

Versão de ACS 5.2 e WLC para pelo exemplo da configuração de autenticação WLAN

TAC

ID do Documento: 118661

Atualizado em: janeiro 14, 2015

Contribuído por Brahadesh Srinivasaraghavan, engenheiro de TAC da Cisco.



[Transferência PDF](#)



[Imprimir](#)

[Feedback](#)

Produtos Relacionados

- [Wireless, LAN \(WLAN\)](#)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar o WLC](#)

[Configurar o Cisco Secure ACS](#)

[Verificar](#)

[Troubleshooting](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este documento fornece um exemplo de configuração para restringir o acesso de usuário per. a um Wireless LAN (WLAN) baseado no Service Set Identifier (SSID).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar o controlador do Wireless LAN (WLC) e o Access point de pouco peso (REGAÇO) para a operação básica
- Como configurar o Serviço de controle de acesso Cisco Secure (ACS)
- Métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point

Componentes Utilizados

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

- Cisco 5500 Series WLC que executa a versão de firmware 7.4.110
- REGAÇO do Cisco 1142 Series
- Versão de servidor 5.2.0.26.11 do Cisco Secure ACS

Configurar

A fim configurar os dispositivos para esta instalação, você precisa:

1. Configurar o WLC para os dois WLAN e servidores Radius.
2. Configurar o Cisco Secure ACS.
3. Configurar os clientes Wireless e verifique a configuração.

Configurar o WLC

Termine estas etapas a fim configurar o WLC para esta instalação:

1. Configurar o WLC a fim enviar as credenciais do usuário a um servidor de raio externo. O servidor de raio externo (Cisco Secure ACS neste caso) então valida as credenciais do usuário e fornece o acesso aos clientes Wireless. Conclua estes passos: Selecione a **Segurança > a autenticação RADIUS** do controlador GUI a fim indicar a página dos servidores de autenticação RADIUS. Clique **novo** a fim definir os parâmetros do servidor Radius. Estes parâmetros incluem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius, o segredo compartilhado, o número de porta, e o status de servidor. As caixas de seleção do usuário de rede e do Gerenciamento determinam se a autenticação Raio-baseada se aplica para o Gerenciamento e os usuários de rede. Este exemplo usa o Cisco Secure ACS como o servidor Radius com endereço IP 10.104.208.56. Clique em Apply.
2. Termine estas etapas a fim configurar um WLAN para o empregado com **empregado** SSID e o outro WLAN para contratantes com **contratante** SSID. Clique **WLAN do** controlador GUI a fim criar um WLAN. A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador. Clique **novo** a fim configurar um WLAN novo. Este exemplo cria um Empregado nomeado WLAN e o ID de WLAN é 1. cliques **aplica-se**. Selecione **WLAN > editam o** indicador e definem os parâmetros específicos ao WLAN: Da ABA de segurança da camada 2, selecione o **802.1x**. À revelia, a opção de segurança da camada 2 é 802.1x. Isto permite 802.1 autenticações do protocolo de autenticação x/Extensible (EAP) para o WLAN. Dos servidores AAA catalogue, selecione o servidor Radius apropriado da lista de

drop-down sob servidores Radius. Os outros parâmetros podem ser alterados basearam na exigência da rede de WLAN. Clique em Apply. Similarmente, a fim criar um WLAN para contratantes, repita as etapas b a D.

Configurar o Cisco Secure ACS

No server do Cisco Secure ACS você precisa:

1. Configurar o WLC como um cliente de AAA.
2. Crie a base de dados de usuário (credenciais) para a autenticação SSID-baseada.
3. Permita a autenticação de EAP.

Termine estas etapas no Cisco Secure ACS:

1. A fim definir o controlador como um cliente de AAA no servidor ACS, selecione **recursos de rede > dispositivos de rede e clientes de AAA do ACS GUI**. Sob dispositivos de rede e clientes de AAA, o clique **cria**.
2. Quando a página da configuração de rede se publica, defina o nome do WLC, o endereço IP de Um ou Mais Servidores Cisco ICM NT, e o segredo e o método de autenticação compartilhados (RAIO).
3. Selecione **usuários e a identidade armazena > grupos da identidade do ACS GUI**. Crie os grupos respectivos para o empregado e o contratante e o clique **criam**. Neste exemplo o grupo criado é nomeado Empregado.
4. **Os usuários seletos e a identidade armazenam > lojas internas da identidade**. Clique **criam** e incorporem o username. Coloque-os no grupo correto, defina-o sua senha, e o clique **submete-se**. Neste exemplo um usuário nomeado employee1 no empregado do grupo é criado. Similarmente, crie um usuário nomeado contractor1 sob os contratantes do grupo.
5. Selecione **elementos da política > condições de rede > filtros da estação final**. Clique em **Criar**. Dê entrada com um nome significativo e sob a aba do **endereço IP de Um ou Mais Servidores Cisco ICM NT** incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC. Neste exemplo os nomes são empregado e contratante. Sob a aba CLI/DNIS, deixe o CLI como - e incorpore o DNIS como ***<SSID>**. Neste exemplo, o campo DNIS é entrado como o ***Employee** como este filtro da estação final é usado para restringir o acesso somente ao empregado WLAN. O atributo DNIS define o SSID que é permitido ao usuário alcançar. O WLC envia o SSID no atributo DNIS ao servidor Radius. Repita as mesmas etapas para o filtro da estação final do contratante.
6. Selecione **elementos da política > autorização e permissões > perfis do acesso de rede > da autorização**. Deve haver um perfil padrão para o acesso da licença.
7. Selecione **políticas de acesso > acesso presta serviços de manutenção > regras de seleção do serviço**. O clique **personaliza**. Adicionar toda a condição apropriada. Este exemplo usa o protocolo como o raio como a circunstância de harmonização. Clique em **Criar**. Nomeie a regra. Selecione o **protocolo** e selecione o **raio**. Sob **resultados**, escolha o serviço apropriado do acesso. Neste exemplo, é deixado como o **acesso de rede padrão**.
8. Selecione **políticas de acesso > acesso presta serviços de manutenção > acesso > identidade de rede padrão**. Escolha a únicas seleção do resultado e **fonte da identidade** como usuários internos. Selecione **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**. O clique **personaliza** e adiciona as circunstâncias personalizadas. Este exemplo usa o grupo da identidade, NDG: Tipo de dispositivo, e filtro da estação final nessa ordem. Clique em **Criar**. Nomeie a regra e escolha

o grupo apropriado da identidade sob todos os grupos. Neste exemplo é empregado. Clique o botão de rádio do **filtro de Stn do fim do empregado** ou dê entrada com o nome que você entra em Step1b “configura na seção WLC”. Verifique a caixa de **verificação de acesso da licença**. Repita as mesmas etapas acima para regras do contratante também. Assegure-se de que a ação padrão seja **negar o acesso**. Uma vez que você terminou a etapa e, suas regras devem olhar como este exemplo:

Isto conclui a configuração. Após esta seção, o cliente precisa de ser configurado em conformidade com o SSID e os parâmetros de segurança a fim conectar.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Era este documento útil? [Sim](#) [nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: janeiro 14, 2015

ID do Documento: 118661