

在ISE中配置RADIUS KeyWrap

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[ISE](#)

[交换机](#)

[PC](#)

[验证](#)

[常见问题解答](#)

[参考](#)

简介

本文档介绍在思科ISE和思科交换机中配置RADIUS KeyWrap的过程。

先决条件

- dot1x知识
- RADIUS协议知识
- EAP知识

使用的组件

- ISE 3.2
- 软件版本为17.09.04a的思科C9300-24U
- Windows 10 PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

密钥包装是一种使用另一个密钥加密一个密钥值的技术。在RADIUS中使用相同的机制来加密密钥材料。此材料通常作为可扩展身份验证协议(EAP)身份验证的副产品生成，并在身份验证成功后返回到“访问接受”消息中。如果ISE在FIPS模式下运行，则此功能是必需的。

这提供了一个保护层，该层将实际的关键材料隔离起来，以防范潜在的攻击。基本上，威胁发起者根本无法访问底层关键材料，即使是在数据拦截的情况下。RADIUS密钥包装的主要目的是防止安

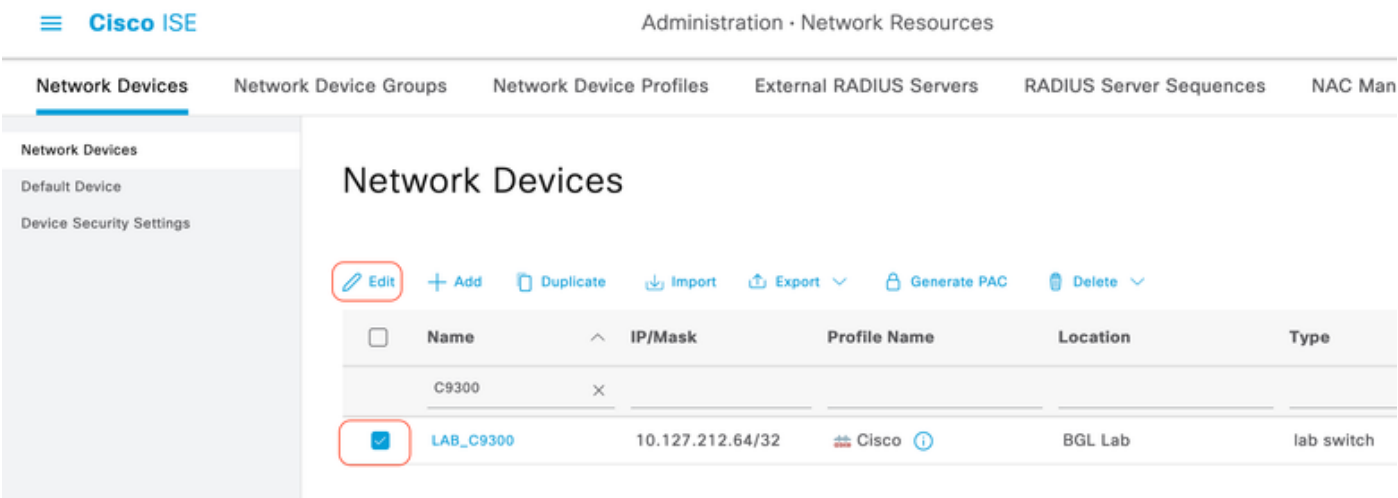
全数字内容的关键材料的曝光，特别是在大规模的企业级网络中。

在ISE中，密钥加密密钥用于使用AES加密和从RADIUS共享密钥分离的消息身份验证器代码密钥来加密密钥材料，以生成消息身份验证器代码。

配置

ISE

步骤 1：导航到Administration > Network Resources > Network Devices。点击要为其配置RADIUS KeyWrap的网络设备的复选框。单击Edit (如果已添加网络设备)。



步骤 2：展开RADIUS身份验证设置。单击Enable KeyWrap复选框。输入密钥加密密钥(Key Encryption Key)和消息验证器代码密钥(Message Authenticator Code Key)。Click Save.

General Settings

☒ Enable KeyWrap ⓘ

Key Encryption Key 22AB0###CA#1b2b1 [Hide](#)

Message
Authenticator Code 12b1CcB202#2Cb1#bCa# [Hide](#)
Key

Key Input Format

☒ ASCII ☐ HEXADECIMAL



注意：密钥加密密钥和消息身份验证器代码密钥必须不同。

交换机

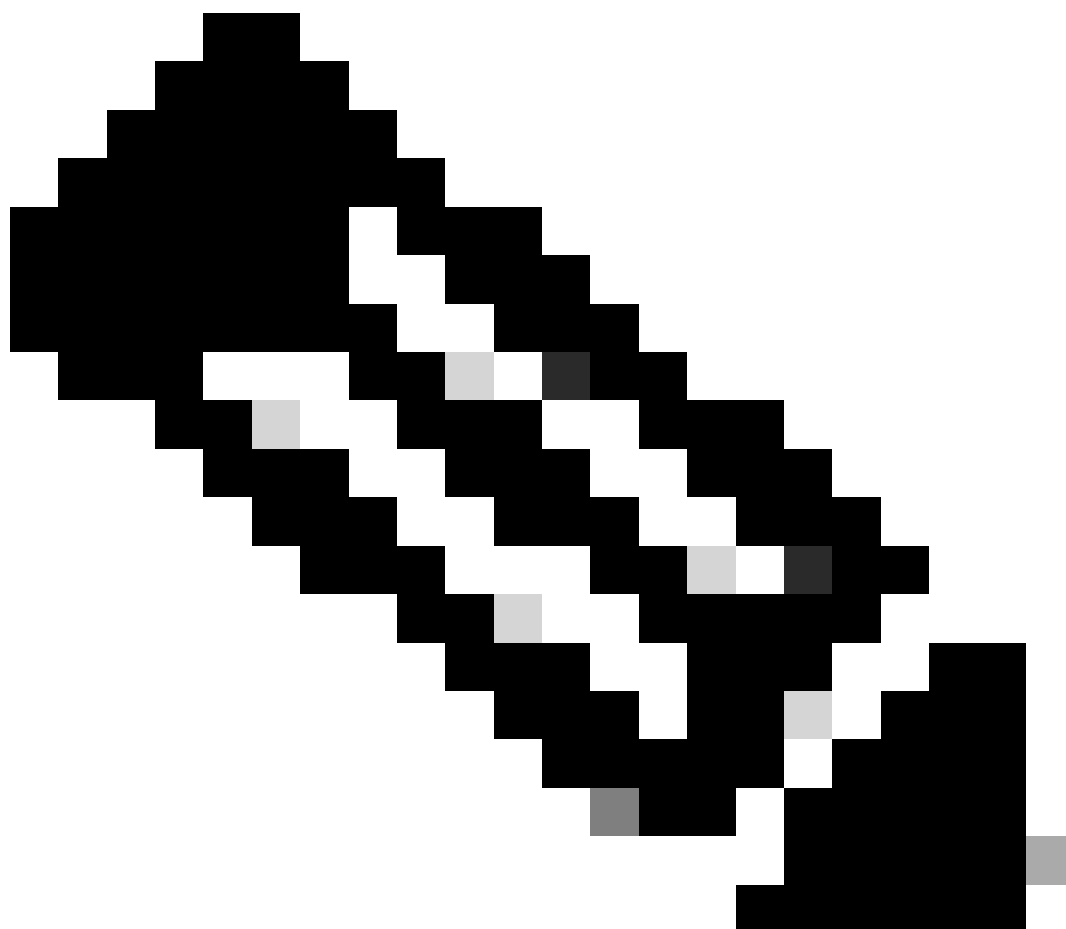
交换机中的AAA配置，以启用RADIUS KeyWrap功能。

```
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
```

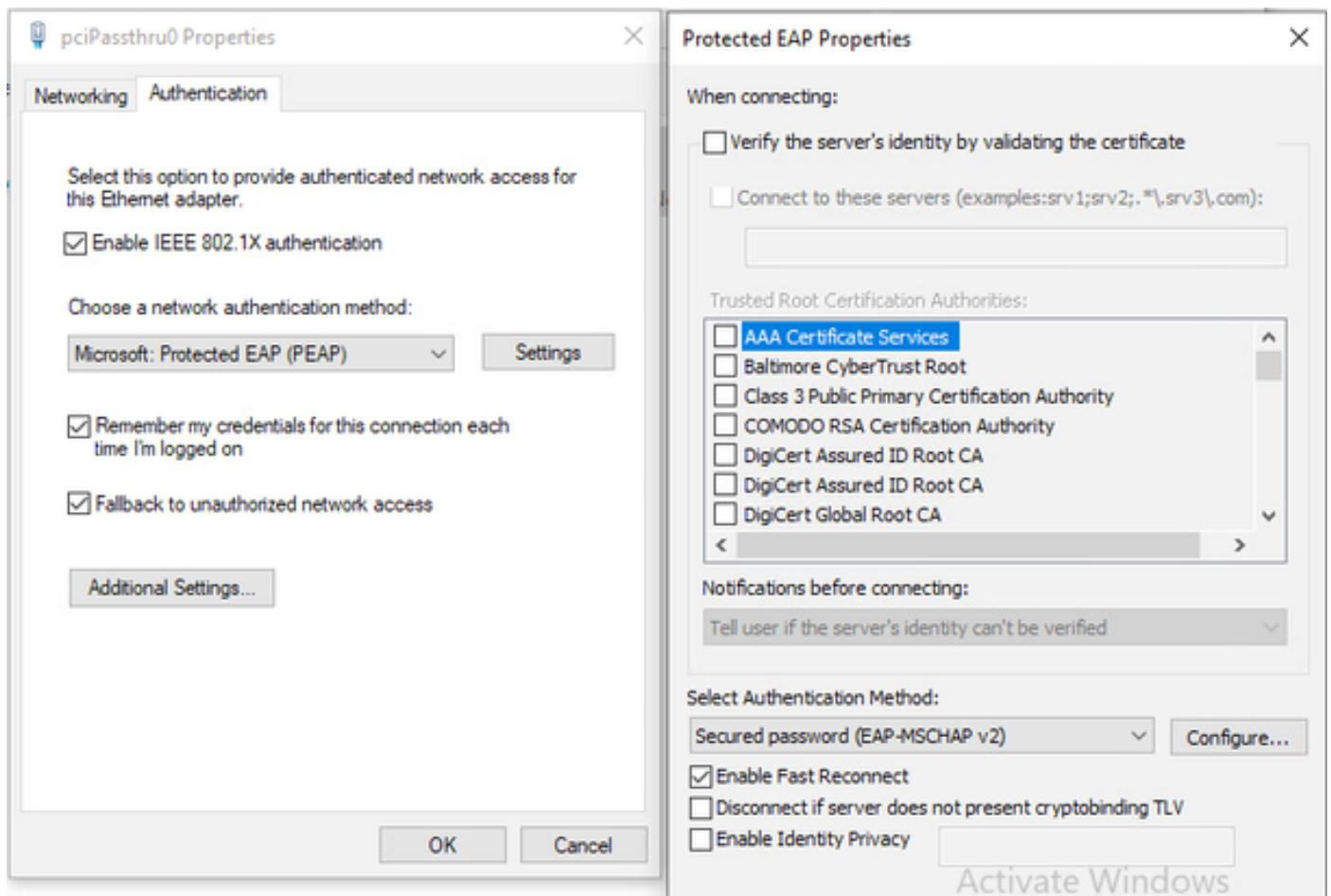
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



注意：encryption-key的长度必须为16个字符，并且必须是message-auth-code和20个字符。

PC

为PEAP-MSCHAPv2配置的Windows 10请求方。



验证

当交换机上未启用RADIUS KeyWrap功能时：

show radius server-group <服务器组名称>

命令输出必须显示Keywrap enabled:FALSE。

```
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
```

在数据包捕获中，您可以看到app-key、random-nonce和separate message-authenticator-code没有Cisco-AV-Pair属性。这表示交换机上禁用了RADIUS KeyWrap。

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 > RADIUS Protocol						
Code: Access-Request (1) Packet identifier: 0x95 (149) Length: 289 Authenticator: 890b5cffdf737affa6b6f0c18d9925ee [The response to this request is in frame 6]						
> 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						

在ISE prrt-server.log中，您可以看到ISE仅验证完整性属性，即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=1abpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=1abpan02/530700707/490,Calling

```

在Access-Accept数据包中，您可以看到MS-MPPE-Send-key和MS-MPPE-Recv-Key从RADIUS服务器发送到身份验证器。MS-MPPE指定EAP方法生成的密钥材料，可用于在对等方和身份验证器之间执行数据加密。这些32字节的密钥由RADIUS共享密钥、请求身份验证器和随机盐派生。

No.	Time	Source	Destination	Protocol	Length	Info	Start	Type
28	38	10.127.197.165	10.127.212.64	RADIUS	333	Access-Accept id=160		
> Frame 28: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) > Ethernet II, Src: Vmware_8b:9a:ba (00:50:56:8b:9a:ba), Dst: Cisco_de:7e:79 (4c:ec:0f:de:7e:79) > Internet Protocol Version 4, Src: 10.127.197.165, Dst: 10.127.212.64 > User Datagram Protocol, Src Port: 1812, Dst Port: 58199 > RADIUS Protocol Code: Access-Accept (2) Packet identifier: 0xa0 (160) Length: 291 Authenticator: 72c12c624ea2e3b85358b5746895bcf3 [This is a response to a request in frame 27] [Time from request: 0.081826000 seconds] > Attribute Value Pairs > AVP: t=User-Name(1) l=10 val=sksarkar > AVP: t=Class(25) l=54 val=434143533a3430443437463041303030303030323739353743364631383a6c616270616e... > AVP: t=EAP-Message(79) l=6 Last Segment[1] > AVP: t=Message-Authenticator(80) l=18 val=54cc0cf47f9a996cf92c49960e7b0ea7 > AVP: t=EAP-Key-Name(102) l=67 val=\031g040000A0\t\036000\006\0350t00C0\u05CB?\u00120\036\0250,000es2F0M\005\024?\033000200\022!00Ap)00#0\003 > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311) Type: 26 Length: 58 Vendor ID: Microsoft (311) > VSA: t=MS-MPPE-Send-Key(16) l=52 val=afb8ce27f0f911330627544ee383e0fb8c6f721ae4fc86ea400e56a28f0026fa2949167d... > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311) Type: 26 Length: 58 Vendor ID: Microsoft (311) > VSA: t=MS-MPPE-Recv-Key(17) l=52 val=fabfda3156c55a1107b8e01264ee00da8a8efd91aecad419a46f7be5293494f9f8d7a2a1...								

当在交换机和ISE上启用RADIUS KeyWrap功能时：

show radius server-group <服务器组名称>

```
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
```

在数据包捕获中，您可以看到app-key（无数据）、random-nonce和单独的消息 — authenticator-code存在Cisco-AV-Pair属性。这向RADIUS服务器指示身份验证器（交换机）支持RADIUS KeyWrap，并且服务器必须使用相同的身份验证。

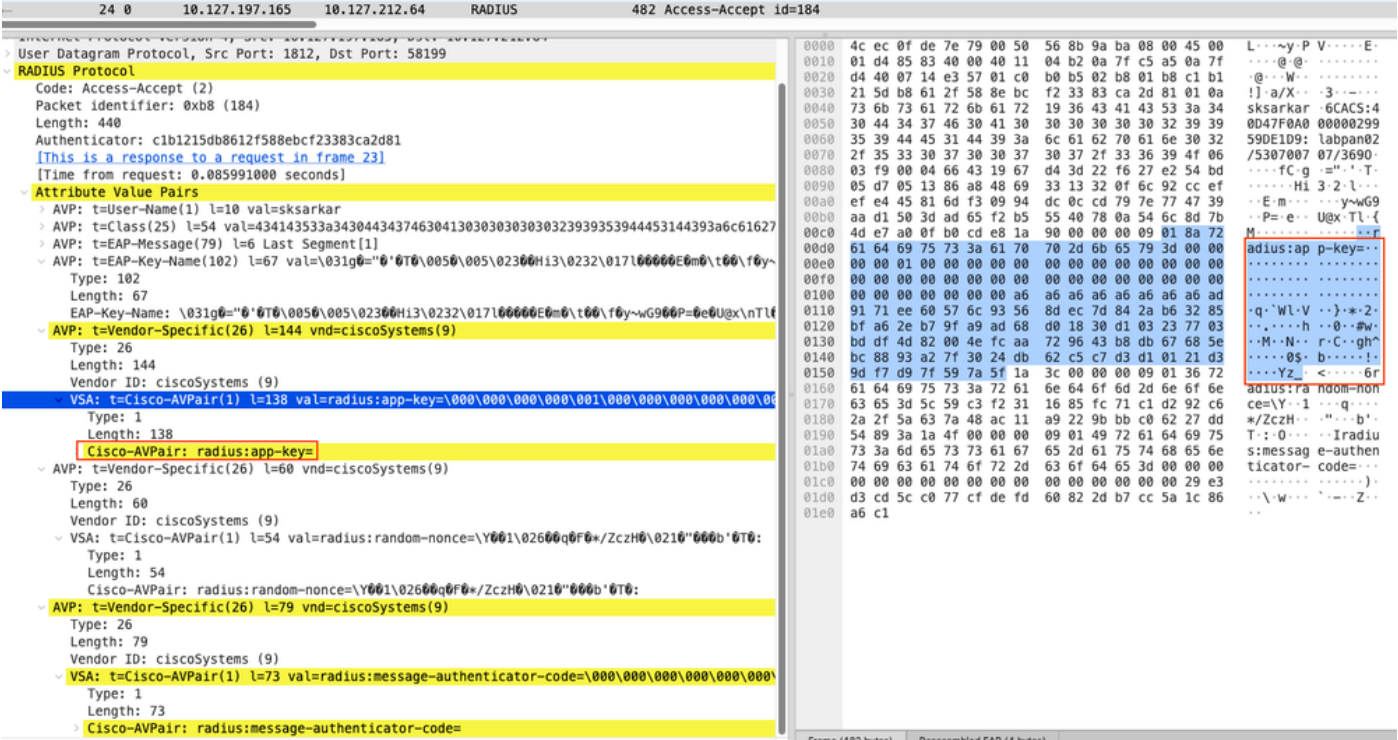
Time	Source	Destination	Protocol	Length	Info	Start	Type	Service-Type	New
1	0	10.127.212.64	10.127.197.165	RADIUS	512	Access-Request id=173	Identity	Framed	
					Cisco-AVPair: method=dot1x	0000	00 50 56 8b 9a ba 4c ec	0f de 7e 79 08 00 45 00	..PV...L...y...E...
					AVP: t=Framed-IP-Address(8) l=6 val=10.127.212.16	0010	01 f2 90 47 00 00 3d 11	3c d0 0a 7f d4 0a 0a 7f	...G...=<...@...
					AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)	0020	c5 a5 e3 57 07 14 01 de	75 02 01 ad 01 d6 b2 74	...W...U...t...
					Type: 26	0030	cc 01 6c b3 5c 17 27 c1	54 5c 9d eb ca a7 01 0a	..L\...T...e...
					Length: 31	0040	73 6b 73 61 72 6b 61 72	06 06 00 00 00 02 1a 1b	sksarkar
					Vendor ID: ciscoSystems(9)	0050	00 00 00 09 01 15 73 65	72 76 69 63 65 2d 74 79	...sk sarkar...
					VSA: t=Cisco-AVPair(1) l=25 val=client-ii-f-id=389191649	0060	70 65 3d 46 72 61 6d 65	64 0c 06 00 00 05 bc 4f	pe=Frame d...=0
					Type: 1	0070	0f 02 01 00 0d 01 73 6b	73 61 72 6b 61 72 66 02	...sk sarkar...
					Length: 25	0080	1a 31 00 00 00 09 01 2b	61 75 64 69 74 2d 73 65	..1...- audit-se
					Cisco-AVPair: client-ii-f-id=389191649	0090	73 73 69 6f 6e 2d 69 64	3d 34 30 44 34 37 46 30	ssion-Id =40D47F0
					AVP: t=NAS-IP-Address(4) l=6 val=10.127.212.64	00a0	41 30 30 30 30 30 30 32	39 39 35 39 44 45 31 44	A0000002 9959DE1D
					AVP: t=NAS-Port-Id(87) l=23 val=GigabitEthernet1/0/22	00b0	39 1a 14 00 00 00 09 01	0e 6d 65 74 68 6f 64 3d	9... method=
					AVP: t=NAS-Port-Id(61) l=6 val=Ethernet(15)	00c0	64 6f 74 31 78 08 06 0a	7f d4 d8 1a 1f 00 00 00	dot1x...
					AVP: t=NAS-Port(5) l=6 val=50122	00d0	09 01 19 63 6c 69 65 6e	74 2d 69 69 6e 2d 69 64	...clien t-ii-f-id
					AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DD-E7	00e0	3d 33 38 39 31 39 31 36	34 39 04 06 0a 7f d4 40	=3891916 49...@...
					AVP: t=Called-Station-Id(30) l=19 val=50-F7-22-B2-D6-16	00f0	17 47 47 69 6f 61 62 69	74 45 74 68 65 72 6e 65	W Gigabi Ethernet
					AVP: t=Vendor-Specific(26) l=60 vnd=ciscoSystems(9)	0100	70 31 2f 30 2f 32 32 3d	06 00 00 00 0f 05 06 00	tl/0/22=
					Type: 26	0110	00 c3 ca 1f 13 42 34 2d	39 36 2d 39 31 2d 32 36	...B4- 96-91-26
					Length: 60	0120	2d 44 42 2d 45 37 1e 13	35 30 2d 46 37 2d 32 32	-DD-E7- 50-F7-22
					Vendor ID: ciscoSystems(9)	0130	2d 42 32 2d 44 36 2d 31	36 1a 3c 00 00 00 09 01	-B2-D6-1 6<...>
					VSA: t=Cisco-AVPair(1) l=54 val=radius:app-key=	0140	36 72 61 64 69 75 73 3a	61 70 70 2d 6b 65 79 3d	6radius: app-key=
					Type: 1	0150	00 00 00 01 00 00 00 00	00 00 00 00 00 00 00 00	
					Length: 54	0160	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
					Cisco-AVPair: radius:app-key=	0170	00 00 00 00 00 1a 3c 00	00 00 00 09 01 36 72 61 64	<...brad
					AVP: t=Vendor-Specific(26) l=60 vnd=ciscoSystems(9)	0180	69 75 73 3a 72 61 6e 64	6f 6d 2d 6e 6f 6e 63 65	ius:rand om-nonce
					Type: 26	0190	3d 10 9a 47 63 82 3f 2b	6a a7 e9 a7 de 2b fa 38	...Gc ?+ j...+ 8
					Length: 60	01a0	dd 6e 05 de da b8 3a f1	e0 fc 46 3c 99 31 06 40	...n...:...F<- 1@
					Vendor ID: ciscoSystems(9)	01b0	41 1a 4f 00 00 00 09 01	49 72 61 64 69 75 73 3a	A 0...:radius:
					VSA: t=Cisco-AVPair(1) l=54 val=radius:random-nonce=	01c0	6d 65 73 73 61 67 65 2d	61 75 74 68 65 6e 74 69	message- authenti
					Type: 1	01d0	63 61 74 6f 72 2d 63 6f	64 65 3d 00 00 00 00 00	cator-co des=
					Length: 54	01e0	00 00 00 00 00 00 00 00	00 00 00 00 27 c8 4e 5d	[N]
					Cisco-AVPair: radius:random-nonce=	01f0	71 06 47 8c f9 c7 a5 d0	d7 2c ac e2 b9 f2 3b 1f	q G...: ,...;

在ISE prrt-server.log中，您可以看到ISE验证属性app-key，并且random-nonce和message-authenticator-code出现在ACCESS-REQUEST数据包中。

```
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-iiif-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

在Access-Accept数据包中，您可以看到app-key属性中的加密密钥材料以及随机事件和消息身份验证器代码。这些属性旨在提供比当前定义的供应商特定MS-MPPE-Send-Key和MS-MPPE-Recv-Key属性更强的保护和更高的灵活性。



常见问题解答

1)是否需要在网络设备和ISE上启用RADIUS KeyWrap才能使其正常工作？

是，RADIUS KeyWrap需要在网络设备和ISE上启用才能正常运行。但是，如果仅在ISE上启用密钥绕行，但在网络设备上不启用，则身份验证仍然有效。但是，如果您在网络设备上启用它，但在ISE中未启用，则身份验证失败。

2)启用KeyWrap是否会增加ISE和网络设备的资源利用率？

否，启用KeyWrap后，ISE和网络设备的资源利用率不会显著提高。

3)RADIUS KeyWrap提供多少额外安全性？

由于RADIUS本身不为其负载提供任何加密，KeyWrap通过加密密钥材料提供额外的安全性。安全级别取决于使用哪种加密算法来加密密钥材料。在ISE中，AES用于加密密钥材料。

参考

- [用于交付密钥材料的思科供应商特定RADIUS属性](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。