ISE에서 RADIUS KeyWrap 구성

목차

소개

이 문서에서는 Cisco ISE 및 Cisco Switch에서 RADIUS KeyWrap를 구성 하는 절차에 대해 설명 합니다.

사전 요구 사항

- dot1x 지식
- RADIUS 프로토콜에 대한 지식
- EAP 지식

사용되는 구성 요소

- ISE 3.2
- Cisco C9300-24U, 소프트웨어 버전 17.09.04a
- 윈도우 10 PC

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

키 래핑은 하나의 키 값이 다른 키를 사용하여 암호화되는 기술입니다. RADIUS에서 키 자료를 암호화하는 데 동일한 메커니즘이 사용됩니다. 이 자료는 일반적으로 EAP(Extensible Authentication Protocol) 인증의 부산물로 생성되고 인증에 성공한 후 Access-Accept 메시지에서 반환됩니다. ISE가 FIPS 모드에서 실행 중인 경우 이 기능은 필수입니다.

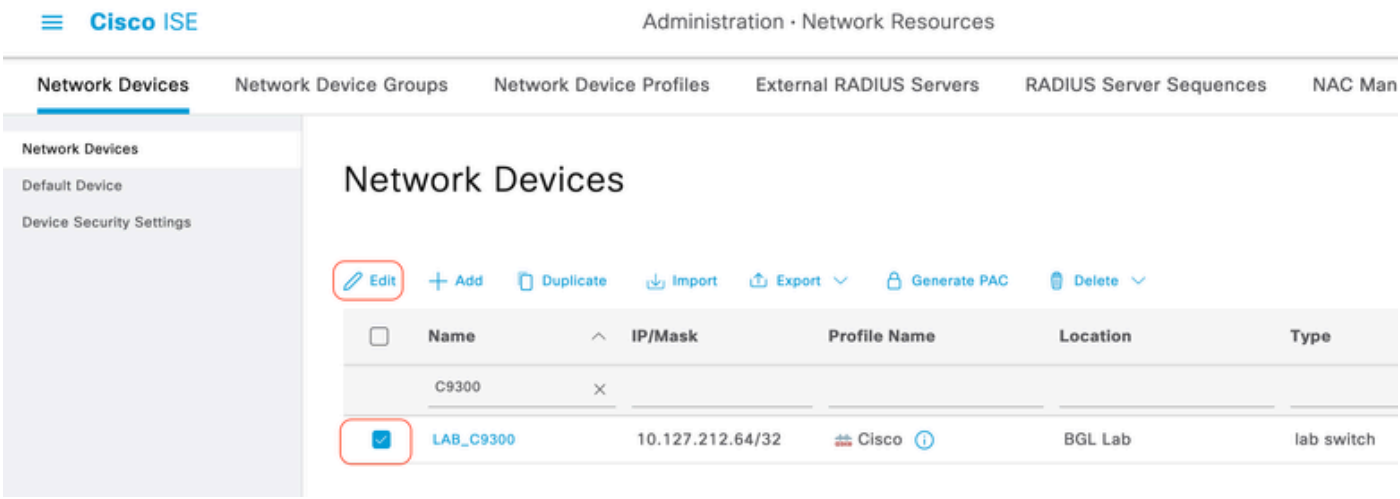
이는 잠재적인 공격으로부터 보호하기 위한 실제 주요 물질을 절연하는 보호 층을 제공한다. 데이터 가로채기가 발생하는 경우에도, 기본적으로 위협적인 행위자가 기본 핵심 자료를 사실상 액세스할 수 없게 됩니다. RADIUS 키 래핑의 주요 목적은 특히 대규모 기업 수준 네트워크에서 디지털 콘텐츠를 보호하는 주요 자료의 노출을 방지하는 것입니다.

ISE에서는 키 암호화 키를 사용하여 AES 암호화로 키 자료를 암호화하고 메시지 인증자 코드를 생성하기 위해 RADIUS 공유 비밀 키에서 분리된 메시지 인증자 코드 키를 암호화합니다.

구성

ISE

1단계: Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. RADIUS KeyWrap를 구성 할 네트워크 장치의 확인 란을 클릭 합니다. Edit(편집)를 클릭합니다(네트워크 디바이스가 이미 추가된 경우).



2단계: RADIUS Authentication Settings(RADIUS 인증 설정)를 확장합니다. Enable KeyWrap(KeyWrap 활성화) 확인란을 클릭합니다. 키 암호화 키 및 메시지 인증자 코드 키를 입력합니다. 저장을 클릭합니다.

General Settings

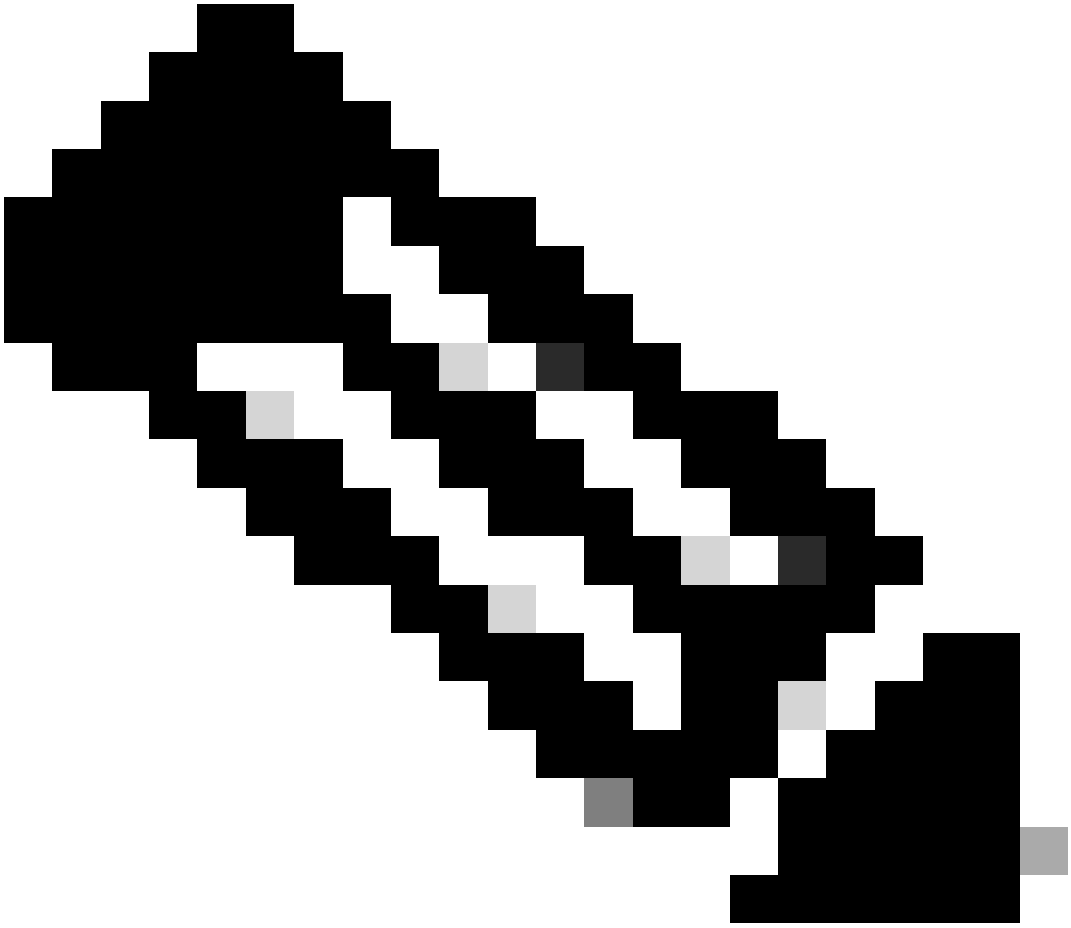
Enable KeyWrap

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

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

Key Input Format

ASCII HEXADECIMAL



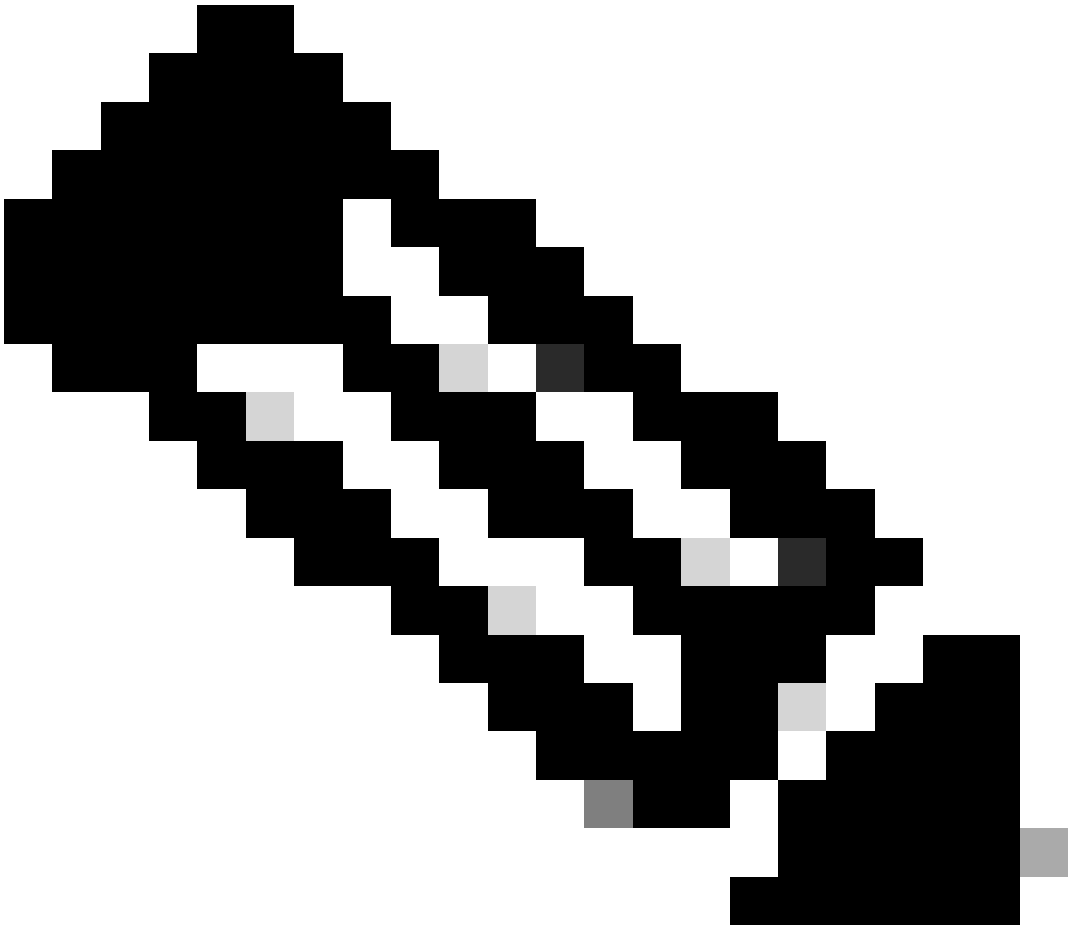
참고: 키 암호화 키와 메시지 인증자 코드 키는 서로 달라야 합니다.

스위치

RADIUS KeyWrap 기능을 활성화하기 위한 스위치의 AAA 컨피그레이션

```
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
```

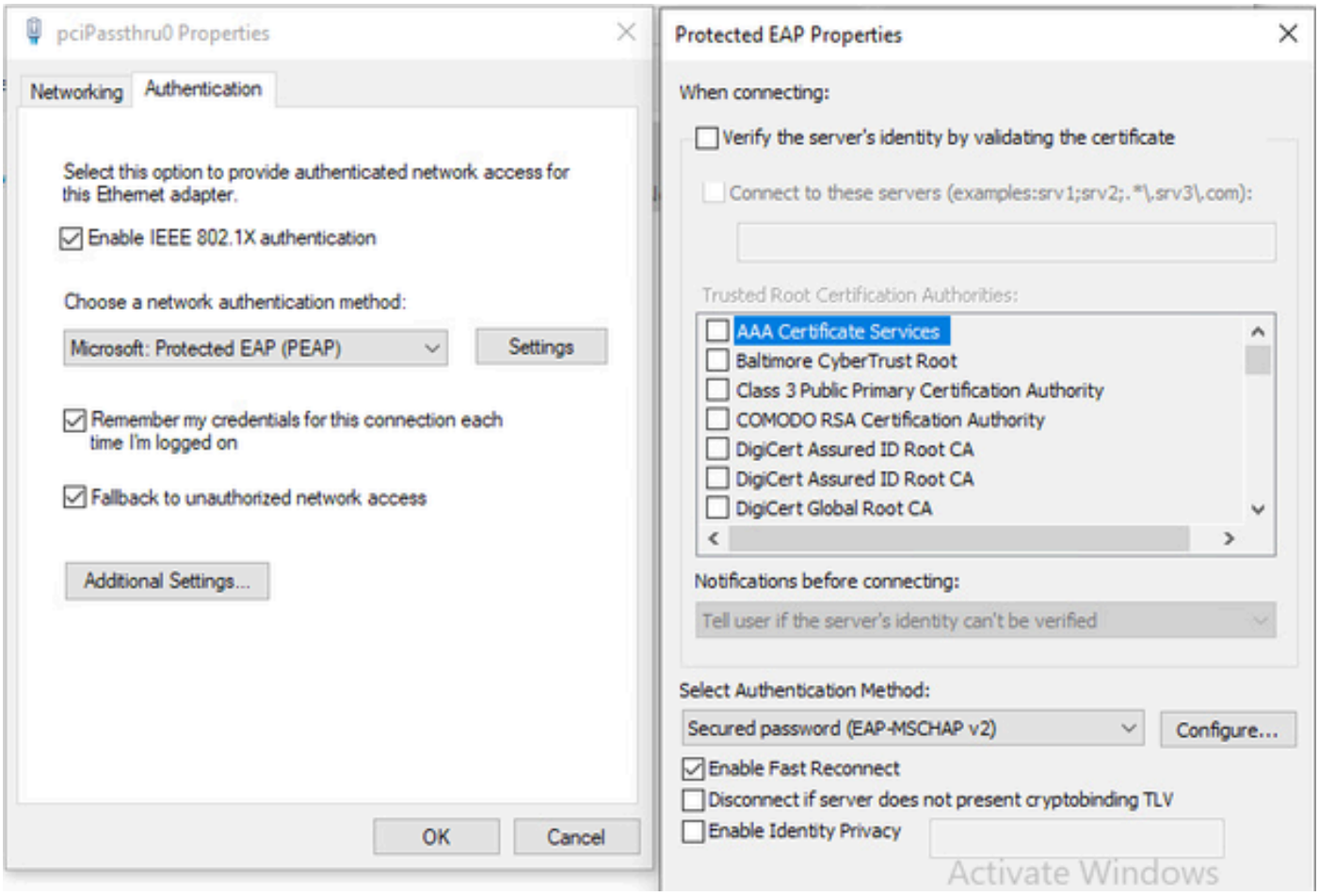
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



참고: encryption-key는 길이가 16자, message-auth-code가 20자여야 합니다.

PC

PEAP-MSCHAPv2에 대해 구성된 Windows 10 신청자.



다음을 확인합니다.

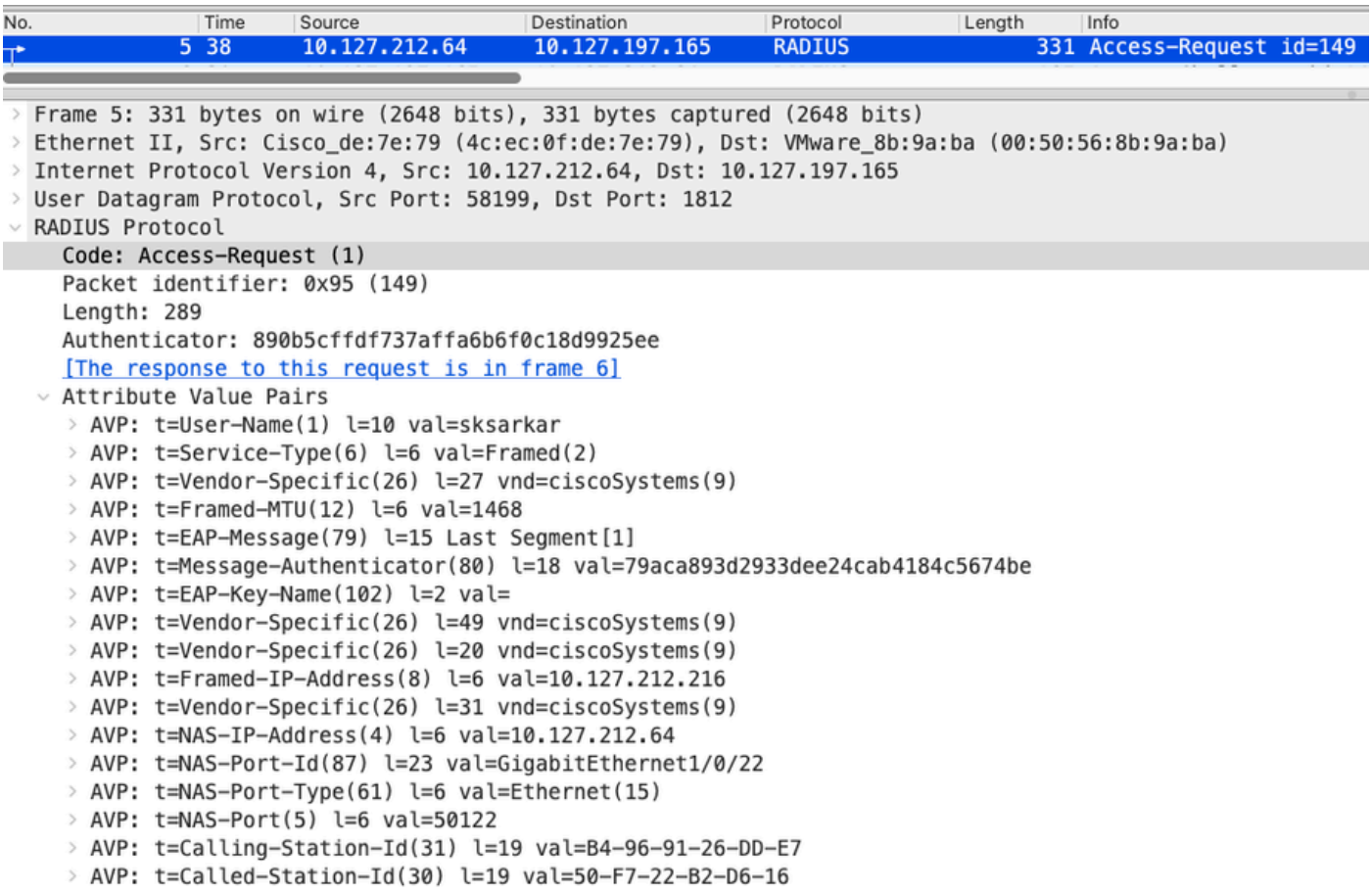
스위치에서 RADIUS KeyWrap 기능이 활성화되지 않은 경우:

show radius server-group <서버 그룹 이름>

명령 출력에는 Keywrap enabled가 표시되어야 합니다. 거짓.

```
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
```

패킷 캡처에서 app-key, random-nonce 및 별도의 message-authenticator-code에 대한 Cisco-AV-Pair 특성이 없음을 확인할 수 있습니다. 이는 스위치에서 RADIUS KeyWrap이 비활성화되었음을 나타냅니다.

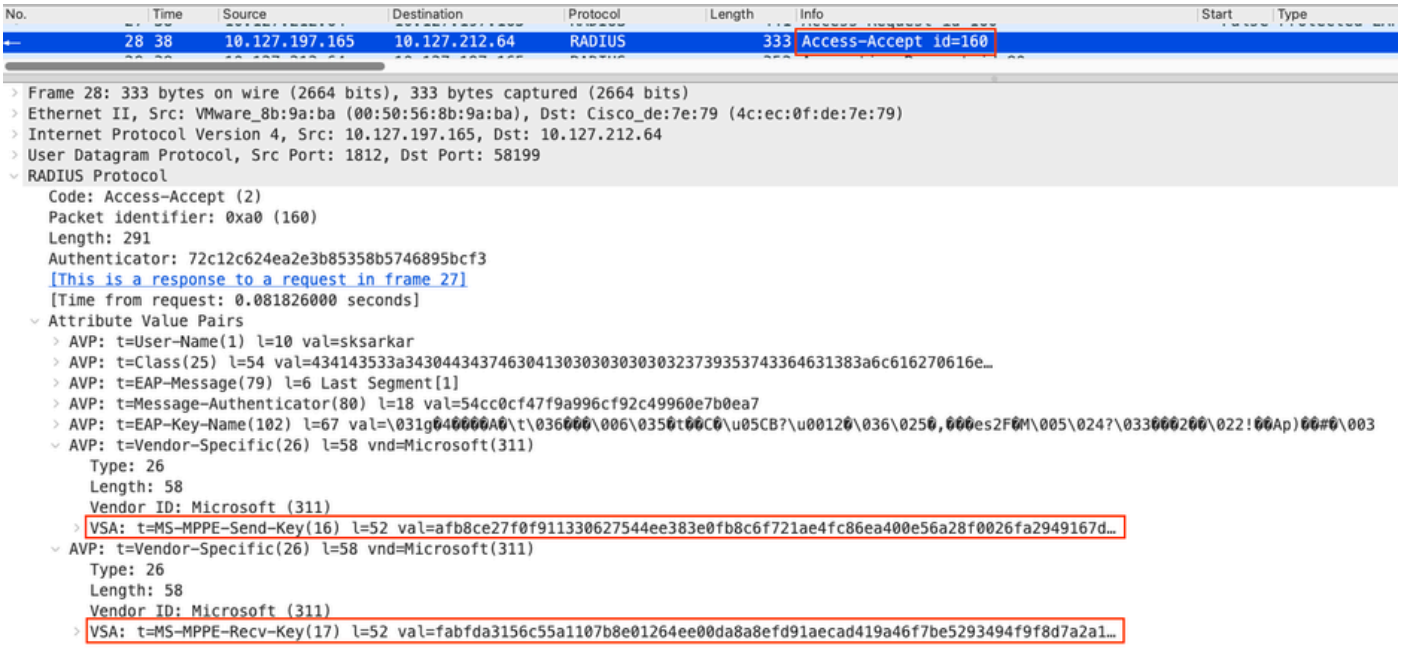


ISE prrt-server.log에서 ISE가 메시지 인증자인 무결성 특성만 검증하는 것을 볼 수 있습니다.

```
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 패킷에서는 MS-MPPE-Send-Key 및 MS-MPPE-Recv-Key가 RADIUS 서버에서 인증자로 전송되는 것을 확인할 수 있습니다. MS-MPPE는 피어와 인증자 간에 데이터 암호화를 수행하는 데 사용할 수 있는 EAP 방법으로 생성된 키 자료를 지정합니다. 이 32바이트 키는 RADIUS 공유 암호, 요청 인증자 및 임의 솔트에서 파생됩니다.



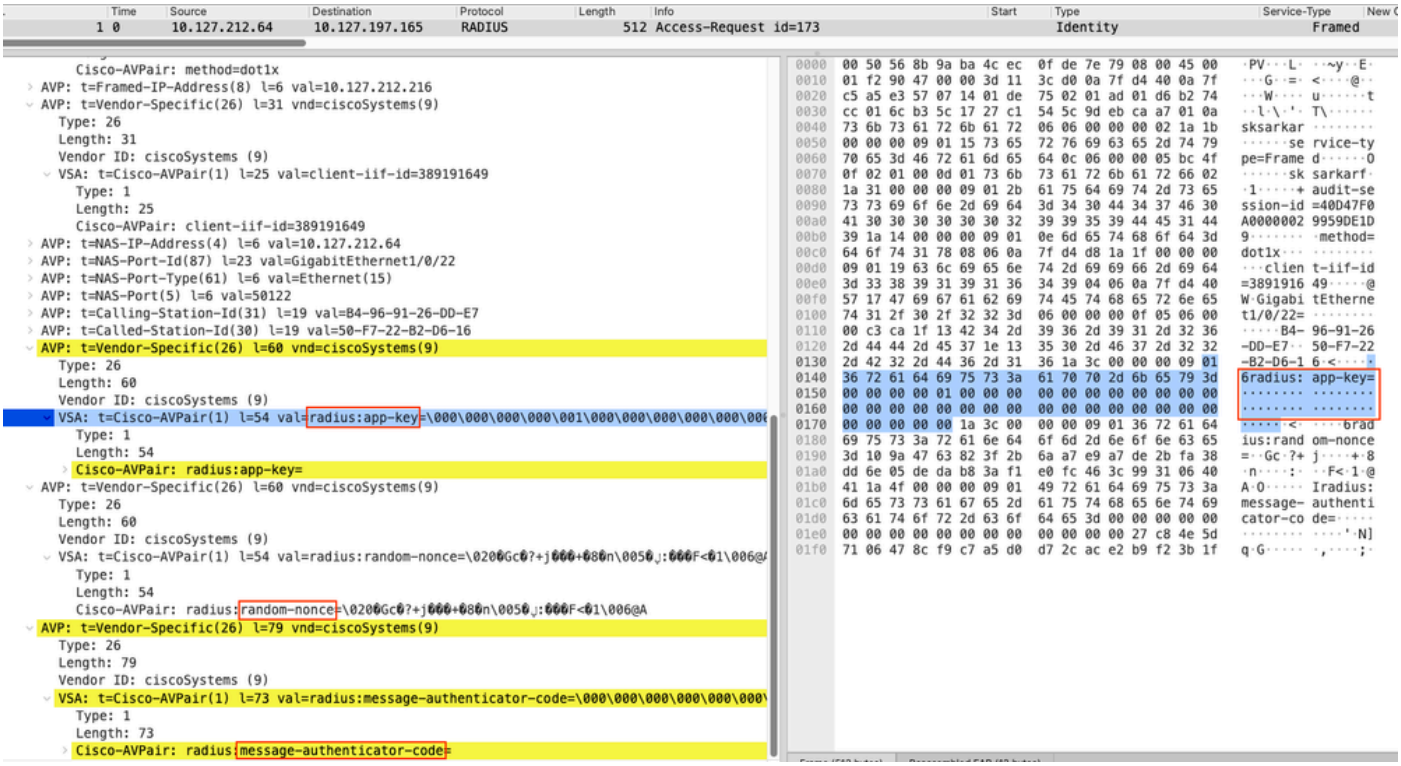
스위치 및 ISE에서 RADIUS KeyWrap 기능이 활성화된 경우:

show radius server-group <서버 그룹 이름>

명령 출력에는 Keywrap enabled가 표시되어야 합니다. 맞아.

```
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
```

패킷 캡처에서 앱 키(데이터 없음), 임의 nonce 및 별도의 메시지 인증자 코드에 대한 Cisco-AV-Pair 특성이 있음을 확인할 수 있습니다. 이는 인증자(스위치)가 RADIUS KeyWrap을 지원하고 서버가 이를 사용해야 함을 RADIUS 서버에 알려줍니다.

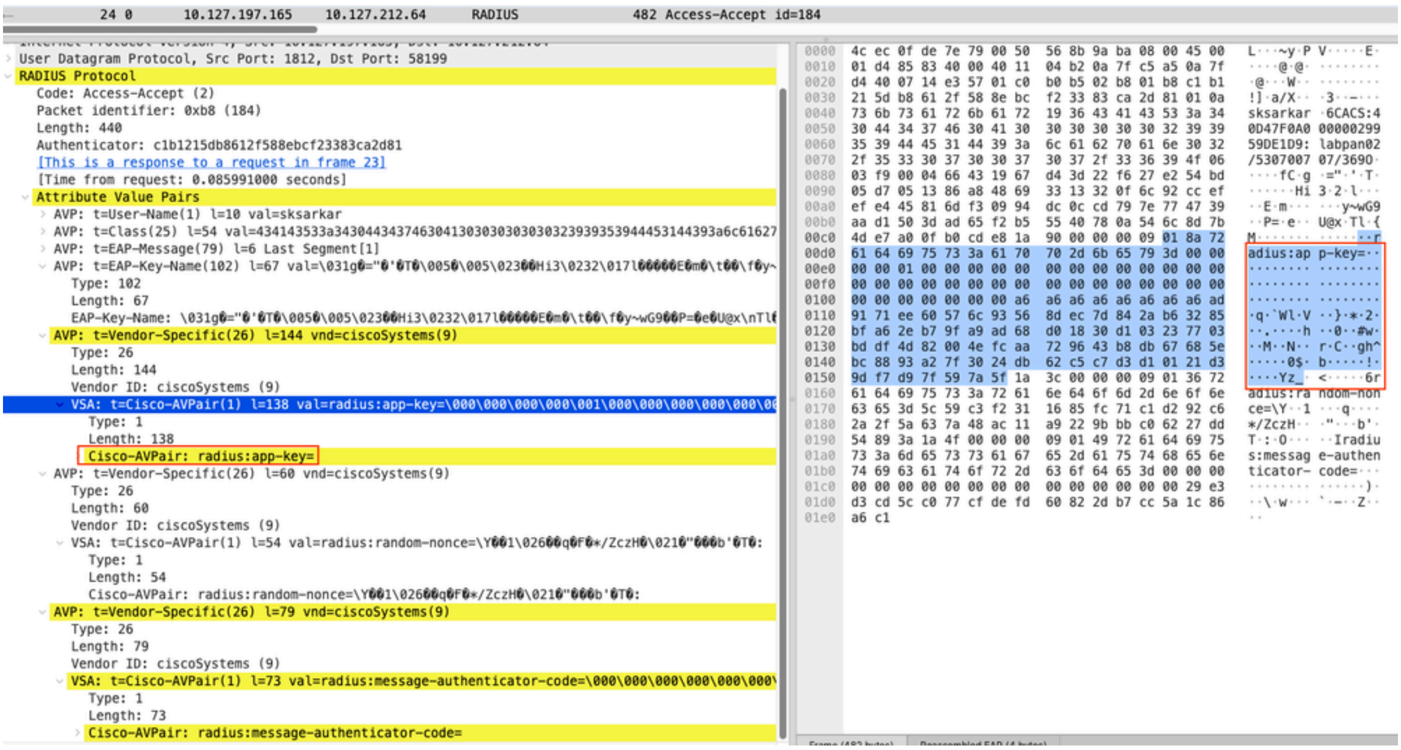


ISE prrt-server.log에서 ISE가 app-key 특성을 검증하고 ACCESS-REQUEST 패킷에 random-nonce 및 message-authenticator-code가 있음을 확인할 수 있습니다.

```
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 패킷에서는 app-key 특성의 암호화된 키 자료를 random-nonce 및 message-authenticator-code와 함께 볼 수 있습니다. 이러한 특성은 현재 정의된 공급업체별 MS-MPPE-Send-Key 및 MS-MPPE-Recv-Key 특성보다 강력한 보호 기능과 더 높은 유연성을 제공하도록 설계되었습니다.



자주 묻는 질문(FAQ)

1) RADIUS KeyWarp를 작동하려면 네트워크 디바이스와 ISE 모두에서 활성화해야 합니까?

예. RADIUS KeyWrap이 작동하려면 네트워크 디바이스와 ISE 모두에서 활성화되어야 합니다. ISE에서만 KeyWrap을 활성화하지만 네트워크 디바이스에서는 활성화하지 않는 경우에도 인증은 계속 작동합니다. 그러나 ISE가 아닌 네트워크 디바이스에서 활성화한 경우 인증이 실패합니다.

2) KeyWrap를 활성화하면 ISE 및 네트워크 디바이스의 리소스 사용률이 증가합니까?

아니요. KeyWrap를 활성화한 후에는 ISE 및 네트워크 디바이스에서 리소스 사용률이 크게 증가하지 않습니다.

3) RADIUS KeyWrap은 얼마나 많은 보안을 제공합니까?

RADIUS 자체는 해당 페이로드에 대한 암호화를 제공하지 않으며, KeyWrap는 키 자료를 암호화하여 추가 보안을 제공합니다. 보안 수준은 어떤 암호화 알고리즘을 사용하여 키 자료를 암호화하느냐에 따라 달라진다. ISE에서 AES는 키 자료를 암호화하는 데 사용됩니다.

참조

- 키 관련 자료 제공을 위한 Cisco 벤더별 RADIUS 특성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.