Configuration du retour automatique à la ligne RADIUS dans ISE

Table des matières

Introduction

Ce document décrit la procédure de configuration de l'encapsulation de clé RADIUS dans Cisco ISE et le commutateur Cisco.

Conditions préalables

- Connaissance de dot1x
- Connaissance du protocole RADIUS
- Connaissance du PAE

Composants utilisés

- ISE 3.2
- Cisco C9300-24U avec version logicielle 17.09.04a
- PC Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'encapsulation de clé est une technique dans laquelle une valeur de clé est chiffrée à l'aide d'une

autre clé. Le même mécanisme est utilisé dans RADIUS pour chiffrer la clé. Cette clé est généralement produite comme sous-produit d'une authentification EAP (Extensible Authentication Protocol) et renvoyée dans le message d'acceptation d'accès après une authentification réussie. Cette fonctionnalité est obligatoire si ISE s'exécute en mode FIPS.

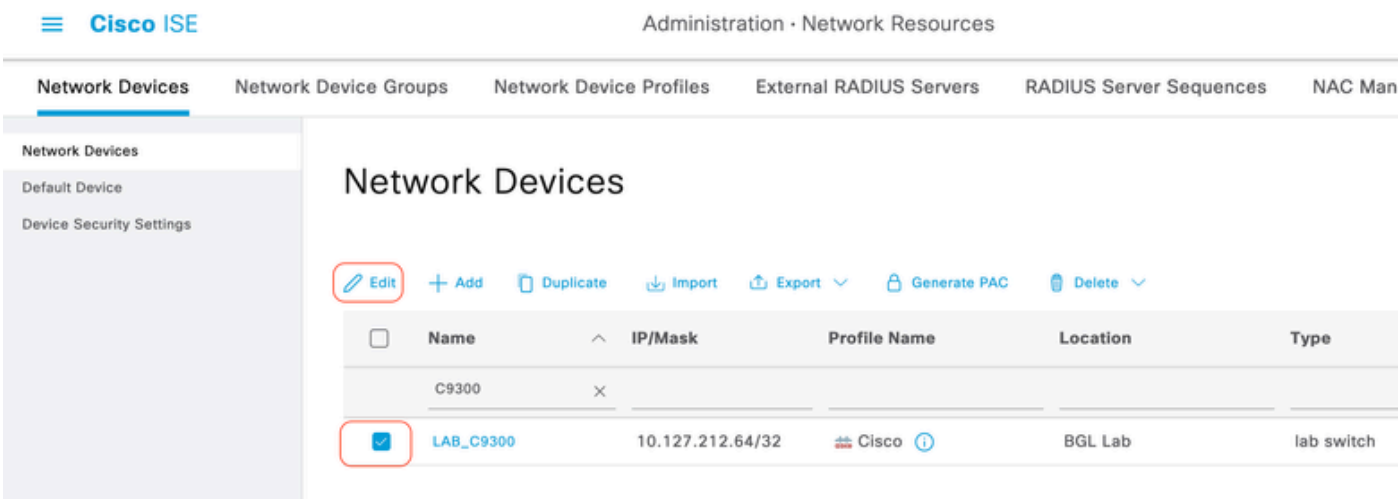
Cela fournit une couche de protection qui isole le matériel clé réel pour la protection contre les attaques potentielles. Les éléments clés sous-jacents deviennent pratiquement inaccessibles aux hackers, même en cas d'interception de données. L'objectif principal de l'encapsulation des clés RADIUS est d'empêcher l'exposition de documents clés qui sécurisent le contenu numérique, en particulier dans un réseau d'entreprise à grande échelle.

Dans ISE, la clé de chiffrement de clé est utilisée pour chiffrer les éléments clés avec le chiffrement AES et la clé de code d'authentificateur de message séparée de la clé secrète partagée RADIUS afin de générer le code d'authentificateur de message.

Configurer

ISE

Étape 1 : Accédez à Administration > Network Resources > Network Devices. Cochez la case correspondant au périphérique réseau pour lequel vous souhaitez configurer l'encapsulation de clé RADIUS. Cliquez sur Edit (si le périphérique réseau est déjà ajouté).



Étape 2 : Développez les paramètres d'authentification RADIUS. Cochez la case Enable KeyWrap. Saisissez la clé de cryptage de clé et la clé de code d'authentificateur de message. Cliquez sur Save.

General Settings

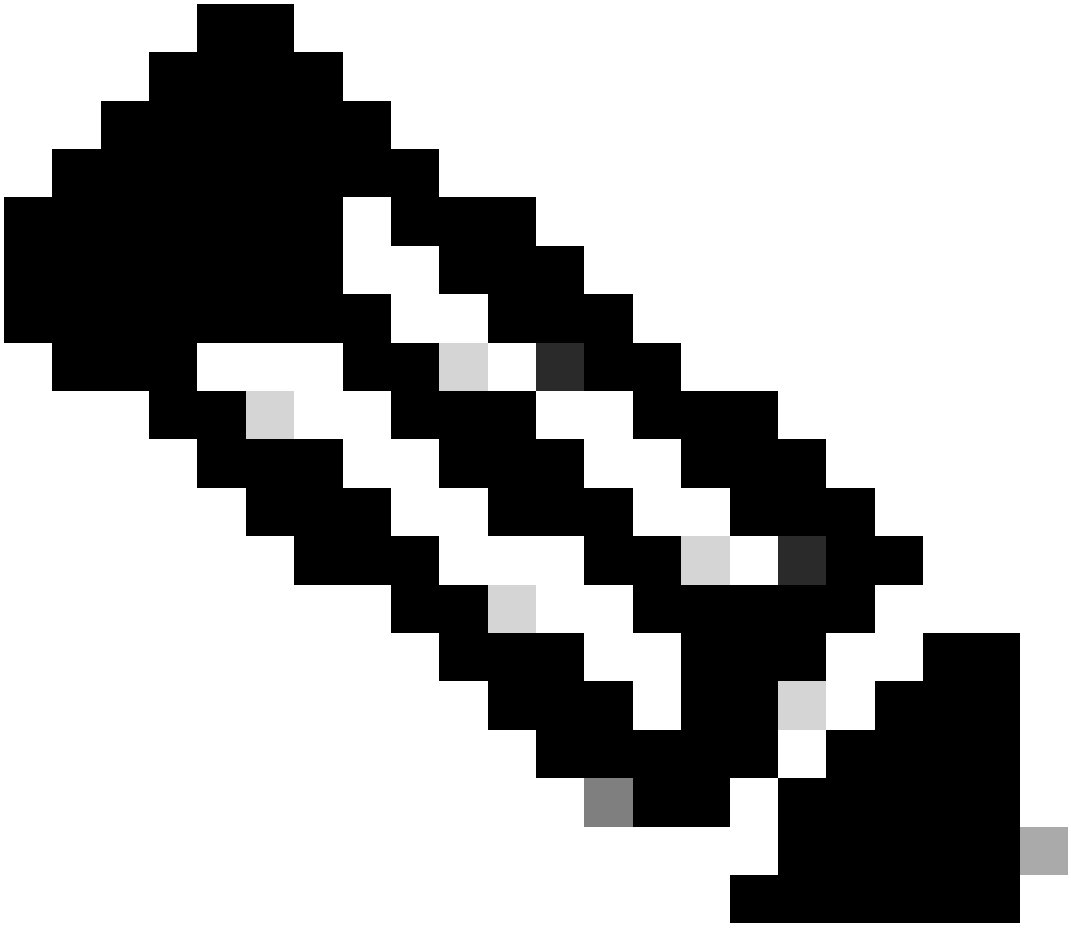
Enable KeyWrap

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

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

Key Input Format

ASCII HEXADECIMAL



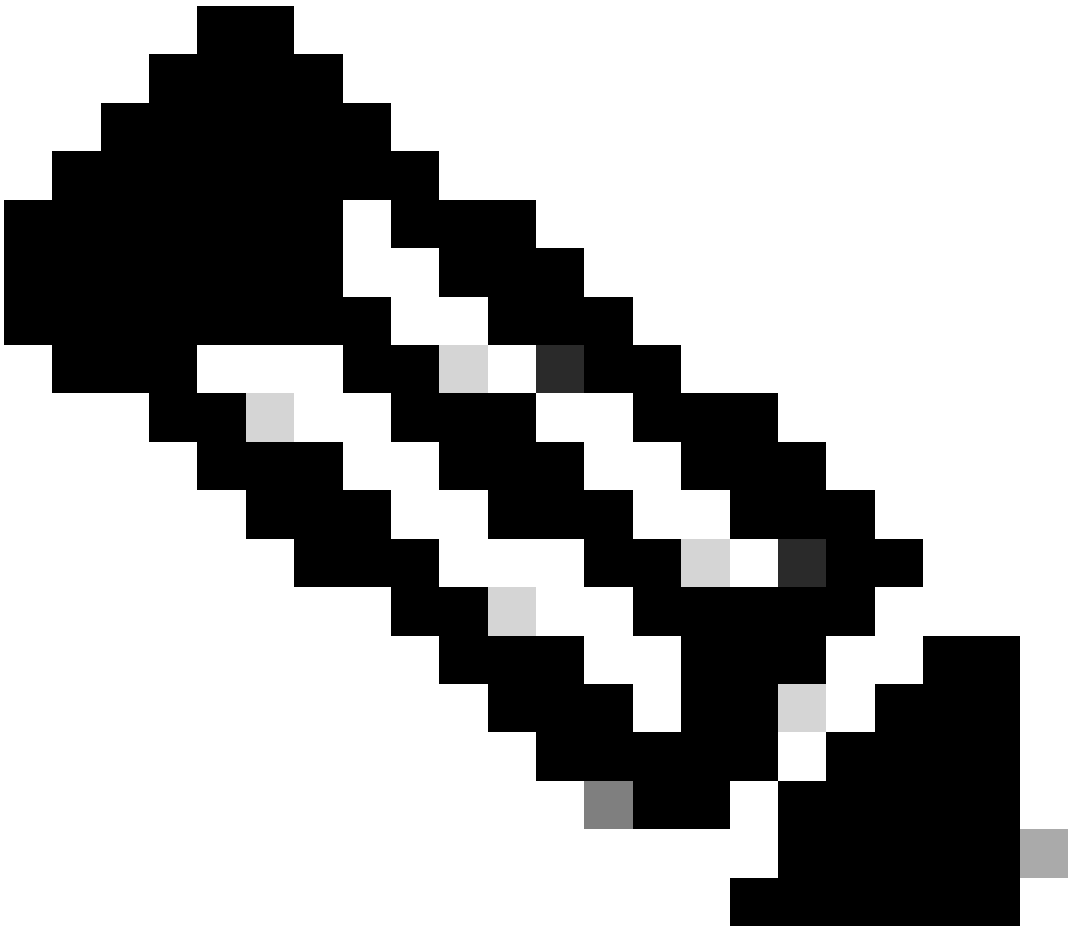
Remarque : la clé de cryptage de clé et la clé de code d'authentificateur de message doivent être différentes.

Commutateur

Configuration AAA dans le commutateur pour activer la fonctionnalité RADIUS KeyWrap.

```
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
```

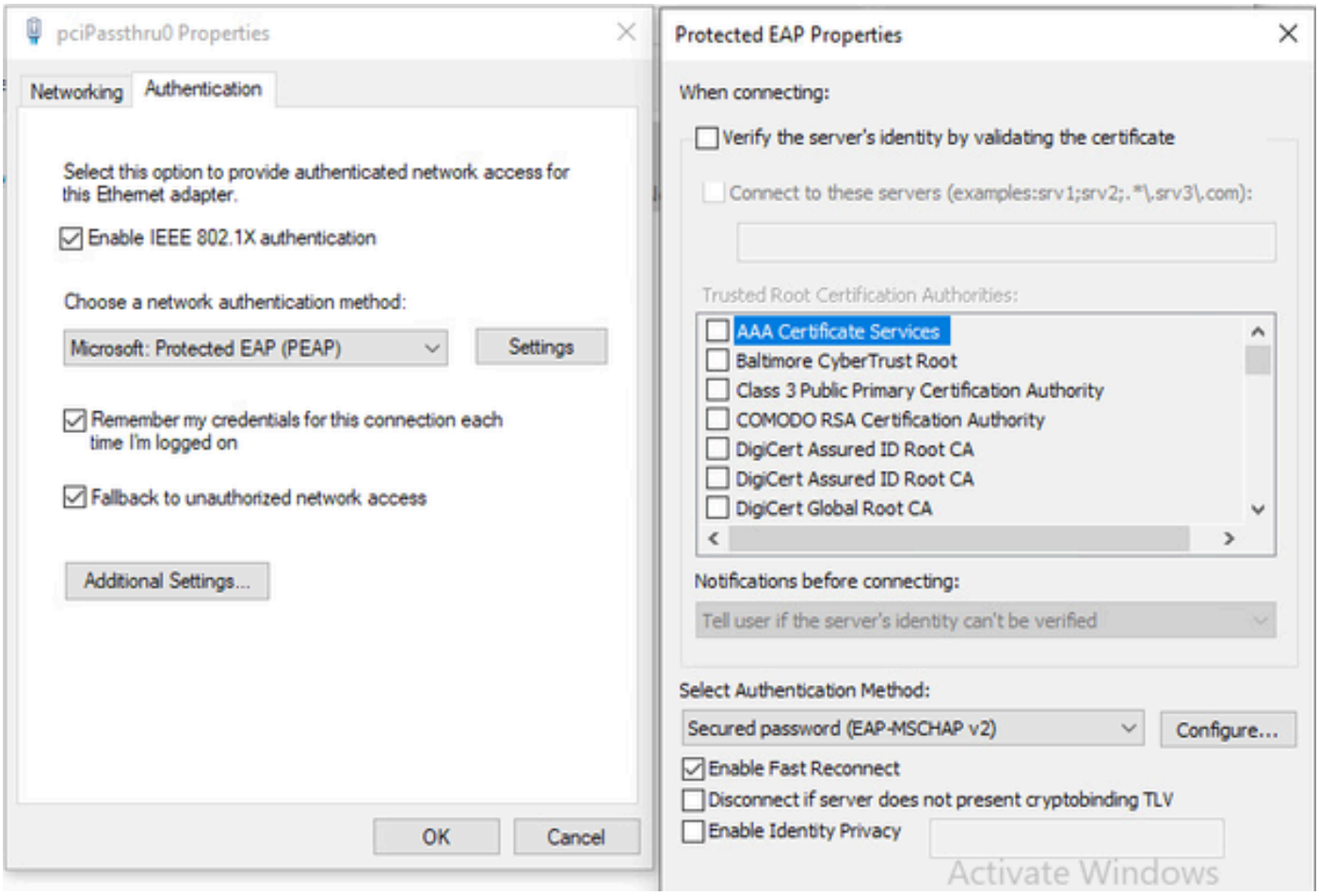
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



> Remarque : La clé de chiffrement doit comporter 16 caractères, le code d'authentification du message et 20 caractères.

PC

Demandeur Windows 10 configuré pour PEAP-MSCHAPv2.



Vérifier

Lorsque la fonction RADIUS KeyWrap n'est pas activée sur le commutateur :

show radius server-group <NOM DU GROUPE DE SERVEURS>

La sortie de la commande doit indiquer Keywrap enabled : FAUX.

```
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
```

Dans la capture de paquets, vous pouvez voir qu'il n'y a pas d'attribut Cisco-AV-Pair pour app-key, random-nonce et message-authenticator-code séparé. Cela indique que le paramètre RADIUS KeyWrap est désactivé sur le commutateur.

```
No.    Time   Source          Destination      Protocol   Length   Info
5      38     10.127.212.64   10.127.197.165   RADIUS     331      Access-Request id=149
```

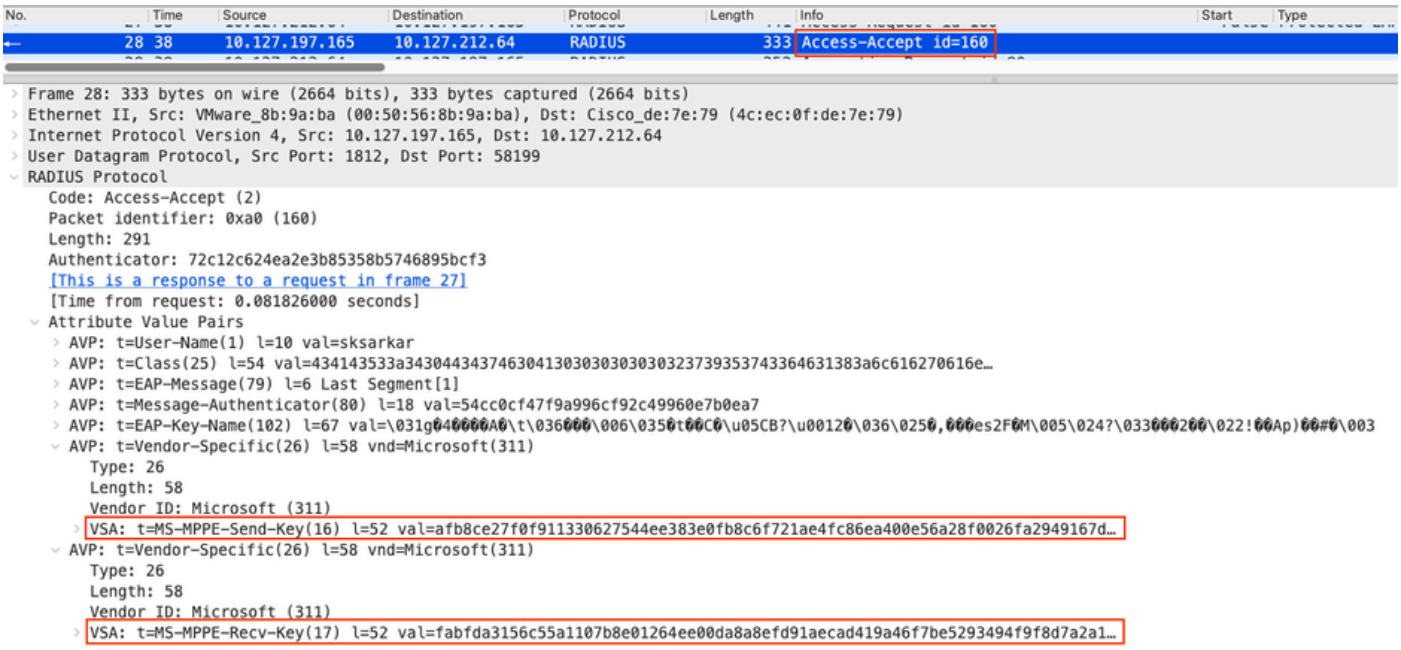
```
> Frame 5: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits)
> Ethernet II, Src: Cisco_de:7e:79 (4c:ec:0f:de:7e:79), Dst: VMware_8b:9a:ba (00:50:56:8b:9a:ba)
> Internet Protocol Version 4, Src: 10.127.212.64, Dst: 10.127.197.165
> User Datagram Protocol, Src Port: 58199, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x95 (149)
    Length: 289
    Authenticator: 890b5cffdf737affa6b6f0c18d9925ee
    [The response to this request is in frame 6]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=10 val=sksarkar
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1468
    > AVP: t=EAP-Message(79) l=15 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=79aca893d2933dee24cab4184c5674be
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=10.127.212.216
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=10.127.212.64
    > AVP: t=NAS-Port-Id(87) l=23 val=GigabitEthernet1/0/22
    > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
    > AVP: t=NAS-Port(5) l=6 val=50122
    > AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DD-E7
    > AVP: t=Called-Station-Id(30) l=19 val=50-F7-22-B2-D6-16
```

Dans le fichier ISE prt-server.log, vous pouvez voir qu'ISE valide uniquement l'attribut d'intégrité qui est Message-Authenticator.

```
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
```

Dans le paquet Access-Accept, vous pouvez voir que les clés MS-MPPE-Send-key et MS-MPPE-Recv-Key sont envoyées du serveur RADIUS à l'authentificateur. MS-MPPE spécifie le matériel clé généré par les méthodes EAP qui peuvent être utilisées pour effectuer le chiffrement des données entre l'homologue et l'authentificateur. Ces clés de 32 octets sont dérivées du secret partagé RADIUS, de l'authentificateur de requête et d'un sel aléatoire.



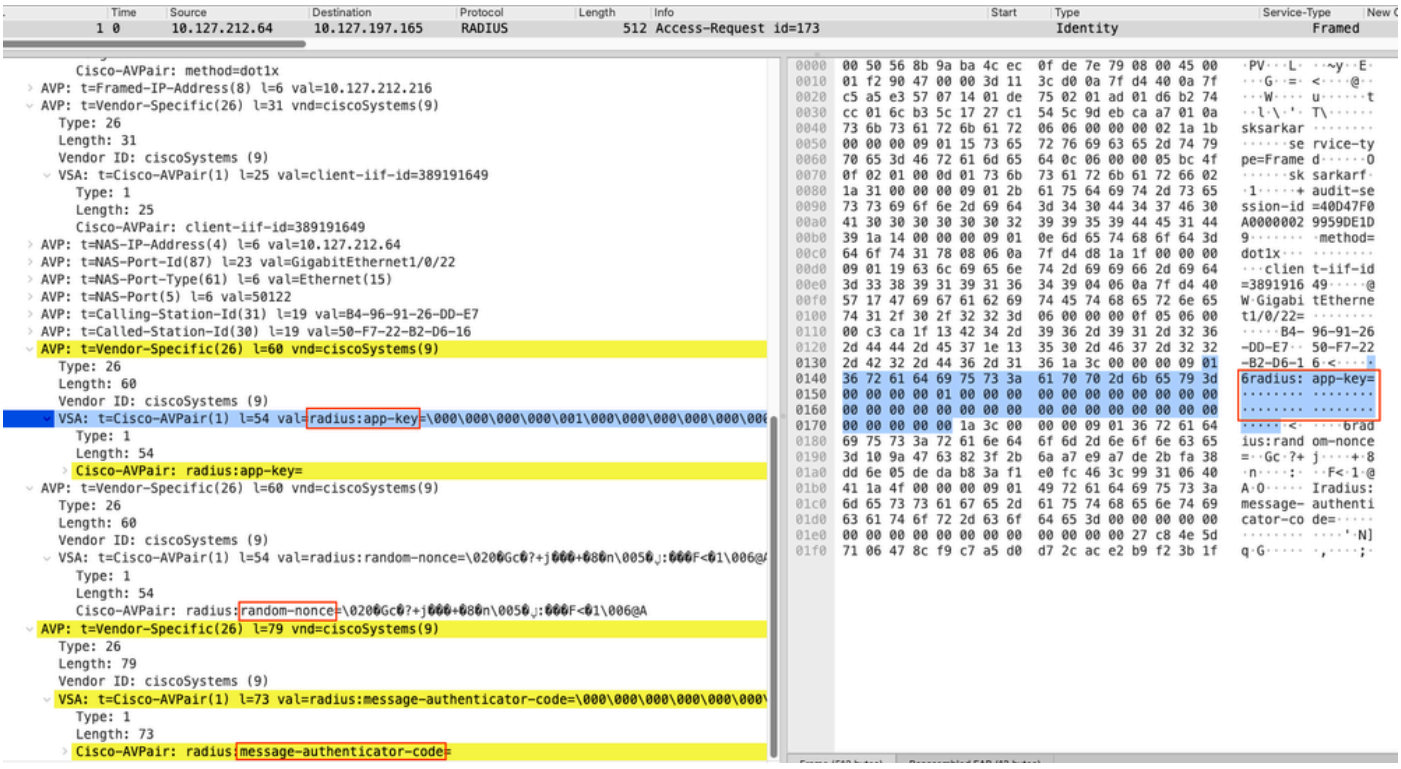
Lorsque la fonction RADIUS KeyWrap est activée sur le commutateur et ISE :

show radius server-group <NOM DU GROUPE DE SERVEURS>

Le résultat de la commande doit indiquer Keywrap enabled : VRAI.

```
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
```

Dans la capture de paquets, vous pouvez voir qu'il y a un attribut Cisco-AV-Pair pour app-key (sans données), random-nonce et message-authenticator-code séparés. Cela indique au serveur RADIUS que l'authentificateur (commutateur) prend en charge l'enveloppe de clé RADIUS et que le serveur doit l'utiliser.

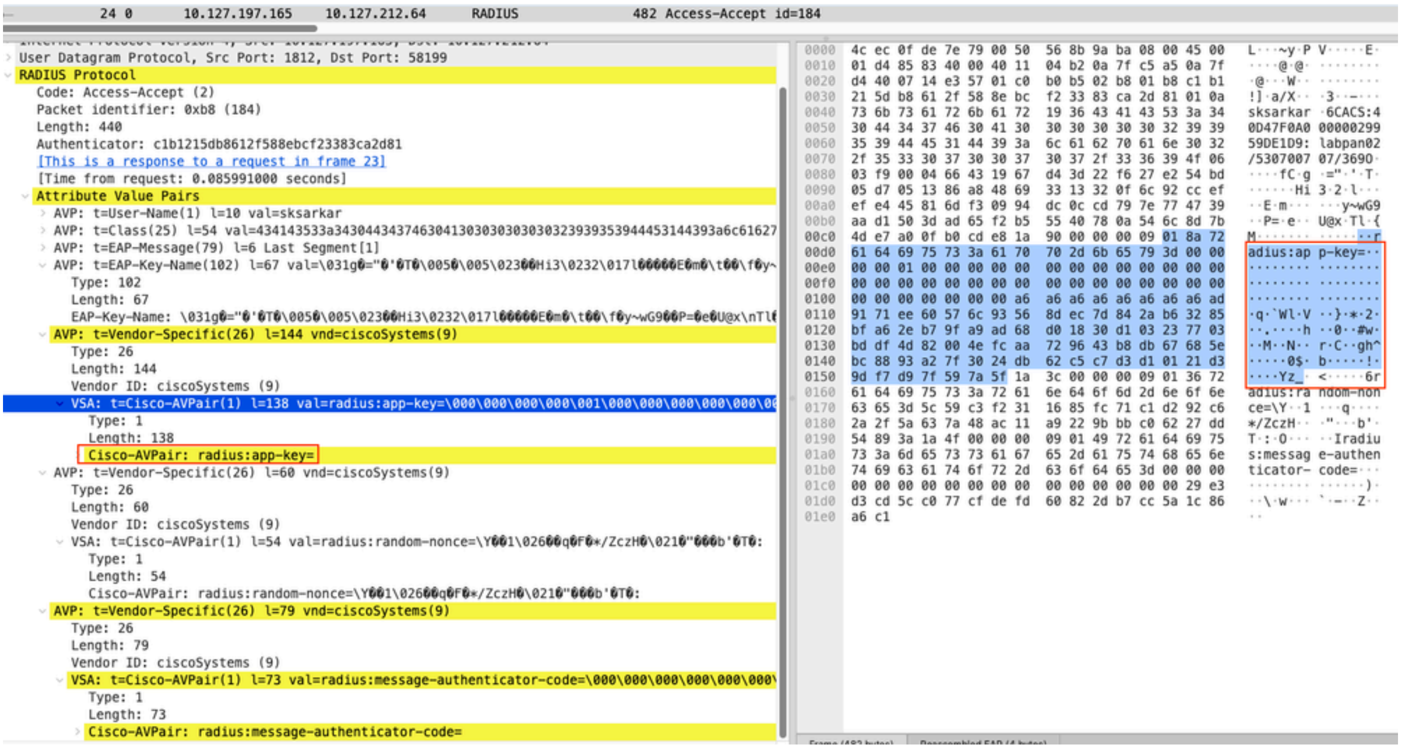


Dans le fichier ISE prt-server.log, vous pouvez voir qu'ISE valide les attributs app-key, et que random-nonce et message-authenticator-code sont venus dans le paquet ACCESS-REQUEST.

```
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
```

Dans le paquet d'acceptation d'accès, vous pouvez voir que les matériaux de clé chiffrés dans l'attribut app-key avec un random-nonce et message-authenticator-code. Ces attributs ont été conçus pour fournir une protection plus forte et une plus grande flexibilité que les attributs MS-MPPE-Send-Key et MS-MPPE-Recv-Key spécifiques au constructeur actuellement définis.



Forum aux questions

1) Est-ce que RADIUS KeyWarp doit être activé sur le périphérique réseau et ISE pour qu'il fonctionne ?

Oui, l'encapsulation de clé RADIUS doit être activée à la fois sur le périphérique réseau et sur ISE pour qu'elle fonctionne. Cependant, si vous activez KeyWrap uniquement sur l'ISE mais pas sur le périphérique réseau, l'authentification fonctionne toujours. Mais si vous l'avez activé sur un périphérique réseau mais pas dans ISE, l'authentification échoue.

2) L'activation de KeyWrap augmente-t-elle l'utilisation des ressources sur l'ISE et le périphérique réseau ?

Non, il n'y a pas d'augmentation significative de l'utilisation des ressources sur l'ISE et le périphérique réseau après l'activation de KeyWrap.

3) Quelle est la sécurité supplémentaire fournie par RADIUS KeyWrap ?

Comme le RADIUS lui-même ne fournit aucun chiffrement à sa charge utile, KeyWrap fournit une sécurité supplémentaire en chiffrant les éléments clés. Le niveau de sécurité dépend de l'algorithme de chiffrement utilisé pour chiffrer le matériel clé. Dans ISE, AES est utilisé pour chiffrer le matériel clé.

Référence

- Attributs RADIUS spécifiques au fournisseur Cisco pour la livraison de matériel de génération de clé

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.