# Catalyst 3750X シリーズ スイッチでの TrustSec Cloud と 802.1x MACsec の設定例

## 内容



## 概要

この記事では、2 台の Catalyst3750X シリーズ スイッチ（3750X）間でリンク暗号化を使用して Cisco TrustSec （CTS）クラウドを設定するのに必要な手順について説明します。

この記事では、Security Association Protocol （SAP）を使用するスイッチ間 Media Access Control Security（MACsec）暗号化プロセスについて説明します。このプロセスは、手動モードの代わりに IEEE802.1x モードを使用します。

次に、関連する手順の一覧を示します。

- シード デバイスおよび非シード デバイス用の Protected Access Credential （PAC）プロビジョニング
- ネットワーク デバイス アドミッション コントロール（NAC）認証およびキー管理のための SAP を使用した MACsec ネゴシエーション
- 環境およびポリシーの更新
- クライアントのポート認証
- セキュリティ グループ タグ（SGT）を使用したトラフィック タギング

- セキュリティ グループ ACL（SGACL）を使用したポリシーの適用

# 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

- CTS コンポーネントの基礎知識
- Catalyst スイッチの CLI 設定に関する基本的な知識
- Identity Services Engine（ISE）設定の経験

## 使用するコンポーネント

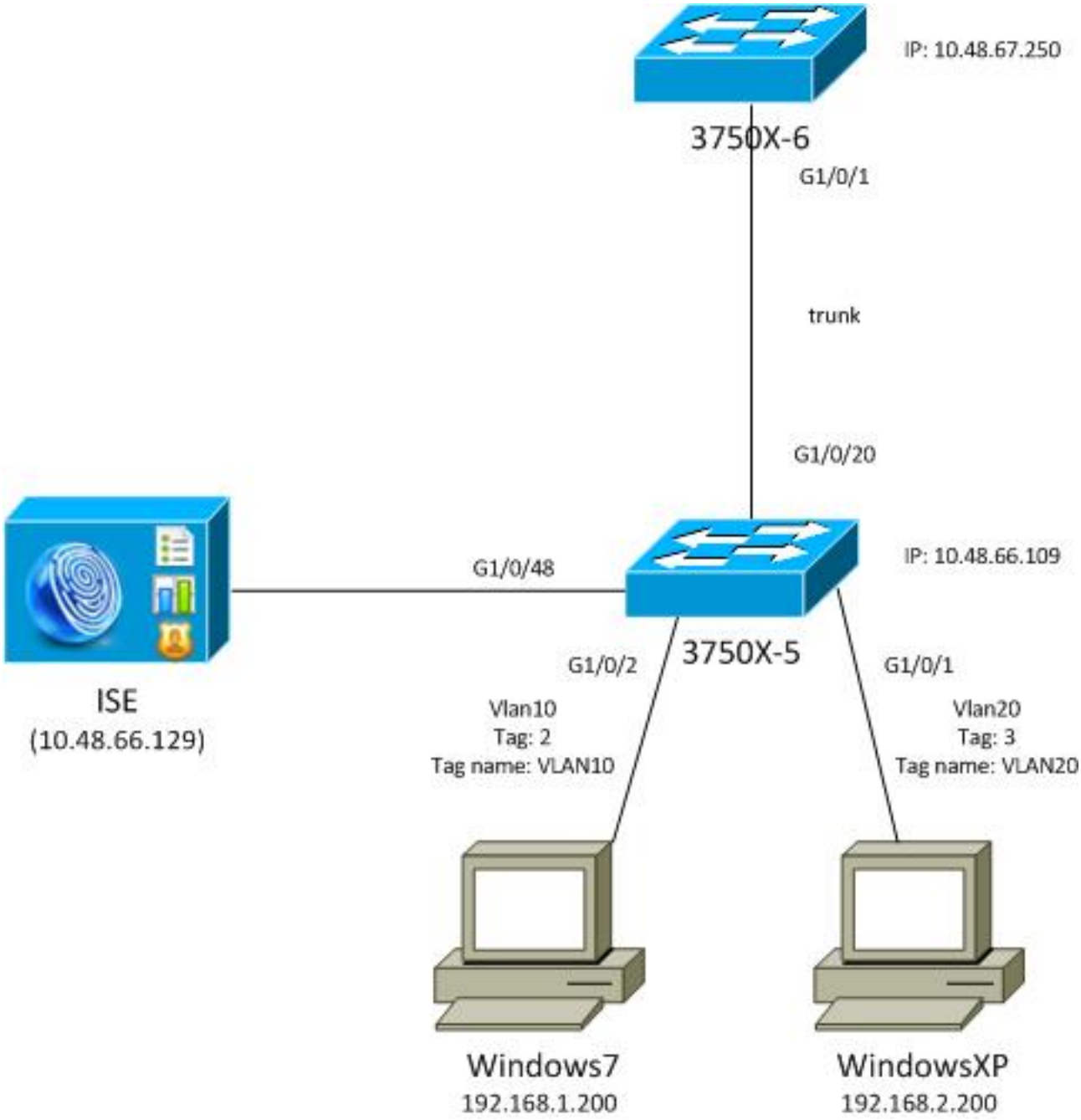
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft（MS）Windows 7 および MS Windows XP
- 3750X ソフトウェア、バージョン 15.0 以降
- ISE ソフトウェア バージョン 1.1.4 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

# 設定

## ネットワーク図




このネットワーク トポロジ図では、3750X-5 スイッチは ISE の IP アドレスを知っているシード デバイスであり、CTS クラウドでの後続の認証に使用される PAC を自動的にダウンロードします。シード デバイスは、非シード デバイス用の 802.1x オーセンティケータとして機能します。Cisco Catalyst 3750X-6 シリーズスイッチ ( 3750X-6 ) は、非シード デバイスです。これは、シード デバイスに対して 802.1x サプリカントとして機能します。非シード デバイスがシード デバイス経由で ISE に対して認証を行うと、CTS クラウドへのアクセスが許可されます。認証が成功すると、3750X-5 スイッチ上の 802.1x ポートのステータスが **authenticated** に変わり、MACsec の暗号化がネゴシエートされます。スイッチ間のトラフィックは、SGT タグ付けされ、暗号化されます。

次のリストは、予想されるトラフィック フローをまとめたものです。

- シード 3750X-5 は、ISE に接続し PAC をダウンロードします。これは、後ほど環境やポリシーの更新に使用されます。
- 非シード 3750X-6 は、認証/承認、および PAC を ISE からダウンロードするために、サプリカント ロールを使用して 802.1x 認証を実行します。
- 3750X-6 は、PAC に基づいて保護されたトンネルと認証を行うために、2 番目の 802.1x

Extensible Authentication Protocol-Flexible Authentication via Secure Protocol（EAP-FAST）セッションを実行します。
- 3750X-5 が自身のために、および 3750X-6 の代わりに、SGA ポリシーをダウンロードします。
- 3750X-5 と 3750 X-6 との間で SAP セッションが生じ、MACsec 暗号がネゴシエートされ、ポリシーが交換されます。
- スイッチ間のトラフィックがタグ付けおよび暗号化されます。

## シード スイッチおよび非シード スイッチの設定

シード デバイス（3750X-5）が、CTS 用の RADIUS サーバとして ISE を使用するように設定されます。

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

cts authorization list ise

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

ロールベース アクセス コントロール リスト（RBACL）およびセキュリティ グループ ベース アクセス コントロール リスト（SGACL）の適用が有効になります（これらは後ほど使用されます）。

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

非シード デバイス（3750X-6）は、RADIUS または CTS 認証を必要とせず、認証、認可、およびアカウンティング（AAA）のためだけに設定されます。

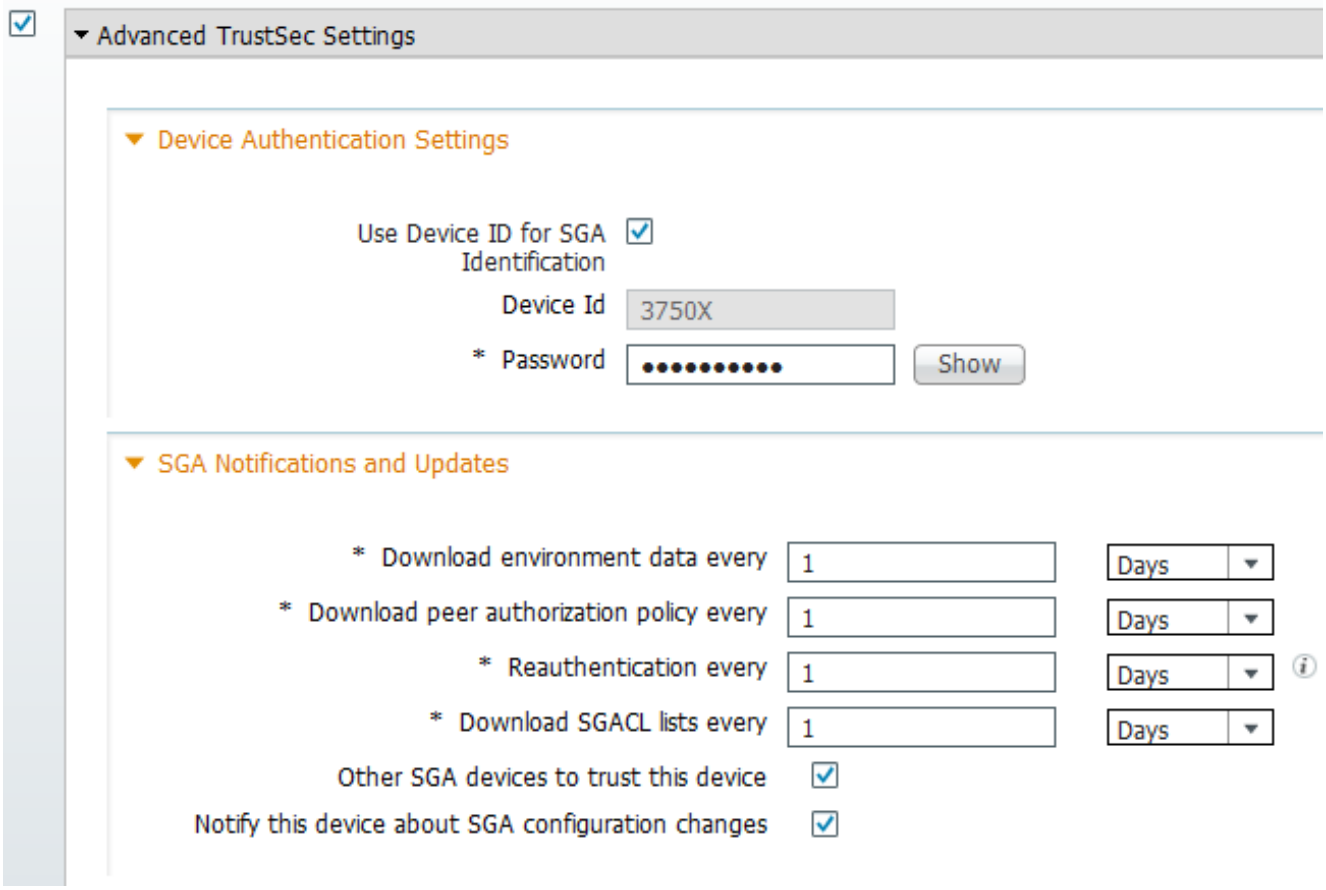
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

インターフェイス上で 802.1x を有効化する前に、ISE を設定する必要があります。

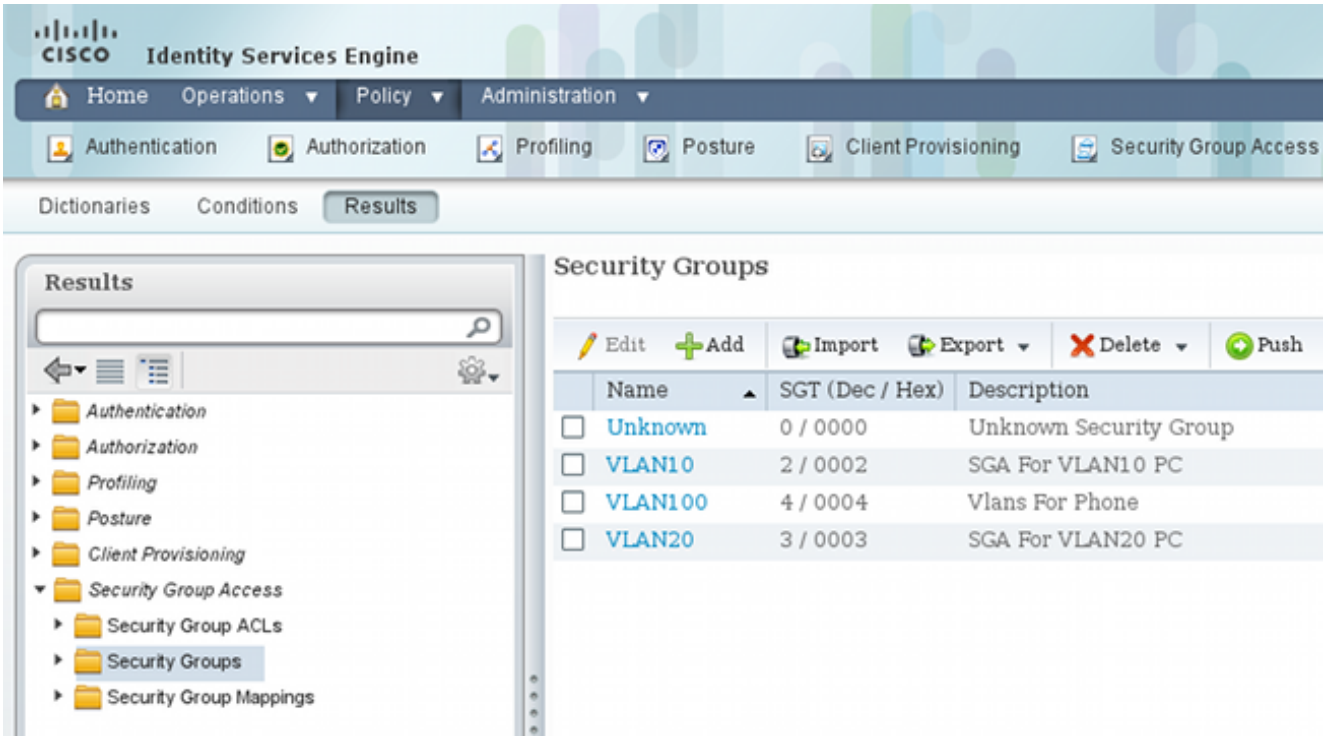
## ISE の設定

ISE を設定するには、次の手順を実行します。

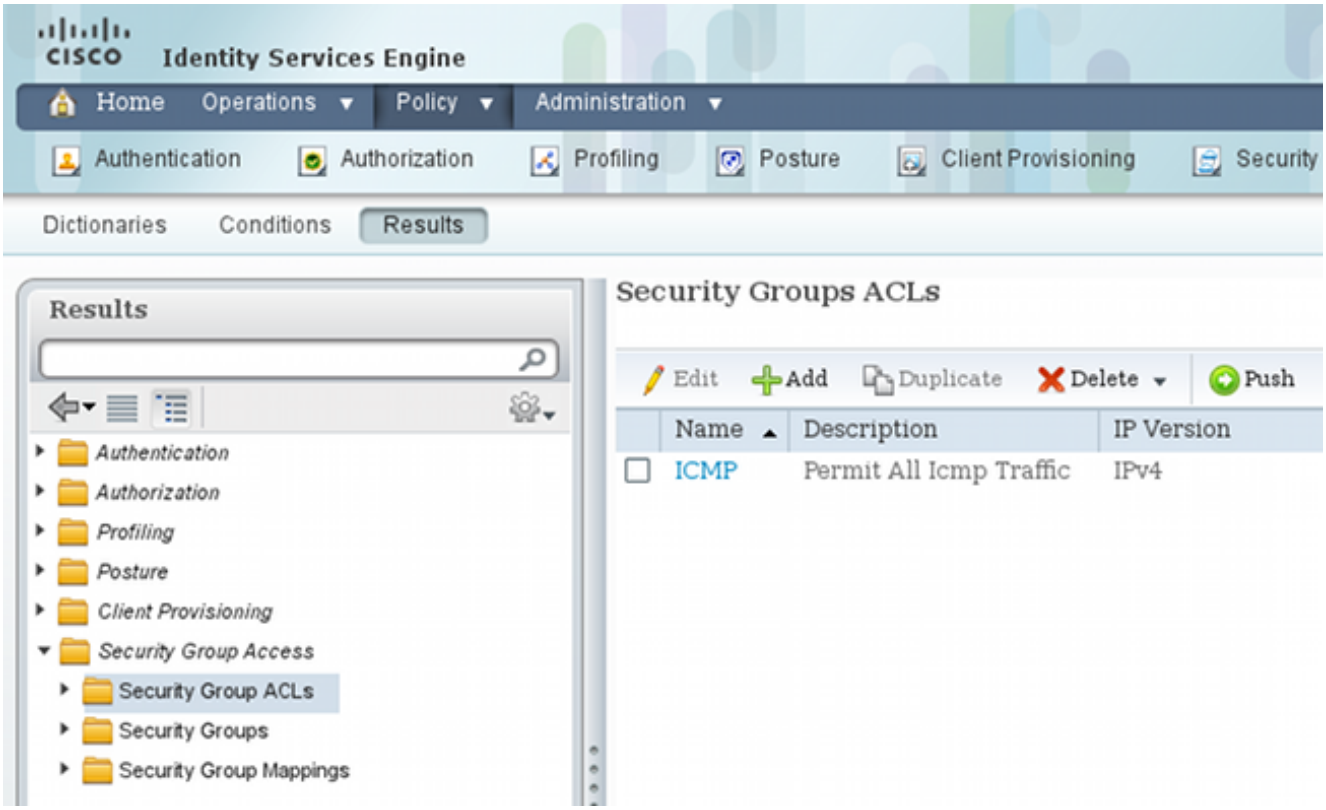
1. [Administration] > [Network Resources] > [Network Devices] に移動し、両スイッチをネットワーク アクセス デバイス（NAD）として追加します。[Advanced TrustSec Settings] で、スイッチ CLI で後ほど使用するための CTS パスワードを設定します。



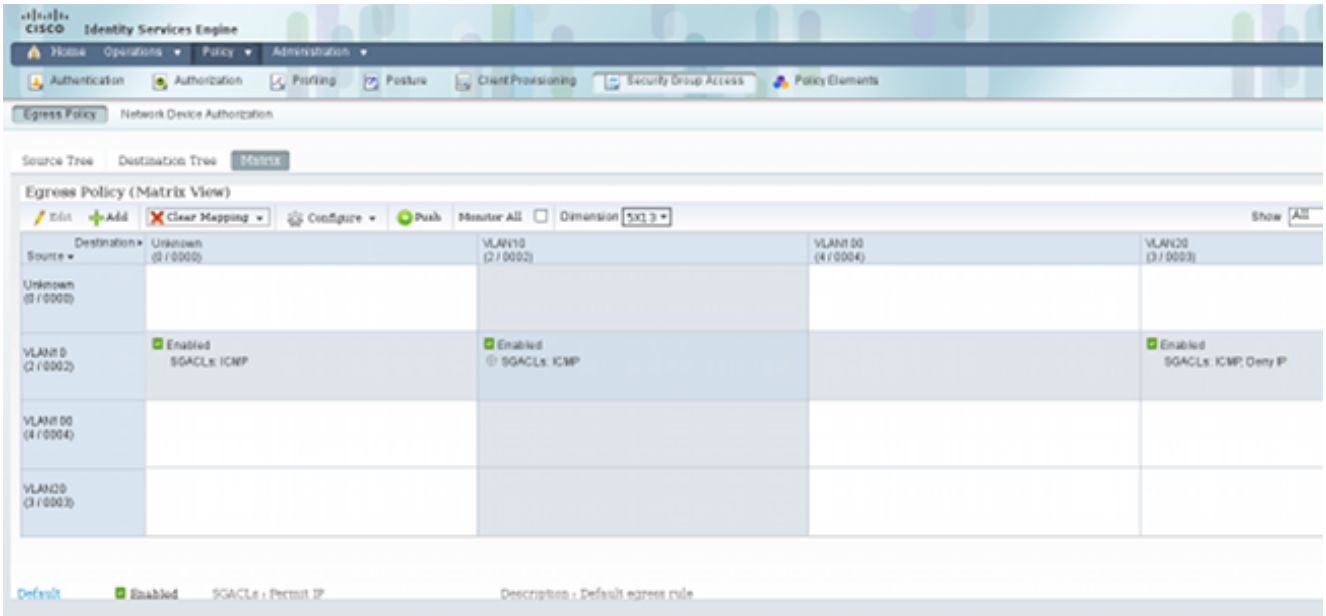

2. [Policy] > [Policy Elements] > [Results] > [Security Group Access] > [Security Groups] に移動し、適切な SGT を追加します。これらのタグは、スイッチが環境の更新を要求するとダウンロードされます。




3. [Policy] > [Policy Elements] > [Results] > [Security Group Access] > [Security Group ACLs] に移動し、SGACL を設定します。




4. [Policy] > [Security Group Access] に移動し、マトリックスを使用してポリシーを定義します。




**注**：正しいタグを受信するように、MS Windowsサプリカントの認可ポリシーを設定する必要があります。この詳細な設定については、『ASA および Catalyst 3750X シリーズ スイッチ TrustSec 設定例およびトラブルシューティング ガイド』を参照してください。

## 3750X-5 用の PAC プロビジョニング

CTS ドメインの認証（EAP-FAST のフェーズ 1）には PAC が必要で、ISE から環境およびポリシーデータを取得するのにも使用されます。正しい PAC がなければ、ISE からデータを取得でき

ません。

正しいクレデンシャルを 3750X-5 で提供すると、それが PAC をダウンロードします。

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

PAC は、CLI で入力されたクレデンシャルおよび ISE で設定されたものと同じクレデンシャルを使用して、Microsoft の Challenge Handshake Authentication Protocol （ MSCHAPv2 ）によって EAP-FAST 経由でダウンロードされます。

PAC は、環境およびポリシーの更新に使用されます。これらのスイッチには、**cisco av-pair cts-pac-opaque** を使用して RADIUS 要求を行います。これは、PAC キーから取得され、ISE で復号できます。

## 3750X-6 および NDAC 認証用の PAC プロビジョニング

新しいデバイスが CTS ドメインに接続できるようにするには、対応するポートで 802.1x を有効にする必要があります。

キー管理および暗号スイートのネゴシエーションには、SAP プロトコルが使用されます。認証には、Galois メッセージ認証コード（ GMAC ）が使用され、暗号化には Galois/Counter （ GCM ）が使用されます。

シード スイッチでは、次の手順を実行します。

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

シード スイッチ以外では、次の手順を実行します。

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

これは、トランク ポート（ スイッチ間の MACsec ）でのみサポートされます。SAP の代わりに

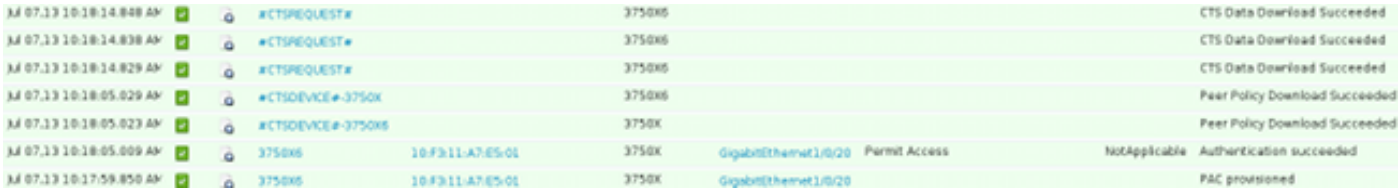
MACsec Key Agreement（MKA）プロトコルを使用する、スイッチとホスト間の MACsec については、「MACsec の暗号化の設定」を参照してください。

ポート上で 802.1x を有効化するとすぐに、非シード スイッチはオーセンティケータであるシード スイッチに対するサプリカントとして機能します。

このプロセスは NDAC と呼ばれ、CATS ドメインに新しいデバイスを接続するためのものです。認証は双方向です。新しいデバイスは、認証サーバISEで検証されるクレデンシャルを持ちます。PAC プロビジョニング後、デバイスは、CTS ドメインに接続しているかも確認します。

> **注**:PACは、EAP-FAST用のTransport Layer Security(TLS)トンネルを構築するために使用されます。3750X-6 は、EAP-TLS 方式のための TLS トンネルのサーバによって提供された証明書をクライアントが信頼するのと同様に、サーバが提供する PAC のクレデンシャルを信頼します。

複数の RADIUS メッセージが交換されます。




3750X（シード スイッチ）からの最初のセッションは、PAC プロビジョニングに使用されます。EAP-FAST は、PAC なしで使用されます（MSCHAPv2 認証のための匿名トンネルが構築されます）。

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

**cts credentials コマンドを使用して設定された MSCHAPv2 のユーザ名とパスワードが使用されます。**さらに、PAC がすでにプロビジョニングされていると、それ以上の認証は必要ないので、最後に RADIUS アクセス拒否が返されます。

ログの 2 番目のエントリは、802.1x 認証を指します。EAP-FAST は、以前にプロビジョニングされた PAC で使用されます。

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

今回、トンネルは匿名ではありませんが、PAC によって保護されています。ここでも、MSCHAPv2 セッション用の同じクレデンシャルが使用されます。その後、そのクレデンシャルが ISE 上の認証ルールと承認ルールに照らして検証され、RADIUS の Access-Accept が返されます。続いて、オーセンティケータ スイッチが返された属性を適用し、そのポートの 802.1x セッションが承認済み状態に移行します。

最初の 802.1x の 2 セッションのプロセスは、シード スイッチからはどのように見えますか？

シードからの最も重要なデバッグは次のとおりです。シードが、ポートが起動していることを検出し、サプリカントまたはオーセンティケータのいずれのロールを 802.1x に使用するか決定しようとします。

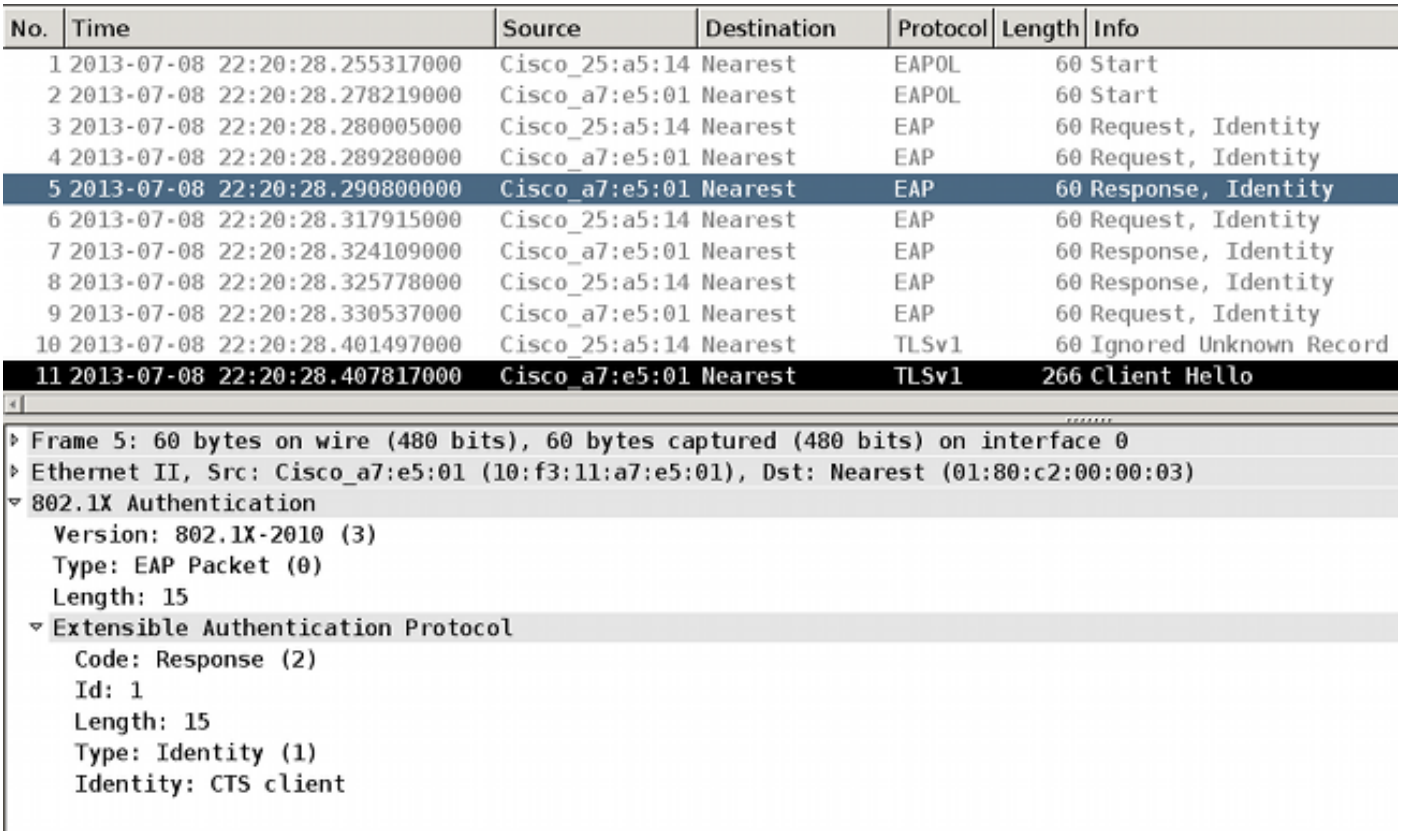
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

最後に、スイッチが ISE にアクセスできるので、オーセンティケータ ロールが使用されます。3750X-6 では、サプリカント ロールが選択されます。

## 802.1x ロール選択の詳細

> **注**：サプリカントスイッチは、PACを取得して802.1x認証を受けた後、環境データ（後述）をダウンロードし、AAAサーバのIPアドレスを学習します。この例では、両方のスイッチが ISE に対する専用（バックボーン）の接続を持っています。その後、ロールは異なっていてもかまいません。AAAサーバから応答を受信した最初のスイッチがオーセンティケータになり、2番目のスイッチがサプリカントになります。

これが可能なのは、ALIVE としてマークされた AAA サーバを持つ両方のスイッチが、拡張可能認証プロトコル（EAP）要求アイデンティティを送信するためです。最初に EAP アイデンティティ応答を受信したスイッチがオーセンティケータになり、その後のアイデンティティ要求をドロップします。




802.1x ロールが選択されると（このシナリオでは、まだ AAA サーバにアクセスできないため、3750X-6 がサプリカント）、次のパケットには PAC プロビジョニングのための EAP-FAST 交換が含まれます。RADIUS 要求のユーザ名、および EAP アイデンティティとして、**CTS client というユーザ名が使用されます。**

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12   "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

匿名 EAP-FAST トンネルが作成されると、ユーザ名 **3750X6（cts credentials）**用に MSCHAPv2 セッションが発生します。これは TLS トンネル（暗号化済み）なので、スイッチ上では確認できませんが、PAC プロビジョニング用の ISE に関する詳細なログの内容でそれを確認できます。RADIUS ユーザ名、および EAP アイデンティティ応答として **CTS client を確認できます。**しかしながら、内部方式（MSCHAP）の場合には、**3750X6** のユーザ名が使用されます。

| | |
|---|---|
| EAP Authentication Method : | EAP-MSCHAPv2 |
| EAP Tunnel Method : | EAP-FAST |
| Username: | 3750X6 |
| RADIUS Username : | CTS client |
| Calling Station ID: | 10:F3:11:A7:E5:01 |

2 回目の EAP-FAST 認証が実行されます。今回は、以前にプロビジョニングされた PAC が使用されます。ここでも、RADIUS ユーザ名および外部アイデンティティとしては **CTS client が使用されますが、内側アイデンティティ（MSCHAP）には 3750X6 が使用されます。**認証が成功します。

| | |
|---|---|
| RADIUS Status: | Authentication succeeded |
| NAS Failure: | |
| Username: | 3750X6 |
| MAC/IP Address: | 10:F3:11:A7:E5:01 |
| Network Device: | 3750X : 10.48.66.109 : GigabitEthernet1/0/20 |
| Allowed Protocol: | NDAC_SGT_Service |
| Identity Store: | Internal CTS Devices |
| Authorization Profiles: | Permit Access |
| SGA Security Group: | Unknown |
| Authentication Protocol : | EAP-FAST(EAP-MSCHAPv2) |

ただし今回は、USE が RADIUS Accept パケット内にいくつかの属性を返します。

Authentication Result

```
User-Name=3750X6
 State=ReauthSession:C0A800010000053A33FD79AF
 Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
 Session-Timeout=86400
 Termination-Action=RADIUS-Request
 EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
 cisco-av-pair=cts:security-group-tag=0000-01
 cisco-av-pair=cts:supplicant-cts-capabilities=sap
 MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
 MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

ここでは、オーセンティケータ スイッチがポートを承認済み状態に変更します。

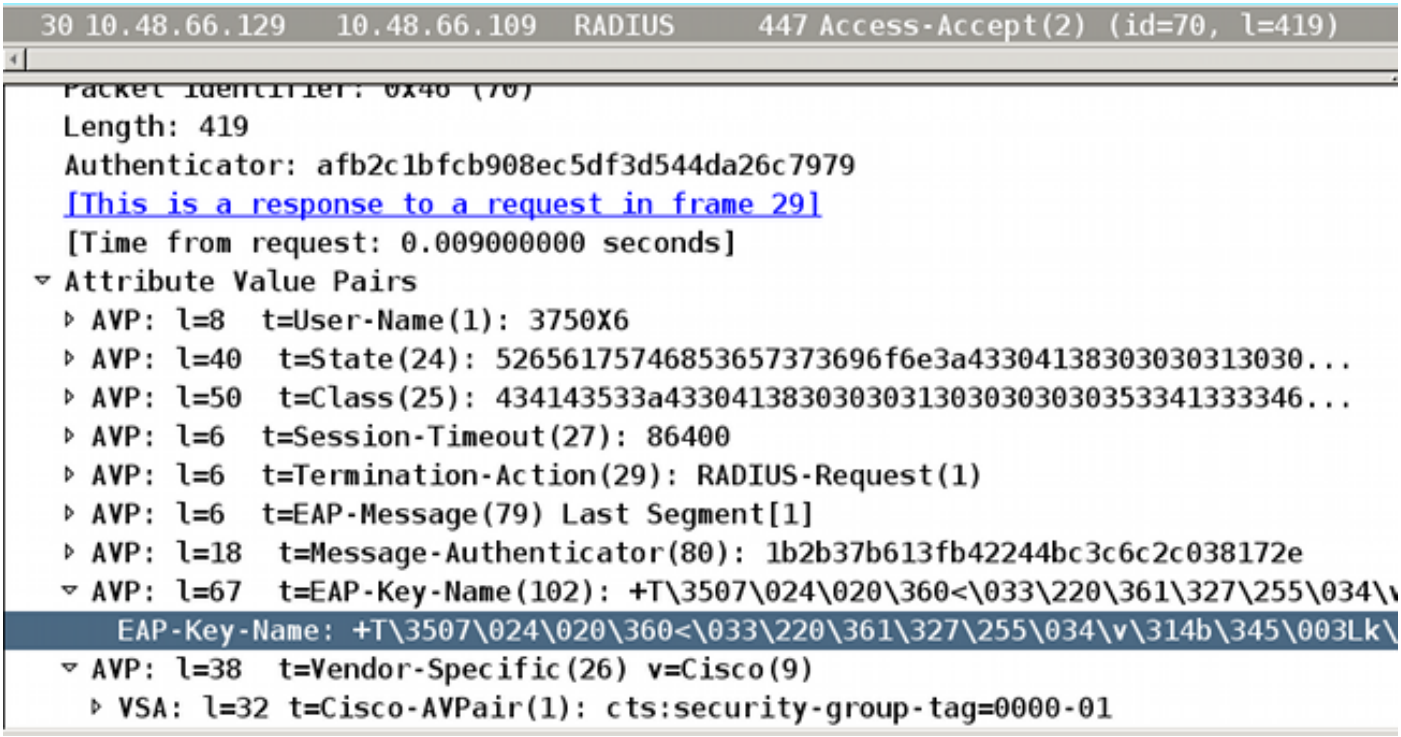
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

オーセンティケータ スイッチは、ユーザ名が 3750X6 であることをどうやって知るのでしょうか。RADIUS ユーザ名と外部 EAP アイデンティティについては、CTS client が使用され、内部アイ

**デンティティは暗号化されオーセンティケータからは見えません。**ISE によってユーザ名が学習されます。最後の RADIUS パケット（Access-Accept）には **username=3750X6** が含まれ、他のすべてのパケットには **username = Cts client** が含まれます。サプリカント スイッチが実際のユーザ名を認識するのはこのような理由からです。この動作は、RFC 準拠です。[RFC3579 セクション 3.0 には次のように記載されています。]

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

802.1x 認証セッションの最後のパケットでは、ISE が **EAP-Key-Name とともに RADIUS Accept メッセージ cisco-av-pair** を返します。

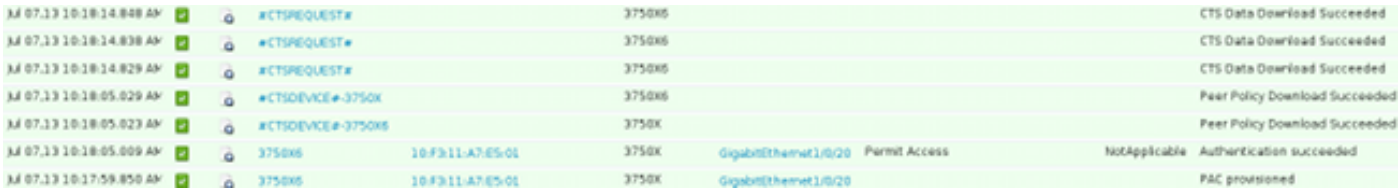



これは、SAP ネゴシエーションのキーイング マテリアルとして使用されます。

また、GST も渡されます。つまり、オーセンティケータ スイッチは、サプリカントからのトラフィックを **default value = 0** でタグ付けします。他の値を返すために、ISE 上に特定の値を設定できます。これはタグなしトラフィックにのみ適用されます。デフォルトでは、オーセンティケータスイッチは認証されたサプリカントからのトラフィックを信頼するため、タグ付きトラフィックは書き換えられません（ただし、これはISEでも変更できます）。

### SGA ポリシーのダウンロード

最初の 2 つの 802.1x EAP-FAST セッション（1 つは PAC プロビジョニング用、もう 1 つは認証用）以外にも追加の RADIUS 交換（EAP なし）があります。以下は、再び ISE のログです。




3番目のログ(**Peer Policy Download**)は、**3760X6**ユーザのRADIUS要求とRADIUS Acceptという単

純なRADIUS交換を示しています。これは、サプリカントからトラフィック用のポリシーをダウンロードするのに必要です。2 つの最も重要な属性は次のとおりです。

```
▽ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

このため、オーセンティケータスイッチはサプリカントによってSGTタグ付けされたトラフィック(**cts:trusted-device=true**)を信頼し、タグ付けされていないトラフィックも**tag=0**でタグ付けします。

4 番目のログは、同様の RADIUS 交換を示します。ただしここでは、**3750X5** ユーザ（オーセンティケータ）が対象です。これは、両方のピアがお互いのポリシーを持つ必要があるためです。サプリカントが引き続き AAA サーバの IP アドレスを知らない点に着目してください。オーセンティケータ スイッチがサプリカントに代わってポリシーをダウンロードするのはこのためです。この情報は、後に SAP ネゴシエーションの中で（ISE の IP アドレスとともに）サプリカントに渡されます。

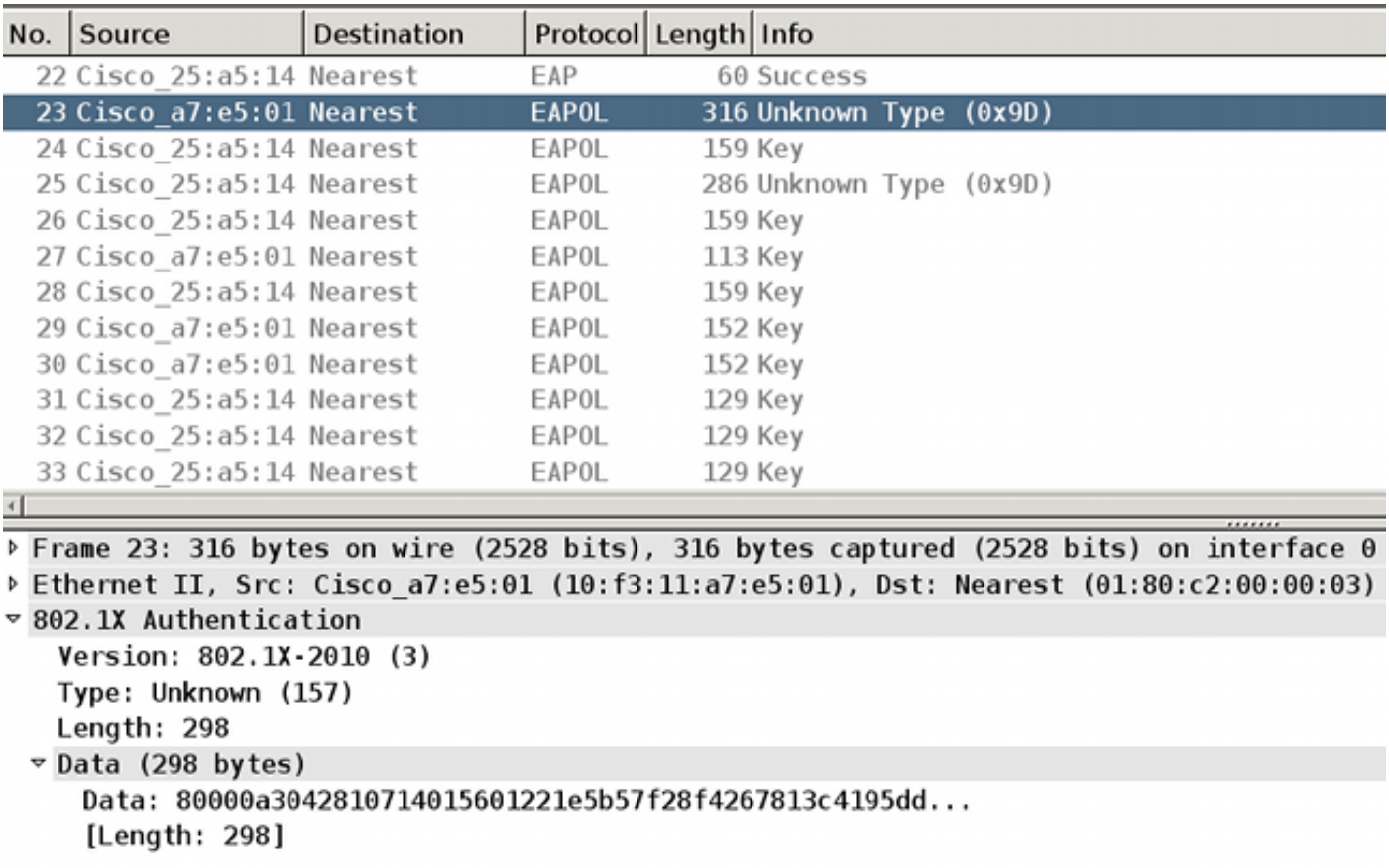
## SAP ネゴシエーション

802.1x 認証セッションが終了するとすぐに、SAP ネゴシエーションが発生します。このネゴシエーションは、次の理由から必要です。

- 暗号化レベルおよび暗号スイートをネゴシエートする（**sap mode-list gcm-encrypt コマンドを使用**）
- データ トラフィック用にセッション キーを抽出する
- キー再作成プロセスを実施する
- 追加のセキュリティ チェックを実行し、前の手順の安全性を確保する

SAP は、802.11i/D6.0 のドラフト バージョンに基づいて Cisco Systems が設計したプロトコルです。詳細については、「Cisco TrustSec Security Association Protocol：Cisco Nexus 7000 用に Cisco Trusted Security をサポートするプロトコル」ページへのアクセスを依頼してください。

SAP 交換は 802.1AE に準拠しています。サプリカントとオーセンティケータの間で Extensible Authentication Protocol over LAN（EAPOL）キーが交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。残念ながら、Wireshark には、必要なすべての EAP タイプに対するデコーダがありません。



| No. | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|
| 22 | Cisco_25:a5:14 | Nearest | EAP | 60 | Success |
| 23 | Cisco_a7:e5:01 | Nearest | EAPOL | 316 | Unknown Type (0x9D) |
| 24 | Cisco_25:a5:14 | Nearest | EAPOL | 159 | Key |
| 25 | Cisco_25:a5:14 | Nearest | EAPOL | 286 | Unknown Type (0x9D) |
| 26 | Cisco_25:a5:14 | Nearest | EAPOL | 159 | Key |
| 27 | Cisco_a7:e5:01 | Nearest | EAPOL | 113 | Key |
| 28 | Cisco_25:a5:14 | Nearest | EAPOL | 159 | Key |
| 29 | Cisco_a7:e5:01 | Nearest | EAPOL | 152 | Key |
| 30 | Cisco_a7:e5:01 | Nearest | EAPOL | 152 | Key |
| 31 | Cisco_25:a5:14 | Nearest | EAPOL | 129 | Key |
| 32 | Cisco_25:a5:14 | Nearest | EAPOL | 129 | Key |
| 33 | Cisco_25:a5:14 | Nearest | EAPOL | 129 | Key |



これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

サプリカント スイッチ上で次の手順を実行します。

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
       authc success:              12
```

```
        authc reject:               1556
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                12
        sap fail:                   0
        authz success:              12
        authz fail:                 0
        port auth fail:             0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

オーセンティケータ上で次の手順を実行します。

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
       Peer ID               : unknown
```

```
        Peer mac               : 0000.0000.0000
        Dot1X role             : unknown
        PMK                    :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

ここでは、ポートは gcm-encrypt モードを使用します。これは、トラフィックが正常に SGT タグ付けされ、認証および暗号化の両方が済んでいることを意味します。いずれのデバイスも、ISE 上の特定のネットワーク デバイス認証ポリシーを使用しません。これは、デバイスから開始されたすべてのトラフィックが 0 のデフォルト タグを使用することを意味します。さらに、両方のスイッチがピアから受信した SGT を信頼します（ピア ポリシーのダウンロード フェーズからの RADIUS 属性のため）。

## 環境およびポリシーの更新

両方のデバイスが CTS クラウドに接続されると、環境およびポリシーの更新が開始されます。環境の更新は、SGT と名前を取得するのに必要で、ポリシーの更新は、ISE で定義された SGACL をダウンロードするのに必要です。

この段階で、サプリカントは AAA サーバの IP アドレスをすでに知っているので、自分自身でこれを実行できます。

環境およびポリシーの更新に関する詳細については、『ASA および Catalyst 3750X シリーズ スイッチ TrustSec 設定例およびトラブルシューティング ガイド』を参照してください。

設定された RADIUS サーバが存在せず、CTS リンク（オーセンティケータ スイッチに向かう）がダウンした場合、サプリカント スイッチは RADIUS サーバの IP アドレスを記憶します。ただし、スイッチに、それを強制的に忘れさせることもできます。

```
bsns-3750-6#show run | i radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
```

```
aaa accounting dot1x default start-stop group radius
radius-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

サプリカント スイッチの環境およびポリシーを確認するには、次のコマンドを入力します。

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running

bsns-3750-6#show cts role-based permissions
```

ポリシーが表示されないのはなぜですか。cts enforcement を有効にしてポリシーに適用しない限

り、ポリシーは表示されません。

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

オーセンティケータには、Unknown をグループ化するのに複数のポリシーがあるのに対し、サプリカントには 1 つしかグループがないのはなぜですか。

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

## クライアントのポート認証

MS Windows クライアントは、3750-5 スイッチの g1/0/1 ポートに接続および認証されています。

```
bsns-3750-5#show authentication sessions int g1/0/1
       Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

ここで、スイッチ 3750-5 は、そのホストからのトラフィックは CTS クラウドに送信される際に SGT=3 でタグ付けされる必要があることを知っています。

## SGT によるトラフィックのタギング

トラフィックをどのようにスニッフィングおよび確認しますか。

次の理由からそれは困難です。

- 組み込みパケット キャプチャは、IP トラフィックに対してのみサポートされます ( これは、SGT および MACsec ペイロードを持つ修正されたイーサネット フレームです ) 。
- **replication キーワードを使用したスイッチド ポート アナライザ ( SPAN ) ポート：うまくいく可能性はありますが、問題は監視セッションの宛先ポートに接続された Wireshark を持つ PC が、802.1AE をサポートしないためにフレームをドロップすることです。これはハードウェア レベルで発生します。**
- **replication キーワードを使用しない SPAN ポートは、宛先ポートにつながる前に cts** ヘッダーを削除します。

## SGACL によるポリシーの適用

CTS クラウドでのポリシーの適用は、常に宛先ポートで実施されます。これは、最後のデバイスのみが、そのスイッチに直接接続されたエンドポイント デバイスの宛先 SGT を知っているからです。パケットは送信元 SGT のみを伝達します。決定するには、送信元と宛先の SGT 両方が必要です。

デバイスが ISE からすべてのポリシーをダウンロードする必要がないのはそのためです。その代わり、デバイスに直接接続されたデバイスがある SGT に関連するポリシーの一部のみが必要です。

次の例は、サプリカント スイッチである 3750-6 です。

```
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
```

この例ではポリシーが 2 つあります。1 つ目はタグなしトラフィック用のデフォルトです ( to/from ) 。2 つ目は **SGT=2 から、0** であるタグなし SGT までのものです。このポリシーは、デバイス自体が USE からの SGA ポリシーを使用し SGT=0 に属しているために存在します。また、**SGT=0** はデフォルトのタグです。したがって、トラフィック to/from SGT=0 に対するルールを持つポリシーすべてをダウンロードする必要があります。マトリックスを見ると、そのようなポリシーが1つだけ表示されます。**2 ~ 0です。**

次の例は、オーセンティケータ スイッチである 3750-5 です。

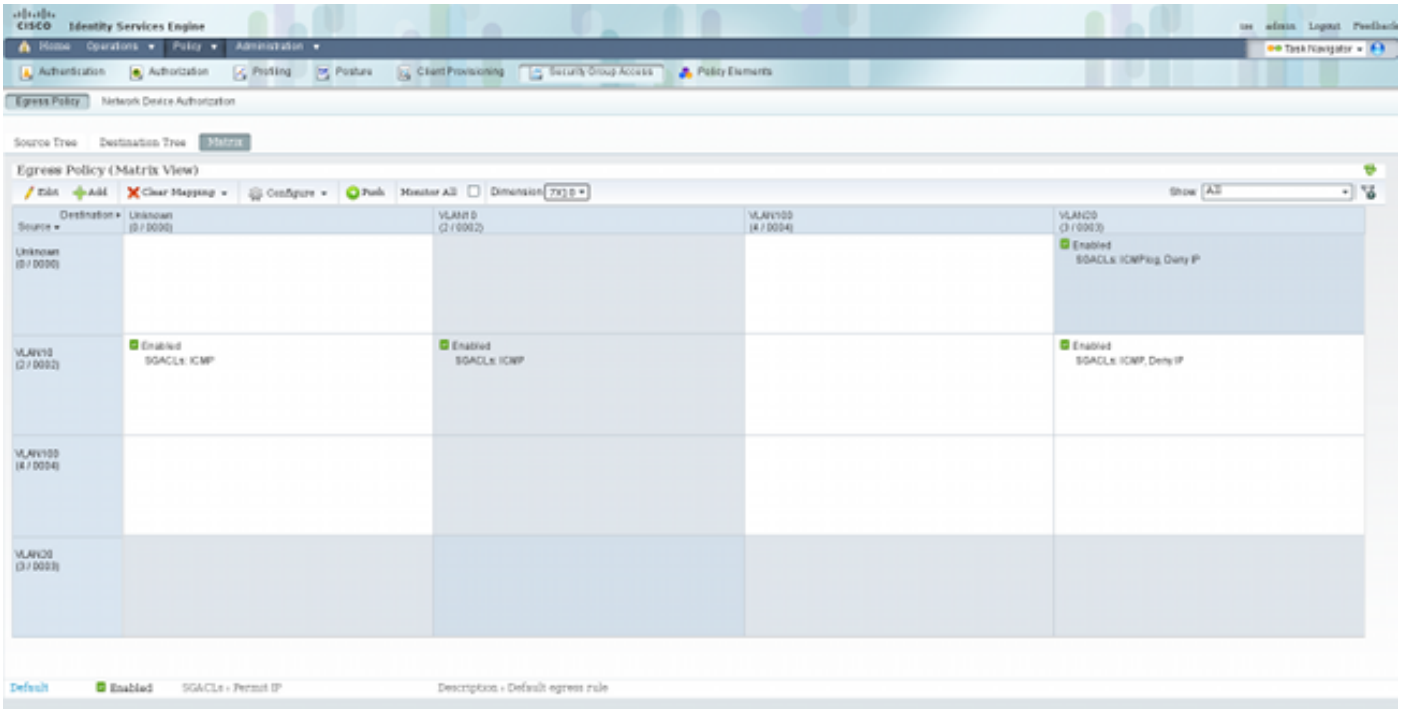
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

もう1つのポリシーは2**から3です。**これは、802.1x クライアント ( MS Windows ) が g1/0/1 に接

続され、**SGT=3** でタグ付けされているからです。**SGT=3** にすべてのポリシーをダウンロードする必要があるのはそのためです。

3750X-6（**SGT=0**）から MS Windows XP（**SGT=3**）に ping を実行してください。3750X-5 は適用する側のデバイスです。

その前に、**SGT=0 から SGT=3** のトラフィック向けに ISE 上でポリシーを設定する必要があります。この例は、**permit icmp log** の 1 行のみを含む SGACL の Internet Control Message Protocol（ICMP）を作成し、**SGT=0 から SGT=3** のトラフィック用にマトリックスの中でそれを使用しています。




次の例は、適用する側のスイッチ上におけるポリシーの更新、および新しいポリシーの検証を示します。

```
bsns-3750-5#cts refresh policy
Policy refresh in progress

bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

アクセス コントロール リスト（ACL）が ISE からダウンロードされたことを確認するには、次のコマンドを入力します。

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

ASA が適用されたこと（ハードウェア サポート）を確認するには、次のコマンドを入力します。

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name    = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
 flag    = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale   = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

次の例は、ICMP の前のカウンタです。

```
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

2       0       0               0               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

次の例は、SGT=0（3750-6 スイッチ）から MS Windows XP（SGT=3）への ping およびカウンタです。

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

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

2       0       0               0               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

次の例は、ACL カウンタです。

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
    10 permit icmp log (5 matches)
```

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- 3750 用 Cisco TrustSec 設定ガイド
- ASA 9.1 用 Cisco TrustSec 設定ガイド
- Cisco TrustSec の展開およびロードマップ
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。