage.

Seul le trafic *déchiffré* tire parti des fonctionnalités de défense contre les menaces et d'application des politiques du système, telles que :

- protection améliorée contre les logiciels malveillants
- Renseignements de sécurité
- Threat Intelligence Director (directeur des informations sur les menaces)
- Détecteurs d'applications
- Filtrage par URL et par catégories

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

Nous vous recommandons de déchiffrer le trafic de manière sélective pour utiliser au mieux les politiques de contrôle d'accès et l'inspection approfondie.

En résumé :

- Le trafic chiffré peut être autorisé ou bloqué par la politique; le trafic chiffré *ne peut pas* être inspecté
- Le trafic déchiffré est soumis à la défense contre les menaces et à l'application des politiques; le trafic déchiffré peut être autorisé ou bloqué par la politique

Sujets connexes

Inspection approfondie à l'aide des politiques de fichier et de prévention des intrusions

Quand déchiffrer le trafic et quand ne pas le déchiffrer

Cette section fournit des instructions sur le moment où vous devez déchiffrer le trafic et quand vous devez l'autoriser à traverser le pare-feu chiffré.

Quand ne pas déchiffrer le trafic

Vous ne devez pas déchiffrer le trafic si cela est interdit par :

- la loi; Par exemple, certaines juridictions interdisent le déchiffrement des renseignements financiers
- la politique de l'entreprise; Par exemple, votre entreprise pourrait interdire le déchiffrement des communications privilégiées
- Règles de confidentialité
- Le trafic qui utilise l'épinglage de certificat (également appelé *TLS/SSL épinglage*) doit rester chiffré pour éviter de rompre la connexion

Snort 2.) Si vous choisissez de contourner le déchiffrement pour certains types de trafic, aucun traitement n'est effectué sur le trafic. Le trafic chiffré est d'abord évalué par politique de déchiffrement, puis passe à la politique de contrôle d'accès, où une décision finale d'autorisation ou de blocage est prise.

(Snort 3.) Politique de déchiffrement n'est *pas* contourné pour les connexions qui correspondent aux règles de contrôle d'accès avec des actions de confiance, de blocage ou de blocage avec réinitialisation, à moins que le trafic soit préfiltré. Le trafic chiffré est d'abord évalué par politique de déchiffrement, puis passe à la politique de contrôle d'accès, où une décision finale d'autorisation ou de blocage est prise.

Le trafic chiffré peut être autorisé ou bloqué dans n'importe quelle condition règle de déchiffrement, y compris, mais sans s'y limiter :

- État du certificat (par exemple, certificat expiré ou non valide)
- Protocole (par exemple, le protocole SSL non sécurisé)
- Réseau (zone de sécurité, adresse IP, balise VLAN, etc.)
- URL ou catégorie d'URL exacte
- Port
- Groupe d'utilisateurs

Les Règles de déchiffrement fournissent une action **Do Not Decrypt (Ne pas déchiffrer)** pour ce trafic; pour en savoir plus, consultez Action Ne pas déchiffrer de la Règle de déchiffrement.

Remarque Les liens vers les informations connexes à la fin de cette rubrique expliquent le fonctionnement de certains aspects de l'évaluation de règles. Des conditions telles que le filtrage d'URL et d'applications comportent des limites en ce qui concerne le trafic chiffré. Assurez-vous de comprendre ces limites.

Pour en savoir plus sur l'utilisation du filtrage d'URL dans les règles **Ne pas déchiffrer**, consultez Action Ne pas déchiffrer de la Règle de déchiffrement.

Quand déchiffrer le trafic

Tout le trafic chiffré doit être déchiffré pour tirer parti des fonctionnalités de protection contre les menaces et d'application des politiques du système. Dans la mesure où votre appareil géré permet le déchiffrement du trafic (sous réserve de sa mémoire et de sa puissance de traitement), vous devez déchiffrer le trafic qui n'est pas interdit par la loi ou la réglementation. Si vous devez décider du trafic à déchiffrer, fondez votre décision sur le risque d'autoriser le trafic sur votre réseau. Le système offre un cadre flexible pour classer le trafic à l'aide de conditions de règles, qui incluent la réputation des URL, le chiffrement, ou de nombreux autres facteurs.

Sujets connexes

Déchiffrer et resigner (trafic sortant), à la page 11
Déchiffrement par clé connue (trafic entrant), à la page 12
Lignes directrices et limites relatives à Règle de déchiffrement
Ordre des règles SSL
Conditions d'URL (filtrage d'URL)
Ordre des règles relatives aux applications
Bonnes pratiques de déchiffrement TLS 1.3

Déchiffrer et resigner (trafic sortant)

L'action **Decrypt – Resign** règle de déchiffrement (Déchiffrer - Resigner) permet au système d'agir comme Man in the middle (personne du milieu), en l'interceptant, en déchiffrant et (si le trafic est autorisé à passer) en l'inspectant et en le rechiffrant. L'action de règle **Decrypt - Resign** est utilisée avec le trafic sortant. c'est-à-dire que le serveur de destination se trouve à l'extérieur de votre réseau protégé.

L'appareil défense contre les menaces négocie avec le client à l'aide d'un objet autorité de certification (CA) interne spécifié dans la règle et crée un tunnel TLS/SSL entre le client et le périphérique défense contre les menaces . En même temps, le périphérique se connecte au site Web de destination et crée un tunnel SSL entre le serveur et le périphérique défense contre les menaces .

Ainsi, le client voit le certificat de l'autorité de certification configuré pour règle de déchiffrement au lieu du certificat du serveur de destination. Le client doit faire confiance au certificat du pare-feu pour terminer la connexion. Le périphérique défense contre les menaces effectue ensuite le déchiffrement/rechiffrement dans les deux sens du trafic entre le client et le serveur de destination.

Préalables

Pour utiliser l'action de règle **Déchiffrer – Resigner**, vous devez créer un objet autorité de certification interne à l'aide d'un fichier d'autorité de certification et d'un fichier de clé privée apparié. Vous pouvez générer une autorité de certification et une clé privée dans le système si vous ne les avez pas déjà.

Remarque Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 11 et Déchiffrement par clé connue (trafic entrant), à la page 12.

Sujets connexes

Actions de déchiffrement de Règle de déchiffrement
Objets de certificat externe

Déchiffrement par clé connue (trafic entrant)

L'action **Déchiffrer – Clé connue** règle de déchiffrement utilise la clé privée d'un serveur pour déchiffrer le trafic. L'action de règle **Déchiffrer - Clé connue** est utilisée avec le trafic entrant; c'est-à-dire que le serveur de destination se trouve dans votre réseau protégé.

L'objectif principal du déchiffrement avec une clé connue est de protéger vos serveurs contre les attaques externes.

Préalables

Pour utiliser l'action de règle **Déchiffrer – Clé connue**, vous devez créer un objet de certificat interne à l'aide du fichier de certificat et du fichier de clé privée jumelé du serveur.

Remarque Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 11 et Déchiffrement par clé connue (trafic entrant), à la page 12.

Sujets connexes

Déchiffrement par clé connue (trafic entrant), à la page 12
Actions de déchiffrement de Règle de déchiffrement
Objets de certificat interne

Autres actions Règle de déchiffrement

Les sections suivantes traitent des autres actions règle de déchiffrement.

Sujets connexes

Actions de blocage de Règle de déchiffrement
Action Monitor (Surveiller) de Règle de déchiffrement

Composants Règle de déchiffrement

Chaque règle de déchiffrement comporte les composants suivants.

État

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles d'un politique de déchiffrement sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. À l'exception des règles de surveillance, la première règle à laquelle le trafic correspond est celle qui gère ce trafic.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Les conditions peuvent correspondre au trafic par zone de sécurité, réseau ou localisation géographique, VLAN, port, application, URL demandée, utilisateur, certificat, sujet ou émetteur de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement. L'utilisation de conditions peut dépendre des licences de périphérique cible.

Action

L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Vous pouvez surveiller, autoriser, bloquer ou déchiffrer le trafic de correspondance chiffré. Le trafic déchiffré et autorisé à être chiffré est soumis à une inspection plus approfondie. Notez que le système n'effectue **pas** d'inspection sur le trafic chiffré bloqué.

Logging (journalisation)

Les paramètres de journalisation d'une règle régissent les enregistrements que le système conserve du trafic qu'il gère. Vous pouvez conserver un enregistrement du trafic qui correspond à une règle. Vous pouvez ouvrir une connexion lorsque le système bloque une session chiffrée ou autorise la transmission sans déchiffrement, selon les paramètres d'un politique de déchiffrementfichier. Vous pouvez également forcer le système à journaliser les connexions qu'il déchiffre pour une évaluation plus approfondie par des règles de contrôle d'accès, quelle que soit la façon dont le système gère ou inspecte le trafic ultérieurement. Vous pouvez enregistrer les connexions à la base de données Cisco Secure Firewall Management Center, au journal système (syslog) ou à un serveur de déroutement SNMP.

Astuces Créer et ordonner correctement des règle de déchiffrement est une tâche complexe. Si vous ne planifiez pas votre politique avec soin, les règles peuvent prévaloir sur d'autres règles, nécessiter des licences supplémentaires ou contenir des configurations non valides. Pour vous assurer que le système gère le trafic comme prévu, l'interface politique de déchiffrement dispose d'un système d'avertissement et d'erreur robuste pour les règles.

Évaluation de l'ordre d'une Règle de déchiffrement

Lorsque vous créez une règle de déchiffrement dans une politique de déchiffrement, vous spécifiez sa position à l'aide de la liste d'**insertion** de l'éditeur de règles. Les règles de déchiffrement dans une politique de déchiffrement sont numérotées en commençant à 1. Le système fait correspondre le trafic aux règles de déchiffrement en ordre descendant par numéro de règle croissant.

Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de déchiffrement, pour leesquelles *toutes* les conditions de la règle correspondent au trafic. Sauf dans le cas des règles Monitor (surveillance) (qui enregistrent le trafic mais n'affectent pas le flux), le système ne continue *pas* à évaluer le trafic par rapport à des règles supplémentaires de priorité inférieure une fois que le trafic correspond à une règle. Les conditions peuvent être simples ou complexes; vous pouvez contrôler le trafic par zone de sécurité, réseau ou emplacement géographique, VLAN, port, application, URL demandée, utilisateur, certificat, nom distinctif de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement.

Chaque règle possède également une *action*, qui détermine si vous surveillez, bloquez ou inspectez le trafic chiffré ou déchiffré correspondant à l'aide du contrôle d'accès. Vous observerez que le système n'inspecte *pas* davantage le trafic chiffré qu'il bloque. Il soumet le trafic chiffré et non déchiffrable au contrôle d'accès. Toutefois, les conditions des règles de contrôle d'accès exigent un trafic non chiffré, de sorte que le trafic chiffré correspond à un nombre réduit de règles.

Les règles qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées avant les règles qui utilisent des conditions *générales* (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus tardivement dans vos règles. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Astuces Un ordre adéquat de règle de déchiffrement réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles. Bien que les règles que vous créez soient uniques à chaque organisation et chaque déploiement, il existe quelques consignes générales à suivre lors de la mise en ordre des règles qui peuvent optimiser les performances tout en répondant à vos besoins.

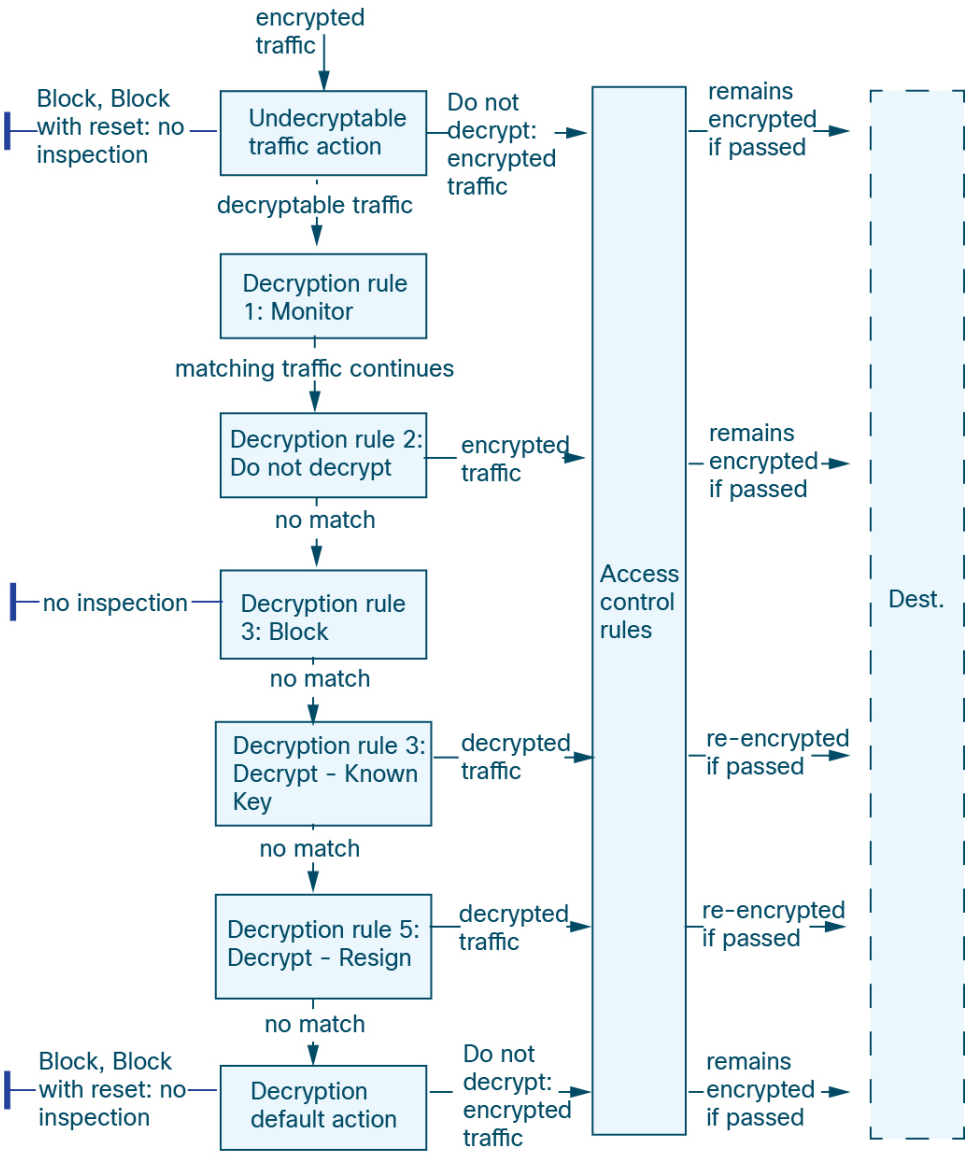
En plus de trier les règles par numéro, vous pouvez regrouper les règles par catégories. Par défaut, le système propose trois catégories : Administrateur, Standard et Racine. Vous pouvez ajouter des catégories personnalisées, mais vous ne pouvez pas supprimer les catégories fournies par le système ni modifier leur ordre.

Sujets connexes

Options de traitement par défaut du trafic non déchiffrable
Ordre des règles SSL
Bonnes pratiques pour les règles de contrôle d'accès

Exemple de règles multiples

Le scénario suivant résume les façons dont règles de déchiffrement gère le trafic dans un déploiement en ligne.



Dans ce scénario, le trafic est évalué comme suit :

- **L'action Undecryptable Traffic** (Trafic non déchiffrable) évalue d'abord le trafic chiffré. En ce qui concerne le trafic que le système ne peut pas déchiffrer, il le bloque sans autre forme d'inspection ou le transmet à l'inspection du contrôle d'accès. Le trafic chiffré qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 1 : La règle Monitor (Surveiller)** évalue ensuite le trafic chiffré. Les règles de surveillance suivent et consignent le trafic chiffré, mais n'affectent pas le flux de trafic. Le système continue de faire correspondre le trafic à des règles supplémentaires pour déterminer s'il doit l'autoriser ou le refuser.
- **Règle de déchiffrement 2 : La règle Do Not Decrypt (Ne pas déchiffrer)** évalue le trafic chiffré en troisième lieu. Le trafic correspondant n'est pas déchiffré; le système inspecte ce trafic à l'aide du contrôle d'accès, mais pas de l'inspection de fichiers ou de la prévention des intrusions. Le trafic qui ne correspond pas passe à la règle suivante.

- **Règle de déchiffrement 3: La règle Block (blocage)** évalue le trafic chiffré en quatrième lieu. Le trafic correspondant est bloqué sans autre inspection. Le trafic qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 4 : Decrypt - Known Key (Déchiffrer – clé connue)** évalue le trafic chiffré en cinquième lieu. Le trafic correspondant entrant dans votre réseau est déchiffré à l'aide d'une clé privée que vous téléversez. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès gèrent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à règle de déchiffrement passe à la règle suivante.
- **Règle de déchiffrement 5 : Decrypt - Resign (Déchiffrer-Resigner)** est la règle finale. Si le trafic correspond à cette règle, le système signe de nouveau le certificat du serveur avec un certificat d'autorité de certification téléversé, puis agit comme un intermédiaire pour déchiffrer le trafic. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès traitent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à la règle SSL passe à la règle suivante.
- **Politique de déchiffrement L'action par défaut** gère tout le trafic qui ne correspond à aucun des règles de déchiffrement. L'action par défaut bloque le trafic chiffré sans autre inspection ou ne le déchiffre pas et le transmet pour l'inspection du contrôle d'accès.

Accélération du chiffrement TLS

Accélération cryptographique TLS accélère les processus suivants :

- Chiffrement et déchiffrement TLS/SSL
- VPN, y compris TLS/SSL et IPsec

Matériel pris en charge

Les modèles de matériel suivants prennent en charge Accélération cryptographique TLS :

- Secure Firewall 3100
- Firepower de la série 2100
- Firepower 4100/9300

  Pour en savoir plus sur la prise en charge de Accélération cryptographique TLS sur les Firepower 4100/9300 Instance de conteneur de défense contre les menaces , consultez le *Guide de configuration FXOS*.

Accélération cryptographique TLS *n'est* pas pris en charge sur aucune appliance virtuelle ni sur aucun matériel à l'exception des éléments précédents.

Remarque Pour en savoir plus sur Accélération cryptographique TLS et les modèles 4100/9300, consultez le *Guide de configuration FXOS*.

Fonctionnalités non prises en charge par Accélération cryptographique TLS

Les fonctionnalités *non* prises en charge par Accélération cryptographique TLS sont les suivantes :

- Périphériques gérés pour lesquels Instance de conteneur de défense contre les menaces est activé.
- Si le moteur d'inspection est configuré pour préserver les connexions et qu'il tombe en panne de manière inattendue, le trafic TLS/SSL est abandonné jusqu'à ce que le moteur redémarre.

  Ce comportement est contrôlé par la commande **configure snort preserve-connection {enable | disable}**.

Lignes directrices et limites relatives à Accélération cryptographique TLS

Gardez les éléments suivants à l'esprit si l'option Accélération cryptographique TLS est activée sur votre périphérique géré.

Performance HTTP uniquement

L'utilisation de Accélération cryptographique TLS sur un périphérique géré qui ne déchiffre pas le trafic peut affecter les performances.

Normes FIPS

Si Accélération cryptographique TLS et les normes FIPS (Federal Information Processing Standards) sont simultanément activées, les connexions avec les options suivantes échouent :

- Clé RSA d'une taille inférieure à 2 048 octets
- Chiffrement Rivest 4 (RC4)
- Norme de chiffrement de données unique (DES unique)
- Merkle–Damgard 5 (MD5)
- SSL v3

Les normes FIPS sont activées lorsque vous configurez centre de gestion et les périphériques gérés pour fonctionner en mode de conformité des certifications de sécurité. Pour autoriser les connexions lorsque vous fonctionnez dans ces modes, vous pouvez configurer les navigateurs Web de façon à ce qu'ils acceptent des options plus sécurisées.

Pour en savoir plus :

- Chiffreurs pris en charge par FIPS : À propos des paramètres SSL.
- Modes de conformité des certifications de sécurité.
- Critères communs

Pulsations TLS

Certaines applications utilisent l'extension de *pulsation TLS* pour les protocoles Transport Layer Security (TLS) et DTLS (Datagram Transport Layer Security) définis par la RFC6520. La pulsation TLS permet de confirmer que la connexion est toujours active : le client ou le serveur envoie un nombre spécifié d'octets de données et demande à l'autre partie de renvoyer la réponse. Si l'opération réussit, des données chiffrées sont envoyées.

Lorsqu'un périphérique géré pour lequel Accélération cryptographique TLS est activé rencontre un paquet qui utilise l'extension de pulsation TLS, le périphérique géré effectue l'action spécifiée par le paramètre de **déchiffrement des erreurs** dans les **Actions indéchiffrables** de politique de déchiffrement :

- Bloquer
- Bloc avec action de réinitialisation

Pour en savoir plus, consultez Options de traitement par défaut du trafic non déchiffrable.

Pour déterminer si les applications utilisent les pulsations TLS, consultez Dépannage de la pulsation TLS.

Vous pouvez configurer la **Max Heartbeat Length** (longueur de pulsation maximale) dans une politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) pour déterminer comment gérer les pulsations TLS. Pour obtenir plus de renseignements, consultez Le préprocesseur SSL.

Surabonnement TLS/SSL

Le surabonnement TLS/SSL est un état dans lequel un périphérique géré est surchargé de trafic TLS/SSL. Tout périphérique géré peut connaître un surabonnement TLS/SSL, mais seuls les périphériques gérés qui prennent en charge Accélération cryptographique TLS offrent un moyen configurable de le gérer.

Lorsqu'un périphérique géré avec Accélération cryptographique TLS activé est surabonné, tout paquet reçu par le périphérique géré est traité en fonction du paramètre des **erreurs d'établissement de liaison** dans les **actions indéchiffrables** de politique de déchiffrement :

- Hériter de l'action par défaut
- Ne pas déchiffrer
- Bloquer
- Bloc avec action de réinitialisation

Si le paramètre des **erreurs d'établissement de liaison** dans les **actions indéchiffrable** de politique de déchiffrement est **Ne pas déchiffrer** et que la politique de contrôle d'accès associée est configurée pour inspecter le trafic, l'inspection a lieu. le déchiffrement ne se produit *pas*.

En cas de surabonnement important, vous avez les options suivantes :

- Mettez à niveau vos périphériques gérés pour augmenter la capacité de traitement TLS/SSL.
- Modifiez vos Politiques de déchiffrement pour ajouter des règles **Ne pas déchiffrer** pour le trafic dont le déchiffrement n'est pas prioritaire.

Afficher l'état de l'accélération du chiffrement TLS

Cette rubrique explique comment déterminer si Accélération cryptographique TLS est activé.

Effectuez la tâche suivante dans centre de gestion.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Périphériques** > **Gestion des périphériques**.

Étape 3 Cliquez sur **Modifier** (✎) pour modifier un périphérique géré.

Étape 4 Cliquez sur la page **Périphérique**. L'état Accélération cryptographique TLS est affiché dans la section Général.

Comment configurer Politiques de déchiffrement et les règles

Cette rubrique fournit un aperçu général des tâches que vous devez effectuer pour configurer Politiques de déchiffrement et règles de déchiffrement dans ces politiques pour bloquer, surveiller ou autoriser le trafic TLS/SSL sur votre réseau.

Vous devez être Admin, Administrateur d'accèsou Administrateur de réseau pour effectuer cette tâche.

Procédure

	Commande ou action	Objectif
Étape 1	Pour **Decrypt - Known Key** (Déchiffrer - Clé connue) règles de déchiffrement (pour déchiffrer le trafic entrant vers un serveur interne), créez un objet de certificat interne.	L'objet de certificat interne utilise le certificat et la clé privée de votre serveur. Consultez Objets de certificat interne.
Étape 2	Pour **Decrypt - Resign** (Déchiffrer – Resigner) règles de déchiffrement (pour déchiffrer le trafic sortant vers un serveur à l'extérieur de votre réseau), créez un objet autorité de certification interne (CA).	L'objet autorité de certification interne utilise une autorité de certification et une clé privée. Consultez Objets Autorité de certification interne.
Étape 3	Créez u de déchiffrement et, éventuellement, des règles.	Vous pouvez créer une politique de déchiffrement avec plusieurs règles à la fois. Vous pouvez également créer une politique de déchiffrement sans règles; par exemple, pour ajouter les règles ultérieurement ou pour créer une politique avec des actions de règle **Ne pas déchiffrer**. Pour en savoir plus, consultez Créer une politique de déchiffrement.
Étape 4	Définissez une action par défaut pour votre politique de déchiffrement.	L'action par défaut est entreprise lorsque le trafic ne correspond à aucune règle définie par politique de déchiffrement. Consultez Actions par défaut Politique de déchiffrement.
Étape 5	Précisez comment le trafic non déchiffrable doit être géré.	Le trafic peut être non déchiffrable pour un certain nombre de raisons, notamment des protocoles non sécurisés, des utilisations et des suites de chiffrement inconnues, ou en cas d'erreurs d'établissement de liaison ou de déchiffrement. Consultez Options de traitement par défaut du trafic non déchiffrable.

	Commande ou action	Objectif
Étape 6	Configurez les paramètres avancés de votre politique de déchiffrement.	Les paramètres avancés comprennent la désactivation des publicités HTTP/3, l'activation du déchiffrement TLS 1.3 et l'activation de la sonde d'identité du serveur TLS. Pour en savoir plus, consultez Options avancées de Politique de déchiffrement.
Étape 7	Associer politique de déchiffrement à une politique de contrôle d'accès.	Sauf si vous associez votre politique de déchiffrement à une politique de contrôle d'accès, cela n'a aucun effet. Après cela, vous pouvez choisir d'autoriser ou de bloquer le trafic correspondant à la règle de contrôle d'accès et effectuer d'autres actions. Consultez Association d'autres politiques au contrôle d'accès.
Étape 8	Configurez vos règles de contrôle d'accès pour autoriser ou bloquer le trafic déchiffré.	Consultez Composants des politiques de contrôle d'accès.
Étape 9	Choisissez d'activer ou non la découverte d'identité du serveur TLS dans la politique de contrôle d'accès.	Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès.
Étape 10	Déployer la politique de contrôle d'accès sur les périphériques gérés.	Avant que votre politique ne puisse prendre effet, elle doit être déployée sur les périphériques gérés. Consultez Déployer les modifications de configuration.

Historique pour Politique de déchiffrement

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Politique de déchiffrement.	20221213	7.3.0	La fonctionnalité a été renommée *Politique de déchiffrement* pour mieux refléter ce qu'elle fait. Nous vous permettons maintenant de configurer une politique de déchiffrement avec une ou plusieurs règles **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue** en même temps. Écrans nouveaux ou modifiés : • **Politiques** > **Contrôle d'accès** > **Déchiffrement**(Créer une nouvelle politique de déchiffrement) • La boîte de dialogue Create Decryption Policy (Créer une politique de déchiffrement) comporte désormais deux pages à onglet : **connexions sortantes** et **connexions entrantes**. Utilisez la page à onglet **Outbound Connections** (connexions sortantes) pour configurer une ou plusieurs règles de déchiffrement avec une action de règle **Déchiffrer - Résigner**. (Vous pouvez téléverser ou générer des autorités de certification en même temps.) Chaque combinaison d'une autorité de certification, de réseaux et de ports génère une règle de déchiffrement. Utilisez la page à l'onglet Inbound Connections (connexions entrantes) pour configurer une ou plusieurs règles de déchiffrement avec une action de règle Decrypt - Known Key (déchiffrer - clé connue). (Vous pouvez télécharger le certificat de votre serveur en même temps.) Chaque combinaison d'un certificat de serveur avec des réseaux et des ports génère une règle de déchiffrement. • **Politiques** > **Contrôle d'accès** > **Déchiffrement** (modifier une règle de déchiffrement) : **les paramètres avancés** comportent de nouvelles options décrites dans Bonnes pratiques de déchiffrement TLS 1.3. • **Politiques** > **Contrôle d'accès** > (modifier une politique de contrôle d'accès), cliquez sur le mot **déchiffrement** pour associer une politique de déchiffrement à une politique de contrôle d'accès.
Déchiffrement TLS 1.3	20220609	7.2.0	Vous pouvez désormais activer le déchiffrement TLS 1.3 dans les actions avancées d'une politique SSL. Le déchiffrement TLS 1.3 nécessite que le périphérique géré exécute Snort 3. D'autres options sont également disponibles; pour en savoir plus, consultez Bonnes pratiques de déchiffrement TLS 1.3. **Écran Nouveau ou modifié** : **Politique SSL** > **Paramètres avancés**

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres avancés de la politique SSL.	20220609	7.2.0	Paramètres avancés de la politique SSL. **Écran Nouveau ou modifié** : **Politique SSL** > **Paramètres avancés**
Possibilité de préciser le traitement des URL de réputation inconnue.	20220609	7.0.3	Pour de plus amples renseignements, consultez la section À propos du filtrage d'URL avec catégorie et réputation.
Modification de ClientHello pour les règles de déchiffrement **: règles de clé connues**.	20220609	7.0.3	Pour de plus amples renseignements, consultez la section Gestion des messages ClientHello, à la page 3.
Possibilité d'extraire le certificat dans le trafic TLS 1.3 pour permettre au trafic de correspondre aux critères d'URL et d'application dans les règles de contrôle d'accès.	20220609		Écran Nouveau ou modifié : lien **Politiques** > **Contrôle d'accès** > **(modifier une politique de contrôle d'accès)** > **Avancé**. Pour de plus amples renseignements, consultez la section Options avancées de Politique de déchiffrement.
Modifications apportées au filtrage d'URL basé sur la catégorie et la réputation.	20220609	7.0.3	Pour de plus amples renseignements, consultez la section À propos du filtrage d'URL avec catégorie et réputation.
Accélération cryptographique TLS ne peut pas être désactivé.	20220609	7.0.3	Accélération cryptographique TLS est activé sur tous les périphériques pris en charge. Sur un périphérique géré avec des interfaces natives, Accélération cryptographique TLS ne peut pas être désactivé. La prise en charge de Accélération cryptographique TLS sur les Instance de conteneur de défense contre les menaces est limitée, comme indiqué à la ligne suivante de ce tableau. Commandes supprimées : **system support ssl-hw-accel enable** **system support ssl-hw-accel disable** **system support ssl-hw-status**

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Prise en charge de Accélération cryptographique TLS sur un Instance de conteneur de défense contre les menaces d'un Firepower 4100/9300 sur un module ou moteur de sécurité.	20220609	7.0.3	Vous pouvez maintenant activer Accélération cryptographique TLS pour un Instance de conteneur de défense contre les menaces sur un module ou moteur de sécurité. Accélération cryptographique TLS est désactivé pour les autres instances de conteneur, mais activé pour les instances natives. Commandes nouvelles ou modifiées : **config hwCrypto enable** **show crypto accelerator status** remplace **system support ssl-hw-status**)
TLS/SSL accélération matérielle est maintenant appelé *Accélération cryptographique TLS*.	20220609	7.0.3	Le changement de nom indique que l'accélération du chiffrement et du déchiffrement TLS/SSL est prise en charge sur un plus grand nombre de périphériques. Selon le périphérique, l'accélération peut être effectuée logiciellement ou matériellement. Écran concerné : Pour afficher l'état de la page générale Accélération cryptographique TLS, **Périphériques** > **Gestion des périphériques** > **Périphérique**.
TLS/SSL accélération matérielle Activé par défaut.	20220609	7.0.3	TLS/SSL accélération matérielle est activée par défaut sur tous les périphériques pris en charge, mais peut être désactivée si vous le souhaitez.
Extension de secret maître étendu prise en charge (voir RFC 7627).	20220609	7.0.3	L'extension du secret maître étendu TLS est prise en charge pour les politiques SSL; plus précisément, les politiques avec une action de règle **Decrypt - Resign** (Déchiffrer - Resigner) ou **Decrypt - Known Key** (Déchiffre - Clé connue).
Rétrogradation dynamique de TLS 1.3.	20220609	7.0.3	La commande CLI **system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** vous permet de déterminer le comportement de rétrogradation du trafic TLS 1.3 vers TLS 1.2. Pour de plus amples renseignements, consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.
Introduction de TLS/SSL accélération matérielle.	20220609	7.0.3	Certains modèles de périphériques gérés effectuent le chiffrement et le déchiffrement TLS/SSL sur le matériel, ce qui améliore les performances. Par défaut, la fonction est activée. Écran concerné : Pour afficher l'état de la page générale TLS/SSL accélération matérielle, **Périphériques** > **Gestion des périphériques** > **Périphérique**.
Conditions de réputation et de catégories prises en charge	20220609	7.0.3	Règles de contrôle d'accès ou règles SSL avec conditions de catégorie ou de réputation.

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
SafeSearch pris en charge.	20220609	7.0.3	Le système affiche une page de réponse HTTP pour les connexions déchiffrées par la politique SSL, puis bloquées (ou bloquées de manière interactive) par les règles de contrôle d'accès ou par l'action par défaut de la politique de contrôle d'accès. Dans ce cas, le système chiffre la page de réponse et l'envoie à la fin du flux SSL rechiffré. SafeSearch filtre le contenu inacceptable et empêche les utilisateurs de rechercher des sites pour adultes.
Politique TLS/SSL.	20220609	7.0.3	Fonctionnalité introduite.

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.