

Configurazione dell'etichettatura in linea di TrustSec ASA 9.3.1

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[ISE - Procedura di configurazione](#)

[1. SGT per la finanza e la commercializzazione](#)

[2. ACL del gruppo di sicurezza per Traffic Marketing > Finance](#)

[3. ACL binding in matrice](#)

[4. Regola di autorizzazione per l'accesso VPN che assegna SGT = 3 \(Marketing\)](#)

[5. Regola di autorizzazione per l'accesso 802.1x che assegna SGT = 2 \(Finanza\)](#)

[6. Aggiunta del dispositivo di rete, generazione della PAC per l'ASA](#)

[7. Aggiunta del dispositivo di rete, configurazione del segreto per l'attivazione automatica della PAC dello switch](#)

[ASA - Procedura di configurazione](#)

[1. Accesso VPN di base](#)

[2. Importare PAC e abilitare le cit](#)

[3. SGACL for Traffic Finance > Marketing](#)

[4. Abilita ct sull'interfaccia interna](#)

[Switch - Procedura di configurazione](#)

[1. Base 802.1x](#)

[2. Configurazione e provisioning CTS](#)

[3. Abilitazione delle funzioni ct sull'interfaccia con l'ASA](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Assegnazione SGT](#)

[Applicazione sull'ASA](#)

[Applicazione switch](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come utilizzare la funzione implementata in Adaptive Security Appliance (ASA) release 9.3.1 - Tagging in linea TrustSec. Questa funzione consente all'ASA di ricevere i frame TrustSec e di inviarli. In questo modo, l'ASA può essere facilmente integrata nel dominio TrustSec senza bisogno di usare TrustSec SGT Exchange Protocol (SXP).

In questo esempio viene illustrato un utente VPN remoto a cui è stato assegnato il tag SGT = 3

(Marketing) e un utente 802.1x a cui è stato assegnato il tag SGT = 2 (Finanza). L'imposizione del traffico viene eseguita da ASA con l'uso del SGACL (Security Group Access Control List) definito a livello locale e dallo switch Cisco IOS® con RBACL (Role Based Access Control List) scaricato da Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ASA CLI e configurazione VPN SSL (Secure Sockets Layer)
- Configurazione della VPN di accesso remoto sull'appliance ASA
- Servizi ISE e TrustSec

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco ASA versione 9.3.1 e successive
- Hardware Cisco ASA 55x5 o ASAv
- Windows 7 con Cisco AnyConnect Secure Mobility Client, versione 3.1
- Switch Cisco Catalyst 3750X con software versione 15.0.2 e successive
- Cisco ISE versione 1.2 e successive

Configurazione

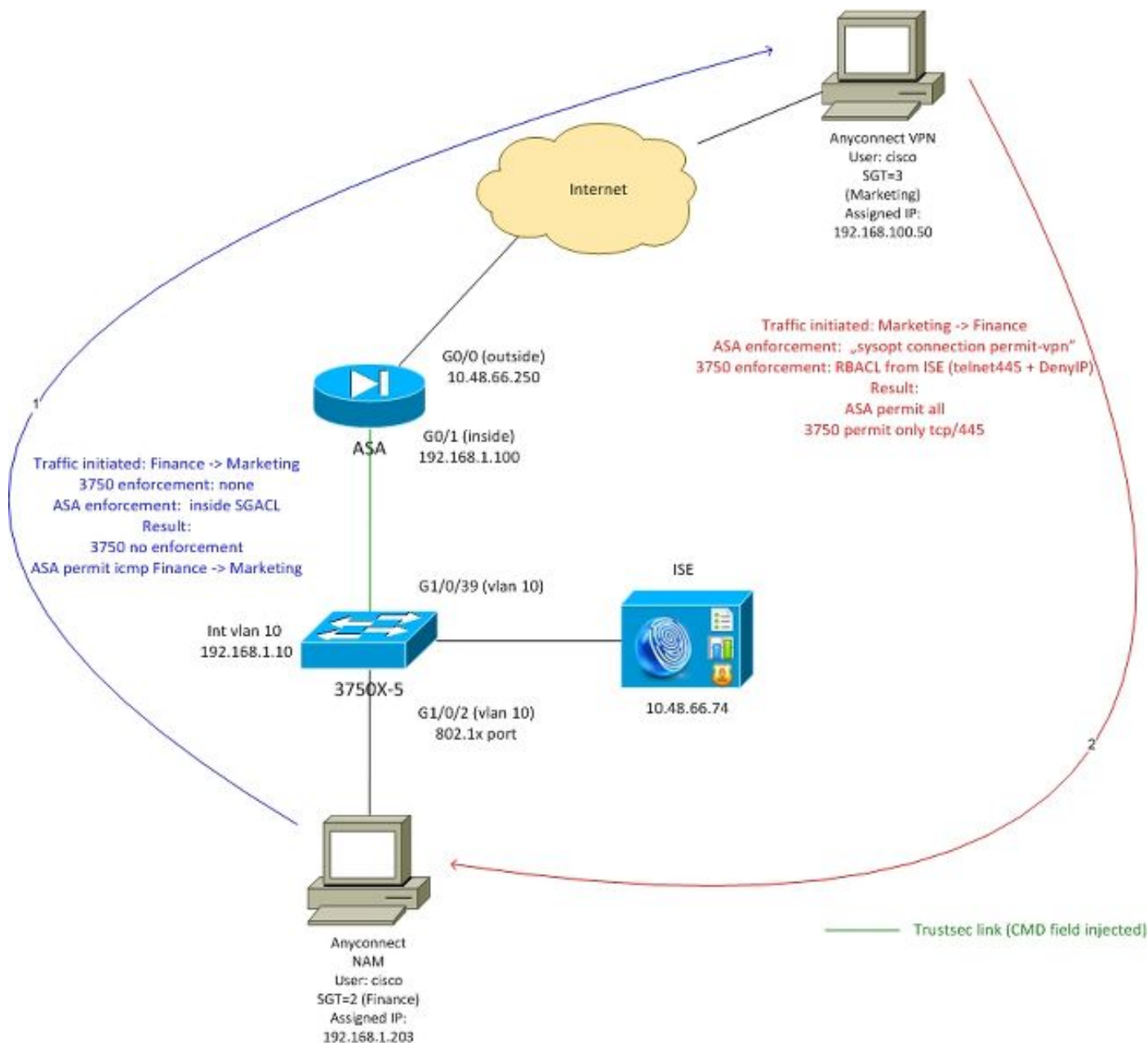
Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi \(solo utenti registrati\)](#).

Esempio di rete

La connessione tra ASA e 3750X è configurata per i collegamenti manuali. Ciò significa che entrambi i dispositivi possono inviare e ricevere frame Ethernet modificati con Cisco Metadata Field (CMD). Il campo include Security Group Tag (SGT), che descrive l'origine del pacchetto.

L'utente VPN remoto termina la sessione SSL sull'appliance ASA e riceve il tag SGT 3 (Marketing).

Utente 802.1x aziendale locale dopo l'assegnazione del tag SGT 2 (Finance).



SGACL è configurato sull'interfaccia interna dell'appliance ASA per consentire il traffico ICMP iniziato dal reparto finanziario al reparto marketing.

L'ASA autorizza tutto il traffico avviato dalla rimozione di un utente VPN (a causa della configurazione "syspot connection allow-vpn").

Il protocollo SGACL sull'appliance ASA è di tipo stateful, quindi una volta creato il flusso, il pacchetto di ritorno viene accettato automaticamente (in base all'ispezione).

Lo switch 3750 utilizza RBACL per controllare il traffico ricevuto dal reparto Marketing e finanza.

RBACL è senza stato, il che significa che ogni pacchetto viene controllato ma l'applicazione TrustSec sulla piattaforma 3750X viene eseguita nella destinazione. In questo modo switch è responsabile dell'applicazione del traffico dal marketing alla finanza.

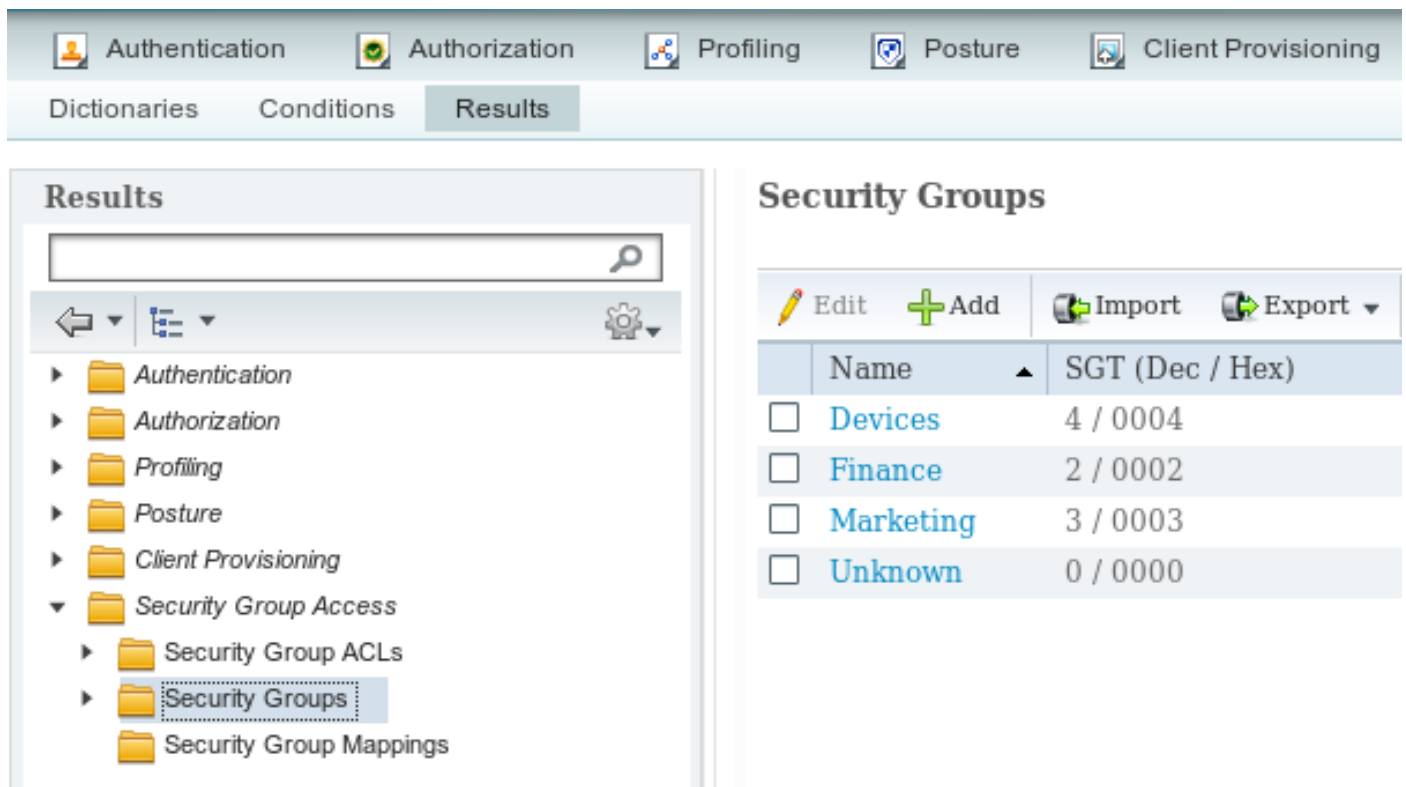
Nota: Per utilizzare un firewall con informazioni sullo stato che supporta Trustsec su un firewall basato su Cisco IOS® Zone, ad esempio, fare riferimento a:

Nota: L'ASA potrebbe avere SGACL che controlla il traffico proveniente dall'utente VPN remoto. Per semplificare lo scenario, non è stato presentato in questo articolo. Ad esempio, consultare: [Esempio di configurazione della classificazione e dell'applicazione VPN SGT di ASA versione 9.2](#)

ISE - Procedura di configurazione

1. SGT per la finanza e la commercializzazione

Passare a **Criterio > Risultati > Accesso al gruppo di sicurezza > Gruppi di sicurezza** e creare SGT for Finance and Marketing come mostrato in questa immagine.



The screenshot displays the Cisco ISE web interface. At the top, there are navigation 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 on the left. The tree view is expanded to 'Security Groups'. On the right, the 'Security Groups' table is visible, listing existing groups: Devices, Finance, Marketing, and Unknown. The table has columns for Name and SGT (Dec / Hex).

	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 del gruppo di sicurezza per Traffic Marketing > Finance

Passare a **Criteri > Risultati > Accesso al gruppo di sicurezza > ACL del gruppo di sicurezza** e creare un ACL utilizzato per controllare il traffico dal reparto marketing a quello finanziario. È consentito solo il protocollo tcp/445, come mostrato nell'immagine.

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 is a secondary bar with 'Dictionaries', 'Conditions', and 'Results' tabs. The 'Results' tab is active, showing a left-hand navigation tree with folders for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access (expanded), Security Group ACLs (selected), Security Groups, and Security Group Mappings. The main content area is titled 'Security Groups ACLs List > telnet445' and 'Security Group ACLs'. It features a form with the following fields: 'Name' (text input containing 'telnet445'), 'Description' (empty text area), 'IP Version' (radio buttons for IPv4, IPv6, and an unlabeled one, with IPv4 selected), and 'Security Group ACL content' (text area containing 'permit tcp dst eq 445').

3. ACL binding in matrice

Passare a **Criterio > Criterio in uscita > Associazione matrice ACL** configurato per l'origine: **Marketing** e destinazione: **Finanza**. Collegare anche **Deny IP** come ultimo ACL che ha rifiutato tutto il traffico, come mostrato nell'immagine. (senza il criterio predefinito che verrà allegato, il valore predefinito è consenti qualsiasi)

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

Source	Destination	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. Regola di autorizzazione per l'accesso VPN che assegna SGT = 3 (Marketing)

Passare a **Criteri > Autorizzazione** e creare una regola per l'accesso VPN remoto. A tutte le connessioni VPN stabilite tramite il client AnyConnect 4.x verrà concesso l'accesso completo (PermitAccess) e verrà assegnato il tag SGT 3 (Marketing). La condizione consiste nell'utilizzare AnyConnect Identity Extentions ([ACIDEX](#)):

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

5. Regola di autorizzazione per l'accesso 802.1x che assegna SGT = 2 (Finanza)

Passare a **Criteri > Autorizzazione** e creare una regola per l'accesso 802.1x. Il richiedente che termina la sessione 802.1x sullo switch 3750 con nome utente **cisco** avrà accesso completo (PermitAccess) e riceverà il tag SGT 2 (Finanza).

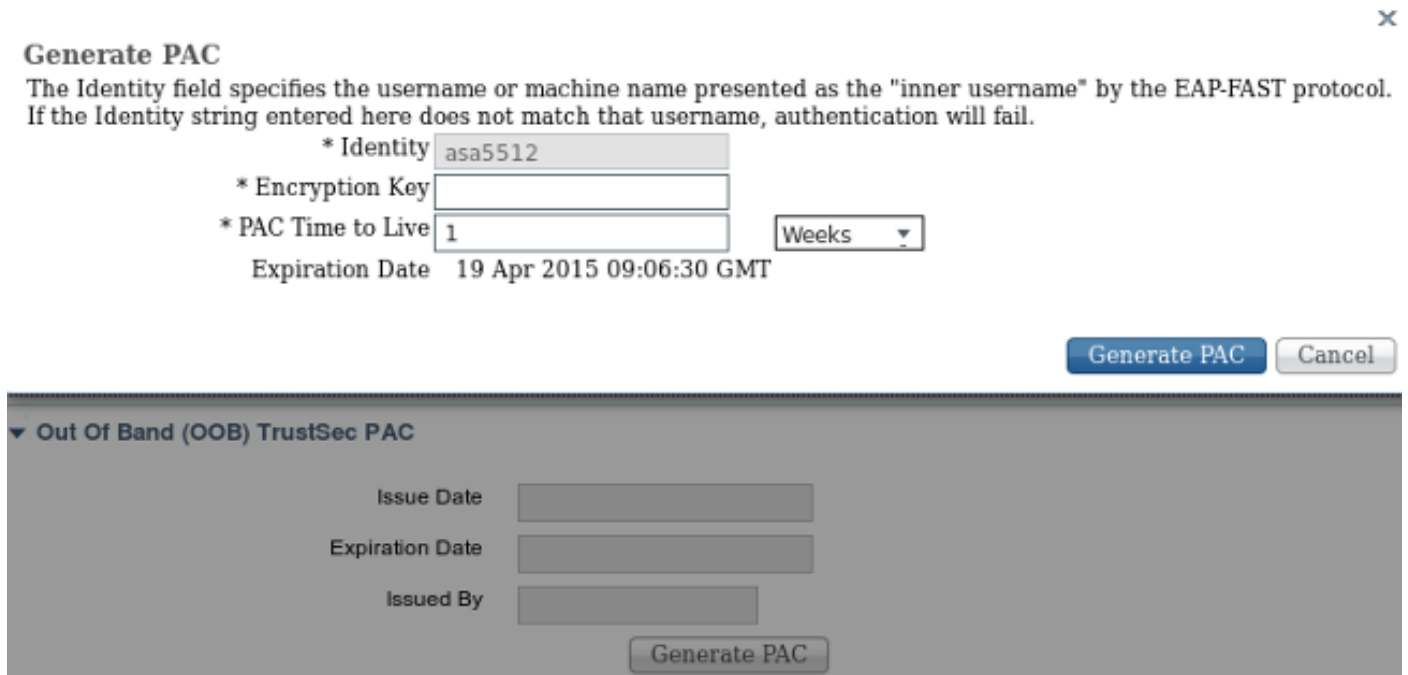
Rule name: 802.1x

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

6. Aggiunta del dispositivo di rete, generazione della PAC per l'ASA

Per aggiungere un'appliance ASA al dominio TrustSec, è necessario generare manualmente il file PAC. Il file viene importato sull'appliance ASA.

Configurabile da **Amministrazione > Dispositivi di rete**. Dopo aver aggiunto l'appliance ASA, scorrere verso il basso fino alle impostazioni TrustSec e generare la PAC, come mostrato nell'immagine.



Generate PAC ✕

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

Gli switch (3750X) supportano la preparazione automatica della PAC, quindi i vari passaggi devono essere eseguiti solo per le appliance ASA che supportano solo la preparazione manuale della PAC.

7. Aggiunta del dispositivo di rete, configurazione del segreto per l'attivazione automatica della PAC dello switch

Per gli switch che utilizzano la preparazione automatica della PAC, è necessario impostare un segreto corretto, come mostrato in questa immagine.

Advanced TrustSec Settings

▼ **Device Authentication Settings**

Use Device ID for SGA Identification

Device Id

* Password

Nota: La PAC viene utilizzata per autenticare l'ISE e scaricare i dati dell'ambiente (ad es. SGT) insieme ai criteri (ACL). L'ASA supporta solo i dati dell'ambiente, le policy devono essere configurate manualmente sull'appliance. Cisco IOS® supporta entrambi, quindi le policy possono essere scaricate da ISE.

ASA - Procedura di configurazione

1. Accesso VPN di base

Configurare l'accesso VPN SSL di base per AnyConnect utilizzando ISE per l'autenticazione.

```

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.62.145.41
key cisco

webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
address-pool (outside) POOL
authentication-server-group ISE
default-group-policy TAC
tunnel-group TAC webvpn-attributes
group-alias TAC enable

ip local pool POOL 192.168.100.50-192.168.100.60 mask 255.255.255.0

```

2. Importare PAC e abilitare le cit

Importazione della PAC generata per l'ASA (dal passaggio 6 della configurazione ISE). Usa la stessa chiave di crittografia:

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


PAC Imported Successfully

Per verificare:

```
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
```

Abilita atti:

```
cts server-group ISE
```

Dopo aver abilitato i cavi, l'ASA deve scaricare i dati dell'ambiente da 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 for Traffic Finance > Marketing

Configurare SGACL sull'interfaccia interna. L'ACL consente di avviare solo il traffico ICMP dal reparto finanziario a quello commerciale.

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

```
access-group inside in interface inside
```

L'appliance ASA deve espandere il nome del tag in numero:

```
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. Abilita ct sull'interfaccia interna

Dopo aver abilitato le funzioni sull'interfaccia interna dell'appliance 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 è in grado di inviare e ricevere frame TrustSec (frame Ethernet con campo CMD). L'ASA presume che tutti i frame in entrata senza tag debbano essere trattati come il tag 100. Tutti i frame in entrata che includono già il tag saranno considerati attendibili.

Switch - Procedura di configurazione

1. Base 802.1x

```
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
```

Con questa configurazione, dopo aver ottenuto l'autorizzazione 802.1x, all'utente (autorizzato tramite ISE) deve essere assegnato il tag 2 (Finance).

2. Configurazione e provisioning CTS

Analogamente, come per l'ASA, il server ECTS è configurato e punta ad ISE:

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

Inoltre, l'imposizione è abilitata sia per il layer 3 sia per il layer 2 (tutte le vlan):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1008-4094
```

Per effettuare il provisioning automatico del PAC:

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

Anche in questo caso, la password deve corrispondere alla configurazione corrispondente su ISE (**Dispositivo di rete > Switch > TrustSec**). Al momento, Cisco IOS® avvia una sessione EAP-FAST con ISE per ottenere la PAC. Per maggiori dettagli su questo processo, consultare:

[Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi](#)

Per verificare se la PAC è installata:

```
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. Abilitazione delle funzioni ct sull'interfaccia con l'ASA

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

Da ora in poi, lo switch deve essere pronto per elaborare e inviare i frame TrustSec e applicare i criteri scaricati da ISE.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

La verifica è trattata nelle singole sezioni del presente documento.

Risoluzione dei problemi

Assegnazione SGT

Dopo aver stabilito la sessione VPN per l'appliance ASA, occorre confermare l'assegnazione corretta del protocollo SGT:

```
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
```

In base alle regole di autorizzazione per ISE, tutti gli utenti AnyConnect4 sono stati assegnati al tag Marketing.

Lo stesso vale per la sessione 802.1x sullo switch. Al termine dell'esecuzione di AnyConnect Network Analysis Module (NAM), lo switch di autenticazione applicherà il tag corretto restituito da 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
```

In base alle regole di autorizzazione per ISE, tutti gli utenti connessi allo switch devono essere assegnati a SGT = 2 (Finanza).

Applicazione sull'ASA

Quando si tenta di inviare un traffico dalla finanza (192.168.1.203) al reparto marketing (192.168.100.50), l'interfaccia dell'ASA viene visualizzata. Per la richiesta echo ICMP, crea la sessione:

```
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)
```

e aumenta i contatori 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)
```

Anche questo può essere confermato osservando le acquisizioni dei pacchetti. Si noti che vengono visualizzati i tag corretti:

```
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
```

È presente una richiesta echo ICMP in arrivo con tag SGT = 2 (Finance) e quindi una risposta dall'utente VPN con tag ASA = 3 (Marketing). Un altro strumento per la risoluzione dei problemi, packet-tracer, è disponibile anche per TrustSec.

Sfortunatamente, il PC 802.1x non legge questa risposta perché è bloccato da un RBACL stateless sullo switch (vedere la spiegazione nella sezione successiva).

Un altro strumento per la risoluzione dei problemi, packet-tracer, è disponibile anche per TrustSec. Confermiamo se il pacchetto ICMP in entrata proveniente dal reparto finanziario verrà accettato:

```
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

Proviamo anche ad avviare una connessione TCP da Finance a Marketing, che deve essere bloccata dall'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]
```

Applicazione switch

Verifichiamo se lo switch ha scaricato correttamente le policy da ISE:

```
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
```

Il criterio che controlla il traffico dal reparto Marketing a quello finanziario è installato correttamente. È consentito solo tcp/445 come per 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
```

Ecco perché la risposta echo ICMP proveniente da Marketing e Finanza è stata scartata. Ciò può essere confermato controllando i contatori per il traffico da SGT 3 a 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
```

I pacchetti sono stati scartati dall'hardware (il contatore corrente è 65 e aumenta ogni 1 secondo).

Cosa succede se la connessione tcp/445 viene avviata dal reparto marketing?

L'ASA permette che (accetta tutto il traffico VPN a causa di "sysost connection allow-vpn"):

```
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)
```

Viene creata la sessione corretta:

```
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
```

Inoltre, Cisco IOS® lo accetta poiché corrisponde a telnet445 RBACL. Aumentano i contatori corretti:

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

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

(l'ultima colonna indica il traffico consentito dall'hardware). Sessione consentita.

Questo esempio viene presentato appositamente per mostrare la differenza nella configurazione e nell'applicazione dei criteri TrustSec su ASA e Cisco IOS®. Tieni presente le differenze tra i criteri Cisco IOS® scaricati da ISE (RBACL senza informazioni sullo stato) e il firewall basato su zona con visibilità TrustSec.

Informazioni correlate

- [Esempio di postura di VPN con ISE versione 9.2.1 di ASA](#)
- [Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi](#)
- [Guida alla configurazione dello switch Cisco TrustSec: Informazioni su Cisco TrustSec](#)
- [Configurazione di un server esterno per l'autorizzazione utente di Security Appliance](#)

- [Guida alla configurazione di Cisco ASA VPN CLI, 9.1](#)
- [Guida dell'utente di Cisco Identity Services Engine, versione 1.2](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)