

在身份服務引擎上配置RADIUS DTLS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[組態](#)

- [1.在ISE上新增網路裝置並啟用DTLS協定。](#)
- [2.配置DTLS埠和空間超時。](#)
- [3.從ISE信任儲存匯出DTLS RADIUS證書的頒發者。](#)
- [4.配置信任點並將證書匯入到驗證器。](#)
- [5.匯出交換機的證書。](#)
- [6.將交換機證書匯入到ISE信任儲存。](#)
- [7.在交換機上配置RADIUS。](#)
- [8.在ISE上配置策略。](#)

[驗證](#)

[疑難排解](#)

- [1. ISE未收到任何請求。](#)
- [2. DTLS握手失敗。](#)

簡介

本檔案介紹透過資料包傳輸層安全通訊協定(DTLS)的RADIUS組態和疑難排解。DTLS為RADIUS提供加密服務，該服務通過安全隧道傳輸。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身分識別服務引擎(ISE)
- RADIUS通訊協定
- Cisco IOS

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎2.2

- 採用IOS 16.6.1的Catalyst 3650

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

組態

1.在ISE上新增網路裝置並啟用DTLS協定。

導覽至Administration > Network Resources > Network Devices。按一下「Add」，並至少提供必填欄位：

- **Name** — 新增裝置的友好名稱。
- **IP地址** — 身份驗證器用於聯絡ISE的IP地址。可以配置一系列裝置。為此，請指定正確的掩碼（小於32）。
- **Device Profile** — 裝置的常規設定。它允許指定處理哪些協定、詳細授權更改(CoA)設定和Radius屬性配置。有關詳細資訊，請導航到**管理>網路資源>網路裝置配置檔案**。
- **網路裝置組** — 設定裝置型別、IPSec功能和裝置位置。此設定不是必需的。如果不選擇自定義值，則採用預設設定。

選中**RADIUS Authentication Settings**覈取方塊，然後在**RADIUS DTLS Settings**下選中**DTLS Required**覈取方塊。這僅允許通過DTLS安全隧道與身份驗證器進行RADIUS通訊。請注意，**Shared Secret**文本框呈灰色顯示。如果是RADIUS DTLS，則此值是固定的，並且身份驗證器端配置了相同的字串。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is Administration > Network Resources > Network Devices. The page title is 'Network Devices List > WLC_3650'. The main heading is 'Network Devices'. The form contains the following fields:

- * Name:
- Description:
- * IP Address: /
- * Device Profile: (with a plus icon for adding more)
- 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 All Device Types Set To Default

IPSEC No Set To Default

Location All Locations Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

CoA Port 2083 Set To Default

Issuer CA of ISE Certificates for CoA Select if required (optional)

General Settings

Enable KeyWrap

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

2. 配置DTLS埠和空閒超時。

您可以在**管理>系統>設定>協定>RADIUS > RADIUS DTLS**處配置用於DTLS通訊和空閒超時的埠。

請注意，DTLS埠與RADIUS埠不同。預設情況下，RADIUS使用對1645、1646和1812、1813。預設情況下，身份驗證、授權、記賬和CoA的DTLS使用埠2083。**Idle Timeout**指定ISE和身份驗證器在不通過任何實際通訊的情況下維護隧道的時間。此超時以秒為測量單位，範圍為60到600秒。

3. 從ISE信任儲存匯出DTLS RADIUS證書的頒發者。

為了建立ISE和身份驗證器之間的隧道，兩個實體都需要交換和驗證證書。身份驗證器必須信任ISE RADIUS DTLS證書，這意味著其頒發者必須存在於身份驗證器的信任儲存中。若要匯出ISE證書的簽名者，請導航到**Administration > System > Certificates**，如下圖所示：

找到分配了RADIUS DTLS角色的證書，並檢查此證書的**Issued By**欄位。這是必須從ISE信任儲存匯出的證書的公用名稱。為此，請導航到**管理>系統>證書受信任的證書**。選中相應證書旁邊的覈取方塊，然後點選匯出。

4. 配置信任點並將證書匯入到驗證器。

要配置信任點，請登入交換機並執行命令：

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

使用命令 `crypto pki authenticate isetp` 匯入證書。當系統提示接受證書時，鍵入 `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-----
MIIDWTCCAkGgAwIBAgIQL9s4RrhtWlpJjBYB5v0dtTANBgkqhkiG9w0BAQUFADA/
MRMwEQYKCZImiZPyLQBGRYDY29tMRcwFQYKCZImiZPyLQBGRYHZXhhbXBsZTEP
MA0GA1UEAxMGTEFCIENBMB4XDTE1MDIxMjA3MzgxM1oXDTE1MDIxMjA3NDgxM1ow
PzETMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2V4YW1wbGUx
DzANBgNVBAMTBkxkYjBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMDSfJwvbjLHHJf4vDTalGjKrDI73c/y269IMZV48xpCruNhglcU8CW/T9Ysj6xk
Oogtx2vpG4XJt7KebDZ/ac1Ymjg7sPBPCnyDZCd2a1b39XakD2puE81Vi4RVkjBH
pss2fTWeuor9dzb/kWb0YqIsgwlsRKQ2Veh1IXmuhX+wDqELHPizgXn/DOBF0qN
vWlevrAlmBTxC04t1aPwyRk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wg
HDvd6C6LKRbpmAvtrqyDtine1/CRAEFH7dZpvUSJBNUh7st3JIG8gVFstweoMmTE
zxUONQw8QrZmXDGTkGqvisECAwEAAANRME8wCwYDVR0PBAQDAGGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEF00TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQB
gjcVAQQDAGEAMA0GCSqGSIb3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVi
xhn7KrEyWxLkWaLsbU2ixsfTeJDCM8pxQIItsj6B0Ey6A05c3YNcvW1iNpupGgc7v
9lMt4/TB6arLVLiJBp9/p2/3SjadCe/YBaOn/vpmfBPPPhUQVPiBM9fy/Al+zsh
t66bc03WcD8ZaKaER0t8Pt/4GHZA0Unx+UxpcNuRRz4COArINXE0ULRfBxpIkkF
pWNjh0rlV55edOga0/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. 匯出交換機的證書。

選擇交換機上要用於DTLS的信任點和證書並匯出它：

```
Switch3650(config)#crypto pki export TP-self-signed-721943660 pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIICKTCCAZKgAwIBAgIBATANBgkqhkiG9w0BAQUFADAwMS4wLAYDVQQDEyVJT1Mt
U2VsZi1TaWduZWQ2Q2VydGlnaWNoZGUtNzIxOTQzNjYwMjA3NDTE2MDQyNzExNDYw
Nl0XDTE1MDIxMjA3MzgxM1oXDTE1MDIxMjA3NDgxM1owPzETMBEGCgmSJomT8ixk
ARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2V4YW1wbGUx DzANBgNVBAMTBkxkYjBD
QTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMDSfJwvbjLHHJf4vDTal
GjKrDI73c/y269IMZV48xpCruNhglcU8CW/T9Ysj6xkOogtx2vpG4XJt7KebDZ/ac
1Ymjg7sPBPCnyDZCd2a1b39XakD2puE81Vi4RVkjBH pss2fTWeuor9dzb/kWb0Y
qIsgwlsRKQ2Veh1IXmuhX+wDqELHPizgXn/DOBF0qNvWlevrAlmBTxC04t1aPwy
Rk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wgHDvd6C6LKRbpmAvtrqyDt
ine1/CRAEFH7dZpvUSJBNUh7st3JIG8gVFstweoMmTEzxUONQw8QrZmXDGTkGqvis
ECAwEAAANRME8wCwYDVR0PBAQDAGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBB
YEF00TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQBgjcVAQQDAGEAMA0GCSqGSI
b3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVixhn7KrEyWxLkWaLsbU2ixsf
TeJDCM8pxQIItsj6B0Ey6A05c3YNcvW1iNpupGgc7v9lMt4/TB6arLVLiJBp9/p2
/3SjadCe/YBaOn/vpmfBPPPhUQVPiBM9fy/Al+zsh t66bc03WcD8ZaKaER0t8Pt
/4GHZA0Unx+UxpcNuRRz4COArINXE0ULRfBxpIkkFpWNjh0rlV55edOga0/r60Cg
1/J9VAHh3qK2/3zXJE53N+A0h9whpG4LYgIFLB9epZDim7KGsf+P3zk7SsKioGB4
kqidHnm34XjlkWFnrCMQH4HC1oEymakV3Kq24
```

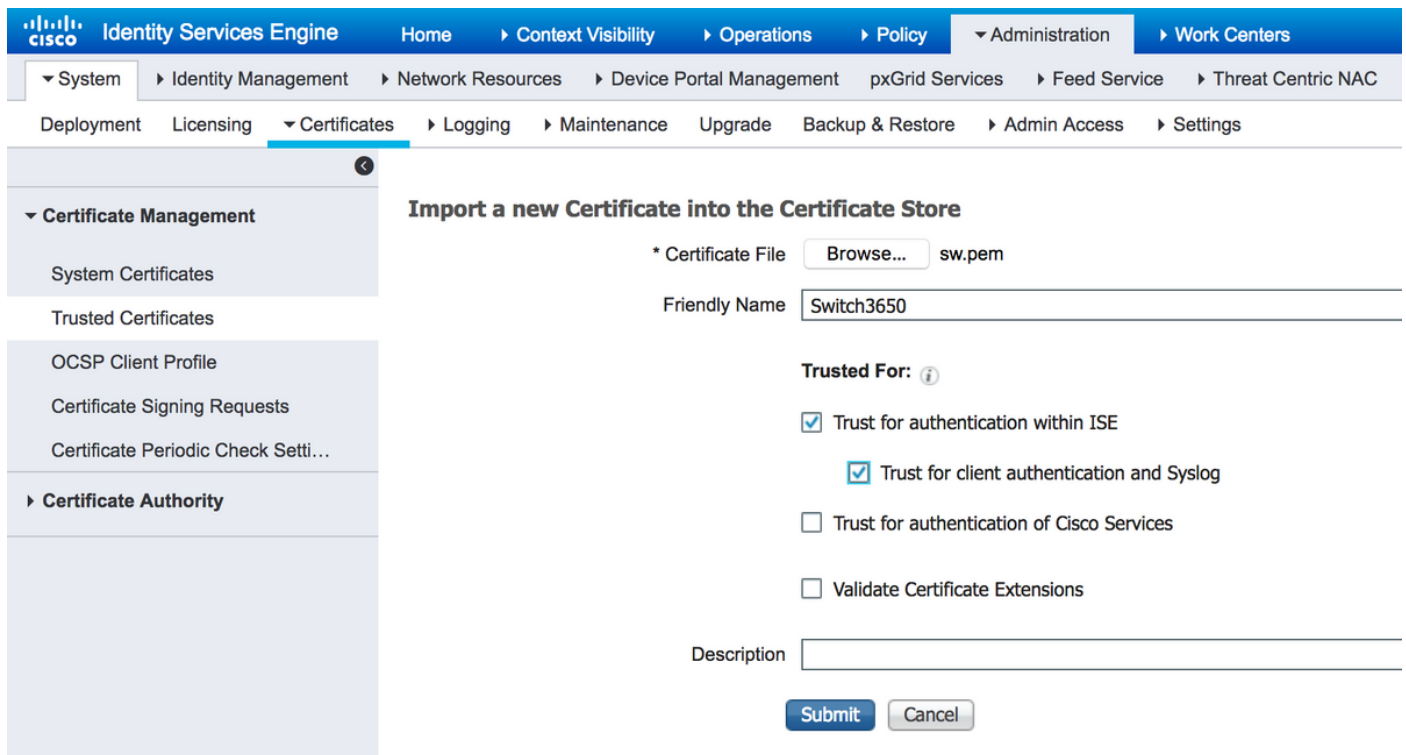
```
wKSS8yBuOH0/jUV7sy3Y9/oV7Z9bW8WfV9QiTQ11ZelVWMTbewozwX2LJvxobGcj
Pi+n99RIH8dBhWwoY19GTN2LVI22GIPX12jNLqps+Mq/u2qxVm0964Sajs501KjQ
69XFfCVot1NA6z2eEP/69oL9x0uaJDZa+6ileh0=
-----END CERTIFICATE-----
```

若要列出所有已配置的信任點，請執行命令 `show crypto pki trustpoints`。將證書列印到控制檯後，將其複製到檔案並儲存到PC上。

6. 將交換機證書匯入到ISE信任儲存。

在ISE上，導航到 **Administration > Certificates > Trusted Certificates**，然後點選 **Import**。

現在，按一下「**Browse**」，然後選擇交換器的憑證。提供（可選）友好名稱並選擇覈取方塊 **Trust for authentication within ISE** 和 **Trust for client authentication and Syslog**。然後按一下「**Submit**」，如下圖所示：



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > Certificates > Trusted Certificates**. The main content area is titled "Import a new Certificate into the Certificate Store". The form includes the following fields and options:

- * Certificate File:** A "Browse..." button next to the text "sw.pem".
- Friendly Name:** A text input field containing "Switch3650".
- Trusted For:** A section with an information icon (i) and 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. 在交換機上配置RADIUS。

在交換機上新增RADIUS配置。要將交換機配置為通過DTLS與ISE通訊，請使用命令：

```
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
```

其餘的AAA特定配置取決於您的要求和設計。請將此組態視為範例：

```
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.在ISE上配置策略。

在ISE上配置身份驗證和授權策略。此步驟也取決於您的設計和要求。

驗證

若要驗證使用者是否可進行驗證，請在交換器上使用**test aaa**指令：

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

USER ATTRIBUTES

```
username 0 "alice"  
Switch3650#
```

您應該會看到消息**User successfully authenticated**。導航到**ISE Operations > RADIUS > LiveLog**，然後選擇相應日誌的詳細資訊（按一下放大鏡）：

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'RADIUS' section is active, showing 'Live Logs' and 'Live Sessions'. Below the navigation bar, there are four summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (42), and 'Client Stopped Responding' (0). A 'Refresh' button is set to 'Every 1 minute'. Below the summary cards, there are options for 'Refresh', 'Reset Repeat Counts', and 'Export To'. The main content area is a table with the following columns: Time, Status, Details, Repeat, Identity, and Endpoint ID. A single log entry is visible for 'alice' with a status of 'Success' and endpoint ID '00:50:56:A5:13:0D'.

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

在報告的右側，有一個步驟列表。檢查清單中的第一個步驟是RADIUS封包已加密。

此外，您可以在ISE上啟動資料包捕獲，並再次執行test aaa 命令。若要開始捕獲，請導航到操作 >故障排除>診斷工具>常規工具> TCP轉儲。選擇用於身份驗證的策略服務節點，然後按一下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

驗證完成後，按一下「Stop」和「Download」。開啟資料包捕獲時，您應該能夠看到使用DTLS加密的流量：

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	18:19:20.750480	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是DTLS握手的一部分。成功協商握手後，將傳輸應用程式資料。請注意，資料包數量可能有所不同，具體取決於使用的身份驗證方法 (PAP、EAP-PEAP、EAP-TLS等)。每個封包的內容均經過加密：

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 (0xfefd)
    Epoch: 1
    Sequence Number: 1
    Length: 96
    Encrypted Application Data: 8d83ddac8b027b5a5f9e355243b0f9155680d2a933c09635...
```

傳輸所有資料時，不會立即關閉隧道。在ISE上配置的IdleTimeout確定可以建立隧道多長時間而不通過它。如果計時器到期且必須將新的訪問請求傳送到ISE，則會執行DTLS握手並重建隧道。

疑難排解

1. ISE未收到任何請求。

請注意，預設DTLS埠為2083。預設RADIUS埠為1645、1646和1812、1813。確保防火牆不會阻止UDP/2083流量。

2. DTLS握手失敗。

在ISE的詳細報告中，您可能會看到DTLS握手失敗：

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

可能的原因是，交換機或ISE不信任在握手期間傳送的證書。驗證證書配置。驗證是否為ISE上的RADIUS DTLS角色和交換機上的信任點分配了正確的證書。