Entender a autenticação da Web em controladoras Wireless LAN (WLC)

Contents

Introduction

Este documento descreve os processos de autenticação da Web em controladoras Wireless LAN (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico da configuração da WLC.

Componentes Utilizados

As informações neste documento são baseadas em todos os modelos de hardware de WLC.

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.

Processos internos de autenticação da Web

Posição da autenticação da Web como um recurso de segurança

A autenticação da Web (WebAuth) é a segurança da camada 3. Ele permite uma segurança de fácil utilização que funciona em qualquer estação que execute um navegador.

Ele pode ser combinado com qualquer segurança de chave pré-compartilhada (PSK) (política de segurança da camada 2).

Embora a combinação de WebAuth e PSK reduza a parte amigável, ela tem a vantagem de criptografar o tráfego do cliente.

WebAuth é um método de autenticação sem criptografia.

O WebAuth não pode ser configurado com 802.1x/RADIUS (Remote Authentication Dial-In User Service) até que o Software WLC Versão 7.4 seja instalado e configurado simultaneamente.

Os clientes devem passar por dot1x e autenticação da Web. Destina-se à adição de um portal da Web para funcionários (que usam 802.1x), não convidados.

Não há um identificador de conjunto de serviços (SSID) completo para dot1x para funcionários ou portal da Web para convidados.

Como funciona o WebAuth

O processo de autenticação do 802.11 está aberto, portanto, você pode se autenticar e se associar sem problemas. Depois disso, você estará associado, mas não na WLC **RUN** estado.

Com a autenticação da Web ativada, você é mantido em **WEBAUTH_REQD** onde você não pode acessar nenhum recurso da rede.

Você deve receber um endereço IP DHCP com o endereço do servidor DNS nas opções.

Digite uma URL válida no navegador. O cliente resolve o URL através do protocolo DNS. Em seguida, o cliente envia sua solicitação HTTP ao endereço IP do site.

A WLC intercepta essa solicitação e retorna o comando **webauth** página de login, que imita o

endereço IP do site. Com um WebAuth externo, a WLC responde com uma resposta HTTP que inclui o endereço IP do seu site e declara que a página foi movida.

A página foi movida para o servidor Web externo usado pela WLC. Ao ser autenticado, você obtém acesso a todos os recursos da rede e é redirecionado para o URL originalmente solicitado por padrão (a menos que um redirecionamento forçado tenha sido configurado no WLC).

Em resumo, a WLC permite que o cliente resolva o DNS e obtenha um endereço IP automaticamente no **WEBAUTH_REQD** estado.

Para observar outra porta em vez da porta 80, use **config network web-auth-port** para criar um redirecionamento nessa porta também.

Um exemplo é a interface da Web do Access Control Server (ACS), que está na porta 2002 ou em outros aplicativos semelhantes.

> **Observação sobre o redirecionamento de HTTPS**: Por padrão, a WLC não redirecionou o tráfego HTTPS. Isso significa que se você digitar um endereço HTTPS no navegador, nada acontecerá. Você deve digitar um endereço HTTP para ser redirecionado à página de logon fornecida em HTTPS.
>
> Na versão 8.0 e posterior, você pode habilitar o redirecionamento do tráfego HTTPS com o comando CLI **config network web-auth https-redirect enable.**
>
> Isso usa muitos recursos para a WLC nos casos em que muitas solicitações HTTPS são enviadas. Não é aconselhável usar esse recurso antes da versão 8.7 da WLC, onde a escalabilidade desse recurso foi melhorada. Observe também que um aviso de certificado é inevitável nesse caso. Se o cliente solicitar qualquer URL (como https://www.cisco.com), a WLC ainda apresentará seu próprio certificado emitido para o endereço IP da interface virtual. Isso nunca corresponde ao endereço URL/IP solicitado pelo cliente e o certificado não é confiável, a menos que o cliente force a exceção em seu navegador.

Queda indicativa de desempenho da versão do software WLC antes da 8.7 medida:

Webauth	Taxa alcançada
3 URLs - HTTP	140/segundo
1ª URL - HTTP 2ª e 3ª URLs - HTTPS	20/segundo
3 URLs - HTTPS (implantação grande)	<1/segundo
3 URLs - HTTPS (máx. de 100 clientes)	10/segundo

Nesta tabela de desempenho, os 3 URLs são referidos como:

- A URL original inserida pelo usuário final
- A URL para a qual a WLC redireciona o navegador
- O envio final de credenciais

A tabela de desempenho fornece o desempenho da WLC no caso de todos os 3 URLs serem HTTP, no caso de todos os 3 URLs serem HTTPS ou se o cliente se mover de HTTP para HTTPS (típico).

Como fazer um WebAuth interno (local) funcionar com uma

página interna

Para configurar uma WLAN com uma interface dinâmica operacional, os clientes também recebem um endereço IP do servidor DNS através do DHCP.

Antes de qualquer **webauth** , estiver definido, verificar se a WLAN está funcionando corretamente, se as solicitações DNS podem ser resolvidas (**nslookup**) e as páginas da Web podem ser navegadas.

Defina a autenticação da Web como recursos de segurança da camada 3. Crie usuários no banco de dados local ou em um servidor RADIUS externo.

Consulte o documento Exemplo de Configuração de Autenticação da Web da Controladora Wireless LAN.

Como configurar uma WebAuth local personalizada com página personalizada

Personalizado **webauth** pode ser configurado com **redirectUrl** nos **Security** guia. Isso força um redirecionamento para uma página da Web específica que você digita.

Quando o usuário é autenticado, ele substitui a URL original solicitada pelo cliente e exibe a página para a qual o redirecionamento foi atribuído.

O recurso personalizado permite usar uma página HTML personalizada em vez da página de logon padrão. Carregue seu pacote de arquivos html e de imagem no controlador.

Na página de upload, procure **webauth bundle** em um formato tar. O PicoZip cria alcatrões que funcionam de forma compatível com a WLC.

Para obter um exemplo de um pacote WebAuth, consulte a página Download Software for Wireless Controller WebAuth Bundles. Selecione a versão apropriada para sua WLC.

Érecomendável personalizar um pacote existente; não crie um novo pacote.

Há algumas limitações com **custom webauth** que variam com versões e bugs.

- o tamanho do arquivo .tar (não mais que 5 MB)
- o número de arquivos no .tar
- o comprimento do nome de arquivo dos arquivos (não mais de 30 caracteres)

Se o pacote não funcionar, tente um pacote personalizado simples. Adicione individualmente arquivos e complexidade para acessar o pacote que o usuário tentou usar. Isso ajuda a identificar o problema.

Para configurar uma página personalizada, consulte Criação de uma Página de Login de Autenticação da Web Personalizada, uma seção no Guia de Configuração da Cisco Wireless LAN Controller Release 7.6.

Substituir Técnica de Configuração Global

Configure com o comando **override global config** e defina um tipo WebAuth para cada WLAN. Isso permite uma WebAuth interna/padrão com uma WebAuth interna/padrão personalizada para outra WLAN.

Isso permite a configuração de diferentes páginas personalizadas para cada WLAN.

Combine todas as páginas no mesmo pacote e carregue-as na WLC.

Defina sua página personalizada com o comando **override global config** em cada WLAN e selecione qual arquivo é a página de login de todos os arquivos dentro do pacote.

Escolha uma página de login diferente dentro do pacote para cada WLAN.

Problema de Redirecionamento

Há uma variável no pacote HTML que permite o redirecionamento. Não coloque sua URL de redirecionamento forçado lá.

Para problemas de redirecionamento no WebAuth personalizado, a Cisco recomenda verificar o pacote.

Se você inserir um URL de redirecionamento com **+=** na GUI da WLC, isso poderá substituir *ou* adicionar ao URL definido dentro do pacote.

Por exemplo, na GUI da WLC, a **redirectURL** é definido como www.cisco.com; no entanto, no pacote ele mostra: **redirectURL+=** '(URL do site)'. O comando **+=** redireciona os usuários para um URL inválido.

Como fazer uma autenticação da Web externa (local) funcionar com uma página externa

A utilização de um servidor WebAuth externo é apenas um repositório externo para a página de login. As credenciais do usuário ainda são autenticadas pela WLC. O servidor Web externo permite apenas uma página de login especial ou diferente.

Etapas executadas para uma WebAuth externa:

1. O cliente (usuário final) abre um navegador da Web e insere um URL.

2. Se o cliente não for autenticado e a autenticação da Web externa for usada, a WLC redirecionará o usuário para a URL do servidor Web externo. A WLC envia um redirecionamento HTTP ao cliente com o endereço IP copiado e aponta para o endereço IP do servidor externo. A URL de logon de autenticação da Web externa é anexada a parâmetros como **AP_Mac_Address**,o **client_url** (endereço URL do cliente) e a **action_URL** necessário para entrar em contato com o servidor Web do switch.

3. A URL externa do servidor Web envia o usuário a uma página de logon. O usuário pode usar uma lista de controle de acesso (ACL) de pré-autenticação para acessar o servidor.

4. A página de login envia a solicitação de credenciais do usuário de volta ao **action_URL**como http://192.0.2.1/login.html, do servidor Web da WLC. Isso é fornecido como um parâmetro de entrada para o URL de redirecionamento, onde 192.0.2.1 é o endereço da interface virtual no switch.

5. O servidor Web da WLC envia o nome de usuário e a senha para autenticação.

6. A WLC inicia a solicitação do servidor RADIUS ou usa o banco de dados local na WLC e, em seguida, autentica o usuário.

7. Se a autenticação for bem-sucedida, o servidor Web da WLC encaminha o usuário para a URL de redirecionamento configurada ou para a URL inserida pelo cliente.

8. Se a autenticação falhar, o servidor Web da WLC redirecionará o usuário de volta ao URL de login do usuário.

   Observação : usamos 192.0.2.1 como um exemplo de ip virtual neste documento. O intervalo 192.0.2.x é recomendado para uso com ip virtual, pois não é roteável. Documentação mais antiga possivelmente se refere a "1.1.1.x" ou ainda é o que está configurado em sua WLC como esta costumava ser a configuração padrão. No entanto, observe que esse ip agora é um endereço ip roteável válido e, portanto, a sub-rede 192.0.2.x é recomendada.

Se os access points (APs) estiverem no modo FlexConnect, um **preauth** A ACL é irrelevante. As ACLs flexíveis podem ser usadas para permitir acesso ao servidor Web para clientes que não foram autenticados.

Consulte o Exemplo de Configuração de Autenticação Externa da Web com Controladoras Wireless LAN.

Passagem da Web

A passagem da Web é uma variação da autenticação da Web interna. Ele exibe uma página com uma advertência ou uma instrução de alerta, mas não solicita credenciais.

O usuário clica em **ok**. Habilite a entrada de e-mail e o usuário pode inserir seu endereço de e-mail que se torna seu nome de usuário.

Quando o usuário estiver conectado, verifique sua lista de clientes ativos e se o usuário está listado com o endereço de e-mail que ele inseriu como o nome de usuário.

Para obter mais informações, consulte o Exemplo de Configuração de Passagem da Web do Wireless LAN Controller 5760/3850.

Redirecionamento Condicional da Web

Se você habilitar um redirecionamento da Web condicional, o usuário será redirecionado condicionalmente para uma página da Web específica após a autenticação 802.1x ter sido concluída com êxito.

Você pode especificar a página e as condições de redirecionamento sob as quais o redirecionamento ocorre em seu servidor RADIUS.

As condições podem incluir a senha quando ela atingir a data de expiração ou quando o usuário precisar pagar uma conta pelo uso/acesso contínuo.

Se o servidor RADIUS retornar o par AV Cisco **url-redirect**, o usuário será redirecionado para a URL especificada quando abrir um navegador.

Se o servidor também retornar o par Cisco AV **url-redirect-acl**, a ACL especificada será instalada como uma ACL de pré-autenticação para este cliente.

O cliente não é considerado totalmente autorizado neste ponto e só pode passar o tráfego permitido pela ACL de pré-autenticação. Depois que o cliente conclui uma operação específica no URL especificado (por exemplo, uma alteração de senha ou pagamento de conta), o cliente deve autenticar novamente.

Quando o servidor RADIUS não retorna um **url-redirect**, o cliente é considerado totalmente autorizado e tem permissão para passar o tráfego.

> **Note**: O recurso de redirecionamento condicional da Web está disponível apenas para WLANs configuradas para segurança 802.1x ou WPA+WPA2 da camada 2.

Após a configuração do servidor RADIUS, configure o redirecionamento da Web condicional no controlador com a GUI ou CLI do controlador. Consulte estes guias passo a passo: Configuração do Web Redirect (GUI) e Configuração do Web Redirect (CLI).

Redirecionamento da Web para Página Inicial

Se você habilitar o redirecionamento da Web da página inicial, o usuário será redirecionado para uma página da Web específica após a autenticação 802.1x ter sido concluída com êxito. Após o redirecionamento, o usuário tem acesso total à rede.

Você pode especificar a página de redirecionamento em seu servidor RADIUS. Se o servidor RADIUS retornar o par AV Cisco **url-redirect**, o usuário será redirecionado para a URL especificada quando abrir um navegador.

O cliente é considerado totalmente autorizado neste ponto e tem permissão para passar tráfego, mesmo que o servidor RADIUS não retorne um **url-redirect**.

> **Note**: O recurso de redirecionamento da página inicial está disponível apenas para WLANs configuradas para segurança da camada 2 802.1x ou WPA+WPA2.

Após a configuração do servidor RADIUS, configure o redirecionamento da Web da página inicial no controlador com a GUI ou CLI do controlador.

Falha de WebAuth no Filtro MAC

Um WebAuth on MAC Filter FaFailure exige que você configure filtros MAC no menu de

segurança da Camada 2.

Se os usuários forem validados com êxito com seus endereços MAC, eles irão diretamente para o **run** estado.

Se não estiverem, eles vão para a **WEBAUTH_REQD** e a autenticação da Web normal ocorre.

> **Note**: Isso não é suportado com a passagem da Web.Para obter mais informações, siga a atividade na solicitação de aprimoramento ID do Cisco Bug CSCtw73512

Autenticação da Web Central

A Autenticação Central da Web se refere a um cenário em que a WLC não hospeda mais nenhum serviço. O cliente é enviado diretamente ao portal da Web do ISE e não passa por 192.0.2.1 no WLC. A página de login e todo o portal são externalizados.

A Autenticação da Web Central ocorre quando o Network Admission Control (NAC) RADIUS está habilitado nas configurações avançadas dos filtros WLAN e MAC.

A WLC envia uma autenticação RADIUS (geralmente para o filtro MAC) ao ISE, que responde com o comando **redirect-url** par de valor de atributo (AV).

O usuário é colocado em **POSTURE_REQD** até que o ISE dê a autorização com uma solicitação de alteração de autorização (CoA). O mesmo cenário acontece em Posture ou WebAuth Central.

A WebAuth central não é compatível com WPA-Enterprise/802.1x porque o portal do convidado não pode retornar chaves de sessão para criptografia como faz com o EAP (Extensible Authentication Protocol).

Autenticação de Usuário Externo (RADIUS)

A Autenticação de Usuário Externo (RADIUS) só é válida para WebAuth Local quando a WLC manipula as credenciais ou quando uma política da Web de Camada 3 está habilitada. Autentique usuários localmente ou na WLC ou externamente via RADIUS.

Há uma ordem na qual a WLC verifica as credenciais do usuário.

1. Em todo o caso, procura primeiro no seu próprio banco de dados.
2. Se ele não encontrar os usuários, ele irá para o servidor RADIUS configurado na WLAN convidada (se houver um configurado).
3. Em seguida, ele verifica a lista global de servidores RADIUS em relação aos servidores RADIUS onde **network user** está marcado.

Esse terceiro ponto responde à pergunta daqueles que não configuram o RADIUS para essa WLAN, mas observe que ele ainda verifica o RADIUS quando o usuário não é encontrado na controladora.

Isso porque **network user** é verificado em relação aos servidores RADIUS na lista global.

A WLC pode autenticar usuários para o servidor RADIUS com o Password Authentication

Protocol (PAP), o Challenge Handshake Authentication Protocol (CHAP) ou o EAP-MD5 (Message Digest5).

Esse é um parâmetro global e pode ser configurado na GUI ou CLI:

Da GUI: navegue até **Controller > Web RADIUS Authentication**

Do CLI: insira **config custom-web RADIUSauth**

> **Nota**:O servidor convidado NAC usa apenas PAP.

Como configurar uma WLAN de convidado com fio

Uma configuração de WLAN de convidado com fio é semelhante à configuração de convidado sem fio. Ele pode ser configurado com um ou dois controladores (somente se um for de ancoragem automática).

Escolha uma VLAN como a VLAN para usuários convidados com fio, por exemplo, na VLAN 50. Quando um convidado com fio deseja acessar a Internet, conecte o laptop a uma porta em um switch configurado para a VLAN 50.

Essa VLAN 50 deve ser permitida e estar presente no caminho através da porta de tronco da WLC.

Em um caso de duas WLCs (uma âncora e uma externa), essa VLAN convidada com fio deve levar à WLC externa (chamada WLC1) e não à âncora.

A WLC1 então cuida do túnel de tráfego para a WLC DMZ (a âncora, chamada WLC2), que libera o tráfego na rede roteada.

Estas são as cinco etapas para configurar o acesso de convidado com fio:

1. **Configure uma interface dinâmica (VLAN) para acesso de usuário convidado com fio.**

   No WLC1, crie uma interface dinâmica VLAN50. No **interface configuration** , marque a caixa de seleção **Guest LAN** caixa. Em seguida, campos como **IP address** e **gateway** desaparecer. A WLC precisa reconhecer que o tráfego é roteado da VLAN 50. Esses clientes são convidados com fio.

2. **Crie uma LAN com fio para acesso de usuário convidado.**

   Em um controlador, uma interface é usada quando associada a uma WLAN. Em seguida, crie uma WLAN nos controladores da matriz. Navegue até **WLANs** e clique em **New**. IN **WLAN Type**, escolha **Guest LAN**.

   Em **Profile Name** e **WLAN SSID**, digite um nome que identifique essa WLAN. Esses nomes podem ser diferentes, mas não podem conter espaços. O termo WLAN é usado, mas esse perfil de rede não está relacionado ao perfil de rede sem fio.

O **General** oferece duas listas suspensas: **Ingress** e **Egress**. Ingress é a VLAN de onde vêm os usuários (VLAN 50); A saída é a VLAN para a qual você as envia.

Para **Ingress**, escolha **VLAN50**.

Para **Egress**, é diferente. Se você tiver apenas um controlador, crie outra interface dinâmica, um **standard** uma desta vez (não uma LAN de convidado) e enviar usuários com fio para esta interface. Nesse caso, envie-os ao controlador DMZ. Por conseguinte, **Egress** , escolha a **Management Interface**.

O **Security** para esta LAN de convidado "WLAN" é WebAuth, o que é aceitável. Clique em **Ok** para validar.

3. Configure o controlador externo (sede).

Nos **WLAN list**, clique em **Mobility Anchor** no final do **Guest LAN** e selecione seu controlador DMZ. Presume-se aqui que ambos os controladores se reconhecem. Caso contrário, vá para **Controller** > **Mobility Management** > **Mobility group**e adicione DMZWLC em WLC1. Em seguida, adicione WLC1 em DMZ. Os dois controladores não devem estar no mesmo grupo de mobilidade. Caso contrário, as regras básicas de segurança serão violadas.

4. Configure o controlador âncora (o controlador DMZ).

O controlador do escritório principal está pronto. Agora prepare o controlador DMZ. Abra uma sessão do navegador da Web para o controlador DMZ e navegue para WLANs. Crie uma nova WLAN. IN **WLAN Type**, escolha **Guest LAN**.

IN **Profile Name** e **WLAN SSID**, digite um nome que identifique esta WLAN. Use os mesmos valores inseridos no controlador do escritório principal.

O **Ingress** aqui é **None**. Não importa porque o tráfego é recebido através do túnel Ethernet sobre IP (EoIP). Não é necessário especificar nenhuma interface de entrada.

O **Egress** é para onde os clientes devem ser enviados. Por exemplo, o **DMZ VLAN** é a VLAN 9. Crie uma interface dinâmica padrão para a VLAN 9 no DMZWLC e escolha **VLAN 9** como a interface de saída.

Configure a extremidade do túnel do Âncora de mobilidade. Na lista WLAN, escolha **Mobility Anchor for Guest LAN**. Envie o tráfego para a controladora local, DMZWLC. As duas extremidades estão prontas agora.

5. Ajuste a LAN convidada.

Você também pode ajustar as configurações de WLAN em ambas as extremidades. As configurações devem ser idênticas em ambas as extremidades. Por exemplo, se você clicar no botão **WLAN Advanced** , **Allow AAA override** em WLC1, marque a mesma caixa em DMZWLC. Se houver diferenças na WLAN em ambos os lados, o túnel será interrompido. DMZWLC recusa o tráfego; você pode ver quando **run debug mobility**.

Lembre-se de que todos os valores são realmente obtidos do DMZWLC: Endereços IP, valores de VLAN e assim por diante. Configure o lado WLC1 de forma idêntica, para que ele transmita a solicitação para a WLCDMZ.

Certificados para a Página de Login

Esta seção fornece os processos para colocar seu próprio certificado na página WebAuth ou para ocultar o URL WebAuth 192.0.2.1 e exibir um URL nomeado.

Carregar um Certificado para a Autenticação da Web do Controlador

Através da GUI (**WebAuth** > **Certificate**) ou CLI (tipo de transferência **webauthcert**), você pode carregar um certificado no controlador.

Seja um certificado criado com sua autoridade de certificação (CA) ou um certificado oficial de terceiros, ele deve estar no formato .pem.

Antes de enviar, você também deve inserir a chave do certificado.

Após o upload, uma reinicialização é necessária para que o certificado esteja em vigor. Uma vez reinicializado, vá para a página do certificado WebAuth na GUI para encontrar os detalhes do certificado carregado (validade e assim por diante).

O campo importante é o nome comum (CN), que é o nome emitido para o certificado. Este campo é discutido neste documento na seção "Autoridade de certificação e outros certificados no controlador".

Após reinicializar e verificar os detalhes do certificado, você verá o novo certificado do controlador na página de login do WebAuth. No entanto, pode haver duas situações.

1. Se o seu certificado foi emitido por uma das poucas CAs raiz principais em que todo computador confia, então não há problema. Um exemplo é o VeriSign, mas você geralmente é assinado por uma sub-CA Verisign e não pela CA raiz. Você pode verificar o armazenamento de certificados do seu navegador se vir que a CA mencionada nele é confiável.

2. Se você recebeu o certificado de uma empresa/CA menor, nem todos os computadores confiam neles. Forneça também o certificado da empresa/CA ao cliente e uma das CAs raiz emitirá esse certificado. Eventualmente, você terá uma cadeia como "O certificado foi emitido pela CA x > O certificado da CA x foi emitido pela CA y > O certificado da CA y foi emitido por esta CA raiz confiável". O objetivo final é atingir uma CA na qual o cliente confia.

Autoridade de certificação e outros certificados no controlador

Para eliminar o aviso "este certificado não é confiável", insira o certificado da CA que emitiu o certificado do controlador no controlador.

Em seguida, o controlador apresenta os dois certificados (o certificado do controlador e seu

certificado CA). O certificado CA deve ser uma CA confiável ou ter os recursos para verificar a CA. Você pode criar uma cadeia de certificados CA que levam a uma CA confiável.

Coloque toda a cadeia no mesmo arquivo. O arquivo então contém conteúdo como este exemplo:

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

Como fazer com que o certificado corresponda ao URL

A URL WebAuth é definida como 192.0.2.1 para se autenticar e o certificado é emitido (esse é o campo CN do certificado WLC).

Para alterar a URL WebAuth para 'myWLC.com', por exemplo, vá para a **virtual interface configuration** (a interface 192.0.2.1) e você pode inserir um **virtual DNS hostname**, como myWLC.com.

Isso substitui o 192.0.2.1 na barra de URL. Esse nome também deve ser resolvível. O farejador de rastreamento mostra como tudo funciona, mas quando a WLC envia a página de login, a WLC mostra o endereço myWLC.com e o cliente resolve esse nome com seu DNS.

Esse nome deve ser resolvido como 192.0.2.1. Isso significa que se você também usar um nome para o gerenciamento da WLC, use um nome diferente para WebAuth.

Se você usar myWLC.com mapeado para o endereço IP de gerenciamento da WLC, deverá usar um nome diferente para o WebAuth, como myWLCwebauth.com.

Solucionar problemas de certificado

Esta seção explica como e o que verificar para solucionar problemas de certificado.

Como verificar

Baixe o OpenSSL (para Windows, procure por OpenSSL Win32) e instale-o. Sem qualquer configuração, você pode ir no diretório bin e tentar **openssl s_client –connect (your web auth URL):443**,

se este URL for o URL no qual sua página WebAuth está vinculada ao DNS, consulte "O que verificar" na próxima seção deste documento.

Se seus certificados usarem uma CA privada, coloque o certificado de CA raiz em um diretório em uma máquina local e use a opção openssl **-CApath**. Se você tiver uma CA intermediária, coloque-a no mesmo diretório também.

Para obter informações gerais sobre o certificado e verificá-lo, use:

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Também é útil converter certificados com o uso de openssl:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

O que deve ser verificado?

Você pode ver quais certificados são enviados ao cliente quando ele se conecta. Leia o certificado do dispositivo — o CN deve ser o URL onde a página da Web pode ser acessada.

Leia a linha "emitido por" do certificado do dispositivo. Ele deve corresponder ao CN do segundo certificado. Esse segundo certificado, "emitido por", deve corresponder ao CN do próximo certificado e assim por diante. Caso contrário, não faz uma cadeia real.

Na saída do OpenSSL mostrada aqui, observe que **openssl** O não pode verificar o certificado do dispositivo porque seu "emitido por" não corresponde ao nome do certificado de CA fornecido.

Saída SSL

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

Outro problema possível é que o certificado não pode ser carregado para o controlador. Nesta situação, não há questão de validade, CA, etc.

Para verificar isso, verifique a conectividade do TFTP (Trivial File Transfer Protocol) e tente

transferir um arquivo de configuração. Se você inserir o comando **debug transfer all enable** observe que o problema é a instalação do certificado.

Isso pode ocorrer devido à chave incorreta usada com o certificado. Também pode ser que o certificado esteja em um formato incorreto ou corrompido.

A Cisco recomenda que você compare o conteúdo do certificado com um certificado válido e conhecido. Isso permite ver se um **LocalkeyID** o atributo mostra todos os 0s (já aconteceu). Em caso afirmativo, o certificado deve ser reconvertido.

Há dois comandos com o OpenSSL que permitem retornar de .pem para .p12 e reemitir um .pem com a chave de sua escolha.

Se você recebeu um .pem que contém um certificado seguido de uma chave, copie/cole a parte da chave: **----BEGIN KEY ---- until ------- END KEY ------** do .pem para "key.pem".

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? Você será avisado com uma tecla; insira **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** Isso resulta em um .pem operacional com a senha **check123.**

Outras situações para solucionar problemas

Embora a **âncora de mobilidade** não tenha sido discutida neste documento, se você estiver em uma situação de **convidado ancorado**, verifique se a troca de mobilidade ocorre corretamente e se você vê o cliente chegar na âncora.

Quaisquer outros problemas de WebAuth precisam ser solucionados na âncora.

Aqui estão alguns problemas comuns que você pode solucionar:

- **Os usuários não podem se associar à WLAN de convidado**.

  Isso não está relacionado a WebAuth. Verifique a configuração do cliente, as configurações de segurança na WLAN, se ela estiver habilitada, se os rádios estão ativos e operacionais e assim por diante.

- **Os usuários não obtêm endereço IP**.

  Em uma situação de âncora de convidado, isso ocorre com mais frequência porque o estrangeiro e a âncora não foram configurados exatamente da mesma forma. Caso contrário, verifique a configuração DHCP, a conectividade e assim por diante.
- Confirme se outras WLANs podem ou não usar o mesmo servidor DHCP sem problemas. Isso ainda não está relacionado a WebAuth.

- **O usuário não é redirecionado para a página de logon**.

  Esse é o sintoma mais comum, mas é mais preciso. Há dois cenários possíveis.

O usuário não é redirecionado (o usuário digita uma URL e nunca acessa a página WebAuth). Para esta situação, verifique:

que um servidor DNS válido foi atribuído ao cliente via DHCP (**ipconfig /all**),

que o DNS pode ser acessado do cliente (**nslookup (website URL**),

que o usuário inseriu uma URL válida para ser redirecionado,

que o usuário entrou em um URL HTTP na porta 80 (por exemplo, para acessar um ACS com http://localhost:2002 não o redireciona desde que você enviou na porta 2002 em vez de 80).

O usuário é redirecionado para 192.0.2.1 corretamente, mas a própria página não é exibida.

Essa situação é provavelmente um problema de WLC (bug) ou um problema do lado do cliente. Pode ser que o cliente tenha algum firewall, software ou bloqueio de política. Também pode ser que tenham configurado um proxy em seu navegador da Web.

Recomendação: Use um farejador de rastreamento no PC cliente. Não há necessidade de um software sem fio especial, apenas o Wireshark, que é executado no adaptador sem fio e mostra se a WLC responde e tenta redirecionar. Você tem duas possibilidades: não há resposta da WLC ou algo está errado com o handshake SSL para a página WebAuth. Para problemas de handshake SSL, você pode verificar se o navegador do usuário permite SSLv3 (alguns só permitem SSLv2) e se ele é muito agressivo na verificação de certificado.

Éuma etapa comum inserir manualmente http://192.0.2.1 para verificar se a página da Web aparece sem DNS. Na verdade, você pode digitar http://10.0.0.0 e obter o mesmo efeito. A WLC redireciona qualquer endereço IP que você digitar. Portanto, se você digitar http://192.0.2.1, isso não fará você trabalhar no redirecionamento da Web. Se você digitar https://192.0.2.1(secure), isso não funcionará porque o WLC não redireciona o tráfego HTTPS (por padrão, isso é realmente possível na versão 8.0 e posterior). A melhor maneira de carregar a página diretamente sem um redirecionamento é digitar https://192.0.2.1/login.html.

- **Os usuários não podem se autenticar**.

  Consulte a seção deste documento que discute a autenticação. Verifique as credenciais localmente no RADIUS.

- **Os usuários podem autenticar-se com êxito através do WebAuth, mas depois não têm acesso à Internet**.

  Você pode remover WebAuth da segurança da WLAN e depois ter uma WLAN aberta. Você pode tentar acessar a Web, o DNS e assim por diante. Se você também tiver problemas, remova as configurações de WebAuth e verifique a configuração das interfaces.

Para obter mais informações, consulte: Troubleshooting de Autenticação da Web em um Wireless

LAN Controller (WLC).

Servidor proxy HTTP e como funciona

Você pode usar um servidor proxy HTTP. Se você precisar que o cliente adicione uma exceção em seu navegador de que 192.0.2.1 não deve passar pelo servidor proxy, você pode fazer o WLC ouvir o tráfego HTTP na porta do servidor proxy (geralmente 8080).

Para entender esse cenário, você precisa saber o que um proxy HTTP faz. É algo que você configura no lado do cliente (endereço IP e porta) no navegador.

O cenário comum quando um usuário visita um site é resolver o nome para IP com DNS e, em seguida, solicitar a página da Web ao servidor da Web. O processo sempre envia a solicitação HTTP para a página ao proxy.

O proxy processa o DNS, se necessário, e encaminha para o servidor Web (se a página já não estiver armazenada em cache no proxy). A discussão é somente entre cliente e proxy. Se o proxy obtém ou não a página Web real é irrelevante para o cliente.

Este é o processo de autenticação da Web:

- O usuário digita em um URL.
- O PC cliente envia ao servidor Proxy.
- A WLC intercepta e imita o IP do servidor proxy; ele responde ao PC com um redirecionamento para 192.0.2.1

Nesse estágio, se o PC não estiver configurado para ele, ele solicitará a página 192.0.2.1 WebAuth ao proxy para que não funcione. O PC deve fazer uma exceção para 192.0.2.1; em seguida, ele envia uma solicitação HTTP para 192.0.2.1 e continua com WebAuth.

Quando autenticadas, todas as comunicações passam pelo proxy novamente. Uma configuração de exceção geralmente está no navegador próximo à configuração do servidor proxy. Em seguida, você verá a mensagem: "Não use proxy para esses endereços IP".

Com o WLC versão 7.0 e posterior, o recurso **webauth proxy redirect** pode ser ativado nas opções de configuração global da WLC.

Quando ativada, a WLC verifica se os clientes estão configurados para usar um proxy manualmente. Nesse caso, eles redirecionam o cliente para uma página que mostra como modificar suas configurações de proxy para que tudo funcione.

O redirecionamento de proxy WebAuth pode ser configurado para funcionar em uma variedade de portas e é compatível com a Autenticação Central da Web.

Para obter um exemplo de redirecionamento de proxy WebAuth, consulte Exemplo de Configuração de Proxy de Autenticação da Web em Controladoras Wireless LAN.

Autenticação da Web em HTTP em vez de HTTPS

Você pode fazer logon na autenticação da Web em HTTP em vez de HTTPS. Se você efetuar login no HTTP, não receberá alertas de certificado.

Para códigos anteriores ao WLC Versão 7.2, você deve desabilitar o gerenciamento HTTPS do WLC e deixar o gerenciamento HTTP. No entanto, isso só permite o gerenciamento da Web da WLC sobre HTTP.

Para o código da WLC versão 7.2, use o comando **config network web-auth secureweb disable** para desativar. Isso só desabilita o HTTPS para a autenticação da Web e não para o gerenciamento. Observe que isso exige a reinicialização do controlador!

Na versão 7.3 e posterior do WLC, você pode habilitar/desabilitar o HTTPS para WebAuth somente via GUI e CLI.

Informações Relacionadas

- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Download de software para pacotes WebAuth de controlador sem fio
- Criando uma página de logon de autenticação da Web personalizada
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Exemplo de Configuração de Passagem da Web do Wireless LAN Controller 5760/3850
- Configurando o Web Redirect (GUI)
- Configuração do Web Redirect (CLI)
- Solução de problemas de autenticação da Web em controladores de LAN sem fio (WLC)
- Exemplo de Configuração de Proxy de Autenticação da Web em uma Controladora Wireless LAN
- Solicitações de Comentários (RFCs)
- 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.