Solucionar problemas de autenticação da Web em uma controladora Wireless LAN (WLC)

Contents

Introduction

Este documento descreve dicas para solucionar problemas de autenticação da Web em um ambiente de Wireless LAN Controller (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controle e provisionamento de access points sem fio (CAPWAP).
- Como configurar o Lightweight Access Point (LAP) e a WLC para a operação básica.
- Conhecimento básico de autenticação da Web e como configurar a autenticação da Web em WLCs.

Para obter informações sobre como configurar a autenticação da Web em WLCs, consulte o Exemplo de Configuração da Autenticação da Web da Controladora Wireless LAN.

Componentes Utilizados

As informações neste documento são baseadas em uma WLC 5500 que executa a versão 8.3.121 do firmware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com este hardware:

- Controladores Cisco 5500 Series Wireless

- Controladores sem fio Cisco 8500 Series
- Controladores Cisco 2500 Series Wireless
- Controlador WLAN Cisco Airespace 3500 Series
- Controlador LAN sem fio Cisco Airespace 4000 Series
- Controladores sem fio Cisco Flex 7500 Series
- Cisco Wireless Services Module 2 (WiSM2)

Autenticação da Web em WLCs

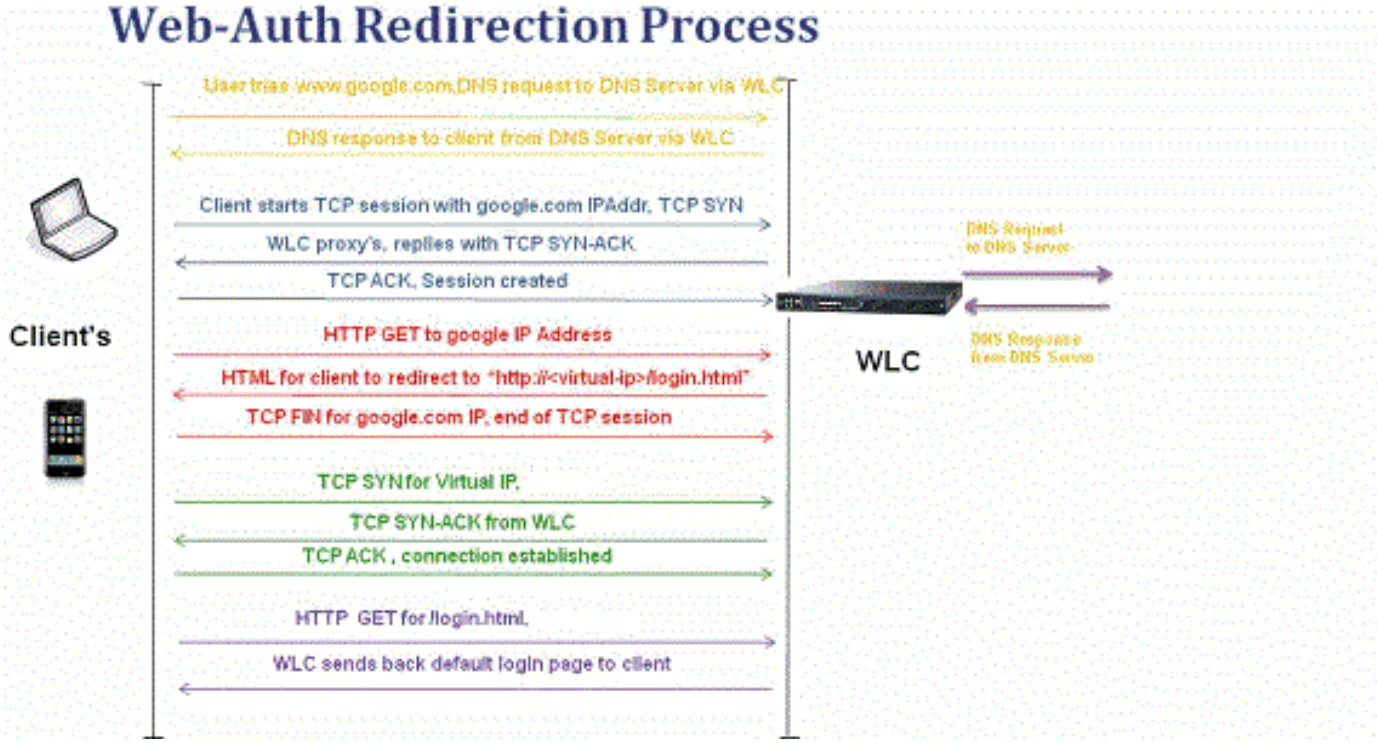
A autenticação da Web é um recurso de segurança da Camada 3 que faz com que o controlador não permita o tráfego IP, exceto pacotes relacionados ao DHCP/pacotes relacionados ao Sistema de Nome de Domínio (DNS - Domain Name System), de um determinado cliente até que esse cliente tenha fornecido corretamente um nome de usuário e uma senha válidos, com exceção do tráfego permitido através de uma lista de controle de acesso (ACL - Access Control List) de pré-autorização. A autenticação da Web é a única política de segurança que permite ao cliente obter um endereço IP antes da autenticação. É um método de autenticação simples em que não é necessário um utilitário cliente ou suplicante. A autenticação da Web pode ser feita localmente em uma WLC ou via servidor RADIUS. A autenticação da Web é usada tipicamente por clientes que desejam implantar uma rede com acesso de convidados.

A autenticação da Web começa quando o controlador intercepta o primeiro pacote TCP HTTP (porta 80) GET do cliente. Para que o navegador da Web do cliente chegue até aqui, o cliente deve primeiro obter um endereço IP e fazer uma tradução do URL para o endereço IP (resolução DNS) do navegador da Web. Isso permite que o navegador da Web saiba qual endereço IP enviar ao HTTP GET.

Quando a autenticação da Web é configurada na WLAN, o controlador bloqueia todo o tráfego (até que o processo de autenticação seja concluído) do cliente, exceto o tráfego DHCP e DNS. Quando o cliente envia o primeiro HTTP GET à porta TCP 80, o controlador redireciona o cliente para https://192.0.2.1/login.html (se este for o IP virtual configurado) para processamento. Esse processo finalmente abre a página da Web de login.

> **Observação**: quando você usa um servidor Web externo para autenticação da Web, as plataformas WLC precisam de uma ACL de pré-autenticação para o servidor Web externo.

Esta seção explica o processo de redirecionamento da autenticação da Web em detalhes.



- Abra o navegador da Web e digite um URL, por exemplo, http://www.site.com. O cliente envia uma solicitação DNS para esse URL a fim de obter o IP de destino. A WLC passa a solicitação DNS ao servidor DNS e o servidor DNS responde com uma resposta DNS, que contém o endereço IP do www.site.com de destino, que por sua vez é encaminhado aos clientes sem fio.
- Então, o cliente tenta então estabelecer uma conexão TCP com o endereço IP de destino. Ele envia um pacote TCP SYN destinado ao endereço IP do www.site.com.
- O WLC tem regras configuradas para o cliente e, portanto, pode agir como um proxy para www.site.com. Ele responde enviando um pacote TCP SYN-ACK ao cliente com a fonte como o endereço IP de www.site.com. O cliente envia de volta um pacote TCP ACK para completar o handshake triplo do TCP e a conexão TCP está totalmente estabelecida.
- O cliente envia um pacote HTTP GET destinado a www.site.com. O WLC intercepta esse pacote e o envia para o processamento de redirecionamento. O gateway de aplicativo HTTP prepara um corpo HTML e o envia de volta como resposta ao HTTP GET solicitado pelo cliente. Esse HTML leva o cliente ao URL padrão da página da Web do WLC, por exemplo, http://<Virtual-Server-IP>/login.html.
- O cliente fecha a conexão TCP com o endereço IP, por exemplo, www.site.com.
- Agora o cliente quer ir para http://<virtualip>/login.html e tentar abrir uma conexão TCP com o endereço IP virtual do WLC. Ele envia um pacote TCP SYN para 192.0.2.1 (que é nosso IP virtual aqui) para a WLC.
- O WLC responde com um TCP SYN-ACK, e o cliente envia de volta um TCP ACK ao WLC para concluir o handshake.
- O cliente envia um HTTP GET para /login.html destinado a 192.0.2.1 para solicitar a página de login.
- Essa solicitação é permitida até o servidor Web da WLC e o servidor responde com a página de login padrão. O cliente recebe a página de login na janela do navegador, e é permitido ao usuário fazer o login.

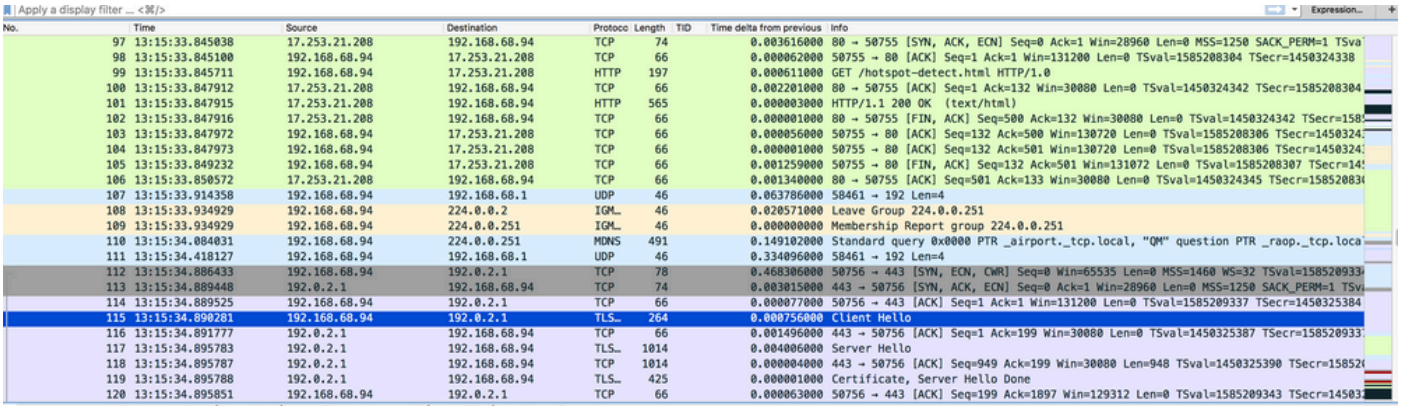
Neste exemplo, o endereço IP do cliente é 192.168.68.94. O cliente resolveu o URL para o servidor Web acessado, 10.1.0.13. Como você pode ver, o cliente fez o handshake triplo para

inicializar a conexão TCP e enviou um pacote HTTP GET que começou com o pacote 96 (00 é o pacote HTTP). Isso não foi acionado pelo usuário, mas foi o sistema operacional que acionou a detecção automática do portal (como podemos adivinhar no URL solicitado). O controlador intercepta os pacotes e responde com o código 200. O pacote de código 200 tem uma URL de redirecionamento:

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1;
URL=https://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

Em seguida, fecha a conexão TCP através do handshake triplo.

Em seguida, o cliente inicia a conexão HTTPS com a URL de redirecionamento que a envia para 192.0.2.1, que é o endereço IP virtual do controlador. O cliente precisa validar o certificado do servidor ou ignorá-lo para ativar o túnel SSL. Nesse caso, é um certificado autoassinado, de modo que o cliente o ignorou. A página da Web de logon é enviada por meio desse túnel SSL. O pacote 112 inicia as transações.



Você tem a opção de configurar o nome de domínio para o endereço IP virtual do WLC. Se você configurar o nome de domínio para o endereço IP virtual, esse nome de domínio será retornado do controlador no pacote HTTP OK em resposta ao pacote HTTP GET do cliente. Em seguida, é necessário executar uma resolução DNS para esse nome de domínio. Quando obtém um endereço IP da resolução DNS, ele tenta abrir uma sessão TCP com esse endereço IP, que é um endereço IP configurado em uma interface virtual do controlador.

Eventualmente, a página da Web passa pelo túnel para o cliente e o usuário retorna o nome de usuário/senha através do túnel SSL.

A autenticação da Web é executada por um destes três métodos:

- Usar uma página da Web Interna (padrão).
- Use uma página de login personalizada.
- Use uma página de logon de um servidor Web externo.

Notas:
- O pacote de autenticação da Web personalizado tem um limite de até 30 caracteres para nomes de arquivo. Certifique-se de que nenhum nome de arquivo dentro do pacote tenha mais de 30 caracteres.

- A partir da versão 7.0 da WLC, se a autenticação da Web estiver habilitada na WLAN e você também tiver regras de ACL de CPU, as regras de autenticação da Web com base no cliente sempre terão maior precedência, desde que o cliente não seja autenticado no estado WebAuth_Reqd. Quando o cliente entra no estado RUN, as regras da ACL da CPU são aplicadas.

- Portanto, se as ACLs de CPU estiverem habilitadas na WLC, uma regra de permissão para o IP da interface virtual será necessária (em QUALQUER direção) nestas condições:
 - Quando a ACL da CPU não tiver uma regra de permissão TOTAL para ambas as direções.
 - Quando existe uma regra de permissão TOTAL, mas também existe uma regra DENY para a porta 443 ou 80 de precedência mais alta.

- A regra de permissão para o IP virtual deve ser para o protocolo TCP e para a porta 80 se o secureweb estiver desabilitado, ou para a porta 443 se o secureweb estiver habilitado. Isso é necessário para permitir o acesso do cliente ao endereço IP da interface virtual após a autenticação bem-sucedida quando as ACLs da CPU estão em vigor.

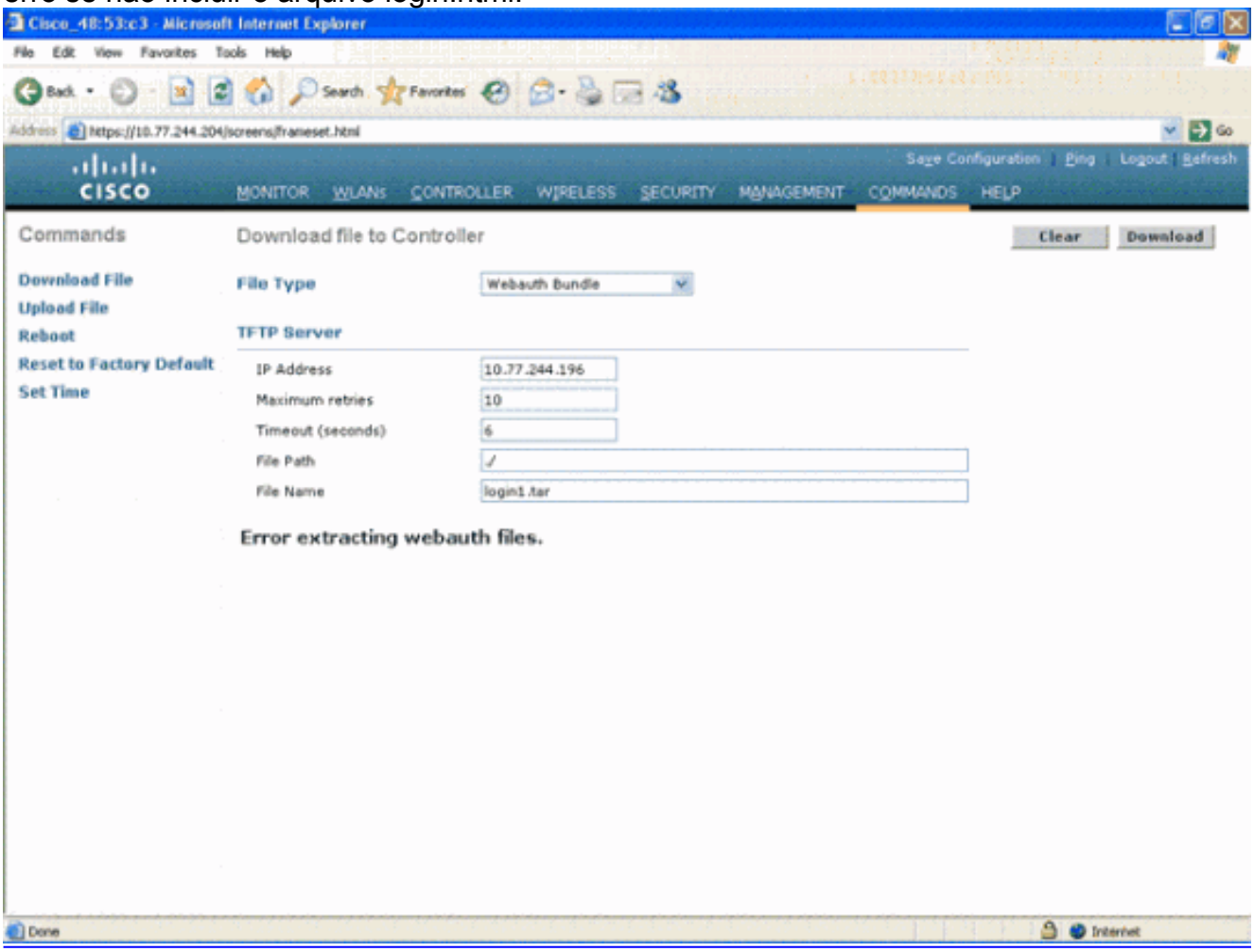
Solução de problemas de autenticação da Web

Depois de configurar a autenticação da Web e se o recurso não funcionar como esperado, conclua estas etapas:

1. Verifique se o cliente obtém um endereço IP. Caso contrário, os usuários podem desmarcar a caixa de seleção **DHCP Required** na WLAN e fornecer ao cliente sem fio um endereço IP estático. Isso pressupõe a associação com o ponto de acesso.
2. A próxima etapa no processo é a resolução DNS do URL no navegador da Web. Quando um cliente WLAN se conecta a uma WLAN configurada para autenticação da Web, o cliente obtém um endereço IP do servidor DHCP. O usuário abre um navegador da Web e insere um endereço de site. Em seguida, o cliente executa a resolução DNS para obter o endereço IP do site. Agora, quando o cliente tenta acessar o site, a WLC intercepta a sessão HTTP GET do cliente e redireciona o usuário para a página de login da autenticação da Web.
3. Portanto, certifique-se de que o cliente seja capaz de executar a resolução DNS para que o redirecionamento funcione. No Microsoft Windows, escolha **Start > Run**, insira **CMD** para abrir uma janela de comando, faça um "nslookup **www.cisco.com**" e veja se o endereço IP retorna. Em Macs/Linux, abra uma janela de terminal e faça um "nslookup www.cisco.com" e veja se o endereço IP retorna.Se você acredita que o cliente não obtém a resolução DNS, você pode:Insira o endereço IP do URL (por exemplo, http://www.cisco.com é http://192.168.219.25).Tente digitar qualquer endereço IP (até mesmo inexistente) que precise ser resolvido através do adaptador sem fio.Quando você digita esse URL, ele exibe a página da Web? Se sim, é mais provável que seja um problema de DNS. Também pode ser um problema de certificado. O controlador, por padrão, usa um certificado autoassinado e a maioria dos navegadores da Web avisa contra seu uso.
4. Para autenticação da Web com uma página da Web personalizada, verifique se o código HTML da página da Web personalizada é apropriado. Você pode baixar um exemplo de script de autenticação da Web em Cisco Software Downloads. Por exemplo, para os controladores 5508, escolha **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN**

Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle e faça download do arquivo **webauth_bundle.zip**.Estes parâmetros são adicionados ao URL quando o navegador de Internet do usuário é redirecionado para a página de login personalizada:ap_mac - O endereço MAC do ponto de acesso ao qual o usuário sem fio está associado.switch_url - A URL do controlador no qual as credenciais do usuário devem ser publicadas.redirect - A URL para a qual o usuário é redirecionado após a autenticação ser bem-sucedida.statusCode - O código de status retornado do servidor de autenticação da Web do controlador.wlan - O SSID da WLAN ao qual o usuário sem fio está associado.Estes são os códigos de status disponíveis:Código de status 1 - "Você já está conectado. Nenhuma outra ação é necessária da sua parte."Código de status 2 - "Você não está configurado para se autenticar no portal da Web. Nenhuma outra ação é necessária da sua parte."Código de status 3 - "O nome de usuário especificado não pode ser usado neste momento. Talvez o nome de usuário já esteja conectado ao sistema?"Código de status 4 - "Você foi excluído."Código de status 5 - "A combinação de Nome de usuário e Senha inserida é inválida. Tente novamente."

5. Todos os arquivos e imagens que precisam aparecer na página da Web personalizada devem ser empacotados em um arquivo .tar antes de serem carregados na WLC. Verifique se um dos arquivos incluídos no pacote .tar é login.html. Você receberá esta mensagem de erro se não incluir o arquivo login.html:



Consulte a seção Diretrizes para Autenticação Personalizada da Web do Exemplo de Configuração de Autenticação da Web de Controlador Wireless LAN para obter mais informações sobre como criar uma janela de autenticação da Web personalizada.**Observação**: arquivos grandes e arquivos com nomes longos podem resultar em um erro de extração. Recomenda-se que as imagens estejam no formato .jpg.

6. Certifique-se de que a opção **Scripting** não esteja bloqueada no navegador do cliente, pois a página da Web personalizada na WLC é basicamente um script HTML.
7. Se você tiver um **nome de host** configurado para a **interface virtual** do WLC, certifique-se de que a resolução DNS esteja disponível para o nome de host da interface virtual.
   Observação: navegue até o menu **Controller > Interfaces** na GUI da WLC para atribuir um **nome de host DNS** à interface virtual.
8. Algumas vezes, firewall instalado no computador cliente bloqueia a página de login da autenticação da Web. Desabilite o firewall antes de tentar alcançar a página de login. O firewall poderá ser habilitado outra vez assim que a autenticação da Web for concluída.
9. O firewall da topologia/solução pode ser colocado entre o cliente e o servidor de autenticação da Web, que depende da rede. Como para cada projeto/solução de rede implementada, o usuário final deve certificar-se de que essas portas sejam permitidas no firewall da rede.

10. Para que a autenticação da Web ocorra, o cliente deve primeiro associar-se à WLAN apropriada na WLC. Navegue para o menu **Monitor > Clients** na GUI da WLC para ver se o cliente está associado à WLC. Verifique se o cliente tem um endereço IP válido.
11. Desabilite as configurações de proxy no navegador do cliente até que a autenticação da Web seja concluída.
12. O método de autenticação da Web padrão é o PAP (Password Authentication Protocol Protocolo de Autenticação de Senha). Certifique-se de que a autenticação PAP seja permitida no servidor RADIUS para que isso funcione. Para verificar o status da autenticação do cliente, verifique as depurações e as mensagens de log do servidor RADIUS. Você pode usar o comando **debug aaa all** no WLC para visualizar as depurações do servidor RADIUS.
13. Atualize o driver de hardware no computador para o código mais recente do site do fabricante.
14. Verifique as configurações no suplicante (programa no laptop).
15. Quando você usa o suplicante Windows Zero Config incorporado ao Windows: Verifique se o usuário tem os patches mais recentes instalados.Execute depurações no suplicante.
16. No cliente, ative os logs EAPOL (WPA+WPA2) e RASTLS a partir de uma janela de comando. Escolha **Start > Run > CMD**:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    Para desabilitar os logs, execute o mesmo comando, mas substitua enable por disable. Para o XP, todos os logs podem estar localizados em C:\Windows\tracing.
17. Se você ainda não tiver uma página da Web de logon, colete e analise essa saída de um único cliente:
    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
18. Se o problema não for resolvido depois que você concluir essas etapas, colete essas depurações e use o Support Case Manager para abrir uma solicitação de serviço.
    ```
    debug pm ssh-appgw enable
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

Informações Relacionadas

- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.