De Cisco Access Registrar en LEAP configureren

Inhoud

Inleiding

Cisco Network Services Access Registrar (AR) 3.0 ondersteunt Light Extensible Authentication Protocol (LEAP-Cisco Wireless). Dit document toont hoe u draadloze Aironet-clientadaptertools en Cisco Aironet 340, 350 of 1200 Series access points (AP's) voor LEAP-verificatie naar de Cisco AR kunt configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

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

- Cisco Aironet® 340, 350 of 1200 Series access points
- AP-firmware 11.21 of hoger voor Cisco LEAP
- Cisco Aironet 340 of 350 Series netwerkinterfacekaarten (NIC's)
- Firmware versies 4.25.30 of hoger voor Cisco LEAP
- Network driver Interface Specification (NDIS) 8.2.3 of hoger voor Cisco LEAP

- Aironet Client Utilities (ACU) versies 5.02 of hoger
- Cisco Access Registrar 3.0 of hoger is vereist om Cisco LEAP- en MAC-verificatieverzoeken uit te voeren en te authentiseren

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

EAP-Cisco draadloos configureren (Cisco LEAP)

Deze sectie bestrijkt de basisconfiguraties van Cisco LEAP op de Cisco AR server, AP, en diverse klanten.

Stapsgewijze instructies

Volg deze instructies om LEAP te configureren:

1. Verander de poort op Cisco AR server.AP stuurt RADIUS-informatie over User Datagram Protocol (UDP)-poorten 1812 (authenticatie) en 1813 (accounting). Aangezien Cisco AR standaard luistert naar UDP-poorten 1645 en 1646, moet u de Cisco AR configureren om te luisteren op UDP-poorten 1812 en 1813.Geef de opdracht **cd/straal/geavanceerde/poorten** uit.Geef de opdracht **add 1812 uit** om poort 1812 toe te voegen.Als u van plan bent om accounting uit te voeren, geeft u de opdracht **1813 toe** om poort 1813 toe te voegen.Sla de configuratie op en start de services opnieuw.
2. U kunt AP aan de Cisco AR server toevoegen door deze opdrachten uit te voeren:**CD/Straal/clientsadd ap350-1cd ap350-1vastgesteld adres 171.69.89.1vastgesteld gedeeld cisco**
3. Om de de zeer belangrijke de sessietijd van de weduwe Equivalent Privacy (GND) te configureren geeft u deze opdrachten aan:**Opmerking:** 802.1x specificeert een optie voor herauthenticatie. Het algoritme van Cisco LEAP gebruikt deze optie om de huidige de sessiesleutel van EFG voor de gebruiker te verlopen en een nieuwe de sessiesleutel van EFG uit te geven.**CD/Straal/profielenprofiel toevoegenprofiel van de cdcd-eigenschappenset sessie-timeout 600**
4. Om een gebruikersgroep te maken die de profielen gebruikt die in Stap 3 zijn toegevoegd, geeft u deze opdrachten uit:**CD/Straal/groepen gebruikerspop-groep toevoegencd-ap-groepbasisprofiel instellen**De gebruikers in deze gebruikersgroep erven het profiel en ontvangen op hun beurt de sessietijd.
5. U kunt gebruikers in een gebruikerslijst maken en de gebruikers toevoegen aan de gebruikersgroep die in Stap 4 is gedefinieerd. U geeft deze opdrachten uit:**CD/Straal/Amerikaanse lijstengebruikers van het pakket toevoegencd-ap-gebruikersadd gebruiker1cd - gebruiker 1wachtwoord instellen Ciscovaste groep**
6. Om een lokale authenticatie- en autorisatieservice te creëren om de gebruikersservice 'service' te gebruiken en het servicetype in te stellen op 'aanloop', geeft u deze opdrachten

uit:**CD/Straal/servicestoevoegen van ap-localservicecd-ap-localserviceinstellen van aanjager typeSet-User-Service API-gebruikersservice**

7. U maakt als volgt een gebruikersservice die "service-gebruiker" is, om de gebruikerslijst te gebruiken die in Stap 5 is gedefinieerd. Geef deze opdrachten uit:**CD/Straal/servicesadd/drop-gebruikersservicecd-ap-localservicetype lokaal instellenselectielijst gebruiker-ap-gebruikers**
8. Om de standaard verificatie- en autorisatieservice in te stellen die Cisco AR gebruikt voor de service die gedefinieerd is in Stap 6, geeft u deze opdrachten uit:**CD/Straalstel de standaardtauthAuthenticationService ap-localservice instel de defaultauthorization service ap-localservice in**
9. Om de configuratie op te slaan en opnieuw te laden, geeft u deze opdrachten uit:**opslaanherladen**

EAP-Cisco (Cisco LEAP) op de AP inschakelen

Stapsgewijze instructies

Volg deze stappen om Cisco LEAP op AP toe te laten:

1. Bladeren naar het AP.
2. Klik op **SETUP** in de pagina Summary Status.
3. Klik in het menu Services op **Security > Verificatieserver**.
4. Selecteer de versie van 802.1x die u op deze AP wilt uitvoeren in het vervolgkeuzemenu van 802.1x Protocol.
5. Configuratie van het IP-adres van de Cisco AR in het tekstvak Naam/IP van de server.
6. Controleer of het vervolgkeuzemenu Server Type op **RADIUS** is ingesteld.
7. Verander het poorttekstvak in **1812**. Dit is het juiste IP-poortnummer dat met de Cisco AR moet worden gebruikt.
8. Configureer het gedeelde tekstvak met de waarde die in de Cisco AR is gebruikt.
9. Selecteer het aankruisvakje **EAP-verificatie**.
10. Wijzig het tekstvak Time-out indien gewenst. Dit is de timeout waarde voor een authenticatieaanvraag voor Cisco AR.
11. Klik op **OK** om terug te keren naar het scherm Security Setup.Als u ook RADIUS-accounting uitvoert, controleer of de poort op de pagina Accounting Setup overeenkomt met de poort die is ingesteld in Cisco AR (ingesteld voor 1813).
12. Klik op **Radio Data Encryption (EFN)**.
13. Configuratie van een sleutel van de uitzending van EFN door een 40 - of 128 bit - zeer belangrijke waarde in het de tekstvakje van de sleutel 1 te typen.
14. Selecteer de te gebruiken authenticatietypen. Zorg ervoor dat ten minste het vakje **netwerk-EAP** is geselecteerd.
15. Controleer of het vervolgkeuzemenu Gebruik van Data Encryption is ingesteld op **optionele** of **Full Encryption**. Optioneel staat het gebruik toe van niet-EFN- en EFN-clients op dezelfde AP. Let erop dat dit een onveilige manier van werken is. Gebruik indien mogelijk volledige encryptie.
16. Klik op **OK** om te voltooien.

ACU 6.00 configureren

Stapsgewijze instructies

Volg deze stappen om de ACU te configureren:

1. Open de ACU.
2. Klik in de werkbalk op **Profile Manager**.
3. Klik op **Add** om een nieuw profiel te maken.
4. Voer de profielnaam in het tekstvak in en klik vervolgens op **OK**.
5. Voer in het juiste Service Set-id (SSID) in het tekstvak SSID1 in.
6. Klik op **Netwerkbeveiliging**.
7. Selecteer **LEAP** in het vervolgkeuzemenu Type netwerkbeveiliging.
8. Klik op **Configureren**.
9. Configureer de wachtwoordinstellingen zoals nodig.
10. Klik op **OK**.
11. Klik op **OK** op het scherm Network Security.

Traces uit Cisco AR

Geef de **overtrek /r 5** uit om sporen output op de Cisco AR te verkrijgen. Als u AP debug nodig hebt, kunt u met AP via telnet verbinden en de opdrachten **eap_diag1_on** en **eap_diag2_on** uitgeven.

```
06/28/2004 16:31:49: P1121: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1121: Checking Message-Authenticator
06/28/2004 16:31:49: P1121: Trace of Access-Request packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 146
06/28/2004 16:31:49: P1121:
   reqauth = e5:4f:91:27:0a:91:82:6b:a4:81:c1:cc:c8:11:86:0b
06/28/2004 16:31:49: P1121: User-Name = user1
06/28/2004 16:31:49: P1121: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1121: NAS-Port = 37
06/28/2004 16:31:49: P1121: Service-Type = Login
06/28/2004 16:31:49: P1121: Framed-MTU = 1400
06/28/2004 16:31:49: P1121: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1121: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1121: NAS-Identifier = frinket
06/28/2004 16:31:49: P1121: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1121: EAP-Message = 02:02:00:0a:01:75:73:65:72:31
06/28/2004 16:31:49: P1121:
   Message-Authenticator = f8:44:b9:3b:0f:33:34:a6:ed:7f:46:2d:83:62:40:30
06/28/2004 16:31:49: P1121: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1121: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1121: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1121: Authenticating and Authorizing with
   Service ap-localservice
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
   skipping Remote Session Management.
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
   skipping Local Session Management.
06/28/2004 16:31:49: P1121: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1121: Trace of Access-Challenge packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 61
06/28/2004 16:31:49: P1121:
```

```
   reqauth = 60:ae:19:8d:41:5e:a8:dc:4c:25:1b:8d:49:a3:47:c4
06/28/2004 16:31:49: P1121: EAP-Message =
   01:02:00:15:11:01:00:08:66:27:c3:47:d6:be:b3:67:75:73:65:72:31
06/28/2004 16:31:49: P1121: Message-Authenticator =
   59:d2:bc:ec:8d:85:36:0b:3a:98:b4:90:cc:af:16:2f
06/28/2004 16:31:49: P1121: Sending response to 10.48.86.230
06/28/2004 16:31:49: P1123: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1123: Checking Message-Authenticator
06/28/2004 16:31:49: P1123: Trace of Access-Request packet
06/28/2004 16:31:49: P1123: identifier = 6
06/28/2004 16:31:49: P1123: length = 173
06/28/2004 16:31:49: P1123:
   reqauth = ab:f1:0f:2d:ab:6e:b7:49:9e:9e:99:00:28:0f:08:80
06/28/2004 16:31:49: P1123: User-Name = user1
06/28/2004 16:31:49: P1123: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1123: NAS-Port = 37
06/28/2004 16:31:49: P1123: Service-Type = Login
06/28/2004 16:31:49: P1123: Framed-MTU = 1400
06/28/2004 16:31:49: P1123: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1123: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1123: NAS-Identifier = frinket
06/28/2004 16:31:49: P1123: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1123: EAP-Message =
   02:02:00:25:11:01:00:18:5e:26:d6:ab:3f:56:f7:db:21:96:f3:b0:fb:ec:6b:
   a7:58:6f:af:2c:60:f1:e3:3c:75:73:65:72:31
06/28/2004 16:31:49: P1123: Message-Authenticator =
   21:da:35:89:30:1e:e1:d6:18:0a:4f:3b:96:f4:f8:eb
06/28/2004 16:31:49: P1123: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1123: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1123: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1123: Authenticating and Authorizing
   with Service ap-localservice
06/28/2004 16:31:49: P1123: Calling external service ap-userservice
   for authentication and authorization
06/28/2004 16:31:49: P1123: Getting User user1's UserRecord
   from UserList ap-users
06/28/2004 16:31:49: P1123: User user1's MS-CHAP password matches
06/28/2004 16:31:49: P1123: Processing UserGroup ap-group's check items
06/28/2004 16:31:49: P1123: User user1 is part of UserGroup ap-group
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's BaseProfiles
   into response dictionary
06/28/2004 16:31:49: P1123: Merging BaseProfile ap-profile
   into response dictionary
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1123: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's Attributes
   into response Dictionary
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1123: Removing all attributes except for
   EAP-Message from response - they will be sent back in the Access-Accept
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,
   skipping Remote Session Management.
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,
   skipping Local Session Management.
06/28/2004 16:31:49: P1123: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1123: Trace of Access-Challenge packet
06/28/2004 16:31:49: P1123: identifier = 6
06/28/2004 16:31:49: P1123: length = 44
06/28/2004 16:31:49: P1123:
   reqauth = 28:2e:a3:27:c6:44:9e:13:8d:b3:60:01:7f:da:8b:62
06/28/2004 16:31:49: P1123: EAP-Message = 03:02:00:04
06/28/2004 16:31:49: P1123: Message-Authenticator =
   2d:63:6a:12:fd:91:9e:7d:71:9d:8b:40:04:56:2e:90
06/28/2004 16:31:49: P1123: Sending response to 10.48.86.230
```

```
06/28/2004 16:31:49: P1125: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1125: Checking Message-Authenticator
06/28/2004 16:31:49: P1125: Trace of Access-Request packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 157
06/28/2004 16:31:49: P1125:
   reqauth = 72:94:8c:34:4c:4a:ed:27:98:ba:71:33:88:0d:8a:f4
06/28/2004 16:31:49: P1125: User-Name = user1
06/28/2004 16:31:49: P1125: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1125: NAS-Port = 37
06/28/2004 16:31:49: P1125: Service-Type = Login
06/28/2004 16:31:49: P1125: Framed-MTU = 1400
06/28/2004 16:31:49: P1125: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1125: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1125: NAS-Identifier = frinket
06/28/2004 16:31:49: P1125: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1125: EAP-Message =
   01:02:00:15:11:01:00:08:3e:b9:91:18:a8:dd:98:ee:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
   8e:73:2b:a6:54:c6:f5:d9:ed:6d:f0:ce:bd:4f:f1:d6
06/28/2004 16:31:49: P1125: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1125: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1125: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1125: Authenticating and Authorizing
   with Service ap-localservice
06/28/2004 16:31:49: P1125: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1125: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1125: Restoring all attributes to response
   that were removed in the last Access-Challenge
06/28/2004 16:31:49: P1125: No default Remote Session Service defined.
06/28/2004 16:31:49: P1125: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1125: Trace of Access-Accept packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 142
06/28/2004 16:31:49: P1125:
   reqauth = 71:f1:ef:b4:e6:e0:c2:4b:0a:d0:95:47:35:3d:a5:84
06/28/2004 16:31:49: P1125: Session-Timeout = 600
06/28/2004 16:31:49: P1125: EAP-Message =
02:02:00:25:11:01:00:18:86:5c:78:3d:82:f7:69:c7:96:70:35:31:bb:51:a7:ba:f8:48:8c:
45:66:00:e8:3c:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
7b:48:c3:17:53:67:44:f3:af:5e:17:27:3d:3d:23:5f
06/28/2004 16:31:49: P1125: Cisco-AVPair =
6c:65:61:70:3a:73:65:73:73:69:6f:6e:2d:6b:65:79:3d:04:f2:c5:2a:de:fb:4e:1e:8a:8d
:b8:1b:e9:2c:f9:9a:3e:83:55:ff:ae:54:57:4b:60:e1:03:05:fd:22:95:4c:b4:62
06/28/2004 16:31:49: P1125: Sending response to 10.48.86.230
```

Gerelateerde informatie

- Ondersteuning van Cisco Access Registrar
- Technische ondersteuning en documentatie – Cisco Systems