

Inspection des protocoles vocaux et vidéo

Les rubriques suivantes expliquent l'inspection des applications pour les protocoles vocaux et vidéo. Pour obtenir des renseignements de base sur la raison pour laquelle vous devez utiliser l'inspection pour certains protocoles et les méthodes globales d'application de l'inspection, consultez Premiers pas avec l'inspection du protocole de la couche application.

- Inspection CTIQBE, à la page 1
- Inspection H.323, à la page 2
- Inspection MGCP, à la page 7
- Inspection RTSP, à la page 10
- Inspection SIP, à la page 14
- Inspection Skinny (SCCP), à la page 20
- Inspection STUN, à la page 23
- Historique de l'inspection des protocoles vocaux et vidéo, à la page 24

Inspection CTIQBE

L'inspection de protocole CTIQBE prend en charge la NAT, la PAT et la NAT bidirectionnelle. Cela permet à Cisco IP SoftPhone et à d'autres applications de Cisco TAPI/JTAPI de fonctionner avec succès avec Cisco CallManager pour la configuration des appels dans l'ensemble de l'ASA.

TAPI et JTAPI sont utilisés par de nombreuses applications VoIP de Cisco. CTIQBE est utilisé par Cisco TSP pour communiquer avec Cisco CallManager.

Pour en savoir plus sur l'activation de l'inspection CTIQBE, consultez Configurer l'inspection du protocole de couche d'application.

Limites de l'inspection CTIQBE

Le basculement dynamique des appels CTQBE n'est pas pris en charge.

La section suivante résume les considérations spéciales lors de l'utilisation de l'inspection d'application CTQBE dans des scénarios précis :

- Si deux téléphones IP de Cisco sont enregistrés sur des centres d'appel Cisco différents, qui sont connectés à différentes interfaces de l'appareil de sécurité adaptable Cisco, les appels entre ces deux téléphones échouent.

- Lorsque Cisco CallManager se trouve sur l'interface de sécurité plus élevée que les téléphones IP de Cisco, si une NAT ou une NAT externe est requise pour l'adresse IP de Cisco CallManager, le mappage doit être statique, car Cisco IP SoftPhone nécessite que l'adresse IP de Cisco CallManager soit spécifiée explicitement dans sa configuration Cisco TSP sur le PC.
- Lors de l'utilisation de la PAT ou de la PAT externe, si l'adresse IP de Cisco CallManager doit être traduite, son port TCP 2748 doit être mappé de manière statique au même port de l'adresse PAT (interface) pour que les enregistrements de Cisco IP SoftPhone réussissent. Le port d'écoute CTIQBE (TCP 2748) est fixe et ne peut pas être configuré par l'utilisateur sur Cisco CallManager, Cisco IP SoftPhone ou Cisco TSP.

Inspection H.323

L'inspection H.323 prend en charge les protocoles RAS, H.225 et H.245, et sa fonctionnalité traduit toutes les adresses IP et tous les ports intégrés. Elle effectue le suivi et le filtrage de l'état et peut effectuer une série d'activations de la fonction d'inspection. L'inspection H.323 prend en charge le filtrage des numéros de téléphone, le contrôle dynamique T.120, le contrôle de tunnellisation H.245, les groupes HSI, le suivi de l'état des protocoles, l'application de la durée des appels H.323, le télécopie T.38 et le contrôle audio/vidéo.

L'inspection H.323 est activée par défaut. Vous ne devez la configurer que si vous souhaitez un traitement autre que celui par défaut.

Les sections suivantes décrivent l'inspection des applications H.323.

Aperçu de l'inspection H.323

L'inspection H.323 prend en charge les applications conformes à la norme H.323, telles que Cisco CallManager. H.323 est un ensemble de protocoles définis par l'Union internationale des télécommunications pour les conférences multimédias sur les réseaux locaux. L'ASA prend en charge H.323 jusqu'à la version 6, y compris la fonctionnalité H.323 v3 Multiple Calls on One Call Signaling Channel.

Lorsque l'inspection H.323 est activée, l'ASA prend en charge plusieurs appels sur le même canal de signalisation d'appel, une fonctionnalité introduite avec la version 3 du protocole H.323. Cette fonctionnalité réduit le temps de configuration des appels et réduit l'utilisation des ports sur l'ASA.

Les deux fonctions principales de l'inspection H.323 sont les suivantes :

- Effectuez la NAT pour les adresses IPv4 intégrées nécessaires dans les messages H.225 et H.245. Comme les messages H.323 sont codés au format de codage PER, l'ASA utilise un décodeur ASN.1 pour décoder les messages H.323.
- Attribuez dynamiquement les connexions H.245 et RTP/RTCP négociées. La connexion H.225 peut également être attribuée dynamiquement lors de l'utilisation de RAS.

Fonctionnement de H.323

L'ensemble de protocoles H.323 peut utiliser jusqu'à deux connexions TCP et de quatre à huit connexions UDP. FastConnect utilise une seule connexion TCP et RAS utilise une seule connexion UDP pour l'enregistrement, les autorisations et l'état.

Un client H.323 peut initialement établir une connexion TCP avec un serveur H.323 en utilisant le port TCP 1720 pour demander la configuration de l'appel Q.931. Dans le cadre du processus de configuration de l'appel, le terminal H.323 fournit un numéro de port au client à utiliser pour une connexion TCP H.245. Dans les environnements où le portier H.323 est utilisé, le paquet initial est transmis à l'aide d'UDP.

L'inspection H.323 surveille la connexion TCP Q.931 pour déterminer le numéro de port H.245. Si les terminaux H.323 n'utilisent pas FastConnect, l'ASA alloue dynamiquement la connexion H.245 en fonction de l'inspection des messages H.225. La connexion H.225 peut également être attribuée dynamiquement lors de l'utilisation de RAS.

Dans chaque message H.245, les terminaux H.323 échangent des numéros de port qui sont utilisés pour les flux de données UDP suivants. L'inspection H.323 inspecte les messages H.245 pour identifier ces ports et crée dynamiquement les connexions nécessaires à l'échange des médias. RTP utilise le numéro de port négocié, tandis que RTCP utilise le numéro de port suivant.

Le canal de contrôle H.323 gère les protocoles H.225, H.245 et H.323 RAS. L'inspection H.323 utilise les ports suivants :

- 1718 : port UDP de découverte du Gatekeeper
- 1719 : port UDP RAS
- 1720 : port de contrôle TCP

Vous devez autoriser le trafic pour le port H.323 1719 pour la signalisation RAS. En outre, vous devez autoriser le trafic pour le port H.323 bien connu 1720 pour la signalisation d'appel H.225; cependant, les ports de signalisation H.245 sont négociés entre les terminaux dans la signalisation H.225. Lorsqu'un portier H.323 est utilisé, l'ASA ouvre une connexion H.225 en fonction de l'inspection des messages d'ACF et de RCF.

Après avoir inspecté les messages H.225, l'ASA ouvre le canal H.245, puis inspecte le trafic envoyé sur le canal H.245. Tous les messages H.245 passant par l'ASA sont soumis à l'inspection d'application H.245, qui traduit les adresses IP intégrées et ouvre les canaux de support négociés dans les messages H.245.

Chaque connexion UDP avec un paquet passant par l'inspection H.323 est marquée comme une connexion H.323 et expire avec le délai H.323, comme configuré avec la commande **timeout**.



Remarque Vous pouvez activer la configuration d'appel entre les terminaux H.323 lorsque le portier se trouve dans le réseau. L'ASA comprend des options pour ouvrir des passages pour les appels en fonction des messages RegistrationRequest/RegistrationConfirm (RRQ/RCF). Comme ces messages RRQ/RCF sont échangés avec le Gatekeeper, l'adresse IP du point terminal appelant est inconnue et l'ASA ouvre un passage avec l'adresse IP source et le port 0/0. Par défaut, cette option est activée. Pour activer l'appel de configuration entre les terminaux H.323, entrez la commande **ras-rcf-pinholes enable** en mode de configuration des paramètres lors de la création d'une liste des politiques d'inspection H.323.

Prise en charge H.239 dans les messages H.245

L'ASA se trouve entre deux points terminaux H.323. Lorsque les deux terminaux H.323 configurent une session de téléprésentation afin que les terminaux puissent envoyer et recevoir une présentation de données, telles que des données de feuille de calcul, l'ASA garantit la négociation réussie du protocole H.239 entre les terminaux.

La norme H.239 est une norme qui permet aux terminaux de la série H.300 d'ouvrir un canal vidéo supplémentaire en un seul appel. Dans un appel, un terminal (comme un téléphone vidéo) envoie un canal pour la vidéo et un canal pour la présentation des données. La négociation H.239 a lieu sur le canal H.245.

L'ASA ouvre des passages pour le canal de support supplémentaire et le canal de contrôle de support. Les terminaux utilisent le message de canal logique ouvert (OLC) pour signaler la création d'un nouveau canal. L'extension de message fait partie de la version 13 du protocole H.245.

Le décodage et l'encodage de la session de téléprésentation sont activés par défaut. L'encodage et le décodage H.239 sont effectués par le codeur ASN.1.

Limites de l'inspection H.323

L'inspection H.323 est testée et prise en charge pour Cisco Unified Communications Manager (CUCM) 7.0. Il n'est pas pris en charge pour CUCM 8.0 et les versions ultérieures. L'inspection H.323 peut fonctionner avec d'autres versions et produits.

Voici quelques-uns des problèmes et des limites connus lors de l'utilisation de l'inspection d'application H.323 :

- La PAT est prise en charge, à l'exception de la PAT étendue ou de la PAT par session.
- La PAT statique peut ne pas traduire correctement les adresses IP intégrées dans les champs facultatifs des messages H.323. Si vous rencontrez ce type de problème, n'utilisez pas la PAT statique avec H.323.
- Non pris en charge avec la NAT entre les interfaces de même niveau de sécurité.
- Non pris en charge avec NAT64.
- La NAT avec inspection H.323 n'est pas compatible avec la NAT lorsqu'elle est effectuée directement sur les terminaux. Si vous effectuez une NAT sur les terminaux, désactivez l'inspection H.323.

Configurer la liste des politiques d'inspection H.323

Vous pouvez créer une liste des politiques d'inspection H.323 pour personnaliser les actions d'inspection H.323 si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

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 classe d'expression régulière.

Procédure

Étape 1 (Facultatif) Créez une carte de trafic d'inspection H.323 en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de classe et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de classe vous permet de créer des critères de correspondance plus complexes, et vous pouvez réutiliser les cartes de classe.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de classe, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect h323** [**match-all** | **match-any**] *class_map_name*

Où *class_map_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un des critères. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

b) (Facultatif) : Ajoutez une description à la carte de trafic : **description** *string*

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} : met en correspondance l'appelé avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} : met en correspondance l'appelant avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **match** [**not**] **media-type** {**audio** | **data** | **video**} : correspond au type de média.

Étape 2 Créer une liste des politiques d'inspection H.323 : **policy-map type inspect h323** *policy_map_name*

Où *policy_map_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

Étape 3 (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*

Étape 4 Pour appliquer les actions au trafic correspondant, procédez comme suit.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez Comment plusieurs classes de trafic sont gérées.

a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :

- Si vous avez créé une carte de trafic H.323, spécifiez-la en entrant la commande suivante : **class** *class_map_name*
- Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic H.323. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop** [**log**] : abandonner le paquet. Pour les correspondances de type de support, vous pouvez inclure le mot-clé **log** pour envoyer un message de journal système.
- **drop-connection** : abandonner le paquet et fermer la connexion. Cette option est disponible pour la correspondance de l'appelé ou de l'appelant.
- **reset** : abandonner le paquet, fermer la connexion et envoyer une réinitialisation TCP au serveur ou au client. Cette option est disponible pour la correspondance de l'appelé ou de l'appelant.

Étape 5 Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **ras-rcf-pinholes enable** : active la configuration des appels entre les terminaux H.323. Vous pouvez activer la configuration d'appel entre les terminaux H.323 lorsque le portier se trouve dans le réseau. Utilisez cette option pour ouvrir des trous d'épingle pour les appels basés sur les messages RegistrationRequest/RegistrationConfirm (RRQ/RCF). Comme ces messages RRQ/RCF sont envoyés vers et depuis le Gatekeeper, l'adresse IP du point d'extrémité appelant est inconnue et l'ASA ouvre un trou d'épingle via l'adresse IP/port source 0/0. Par défaut, cette option est activée.
- **timeout users** *time* : définit la limite de durée de l'appel H.323 (au format hh:mm:ss). Pour n'avoir aucun délai d'expiration, spécifiez 00:00:00. La plage est comprise entre 0:0:0 et 1193:0:0.
- **call-party-number** : applique l'envoi du numéro de partie d'appel lors de l'établissement de l'appel.
- **action h245-tunnel-block** {**drop-connection** | **log**} : applique le blocage de tunnel H.245. Précisez si vous souhaitez abandonner la connexion ou simplement la journaliser.
- **rtp-conformance** [**enforce-payloadtype**] : vérifie les paquets RTP circulant dans les passages pour vérifier la conformité du protocole. Le mot-clé facultatif enforce-payloadtype applique le type de charge utile pour qu'il soit audio ou vidéo en fonction de l'échange de signalisation.
- **state-checking** {**h225** | **ras**} : active la validation de la vérification de l'état. Vous pouvez saisir la commande séparément pour activer la vérification de l'état pour H.225 et RAS.
- **early-message** *message_type* : s'il faut autoriser le type spécifié de messages H.225 avant le message SETUP H.225. Vous pouvez autoriser le message **facility** à arriver tôt, conformément à la norme H.460.18.

  Si vous rencontrez des problèmes de configuration d'appels, où les connexions sont fermées avant d'être terminées lors de l'utilisation de H.323/H.225, utilisez cette commande pour autoriser les messages précoces. Assurez-vous également d'activer l'inspection pour les services RAS H.323 et H.225 (ils sont tous deux activés par défaut).

Étape 6 Tout en étant toujours en mode de configuration des paramètres, vous pouvez configurer les groupes HSI.

a) Définissez un groupe HSI et passez en mode de configuration de groupe HSI : **hsi-group** *id*

Où *id* est l'identifiant de groupe HSI. La plage est comprise entre 0 et 2 147 483 647.

b) Ajoutez un HSI au groupe de HSI en utilisant l'adresse IP : **hsi** *ip_address*

Vous pouvez ajouter un maximum de cinq hôtes par groupe de HSI.

c) Ajouter un terminal au groupe HSI : **endpoint** *ip_address if_name*

Où *ip_address* est le terminal à ajouter et *if_name* est l'interface par laquelle le terminal est connecté à l'ASA. Vous pouvez ajouter un maximum de dix terminaux par groupe de HSI.

Exemple

L'exemple suivant montre comment configurer le filtrage de numéro de téléphone :

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection MGCP

L'inspection MGCP n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports MGCP par défaut, de sorte que vous pouvez simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection MGCP. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent l'inspection des applications MGCP.

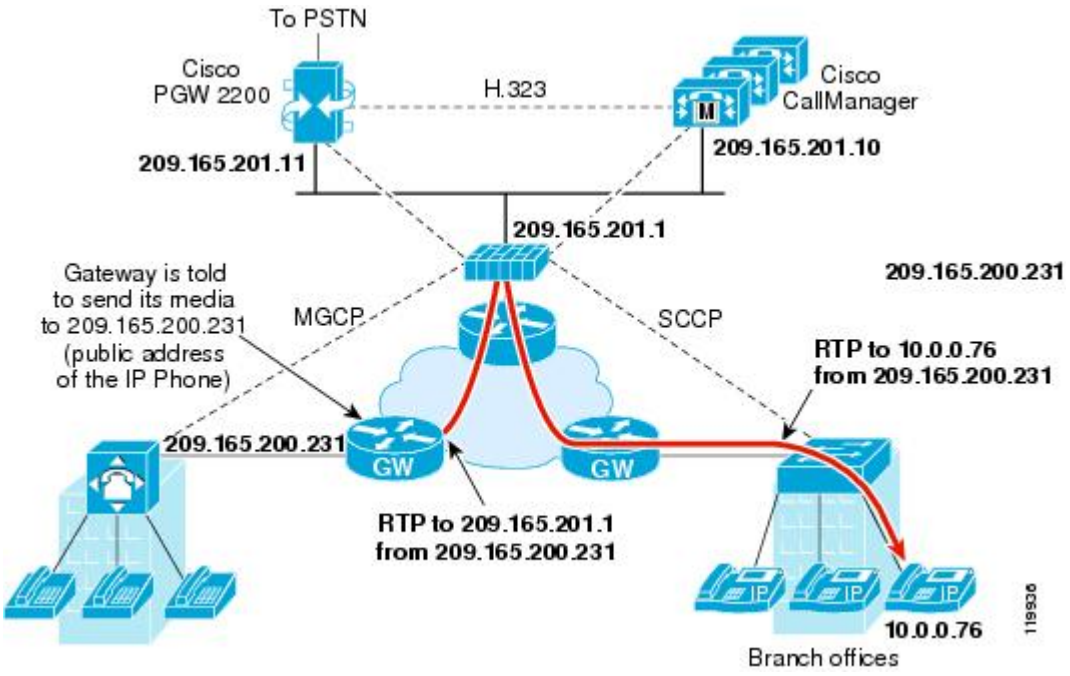
Aperçu de l'inspection MGCP

MGCP est utilisé pour contrôler les passerelles multimédias à partir d'éléments de contrôle d'appel externes appelés contrôleurs de passerelle multimédia ou agents d'appel. Une passerelle multimédia est généralement un élément de réseau qui assure la conversion entre les signaux audio acheminés sur les circuits téléphoniques et les paquets de données acheminés sur Internet ou d'autres réseaux de paquets. L'utilisation de la NAT et de la PAT avec MGCP vous permet de prendre en charge un grand nombre de périphériques sur un réseau interne avec un ensemble limité d'adresses externes (globales). Des exemples de passerelles multimédias sont les suivants :

- Passerelles de liaison, qui assurent l'interface entre le réseau téléphonique et un réseau de voix sur IP. Ces passerelles gèrent généralement un grand nombre de circuits numériques.
- Passerelles résidentielles, qui fournissent une interface analogique traditionnelle (RJ11) à un réseau de voix sur IP. Les exemples de passerelles résidentielles comprennent les modems câble ou les décodeurs câble, les périphériques xDSL et les périphériques sans fil à large bande.
- Passerelles d'entreprise, qui fournissent une interface PBX numérique traditionnelle ou une interface PBX logicielle intégrée à un réseau de voix sur IP.

Les messages MGCP sont transmis sur UDP. Une réponse est renvoyée à l'adresse source (adresse IP et numéro de port UDP) de la commande, mais la réponse peut ne pas provenir de la même adresse que celle à laquelle la commande a été envoyée. Cela peut se produire lorsque plusieurs agents d'appel sont utilisés dans une configuration de basculement et que l'agent d'appel qui a reçu la commande a transmis le contrôle à un agent d'appel de secours, qui envoie ensuite la réponse. La figure suivante illustre comment vous pouvez utiliser la NAT avec MGCP.

Illustration 1 : Utilisation de la NAT avec MGCP



Les terminaux MGCP sont des sources et des destinations physiques ou virtuelles de données. Les passerelles multimédias contiennent des points d'extrémité sur lesquels l'agent d'appel peut créer, modifier et supprimer des connexions pour établir et contrôler les sessions multimédias avec d'autres points d'extrémité multimédias. En outre, l'agent d'appel peut demander aux terminaux de détecter certains événements et de générer des signaux. Les terminaux communiquent automatiquement les modifications de l'état de service à l'agent appelant.

- Les passerelles sont généralement à l'écoute du port UDP 2427 pour recevoir des commandes de l'agent appelant.
- Le port sur lequel l'agent d'appel reçoit les commandes de la passerelle. Les agents d'appel écoutent généralement le port UDP 2727 pour recevoir des commandes de la passerelle.

Remarque L'inspection MGCP ne prend pas en charge l'utilisation d'adresses IP différentes pour la signalisation MGCP et les données RTP. Une pratique courante et recommandée consiste à envoyer les données RTP à partir d'une adresse IP résiliente, telle qu'une adresse de bouclage ou une adresse IP virtuelle; cependant, l'ASA exige que les données RTP proviennent de la même adresse que la signalisation MGCP.

Configurer une liste des politiques d'inspection MGCP

Si le réseau comporte plusieurs agents d'appel et passerelles pour lesquels l'ASA doit ouvrir des passages, créez une liste MGCP. Vous pouvez ensuite appliquer la liste MGCP lorsque vous activez l'inspection MGCP.

Procédure

Étape 1 Pour créer une liste des politiques d'inspection MGCP : **policy-map type inspect mgcp** *policy_map_name*

Où *policy_map_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

Étape 2 (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*

Étape 3 Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

Étape 4 Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option.

- **call-agent** *ip_address group_id* : configure les groupes d'agents d'appel qui peuvent gérer une ou plusieurs passerelles. Les informations de groupe d'agents d'appel sont utilisées pour ouvrir des connexions pour les agents d'appel du groupe (hormis celui auquel une passerelle envoie une commande), afin que n'importe quel agent d'appel puisse envoyer la réponse. Les agents d'appel avec le même group_id appartiennent au même groupe. Un agent d'appel peut appartenir à plusieurs groupes. L'option group_id est un nombre compris entre 0 et 4 294 967 295. L'option ip_address spécifie l'adresse IP de l'agent d'appel.

  Remarque
  Les agents d'appel MGCP envoient des messages AUEP pour déterminer si les terminaux MGCP sont présents. Cela établit un flux dans l'ASA et permet aux terminaux MGCP de s'enregistrer auprès de l'agent d'appel.

- **gateway** *ip_address group_id* : identifie quel groupe d'agents d'appel gère une passerelle particulière. L'adresse IP de la passerelle est spécifiée avec l'option ip_address. L'option group_id est un nombre compris entre 0 et 4 294 967 295 qui doit correspondre à l'identifiant de groupe des agents d'appel qui gèrent la passerelle. Une passerelle ne peut appartenir qu'à un seul groupe.

- **command-queue** *command_limit* : définit le nombre maximal de commandes autorisées dans la file d'attente de commande MGCP, de 1 à 2 147 483 647. Par défaut, c'est 200.

Exemple

L'exemple suivant montre comment définir une liste MGCP :

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection RTSP

L'inspection RTSP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut. Les sections suivantes décrivent l'inspection des applications RTSP.

Survol de l'inspection RTSP

Le moteur d'inspection RTSP permet à l'ASA de transmettre les paquets RTSP. RTSP est utilisé par RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer et Cisco IP/TV.



Remarque Pour Cisco IP/TV, utilisez les ports TCP RTSP 554 et 8554.

Les applications RTSP utilisent le port bien connu 554 avec TCP (rarement UDP) comme canal de contrôle. L'ASA ne prend en charge que TCP, conformément à la RFC 2326. Ce canal de contrôle TCP est utilisé pour négocier les canaux de données utilisés pour transmettre le trafic audio/vidéo, en fonction du mode de transport configuré sur le client.

Les services de transport RDT pris en charge sont les suivants : rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp et x-pn-tng/udp.

L'ASA analyse les messages de réponse Setup avec un code d'état de 200. Si le message de réponse se déplace vers l'intérieur, le serveur est à l'extérieur par rapport à l'ASA et des canaux dynamiques doivent être ouverts

pour les connexions entrantes du serveur. Si le message de réponse est sortant, l'ASA n'a pas besoin d'ouvrir de canaux dynamiques.

L'inspection RTSP ne prend pas en charge la PAT ou la double NAT. En outre, l'ASA ne peut pas reconnaître le camouflage HTTP où les messages RTSP sont masqués dans les messages HTTP.

Exigences de configuration de RealPlayer

Lorsque vous utilisez RealPlayer, il est important de configurer correctement le mode de transport. Pour l'ASA, ajoutez une commande **access-list** du serveur au client, ou vice versa. Pour RealPlayer, modifiez le mode de transport en cliquant sur **Options** > **Preferences (Préférences)** > **Transport** > **RTSP Settings (Paramètres RTSP)**.

Si vous utilisez le mode TCP sur RealPlayer, cochez les cases **Use TCP to Connect to Server** (Utiliser TCP pour la connexion au serveur) et **Attempt to use TCP for all content** (Tenter d'utiliser TCP pour tout le contenu). Sur l'ASA, il n'est pas nécessaire de configurer le moteur d'inspection.

Si vous utilisez le mode UDP sur RealPlayer, cochez les cases **Use TCP to Connect to Server** (Utiliser TCP pour se connecter au serveur) et **Attempt to use UDP for static content** (Tenter d'utiliser UDP pour le contenu statique), et pour le contenu en direct non disponible par multidiffusion. Sur l'ASA, ajoutez une commande **inspect rtsp**.

Limites de l'inspection RSTP

Les restrictions suivantes s'appliquent à l'inspection RSTP :

- L'ASA ne prend pas en charge la multidiffusion RTSP ni les messages RTSP sur UDP.
- L'ASA n'a pas la capacité de reconnaître le camouflage HTTP où les messages RTSP sont masqués dans les messages HTTP.
- L'ASA ne peut pas effectuer la NAT sur les messages RTSP, car les adresses IP intégrées sont contenues dans les fichiers SDP dans le cadre des messages HTTP ou RTSP. Les paquets peuvent être fragmentés et l'ASA ne peut pas effectuer de NAT sur les paquets fragmentés.
- Avec Cisco IP/TV, le nombre de traductions effectuées par l'ASA sur la partie SDP du message est proportionnel au nombre de listes de programmes dans le gestionnaire de contenu (chaque liste de programme peut avoir au moins six adresses IP intégrées).
- Vous pouvez configurer la NAT pour Apple QuickTime 4 ou RealPlayer. Cisco IP/TV ne fonctionne qu'avec la NAT si la visionneuse et le gestionnaire de contenu se trouvent sur le réseau externe et si le serveur se trouve sur le réseau interne.

Configurer une liste des politiques d'inspection RTSP

Vous pouvez créer une liste des politiques d'inspection RTSP pour personnaliser les actions d'inspection RTSP si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

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 (Facultatif) Créez une carte de trafic d'inspection FTP en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de trafic vous permet de créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de trafic, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de classes.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à appliquer dans la liste des politiques d'inspection.

Si vous souhaitez effectuer des actions différentes pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect rtsp** [**match-all** | **match-any**] *class_map_name*

Où *class_map_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un des critères. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

b) (Facultatif) Ajoutez une description à la carte de trafic : **description** *string*

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match** [**not**] **request-method** *method* : correspond à une méthode de demande RTSP. Les méthodes sont les suivantes : announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameter, teardown.
- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*} : correspond à l'URL avec l'expression régulière ou à la liste d'expressions régulières spécifiée.

Étape 2 Pour créer une liste des politiques d'inspection RTSP : **policy-map type inspect rtsp** *policy_map_name*

Où *policy_map_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

Étape 3 (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*

Étape 4 Pour appliquer les actions au trafic correspondant, procédez comme suit.

a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :

- Si vous avez créé une carte de trafic RTSP, spécifiez-la en entrant la commande suivante : **class** *class_map_name*

- Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic RTSP. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop-connection** [**log**] : abandon du paquet, fermeture de la connexion et éventuellement envoi d'un message de journal système. Cette option est disponible pour la mise en correspondance d'URL.
- **log** : envoie un message de journal système.
- **rate-limit** *message_rate* : limite le débit de messages par seconde. Cette option est disponible pour la mise en correspondance de la méthode de demande.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la carte de politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez Comment plusieurs classes de trafic sont gérées.

Étape 5 Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **reserve-port-protect** : restreint l'utilisation des ports de réservation lors de la négociation du support.
- **url-length-limit** *bytes* : définit une limite de longueur d'URL autorisée dans le message, de 0 à 6 000 octets.

Exemple

L'exemple suivant montre comment définir une liste des politiques d'inspection RTSP.

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
```

```
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection SIP

SIP est un protocole très utilisé pour la conférence Internet, la téléphonie, la présence, la notification d'événements et la messagerie instantanée. En partie en raison de leur nature textuelle et en partie en raison de leur flexibilité, les réseaux SIP sont soumis à un grand nombre de menaces de sécurité.

L'inspection des applications SIP fournit la traduction d'adresses dans l'en-tête et le corps du message, l'ouverture dynamique de ports et les vérifications de base de l'intégrité. Elle prend également en charge la sécurité des applications et la conformité des protocoles, qui appliquent l'intégrité des messages SIP et détectent les attaques basées sur SIP.

L'inspection SIP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut ou si vous souhaitez identifier un serveur proxy TLS pour activer l'inspection du trafic chiffré. Les rubriques suivantes expliquent l'inspection SIP plus en détail.

Présentation de l'inspection SIP

Le protocole SIP, tel que défini par l'IETF, permet les sessions de traitement d'appels, en particulier les conférences audio à deux parties, ou « appels ». SIP fonctionne avec SDP pour la signalisation d'appel. SDP spécifie les ports pour le flux de support. À l'aide du protocole SIP, l'ASA peut prendre en charge toutes les passerelles VoIP SIP et tous les serveurs proxy VoIP SIP. SIP et SDP sont définis dans les RFC suivantes :

- SIP : protocole d'initiation de session, RFC 3261
- SDP : protocole de description de session, RFC 2327

Pour prendre en charge les appels SIP par l'intermédiaire de l'ASA, les messages de signalisation pour les adresses de connexion du support, les ports du support et les connexions embryonnaires du support doivent être inspectés, car même si la signalisation est envoyée sur un port de destination bien connu (UDP/TCP 5060), les flux de support sont alloués dynamiquement. De plus, SIP intègre les adresses IP dans la partie données utilisateur du paquet IP. Notez que la longueur maximale de l'URI de la demande SIP prise en charge par l'ASA est de 255.

Les applications de messagerie instantanée (IM) utilisent également des extensions SIP (définies dans la RFC 3428) et des notifications d'événements spécifiques à SIP (RFC 3265). Une fois que les utilisateurs ont lancé une session de conversation (enregistrement/abonnement), les applications de messagerie instantanée utilisent les méthodes MESSAGE/INFO et les réponses 202 Accept lorsque les utilisateurs communiquent entre eux. Par exemple, deux utilisateurs peuvent être en ligne à tout moment, mais pas communiquer pendant des heures. Par conséquent, le moteur d'inspection SIP ouvre des passages qui expirent en fonction de la valeur de délai d'expiration SIP configurée. Cette valeur doit être configurée au moins cinq minutes de plus que la durée de

l'abonnement. La durée de l'abonnement est définie dans la valeur Contact Expires et est généralement de 30 minutes.

Comme les demandes MESSAGE/INFO sont généralement envoyées en utilisant un port alloué dynamiquement autre que le port 5060, elles doivent passer par le moteur d'inspection SIP.



Remarque L'inspection SIP prend en charge uniquement la fonctionnalité de conversation. Le tableau blanc, le transfert de fichiers et le partage d'application ne sont pas pris en charge. Le client RTC 5.0 n'est pas pris en charge.

Limites pour l'inspection SIP

L'inspection SIP est testée et prise en charge pour Cisco Unified Communications Manager (CUCM) 7.0, 8.0, 8.6 et 10.5. Il n'est pas pris en charge pour CUCM 8.5 ou 9.x. L'inspection SIP peut fonctionner avec d'autres versions et produits.

Si vous constatez que les téléphones SIP ne se connectent pas au gestionnaire d'appels, vous pouvez essayer d'augmenter le nombre maximal de segments TCP non traités dans le CLI en utilisant la commande suivante : **sysopt connection tcp-max-unprocessed-seg** *6-24*. La valeur par défaut est 6, alors essayez un nombre plus élevé.

L'inspection SIP ne prend pas en charge le protocole IFP (Internet Facsimile Protocol) T.38. L'inspection SIP rejette les invitations SIP qui utilisent le sous-type audio MIME T.38. Si vous devez autoriser ce type, désactivez l'inspection SIP et écrivez une règle de contrôle d'accès qui autorise les flux RTP.

Limites de la NAT pour l'inspection SIP

- L'inspection SIP applique la NAT pour les adresses IP intégrées. Toutefois, si vous configurez la NAT pour traduire les adresses de source et de destination, l'adresse externe (« from » dans l'en-tête SIP pour le message de réponse « trying ») n'est pas réécrite. Ainsi, vous devez utiliser la NAT d'objet lorsque vous utilisez le trafic SIP afin d'éviter de traduire l'adresse de destination.
- Ne configurez pas la NAT ou la PAT pour les interfaces avec des niveaux de sécurité identiques ou inférieurs (source) à des niveaux de sécurité supérieurs (destination). Cette configuration n'est pas prise en charge.
- Si vous configurez l'inspection SIP pour une classe de trafic ciblé (c'est-à-dire pas la classe de trafic inspection_default), veillez à utiliser une liste de contrôle d'accès bidirectionnelle et à préciser uniquement le port de destination 5060. Sinon, vous risquez d'avoir des problèmes de NAT dans lesquels l'adresse IP dans l'en-tête SIP n'est pas traduite, même si le paquet IP est correctement traduit.
- Si vous codez en dur l'adresse mappée dans l'en-tête VIA de l'invitation SIP, n'activez pas l'inspection SIP. Vous pouvez rencontrer des problèmes si vous utilisez une NAT statique pour traduire l'adresse du client source et que l'interface de la route par défaut est différente de l'interface de la route connectée utilisée par le client.

Limitations de la PAT pour l'inspection SIP

Les limitations et restrictions suivantes s'appliquent lorsque vous utilisez la PAT avec SIP :

- Si un terminal distant tente de s'enregistrer auprès d'un proxy SIP sur un réseau protégé par l'ASA, l'enregistrement échoue dans des conditions très spécifiques, comme suit :

- La PAT est configurée pour le terminal distant.
- Le serveur d'enregistrement SIP se trouve sur le réseau externe.
- Le port est manquant dans le champ de contact du message REGISTER envoyé par le terminal au proxy.

- Si un périphérique SIP transmet un paquet dans lequel la partie SDP a une adresse IP dans le champ du propriétaire/créateur (o=) qui est différente de l'adresse IP dans le champ de connexion (c=), l'adresse IP dans le champ o= peut ne pas être correctement traduite. Cela est causé par une limitation du protocole SIP, qui ne fournit pas de valeur de port dans le champ o=. Comme la PAT a besoin d'un port pour la traduction, la traduction échoue.
- Lors de l'utilisation de la PAT, tout champ d'en-tête SIP qui contient une adresse IP interne sans port peut ne pas être traduit et, par conséquent, l'adresse IP interne sera transmise à l'extérieur. Si vous souhaitez éviter cette fuite, configurez la NAT au lieu de la PAT.

Inspection SIP par défaut

L'inspection SIP est activée par défaut à l'aide de la carte d'inspection par défaut, qui comprend les éléments suivants :

- Extensions de messagerie instantanée SIP : activées.
- Trafic non SIP sur le port SIP : abandonné.
- Masquer les adresses IP du serveur et du terminal : désactivé.
- Masquer la version du logiciel et les URI non SIP : désactivé.
- Assurez-vous que le nombre de sauts vers la destination est supérieur à 0 : activé.
- Conformité RTP : non appliquée.
- Conformité SIP : n'effectuez pas la vérification de l'état et la validation de l'en-tête.

Notez également que l'inspection du trafic chiffré n'est pas activée. Vous devez configurer un proxy TLS pour inspecter le trafic chiffré.

Configurer une liste des politiques d'inspection SIP

Vous pouvez créer une liste des politiques d'inspection SIP pour personnaliser les actions d'inspection SIP si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

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 classe d'expression régulière.

Procédure

Étape 1 (Facultatif) Créez une carte de trafic d'inspection SIP en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de trafic vous permet de créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de classe, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect sip** [**match-all** | **match-any**] *class_map_name*

Où *nclass_map_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé match-any spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

b) (Facultatif) : Ajoutez une description à la carte de trafic : **description** *string*

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} : correspond à l'appelé, comme spécifié dans l'en-tête To, en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} : correspond à l'appelant, tel qu'il est indiqué dans l'en-tête From, en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match** [**not**] **content length gt** *bytes* : correspond aux messages dont la longueur du contenu dans l'en-tête SIP est supérieure au nombre d'octets spécifié, entre 0 et 65 536.
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*} : correspond au type de contenu SDP ou à l'expression régulière ou à la liste d'expressions régulières spécifiée.
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*} : correspond à l'abonné SIP IM en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*} : correspond à l'en-tête Via SIP en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.

- **match** [**not**] **request-method** *method* : correspond à une méthode de requête SIP : ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- **match** [**not**] **third-party-registration regex** {*regex_name* | **class** *class_name*} : correspond au demandeur d'un enregistrement tiers en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match** [**not**] **uri {sip | tel} length gt** *bytes* : correspond à un URI des en-têtes SIP du type sélectionné (SIP ou TEL) dont la longueur est supérieure à la valeur spécifiée, entre 0 et 65 536 octets.

d) Saisissez **exit** pour quitter le mode de configuration class-map.

Étape 2 Créez une liste des politiques d'inspection SIP : **policy-map type inspect sip** *policy_map_name*

Où *policy_map_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

Étape 3 (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*

Étape 4 Pour appliquer les actions au trafic correspondant, procédez comme suit.

a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :

- Si vous avez créé une carte de trafic SIP, spécifiez-la en entrant la commande suivante : **class** *class_map_name*
- Définissez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic SIP. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop** : abandon de tous les paquets qui correspondent.
- **drop-connection** : abandon du paquet et fermeture de la connexion.
- **reset** : abandon du paquet, fermeture de la connexion et envoi d'une réinitialisation TCP au serveur ou au client.
- **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.
- **rate-limit** *message_rate* : limite le débit des messages. La limitation de débit est disponible pour les correspondances de méthode de demande « invite » et « register » uniquement.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez Comment plusieurs classes de trafic sont gérées.

Étape 5 Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **im** : active la messagerie instantanée.
- **ip-address-privacy** : active la confidentialité des adresses IP, qui masque les adresses IP du serveur et des terminaux.
- **max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**] : vérifie la valeur de l'en-tête Max-Forwards, qui ne peut pas être zéro avant d'atteindre la destination. Vous devez également choisir l'action à prendre pour le trafic non conforme (abandon de paquet, abandon de connexion, réinitialisation ou journalisation) et activer ou désactiver la journalisation.
- **rtp-conformance** [**enforce-payloadtype**] : vérifie les paquets RTP circulant dans les passages pour vérifier la conformité du protocole. Le mot-clé facultatif enforce-payloadtype applique le type de charge utile pour qu'il soit audio ou vidéo en fonction de l'échange de signalisation.
- **software-version action** {**mask [log]** | **log**} : identifie la version du logiciel à l'aide des champs d'en-tête Server et User-Agent (terminal). Vous pouvez masquer la version du logiciel dans les messages SIP et éventuellement la consigner ou tout simplement la consigner.
- **state-checking action** {**drop** | **drop-connection** | **reset** | **log**} [**log**] : active la vérification des transitions d'état. Vous devez également choisir l'action à prendre pour le trafic non conforme (abandon de paquet, abandon de connexion, réinitialisation ou journalisation) et activer ou désactiver la journalisation.
- **strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**] : active la vérification stricte des champs d'en-tête des messages SIP conformément à la RFC 3261. Vous devez également choisir l'action à prendre pour le trafic non conforme (abandon de paquet, abandon de connexion, réinitialisation ou journalisation) et activer ou désactiver la journalisation.
- **traffic-non-sip** : autorise le trafic non SIP sur le port de signalisation SIP bien connu.
- **trust-verification-server ip** *ip_address* : identifie les serveurs Trust Verification Services, qui permettent aux téléphones Cisco Unified IP d'authentifier les serveurs d'applications lors de l'établissement d'une connexion HTTPS. Vous pouvez entrer la commande jusqu'à quatre fois pour identifier quatre serveurs. L'inspection SIP ouvre des passages sur chaque serveur pour chaque téléphone enregistré, et le téléphone décide lequel utiliser. Configurez le serveur des Services de vérification de confiance sur le serveur CUCM.
- **trust-verification-server port** *number* : identifie le port des services de vérification de confiance. Le port par défaut est 2445. Utilisez donc cette commande uniquement si le serveur utilise un port différent. La plage de ports autorisée est de 1 026 à 32 768.
- **uri-non-sip action** {**mask [log]** | **log**} : identifie les URI non SIP présents dans les champs d'en-tête Alert-Info et Call-Info. Vous pouvez masquer les informations dans les messages SIP et éventuellement les consigner, ou tout simplement les consigner.

Exemples

L'exemple suivant montre comment désactiver la messagerie instantanée sur SIP :

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im
```

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

L'exemple suivant montre comment identifier quatre serveurs de services de vérification de confiance.

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection Skinny (SCCP)

L'inspection d'application SCCP (Skinny) effectue la traduction de l'adresse IP et des numéros de port intégrés dans les données de paquets et l'ouverture dynamique de passages. Il effectue également des vérifications supplémentaires de conformité de protocole et un suivi de l'état de base.

L'inspection SCCP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut ou si vous souhaitez identifier un serveur proxy TLS pour activer l'inspection du trafic chiffré.

Les sections suivantes décrivent l'inspection des applications SCCP.

Aperçu de l'inspection SCCP

Skinny (SCCP) est un protocole simplifié utilisé dans les réseaux VoIP. Les téléphones IP Cisco utilisant SCCP peuvent coexister dans un environnement H.323. Lorsqu'il est utilisé avec Cisco CallManager, le client SCCP peut interopérer avec les terminaux conformes à la norme H.323.

L'ASA prend en charge la PAT et la NAT pour SCCP. La PAT est nécessaire si vous avez plus de téléphones IP que d'adresses IP globales pour les téléphones IP à utiliser. En prenant en charge la NAT et la PAT des paquets de signalisation SCCP, l'inspection d'application Skinny garantit que tous les paquets de signalisation et de médias SCCP peuvent traverser l'ASA.

Le trafic normal entre Cisco CallManager et les téléphones IP Cisco utilise SCCP et est géré par l'inspection SCCP sans configuration spéciale. L'ASA prend également en charge les options DHCP 150 et 66, ce qu'il fait en envoyant l'emplacement d'un serveur TFTP aux téléphones IP Cisco et à d'autres clients DHCP. Les téléphones IP Cisco peuvent également inclure l'option DHCP 3 dans leurs demandes, qui définit la route par défaut.

Remarque L'ASA prend en charge l'inspection du trafic des téléphones IP Cisco exécutant le protocole SCCP version 22 et antérieures.

Prise en charge des téléphones IP Cisco

Dans les topologies où Cisco CallManager se trouve sur l'interface de sécurité la plus élevée par rapport aux téléphones IP Cisco, si la NAT est requise pour l'adresse IP Cisco CallManager, le mappage doit être statique, car un téléphone IP Cisco nécessite que l'adresse IP Cisco CallManager soit précisée explicitement dans sa configuration. Une entrée d'identité statique permet à Cisco CallManager sur l'interface de sécurité supérieure d'accepter les enregistrements des téléphones IP Cisco.

Les téléphones IP Cisco nécessitent d'accéder à un serveur TFTP pour télécharger les informations de configuration dont ils ont besoin pour se connecter au serveur Cisco CallManager.

Lorsque les téléphones IP Cisco se trouvent sur une interface de sécurité inférieure à celle du serveur TFTP, vous devez utiliser une liste de contrôle d'accès pour vous connecter au serveur TFTP protégé sur le port UDP 69. Bien que vous ayez besoin d'une entrée statique pour le serveur TFTP, il n'est pas nécessaire qu'il s'agisse d'une entrée statique d'identité. Lors de l'utilisation de la NAT, une entrée statique d'identité est mappée à la même adresse IP. Lors de l'utilisation de la PAT, elle est mappée à la même adresse IP et au même port.

Lorsque les téléphones IP Cisco se trouvent sur une interface de sécurité plus élevée que le serveur TFTP et Cisco CallManager, aucune entrée d'ACL ou statique n'est requise pour permettre aux téléphones IP Cisco d'établir la connexion.

Limites de l'inspection SCCP

L'inspection SCCP est testée et prise en charge pour Cisco Unified Communications Manager (CUCM) 7.0, 8.0, 8.6 et 10.5. Il n'est pas pris en charge pour CUCM 8.5 ou 9.x. L'inspection SCCP peut fonctionner avec d'autres versions et produits.

Si l'adresse d'un Cisco CallManager interne est configurée pour la NAT ou la PAT vers une adresse IP ou un port différent, les enregistrements pour les téléphones IP Cisco externes échouent, car l'ASA ne prend pas en charge la NAT ou la PAT pour le contenu du fichier transféré sur TFTP. Bien que l'ASA prenne en charge la NAT des messages TFTP et qu'il ouvre un passage pour le fichier TFTP, l'ASA ne peut pas traduire l'adresse IP et le port Cisco CallManager intégrés dans les fichiers de configuration du téléphone IP Cisco qui sont transférés par TFTP lors de l'enregistrement du téléphone.

Remarque L'ASA prend en charge le basculement avec état des appels SCCP, à l'exception des appels en cours d'établissement.

Inspection SCCP par défaut

L'inspection SCCP est activée par défaut en utilisant les valeurs par défaut suivantes :

- Enregistrement : non appliqué.
- ID de message maximal : 0x181.

- Longueur minimale du préfixe : 4
- Délai d'expiration du support : 00:05:00
- Délai d'expiration de la signalisation : 01:00:00.
- Conformité RTP : Non appliquée.

Configurer une liste des politiques d'inspection Skinny (SCCP)

Pour préciser les actions lorsqu'un message enfreint un paramètre, créez une liste des politiques d'inspection SCCP. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection SCCP.

Procédure

Étape 1 Créez une liste des politiques d'inspection SCCP : **policy-map type inspect skinny** *policy_map_name*

Où *policy_map_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

Étape 2 (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*

Étape 3 (Facultatif) Abandonnez le trafic en fonction du champ d'ID de message de station dans les messages SCCP.

a) Identifiez le trafic en fonction de la valeur de l'ID du message de la station en hexadécimal, de 0x0 à 0xffff. Vous pouvez spécifier un ID unique ou une plage d'ID à l'aide de la commande **match** [**not**] **message-id**. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

match message-id {*value* | **range** *start_value end_value*}

Exemple :

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```

b) Précisez l'action à effectuer sur les paquets correspondants. Vous pouvez abandonner le paquet et éventuellement le journaliser : **drop** [**log**]

c) Répétez le processus jusqu'à ce que vous identifiiez tous les ID de message que vous souhaitez supprimer.

Étape 4 Configurez les paramètres qui influent sur le moteur d'inspection.

a) Entrez en mode de configuration des paramètres.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes ; utilisez la forme **no** de la commande pour désactiver l'option :

- **enforce-registration** : applique l'enregistrement avant que les appels ne puissent être placés.

- **message-ID max** *hex_value* : définit l'ID maximal de message de station SCCP autorisé. L'ID du message est en hexadécimal et le maximum par défaut est 0x181.
- **rtp-conformance** [**enforce-payloadtype**] : vérifie les paquets RTP circulant dans les passages pour vérifier la conformité du protocole. Le mot-clé facultatif enforce-payloadtype applique le type de charge utile pour qu'il soit audio ou vidéo en fonction de l'échange de signalisation.
- **sccp-prefix-len** {**max** | **min**} *length* : définit la valeur de longueur maximale ou minimale du préfixe SCCP autorisée. Entrez la commande deux fois pour définir une valeur minimale et maximale. Le minimum par défaut est 4, et il n'y a pas de maximum par défaut.
- **timeout** {**media** | **signaling**} *time* : définit les délais d'expiration pour les connexions du support et de la signalisation (au format hh:mm:ss). Pour n'avoir aucun délai d'expiration, spécifiez 0 pour le nombre. Le délai d'expiration de support par défaut est de 5 minutes et le délai d'expiration de signalisation par défaut est d'une heure.

Exemple

L'exemple suivant montre comment définir une liste des politiques d'inspection SCCP.

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection STUN

Les utilitaires de traversée de session pour la NAT (STUN), définis dans la RFC 5389, sont utilisés par les clients WebRTC pour les communications en temps réel basées sur navigateur, de sorte que les modules d'extension ne sont pas nécessaires. Les clients WebRTC utilisent souvent des serveurs STUN en nuage pour connaître leurs adresses IP publiques et leurs ports. WebRTC utilise l'établissement de connectivité interactif (ICE, RFC 5245) pour vérifier la connectivité entre les clients. Ces clients utilisent généralement UDP, bien qu'ils puissent également utiliser TCP ou d'autres protocoles.

Comme les pare-feu bloquent souvent le trafic UDP sortant, les produits WebRTC tels que Cisco Spark peuvent avoir des problèmes pour effectuer les connexions. L'inspection STUN ouvre des passages pour les terminaux STUN et applique la conformité de base STUN et ICE pour permettre les communications pour

les clients si la vérification de connectivité est reconnue par les deux côtés. Ainsi, vous pouvez éviter d'ouvrir de nouveaux ports dans vos règles d'accès pour activer ces applications.

Lorsque vous activez l'inspection STUN sur la carte de trafic d'inspection par défaut, le port TCP/UDP 3478 est surveillé pour le trafic STUN. L'inspection prend en charge uniquement les adresses IPv4 et TCP/UDP.

Il y a certaines limites de NAT pour l'inspection STUN. Pour le trafic WebRTC, les traductions NAT/PAT44 statiques sont prises en charge. Cisco Spark peut prendre en charge d'autres types de NAT, car Spark ne nécessite pas de passages. Vous pouvez également utiliser NAT/PAT64, y compris la NAT/PAT dynamique, avec Cisco Spark.

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Remarque L'inspection STUN utilise des identifiants de transaction pour faire correspondre les demandes et les réponses. Si vous utilisez le débogage pour résoudre les problèmes d'abandon de connexion, notez que le système modifie le format (endianness) des ID pour la sortie de débogage, de sorte qu'ils ne sont pas comparés directement à ceux que vous pourriez voir dans un pcap.

Pour en savoir plus sur l'activation de l'inspection STUN, consultez Configurer l'inspection du protocole de couche d'application.

Historique de l'inspection des protocoles vocaux et vidéo

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de SIP, SCCP et du proxy TLS pour IPv6	9.3(1)	Vous pouvez désormais inspecter le trafic IPv6 lorsque vous utilisez SIP, SCCP et le proxy TLS (à l'aide de SIP ou SCCP). Nous n'avons pas modifié de commandes.
Prise en charge SIP pour les services de vérification de confiance, NAT66, CUCM 10.5 et les téléphones du modèle 8831.	9.3(2)	Vous pouvez maintenant configurer les serveurs des services de vérification de confiance dans l'inspection SIP. Vous pouvez également utiliser NAT66. L'inspection SIP a été testée avec CUCM 10.5. Nous avons ajouté la commande de paramètre **trust-verification-server**.
Amélioration des performances d'inspection SIP sur un ASA à plusieurs cœurs.	9.4(1)	Si vous avez plusieurs flux de signalisation SIP passant dans un ASA à plusieurs cœurs, les performances de l'inspection SIP ont été améliorées. Cependant, vous n'afficherez pas d'amélioration des performances si vous utilisez un mandataire TLS, téléphonique ou IME. Nous n'avons pas modifié de commandes.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'inspection SIP dans la mise en grappe d'ASA	9.4(1)	Vous pouvez maintenant configurer l'inspection SIP sur la grappe ASA. Un flux de contrôle peut être créé sur n'importe quelle unité (en raison de l'équilibrage de charges), mais ses flux de données enfants doivent résider sur la même unité. La configuration du mandataire TLS n'est pas prise en charge. Nous avons introduit la commande suivante : **show cluster service-policy**.
La prise en charge de l'inspection SIP pour le mandataire téléphonique et le mandataire UC-IME a été supprimée.	9.4(1)	Vous ne pouvez plus utiliser le mandataire téléphonique ou le mandataire UC-IME lors de la configuration de l'inspection SIP. Utilisez le mandataire TLS pour inspecter le trafic chiffré. Nous avons supprimé les commandes suivantes : **phone-proxy**, **uc-ime**. Nous avons supprimé les mots-clés **phone-proxy** et **uc-time** de la commande **inspect sip**.
Prise en charge de l'inspection H.323 pour le message H.255 FACILITY entrant avant le message H.225 SETUP pour la compatibilité avec H.460.18.	9.6(1)	Vous pouvez maintenant configurer une liste de politiques d'inspection H.323 pour permettre aux messages H.225 FACILITY de venir avant le message H.225 SETUP, ce qui peut se produire lorsque les terminaux sont conformes à H.460.18. Nous avons introduit la commande suivante : **early-message**.
Inspection STUN (Session Traversal Utilities for NAT)	9.6(2)	Vous pouvez désormais inspecter le trafic STUN pour les applications WebRTC, y compris Cisco Spark. L'inspection ouvre les trous d'épingle nécessaires au trafic de retour. Nous avons ajouté ou modifié les commandes suivantes : **inspect stun**, **show asp drop**, **show conn detail**, **show service-policy inspect stun**.
Prise en charge de TLSv1.2 dans le mandataire TLS et Cisco Unified Communications Manager 10.5.2.	9.7(1)	Vous pouvez désormais utiliser TLSv1.2 avec le mandataire TLS pour l'inspection SIP ou SCCP chiffrée avec Cisco Unified Communications Manager 10.5.2. Le mandataire TLS prend en charge les suites de chiffrement TLSv1.2 supplémentaires ajoutées dans le cadre de la commande **client cipher-suite**. Nous avons modifié les commandes suivantes : **client cipher-suite**.
Le serveur mandataire TLS est obsolète pour l'inspection SCCP (Skinny).	9.13(1)	Le mot clé **tls-proxy** et la prise en charge de l'inspection chiffrée SCCP/Skinny sont désormais obsolètes. Le mot clé sera supprimé de la commande **inspect skinny** dans une version ultérieure.
La prise en charge du proxy TLS a été supprimée pour l'inspection SCCP (Skinny).	9.14(1)	Le mot-clé **tls-proxy** et la prise en charge de l'inspection chiffrée SCCP/Skinny ont été supprimés.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La liste des politiques d'inspection SIP par défaut abandonne le trafic non SIP.	9.16(1)	Pour le trafic inspecté pour le SIP, la valeur par défaut consiste désormais à abandonner le trafic non SIP. Auparavant, le trafic non SIP était autorisé sur les ports inspectés pour le SIP. Nous avons modifié la liste des politiques SIP par défaut pour inclure la commande **no traffic-non-sip**.

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.

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.

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.

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.

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.