

Inspection des réseaux mobiles

Les rubriques suivantes expliquent l'inspection des applications pour les protocoles utilisés dans les réseaux mobiles tels que LTE. Ces inspections nécessitent la licence Carrier (exploitant). Pour en savoir plus sur la raison pour laquelle vous devez utiliser l'inspection pour certains protocoles et sur les méthodes globales d'application de l'inspection, consultez Premiers pas avec l'inspection du protocole de la couche application.

- Aperçu de l'inspection du réseau mobile, à la page 1
- Licences pour l'inspection des protocoles de réseau mobile, à la page 9
- Valeurs par défaut pour l'inspection GTP, à la page 9
- Configurer l'inspection du réseau mobile, à la page 10
- Surveillance de l'inspection du réseau mobile, à la page 34
- Historique de l'inspection du réseau mobile, à la page 38

Aperçu de l'inspection du réseau mobile

Les rubriques suivantes expliquent les inspections disponibles pour les protocoles utilisés dans les réseaux mobiles tels que LTE. D'autres services sont disponibles pour le trafic SCTP en plus de l'inspection.

Présentation de l'inspection GTP

Le protocole de tunnellisation GPRS (GTP) est utilisé dans les réseaux GSM, UMTS et LTE pour le trafic GPRS (General Packet Radio Service). GTP fournit un protocole de gestion et de contrôle de tunnel pour fournir un accès réseau GPRS à une station mobile par la création, la modification et la suppression de tunnels. GTP utilise également un mécanisme de tunnellisation pour acheminer les paquets de données des utilisateurs.

Les réseaux des fournisseurs de services utilisent GTP pour tunnelliser les paquets multiprotocoles à travers le réseau fédérateur GPRS entre les terminaux. Dans GTPv0-1, GTP est utilisé pour la signalisation entre les nœuds de prise en charge GPRS de passerelle (GGSN) et les nœuds de prise en charge GPRS de service (SGSN). Dans GTPv2, la signalisation se fait entre les passerelles de réseau de données par paquets (PGW) et la passerelle de desserte (SGW), ainsi que d'autres terminaux. Le GGSN/PGW est l'interface entre le réseau de données sans fil GPRS et d'autres réseaux. Le SGSN/SGW effectue la mobilité, la gestion des sessions de données et la compression des données.

Vous pouvez utiliser l'ASA pour assurer une protection contre les partenaires d'itinérance pirates. Placez le périphérique entre le GGSN/PGW d'origine et les terminaux SGSN/SGW visités, et utilisez l'inspection GTP sur le trafic. L'inspection GTP fonctionne uniquement sur le trafic entre ces terminaux. Dans GTPv2, cela s'appelle l'interface S5/S8.

GTP et les normes associées sont définies par le 3GPP (3e génération Partnership Project). Pour de plus amples renseignements, voir http://www.3gpp.org.

Suivi des changements d'emplacement pour les stations mobiles

Vous pouvez utiliser l'inspection GTP pour suivre les modifications d'emplacement des stations mobiles. Le suivi des modifications d'emplacement peut vous aider à identifier les frais d'itinérance frauduleux, par exemple, si vous voyez une station mobile se déplacer d'un emplacement à un autre dans un laps de temps improbable, comme le déplacement d'une cellule aux États-Unis vers une en Europe en 30 minutes.

Lorsque vous activez la journalisation de l'emplacement, le système génère des messages de journal système pour l'emplacement nouveau ou modifié pour chaque identité internationale d'abonné mobile (IMSI) :

- 324010 indique la création d'un nouveau contexte PDP et comprend le code de pays mobile (MCC), le code de réseau mobile (MNC), les éléments d'information et, éventuellement, l'ID de cellule où l'utilisateur est actuellement enregistré. L'ID de cellule est extrait de l'identification globale de cellule (CGI) ou de l'identifiant global de cellule E-UTRAN (ECGI).
- 324011 indique que l'IMSI s'est déplacée de celle stockée lors de la création du contexte PDP. Le message affiche le MCC/MNC précédent et actuel, les éléments d'information et, éventuellement, l'ID de cellule.

Par défaut, les messages syslog n'incluent pas d'informations d'horodatage. Si vous prévoyez d'analyser ces messages pour identifier l'itinérance improbable, vous devez également activer les horodatages. La journalisation de l'horodatage ne fait pas partie de la liste d'inspection GTP. Accédez à **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration Syslog)** et sélectionnez l'option **Enable Timestamp on Syslog Messages (Activer l'horodatage des messages Syslog)**.

Pour plus d'informations sur l'activation de la journalisation de l'emplacement, consultez Configurer une liste des politiques d'inspection GTP, à la page 10.

Limites d'inspection GTP

Voici quelques limites à l'inspection GTP :

- Les messages de superposition GTPv2 ne sont pas pris en charge. Ils sont toujours abandonnés.
- L'attachement d'UE d'urgence GTPv2 est pris en charge uniquement s'il contient l'IMSI (Identité Internationale d'Abonné Mobile).
- L'inspection GTP n'inspecte pas les données précoces. C'est-à-dire les données envoyées par un PGW ou SGW immédiatement après une demande de création de session, mais avant la réponse de création de session.
- Pour GTPv2, l'inspection prend en charge jusqu'à 3GPP 29.274 V15.5.0. Pour GTPv1, la prise en charge va jusqu'à 3GPP 29.060 V15.2.0. Pour GTPv0, la prise en charge est jusqu'à la version 8.
- L'inspection GTP ne prend pas en charge le transfert inter-SGSN vers le contexte PDP secondaire. L'inspection doit effectuer le transfert pour les contextes PDP principal et secondaire.
- Lorsque vous activez l'inspection GTP, les connexions qui utilisent l'encapsulation GTP-in-GTP sont toujours abandonnées.

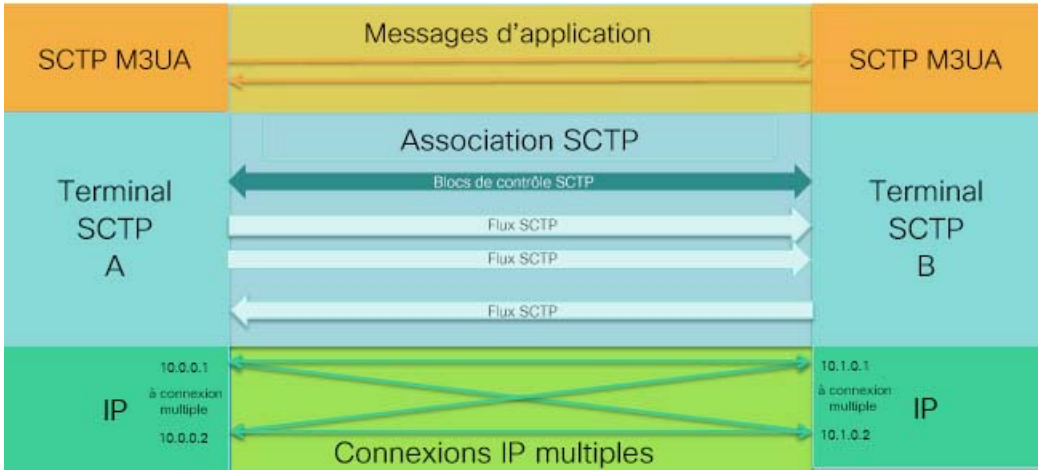
Inspection et contrôle d'accès SCTP (Stream Control Transmission Protocol)

Le protocole SCTP (Stream Control Transmission Protocol) est décrit dans la RFC 4960. Le protocole prend en charge le protocole de signalisation téléphonique SS7 sur IP et est également un protocole de transport pour plusieurs interfaces dans l'architecture de réseau mobile LTE 4G.

SCTP est un protocole de couche de transport fonctionnant au-dessus de l'IP dans la pile de protocoles, semblable à TCP et UDP. Cependant, SCTP crée un canal de communication logique, appelé association, entre deux nœuds terminaux sur une ou plusieurs adresses IP source ou de destination. C'est ce qu'on appelle la multilocalisation. Une association définit un ensemble d'adresses IP sur chaque nœud (source et destination) et un port sur chaque nœud. Toute adresse IP dans l'ensemble peut être utilisée comme adresse IP source ou de destination des paquets de données associés à cette association pour former plusieurs connexions. Dans chaque connexion, plusieurs flux peuvent exister pour envoyer des messages. Un flux dans SCTP représente un canal de données d'application logique.

La figure suivante illustre la relation entre une association et ses flux.

Illustration 1 : Relation entre l'association SCTP et les flux



Si vous avez un trafic SCTP passant par l'ASA, vous pouvez contrôler l'accès en fonction des ports SCTP et mettre en œuvre l'inspection de la couche d'application pour activer les connexions et éventuellement filtrer en fonction de l'ID du protocole de charge utile pour supprimer, consigner ou limiter le débit de manière sélective.

Remarque Chaque nœud peut avoir jusqu'à trois adresses IP. Toutes les adresses au-delà de la limite de trois sont ignorées et ne sont pas incluses dans l'association. Les passages pour les adresses IP secondaires s'ouvrent automatiquement. Vous n'avez pas besoin d'écrire de règles de contrôle d'accès pour les autoriser.

Pulsations et état d'association

Pour maintenir l'association et assurer un suivi précis, le moteur d'inspection surveille les pulsations SCTP. Le système relie la durée de la connexion aux signaux de pulsation. En cas de perte de la pulsation ou de fin explicite de l'association, le périphérique met fin à la connexion et termine la durée de l'événement.

Rapport d'association SCTP et de port

L'inspection SCTP est basée sur les associations plutôt que sur les flux. Comme le périphérique suit l'association complète comme une seule unité, il n'associe pas les ports de flux individuels aux champs de port traditionnels dans la sortie de journalisation. Par conséquent, lorsque vous affichez les détails de la connexion, vous pouvez observer les ports source et de destination affichés comme `0`. En effet, l'association est identifiée de manière unique par les adresses IP et l'ID d'association, plutôt que par les paires individuelles de ports source/destination.

Inspection dynamique SCTP

Comme pour le protocole TCP, le trafic SCTP est automatiquement inspecté au niveau de la couche 4 pour assurer un trafic bien structuré et une application limitée de la norme RFC 4960. Les éléments de protocole suivants sont inspectés et appliqués :

- Types de fragments, indicateurs et longueur.
- Étiquettes de vérification.
- Ports source et de destination pour empêcher les attaques par redirection d'association.
- Adresses IP.

L'inspection dynamique SCTP accepte ou rejette les paquets en fonction de l'état de l'association :

- Validation des séquences d'ouverture et de fermeture à 4 voies pour l'établissement initial de l'association.
- Vérification de la progression directe du TSN dans une association et un flux.
- Mettre fin à une association en voyant le chunk ABORT en raison d'une défaillance de pulsation. Les terminaux SCTP peuvent envoyer le chunk ABORT en réponse à des attaques de bombardement.

Si vous décidez que vous ne souhaitez pas ces vérifications d'application, vous pouvez configurer le contournement de l'état SCTP pour des classes de trafic spécifiques, comme expliqué dans la section Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services).

Contrôle d'accès SCTP

Vous pouvez créer des règles d'accès pour le trafic SCTP. Ces règles sont similaires aux règles basées sur les ports TCP/UDP, où vous utilisez simplement **sctp** comme protocole et où les numéros de port sont des ports SCTP. Vous pouvez créer des objets ou des groupes de service pour SCTP, ou préciser directement les ports. Consultez les rubriques suivantes:

- Configurer des objets de service et des groupes de services
- Configurer les ACL étendues
- Configurer les règles d'accès

NAT SCTP

Vous pouvez appliquer la NAT d'objet réseau statique aux adresses dans les messages d'établissement d'association SCTP. Bien que vous puissiez configurer deux NAT statique, cela n'est pas recommandé, car la topologie de la partie destination de l'association SCTP est inconnue. Vous ne pouvez pas utiliser de NAT/PAT dynamique.

La NAT pour SCTP dépend de l'inspection dynamique SCTP plutôt que de l'inspection de la couche d'application SCTP. Ainsi, vous ne pouvez pas effectuer de trafic NAT si vous configurez le contournement de l'état SCTP.

Inspection de la couche application SCTP

Vous pouvez affiner vos règles d'accès en activant l'inspection et le filtrage SCTP sur les applications SCTP. Vous pouvez supprimer, consigner ou limiter de débit sélectivement des classes de trafic SCTP en fonction de l'identifiant de protocole de charge utile (PPID).

Si vous décidez d'effectuer un filtrage sur PPID, gardez les éléments suivants à l'esprit :

- Les PPID se trouvent dans des fragments de données, et un paquet donné peut avoir plusieurs fragments de données ou même un fragment de contrôle. Si un paquet comprend un fragment de contrôle ou plusieurs fragments de données, le paquet ne sera pas abandonné, même si l'action attribuée est abandonnée.
- Si vous utilisez le filtrage PPID pour abandonner ou limiter le débit des paquets, sachez que l'émetteur renvoyera tous les paquets abandonnés. Bien qu'un paquet pour un PPID à débit limité puisse passer lors de la prochaine tentative, un paquet pour un PPID abandonné sera de nouveau abandonné. Vous pouvez évaluer les conséquences ultérieures de ces abandons répétés sur votre réseau.

Limites de SCTP

La prise en charge de SCTP comprend les limites suivantes :

- Chaque nœud peut avoir jusqu'à trois adresses IP. Toutes les adresses au-delà de la limite de trois sont ignorées et ne sont pas incluses dans l'association. Les passages pour les adresses IP secondaires s'ouvrent automatiquement. Vous n'avez pas besoin d'écrire de règles de contrôle d'accès pour les autoriser.
- Les passages inutilisés expirent en 5 minutes.
- Les adresses IPv4 et IPv6 à double pile sur les terminaux multihébergés ne sont pas prises en charge.
- La NAT statique des objets réseau est le seul type de NAT pris en charge. De plus, NAT46 et NAT64 ne sont pas pris en charge.
- La fragmentation et le réassemblage des paquets SCTP sont effectués uniquement pour le trafic géré par l'inspection Diameter, M3UA et SCTP basée sur PPID.
- Les fragments ASCONF, qui sont utilisés pour ajouter ou supprimer dynamiquement des adresses IP dans SCTP, ne sont pas pris en charge.
- Le paramètre Hostname dans les messages INIT et INIT-ACK SCTP, qui est utilisé pour spécifier un nom d'hôte qui peut ensuite être résolu en une adresse IP, n'est pas pris en charge.
- SCTP/M3UA ne prend pas en charge le routage multichemin à coût égal (ECMP), qu'il soit configuré sur l'ASA ou ailleurs dans le réseau. Avec ECMP, les paquets peuvent être acheminés vers une destination sur plusieurs meilleurs chemins. Cependant, une réponse de paquet SCTP/M3UA à une destination unique doit revenir sur la même interface par laquelle elle est sortie. Même si la réponse peut provenir de n'importe quel serveur M3UA, elle doit toujours revenir sur la même interface par laquelle elle est sortie. Le signe de ce problème est que les paquets SCTP INIT-ACK sont abandonnés, ce que vous pouvez voir dans le compteur **show asp drop flow sctp-chunk-init-timeout** :

```
Flow drop:
SCTP INIT timed out (not receiving INIT ACK)(sctp-chunk-init-timeout)
```

Si vous rencontrez ce problème, vous pouvez le résoudre en configurant des routes statiques vers les serveurs M3UA ou en configurant le routage basé sur les politiques pour mettre en œuvre une conception de réseau qui garantit que les paquets INIT-ACK passent par la même interface que les paquets INIT.

Inspection Diameter

Diameter est un protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans les réseaux de télécommunications fixes et mobiles de nouvelle génération tels que EPS (Evolved Packet System) pour LTE (Long Term Evolution) et IMS (IP Multimedia Subsystem). Il remplace RADIUS et TACACS dans ces réseaux.

Diameter utilise TCP et SCTP comme couche de transport et sécurise les communications en utilisant TCP/TLS et SCTP/DTLS. Il peut également fournir le chiffrement d'objet de données, en option. Pour en savoir plus sur Diameter, consultez la RFC 6733.

Les applications Diameter effectuent des tâches de gestion de services telles que la décision d'accès de l'utilisateur, l'autorisation de service, la qualité de service et le taux de facturation. Bien que les applications Diameter puissent apparaître sur de nombreuses interfaces de plan de commande différentes dans l'architecture LTE, l'ASA inspecte les codes de commande Diameter et les paires attribut-valeur (AVP) pour les interfaces suivantes uniquement :

- S6a : Entité de gestion de la mobilité (MME) – Service d'abonnement local (HSS).
- S9 : Passerelle PDN (PDG) – serveur proxy/serveur AAA 3GPP.
- Rx : fonction des règles de politique et de facturation (PCRF) – fonction de contrôle de session d'appel (CSCF).

L'inspection Diameter ouvre les passages nécessaires pour permettre la communication avec les terminaux Diameter. L'inspection prend en charge 3GPP version 12 et est conforme à la norme RFC 6733. Vous pouvez l'utiliser pour TCP/TLS (en spécifiant un serveur proxy TLS lorsque vous activez l'inspection) et SCTP, mais pas SCTP/DTLS. Utilisez IPsec pour assurer la sécurité des sessions SCTP Diameter.

Vous pouvez éventuellement utiliser une liste des politiques d'inspection Diameter pour filtrer le trafic en fonction de l'ID d'application, des codes de commande et des AVP, afin d'appliquer des actions spéciales telles que l'abandon de paquets ou de connexions, ou leur journalisation. Vous pouvez créer un AVP personnalisé pour les applications Diameter nouvellement enregistrées. Le filtrage vous permet d'affiner le trafic que vous autorisez sur votre réseau.

Remarque Les messages Diameter pour les applications qui fonctionnent sur d'autres interfaces seront autorisés et transmis par défaut. Cependant, vous pouvez configurer une liste des politiques d'inspection Diameter pour abandonner ces applications par ID d'application, bien que vous ne puissiez pas spécifier d'actions en fonction des codes de commande ou des AVP pour ces applications non prises en charge.

Inspection M3UA

M3UA : MTP3 User Adaptation (M3UA) est un protocole client/serveur qui fournit une passerelle vers le réseau SS7 pour les applications IP qui communiquent avec la couche SS7 Message Transfer Part 3 (MTP3). M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP. M3UA est défini dans la RFC 4666.

M3UA utilise SCTP comme couche de transport. Le port SCTP 2905 est le port par défaut.

La couche MTP3 fournit des fonctions de réseau telles que le routage et l'adressage de nœud, mais utilise des codes de point pour identifier les nœuds. La couche M3UA échange les codes de point d'origine (OPC) et les codes de point de destination (DPC). C'est similaire à la façon dont IP utilise les adresses IP pour identifier les nœuds.

L'inspection M3UA fournit une conformité de protocole limitée. Vous pouvez éventuellement mettre en œuvre une vérification stricte de l'état du processus de serveur d'applications (ASP) et une validation supplémentaire des messages pour certains messages. Une vérification stricte de l'état de l'ASP est requise si vous souhaitez un basculement dynamique ou si vous souhaitez effectuer des opérations dans une grappe. Cependant, la vérification stricte de l'état ASP fonctionne uniquement en mode Override, elle ne fonctionne pas si vous êtes en mode Loadsharing ou Broadcast (selon la RFC 4666). L'inspection suppose qu'il y ait un et un seul ASP par terminal.

Vous pouvez éventuellement appliquer la politique d'accès en fonction des codes de point ou des indicateurs de service (SI). Vous pouvez également appliquer une limitation de débit en fonction de la classe et du type de message.

Conformité au protocole M3UA

L'inspection M3UA fournit l'application limitée du protocole suivante. L'inspection abandonne et journalise les paquets qui ne répondent pas aux exigences.

- En-tête du message commun. L'inspection valide tous les champs de l'en-tête commun.
  - Version 1 uniquement.
  - La longueur du message doit être correcte.
  - La classe de type de message avec une valeur réservée n'est pas autorisée.
  - Un ID de message non valide dans la classe de message n'est pas autorisé.
- Message de données de charge utile.
  - Un seul paramètre d'un type donné est autorisé.
  - Les messages de données sur le flux SCTP 0 ne sont pas autorisés.
- Le champ Affected Point Code doit être présent dans les messages suivants ou le message est abandonné : Destination disponible (DAVA), Destination non disponible (DUNA), Audit de l'état de destination (DAUD), Congestion de la signalisation (SCON), Partie utilisateur de destination non disponible (DUPU), Destination restreinte (DRST).
- Si vous activez la validation des balises de message pour les messages suivants, le contenu de certains champs est vérifié et validé. Les messages qui échouent à la validation sont abandonnés.
  - Destination User Part Unavailable (DUPU) : le champ Utilisateur/Cause doit être présent et ne doit contenir que des codes de cause et d'utilisateur valides.
  - Erreur : tous les champs obligatoires doivent être présents et contenir uniquement des valeurs autorisées. Chaque message d'erreur doit contenir les champs obligatoires pour ce code d'erreur.
  - Notification : les champs Type d'état et Informations sur l'état ne doivent contenir que des valeurs autorisées.

- Si vous activez la validation stricte de l'état du processus de serveur d'applications (ASP), le système conserve les états ASP des sessions M3UA et autorise ou abandonne les messages ASP en fonction du résultat de la validation. Si vous n'activez pas la validation stricte de l'état ASP, tous les messages ASP sont transmis sans inspection.

Limites d'inspection M3UA

Voici quelques limites relatives à l'inspection M3UA.

- La NAT n'est pas prise en charge pour les adresses IP intégrées dans les données M3UA.
- La validation stricte de l'état du processus de serveur d'applications (ASP) M3UA dépend de l'inspection avec état SCTP. Ne mettez pas en œuvre le contournement de l'état SCTP et la validation stricte ASP M3UA sur le même trafic.
- Une vérification stricte de l'état de l'ASP est requise si vous souhaitez un basculement dynamique ou si vous souhaitez effectuer des opérations dans une grappe. Cependant, la vérification stricte de l'état ASP ne fonctionne qu'en mode Override. Elle ne fonctionne pas si vous utilisez le mode Loadsharing ou Broadcast (selon la RFC 4666). L'inspection suppose qu'il y ait un et un seul ASP par terminal.

Aperçu de l'inspection de comptabilité RADIUS

L'objectif de l'inspection de comptabilité RADIUS est d'empêcher les attaques de surfacturation sur les réseaux GPRS qui utilisent des serveurs RADIUS. Bien que vous n'ayez pas besoin de la licence Carrier (exploitant) pour mettre en œuvre l'inspection de comptabilité RADIUS, elle n'a d'objet que si vous mettez en œuvre l'inspection GTP et que vous avez une configuration GPRS.

L'attaque par surfacturation dans les réseaux GPRS entraîne la facturation aux consommateurs de services qu'ils n'ont pas utilisés. Dans ce cas, un agresseur malveillant établit une connexion à un serveur et obtient une adresse IP du SGSN. Lorsque l'agresseur met fin à l'appel, le serveur malveillant continue de lui envoyer des paquets, qui sont abandonnés par le GGSN, mais la connexion du serveur reste active. L'adresse IP attribuée à l'agresseur malveillant est libérée et réattribuée à un utilisateur légitime qui sera ensuite facturé pour les services que l'agresseur utilisera.

L'inspection de comptabilité RADIUS empêche ce type d'attaque en vérifiant que le trafic vu par le GGSN est légitime. Avec la fonctionnalité de comptabilité RADIUS correctement configurée, l'ASA rompt une connexion en fonction de la correspondance de l'attribut Framed IP dans le message Radius Accounting Request Start avec le message Radius Accounting Request Stop. Lorsque le message Stop s'affiche avec l'adresse IP correspondante dans l'attribut Framed IP, l'ASA recherche toutes les connexions dont la source correspond à l'adresse IP.

Vous avez la possibilité de configurer une clé secrète prépartagée avec le serveur RADIUS afin que l'ASA puisse valider le message. Si le secret partagé n'est pas configuré, l'ASA vérifiera uniquement que l'adresse IP source fait partie des adresses configurées autorisées à envoyer les messages RADIUS.



Remarque Lors de l'utilisation de l'inspection de comptabilité RADIUS avec GPRS activé, l'ASA vérifie 3GPP-Session-Stop-Indicator dans les messages Accounting Request STOP afin de gérer correctement les contextes PDP secondaires. Plus précisément, l'ASA exige que les messages Accounting Request STOP comprennent l'attribut 3GPP-SGSN-Address avant de mettre fin aux sessions utilisateur et à toutes les connexions associées. Certains GGSN tiers peuvent ne pas envoyer cet attribut par défaut.

Licences pour l'inspection des protocoles de réseau mobile

L'inspection des protocoles suivants nécessite la licence indiquée dans le tableau ci-dessous.

- GTP
- SCTP
- Diamètre
- M3UA

Modèle	Exigence de licence
ASA virtuel, (tous les modèles)	Licence Carrier (exploitant) (activée par défaut)
Secure Firewall 3100	Licence d'opérateur
Firepower 4100	Licence d'opérateur
Firepower 9300	Licence Mobile Carrier
Tous les autres modèles	La licence Carrier (exploitant) n'est pas disponible sur les autres modèles. Vous ne pouvez pas inspecter ces protocoles.

Valeurs par défaut pour l'inspection GTP

L'inspection GTP n'est pas activée par défaut. Toutefois, si vous l'activez sans préciser votre propre liste d'inspection, une liste par défaut est utilisée et fournit le traitement suivant. Vous ne devez configurer une liste que si vous souhaitez des valeurs différentes.

- Les erreurs ne sont pas autorisées.
- Le nombre maximal de requêtes est de 200.
- Le nombre maximal de tunnels est de 500. Cela équivaut au nombre de contextes PDP (terminaux).
- Le délai d'expiration du terminal GTP est de 30 minutes. Les terminaux comprennent les réseaux GSN (GTPv0,1) et SGW/PGW (GTPv2).
- Le délai d'expiration du contexte PDP est de 30 minutes. Dans GTPv2, il s'agit du délai d'expiration du contexte du support.
- Le délai d'expiration de la demande est de 1 minute.
- Le délai d'expiration de signalisation est de 30 minutes.
- Le délai d'expiration de la tunnellisation est de 1 heure.
- Le délai d'expiration de réponse T3 est de 20 secondes.
- Les ID de message inconnus sont autorisés. Vous pouvez configurer les commandes **match message v1/v2 id range** pour supprimer et consigner toutes les commandes que vous ne prenez pas en charge ou

que vous souhaitez autoriser. Les messages sont considérés comme inconnus s'ils sont non définis ou définis dans les versions GTP que le système ne prend pas en charge.

Configurer l'inspection du réseau mobile

Les inspections pour les protocoles utilisés dans les réseaux mobiles ne sont pas activées par défaut. Vous devez les configurer si vous souhaitez prendre en charge les réseaux mobiles.

Procédure

Étape 1 (Facultatif) Configurer une liste des politiques d'inspection GTP, à la page 10.

Étape 2 (Facultatif) Configurer une liste des politiques d'inspection SCTP, à la page 14.

Étape 3 (Facultatif) Configurer une liste des politiques d'inspection Diameter, à la page 16.

Si vous souhaitez filtrer sur des paires attribut-valeur (AVP) qui ne sont pas encore prises en charge dans le logiciel, vous pouvez créer une AVP personnalisée à utiliser dans la liste des politiques d'inspection Diameter. Consultez Créer une paire attribut-valeur (AVP) de Diameter personnalisée, à la page 19.

Étape 4 (Facultatif) Si vous souhaitez inspecter le trafic Diameter TCP/TLS chiffré, créez le proxy TLS requis, comme décrit dans Inspection des sessions Diameter chiffrées, à la page 20

Étape 5 (Facultatif) Configurer une liste des politiques d'inspection M3UA, à la page 28

Étape 6 Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Étape 7 (Facultatif) Configurer l'inspection de comptabilité RADIUS, à la page 32.

L'inspection de comptabilité RADIUS protège contre les attaques de surfacturation.

Configurer une liste des politiques d'inspection GTP

Si vous souhaitez appliquer des paramètres supplémentaires au trafic GTP et que la carte par défaut ne répond pas à vos besoins, créez et configurez une carte GTP.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **GTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Cliquez sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue GTP Inspect Map (Liste d'inspection GTP), affichez la configuration actuelle de la liste.

La vue indique si la liste utilise les valeurs par défaut ou si vous l'avez personnalisée. Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces
Le bouton **IMSI Prefix Filtering** (Filtrage de préfixe IMSI) est un raccourci pour configurer le filtrage de préfixe IMSI, qui est expliqué plus loin dans cette procédure.

Étape 5 Cliquez sur l'onglet **Permit Parameters** (Paramètres d'autorisation) et configurez les options souhaitées.

- **Autoriser la réponse** : lorsque l'ASA effectue l'inspection GTP, l'ASA abandonne par défaut les réponses GTP des GSN ou des PGW qui n'ont pas été spécifiées dans la demande GTP. Cette situation se produit lorsque vous utilisez l'équilibrage de charge parmi un ensemble de terminaux GSN/PGW pour assurer l'efficacité et l'évolutivité de GPRS.

  Pour configurer le regroupement GSN/PGW et ainsi prendre en charge l'équilibrage de charge, créez un groupe d'objets réseau qui spécifie les terminaux GSN/PGW et sélectionnez-le en tant que **From Object Group** (Groupe d'objets source). De même, créez un groupe d'objets réseau pour le SGSN/SGW et sélectionnez-le comme «**To Object Group**» (Groupe d'objets de destination). Si le GSN/PGW qui répond appartient au même groupe d'objets que le GSN/PGW auquel la demande GTP a été envoyée et si le SGSN/SGW se trouve dans un groupe d'objets auquel le GSN/PGW qui répond est autorisé à envoyer une réponse GTP, l'ASA permet la réponse.

  Le groupe d'objets réseau peut identifier les terminaux par adresse d'hôte ou par le sous-réseau qui les contient.

- **Erreurs d'autorisation** : indique s'il faut autoriser tous les paquets, y compris les paquets GTP non valides ou les paquets qui échoueraient sinon à l'analyse et seraient abandonnés. Des paquets peuvent toujours être abandonnés en fonction des actions que vous définissez dans la liste des politiques.

Étape 6 Cliquez sur l'onglet **General Parameters** (Paramètres généraux) et configurez les options souhaitées :

- **Nombre maximal de demandes** : le nombre maximal de demandes GTP qui seront mises en file d'attente en attente d'une réponse.
- **Nombre maximal de tunnels** : le nombre maximal de tunnels GTP actifs autorisés. Cela équivaut au nombre de contextes PDP ou de terminaux. La valeur par défaut est 500. Les nouvelles demandes seront abandonnées une fois le nombre maximal de tunnels atteint.
- **Appliquer le délai d'inactivité** : s'il faut appliquer les délais d'inactivité pour les comportements suivants. Les délais d'expiration sont au format hh:mm:ss.
  - Terminal : période maximale d'inactivité avant le retrait d'un terminal GTP.
  - PDP-Context : période maximale d'inactivité avant la suppression du contexte PDP pour une session GTP. Dans GTPv2, il s'agit du contexte de support.

- Demande : période maximale d'inactivité après laquelle une demande est supprimée de la file d'attente de demande. Toutes les réponses ultérieures à une demande abandonnée seront également abandonnées.
- Signalisation : période maximale d'inactivité avant la suppression de la signalisation GTP.
- Délai d'attente de réponse T3 : délai d'attente maximal pour une réponse avant de retirer la connexion.
- Tunnel : période maximale d'inactivité du tunnel GTP avant son démontage.

Étape 7 Cliquez sur l'onglet **IMSI Prefix Filtering (Filtrage de préfixe IMSI)** et configurez le filtrage de préfixe IMSI si vous le souhaitez.

Par défaut, l'inspection GTP ne vérifie pas les combinaisons valides du code de pays mobile (MCC)/du code de réseau mobile (MNC). Si vous configurez le filtrage de préfixe IMSI, le MCC et le MNC dans l'IMSI du paquet reçu sont comparés aux combinaisons MCC/MNC configurées. Le système prend ensuite l'une des actions suivantes en fonction de l'option **Drop** (abandon) :

- **Drop not selected** (abandon non sélectionné) (par défaut) : le paquet est abandonné s'il ne correspond à aucune des combinaisons.
- **Drop selected** (abandon sélectionné) : le paquet est abandonné s'il correspond à au moins une combinaison.

Le code de pays mobile est une valeur non nulle à trois chiffres; ajoutez des zéros comme préfixe pour les valeurs à un ou à deux chiffres. Le code de réseau mobile est une valeur à deux ou trois chiffres.

Ajoutez toutes les combinaisons MCC et MNC que vous souhaitez autoriser ou abandonner. Par défaut, l'ASA ne vérifie pas la validité des combinaisons MNC et MCC. Vous devez donc vérifier la validité des combinaisons configurées. Pour en savoir plus sur les codes MCC et MNC, consultez la recommandation de l'UIT E.212, *Plan d'identification pour les stations mobiles terrestres*.

Étape 8 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère :
   - **Access Point Name** (Nom du point d'accès) : correspond au nom du point d'accès avec l'expression régulière ou la liste d'expressions régulières spécifiée. Par défaut, tous les messages avec des noms de point d'accès valides sont inspectés et n'importe quel nom est autorisé.
   - **Message ID** (ID du message) : correspond à l'ID du message, de 1 à 255. Vous pouvez spécifier une valeur ou une plage de valeurs. Vous devez préciser si le message est destiné à GTPv1 (qui comprend GTPv0) ou GTPv2. Par défaut, tous les ID de message valides sont autorisés.
   - **Message Length** (Longueur du message) : correspond aux messages dans lesquels la longueur de la charge utile UDP est comprise entre la longueur minimale et la longueur maximale spécifiées.

- **Version** : correspond à la version GTP, de 0 à 255. Vous pouvez spécifier une valeur ou une plage de valeurs. Par défaut, toutes les versions de GTP sont autorisées.
- **MSISDN** : correspond à l'élément d'information Mobile Station International Subscriber Directory Number (MSISDN) dans les messages Create PDP Context request, Create session request et Modify Bearer Response par rapport à l'expression régulière ou à la liste d'expressions régulières spécifiée. L'expression régulière peut identifier un MSISDN spécifique ou une plage de MSISDN en fonction du premier nombre x de chiffres. Le filtrage MSISDN est pris en charge pour GTPv1 et GTPv2 uniquement.
- **Selection Mode** (Mode de sélection) : correspond à l'élément d'information Selection Mode dans la demande Create PDP Context request. Le mode de sélection spécifie l'origine du nom de point d'accès (APN) dans le message et peut être l'un des suivants. Le filtrage en mode de sélection est pris en charge pour GTPv1 et GTPv2 uniquement.
  - 0 : vérifié. L'APN a été fourni par la station mobile ou le réseau, et l'abonnement est vérifié.
  - 1 : station mobile. L'APN a été fourni par la station mobile, et l'abonnement n'est pas vérifié.
  - 2 : réseau. L'APN a été fourni par le réseau, et l'abonnement n'est pas vérifié.
  - 3 : réservé, non utilisé.

c) Pour la correspondance d'ID de message, choisissez d'abandonner le paquet ou d'appliquer une limite de débit en paquets par seconde. L'action pour toutes les autres correspondances est d'abandonner le paquet. Pour toutes les correspondances, vous pouvez choisir d'activer la journalisation.
d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 9 Cliquez sur l'onglet **Anti-Replay Protection** (Protection anti-replay) et configurez les options anti-replay.

- **Activer la fenêtre de relecture des paquets de données** : s'il faut activer l'anti-relecture en spécifiant une fenêtre glissante pour les messages GTP-U. La taille de la fenêtre glissante est en nombre de messages et peut être de 128, 256, 512 ou 1 024. Lorsque des messages valides s'affichent, la fenêtre se déplace vers les nouveaux numéros de séquence. Les numéros de séquence sont compris entre 0 et 65 535, avec encapsulation lorsqu'ils atteignent le maximum, et ils sont uniques par contexte PDP. Les messages sont considérés comme valides si leurs numéros de séquence se trouvent dans la fenêtre. L'anti-replay permet d'éviter le détournement de session ou les attaques DoS, qui peuvent se produire lorsqu'un pirate capture des paquets de données GTP et les rejoue.

Étape 10 Cliquez sur l'onglet **User-Spoofing** (Usurpation d'utilisateur) et configurez les options anti-usurpation d'utilisateur.

- **GTP Header Check** (Vérification de l'en-tête GTP) : indique s'il faut vérifier que la charge utile interne d'un paquet de données GTP est un paquet IP valide, et abandonner le paquet s'il a un en-tête non IP. Vous devez sélectionner cette option pour mettre en œuvre l'anti-usurpation d'adresse.
- **Anti-Spoofin**g (Anti-usurpation d'adresse) : indique s'il faut vérifier que l'adresse IP de l'utilisateur mobile dans l'en-tête IP de la charge utile interne correspond à l'adresse IP attribuée dans les messages de contrôle GTP tels que Create Session Response, et abandonner le message si les adresses IP ne correspondent pas. Les pirates peuvent se faire passer pour un autre client en utilisant une adresse IP différente de celle attribuée par GTP-C. L'anti-usurpation d'adresse vérifie si l'adresse GTP-U utilisée est bien celle qui a été attribuée à l'aide de GTP-C. Cette vérification prend en charge les types de PDN IPv4, IPv6 et IPv4v6.

Si la station mobile obtient son adresse à l'aide de DHCP, l'adresse IP de l'utilisateur final dans GTPv2 est 0.0.0.0 (IPv4) ou *le préfixe*::0 (IPv6). Dans ce cas, le système met à jour l'adresse IP de l'utilisateur final avec la première adresse IP trouvée dans les paquets internes. Vous pouvez modifier le comportement par défaut des adresses obtenues par DHCP à l'aide des mots-clés suivants :

- **GTPV2-DHCP-ByPass** : ne mettez pas à jour l'adresse 0.0.0.0 ou *le préfixe*::0. Au lieu de cela, autorisez les paquets dont l'adresse IP de l'utilisateur final est 0.0.0.0 ou *le préfixe*::0. Cette option contourne la vérification anti-usurpation d'adresse lorsque DHCP est utilisé pour obtenir l'adresse IP.
- **GTPV2-DHCP-DROP** : ne mettez pas à jour l'adresse 0.0.0.0 ou *le préfixe*::0. Au lieu de cela, abandonnez tous les paquets dont l'adresse IP de l'utilisateur final est 0.0.0.0 ou *le préfixe*::0. Cette option empêche l'accès pour les utilisateurs qui utilisent DHCP pour obtenir l'adresse IP.

Étape 11 Cliquez sur l'onglet **Location-Logging** (journalisation de l'emplacement) et configurez les options de journalisation de l'emplacement.

- **Location Logging** (Journalisation de l'emplacement) : indique s'il faut consigner l'emplacement des abonnés pour suivre les modifications d'emplacement des stations mobiles. Le suivi des modifications d'emplacement peut vous aider à identifier les frais d'itinérance potentiellement frauduleux. Lorsque vous activez la journalisation des emplacements, le système génère des messages de journal système pour les emplacements nouveaux (message 324010) ou modifiés (message 324011) pour chaque identité internationale d'abonné mobile (IMSI).

  Sélectionnez l'option **Cell-ID** (ID de cellule) si vous souhaitez que les messages de journalisation comprennent l'identification globale de cellule (CGI) ou l'identifiant global de cellule E-UTRAN (ECGI) où l'utilisateur est actuellement enregistré.

Étape 12 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection GTP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection GTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Configurer une liste des politiques d'inspection SCTP

Pour appliquer d'autres actions au trafic SCTP en fonction de l'identifiant de protocole de charge utile (PPID) spécifique à l'application, comme la limitation de débit, créez une liste des politiques d'inspection SCTP à utiliser par la politique de service.

Remarque Les PPID se trouvent dans des fragments de données, et un paquet donné peut avoir plusieurs fragments de données ou même un fragment de contrôle. Si un paquet comprend un fragment de contrôle ou plusieurs fragments de données, le paquet ne sera pas abandonné, même si l'action attribuée est abandonnée. Par exemple, si vous configurez une liste des politiques d'inspection SCTP pour abandonner le PPID 26 et qu'un bloc de données PPID 26 est combiné dans un paquet avec un bloc de données PPID Diameter, ce paquet ne sera pas abandonné.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SCTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Abandonnez, limitez le débit ou journalisez le trafic en fonction du PPID dans les fragments de données SCTP.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (Correspondance) (le trafic doit correspondre au PPID) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au PPID).

Par exemple, si vous sélectionnez No Match (Aucune correspondance) pour le PPID Diameter, tous les PPID, à l'exception de Diameter, sont exclus de la carte de trafic.

c) Choisissez **Minimum Payload PID** (PID de charge utile minimal) et, éventuellement, **Maximum Payload PID** (PID de charge utile maximal) à faire correspondre.

Vous pouvez saisir les PPID par nom ou par numéro (0 à 4 294 967 295). Cliquez sur le bouton **...** dans chaque champ pour effectuer une sélection dans une liste de PPID. Si vous sélectionnez un PPID maximal, la correspondance s'applique à la plage de PPID

Vous pouvez trouver la liste actuelle des PPID SCTP à l'adresse http://www.iana.org/assignments/sctp-paramètres/sctp-paramètres.xhtml#sctp-paramètres-25.

d) Choisissez d'abandonner (et de journaliser), de journaliser ou de limiter le débit (en kilobits par seconde, kbps) des paquets correspondants.

e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 5 Cliquez sur **OK** dans la boîte de dialogue SCTP Inspect Map (Liste d'inspection SCTP).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection SCTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Configurer une liste des politiques d'inspection Diameter

Vous pouvez créer une liste des politiques d'inspection Diameter pour filtrer divers éléments de protocole Diameter. Vous pouvez ensuite supprimer ou journaliser sélectivement les connexions.

Pour configurer le filtrage de message Diameter, vous devez avoir une bonne connaissance de ces éléments de protocole tels qu'ils sont définis dans les RFC et les spécifications techniques. Par exemple, l'IETF dispose d'une liste des applications enregistrées, des codes de commande et des paires attribut-valeur à l'adresse http://www.iana.org/assignments/aaa-paramètres/aaa-paramètres.xhtml, bien que l'inspection Diameter ne prenne pas en charge tous éléments répertoriés. Consultez le site Web de 3GPP pour connaître leurs caractéristiques techniques.

Vous pouvez éventuellement créer une carte de trafic d'inspection Diameter pour définir les critères de filtrage des messages pour l'inspection Diameter. L'autre option consiste à définir les critères de filtrage directement dans la liste des politiques d'inspection Diameter. La différence entre la création d'une carte de trafic et la définition des critères de filtrage directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafics. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafic sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic Diameter en sélectionnant **Configuration** > **Firewall** > **Objects** > **Class Maps (Cartes de trafic)** > **Diameter** > **(Configuration** > **Pare-feu** > **Objets** > **cartes de trafic** > **Diameter**), ou en les créant lors de la configuration de la liste des politiques d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **Diameter**

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.

- Sélectionnez une liste et cliquez sur **Edit** (Modifier) pour afficher son contenu.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Parameters** (Paramètres) et choisissez les options souhaitées. si vous souhaitez consigner les messages contenant des éléments Diameter non pris en charge.

- **Unsupported Parameters** (Paramètres non pris en charge) : indique si vous souhaitez consigner les messages contenant des éléments Diameter non pris en charge. Vous pouvez consigner les éléments **Application ID** (ID d'application), **Command Code** (Code de commande) ou **Attribute Value Pair (AVP)** (Paire attribut-valeur (AVP)) qui ne sont pas directement pris en charge.
- **Strict Diameter Validation Parameters** (Paramètres de validation Diameter stricte) : active la conformité stricte du protocole Diameter à la RFC 6733. Par défaut, l'inspection garantit que les trames Diameter sont conformes à la RFC. Vous pouvez ajouter une validation de message liée à la session et une validation de machine d'état.

Étape 5 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic Diameter, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir directement le critère, ou **Multiple Match** (Correspondances multiples), auquel cas vous sélectionnez la carte de trafic Diameter qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère comme suit :

- **Application ID** (ID d'application) : saisissez le nom ou le numéro de l'application Diameter (de 0 à 4 294 967 295). S'il y a une plage d'applications numérotées consécutivement que vous souhaitez mettre en correspondance, vous pouvez inclure un deuxième identifiant. Vous pouvez définir la plage par nom ou numéro d'application, et elle s'applique à tous les nombres entre le premier et le deuxième ID.

  Ces applications sont enregistrées auprès de l'IANA. Voici les applications principales prises en charge, mais vous pouvez filtrer d'autres applications.

  - **3gpp-rx-ts29214** (16777236)
  - **3gpp-s6a** (16777251)
  - **3gpp-s9** (16777267)
  - **common-message** (0). Il s'agit du protocole Diameter de base.

- **Command Code** (Code de commande) : saisissez le nom ou le numéro du code de commande Diameter (0 à 4 294 967 295). S'il existe une plage de codes de commande numérotés consécutivement à laquelle vous souhaitez mettre en correspondance, vous pouvez inclure un deuxième code. Vous

pouvez définir la plage par nom ou numéro de code de commande, et elle s'applique à tous les nombres entre le premier et le deuxième codes.

Par exemple, pour faire correspondre le code de commande de demande/réponse d'échange de capacité, CER/CEA, saisissez **cer-cea**.

- **Attribute Value Pair** (Paire attribut-valeur) : vous pouvez mettre en correspondance l'AVP par attribut uniquement, une plage d'AVP ou un AVP en fonction de la valeur de l'attribut. Pour **AVP Begin Value** (Valeur de début d'AVP), vous pouvez spécifier le nom d'un AVP personnalisé ou enregistré dans les spécifications techniques des RFC ou de 3GPP et directement pris en charge dans le logiciel. Cliquez sur le bouton **...** dans le champ pour choisir un élément dans une liste.

  Si vous souhaitez faire correspondre une plage d'AVP, spécifiez AVP **End Value** (Valeur de fin d'AVP) par numéro uniquement. Si vous souhaitez faire correspondre un AVP par sa valeur, vous ne pouvez pas spécifier de deuxième code.

  Vous pouvez affiner la correspondance en précisant l' **ID de fournisseur**facultatif, de 0 à 4 294 967 295. Par exemple, l'ID du fournisseur 3GPP est 10415, l'IETF est 0.

  Vous pouvez configurer la mise en correspondance de valeur uniquement si le type de données de l'AVP est pris en charge. Par exemple, vous pouvez spécifier une adresse IP pour un AVP qui a le type de données d'adresse. La liste des AVP affiche le type de données pour chacun. La façon dont vous spécifiez la valeur diffère en fonction du type de données AVP :

  - Diameter Identity, Diameter URI, Octet String : sélectionnez l'expression régulière ou les objets de liste d'expressions régulières pour correspondre à ces types de données.
  - Adresse : spécifiez l'adresse IPv4 ou IPv6 pour la correspondance. Par exemple, 10.100.10.10 ou 2001:DB8::0DB8:800:200C:417A.
  - Temps : précisez les dates et l'heure de début et de fin. Les deux sont requis. L'heure est au format 24 heures.
  - Numérique : spécifiez une plage de numéros. La plage de numéros valide dépend du type de données :
    - Integer32 : -2 147 483 647 à 2 147 483 647
    - Integer64 : -9 223 372 036 854 775 807 à 9 223 372 036 854 775 807
    - Unsigned32 : 0 à 4 294 967 295
    - Unsigned64 : 0 à 18 446 744 073 709 551 615
    - Float32 : représentation en point décimal avec une précision de 8 chiffres
    - Float64 : représentation en point décimal avec une précision de 16 chiffres

d) Choisissez l'action à entreprendre pour le trafic correspondant : abandonner le paquet, abandonner la connexion ou se connecter.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue Diameter Inspect Map (Liste d'inspection Diameter).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection Diameter.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Créer une paire attribut-valeur (AVP) de Diameter personnalisée

À mesure que de nouvelles paires attribut-valeur (AVP) sont définies et enregistrées, vous pouvez créer des AVP Diameter personnalisées pour les définir et les utiliser dans votre liste des politiques d'inspection Diameter. Vous obtiendriez les informations dont vous avez besoin pour créer l'AVP à partir de la RFC ou d'une autre source qui définit l'AVP.

Créez des AVP personnalisées uniquement si vous souhaitez les utiliser dans une liste des politiques d'inspection Diameter ou une carte de trafic pour la correspondance d'AVP.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **Diameter AVP (AVP Diameter)** .

Étape 2 Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.

Lorsque vous modifiez un AVP, vous pouvez modifier la description uniquement.

Étape 3 Configurez les options suivantes :

- **Name**(nom) : le nom de l'AVP personnalisé que vous créez, jusqu'à 32 caractères. Vous vous référerez à ce nom dans une liste des politiques d'inspection ou une carte de trafic lors de la définition d'une correspondance de paire attribut-valeur.
- **Custom Code** (Code personnalisé) : valeur du code AVP personnalisé, de 256 à 4 294 967 295. Vous ne pouvez pas saisir une combinaison de code et d'identifiant de fournisseur qui est déjà définie dans le système.
- **Data Type** (Type de données) : type de données de l'AVP. Vous pouvez définir les types d'AVP suivants. Si le nouvel AVP est d'un type différent, vous ne pouvez pas créer d'AVP personnalisé pour celui-ci.
  - Adresse (pour les adresses IP)
  - Identité de Diameter
  - Identifiant de ressource uniforme (URI) Diameter
  - Nombre à virgule flottante 32 bits
  - Nombre à virgule flottante 64 bits
  - Nombre entier de 32 bits
  - Nombre entier de 64 bits
  - Chaîne d'octets
  - Durée
  - Entier non signé 32 bits

- Entier non signé 64 bits

- **Vendor ID** (ID du fournisseur) : facultatif. Le numéro d'ID du fournisseur qui a défini l'AVP, de 0 à 4 294 967 295. Par exemple, l'ID du fournisseur 3GPP est 10415, l'IETF est 0.
- **Description** : (facultatif.) Une description de l'AVP, jusqu'à 80 caractères.

Étape 4 Cliquez sur **OK**.

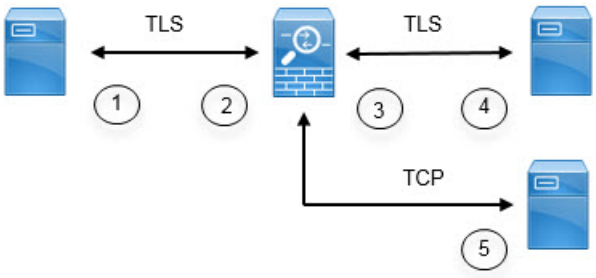
Inspection des sessions Diameter chiffrées

Si une application Diameter utilise des données chiffrées sur TCP, l'inspection ne peut pas voir à l'intérieur des paquets pour mettre en œuvre vos règles de filtrage de message. Ainsi, si vous créez des règles de filtrage et que vous souhaitez qu'elles s'appliquent également au trafic TCP chiffré, vous devez configurer un proxy TLS. Vous avez également besoin d'un proxy si vous souhaitez appliquer strictement le protocole sur le trafic chiffré. Cette configuration ne s'applique pas au trafic SCTP/DTLS.

Le proxy TLS agit en tant qu'homme du milieu. Il déchiffre le trafic, l'inspecte, puis le chiffre à nouveau et l'envoie à la destination prévue. Ainsi, les deux côtés de la connexion, le serveur Diameter et le client Diameter, doivent faire confiance à l'ASA et toutes les parties doivent avoir les certificats requis. Vous devez avoir une bonne compréhension des certificats numériques pour mettre en œuvre le proxy TLS. Veuillez lire le chapitre sur les certificats numériques dans le guide de configuration générale ASA.

L'illustration suivante montre la relation entre le client et le serveur Diameter, l'ASA et les exigences de certification pour établir la confiance. Dans ce modèle, un client Diameter est un MME (Mobility Management Entity) et non un utilisateur final. Le certificat de l'autorité de certification de chaque côté d'un lien est celui utilisé pour signer le certificat de l'autre côté du lien. Par exemple, le certificat de l'autorité de certification du proxy TLS de l'ASA est celui utilisé pour signer le certificat client Diameter/TLS.

Illustration 2 : Inspection TLS Diameter



1	Client TLS Diameter (MME) • Certificat d'identité du client • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur proxy TLS ASA	2	Serveur proxy TLS ASA • Certificat d'identité du serveur • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du client TLS Diameter

3	Client proxy TLS ASA • Certificat d'identité du client (statique ou LDC) • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur TLS Diameter	4	Serveur TLS Diameter (proxy complet) • Certificat d'identité du serveur • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du client proxy TLS ASA
5	Serveur TCP Diameter (déchargement TLS).	—	—

Vous avez les options suivantes pour configurer le proxy TLS pour l'inspection Diameter :

- Proxy TLS complet : chiffrez le trafic entre l'ASA et les clients Diameter, ainsi qu'entre l'ASA et le serveur Diameter. Vous avez les options suivantes pour établir la relation d'approbation avec le serveur TLS :
  - Utilisez un point de confiance client proxy statique. L'ASA présente le même certificat pour chaque client Diameter lors de la communication avec le serveur Diameter. Comme tous les clients se présentent de la même manière, le serveur Diameter ne peut pas fournir de services différentiels par client. D'autre part, cette option est plus rapide que la méthode LDC.
  - Utilisez des certificats dynamiques locaux (LDC). Avec cette option, l'ASA présente des certificats uniques par client Diameter lors de la communication avec le serveur Diameter. Le LDC conserve tous les champs du certificat d'identité du client reçu, à l'exception de sa clé publique et d'une nouvelle signature de l'ASA. Cette méthode donne au serveur Diameter une meilleure visibilité sur le trafic client, ce qui permet de fournir des services différentiels en fonction des caractéristiques du certificat client.
- Déchargement TLS : chiffrez le trafic entre l'ASA et le client Diameter, mais utilisez une connexion en texte clair entre l'ASA et le serveur Diameter. Cette option est viable si le serveur Diameter se trouve dans le même centre de données que l'ASA, où vous êtes certain que le trafic entre les périphériques ne quittera pas la zone protégée. L'utilisation du déchargement TLS peut améliorer les performances, car elle réduit la quantité de traitement de chiffrement requise. Il devrait s'agir de l'option la plus rapide. Le serveur Diameter peut appliquer des services différentiels en fonction de l'adresse IP du client uniquement.

Les trois options utilisent la même configuration pour la relation d'approbation entre l'ASA et les clients Diameter.

Remarque Le proxy TLS utilise TLSv1.0 - 1.2. Vous pouvez configurer la version TLS et la suite de chiffrement.

Les rubriques suivantes expliquent comment configurer le proxy TLS pour l'inspection Diameter.

Configurer la relation de confiance du serveur avec les clients Diameter

L'ASA agit en tant que serveur proxy TLS par rapport aux clients Diameter. Pour établir la relation de confiance mutuelle :

- Vous devez importer le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur de l'ASA dans le client Diameter. Il peut s'agir du magasin de certificats de l'autorité de

certification du client ou de tout autre emplacement utilisé par le client. Consultez la documentation du client pour obtenir les détails exacts de l'utilisation des certificats.

- Vous devez importer le certificat d'autorité de certification utilisé pour signer le certificat du client TLS Diameter afin que l'ASA puisse faire confiance au client.

La procédure suivante explique comment importer le certificat d'autorité de certification utilisé pour signer le certificat du client Diameter et importer un certificat d'identité à utiliser pour le serveur proxy TLS ASA. Au lieu d'importer un certificat d'identité, vous pouvez créer un certificat autosigné sur l'ASA. Sinon, vous pouvez importer ces certificats lorsque vous créez le serveur proxy TLS.

Procédure

Étape 1 Importez le certificat d'autorité de certification utilisé pour signer le certificat du client Diameter dans un point de confiance ASA.

Cette étape permet à l'ASA de faire confiance aux clients Diameter.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats d'autorité de certification)**.
b) Cliquez sur **Add** (Ajouter) et saisissez un nom pour le point de confiance. 5917 Par exemple, **diameter-clients**.
c) Ajoutez le certificat.

Vous pouvez importer le certificat à partir d'un fichier, le coller au format PEM ou utiliser SCEP pour l'importer.

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

Étape 2 Importez le certificat et créez un point de confiance pour le certificat d'identité et la paire de clés du serveur proxy ASA.

Cette étape permet aux clients Diameter de faire confiance à l'ASA.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.
b) Cliquez sur **Add** (Ajouter) et saisissez un nom pour le point de confiance. 5917 Par exemple, **tls-proxy-server-tp**.
c) Sélectionnez **Import the identity certificate from a file** (Importer le certificat d'identité à partir d'un fichier), saisissez la phrase secrète de déchiffrement et sélectionnez le fichier (au format pkcs12).

Vous pouvez également créer un nouveau certificat.

d) Cliquez sur **Add Certificate** (Ajouter le certificat).

Configurer le proxy TLS complet avec un certificat client statique pour l'inspection Diameter

Si le serveur Diameter peut accepter le même certificat pour tous les clients, vous pouvez configurer un certificat client statique que l'ASA utilisera lors de la communication avec le serveur Diameter.

Avec cette configuration, vous devez établir la relation de confiance mutuelle entre l'ASA et les clients (comme expliqué dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 21), ainsi que l'ASA et le serveur Diameter. Voici les exigences de confiance de l'ASA et du serveur Diameter.

- Vous devez importer le certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur Diameter afin que l'ASA puisse valider le certificat d'identité du serveur pendant l'établissement de liaison TLS.
- Vous devez importer le certificat client, un certificat auquel le serveur Diameter fait également confiance. Si le serveur Diameter ne fait pas déjà confiance au certificat, importez le certificat d'autorité de certification utilisé pour le signer sur le serveur. Consultez la documentation du serveur Diameter pour en savoir plus.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy** > **(Configuration Pare-feu Communications unifiées proxy TLS)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Attribuez un nom au proxy TLS, par exemple, **diameter-tls-statique-proxy**. Cliquez sur **Next** (suivant).

Étape 4 Sélectionnez le certificat d'identité du proxy TLS que vous avez ajouté dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 21. Cliquez sur **Next** (suivant).

Si vous n'avez pas encore créé le certificat d'identité, vous pouvez cliquer sur **Manage** (Gérer) pour l'ajouter. Vous pouvez également installer le certificat CA du client Diameter en cliquant sur **Install TLS Server's Certificate** (Installer le certificat du serveur TLS).

Vous pouvez également définir les algorithmes de sécurité (chiffrements) que le serveur peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs. Si vous ne spécifiez pas de chiffrement, les chiffrements par défaut du système sont utilisés.

Remarque
À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et désélectionner l'option **Enable client authentication during TLS Proxy handshake** (Activer l'authentification du client pendant l'établissement de liaison du proxy TLS) dans la configuration du proxy TLS.

Étape 5 Sélectionnez **Specify the proxy certificate for TLS client** (Spécifier le certificat proxy pour le client TLS) et procédez comme suit :

a) Sélectionnez le certificat pour le client du proxy TLS ASA.

Si vous n'avez pas encore ajouté le certificat, cliquez sur **Manage** (Gérer) et ajoutez-le maintenant.

b) Si vous n'avez pas encore ajouté le certificat d'autorité de certification qui a été utilisé pour signer le certificat du serveur Diameter, cliquez sur **Install TLS Client's Certificate** (Installer le certificat du client TLS) et ajoutez-le.

c) (Facultatif) Définissez les algorithmes de sécurité (chiffrements) que le client peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par les paramètres de chiffrement **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)**. Par défaut, le

niveau de chiffrement global est moyen, ce qui signifie que tous les chiffrements sont disponibles, à l'exception de NULL-SHA, DES-CBC-SHA et RC4-MD5. Précisez les chiffrements spécifiques au proxy TLS uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

d) Cliquez sur **Next** (suivant).

Étape 6 Cliquez sur **Finish** (Terminer), puis cliquez sur **Apply** (Appliquer).

Prochaine étape

Vous pouvez maintenant utiliser le proxy TLS dans l'inspection Diameter. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Configurer le proxy TLS complet avec des certificats dynamiques locaux pour l'inspection Diameter

Si le serveur Diameter a besoin de certificats uniques pour chaque client, vous pouvez configurer l'ASA pour générer des certificats dynamiques locaux (LDC). Ces certificats existent pour la durée de la connexion du client et sont ensuite supprimés.

Avec cette configuration, vous devez établir la relation de confiance mutuelle entre l'ASA et les clients (comme expliqué dans la section Configurer la relation de confiance du serveur avec les clients Diameter, à la page 21), ainsi que l'ASA et le serveur Diameter. La configuration est similaire à celle décrite dans Configurer le proxy TLS complet avec un certificat client statique pour l'inspection Diameter, à la page 22, sauf qu'au lieu d'importer un certificat client Diameter, vous configurez le LDC sur l'ASA. Voici les exigences de confiance de l'ASA et du serveur Diameter.

- Vous devez importer le certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur Diameter afin que l'ASA puisse valider le certificat d'identité du serveur pendant l'établissement de liaison TLS.
- Vous devez créer le point de confiance LDC. Vous devez exporter le certificat d'autorité de certification du serveur LDC et l'importer dans le serveur Diameter. L'étape d'exportation est expliquée ci-dessous. Consultez la documentation du serveur Diameter pour obtenir des renseignements sur l'importation des certificats.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy** > **(Configuration Pare-feu Communications unifiées proxy TLS)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Attribuez un nom au proxy TLS, par exemple, **diameter-tls-ldc-proxy**.

Étape 4 Sélectionnez le certificat d'identité du proxy TLS que vous avez ajouté dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 21. Cliquez sur **Next** (suivant).

Si vous n'avez pas encore créé le certificat d'identité, vous pouvez cliquer sur **Manage** (Gérer) pour l'ajouter. Vous pouvez également installer le certificat CA du client Diameter en cliquant sur **Install TLS Server's Certificate** (Installer le certificat du serveur TLS).

Vous pouvez également définir les algorithmes de sécurité (chiffrements) que le serveur peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs. Si vous ne spécifiez pas de chiffrement, les chiffrements par défaut du système sont utilisés.

Remarque
À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et désélectionner l'option **Enable client authentication during TLS Proxy handshake** (Activer l'authentification du client pendant l'établissement de liaison du proxy TLS) dans la configuration du proxy TLS.

Étape 5 Sélectionnez **Specify the internal Certificate Authority to sign for local dynamic certificates** (Spécifier l'autorité de certification interne devant signer les certificats dynamiques locaux) et procédez comme suit (ignorez tout texte lié aux téléphones IP).

Cette procédure suppose que vous créiez un nouveau certificat et une clé. Si vous avez déjà créé le certificat et la clé nécessaires, sélectionnez-les et passez à l'étape des algorithmes de sécurité.

a) Pour Local Dynamic Certificate Key Pair (Paire de clés de certificat dynamique local), cliquez sur **New** (Nouveau). (Vous devrez peut-être redimensionner la boîte de dialogue pour voir le bouton.)
b) Créez un certificat RSA à usage général avec un nouveau nom de paire de clés, tel que **ldc-signer-key**. Cliquez sur **Generate Now** (Générer maintenant) pour créer la clé.

   Vous êtes renvoyé à la boîte de dialogue Gérer les certificats d'identité.

c) Sélectionnez **Certificate** (Certificat) et cliquez sur **Manage** (Gérer) pour créer le certificat et la clé pour le client du proxy TLS ASA.
d) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Gérer les certificats d'identité.
e) Attribuez un nom au point de confiance, tel que **ldc-server**.
f) Sélectionnez **Ajouter un nouveau certificat d'identité**.
g) Pour **Key Pair** (Paire de clés), sélectionnez la même clé que vous avez créée pour la clé de certificat dynamique locale.
h) Pour **Certificate Subnet DN** (DN du sous-réseau du certificat), sélectionnez les attributs de nom distinctif dont vous avez besoin.

   Le nom usuel du périphérique est le nom par défaut. Vérifiez si l'application Diameter a des exigences spécifiques pour le nom du sujet.

i) Sélectionnez **Generate self-signed certificate** (Générer un certificat autosigné). Cette opération est obligatoire.
j) Sélectionnez **Act as a local certificate authority and issue dynamic certificates to TLS Proxy** (Agir en tant qu'autorité de certification locale et émettre des certificats dynamiques vers le proxy TLS). Cette option fait de ce certificat un émetteur LDC.
k) Cliquez sur **Add Certificate** (Ajouter le certificat).

   Vous êtes renvoyé à la boîte de dialogue Gérer les certificats d'identité.

l) Sélectionnez le certificat que vous venez de créer et cliquez sur **Export** (Exporter).

   Vous devez exporter le certificat pour pouvoir l'importer dans le serveur Diameter. Précisez un nom de fichier et un format PEM, puis cliquez sur **Export Certificate** (Exporter le certificat).

   Vous êtes renvoyé à la boîte de dialogue Gérer les certificats d'identité.

m) Avec le certificat toujours sélectionné, cliquez sur **OK**.

Vous êtes renvoyé à l'assistant de proxy TLS. Si le certificat n'est pas sélectionné dans le champ Certificate (Certificat), sélectionnez-le maintenant.

n) (Facultatif) Définissez les algorithmes de sécurité (chiffrements) que le client peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par les paramètres de chiffrement **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)**. Par défaut, le niveau de chiffrement global est moyen, ce qui signifie que tous les chiffrements sont disponibles, à l'exception de NULL-SHA, DES-CBC-SHA et RC4-MD5. Précisez les chiffrements spécifiques au proxy TLS uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

o) Cliquez sur **Next** (suivant).

Étape 6 Cliquez sur **Finish** (Terminer), puis cliquez sur **Apply** (Appliquer).

Étape 7 Vous pouvez maintenant importer le certificat de l'autorité de certification LDC dans le serveur Diameter. Consultez la documentation du serveur Diameter pour connaître la procédure. Notez que les données sont au format Base64. Si votre serveur exige le format binaire ou DER, vous devrez utiliser les outils OpenSSL pour convertir les formats.

Prochaine étape

Vous pouvez maintenant utiliser le proxy TLS dans l'inspection Diameter. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Configurer le serveur mandataire TLS avec déchargement TLS pour l'inspection Diameter

Si vous êtes certain que le chemin réseau entre l'appareil de sécurité adaptable Cisco et le serveur Diameter est sécurisé, vous pouvez éviter le coût de performance du chiffrement des données entre l'appareil de sécurité adaptable Cisco et le serveur. Avec le déchargement TLS, le serveur proxy TLS chiffre/déchiffre les sessions entre le client Diameter et l'ASA, mais utilise du texte en clair avec le serveur Diameter.

Avec cette configuration, vous devez établir la relation d'approbation mutuelle entre l'appareil de sécurité adaptable Cisco et les clients uniquement, ce qui simplifie la configuration. Avant d'effectuer la procédure suivante, effectuez les étapes dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 21.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy** > **(Configuration** > **Pare-feu** > **Communications unifiées** > **Serveur proxy TLS)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Attribuez un nom au serveur proxy TLS, par exemple, **Diameter-tls-offload-proxy**.

Étape 4 Sélectionnez le certificat d'identité du serveur proxy TLS que vous avez ajouté dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 21. Cliquez sur **Next** (suivant).

Si vous n'avez pas encore créé le certificat d'identité, vous pouvez cliquer sur **Manage** (Gérer) pour l'ajouter. Vous pouvez également installer le certificat CA du client Diameter en cliquant sur **Install TLS Server's Certificate** (Installer le certificat du serveur TLS).

Vous pouvez également définir les algorithmes de sécurité (chiffrements) que le serveur peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs. Si vous ne spécifiez pas de chiffrement, les chiffrements par défaut du système sont utilisés.

Remarque
À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et désélectionner l'option **Enable client authentication during TLS Proxy handshake** (Activer l'authentification du client pendant l'établissement de liaison du serveur proxy TLS) dans la configuration du serveur proxy TLS.

Étape 5 Sélectionnez **Configure the proxy client to use clear text to communicate with the remote TCP client** (Configurer le client du serveur proxy afin qu'il utilise du texte en clair pour communiquer avec le client TCP distant), puis cliquez sur **Next** (Suivant).

Étape 6 Cliquez sur **Finish** (Terminer), puis **Apply** (Appliquer).

Étape 7 Comme les ports Diameter sont différents pour TCP et TLS, configurez une règle NAT pour traduire le port TCP en port TLS pour le trafic passant du serveur Diameter vers le client.

Créez une règle NAT d'objet pour chaque serveur Diameter.

a) Choisissez **Configuration** > **Firewall** > **NAT** > **(Configuration** > **Pare-feu** > **NAT)**.
b) Cliquez sur **Add** > **Object NAT Rule** > **(Ajouter Règle NAT d'objet)**.
c) Configurez les propriétés de base :

- **Name** (Nom) : nom de l'objet, par exemple DiameterServerA.
- **Type** (pour l'objet : sélectionnez **Host** (Hôte).
- **IP Version** (Version IP) : IPv4 ou IPv6, selon le cas.
- **IP Address** (Adresse IP) : l'adresse IP du serveur Diameter, par exemple, 10.100.10.10.
- **Add Automatic Address Translation** (Ajouter une traduction automatique d'adresses) : assurez-vous de sélectionner cette option.
- **Type** (pour la règle NAT) : sélectionnez **Static** (Statique).
- **ranslated Addr** (Adresse traduite) : l'adresse IP du serveur Diameter. Il s'agirait de la même adresse IP de l'objet, par exemple, 10.100.10.10.

d) Cliquez sur **Advanced** (Avancé) et configurez les options **Interface** et **Service** suivantes :

- **Source Interface** (Interface source) : sélectionnez l'interface qui se connecte au serveur Diameter.
- **Destination Interface** (Interface de destination) : sélectionnez l'interface qui se connecte au client Diameter.
- **Protocol** (Protocole) : sélectionnez **TCP**.
- **Real Port** (Port réel) : saisissez 3868, qui est le numéro de port TCP Diameter par défaut.
- **Mapped Port** (Port mappé) : saisissez 5868, qui est le numéro de port TLS Diameter par défaut.

e) Cliquez sur **OK**, puis de nouveau sur **OK** dans la boîte de dialogue Add Network Object (Ajouter un objet réseau).

Prochaine étape

Vous pouvez maintenant utiliser le serveur proxy TLS dans l'inspection Diameter. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Configurer une liste des politiques d'inspection M3UA

Utilisez une liste des politiques d'inspection M3UA pour configurer le contrôle d'accès en fonction des codes de point. Vous pouvez également abandonner et limiter le débit des messages par classe et type.

Le format de code de point par défaut est ITU. Si vous utilisez un format différent, précisez le format requis dans la liste des politiques.

Si vous ne souhaitez pas appliquer de politique en fonction du code de point ou de la classe de message, vous n'avez pas besoin de configurer une liste des politiques M3UA. Vous pouvez activer l'inspection sans liste.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **M3UA**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste et cliquez sur **Edit** (Modifier) pour modifier la liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées :

- **SS7** : la variante de SS7 utilisée dans votre réseau : ITU, ANSI, Japon, Chine. Cette option détermine le format valide pour les codes de point. Après avoir configuré l'option et déployé une politique M3UA, vous ne pouvez pas la modifier, sauf si vous avez d'abord supprimé la politique. La variante par défaut est ITU.
- **Enable M3UA Application Server Process (ASP) state validation** (Activer la validation de l'état du processus de serveur d'applications [ASP] M3UA) : indique s'il faut effectuer une validation stricte de l'état du processus de serveur d'applications (ASP). Le système conserve les états ASP des sessions M3UA et autorise ou abandonne les messages ASP en fonction du résultat de la validation. Si vous n'activez pas la validation stricte de l'état ASP, tous les messages ASP sont transmis sans inspection. Une vérification stricte de l'état de l'ASP est requise si vous souhaitez un basculement dynamique ou si vous souhaitez effectuer des opérations dans une grappe. Cependant, la vérification stricte de l'état ASP ne fonctionne qu'en mode Override. Elle ne fonctionne pas si vous utilisez le mode Loadsharing ou Broadcast (selon la RFC 4666). L'inspection suppose qu'il y ait un et un seul ASP par terminal.

- **Enforce Timeout Endpoint (** > Appliquer le délai d'expiration du terminal) : délai d'inactivité pour supprimer les statistiques d'un terminal M3UA, au format hh:mm:ss. Pour n'avoir aucun délai d'expiration, spécifiez 0. La valeur par défaut est de 30 minutes (00:30:00).
- **Enforce Timeout** > **Session** (Appliquer le délai d'expiration de la session) : délai d'inactivité pour supprimer une session M3UA si vous activez la validation stricte de l'état ASP, au format hh:mm:ss. Pour n'avoir aucun délai d'expiration, spécifiez 0. La valeur par défaut est de 30 minutes (00:30:00). La désactivation de ce délai d'expiration peut empêcher le système de supprimer les sessions périmées.
- **Message Tag Validation** (Validation de la balise de message) : indique s'il faut vérifier et valider le contenu de certains champs pour le type de message précisé. Les messages qui échouent à la validation sont abandonnés. La validation diffère en fonction du type de message. Sélectionnez les messages que vous souhaitez valider.
  - Destination User Part Unavailable (DUPU) : le champ Utilisateur/Cause doit être présent et ne doit contenir que des codes de cause et d'utilisateur valides.
  - Erreur : tous les champs obligatoires doivent être présents et contenir uniquement des valeurs autorisées. Chaque message d'erreur doit contenir les champs obligatoires pour ce code d'erreur.
  - Notification : les champs Type d'état et Informations sur l'état ne doivent contenir que des valeurs autorisées.

Étape 5 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (le trafic doit correspondre au critère) ou **No Match** (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère :
   - **Class ID** (ID de classe) : correspond à la classe et au type de message M3UA. Le tableau suivant répertorie les valeurs possibles. Consultez les RFC M3UA et la documentation pour obtenir des renseignements détaillés sur ces messages.

Classe de message M3UA	Type de message
0 (messages de gestion)	0-1
1 (messages de transfert)	1
2 (messages de gestion du réseau de signalisation SS7)	1-6
3 (messages de maintenance de l'état ASP)	1-6
4 (messages de maintenance du trafic ASP)	1 à 4
9 (messages de gestion des clés de routage)	1 à 4

- **OPC** : correspond au code de point d'origine, c'est-à-dire à la source du trafic. Le code de point est au format *zone-région-sp*, où les valeurs possibles pour chaque élément dépendent de la variante SS7 :
  - **ITU** : les codes de point sont de 14 bits au format 3-8-3. Les plages de valeurs sont [0-7]-[0-255]-[0-7].
  - **ANSI** : les codes de point sont de 24 bits au format 8-8-8. Les plages de valeurs sont [0-255]-[0-255]-[0-255].
  - **Japan** : les codes de point sont de 16 bits au format 5-4-7. Les plages de valeurs sont [0-31]-[0-15]-[0-127].
  - **China** : les codes de point sont de 24 bits au format 8-8-8. Les plages de valeurs sont [0-255]-[0-255]-[0-255].
- **DPC** : correspond au code du point de destination. Le code de point est au format *zone-région-sp*, comme expliqué pour **OPC**.
- **Service Indicator** (Indicateur de service) : correspond au numéro d'indicateur de service, de 0 à 15. Voici les indicateurs de service disponibles. Consultez les RFC et la documentation de M3UA pour obtenir des renseignements détaillés sur ces indicateurs de service.
  - 0—Messages de gestion du réseau de signalisation
  - 1—Messages de test et de maintenance du réseau de signalisation
  - 2—Messages spéciaux de test et de maintenance du réseau de signalisation
  - 3—SCCP
  - 4—Partie utilisateur téléphonique
  - 5—Partie utilisateur RNIS
  - 6—Partie utilisateur de données (messages liés aux appels et aux circuits)
  - 7—Partie utilisateur de données (messages d'enregistrement et d'annulation des installations)
  - 8—Réservé pour la partie utilisateur de test MTP
  - 9—Partie utilisateur RNIS à large bande
  - 10—Partie utilisateur RNIS par satellite
  - 11—Réservé
  - 12—Signalisation de type AAL 2
  - 13—Contrôle d'appel indépendant du support
  - 14—Protocole de contrôle de passerelle
  - 15—Réservé

c) Pour la correspondance Class ID (ID de classe), choisissez d'abandonner le paquet ou d'appliquer une limite de débit en paquets par seconde. L'action pour toutes les autres correspondances est d'abandonner le paquet. Pour toutes les correspondances, vous pouvez choisir d'activer la journalisation.

d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue M3UA Inspect Map.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection M3UA.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 31.

Configurer la politique de service d'inspection de réseau mobile

Les inspections pour les protocoles utilisés dans les réseaux mobiles ne sont pas activées dans la politique d'inspection par défaut, vous devez donc les activer si vous avez besoin de ces inspections. Vous pouvez simplement modifier la politique d'inspection globale par défaut pour ajouter ces inspections. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

- Pour modifier la politique globale par défaut, sélectionnez la règle « inspection_default » dans le dossier Global, puis cliquez sur **« Edit »** (Modifier).
- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter)** > **Add** > **Service Policy Rule** > **(Ajouter une règle de politique de service)**. Passez par l'assistant jusqu'à la page Rules (Règles).
- Si vous avez une règle d'inspection de réseau mobile ou une règle à laquelle vous ajoutez ces inspections, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 2 Sur la page ou l'onglet de l'assistant Rule Actions (Actions name), sélectionnez l'onglet **Protocol Inspection** (Inspection de protocole).

Étape 3 (Pour modifier une politique en cours d'utilisation.) Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez désactiver les inspections, puis les réactiver avec le nouveau nom de liste des politiques d'inspection :

a) Décochez les cases pertinentes déjà sélectionnées : **GTP**, **SCTP**, **Diameter**, **M3UA**.
b) Cliquez sur **OK**.
c) Cliquez sur **Apply** (Appliquer).
d) Répétez ces étapes pour revenir à l'onglet Protocol Inspections (Inspections de protocole).

Étape 4 Sélectionnez les protocoles de réseau mobile souhaités : **GTP**, **SCTP**, **Diameter**, **M3UA**.

Étape 5 Si vous souhaitez une inspection autre que celle par défaut pour un ou plusieurs de ces protocoles, cliquez sur **Configure** (Configurer) à côté des options et procédez comme suit :

a) Choisissez d'utiliser la liste par défaut ou d'utiliser une liste des politiques d'inspection que vous avez configurée. Vous pouvez créer la liste à ce moment-ci.

b) (Diameter uniquement.) Pour activer l'inspection Diameter des messages chiffrés, sélectionnez **Enable Encrypted Traffic Inspection** (Activer l'inspection du trafic chiffré) et sélectionnez un proxy TLS à utiliser pour le déchiffrement.

Remarque
Si vous spécifiez un proxy TLS pour l'inspection Diameter et que vous appliquez la redirection de port NAT au trafic du serveur Diameter (par exemple, rediriger le trafic du serveur du port 5868 au port 3868), configurez l'inspection globalement ou sur l'interface d'entrée uniquement. Si vous appliquez l'inspection à l'interface de sortie, le trafic Diameter NATisé contourne l'inspection.

c) Cliquez sur **OK** dans la boîte de dialogue Select Inspect Map (Sélectionner une liste d'inspection).

Étape 6 Cliquez sur **OK** ou **Finish** (Terminer) pour enregistrer la règle de politique de service.

Configurer l'inspection de comptabilité RADIUS

L'inspection de comptabilité RADIUS n'est pas activée par défaut. Vous devez le configurer si vous souhaitez effectuer une inspection de la comptabilité RADIUS.

Procédure

Étape 1 Configurer une liste des politiques d'inspection de comptabilité RADIUS, à la page 32.
Étape 2 Configurer la politique de service d'inspection de comptabilité RADIUS, à la page 33.

Configurer une liste des politiques d'inspection de comptabilité RADIUS

Vous devez créer une liste des politiques d'inspection de comptabilité RADIUS) pour configurer les attributs nécessaires à l'inspection.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **RADIUS Accounting (Comptabilité RADIUS)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Host Parameters** (paramètres de l'hôte) et ajoutez les adresses IP de chaque serveur RADIUS ou GGSN.

Vous pouvez éventuellement inclure une clé secrète afin que l'ASA puisse valider le message. Sans la clé, seule l'adresse IP est vérifiée. L'ASA reçoit une copie des messages de comptabilité RADIUS de ces hôtes.

Étape 5 Cliquez sur l'onglet **Other Parameters** (autres paramètres) et configurez les options souhaitées.

- **Send responses to the originator of the RADIUS accounting message** (Envoyer des réponses à l'initiateur du message de comptabilité RADIUS) : indique s'il faut envoyer des réponses à l'initiateur du message de comptabilité RADIUS.
- **Enforce user timeout** (Appliquer le délai d'inactivité des utilisateurs) : indique s'il faut mettre en œuvre un délai d'inactivité pour les utilisateurs, ainsi que la valeur de ce délai La valeur par défaut est de 1 heure.
- **Enable detection of GPRS accounting** (Activer la détection de la comptabilité GPRS) : indique s'il faut mettre en œuvre la protection contre la surcharge GPRS. L'ASA vérifie l'attribut 3GPP VSA 26-10415 dans les messages d'arrêt et de déconnexion de la demande de comptabilité afin de gérer correctement les contextes de PDP secondaires. Si cet attribut est présent, l'ASA supprime toutes les connexions dont l'adresse IP source correspond à l'adresse IP de l'utilisateur sur l'interface configurée.
- **Validate Attribute** (Valider l'attribut) : critères supplémentaires à utiliser lors de la création d'un tableau des comptes utilisateur lors de la réception des messages Accounting-Request Start. Ces attributs sont utiles lorsque l'ASA décide s'il faut supprimer les connexions.

  Si vous ne spécifiez pas d'attributs supplémentaires à valider, la décision est basée uniquement sur l'adresse IP dans l'attribut d'adresse IP encapsulée. Si vous configurez des attributs supplémentaires et que l'ASA reçoit un message de comptabilité de démarrage qui comprend une adresse en cours de suivi, mais que les autres attributs à valider sont différents, toutes les connexions commencées à l'aide des anciens attributs sont abandonnées, en supposant que l'adresse IP a été réassignée à un nouvel utilisateur.

  Les valeurs sont comprises entre 1 et 191, et vous pouvez entrer la commande plusieurs fois. Pour obtenir la liste des numéros d'attributs et leurs descriptions, consultez le site http://www.iana.org/assignments/radius-types.

Étape 6 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection de comptabilité RADIUS.

Configurer la politique de service d'inspection de comptabilité RADIUS

L'inspection de comptabilité RADIUS n'est pas activée dans la politique d'inspection par défaut. Vous devez donc l'activer si vous avez besoin de cette inspection. Comme l'inspection de comptabilité RADIUS s'adresse au trafic dirigé vers l'ASA, vous devez la configurer comme règle d'inspection de gestion plutôt que comme règle standard.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter) > Add Management Service Policy Rule (Ajouter une règle de politique de service de gestion)**. Passez par l'assistant jusqu'à la page Rules (Règles).
- Si vous avez une règle d'inspection de comptabilité RADIUS ou une règle de gestion à laquelle vous ajoutez l'inspection de comptabilité RADIUS, sélectionnez-la, cliquez sur **Edit** (Modifier), puis cliquez sur l'onglet **Rule Actions** (Actions de règle).

Étape 2 (Pour modifier une politique en cours d'utilisation) Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez désactiver l'inspection de comptabilité RADIUS, puis la réactiver avec le nouveau nom de liste des politiques d'inspection :

a) Sélectionnez **None** (Aucun) pour la liste de comptabilité RADIUS.
b) Cliquez sur **OK**.
c) Cliquez sur **Apply** (Appliquer).
d) Répétez ces étapes pour revenir à l'onglet Protocol Inspections (Inspections de protocole).

Étape 3 Choisissez la liste **RADIUS Accounting** (Comptabilité RADIUS) souhaitée. Vous pouvez créer la liste à ce moment-ci. Pour de plus amples renseignements, voir Configurer une liste des politiques d'inspection de comptabilité RADIUS, à la page 32.

Étape 4 Cliquez sur **OK** ou **Finish** (Terminer) pour enregistrer la règle de politique de service.

Surveillance de l'inspection du réseau mobile

Les rubriques suivantes expliquent comment surveiller l'inspection du réseau mobile.

Surveillance de l'inspection GTP

Pour afficher la configuration GTP, saisissez la commande **show service-policy inspect gtp** en mode d'exécution privilégié. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

Utilisez la commande **show service-policy inspect gtp statistics** pour afficher les statistiques de l'inspection GTP. Voici un exemple de sortie :

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

Vous pouvez obtenir des statistiques pour un terminal GTP spécifique en saisissant l'adresse IP dans la commande **show service-policy inspect gtp statistics** *ip_address*.

```
firewall(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
 GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
  Tunnels Active                    0
  Tunnels Created                   1
  Tunnels Destroyed                 0
  Total Messages Received           1
                         Signalling Messages        Data Messages
  total received                   1                          0
  dropped                          0                          0
  forwarded                        1                          0
```

Utilisez la commande **show service-policy inspect gtp pdp-context** pour afficher les informations liées au contexte PDP. Pour GTPv2, il s'agit du contexte de support. Par exemple :

```
ciscoasa(config)# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:06:14,   Timeout 3:00:00,   APN ssenoauth146

    user_name (IMSI):  50502410121507    MS address: 2005:a00::250:56ff:fe96:eec
    nsapi: 5                linked nsapi: 5
    primary pdp: Y         sgsn is Remote
    sgsn_addr_signal: 10.0.203.22    sgsn_addr_data: 10.0.203.22
    ggsn_addr_signal: 10.0.202.22    ggsn_addr_data: 10.0.202.22
    sgsn control teid:     0x00000001    sgsn data teid:        0x000003e8
    ggsn control teid:     0x000f4240    ggsn data teid:        0x001e8480
    signal_sequence:               18     state:    Ready
...
```

Le contexte de PDP ou de support est identifié par l'ID de tunnel (TID), qui est une combinaison des valeurs d'IMSI et de NSAPI (GTPv0-1) ou d'IMSI et d'EBI (GTPv2). Un tunnel GTP est défini par deux contextes associés dans différents nœuds GSN ou SGW/PGW et est identifié par un ID de tunnel. Un tunnel GTP est nécessaire pour transférer les paquets entre un réseau de données de paquets externe et un utilisateur d'abonné mobile (MS).

Surveillance SCTP

Vous pouvez utiliser les commandes suivantes pour surveiller SCTP. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

- **show service-policy inspect sctp**

  Affiche les statistiques d'inspection SCTP. Le compteur sctp-drop-override s'incrémente chaque fois qu'un PPID correspond à une action d'abandon, mais le paquet n'a pas été abandonné car il contenait des fragments de données avec des PPID différents. Par exemple :

```
ciscoasa# show service-policy inspect sctp
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0, sctp-drop-override 4910
        Match ppid 30 35
          rate-limit 1000 kbps, chunk 2354, dropped 10, bytes 21408, dropped-bytes 958

        Match: ppid 40
           drop, chunk 5849
        Match: ppid 55
           log, chunk 9546
```

- **show sctp** [**detail**]

  Affiche les témoins et les associations SCTP actuels. Ajoutez le mot-clé **detail** pour voir des informations détaillées sur les associations SCTP. La vue détaillée affiche également des informations sur le multi-homing, les flux multiples et le réassemblage de fragments.

```
ciscoasa# show sctp

AssocID: 71adeb15
Local:  192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:
    192.168.108.12(192.168.108.12):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.12(192.168.108.12):2905
    192.168.108.122(192.168.108.122):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.122(192.168.108.122):2905
    192.168.108.12(192.168.108.12):2905 to 192.168.107.12(192.168.107.12):50001
    192.168.107.12(192.168.107.12):50001 to 192.168.108.12(192.168.108.12):2905
```

- **show conn protocol sctp**

  Affiche des renseignements sur les connexions SCTP actuelles.

- **show local-host** [**connection sctp** *start*[*-end*]]

  Affiche les informations sur les hôtes qui effectuent des connexions SCTP par l'intermédiaire de l'ASA, par interface. Ajoutez le mot-clé **connection sctp** pour voir uniquement les hôtes avec le nombre ou la plage spécifié de connexions SCTP.

- **show traffic**

  Affiche les statistiques de connexion SCTP et d'inspection par interface si vous activez la commande **sysopt traffic detailed-statistics**.

Surveillance de Diameter

Vous pouvez utiliser les commandes suivantes pour surveiller Diameter. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

- **show service-policy inspect diameter**

  Affiche les statistiques d'inspection de Diameter. Par exemple :

```
ciscoasa# show service-policy inspect diameter
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        Class-map: log_app
            Log: 5849
         Class-map: block_ip
             drop-connection: 2
```

- **show diameter**

  Affiche les informations d'état pour chaque connexion Diameter. Par exemple :

```
ciscoasa# show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

- **show conn detail**

  Affiche les informations de connexion. Les connexions Diameter sont marquées avec l'indicateur Q.

- **show tls-proxy**

  Affiche les informations sur le proxy TLS si vous en utilisez un dans l'inspection Diameter.

Surveillance M3UA

Vous pouvez utiliser les commandes suivantes pour surveiller M3UA. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

- **show service-policy inspect m3ua drops**

  Affiche les statistiques de rejet pour l'inspection M3UA.

- **show service-policy inspect m3ua endpoint** [*IP_address*]

  Affiche les statistiques pour les terminaux M3UA. Vous pouvez spécifier une adresse IP de terminal pour afficher les informations sur un terminal spécifique. Pour les systèmes à haute disponibilité ou en grappe, les statistiques sont fournies par unité et ne sont pas synchronisées entre les unités. Par exemple :

```
ciscoasa# sh service-policy inspect m3ua endpoint
```

```
M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
                  Forwarded        Dropped          Total Received
All Messages      21                5                 26
DATA Messages     9                 5                 14
M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
                  Forwarded        Dropped          Total Received
All Messages      21                8                 29
DATA Messages     9                 8                 17
```

- **show service-policy inspect m3ua session**

  Affiche les informations sur les sessions M3UA si vous activez la validation stricte de l'état du processus de serveur d'applications (ASP). Les informations comprennent l'ID d'association source, si la session est en échange unique ou double, et dans la mise en grappe, s'il s'agit d'une session de propriétaire de grappe ou d'une session de sauvegarde. Dans une grappe de 3 unités ou plus, vous pouvez voir des sessions de sauvegarde périmées si une unité quitte puis revient à la grappe. Ces sessions périmées sont supprimées lorsqu'elles expirent, sauf si vous avez désactivé le délai d'expiration de session.

```
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
       d - double exchange      , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os
```

- **show service-policy inspect m3ua table**

  Affiche la table d'inspection M3UA en cours d'exécution, y compris les règles de classification.

- **show conn detail**

  Affiche les informations de connexion. Les connexions M3UA sont marquées du drapeau v.

Historique de l'inspection du réseau mobile

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Inspection GTPv2 et améliorations de l'inspection GTPv0/1	9.5(1)	L'inspection GTP peut désormais gérer GTPv2. En outre, l'inspection GTP pour toutes les versions prend désormais en charge les adresses IPv6. Nous avons modifié la boîte de dialogue **GTP Inspect Map (Liste d'inspection GTP)** > **Inspections** pour vous permettre de configurer la mise en correspondance d'ID de message distincts pour GTPv1 et GTPv2. Dans l'onglet **General Parameters** (Paramètres généraux), le délai d'expiration du **GSN** est maintenant le délai d'expiration du **terminal**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Inspection SCTP	9.5(2)	Vous pouvez maintenant appliquer l'inspection de couche d'application au trafic du protocole SCTP (Stream Control Transmission Protocol) pour appliquer des actions en fonction de l'identifiant de protocole de charge utile (PPID). Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **SCTP** ; onglet **Rule Actions (Actions de règle)** > **Protocol Inspection (Inspection de protocole)** de l'assistant d'ajout/de modification **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)** .
Inspection Diameter	9.5(2)	Vous pouvez désormais appliquer l'inspection de couche d'application au trafic Diameter et appliquer des actions en fonction de l'ID d'application, du code de commande et du filtrage de paire attribut-valeur (AVP). Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall** > **(Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **Diameter** et **Diameter AVP (AVP Diameter)** ; onglet **Rule Actions (Actions de règle)** > **Protocol Inspection (Inspection de protocole)** de l'assistant d'ajout/de modification **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)** .
Améliorations de l'inspection Diameter	9.6(1)	Vous pouvez désormais inspecter Diameter sur le trafic TCP/TLS, appliquer une vérification stricte de la conformité du protocole et inspecter Diameter sur SCTP en mode grappe. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **Diameter** ; onglet **Rule Actions (Actions de règle)** > **Protocol Inspection (Inspection du protocole)** de l'assistant d'ajout/de modification **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)** .
Inspection avec état SCTP en mode grappe	9.6(1)	L'inspection dynamique de paquets SCTP fonctionne désormais en mode grappe. Vous pouvez également configurer le contournement d'inspection dynamique de SCTP en mode grappe. Nous n'avons pas ajouté ni modifié d'écrans.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Inspection de l'adaptation de l'utilisateur MTP3 (M3UA)	9.6(2)	Vous pouvez désormais inspecter le trafic M3UA et appliquer des actions en fonction du code de point, de l'indicateur de service, ainsi que de la classe et du type de message. Nous avons ajouté ou modifié les pages suivantes : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **M3UA**; l'onglet **Rule Action (Action de règle)** > **Protocol Inspection (Inspection de protocole)** pour les règles de politique de service
Prise en charge de la réorganisation, du réassemblage et de la fragmentation des flux multiples SCTP. Prise en charge du multi-hébergement SCTP, où les terminaux SCTP ont plusieurs adresses IP.	9.7(1)	Le système prend désormais entièrement en charge la réorganisation, le réassemblage et la fragmentation des flux multiples SCTP, ce qui améliore l'efficacité des inspections Diameter et M3UA pour le trafic SCTP. Le système prend également en charge le multi-hébergement SCTP, où les terminaux ont plusieurs adresses IP chacun. Pour le multi-hébergement, le système ouvre des passages pour les adresses secondaires afin que vous n'ayez pas besoin d'écrire des critères d'accès pour les autoriser. Les terminaux SCTP doivent être limités à 3 adresses IP chacun. Nous n'avons pas modifié d'écrans ASDM.
Améliorations de l'inspection M3UA.	9.7(1)	L'inspection M3UA prend désormais en charge le basculement dynamique, la mise en grappe semi-distribuée et la connexion à plusieurs réseaux. Vous pouvez également configurer la validation stricte de l'état du processus du serveur d'application (ASP) et la validation de divers messages. Une validation stricte de l'état ASP est requise pour le basculement dynamique et la mise en grappe. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **M3UA** Boîtes de dialogue Add/Edit (Ajouter/modifier).
Prise en charge de la définition de la suite de chiffrement SSL du proxy TLS.	9.8(1)	Vous pouvez maintenant définir la suite de chiffrement SSL lorsque l'ASA agit en tant que serveur mandataire TLS. Auparavant, vous ne pouviez définir que les paramètres globaux pour l'ASA sur la page **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)** > **Encryption (Chiffrement)** . Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Unified Communications (Communications unifiées)** > **TLS Proxy (Mandataire TLS)**, boîtes de dialogue Add/Edit (Ajouter/modifier), page **Server Configuration** (Configuration du serveur).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Améliorations de l'inspection GTP pour le filtrage des MSISDN et du mode de sélection, les attaques par rejeu et la protection contre l'usurpation d'adresse de l'utilisateur	9.10(1)	Vous pouvez maintenant configurer l'inspection GTP pour abandonner les messages de création d'un contexte PDP en fonction du numéro de répertoire international de l'abonné de la station mobile (MSISDN) ou du mode de sélection. Vous pouvez également mettre en œuvre une protection contre l'anti-relecture et l'usurpation d'adresse de l'utilisateur. Boîte de dialogue **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **GTP** > **Add/Edit (Ajouter/Modifier)**
Prise en charge de GTPv1 version 10.12.	9.12(1)	Le système prend désormais en charge GTPv1 version 10.12. Auparavant, le système prenait en charge la version 6.1. La nouvelle prise en charge comprend la reconnaissance de 25 messages GTPv1 supplémentaires et de 66 éléments d'information. De plus, il y a un changement de comportement. Désormais, tous les ID de message inconnus sont autorisés. Auparavant, les messages inconnus étaient abandonnés et enregistrés. Nous n'avons pas ajouté ni modifié d'écrans.
Journalisation de la localisation pour les stations mobiles (inspection GTP).	9.13(1)	Vous pouvez configurer l'inspection GTP pour enregistrer l'emplacement initial d'une station mobile et les modifications ultérieures de cet emplacement. Le suivi des modifications d'emplacement peut vous aider à identifier les frais d'itinérance potentiellement frauduleux. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **GTP**
Prise en charge de GTPv2 et GTPv1 version 15.	9.13(1)	Le système prend désormais en charge GTPv2 3GPP 29.274 V15.5.0. Pour GTPv1, la prise en charge va jusqu'à 3GPP 29.060 V15.2.0. La nouvelle prise en charge comprend la reconnaissance de 2 messages supplémentaires et de 53 éléments d'information. Nous n'avons pas modifié d'écrans.
Possibilité de spécifier les préfixes IMSI à abandonner lors de l'inspection GTP.	9.16(1)	L'inspection GTP vous permet de configurer le filtrage de préfixes IMSI, pour identifier les combinaisons code de pays mobile/code de réseau mobile (MCC/MNC) à autoriser. Vous pouvez maintenant effectuer le filtrage IMSI sur les combinaisons MCC/MNC que vous souhaitez abandonner. De cette façon, vous pouvez répertorier les combinaisons indésirables et autoriser toutes les autres combinaisons par défaut. Nous avons modifié les écrans suivants : l'option Drop (Abandon) a été ajoutée à l'onglet IMSI Prefix Filtering (Filtrage des préfixes IMSI) pour les cartes d'inspection GTP.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Secure Firewall 3100 pour la licence d'opérateur	9.18(1)	La licence d'opérateur permet l'inspection des protocoles Diameter, GTP/GPRS et SCTP. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)** .

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.