

# ASA 9.3.1 TrustSec インライン タギング - 設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ISE：設定手順](#)

- [1. 財務およびマーケティングの SGT](#)
- [2. マーケティングから財務へのトラフィックに対するセキュリティグループ ACL](#)
- [3. マトリクス形式の ACL バインディング](#)
- [4. SGT = 3 \( マーケティング \) を割り当てる、VPN アクセスに対する認証ルール](#)
- [5. SGT = 2 \( 財務 \) を割り当てる、802.1x アクセスに対する認証ルール](#)
- [6. ネットワーク デバイスの追加および ASA の PAC 生成](#)
- [7. ネットワーク デバイスの追加およびスイッチ自動 PAC プロビジョニングのシークレット設定](#)

[ASA：設定手順](#)

- [1. 基本的な VPN アクセス](#)
- [2. PAC のインポートおよび cts の有効化](#)
- [3. 財務からマーケティングへのトラフィックに対する SGACL](#)
- [4. 内部インターフェイス上での cts の有効化](#)

[スイッチ：設定手順](#)

- [1. 基本的な 802.1x](#)
- [2. CTS の設定およびプロビジョニング](#)
- [3. インターフェイス上での ASA に対する cts の有効化](#)

[トラブルシューティング](#)

[SGT 割り当て](#)

[ASA での適用](#)

[スイッチでの適用](#)

[参考資料](#)

[Cisco サポート コミュニティ - 特集対話](#)

## 概要

このドキュメントでは、適応型セキュリティ アプライアンス ( ASA ) リリース 9.3.1 に実装された TrustSec インライン タギング機能を使用する方法を説明します。この機能を使用することで、ASA は TrustSec フレームを送受信できるようになります。したがって、TrustSec SGT Exchange Protocol ( SXP ) を使用せずに、ASA を簡単に TrustSec ドメインに統合できます。

この例では、リモート VPN ユーザにはセキュリティグループ タグ ( SGT ) = 3 ( マーケティング ) が割り当てられ、802.1x ユーザには SGT = 2 ( 財務 ) が割り当てられます。ローカルに定義

されたセキュリティ グループ アクセス コントロール リスト ( SGACL ) を使用する ASA と、 Identity Services Engine ( ISE ) からダウンロードしたロール ベース アクセス コントロール リスト ( RBACL ) を使用する IOS スイッチの両方によって、トラフィックにセキュリティ ポリシーが適用されます。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- ASA CLI 設定およびセキュア ソケット レイヤ ( SSL ) VPN 設定に関する基本的な知識
- ASA でのリモート アクセス VPN 設定に関する基本的な知識
- Identity Services Engine ( ISE ) および TrustSec サービスに関する基本的な知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco ASA ソフトウェア バージョン 9.3.1 以降
- Cisco ASA ハードウェア 55x5 または ASA v
- Cisco AnyConnect Secure Mobility Client リリース 3.1 がインストールされた Windows 7
- ソフトウェア 15.0.2 以降がインストールされた Cisco Catalyst 3750X スイッチ
- Cisco ISE リリース 1.2 以降

## 設定

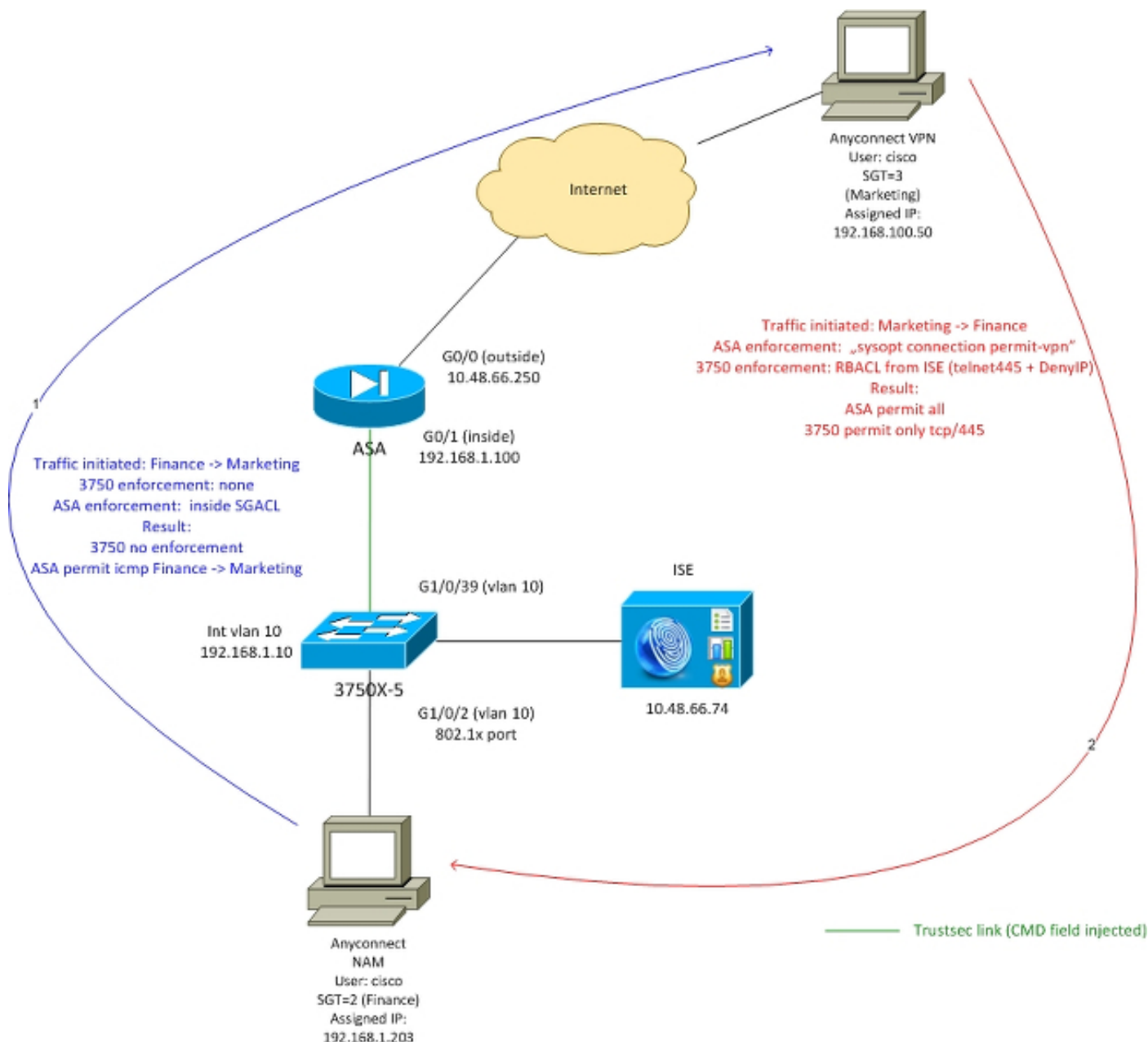
注: このセクションで使用されているコマンドの詳細を調べるには、 [Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

### ネットワーク図

ASA と 3750X 間の接続は、手動 cts 用に設定されています。これは、両方のデバイスが、Cisco メタデータ フィールド ( CMD ) を使用して、変更されたイーサネット フレームを送受信できることを意味します。このフィールドには、パケットの送信元を表す SGT タグが含まれます。

ASA での SSL セッションを終了するリモート VPN ユーザには、SGT タグ 3 ( マーケティング ) が割り当てられます。

ローカルの社内 802.1x ユーザには、認証に成功した後、SGT タグ 2 ( 財務 ) が割り当てられません。



ASA の内部インターフェイスに設定されている SGACL では、財務からマーケティングに対する ICMP トラフィックが許可されます。

ASA は、(「sysopt connection permit-vpn」設定により) リモート VPN ユーザから開始されたすべてのトラフィックを許可します。

ASA 上の SGACL はステートフルです。つまり、フローが作成されると、(検査に基づき) 戻りパケットが自動的に受け入れられます。

3750 スイッチでは RBACL を使用して、マーケティングから送信されて財務で受信するトラフィックを制御します。

RBACL はステートレスです。これは、すべてのパケットがチェックされることを意味します。ただし、3750X プラットフォームでの TrustSec 適用は宛先で行われます。したがって、マーケティングから財務へのトラフィックには、スイッチによって TrustSec が適用されます。

注：

IOS での TrustSec 対応ステートフル ファイアウォールには、ゾーンベース ファイアウォールを

使用できます。例については、以下を参照してください。

注：

ASA の SGACL でリモート VPN ユーザからのトラフィックを制御することもできます。シナリオを単純化するために、このドキュメントではその方法については紹介しません。例については、以下を参照してください。

## [ASA バージョン 9.2 の VPN SGT の分類と適用の設定例](#)

### ISE : 設定手順

#### 1. 財務およびマーケティングの SGT

[Policy] -> [Results] -> [Security Group Access] -> [Security Groups] に移動して、財務およびマーケティングの SGT を作成します。

The screenshot shows the Cisco ISE Results page. The top navigation bar includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below this, there are tabs for Dictionaries, Conditions, and Results. The Results tab is active. On the left, a tree view shows the navigation structure, with Security Groups selected under Security Group Access. On the right, the Security Groups table is displayed with columns for Name and SGT (Dec / Hex). The table lists four groups: Devices, Finance, Marketing, and Unknown.

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. マーケティングから財務へのトラフィックに対するセキュリティ グループ ACL

[Policy] -> [Results] -> [Security Group Access] -> [Security Group ACL] に移動して、マーケティングから財務へのトラフィックを制御するために使用する ACL を作成します。tcp/445 だけを許可します。

The screenshot displays a network management interface with a top navigation bar containing icons 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, 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' (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. マトリクス形式の ACL バインディング

[Policy] -> [Egress Policy] -> [Matrix] に移動して、送信先 : マーケティング、宛先 : 財務に対して設定済みの ACL をバインドします。また、他のすべてのトラフィックをドロップするために、最終 ACL として拒否 IP を関連付けます ( これを行わない場合、デフォルト ポリシーが関連付けられます。デフォルトは permit any です )。

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. SGT = 3 ( マーケティング ) を割り当てる、VPN アクセスに対する認証ルール

[Policy] -> [Authorization] に移動して、リモート VPN アクセスに対するルールを作成します。AnyConnect 4.x クライアントによって確立されたすべての VPN 接続にはフル アクセス ( PermitAccess ) を与え、SGT タグ 3 ( マーケティング ) を割り当てます。条件では AnyConnect Identity Extentions ( [ACIDEX](#) ) を使用します。

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

#### 5. SGT = 2 ( 財務 ) を割り当てる、802.1x アクセスに対する認証ルール

[Policy] -> [Authorization] に移動して、802.1x アクセスに対するルールを作成します。3750 スイッチ上で 802.1x セッションを終了する、ユーザ名 cisco のサブリカントにはフル アクセス ( PermitAccess ) が付与され、SGT タグ 2 ( 財務 ) が割り当てられます。

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. ネットワーク デバイスの追加および ASA の PAC 生成

ASA を TrustSec ドメインに追加するには、PAC ファイルを手動で生成する必要があります。そのファイルが ASA にインポートされます。

これを設定するには、[Administration] -> [Network Devices] に移動します。ASA を追加した後、[TrustSec] 設定までスクロール ダウンして、PAC を生成します。

✕

### 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

スイッチ (3750X) では自動 PAC プロビジョニングをサポートしているため、上記の手順は、手動 PAC プロビジョニングだけをサポートする ASA に対してのみ実行する必要があります。

## 7. ネットワーク デバイスの追加およびスイッチ自動 PAC プロビジョニングのシークレット設定

自動 PAC プロビジョニングを使用するスイッチでは、正しいシークレットの設定のみが必要です。

▼ Advanced TrustSec Settings

▼ Device Authentication Settings

Use Device ID for SGA Identification

Device Id

\* Password

注：

PAC は ISE に対する認証と環境データ (SGT など) およびポリシー (ACL) のダウンロードに使用されます。ASA では環境データのみがサポートされるため、ASA には手動でポリシーを設定する必要があります。IOS ではどちらもサポートされるため、ISE からポリシーをダウンロードできます。

## ASA : 設定手順

### 1. 基本的な VPN アクセス

ISE を使用して認証する、AnyConnect の基本的な SSL VPN アクセスを設定します。

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

### 2. PAC のインポートおよび cts の有効化

ASA 用に生成した PAC (ISE 設定のステップ 6) をインポートします。同じ暗号キーを使用します。

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

確認するには、次のコマンドを実行します。

```
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
25301ffffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

cts を有効にします。

```
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
25301ffffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
```



```
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

cts を有効にした後で、ASA が ISE から環境データをダウンロードする必要があります。

```
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. 財務からマーケティングへのトラフィックに対する SGACL

内部インターフェイスに SGACL を設定します。この ACL では、財務からマーケティングへの ICMP トラフィックのみの開始が許可されます。

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

ASA はタグの名前を番号に展開する必要があります。

```
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. 内部インターフェイス上での cts の有効化

ASA の内部インターフェイスで cts を有効にした後、以下のコマンドを実行します。

```
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
```

これで、ASA は TrustSec フレーム ( CMD フィールドを持つイーサネット フレーム ) を送受信できるようになります。ASA は、タグのないすべての入力フレームをタグ 100 のフレームとして処理する必要があると想定します。タグがすでに組み込まれている入力フレームはすべて信頼されます。

## スイッチ：設定手順

### 1. 基本的な 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
```

上記の設定により、802.1x 認証が成功すると、( ISE によって許可された ) ユーザにタグ 2 ( 財務 ) が割り当てられます。

## 2. CTS の設定およびプロビジョニング

同様に、ASA についても cts を設定し、ISE を参照させます。

```
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
```

また、レイヤ 3 とレイヤ 2 の両方 ( すべての VLAN ) に対してポリシー適用を有効にします。

```
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
```

PAC を自動的にプロビジョニングするには、以下のようにします。

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

この場合も、パスワードが ISE 上の対応する設定 ( [Network Device] -> [Switch] -> [TrustSec] ) と一致する必要があります。現時点で、IOS は ISE との EAP-FAST セッションを開始して、PAC を取得します。このプロセスの詳細については、以下を参照してください。

## [ASA および Catalyst 3750X シリーズ スイッチ TrustSec の設定例およびトラブルシューティングガイド](#)

PAC がインストールされているかどうかを確認するには、以下のコマンドを実行します。

```
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. インターフェイス上での ASA に対する cts の有効化

```
interface GigabitEthernet1/0/39
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
cts manual
```

```
policy static sgt 101 trusted
```

これで、スイッチが TrustSec フレームを処理して送信し、ISE からダウンロードされたポリシーを適用できるようになりました。

## トラブルシューティング

### SGT 割り当て

ASA との VPN セッションが確立された後、SGT が正しく割り当てられることを確認する必要があります。

```
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**

ISE 上の認証ルールによると、すべての AnyConnect4 ユーザにはマーケティング タグが割り当てられています。

これは、スイッチ上の 802.1x セッションにも当てはまります。AnyConnect NAM が認証を完了した後は、スイッチが ISE から返された正しいタグを適用します。

```
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
<b>dot1x</b>	<b>Authc Success</b>
mab	Stopped

ISE 上の認証ルールによると、そのスイッチに接続されたすべてのユーザには SGT = 2 (財務) が割り当てられているはずですが。

## ASA での適用

財務 ( 192.168.1.203 ) からマーケティング ( 192.168.100.50 ) にトラフィックを送信しようとする、そのトラフィックは ASA の内部インターフェイスに到達します。ICMP エコー要求に対してセッションが作成され、

```
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)
```

ACL カウンタが増分されます。

```
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)
```

これは、パケットキャプチャを調べることで確認できます。正しいタグは、次のように表示されることに注意してください。

```
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
```

SGT = 2 ( 財務 ) のタグが付けられた着信 ICMP エコー要求と、ASA によって SGT = 3 ( マーケティング ) のタグが付けられた VPN ユーザからの応答があります。別のトラブルシューティング ツールとして、パケットトレーサも TrustSec に対応しています。

ただし、802.1x PC では応答を確認できません。スイッチ上のステートレス RBACL によって応答がブロックされるためです ( 次のセクションで説明します )。

別のトラブルシューティング ツールとして、パケットトレーサも TrustSec に対応しています。財務からの着信 ICMP パケットが受け入れられるかどうか確認します。

```
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**

また、財務からマーケティングへの TCP 接続を開始して、この接続試行が ASA によってブロックされることを確認します。

```
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]
```

## スイッチでの適用

スイッチが ISE から正常にポリシーをダウンロードしたことを確認します。

```
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
```

マーケティングから財務へのトラフィックを制御するポリシーは、正しくインストールされています。RBACL に従って、tcp/445 だけが許可されます。

```
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
```

これが、マーケティングから財務への ICMP エコー応答はドロップされた理由です。これを確認するには、SGT 3 から SGT 2 へのトラフィックのカウンタをチェックします。

```
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
```

パケットはハードウェアによってドロップされています ( 現行のカウンタ値は 65 で、この値は 1 秒ごとに増分しています )。

tcp/445 接続をマーケティングから開始した場合にはどうなるでしょうか。

ASA はその接続を許可します ( 「sysopt connection permit-vpn」により、すべての VPN トラフィックを受け入れます )。

```
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)
```

正しいセッションが確立されます。

```
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
```

また、telnet445 RBACL と一致することから、IOS も受け入れます。正しいカウンタが増分されます。

```
bsns-3750-5#show cts role-based counters from 3 to 2
3         2         0           65          0              3
```

(最後の列はハードウェアによって許可されたトラフィックを示します)。セッションは許可されます。

この例は、ASA と IOS での TrustSec ポリシーの設定および適用の違いを説明する目的で記載しています。また、ISE からダウンロードされる IOS ポリシー ( ステートレス RBACL ) と TrustSec 対応のステートフルなゾーンベース ファイアウォールとの違いにも注意してください。

## 参考資料

- [ASA バージョン 9.2.1 VPN ポスチャおよび ISE の設定例](#)
- [ASA および Catalyst 3750X シリーズ スイッチ TrustSec の設定例およびトラブルシューティングガイド](#)
- [Cisco TrustSec スイッチ コンフィギュレーション ガイド Cisco TrustSec について](#)

- [セキュリティ アプライアンスのユーザ承認用の外部サーバの設定](#)
- [Cisco ASA シリーズ VPN CLI 構成ガイド 9.1](#)
- [『Cisco Identity Services Engine User Guide, Release 1.2 \( Cisco Identity Services Engine ユーザ ガイド リリース 1.2 \)』](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)