ISEでのRADIUSキーラップの設定

内容

はじめに

このドキュメントでは、Cisco ISEおよびCiscoスイッチでRADIUSキーラップを設定する手順について説明します。

前提条件

- dot1xの知識
- RADIUSプロトコルの知識
- EAPに関する知識

使用するコンポーネント

- ISE 3.2
- ソフトウェアバージョン17.09.04aが稼働するCisco C9300-24U
- Windows 10 PC

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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

キーラッピングは、あるキー値を別のキーを使用して暗号化する手法です。RADIUSでは、同じメカニズムを使用してキーマテリアルを暗号化します。 この資料は通常、拡張可能認証プロトコ

ル(EAP)認証の副産物として作成され、認証が成功した後にAccess-Acceptメッセージで返されます。ISEがFIPSモードで実行されている場合、この機能は必須です。

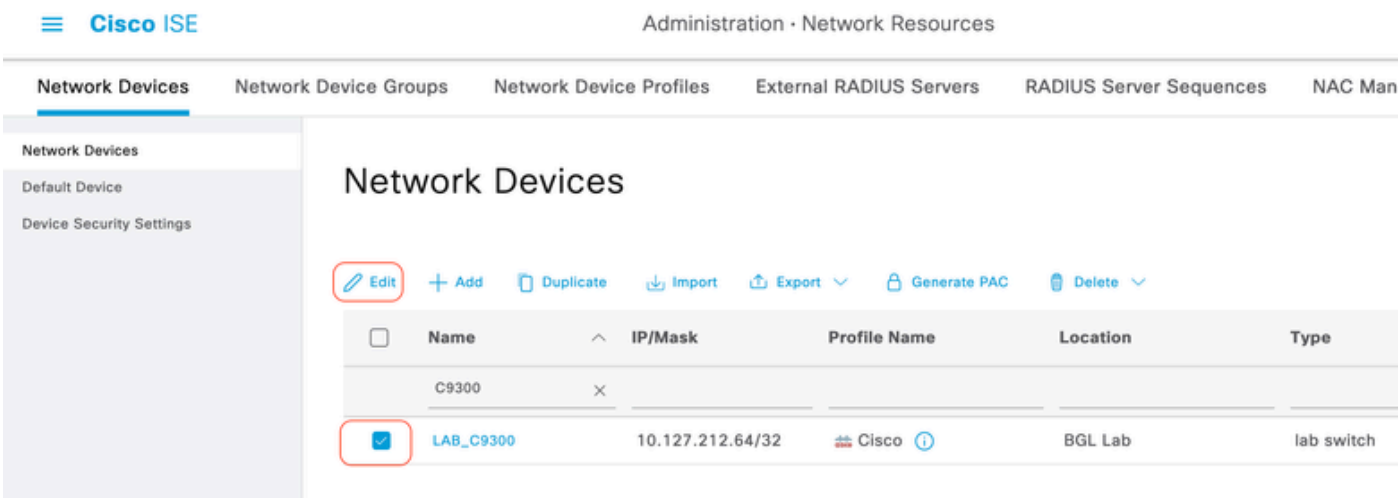
これにより、潜在的な攻撃から保護するために、実際の主要な要素を分離する保護層が提供されます。データ傍受の場合でも、基本的に基盤となる重要な情報に脅威アクターは実質的にアクセスできなくなります。RADIUSキーラッピングの主な目的は、デジタルコンテンツを保護する主要な資料の漏洩を防止することです。特に、大規模な企業レベルのネットワークにおいて顕著です。

ISEでは、メッセージ認証コードを生成するために、AES暗号化とRADIUS共有秘密キーから分離されたメッセージ認証コードキーを使用してキー資料を暗号化するために、キー暗号化キー(KEK)が使用されます。

設定

ISE

ステップ1:Administration > Network Resources > Network Devicesの順に移動します。RADIUSキーラップを設定するネットワークデバイスのチェックボックスをオンにします。Editをクリックします（ネットワークデバイスがすでに追加されている場合）。



ステップ2:RADIUS認証設定を展開します。Enable KeyWrapチェックボックスをクリックします。Key Encryption KeyとMessage Authenticator Code Keyを入力します。[Save] をクリックします。

General Settings

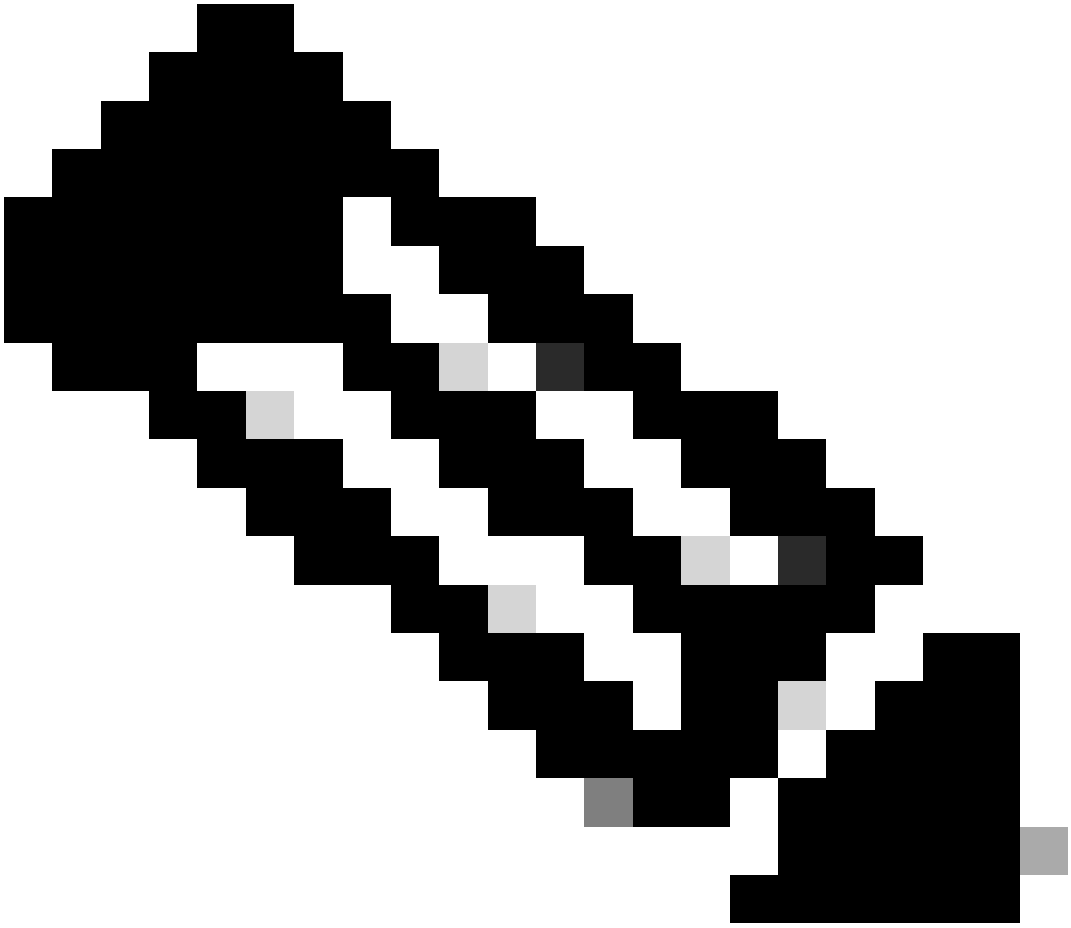
Enable KeyWrap

Key Encryption Key 22AB0###CA#1b2b1 Hide

Message Authenticator Code Key 12b1CcB202#2Cb1#bCa# Hide

Key Input Format

ASCII HEXADECIMAL



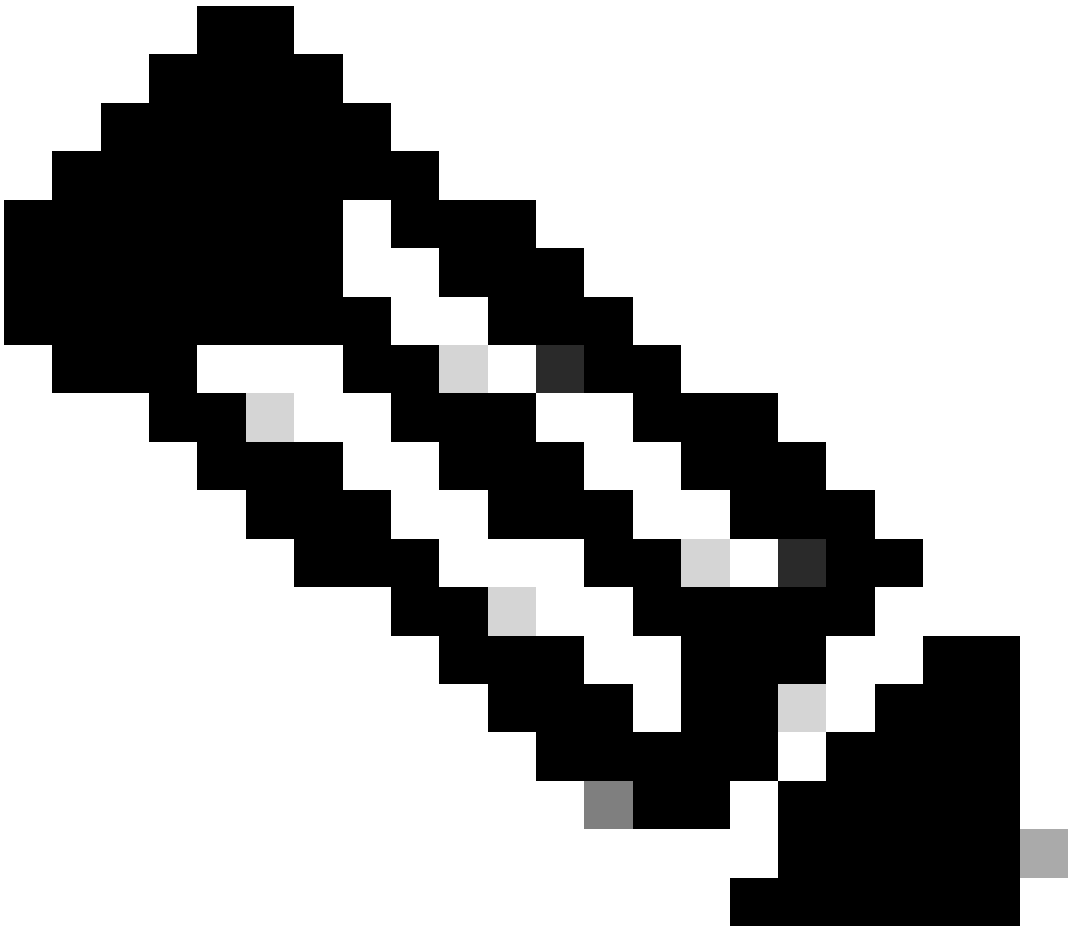
注:Key Encryption KeyとMessage Authenticator Code Keyは異なっている必要があります。

最大 300 のアクセス ポイント グループ

RADIUSキーラップ機能を有効にするためのスイッチでのAAA設定。

```
aaa authentication dot1x default group RADGRP
aaa authorization network default group RADGRP
aaa accounting dot1x default start-stop group RADGRP

radius server ISERAD
 address ipv4 10.127.197.165 auth-port 1812 acct-port 1813
 key-wrap encryption-key 0 22AB0###CA#1b2b1 message-auth-code-key 0 12b1CcB202#2Cb1#bCa# format ascii
 key Iselab@123

aaa group server radius RADGRP
 server name ISERAD
 key-wrap enable
```

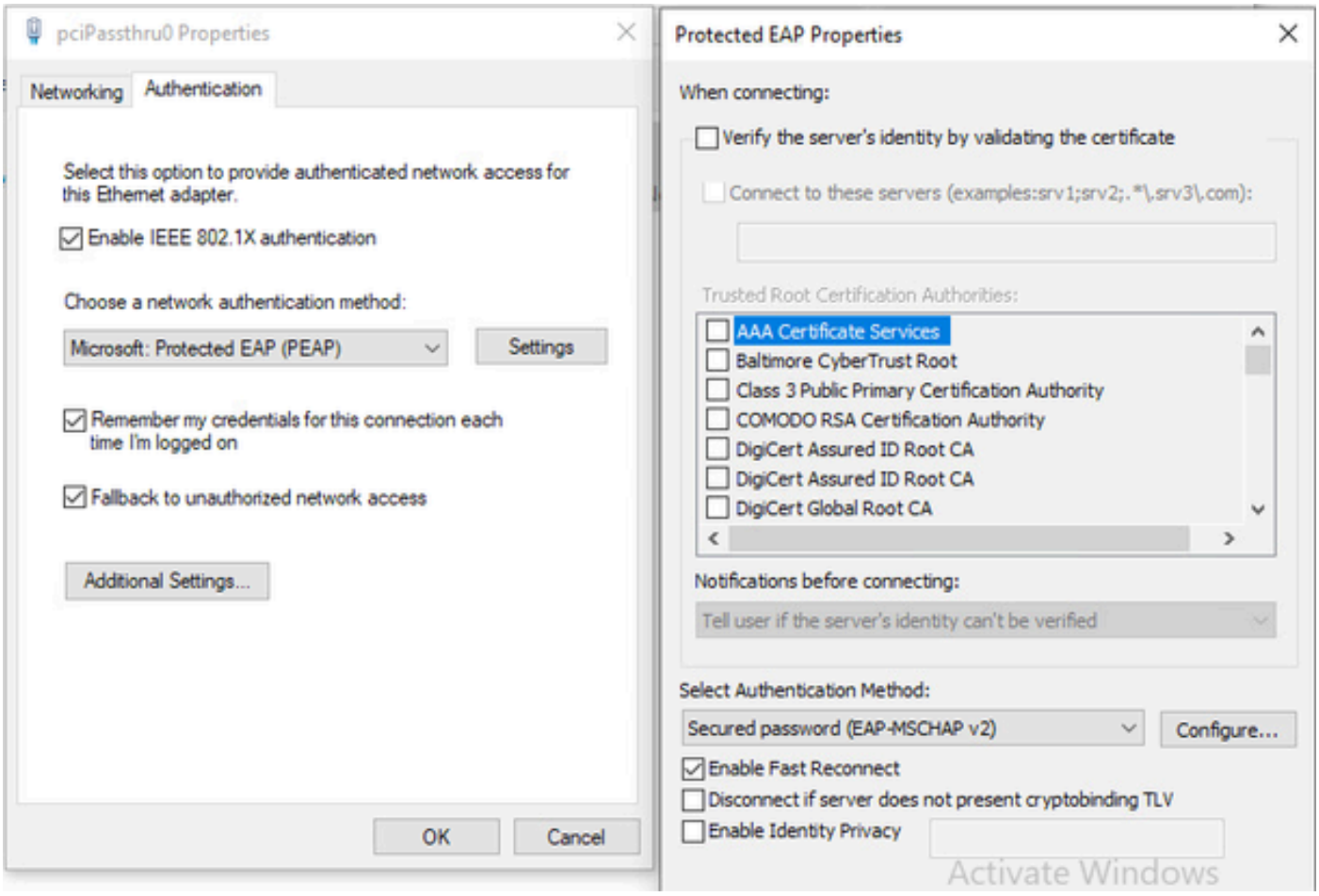
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



注：暗号化キーは、16文字の長さとmessage-auth-code、20文字の長さにする必要があります。

PC

PEAP-MSCHAPv2用に設定されたWindows 10サプリカント。



確認

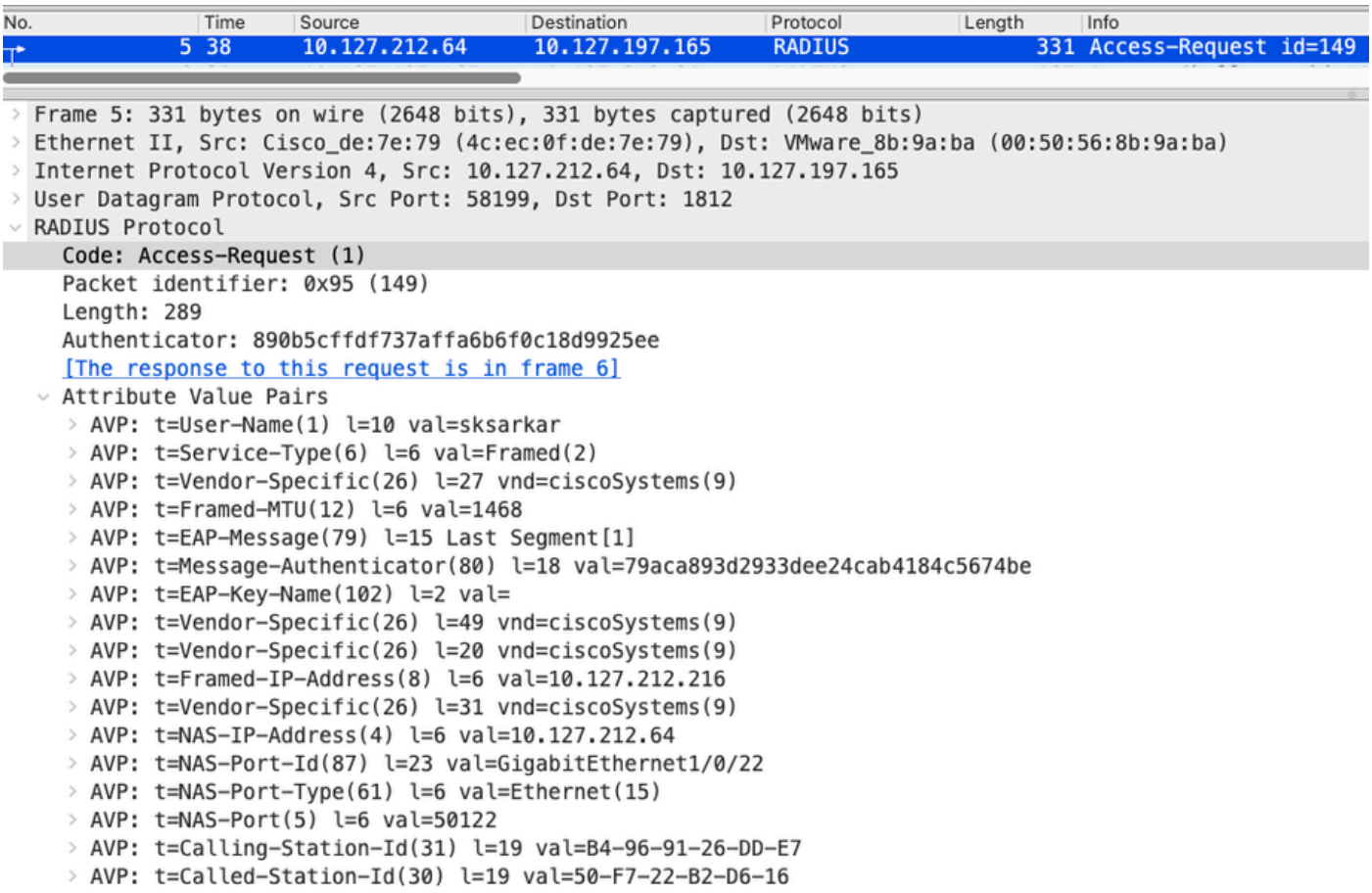
スイッチでRADIUSキーラップ機能が有効になっていない場合：

show radius server-group <サーバグループ名>

このコマンドの出力では、Keywrap enabled: FALSEと表示されている必要があります。

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: FALSE
```

パケットキャプチャでは、app-key、random-nonce、およびseparate message-authenticator-codeに対するCisco-AV-Pair属性がないことがわかります。これは、RADIUS KeyWrapがスイッチで無効になっていることを示しています。

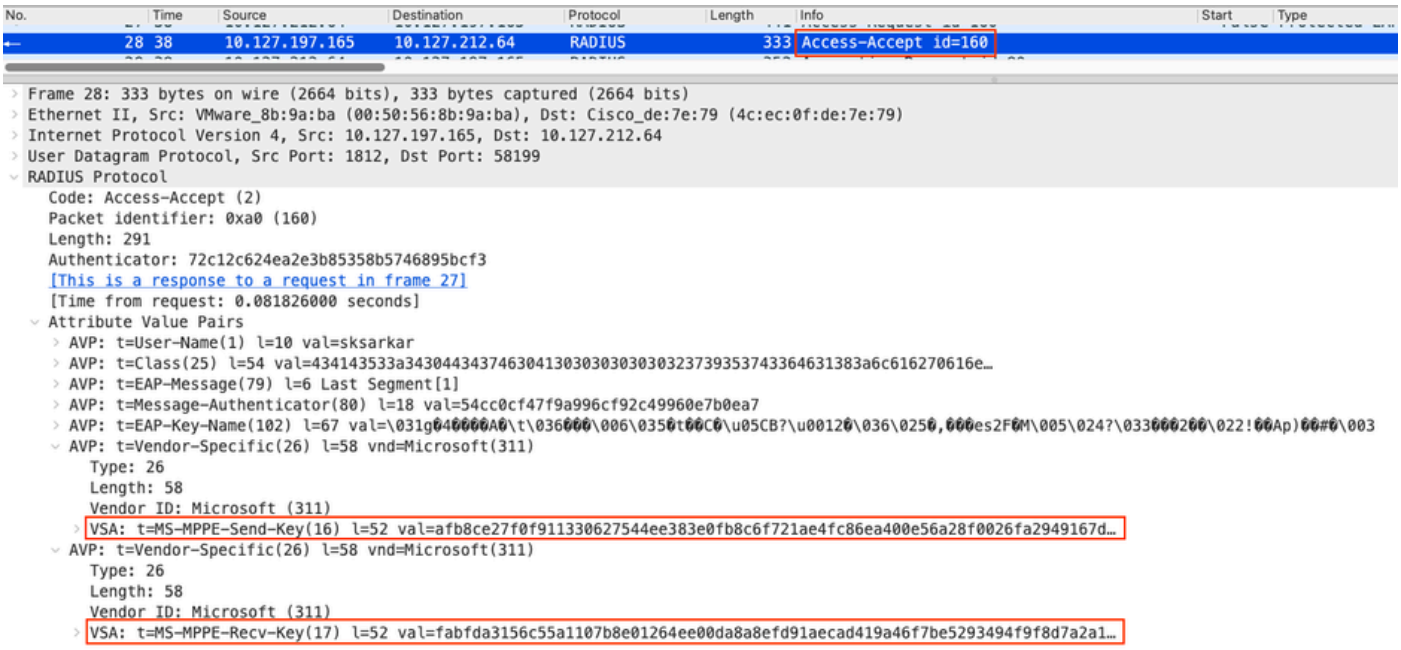


ISE prrt-server.logでは、ISEがメッセージ認証者である整合性属性のみを検証することが確認できます。

```
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
[6] Service-Type - value: [Framed]
[8] Framed-IP-Address - value: [10.127.212.216]
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[80] Message-Authenticator - value: [<88>/`f

       |

        >

         <18><06>(
```

```
          ?


            ]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A0000002B9E06997E]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=292332370] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
```

Access-Acceptパケットには、MS-MPPE-Send-keyとMS-MPPE-Recv-KeyがRADIUSサーバからオーセンティケータに送信されたことが示されています。MS-MPPEは、ピアとオーセンティケータの間でデータの暗号化を実行するために使用できるEAP方式によって生成されるキー情報を指定します。これらの32バイトのキーは、RADIUS共有秘密、要求オーセンティケータ、およびランダムなsaltから取得されます。



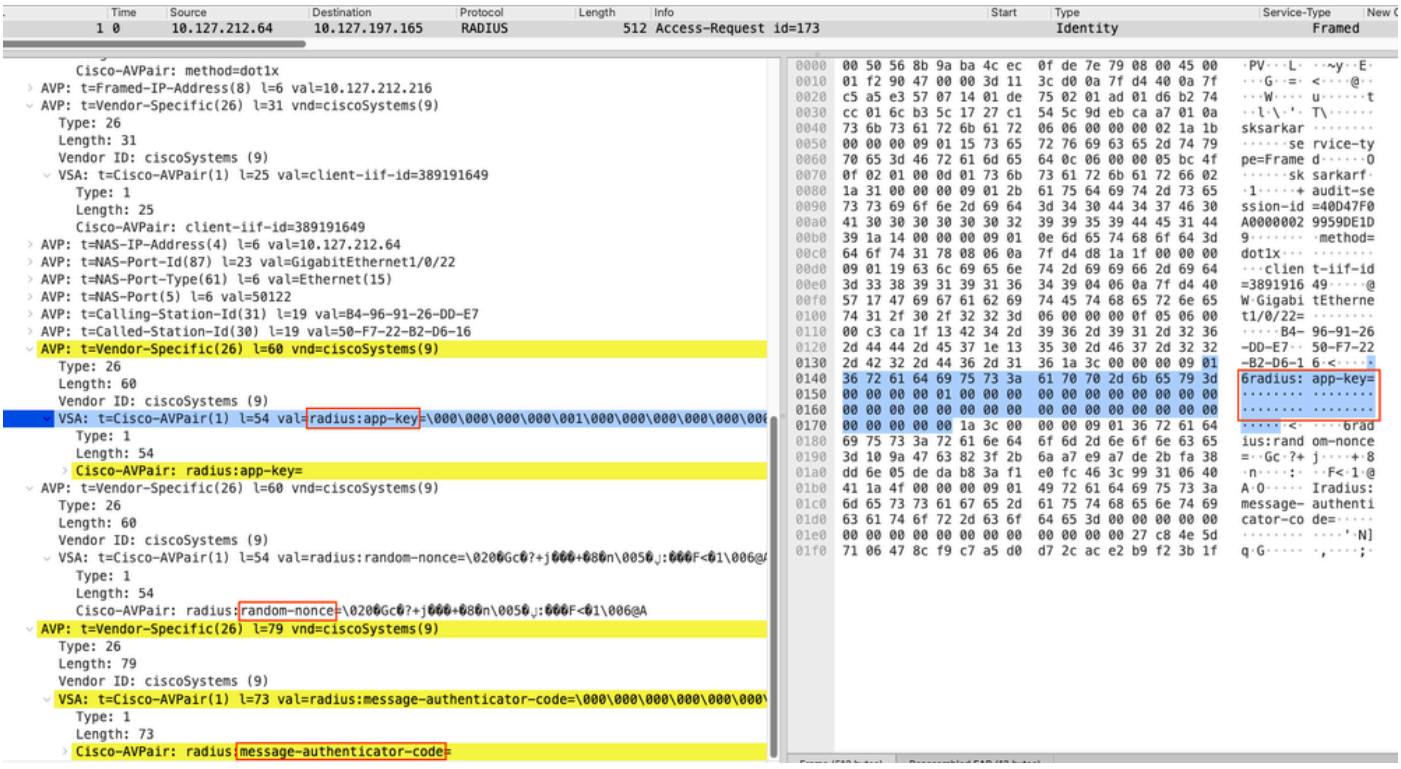
RADIUSキーラップ機能がスイッチとISEで有効になっている場合：

show radius server-group <サーバグループ名>

このコマンドの出力には、Keywrap enabled: TRUEと表示される必要があります。

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: TRUE
```

パケットキャプチャでは、app-key（データなし）、random-nonce、および個別のmessage-authenticator-codeに対するCisco-AV-Pair属性が存在することがわかります。これは、オーセンティケータ（スイッチ）がRADIUS KeyWrapをサポートし、サーバが同じキーを使用する必要があることをRADIUSサーバに示します。

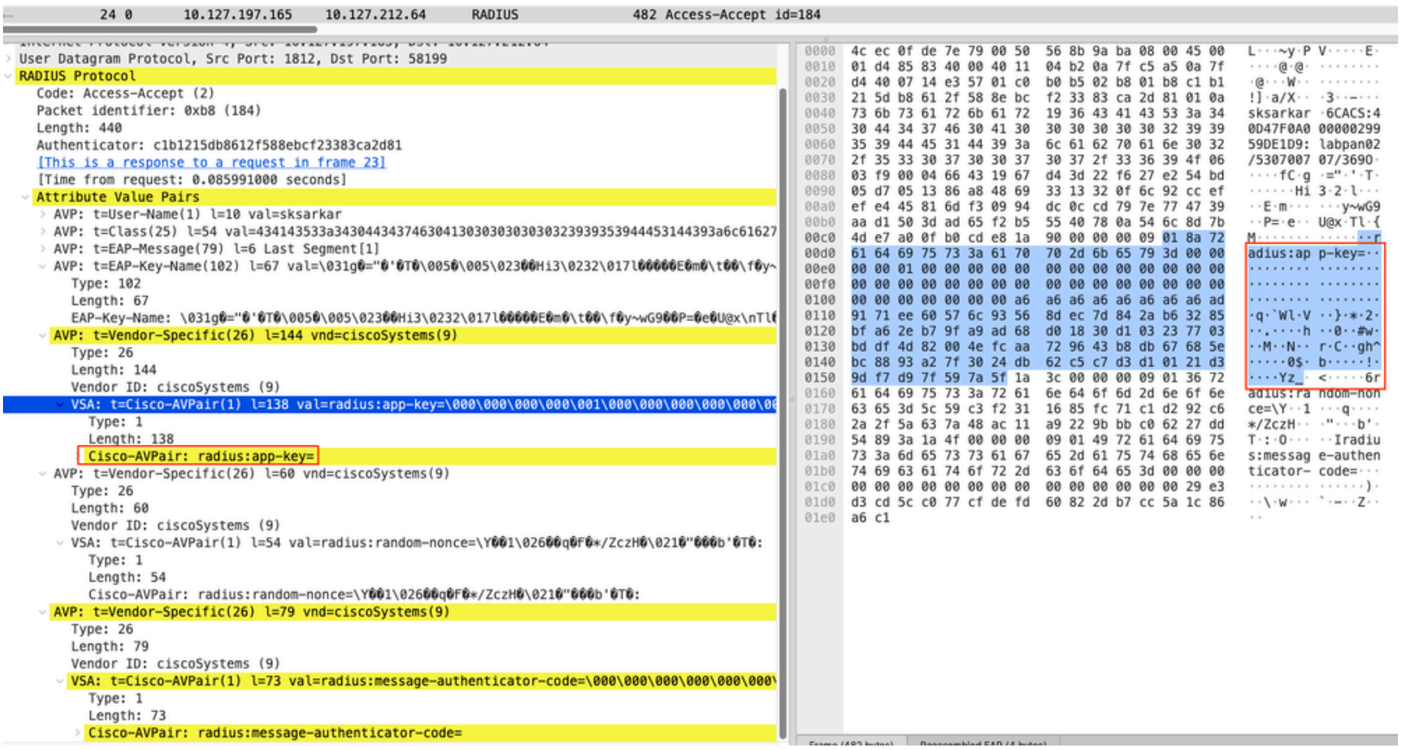


ISE prrt-server.logでは、ISEが属性app-keyを検証し、ACCESS-REQUESTパケットにrandom-nonceおよびmessage-authenticator-codeが含まれていることを確認できます。

```
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
[6] Service-Type - value: [Framed]
```

```
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A000000319E1CAEFD]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=293712201]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
```

Access-Acceptパケットでは、app-key属性の暗号化されたキーの内容が、random-nonceおよびmessage-authenticator-codeとともに表示されます。これらの属性は、現在定義されているベンダー固有のMS-MPPE-Send-Key属性およびMS-MPPE-Recv-Key属性よりも強力な保護と柔軟性を提供するように設計されています。



よく寄せられる質問（FAQ）

1)機能させるには、ネットワークデバイスとISEの両方でRADIUS KeyWarpを有効にする必要がありますか。

はい。RADIUS KeyWrapを機能させるには、ネットワークデバイスとISEの両方で有効にする必要があります。KeyWrapを有効にするのはISEだけで、ネットワークデバイスでは有効にしていない場合でも、認証は機能します。ただし、ISEではなくネットワークデバイスで有効にすると、認証は失敗します。

2) KeyWrapを有効にすると、ISEとネットワークデバイスのリソース使用率が増加しますか。

いいえ。KeyWrapを有効にしても、ISEとネットワークデバイスのリソース使用率は大幅に増加しません。

3) RADIUS KeyWrapではどのくらいのセキュリティが追加されますか。

RADIUS自体はペイロードに暗号化を提供しないため、KeyWrapはキーの内容を暗号化することでセキュリティを強化します。セキュリティレベルは、キーの内容の暗号化に使用される暗号化アルゴリズムによって異なります。ISEでは、キー関連情報の暗号化にAESが使用されます。

参考

- キー関連情報の配信に使用するCiscoベンダー固有のRADIUSアトリビュート

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。