Configurazione del KeyWrap RADIUS in ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

- [ISE](#)
- [Switch](#)
- [PC](#)

[Verifica](#)

[Domande frequenti](#)

[Riferimento](#)

Introduzione

In questo documento viene descritta la procedura per configurare RADIUS KeyWrap in Cisco ISE e Cisco Switch.

Prerequisiti

- Conoscenza del dot1x
- Conoscenza del protocollo RADIUS
- Conoscenza di EAP

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il wrapping della chiave è una tecnica in cui un valore di chiave viene crittografato utilizzando un'altra chiave. Lo stesso meccanismo viene utilizzato in RADIUS per crittografare il materiale della chiave. Tale materiale viene in genere prodotto come sottoprodotto di un'autenticazione EAP

(Extensible Authentication Protocol) e restituito nel messaggio Access-Accept dopo un'autenticazione riuscita. Questa funzione è obbligatoria se ISE è in esecuzione in modalità FIPS.

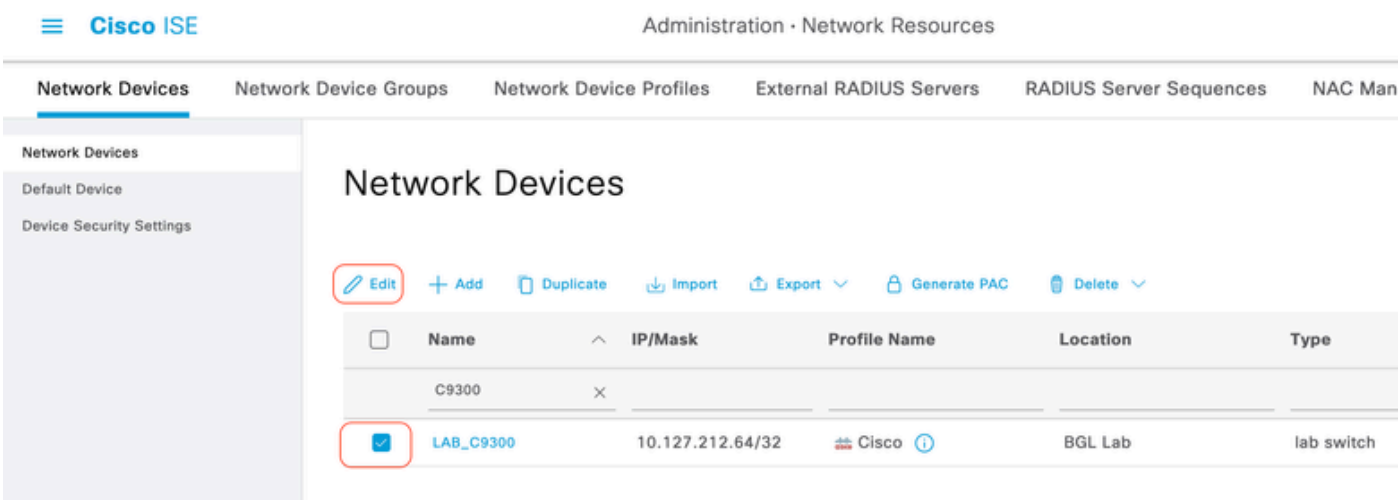
Questo fornisce uno strato protettivo che isola il materiale chiave reale per la protezione contro potenziali attacchi. Il materiale fondamentale diventa praticamente inaccessibile agli attori della minaccia, anche in caso di intercettazione dei dati. L'intenzione principale dietro il key wrapping RADIUS è prevenire l'esposizione di materiale chiave che protegge i contenuti digitali, in particolare in una rete su larga scala di livello aziendale.

In ISE, la chiave di crittografia viene utilizzata per crittografare il materiale della chiave con la crittografia AES e la chiave del codice autenticatore del messaggio separate dalla chiave segreta condivisa RADIUS per generare il codice autenticatore del messaggio.

Configurazione

ISE

Passaggio 1: Selezionare Amministrazione > Risorse di rete > Dispositivi di rete. Selezionare la casella di controllo relativa al dispositivo di rete per il quale si desidera configurare il KeyWrap RADIUS. Fare clic su Modifica (se la periferica di rete è già stata aggiunta).



Passaggio 2: Espandere le impostazioni di autenticazione RADIUS. Selezionare la casella di controllo Attiva KeyWrap. Immettere la chiave di crittografia e la chiave del codice autenticatore del messaggio. Fare clic su Save (Salva).

General Settings

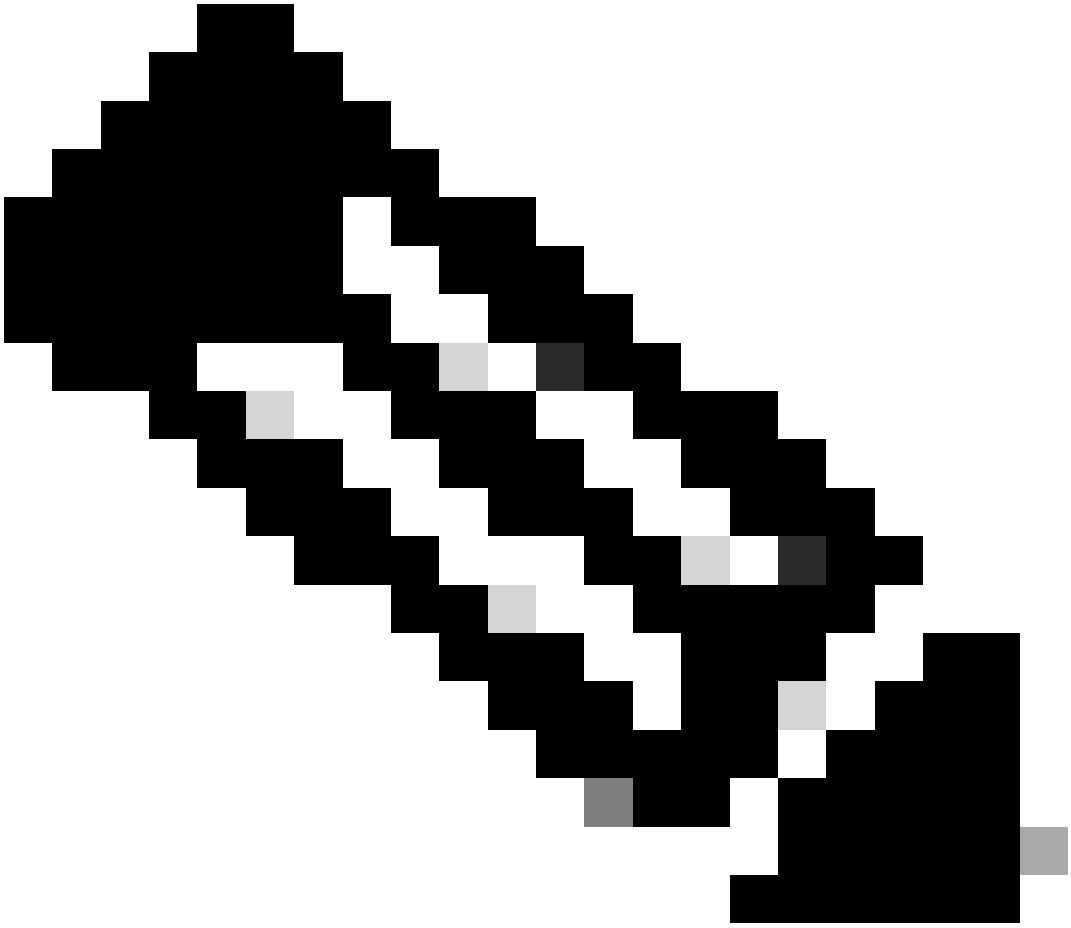
Enable KeyWrap

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

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

Key Input Format

ASCII HEXADECIMAL



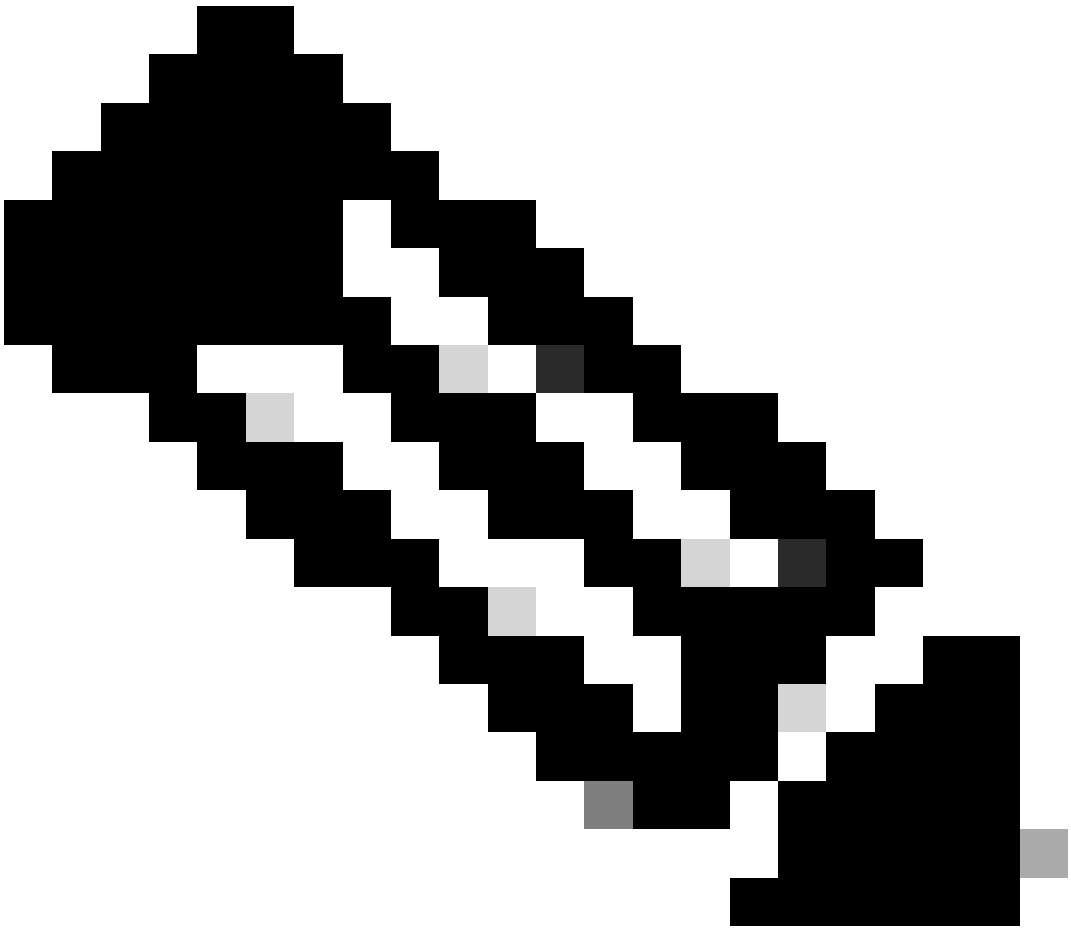
Nota: la chiave di crittografia della chiave e la chiave del codice dell'autenticatore del messaggio devono essere diverse.

Switch

Configurazione AAA nello switch per abilitare la funzionalità KeyWrap 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
```

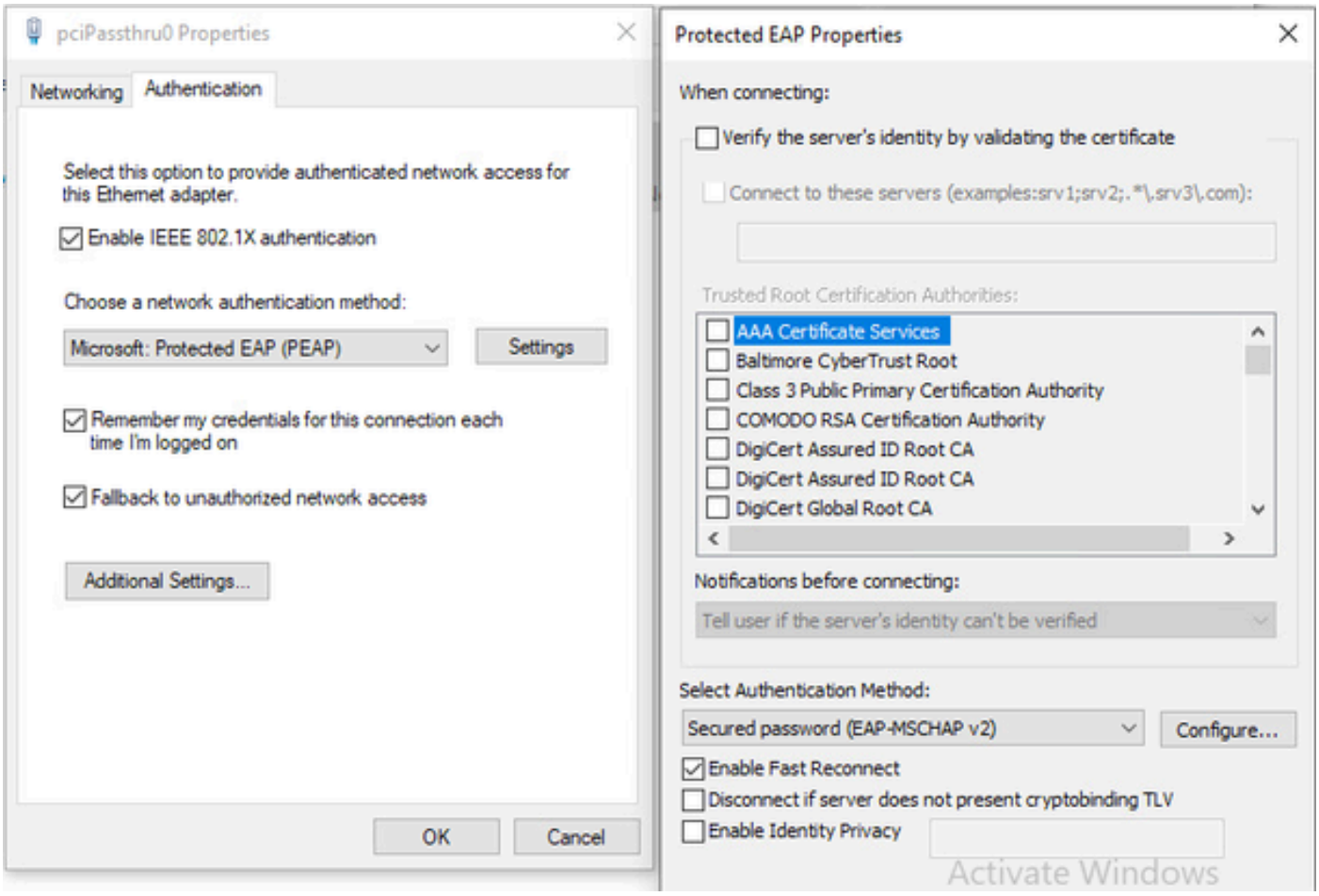
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



Nota: La chiave di crittografia deve essere lunga 16 caratteri, il codice di autenticazione del messaggio e 20 caratteri.

PC

Windows 10 Supplicant configurato per PEAP-MSCHAPv2.



Verifica

Se la funzione KeyWrap RADIUS non è attivata sullo switch:

show radius server-group <NOME GRUPPO SERVER>

L'output del comando deve mostrare la funzione Keywrap abilitata: 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
```

Nell'acquisizione del pacchetto, è possibile notare che non esiste alcun attributo Cisco-AV-Pair per app-key, random-nonce e message-authenticator-code separato. Ciò indica che la funzionalità KeyWrap RADIUS è disabilitata sullo switch.

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

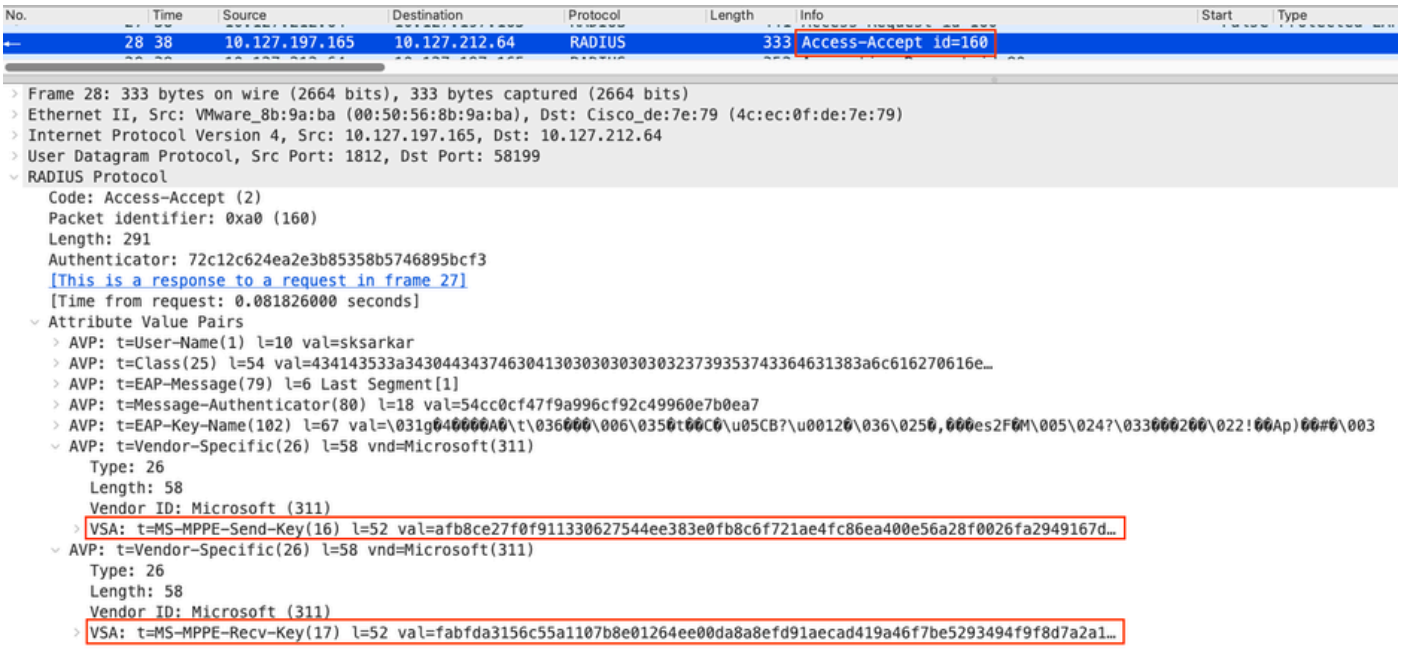
```
> Frame 5: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits)
> Ethernet II, Src: Cisco_de:7e:79 (4c:ec:0f:de:7e:79), Dst: VMware_8b:9a:ba (00:50:56:8b:9a:ba)
> Internet Protocol Version 4, Src: 10.127.212.64, Dst: 10.127.197.165
> User Datagram Protocol, Src Port: 58199, Dst Port: 1812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

In ISE prrt-server.log, è possibile notare che ISE convalida solo l'attributo di integrità che è il 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
```

Nel pacchetto Access-Accept, è possibile notare che la chiave MS-MPPE-Send-key e la chiave MS-MPPE-Recv-Key vengono inviate dal server RADIUS all'autenticatore. MS-MPPE specifica il materiale chiave generato dai metodi EAP che può essere utilizzato per eseguire la crittografia dei dati tra peer e Authenticator. Queste chiavi da 32 byte derivano dal segreto condiviso RADIUS, dall'autenticatore delle richieste e da un salt casuale.



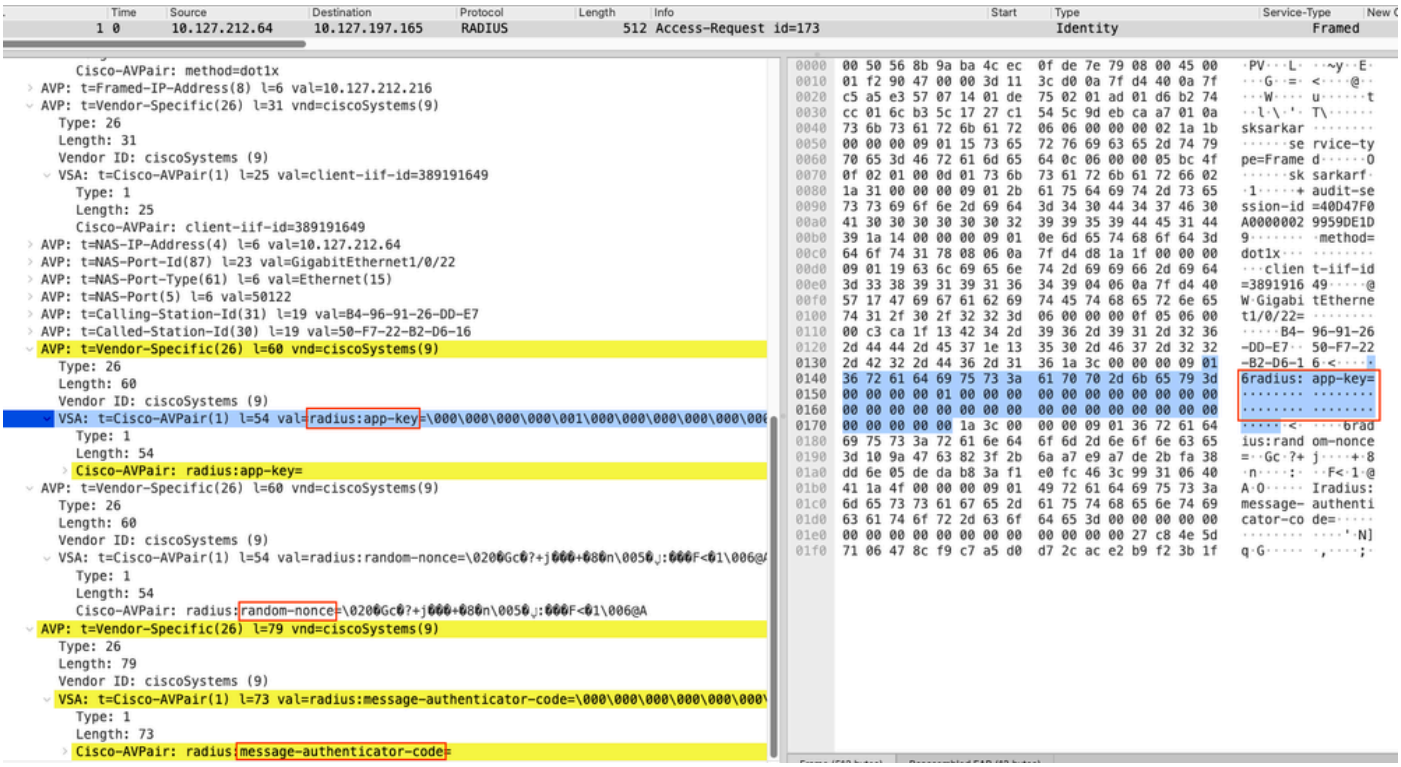
Quando la funzione RAGGIO KeyWrap è attivata su Switch e ISE:

show radius server-group <NOME GRUPPO SERVER>

L'output del comando deve restituire il comando Keywrap abilitato: VERO.

```
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
```

Nell'acquisizione del pacchetto, è presente un attributo Cisco-AV-Pair per app-key (senza dati), random-nonce e message-authenticator-code separato. Ciò indica al server RADIUS che l'autenticatore (switch) supporta il KeyWrap RADIUS e che il server deve utilizzare lo stesso.

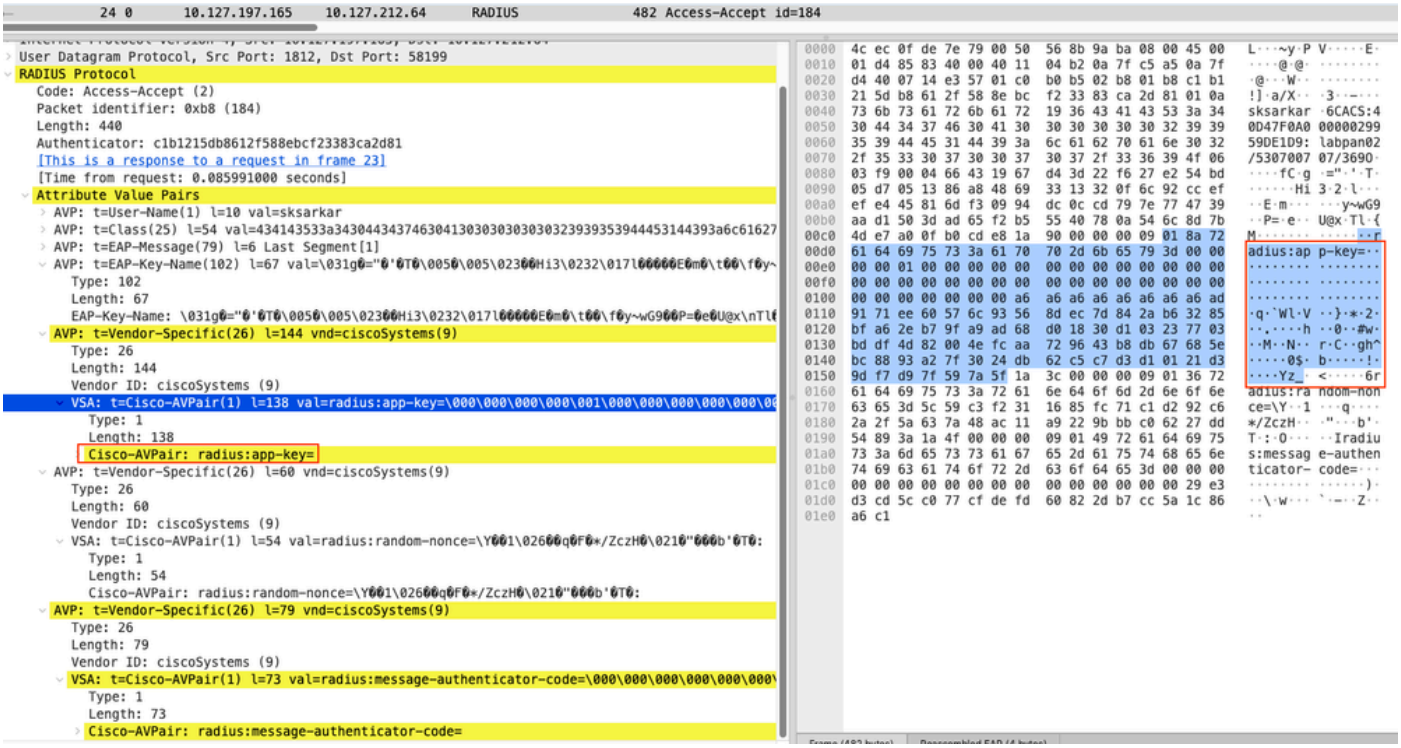


Nel file ISE prrt-server.log, è possibile notare che ISE convalida gli attributi app-key e che nel pacchetto ACCESS-REQUEST sono stati inclusi sia la nonce casuale che il codice dell'autenticatore del messaggio.

```
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
```

Nel pacchetto Access-Accept, è possibile vedere che il materiale della chiave crittografata nell'attributo app-key insieme a un nonce casuale e a un codice di autenticazione del messaggio. Questi attributi sono stati progettati per fornire una protezione più avanzata e una maggiore flessibilità rispetto agli attributi MS-MPPE-Send-Key e MS-MPPE-Recv-Key attualmente definiti per il fornitore.



Domande frequenti

1) È necessario abilitare RADIUS KeyWarp sia sul dispositivo di rete che sull'ISE per poterlo utilizzare?

Sì, è necessario abilitare RADIUS KeyWrap sia sul dispositivo di rete che su ISE per farlo funzionare. Tuttavia, se si attiva la funzione KeyWrap solo sull'ISE ma non sulla periferica di rete, l'autenticazione continua a funzionare. Tuttavia, se l'opzione è stata abilitata sul dispositivo di rete ma non sull'ISE, l'autenticazione non riesce.

2) L'abilitazione di KeyWrap aumenta l'utilizzo delle risorse sul dispositivo ISE e di rete?

No, non vi è alcun aumento significativo nell'utilizzo delle risorse sull'ISE e sul dispositivo di rete dopo l'abilitazione di KeyWrap.

3) Qual è il livello di sicurezza aggiuntivo offerto da RADIUS KeyWrap?

Poiché la tecnologia RADIUS non fornisce alcuna crittografia per il payload, KeyWrap offre una maggiore sicurezza tramite la crittografia del materiale della chiave. Il livello di protezione dipende dall'algoritmo di crittografia utilizzato per crittografare il materiale della chiave. Ad ISE, viene usato l'AES per criptare il materiale della chiave.

Riferimento

- Attributi RADIUS specifici del fornitore per la consegna del materiale per le chiavi

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).