Cisco AnyConnect と ISE を使用した MACsec スイッチ/ホスト間暗号化の設定例

Document ID: 117277

Updated: 2014 年 1 月 31 日

著者：Cisco TAC エンジニア、Michal Garcarz および Roman Machulik

関連製品

- セキュリティ
- 802.1X
- Cisco Identity Services Engine

目次

概要

このドキュメントでは、802.1x サプリカント（Cisco AnyConnect モバイル セキュリティ）とオーセンティケータ（スイッチ）間での Media Access Control Security（MACsec）の暗号化の設定例を紹介しています。 Cisco Identity Services Engine（ISE）は、認証およびポリシー サーバとして使用されます。

MACsec は 802.1AE で標準化され、Cisco 3750X、3560X、および 4500 SUP7E のスイッチでサポートされます。 802.1AE は、アウトオブバンド キーを使用する有線ネットワーク上のリンク暗号化を定義します。 これらの暗号化キーは、802.1X 認証が成功した後に使用される MACsec Key Agreement（MKA）プロトコルとネゴシエートされます。 MKA は、IEEE 802.1X-2010 で標準化されています。

PC とスイッチ（ポイントツーポイントの暗号化）間のリンク上のパケットのみが暗号化されます。 スイッチで受信されたパケットは復号化され、暗号化されたアップリンクを介して送信されます。 スイッチ間の伝送を暗号化するには、スイッチ間暗号化が推奨されています。 この暗号化では、キーをネゴシエートし、再生成するために、Security Association Protocol（SAP）が使用されます。 SAP は、シスコによって開発された先行標準のキー アグリーメント プロトコルです。

前提条件

要件

次の項目に関する知識が推奨されます。

- 802.1x の設定に関する基本的な知識
- Catalyst スイッチの CLI 設定に関する基本的な知識
- 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くものです。

- Microsoft Windows 7 および Microsoft Windows XP オペレーティング システム
- Cisco 3750X ソフトウェア バージョン 15.0 以降
- Cisco ISE ソフトウェア バージョン 1.1.4 以降
- Network Access Manager（NAM）バージョン 3.1 以降を備えた Cisco AnyConnect Mobile Security

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

ネットワーク ダイアグラムとトラフィック フロー

ステップ 1： サプリカント（AnyConnect NAM）は 802.1x セッションを開始します。 スイッチはオーセンティケータになり、ISE は認証サーバになります。 Extensible Authentication Protocol over LAN（EAPOL）プロトコルは、サプリカントとスイッチ間の EAP の転送として使用されます。 RADIUS は、スイッチと ISE 間の EAP の転送プロトコルとして使用されます。 EAPOL キーを ISE から返し、MACsec Key Agreement（MKA）セッションに使用する必要があるため、MAC 認証バイパス（MAB）は使用できません。

ステップ 2： 802.1x セッションが完了した後、スイッチはトランスポート プロトコルとして EAPOL を使用して MKA セッションを開始します。 サプリカントが正しく設定されている場合は、対称 128 ビット AES-GCM（ガロア/カウンタ モード）暗号化のキーが一致します。

ステップ 3： サプリカントとスイッチ間のすべての後続パケットは暗号化されます（802.1AE カプセル化）。

設定

ISE

ISE 設定には、暗号化ポリシーが含まれることのある認可プロファイルの例外を除き、一般的な 802.1X シナリオが含まれます。

[Administration] > [Network Resources] > [Network Devices] の順に選択して、スイッチをネットワーク デバイスとして追加します。 RADIUS の事前共有鍵（共有秘密）を入力します。

デフォルトの認証ルールを使用できます（ISE のローカルで定義されているユーザの場合）。

[Administration] > [Identity Management] > [Users] の順に選択し、ユーザ「cisco」をローカルで定義します。

認可プロファイルに暗号化ポリシーが含まれる場合があります。 次の例に示すように、[Policy] > [Results] > [Authorization Profiles] の順に選択し、リンクの暗号化が必須になるスイッチに ISE が返す情報を表示します。 また、VLAN 番号（10）が設定されています。

認可ルールの認可プロファイルを使用するために、[Policy] > [Authorization] の順に選択します。 この例では、ユーザ「cisco」に設定されているプロファイルを返します。 802.1x が成功した場合、ISE は Radius-Accept を Cisco AVPair linksec-policy=must-secure でスイッチに返します。 この属性によって、スイッチは MKA セッションを開始します。 そのセッションが失敗すると、スイッチでの 802.1x 認証も失敗します。

スイッチ

一般的な 802.1X ポート設定には以下が含まれます（先頭の一部が示されています）。

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

```
aaa group server radius ISE
 server name ISE

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order dot1x
 authentication port-control auto
 dot1x pae authenticator

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 timeout 5
 retransmit 2
key cisco
```

ローカル MKA ポリシーが作成され、インターフェイスに適用されます。 また、MACsec がインターフェイスで有効にされます。

```
mka policy mka-policy
 replay-protection window-size 5000

interface GigabitEthernet1/0/2
 macsec
 mka policy mka-policy
```

ローカル MKA ポリシーでは、ISE からプッシュできない詳細設定を設定することができます。 ローカル MKA ポリシーは、オプションです。

AnyConnect NAM

802.1X サプリカントのプロファイルは、手動で設定するか、Cisco ASA を介してプッシュできます。 次の手順には、手動設定が示されています。

NAM プロファイルを管理するには、以下の手順を実行します。

MACsec で新しい 802.1x プロファイルを追加します。 802.1x の場合、Protected Extensible Authentication Protocol（PEAP）が使用されます（ISE で設定済みのユーザ「cisco」）。

確認

ここでは、設定が正常に動作していることを確認します。

EAP-PEAP に設定された AnyConnect NAM には、正しいクレデンシャルが必要です。

スイッチのセッションは、認証および許可する必要があります。 セキュリティ ステータスが「Secured」である必要があります。

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
```

```
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Secured
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D56FD55B3BF
     Acct Session ID:  0x00011CB4
              Handle:  0x97000D57

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

スイッチの MACsec 統計情報には、ローカル ポリシー設定、送受信トラフィックのセキュア チャネル ID（SCI）、ポートの統計やエラーに関する詳細が示されます。

```
bsns-3750-5#show macsec interface g1/0/2
 MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
  Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
  SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

AnyConnect では、統計情報に暗号化の使用率およびパケットの統計が示されます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

作業シナリオのデバッグ

スイッチ上でのデバッグを有効にします（一部の出力は、わかりやすくするために省略されています）。

```
bsns-3750-5#show macsec interface g1/0/2
 MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
  Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
  SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

802.1x セッションが確立されると、複数の EAP パケットが EAPOL 上で交換されます。 Radius-Acccept 内で伝達される ISE からの最後の成功応答（EAP 成功）にも、複数の RADIUS 属性が含まれています。

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS:  EAP-Key-Name        [102] 67  *
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "linksec-policy=must-secure"
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Send-Key   [16]  52  *
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Recv-Key   [17]  52  *
```

MKA セッションでは EAP キー名が使用されます。 linksec ポリシーによって、スイッチでは MACsec が使用されます（MACsec が完全でない場合、認証は失敗します）。 これらの属性は、パケット キャプチャでも確認できます。

Authentication is successful.

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

スイッチは属性を適用します（これには送信されたオプションの VLAN 番号も含まれます）。

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

スイッチは、EAPOL パケットを送受信すると MKA セッションを開始します。

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

その後、4 個のパケット交換セキュア ID が受信（RX）セキュリティ アソシエーションとともに作成されます。

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```

セッションは終了し、送信（TX）セキュリティ アソシエーションが追加されます。

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
HULC-MACsec: Process install TxSA request66B4EEC for interface GigabitEthernet1/0/
```

ポリシー「must-secure」が一致すると、認証が成功します。

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

2 秒 ごとに MKA Hello パケットが交換され、すべての対象が動作していることが確認されます。

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

失敗シナリオのデバッグ

サプリカントが MKA に対して設定されていないときに、正常な 802.1X 認証の後で ISE が暗号化を要求する場合：

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

スイッチは 5 個の EAPOL パケットを送信するときに MKA セッションを開始しようとします。

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

最終的にタイムアウトになり、認証は失敗します。

```
 %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) MKA Session was stopped by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

802.1x セッションは正常な認証を報告しますが、認証は失敗します。

```
bsns-3750-5#show authentication sessions int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Failed
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D55FD4D7529
     Acct Session ID:  0x00011CA0
              Handle:  0xA4000D56

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

データ トラフィックはブロックされます。

パケット キャプチャ

サプリカント サイトでトラフィックがキャプチャされると、4 個の Internet Control Message Protocol（ICMP）エコー要求/応答が送受信され、以下が実行されます。

- 4 個の暗号化 ICMP エコー要求をスイッチに送信（802.1AE のために 88e5 が予約されています）
- 4 個の復号化 ICMP エコー応答を受信

これは AnyConnect が Windows API にフックされる方法のためです（パケットが送信されるときの libpcap の前、およびパケットが受信されるときの libpcap の前）。

> **注:** スイッチド ポート アナライザ（SPAN）または組み込みパケット キャプチャ（EPC）などの機能を持つスイッチで MKA または 802.1AE トラフィックをスニフィングする機能はサポートされていません。

MACsec と 802.1x モード

MACsec では、すべての 802.1x モードがサポートされているわけではありません。

『*Cisco TrustSec 3.0 How-To Guide: Introduction to MACsec and NDAC*』では、以下のように説明されています。

- **Single-Host モード**： Single-Host モードでは、**MACsec は完全にサポート**されます。 このモードでは、単一の MAC アドレスまたは IP アドレスだけが認証され、MACsec で保護されます。 エンドポイントが認証した後に別の MAC アドレスがポートで検出されると、セキュリティ違反がポートでトリガーされます。
- **Multi-Domain Authentication (MDA) モード**： このモードでは、1 つのエンドポイントをデータ ドメイン上に配置し、別のエンドポイントを音声ドメイン上に配置することができます。 **MDA モードでは、MACsec は 完全にサポートされます。** 両方のエンドポイントが MACsec 可能であれば、それぞれの独立した MACsec セッションによってそれぞれが保護されます。 一方のエンドポイントだけが MACsec 可能である場合、そのエンドポイントは保護できますが、もう一方のエンドポイントでは暗号化されずにパケットが送信されます。
- **Multi-Authentication モード**： このモードでは、単一のスイッチ ポートに対して事実上無制限の数のエンドポイントを認証できます。 **このモードでは MACsec はサポートされていません。**
- **Multi-Host モード**： このモードで MACsec を使用することは技術上可能ですが、**推奨されていません。** Multi-Host モードでは、ポートの最初のエンドポイントが認証され、追加のエンドポイントはすべて、最初の認証を介してネットワークで許可されます。 MACsec は最初に接続されたホストでは機能しますが、それ以外のエンドポイントのトラフィックは、暗号化されたトラフィックではないため、実際には通過しません。

関連情報

- 3750 用 Cisco TrustSec 設定ガイド
- ASA 9.1 用 Cisco TrustSec 設定ガイド
- Identity-Based Networking Services： MAC セキュリティ
- TrustSec Cloud with 802.1x MACsec on Catalyst 3750X シリーズ スイッチの設定例
- 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 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

Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Updated: 2014 年 1 月 31 日
Document ID: 117277