設定 ASA 9.3.1 TrustSec インライン タギング

目次

概要

この資料に適応型セキュリティ アプライアンス (ASA) ソフトウェア設定されるで機能を (ASA) リリース使用する方法を 9.3.1 - TrustSec インライン タギング記述されています。 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。 トラフィック適

用は基づいたアクセス制御リスト ロールのを使用してローカルでおよび Cisco IOS ® スイッチ Identity Services Engine （ ISE ）からダウンロードされる（ RBACL ）定義されるセキュリティグループ アクセス制御リスト（ SGACL ）の使用の ASA によって実行された。

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
- ASA のリモートアクセス VPN 設定
- ISE および TrustSec サービス

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 および それ 以降
- Cisco ASA ハードウェア 55x5 か ASAv
- Cisco AnyConnect セキュア モビリティ クライアントが付いている Windows 7、リリース 3.1
- 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 およびそれ以降

設定

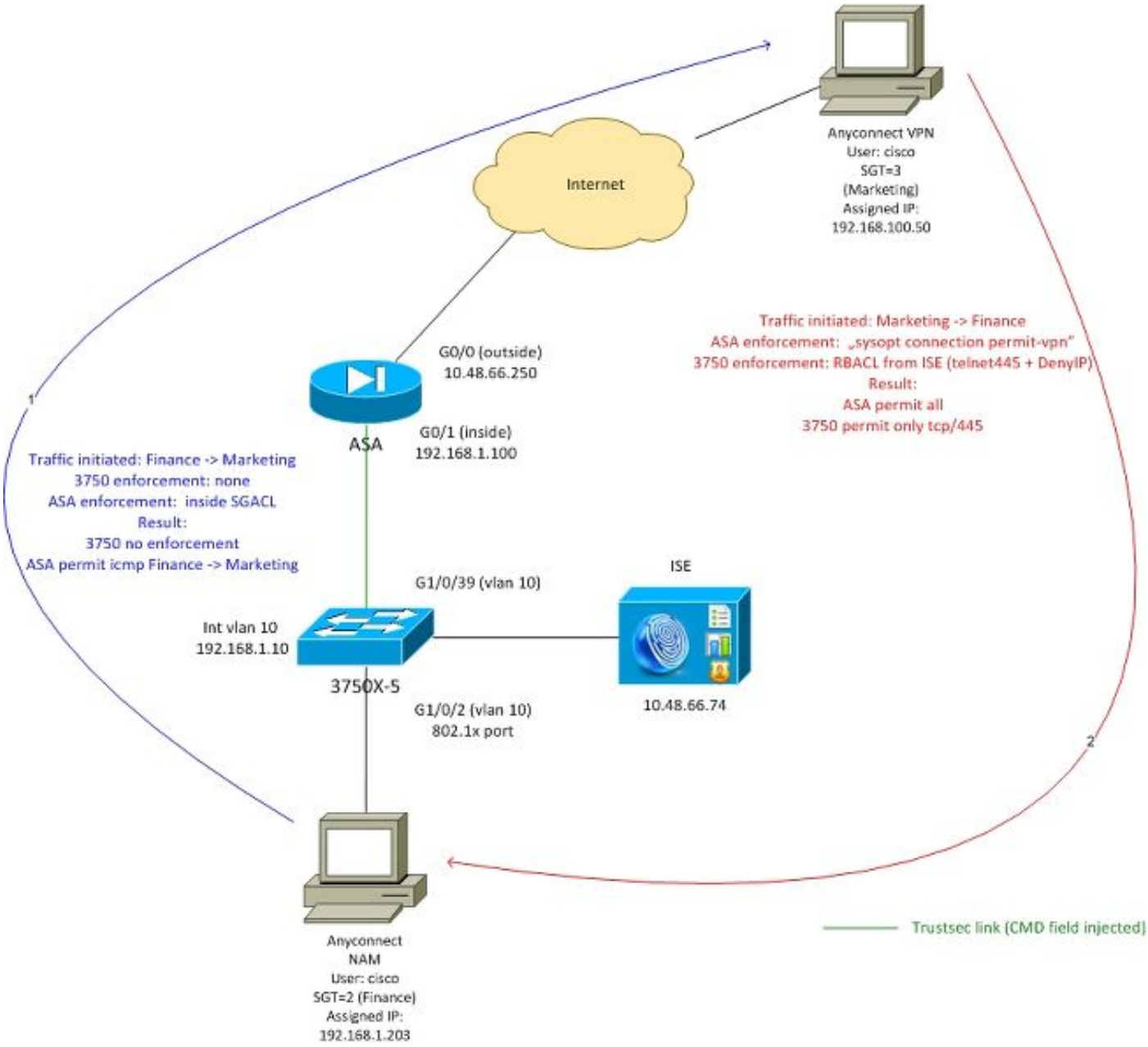
> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

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。 そのフィールドはセキュリティグループ タグ（ SGT ）が含まれていますパケットの出典を記述する。

リモート VPN ユーザは ASA の SSL セッションを終了し、SGT タグ 3 （ マーケティング ）を割り当てられます。

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 ）が割り当てられます。



ASA に財務からマーケティングに初期化される ICMP トラフィックを可能にする内部インターフェイスで設定される SGACL があります。

ASA 割り当てはから初期化されるすべてのトラフィック VPN ユーザを取除きます（「sysopt 接続許可 VPN」設定が理由で）。

一度フローは作成されることを、リターンパケット自動的に受け入れられる意味する ASA の SGACL はステートフルです（インスペクションに基づいて）。

3750 のスイッチ使用 RBACL 融資するためにマーケティングから受信されるトラフィックを制御するため。

各パケットはチェックされるが、3750X プラットフォームの TrustSec 適用は宛先で実行されたことを意味する RBACL はステートレスです。 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。

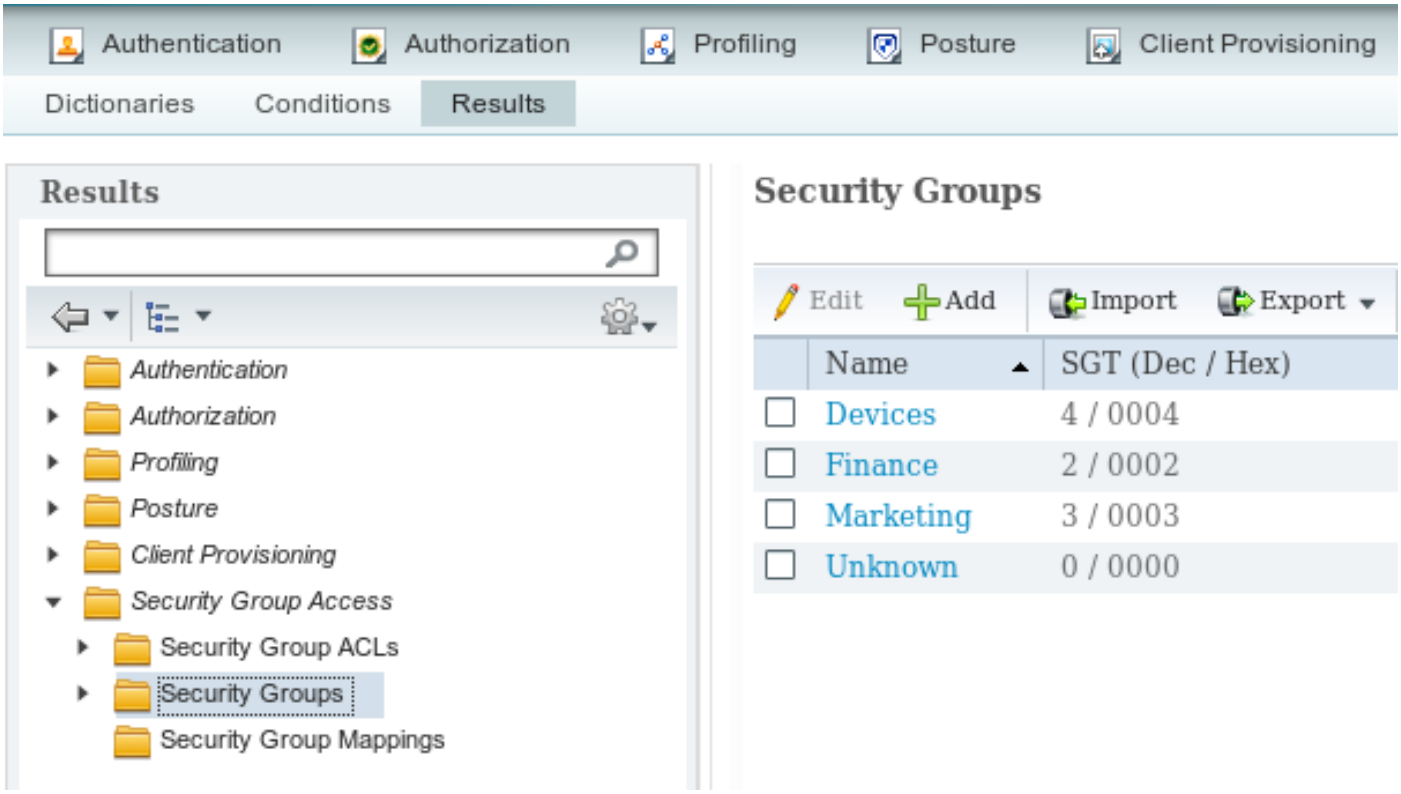
> **注:** Trustsec わかっているステートフル ファイアウォール on Cisco IOS ® ゾーンによって基づくファイアウォールの場合使用することができますたとえば、参照して下さい:

注: リモート VPN ユーザから来る ASA は SGACL 制御トラフィックがある可能性があります。 シナリオを簡素化するために、それはこの技術情報で示されませんでした。 たとえば参照して下さい: [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

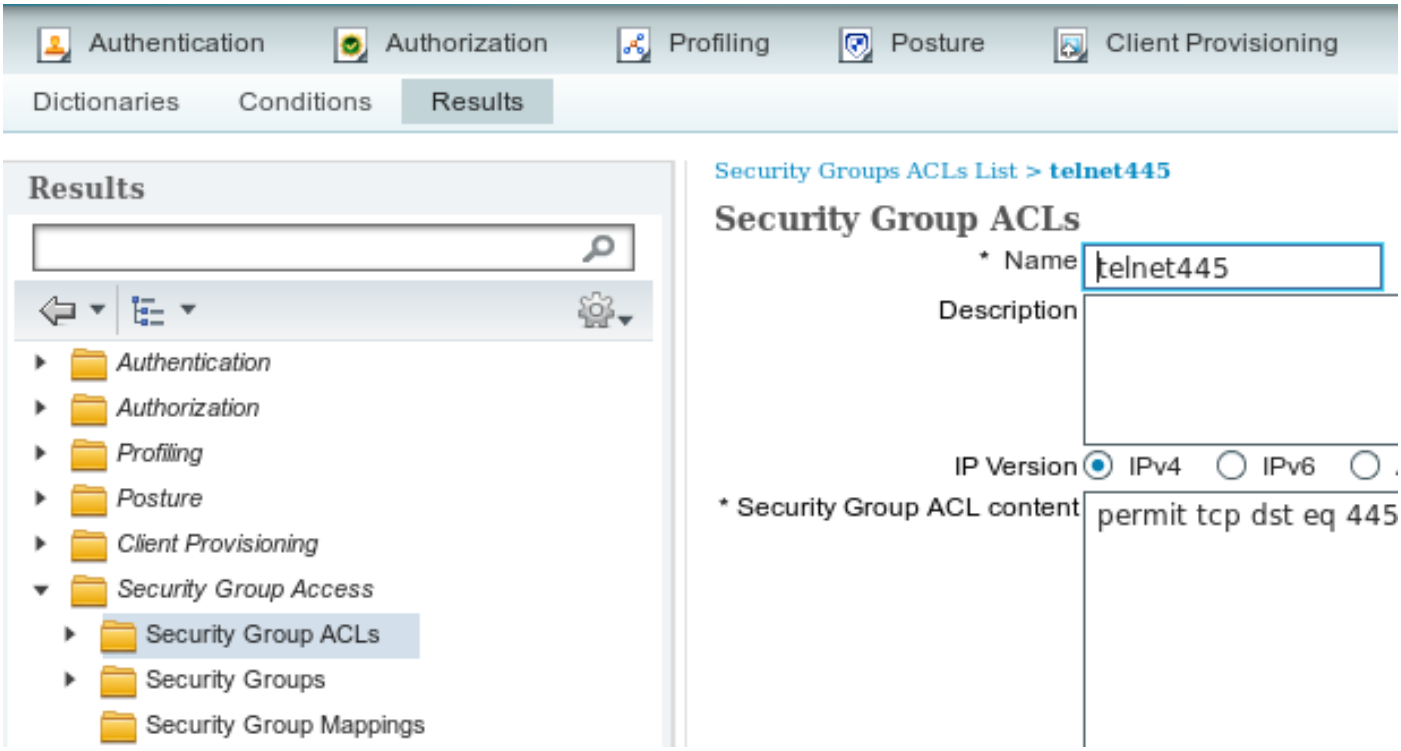
1. 財務およびマーケティングの SGT

ポリシー > 結果 > Security へのナビゲートはこのイメージに示すように**グループ アクセス > Security グループ**および財務のための SGT およびマーケティングを作成します。



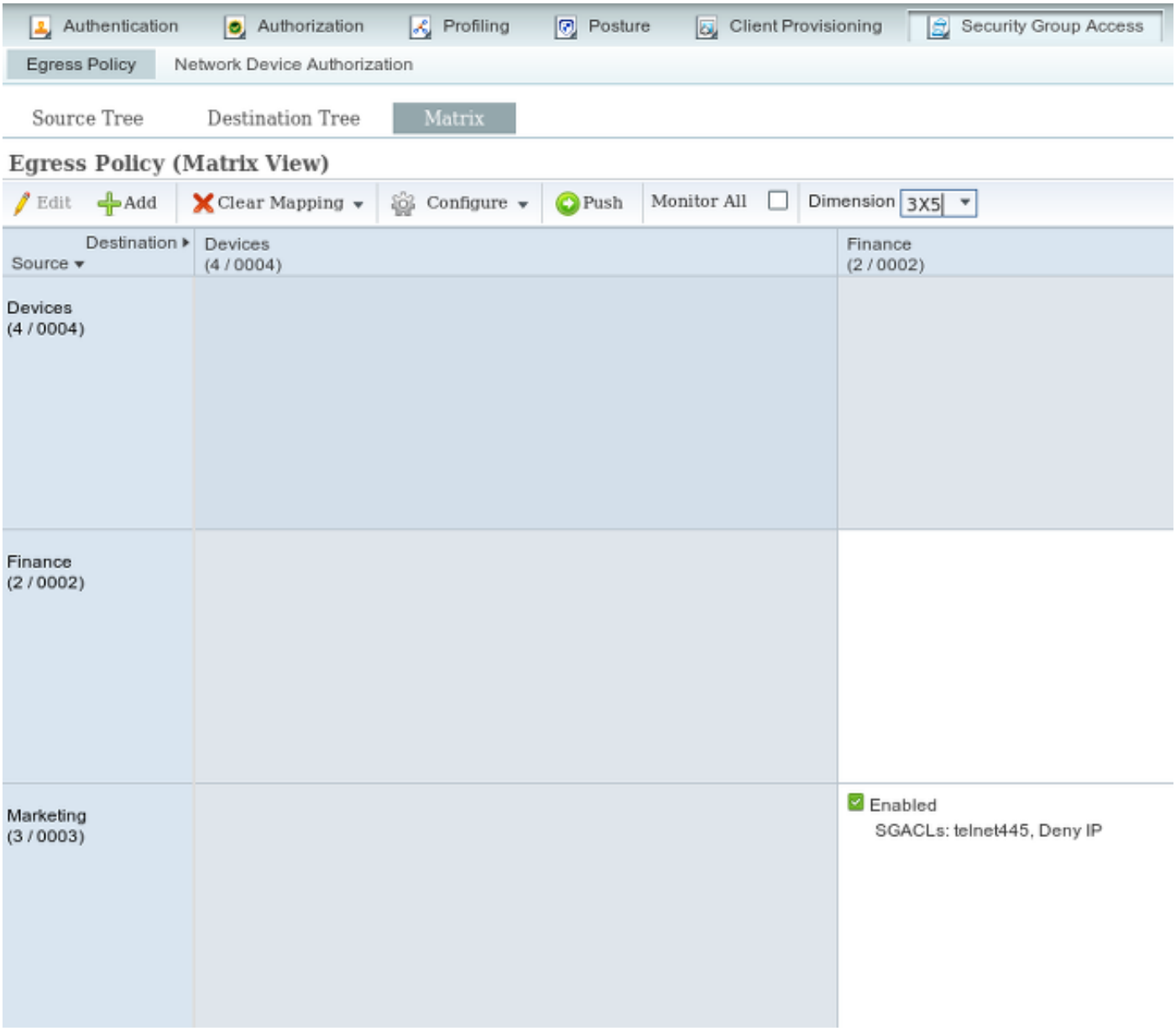
2. トラフィック マーケティング > 財務のためのセキュリティグループ ACL

ポリシー > 結果 > Security へのナビゲートは**グループ アクセス > Security グループ ACL** およびマーケティングからのコントロール トラフィックに融資するのに使用されている ACL を作成します。 tcp/445 だけこのイメージに示すように許可されます。



3. マトリクス形式の ACL バインディング

ポリシー > 出力ポリシー > 行列バインドへのナビゲートは出典のための ACL を設定しました: ：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。 またイメージに示すように他のすべてのトラフィックを廃棄する最後の ACL として付加**拒否 IP**。 （そのデフォルトポリシーなしで、デフォルトです割り当て接続されます）



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

ポリシー > 許可へのナビゲートはおよびリモート VPN アクセスのための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。 条件は AnyConnect 識別 Extentions （ ACIDEX ）を使用することです:

```
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

ポリシー > 許可へのナビゲートはおよび 802.1X アクセスのための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 のサプリカントにはフル 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。

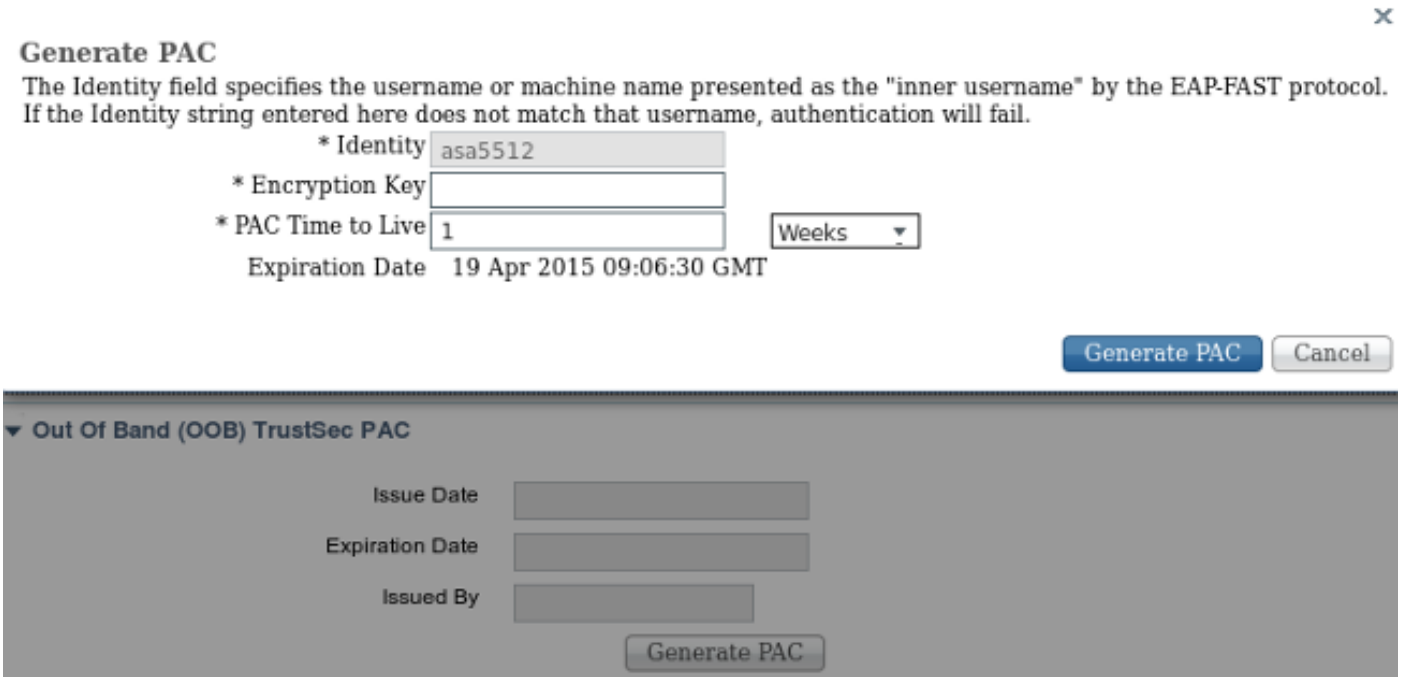
```
Rule name: 802.1x
```

```
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ために、PAC ファイルを手動で生成することは必要です。そのファイルは ASA でインポートされます。

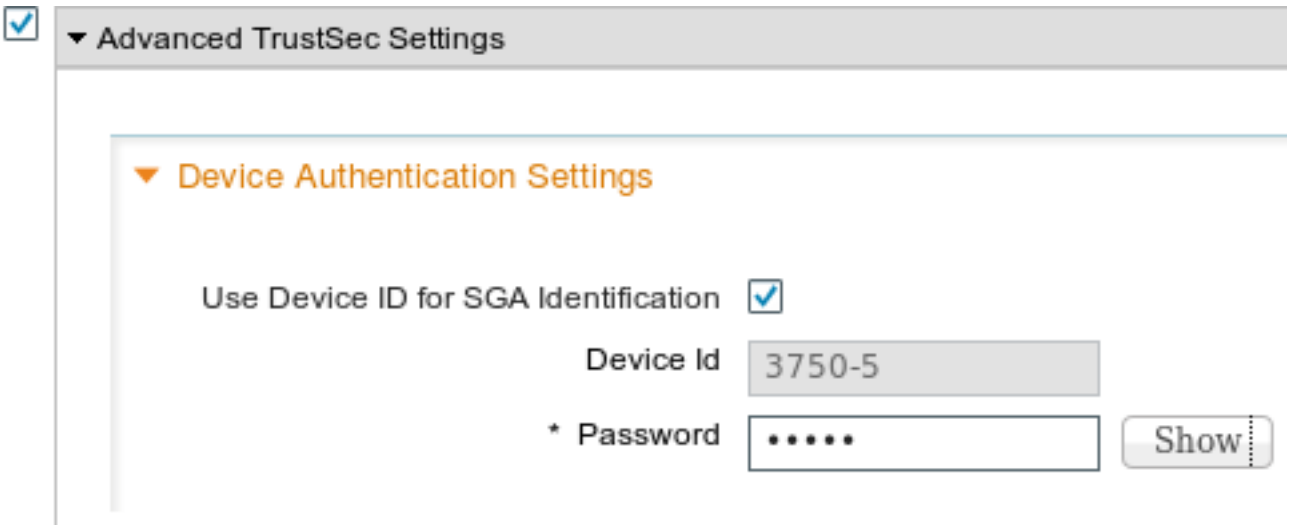
これは [Administration] > [Network Devices] から設定できます。 ASA が追加された後、**TrustSec 設定**にスクロールし、このイメージに示すように **PAC を生成して下さい**。



ステップが手動 PAC プロビジョニングだけサポートする ASA のためにだけ実行される必要があるように、スイッチ（3750X）は自動 PAC プロビジョニングをサポートします。

7. ネットワークデバイスを、スイッチ自動 PAC プロビジョニングのための設定 シークレット追加して下さい

スイッチに関しては自動 PAC プロビジョニングを使用する、正しいシークレットはこのイメージに示すように、設定 する必要があります。



注: PAC が ISE を認証し、ポリシー（ACL）と共に環境 データ（例えば SGT）をダウンロードするのに使用されています。 ASA は環境 データだけ、ポリシー ASA で手動で設定される必要がありますサポートします。 Cisco IOS ® は両方ともサポートします、従ってポリシーは ISE からダウンロードすることができます。

ASA： 設定手順

1. 基本的な VPN アクセス

認証のための ISE を使用した AnyConnect のための設定基本 SSL VPN アクセス。

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

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
```

確認するため:

```
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
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   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
```

```
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

cts を有効に した後、ASA は 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. トラフィック財務 > マーケティングのための SGACL

内部インターフェイスに SGACL を設定します。 ACL は財務からマーケティングに ICMP トラフィックだけ初期化することを割り当てます。

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

ASA は番号が付くためにタグの名前を拡張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のイネーブル cts

ASA の内部インターフェイスの cts を有効に した後:

```
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
```

ASA は TrustSec 帯 (CMD フィールドのイーサネットフレーム) を送信 し、受信できます。 ASA はタグのないすべての入力フレームがタグ 100 と同様に扱う必要があると仮定します。 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
```

その設定によって、後成功した 802.1X 許可はユーザ（ISE によって許可される）タグ 2（財務）を割り当てる必要がありました。

2. CTS の設定およびプロビジョニング

同様に、ASA に関しては、cts は ISE へのポイント設定され、:

```
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、適用は Layer3 および Layer2（すべての VLAN）のために両方有効に なります:

```
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 を自動的に提供するため:

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

再度、パスワードは ISE（**ネットワークデバイス > スイッチ > TrustSec**）の対応した 設定とマッチする必要があります。 今は、Cisco IOS ® は PAC を得るために ISE の EAP-FAST な セッションを始めます。 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確認するため:

```
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:
000200B000030001000400010EA48096688D96EF7B94C679A17BDAD6F000600940003010036 5AB3133998C86C1BA1B418
968C6069000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
 Refresh timer is set for 4y14w
```

3. ASA へのインターフェイスのイネーブル cts

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

今後は、スイッチは処理し、TrustSec 帯を送信 し、ISE からダウンロードされるポリシーを実施して準備ができる必要があります。

確認

このセクションでは、設定が正常に機能していることを確認します。

確認はこの資料の個々のセクションで力バーされます。

トラブルシューティング

SGT 割り当て

ASA への VPN セッションが設定された後、正しい SGT 割り当ては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 の承認規則によって、すべての AnyConnect4 ユーザはマーケティング タグに割り当てられました。

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 Network Analysis Module （NAM）完了の後で、認証 スイッチは ISE から戻っ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
      dot1x            Authc Success
      mab              Stopped
```

ISE の承認規則によって、そのスイッチに接続されるすべてのユーザは SGT = 2 に割り当てる必要があります（財務）。

ASA での適用

財務からのトラフィックを送信 することを試みるとき（192.168.1.203）マーケティングに（192.168.100.50）、ASA の内部インターフェイスを見つけます。 ICMPエコー要求に関しては、それはセッションを作成します:

```
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)
```
そして ACL カウンターを高めます:

```
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も確認できます。 正しいタグが表示することに注目して下さい:

```
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。 もう一つのトラブルシューティング ツールはまた、パケット トレーサー準備ができた TrustSec です。

スイッチ (次の セクションの説明) のステートレス RBACL によってブロックしたので残念ながら、802.1X PC はその返事を見ません。

もう一つのトラブルシューティング ツールはまた、パケット トレーサー準備ができた TrustSec です。 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
```

それは ASA によってブロックする必要がありますまた財務からのマーケティングへの TCP 接続を開始することを試みる:

```
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
```

ポリシーは融資するためにマーケティングからのトラフィックを制御する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
```

それはマーケティングから融資することを来る ICMPエコー応答がなぜ廃棄されたか原因です。 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 接続がマーケティングから開始される場合はどうしたらいいのですか。

ASA 割り当て (「sysopt 接続許可 VPN」が理由ですべての 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)
```

正しいセッションは作成されます:

```
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
```

そして、Cisco IOS ® は telnet445 RBACL と一致するのでそれを受け入れます。 正しいカウンター増加:

```
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 TrustSec ポリシー設定で違いおよび ASA および Cisco IOS ® の適用を示すために故意に示されます。 ISE (ステートレス RBACL) および TrustSec わかっているステートフル ゾーンによって基づくファイアウォールからダウンロードされる Cisco IOS ® ポリシーの違いを理解しておいて下さい。

関連情報

- 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