

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 13
- Inspection Skinny (SCCP), à la page 18
- Inspection STUN, à la page 21
- Historique de l'inspection des protocoles vocaux et vidéo, à la page 22

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 CTQBE

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 le configurer que si vous souhaitez un traitement autre que celui par défaut.

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

Survol 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 dont un paquet est soumis à l'inspection H.323 est marquée comme une connexion H.323 et expire selon le délai H.323 configuré dans Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux).



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.

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.

Vous pouvez éventuellement créer une carte de trafic d'inspection H.323 pour définir la classe de trafic pour l'inspection H.323. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection H.323. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic 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 trafic. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic H.323 en sélectionnant **Configuration** > **Firewall** > **Objects** > **Class Maps (Cartes de trafic)** > **H.323**, ou en les créant lors de la configuration de la liste 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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **H.323**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer 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 la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue H.323 Inspect Map (Liste d'inspection H.323), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Bas.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection H.323.

Astuces

Le bouton **Phone Number Filtering** (Filtrage de numéro de téléphone) est un raccourci pour configurer l'inspection de l'appelé ou de l'appelant, qui est expliquée ultérieurement dans cette procédure.

Étape 5 Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails), puis procédez comme suit :

a) Cliquez sur l'onglet **State Checking** (Vérification de l'état) et choisissez d'activer la vérification de la transition d'état des messages RAS et H.225.

Vous pouvez également vérifier les messages RCF et ouvrir des passages pour les adresses de signal d'appel présentes dans les messages RRQ, ce qui permet la configuration d'appel entre les terminaux H.323 lorsque le portier se trouve dans le réseau. Utilisez cette option pour ouvrir des passages pour les appels en fonction des messages RegistrationRequest/RegistrationConfirm (RRQ/RCF). Comme ces messages RRQ/RCF sont envoyés à et par le portier, l'adresse IP du terminal appelant est inconnue et l'ASA ouvre un passage par l'adresse IP source/le port 0/0. Par défaut, cette option est activée.

b) Cliquez sur l'onglet **Call Attributes** (Attributs d'appel) et choisissez d'appliquer une limite de durée d'appel (maximum 1 193 heures) ou d'appliquer la présence de numéros d'appelant et d'appelé lors de l'établissement de l'appel.

Vous pouvez également autoriser les messages H.225 FACILITY à arriver avant les messages H.225 SETUP 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, sélectionnez

cette option 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).

c) Cliquez sur l'onglet **Tunneling and Protocol Conformance** (Conformité du protocole et tunnellisation) et choisissez de vérifier la tunnellisation H.245 ; vous pouvez soit abandonner la connexion, soit la journaliser.

Vous pouvez également choisir de vérifier la conformité du protocole des paquets RTP qui passent par les passages. Si vous vérifiez la conformité, vous pouvez également choisir de limiter la charge utile à l'audio ou à la vidéo, en fonction de l'échange de signalisation.

Étape 6 Si nécessaire, cliquez sur l'onglet **HSI Group Parameters** (Paramètres de groupe HSI) et définissez les groupes HSI.

a) Effectuez l'une des actions suivantes :

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

b) Précisez l'ID de groupe (de 0 à 2 147 483 647) et l'adresse IP du HSI.

c) Pour ajouter un terminal au groupe HSI, saisissez l'adresse IP, sélectionnez l'interface par laquelle le terminal est connecté à l'ASA, puis cliquez sur **Add>>** (Ajouter). Supprimez les terminaux qui ne sont plus nécessaires. Vous pouvez avoir jusqu'à 10 terminaux par groupe.

d) Cliquez sur **OK** pour ajouter le groupe. Répétez le processus au besoin.

Étape 7 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 HTTP, 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** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic H.323 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 :

- **Called Party** (Partie appelée) : fait correspondre la partie appelée H.323 à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Calling Party** (Partie appelante) : fait correspondre la partie appelante H.323 à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Media Type** (Type de support) : correspond au type de support : audio, vidéo ou données.

d) Choisissez l'action à entreprendre pour le trafic correspondant. Pour la correspondance de la partie appelante ou appelée, vous pouvez abandonner le paquet, abandonner la connexion ou réinitialiser la connexion. Pour la correspondance du type de support, l'action est toujours d'abandonner le paquet; vous pouvez activer la journalisation pour cette action.

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

Étape 8 Cliquez sur **OK** dans la boîte de dialogue H.323 Inspect Map (Liste d'inspection H.323).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection H.323.

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.

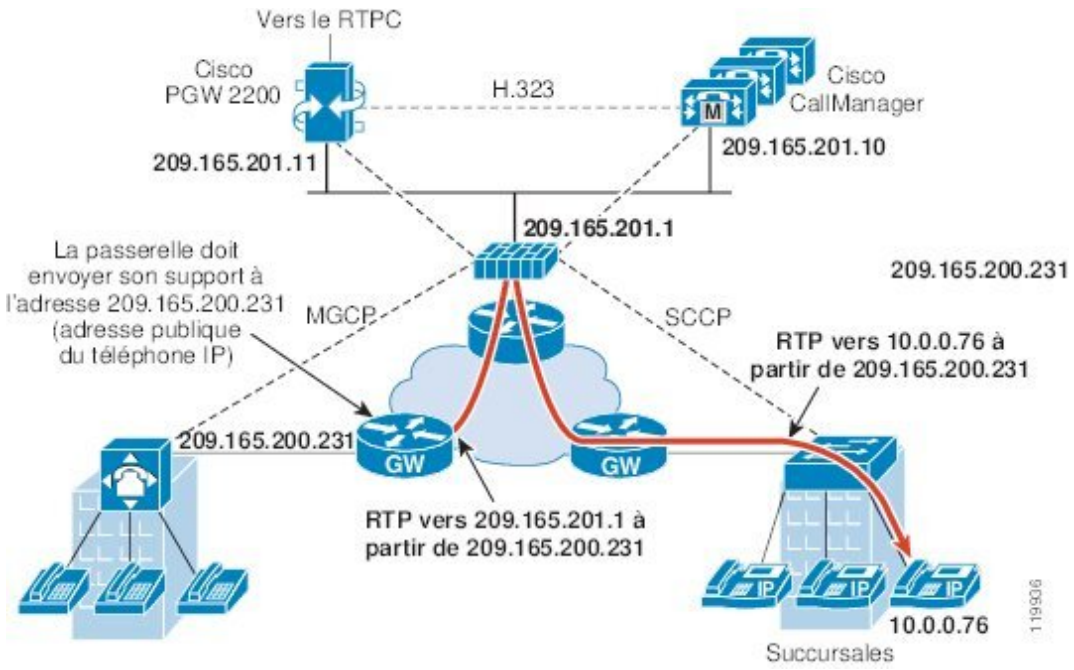
Aperçu de l'inspection MGCP

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

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 (Facultatif) Cliquez sur l'onglet **Command Queue** (File d'attente de commandes) et spécifiez le nombre maximal de commandes autorisées dans la file d'attente de commande MGCP. La valeur par défaut est 200, et la plage autorisée est de 1 à 2 147 483 647.

Étape 5 Cliquez sur l'onglet **Gateways and Call Agents** (Passerelles et agents d'appel) et configurez les groupes de passerelles et les agents d'appel pour la liste.

a) Cliquez sur **Add** (Ajouter) pour créer un nouveau groupe, ou sélectionnez un groupe et cliquez sur **Edit** (Modifier).

b) Saisissez le **Group ID** (ID de groupe) du groupe d'agents d'appel. Un groupe d'agents d'appel associe un ou plusieurs agents d'appel à une ou plusieurs passerelles de support MGCP. La plage valide est de 0 à 2 147 483 647.

c) Ajoutez les adresses IP des passerelles de support qui sont contrôlées par les agents d'appel associés au groupe en les saisissant dans **Gateway to Be Added** (Passerelle à ajouter) et en cliquant sur **Add**>> (Ajouter). Supprimez les passerelles qui ne sont plus utilisées.

   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. Normalement, une passerelle envoie des commandes au port MGCP par défaut pour les agents d'appel, UDP 2727.

d) Ajoutez les adresses IP des agents d'appel qui contrôlent les passerelles de support MGCP en les saisissant dans **Call Agent to Be Added** (Agent d'appel à ajouter) et en cliquant sur **Add**>> (Ajouter). Supprimez tous les agents qui ne sont plus nécessaires.

   Normalement, un agent d'appel envoie des commandes au port MGCP par défaut pour les passerelles, UDP 2427.

e) Cliquez sur **OK** dans la boîte de dialogue MGCP Group (Groupe MGCP). Répétez le processus pour ajouter d'autres groupes, au besoin.

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

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

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 NAT Twice. 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 le RTSP de multidiffusion 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.
- 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.

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

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

- **Enforce Reserve Port Protection** (Appliquer la protection des ports réservés) : indique s'il faut restreindre l'utilisation des ports réservés pendant la négociation du port de support.
- **Maximum URL Length** (Longueur maximale de l'URL) : longueur maximale de l'URL autorisée dans le message, de 0 à 6 000.

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 HTTP, 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 le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic RTSP 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). Par exemple, si No Match est sélectionné sur la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :
   - **URL Filter** (Filtre d'URL) : met en correspondance l'URL avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
   - **Request Method** (Méthode de demande) : correspond à la méthode de demande : announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameters, teardown.

d) Choisissez l'action à entreprendre pour le trafic correspondant. Pour la correspondance d'URL, vous pouvez abandonner la connexion ou la journaliser, et vous pouvez activer la journalisation des connexions abandonnées. Pour les correspondances de méthode de demande, vous pouvez appliquer une limite de débit en paquets par seconde.

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

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

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

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.

Limites 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 liste 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.

Vous pouvez éventuellement créer une carte de trafic d'inspection SIP pour définir la classes de trafic pour l'inspection SIP. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection SIP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic 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 SIP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **SIP**, ou en les créant lors de la configuration de la liste 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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SIP** .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier directement le niveau de sécurité ou cliquer 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 la vue **Security Level** (Niveau de sécurité) de la boîte de dialogue SIP Inspect Map (liste d'inspection SIP), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Low (Bas).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection SIP.

Étape 5 Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails), puis procédez comme suit :

a) Cliquez sur l'onglet **Filtering** (Filtrage) et choisissez d'activer les extensions de messagerie instantanée SIP ou d'autoriser le trafic non SIP sur le port SIP.

b) Cliquez sur l'onglet **IP Address Privacy** (Confidentialité des adresses IP) et choisissez de masquer les adresses IP du serveur et du terminal.

c) Cliquez sur l'onglet **Hop Count** (Nombre de sauts) et choisissez de vérifier que le nombre de sauts jusqu'à la destination est supérieur à 0. Cela vérifie la valeur de l'en-tête Max-Forwards, qui ne peut pas être nulle 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.

d) Cliquez sur l'onglet **Conformité RTP** et choisissez de vérifier ou non les paquets RTP qui passent par les passages pour vérifier la conformité du protocole. Si vous vérifiez la conformité, vous pouvez également choisir de limiter la charge utile à l'audio ou à la vidéo, en fonction de l'échange de signalisation.

e) Cliquez sur l'onglet **SIP Conformance** (Conformité SIP) et choisissez d'activer la vérification des transitions d'état et la validation stricte des champs d'en-tête. Pour chaque option que vous choisissez, sélectionnez l'action à entreprendre pour le trafic non conforme (abandon de paquet, abandon de connexion, réinitialisation ou journal) et indiquez si la journalisation doit être activée ou désactivée.

f) Cliquez sur l'onglet **Field Masking** (Masquage des champs) et choisissez d'inspecter les URI non SIP dans les en-têtes Alert-Info et Call-Info ainsi que la version du logiciel du serveur et du terminal dans les en-têtes User-Agent et Server. Pour chaque option choisie, sélectionnez l'action à appliquer (masquage ou journalisation) et indiquez si la journalisation doit être activée ou désactivée.

g) Cliquez sur l'onglet **TVS Server** (Serveur TVS) et identifiez 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 identifier jusqu'à quatre serveurs; saisissez leurs adresses IP séparées par des virgules. 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. Si la configuration utilise un port autre que celui par défaut, entrez le numéro de port (dans la plage de 1026 à 32 768). La valeur du port par défaut est 2445.

Étape 6 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 à l'aide des cartes de trafic SIP, en configurant directement les correspondances dans la liste d'inspection, ou en combinant les deux méthodes.

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** (Correspondance multiple), puis sélectionnez la carte de trafic SIP 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). Par exemple, si No Match (Aucune correspondance) est sélectionné pour la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :

- **Partie appelée** : correspond à la partie appelée, comme spécifié dans l'en-tête To, avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Partie appelante** : correspond à la partie appelante, comme spécifié dans l'en-tête From, avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Longueur du contenu** : correspond à un en-tête de contenu SIP d'une longueur supérieure à celle spécifiée, entre 0 et 65 536 octets.
- **Type de contenu** : correspond à l'en-tête Content Type, soit le type SDP, soit un type qui correspond à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Abonné IM** : correspond à l'abonné SIP IM à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Chemin du message** : correspond à l'en-tête SIP Via avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Méthode de demande** : correspond à la méthode de demande SIP : ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- **Enregistrement tiers** : correspond au demandeur d'un enregistrement tiers avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Longueur de l'URI** : correspond à un URI dans les en-têtes SIP du type sélectionné (SIP ou TEL) qui est supérieur à la longueur spécifiée, entre 0 et 65 536 octets.

d) Choisissez l'action à prendre pour le trafic correspondant (abandon de paquet, perte de connexion, réinitialisation, journal) et s'il faut activer ou désactiver la journalisation. Pour les correspondances de méthode de demande avec « invite » et « register », vous pouvez également appliquer une limite de débit en paquets par seconde.

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

Étape 7 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection SIP.

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

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, il est mappé 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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SCCP (Skinny)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer 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 la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue SCCP (Skinny) Inspect Map (Liste d'inspection SCCP [Skinny]), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Low (Bas).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection SCCP.

Étape 5 Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails), puis procédez comme suit :

a) Cliquez sur l'onglet **Parameters** (Paramètres) et choisissez les options souhaitées.

- **Enforce endpoint registration** (Appliquer l'enregistrement des terminaux) : indique si les terminaux Skinny doivent s'enregistrer avant de passer ou de recevoir des appels.
- **Maximum Message ID** (ID de message maximal) : ID maximal de message de station SCCP autorisé. La valeur par défaut est 0x181. Le nombre hexadécimal peut être compris entre 0x0 et 0xffff.
- **SCCP Prefix Length** (Longueur du préfixe SCCP) : longueur maximale et minimale du préfixe SCCP. Le minimum par défaut est 4, et il n'y a pas de maximum par défaut.
- **Timeouts** (Délais d'expiration) : indique s'il faut définir des délais d'expiration pour les connexions de support et de signalisation, ainsi que la valeur de ces délais d'expiration. Les valeurs par défaut sont de 5 minutes pour les supports et de 1 heure pour la signalisation.

b) Cliquez sur l'onglet **RTP Conformance** (Conformité RTP) et choisissez de vérifier ou non les paquets RTP qui passent par les passages pour vérifier la conformité du protocole. Si vous vérifiez la conformité, vous pouvez également choisir de limiter la charge utile à l'audio ou à la vidéo, en fonction de l'échange de signalisation.

Étape 6 (Facultatif) Cliquez sur l'onglet **Message ID Filtering** (Filtrage d'ID de message) pour identifier le trafic à abandonner en fonction du champ d'ID de message de station dans les messages SCCP.

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).
c) Dans les champs **Value** (Valeur), identifiez le trafic en fonction de la valeur de l'ID de message de station en hexadécimal, de 0x0 à 0xffff. Saisissez la valeur d'un seul ID de message ou saisissez la valeur de début et de fin pour une plage d'ID.
d) Choisissez d'activer ou de désactiver la journalisation. L'action est toujours d'abandonner le paquet.
e) Cliquez sur **OK** pour ajouter le filtre. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue SCCP (Skinny) Inspect Map (Liste d'inspection SCCP [Skinny]).

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

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 passages 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 d'écrans ASDM.
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 prise en charge de Trust Verification Services Server à la liste des politiques d'inspection SIP.
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 d'écrans ASDM.
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 n'avons pas modifié d'écrans.
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 le mandataire téléphonique et le mandataire UC-IME de la boîte de dialogue de politique de service Select SIP Inspect Map (Sélectionner la carte d'inspection SIP).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'inspection H.323 pour le message H.225 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 ajouté une option à l'onglet Call Attributes (Attributs d'appel) dans la liste des politiques d'inspection H.323.
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 passages nécessaires au trafic de retour. Nous avons ajouté une option à l'onglet Rule Actions (Actions de règles) > Protocol Inspection (Inspection de protocole) de la boîte de dialogue Add/Edit Service Policy (Ajouter/modifier une politique de service).
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 n'avons pas modifié d'écrans.
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.
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.