

Configurez l'étiquetage intégré ASA 9.3.1 TrustSec

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[ISE - Configuration Steps](#)

1. [SGT pour des finances et le marketing](#)
2. [ACL de groupe de sécurité pour le marketing > les finances du trafic](#)
3. [ACL obligatoire dans la matrice](#)
4. [Règle d'autorisation pour l'accès VPN assignant SGT = 3 \(vente\)](#)
5. [Règle d'autorisation pour le 802.1x Access assignant SGT = 2 \(finances\)](#)
6. [Ajoutant le périphérique de réseau, générant le PAC pour l'ASA](#)
7. [Ajoutez le périphérique de réseau, configurez le secret pour le ravitaillement automatique PAC de commutateur](#)

[ASA - Configuration Steps](#)

1. [Accès VPN de base](#)
2. [Cts de l'importation PAC et de l'enable](#)
3. [SGACL pour des finances > le marketing du trafic](#)
4. [Cts d'enable sur l'interface interne](#)

[Commutateur - Étapes de configuration](#)

1. [802.1x de base](#)
2. [Configuration et ravitaillement CTS](#)
3. [Cts d'enable sur l'interface à l'ASA](#)

[Vérifier](#)

[Dépanner](#)

[Affectation SGT](#)

[Application sur l'ASA](#)

[Commutez l'application](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser la caractéristique mise en application dans la version 9.3.1 de l'appliance de sécurité adaptable (ASA) - étiquetage intégré de TrustSec. Que la caractéristique permet à l'ASA pour recevoir des trames de TrustSec aussi bien que pour les envoyer. De cette façon ASA peut être facilement intégrée dans le domaine de TrustSec sans nécessité d'utiliser le protocole d'échange de TrustSec SGT (SXP).

Cet exemple présente l'utilisateur distant VPN qui ont été assignés la balise de la balise de groupe de sécurité (SGT) = 3 (vente) et l'utilisateur de 802.1x qui ont été assignés la balise SGT = 2 (des finances). L'application du trafic est exécutée par ASA avec l'utilisation du groupe de sécurité que la liste de contrôle d'accès (SGACL) a défini localement et le commutateur de Cisco IOS® utilisant le rôle a basé la liste de contrôle d'accès (RBACL) téléchargée du Cisco Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration ASA CLI et configuration du VPN de Protocole SSL (Secure Socket Layer)
- Configuration du VPN d'Accès à distance sur l'ASA
- Services ISE et de TrustSec

Composants utilisés

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

- Logiciel de Cisco ASA, version 9.3.1 et ultérieures
- Matériel 55x5 ou ASA v de Cisco ASA
- Windows 7 avec le Client à mobilité sécurisé Cisco AnyConnect, version 3.1
- Commutateur de Cisco Catalyst 3750X avec le logiciel 15.0.2 et plus tard
- Cisco ISE, version 1.2 et ultérieures

Configurer

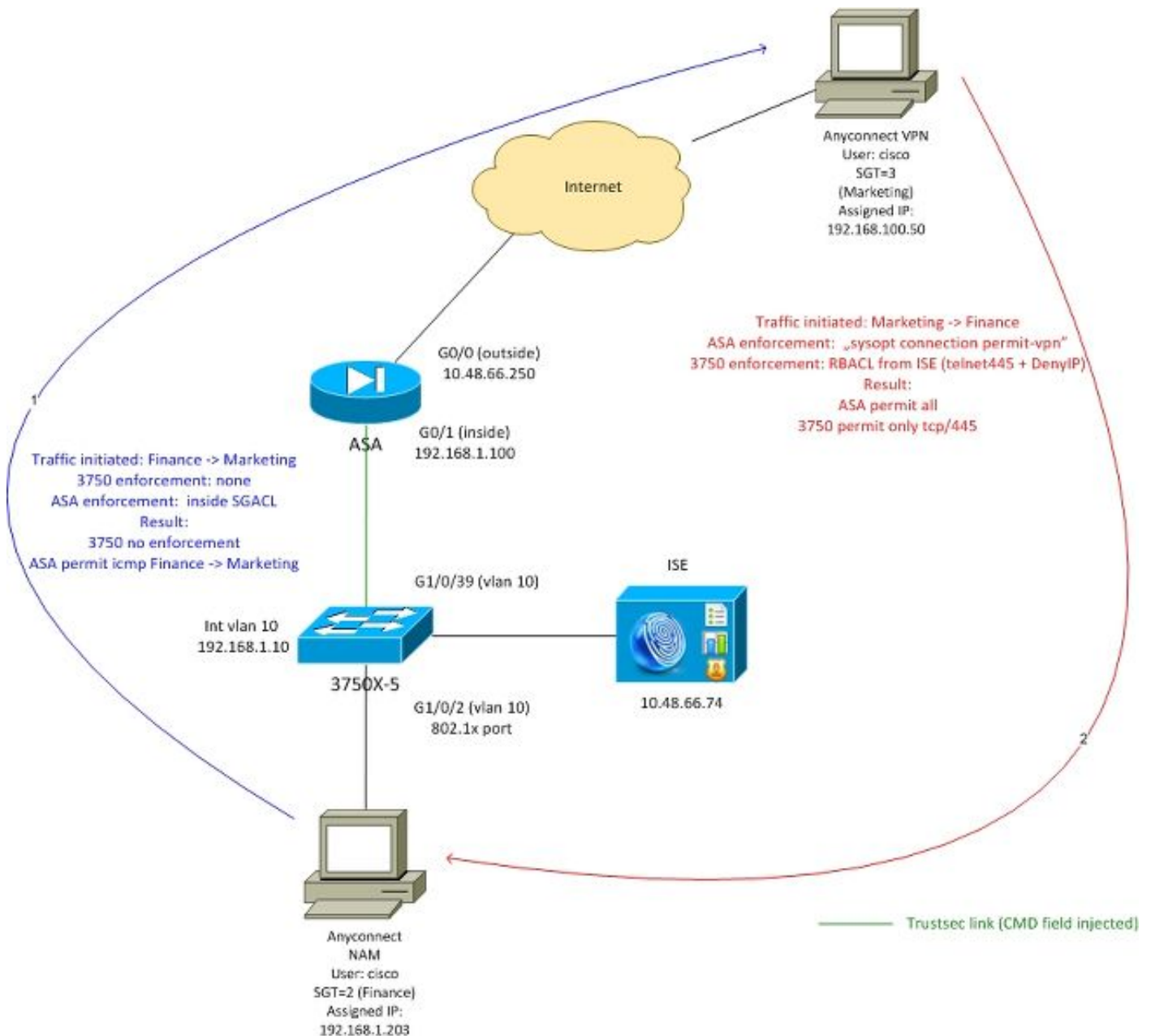
Note: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

La connexion entre l'ASA et le 3750X est configurée pour les cts manuels. Cela signifie que les deux périphériques peuvent envoyer et recevoir les trames Ethernet modifiées avec des métadonnées de Cisco mettez en place (CMD). Ce champ inclut la balise de groupe de sécurité (SGT) qui décrit la source du paquet.

L'utilisateur distant VPN termine la session SSL sur l'ASA et est assigné la balise 3 (vente) SGT.

Utilisateur entreprise local de 802.1x après que l'authentification réussie ait été assignée la balise 2 (finances) SGT.



L'ASA a SGACL configuré sur l'interface interne qui tient compte du trafic d'ICMP initié des finances au marketing.

L'ASA permet tout le trafic initié de retirer l'utilisateur VPN (en raison de la configuration « d'autorisation-VPN de connexion de sysopt »).

SGACL sur l'ASA est l'avec état qui signifie qu'une fois l'écoulement est créé, le paquet de retour est reçu automatiquement (basé sur l'inspection).

3750 utilisations RBACL de commutateur afin de contrôler le trafic reçu du marketing pour financer.

RBACL est sans état qui signifie que chaque paquet est vérifié mais l'application de TrustSec sur la plate-forme 3750X est exécutée à la destination. Ce commutateur de manière est responsable de l'application du trafic du marketing pour financer.

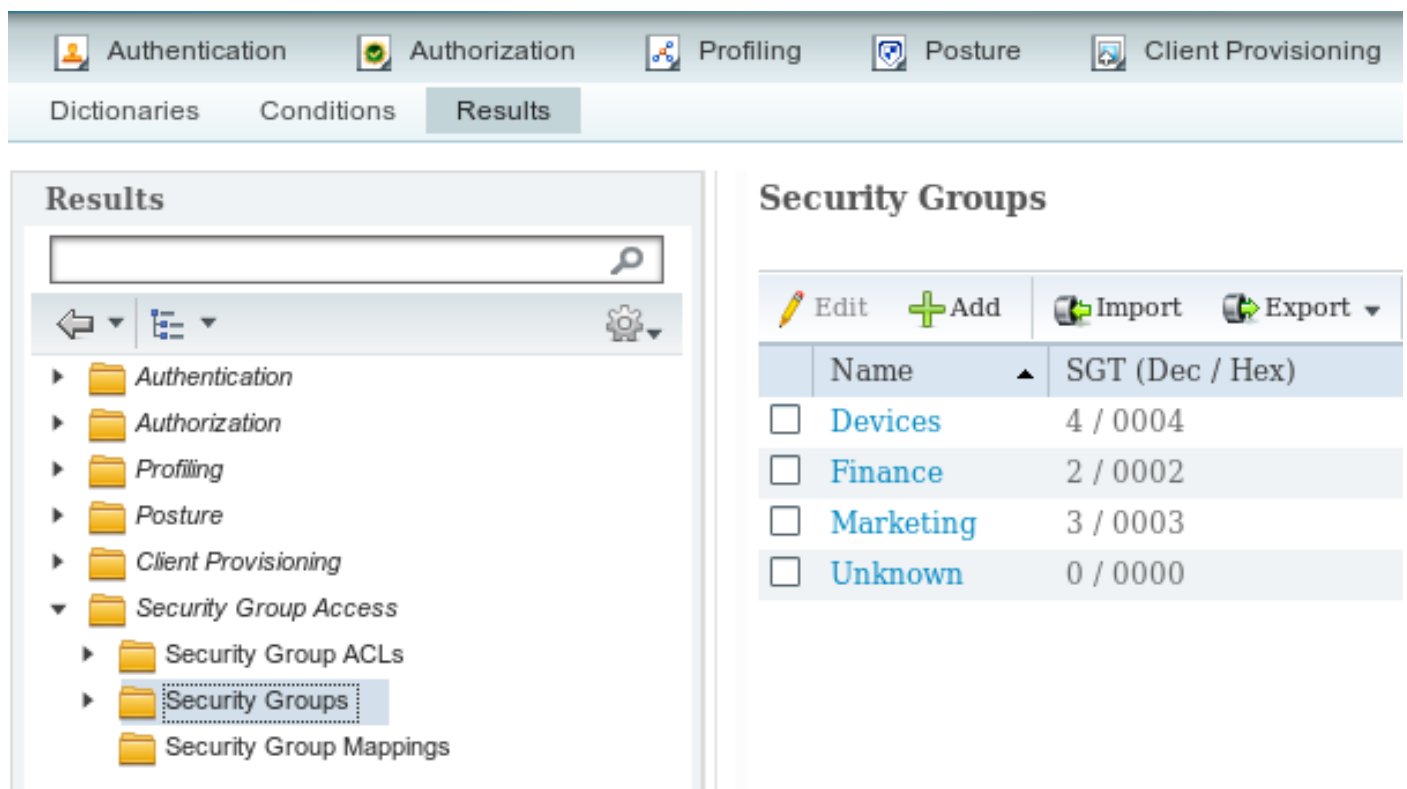
Note: Pour Trustsec le pare-feu dynamique averti sur le Pare-feu basé par zone de Cisco IOS® peut être utilisé, par exemple, référez-vous :

Note: L'ASA pourrait avoir le trafic de contrôle SGACL qui provient l'utilisateur distant VPN. Afin de simplifier le scénario, il n'a pas été présenté en cet article. Par exemple référez-vous : [Exemple de configuration de la classification et de la mise en œuvre du SGT pour le VPN de l'ASA version 9.2](#)

ISE - Configuration Steps

1. SGT pour des finances et le marketing

Naviguez vers la **stratégie > les résultats > le groupe de sécurité Access > groupes de sécurité** et créez SGT pour des finances et le marketing suivant les indications de cette image.



The screenshot shows the ISE configuration interface. At the top, there are tabs for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below these are sub-tabs for Dictionaries, Conditions, and Results. The Results tab is active, showing a search bar and a tree view of the configuration hierarchy. The tree view shows the following structure:

- Authentication
- Authorization
- Profiling
- Posture
- Client Provisioning
- Security Group Access
 - Security Group ACLs
 - Security Groups
 - Security Group Mappings

On the right side, the 'Security Groups' table is displayed with the following data:

	Name	SGT (Dec / Hex)
<input type="checkbox"/>	Devices	4 / 0004
<input type="checkbox"/>	Finance	2 / 0002
<input type="checkbox"/>	Marketing	3 / 0003
<input type="checkbox"/>	Unknown	0 / 0000

2. ACL de groupe de sécurité pour le marketing > les finances du trafic

Naviguez vers l'**ACL de stratégie > de résultats > de groupe de sécurité Access > de groupe de sécurité** et créez l'ACL qui est utilisé pour contrôler le trafic du marketing pour financer. On permet seulement tcp/445 suivant les indications de cette image.

The screenshot displays a network management interface with a top navigation bar containing icons and labels for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below this, a secondary bar shows 'Dictionaries', 'Conditions', and 'Results' tabs, with 'Results' being the active tab.

The main content area is divided into two sections. On the left, a 'Results' sidebar features a search bar and a tree view of configuration categories: Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access (expanded to show Security Group ACLs, Security Groups, and Security Group Mappings), and Security Group Mappings. The 'Security Group ACLs' folder is selected.

On the right, the configuration page for 'telnet445' is shown. It includes a breadcrumb 'Security Groups ACLs List > telnet445' and a title 'Security Group ACLs'. The configuration fields are: 'Name' (telnet445), 'Description' (empty), 'IP Version' (radio buttons for IPv4, IPv6, and an unlabeled one, with IPv4 selected), and 'Security Group ACL content' (permit tcp dst eq 445).

3. ACL obligatoire dans la matrice

Naviguez l'ACL configuré par grippage vers **stratégie > de stratégie > de matrice de sortie** pour la source : **Vente** et destination : **Finances**. Également l'attache **refusent l'IP** comme dernier ACL pour relâcher tout autre trafic suivant les indications de l'image. (sans cette stratégie par défaut sera relié, par défaut est autorisation)

Authentication Authorization Profiling Posture Client Provisioning Security Group Access

Egress Policy Network Device Authorization

Source Tree Destination Tree **Matrix**

Egress Policy (Matrix View)

Edit Add Clear Mapping Configure Push Monitor All Dimension 3X5

Destination Source	Devices (4 / 0004)	Finance (2 / 0002)
Devices (4 / 0004)		
Finance (2 / 0002)		
Marketing (3 / 0003)		<input checked="" type="checkbox"/> Enabled SGACLs: telnet445, Deny IP

4. Règle d'autorisation pour l'accès VPN assignant SGT = 3 (vente)

Naviguez vers la **stratégie > l'autorisation** et créez une règle pour l'accès VPN distant. Toutes les connexions VPN établies par l'intermédiaire du client d'AnyConnect 4.x obtiendront l'accès complet (PermitAccess) et seront assignées la balise 3 (vente) SGT. La condition est d'utiliser l'identité Extentions ([ACIDEX](#)) d'AnyConnect :

```
Rule name: VPN
Condition: Cisco:cisco-av-pair CONTAINS mdm-tlv=ac-user-agent=AnyConnect Windows 4
Permissions: PermitAccess AND Marketing
```

5. Règle d'autorisation pour le 802.1x Access assignant SGT = 2 (finances)

Naviguez vers la **stratégie > l'autorisation** et créez une règle pour l'accès de 802.1x. Le supplicant terminant la session de 802.1x sur le commutateur 3750 avec le nom d'utilisateur **Cisco** obtiendra l'accès complet (PermitAccess) et sera assigné la balise 2 (finances) SGT.

```
Rule name: 802.1x
```

Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance

6. Ajoutant le périphérique de réseau, générant le PAC pour l'ASA

Afin d'ajouter l'ASA au domaine de TrustSec, il est nécessaire de générer le fichier PAC manuellement. Ce fichier est importé sur l'ASA.

Il peut être configuré à partir de : **Administration > Network Devices**. Après que l'ASA soit ajoutée, faites descendre l'écran aux **configurations de TrustSec** et **générez le PAC** suivant les indications de cette image.

Generate PAC X

The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* Identity

* Encryption Key

* PAC Time to Live

Expiration Date 19 Apr 2015 09:06:30 GMT

▼ **Out Of Band (OOB) TrustSec PAC**

Issue Date

Expiration Date

Issued By

Les Commutateurs (3750X) prennent en charge le ravitaillement automatique PAC, de sorte que des étapes doivent être exécutées seulement pour l'ASA qui prend en charge seulement le ravitaillement manuel PAC.

7. Ajoutez le périphérique de réseau, configurez le secret pour le ravitaillement automatique PAC de commutateur

Pour le commutateur qui utilise le ravitaillement automatique PAC, un secret correct doit être placé, suivant les indications de cette image.

Advanced TrustSec Settings

▼ **Device Authentication Settings**

Use Device ID for SGA Identification

Device Id

* Password

Note: Le PAC est utilisé pour authentifier ISE et pour télécharger les données d'environnement (par exemple SGT) avec la stratégie (ACL). L'ASA prend en charge seulement des données d'environnement, des stratégies doit être manuellement configurée sur l'ASA. Le Cisco IOS® prend en charge chacun des deux, ainsi les stratégies peuvent être téléchargées d'ISE.

ASA - Configuration Steps

1. Accès VPN de base

Configurez l'accès de base de VPN SSL pour AnyConnect utilisant ISE pour l'authentification.

```
Rule name: 802.1x
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess ANDFinance
```

2. Cts de l'importation PAC et de l'enable

Importation PAC générée pour l'ASA (d'étape 6 de configuration ISE). Utilisez la même clé de chiffrement :

```
BSNS-ASA5512-4# cts import-pac http://10.229.20.86/asa5512.pac password ciscocisco
PAC Imported Successfully
```

Afin de vérifier :

```
BSNS-ASA5512-4# show cts pac
```

```
PAC-Info:
Valid until: Apr 11 2016 10:16:41
AID:        c2dcb10f6e5474529815aed11ed981bc
I-ID:       asa5512
A-ID-Info:  Identity Services Engine
PAC-type:   Cisco Trustsec
PAC-Opaque:
000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
```



```
25301ffffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ealdca530e24274
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

Cts d'enable :

```
BSNS-ASA5512-4# show cts pac
```

PAC-Info:

```
Valid until: Apr 11 2016 10:16:41
AID:         c2dcb10f6e5474529815aed11ed981bc
I-ID:        asa5512
A-ID-Info:   Identity Services Engine
PAC-type:    Cisco Trustsec
```

PAC-Opaque:

```
000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
25301ffffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ealdca530e24274
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

Après que vous activez des cts, l'ASA doit télécharger des données d'environnement d'ISE :

```
BSNS-ASA5512-4# show cts environment-data
```

CTS Environment Data

=====

```
Status:                Active
Last download attempt: Successful
Environment Data Lifetime: 86400 secs
Last update time:      10:21:41 UTC Apr 11 2015
Env-data expires in:   0:00:37:31 (dd:hr:mm:sec)
Env-data refreshes in: 0:00:27:31 (dd:hr:mm:sec)
```

3. SGACL pour des finances > le marketing du trafic

Configurez SGACL sur l'interface interne. L'ACL laisse initier seulement le trafic d'ICMP des finances au marketing.

```
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
access-group inside in interface inside
```

L'ASA doit développer le nom de la balise pour numéroter :

```
BSNS-ASA5512-4(config)# show access-list inside
```

```
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=47) 0x5633b153
```

4. Cts d'enable sur l'interface interne

Après que vous activez des cts sur l'interface interne de l'ASA :

```
interface GigabitEthernet0/1
 nameif inside
 cts manual
 policy static sgt 100 trusted
 security-level 100
```

```
ip address 192.168.1.100 255.255.255.0
```

L'ASA peut envoyer et recevoir les trames de TrustSec (trames d'Ethernets avec le champ CMD). L'ASA suppose que toutes les trames d'entrée sans balise doivent être traitées comme avec la balise 100. Toutes les trames d'entrée qui incluent déjà la balise sont de confiance.

Commutateur - Étapes de configuration

1. 802.1x de base

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
description windows7
switchport access vlan 10
switchport mode access
authentication host-mode multi-domain
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

Avec cette configuration, après que réussi l'autorisation de 802.1x l'utilisateur (autorisé par l'intermédiaire d'ISE) doit être assignée la balise 2 (finances).

2. Configuration et ravitaillement CTS

De même, quant à l'ASA, des cts est configurés et point à ISE :

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
description windows7
switchport access vlan 10
switchport mode access
authentication host-mode multi-domain
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

En outre, l'application est activée pour Layer3 et Layer2 (tous les VLAN) :

```
aaa new-model

aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
```

```
dot1x system-auth-control
```

```
interface GigabitEthernet1/0/2
description windows7
switchport access vlan 10
switchport mode access
authentication host-mode multi-domain
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
```

```
radius-server host 10.48.66.74 pac key cisco
```

Afin de provision le PAC automatiquement :

```
bsns-3750-5#cts credentials id 3750-5 password ciscocisco
```

De nouveau, le mot de passe doit correspondre à la configuration correspondante sur ISE (périphérique > commutateur > TrustSec de réseau). En ce moment, le Cisco IOS® initie la session d'EAP-FAST avec ISE afin d'obtenir le PAC. Plus de détail sur ce processus peut être trouvé ici :

[Exemple de configuration de l'ASA et du commutateur Catalyst de la série 3750X TrustSec et guide de dépannage](#)

Afin de vérifier si le PAC est installé :

```
bsns-3750-5#show cts pacs
```

```
AID: EA48096688D96EF7B94C679A17BDAD6F
```

```
PAC-Info:
```

```
  PAC-type = Cisco Trustsec
```

```
  AID: EA48096688D96EF7B94C679A17BDAD6F
```

```
  I-ID: 3750-5
```

```
  A-ID-Info: Identity Services Engine
```

```
  Credential Lifetime: 14:41:24 CEST Jul 10 2015
```

```
PAC-Opaque:
```

```
000200B00003000100040010EA48096688D96EF7B94C679A17BDAD6F0006009400030100365AB3133998C86C1BA1B418
968C60690000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
```

```
Refresh timer is set for 4y14w
```

3. Cts d'enable sur l'interface à l'ASA

```
interface GigabitEthernet1/0/39
switchport access vlan 10
switchport mode access
cts manual
  policy static sgt 101 trusted
```

Dorénavant, le commutateur doit être prêt à traiter et envoyer des trames de TrustSec et à imposer les stratégies téléchargées d'ISE.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

La vérification est couverte dans différentes sections de ce document.

Dépanner

Affectation SGT

Après que la session VPN à l'ASA soit établie, l'affectation correcte SGT doit être confirmée :

```
BSNS-ASA5512-4# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : cisco                      Index       : 13
Assigned IP   : 192.168.100.50             Public IP   : 10.229.20.86
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA1
Bytes Tx      : 10308                      Bytes Rx    : 10772
Group Policy  : TAC                        Tunnel Group : TAC
Login Time    : 15:00:13 UTC Mon Apr 13 2015
Duration      : 0h:00m:25s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                        VLAN        : none
Audt Sess ID  : c0a801640000d000552bd9fd
Security Grp  : 3:Marketing
```

Selon l'autorisation ordonne sur ISE, tous les utilisateurs AnyConnect4 a été assigné à la balise de vente.

Les mêmes avec la session de 802.1x sur le commutateur. Après que les finitions du module d'analyse réseau d'AnyConnect (NAM), commutateur d'authentification appliquent la balise correcte retournée d'ISE :

```
bsns-3750-5#show authentication sessions interface g1/0/2 details
```

```
Interface: GigabitEthernet1/0/2
MAC Address: 0050.5699.36ce
IPv6 Address: Unknown
IPv4 Address: 192.168.1.203
User-Name: cisco
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 0A30426D000000130001B278
Acct Session ID: Unknown
Handle: 0x53000002
Current Policy: POLICY_Gi1/0/2
```

```
Local Policies:
```

```
Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure
```

```
Server Policies:
```

```
SGT Value: 2
```

Method status list:

Method	State
dot1x	Authc Success
mab	Stopped

Selon l'autorisation ordonne sur ISE, tous les utilisateurs connectés à ce commutateur doit être assigné à SGT = 2 (des finances).

Application sur l'ASA

Quand vous essayez d'envoyer un trafic des finances (192.168.1.203) à la commercialisation (192.168.100.50), elle frappe l'interface interne de l'ASA. Pour la requête d'écho d'ICMP, il crée la session :

```
Built outbound ICMP connection for faddr 192.168.100.50/0(LOCAL\cisco, 3:Marketing) gaddr 192.168.1.203/1 laddr 192.168.1.203/1(2)
```

et augmente les compteurs d'ACL :

```
BSNS-ASA5512-4(config)# sh access-list
```

```
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-group name Marketing(tag=3) any (hitcnt=138)
```

Cela peut être également confirmé regardant des captures de paquet. Notez que les balises correctes sont affichées :

```
BSNS-ASA5512-4(config)# capture CAP interface inside
BSNS-ASA5512-4(config)# show capture CAP
```

```
1: 15:13:05.736793      INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
2: 15:13:05.772237      INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
3: 15:13:10.737236      INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
4: 15:13:10.772726      INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
```

Il y a requête d'écho entrante d'ICMP étiquetée avec SGT = 2 (des finances) et puis une réponse de l'utilisateur VPN avec lequel est étiqueté par ASA SGT = 3 (vente). Un autre outil de dépannage, traceur de paquets est également TrustSec prêt.

Malheureusement, le PC de 802.1x ne voit pas cette réponse parce qu'elle a bloqué par RBACL sans état sur le commutateur (explication dans la section suivante).

Un autre outil de dépannage, traceur de paquets est également TrustSec prêt. Confirmons si le paquet entrant d'ICMP des finances sera reçu :

```
BSNS-ASA5512-4# packet-tracer input inside icmp inline-tag 2 192.168.1.203 8 0 192.168.100.50
Mapping security-group 3:Marketing to IP address 192.168.100.50
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.48.66.1 using egress ifc outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group name Finance any security-group name Marketing any
Additional Information:

<some output omitted for clarity>

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4830, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: allow

Également essayons d'initier n'importe quelle connexion TCP des finances à la commercialisation, cela doit être bloqué par l'ASA :

```
Deny tcp src inside:192.168.1.203/49236 dst outside:192.168.100.50/445(LOCAL\cisco, 3:Marketing)
by access-group "inside" [0x0, 0x0]
```

Commutez l'application

Vérifions si le commutateur a téléchargé des stratégies d'ISE correctement :

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
    Permit IP-00
IPv4 Role-based permissions from group 2:Finance to group Unknown:
    test_deny-30
```

```
IPv4 Role-based permissions from group 8 to group Unknown:
    permit_icmp-10
IPv4 Role-based permissions from group Unknown to group 2:Finance:
    test_deny-30
    Permit IP-00
IPv4 Role-based permissions from group 3:Marketing to group 2:Finance:
    telnet445-60
    Deny IP-00
```

```
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

La stratégie qui contrôle le trafic du marketing pour financer est installée correctement. On permet seulement tcp/445 selon RBACL :

```
bsns-3750-5#show cts rbacl telnet445
CTS RBACL Policy
=====
RBACL IP Version Supported: IPv4
name      = telnet445-60
IP protocol version = IPV4
refcnt    = 2
flag      = 0x41000000
stale     = FALSE
RBACL ACEs:
    permit tcp dst eq 445
```

C'est la raison pour laquelle la réponse d'écho d'ICMP qui provient le marketing pour financer a été abandonnée. Cela peut être confirmé en vérifiant les compteurs pour le trafic de SGT 3 à SGT 2 :

```
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
*       *       0            0            223613         3645233
0       2       0            0            0              122
3       2       0            65           0              0
2       0       0            0            179            0
8       0       0            0            0              0
```

Des paquets a été lâchés par le matériel (le compteur de courant est 65 et augmentation de chaque 1 seconde).

Ce qui si la connexion tcp/445 est initiée du marketing ?

L'ASA admet que (reçoit tout le trafic VPN en raison de la « connexion autorisation-VPN de sysopt ») :

```
Built inbound TCP connection 4773 for outside:192.168.100.50/49181
(192.168.100.50/49181)(LOCAL\cisco, 3:Marketing) to inside:192.168.1.203/445 (192.168.1.203/445)
(cisco)
```

La session correcte est créée :

```
BSNS-ASA5512-4(config)# show conn all | i 192.168.100.50
```

```
TCP outside 192.168.100.50:49181 inside 192.168.1.203:445, idle 0:00:51, bytes 0, flags UB
```

Et, le Cisco IOS® le reçoit puisqu'il apparie telnet445 RBACL. Les augmentations correctes de compteurs :

```
bsns-3750-5#show cts role-based counters from 3 to 2
```

```
3      2      0      65      0      3
```

(la dernière colonne est le trafic permis par le matériel). On permet la session.

Cet exemple est présenté sur le but afin d'afficher la différence dans des stratégies configuration et application de TrustSec sur l'ASA et le Cisco IOS®. Rendez-vous compte des différences des stratégies de Cisco IOS® téléchargées d'ISE (RBACL sans état) et de Pare-feu basé par zone avertie d'avec état de TrustSec.

[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 TrustSec Cisco : À propos de TrustSec Cisco](#)
- [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](#)
- [Support et documentation techniques - Cisco Systems](#)