Exemple de configuration de la classification et de la mise en œuvre du SGT pour le VPN de l'ASA version 9.2

Table des matières

Introduction

Ce document décrit comment utiliser une nouvelle fonctionnalité de la classification SGT (Security Group Tag) TrustSec ASA (Adaptive Security Appliance) version 9.2.1 pour les utilisateurs VPN. Cet exemple présente deux utilisateurs VPN auxquels a été attribué un SGT et un pare-feu de groupe de sécurité (SGFW) différents, qui filtrent le trafic entre les utilisateurs VPN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

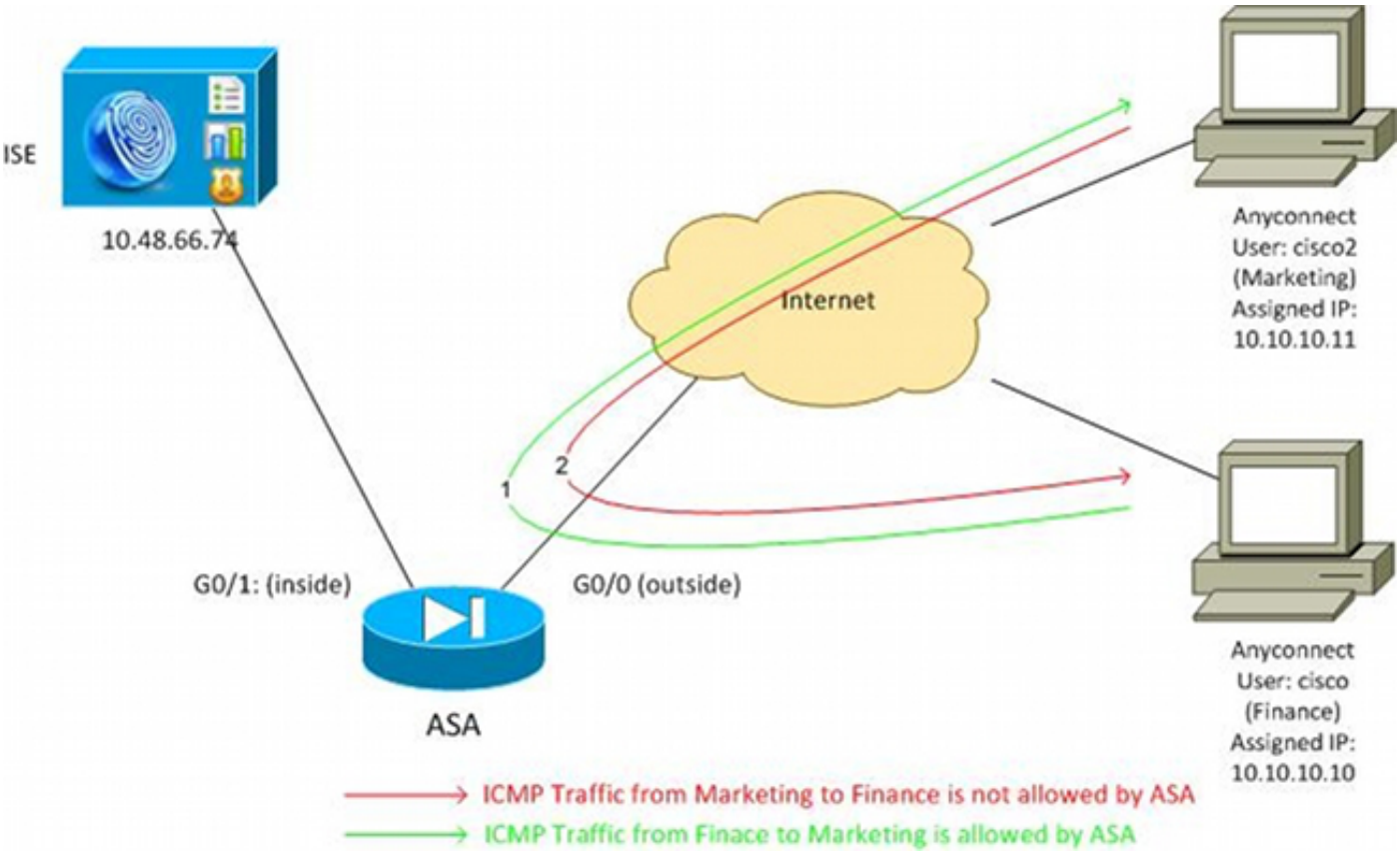
- Logiciel Cisco ASA, versions 9.2 et ultérieures
- Windows 7 avec Cisco AnyConnect Secure Mobility Client, version 3.1
- Cisco ISE, versions 1.2 et ultérieures

Configurer

> **Remarque** : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

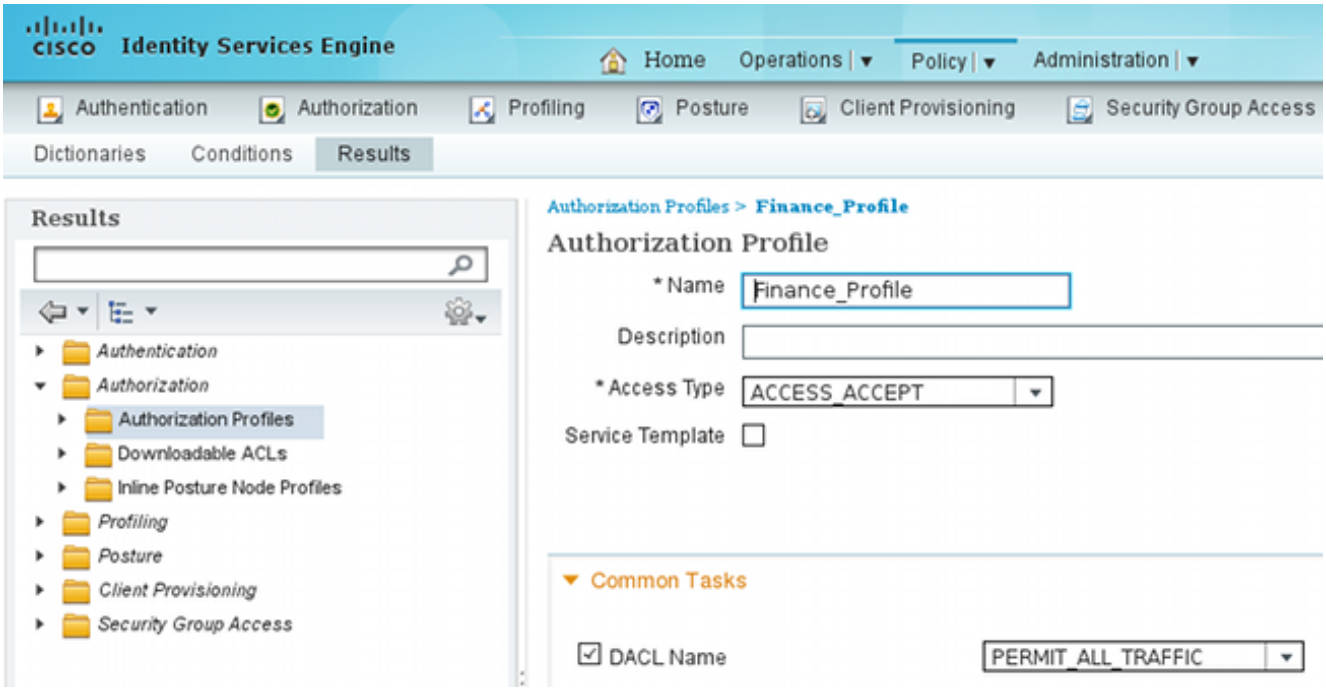
L'utilisateur VPN « cisco » est affecté à l'équipe financière, qui est autorisée à établir une connexion ICMP (Internet Control Message Protocol) avec l'équipe marketing. L'utilisateur VPN « cisco2 » est affecté à l'équipe marketing, qui n'est pas autorisée à établir des connexions.



Configuration ISE

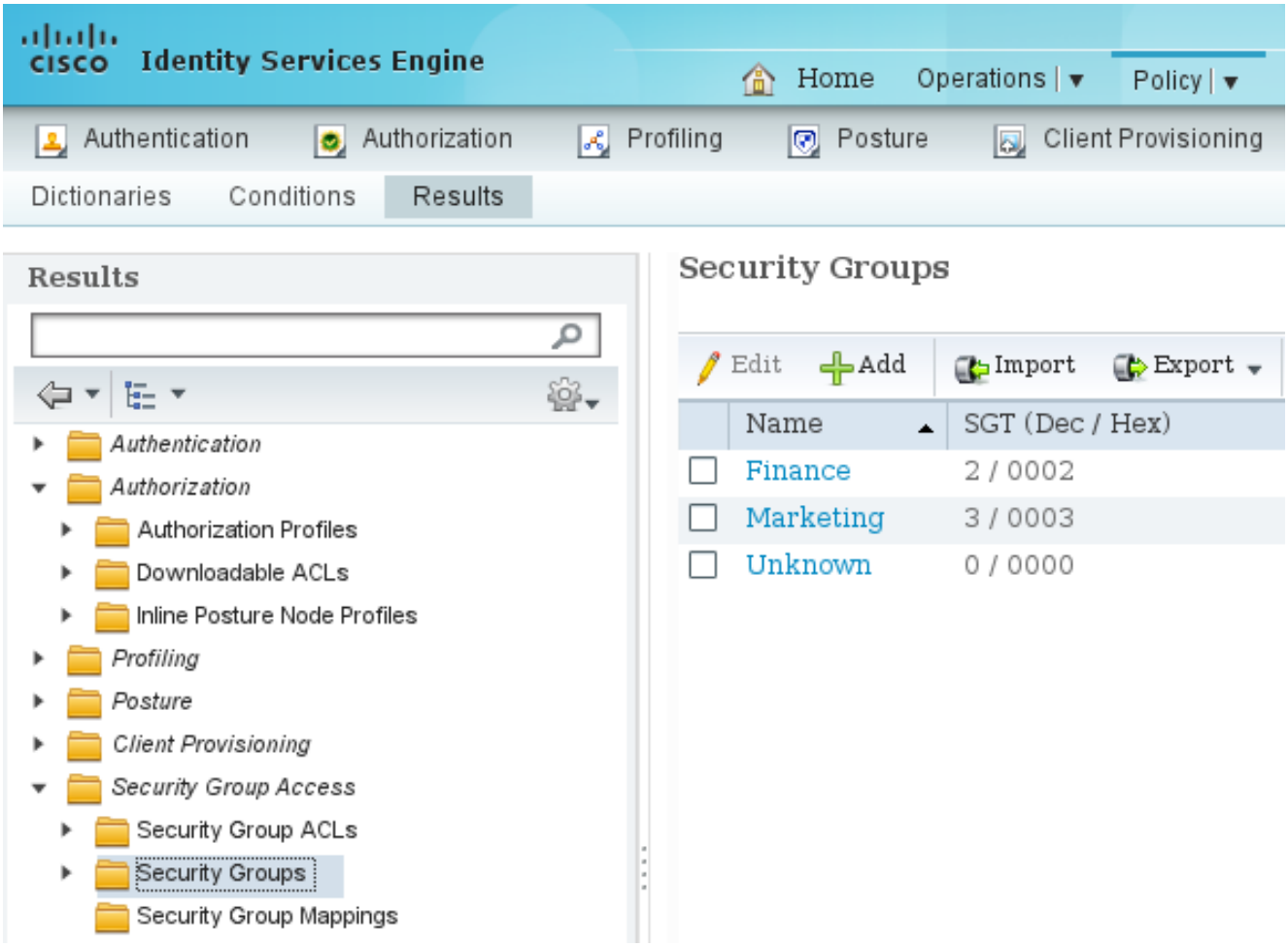
1. Choisissez **Administration > Identity Management > Identities** afin d'ajouter et de configurer l'utilisateur 'cisco' (de Finance) et 'cisco2' (de Marketing).
2. Choisissez **Administration > Network Resources > Network Devices** afin d'ajouter et de configurer l'ASA comme périphérique réseau.
3. Choisissez **Policy > Results > Authorization > Authorization Profiles** afin d'ajouter et de

configurer les profils d'autorisation Finance et Marketing.Les deux profils incluent un seul attribut, la liste de contrôle d'accès téléchargeable (DACL), qui autorise tout le trafic. Un exemple pour Finance est présenté ici
:

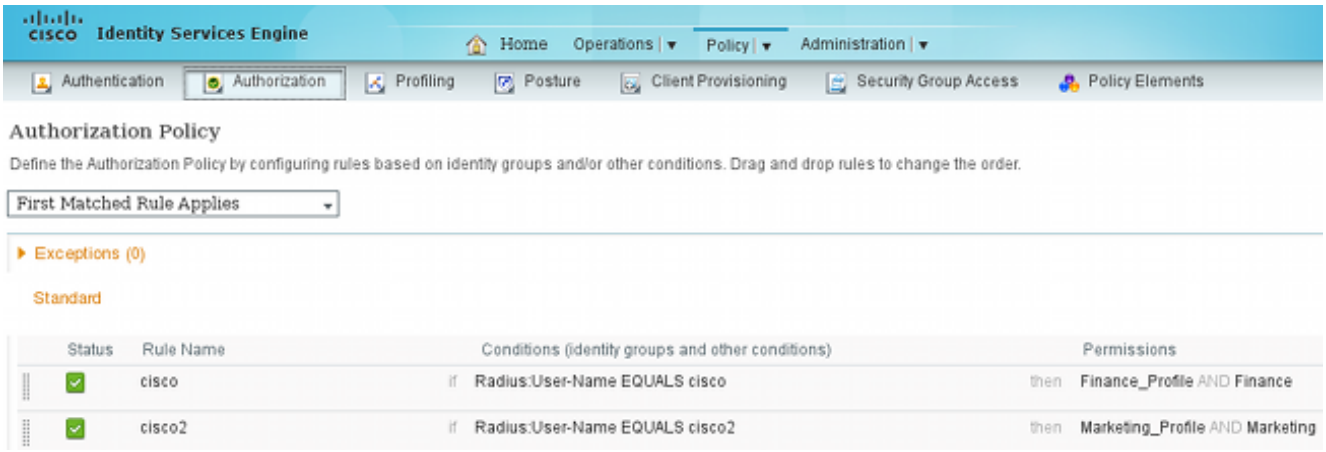


Chaque profil peut avoir une liste de contrôle d’accès spécifique et restrictive, mais pour ce scénario, tout le trafic est autorisé. L'application est effectuée par le SGFW, et non par la DACL attribuée à chaque session VPN. Le trafic filtré avec un SGFW permet d'utiliser uniquement des balises de groupe de sécurité au lieu d'adresses IP utilisées par la liste de contrôle d'accès.

4. Choisissez **Policy > Results > Security Group Access > Security Groups** afin d'ajouter et de configurer les groupes SGT Finance et
Marketing.



5. Choisissez **Policy > Authorization** afin de configurer les deux règles d'autorisation. La première règle attribue le profil Finance_profile (DACL qui autorise le trafic entier) ainsi que le groupe SGT Finance à l'utilisateur « cisco ». La deuxième règle attribue le profil Marketing_profile (DACL qui autorise tout le trafic) ainsi que le groupe SGT Marketing à l'utilisateur « cisco2
»).



Configuration ASA

1. Terminez la configuration 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
```

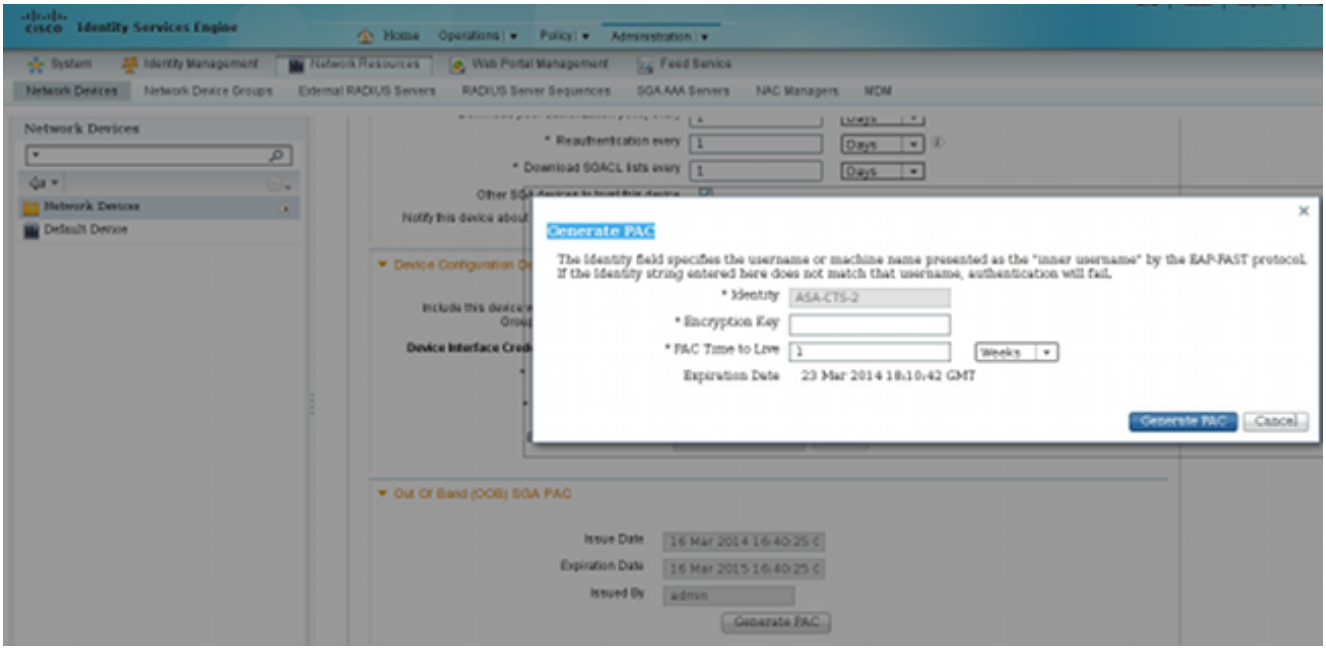
```
group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

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 la configuration ASA AAA et TrustSec.

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

   Pour rejoindre le cloud TrustSec, l'ASA doit s'authentifier avec les informations d'identification d'accès protégé (PAC). L'ASA ne prend pas en charge le provisionnement PAC automatique, c'est pourquoi ce fichier doit être généré manuellement sur l'ISE et importé sur l'ASA.

3. Choisissez **Administration > Network Resources > Network Devices > ASA > Advanced TrustSec Settings** afin de générer un PAC sur l'ISE. Choisissez **Out of Band (OOB) PAC** provisioning afin de générer le fichier.



4. Importez le PAC dans l'ASA.Le fichier généré peut être placé sur un serveur HTTP/FTP. L'ASA l'utilise pour 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:
  000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
  0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
  e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
  2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
  99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
  11d8378829cc007b91ced9117a
```

Lorsque vous disposez du PAC correct, l'ASA effectue automatiquement une actualisation de l'environnement. Les informations relatives aux groupes SGT actuels sont téléchargées à partir de l'ISE.

```
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 consiste à configurer la liste de contrôle d'accès sur l'interface externe qui autorise le trafic ICMP de Finance vers 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 du groupe de sécurité peut être utilisé à la place 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 défaut autorise le trafic VPN sans validation via l'ACL d'interface.

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

L'ASA doit maintenant être prêt à classer les utilisateurs VPN et à appliquer les règles en fonction des balises de groupe de sécurité .

Vérifier

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

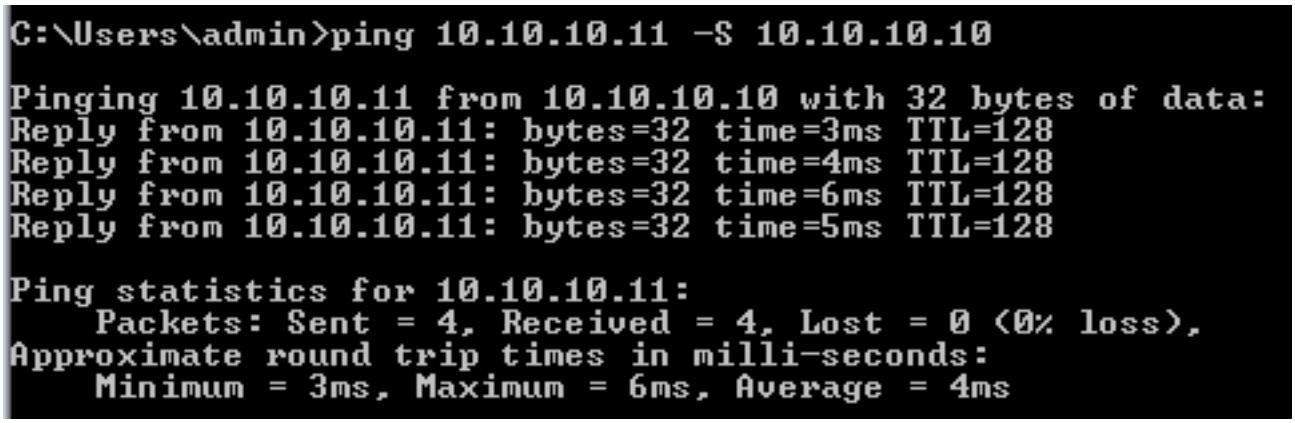
Les Outil Interpréteur de sortie (nominatif clients uniquement) prend en charge certains **être manifeste** de l'assistant. Utilisez l'outil Output Interpreter Tool afin de visualiser une analyse de **être manifeste** résultat de la commande.

Une fois le VPN 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 prend en charge le trafic ICMP de Finance (SGT=2) vers Marketing (SGT=3). C'est pourquoi l'utilisateur « cisco » peut envoyer une requête ping à l'utilisateur « cisco2 ».



Les compteurs augmentent :

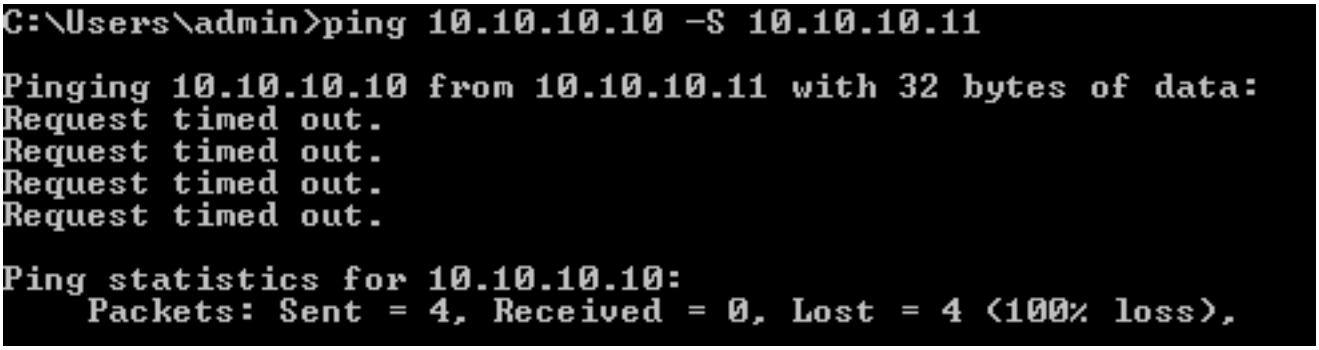
```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
tag 2(name="Finance") any security-group tag 3(name="Marketing")
any (hitcnt=4) 0x071f07fc
```

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 accepté, car l'inspection ICMP est activée.

Lorsque vous essayez d'envoyer une requête ping de Marketing (SGT=3) vers Finance (SGT=2) :



ASA rapporte :

```
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]
```

Dépannage

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

Voir ces documents :

- Exemple de configuration d'un cloud TrustSec avec 802.1x MACsec sur un commutateur de la gamme Catalyst 3750X
- Exemple de configuration de l'ASA et du commutateur Catalyst de la série 3750X TrustSec et guide de dépannage

Résumé

Cet article présente un exemple simple sur la façon de classer les utilisateurs VPN et d'effectuer l'application de base. Le SGFW filtre également le trafic entre les utilisateurs VPN et le reste du réseau. SXP (TrustSec SGT Exchange Protocol) peut être utilisé sur un ASA pour obtenir les informations de mappage entre IP et SGT. Cela permet à un ASA d'effectuer l'application pour tous les types de sessions qui ont été correctement classifiées (VPN ou LAN).

Dans le logiciel ASA, versions 9.2 et ultérieures, l'ASA prend également en charge le changement d'autorisation RADIUS (RFC 5176). Un paquet RADIUS CoA envoyé par ISE après une posture VPN réussie peut inclure cisco-av-pair avec un SGT qui attribue un utilisateur conforme à un groupe différent (plus sécurisé). Pour plus d'exemples, consultez les articles de la section Informations connexes.

Informations connexes

- Posture de la version 9.2.1 VPN ASA avec exemple de configuration de l'ISE
- Exemple de configuration de l'ASA et du commutateur Catalyst de la série 3750X TrustSec et guide de dépannage
- Guide de configuration du commutateur Cisco TrustSec : Présentation de Cisco TrustSec
- Configuration d'un serveur externe pour l'autorisation de l'utilisateur de l'appareil de sécurité

- Guide de configuration du CLI VPN de la série Cisco ASA, 9.1
- Guide de l'utilisateur de la plateforme de services d'identité de Cisco, version 1.2
- 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.