RADIUS-toetsterugloop in ISE configureren

Inhoud

Inleiding

Dit document beschrijft de procedure om RADIUS KeyWrap te configureren in Cisco ISE en Cisco Switch.

Voorwaarden

- Kennis van dot1x
- Kennis van het RADIUS-protocol
- Kennis van EAP

Gebruikte componenten

- ISE-lijnkaart 3.2
- Cisco C9300-24U met software versie 17.09.04a
- Windows 10 PC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Key wrapping is een techniek waarbij een sleutelwaarde versleuteld wordt met een andere sleutel. Hetzelfde mechanisme wordt in RADIUS gebruikt om het belangrijkste materiaal te versleutelen. Dit materiaal wordt gewoonlijk geproduceerd als een bijproduct van een EAP-verificatie

(Extensible Verification Protocol) en na een succesvolle verificatie teruggestuurd naar het bericht Access-Accept. Deze optie is verplicht als ISE in de FIPS-modus wordt uitgevoerd.

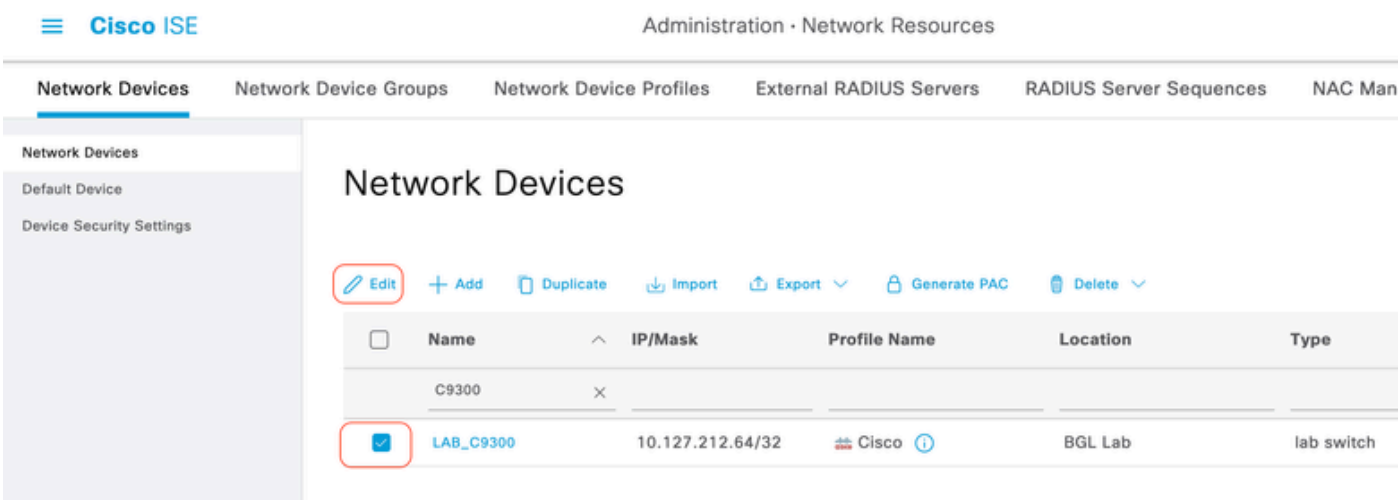
Dit biedt een beschermlaag die het feitelijke belangrijkste materiaal beschermt tegen mogelijke aanvallen. Het onderliggende kernmateriaal wordt vrijwel ontoegankelijk voor bedreigende actoren, zelfs in gevallen van gegevensonderschepping. De belangrijkste bedoeling achter RADIUS-sleutelomwikkeling is te voorkomen dat belangrijke materialen die digitale inhoud beveiligen, in het bijzonder in een grootschalig netwerk op ondernemingsniveau, aan het licht komen.

In ISE wordt de Key Encryption Key gebruikt om de sleutelmaterialen te versleutelen met de AES-encryptie en de Message Authenticator Code Key gescheiden van de RADIUS gedeelde geheime sleutel om Message Authenticator Code te genereren.

Configureren

ISE

Stap 1: Ga naar Beheer > Netwerkbronnen > Netwerkapparaten. Klik op het aanvinkvakje voor het netwerkapparaat waarvoor u RADIUS KeyWrap wilt configureren. Klik op Bewerken (als het netwerkapparaat al is toegevoegd).



Stap 2: Breid de RADIUS-verificatie-instellingen uit. Klik op het aanvinkvakje Enable KeyWrap. Voer de Key Encryption Key en de Message Authenticator Code Key in. Klik op Save (Opslaan).

General Settings

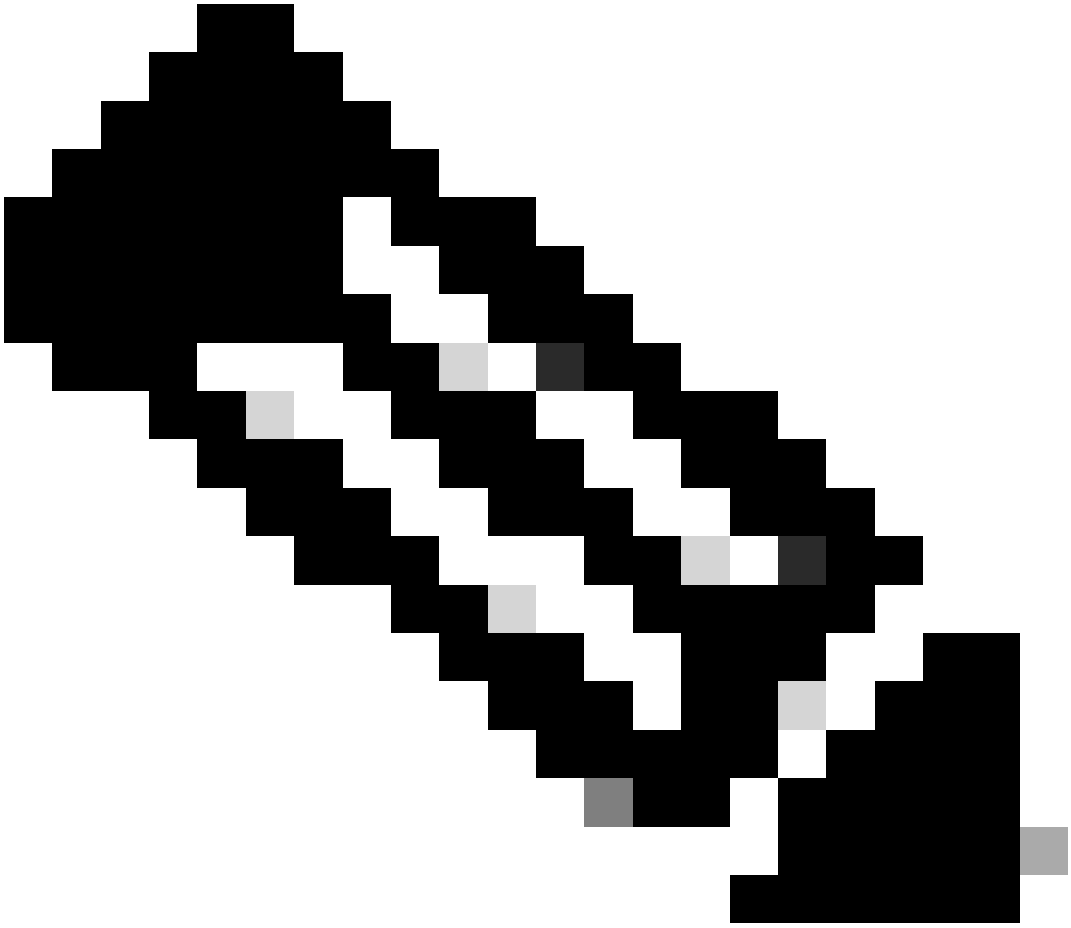
Enable KeyWrap

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

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

Key Input Format

ASCII HEXADECIMAL



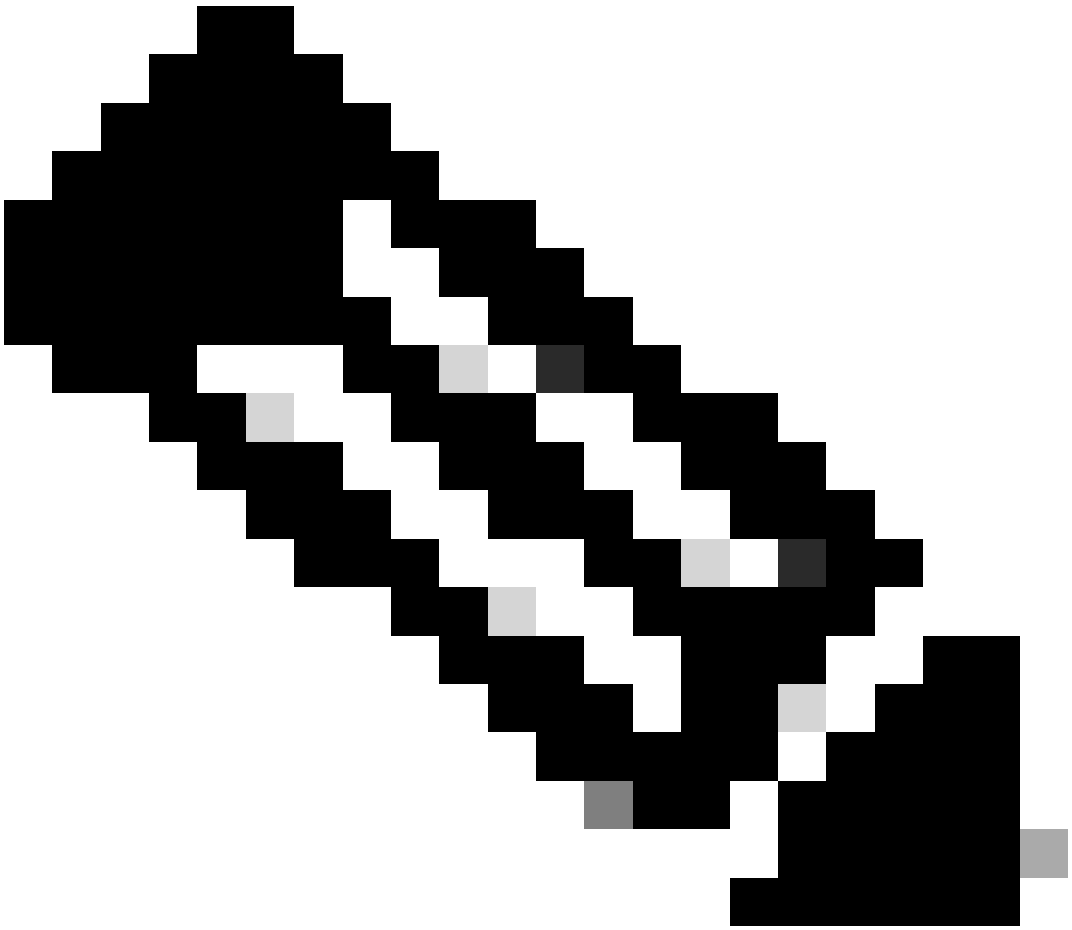
Opmerking: de sleutel voor de encryptie van de sleutel en de sleutel voor de verificatiecode van het bericht moeten verschillen.

Switch

AAA-configuratie in Switch om de RADIUS KeyWrap-functie in te schakelen.

```
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
```

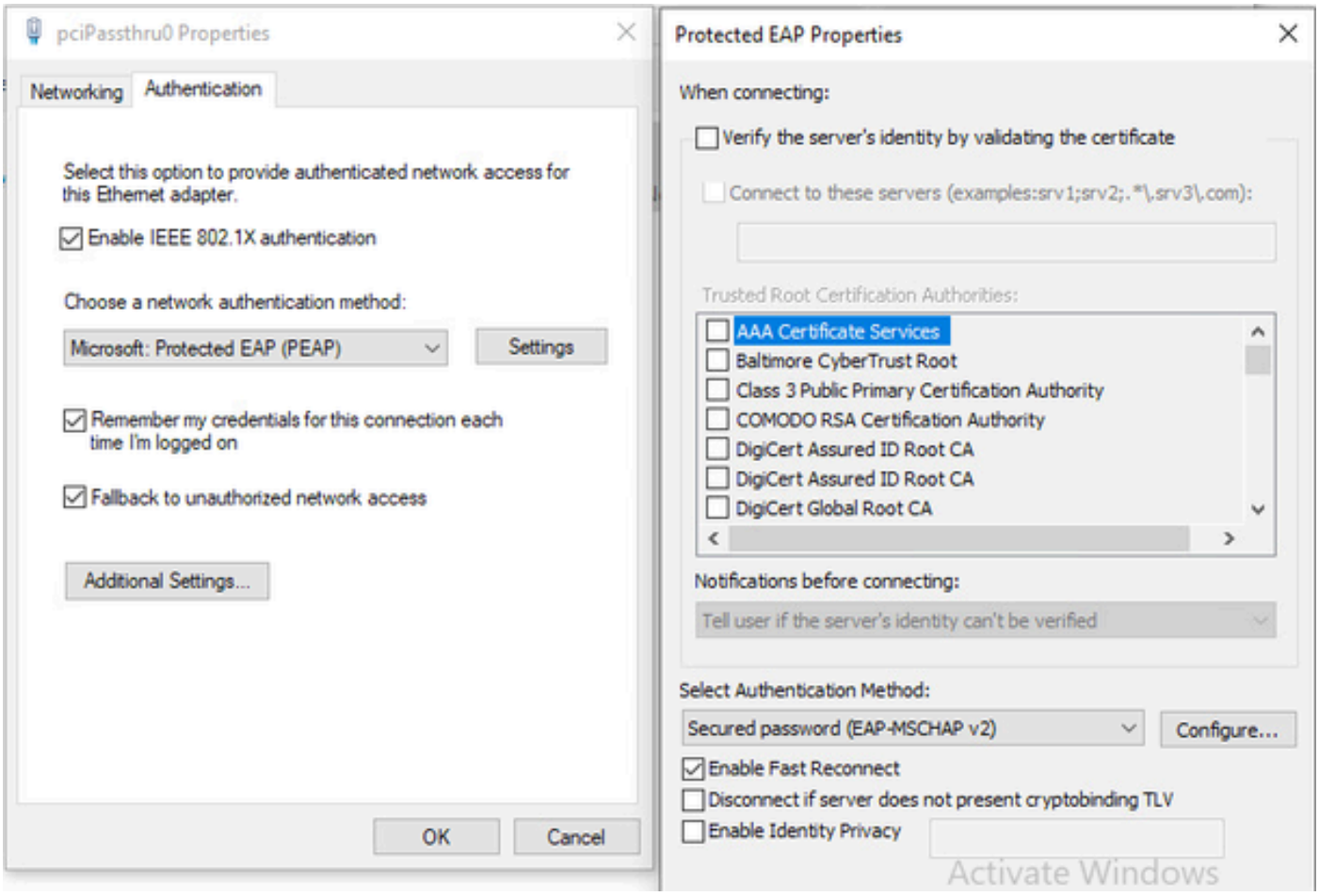
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



> Opmerking: De encryptie-sleutel moet 16 karakters lang en bericht-auth-code en 20 karakters lang zijn.

PC

Windows 10 Supplicant geconfigureerd voor PEAP-MSCHAPv2.



Verifiëren

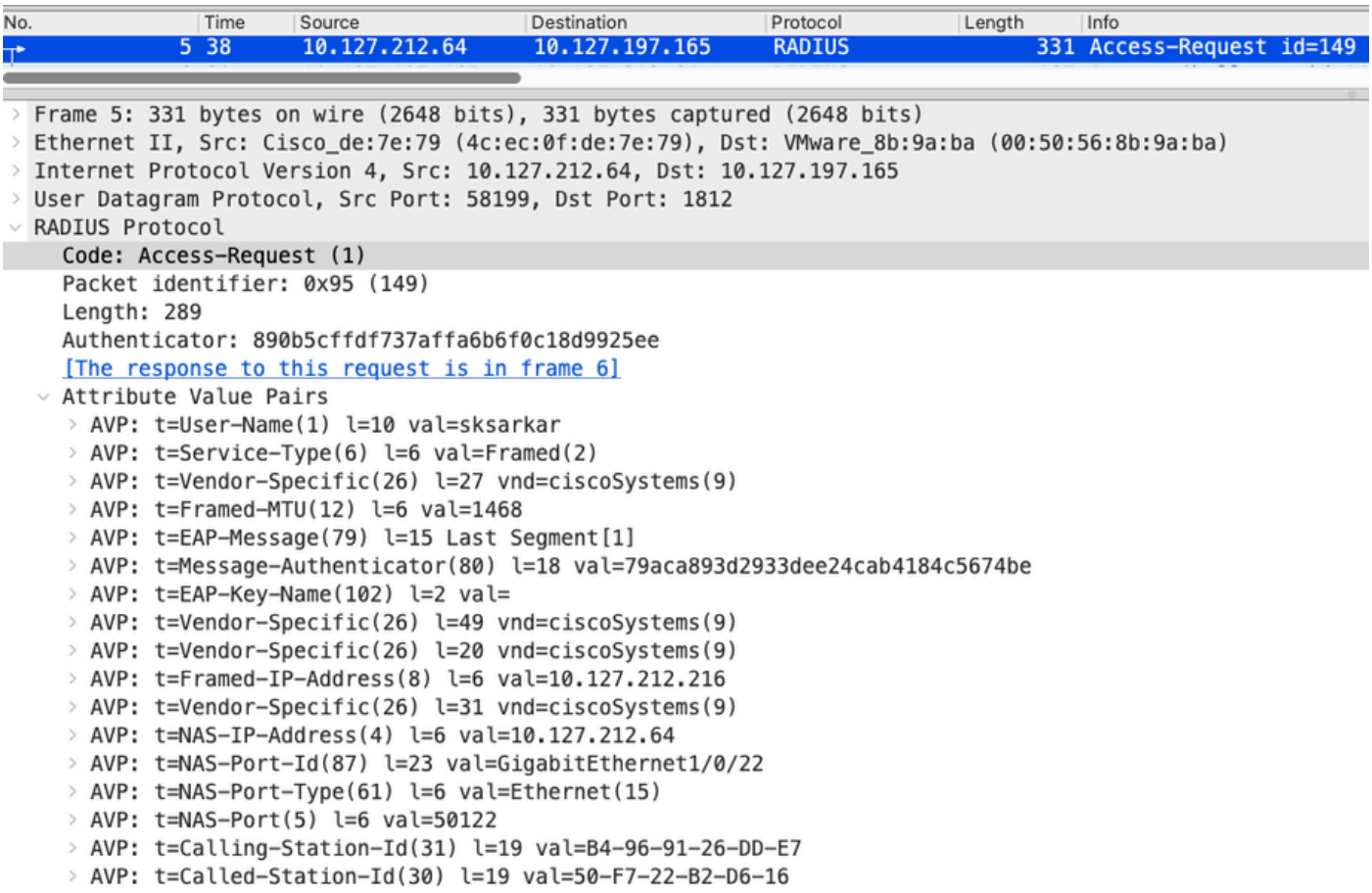
Wanneer de RADIUS KeyWrap-functie niet op de Switch is ingeschakeld:

radius server-group <NAAM SERVERGROEP> weergeven

De opdrachtoutput moet tonen dat Keywrap is ingeschakeld: ONJUIST.

```
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
```

In de pakketopname kunt u zien dat er geen Cisco-AV-paar attributen zijn voor app-key, random-nonce en afzonderlijke message-authenticator-code. Dit geeft aan dat RADIUS KeyWrap op de switch is uitgeschakeld.

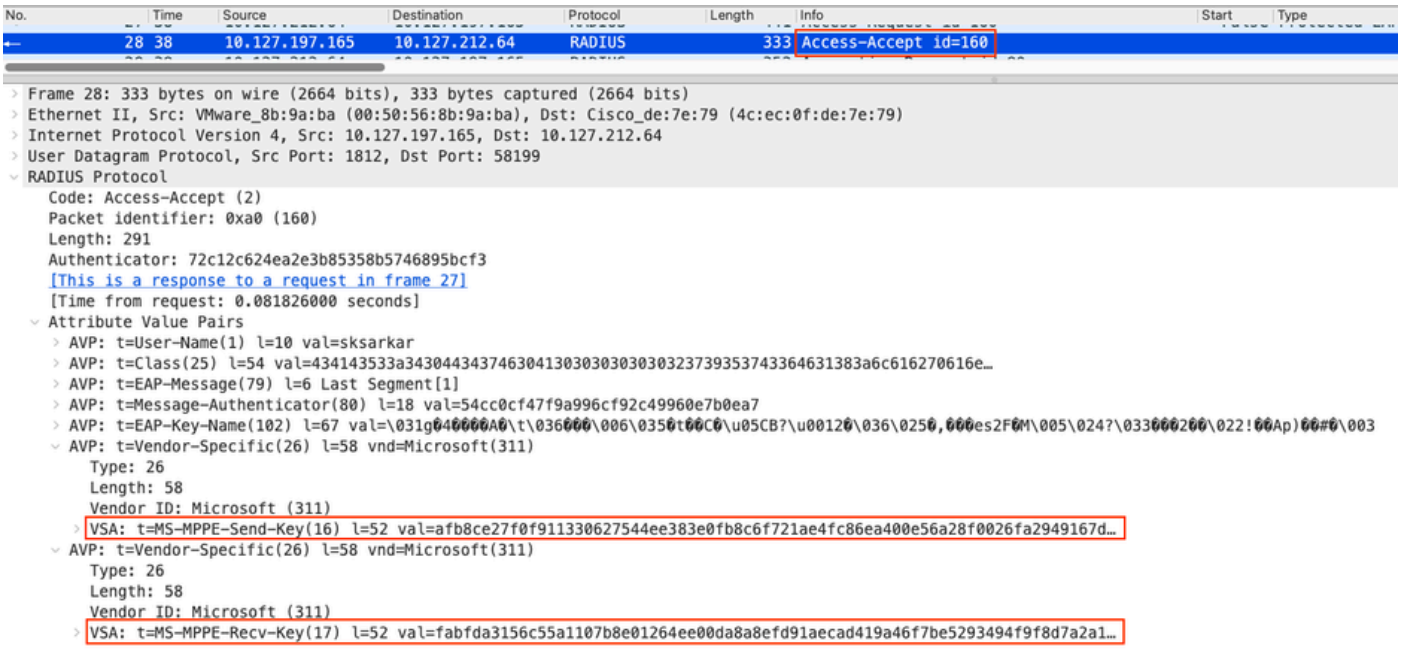


In het ISE-prt-server.log kunt u zien dat ISE alleen het integriteitskenmerk valideert, dat de Message-Authenticator is.

```
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
```

In het pakket Access-Accept kunt u zien dat de MS-MPPE-Send-key en MS-MPPE-Recv-Key worden verzonden van de RADIUS-server naar de Authenticator. MS-MPPE specificeert het belangrijkste materiaal dat met de EAP-methoden wordt gegenereerd en dat kan worden gebruikt om gegevenscodering tussen peer en Authenticator uit te voeren. Deze 32-bytesleutels zijn afgeleid van het RADIUS gedeelde geheim, request authenticator en een willekeurig zout.



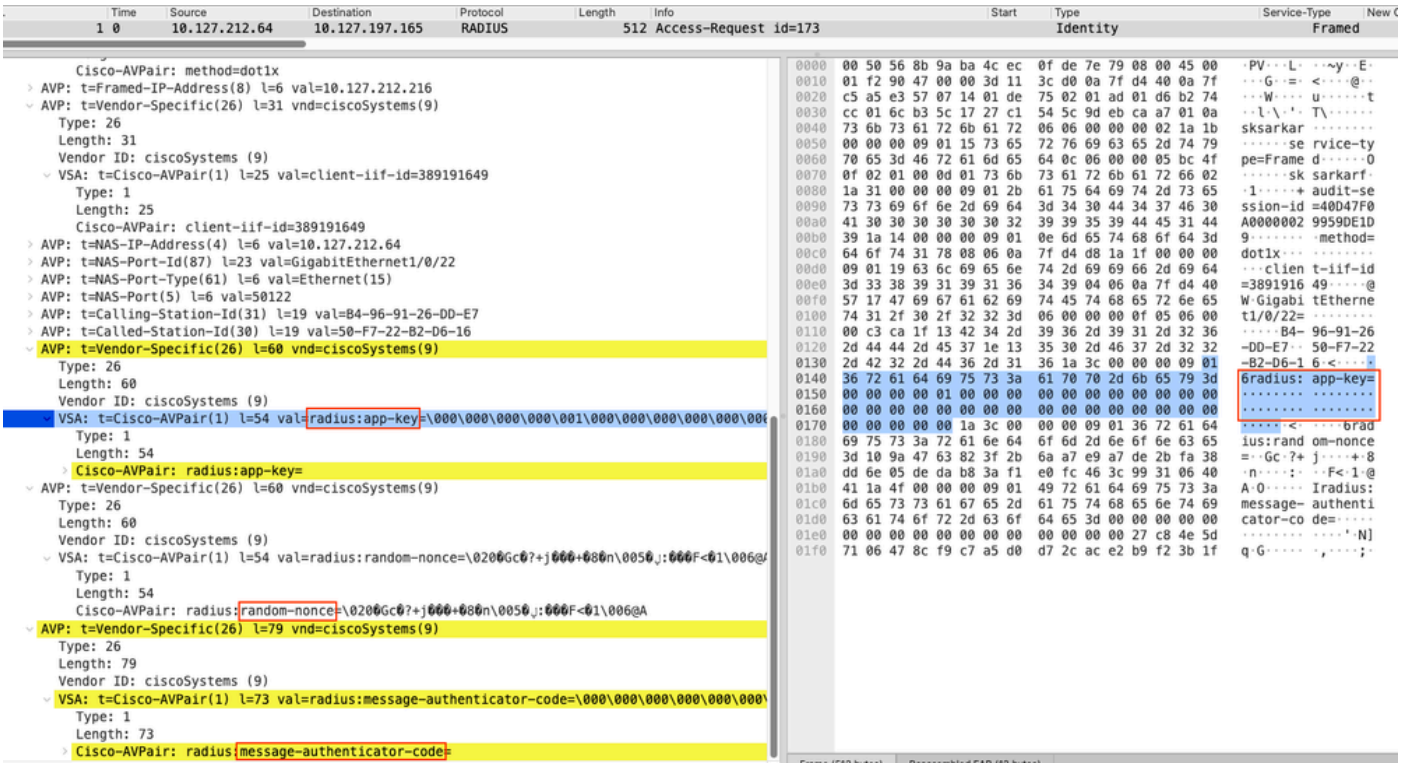
Wanneer de RADIUS KeyWrap-functie is ingeschakeld op Switch en ISE:

radius server-group <NAAM SERVERGROEP> weergeven

De opdrachtoutput moet Keywrap enabled tonen: WAAR.

```
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
```

In de pakketopname kunt u zien dat er een Cisco-AV-paar attribuut voor app-key (zonder gegevens), willekeurige en afzonderlijke bericht-authenticator-code aanwezig zijn. Dit geeft aan de RADIUS-server aan dat de Authenticator (Switch) de RADIUS KeyWrap ondersteunt en dat de server hetzelfde moet gebruiken.

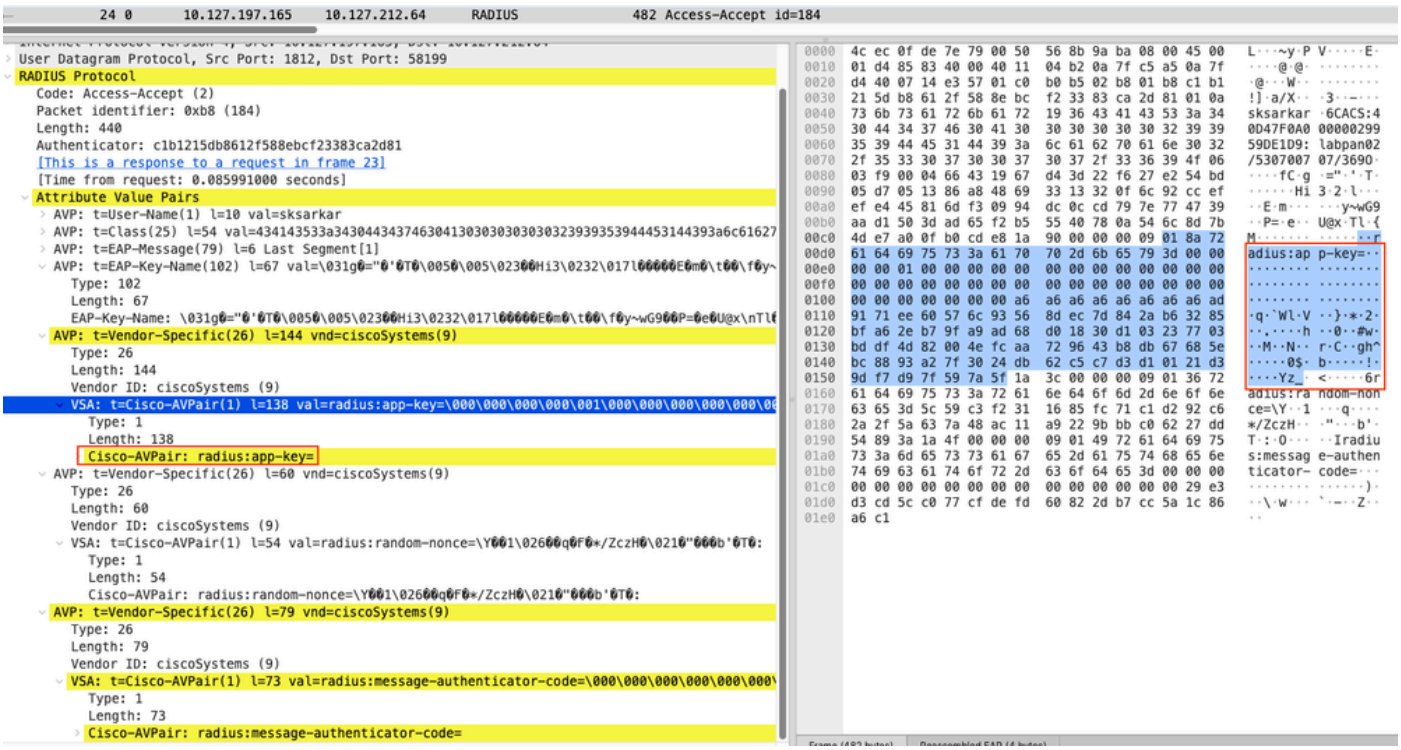


In het ISE prt-server.log kunt u zien dat ISE de attributen app-key valideert en dat willekeurige-eenmalige en bericht-authenticator-code in het ACCESS-REQUEST pakket kwam.

```
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
```

In het pakket Access-Accept kunt u zien dat de versleutelde sleutelmaterialen in de app-key attributen samen met een willekeurige en bericht-authenticator-code. Deze eigenschappen zijn ontworpen om een sterkere bescherming en meer flexibiliteit te bieden dan de momenteel gedefinieerde leverancierspecifieke eigenschappen MS-MPPE-Send-Key en MS-MPPE-Recv-Key.



Veelgestelde vragen

1) Moet RADIUS KeyWarp worden ingeschakeld op zowel het netwerkapparaat als ISE om het te laten werken?

Ja, RADIUS KeyWrap moet zijn ingeschakeld op zowel het netwerkapparaat als ISE om het te laten werken. Hoewel, als u de KeyWrap alleen op de ISE maar niet op het netwerkapparaat inschakelt, werkt verificatie nog steeds. Maar als u het hebt ingeschakeld op het netwerkapparaat maar niet in ISE, mislukt de verificatie.

2) Verhoogt het inschakelen van KeyWrap het resourcegebruik op het ISE- en netwerkapparaat?

Nee, er is geen belangrijke toename in resourcegebruik op de ISE en het netwerkapparaat na het inschakelen van KeyWrap.

3) Hoeveel extra beveiliging biedt RADIUS KeyWrap?

Omdat de RADIUS zelf geen encryptie biedt voor de payload, biedt KeyWrap extra beveiliging door de belangrijkste materialen te versleutelen. Het beveiligingsniveau hangt af van het coderingsalgoritme dat wordt gebruikt om het sleutelmateriaal te versleutelen. In ISE wordt AES gebruikt om het belangrijkste materiaal te versleutelen.

Referentie

- Cisco-leverancierspecifieke RADIUS-kenmerken voor de levering van sleutelmateriaal

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.