Exemple de configuration de classification et d'application de la version 9.2 VPN SGT ASA

Contenu

Introduction

Ce document décrit comment utiliser une nouvelle caractéristique dans la version 9.2.1 de l'appliance de sécurité adaptable (ASA), classification de la balise de groupe de sécurité de TrustSec (SGT) pour des utilisateurs VPN. Cet exemple présente deux utilisateurs VPN qui ont été assignés un Pare-feu différent SGT et de groupe de sécurité (SGFW), qui filtre le trafic entre les utilisateurs VPN.

Contribué par Michal Garcarz, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de configuration ASA CLI et de configuration du VPN de Protocole SSL (Secure Socket Layer)
- Connaissance de base de configuration du VPN d'Accès à distance sur l'ASA
- Connaissance de base des services du Cisco Identity Services Engine (ISE) et du TrustSec

Composants utilisés

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

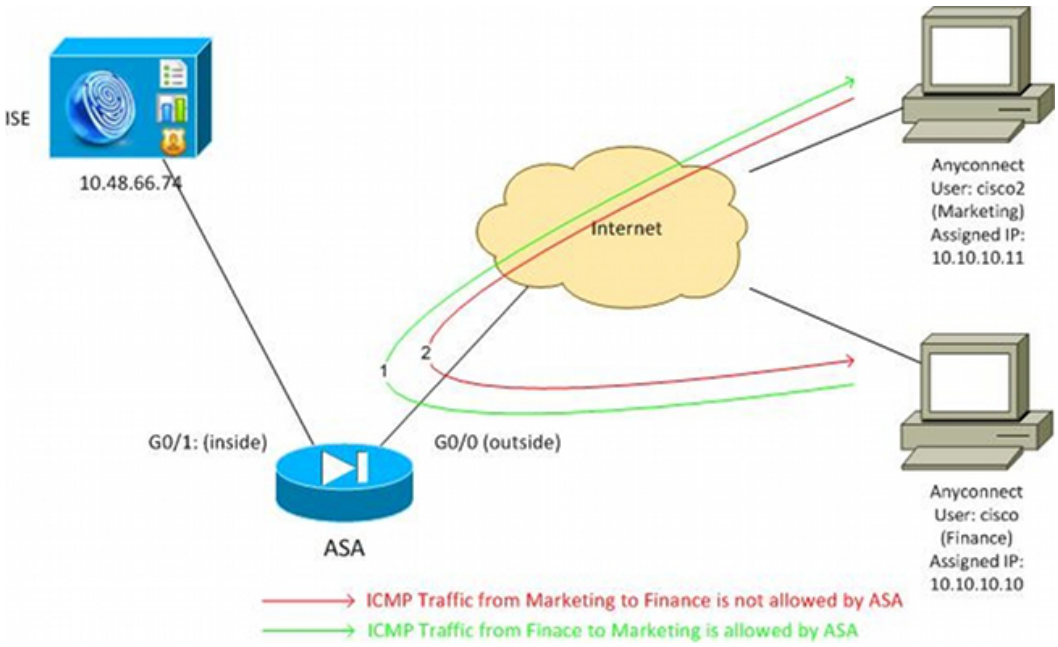
- Logiciel de Cisco ASA, version 9.2 et ultérieures
- Windows 7 avec le Client à mobilité sécurisé Cisco AnyConnect, version 3.1
- Cisco ISE, version 1.2 et ultérieures

Configurez

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

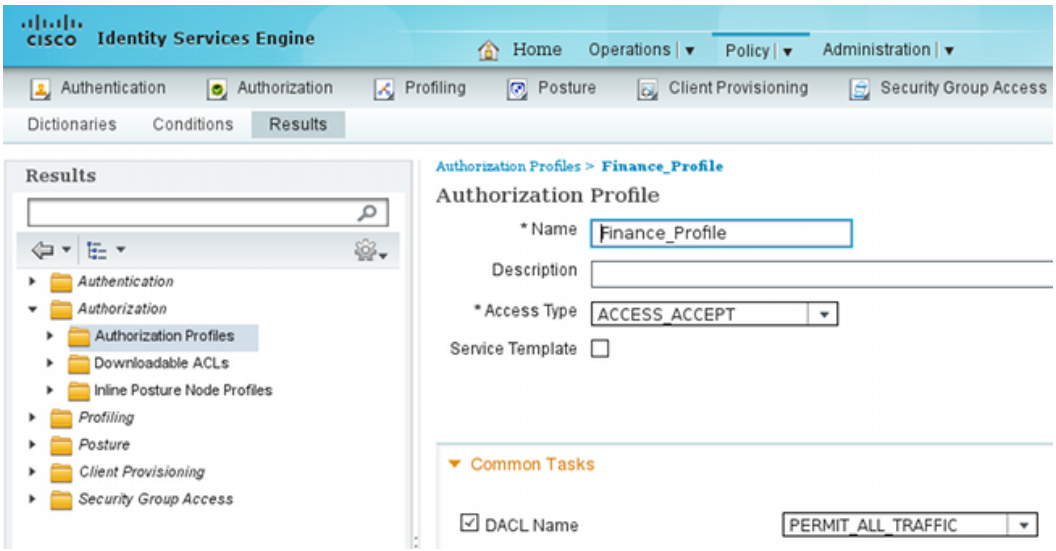
L'utilisateur « Cisco » VPN est assigné à l'équipe de finances, qui est permise pour initier une connexion de Protocole ICMP (Internet Control Message Protocol) à l'équipe de vente. L'utilisateur 'cisco2 VPN est assigné à l'équipe de vente, qui n'est pas permise pour n'initier aucune connexion.



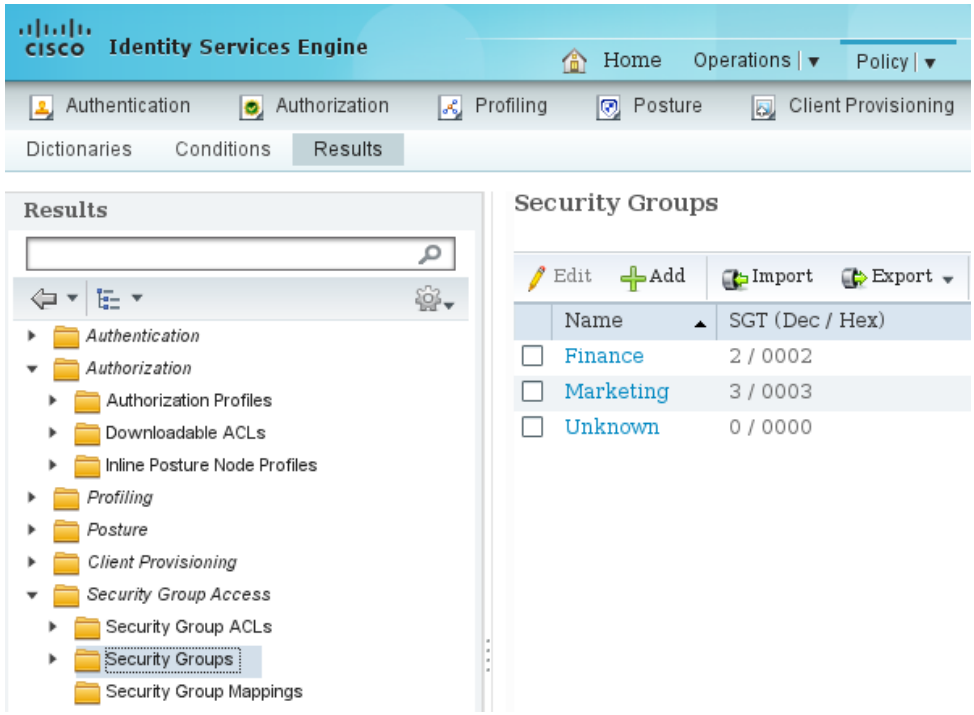
Configuration ISE

1. Choisissez la **gestion > la Gestion de l'identité > les identités** afin d'ajouter et configurer l'utilisateur « Cisco » (des finances) et 'cisco2 (du marketing).
2. Choisissez la **gestion > les ressources de réseau > les périphériques de réseau** afin d'ajouter et configurer l'ASA comme périphérique de réseau.
3. Choisissez la **stratégie > les résultats > l'autorisation > les profils d'autorisation** afin de des profils ajouter et configurer de finances et de vente autorisation.

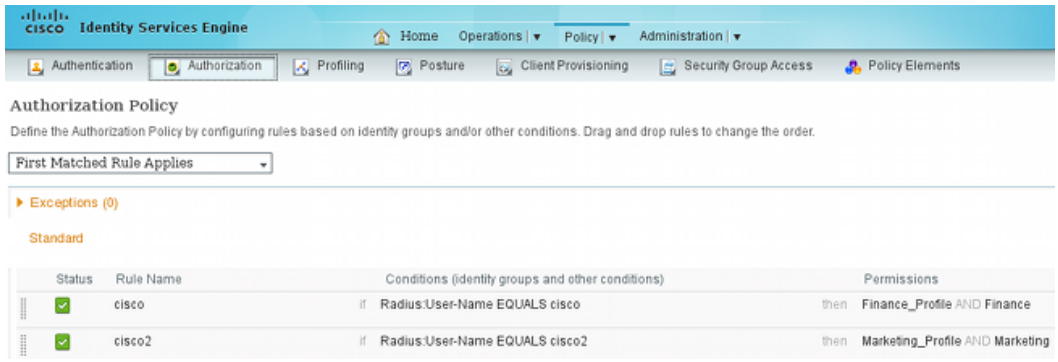
   Les deux profils incluent juste un attribut, la liste de contrôle d'accès téléchargeable (DACL), qui permet tout le trafic. Un exemple pour des finances est affiché ici :



   Chaque profil pourrait avoir un DACL spécifique et restrictif, mais pour ce scénario tout le trafic est permis. L'application n'est exécutée par le SGFW, pas le DACL assigné à chaque session VPN. Trafiquez qui est filtré avec un SGFW tient compte de l'usage juste de SGTs au lieu des adresses IP utilisées par DACL.
4. Choisissez la **stratégie > les résultats > le groupe de sécurité Access > groupes de sécurité** afin d'ajouter et configurer les finances et les groupes de commercialisation SGT.

4. 

5. Choisissez la **stratégie > l'autorisation** afin de configurer les deux règles d'autorisation. La première règle assigne le Finance_profile (DACL qui permet le trafic entier) avec les finances de groupe SGT à l'utilisateur de « Cisco ». La deuxième règle assigne le Marketing_profile (DACL qui permet le trafic entier) avec le groupe SGT lançant sur le marché à l'utilisateur 'cisco2.



Configuration ASA

1. Terminez-vous la configuration du VPN de base.

```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

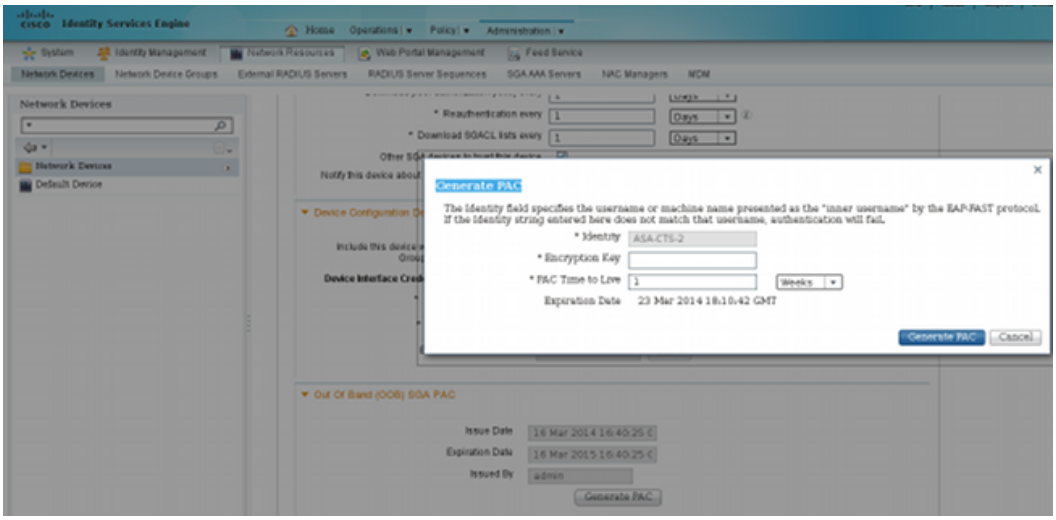
2. Terminez-vous l'AAA ASA et la configuration de TrustSec.

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
 key *****
cts server-group ISE
```

Afin de joindre le nuage de TrustSec, l'ASA doit authentifier avec le laisser-passer de Protected Access (PAC). L'ASA ne prend en charge pas le ravitaillement automatique PAC, qui est pourquoi ce fichier doit être manuellement généré sur l'ISE et être importé à l'ASA.

3. Choisissez la **gestion > les ressources de réseau > les périphériques de réseau > l'ASA > a avancé des configurations de TrustSec**

afin de générer un PAC sur l'ISE. Choisissez **hors du** ravitaillement **PAC de la bande (OOB)** afin de générer le fichier.



4. Importez le PAC à l'ASA.

   Le fichier généré a pu être mis sur un ftp server HTTP. Les utilisations ASA qui d'importer le fichier.

```
ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678
!PAC Imported Successfully
ASA#
ASA# show cts pac

  PAC-Info:
    Valid until: Mar 16 2015 17:40:25
    AID:         ea48096688d96ef7b94c679a17bdad6f
    I-ID:        ASA-CTS-2
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b800030001000400010ea48096688d96ef7b94c679a17bdad6f0006009c000301
    0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
    e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
    2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
    99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
    11d8378829cc007b91ced9117a
```

   Quand vous avez le PAC correct, l'ASA exécute automatiquement un environnement régénèrent. Ceci télécharge les informations de l'ISE au sujet des groupes en cours SGT.

```
ASA# show cts environment-data sg-table

Security Group Table:
Valid until: 17:48:12 CET Mar 17 2014
Showing 4 of 4 entries

SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
Unknown                               0     unicast
Finance                               2     unicast
Marketing                             3     unicast
```

5. Configurez le SGFW. La dernière étape est de configurer l'ACL sur l'interface extérieure qui tient compte du trafic d'ICMP des finances au marketing.

```
access-list outside extended permit icmp security-group tag 2 any security-group
tag 3 any
access-group outside in interface outside
```

   En outre, le nom de groupe de sécurité a pu être utilisé au lieu de la balise.

```
access-list outside extended permit icmp security-group name Finance any
security-group name Marketing any
```

   Afin de s'assurer que l'ACL d'interface traite le trafic VPN, il est nécessaire de désactiver l'option qui par le trafic VPN par défaut d'autorisations sans validation par l'intermédiaire de l'ACL d'interface.

```
no sysopt connection permit-vpn
```

Maintenant l'ASA devrait être prête à classifier des utilisateurs VPN et à exécuter l'application basée sur SGTs.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show**.**

Après que le VPN soit établi, l'ASA présente un SGT appliqué à chaque session.

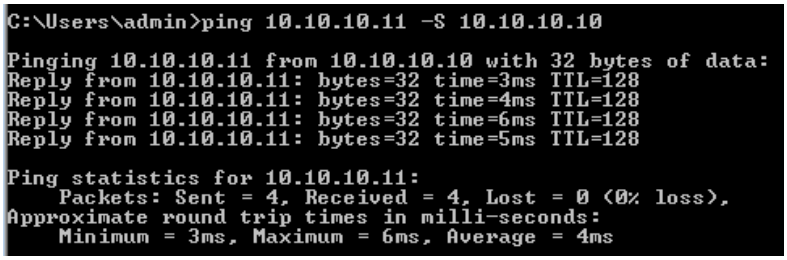
```
ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 10.10.10.10            Public IP    : 192.168.10.68
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 35934                  Bytes Rx     : 79714
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:49:15 CET Sun Mar 16 2014
Duration     : 0h:22m:57s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000010005325d60b
Security Grp : 2:Finance

Username     : cisco2                 Index        : 2
Assigned IP  : 10.10.10.11            Public IP    : 192.168.10.80
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 86171                  Bytes Rx     : 122480
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:52:27 CET Sun Mar 16 2014
Duration     : 0h:19m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000020005325d6cb
Security Grp : 3:Marketing
```

Le SGFW tient compte du trafic d'ICMP des finances (SGT=2) à la commercialisation (SGT=3). C'est pourquoi l'utilisateur « Cisco » peut cingler l'utilisateur 'cisco2.



L'augmentation de compteurs :

```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
tag 2(name="Finance") any security-group tag 3(name="Marketing")
any (hitcnt=4) 0x071f07fc
```

La connexion a été créée :

```
Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for
faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0
laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco)
```

Le trafic de retour est automatiquement reçu, parce que l'inspection d'ICMP est activée.

Quand vous essayez de cingler du marketing (SGT=3) pour financer (SGT=2) :

```
C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

États ASA :

```
Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2,
3:Marketing) dst outside:10.10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by
access-group "outside" [0x0, 0x0]
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Voir les ces documents :

- Le nuage de TrustSec avec le 802.1x MACsec sur la gamme du Catalyst 3750X commutent l'exemple de configuration
- L'ASA et les séries du Catalyst 3750X commutent l'exemple de configuration de TrustSec et dépannent le guide

Résumé

Cet article présente un exemple simple sur la façon dont classifier des utilisateurs VPN et exécuter l'application de base. Les filtres SGFW également trafiquent entre les utilisateurs VPN et le reste du réseau. SXP (protocole d'échange de TrustSec SGT) peut être utilisé sur une ASA pour obtenir les informations de mappage entre l'IP et le SGTs. Cela permet à une ASA pour exécuter l'application pour tous les types de sessions qui a été correctement classifiée (VPN ou RÉSEAU LOCAL).

Dans le logiciel ASA, la version 9.2 et ultérieures, l'ASA prend en charge également la modification de RAYON de l'autorisation (CoA) (RFC 5176). Un paquet CoA de RAYON envoyé d'ISE après qu'une posture réussie VPN puisse inclure des Cisco-poids du commerce-paires avec un SGT qui affecte un utilisateur conforme à un groupe (plus sécurisé) différent. Pour plus d'exemples, voyez les articles dans la section Informations connexes.

Informations connexes

- **Posture de la version 9.2.1 VPN ASA avec l'exemple de configuration ISE**
- **L'ASA et les séries du Catalyst 3750X commutent l'exemple de configuration de TrustSec et dépannent le guide**
- **Guide de configuration de commutateur de Cisco TrustSec : Compréhension du Cisco TrustSec**
- **Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité**
- **Guide de configuration de la gamme VPN CLI de Cisco ASA, 9.1**
- **Guide de l'utilisateur de Logiciel Cisco Identity Services Engine, version 1.2**
- **Support et documentation techniques - Cisco Systems**

Date du fichier PDF généré: 16 décembre 2015

http://www.cisco.com/cisco/web/support/CA/fr/112/1123/1123544_117694-config-asa-00.html