Configuración de KeyWrap de RADIUS en ISE

Contenido

Introducción

Este documento describe el procedimiento para configurar RADIUS KeyWrap en Cisco ISE y Cisco Switch.

Prerequisites

- Conocimiento de dot1x
- Conocimiento del protocolo RADIUS
- Conocimiento de EAP

Componentes Utilizados

- ISE 3.2
- Cisco C9300-24U con versión de software 17.09.04a
- PC con Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El ajuste de clave es una técnica en la que un valor de clave se cifra mediante otra clave. El mismo mecanismo se utiliza en RADIUS para cifrar el material de clave. Este material se suele producir como un subproducto de una autenticación EAP (protocolo de autenticación extensible) y

se devuelve en el mensaje Access-Accept después de una autenticación correcta. Esta función es obligatoria si ISE se está ejecutando en modo FIPS.

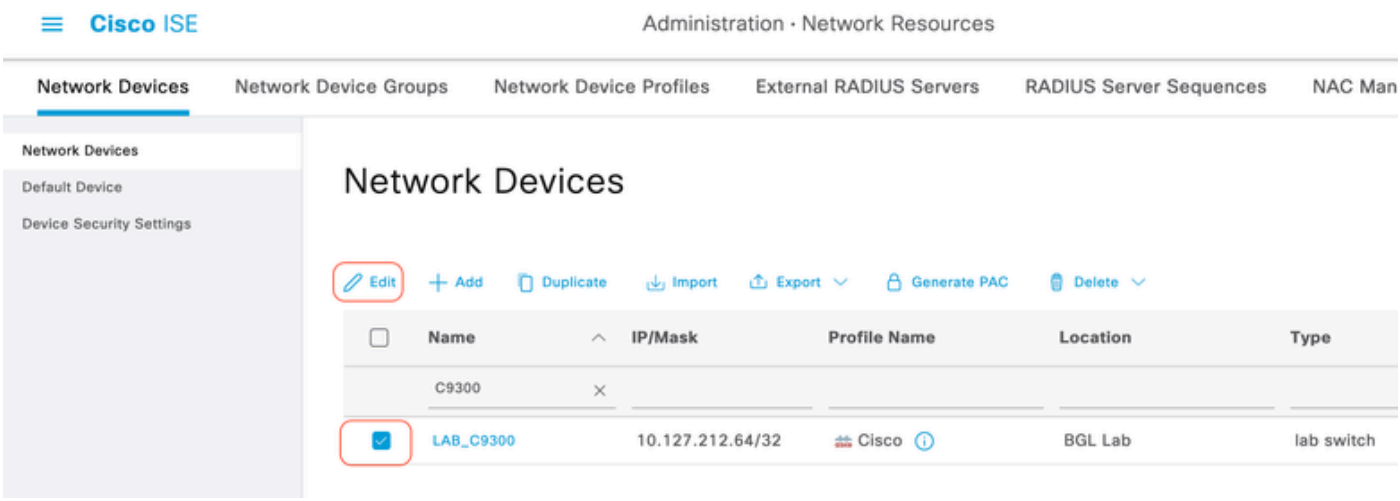
Esto proporciona una capa protectora que aísla el material clave real para protegerlo frente a posibles ataques. El material clave subyacente se vuelve prácticamente inaccesible para los agentes de amenazas, incluso en casos de interceptación de datos. La principal intención detrás de la envoltura de claves RADIUS es evitar la exposición de material clave que proteja el contenido digital, especialmente en una red a gran escala de nivel empresarial.

En ISE, la clave de cifrado de claves se utiliza para cifrar los materiales de claves con el cifrado AES y la clave de código de autenticador de mensajes separada de la clave secreta compartida RADIUS para generar el código de autenticador de mensajes.

Configurar

ISE

Paso 1: Vaya a Administration > Network Resources > Network Devices. Haga clic en la casilla de verificación del dispositivo de red para el que desea configurar el ajuste de clave RADIUS. Haga clic en Edit (si el dispositivo de red ya está agregado).



Paso 2: Expanda la Configuración de autenticación RADIUS. Haga clic en la casilla de verificación Enable KeyWrap. Introduzca la clave de cifrado de clave y la clave de código de autenticador de mensaje. Click Save.

General Settings

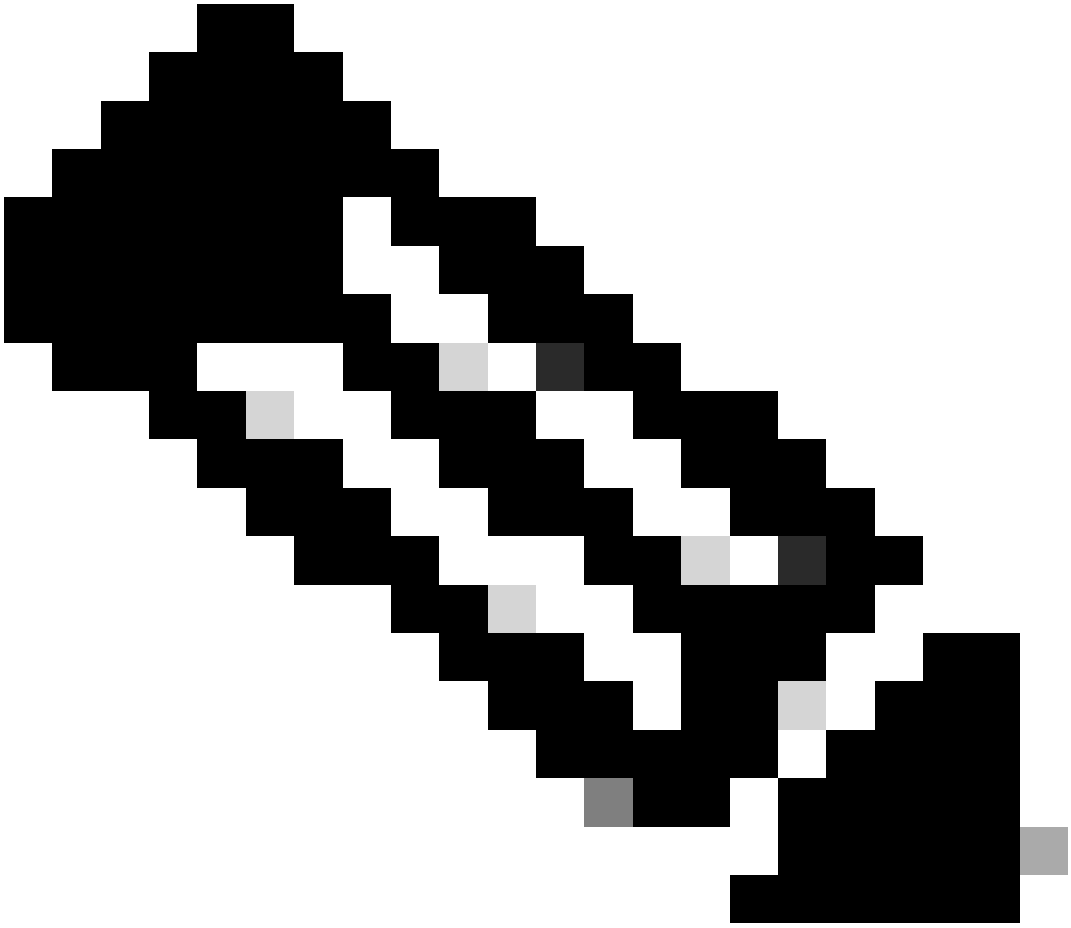
Enable KeyWrap

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

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

Key Input Format

ASCII HEXADECIMAL



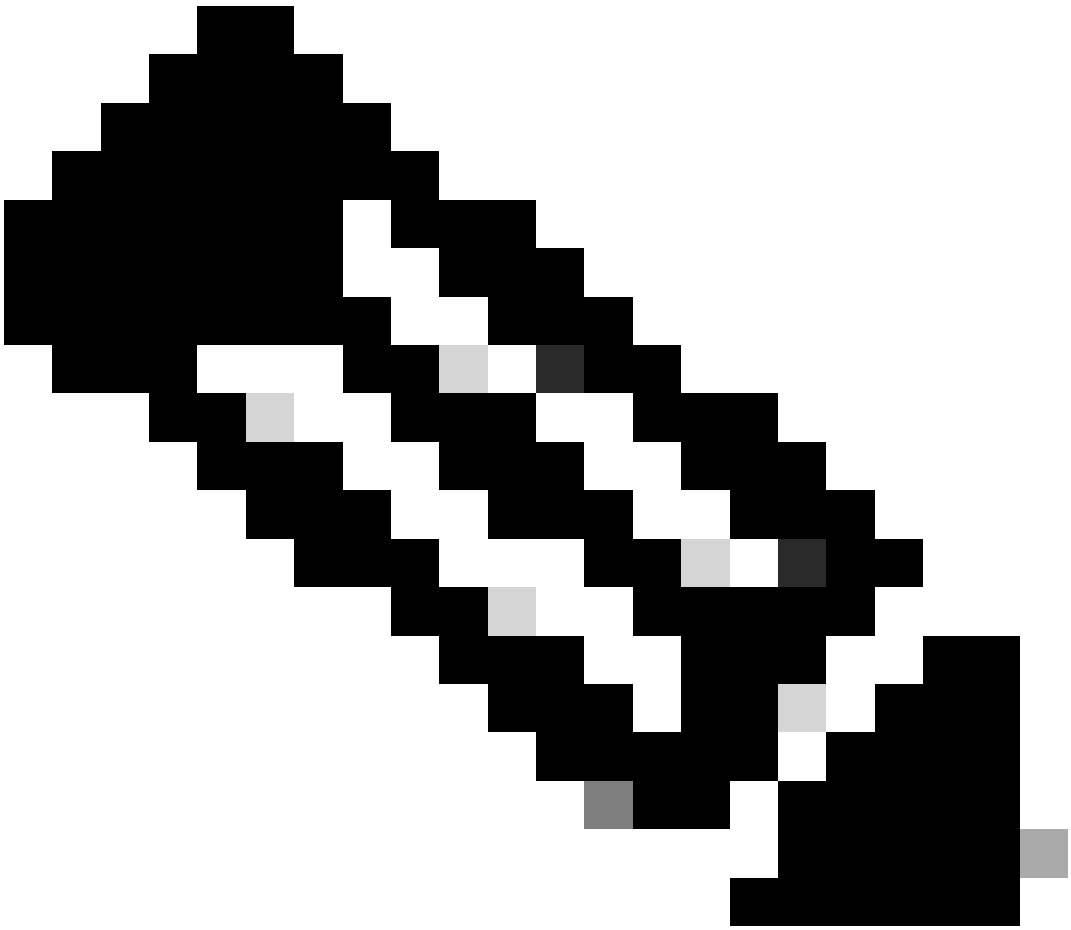
Nota: La clave de cifrado de clave y la clave de código de autenticador de mensaje deben ser diferentes.

Switch

Configuración de AAA en el switch para activar la función KeyWrap de RADIUS.

```
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
```

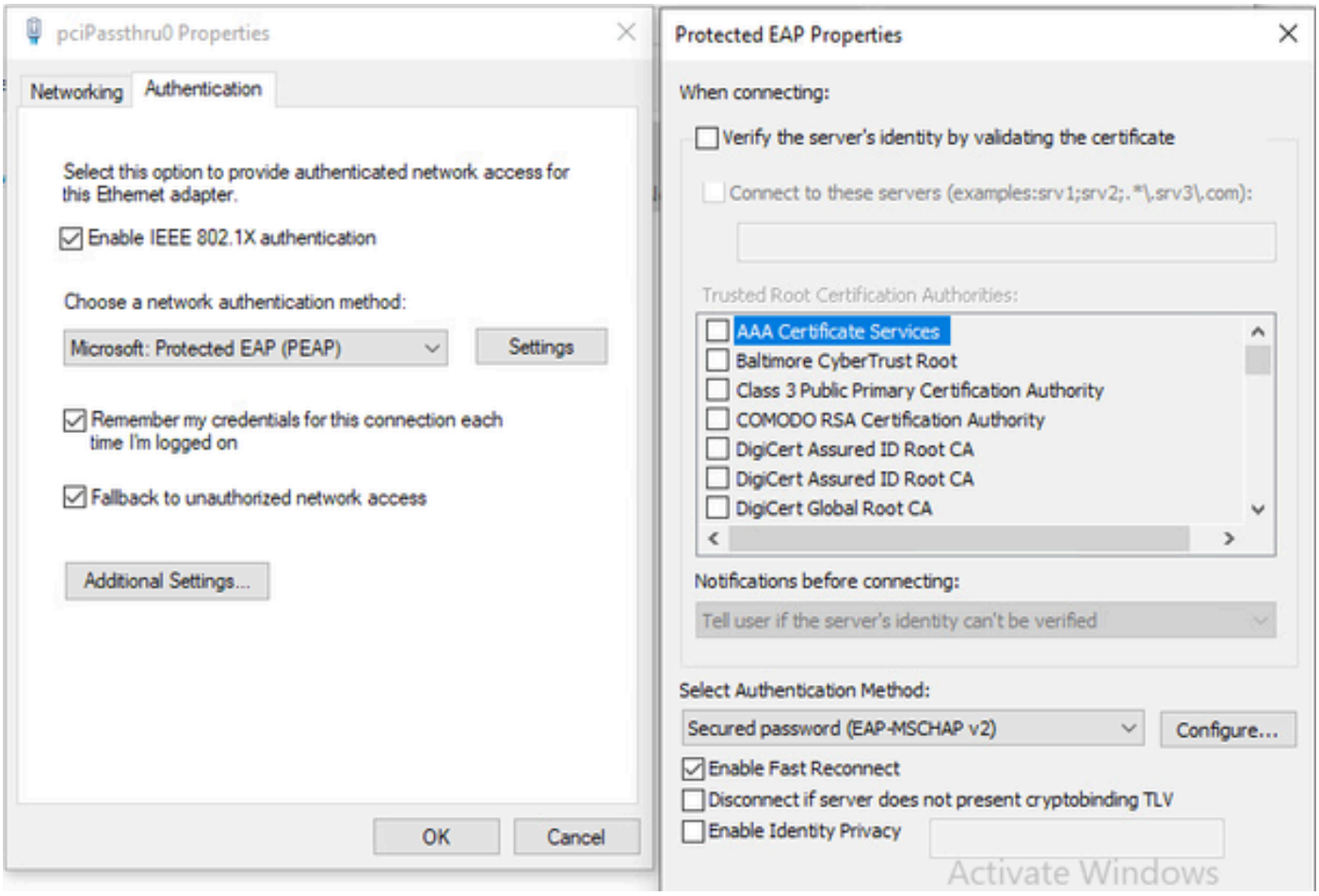
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



> Nota: La clave de cifrado debe tener 16 caracteres de longitud y el código de autenticación del mensaje y 20 caracteres de longitud.

PC

Suplicante de Windows 10 configurado para PEAP-MSCHAPv2.



Verificación

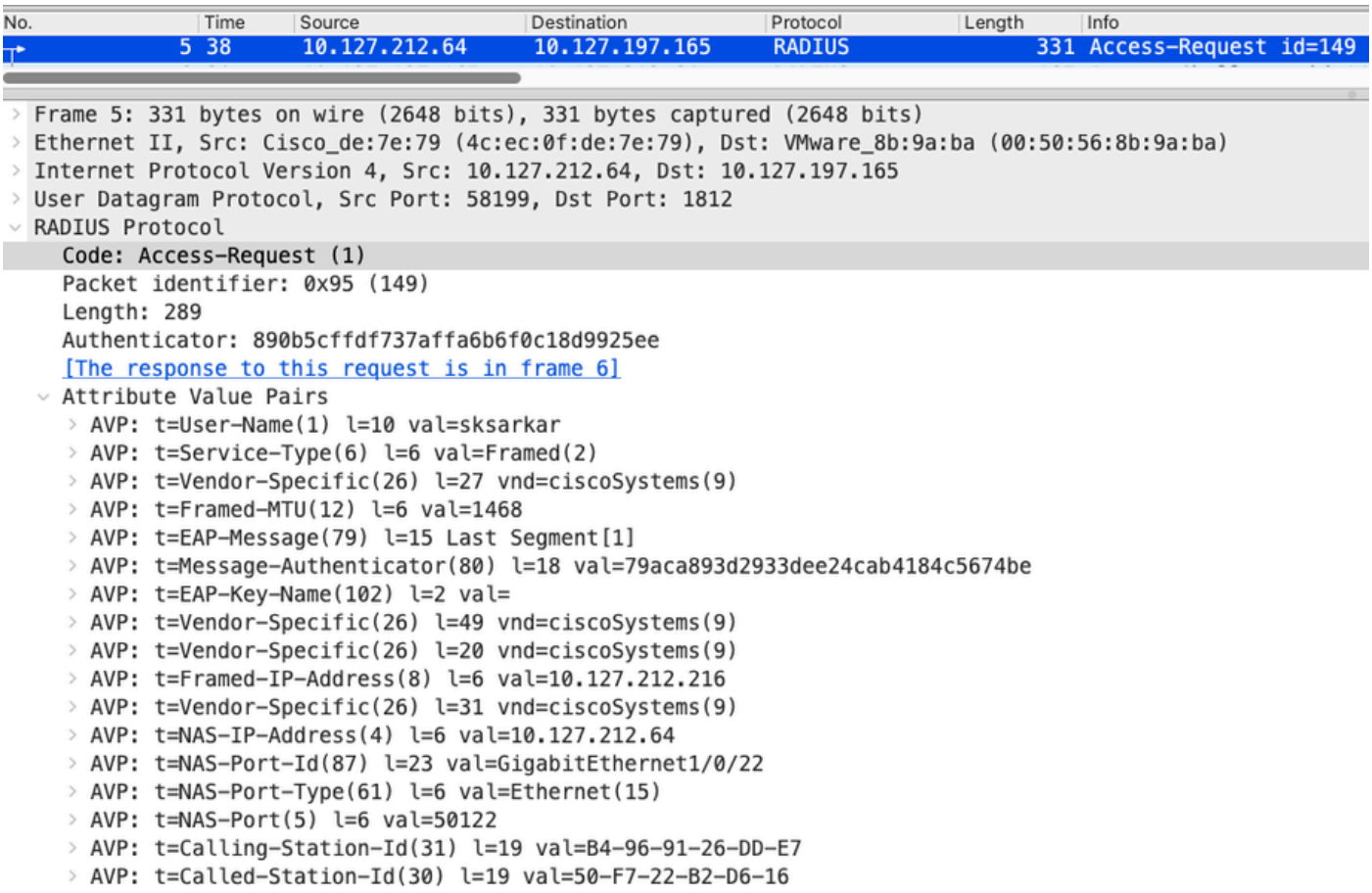
Cuando la función KeyWrap de RADIUS no está habilitada en el switch:

show radius server-group <SERVER GROUP NAME>

El resultado del comando debe mostrar Keywrap enabled: FALSO.

```
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
```

En la captura de paquetes, puede ver que no hay ningún atributo Cisco-AV-Pair para app-key, random-nonce y message-authenticator-code separado. Esto indica que el KeyWrap de RADIUS está inhabilitado en el switch.



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

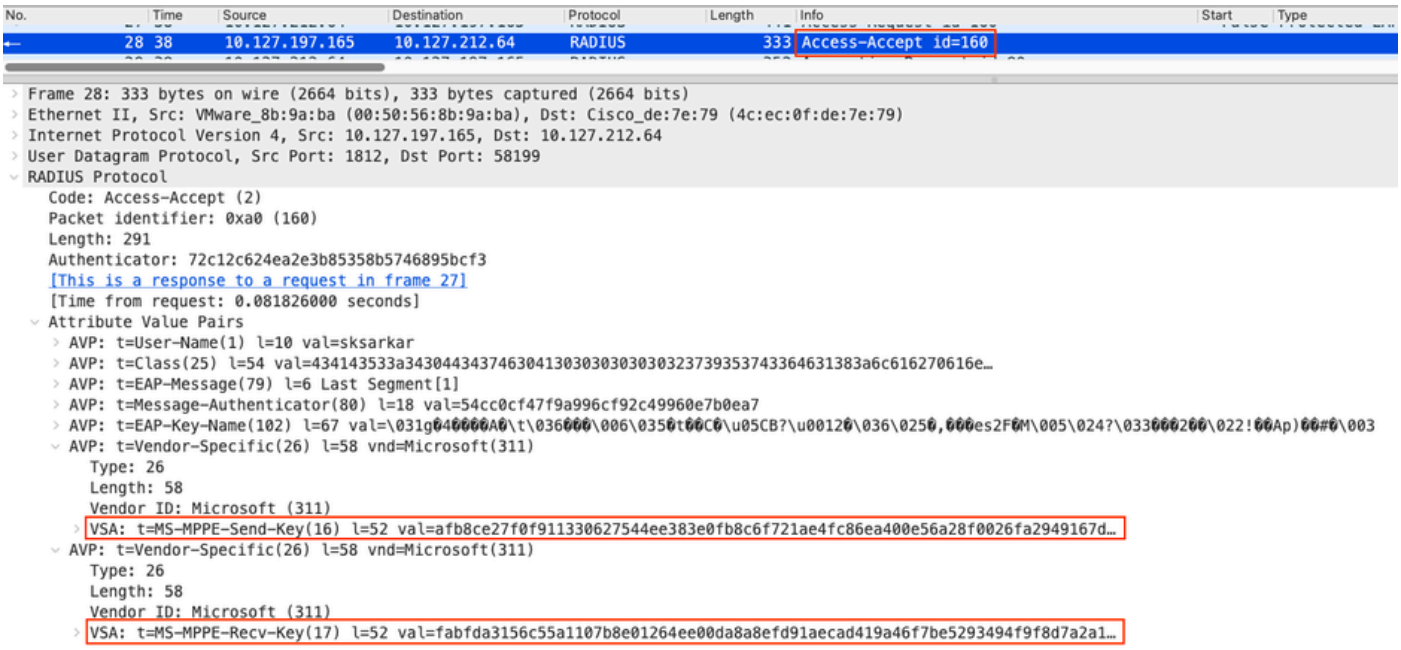
```
> Frame 5: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits)
> Ethernet II, Src: Cisco_de:7e:79 (4c:ec:0f:de:7e:79), Dst: VMware_8b:9a:ba (00:50:56:8b:9a:ba)
> Internet Protocol Version 4, Src: 10.127.212.64, Dst: 10.127.197.165
> User Datagram Protocol, Src Port: 58199, Dst Port: 1812
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
```

En el archivo port-server.log de ISE, puede ver que ISE sólo valida el atributo de integridad que es 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
```

En el paquete Access-Accept, puede ver que MS-MPPE-Send-key y MS-MPPE-Recv-Key se envían desde el servidor RADIUS al autenticador. MS-MPPE especifica el material de clave generado por los métodos EAP que se puede utilizar para realizar el cifrado de datos entre el peer y el autenticador. Estas claves de 32 bytes se derivan del secreto compartido RADIUS, el autenticador de solicitud y una sal aleatoria.



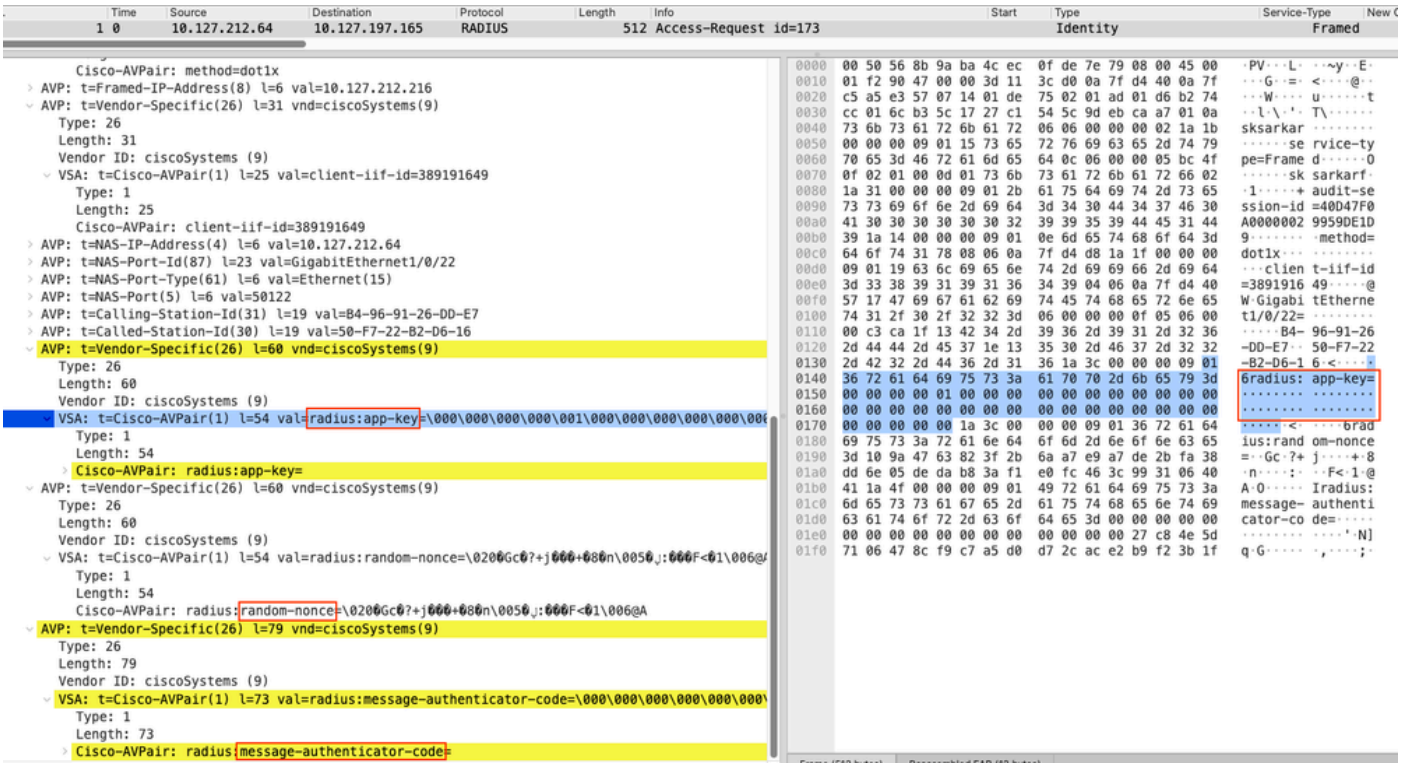
Cuando la función KeyWrap de RADIUS está habilitada en Switch e ISE:

show radius server-group <SERVER GROUP NAME>

El resultado del comando debe mostrar Keywrap enabled: VERDADERO.

```
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
```

En la captura de paquetes, puede ver que hay un atributo Cisco-AV-Pair para app-key (sin datos), random-nonce y message-authenticator-code separado. Esto indica al servidor RADIUS que el autenticador (switch) soporta el KeyWrap RADIUS y que el servidor debe utilizar el mismo.

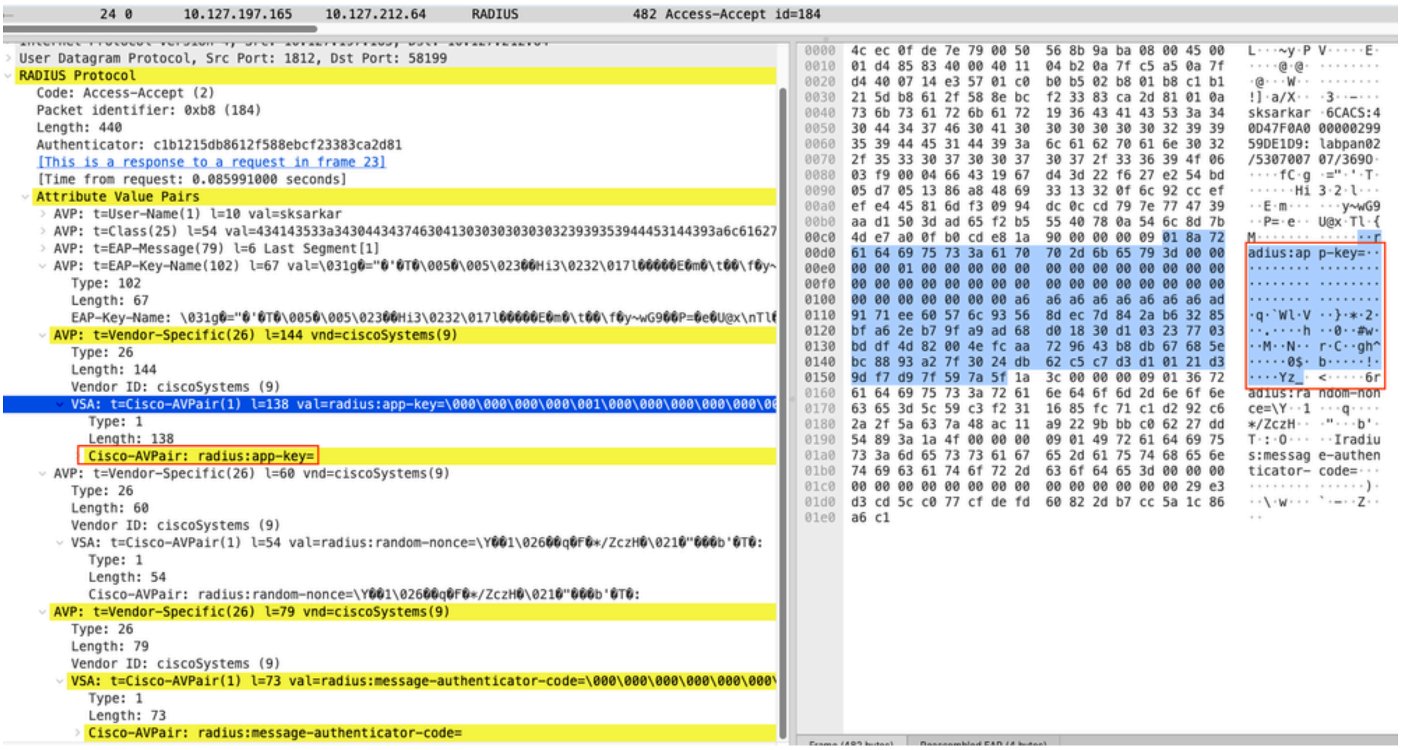


En el archivo port-server.log de ISE, puede ver que ISE valida los atributos app-key y que random-nonce y message-authenticator-code se incluyeron en el paquete ACCESS-REQUEST.

```
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
```

En el paquete Access-Accept, puede ver que los materiales de clave cifrada en el atributo app-key junto con un código de autenticación de mensaje y nombre aleatorio. Estos atributos se diseñaron para proporcionar una protección más fiable y una mayor flexibilidad que los atributos MS-MPPE-Send-Key y MS-MPPE-Recv-Key específicos del proveedor definidos actualmente.



Preguntas Frecuentes

1) ¿Es necesario habilitar RADIUS KeyWarp tanto en el dispositivo de red como en ISE para que funcione?

Sí, RADIUS KeyWrap debe activarse tanto en el dispositivo de red como en ISE para que

funcione. Aunque, si habilita KeyWrap sólo en ISE pero no en el dispositivo de red, la autenticación sigue funcionando. Sin embargo, si lo habilitó en el dispositivo de red pero no en ISE, la autenticación fallará.

2) ¿La activación de KeyWrap aumenta la utilización de recursos en ISE y el dispositivo de red?

No, no se ha producido un aumento significativo en la utilización de recursos en los dispositivos ISE y de red después de habilitar KeyWrap.

3) ¿Cuánta seguridad adicional proporciona el KeyWrap de RADIUS?

Como el propio RADIUS no proporciona cifrado a su carga, KeyWrap proporciona seguridad adicional mediante el cifrado de los materiales de claves. El nivel de seguridad depende del algoritmo de cifrado que se utilice para cifrar el material de la clave. En ISE, AES se utiliza para cifrar el material de la clave.

Referencia

- Atributos RADIUS específicos del proveedor de Cisco para la entrega de material de claves

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).