Exemple de configuration de l’ASA et du commutateur Catalyst de la série 3750X TrustSec et guide de dépannage

Table des matières

Introduction

Cet article décrit comment configurer Cisco TrustSec (CTS) sur le dispositif de sécurité adaptatif sécurisé Cisco (ASA) et sur un commutateur Cisco Catalyst 3750X (3750X).

Afin d'apprendre le mappage entre les balises de groupe de sécurité (SGT) et les adresses IP,

l'ASA utilise le protocole SXP (SGT Exchange Protocol). Ensuite, des listes de contrôle d'accès (ACL) basées sur SGT sont utilisées afin de filtrer le trafic. Le commutateur 3750X télécharge les politiques RBACL (Role-Based Access Control List) depuis Cisco Identity Services Engine (ISE) et filtre le trafic en fonction de ces politiques. Cet article détaille le niveau des paquets afin de décrire le fonctionnement de la communication et les débogages attendus.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Composants CTS
- Configuration CLI d'ASA et de Cisco IOS®

Composants utilisés

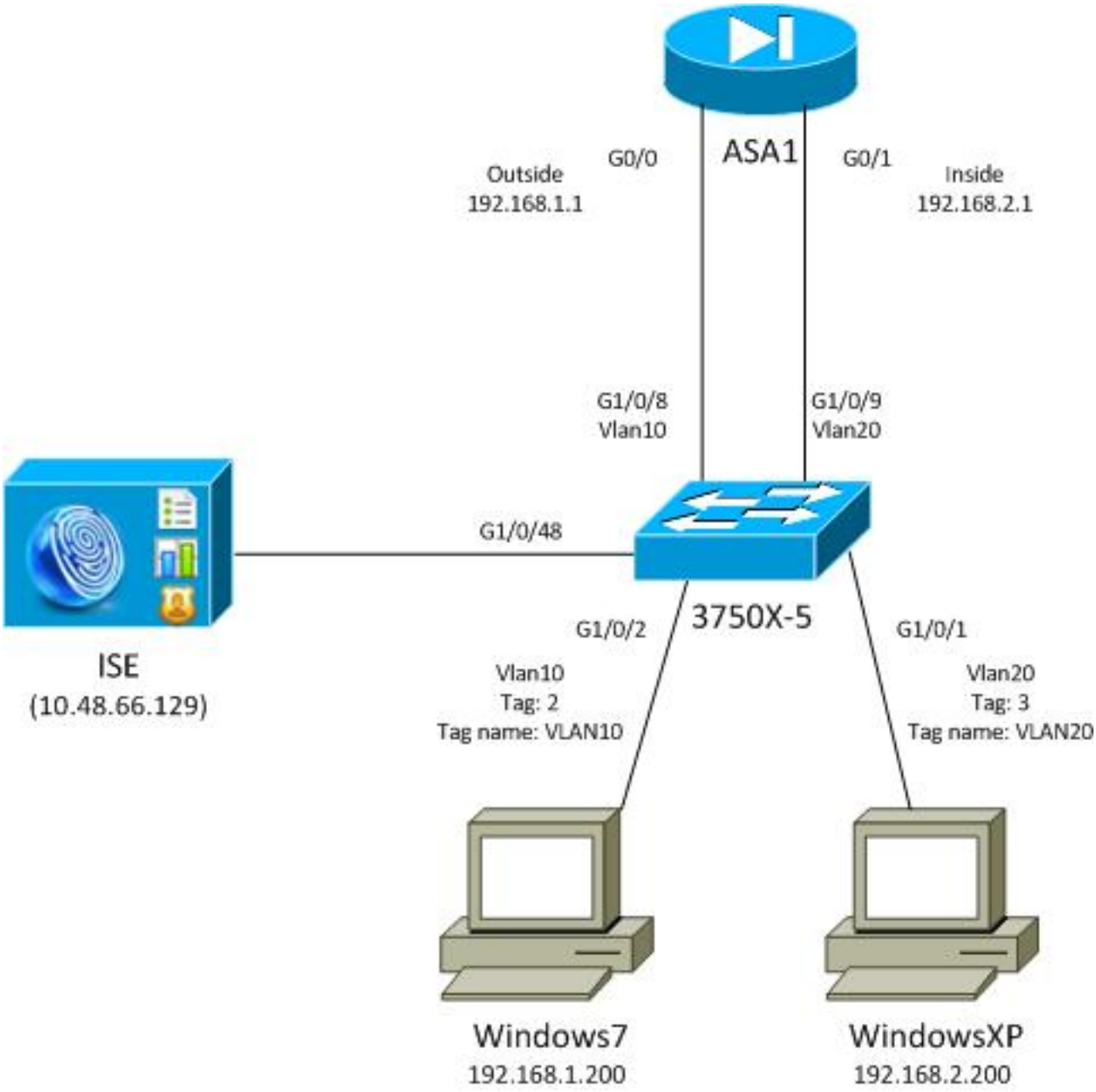
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco ASA, versions 9.1 et ultérieures
- Microsoft (MS) Windows 7 et MS Windows XP
- Logiciel Cisco 3750X, versions 15.0 et ultérieures
- Logiciel Cisco 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



Flux de trafic

Voici le flux de trafic :

- Le 3750X est configuré sur **G1/0/1** et **G1/0/2** pour l'authentification de port.
- ISE est utilisé comme serveur AAA (Authentication, Authorization, and Accounting).
- Le contournement d'adresse MAC (MAB) est utilisé pour l'authentification pour MS Windows 7.
- IEEE 802.1x est utilisé pour MS Windows XP afin de démontrer qu'il n'a pas d'importance quelle méthode d'authentification est utilisée.

Une fois l'authentification réussie, l'ISE renvoie le SGT et le commutateur 3750X lie cette balise à la session d'authentification. Le commutateur apprend également les adresses IP des deux stations avec la commande **ip device tracking**. Le commutateur utilise ensuite SXP afin d'envoyer la table de mappage entre le SGT et l'adresse IP à l'ASA. Les deux PC MS Windows ont un routage par défaut qui pointe vers l'ASA.

Une fois que l'ASA reçoit le trafic de l'adresse IP qui est mappée au SGT, il peut utiliser la liste de

contrôle d'accès basée sur le SGT. En outre, lorsque vous utilisez 3750X comme routeur (passerelle par défaut pour les deux stations MS Windows), il est en mesure de filtrer le trafic en fonction des stratégies téléchargées à partir de l'ISE.

Voici les étapes de configuration et de vérification, chacune étant détaillée dans sa propre section plus loin dans le document :

- Authentification de port avec la commande **ip device tracking** sur le 3750X
- Configuration ISE pour les stratégies d'authentification, SGT et SGACL (Security Group Access Control List)
- Configuration CTS sur l'ASA et le 3750X
- Mise en service PAC (Protected Access Credential) sur le 3750X (automatique) et l'ASA (manuel)
- Actualisation de l'environnement sur ASA et le 3750X
- Vérification et application de l'authentification des ports sur le 3750X
- Actualisation de la stratégie sur le 3750X
- Échange SXP (ASA en tant qu'écouteur et 3750X en tant que haut-parleur)
- Filtrage du trafic sur l'ASA avec ACL SGT
- Filtrage du trafic sur le commutateur 3750X avec des stratégies téléchargées à partir de l'ISE

Configurations

Authentification de port avec la commande *ip device tracking* sur le 3750X

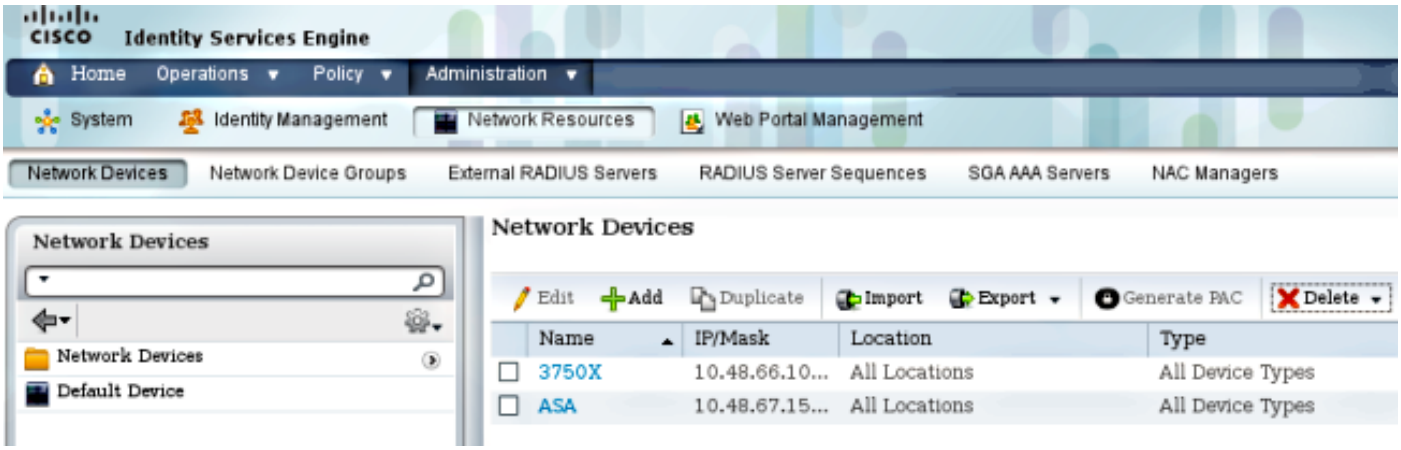
Il s'agit de la configuration type pour 802.1x ou MAB. Le changement d'autorisation RADIUS n'est nécessaire que si vous utilisez la notification active de l'ISE.

```
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

!Radius COA
aaa server radius dynamic-author
 client 10.48.66.129 server-key cisco
 server-key cisco

ip device tracking

interface GigabitEthernet1/0/1
 description windowsxp
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order mab dot1x
```

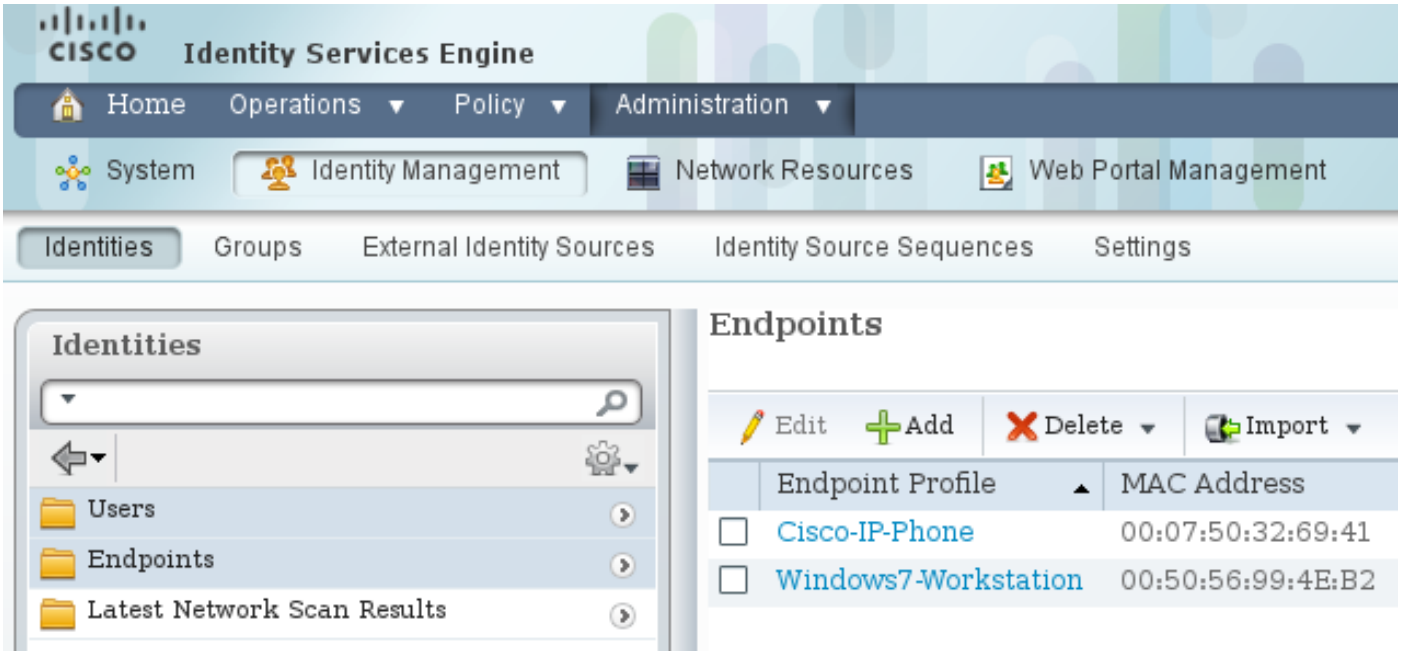
```
 authentication port-control auto
 mab
 dot1x pae authenticator
spanning-tree portfast

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
```

Configuration ISE pour les politiques d'authentification, SGT et SGACL

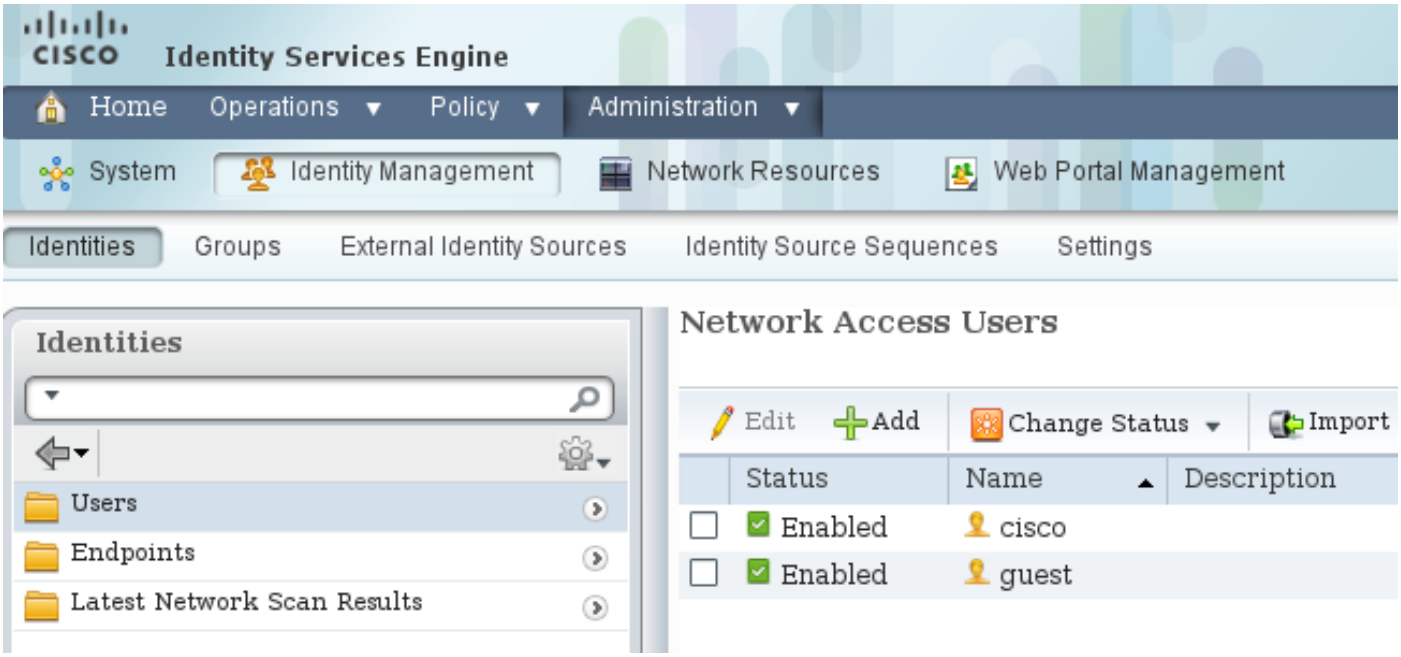
Les deux périphériques réseau de l'ISE doivent être configurés sous **Administration > Network Devices** :



Pour MS Windows 7, qui utilise l'authentification MAB, vous devez créer une identité de point de terminaison (adresse MAC) sous **Administration > Identity Management > Identities > Endpoints** :

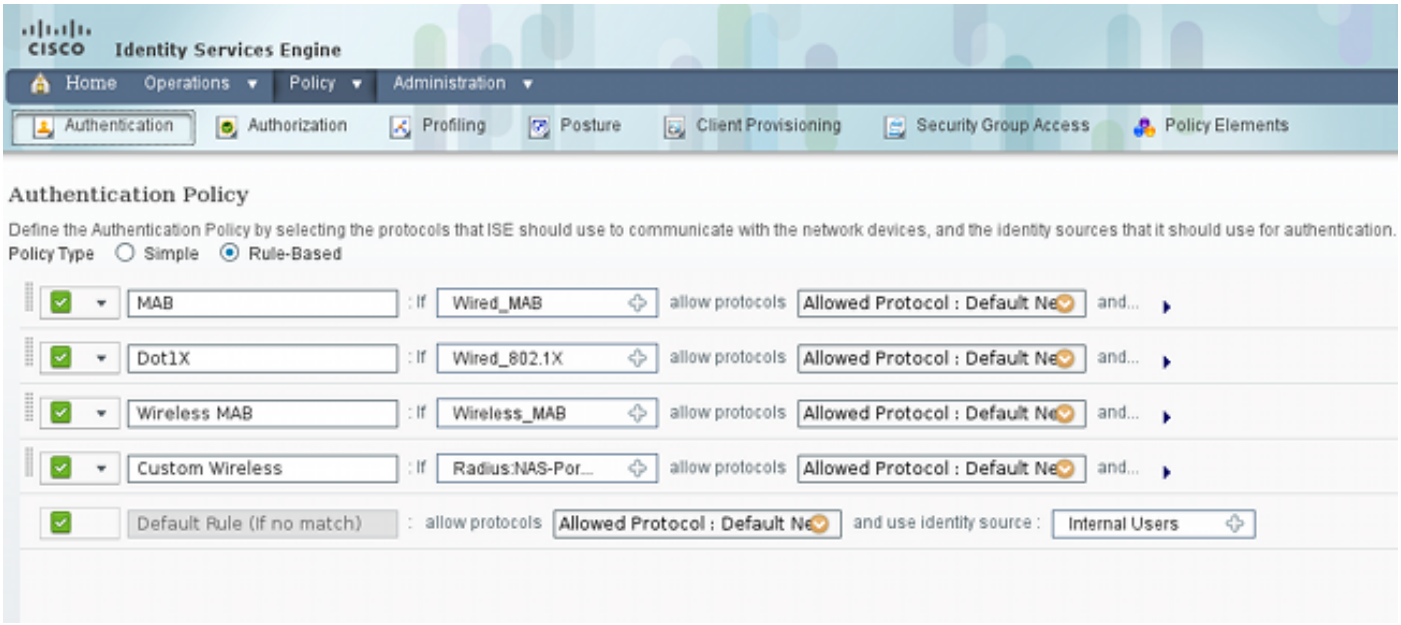


Pour MS Windows XP, qui utilise l'authentification 802.1x, vous devez créer une identité d'utilisateur (nom d'utilisateur) sous **Administration > Identity Management > Identities > Users** :

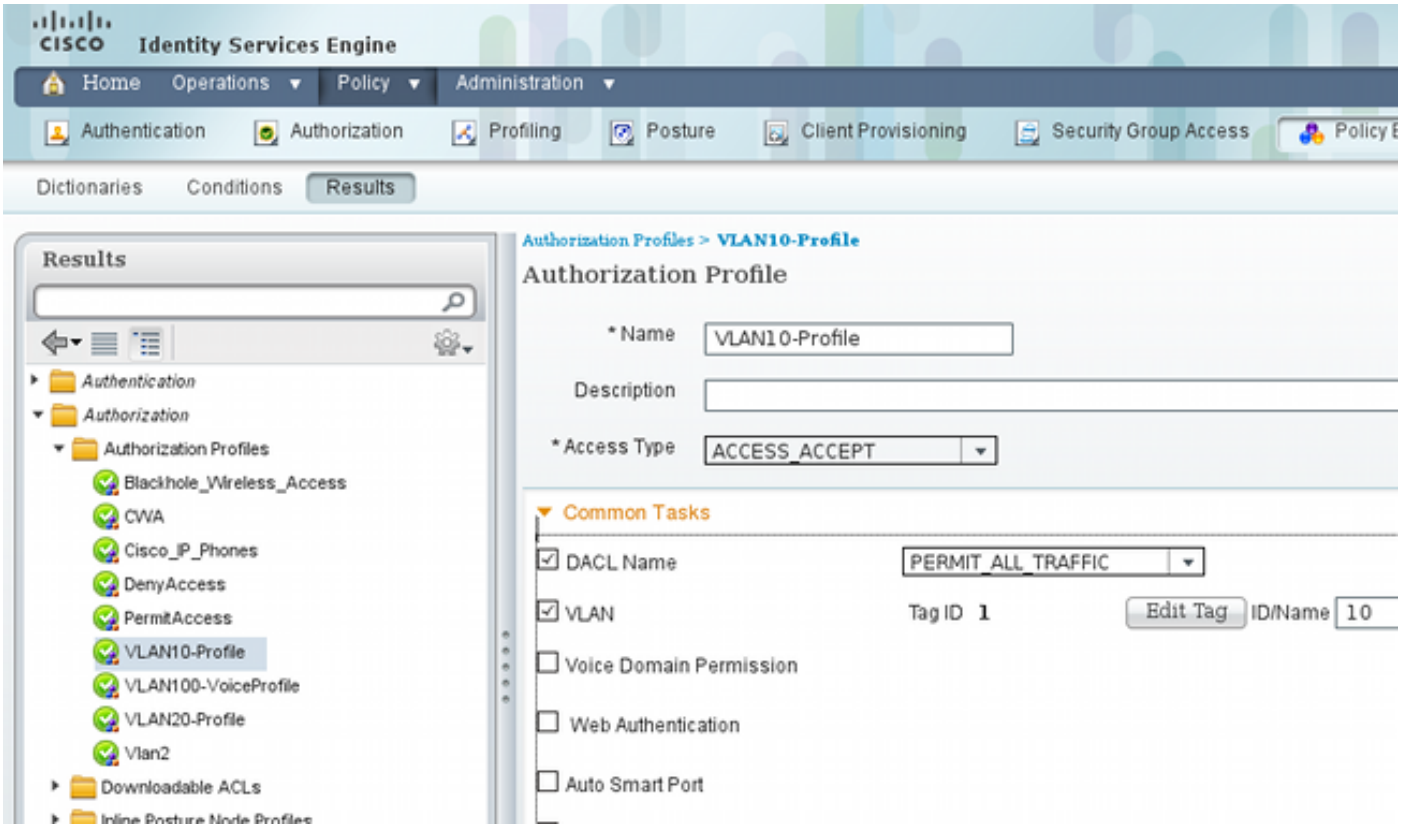


Le nom d'utilisateur **cisco** est utilisé. Configurez MS Windows XP pour le protocole EAP (Extensible Authentication Protocol-Protected EAP) avec ces informations d'identification.

Sur l'ISE, les stratégies d'authentification par défaut sont utilisées (ne modifiez pas cela). La première est la stratégie d'authentification MAB et la seconde est 802.1x :



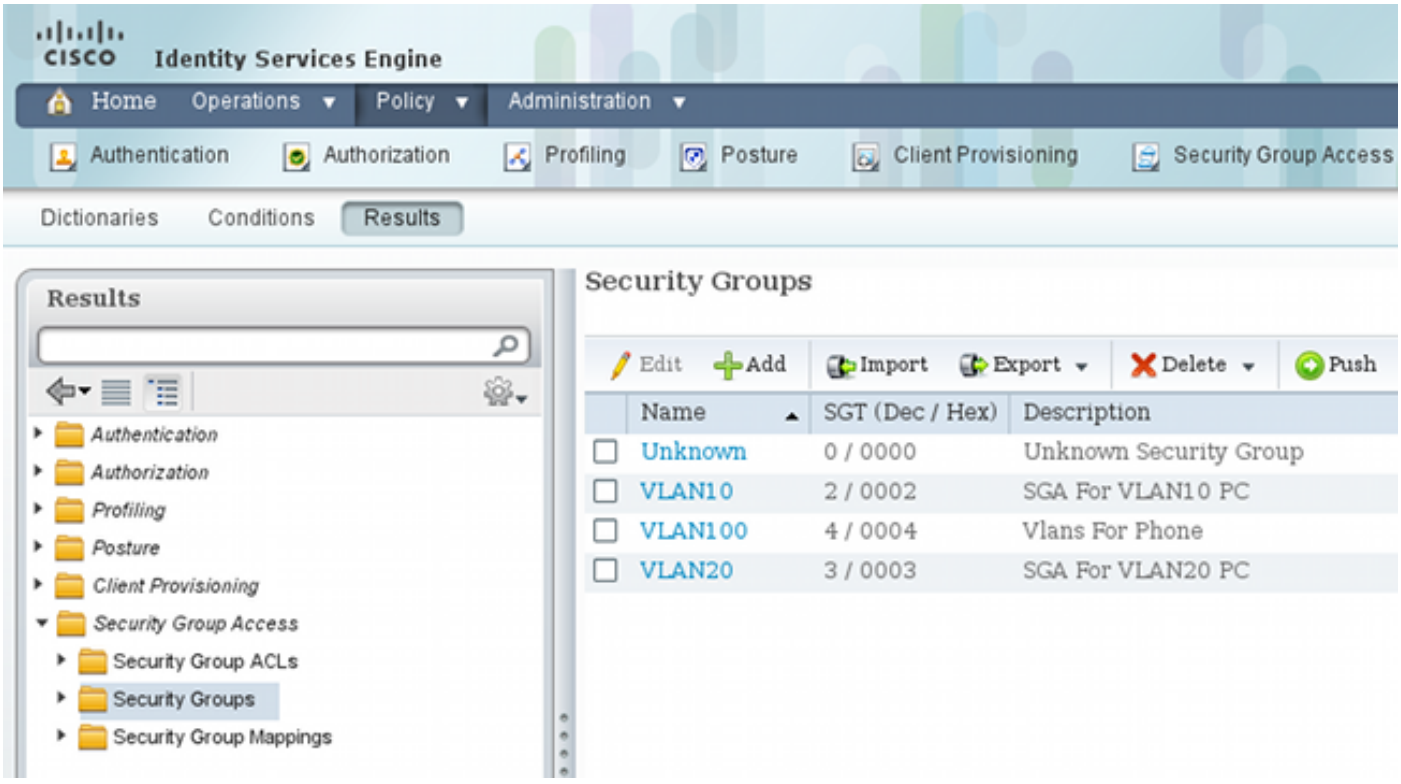
Afin de configurer des stratégies d'autorisation, vous devez définir des profils d'autorisation sous **Stratégie > Résultats > Autorisation > Profils d'autorisation**. Le VLAN10-Profile avec DACL (Downloadable ACL), qui autorise tout le trafic, est utilisé pour le profil MS Windows 7 :



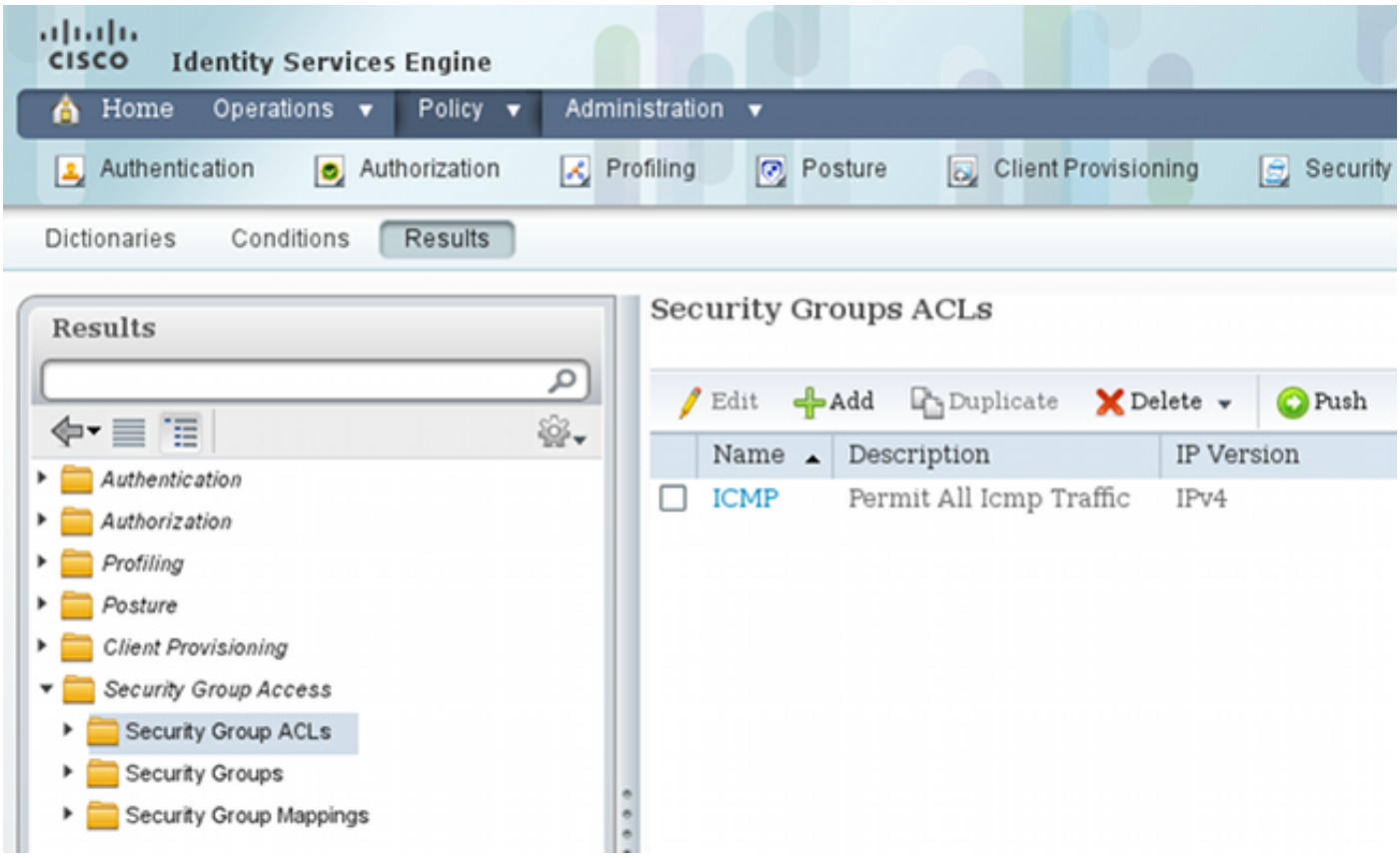
Une configuration similaire, VLAN20-Profile, est utilisée pour MS Windows XP, à l'exception du numéro de VLAN (20).

Afin de configurer les groupes SGT (balises) sur ISE, naviguez vers **Policy > Results > Security Group Access > Security Groups**.

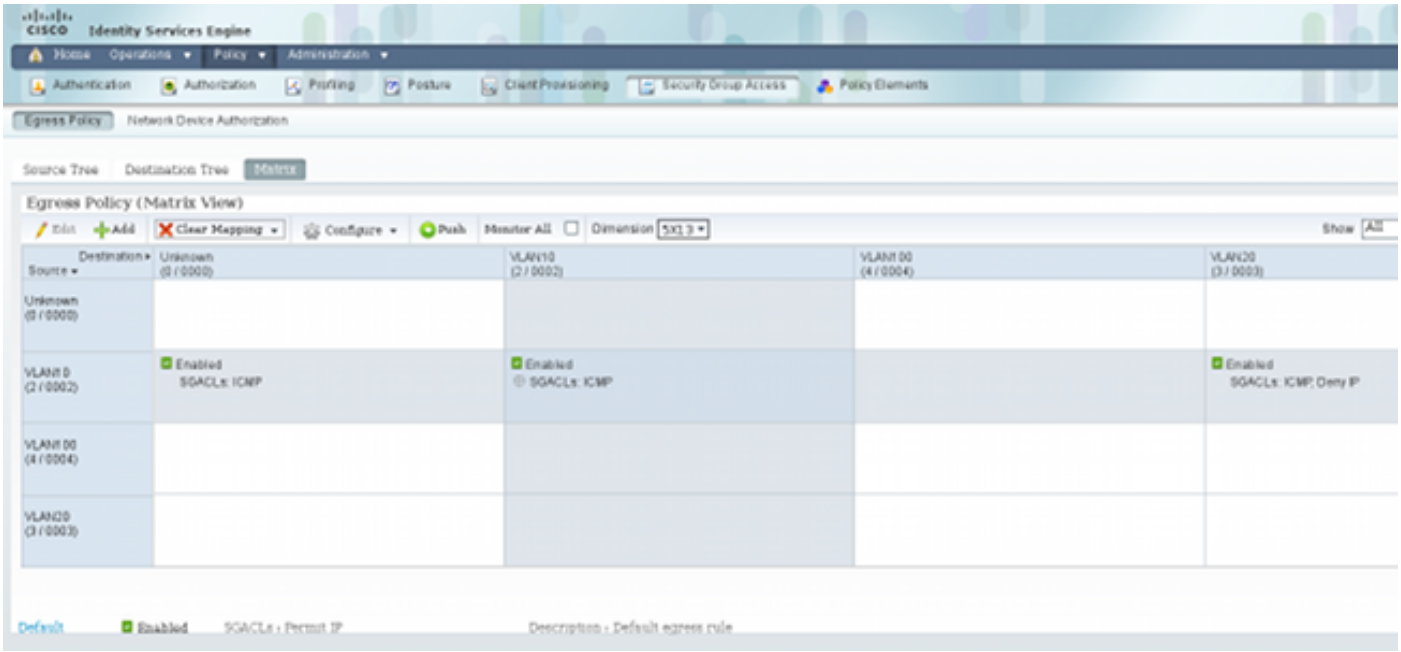
> **Remarque** : il n'est pas possible de choisir un numéro de balise ; il est sélectionné automatiquement par le premier numéro libre sauf 1. Vous ne pouvez configurer que le nom de SGT.



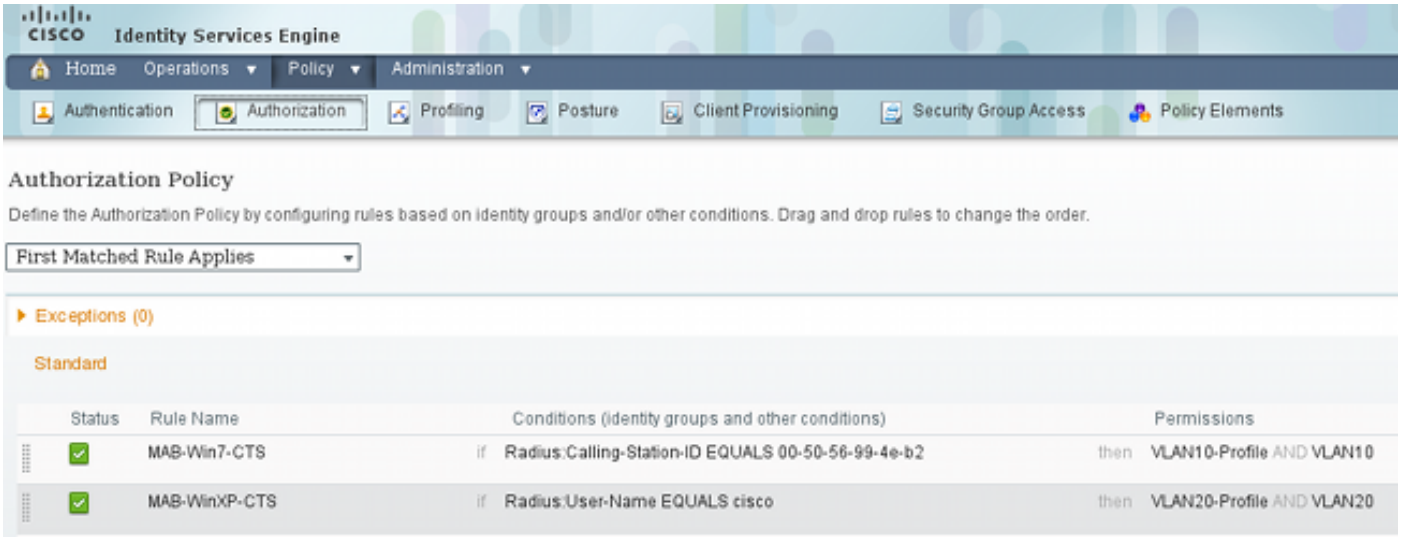
Afin de créer la SGACL pour permettre le trafic ICMP (Internet Control Message Protocol), naviguez vers **Policy > Results > Security Group Access > Security Group ACLs** :



Afin de créer des stratégies, accédez à **Stratégie > Accès au groupe de sécurité > Stratégie de sortie**. Pour le trafic entre VLAN10 et le VLAN inconnu ou VLAN10 ou VLAN20, la liste de contrôle d'accès ICMP est utilisée (**permit icmp**) :



Afin de définir des règles d'autorisation, naviguez à **Policy > Authorization**. Pour MS Windows 7 (adresse MAC spécifique), **VLAN10-Profile** est utilisé, retournant VLAN10 et DACL, et le profil de sécurité VLAN10 avec le SGT nommé **VLAN10**. Pour MS Windows XP (nom d'utilisateur spécifique), **VLAN20-Profile** est utilisé, retournant VLAN 20 et DACL, et le profil de sécurité VLAN20 avec le SGT nommé **VLAN20**.



Terminez la configuration du commutateur et de l'ASA afin qu'ils acceptent les attributs SGT RADIUS.

Configuration CTS sur ASA et le 3750X

Vous devez configurer les paramètres CTS de base. Sur le commutateur 3750X, vous devez indiquer à partir de quelle stratégie de serveur télécharger :

```
aaa authorization network ise group radius
cts authorization list ise
```

Sur l'ASA, seul le serveur AAA est nécessaire avec CTS qui pointe vers ce serveur :

```
aaa-server ISE protocol radius
aaa-server ISE (mgmt) host 10.48.66.129
 key *****
cts server-group ISE
```

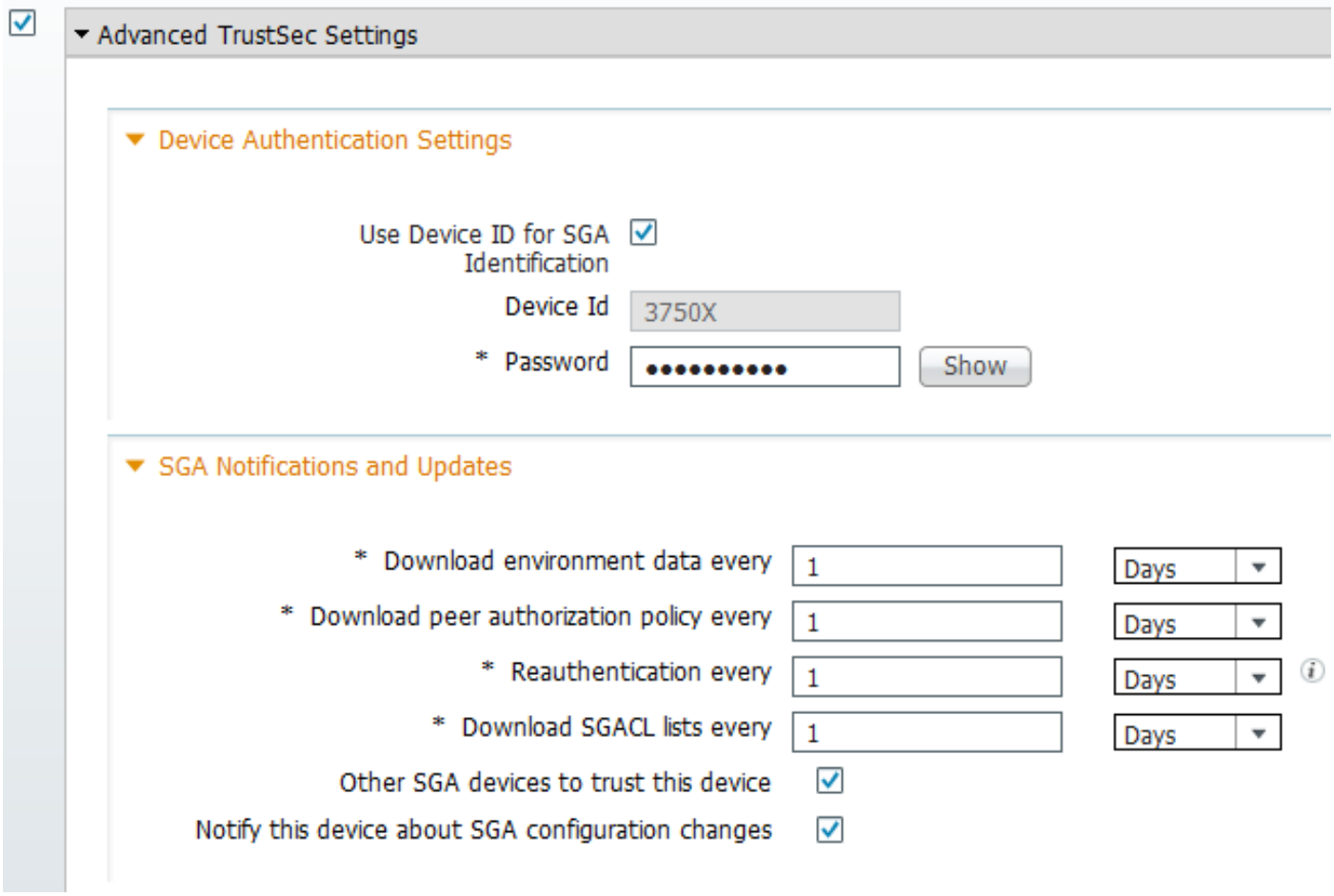
> **Remarque** : sur le commutateur 3750X, vous devez pointer explicitement vers le serveur ISE à l'aide de la commande **group radius**. En effet, le modèle 3750X utilise la mise en service PAC automatique.

Provisionnement PAC sur le 3750X (automatique) et l'ASA (manuel)

Chaque périphérique du cloud CTS doit s'authentifier auprès du serveur d'authentification (ISE) pour être approuvé par les autres périphériques. Il utilise pour cela la méthode EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Protocol) (RFC 4851). Cette méthode nécessite que le PAC soit livré hors bande. Ce processus est également appelé **phase0**, et n'est défini dans aucune RFC. PAC pour EAP-FAST a un rôle similaire à celui du certificat pour EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAC est utilisé afin d'établir un tunnel sécurisé (phase1), qui est nécessaire pour l'authentification dans la phase2.

Mise en service PAC sur le 3750X

Le modèle 3750X prend en charge le provisionnement PAC automatique. Un mot de passe partagé est utilisé sur le commutateur et l'ISE afin de télécharger PAC. Ce mot de passe et cet ID doivent être configurés sur l'ISE sous **Administration > Network Resources > Network Devices**. Sélectionnez le commutateur et développez la section **Advanced TrustSec Settings** afin de configurer :



Pour que PAC utilise ces informations d'identification, entrez les commandes suivantes :

```
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: 08:04:40 UTC Sep 25 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC59784000600940003
010094F559DAE0C837D7847F2454CAD7E80B0000001351C8235900093A803D7D427BFB5C6F0FBBDF
7EDF0818C58FECF97F8BDECF1B115FB0240260ADA8C96A46AA2A64C9EA2DB51E0E886768CA2D133D
2468D9D33339204BAA7E4CA2DE8E37FF1EB5BCB343408E9847998E301C26DDC6F91711F631A5B4C7
C2CB09EAB028630A3B22901FE3EF44F66FD019D09D2C46D92283
 Refresh timer is set for 2y24w
```

Approvisionnement PAC sur l'ASA

L'ASA prend uniquement en charge le provisionnement PAC manuel. Cela signifie que vous devez le générer manuellement sur l'ISE (dans Network Devices/ASA) :

Ensuite, le fichier doit être installé (par exemple, avec FTP) :

```
bsns-asa5510-17(config)# cts import-pac ftp://ftp:ftp@10.147.25.80/ASA.pac
password ciscocisco
!PAC Imported Successfully

bsns-asa5510-17(config)# show cts pac

 PAC-Info:
   Valid until: Jul 04 2014 13:33:02
   AID:         c40a15a339286ceac28a50dbbac59784
   I-ID:        ASA
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200a800030001000400010c40a15a339286ceac28a50dbbac597840006008c000301
   0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
   e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
   c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
   7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

Actualisation de l'environnement sur ASA et le 3750X

Àce stade, PAC est installé correctement sur les deux périphériques et commence automatiquement à télécharger les données d'environnement ISE. Ces données sont en fait des numéros d'étiquettes et leurs noms. Afin de déclencher une actualisation de l'environnement sur l'ASA, entrez cette commande :

```
bsns-asa5510-17# cts refresh environment-data
```

Afin de le vérifier sur l'ASA (malheureusement vous ne pouvez pas voir les balises/noms SGT spécifiques, mais il est vérifié plus tard), entrez cette commande :

```
bsns-asa5510-17(config)# show cts environment-data
CTS Environment Data
====================
Status:                  Active
Last download attempt:   Successful
Environment Data Lifetime: 86400 secs
Last update time:        05:05:16 UTC Apr 14 2007
Env-data expires in:     0:23:56:15 (dd:hr:mm:sec)
Env-data refreshes in:   0:23:46:15 (dd:hr:mm:sec)
```

Afin de le vérifier sur 3750X, déclenchez une actualisation de l'environnement avec cette commande :

```
bsns-3750-5#cts refresh environment-data
```

Afin de vérifier les résultats, entrez cette commande :

```
bsns-3750-5#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE    flag(0x11)
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Security Group Name Table:
 0001-60 :
    0-47:Unknown
    2-47:VLAN10
    3-47:VLAN20
    4-47:VLAN100
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 05:33:49 UTC Thu Apr 7 2011
Env-data expires in   0:16:46:50 (dd:hr:mm:sec)
Env-data refreshes in 0:16:46:50 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

Cela montre que toutes les balises et les noms correspondants sont correctement téléchargés.

Vérification et application de l'authentification des ports sur le commutateur 3750X

Une fois que le commutateur 3750X dispose des données d'environnement, vous devez vérifier que les balises SGT sont appliquées aux sessions authentifiées.

Afin de vérifier si MS Windows 7 est authentifié correctement, entrez cette commande :

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.4eb2
          IP Address:  192.168.1.200
           User-Name:  00-50-56-99-4E-B2
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                 SGT:  0002-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001002B67334C
```

```
     Acct Session ID:  0x00000179
              Handle:  0x94000101

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

Le résultat montre que **VLAN10** est utilisé avec le **SGT 0002** et la DACL autorisant pour tout le trafic.

Afin de vérifier si MS Windows XP est authentifié correctement, entrez cette commande :

```
bsns-3750-5#sh authentication sessions interface 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:  C0A80001000000FE2B67334C
     Acct Session ID:  0x00000177
              Handle:  0x540000FF

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

Le résultat montre que le **VLAN 20** est utilisé avec le **SGT 0003** et la DACL autorisant pour tout le trafic

Les adresses IP sont détectées avec la fonctionnalité de **suivi de périphérique ip**. Le commutateur DHCP doit être configuré pour la surveillance **dhcp**. Ensuite, après la réponse DHCP de surveillance, il apprend l'adresse IP du client. Pour une adresse IP configurée de manière statique (comme dans cet exemple), la fonctionnalité de **surveillance arp** est utilisée, et un PC doit envoyer n'importe quel paquet pour que le commutateur puisse détecter son adresse IP.

Pour le **suivi de périphérique**, une commande masquée peut être nécessaire afin de l'activer sur les ports :

```
bsns-3750-5#ip device tracking interface g1/0/1
bsns-3750-5#ip device tracking interface g1/0/2
bsns-3750-5#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface               STATE
```

```
-------------------------------------------------------------------------
192.168.1.200   0050.5699.4eb2  10   GigabitEthernet1/0/2     ACTIVE
192.168.2.200   0050.5699.4ea1  20   GigabitEthernet1/0/1     ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:
 Gi1/0/1, Gi1/0/2
```

Actualisation de la stratégie sur le 3750X

Le commutateur 3750X (contrairement à l'ASA) peut télécharger des stratégies à partir de l'ISE. Avant de télécharger et d'appliquer une stratégie, vous devez l'activer à l'aide des commandes suivantes :

```
bsns-3750-5(config)#cts role-based enforcement
bsns-3750-5(config)#cts role-based enforcement vlan-list 1-1005,1007-4094
```

Si vous ne l'activez pas, la stratégie est téléchargée, mais n'est pas installée et n'est pas utilisée pour l'application.

Afin de déclencher une actualisation de stratégie, entrez cette commande :

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

Afin de vérifier que la stratégie est téléchargée à partir de l'ISE, entrez cette commande :

```
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 2:VLAN10:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Le résultat montre que seule la partie nécessaire de la stratégie est téléchargée.

Dans le cloud CTS, le paquet contient le SGT de l'hôte source et l'**application est effectuée au niveau du périphérique de destination**. Cela signifie que le paquet est transféré de la source au dernier périphérique, qui est connecté directement à l'hôte de destination. Ce périphérique est le point d'application, car il connaît les SGT de ses hôtes directement connectés et sait si le paquet entrant avec un SGT source doit être autorisé ou refusé pour le SGT de destination spécifique.

Cette décision est basée sur les politiques téléchargées depuis l'ISE.

Dans ce scénario, toutes les stratégies sont téléchargées. Cependant, si vous effacez la session d'authentification MS Windows XP (SGT=VLAN20), alors il n'est pas nécessaire que le commutateur télécharge une stratégie (ligne) qui correspond à VLAN20, car il n'y a plus de périphériques de ce SGT connectés au commutateur.

La section Advanced (Troubleshooting) explique comment le commutateur 3750X décide des stratégies à télécharger en examinant le niveau des paquets.

SXP Exchange (ASA en tant que récepteur et 3750X en tant que haut-parleur)

L'ASA ne prend pas en charge SGT. Toutes les trames avec SGT sont abandonnées par l'ASA. C'est pourquoi le 3750X ne peut pas envoyer de trames étiquetées SGT à l'ASA. SXP est utilisé à la place. Ce protocole permet à l'ASA de recevoir des informations du commutateur concernant le mappage entre les adresses IP et les balises de groupe de sécurité. Grâce à ces informations, l'ASA est en mesure de mapper des adresses IP à des balises SGT et de prendre une décision basée sur la liste SGACL.

Afin de configurer le 3750X comme haut-parleur, entrez ces commandes :

```
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.1 password default mode local
```

Afin de configurer l'ASA en tant qu'écouteur, entrez ces commandes :

```
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 192.168.1.1
cts sxp connection peer 192.168.1.10 password default mode local listener
```

Afin de vérifier que l'ASA a reçu les mappages, entrez cette commande :

```
bsns-asa5510-17# show cts sxp sgt-map ipv4 detail
Total number of IP-SGT mappings : 2
Total number of IP-SGT mappings shown: 2

SGT        : 2:VLAN10
IPv4       : 192.168.1.200
Peer IP    : 192.168.1.10
Ins Num    : 1
Status     : Active
Seq Num    : 49

SGT        : 3:VLAN20
IPv4       : 192.168.2.200
Peer IP    : 192.168.1.10
Ins Num    : 1
Status     : Active
Seq Num    : 39
```

Maintenant, quand l'ASA reçoit le paquet entrant avec l'adresse IP source **192.168.1.200**, il est capable de le traiter comme s'il venait de **SGT=2**. Pour l'adresse IP source **192.168.200.2**, il est capable de la traiter comme si elle venait de **SGT=3**. Il en va de même pour l'adresse IP de destination.

> **Remarque** : le commutateur 3750X doit connaître l'adresse IP de l'hôte associé. Cette opération est effectuée par le suivi des périphériques IP. Pour une adresse IP configurée de manière statique sur l'hôte d'extrémité, le commutateur doit recevoir tout paquet après l'authentification. Cela déclenche le suivi du périphérique IP afin de trouver son adresse IP, ce qui déclenche une mise à jour SXP. Lorsque seul le SGT est connu, il n'est pas envoyé via SXP.

Filtrage du trafic sur ASA avec ACL SGT

Voici une vérification de la configuration ASA :

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
```

Une liste de contrôle d'accès est créée et appliquée à l'interface interne. Il autorise tout le trafic ICMP de **SGT=3** à **SGT=2** (appelé **VLAN10**) :

```
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
access-group inside in interface inside
```

> **Remarque** : vous pouvez utiliser le numéro ou le nom de la balise.

Si vous envoyez une requête ping à partir de MS Windows XP avec l'adresse IP source **192.168.2.200** (**SGT=3**) vers MS Windows 7 avec l'adresse IP **192.168.1.200** (**SGT=2**), l'ASA établit une connexion :

```
%ASA-6-302020: Built outbound ICMP connection for faddr 192.168.1.200/0
(2:VLAN10) gaddr 192.168.2.200/512 laddr 192.168.2.200/512(3:VLAN20)
```

Lorsque vous tentez la même chose avec Telnet, le trafic est bloqué :

```
Deny tcp src inside:192.168.2.200/2478(3:VLAN20) dst outside:192.168.1.200/23
(2:VLAN10) by access-group "inside"
```

Il existe d'autres options de configuration sur l'ASA. Il est possible d'utiliser une balise de sécurité et une adresse IP pour la source et la destination. Cette règle autorise le trafic d'écho ICMP depuis l'**étiquette SGT = 3** et l'adresse IP **192.168.2.200** vers l'étiquette SGT nommée **VLAN10** et l'adresse d'hôte de destination **192.168.1.200** :

```
access-list inside extended permit icmp security-group tag 3 host 192.168.2.200
security-group name VLAN10 host 192.168.1.200 echo
```

Ceci peut également être réalisé avec des groupes d'objets :

```
object-group security SGT-VLAN-10
 security-group name VLAN10
object-group security SGT-VLAN-20
 security-group tag 3
object-group network host1
 network-object host 192.168.1.200
object-group network host2
 network-object host 192.168.2.200
object-group service my-icmp-echo
 service-object icmp echo
```

```
access-list inside extended permit object-group my-icmp-echo
object-group-security SGT-VLAN-20 object-group host2 object-group-security
SGT-VLAN-10 object-group host1
```

Filtrage du trafic sur le commutateur 3750X avec des stratégies téléchargées depuis l'ISE (RBACL)

Il est également possible de définir des politiques locales sur le commutateur. Cependant, cet exemple présente des stratégies téléchargées à partir de l'ISE. Les stratégies définies sur l'ASA sont autorisées à utiliser à la fois les adresses IP et les balises SGT (ainsi que le nom d'utilisateur d'Active Directory) dans une seule règle. Les politiques définies sur le commutateur (à la fois en local et à partir de l'ISE) autorisent uniquement les balises de groupe de sécurité. Si vous devez utiliser des adresses IP dans vos règles, le filtrage sur l'ASA est recommandé.

Le trafic ICMP entre MS Windows XP et MS Windows 7 est testé. Pour cela, vous devez changer la passerelle par défaut de l'ASA au 3750X sur MS Windows. Le commutateur 3750X possède des interfaces de routage et peut acheminer les paquets :

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
!
interface Vlan20
 ip address 192.168.2.10 255.255.255.0
```

Les stratégies sont déjà téléchargées depuis ISE. Afin de les vérifier, entrez cette commande :

```
 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 2:VLAN10:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Le trafic de VLAN10 (MS Windows 7) vers VLAN20 (MS Windows XP) est soumis à l'ACL ICMP-20, qui est téléchargé à partir de l'ISE :

```
bsns-3750-5#show ip access-lists ICMP-20
Role-based IP access list ICMP-20 (downloaded)
   10 permit icmp
```

Afin de vérifier la liste de contrôle d'accès, entrez cette commande :

```
bsns-3750-5#show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
 name   = Deny IP-00
 IP protocol version = IPV4
```

```
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   deny ip

  name   = ICMP-20
 IP protocol version = IPV4
 refcnt = 6
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
    permit icmp

 name   = Permit IP-00
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   permit ip
```

Afin de vérifier le mappage SGT pour s'assurer que le trafic des deux hôtes est correctement étiqueté, entrez cette commande :

```
bsns-3750-5#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.1.200           2       LOCAL
192.168.2.200           3       LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

ICMP de MS Windows 7 (**SGT=2**) à MS Windows XP (**SGT=3**) fonctionne correctement avec ACL ICMP-20. Ceci est vérifié en vérifiant les compteurs pour le trafic de **2** à **3** (15 paquets autorisés) :

```
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               1695            224
2       2       0               -               0               -

*       *       0               0               133258          132921

2       3       0               0               0               15
```

Après avoir tenté d'utiliser le compteur Telnet, les paquets refusés augmentent (il n'est pas autorisé sur l'ACL ICMP-20) :

```
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               1695            224
2       2       0               -               0               -

*       *       0               0               133281          132969

2       3       0               2               0               15
```

Remarque : le caractère étoile (*) affiché dans le résultat est lié à tout le trafic qui n'est pas étiqueté (cette colonne et cette ligne sont appelées **unknown** dans Matrix sur l'ISE, et utilisent le numéro d'étiquette **0**).

Lorsque vous avez une entrée de liste de contrôle d’accès avec le mot clé log (défini sur l’ISE), les détails du paquet correspondant et les actions entreprises sont consignés comme dans n’importe quelle liste de contrôle d’accès avec le mot clé log.

Vérifier

Reportez-vous aux différentes sections de configuration pour connaître les procédures de vérification.

Dépannage

Provisionnement PAC

Des problèmes peuvent apparaître lorsque vous utilisez l'approvisionnement PAC automatique. N'oubliez pas d'utiliser le mot clé **pac** pour le serveur RADIUS. L'approvisionnement PAC automatique sur le 3750X utilise la méthode EAP-FAST avec le protocole d'authentification extensible avec la méthode interne utilisant l'authentification EAP-MSCHAPv2 (Challenge Handshake Authentication Protocol) de Microsoft. Lorsque vous déboguez, vous voyez plusieurs messages RADIUS qui font partie de la négociation EAP-FAST utilisée afin de construire le tunnel sécurisé, qui utilise EAP-MSCHAPv2 avec l'ID et le mot de passe configurés pour l'authentification.

La première demande RADIUS utilise AAA **service-type=cts-pac-provisioning** afin d'informer l'ISE qu'il s'agit d'une demande PAC.

```
bsns-3750-5#debug cts provisioning events
bsns-3750-5#debug cts provisioning packets

*Mar  1 09:55:11.997: CTS-provisioning: New session socket: src=
10.48.66.109:57516 dst=10.48.66.129:1645
*Mar  1 09:55:11.997: CTS-provisioning: Sending EAP Response/Identity to
10.48.66.129
*Mar  1 09:55:11.997: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
```

```
*Mar  1 09:55:11.997: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.006: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.006: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.006: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.106: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.115: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.744: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.744: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.744: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.853: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.853: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.853: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.853: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.861: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.861: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.861: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.861: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.886: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.886: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.886: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.895: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.895: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.903: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.920: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.920: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.920: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.970: CTS-pac-refresh: PAC C40A15A339286CEAC28A50DBBAC59784
refresh timer has been set for 20y30w
*Mar  1 09:55:12.970: CTS-provisioning: Ignoring key data.
*Mar  1 09:55:12.979: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.979: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.979: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: Received RADIUS reject from 10.48.66.129.
*Mar  1 09:55:12.995: CTS-provisioning: Successfully obtained PAC for A-ID
c40a15a339286ceac28a50dbbac59784
*Mar  1 09:55:12.995: CTS-provisioning: cts_provi_server_cleanup: 10.48.66.129
*Mar  1 09:55:12.995: CTS-provisioning: work complete, process terminating.
```

Le **rejet RADIUS** à la fin de la sortie est attendu puisque vous avez déjà reçu PAC, et n'a pas suivi avec un processus d'authentification supplémentaire.

N'oubliez pas que le PAC est requis pour toutes les autres communications avec l'ISE. Toutefois, si vous ne l'avez pas, le commutateur tente toujours d'actualiser l'environnement ou la stratégie

lorsqu'il est configuré. Ensuite, il n'attache pas **cts-opaqueue** (PAC) dans les requêtes RADIUS, ce qui provoque les échecs.

Si votre clé PAC est incorrecte, ce message d'erreur s'affiche sur l'ISE :

```
The Message-Authenticator RADIUS attribute is invalid
```

Vous voyez également cette sortie de debugs (**debug cts provisioning + debug radius**) sur le commutateur si votre clé PAC est incorrecte :

```
Apr 20 10:07:11.768: CTS-provisioning: Sending EAP Response/Identity t
Apr 20 10:07:15.325: RADIUS(0000024B): Request timed out!
Apr 20 10:07:15.325: RADIUS: No response from (10.62.84.224:1645,1646) for
id 1645/37
```

Si vous utilisez la convention de **serveur RADIUS** moderne, ceci affiche :

```
radius server KRK-ISE
 address ipv4 10.62.84.224 auth-port 1645 acct-port 1646
 pac key CISCO
```

> **Remarque** : vous devez utiliser le même mot de passe sur l'ISE que celui utilisé dans les **paramètres d'authentification** du **périphérique**.

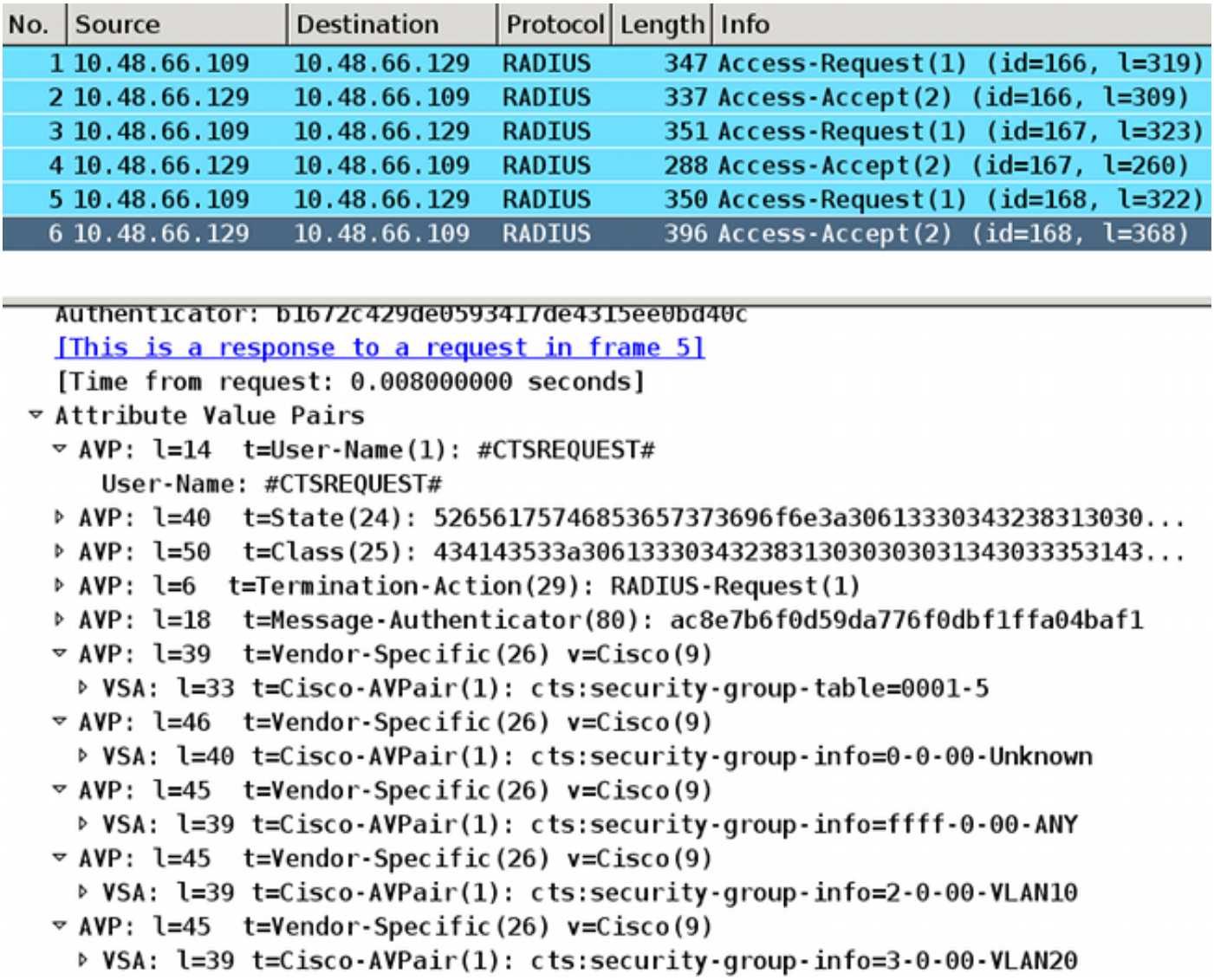
Une fois l'approvisionnement PAC réussi, le message suivant s'affiche sur l'ISE :

Authentication Summary	
Logged At:	June 26,2013 1:36:32.676 PM
RADIUS Status:	PAC provisioned
NAS Failure:	
Username:	3750
MAC/IP Address:	BC:16:65:25:A5:00
Network Device:	3750X : 10.48.66.109 :
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Actualisation de l'environnement

L'actualisation de l'environnement est utilisée afin d'obtenir des données de base de l'ISE, qui inclut le numéro et le nom de SGT. Le niveau paquet indique qu'il ne s'agit que de trois requêtes et réponses RADIUS avec des attributs.

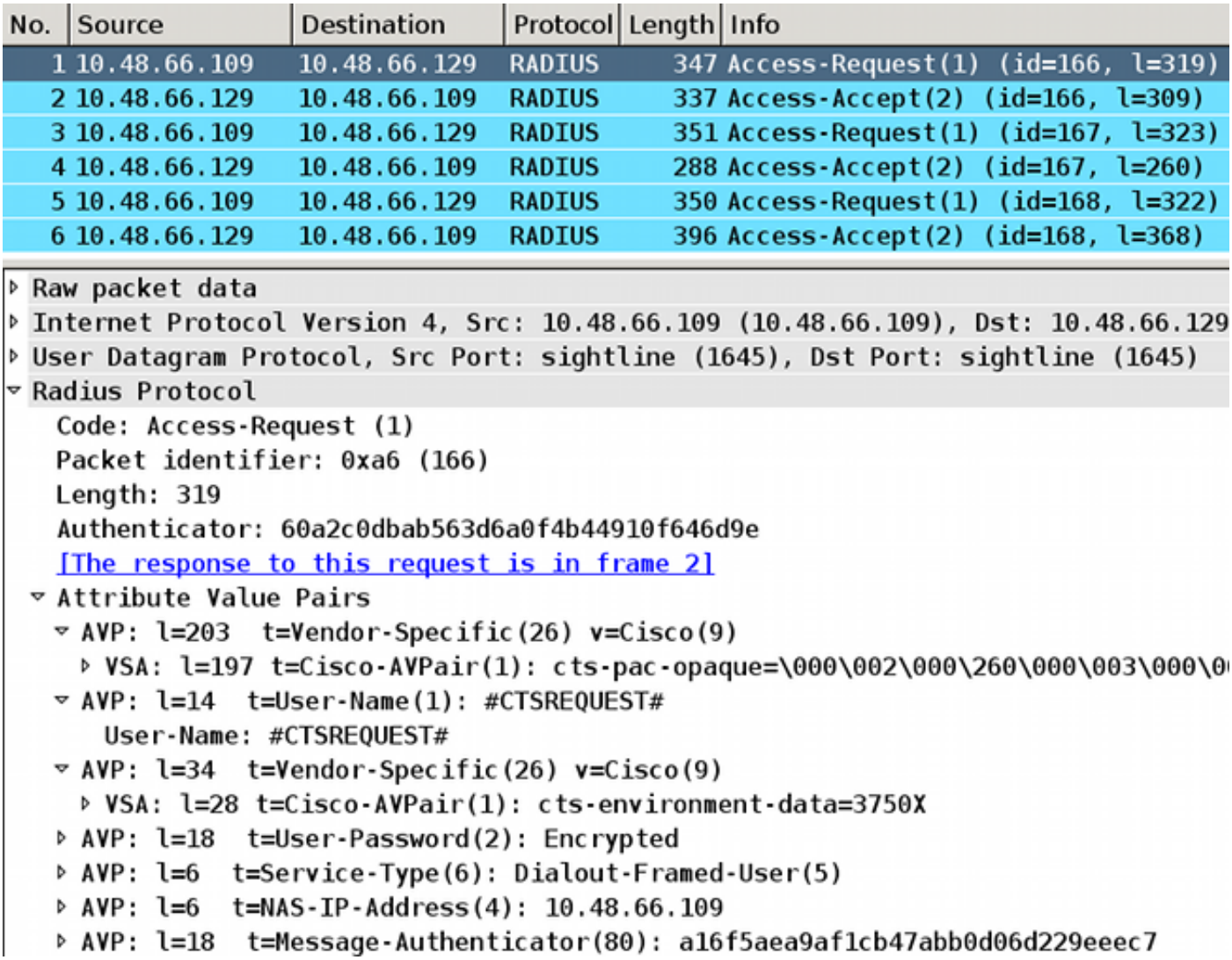
Pour la première requête, le commutateur reçoit le nom **CTSServerlist**. Pour la seconde, il reçoit les détails de cette liste, et pour la dernière, il reçoit tous les SGT avec des tags et des noms :



No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

Ici, vous voyez le **SGT 0**, **ffff**, et aussi deux personnalisées-définies : SGT tag 2 est nommé **VLAN10** et SGT tag 3 est nommé **VLAN20**.

Remarque : toutes les demandes RADIUS incluent **cts-pac-opaque** suite à l'approvisionnement PAC.



No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

Sur le 3750X, vous devriez voir des débogages pour les trois réponses RADIUS et les listes correspondantes, les détails de la liste et la liste SGT-inside spécifique :

```
bsns-3750-5#debug cts environment-data all

*Mar  1 10:05:07.454: CTS env-data&colon; cleanup mcast SGT table
*Mar  1 10:05:18.057: CTS env-data&colon; Force environment-data refresh
*Mar  1 10:05:18.057: CTS env-data&colon; download transport-type =
CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057:     cts_env_data START: during state env_data_complete,
got event 0(env_data_request)
*Mar  1 10:05:18.057: @@@ cts_env_data START: env_data_complete ->
env_data_waiting_rsp
*Mar  1 10:05:18.057: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: cts_env_data_is_complete: FALSE, req(x0), rec(x0),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)AAA req(x7C3DF10)
*Mar  1 10:05:18.057: cts_aaa_attr_add: AAA req(0x7C3DF10)
*Mar  1 10:05:18.057:   username = #CTSREQUEST#
*Mar  1 10:05:18.057:   cts-environment-data = 3750X
*Mar  1 10:05:18.057: cts_aaa_req_send: AAA req(0x7C3DF10) successfully sent to AAA.
*Mar  1 10:05:18.083: cts_aaa_callback: (CTS env-data)AAA req(0x7C3DF10)
response success
```

```
*Mar  1 10:05:18.083:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.083:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.083:   AAA attr: security-group-tag = 0000-00.
*Mar  1 10:05:18.083:   AAA attr: environment-data-expiry = 86400.
*Mar  1 10:05:18.083:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.083: CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SLIST
    slist name(CTSServerList1) received in 1st Access-Accept
   slist name(CTSServerList1) created
 CTS_AAA_SECURITY_GROUP_TAG - SGT = unicast-unknown-00
 CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
 CTS_AAA_SGT_NAME_LIST
   table(0001) received in 1st Access-Accept
   old name(), gen()
   new name(0001), gen(50)
 CTS_AAA_DATA_END
*Mar  1 10:05:18.083:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.083: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.083: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.083: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.083: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.083: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)AAA req(x792FFD0)
*Mar  1 10:05:18.083: cts_aaa_attr_add: AAA req(0x792FFD0)
*Mar  1 10:05:18.091:   username = #CTSREQUEST#
*Mar  1 10:05:18.091:   cts-server-list = CTSServerList1
*Mar  1 10:05:18.091: cts_aaa_req_send: AAA req(0x792FFD0) successfully sent to AAA.
*Mar  1 10:05:18.099: cts_aaa_callback: (CTS env-data)AAA req(0x792FFD0)
response success
*Mar  1 10:05:18.099:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.099:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.099:   AAA attr: server = c40a15a339286ceac28a50dbbac59784:
10.48.66.129:1812.
*Mar  1 10:05:18.099: CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SLIST
    2nd Access-Accept slist name(CTSServerList1), gen(0001)
 CTS_AAA_SERVERS
   server (c40a15a339286ceac28a50dbbac59784:10.48.66.129:1812) added
 CTS_AAA_DATA_END
*Mar  1 10:05:18.099:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.099: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.099: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.099: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
```

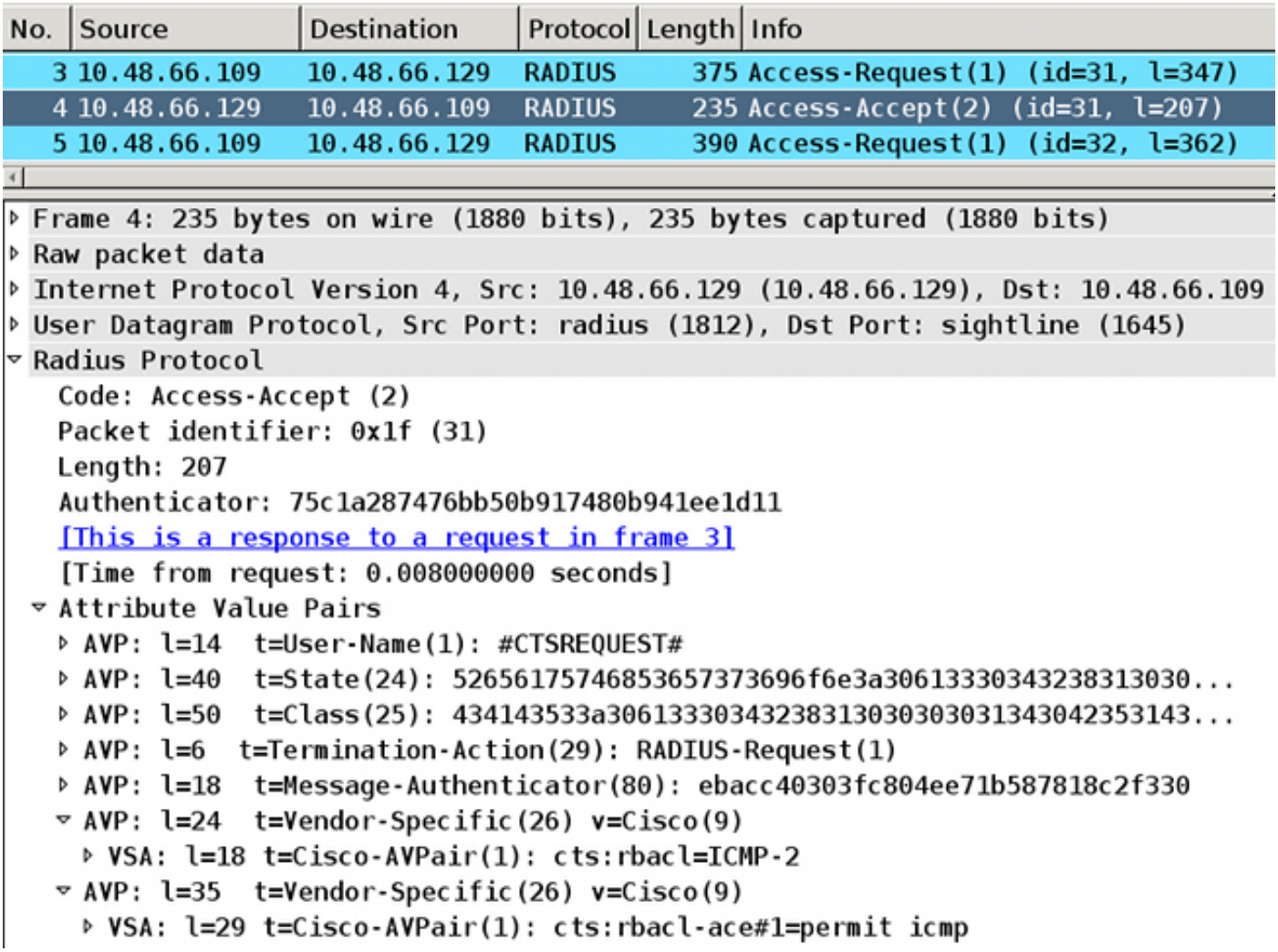
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)Using private server group
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)AAA req(x7A6C4AC)
*Mar  1 10:05:18.099: cts_aaa_attr_add: AAA req(0x7A6C4AC)
*Mar  1 10:05:18.099:   username = #CTSREQUEST#
*Mar  1 10:05:18.099:   cts-security-group-table = 0001
*Mar  1 10:05:18.099: cts_aaa_req_send: AAA req(0x7A6C4AC) successfully sent to AAA.
*Mar  1 10:05:18.108: cts_aaa_callback: (CTS env-data)AAA req(0x7A6C4AC)
response success
*Mar  1 10:05:18.108:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.108:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 0-0-00-Unknown.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = ffff-0-00-ANY.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 2-0-00-VLAN10.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 3-0-00-VLAN20.
*Mar  1 10:05:18.108:  CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SGT_NAME_LIST
   table(0001) received in 2nd Access-Accept
   old name(0001), gen(50)
   new name(0001), gen(50)
 CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-unknown-00
   flag (128) server name (Unknown) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-default-00
   flag (128) server name (ANY) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = 2-00
   flag (128) server name (VLAN10) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = 3-00
   flag (128) server name (VLAN20) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_DATA_END
*Mar  1 10:05:18.108:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.108: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.108: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.108: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.116: cts_env_data_is_complete: TRUE, req(x2085), rec(x2C87),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.116:     cts_env_data ASSESSING: during state env_data_assessing,
got event 4(env_data_complete)
*Mar  1 10:05:18.116: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_complete
*Mar  1 10:05:18.116: env_data_complete_enter: state = COMPLETE
*Mar  1 10:05:18.116: env_data_install_action: state = COMPLETE
```

Actualisation des stratégies

L'actualisation de la stratégie est prise en charge uniquement sur le commutateur. Elle est similaire à l'actualisation de l'environnement. Il s'agit simplement de demandes et d'acceptations RADIUS.

Le commutateur demande toutes les listes de contrôle d'accès de la liste par défaut. Ensuite, pour chaque liste de contrôle d'accès qui n'est pas à jour (ou qui n'existe pas), il envoie une autre demande pour obtenir les détails.

Voici un exemple de réponse lorsque vous demandez une liste de contrôle d'accès ICMP-20 :



N'oubliez pas que vous devez avoir configuré l'**application basée sur les rôles cts** pour appliquer cette liste de contrôle d'accès.

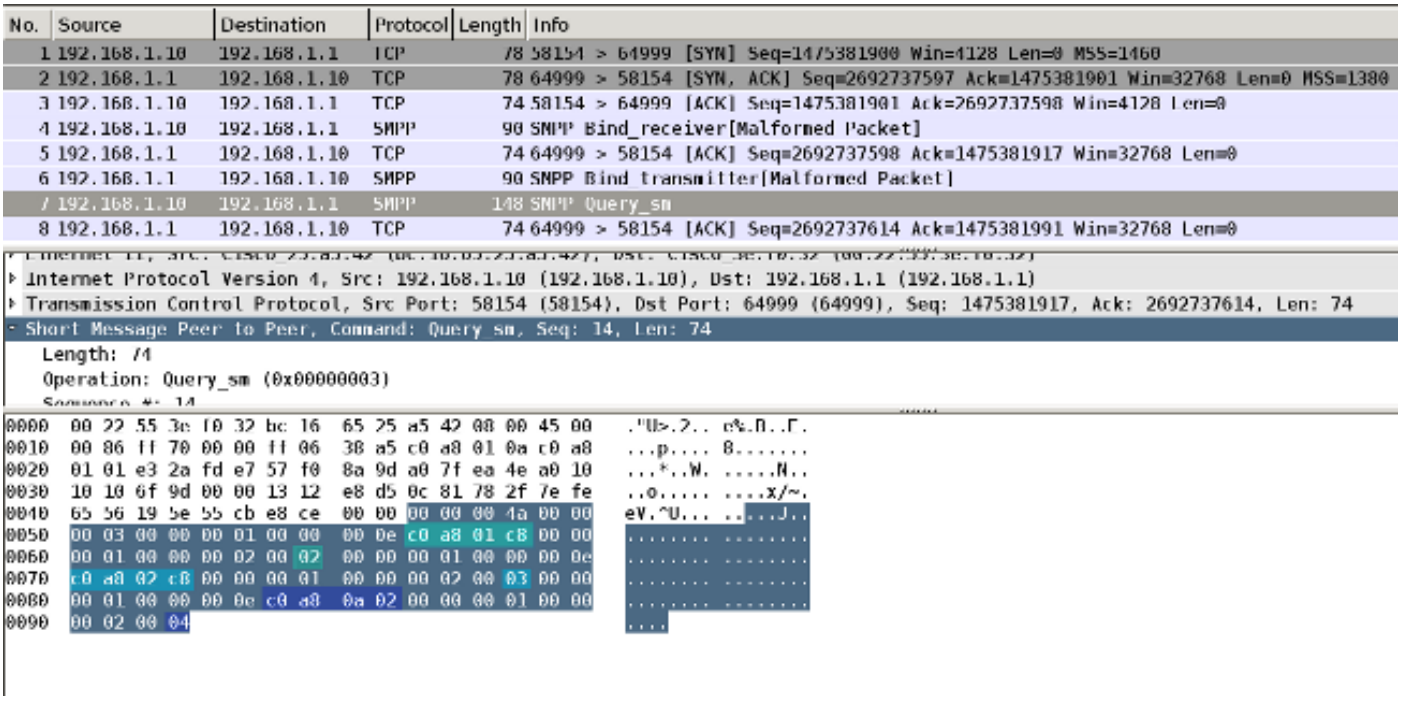
Les débogages indiquent s'il y a des modifications (en fonction de l'ID de génération). Si c'est le cas, vous pouvez désinstaller l'ancienne stratégie si nécessaire et en installer une nouvelle. Cela inclut la programmation ASIC (support matériel).

```
bsns-3750-5#debug cts all

Mar 30 02:39:37.151:  CTS authz entry: peer(Unknown-2) Receiving AAA attributes
   rcv rbacl list: flags: req(81)rcv(0)wait(80)prev(0)install(880)
    - SGT = 2-01:VLAN10
    - SGT = 2-01:VLAN10
   current arg_cnt=8, expected_num_args=11
   3rd Access-Accept rbacl received name(ICMP), gen(20)
   received_policyp->sgt(2-01:VLAN10)
```

```
   existing sgt_policy(73FFDB4) sgt(2-01:VLAN10)
   RBACL name(ICMP-20)flag(40000000) already exists
  acl_listp(740266C) old_acl_infop(0),exist_rbacl_type(0)
 CTS_AAA_AUTHORIZATION_EXPIRY = 86400.
 CTS_AAA_DATA_END

Mar 30 02:39:37.176: cts_authz_entry_complete_action: Policy download complete -
peer(Unknown-2) SGT(2-01:VLAN10) status(RBACL-POLICY SUCCEEDED)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV6
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(C0000000)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV4
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(40000000)

Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV6
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(C0000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Waiting for more RBM callback
for remaining IP version(40000000) RBACL policy(73FFDB4) for SGT(2-01:VLAN10)
flag(41400001)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb:
Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV4
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(40000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Program RBACL policy(73FFDB4)
for SGT(2-01:VLAN10) flag(41400001) success
```

Exchange SXP

La mise à jour SXP est déclenchée par le code de suivi de périphérique IP qui trouve l'adresse IP du périphérique. Ensuite, le protocole SMPP (Short Message Peer-to-Peer) est utilisé pour envoyer les mises à jour. Il utilise l'option TCP 19 pour l'authentification, qui est la même que le protocole BGP (Border Gateway Protocol). La charge utile SMPP n'est pas chiffrée. Wireshark ne dispose pas d'un décodeur approprié pour la charge utile SMPP, mais il est facile d'y trouver des données :



- Le premier, **c0 a8 01 c8**, est **192.168.1.200** et a l'**étiquette 2**.
- Le second, **c0 a8 02 c8**, est **192.168.2.200** et a l'**étiquette 3**.
- Le troisième, **c0 a8 0a 02,** est **192.168.10.2** et a l'**étiquette 4** (celle-ci a été utilisée afin de tester le téléphone **SGT=4**)

Voici quelques débogages sur le 3750X après que le suivi de périphérique IP a trouvé l'adresse IP de MS Windows 7 :

```
bsns-3750-5#debug cts sxp message
bsns-3750-5#debug cts sxp internal
bsns-3750-5#debug cts sxp conn
bsns-3750-5#debug cts sxp mdb
bsns-3750-5#debug cts sxp error

Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_message_event = CTS_SXPMSG_REQUEST
Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_request  CTS_SXPMSG_REQ_CONN_NVGEN
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_process_request boolean set
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_send_request set boolean after
Apr  7 00:40:05.418: CTS-SXP-CONN:is_cts_sxp_rf_active
Apr  7 00:40:05.418: CTS-SXP-MDB:sxp_export_ipsgt_change 192.168.1.200/32 add 1
```

Voici les débogages correspondants sur l'ASA :

```
bsns-asa5510-17# debug cts sxp all

%ASA-7-776018: CTS SXP: Binding 192.168.1.200->2:VLAN10 from peer 192.168.1.10
(instance 1) added in SXP database.
%ASA-7-776019: CTS SXP: Binding 192.168.1.200->2:VLAN10 added. Update binding
manager.
%ASA-6-776251: CTS SGT-MAP: Binding 192.168.1.200->2:VLAN10 from SXP added to
binding manager.
%ASA-7-776014: CTS SXP: SXP received binding forwarding request (add) binding
192.168.1.200->2:VLAN10.
```

Afin de voir plus de débogages sur l'ASA, vous pouvez activer le niveau de verbosité de débogage :

```
bsns-asa5510-17# debug cts condition level detail
debug cts condition level detail is enable
```

SGACL sur l'ASA

Une fois que l'ASA a correctement installé les mappages SGT reçus par SXP, la liste de contrôle d'accès des groupes de sécurité devrait fonctionner correctement. Lorsque vous rencontrez des problèmes avec le mappage, saisissez :

```
bsns-asa5510-17# debug cts sgt-map
```

La liste de contrôle d'accès avec le groupe de sécurité fonctionne exactement de la même manière que pour l'adresse IP ou l'identité de l'utilisateur. Les journaux révèlent des problèmes et l'entrée exacte de la liste de contrôle d'accès qui a été atteinte.

Voici une requête ping de MS Windows XP vers MS Windows 7 qui montre que Packet Tracer fonctionne correctement :

```
bsns-asa5510-17# packet-tracer input inside icmp 192.168.2.200 8 0 192.168.1.200
detailed
<output ommitted>

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xaaf2ae80, priority=13, domain=permit, deny=false
       hits=185, user_data=0xaa2f5040, cs_id=0x0, use_real_addr, flags=0x0,
protocol=1
       src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=3:VLAN20
       dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=2:VLAN10, dscp=0x0
       input_ifc=inside, output_ifc=any

<output ommitted>
```

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.