Configurazione di Cisco Access Registrar e LEAP

Sommario

Introduzione

Cisco Networking Services Access Registrar (AR) 3.0 supporta il protocollo LEAP (Light Extensible Authentication Protocol) (EAP-Cisco Wireless). In questo documento viene spiegato come configurare le utility client Aironet wireless e i Cisco Aironet serie 340, 350 o 1200 Access Point (AP) per l'autenticazione LEAP su Cisco ASR.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Access point Cisco Aironet® serie 340, 350 o 1200
- AP Firmware 11.21 o versione successiva per Cisco LEAP
- Cisco Aironet serie 340 o 350 Network Interface Card (NIC)
- Firmware versione 4.25.30 o successive per Cisco LEAP

- Network Driver Interface Specification (NDIS) 8.2.3 o versioni successive per Cisco LEAP
- Aironet Client Utilities (ACU) versione 5.02 o successive
- Per eseguire e autenticare le richieste di autenticazione Cisco LEAP e MAC è necessario Cisco Access Registrar 3.0 o versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione di EAP-Cisco Wireless (Cisco LEAP)

In questa sezione vengono illustrate le configurazioni di base di Cisco LEAP sul server AR Cisco, sull'access point e su vari client.

Istruzioni dettagliate

Seguire queste istruzioni per configurare LEAP:

1. Modificare la porta sul server Cisco ASR.L'access point invia informazioni RADIUS sulle porte UDP (User Datagram Protocol) 1812 (autenticazione) e 1813 (accounting). Poiché per impostazione predefinita Cisco ASR resta in ascolto sulle porte UDP 1645 e 1646, è necessario configurare Cisco ASR per l'ascolto sulle porte UDP 1812 e 1813.Eseguire il comando **cd /radius/advanced/ports**.Eseguire il comando **add 1812** per aggiungere la porta 1812.Se si intende eseguire l'accounting, utilizzare il comando **add 1813** per aggiungere la porta 1813.Salvare la configurazione, quindi riavviare i servizi.
2. Per aggiungere l'access point al server Cisco ASR, eseguire questi comandi:**cd/Radius/Clientadd ap350-1cd ap350-1set ipaddress 171.69.89.1set sharedsecret cisco**
3. Per configurare il timeout della sessione della chiave WEP (Wired Equivalent Privacy), eseguire i comandi seguenti:**Nota:** 802.1x specifica un'opzione di riautenticazione. L'algoritmo Cisco LEAP utilizza questa opzione per far scadere la chiave di sessione WEP corrente per l'utente e rilasciare una nuova chiave di sessione WEP.**cd/Raggio/Profiliaggiungi profilo apcd ap-profileattributi cdset session-timeout 600**
4. Per creare un gruppo di utenti che utilizzi i profili aggiunti nel passaggio 3, eseguire questi comandi:**cd /Radius/Gruppi di utentiaggiungi gruppo apcd ap-groupset baseprofile ap-profile**Gli utenti di questo gruppo ereditano il profilo e a loro volta ricevono il timeout della sessione.
5. Per creare utenti in un elenco utenti e aggiungere gli utenti al gruppo definito nel passaggio 4, eseguire questi comandi:**cd /Radius/Elenchi utentiaggiungere utenti aputenti cd apaggiungi utente1cd utente1impostare la password Ciscoset group ap-group**
6. Per creare un servizio di autenticazione e autorizzazione locale in modo da utilizzare UserService "ap-userservice" e impostare il tipo di servizio su "eap-leap", eseguire i comandi seguenti:**cd/Radius/Serviziaggiungi ap-localservicecd ap-localserviceset type eap-leapset**

UserService ap-userservice

7. Per creare un servizio utente "ap-userservice" per utilizzare l'elenco di utenti definito nel passo 5, eseguire questi comandi:**cd/Radius/Serviziadd ap-userservicecd ap-localserviceimposta tipo localeset userlist ap-users**
8. Per impostare il servizio di autenticazione e autorizzazione predefinito utilizzato da Cisco ASR sul servizio definito nel passaggio 6, eseguire i comandi seguenti:**cd/raggioimposta defaultauthenticationservice ap-localserviceimpostare defaultauthorizationservice ap-localservice**
9. Per salvare e ricaricare la configurazione, utilizzare i seguenti comandi:**salvarericaricare**

Abilitazione di EAP-Cisco (Cisco LEAP) sull'access point

Istruzioni dettagliate

Per abilitare Cisco LEAP sull'access point, attenersi alla procedura seguente:

1. Selezionare l'access point.
2. Nella pagina Stato riepilogo fare clic su **SETUP**.
3. Scegliere **Protezione > Server di autenticazione** dal menu Servizi.
4. Selezionare la versione di 802.1x da eseguire sull'access point nel menu a discesa Versione protocollo 802.1x.
5. Configurare l'indirizzo IP della Cisco ASR nella casella di testo Nome/IP server.
6. Verificare che il menu a discesa Tipo di server sia impostato su **RADIUS**.
7. Impostate la casella di testo Port a **1812**. Questo è il numero di porta IP corretto da utilizzare con Cisco ASR.
8. Configurare la casella di testo Segreto condiviso con il valore utilizzato in Cisco ASR.
9. Selezionare la casella di controllo **Autenticazione EAP**.
10. Se desiderato, modificare la casella di testo Timeout. Valore di timeout per una richiesta di autenticazione per Cisco ASR.
11. Fare clic su **OK** per tornare alla schermata Security Setup (Impostazione protezione).Se si sta eseguendo anche l'accounting RADIUS, verificare che la porta nella pagina di impostazione dell'accounting sia compatibile con la porta configurata in Cisco ASR (impostata per 1813).
12. Fare clic su **Crittografia dati radio (WEP)**.
13. Configurare una chiave WEP di trasmissione digitando un valore di chiave a 40 o 128 bit nella casella di testo Chiave WEP 1.
14. Selezionare i tipi di autenticazione da utilizzare. Verificare che almeno la casella di controllo **Network-EAP** sia selezionata.
15. Verificare che il menu a discesa Use of Data Encryption (Usa crittografia dati) sia impostato su **Optional** o **Full Encryption** (Crittografia completa). Facoltativo: consente l'utilizzo di client non WEP e WEP sullo stesso punto di accesso. Si tratta di una modalità di funzionamento non sicura. Se possibile, utilizzare la crittografia completa.
16. Fate clic su **OK** per completare l'operazione.

Configurazione di ACU 6.0

Istruzioni dettagliate

Per configurare l'ACU, attenersi alla procedura seguente:

1. Aprire l'ACU.
2. Fare clic su **Gestione profili** sulla barra degli strumenti.
3. Fare clic su **Aggiungi** per creare un nuovo profilo.
4. Immettere il nome del profilo nella casella di testo e quindi fare clic su **OK**.
5. Immettere il valore SSID nella casella di testo SSID1.
6. Fare clic su **Protezione di rete**.
7. Selezionare **LEAP** dal menu a discesa Tipo di protezione di rete.
8. Fare clic su **Configura**.
9. Configurare le impostazioni della password in base alle esigenze.
10. Fare clic su **OK**.
11. Fare clic su **OK** nella schermata Network Security (Sicurezza di rete).

Tracce da Cisco ASR

Utilizzare il comando **trace /r 5** per ottenere l'output di analisi in Cisco ASR. Se è necessario eseguire il debug, è possibile connettersi all'access point in modalità Telnet e usare i comandi **eap_diag1_on** e **eap_diag2_on**.

```
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
```

Informazioni correlate

- Pagina di supporto di Cisco Access Registrar
- Documentazione e supporto tecnico – Cisco Systems