ASA et Cisco TrustSec

Ce chapitre décrit comment mettre en œuvre Cisco TrustSec pour l'ASA.

À propos de Cisco TrustSec

Traditionnellement, les fonctionnalités de sécurité telles que les pare-feu effectuent un contrôle d'accès en fonction d'adresses IP, de sous-réseaux et de protocoles prédéfinis. Cependant, avec la transition des entreprises vers des réseaux sans frontières, la technologie utilisée pour connecter les personnes et les entreprises ainsi que les exigences de sécurité pour la protection des données et des réseaux ont considérablement changé. Les terminaux sont de plus en plus mobiles et les utilisateurs utilisent souvent une variété de terminaux (par exemple, ordinateur portable ou ordinateur de bureau, téléphone intelligent ou tablette), ce qui signifie qu'une combinaison d'attributs d'utilisateur et d'attributs de terminal fournit les caractéristiques clés (en plus des règles basées sur des 6-tuples), que les périphériques d'application tels que les commutateurs et les routeurs avec fonctionnalités de pare-feu ou pare-feu dédiés peuvent utiliser de manière fiable pour prendre des décisions en matière de contrôle d'accès.

Par conséquent, la disponibilité et la propagation des attributs de terminal ou des attributs d'identité du client sont devenues des exigences de plus en plus importantes pour assurer la sécurité sur les réseaux des clients, aux couches d'accès, de distribution et de cœur du réseau, ainsi que dans le centre de données.

Cisco TrustSec fournit un contrôle d'accès qui s'appuie sur une infrastructure existante de prise en compte de l'identité pour assurer la confidentialité des données entre les périphériques réseau et intégrer les services d'accès de sécurité sur une seule plateforme. Dans la fonctionnalité Cisco TrustSec, les appareils d'application utilisent une combinaison d'attributs d'utilisateur et d'attributs de terminal pour prendre des décisions de contrôle d'accès basées sur les rôles et l'identité. La disponibilité et la propagation de ces informations permettent la sécurité sur les réseaux au niveau de l'accès, de la distribution et du cœur du réseau.

La mise en œuvre de Cisco TrustSec dans votre environnement présente les avantages suivants :

- Fournit à une main-d'œuvre mobile et complexe en pleine croissance un accès approprié et plus sécurisé à partir de n'importe quel périphérique

- Réduit les risques de sécurité en fournissant une visibilité complète sur qui et ce qui se connecte au réseau filaire ou sans fil
- Offre un contrôle exceptionnel sur l'activité des utilisateurs du réseau qui accèdent aux ressources informatiques physiques ou en nuage
- Réduit le coût total d'acquisition grâce à une gestion centralisée et hautement sécurisée des politiques d'accès et à des mécanismes d'application évolutifs
- Pour en savoir plus, consultez les URL suivantes :
  - Description du système Cisco TrustSec et de l'architecture pour l'entreprise.

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
  - Des instructions pour le déploiement de la solution Cisco TrustSec dans l'entreprise, y compris des liens vers des guides de conception de composants.

    http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html
  - Un aperçu de la solution Cisco TrustSec lorsqu'elle est utilisée avec l'ASA, les commutateurs, les contrôleurs de réseau local sans fil (WLAN) et les routeurs.

    http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf
  - La matrice de prise en charge de la plateforme Cisco TrustSec, qui répertorie les produits Cisco qui prennent en charge la solution Cisco TrustSec.

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

À propos de la prise en charge de SGT et SXP dans Cisco TrustSec

Dans la fonctionnalité Cisco TrustSec, l'accès de groupe de sécurité modifie un réseau compatible avec la topologie en un réseau basé sur les rôles, ce qui permet l'application des politiques de bout en bout sur la base du contrôle d'accès basé sur les rôles (RBAC). Les informations d'authentification du périphérique et de l'utilisateur obtenues lors de l'authentification sont utilisées pour classer les paquets par groupe de sécurité. Chaque paquet entrant dans le nuage Cisco TrustSec est marqué par une balise de groupe de sécurité (SGT). Le balisage aide les intermédiaires de confiance à identifier l'identité de la source du paquet et à appliquer les politiques de sécurité tout au long du chemin de données. Une balise SGT peut indiquer un niveau de privilège dans le domaine lorsqu'elle est utilisée pour définir une liste de contrôle d'accès de groupe de sécurité.

Une balise SGT est attribuée à un périphérique par le biais de l'authentification IEEE 802.1X, de l'authentification Web ou du contournement de l'authentification MAC (MAB), qui se produit avec un attribut propre au fournisseur RADIUS. Une balise SGT peut être affectée de manière statique à une adresse IP particulière ou à une interface de commutation. Une balise SGT est transmise dynamiquement à un commutateur ou à un point d'accès après l'authentification réussie.

Le protocole SXP (Security-group eXchange Protocol) est un protocole mis au point par Cisco TrustSec pour propager la base de données de mappage IP-SGT entre les périphériques réseau qui ne prennent pas en charge le matériel compatible avec SGT vers le matériel qui prend en charge les SGT et les listes de contrôle d'accès de groupes de sécurité. SXP, un protocole de plan de commande, transmet le mappage IP-SGT des points d'authentification (comme les commutateurs de couche d'accès existants) aux périphériques en amont dans le réseau.

Les connexions SXP sont point à point et utilisent TCP comme protocole de transport sous-jacent. SXP utilise le port TCP 64999 pour amorcer une connexion. En outre, une connexion SXP est identifiée de manière unique par les adresses IP source et de destination.

Rôles dans la fonctionnalité Cisco TrustSec

Pour fournir une application d'identité et d'accès basée sur les politiques, la fonctionnalité Cisco TrustSec comprend les rôles suivants :

- Demandeur d'accès (AR) : Les demandeurs d'accès sont des périphériques terminaux qui demandent l'accès aux ressources protégées dans le réseau. Ce sont des sujets principaux de l'architecture et leur privilège d'accès dépend de leurs informations d'authentification.

  Les demandeurs d'accès comprennent des périphériques de terminal tels que les PC, les ordinateurs portables, les téléphones portables, les imprimantes, les caméras et les téléphones IP compatibles avec le protocole MACsec.

- Point de décision des politiques (PDP) : un point de décision des politiques est responsable de prendre des décisions en matière de contrôle d'accès. Le PDP fournit des fonctionnalités telles que 802.1x, MAB et l'authentification Web. Le PDP prend en charge l'autorisation et l'application par le biais du VLAN, de la DACL et de l'accès au groupe de sécurité (SGACL/SXP/SGT).

  Dans la fonctionnalité Cisco TrustSec, le moteur de services de vérification des identités de Cisco (ISE) agit comme PDP. Cisco ISE fournit des fonctionnalités de politique de contrôle d'identité et d'accès.

- Point d'information sur les politiques (PIP) : un point d'information sur les politiques est une source qui fournit des informations externes (par exemple, réputation, emplacement et attributs LDAP) aux points de décision des politiques.

  Les points d'information sur les politiques comprennent des périphériques tels que le répertoire de session, le capteur IPS et le gestionnaire de communication.

- Point d'administration des politiques (PAP) : un point d'administration des politiques définit et insère les politiques dans le système d'autorisation. La PAP agit comme un référentiel d'identité en fournissant un mappage d'identité balise Cisco TrustSec-utilisateur et un mappage d'identité balise-serveur Cisco TrustSec.

  Dans la fonctionnalité Cisco TrustSec, le système de contrôle d'accès sécurisé Cisco (un serveur de politiques avec prise en charge intégrée de 802.1x et SGT) sert de PAP.

- Point d'application des politiques (PEP) : un point d'application des politiques est l'entité qui exécute les décisions (règles et actions de politique) prises par le PDP pour chaque AR. Les périphériques PEP obtiennent des informations d'identité par le biais du chemin de communication principal qui existe dans les réseaux. Les périphériques PEP connaissent les attributs d'identité de chaque AR de nombreuses sources, telles que les agents de terminal, les serveurs d'autorisation, les périphériques d'application homologues et les flux réseau. À leur tour, les périphériques PEP utilisent SXP pour propager le mappage IP-SGT vers des périphériques homologues de confiance mutuelle dans le réseau.

  Les points d'application des politiques comprennent des périphériques réseau tels que les commutateurs Catalyst, les routeurs, les pare-feu (en particulier l'ASA), les serveurs, les périphériques VPN et les périphériques SAN.

L'ASA sert le rôle de PEP dans l'architecture d'identité. À l'aide de SXP, l'ASA obtient les informations d'identité directement des points d'authentification et les utilise pour appliquer les politiques basées sur l'identité.

Application de la politique de groupe de sécurité

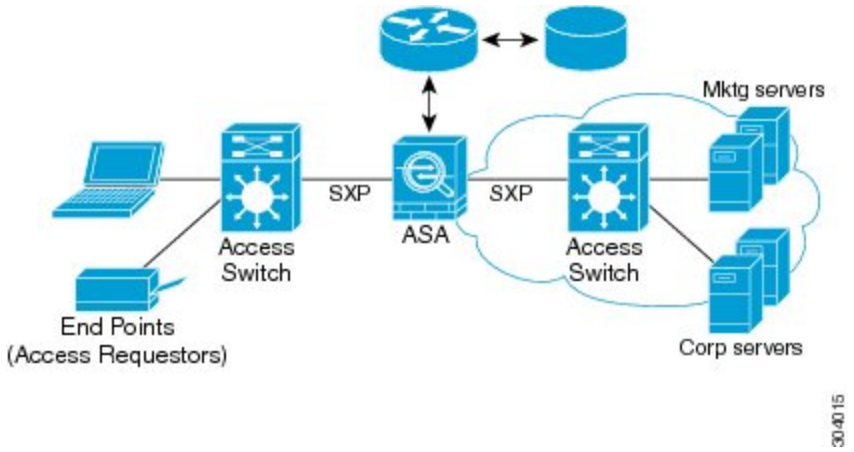
L'application de la politique de sécurité est basée sur le nom du groupe de sécurité. Un périphérique terminal tente d'accéder à une ressource dans le centre de données. Par rapport aux politiques traditionnelles basées sur IP configurées sur les pare-feu, les politiques basées sur l'identité sont configurées en fonction des identités d'utilisateur et de périphérique. Par exemple, mktg-contractor est autorisé à accéder à mktg-servers; mktg-corp-users sont autorisés à accéder à mktg-server et corp-servers.

Les avantages de ce type de déploiement sont les suivants :

- Le groupe d'utilisateurs et les ressources sont définis et appliqués à l'aide d'une gestion simplifiée des politiques d'objet unique (SGT).
- L'identité de l'utilisateur et l'identité de la ressource sont conservées dans toute l'infrastructure de commutation compatible avec Cisco TrustSec.

La figure suivante montre un déploiement pour l'application d'une politique basée sur le nom de groupe de sécurité.

Illustration 1 : Déploiement de l'application des politiques basées sur le nom de groupe de sécurité



La mise en œuvre de Cisco TrustSec vous permet de configurer des politiques de sécurité qui prennent en charge la segmentation des serveurs et comprend les fonctionnalités suivantes :

- Un ensemble de serveurs peut se voir attribuer une balise SGT pour simplifier la gestion des politiques.
- Les informations SGT sont conservées dans l'infrastructure des commutateurs compatibles avec Cisco TrustSec.
- L'ASA peut utiliser le mappage IP-SGT pour appliquer les politiques dans le domaine Cisco TrustSec.
- La simplification du déploiement est possible, car l'autorisation 802.1x pour les serveurs est obligatoire.

Comment l'ASA applique les politiques basées sur les groupes de sécurité

Remarque Les politiques de sécurité basées sur l'utilisateur et les politiques basées sur les groupes de sécurité peuvent coexister sur l'ASA. Toute combinaison d'attributs de réseau, d'utilisateurs et de groupes de sécurité peut être configurée dans une politique de sécurité.

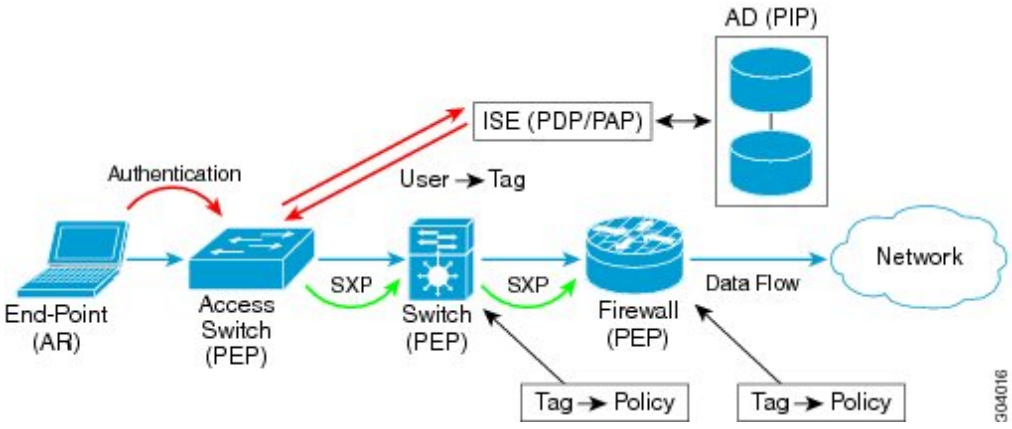
Pour configurer l'ASA pour qu'il fonctionne avec Cisco TrustSec, vous devez importer un fichier d'identifiant d'accès protégé (PAC) à partir de l'ISE.

L'importation du fichier PAC dans l'ASA établit un canal de communication sécurisé avec l'ISE. Une fois le canal établi, l'ASA amorce une transaction RADIUS sécurisée PAC avec l'ISE et télécharge les données d'environnement Cisco TrustSec (c'est-à-dire la table du groupe de sécurité). La table des groupes de sécurité mappe les balises SGT aux noms de groupes de sécurité. Les noms de groupes de sécurité sont créés sur l'ISE et fournissent des noms conviviaux pour les groupes de sécurité.

La première fois que l'ASA télécharge la table de groupes de sécurité, il parcourt toutes les entrées de la table et résout tous les noms de groupes de sécurité inclus dans les politiques de sécurité qui ont été configurées sur celui-ci; puis l'ASA active ces politiques de sécurité localement. Si l'ASA ne peut pas résoudre un nom de groupe de sécurité, il génère un message syslog pour le nom de groupe de sécurité inconnu.

La figure suivante montre comment une politique de sécurité est appliquée dans Cisco TrustSec.

Illustration 2 : Application de la politique de sécurité



1. Un terminal se connecte à un périphérique de couche d'accès directement ou par accès à distance et s'authentifie auprès de Cisco TrustSec.
2. Le périphérique de couche d'accès authentifie le terminal auprès de l'ISE en utilisant des méthodes d'authentification telles que 802.1X ou l'authentification Web. Le terminal transmet les informations de rôle et d'appartenance au groupe pour classer le périphérique dans le groupe de sécurité approprié.
3. Le périphérique de couche d'accès utilise SXP pour propager le mappage IP-SGT vers les périphériques en amont.
4. L'ASA reçoit le paquet et recherche les SGT des adresses IP source et de destination à l'aide du mappage IP-SGT transmis par SXP.

   Si le mappage est nouveau, l'ASA l'enregistre dans sa base de données IP-SGT Manager locale. La base de données IP-SGT Manager, qui s'exécute dans le plan de commande, suit le mappage IP-SGT pour

chaque adresse IPv4 ou IPv6. La base de données enregistre la source à partir de laquelle le mappage a été appris. L'adresse IP homologue de la connexion SXP est utilisée comme source du mappage. Plusieurs sources peuvent exister pour chaque entrée mappée IP-SGT.

Si l'ASA est configuré en tant que Speaker, l'ASA transmet toutes les entrées de mappage IP-SGT à ses homologues SXP.

5. Si une politique de sécurité est configurée sur l'ASA avec ce SGT ou ce nom de groupe de sécurité, l'ASA applique la politique. (Vous pouvez créer des politiques de sécurité sur l'ASA qui incluent des SGT ou des noms de groupes de sécurité. Pour appliquer les politiques en fonction des noms de groupe de sécurité, l'ASA a besoin de la table de groupe de sécurité pour mapper les noms de groupe de sécurité aux SGT.)

   Si l'ASA ne peut pas trouver de nom de groupe de sécurité dans la table des groupes de sécurité et qu'il est inclus dans une politique de sécurité, l'ASA considère le nom du groupe de sécurité comme inconnu et génère un message syslog. Après que l'ASA a actualisé la table des groupes de sécurité à partir de l'ISE et a appris le nom du groupe de sécurité, l'ASA génère un message syslog indiquant que le nom du groupe de sécurité est connu.

Effets des modifications des groupes de sécurité sur l'ISE

L'ASA actualise périodiquement la table du groupe de sécurité en téléchargeant une table mise à jour à partir de l'ISE. Les groupes de sécurité peuvent changer sur l'ISE entre les téléchargements. Ces modifications ne sont pas répercutées sur l'ASA tant qu'il n'a pas actualisé la table des groupes de sécurité.

Astuces Nous vous recommandons de planifier les modifications de configuration des politiques sur l'ISE pendant une fenêtre de maintenance, puis d'actualiser manuellement la table des groupes de sécurité sur l'ASA pour vous assurer que les modifications des groupes de sécurité ont été intégrées.

Le traitement des modifications de configuration des politiques de cette manière optimise les possibilités de résolution du nom de groupe de sécurité et d'activation immédiate des politiques de sécurité.

La table du groupe de sécurité est automatiquement actualisée à l'expiration du temporisateur des données d'environnement. Vous pouvez également déclencher une actualisation du tableau de groupe de sécurité sur demande.

Si un groupe de sécurité change sur l'ISE, les événements suivants se produisent lorsque l'ASA actualise la table du groupe de sécurité :

- Seules les politiques de groupes de sécurité qui ont été configurées à l'aide de noms de groupes de sécurité doivent être résolues avec la table de groupes de sécurité. Les politiques qui comprennent des balises de groupe de sécurité sont toujours actives.
- Lorsque la table des groupes de sécurité est disponible pour la première fois, toutes les politiques utilisant des noms de groupes de sécurité sont parcourues, les noms de groupes de sécurité sont résolus et les politiques sont activées. Toutes les politiques utilisant des balises sont parcourues et des messages syslog sont générés pour les balises inconnues.
- Si la table de groupe de sécurité a expiré, les politiques continuent d'être appliquées en fonction de la dernière table de groupe de sécurité téléchargée jusqu'à ce que vous l'effaciez ou qu'une nouvelle table soit disponible.
- Lorsqu'un nom de groupe de sécurité résolu devient inconnu sur l'ASA, la politique de sécurité est désactivée; toutefois, elle demeure dans la configuration en cours d'exécution de l'ASA.

- Si un groupe de sécurité existant est supprimé sur le PAP, une balise de groupe de sécurité connue précédemment peut devenir inconnue, mais aucun changement dans l'état de la politique ne se produit sur l'ASA. Un nom de groupe de sécurité connu précédemment peut ne pas être résolu, et la politique est alors inactivée. Si le nom du groupe de sécurité est réutilisé, la politique est recompilée à l'aide de la nouvelle balise.
- Si un nouveau groupe de sécurité est ajouté sur le PAP, une balise de groupe de sécurité inconnue précédemment peut devenir connue, un message syslog est généré, mais aucun changement dans l'état de la politique ne se produit. Un nom de groupe de sécurité inconnu précédemment peut être résolu, et les politiques associées sont ensuite activées.
- Si une balise a été renommée sur le PAP, les politiques qui ont été configurées à l'aide de balises affichent le nouveau nom, et aucun changement dans l'état des politiques ne se produit. Les politiques qui ont été configurées avec des noms de groupes de sécurité sont recompilées à l'aide de la nouvelle valeur de balise.

Rôles de speaker et de listener sur l'ASA

L'ASA prend en charge SXP pour envoyer et recevoir des entrées de mappage IP-SGT à destination et en provenance d'autres périphériques réseau. L'utilisation de SXP permet aux périphériques de sécurité et aux pare-feu d'obtenir les informations d'identité des commutateurs d'accès sans qu'il soit nécessaire de procéder à des mises à niveau ou à des modifications du matériel. SXP peut également être utilisé pour transmettre les entrées de mappage IP-SGT des périphériques en amont (comme les périphériques de centre de données) vers les périphériques en aval. L'ASA peut recevoir des informations des directions en amont et en aval.

Lors de la configuration d'une connexion SXP sur l'ASA avec un homologue SXP, vous devez désigner l'ASA comme Speaker ou Listener pour cette connexion afin qu'il puisse échanger des informations d'identité :

- Mode Speaker : configure l'ASA afin qu'il puisse transférer toutes les entrées de mappage IP-SGT actives collectées sur l'ASA vers des périphériques en amont pour l'application des politiques.
- Mode Listener : configure l'ASA afin qu'il puisse recevoir des entrées de mappage IP-SGT des périphériques en aval (commutateurs compatibles avec SGT) et utiliser ces informations pour créer des définitions de politique.

Si une extrémité d'une connexion SXP est configurée en tant que Speaker, l'autre extrémité doit être configurée en tant que Listener, et vice versa. Si les deux périphériques à chaque extrémité d'une connexion SXP sont configurés avec le même rôle (soit les deux comme Speakers, soit les deux comme Listeners), la connexion SXP échoue et l'ASA génère un message syslog.

Plusieurs connexions SXP peuvent apprendre les entrées de mappage IP-SGT qui ont été téléchargées à partir de la base de données de mappage IP-SGT. Après l'établissement d'une connexion SXP avec un homologue SXP sur l'ASA, le Listener télécharge l'ensemble de la base de données de mappage IP-SGT à partir du Speaker. Toutes les modifications apportées après cela ne sont envoyées que lorsqu'un nouveau périphérique apparaît sur le réseau. Par conséquent, le débit du flux d'informations SXP est conditionnel au débit auquel les hôtes terminaux s'authentifient auprès du réseau.

Les entrées de mappage IP-SGT qui ont été apprises des connexions SXP sont conservées dans la base de données de mappage SXP IP-SGT. Les mêmes entrées de mappage peuvent être apprises de différentes connexions SXP. La base de données de mappage conserve une copie pour chaque entrée de mappage apprise. Plusieurs entrées de mappage de la même valeur de mappage IP-SGT sont identifiées par l'adresse IP homologue de la connexion à partir de laquelle le mappage a été appris. SXP demande au gestionnaire IP-SGT d'ajouter

une entrée de mappage lorsqu'un nouveau mappage est appris pour la première fois et de supprimer une entrée de mappage lorsque la dernière copie dans la base de données SXP est supprimée.

Chaque fois qu'une connexion SXP est configurée en tant que Speaker, SXP demande au gestionnaire IP-SGT de transférer toutes les entrées de mappage collectées sur le périphérique vers l'homologue. Lorsqu'un nouveau mappage est appris localement, le gestionnaire IP-SGT demande à SXP de le transmettre par des connexions configurées comme Speakers.

La configuration de l'ASA pour qu'il soit à la fois Speaker et Listener pour une connexion SXP peut entraîner une boucle SXP, ce qui signifie que les données SXP peuvent être reçues par un homologue SXP qui les a transmises à l'origine.

Enregistrer l'ASA auprès de l'ISE

L'ASA doit être configurée comme un appareil réseau Cisco TrustSec reconnu dans l'ISE avant que l'ASA puisse importer avec succès un fichier PAC. Pour enregistrer l'ASA auprès de l'ISE, procédez comme suit :

Procédure

Étape 1 Connectez-vous à l'ISE.

Étape 2 Choisissez **Administration** > **Network Devices (Périphériques réseau)** > **Network Devices (Périphériques réseau)**.

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Saisissez l'adresse IP de l'ASA.

Étape 5 Lorsque l'ISE est utilisé pour l'authentification des utilisateurs, saisissez un secret partagé dans la zone Authentication Settings (paramètres d'authentification).

Lorsque vous configurez le serveur AAA sur l'ASA, fournissez le secret partagé que vous créez ici sur l'ISE. Le serveur AAA sur l'ASA utilise ce secret partagé pour communiquer avec l'ISE.

Étape 6 Précisez un nom de périphérique, un ID de périphérique, un mot de passe et un intervalle de téléchargement pour l'ASA. Consultez la documentation d'ISE pour savoir comment effectuer ces tâches.

Créer un groupe de sécurité sur l'ISE

Lors de la configuration de l'ASA pour communiquer avec l'ISE, vous spécifiez un serveur AAA. Lors de la configuration du serveur AAA sur l'ASA, vous devez spécifier un groupe de serveurs. Le groupe de sécurité doit être configuré pour utiliser le protocole RADIUS. Pour créer un groupe de sécurité sur l'ISE, procédez comme suit :

Procédure

Étape 1 Connectez-vous à l'ISE.

Étape 2 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Security Group Access (Accès au groupe de sécurité)** > **Security Group (Groupe de sécurité)**.

Étape 3 Ajoutez un groupe de sécurité pour l'ASA. (Les groupes de sécurité sont globaux et non spécifiques à l'ASA.)

L'ISE crée une entrée sous Security Groups (Groupes de sécurité) avec une balise.

Étape 4 Dans la zone Security Group Access (Accès au groupe de sécurité), configurez les informations d'authentification d'ID de périphérique et un mot de passe pour l'ASA.

Générer le fichier PAC

Pour générer le fichier PAC, procédez comme suit.

Remarque Le fichier PAC comprend une clé partagée qui permet à l'ASA et à l'ISE de sécuriser les transactions RADIUS qui se produisent entre eux. Pour cette raison, assurez-vous de le stocker en toute sécurité sur l'ASA.

Procédure

Étape 1 Connectez-vous à l'ISE.

Étape 2 Choisissez **Administration** > **Network Resources (Ressources réseau)** > **Network Devices (Périphériques réseau)**.

Étape 3 Dans la liste des périphériques, choisissez l'ASA.

Étape 4 Sous Security Group Access (SGA) (Accès aux groupes de sécurité), cliquez sur **Generate PAC** (Générer le PAC).

Étape 5 Pour chiffrer le fichier PAC, saisissez un mot de passe.

Le mot de passe (ou la clé de chiffrement) que vous saisissez pour chiffrer le fichier PAC est indépendant du mot de passe qui a été configuré sur l'ISE dans le cadre des informations d'authentification du périphérique.

L'ISE génère le fichier PAC. L'ASA peut importer le fichier PAC à partir de la mémoire flash ou d'un serveur distant via TFTP, FTP, HTTP, HTTPS ou SMB. (Le fichier PAC ne doit pas résider sur la mémoire flash de l'ASA avant que vous puissiez l'importer.)

Lignes directrices relatives à Cisco TrustSec

Cette section comprend les lignes directrices et les limites que vous devez consulter avant de configurer Cisco TrustSec.

Basculement

- Vous pouvez configurer des politiques basées sur des groupes de sécurité sur l'ASA dans les configurations actif/actif et actif/veille.

- Lorsque l'ASA fait partie d'une configuration de basculement, vous devez importer le fichier PAC sur le périphérique ASA principal. Vous devez également actualiser les données d'environnement sur le périphérique principal.
- L'ASA peut communiquer avec l'ISE configuré pour la haute disponibilité (HA).
- Vous pouvez configurer plusieurs serveurs ISE sur l'ASA et si le premier serveur est inaccessible, il continue vers le serveur suivant, etc. Toutefois, si la liste de serveurs est téléchargée dans le cadre des données d'environnement Cisco TrustSec, elle est ignorée.
- Si le fichier PAC téléchargé depuis l'ISE expire sur l'ASA et que celui-ci ne parvient pas à télécharger une table de groupes de sécurité mise à jour, l'ASA continue d'appliquer les politiques de sécurité selon la dernière table de groupes de sécurité téléchargée, jusqu'au téléchargement d'une table mise à jour.

Mise en grappes

- Lorsque l'ASA fait partie d'une configuration de mise en grappe, vous devez importer le fichier PAC dans l'unité de contrôle.
- Lorsque l'ASA fait partie d'une configuration de mise en grappe, vous devez actualiser les données d'environnement sur l'unité de contrôle.

IPv6

L'ASA prend en charge SXP pour IPv6 et les périphériques réseau compatibles avec IPv6. Le serveur AAA doit utiliser une adresse IPv4.

Imposition de la balise de groupe de sécurité de couche 2

- Pris en charge uniquement sur les interfaces physiques, les sous-interfaces et les interfaces EtherChannel.
- Non pris en charge sur les interfaces logiques ou les interfaces virtuelles, comme les BVI.
- Ne prend pas en charge le chiffrement de liaison à l'aide de la négociation SAP et de MACsec.
- Aucune prise en charge sur les liaisons de basculement.
- Aucune prise en charge sur les liaisons de commande de grappe.
- L'ASA ne reclasse pas les flux existants si la balise SGT est modifiée. Toutes les décisions de politique prises en fonction de la balise SGT précédente restent en vigueur pendant la durée du flux. Cependant, l'ASA peut refléter immédiatement les modifications de SGT sur les paquets de sortie, même si les paquets appartiennent à un flux dont la classification était basée sur une SGT précédente.
- Les ports de commutation Firepower 1010 et les interfaces VLAN ne prennent pas en charge l'application du balisage de groupe de sécurité de couche 2.

Lignes directrices supplémentaires

- L'ASA prend en charge SXP version 3. L'ASA négocie les versions de SXP avec différents périphériques réseau compatibles avec SXP.
- Vous pouvez configurer l'ASA pour actualiser la table de groupes de sécurité à l'expiration du temporisateur de resynchronisation SXP et télécharger la table de groupes de sécurité à la demande.

Lorsque la table de groupe de sécurité sur l'ASA est mise à jour à partir d'ISE, les modifications sont répercutées dans les politiques de sécurité appropriées.

- Cisco TrustSec prend en charge la fonctionnalité Smart Call Home en mode contexte unique et multi-contexte, mais pas dans le contexte du système.
- L'ASA ne peut être configurée que pour l'interopérabilité dans un seul domaine Cisco TrustSec.
- L'ASA ne prend pas en charge la configuration statique du mappage de nom SGT sur le périphérique.
- La NAT n'est pas prise en charge dans les messages SXP.
- SXP achemine le mappage IP-SGT vers les points d'application dans le réseau. Si un commutateur de couche d'accès appartient à un domaine NAT différent de celui du point d'application, le mappage IP-SGT qu'il charge n'est pas valide et une recherche de base de données de mappage IP-SGT sur le périphérique d'application ne donne pas de résultats valides. Par conséquent, l'ASA ne peut pas appliquer la politique de sécurité compatible avec les groupes de sécurité sur le périphérique d'application.
- Vous pouvez configurer un mot de passe par défaut que l'ASA utilise pour les connexions SXP, ou vous pouvez choisir de ne pas utiliser de mot de passe; cependant, les mots de passe spécifiques à la connexion ne sont pas pris en charge pour les homologues SXP. Le mot de passe SXP par défaut configuré doit être cohérent sur le réseau de déploiement. Si vous configurez un mot de passe de connexion spécifique, les connexions peuvent échouer et un message d'avertissement s'affiche. Si vous configurez la connexion avec le mot de passe par défaut, mais qu'il n'est pas configuré, le résultat est le même que lorsque vous avez configuré la connexion sans mot de passe.
- L'ASA peut être configuré comme un Speaker ou un Listener SXP, ou les deux. Cependant, des boucles de connexion SXP peuvent se former lorsqu'un périphérique a des connexions bidirectionnelles avec un homologue ou fait partie d'une chaîne de périphériques connectés de manière unidirectionnelle. (L'ASA peut apprendre le mappage IP-SGT pour les ressources de la couche d'accès dans le centre de données. L'ASA pourrait avoir besoin de propager ces balises vers les périphériques en aval.) Les boucles de connexion SXP peuvent entraîner un comportement inattendu du transport des messages SXP. Dans les cas où l'ASA est configuré pour être un Speaker et un Listener, une boucle de connexion SXP peut se produire, ce qui fait que les données SXP sont reçues par l'homologue qui les a transmises à l'origine.
- Lors de la modification de l'adresse IP locale de l'ASA, vous devez vous assurer que tous les homologues SXP ont mis à jour leur liste d'homologues. En outre, si les homologues SXP modifient leurs adresses IP, vous devez vous assurer que ces modifications sont répercutées sur l'ASA.
- Le provisionnement automatique du fichier PAC n'est pas pris en charge. L'administrateur de l'ASA doit demander le fichier PAC à l'interface d'administration ISE et l'importer dans l'ASA.
- Les fichiers PAC ont des dates d'expiration. Vous devez importer le fichier PAC mis à jour avant que le fichier PAC actuel n'expire; sinon, l'ASA ne peut pas récupérer les mises à jour des données d'environnement. Si le fichier PAC téléchargé depuis l'ISE expire sur l'ASA et que celui-ci ne parvient pas à télécharger une table de groupes de sécurité mise à jour, l'ASA continue d'appliquer les politiques de sécurité selon la dernière table de groupes de sécurité téléchargée, jusqu'au téléchargement d'une table mise à jour.
- Lorsqu'un groupe de sécurité change sur ISE (par exemple, il est renommé ou supprimé), l'ASA ne modifie pas l'état des politiques de sécurité ASA qui contiennent une balise SGT ou un nom de groupe de sécurité associé au groupe de sécurité modifié ; cependant, l'ASA génère un message syslog pour indiquer que ces politiques de sécurité ont été modifiées.
- Les types de multidiffusion ne sont pas pris en charge dans ISE 1.0.

- Une connexion SXP reste dans l'état d'initialisation entre deux homologues SXP interconnectés par l'ASA; comme le montre l'exemple suivant :

```
(SXP peer A) - - - - (ASA) - - - (SXP peer B)
```

Par conséquent, lors de la configuration de l'ASA pour l'intégration à Cisco TrustSec, vous devez activer les options TCP no-NAT, no-SEQ-RAND et MD5-AUTHENTICATION sur l'ASA pour configurer les connexions SXP. Créez une politique de contournement d'état TCP pour le trafic destiné au port SXP TCP 64999 entre les homologues SXP. Appliquez ensuite la politique sur les interfaces appropriées.

Par exemple, l'ensemble de commandes suivant montre comment configurer l'ASA pour une politique de contournement de l'état TCP :

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

Configurer l'ASA pour s'intégrer à Cisco TrustSec

Pour configurer l'ASA afin qu'il s'intègre à Cisco TrustSec, effectuez les tâches suivantes.

Avant de commencer

Avant de configurer l'ASA pour qu'il s'intègre à Cisco TrustSec, vous devez effectuer les tâches suivantes dans ISE :

- Enregistrer l'ASA auprès de l'ISE, à la page 8
- Créer un groupe de sécurité sur l'ISE, à la page 8
- Générer le fichier PAC, à la page 9

Procédure

Étape 1 Configurer le serveur AAA pour l'intégration de Cisco TrustSec, à la page 13

Étape 2 Importer un fichier PAC, à la page 15

Étape 3 Configurer le protocole d'échange de sécurité, à la page 16

Cette tâche active et définit les valeurs par défaut pour SXP.

Étape 4 Ajouter un homologue de connexion SXP, à la page 18

Étape 5 Actualiser les données d'environnement, à la page 20

Effectuez cette opération selon les besoins.

Étape 6 Configurer la politique de sécurité, à la page 20

Étape 7 Configurer l'imposition du balisage de groupe de sécurité de couche 2, à la page 22

Configurer le serveur AAA pour l'intégration de Cisco TrustSec

Cette section décrit comment intégrer le serveur AAA pour Cisco TrustSec. Pour configurer le groupe de serveurs AAA afin de communiquer avec l'ISE sur l'ASA, procédez comme suit.

Avant de commencer

- Le groupe de serveurs référencé doit être configuré pour utiliser le protocole RADIUS. Si vous ajoutez un groupe de serveurs non RADIUS à l'ASA, la configuration échoue.
- Si ISE est également utilisé pour l'authentification des utilisateurs, obtenez le secret partagé qui a été saisi sur ISE lorsque vous avez enregistré l'ASA auprès d'ISE. Communiquez avec votre administrateur ISE pour obtenir ces informations.

Procédure

Étape 1 Créez le groupe de serveurs AAA et configurez les paramètres de serveur AAA pour que l'ASA communique avec le serveur ISE.

aaa-server *server_tag* **protocol radius**

Exemple :

```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

L'argument *server-tag* spécifie le nom du groupe de serveurs.

Étape 2 Quittez le mode de configuration de groupe de serveurs aaa.

exit

Exemple :

```
ciscoasa(config-aaa-server-group)# exit
```

Étape 3 Configurez un serveur AAA dans le cadre d'un groupe de serveurs AAA et définissez des données de connexion spécifiques à l'hôte.

```
ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip
```

Exemple :

```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

L'argument *interface-name* spécifie l'interface réseau dans laquelle se trouve le serveur ISE. Les parenthèses sont requises dans ce paramètre. L'argument *server-tag* est le nom du groupe de serveurs AAA. L'argument *server-ip* spécifie l'adresse IP du serveur ISE.

Étape 4 Spécifiez la valeur de clé secrète de serveur utilisée pour authentifier l'ASA auprès du serveur ISE.

key *key*

Exemple :

```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

L'argument *de clé* est un mot-clé alphanumérique de 127 caractères maximum.

Si ISE est également utilisé pour l'authentification des utilisateurs, saisissez le secret partagé qui a été saisi sur ISE lorsque vous avez enregistré l'ASA auprès d'ISE.

Étape 5 Quittez le mode de configuration de l'hôte du serveur AAA.

exit

Exemple :

```
ciscoasa(config-aaa-server-host)# exit
```

Étape 6 Déterminez le groupe de serveurs AAA utilisé par Cisco TrustSec pour la récupération des données d'environnement.

cts server-group *AAA-server-group-name*

Exemple :

```
ciscoasa(config)# cts server-group ISEserver
```

L'argument *AAA-server-group-name* est le nom du groupe de serveurs AAA que vous avez spécifié à l'étape 1 dans l'argument *server-tag*.

Remarque
Vous ne pouvez configurer qu'une seule instance du groupe de serveurs sur l'ASA pour Cisco TrustSec.

L'exemple suivant montre comment configurer l'ASA pour qu'il communique avec le serveur ISE pour l'intégration de Cisco TrustSec :

```
ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
```

```
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

Importer un fichier PAC

Cette section décrit comment importer un fichier PAC.

Avant de commencer

- L'ASA doit être configurée comme périphérique réseau Cisco TrustSec reconnu dans l'ISE avant que l'ASA puisse générer un fichier PAC.
- Obtenez le mot de passe utilisé pour chiffrer le fichier PAC lors de sa génération sur l'ISE. L'ASA nécessite ce mot de passe pour importer et déchiffrer le fichier PAC.
- Lors de l'importation, le fichier PAC réside dans la NVRAM. Lors du fonctionnement en mode haute disponibilité, si vous configurez correctement les liens de basculement et les liaisons avec état, l'importation du fichier PAC dans l'unité active entraînera la réplication sur l'unité secondaire. Comme le fichier importé réside dans la NVRAM, vous devez importer le fichier à nouveau chaque fois que le périphérique redémarre, par exemple, après une mise à niveau logicielle.
- Le périphérique utilise un seul fichier PAC. Si vous en importez plusieurs, chaque fichier PAC importé remplace le fichier importé précédemment.
- L'ASA nécessite d'accéder au fichier PAC généré par l'ISE. L'ASA peut importer le fichier PAC à partir de la mémoire flash ou d'un serveur distant via TFTP, FTP, HTTP, HTTPS ou SMB. (Le fichier PAC n'a pas besoin de résider sur la mémoire flash ASA avant que vous puissiez l'importer.)
- Le groupe de serveurs a été configuré pour l'ASA.

Procédure

Importer un fichier PAC Cisco TrustSec.

cts import-pac *filepath* **password** *value*

Exemple :

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

L'argument *value* spécifie le mot de passe utilisé pour chiffrer le fichier PAC. Le mot de passe est indépendant du mot de passe qui a été configuré sur l'ISE dans le cadre des informations d'authentification du périphérique. L'argument *filepath* est saisi comme l'une des options suivantes :

Mode unique

- **disk0** : chemin d'accès et nom de fichier sur disk0
- **disk1** : chemin d'accès et nom de fichier sur disk1
- **flash** : chemin d'accès et nom de fichier en mémoire flash

- **ftp** : chemin d'accès et nom de fichier sur FTP
- **http** : chemin d'accès et nom de fichier sur HTTP
- **https** : chemin d'accès et nom de fichier sur HTTPS
- **smb** : chemin d'accès et nom de fichier sur SMB
- **tftp** : chemin d'accès et nom de fichier sur TFTP

Multi-mode

- **http** : chemin d'accès et nom de fichier sur HTTP
- **https** : chemin d'accès et nom de fichier sur HTTPS
- **smb**: chemin d'accès et nom de fichier sur SMB
- **tftp** : chemin d'accès et nom de fichier sur TFTP

L'exemple suivant montre comment importer un fichier PAC dans l'ASA :

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

Configurer le protocole d'échange de sécurité

Vous devez activer et configurer le protocole SXP (Security Exchange Protocol) pour utiliser Cisco Trustsec.

Avant de commencer

Au moins une interface doit être à l'état UP/UP. Si vous activez SXP avec toutes les interfaces en panne, l'ASA n'affiche pas de message indiquant que SXP ne fonctionne pas ou qu'il n'a pas pu être activé. Si vous vérifiez la configuration en saisissant la commande **show running-config**, la sortie affiche le message suivant :

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

Procédure

Étape 1 Activez SXP sur l'ASA. Par défaut, SXP est désactivé.

cts sxp enable

Exemple :

```
ciscoasa(config)# cts sxp enable
```

Étape 2 (Facultatif ; non recommandé.) Configurez l'adresse IP source par défaut pour les connexions SXP.

cts sxp default source-ip *ipaddress*

Exemple :

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

L'argument *ipaddress* peut être une adresse IPv4 ou IPv6.

Lorsque vous configurez une adresse IP source par défaut pour les connexions SXP, vous devez spécifier la même adresse que l'interface sortante ASA. Si l'adresse IP source ne correspond pas à l'adresse de l'interface sortante, les connexions SXP échouent.

Lorsqu'une adresse IP source pour une connexion SXP n'est pas configurée, l'ASA effectue une recherche de routage/ARP pour déterminer l'interface sortante pour la connexion SXP. Nous vous recommandons de ne pas configurer d'adresse IP source par défaut pour les connexions SXP et de permettre à l'ASA d'effectuer une recherche de routage/ARP pour déterminer l'adresse IP source d'une connexion SXP.

Étape 3 (Facultatif) Configurez le mot de passe par défaut pour l'authentification TCP MD5 avec les homologues SXP. Par défaut, les connexions SXP n'ont pas de mot de passe.

cts sxp default password [**0** | **8**] *password*

Exemple :

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

Configurez un mot de passe par défaut si et seulement si vous configurez les homologues de connexion SXP pour utiliser le mot de passe par défaut.

La longueur du mot de passe dépend du niveau de déchiffrement, qui prend la valeur 0 par défaut si vous ne le spécifiez pas :

- **0** : texte en clair non chiffré. Le mot de passe peut comporter jusqu'à 80 caractères.
- **8** : texte chiffré. Le mot de passe peut comporter jusqu'à 162 caractères.

Étape 4 (Facultatif) Précisez l'intervalle de temps entre les tentatives de l'ASA pour configurer de nouvelles connexions SXP entre les homologues SXP.

cts sxp retry period *timervalue*

Exemple :

```
ciscoasa(config)# cts sxp retry period 60
```

L'ASA continue de faire des tentatives de connexion jusqu'à ce qu'une connexion réussisse, en attendant l'intervalle de nouvelle tentative avant de réessayer après un échec de tentative. Vous pouvez spécifier une période de nouvelle tentative comprise entre 0 et 64 000 secondes. La valeur par défaut est de 120 secondes. Si vous spécifiez 0 seconde, l'ASA ne tente pas de se connecter aux homologues SXP.

Nous vous recommandons de configurer le temporisateur de nouvelle tentative à une valeur différente de celle des périphériques homologues SXP.

Étape 5 (Facultatif) Précisez la valeur du temporisateur de resynchronisation.

cts sxp reconciliation period *timervalue*

Exemple :

```
ciscoasa(config)# cts sxp reconciliation period 60
```

Une fois qu'un homologue a mis fin à une connexion SXP, une temporisateur de maintien démarre. Si un homologue SXP se connecte pendant l'exécution du temporisateur de maintien, l'ASA démarre le temporisateur de resynchronisation ; puis, l'ASA met à jour la base de données de mappage SXP pour connaître les derniers mappages.

À l'expiration du temporisateur de resynchronisation, l'ASA analyse la base de données de mappage SXP pour identifier les entrées de mappage périmées (qui ont été apprises lors d'une session de connexion précédente). L'ASA marque ces connexions comme obsolètes. À l'expiration du temporisateur de resynchronisation, l'ASA supprime les entrées obsolètes de la base de données de mappage SXP.

Vous pouvez spécifier une période de rapprochement comprise entre 1 et 64 000 secondes. La valeur par défaut est de 120 secondes.

Étape 6 (Facultatif) Configurez le temporisateur de maintien de suppression pour les mappages IP-SGT appris d'un homologue après qu'un homologue SXP ait mis fin à sa connexion SXP.

cts sxp delete-hold-down period *timervalue*

La valeur du temporisateur spécifie le nombre de secondes, de 120 à 64 000, pendant lesquelles les mappages IP-SGT appris d'une connexion SXP interrompue sont conservés avant d'être supprimés.

Exemple :

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

Chaque connexion SXP est associée à un temporisateur de maintien de suppression. Ce temporisateur est déclenché lorsqu'une connexion SXP du côté de l'écouteur est interrompue. Les mappages IP-SGT appris de cette connexion SXP ne sont pas supprimés immédiatement. Au lieu de cela, ils sont conservés jusqu'à l'expiration du temporisateur de maintien de suppression. Les mappages sont supprimés à l'expiration de ce temporisateur.

Étape 7 (Facultatif) Configurez la profondeur d'expansion du sous-réseau IPv4 lorsque l'ASA agit en tant que speaker pour des homologues utilisant SXPv2 ou une version antérieure.

cts sxp mapping network-map *maximum_hosts*

Si un homologue utilise SXPv2 ou une version antérieure, il ne peut pas comprendre les liaisons entre SGT et sous-réseaux. L'ASA peut étendre les liaisons de sous-réseau IPv4 aux liaisons d'hôtes individuels (les liaisons IPv6 ne sont pas étendues). Cette commande spécifie le nombre maximal de liaisons d'hôte qui peuvent être générées à partir d'une liaison de sous-réseau.

Vous pouvez spécifier que le nombre maximal est compris entre 0 et 65 535. La valeur par défaut est 0, ce qui signifie que les liaisons de sous-réseau ne sont pas développées en liaisons d'hôte.

Ajouter un homologue de connexion SXP

Pour ajouter un homologue de connexion SXP, procédez comme suit :

Procédure

Établissez une connexion SXP avec un homologue SXP.

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **none**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

Exemple :

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

Les connexions SXP sont définies par adresse IP; une seule paire de périphériques peut assurer plusieurs connexions SXP.

L'argument*peer_ip_address* est l'adresse IPv4 ou IPv6 de l'homologue SXP. L'adresse IP de l'homologue doit être accessible à partir de l'interface sortante de l'ASA.

L'argument *source_ip_address* est l'adresse locale IPv4 ou IPv6 de la connexion SXP. L'adresse IP source doit être la même que celle de l'interface sortante de l'ASA, sinon la connexion échoue.

Nous vous recommandons de ne pas configurer d'adresse IP source pour une connexion SXP et de permettre à l'ASA d'effectuer une recherche de routage/ARP pour déterminer l'adresse IP source de la connexion SXP.

Indiquez s'il faut utiliser ou non la clé d'authentification pour la connexion SXP :

- **default** : utilisez le mot de passe par défaut configuré pour les connexions SXP.
- **none** : n'utilisez pas de mot de passe pour la connexion SXP.

Indiquez le mode de la connexion SXP :

- **local** : utilisez le périphérique SXP local.
- **peer** : utilisez le périphérique SXP homologue.

Indiquez si l'ASA fonctionne comme speaker ou comme listener pour la connexion SXP.

- **speaker** : l'ASA peut transférer le mappage IP-SGT vers des périphériques en amont.
- **listener** : l'ASA peut recevoir un mappage IP-SGT de la part de périphériques en aval.

L'exemple suivant montre comment configurer les homologues SXP sur l'ASA :

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default
mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default
mode peer speaker
```

Actualiser les données d'environnement

L'ASA télécharge les données d'environnement à partir de l'ISE, qui comprend la table de noms de balise de groupe de sécurité (SGT). L'ASA actualise automatiquement ses données d'environnement obtenues auprès de l'ISE lorsque vous effectuez les tâches suivantes sur l'ASA :

- Configurez un serveur AAA pour communiquer avec l'ISE.
- Importez un fichier PAC à partir de l'ISE.
- Déterminez le groupe de serveurs AAA que l'ASA utilisera pour récupérer les données d'environnement Cisco TrustSec.

Normalement, vous n'avez pas besoin d'actualiser manuellement les données d'environnement à partir de l'ISE; cependant, les groupes de sécurité peuvent changer sur l'ISE. Ces modifications ne sont pas répercutées sur l'ASA tant que vous n'avez pas actualisé les données dans la table des groupes de sécurité de l'ASA. Actualisez donc les données sur l'ASA pour vous assurer que toutes les modifications de groupe de sécurité apportées sur l'ISE sont répercutées sur l'ASA.

Remarque Nous vous recommandons de planifier les modifications de configuration des politiques sur l'ISE et l'actualisation manuelle des données sur l'ASA pendant une fenêtre de maintenance. Le traitement des modifications de configuration des politiques de cette manière maximise les possibilités de résolution des noms de groupes de sécurité et l'activation immédiate des politiques de sécurité sur l'ASA.

Pour actualiser les données d'environnement, procédez comme suit :

Procédure

Actualisez les données d'environnement depuis l'ISE et réinitialisez le temporisateur de resynchronisation à la valeur par défaut configurée.

```
cts refresh environment-data
```

Exemple :

```
ciscoasa(config)# cts refresh environment-data
```

Configurer la politique de sécurité

Vous pouvez intégrer la politique Cisco TrustSec dans de nombreuses fonctionnalités ASA. Toute fonctionnalité qui utilise des listes de contrôle d'accès étendues (sauf si elle est répertoriée dans ce chapitre comme non prise en charge) peut tirer parti de Cisco TrustSec. Vous pouvez ajouter des arguments de groupe de sécurité aux listes de contrôle d'accès étendues, ainsi qu'aux paramètres basés sur le réseau traditionnel.

- Pour configurer une liste de contrôle d'accès étendue, consultez Ajouter une ACE étendue pour la correspondance basée sur un groupe de sécurité (Cisco TrustSec).

- Pour configurer les groupes d'objets de groupe de sécurité qui peuvent être utilisés dans l'ACL, consultez Configurer les groupes d'objets de sécurité.

Par exemple, une règle d'accès autorise ou refuse le trafic sur une interface en utilisant les informations réseau. Grâce à Cisco TrustSec, vous pouvez contrôler l'accès en fonction du groupe de sécurité. Par exemple, vous pouvez créer une règle d'accès pour sample_securitygroup1 10.0.0.0 255.0.0.0, ce qui signifie que le groupe de sécurité peut avoir n'importe quelle adresse IP sur le sous-réseau 10.0.0.0/8.

Vous pouvez configurer des politiques de sécurité en fonction de combinaisons de noms de groupes de sécurité (serveurs, utilisateurs, périphériques non gérés, etc.), d'attributs basés sur l'utilisateur et d'objets basés sur l'adresse IP traditionnelle (adresse IP, objet Active Directory et nom de domaine complet FQDN). L'appartenance au groupe de sécurité peut s'étendre au-delà des rôles pour inclure les attributs de périphérique et d'emplacement et est indépendante de l'appartenance au groupe d'utilisateurs.

L'exemple suivant montre comment créer une liste de contrôle d'accès qui utilise un groupe d'objets de sécurité défini localement :

```
object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
   security-group name hr-admin-sg-name  // single sg_name
   group-object it-admin     // locally defined object-group as nested object
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
object-group security objgrp-hr-network
security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

La liste de contrôle d'accès configurée dans l'exemple précédent peut être activée en configurant un groupe d'accès ou le cadre de politique modulaire.

Exemples supplémentaires :

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group
name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSCO\mary any security-group
name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
! to dst objgrp-hr-servers any network
access-list idfw-acl permit ip user CSCO\Jack object-group-security
objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
```

```
object network net-google
fqdn google.com
access-list sgacl permit ip sec name mktg any object net-google

! If user Tom or object_group security objgrp-hr-admin needs to be matched,
! multiple ACEs can be defined as follows:
access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin
    10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any
```

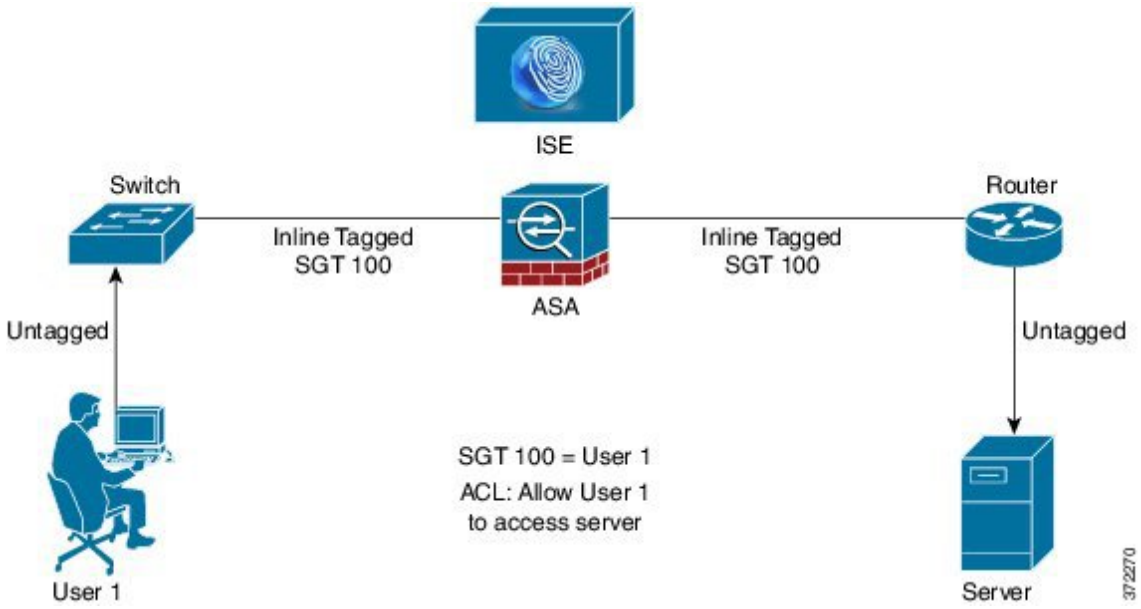
Configurer l'imposition du balisage de groupe de sécurité de couche 2

Cisco TrustSec identifie et authentifie chaque utilisateur et ressource du réseau et attribue un numéro de 16 bits appelé balise de groupe de sécurité (SGT). Cet identifiant est à son tour propagé entre les sauts de réseau, ce qui permet à tous les périphériques intermédiaires tels que les ASA, les commutateurs et les routeurs d'appliquer des politiques en fonction de cette balise d'identité.

SGT plus Ethernet Tagging, également appelé Imposition SGT de couche 2, permet à l'ASA d'envoyer et de recevoir des balises de groupe de sécurité sur les interfaces Ethernet à l'aide du cadrage Ethernet propriétaire de Cisco (EtherType 0x8909), qui permet l'insertion de balises de groupe de sécurité source dans des trames Ethernet en texte brut. L'ASA insère des balises de groupe de sécurité sur le paquet sortant et traite les balises de groupe de sécurité sur le paquet entrant, en fonction d'une configuration manuelle par interface. Cette fonctionnalité permet la propagation en ligne, saut par saut, de l'identité des terminaux sur les périphériques réseau et fournit une imposition SGT de couche 2 transparente entre chaque saut.

La figure suivante montre un exemple typique d'imposition SGT de couche 2.

Illustration 3 : Imposition SGT de couche 2



Scénarios d'utilisation

Le tableau suivant décrit le comportement attendu pour le trafic d'entrée lors de la configuration de cette fonctionnalité.

Tableau 1 : Trafic d'entrée

Configuration de l'interface	Paquet étiqueté reçu	Paquet non étiqueté reçu
Aucune commande n'est envoyée.	Paquet abandonné.	La valeur SGT provient du gestionnaire IP-SGT.
La commande **cts manual** est émise.	La valeur SGT provient du gestionnaire IP-SGT.	La valeur SGT provient du gestionnaire IP-SGT.
La commande **cts manual** et la commande **policy static sgt** *sgt_number* sont toutes deux émises.	La valeur SGT provient de la commande **policy static sgt** *sgt_number* .	La valeur SGT provient de la commande **policy static sgt** *sgt_number* .
La commande **cts manual** et la commande **policy static sgt** *sgt_number* **trusted** sont toutes deux émises.	La valeur SGT provient de la SGT en ligne dans le paquet.	La valeur SGT provient de la commande **policy static sgt** *sgt_number* .

Remarque S'il n'y a pas de mappage IP-SGT correspondant à partir du gestionnaire IP-SGT, une valeur SGT réservée de « 0x0 » pour « Inconnu » est utilisée.

Le tableau suivant décrit le comportement attendu pour le trafic de sortie lors de la configuration de cette fonctionnalité.

Tableau 2 : Trafic de sortie

Configuration de l'interface	Paquet étiqueté ou non étiqueté envoyé
Aucune commande n'est envoyée.	Non balisé
La commande **cts manual** est émise.	Balisé
La commande **cts manual** et la commande **propagate sgt** sont toutes deux émises.	Balisé
La commande **cts manual** et la commande **no propagate sgt** sont toutes deux émises.	Non balisé

Le tableau suivant décrit le comportement attendu du trafic vers le boîtier et à partir du boîtier lors de la configuration de cette fonctionnalité.

Tableau 3 : Trafic entrant et sortant

Configuration de l'interface	Paquet étiqueté ou non étiqueté reçu
Aucune commande n'est émise sur l'interface d'entrée pour le trafic vers le boîtier.	Paquet abandonné.
La commande **cts manual** est émise sur l'interface d'entrée pour le trafic vers le boîtier.	Le paquet est accepté, mais il n'y a pas d'applicatio ni de propagation de SGT.

Configuration de l'interface	Paquet étiqueté ou non étiqueté reçu
La commande **cts manual** n'est pas émise ou la commande **cts manual** et **no propagate sgt** sont toutes deux émises sur l'interface de sortie pour le trafic à partir du boîtier.	Un paquet non étiqueté est envoyé, mais il n'y a pas d'a de la politique. Le numéro SGT provient du gestionnair
La commande **cts manual** est émise ou la commande **cts manual** et la commande **propagate sgt** sont toutes deux émises sur l'interface de sortie pour le trafic à partir du boîtier.	Le paquet étiqueté est envoyé. Le numéro SGT provie gestionnaire IP-SGT.

Remarque S'il n'y a pas de mappage IP-SGT correspondant à partir du gestionnaire IP-SGT, une valeur SGT réservée de « 0x0 » pour « Inconnu » est utilisée.

Configurer une balise de groupe de sécurité sur une interface

Pour configurer une balise de groupe de sécurité sur une interface, procédez comme suit :

Procédure

Étape 1 Configurez une interface et passez en mode de configuration d'interface :

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
```

Étape 2 Activez l'imposition SGT de couche 2 et passez en mode de configuration d'interface cts manual.

cts manual

Exemple :

```
ciscoasa(config-if)# cts manual
```

Étape 3 Activez la propagation d'une balise de groupe de sécurité sur une interface. La propagation est activée par défaut.

propagate sgt

Exemple :

```
ciscoasa(config-if-cts-manual)# propagate sgt
```

Étape 4 Appliquez une politique à une liaison CTS configurée manuellement.

policy static sgt *sgt_number* [**trusted**]

Exemple :

```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

Le mot-clé **static** spécifie une politique SGT pour le trafic entrant sur la liaison.

La paire mot-clé-argument **sgt** *sgt_number* spécifie le numéro SGT à appliquer au trafic entrant de l'homologue. Les valeurs valides sont comprises entre 2 et 65 519.

Le mot-clé **trusted** indique que le trafic d'entrée sur l'interface avec la SGT spécifiée dans la commande ne devrait pas voir sa SGT remplacée. Untrusted est la valeur par défaut.

L'exemple suivant active une interface pour l'application de la balise SGT de couche 2 et définit si l'interface est fiable ou non :

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

Configurer manuellement les liaisons IP-SGT

Pour configurer manuellement les liaisons IP-SGT, procédez comme suit :

Procédure

Configurez les liaisons IP-SGT manuellement.

cts role-based sgt-map {*IPv4_addr*[/*mask*] | *IPv6_addr*[/*prefix*]} **sgt** *sgt_value*

Exemple :

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

Vous pouvez utiliser une adresse IPv4 ou IPv6. Vous pouvez également spécifier des adresses réseau en incluant un masque de sous-réseau ou une valeur de préfixe (pour IPv6), comme 10.100.10.0/24. La *valeur sgt_value* est le numéro SGT, de 2 à 65 519.

Astuces de dépannage

Utilisez la commande **packet-tracer** pour déterminer pourquoi une session particulière a été autorisée ou refusée, quelle valeur SGT est utilisée (de SGT dans le paquet, du gestionnaire IP-SGT ou de la commande **policy static sgt** configurée sur l'interface), et quelles politiques de sécurité basées sur des groupes de sécurité ont été appliquées.

L'exemple suivant affiche la sortie de la commande **packet-tracer** pour afficher le mappage de la balise de groupe de sécurité vers une adresse IP :

```
ciscoasa# packet-tracer input inside tcp inline-tag 100
```

```
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
---------------More---------------------
```

Utilisez la commande **capture** *capture-name* **type inline-tag** *tag* pour capturer uniquement les paquets Cisco CMD (EtherType 0x8909) avec ou sans une valeur SGT spécifique.

L'exemple suivant affiche la sortie de la commande **show capture** pour une valeur SGT spécifiée :

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

Exemple pour Cisco TrustSec

L'exemple suivant montre comment configurer l'ASA pour utiliser Cisco TrustSec :

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cts server-group cts-server-list
// Configure SXP peers
cts sxp enable
cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
   interface gi0/1
   cts manual
   propagate sgt
   policy static sgt 100 trusted
   cts role-based sgt-map 10.1.1.100 sgt 50
```

Prise en charge des VPN sécurisés) pour Cisco TrustSec

L'ASA prend en charge le balisage de groupe de sécurité des sessions VPN. Vous pouvez attribuer une balise de groupe de sécurité (SGT) à une session VPN en utilisant un serveur AAA externe, ou en configurant une balise de groupe de sécurité pour un utilisateur local ou pour une politique de groupe VPN. Cette balise peut ensuite être propagée par l'intermédiaire du système Cisco TrustSec sur Ethernet de couche 2. Les balises de groupe de sécurité sont utiles sur les politiques de groupe et pour les utilisateurs locaux lorsque le serveur AAA ne peut pas fournir de SGT.

Voici le processus typique d'attribution d'une balise SGT à un utilisateur de VPN :

1. Un utilisateur se connecte à un VPN d'accès à distance qui utilise un groupe de serveurs AAA contenant des serveurs ISE.
2. L'ASA demande des informations AAA à ISE, qui peuvent inclure une balise SGT.L'ASA attribue également une adresse IP au trafic tunnelisé de l'utilisateur.
3. L'ASA utilise les informations AAA pour authentifier l'utilisateur et crée un tunnel.
4. L'ASA utilise la balise SGT à partir des informations AAA et l'adresse IP attribuée pour ajouter une balise SGT dans l'en-tête de la couche 2.
5. Les paquets qui comprennent la balise SGT sont transmis au périphérique homologue suivant dans le réseau Cisco TrustSec.

S'il n'y a pas de SGT dans les attributs du serveur AAA pour l'affecter à un utilisateur VPN, l'ASA utilise la balise dans la politique de groupe. S'il n'y a pas de balise SGT dans la politique de groupe, la balise 0x0 est attribuée.

Remarque Vous pouvez également utiliser ISE pour appliquer les politiques à l'aide de la modification d'autorisation (CoA) ISE. Pour en savoir plus sur la configuration de l'application des politiques, consultez le guide de configuration VPN.

Ajouter une balise SGT aux politiques de groupe du VPN d'accès à distance et aux utilisateurs locaux

Pour configurer un attribut SGT sur les politiques de groupe VPN d'accès à distance ou sur la politique VPN pour un utilisateur défini dans la base de données d'utilisateurs LOCAL, procédez comme suit.

Il n'y a pas de balise SGT par défaut pour les politiques de groupe ou les utilisateurs locaux.

Procédure

Étape 1 Pour configurer une SGT sur une politique de groupe VPN d'accès à distance :

a) Entrez dans le mode de configuration des attributs group-policy.

group-policy *name*

Exemple :

```
ciscoasa(config)# group policy Grpolicy1
```

b) Configurez la balise SGT pour la politique de groupe.

security-group-tag {**none** | **value** *sgt*}

Si vous définissez une balise à l'aide de **value**, la balise peut être comprise entre 2 et 65 519. Précisez **none** pour ne définir aucune SGT.

Exemple :

```
ciscoasa(config-group-policy# security-group-tag value 101
```

Étape 2 Pour configurer une SGT pour un utilisateur dans la base de données LOCAL :

a) Si nécessaire, créez l'utilisateur.

username *name* {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

Exemple :

```
ciscoasa(config)# username newuser password changeme encrypted privilege 15
```

b) Entrez dans le mode de configuration du nom d'utilisateur.

username *name* **attributes**

Exemple :

```
asa3(config)# username newuser attributes
asa3(config-username)#
```

c) Configurez la SGT pour l'utilisateur.

security-group-tag {**none** | **value** *sgt*}

Si vous définissez une balise à l'aide de **value**, la balise peut être comprise entre 2 et 65 519. Précisez **none** pour ne définir aucune SGT.

Exemple :

```
ciscoasa(config-username)# security-group-tag value 101
```

Surveillance de Cisco TrustSec

Consultez les commandes suivants pour superviser Cisco TrustSec :

- **show running-config cts**
- **show running-config** [**all**] **cts role-based** [**sgt-map**]

Cette commande affiche les entrées du tableau de liaison IP-SGT définies par l'utilisateur.

- **show cts sxp connections**

  Cette commande affiche les connexions SXP sur l'ASA pour un contexte d'utilisateur particulier lorsque le mode contexte multiple est utilisé.

- **show conn security-group**

  Affiche les données de toutes les connexions SXP.

- **show cts environment-data**

  Affiche les informations sur l'environnement Cisco TrustSec contenues dans la table des groupes de sécurité sur l'ASA.

- **show cts sgt-map**

  Affiche les entrées du gestionnaire de tableau de groupe de sécurité d'adresse IP dans le chemin de contrôle.

- **show asp table cts sgt-map**

  Cette commande affiche les entrées de mappage de la table du groupe de sécurité IP de la base de données de mappage de la table du groupe de sécurité IP gérée dans le chemin de données.

- **show cts pac**

  Affiche les informations sur le fichier PAC importé dans l'ASA à partir de l'ISE et comprend un message d'avertissement lorsque le fichier PAC a expiré ou se trouve dans les 30 jours de son expiration.

Historique de Cisco TrustSec

Tableau 4 : Historique de Cisco TrustSec

Nom de la caractéristique	Versions de plateforme	Description
TrustSec de Cisco	9.0(1)	Cisco TrustSec fournit un contrôle d'accès qui s'appuie sur une infrastructure existante de prise en compte de l'identité pour assurer la confidentialité des données entre les périphériques réseau et intégrer les services d'accès de sécurité sur une seule plateforme. Dans la fonctionnalité Cisco TrustSec, les appareils d'application utilisent une combinaison d'attributs d'utilisateur et d'attributs de terminal pour prendre des décisions de contrôle d'accès basées sur les rôles et l'identité. Dans cette version, l'ASA s'intègre à Cisco TrustSec pour fournir une application des politiques basées sur des groupes de sécurité. Les politiques d'accès au sein du domaine Cisco TrustSec sont indépendantes de la topologie, en fonction des rôles des périphériques source et de destination plutôt que des adresses IP du réseau. L'ASA peut utiliser Cisco TrustSec pour d'autres types de politiques basées sur des groupes de sécurité, telles que l'inspection des applications; par exemple, vous pouvez configurer une carte de trafic qui comprend une politique d'accès basée sur un groupe de sécurité. Nous avons introduit ou modifié les commandes suivantes : **access-list extended**, **cts sxp enable**, **cts server-group**, **cts sxp default**, **cts sxp retry period**, **cts sxp reconciliation period**, **cts sxp connection peer**, **cts import-pac**, **cts refresh environment-data**, **object-group security**, **security-group**, **show running-config cts**, **show running-config object-group**, **clear configure cts**, **clear configure object-group**, **show cts pac**, **show cts environment-data**, **show cts environment-data sg-table**, **show cts sxp connections**, **show object-group**, **show configure security-group**, **clear cts environment-data**, **debug cts,** et **packet-tracer**.
Imposition de balises de groupe de sécurité de couche 2	9.3(1)	Vous pouvez désormais utiliser le balisage de groupe de sécurité combiné au balisage Ethernet pour appliquer les politiques. SGT plus Ethernet Tagging, également appelé Layer 2 SGT Imposition, permet à l'ASA d'envoyer et de recevoir des balises de groupe de sécurité sur les interfaces Ethernet à l'aide du cadrage Ethernet propriétaire de Cisco (EtherType 0x8909), qui permet l'insertion de balises de groupe de sécurité source dans des trames Ethernet en texte clair. Nous avons introduit ou modifié les commandes suivantes : **cts manual**, **policy static sgt**, **propagate sgt**, **cts role-based sgt-map**, **show cts sgt-map**, **packet-tracer**, **capture**, **show capture**, **show asp drop**, **show asp table classify**, **show running-config all**, **clear configure all** et **write memory**.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge par Cisco Trustsec du protocole SXP (Security Exchange Protocol) version 3.	9.6(1)	Cisco Trustsec sur l'ASA implémente désormais SXPv3, qui permet des liaisons SGT-sous-réseau, plus efficaces que les liaisons hôte. Nous avons introduit ou modifié les commandes suivantes : **cts sxp mapping network-map**, **cts role-based sgt-map**, **show cts sgt-map**, **show cts sxp sgt-map**, **show asp table cts sgt-map**.
Temporisateur de retenue de suppression configurable de la connexion Trustsec SXP	9.8(3)	Le temporisateur de retenue de la connexion SXP par défaut est de 120 secondes. Vous pouvez maintenant configurer ce temporisateur, entre 120 et 64 000 secondes. Commandes nouvelles/modifiées : **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections**

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.