Exemple de configuration d'un cloud TrustSec avec 802.1x MACsec sur un commutateur de la gamme Catalyst 3750X

Table des matières

Introduction

Cet article décrit les étapes requises pour configurer un nuage Cisco TrustSec (CTS) avec chiffrement de liaison entre deux commutateurs de la gamme Catalyst 3750X (3750X).

Cet article explique le processus de chiffrement MACsec (Media Access Control Security) de commutateur à commutateur qui utilise le protocole SAP (Security Association Protocol). Ce processus utilise le mode IEEE 802.1x au lieu du mode manuel.

Voici une liste des étapes impliquées :

- Mise en service des PAC (Protected Access Credential) pour les périphériques d'amorçage et non d'amorçage
- Authentification NDAC (Network Device Admission Control) et négociation MACsec avec SAP pour la gestion des clés
- Actualisation de l'environnement et des politiques

- Authentification de port pour les clients
- Étiquetage du trafic avec l'étiquette de groupe de sécurité (SGT)
- Application des stratégies avec la liste de contrôle d'accès du groupe de sécurité (SGACL)

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base des composants CTS
- Connaissances de base de la configuration CLI des commutateurs Catalyst
- Expérience de la configuration ISE (Identity Services Engine)

Composants utilisés

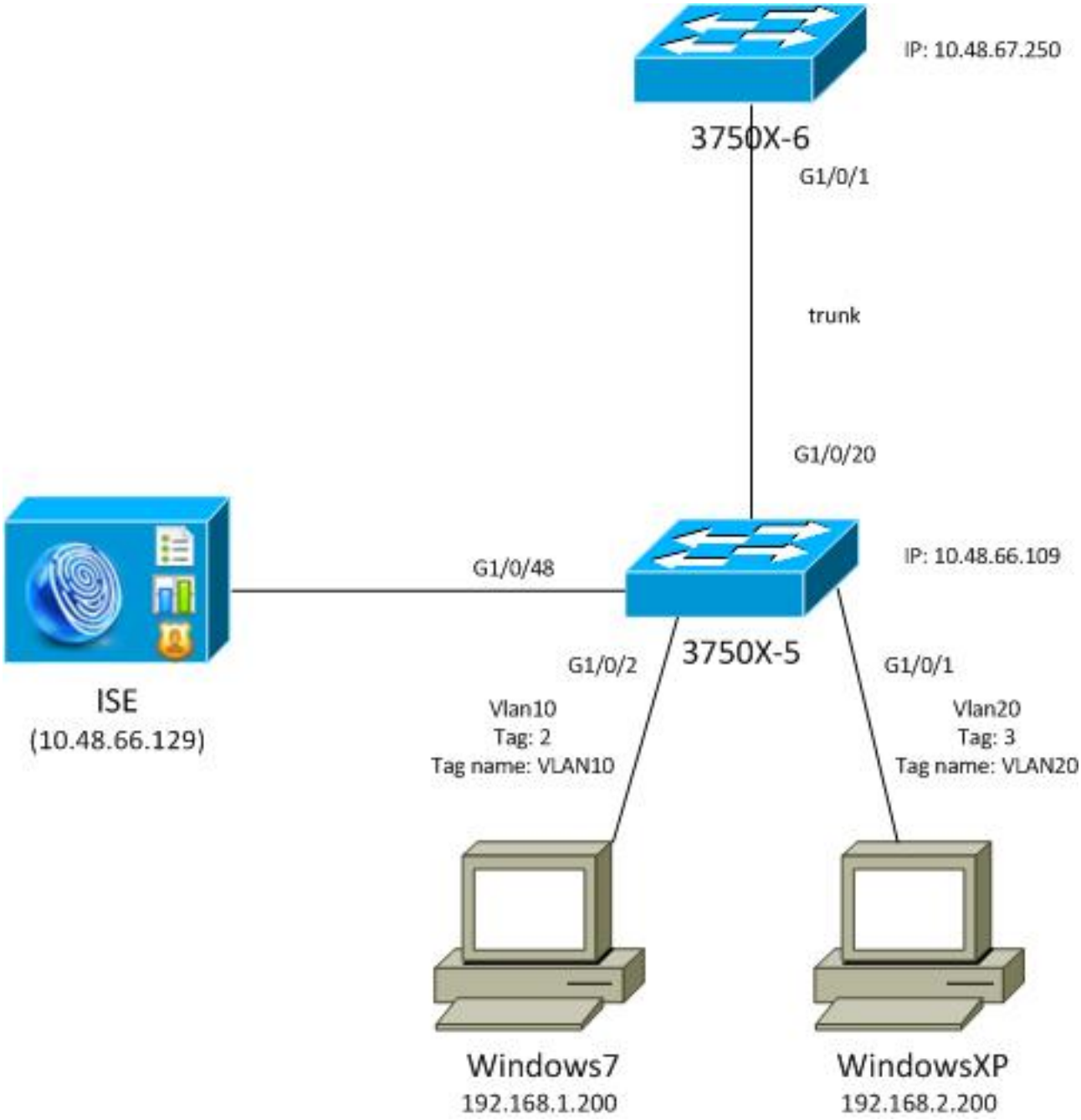
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft (MS) Windows 7 et MS Windows XP
- Logiciel 3750X, versions 15.0 et ultérieures
- Logiciel ISE, versions 1.1.4 et ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Diagramme du réseau



Dans ce schéma de topologie de réseau, le commutateur 3750X-5 est le périphérique d'amorçage qui connaît l'adresse IP de l'ISE et télécharge automatiquement le PAC utilisé pour l'authentification ultérieure dans le cloud CTS. Le périphérique d'amorçage agit comme un authentificateur 802.1x pour les périphériques non d'amorçage. Le commutateur de la gamme Cisco Catalyst 3750X-6 (3750X-6) n'est pas le périphérique d'amorçage. Il agit en tant que demandeur 802.1x pour le périphérique d'amorçage. Une fois que le périphérique non amorce s'est authentifié auprès de l'ISE via le périphérique amorce, il est autorisé à accéder au cloud CTS. Après une authentification réussie, l'état du port 802.1x sur le commutateur 3750X-5 est changé en **authentifié**, et le cryptage MACsec est négocié. Le trafic entre les commutateurs est alors étiqueté avec SGT et chiffré.

Cette liste récapitule le flux de trafic attendu :

- Le seed 3750X-5 se connecte à l'ISE et télécharge le PAC, qui est ensuite utilisé pour l'actualisation de l'environnement et des politiques.
- Le modèle 3750X-6 non amorce effectue une authentification 802.1x avec le rôle demandeur afin d'authentifier/autoriser et télécharger le PAC à partir de l'ISE.

- Le 3750X-6 exécute une deuxième session 802.1x Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST) afin de s'authentifier avec le tunnel protégé basé sur le PAC.
- Le 3750X-5 télécharge les politiques SGA pour lui-même et pour le compte du 3750X-6.
- Une session SAP se produit entre les modèles 3750X-5 et 3750X-6, les chiffrements MACsec sont négociés et la stratégie est échangée.
- Le trafic entre les commutateurs est étiqueté et chiffré.

Configuration des commutateurs d'amorçage et non d'amorçage

Le périphérique d'amorçage (3750X-5) est configuré afin d'utiliser l'ISE comme serveur RADIUS pour CTS :

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

cts authorization list ise

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

L'application des listes de contrôle d'accès basées sur les rôles (RBACL) et des listes de contrôle d'accès basées sur les groupes de sécurité (SGACL) est activée (elles sont utilisées ultérieurement) :

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

Le périphérique non amorce (3750X-6) est configuré uniquement pour l'authentification, l'autorisation et la comptabilité (AAA) sans nécessiter d'autorisation RADIUS ou CTS :

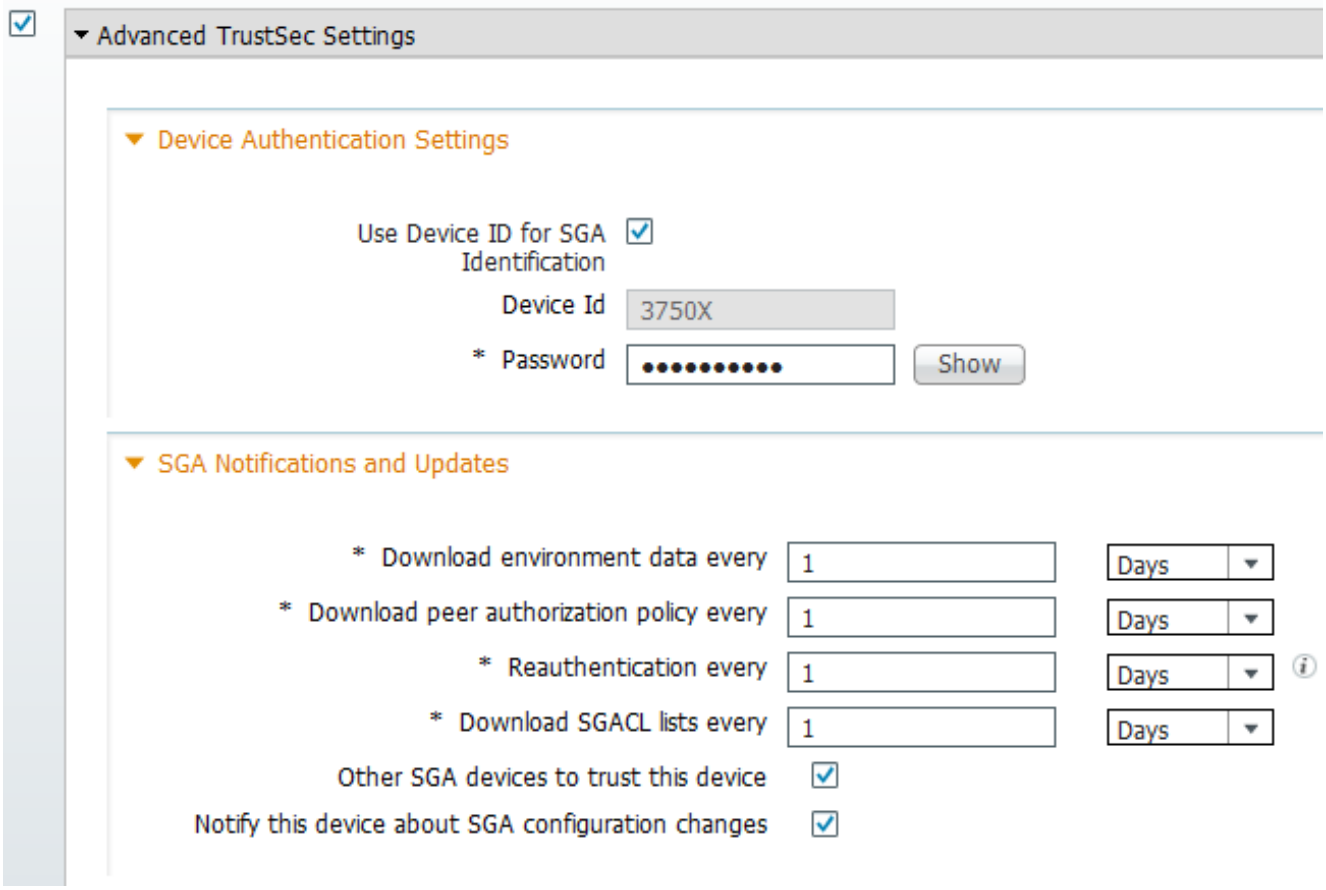
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Avant d'activer 802.1x sur l'interface, il est nécessaire de configurer l'ISE.

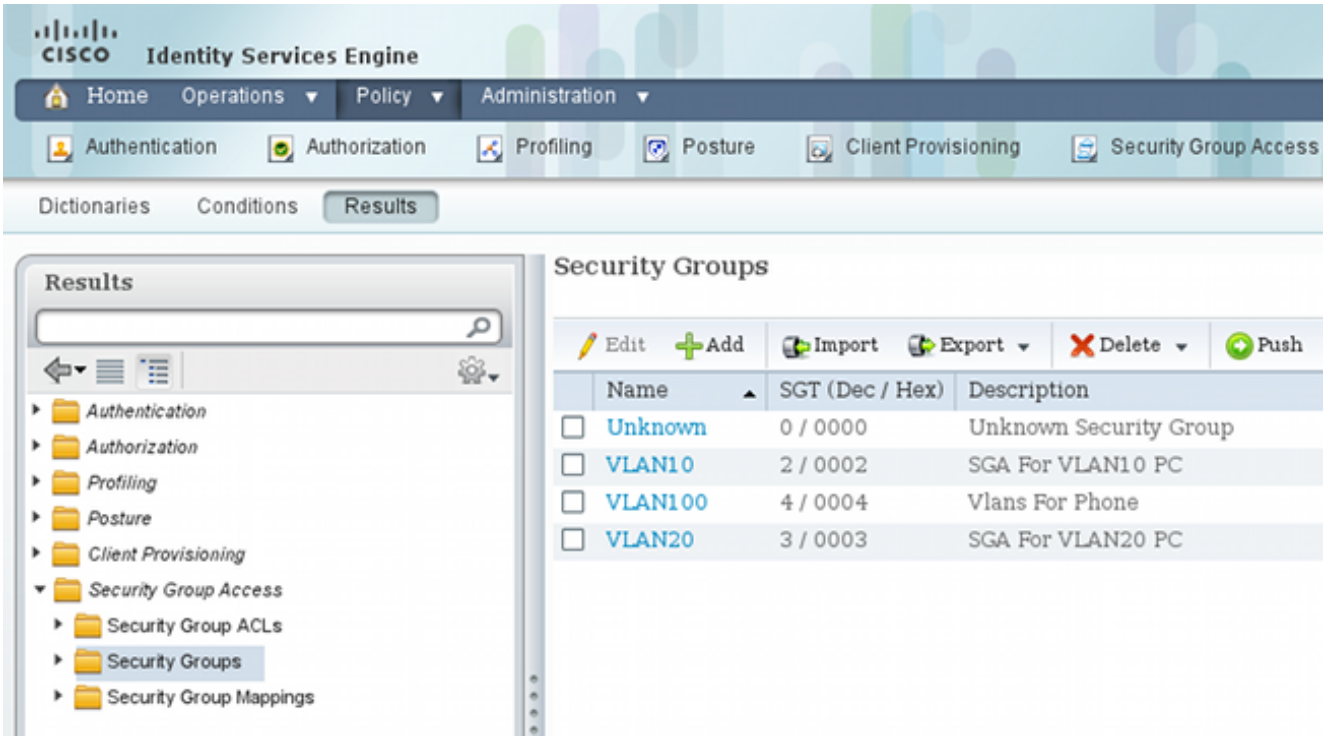
Configuration de l'ISE

Complétez ces étapes afin de configurer l'ISE :

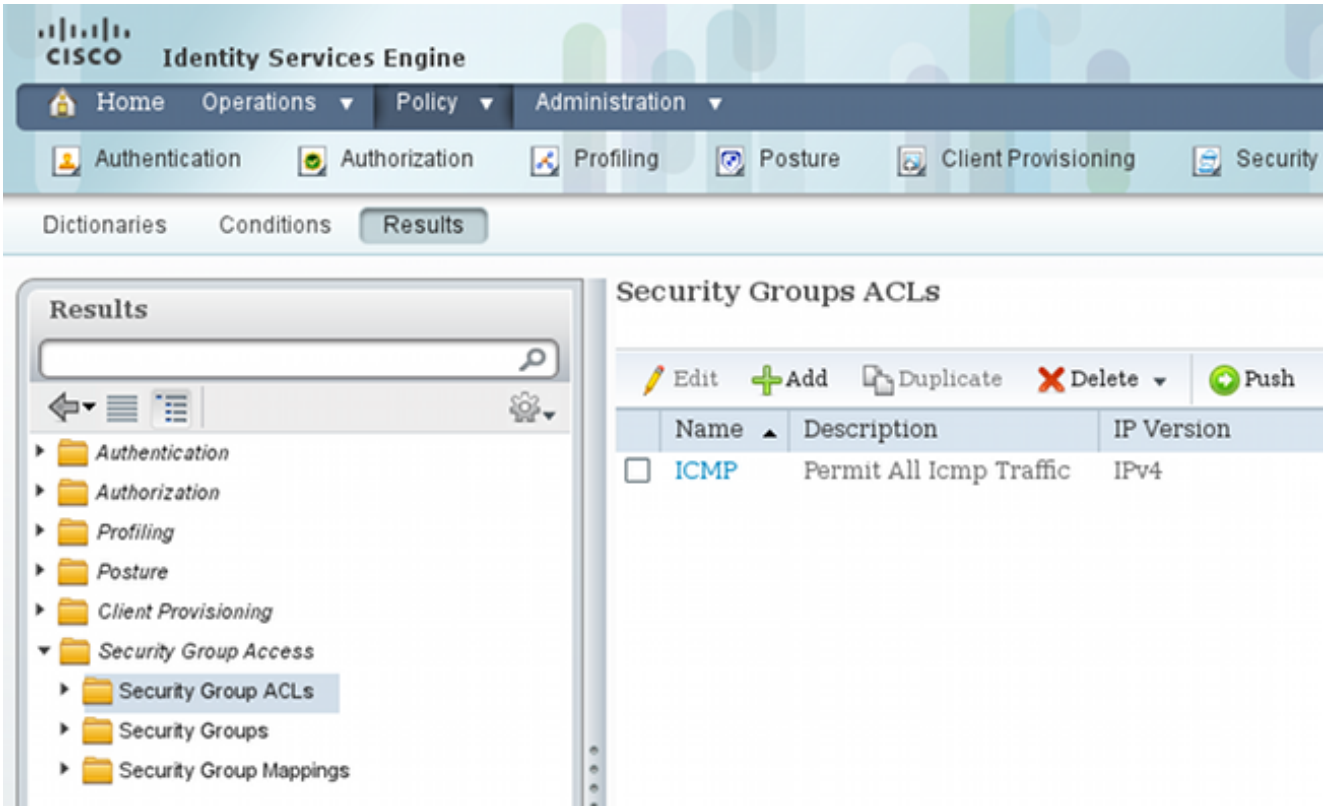
1. Accédez à **Administration > Network Resources > Network Devices**, et ajoutez les deux commutateurs en tant que Network Access Devices (NAD). Sous **Advanced TrustSec Settings**, configurez un mot de passe CTS pour une utilisation ultérieure sur l'interface de ligne de commande du commutateur.



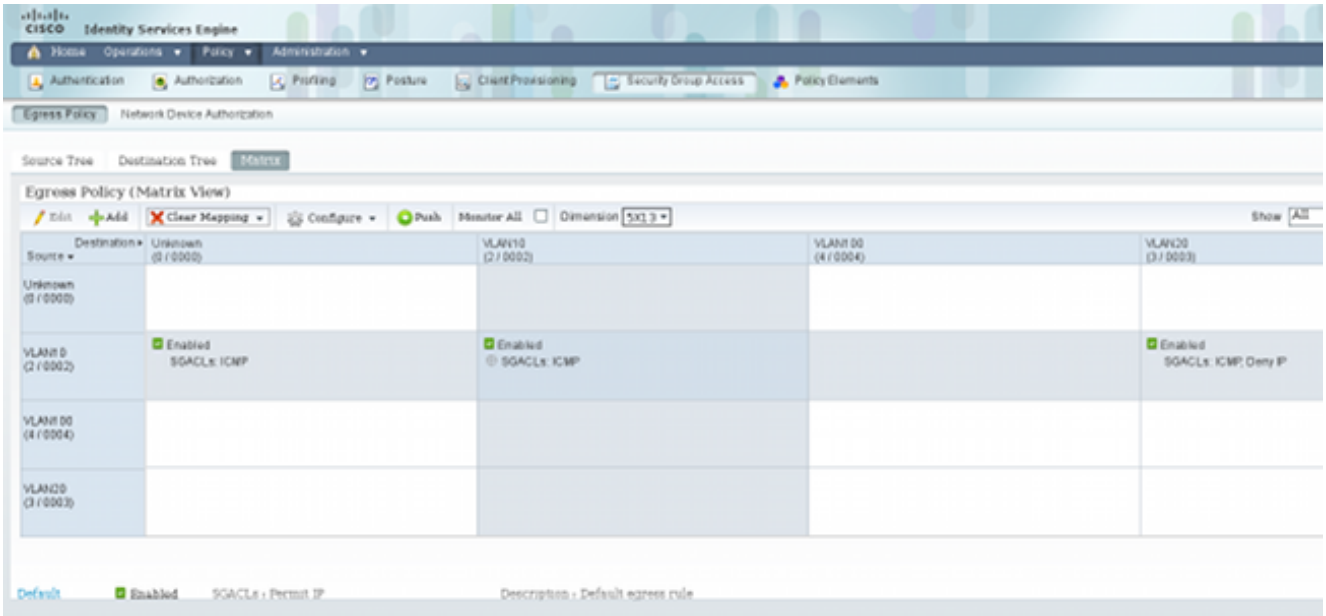
2. Accédez à **Policy > Policy Elements > Results > Security Group Access > Security Groups**, et ajoutez les SGT appropriées. Ces balises sont téléchargées lorsque les commutateurs demandent une actualisation de l'environnement.



3. Accédez à **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**, et configurez une SGACL.



4. Accédez à **Policy > Security Group Access**, et définissez une stratégie avec la matrice.



Remarque : vous devez configurer la stratégie d'autorisation pour le demandeur MS Windows, afin qu'il reçoive la balise correcte. Référez-vous à Exemple de configuration et guide de dépannage de TrustSec des commutateurs ASA et Catalyst 3750X pour une configuration détaillée pour ceci.

Approvisionnement PAC pour le 3750X-5

PAC est nécessaire pour l'authentification dans le domaine CTS (comme phase1 pour EAP-FAST), et il est également utilisé afin d'obtenir des données d'environnement et de politique à

partir de l'ISE. Sans le PAC correct, il n'est pas possible d'obtenir ces données de l'ISE.

Une fois que vous avez fourni les informations d'identification correctes sur le 3750X-5, il télécharge le PAC :

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

Le PAC est téléchargé via EAP-FAST avec le protocole MSCHAPv2 (Challenge Handshake Authentication Protocol) de Microsoft, avec les informations d'identification fournies dans la CLI et les mêmes informations d'identification configurées sur l'ISE.

Le PAC est utilisé pour l'actualisation de l'environnement et des politiques. Pour ces commutateurs, utilisez des requêtes RADIUS avec **cisco av-pair cts-pac-opaque**, qui est dérivé de la clé PAC et peut être décrypté sur l'ISE.

Provisionnement PAC pour l'authentification 3750X-6 et NDAC

Pour qu'un nouveau périphérique puisse se connecter au domaine CTS, il est nécessaire d'activer 802.1x sur les ports correspondants.

Le protocole SAP est utilisé pour la gestion des clés et la négociation de la suite de chiffrement. Galois Message Authentication Code (GMAC) est utilisé pour l'authentification et Galois/Counter Mode (GCM) pour le cryptage.

Sur le commutateur d'amorçage :

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

Sur le commutateur non amorce :

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

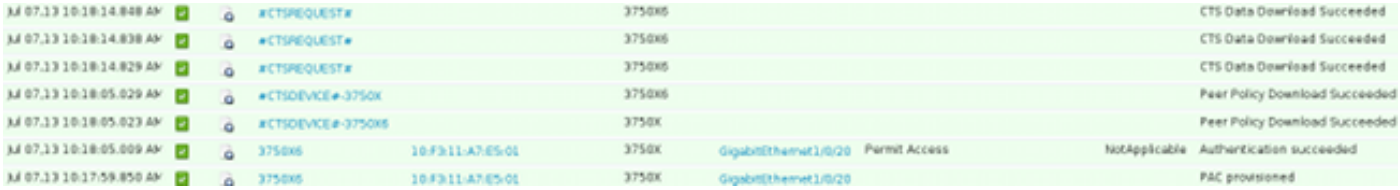
Ceci est pris en charge uniquement sur les ports trunk (commutateur-commutateur MACsec). Pour le commutateur-hôte MACsec, qui utilise le protocole MACsec Key Agreement (MKA) à la place de SAP, référez-vous à Configuration du chiffrement MACsec.

Immédiatement après avoir activé 802.1x sur les ports, le commutateur non-amorce agit comme demandeur du commutateur amorce, qui est l'authentificateur.

Ce processus est appelé NDAC et son objectif est de connecter un nouveau périphérique au domaine CTS. L'authentification est bidirectionnelle ; le nouveau périphérique possède des informations d'identification qui sont vérifiées sur le serveur d'authentification ISE. Après le provisionnement PAC, le périphérique est également sûr qu'il se connecte au domaine CTS.

> **Remarque** : le protocole PAC est utilisé afin de construire un tunnel TLS (Transport Layer Security) pour EAP-FAST. Le 3750X-6 approuve les informations d'identification PAC fournies par le serveur de la même manière qu'un client approuve le certificat fourni par le serveur pour le tunnel TLS pour la méthode EAP-TLS.

Plusieurs messages RADIUS sont échangés :



La première session du 3750X (commutateur d'amorçage) est utilisée pour le provisionnement PAC. EAP-FAST est utilisé sans PAC (un tunnel anonyme pour l'authentification MSCHAPv2 est construit).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

Le nom d'utilisateur et le mot de passe MSCHAPv2 configurés via la commande **cts credentials** sont utilisés. En outre, un message RADIUS Access-Reject est renvoyé à la fin, car une fois que le PAC a déjà été configuré, aucune authentification supplémentaire n'est nécessaire.

La deuxième entrée du journal fait référence à l'authentification 802.1x. EAP-FAST est utilisé avec le PAC qui a été provisionné précédemment.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

Cette fois, le tunnel n'est pas anonyme, mais protégé par PAC. Là encore, les mêmes informations d'identification pour la session MSCHAPv2 sont utilisées. Ensuite, il est vérifié par rapport aux règles d'authentification et d'autorisation sur l'ISE, et un ACCEPTATION D'ACCÈS RADIUS est renvoyé. Ensuite, le commutateur d'authentification applique les attributs renvoyés et la session 802.1x pour ce port passe à un état autorisé.

Àquoi ressemble le processus pour les deux premières sessions 802.1x à partir du commutateur d'amorçage ?

Voici les débogages les plus importants de la graine. La valeur de départ détecte que le port est actif et tente de déterminer quel rôle doit être utilisé pour 802.1x - le demandeur ou l'authentificateur :

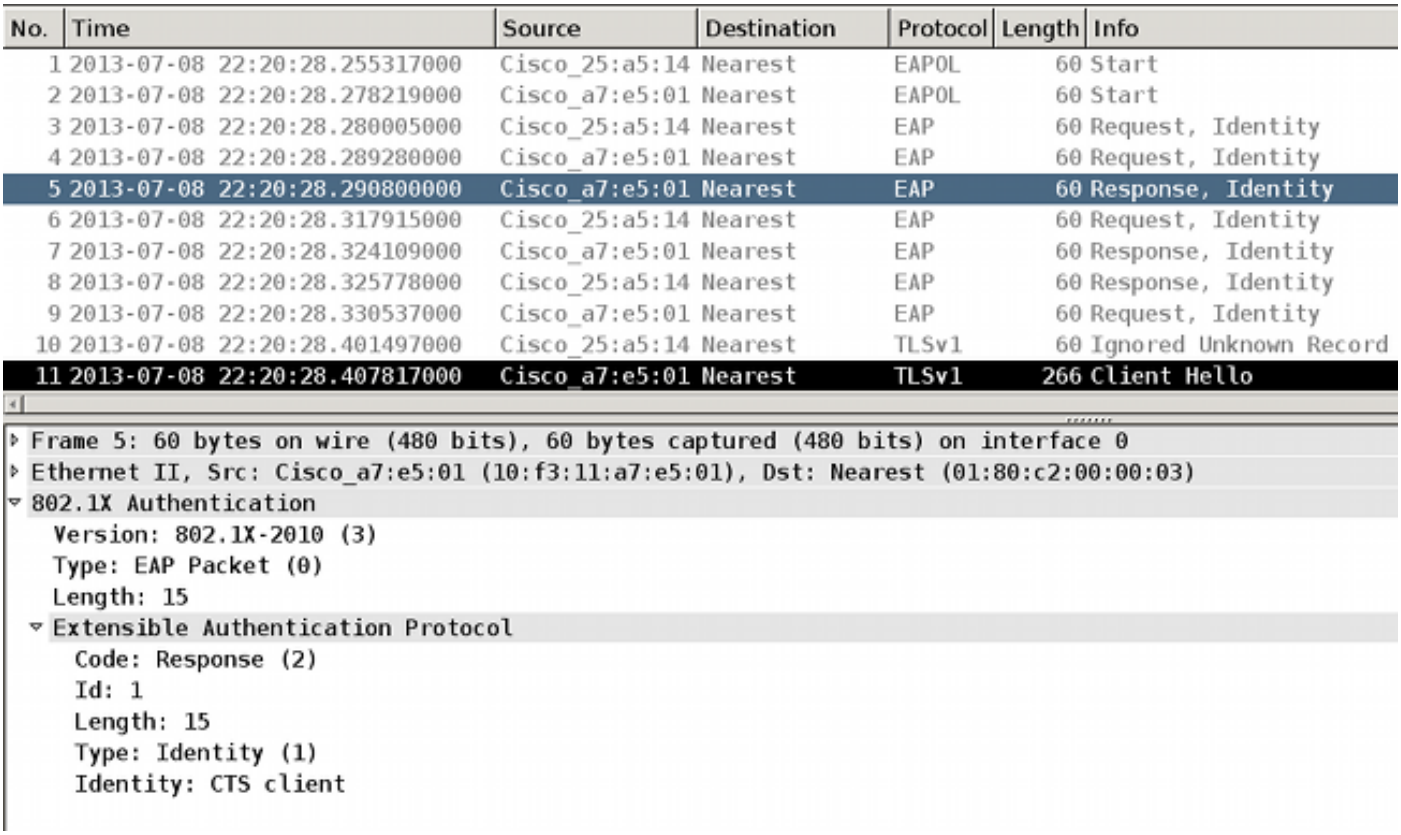
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

Enfin, le rôle d'authentificateur est utilisé, car le commutateur a accès à l'ISE. Sur le modèle 3750X-6, le rôle demandeur est choisi.

Détails sur la sélection du rôle 802.1x

> **Remarque** : une fois que le commutateur demandeur a obtenu le PAC et qu'il est authentifié 802.1x, il télécharge les données d'environnement (décrites plus loin) et apprend l'adresse IP du serveur AAA. Dans cet exemple, les deux commutateurs disposent d'une connexion dédiée (backbone) pour ISE. Plus tard, les rôles peuvent être différents ; le premier commutateur qui reçoit une réponse du serveur AAA devient l'authentificateur et le second devient le demandeur.

Cela est possible parce que les deux commutateurs avec le serveur AAA marqué comme ALIVE envoient une identité de requête EAP (Extensible Authentication Protocol). Celui qui reçoit en premier la réponse d'identité EAP devient l'authentificateur et abandonne les demandes d'identité suivantes.



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

Une fois le rôle 802.1x sélectionné (dans ce scénario, le 3750X-6 est le demandeur, car il n'a pas encore accès au serveur AAA), les paquets suivants impliquent l'échange EAP-FAST pour la mise en service PAC. Le **client CTS** du nom d'utilisateur est utilisé pour le nom d'utilisateur de la requête RADIUS et comme identité EAP :

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

Une fois le tunnel EAP-FAST anonyme créé, une session MSCHAPv2 se produit pour le nom d'utilisateur **3750X6** (**informations d'identification cts**). Il est impossible de le voir sur le commutateur, car il s'agit d'un tunnel TLS (chiffré), mais des journaux détaillés sur l'ISE pour le provisionnement PAC le prouvent. Vous pouvez voir le **client CTS** pour le nom d'utilisateur RADIUS et comme réponse d'identité EAP. Cependant, pour la méthode interne (MSCHAP), le nom d'utilisateur **3750X6** est utilisé :

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

La deuxième authentification EAP-FAST a lieu. Cette fois, il utilise le PAC qui a été provisionné précédemment. Là encore, le **client CTS** est utilisé comme nom d'utilisateur RADIUS et identité externe, mais **3750X6** est utilisé pour l'identité interne (MSCHAP). Authentification réussie :

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Cependant, cette fois, l'ISE renvoie plusieurs attributs dans le paquet RADIUS Accept :

Authentication Result

```
User-Name=3750X6
State=ReauthSession:C0A800010000053A33FD79AF
Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
Session-Timeout=86400
Termination-Action=RADIUS-Request
EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
cisco-av-pair=cts:security-group-tag=0000-01
cisco-av-pair=cts:supplicant-cts-capabilities=sap
MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

Ici, le commutateur d'authentification fait passer le port à l'état autorisé :

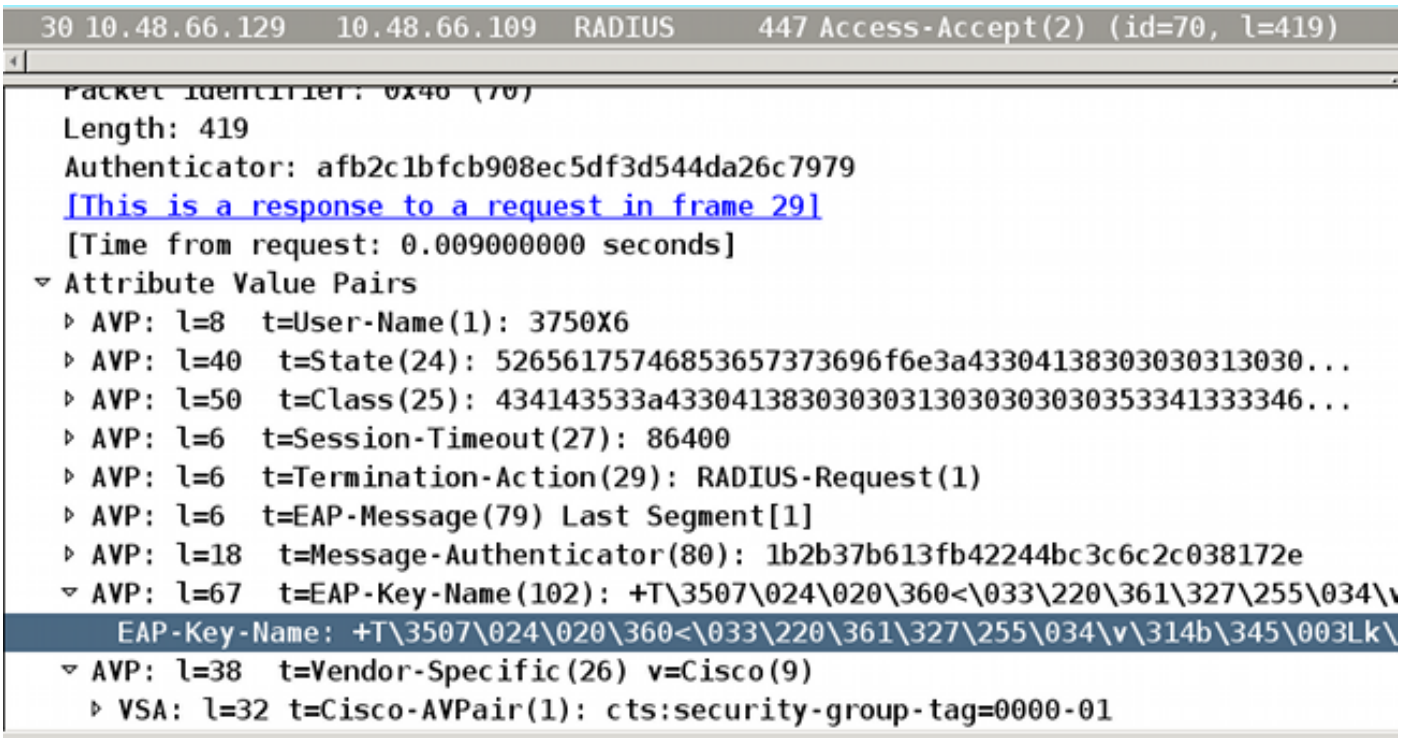
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

Comment le commutateur d'authentification apprend-il que le nom d'utilisateur est **3750X6** ? Pour le nom d'utilisateur RADIUS et l'identité EAP externe, le **client CTS** est utilisé, et l'identité interne

est chiffrée et non visible pour l'authentificateur. Le nom d'utilisateur est appris par l'ISE. Le dernier paquet RADIUS (Access-Accept) contient **username=3750X6**, tandis que tous les autres contenaient **username = Cts client**. C'est pourquoi le demandeur reconnaît le nom d'utilisateur réel. Ce comportement est conforme aux RFC. Dans la section 3.0 du document RFC3579 :

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

Dans le dernier paquet de la session d'authentification 802.1x, l'ISE retourne un message d'acceptation RADIUS **cisco-av-pair** avec le **EAP-Key-Name** :

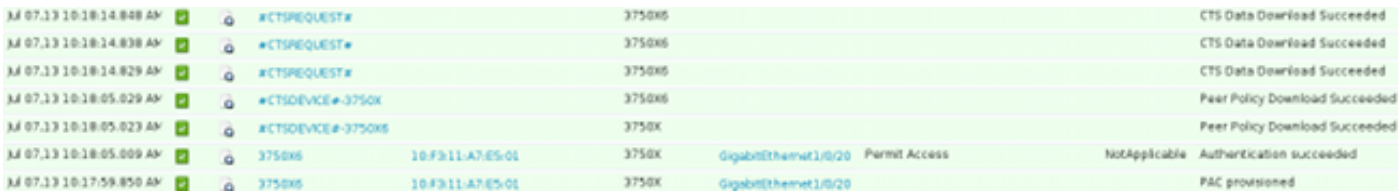


Il s'agit d'un élément clé de la négociation SAP.

En outre, le SGT est passé. Cela signifie que le commutateur d'authentification étiquette le trafic provenant du demandeur avec une **valeur par défaut = 0**. Vous pouvez configurer une valeur spécifique sur l'ISE pour renvoyer toute autre valeur. Ceci s'applique uniquement au trafic non étiqueté ; le trafic étiqueté n'est pas réécrit car, par défaut, le commutateur d'authentificateur approuve le trafic provenant du demandeur authentifié (mais cela peut également être modifié sur l'ISE).

Téléchargement de la stratégie SGA

Il existe des échanges RADIUS supplémentaires (sans EAP) autres que les deux premières sessions EAP-FAST 802.1x (la première pour l'approvisionnement PAC et la seconde pour l'authentification). Voici à nouveau les journaux ISE :



Le troisième journal (**Peer Policy Download**) indique un échange RADIUS simple : RADIUS Request and RADIUS Accept pour l'utilisateur **3760X6**. Cela est nécessaire afin de télécharger les politiques pour le trafic du demandeur. Les deux attributs les plus importants sont :

```
▽ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

Pour cette raison, le commutateur d'authentificateur approuve le trafic étiqueté SGT par le demandeur (**cts : trusted-device=true**) et étiquette également le trafic non étiqueté avec **tag=0**.

Le quatrième journal indique le même échange RADIUS. Cependant, cette fois, c'est pour l'utilisateur **3750X5** (authentificateur). En effet, les deux homologues doivent avoir une stratégie l'un pour l'autre. Il est intéressant de noter que le demandeur ne connaît toujours pas l'adresse IP du serveur AAA. C'est pourquoi le commutateur d'authentification télécharge la stratégie pour le compte du demandeur. Ces informations sont transmises ultérieurement au demandeur (avec l'adresse IP ISE) lors de la négociation SAP.

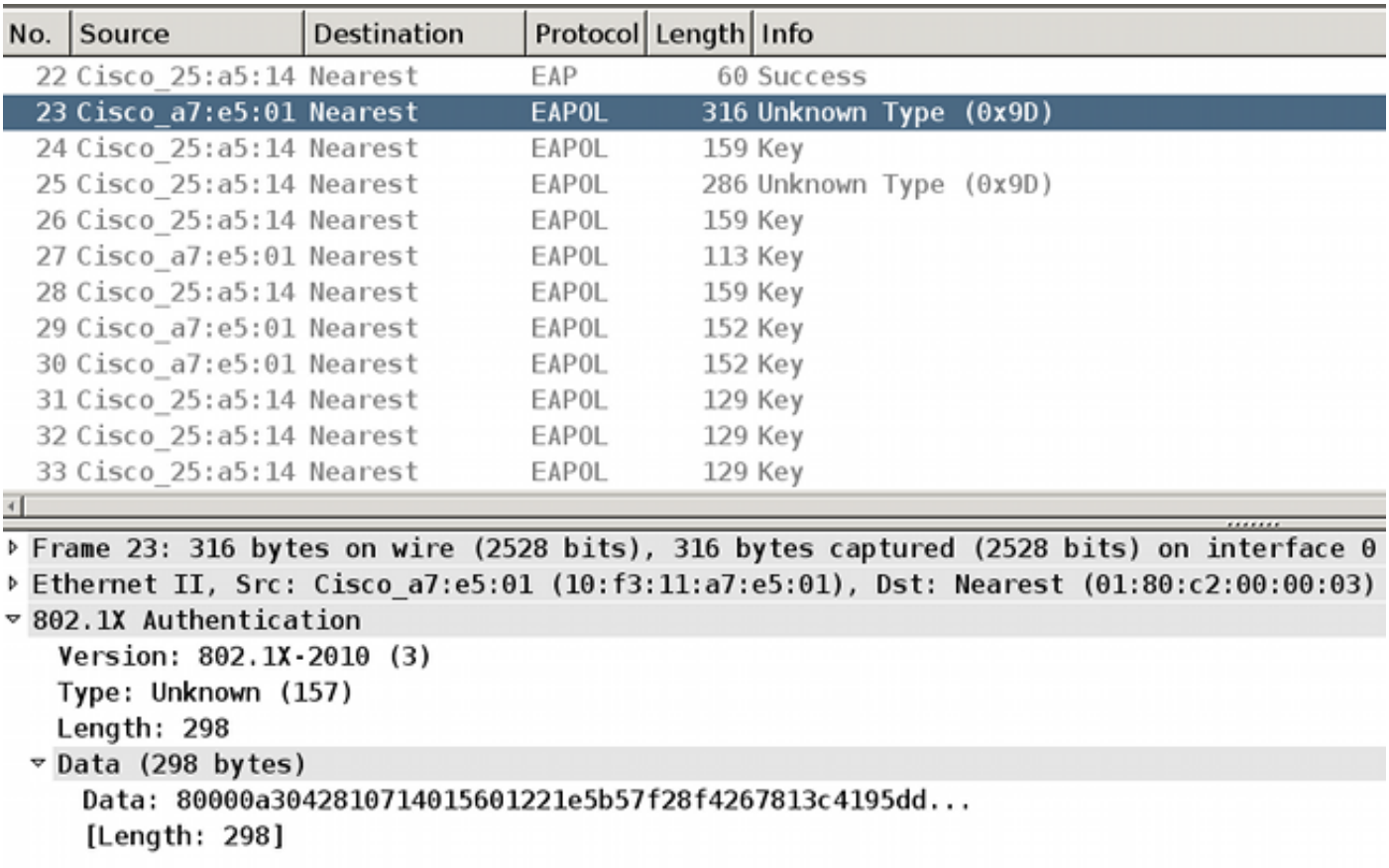
Négociation SAP

Immédiatement après la fin de la session d'authentification 802.1x, la négociation SAP a lieu. Cette négociation est nécessaire afin de :

- Négocier les niveaux de chiffrement (avec la commande **sap mode-list gcm-encrypt**) et les suites de chiffrement
- Dériver des clés de session pour le trafic de données
- Faire l'objet d'une nouvelle saisie
- Effectuez des vérifications de sécurité supplémentaires et assurez-vous que les étapes précédentes sont sécurisées

SAP est un protocole conçu par Cisco Systems sur la base d'une version préliminaire de 802.11i/D6.0. Pour plus d'informations, demandez l'accès à la page Cisco TrustSec Security Association Protocol - protocole prenant en charge Cisco Trusted Security pour Cisco Nexus 7000.

L'échange SAP est conforme à la norme 802.1AE. Un échange de clés EAPOL (Extensible Authentication Protocol over LAN) a lieu entre le demandeur et l'authentificateur afin de négocier une suite de chiffrement, d'échanger des paramètres de sécurité et de gérer des clés. Malheureusement, Wireshark ne dispose pas de décodeur pour tous les types EAP requis :



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

La réussite de ces tâches entraîne la création d'une association de sécurité (SA).

Sur le commutateur demandeur :

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
       authc success:              12
```

```
       authc reject:              1556
       authc failure:             0
       authc no response:         0
       authc logoff:              0
       sap success:               12
       sap fail:                  0
       authz success:             12
       authz fail:                0
       port auth fail:            0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

Sur l'authentificateur :

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
       Peer ID               : unknown
```

```
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Ici, les ports utilisent le mode **gcm-encrypt**, ce qui signifie que le trafic est à la fois authentifié et chiffré, ainsi que correctement étiqueté SGT. Aucun périphérique n'utilise de stratégie d'autorisation de périphérique réseau spécifique sur l'ISE, ce qui signifie que tout le trafic initié à partir du périphérique utilise l'étiquette par défaut **0**. En outre, les deux commutateurs approuvent les balises SGT reçues de l'homologue (en raison des attributs RADIUS de la phase de téléchargement de la stratégie homologue).

Actualisation de l'environnement et des politiques

Une fois les deux périphériques connectés au cloud CTS, une actualisation de l'environnement et des politiques est lancée. L'actualisation de l'environnement est nécessaire afin d'obtenir les SGT et les noms, et une actualisation des politiques est nécessaire afin de télécharger la SGACL définie sur l'ISE.

Àce stade, le demandeur connaît déjà l'adresse IP du serveur AAA, de sorte qu'il peut le faire lui-même.

Référez-vous à Exemple de configuration et guide de dépannage de TrustSec des commutateurs ASA et Catalyst 3750X pour plus de détails sur l'actualisation de l'environnement et des politiques.

Le demandeur se souvient de l'adresse IP du serveur RADIUS, même si aucun serveur RADIUS n'est configuré et que la liaison CTS est interrompue (vers le commutateur d'authentification). Cependant, il est possible de forcer le commutateur à l'oublier :

```
bsns-3750-6#show run | i radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

```
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
radius-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

Afin de vérifier l'environnement et la politique sur le commutateur demandeur, entrez ces commandes :

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

```
bsns-3750-6#show cts role-based permissions
```

Pourquoi aucune stratégie ne s'affiche-t-elle ? Aucune stratégie ne s'affiche, car vous devez activer l'**application cts** pour les appliquer :

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

Pourquoi le demandeur n'a-t-il qu'une seule stratégie pour **grouper les éléments inconnus** alors que l'authentificateur en a plusieurs ?

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Authentification de port pour les clients

Le client MS Windows est connecté et authentifié au port **g1/0/1** du commutateur 3750-5 :

```
bsns-3750-5#show authentication sessions int g1/0/1
       Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

Ici, le commutateur 3750-5 sait que le trafic de cet hôte doit être étiqueté avec **SGT=3** lorsqu'il est envoyé au cloud CTS.

Étiquetage du trafic avec le SGT

Comment détectez-vous et vérifiez-vous le trafic ?

C'est difficile parce que :

- La capture de paquets intégrée est prise en charge uniquement pour le trafic IP (et il s'agit d'une trame Ethernet modifiée avec des balises SGT et des données utiles MACsec).
- Port SPAN (Switched Port Analyzer) avec le mot clé **replication** - cela peut fonctionner, mais le problème est que tout PC avec Wireshark connecté au port de destination d'une session de surveillance abandonne les trames en raison du manque de prise en charge de 802.1ae, ce qui peut se produire au niveau matériel.
- Le port SPAN sans le mot-clé **replication** supprime l'en-tête **cts** avant de le placer sur un port de destination.

Application des politiques avec la SGACL

L'application des politiques dans le cloud CTS est toujours effectuée au niveau du port de destination. En effet, seul le dernier périphérique connaît le SGT de destination du périphérique d'extrémité qui est connecté directement à ce commutateur. Le paquet transporte uniquement le SGT source. Les balises de groupe source et de destination sont requises pour prendre une décision.

C'est pourquoi les périphériques n'ont pas besoin de télécharger toutes les stratégies depuis ISE. Au lieu de cela, ils n'ont besoin que de la partie de la politique qui est liée à la SGT pour laquelle le périphérique a des périphériques connectés directement.

Voici le 3750-6, qui est le commutateur demandeur :

```
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
```

Il y a deux politiques ici. La première est la valeur par défaut pour le trafic non étiqueté (vers/depuis). La seconde est de **SGT=2** à la SGT non étiquetée, qui est **0**. Cette stratégie existe car le périphérique lui-même utilise la stratégie SGA de l'ISE et appartient à **SGT=0**. En outre, **SGT=0** est une balise par défaut. Par conséquent, vous devez télécharger toutes les stratégies qui ont les règles pour le trafic **vers/depuis SGT=0**. Si vous regardez la matrice, vous ne voyez qu'une seule de ces politiques : **de 2 à 0**.

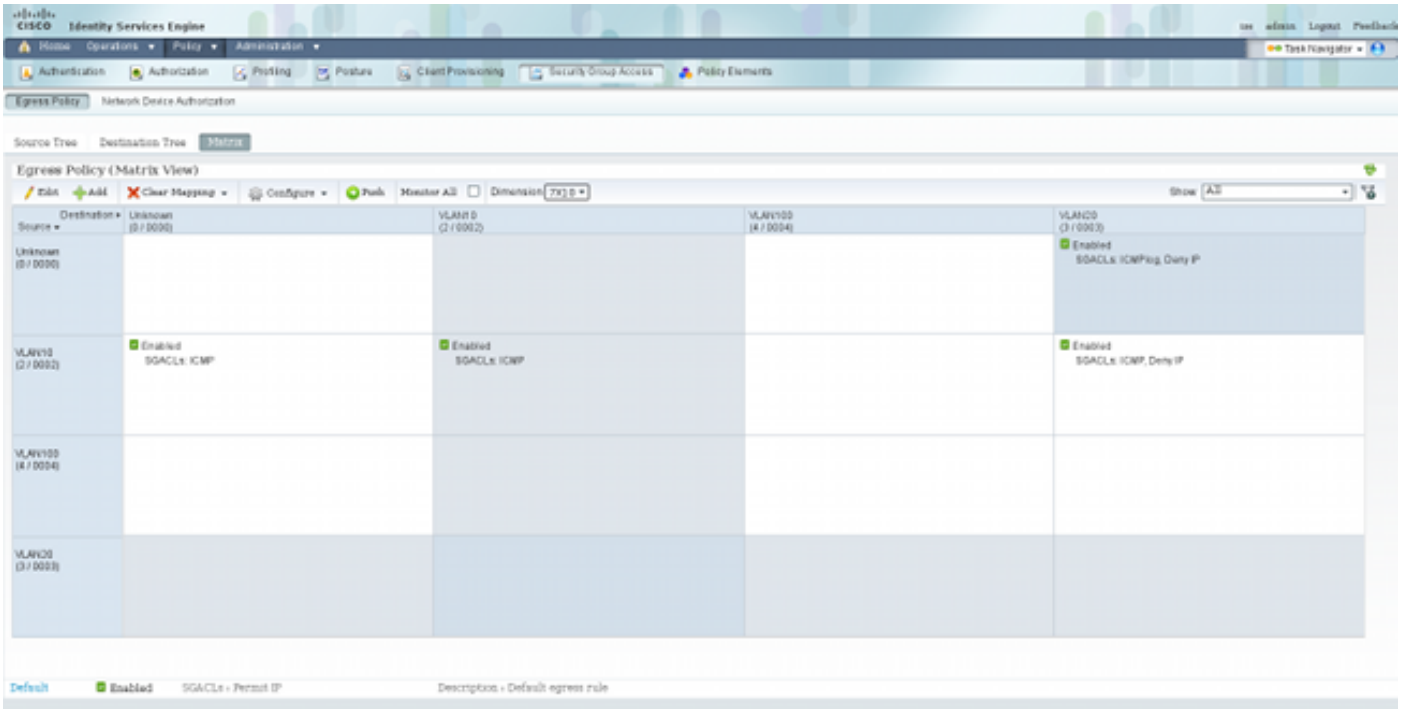
Voici le 3750-5, qui est le commutateur d'authentification :

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Il y a une autre politique ici : **de 2 à 3**. En effet, le client 802.1x (MS Windows) est connecté à **g1/0/1** et étiqueté avec **SGT=3**. C'est pourquoi vous devez télécharger toutes les stratégies **vers SGT=3**.

Essayez d'envoyer une requête ping de 3750X-6 (**SGT=0**) vers MS Windows XP (**SGT=3**). Le 3750X-5 est le périphérique d'application.

Avant cela, vous devez configurer une stratégie sur l'ISE pour le trafic de **SGT=0 à SGT=3**. Cet exemple a créé un journal ICMP (Internet Control Message Protocol) SGACL avec seulement la ligne **permit icmp log**, et l'a utilisé dans la matrice pour le trafic de **SGT=0 à SGT=3** :



Voici une actualisation de la stratégie sur le commutateur d'application et une vérification de la nouvelle stratégie :

```
bsns-3750-5#cts refresh policy
Policy refresh in progress

bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Afin de vérifier que la liste de contrôle d'accès (ACL) est téléchargée à partir de l'ISE, entrez cette commande :

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

Afin de vérifier que la liste de contrôle d'accès est appliquée (prise en charge matérielle), entrez cette commande :

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name   = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale  = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

Voici les compteurs avant ICMP :

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

Voici une requête ping de **SGT=0** (commutateur 3750-6) vers MS Windows XP (**SGT=3**) et les compteurs :

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

Voici les compteurs de la liste de contrôle d’accès :

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
    10 permit icmp log (5 matches)
```

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration Cisco TrustSec pour 3750
- Guide de configuration de Cisco TrustSec pour ASA 9.1
- Déploiement et feuille de route de Cisco TrustSec
- Technical Support & Documentation - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.