

Configure RADIUS DTLS on Identity Services Engine

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configurations](#)

- [1. Add network device on ISE and enable DTLS protocol.](#)
- [2. Configure DTLS port and idle timeout.](#)
- [3. Export issuer of DTLS RADIUS certificate from ISE trust store.](#)
- [4. Configure Trust Point and import certificate to authenticator.](#)
- [5. Export certificate of the switch.](#)
- [6. Import switch certificate to ISE Trust Store.](#)
- [7. Configure RADIUS on the switch.](#)
- [8. Configure Policies on ISE.](#)

[Verify](#)

[Troubleshoot](#)

- [1. ISE does not receive any requests.](#)
- [2. DTLS handshake fails.](#)

Introduction

This document describes configuration and troubleshooting of RADIUS over Datagram Transport Layer Security protocol (DTLS). DTLS provides encryption services for RADIUS, which is transported over a secure tunnel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine (ISE)
- RADIUS protocol
- Cisco IOS

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine 2.2
- Catalyst 3650 with IOS 16.6.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Configurations

1. Add network device on ISE and enable DTLS protocol.

Navigate to **Administration > Network Resources > Network Devices**. Click **Add** and provide at least mandatory fields:

- **Name** - A friendly name of the device is added.
- **IP Address** - IP address, which authenticator uses to contact ISE. It is possible to configure a range of devices. In order to do that, specify proper mask (smaller than 32).
- **Device Profile** - General settings for the device. It allows to specify what protocols are handled, detailed Change of Authorization (CoA) settings and Radius attributes configuration. For more details, navigate to **Administration > Network Resources > Network Device Profiles**.
- **Network Device Group** - Set device type, IPSec the capabilities and device location. This setting is not mandatory. If you do not select custom values, default settings are assumed.

Select checkbox **RADIUS Authentication Settings** and under **RADIUS DTLS Settings** select checkbox **DTLS Required**. This allows RADIUS communication with authenticator only via DTLS secure tunnel. Note that **Shared Secret** textbox is grayed out. This value in case of RADIUS DTLS is fixed and the same string is configured on authenticator side.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Manager

Network devices

Default Device

Device Security Settings



Network Devices List > **WLC_3650**

Network Devices

* Name

Description

* IP Address: /

* Device Profile  Cisco 

Model Name

Software Version

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


Network devices


Default Device

Device Security Settings

* Network Device Group

Device Type 

IPSEC 

Location 

☒ **RADIUS Authentication Settings**


RADIUS UDP Settings


Protocol **RADIUS**

* Shared Secret


CoA Port

RADIUS DTLS Settings


DTLS Required ☐ 

Shared Secret 

CoA Port

Issuer CA of ISE Certificates for CoA 

General Settings

Enable KeyWrap ☐ 

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ☒ ASCII ☐ HEXADECIMAL

2. Configure DTLS port and idle timeout.

You can configure the port which is used for DTLS communication and idle timeout at

Administration > System > Settings > Protocols > RADIUS > RADIUS DTLS.

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

Deployment Licensing > Certificates > Logging > Maintenance Upgrade Backup & Restore > Admin Access > **Settings**

Client Provisioning
FIPS Mode
Alarm Settings
Posture
Profiling

Protocols

EAP-FAST

EAP-TLS
PEAP
EAP-TTLS

RADIUS

IPSec
Security Settings
Proxy
SMTP Server
SMS Gateway

Detection Interval: 5 (in minutes)
Reporting Interval: 15 (in minutes)
Reject RADIUS Requests: ☒
Failures prior to Rejection: 5 (valid range 2 to 100)
Request Rejection Interval: 60 (in minutes)

Suppress Repeated Successful Authentications: ☐
Accounting Suppression Interval: 5 (in seconds)
Long Processing Step Threshold Interval: 1,000 (in milliseconds)

Radius UDP ports

*Authentication Ports: 1812,1645
*Accounting Ports: 1813,1646

Radius DTLS

*Authentication & Accounting Ports: 2083
Idle Timeout: 60 (in second, valid range 60 to 600)

Save Reset Reset To Defaults

Note that DTLS port is different from RADIUS ports. By default, a RADIUS uses pairs 1645, 1646 and 1812, 1813. By default DTLS for authentication, authorization, accounting and CoA uses port 2083. **Idle Timeout** specifies how long ISE and authenticator maintain tunnel without any actual communication going through it. This timeout is measured in seconds and ranges from 60 to 600 seconds.

3. Export issuer of DTLS RADIUS certificate from ISE trust store.

In order to establish the tunnel between ISE and authenticator, both entities need to exchange and verify certificates. Authenticator has to trust ISE RADIUS DTLS certificate, which means that its issuer has to be present in authenticator's Trust Store. In order to export signer of ISE certificate, navigate to **Administration > System > Certificates**, as shown in the image:

System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Click here to do wireless setup and visibility setup Do not show this again.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
<input type="checkbox"/>	ISE22-1ek.example.com#Certificate Services Endpoint Sub CA - ISE22-1ek#00001	pxGrid		ISE22-1ek.example.com	Certificate Services Endpoint Sub CA - ISE22-1ek	Wed, 19 Oct 2016	Wed, 20 Oct 2021	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ISE22-1ek.example.com, ISE22-1ek.example.com, ISE22-1ek.example.com#LAB CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	ISE22-1ek.example.com	LAB CA	Mon, 31 Oct 2016	Wed, 31 Oct 2018	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_ISE22-1ek.example.com	SAML		SAML_ISE22-1ek.example.com	SAML_ISE22-1ek.example.com	Thu, 20 Oct 2016	Fri, 20 Oct 2017	<input checked="" type="checkbox"/>

Locate certificate with RADIUS DTLS role assigned and check **Issued By** field for this certificate. This is the Common Name of certificate that has to be exported from ISE Trust Store. In order to

do that, navigate to **Administration > System > Certificates Trusted Certificates**. Select checkbox next to the appropriate certificate and click **Export**.

4. Configure Trust Point and import certificate to authenticator.

In order to configure trustpoint, log in to the switch and execute commands:

```
configure terminal
crypto pki trustpoint isetp
enrollment terminal
revocation-check none
exit
```

Import certificate with command **crypto pki authenticate isetp**. When prompted to accept certificate, type **yes**.

```
Switch3650(config)#crypto pki authenticate isetp
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIDWTCCAkgAwIBAgIQI9s4RrhtWlpJjBYB5v0dtTANBgkqhkiG9w0BAQUFADA/
MRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYKCZImiZPyLGBGRYHZXhhbXBsZTEP
MA0GA1UEAxMGTEFCIENBMB4XDTE1MDIxMjA3MzgxM1oXDTI1MDIxMjA3NDgxMlow
PzETMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2V4YW1wbGUx
DzANBgNVBAMTBkxvBQIDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMDSfJwvbjLHHJf4vDTalGjKrDI73c/y269IMZV48xpCruNhglcU8CW/T9Ysj6xk
Oogtx2vpG4XJt7KebDZ/ac1Ymjg7sPBpcnyDZCd2a1b39XakD2puE8lVi4RVkjBH
pss2fTWeuor9dzgb/kWb0YqIsgwlsRKQ2Veh1IXmuhX+wDqELHPIzgXn/DOBF0qN
vWlevrAlmBTx04t1aPwyRk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wg
HDvd6C6LKRbpmAvtrqyDtinEl/CRAEFH7dZpvUSJBNUh7st3JIG8gVFstweoMmTE
zxUONQw8QrZmXDGTKgqvisECAwEAAANRME8wCwYDVR0PBAQDAGGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEF00TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQB
gjcVAQQDAGEAMA0GCSqGSIb3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVi
xhn7KrEyWxLkWaLsbU2ixsfTeJDCM8pxQItsj6B0Ey6A05c3YNcvW1iNpupGgc7v
9lMt4/TB6aRLVLijBPB9/p2/3SJadCe/YBaOn/vpmfBPPhxUQVPiBM9fy/Al+zsh
t66bc03WcD8ZaKaER0oT8Pt/4GHZA0Unx+UxpcNuRRz4COArINXE0ULRfBxpIkkF
pWNjH0r1V55edOga0/r60Cg1/J9VAHh3qK2/3zXJE53N+A0h9whpG4LYgIFLB9ep
ZDim7KGsf+P3zk7SsKioGB4kqidHnm34XjlkWFnrCMQH4HC1oEymakV3Kq24
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: B33EAD49 87F18924 590616B9 C8880D9D

Fingerprint SHA1: FD729A3B B533726F F8450358 A2F7EB27 EC8A1178

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

5. Export certificate of the switch.

Select trustpoint and certificate to be used for DTLS on the switch and export it:

```
Switch3650(config)#crypto pki export TP-self-signed-721943660 pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIICKTCAZKgAwIBAgIBATANBgkqhkiG9w0BAQUFADAwMS4wLAYDVQQDEyVJT1Mt
U2VsZi1TaWduZWQtQ2VydGlmZWVhdGUtNzIxOTQzNjYwMB4XDTE1MDIxMjA3MzgxM1oXDTI1MDIxMjA3NDgxMlow
PzETMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2V4YW1wbGUx
DzANBgNVBAMTBkxvBQIDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMDSfJwvbjLHHJf4vDTalGjKrDI73c/y269IMZV48xpCruNhglcU8CW/T9Ysj6xk
Oogtx2vpG4XJt7KebDZ/ac1Ymjg7sPBpcnyDZCd2a1b39XakD2puE8lVi4RVkjBH
pss2fTWeuor9dzgb/kWb0YqIsgwlsRKQ2Veh1IXmuhX+wDqELHPIzgXn/DOBF0qN
vWlevrAlmBTx04t1aPwyRk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wg
HDvd6C6LKRbpmAvtrqyDtinEl/CRAEFH7dZpvUSJBNUh7st3JIG8gVFstweoMmTE
zxUONQw8QrZmXDGTKgqvisECAwEAAANRME8wCwYDVR0PBAQDAGGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEF00TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQB
gjcVAQQDAGEAMA0GCSqGSIb3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVi
xhn7KrEyWxLkWaLsbU2ixsfTeJDCM8pxQItsj6B0Ey6A05c3YNcvW1iNpupGgc7v
9lMt4/TB6aRLVLijBPB9/p2/3SJadCe/YBaOn/vpmfBPPhxUQVPiBM9fy/Al+zsh
t66bc03WcD8ZaKaER0oT8Pt/4GHZA0Unx+UxpcNuRRz4COArINXE0ULRfBxpIkkF
pWNjH0r1V55edOga0/r60Cg1/J9VAHh3qK2/3zXJE53N+A0h9whpG4LYgIFLB9ep
ZDim7KGsf+P3zk7SsKioGB4kqidHnm34XjlkWFnrCMQH4HC1oEymakV3Kq24
-----END CERTIFICATE-----
```

```
xRybTGD526rPYuD2puMJU8ANcDqQnwunIERgvIWOLwBovuAu7WcRmzw1IDTDryOH
Pxt1n5GcQSAOgn+9QdvKl1Z43ZkRWK5E7EGmjM/aL1287mg4/NlrWr4KMSwDQBJI
noJ5S2CABXUoApuiiJ8Ya4gOYeP0TmsZtxP1N+s+wqjMCAwEAAaNTMFewDwYDVR0T
AQH/BAUwAwEB/zAfBgNVHSMEGDAWgBSEOKlAPAHBPedwichXL+qUM+1riTAdBgNV
HQ4EFgQUhDipQDwBwT3ncInIVy/q1DPta4kwDQYJKoZIhvcNAQEFBQADgYEA1BNN
wKSS8yBuOH0/jUV7sy3Y9/oV7Z9bW8WfV9QiTQ11ZelvWMTbewozwX2LJvxobGcj
Pi+n99RIH8dBhWwoYl9GTN2LVI22GIPX12jNLqps+Mq/u2qxVm0964Sajs50lKjQ
69XFfCVot1NA6z2eEP/69oL9x0uaJDZa+6ileh0=
-----END CERTIFICATE-----
```

In order to list all trustpoints configured, execute command **show crypto pki trustpoints**. Once the certificate is printed to console, copy it to a file and save on your PC.

6. Import switch certificate to ISE Trust Store.

On ISE, navigate to **Administration > Certificates > Trusted Certificates** and click **Import**.

Now click **Browse** and select certificate of the switch. Provide (optionally) Friendly Name and select checkboxes **Trust for authentication within ISE** and **Trust for client authentication and Syslog**. Then click **Submit**, as shown in the image:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' tab is selected, and the left sidebar shows 'Certificate Management' with options like 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Setti...'. The main content area is titled 'Import a new Certificate into the Certificate Store'. It contains the following fields and options:

- * Certificate File: A 'Browse...' button followed by the text 'sw.pem'.
- Friendly Name: A text input field containing 'Switch3650'.
- Trusted For: A section with three checkboxes:
 - ☒ Trust for authentication within ISE
 - ☒ Trust for client authentication and Syslog
 - ☐ Trust for authentication of Cisco Services
- ☐ Validate Certificate Extensions
- Description: An empty text input field.
- Buttons: 'Submit' and 'Cancel' buttons at the bottom.

7. Configure RADIUS on the switch.

Add RADIUS configuration on the switch. In order to configure the switch to communicate with ISE over DTLS, use commands:

```
radius server ISE22
address ipv4 10.48.23.86
key radius/dtls
dtls port 2083
dtls trustpoint client TP-self-signed-721943660
dtls trustpoint server isetp
```

Rest of AAA specific configuration depends on your requirements and design. Treat this configuration as an example:

```

aaa group server radius ISE
  server name ISE22

radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include

aaa authentication dot1x default group ISE
aaa authorization network default group ISE

```

8. Configure Policies on ISE.

Configure authentication and authorization policies on ISE. This step depends on your design and requirements as well.

Verify

In order to verify that users can authenticate, use **test aaa** command on the switch:

```

Switch3650#test aaa group ISE alice Krakow123 new-code
User successfully authenticated

```

USER ATTRIBUTES

```

username          0    "alice"
Switch3650#

```

You should see message **User successfully authenticated**. Navigate to **ISE Operations > RADIUS > LiveLog** and select details for appropriate log (Click on magnifying glass):

The screenshot displays the Cisco Identity Services Engine (ISE) Operations page. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled 'RADIUS' and shows a summary of RADIUS statistics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (42), and Client Stopped Responding (0). Below this summary is a table of live logs with columns for Time, Status, Details, Repeat, Identity, and Endpoint ID. A single log entry is visible for 'alice' with a status of 'Success' and a timestamp of 'Jan 25, 2017 07:55:49.801 PM'.

Time	Status	Details	Repeat	Identity	Endpoint ID
Jan 25, 2017 07:55:49.801 PM	Success			alice	00:50:56:A5:13:0D

Overview

Event	5200 Authentication succeeded
Username	alice
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2017-01-25 18:19:24.672
Received Timestamp	2017-01-25 18:19:24.673
Policy Server	ISE22-1ek
Event	5200 Authentication succeeded
Username	alice
User Type	User
Authentication Identity Store	Internal Users

Steps

91055	RADIUS packet is encrypted
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 - Normalised Radius.RadiusFlowType (4 times)
15006	Matched Default Rule
15041	Evaluating Identity Policy
15006	Matched Default Rule
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - alice
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - DEVICE.IPSEC
15048	Queried PIP - Threat.Rapid7 Nexpose-CVSS_Base_Score
15048	Queried PIP - Network Access.UseCase
15048	Queried PIP - Normalised Radius.RadiusFlowType (2 times)
15048	Queried PIP - Network Access.AuthenticationStatus
15004	Matched rule - Basic_Authenticated_Access
15016	Selected Authorization Profile - PermitAccess
22080	New accounting session created in Session cache
11002	Returned RADIUS Access-Accept

On the right side of the report, there is a list of **Steps**. Check that first step in the list is **RADIUS packet is encrypted**.

Additionally, you can start packet capture on ISE and execute **test aaa** command one more time. In order to start capture, navigate to **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**. Select Policy Service Node used for authentication and click **Start**:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Diagnostic Tools Download Logs

General Tools

- RADIUS Authentication Trouble...
- Execute Network Device Comm...
- Evaluate Configuration Validator
- Posture Troubleshooting
- EndPoint Debug
- TCP Dump
- Session Trace Test Cases

TrustSec Tools

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status ■ Stopped Start

Host Name

Network Interface

Promiscuous Mode ☒ On ☐ Off

Filter

Example: 'ip host helios and not iceberg'

Format

Dump File Last created on Wed Jan 25 18:25:43 CET 2017
 File size: 212,627 bytes
 Format: Raw Packet Data
 Host Name: ISE22-1ek
 Network Interface: GigabitEthernet 0
 Promiscuous Mode: On

Download Delete

When authentication is finished, click **Stop** and **Download**. When you open packet capture, you should be able to see traffic encrypted with DTLS:

813	2017-01-25	18:19:20.699601	10.229.20.241	10.48.23.86	DTLSv1.2	180 Client Hello
815	2017-01-25	18:19:20.702006	10.48.23.86	10.229.20.241	DTLSv1.2	1311 Server Hello, Certificate (Fragment), Certificate (...)
816	2017-01-25	18:19:20.750400	10.229.20.241	10.48.23.86	DTLSv1.2	270 Certificate (Fragment)
817	2017-01-25	18:19:20.750604	10.229.20.241	10.48.23.86	DTLSv1.2	270 Certificate (Fragment)
818	2017-01-25	18:19:20.755830	10.229.20.241	10.48.23.86	DTLSv1.2	270 Certificate (Reassembled), Client Key Exchange (Fra...
819	2017-01-25	18:19:20.756049	10.229.20.241	10.48.23.86	DTLSv1.2	270 Client Key Exchange (Fragment)
820	2017-01-25	18:19:20.777474	10.229.20.241	10.48.23.86	DTLSv1.2	258 Client Key Exchange (Reassembled), Certificate Veri...
821	2017-01-25	18:19:20.779217	10.229.20.241	10.48.23.86	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
822	2017-01-25	18:19:20.794575	10.48.23.86	10.229.20.241	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
823	2017-01-25	18:19:20.830404	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data
824	2017-01-25	18:19:20.880231	10.48.23.86	10.229.20.241	DTLSv1.2	279 Application Data
832	2017-01-25	18:19:23.646428	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data
833	2017-01-25	18:19:23.693076	10.48.23.86	10.229.20.241	DTLSv1.2	279 Application Data
834	2017-01-25	18:19:24.622672	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data
835	2017-01-25	18:19:24.674113	10.48.23.86	10.229.20.241	DTLSv1.2	279 Application Data

Packets #813 - #822 are part of DTLS handshake. When the handshake is successfully negotiated, Application Data is transferred. Note that number of packets may vary and depends for example on the authentication method used (PAP, EAP-PEAP, EAP-TLS, etc). Contents of each packet are encrypted:

822	2017-01-25	18:19:20.794575	10.48.23.86	10.229.20.241	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
823	2017-01-25	18:19:20.830404	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data

▶ Frame 823: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
 ▶ Ethernet II, Src: CiscoInc_1c:e8:00 (00:07:4f:1c:e8:00), Dst: Vmware_99:64:0c (00:50:56:99:64:0c)
 ▶ Internet Protocol Version 4, Src: 10.229.20.241, Dst: 10.48.23.86
 ▶ User Datagram Protocol, Src Port: 51598 (51598), Dst Port: 2083 (2083)
 ▼ Datagram Transport Layer Security
 ▼ DTLSv1.2 Record Layer: Application Data Protocol: Application Data
 Content Type: Application Data (23)
 Version: DTLS 1.2 (0xfe)
 Epoch: 1
 Sequence Number: 1
 Length: 96
 Encrypted Application Data: 8d83ddac8b027b5a5f9e355243b0f9155680d2a933c09635...

When all data is transmitted, the tunnel is not torn down immediately. **IdleTimeout** configured on ISE determines how long tunnel can be established without communication going through it. If the timer expires and new Access-Request has to be sent to ISE, DTLS handshake is performed and

the tunnel is rebuilt.

Troubleshoot

1. ISE does not receive any requests.

Note that default DTLS port is 2083. Default RADIUS ports are 1645,1646 and 1812,1813. Ensure that firewall does not block UDP/2083 traffic.

2. DTLS handshake fails.

In the detailed report on ISE you may see that DTLS handshake failed:

Overview

Event	5450 RADIUS DTLS handshake failed
Username	
Endpoint Id	
Endpoint Profile	
Authorization Result	

Steps

91030	RADIUS DTLS handshake started
91031	RADIUS DTLS: received client hello message
91032	RADIUS DTLS: sent server hello message
91033	RADIUS DTLS: sent server certificate
91034	RADIUS DTLS: sent client certificate request
91035	RADIUS DTLS: sent server done message
91036	RADIUS DTLS: received client certificate

Authentication Details

Source Timestamp	2017-01-25 16:15:36.092
Received Timestamp	2017-01-25 16:15:36.094
Policy Server	ISE22-1ek
Event	5450 RADIUS DTLS handshake failed
NAS IPv4 Address	10.229.20.241

Possible reason is that either switch or ISE does not trust certificate sent during the handshake. Verify certificate configuration. Verify that proper certificate is assigned to RADIUS DTLS role on ISE and to trustpoints on the switch.