Configurando o Cisco Access Registrar e o LEAP

Índice

Introdução

O 3.0 do Access Registrar do Cisco networking services (AR) apoia o protocolo light extensible authentication (PULO) (Sem fio do EAP-Cisco). Este documento mostra como configurar o Aironet Client Utilities wireless e o Cisco Aironet 340, 350, ou os Access point do 1200 Series (AP) para a autenticação de leap a Cisco AR.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Aironet® 340, 350, ou Access point do 1200 Series
- Firmware AP 11.21 ou mais atrasado para o PULO de Cisco
- Cisco Aironet 340 ou Network Interface Cards do 350 Series (NIC)
- Versões de firmware 4.25.30 ou mais atrasado para o PULO de Cisco
- Network Driver Interface Specification (NDIS) 8.2.3 ou mais atrasado para o PULO de Cisco

- Versões 5.02 ou mais recente do Aironet Client Utilities (ACU)
- São exigidos o Cisco Access Registrar 3.0 ou mais tarde para ser executado e para autenticar Cisco pedidos PULE e do autenticação de MAC

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurando EAP-Cisco Wireless (Cisco LEAP)

Esta seção cobre as configurações básicas do PULO de Cisco no server de Cisco AR, no AP, e em vários clientes.

Instruções passo a passo

Siga estas instruções para configurar o PULO:

1. Mude a porta no server de Cisco AR.O AP envia a informação radius nas portas 1812 (autenticação) e 1813 do User Datagram Protocol (UDP) (contabilidade). Desde que Cisco AR escuta nas portas 1645 e 1646 UDP à revelia, você deve configurar Cisco AR para escutar nas portas 1812 e 1813 UDP.Emita o comando de **/radius/advanced/ports do CD**.Emita o **comando add 1812** adicionar a porta 1812.Se você planeia fazer a contabilidade, emita o **comando add 1813** adicionar a porta 1813.Salvar a configuração, e reinicie então os serviços.
2. Para adicionar o AP ao server de Cisco AR, emita estes comandos:**CD /Radius/Clientsadicionar ap350-1CD ap350-1ajuste o IP address 171.69.89.1ajuste o sharedsecret Cisco**
3. Para configurar o timeout de sessão da chave do Wired Equivalent Privacy (WEP), emita estes comandos:**Note**: o 802.1x especifica uma opção de nova autenticação. Cisco PULA o algoritmo utiliza esta opção para expirar a chave de sessão atual WEP para o usuário e para emitir uma chave de sessão nova WEP.**CD /Radius/Profilesadicionar o ap-perfilap-perfil do CDatributos do CDajuste o sessão-intervalo 600**
4. Para criar um grupo de usuário que usasse os perfis adicionou em etapa 3, emitem estes comandos:**CD /Radius/Usergroupsadicionar o grupo APgrupo AP do CDajuste o ap-perfil baseprofile**Os usuários neste grupo de usuário herdam o perfil e recebem por sua vez o timeout de sessão.
5. Para criar usuários em uma lista de usuários e adicionar os usuários ao grupo de usuário definido em etapa 4, emita estes comandos:**CD /Radius/Userlistsadicionar ap-USERCD ap-USERadicionar o usuário1usuário1 do CDajuste a senha do Ciscoajuste o grupo AP do grupo**
6. Para criar um serviço da autenticação local e da autorização para usar UserService “ap-userservice” e para ajustar o tipo de serviço “EAP-pulo”, emita estes comandos:**CD /Radius/Servicesadicionar o ap-localserviceCD ap-localserviceajuste o tipo EAP-puloajuste**

UserService ap-userservice

7. Para criar um serviço de usuário “ap-userservice” para usar a lista de usuários definida na etapa 5, emita estes comandos:**CD /Radius/Servicesadicionar o ap-userserviceCD ap-localservicelocal de tipo de conjuntoajuste o userlist ap-USER**
8. Para ajustar a autenticação padrão e a autorização preste serviços de manutenção que os usos de Cisco AR ao serviço definido na etapa 6, emitem estes comandos:**CD /radiusajuste o defaultauthenticationservice ap-localserviceajuste o defaultauthorizationservice ap-localservice**
9. Para salvar e recarregar a configuração, emita estes comandos:**savereload**

Ativando o EAP-Cisco (Cisco LEAP) no AP

Instruções passo a passo

Siga estas etapas para permitir Cisco PULAM no AP:

1. Consulte ao AP.
2. Da página do status sumário, clique a **INSTALAÇÃO**.
3. No menu dos serviços, clique **Security > Authentication o server**.
4. Selecione a versão do 802.1x para ser executado neste AP no menu suspenso da versão do protocolo do 802.1x.
5. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT de Cisco AR na caixa de texto do server Name/IP.
6. Verifique que o menu suspenso do tipo de servidor está ajustado ao **RAIO**.
7. Mude a caixa de texto da porta a **1812**. Este é o número de porta correto IP a usar-se com Cisco AR.
8. Configurar a caixa de texto secreta compartilhada com o valor usado em Cisco AR.
9. Selecione a caixa de verificação da **autenticação de EAP**.
10. Altere a caixa de texto de intervalo se desejado assim. Este é o valor de timeout para um pedido de autenticação para Cisco AR.
11. Clique a **APROVAÇÃO** para retornar à tela da instalação de segurança.Se você igualmente está fazendo a contabilidade do RAIO, verifique que a porta na página de instalação da contabilidade concorda com a porta configurada em Cisco AR (se ajusta para 1813).
12. Clique em Radio Data Encryption (WEP).
13. Configurar uma chave de WEP da transmissão datilografando em um 40- ou o valor chave do 128-bit na caixa de texto da chave de WEP 1.
14. Selecione os tipos do autenticação para usar-se. Certifique-se de que, pelo menos, a **caixa de verificação de EAP de rede** está selecionada.
15. Verifique que o menu suspenso está ajustado Use of Data Encryption à **criptografia completa ou opcional**. Opcional permite o uso do NON-WEP e dos clientes WEP no mesmo AP. Esteja ciente que este é um modo incerto de operação. Use a criptografia total quando possível.
16. Clique a **APROVAÇÃO** para terminar.

Configurando ACU 6.00

Instruções passo a passo

Siga estas etapas para configurar o ACU:

1. Abra o ACU.
2. Clique o **gerente do perfil na** barra de ferramentas.
3. O clique **adiciona** para criar um perfil novo.
4. Dê entrada com o nome de perfil na caixa de texto, e clique então a **APROVAÇÃO**.
5. Entre no Service Set Identifier (SSID) apropriado na caixa de texto SSID1.
6. Clique a **segurança de rede**.
7. Selecione o **PULO do** tipo menu suspenso da segurança de rede.
8. Clique em Configurar.
9. Configurar as configurações de senha como necessárias.
10. Click **OK**.
11. Clique a **APROVAÇÃO na** tela de segurança de rede.

Rastreios do Cisco AR

Emita o **traço /r 5** para obter saídas de rastreamento em Cisco AR. Se você precisa o AP debugar, você pode conectar ao AP através do telnet e emitir os **comandos 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
```

Informações Relacionadas

- Página de suporte do Cisco Access Registrar
- Suporte Técnico e Documentação - Cisco Systems