

دعب نع لوصولل VPN ۋە كېش نىوكت طي طخت ئىلع RADIUS مادختساب و Group-Policy

تايي وتحمل

[قىدقملا](#)

[قيس اس ألا تابلطتملا](#)

[تابلطتملا](#)

[قىدختسملا تانوكملا](#)

[نىوكتلى](#)

[نىوكتلى](#)

[ASA](#)

[\(ISE\) قىوهلا فىشك تامدخ كرحم](#)

[قىصىلانم قىرحتلى](#)

[لمعلا وىرىانىس](#)

[اچالص او عاطخالا فاشكىتسا](#)

[1 لمعلا مدع وىرىانىس](#)

[2 لمعلا مدع وىرىانىس](#)

[3 لمعلا مدع وىرىانىس](#)

[وىدىفلى](#)

قىدقملا

قىدقملا ئىس ئىيىعتل دعب نع لوصولل VPN ۋە كېش نىوكت دنتسىمىلا اذه فصىي فىرعت تامدخ كرحم مادختساب Cisco (ISE).

قيس اس ألا تابلطتملا

تابلطتملا

قىيلاتلا عيضاوملاپ ئەفرۇم كىدل نوكت نأب Cisco يىصوت:

- Cisco Secure Client (AnyConnect)
- Cisco ISE
- Cisco ASA (مۇ فىيكتىلل لباقلانامالا زاھج ئىلع دعب نع لوصولل VPN ۋە كېش Cisco)

قىدختسملا تانوكملا

قىيلاتلا ئىداملا تانوكملا وجماربلا تارادصا ئىل دنتسىمىلا اذه ىوتحم دنتسىي.

- ASA 5506 ةغىص جمانرب عم 9.8.1
- AnyConnect نم 4.8 رادصإلا
- ISE 2.4 رادصإلا

ةصالخ ةيلمعم ةئيب يف ةدوچوملا ةزهچألا نم دنتسملا اذه يف ةدراولا تامولعملاءاشنإ مت تناك اذا .(يضرارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهچألا عيمج تأدب رمأ يأ لمحملارياحتسلالكمهف نم داكتف ،ليغشتلا ديق كتكبش.

نيوكتلا

VPN رباع ASA ب نولصتي نيدللا نيديعبلا نيمدختسمملل حمسى ال ،اذه نيوكتلا لاثم يف نم (قافنأ ةعومجم) لاصتا فيرعت فلم ديدحتب Cisco Secure Client (AnyConnect) مادختساب ىلا ادانتسا ددحم ةعومجم جهـن ىـلا مـهـنـيـيـعـتـبـ Cisco ISE مـوقـيـ ثـيـحـ ،ـقـلـدـسـنـمـلـاـ ـةـمـيـاـقـلـاـ اـهـنـيـوـكـتـ مـتـ يـتـلـاـ تـاسـاـيـسـلـاـ.

ISE لالخ نم AnyConnect مـدـخـتـسـمـ لـكـلـ ةـعـوـمـجـمـ ةـسـاـيـسـ نـيـيـعـتـ كـنـكـمـيـ ،ـدـادـعـ إـلـاـ اـذـهـ مـادـخـتـسـابـ يـفـ نـوـنـوـكـيـ مـهـنـإـفـ ،ـقـفـنـلـاـ ةـعـوـمـجـمـ دـيـدـحـتـلـ رـايـخـلـاـ مـهـيـدـلـ سـيـلـ نـيـمـدـخـتـسـمـلـاـ نـأـلـ اـرـظـنـوـ دـعـبـ DfltGrpPolicy. قـفـنـلـاـ ةـعـوـمـجـمـبـ نـيـلـصـتـمـ ةـيـادـبـلـاـ ةـبـاجـتـسـاـ نـمـضـ ISE ةـطـسـاوـبـ (ـعـوـمـجـمـلـاـ جـهـنـ) RADIUS ةـئـفـ ةـمـسـ لـاسـرـاـ مـتـ اـذـاـ ،ـقـدـاـصـمـلـاـ يـقـلـتـ مـتـيـ يـلـاتـلـابـوـ ،ـقـبـاطـمـلـاـ ةـعـوـمـجـمـلـاـ جـهـنـ ىـلـاـ مـدـخـتـسـمـلـاـ نـيـيـعـتـ مـتـيـ ،ـقـدـاـصـمـلـاـ مـلـ ةـعـوـمـجـمـ جـهـنـ ةـيـمـسـتـ عـاجـرـاـ وـأـ ةـيـفـلـاـ نـمـ ةـمـسـ يـأـ عـاجـرـابـ ISE مـقـيـ مـلـ اـذـاـ .ـقـبـسـانـمـلـاـ تـانـوـذـأـلـاـ نـيـمـدـخـتـسـمـلـاـ عـنـمـلـ DfltGrpPolicy. ىـلـاـ اـنـيـعـمـ مـدـخـتـسـمـلـاـ لـظـيـسـفـ ،ـقـلـعـ اـهـنـيـوـكـتـ مـتـيـ رـمـأـلـاـ نـيـوـكـتـ كـنـكـمـيـ ،ـقـكـبـشـ لـالـخـ نـمـ لـاصـتـالـاـ نـمـ نـيـعـمـ ةـعـوـمـجـمـ جـهـنـ مـهـيـدـلـ سـيـلـ نـيـذـلـاـ vpn-synchronins ةـعـوـمـجـمـلـاـ جـهـنـ نـمـضـ 0 DfltGrpPolicy.

نيوكتلا

ASA

مـداـخـ AAA

```
aaa-server ISE_AAA protocol radius
aaa-server ISE_AAA (Outside) host 10.31.124.82
key cisco123
```

دعـبـ نـعـ لـوـصـوـلـلـ VPNـ نـيـوـكـتـ

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
anyconnect enable

tunnel-group DefaultWEBVPNGroup general-attributes
address-pool Remote_users
authentication-server-group ISE_AAA
```

```

group-policy DfltGrpPolicy attributes
banner value ###YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES###
vpn-simultaneous-logins 0
vpn-tunnel-protocol ssl-client

group-policy RADIUS-USERS internal
group-policy RADIUS-USERS attributes
banner value YOU ARE CONNECTED TO ### RADIUS USER AUTHENTICATION###
vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
split-tunnel-network-list value SPLIT_ACL

group-policy RADIUS-ADMIN internal
group-policy RADIUS-ADMIN attributes
banner value YOU ARE CONNECTED TO ###RADIUS ADMIN AUTHENTICATION ###
vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
split-tunnel-network-list none

```

رقمه داخلي فشـك (ISE)

لـ كـرتـشمـلا يـرسـلـا حـاتـفـمـلا نـيـوـكـتـبـ مـقـوـ اـىـلـعـ حـلـاصـ ظـكـبـشـ زـاهـجـكـ ASA لـجـسـ . 1ـ ظـوـطـخـلـ رـادـيـعـ . ظـكـبـشـلـا ظـهـجـأـ ظـكـبـشـلـا درـاوـمـ > ظـرـادـإـلـا اـىـلـا لـقـتـنـاـ ، ضـغـلـا اـذـهـلـ.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Network Devices List > ASA**v**

Network Devices

* Name 

Description

IP Address * IP : / 

* Device Profile 

Model Name Software Version

* Network Device Group

Location Set To Default 

IPSEC Set To Default 

Device Type Set To Default 

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol 

* Shared Secret Hide 

Use Second Shared Secret 

CoA Port Show 

RADIUS DTLS Settings 

ةيوه تاعومجم عاشنإ 2. ۋوطخلا.

نومساقتى نيذل او ۋلېتامم صىاصىخ ب نىمدىختسىملا نارقىل ئىوهلا تاعومجم فىرعتب مقتاعومجم > ئەرادىلا ىلى لىقتنىا. ئىلاتلى تاوطخلا يىف رصانعلا ھىزىمداختسا مىتى. ۋلېتامم نوذا مدىختسىملا ئىوه.

User Identity Groups > RADIUS_ANYCONNECT_ADMIN

Identity Group

- * Name: RADIUS_ANYCONNECT
- Description:

Member Users

Status	Email	Username	First Name	Last Name
<input type="checkbox"/> Enabled		user1		

ةي وهلا تاع و مجمب نيم دختس مل ا نارقا 3. ۋوطخلما.

نيم دختس مل ا تاي و ه رادا ىل ا لقتنا . ٤. حيحصل ا ئي وهلا ئاع و مجمب نيم دختس مل ا نارقا.

Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	user1					RADIUS_ANYCONNECT	
<input type="checkbox"/> Enabled	user2					RADIUS_ANYCONNECT_USER	
<input type="checkbox"/> Enabled	user3						

تاس اي س ئاع و مجم ئاشن ا 4. ۋوطخلما.

لاثملا اذه يف . ئاس اي سلا قب اطلا يتللا طورشلا ديدحت و ئدي ديج تاس اي س ئاع و مجم ديدحت بمق تاع و مجم جه نلا ىل ا لقتنا ، ضرغلا اذهل . طورشلا تحت ئزه جالا عاونا عيمج ب حامسلا متى ج. 55.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	New Policy Set 1		DEVICE Device Type EQUALS All Device Types	Default Network Access	27		
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	0		

ل ي و خ ت ئاس اي س ئاشن ا 5. ۋوطخلما.

تاع و مجم نيم ضت نم دكأت . جه نلا ئاقب اطمبل ئاب ديدج ل ي و خ ت ج 55 ديدحت بمق طرشك 2 ۋوطخلما يف اهؤاشن ا مت يتللا ئي وهلا.

لـيـوـخـتـ فـيـرـعـتـ فـلـمـ عـاـشـنـاـ 6ـ ـوـطـخـلـاـ.

لـيـوـخـتـلـاـ ةـسـاـيـسـ ةـقـبـاطـمـ دـنـعـ اـهـذـاخـتـاـ مـتـيـ يـتـلـاـ تـاءـاـجـ إـلـاـ لـيـوـخـتـلـاـ فـيـرـعـتـ فـلـمـ نـمـضـتـيـ:ـ ةـيـلـاتـلـاـ تـامـسـلـاـ نـمـضـتـيـ دـيـدـجـ لـيـوـخـتـ فـيـرـعـتـ فـلـمـ عـاـشـنـاـ:

- ةـئـفـ RADIUS = <group-policy-ASA>
- لـوـصـوـلـاـ عـونـ: ACCESS_ACCEPT.

جـنـ مـسـاـ ةـقـبـاطـمـلـ ةـقـبـاسـلـاـ روـصـلـاـ يـفـ ضـوـعـمـلـاـ نـيـوـكـتـلـاـ رـيـرـحـتـ بـجـيـ:ـ ظـاحـالـمـ كـبـ صـاـخـلـاـ NـA~S~Aـ نـيـوـكـتـ يـفـ اـهـفـيـرـعـتـبـ تـمـقـ يـتـلـاـ ةـعـوـمـجـمـلـاـ.

Add New Standard Profile

Authorization Profile

* Name CLAS_25_RADIUS_ADMIN

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

This should be the Group-policy name

Advanced Attributes Settings

Radius:Class = RADIUS-ADMIN

Attributes Details

Access Type = ACCESS_ACCEPT
Class = RADIUS-ADMIN

Save Cancel

Lيوجتلا فيرعت فلم نيوكت عجار 7. ۋەطخىلا.

Identity Services Engine

Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration ▶ Work Centers

Policy Sets Profiling Posture Client Provisioning ▶ Policy Elements

Dictionaries ▶ Conditions ▶ Results

Authorization Profiles

Authorization Profile

* Name: CLASS_25_RADIUS_ADMIN

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Passive Identity Tracking: ⓘ

Common Tasks

Advanced Attributes Settings

Radius:Class = RADIUS-ADMIN

Attributes Details

Access Type = ACCESS_ACCEPT
Class = RADIUS-ADMIN

Save Reset

لک نییعت یف لیوخت جهن کي دل نوكی نأ نكمي، جهنهنلا ڈعو و مجم سفن یف: ظحالم یف ددم ددم ڈعو و مجم جهنهن لیا ڈي و ڈعو و مجم ASA.

The screenshot shows the Cisco Identity Services Engine (ISE) Policy Sets interface. A new policy set named "New Policy Set 1" is being created. The interface includes sections for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The Conditions section shows a rule for "DEVICE Device Type EQUALS All Device Types". The Authorization Policy section contains three rules: "ISE_CLASS_ADMIN", "ISE_CLASS_USER", and "Default". The "ISE_CLASS_ADMIN" and "ISE_CLASS_USER" rules both have conditions for "DEVICE Device Type EQUALS All Device Types" and "IdentityGroup Name EQUALS User Identity Groups:RADIUS_ANYCONNECT". The "ISE_CLASS_ADMIN" rule also has a condition for "CLASS_25_RADIUS_ADMIN" (highlighted with a red box). The "ISE_CLASS_USER" rule has a condition for "CLASS_25_RADIUS_USER" (also highlighted with a red box). The "Default" rule has a condition for "DenyAccess". The interface also includes search, reset, and save buttons.

مدختسم لکل يكيماني دلکشب ٰعوومجمل جهن نيعت كنكمي ،اذه نيوكتل ا لاثم مادختساب
مدختسملا اهيلا يمتنني يتلا ٰعيوهلا ٰعوومجم ىلا ادانتسا ISE نيوكت لالخ نم نما ليمع

ٰحصـلـا نـم قـقـحتـلـا

ٰقداصـم بـلـط لـيـصـافـت ضـرـعـي وـهـوـ debug radius . وـهـ ٰدـىـافـ عـاطـخـأـلـا حـيـحـصـت رـثـكـأـ دـحـأـ

```
debug radius
```

وـأـلـوـبـقـم ٰقداصـمـلـا تـنـاـكـ اـذـاـمـ ىـرـتـ نـآـلـاـ تـنـأـ رـمـأـلـاـ يـهـ ىـرـخـأـ ٰدـيـفـمـ ٰـدـأـ
ٰقداصـمـلـاـ ٰـيـلـمـعـ يـفـ اـهـلـدـابـتـ مـتـ يـتـلـاـ (ـلـاثـمـلـاـ اـذـهـ يـفـ ٰـقـيـفـلـاـ ٰـقـمـسـ)ـ تـامـسـلـاـوـ ٰـقـصـوـفـرـمـ

```
test aaa-server authentication
```

```
[host
```

```
|
```

```
] username
```

```
password
```

لەمۇلا ويرانىس

لەل لە RADIUS-Admin ۋە ئەنچەم جىھەن ئىلاردا مەختىسىملا يەمتنى، اقىبا سرۆكىمىلا نىيوكىتلا لەل اشىم يەف نىيكمەت و aaa-server راپتىخالا لېغىشتىپ تەملىق اذىتەتھىص نەم قىقەتلا نەكمىي ئىلاردا نىيوكىت نەم ئەلصلە تاد رەطسەلە ئىلۇق قىماڭلە طخلىپ ئەم الاع عضو مەتىي ASA. ئىلۇق radius ئاطاخ ئەنچەم حىچھىصەت ئەنچەم ئەنچەم حىچھىصەت تايىلمۇع.

<#root>

```
ASAv# debug radius
ASAv#test aaa-server authentication ISE_AAA host 10.31.124.82 username user1 password *****
INFO: Attempting Authentication test to IP address (10.31.124.82) (timeout: 12 seconds)
```

RADIUS packet decode (authentication request)

```
-----
Raw packet data (length = 84).....
01 1e 00 54 ac b6 7c e5 58 22 35 5e 8e 7c 48 73 | ...T...|.X"5^.|Hs
04 9f 8c 74 01 07 75 73 65 72 31 02 12 ad 19 1c | ...t..user1.....
40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f 04 06 0a | @C...F.5.R.o...
1f 7c 55 05 06 00 00 00 06 3d 06 00 00 00 05 1a | .|U.....=.....
15 00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d | .....coa-push=
74 72 75 65 | true
```

Parsed packet data.....

```
Radius: Code = 1 (0x01)
Radius: Identifier = 30 (0x1E)
Radius: Length = 84 (0x0054)
Radius: Vector: ACB67CE55822355E8E7C4873049F8C74
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31 |
```

user1

```
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
ad 19 1c 40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f | ...@.C...F.5.R.o
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.31.124.85 (0x0A1F7C55)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x6
```

```

Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 10.31.124.82/1645
rip 0x00007f03b419fb08 state 7 id 30
rad_vrfy() : response message verified
rip 0x00007f03b419fb08
: chall_state ''
: state 0x7
: reqauth:
    ac b6 7c e5 58 22 35 5e 8e 7c 48 73 04 9f 8c 74
: info 0x00007f03b419fc48
    session_id 0x80000007
    request_id 0x1e
    user 'user1'
    response '***'
    app 0
    reason 0
    skey 'cisco123'
    sip 10.31.124.82
    type 1

```

RADIUS packet decode (response)

```

-----
Raw packet data (length = 188).....
02 1e 00 bc 9e 5f 7c db ad 63 87 d8 c1 bb 03 41 | .....|...c.....A
37 3d 7a 35 01 07 75 73 65 72 31 18 43 52 65 61 | 7=z5..user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37 | uthSession:0a1f7
63 35 32 52 71 51 47 52 72 70 36 5a 35 66 4e 4a | c52RqQGRrp6Z5fNj
65 4a 39 76 4c 54 6a 73 58 75 65 59 35 4a 70 75 | eJ9vLTjsXueY5Jpu
70 44 45 61 35 36 34 66 52 4f 44 57 78 34 19 0e | pDEa564fRODWx4..
52 41 44 49 55 53 2d 41 44 4d 49 4e 19 50 43 41 | RADIUS-ADMIN.PCA
43 53 3a 30 61 31 66 37 63 35 32 52 71 51 47 52 | CS:0a1f7c52RqQGR
72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 6a 73 | rp6Z5fNJeJ9vLTjs
58 75 65 59 35 4a 70 75 70 44 45 61 35 36 34 66 | XueY5JpupDEa564f
52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 34 2f | RODWx4:iseamy24/
33 37 39 35 35 36 37 34 35 2f 33 31 | 379556745/31

```

Parsed packet data.....

```

Radius: Code = 2 (0x02)
Radius: Identifier = 30 (0x1E)
Radius: Length = 188 (0x00BC)
Radius: Vector: 9E5F7CDBAD6387D8C1BB0341373D7A35
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31

```

user1

```

Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)

```

```

Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 | ReauthSession:0a
31 66 37 63 35 32 52 71 51 47 52 72 70 36 5a 35 | 1f7c52RqQGrp6Z5
66 4e 4a 65 4a 39 76 4c 54 6a 73 58 75 65 59 35 | fNJeJ9vLTjsXueY5
4a 70 75 70 44 45 61 35 36 34 66 52 4f 44 57 78 | JpupDEa564fRODWx
34 | 4

```

Radius: Type = 25 (0x19) Class

```

Radius: Length = 14 (0x0E)
Radius: Value (String) =
52 41 44 49 55 53 2d 41 44 4d 49 4e

```

|

RADIUS-ADMIN

```

Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 52 71 51 | CACS:0a1f7c52RqQ
47 52 72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 | GRrp6Z5fNJeJ9vLT
6a 73 58 75 65 59 35 4a 70 75 70 44 45 61 35 36 | jsXueY5JpupDEa56
34 66 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 | 4fRODWx4:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 31 | 4/379556745/31
rad_procpkt: ACCEPT

```

RADIUS_ACCESS_ACCEPT

```

: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000007 id 30
free_rip 0x00007f03b419fb08
radius: send queue empty

```

INFO: Authentication Successful

لبق نم 1 مدخلت سملل حيحصل افعوم جمل اجهن نيعي مث اذا ام نم ققحتلل يرخاً ٰ قيرط كانه ISE show vpn-sessionDB AnyConnect.

<#root>

ASAv#

show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username	:	user1			
	Index	: 28			
Assigned IP	:	10.100.2.1	Public IP	:	10.100.1.3
Protocol	:	AnyConnect-Parent SSL-Tunnel DTLS-Tunnel			
License	:	AnyConnect Premium			
Encryption	:	AnyConnect-Parent: (1)none	SSL-Tunnel: (1)AES-GCM-256	DTLS-Tunnel: (1)AES256	
Hashing	:	AnyConnect-Parent: (1)none	SSL-Tunnel: (1)SHA384	DTLS-Tunnel: (1)SHA1	
Bytes Tx	:	15604	Bytes Rx	:	28706

Group Policy : RADIUS-ADMIN

```

Tunnel Group : DefaultWEBVPNGroup

Login Time   : 04:14:45 UTC Wed Jun 3 2020
Duration     : 0h:01m:29s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A           VLAN      : none
Audit Sess ID : 0a6401010001c0005ed723b5
Security Grp : none

```

اهحالص او عاطخألا فاشكتس ا

دع اهحالص او عاطخألا فاشكتس ال debug radius و gtest aaa-server رم او امادختس ا اضيأ كنكمي لبقتسملا يف اعويش رثكألا اياضقلالا فصوص متيمث .لكاشم ثودح.

1 لمعلا مدع ويرانيس

نارتقا نم ققحتلا بجي .ضفرب دري ISE ناكو AnyConnect ىلع ٽقداصملالا تلشف اذا ىلإ لقتنا .ةحيحص ريع رورملالا ٽملك نأ وأ مدخلتسملالا ٽيوه ٽعومجممب مدخلتسملالا لياتفتلالا > ٽرشابملالا تالجسلا>تاي لمعلالا.

```

<#root>

RADIUS packet decode (response)

-----
Raw packet data (length = 20).....
03 21 00 14 dd 74 bb 43 8f 0a 40 fe d8 92 de 7a    | .!...t.C..@....z
27 66 15 be                                         | 'f..

Parsed packet data.....
Radius: Code = 3 (0x03)
Radius: Identifier = 33 (0x21)
Radius: Length = 20 (0x0014)
Radius: Vector: DD74BB438F0A40FED892DE7A276615BE
rad_procpkt:

REJECT

RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000009 id 33
free_rip 0x00007f03b419fb08
radius: send queue empty

ERROR: Authentication Rejected: AAA failure

```

The screenshot shows the ISE interface with two main sections: 'Overview' and 'Steps'.

Overview:

Event	5400 Authentication failed
Username	user1
Endpoint Id	
Endpoint Profile	
Authentication Policy	New Policy Set 1 >> Default
Authorization Policy	New Policy Set 1 >> Default
Authorization Result	DenyAccess

Steps:

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - user1
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - DEVICE.Device Type
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - IdentityGroup.Name
15016	Selected Authorization Profile - DenyAccess
15039	Rejected per authorization profile
11003	Returned RADIUS Access-Reject

Authentication Details:

Source Timestamp	2020-06-02 23:22:53.577
Received Timestamp	2020-06-02 23:22:53.577
Policy Server	iseamy24
Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile

هـنـاـفـ ،ـيـلـاـتـلـاـبـوـ .ـمـدـخـتـسـمـ ةـيـوـهـ ةـعـوـمـجـمـ يـأـبـ user1ـ نـرـتـقـيـ اـلـ ،ـلـاثـمـلـاـ اـذـهـ يـفـ ةـظـحـاـلـمـ ةـدـيـدـجـلـاـ تـاسـاـيـسـلـاـ ةـعـوـمـجـمـ نـمـضـ ةـيـضـارـتـفـالـاـ ضـيـوـفـتـلـاـوـ ةـقـدـاـصـمـلـاـ تـاسـاـيـسـ ذـفـنـيـ جـهـنـ يـفـ AllowedAccessـ ىـلـاـ اـذـهـ لـيـدـعـتـ كـنـكـمـيـ DenyAccessـ .ـعـارـجـإـلـاـ مـادـخـتـسـابـ 1ـ مـدـخـتـسـمـلـاـ ةـيـوـهـ ةـعـوـمـجـمـ دـجـوـتـ اـلـ نـيـذـلـاـ نـيـمـدـخـتـسـمـلـلـ حـامـسـلـلـ يـضـارـتـفـالـاـ لـيـوـخـتـلـاـ .ـقـدـاـصـمـلـاـبـ ةـنـرـتـقـمـلـاـ.

2 لـمـعـلـاـ مـدـعـ وـيـرـانـيـسـ

مـتـيـ،ـيـضـارـتـفـالـاـ لـيـوـخـتـلـاـ جـهـنـ نـاـكـوـ AnyConnectـ وـهـ يـفـ ةـقـدـاـصـمـلـاـ تـلـشـفـ اـذـاـ مـتـيـ،ـيـضـارـتـفـالـاـ لـيـوـخـتـلـاـ PermitAccessـ .ـيـلـاـتـلـاـبـوـ ،ـRADIUSـ ةـبـاجـتـسـاـ يـفـ ةـئـفـلـاـ ةـمـسـ مـيـدـقـتـ مـتـيـ اـلـ ،ـكـلـذـعـمـوـ .ـقـدـاـصـمـلـاـ لـوـبـقـ تـاـيـلـمـعـ :ـهـنـيـوـكـتـ مـتـ يـذـلـاـ رـمـأـلـاـ بـبـسـبـ لـصـتـيـ اـلـوـ DfltGrpPolicyـ يـفـ اـدـوـجـوـمـ مـدـخـتـسـمـلـاـ نـوـكـيـ لـ ةـنـمـاـزـتـمـلـاـ لـوـخـدـلـاـ لـيـجـسـتـ .ـV~P~N~O~

<#root>

```
RADIUS packet decode (response)
```

```
-----  
Raw packet data (length = 174).....  
02 24 00 ae 5f 0f bc b1 65 53 64 71 1a a3 bd 88 | .$._____.eSdq....  
7c fe 44 eb 01 07 75 73 65 72 31 18 43 52 65 61 | l.D...user1.CRea  
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37 | uthSession:0a1f7  
63 35 32 32 39 54 68 33 47 68 6d 44 54 49 35 71 | c5229Th3GhmDTI5q  
37 48 46 45 30 7a 6f 74 65 34 6a 37 50 76 69 4b | 7HFE0zote4j7PvIK  
5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a 6f 19 50 | Z5wqkx1P93B1Jo.P  
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54 | CACS:0a1f7c5229T  
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a | h3GhmDTI5q7HFE0z  
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78 | ote4j7PvIKZ5wqkx  
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32 | 1P93B1Jo:iseamy2  
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37 | 4/379556745/37
```

```

Parsed packet data.....  

Radius: Code = 2 (0x02)  

Radius: Identifier = 36 (0x24)  

Radius: Length = 174 (0x00AE)  

Radius: Vector: 5F0FBCB1655364711AA3BD887CFE44EB  

Radius: Type = 1 (0x01) User-Name  

Radius: Length = 7 (0x07)  

Radius: Value (String) =  

75 73 65 72 31 |  
  

user1  
  

Radius: Type = 24 (0x18) State  

Radius: Length = 67 (0x43)  

Radius: Value (String) =  

52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 | ReauthSession:0a  

31 66 37 63 35 32 32 39 54 68 33 47 68 6d 44 54 | 1f7c5229Th3GhmDT  

49 35 71 37 48 46 45 30 7a 6f 74 65 34 6a 37 50 | I5q7HFE0zote4j7P  

76 69 4b 5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a | viKZ5wqkx1P93B1J  

6f | o  
  

Radius: Type = 25 (0x19) Class  

Radius: Length = 80 (0x50)  

Radius: Value (String) =  

43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54 | CACS:0a1f7c5229T  

68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a | h3GhmDTI5q7HFE0z  

6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78 | ote4j7PviKZ5wqkx  

6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32 | 1P93B1Jo:i_seamy2  

34 2f 33 37 39 35 35 36 37 34 35 2f 33 37 | 4/379556745/37  
  

rad_procpkt: ACCEPT  
  

RADIUS_ACCESS_ACCEPT  
  

: normal termination  

RADIUS_DELETE  

remove_req 0x00007f03b419fb08 session 0x8000000b id 36  

free_rip 0x00007f03b419fb08  

radius: send queue empty  
  

INFO: Authentication Successful  
  

ASAv#
```

امك مدخلت سملـا لـصـتـي ، "1" يـلـا 0 نـمـ لـ ظـنـمـاـزـتـمـلـا لـوـخـدـلـا لـيـجـسـتـ تـاـيـلـمـعـ رـيـيـغـتـ مـتـ اـذـاـ جـاـرـخـإـلـا يـفـ حـضـوـمـ وـهـ:

```

<#root>  
  

ASAv# show vpn-sessiondb anyconnect  
  

Session Type: AnyConnect  
  

Username : user1  

Index : 41  

Assigned IP : 10.100.2.1 Public IP : 10.100.1.3  

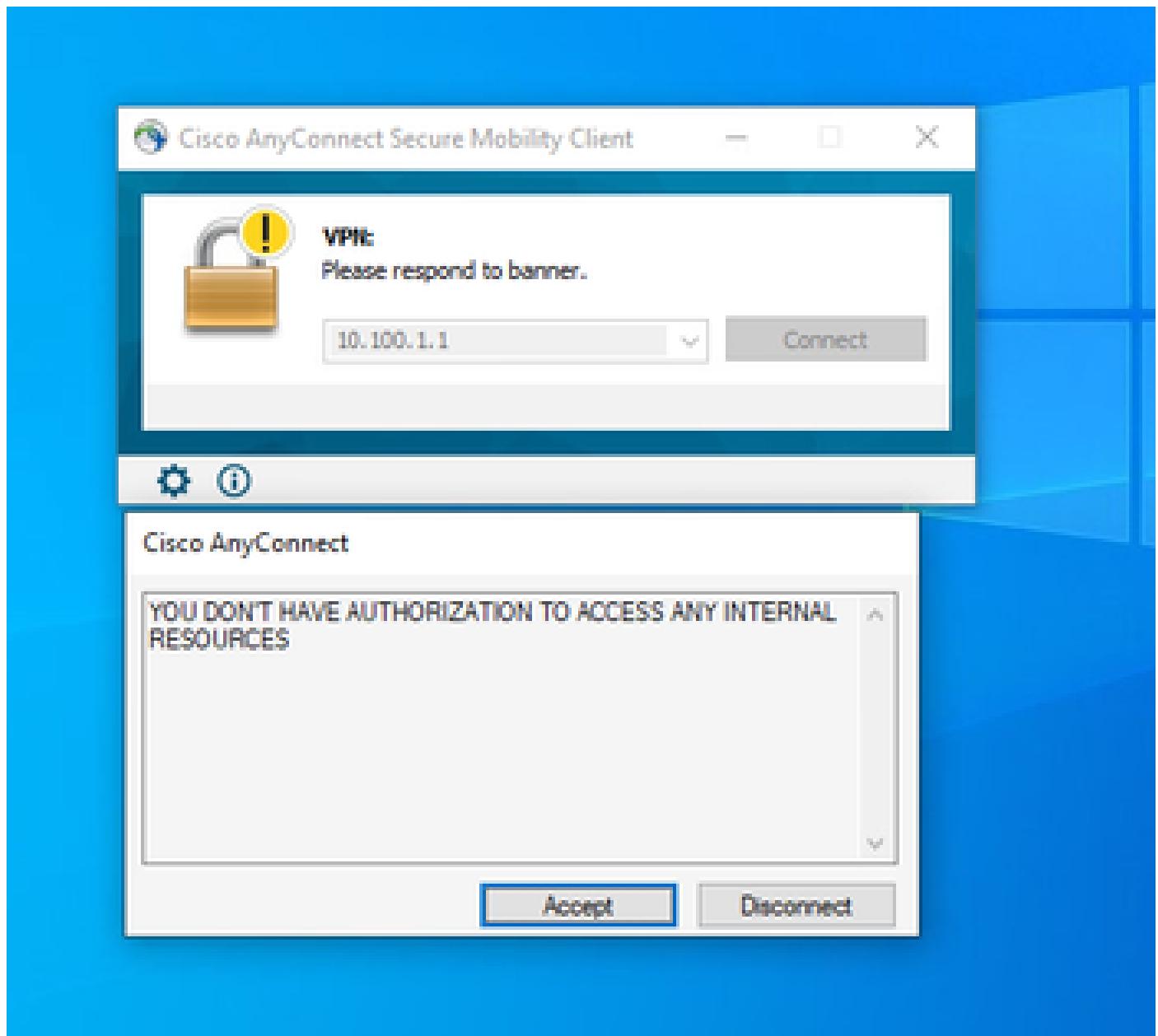
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  

License : AnyConnect Premium  

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256  

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
```

```
Bytes Tx      : 15448          Bytes Rx      : 15528
Group Policy : DfltGrpPolicy    Tunnel Group : DefaultWEBVPNGroup
Login Time   : 18:43:39 UTC Wed Jun 3 2020
Duration     : 0h:01m:40s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A           VLAN       : none
Audit Sess ID : 0a640101000290005ed7ef5b
Security Grp : none
```



3 لمعلا مدع ويرانيس

اذا ، لاثمل ا ليبس ىلع ، وقبطملا ٰ حيحصل ا جهنلا مدخلتسمل ا ىدل نكي مل و وقادصمل ا ترم اذا . بجي امك لماكلا قفنلا نم الدب مسقمل ا قفنلا ىلع يوتحي لصتملا ٰ عومجملا جهن ناك . أطخلا مدخلتسمل ا ٰ يوه ٰ عومجم يف مدخلتسمل ا نوكبي نأ نكمي .

```
<#root>
```

```
ASA# sh vpn-sessiondb anyconnect
```

Session Type: AnyConnect

Username : user1

Index : 29

Assigned IP : 10.100.2.1 Public IP : 10.100.1.3

Protocol : AnyConnect-Parent SSL-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384

Bytes Tx : 15592 Bytes Rx : 0

Group Policy : RADIUS-USERS

Tunnel Group : DefaultWEBVPNGroup

Login Time : 04:36:50 UTC Wed Jun 3 2020

Duration : 0h:00m:20s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audit Sess ID : 0a6401010001d0005ed728e2

Security Grp : none

ويديفل

نیيعدل ئىفل ا ئەمس و ISE ۋىچىتلىك تاوطخىلا ويديفل ا ادھ رفوي
ۋە جۇمۇجىلە.

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).