

RADIUS-DTLS configureren op Identity Services Engine

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties](#)

- [1. Voeg netwerkapparaat toe op ISE en schakel het DTLS-protocol in.](#)
- [2. Configuratie van DTLS poort en ongebruikte tijdslimiet.](#)
- [3. Exportemittent van het DTLS RADIUS-certificaat bij ISE-trustwinkel.](#)
- [4. Het vertrouwenspunt configureren en het invoercertificaat ter authenticatie instellen.](#)
- [5. Exportcertificaat van de schakelaar.](#)
- [6. Importeer switch certificaat aan ISE Trust Store.](#)
- [7. Configureer de RADIUS op de schakelaar.](#)
- [8. Het beleid op ISE configureren.](#)

[Verifiëren](#)

[Problemen oplossen](#)

- [1. ISE ontvangt geen verzoeken.](#)
- [2. DTLS-handdruk mislukt.](#)

Inleiding

Dit document beschrijft de configuratie en probleemoplossing van RADIUS via Datagram Transport Layer Security Protocol (DTLS). DTLS biedt encryptiediensten voor RADIUS, dat over een beveiligde tunnel wordt getransporteerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Configuraties

1. Voeg netwerkapparaat toe op ISE en schakel het DTLS-protocol in.

Navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**. Klik op **Toevoegen** en geef ten minste de verplichte velden op:

- **Naam** - Er wordt een gebruiksvriendelijke naam van het apparaat toegevoegd.
- **IP Address** - IP Address, waarvan authenticator gebruik maakt om contact op ISE op te nemen. Het is mogelijk om een reeks apparaten te configureren. Specificeer daartoe een goed masker (kleiner dan 32).
- **Apparaatprofiel** - Algemene instellingen voor het apparaat. Het stelt in staat te specificeren welke protocollen worden verwerkt, welke wijzigingen van de CoA-instellingen (Authorization) en de configuratie van de Radius-kenmerken worden aangebracht. Voor meer informatie, navigeer naar **Beheer > Netwerkbronnen > Netwerkprofielen**.
- **Network Devices Group** - Stel een apparaattype in, IPSec de functies en de locatie van het apparaat. Deze instelling is niet verplicht. Als u geen aangepaste waarden selecteert, worden de standaardinstellingen verondersteld.

Selecteer **RADIUS-verificatie-instellingen** en selecteer **DTLS-instellingen van RADIUS** en **DTLS verplicht**. Dit maakt RADIUS-communicatie met authenticator alleen mogelijk via DTLS beveiligde tunnel. Merk op dat het **gedeelde geheime** tekstvak gegraveerd is. Deze waarde in het geval van RADIUS DTLS is vastgelegd en de zelfde string is ingesteld aan de kant van de authenticator.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

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

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. Configuratie van DTLS poort en ongebruikte tijdslimiet.

U kunt de poort configureren die wordt gebruikt voor communicatie met het DTLS-netwerk en

tijdelijke uitvoer bij **Beheer > Systeem > Instellingen > Protocollen > RADIUS > RADIUS-TLS**.

The screenshot shows the RADIUS-TLS configuration page in the Cisco ISE Administration console. The left sidebar contains navigation options like Client Provisioning, Posture, Protocols, and Security Settings. The main content area is divided into sections for RADIUS and DTLS settings.

Section	Parameter	Value	Unit / Note
RADIUS	Detection Interval	5	(in minutes)
	Reporting Interval	15	(in minutes)
	Reject RADIUS Requests	<input checked="" type="checkbox"/>	
	Failures prior to Rejection	5	(valid range 2 to 100)
	Request Rejection Interval	60	(in minutes)
	Suppress Repeated Successful Authentications	<input type="checkbox"/>	
RADIUS UDP ports	*Authentication Ports	1812,1645	
	*Accounting Ports	1813,1646	
	*Authentication & Accounting Ports	2083	
RADIUS DTLS	Accounting Suppression Interval	5	(in seconds)
	Long Processing Step Threshold Interval	1,000	(in milliseconds)
RADIUS DTLS	Idle Timeout	60	(in second, valid range 60 to 600)

Buttons at the bottom: Save, Reset, Reset To Defaults.

Merk op dat DTLS poort anders is dan RADIUS poorten. Standaard gebruikt een RADIUS paren 1645, 1646 en 1812, 1813. Standaard DTLS voor authenticatie, autorisatie, accounting en CoA gebruik van poort 2083. **De inactiviteitstimer** specificeert hoe lang ISE en authenticator tunnels onderhouden zonder enige echte communicatie die het doorvoert. Deze timeout wordt in seconden gemeten en varieert van 60 tot 600 seconden.

3. Exportemittent van het DTLS RADIUS-certificaat bij ISE-trustwinkel.

Om de tunnel tussen ISE en authenticator te creëren, moeten beide entiteiten certificaten uitwisselen en controleren. Authenticator moet het ISE RADIUS DTLS-certificaat vertrouwen, wat betekent dat zijn emittent aanwezig moet zijn in de Trust Store van de authenticator. Om de ondertekenaar van het ISE-certificaat te kunnen exporteren, navigeer naar **Administratie > Systeem > Certificaten**, zoals in de afbeelding:

The screenshot shows the 'System Certificates' page in the Cisco ISE Administration console. A table lists the certificates, including their names, used by, portal group tags, issued to, issued by, valid from, and expiration date.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
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
ISE22-1ek.example.com,ISE22-1ek.example.com,"example.com#LAB CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group (i)	ISE22-1ek.example.com	LAB CA	Mon, 31 Oct 2016	Wed, 31 Oct 2018
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

Lokaliseer certificaat met RADIUS DTLS rol toegewezen en controleer **afgegeven door** veld voor

dit certificaat. Dit is de Gemeenschappelijke Naam van certificaat dat uit ISE Trust Store moet worden geëxporteerd. Om dat te doen, navigeer dan naar **Administratie > Systeem > Certificaten Trusted Certificaten**. Selecteer selectieteken naast het juiste certificaat en klik op **Exporteren**.

4. Het vertrouwenspunt configureren en het invoercertificaat ter authenticatie instellen.

U kunt als volgt een trustpunt instellen door aan de knop te loggen en opdrachten uit te voeren:

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

Importeer certificaat met commando **crypto pki authenticate isetp**. Typ ja bij ontvangst van het certificaat.

```
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/
MRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYKCZImiZPyLGBGRYHZXhhbXBsZTEP
MA0GA1UEAxMGTEFCIENBMB4XDTE1MDIxMjA3MzgxM1oXDTE1MDIxMjA3NDgxM1ow
PzETMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2V4YW1wbGUx
DzANBgNVBAMTBkxkYDQTCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMDSfJwvbjLHHJf4vDTalGjKrDI73c/y269IMZV48xpCruNhglcU8CW/T9Ysj6xk
Oogtx2vpG4XJt7KebDZ/ac1Ymjg7sPBPCnyDZCd2a1b39XakD2puE81Vi4RVkjBH
pss2fTWeuor9dzgb/kWb0YqIsgw1sRKQ2Veh1IXmuhX+wDqELHPIzgXn/DOBF0qN
vWlevrAlmBTxC04t1aPwyRk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wg
HDvd6C6LKRbpmAvtrqyDtine1/CraEFH7dZpvUSJBNUh7st3JIG8gVFstweoMmTE
zxUONQw8QrZmXDGTKgqvisECAwEAAaNRME8wCwYDVR0PBAQDAgGMA8GA1UEEwEB
/wQFMAMBaf8wHQYDVR0OBBYEF0TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQB
ggjcVAQDAQEAMA0GCSqSIB3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVi
xhn7KrEyWxLkWaLsbU2ixsfTeJDCM8pxQItsj6B0Ey6A05c3YNcvW1iNpupGgc7v
9lMt4/TB6aRLVLijBPB9/p2/3SJaDce/YBaOn/vpmfBPPPhUQVPiBM9fy/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. Exportcertificaat van de schakelaar.

Selecteer vertrouwen en certificaat dat voor DTLS op de schakelaar moet worden gebruikt en voer het uit:

```
Switch3650(config)#crypto pki export TP-self-signed-721943660 pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIICKTCCAzKgAwIBAgIBATANBgkqhkiG9w0BAQUFADAwMS4wLAYDVQQDEyVJT1Mt
U2VsZi1TaWduZWQtQ2VydGlmawNhdGUtNzIxOTQzNjYwMB4XDTE2MDQyNzExNDYw
Nl0XDTEwMDEwMTAwMDAwMFowMDEuMDEuMDEuMDEuMDEuMDEuMDEuMDEuMDEuMDEu
cnRpZm1jYXR1L1Rlcj0MzY2MDCBnzANBjKqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
xRybTGD526rPYu2puMJU8ANcDqQnwunIERgvIWoLwBovuAu7WcRmzw1IDTDryOH
PXt1n5GcQSAOgn+9QdvKl1Z43ZkRWK5E7EGmjM/aL1287mg4/NlrWr4KMSwDQBJI
noJ52CABXUoApuiiJ8Ya4gOYeP0TmsZtxP1N+s+wqjMCAwEAAaNTMFEwDwYDVR0T
AQH/BAUwAwEB/zAfBgNVHSMEGDAWgBSEOKlAPAHBPedwichXL+qUM+1riTAdBgNV
HQ4EFgQUhDipQDwBwT3ncInIVy/q1DPta4kWDQYJKoZIhvcNAQEFBQADgYEA1BNN
wKSS8yBuOH0/jUV7sy3Y9/oV7Z9bW8WfV9QiTQ11ZelvWMTbewozwX2LJvxobGcj
Pi+n99RIH8dBhWwoY19GTN2LVI22GIPX12jNLqps+Mq/u2qxVm0964Sajs501KjQ
69XFfCVot1NA6z2eEP/69oL9x0uaJDZa+6ileh0=
-----END CERTIFICATE-----
```

Om een lijst te maken van alle gevormde trustpoints, **moet** je opdracht uitvoeren om **cryptografische poppen te tonen**. Nadat het certificaat is afgedrukt om te troosten, kopieert u het naar een bestand en slaat u het op uw pc.

6. Importeer switch certificaat aan ISE Trust Store.

Op ISE, navigeer naar **Beheer > Certificaten > Vertrouwde certificaten** en klik op **Importeren**.

Klik nu op **Bladeren** en selecteer certificaat van de switch. Verstrek (optioneel) vriendschappelijke naam en selecteer selectietekens **Vertrouwen voor authenticatie binnen ISE** en **Vertrouwen voor cliëntauthenticatie en Syslog**. Klik vervolgens op **Inzenden**, zoals in de afbeelding:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. 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'. The form includes the following fields and options:

- * Certificate File: sw.pem
- Friendly Name:
- Trusted For:
- Trust for authentication within ISE:
- Trust for client authentication and Syslog:
- Trust for authentication of Cisco Services:
- Validate Certificate Extensions:
- Description:
- Buttons:

7. Configureer de RADIUS op de schakelaar.

Voeg de configuratie van RADIUS toe op de schakelaar. Om de schakelaar te configureren om met ISE via DTLS te communiceren, gebruikt u opdrachten:

```
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
```

De rest van de AAA-specifieke configuratie is afhankelijk van uw vereisten en ontwerp. Behandel deze configuratie als voorbeeld:

```
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. Het beleid op ISE configureren.

Verificatie- en autorisatiebeleid ten aanzien van ISE configureren. Deze stap is ook afhankelijk van uw ontwerp en uw vereisten.

Verifiëren

Om te verifiëren dat de gebruikers voor authenticatie kunnen zorgen, gebruik **test aaa** opdracht op de schakelaar:

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

USER ATTRIBUTES

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

U dient het bericht **te zien dat de gebruiker is echt verklaard**. navigeren naar **ISE Operations > RADIUS > LiveLog** en selecteer details voor aangepast logbestand (klik op vergroot glas):

The screenshot shows the Cisco Identity Services Engine (ISE) Operations console. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'RADIUS' section is active, showing 'Threat-Centric NAC Live Logs', 'TACACS', 'Troubleshoot', 'Adaptive Network Control', and 'Reports'. A 'Click here' button is visible in the top right corner.

Summary statistics:

- Misconfigured Supplicants: 0
- Misconfigured Network Devices: 0
- RADIUS Drops: 42
- Client Stopped Responding: 0

Refresh: Every 1 minute

Actions: Refresh, Reset Repeat Counts, Export To

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

Aan de rechterkant van het verslag staat een lijst met **stappen**. Controleer of de eerste stap in de lijst met **RADIUS** is versleuteld.

Daarnaast kunt u pakketvastlegging op ISE starten en de opdracht **testgegevens** één keer uitvoeren. Om de opname te starten, navigeer naar **Operations > Troubleshooter > Diagnostische tools > General Tools > TCP-pomp**. Selecteer Policy Service Node voor verificatie en klik op **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

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

Als de verificatie is voltooid, klikt u op **Stoppen** en **Downloaden**. Wanneer u pakketvastlegging opent, dient u verkeer versleuteld met DTLS te kunnen zien:

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 maken deel uit van de handdruk van DTLS. Wanneer de handdruk met succes is onderhandeld, worden de Application Data verzonden. Merk op dat het aantal pakketten kan variëren en afhankelijk is van bijvoorbeeld de gebruikte authenticatiemethode (PAP, EAP-PEAP, EAP-TLS, enz.). De inhoud van elk pakket is versleuteld:

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...

Wanneer alle gegevens worden verzonden, wordt de tunnel niet onmiddellijk afgebroken. De op ISE **ingestelde Idle-out** bepaalt hoe lange tunnel kan worden ingericht zonder communicatie door het te voeren. Als de timer verlopen en het nieuwe toegangsverzoek naar ISE moet worden

verzonden, wordt de DTLS-handdruk uitgevoerd en de tunnel wordt opnieuw gebouwd.

Problemen oplossen

1. ISE ontvangt geen verzoeken.

Merk op dat de standaard DTLS poort 2083 is. Standaard RADIUS-poorten zijn 1645,1646 en 1812,1813. Zorg ervoor dat de firewall het UDP/2083-verkeer niet blokkeert.

2. DTLS-handdruk mislukt.

In het gedetailleerde rapport over ISE ziet u mogelijk dat de DTLS-handdruk is mislukt:

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

Mogelijke reden is dat de schakelaar of ISE geen certificaat vertrouwt dat tijdens de handdruk wordt verstuurd. Controleer de configuratie van het certificaat. Controleer dat het juiste certificaat is toegewezen aan RADIUS DTLS rol op ISE en aan de trustpoints op de switch.