Autenticação da Web no controlador de WLAN

Índice

Introdução

Este documento explica os processos para a autenticação da Web em um controlador do Wireless LAN (WLC).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico da configuração WLC.

Componentes Utilizados

A informação neste documento é baseada em todos os modelos de hardware WLC.

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Processos internos da autenticação da Web

Posição da autenticação da Web como uns recursos de segurança

A autenticação da Web (WebAuth) é Segurança da camada 3. Permite a Segurança fácil de usar que trabalha em toda a estação que executar um navegador. Pode igualmente ser combinada com toda a Segurança da chave pré-compartilhada (PSK) (política de segurança da camada 2). Embora a combinação de WebAuth e de PSK reduza a parcela fácil de usar significativamente e não seja usada frequentemente, ainda tem a vantagem para cifrar o tráfego do cliente. WebAuth é um método de autenticação sem criptografia.

WebAuth não pode ser configurado com 802.1x/RADIUS (Remote Authentication Dial-In User Service) até que a liberação de software WLC 7.4 esteja instalada onde pode ser configurada ao mesmo tempo. Contudo, esteja ciente que os clientes devem atravessar o dot1x e a autenticação da Web. Não se significa para o convidado, mas para a adição de um portal da web para empregados (quem 802.1x do uso). Não há um Service Set Identifier (SSID) completo para o dot1x para empregados ou o portal da web para convidados.

Como WebAuth trabalha

O processo de autenticação do 802.11 está aberto, assim que você pode autenticar e associar sem problemas. Após isso, você é associado, mas não no estado de **CORRIDA** WLC. Com a autenticação da Web permitida, você é mantido em **WEBAUTH_REQD** onde você não pode alcançar nenhuns recursos de rede (nenhum sibilo, e assim por diante). Você deve receber um endereço IP de Um ou Mais Servidores Cisco ICM NT DHCP com o endereço do servidor DNS nas opções.

Você deve datilografar uma URL válida em seu navegador. O cliente resolve a URL com o protocolo DNS. O cliente envia então seu pedido do HTTP ao endereço IP de Um ou Mais Servidores Cisco ICM NT do Web site. As intercepções WLC que pedem e retornam a página de login do **webauth**, que paródias o endereço IP de Um ou Mais Servidores Cisco ICM NT do Web site. No caso de um WebAuth externo, o WLC responde com uma resposta HTTP que inclua seu endereço IP de Um ou Mais Servidores Cisco ICM NT do Web site e indica que a página se moveu. A página foi movida para o servidor de Web externo usado pelo WLC. Quando você é autenticado, você acede a todos os recursos de rede e está reorientado à URL pedida originalmente, à revelia (a menos que um forçado reorienta foi configurado no WLC). Em resumo, o WLC permite que o cliente resolva o DNS e obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT automaticamente no estado **WEBAUTH_REQD**.

Tip: Se você quer o WLC olhar uma outra porta em vez da porta 80, você pode usar o **number>**

do <port da Web-AUTH-porta da rede da configuração para criar igualmente uma reorientação nesta porta. Um exemplo é a interface da WEB do Access Control Server (ACS), que está em aplicativos similares da porta 2002 ou outro.

> **Note sobre o redirecionamento em https**: À revelia e nas versões 7.x e mais cedo, o WLC não reorientou o tráfego HTTPS. Isto significa que se você abre seu navegador e datilografa um endereço HTTPS, nada acontece. Você deve datilografar um endereço HTTP a fim obter reorientado à página de login que foi servida no HTTPS.
>
> Na versão 8.0 e mais recente, você pode permitir a reorientação do tráfego HTTPS com o comando CLI o Web-**AUTH da rede que da configuração https-reorienta permite.**
>
> Esteja ciente que este é recurso que consome para o WLC caso que muitos pedidos HTTPS são enviados. Recomenda-se para não usar esta característica antes da versão 8.7 WLC onde a escalabilidade desta característica foi aumentada. Igualmente note que um aviso do certificado é inevitável neste caso. Certamente, se seus pedidos do cliente alguma URL (tal como https://www.cisco.com), o WLC ainda apresenta seu próprio certificado emitido para o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface virtual. Isto obviamente nunca combinará o endereço IP de Um ou Mais Servidores Cisco ICM NT URL pedido pelo cliente e o certificado não será confiado a menos que o cliente forçar a exceção em seu navegador.

Queda de desempenho indicativa da liberação de software WLC antes de 8.7 medidos:

Webauth	Taxa conseguida
3 URL - HTTP	140/em segundo
?a URL - HTTP ?as e?ns URL - HTTPS	20/em segundo
3 URL - HTTPS (grande desenvolvimento)	<1/em segundo
3 URL - HTTPS (máximo de 100 clientes)	10/em segundo

Nesta tabela do desempenho, as 3 URL são referidas como:

- A URL original entrou pelo utilizador final (o Web site que o usuário quer consultar a)
- A URL o WLC reorienta o navegador a
- A submissão final das credenciais

A tabela do desempenho dá o desempenho WLC caso que todas as 3 URL são HTTP, caso que todas as 3 URL são HTTPS, ou se o cliente se transporta do HTTP A HTTPS (mais o cenário típico).

Como fazer um trabalho (local) interno de WebAuth com uma página interna

Se você precisa de configurar um WLAN com uma interface dinâmica operacional, os clientes devem igualmente receber um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DNS com o DHCP. Antes que você ajuste todo o **webauth**, você deve testar que seu WLAN trabalha corretamente, que você pode resolver pedidos DNS (**nslookup**), e que você pode consultar página da web. Então, você pode ajustar a autenticação da Web como recursos de segurança da camada 3. Você pode criar seus usuários no base de dados local ou em um servidor de raio externo, por exemplo. Refira o documento do exemplo de configuração da

autenticação da Web do controlador do Wireless LAN.

Como configurar um WebAuth local feito sob encomenda com página feita sob encomenda

O webauth feito sob encomenda pode ser configurado com **redirectUrl da ABA de segurança**. Isto força uma reorientação a um página da web que específico você incorpora. Quando o usuário é autenticado, cancela a URL original o cliente pedido e indica a página para que a reorientação foi atribuída.

Os recursos personalizados permitem que você use uma página html feita sob encomenda em vez da página de login do padrão. Transfira arquivos pela rede seus HTML e arquivos de imagem empacotam ao controlador. Na página da transferência de arquivo pela rede, procure o **pacote do webauth em um** formato do alcatrão. Geralmente, PicoZip cria os alcatrões que trabalham compativelmente com o WLC. Para um exemplo de um pacote de WebAuth, refira a página de software da transferência para pacotes wireless de WebAuth do controlador. Seja certo selecionar a liberação apropriada para seu WLC. Uma boa recomendação é personalizar um pacote que exista; não crie um pacote a partir do zero.

Há algumas limitações com **webauth feito sob encomenda** que variam com versões e erros. As coisas a olhar para incluem:

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

Se seu pacote do cliente não trabalha, para tentar com um pacote feito sob encomenda simples. Adicionar então arquivos e complexidade um de cada vez para alcançar o pacote o cliente tentado usar-se. Isto deve ajudá-lo a identificar o problema. Para um exemplo em como configurar uma página feita sob encomenda, refira a criação de uma página de login personalizada da autenticação da Web, uma seção dentro do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 7.0.

Cancele a técnica da configuração global

Para cada WLAN, você configura com o **comando global config da ultrapassagem** e ajusta um tipo de WebAuth para cada WLAN. Isto significa que você pode ter um interno/padrão WebAuth com um interno/padrão feitos sob encomenda WebAuth para um outro WLAN. Isto igualmente permite que você configure páginas feitas sob encomenda diferentes para cada WLAN. Você deve combinar todas suas páginas no mesmo pacote e transferi-las arquivos pela rede ao WLC. Então, você pode ajustar sua página feita sob encomenda com o **comando global config da ultrapassagem em** cada WLAN e selecioná-la que o arquivo é a página de login de todos os arquivos dentro do pacote. Você pode escolher uma página de login diferente dentro do pacote para cada WLAN.

Edição da reorientação

Há uma variável dentro do pacote HTML que permite a reorientação. Não põe sua reorientação

forçada URL lá. Para toda a reorientação emite em WebAuth feito sob encomenda, Cisco recomenda verificar o pacote. Se você incorpora uma reorientação URL com o **+= ao** WLC GUI, este poderia overwrite *ou* adicionar à URL definida dentro do pacote. Por exemplo, no WLC GUI, o campo do **redirectURL** é ajustado a www.cisco.com; contudo, no pacote mostra: **redirectURL+=** "www.google.com". **O +=** reorienta usuários a www.cisco.comwww.google.com, que é uma URL inválida.

Como fazer um trabalho (local) externo da autenticação da Web com uma página externo

Como explicado já momentaneamente, a utilização de um server externo de WebAuth é apenas um repositório externo para a página de login. As credenciais do usuário são autenticadas ainda pelo WLC. O servidor de Web externo permite somente que você use uma página de login especial ou diferente. Estão aqui as etapas executadas para um WebAuth externo:

1. O cliente (utilizador final) abre um navegador da Web e incorpora uma URL.

2. Se o cliente não é autenticado e autenticação do web externa está usado, o WLC reorienta o usuário ao servidor de Web externo URL. Ou seja o WLC envia um HTTP reorienta ao cliente com endereço IP de Um ou Mais Servidores Cisco ICM NT falsificado do Web site e aos pontos ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor interno. A autentificação de login URL do web externa é adicionada com parâmetros tais como o **AP_Mac_Address**, o **client_url** (www.website.com), e o **action_URL** esse as necessidades de cliente de contactar o servidor de Web do interruptor.

3. O servidor de Web externo URL envia o usuário a uma página de login. Então o usuário pode usar um Access Control List da PRE-autenticação (ACL) a fim alcançar o server. O ACL é precisado para todos os modelos WLC exceto o 4400 Series e o Wism1.

4. A página de login toma as credenciais do usuário entradas e envia o pedido de volta ao **action_URL**, tal como http://192.0.2.1/login.html, do servidor de Web WLC. Isto é fornecido enquanto um parâmetro de entrada ao cliente reorienta a URL, onde 192.0.2.1 é o endereço da interface virtual no interruptor.

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

6. O WLC inicia o pedido do servidor Radius ou usa o base de dados local no WLC, e autentica então o usuário.

7. Se a autenticação é bem sucedida, o servidor de Web WLC qualquer um para a frente o usuário ao configurado reorienta a URL ou à URL o cliente entrou.

8. Se a autenticação falha, a seguir o servidor de Web WLC reorienta o usuário de volta ao início de uma sessão URL do cliente.

   Note: Nós usamos 192.0.2.1 como exemplo do IP virtual neste documento. A escala 192.0.2.x é recomendada para o uso para o IP virtual porque é não-roteável. Uma documentação mais velha pode referir "1.1.1.x" ou aquele pode ainda ser o que é configurado em seu WLC como este se usou para ser a configuração padrão. Contudo, note

que este IP agora um endereço IP roteável válido e consequentemente a sub-rede 192.0.2.x está recomendado pelo contrário.

Note: Se os Access point (AP) reagem do modo de FlexConnect, um **preauth** ACL é irrelevante. O cabo flexível ACL pode ser usado para permitir o acesso ao servidor de Web para os clientes que não foram autenticados. Refira a autenticação do web externa com exemplo de configuração dos controladores do Wireless LAN.

Transmissão da Web

Esta é uma variação da autenticação do web interna. Indica uma página com uma indicação de advertência ou alerta, mas não a alerta para credenciais. O usuário deve clicar a **aprovação**. Você pode permitir o email de entrar, e o usuário pode incorporar seu endereço email, que se transforma seu username. Quando o usuário é conectado, verifique sua lista dos clientes ativo; que o usuário está alistado com o endereço email eles entrou como o username. Para mais informação, refira o exemplo de configuração da transmissão da Web do controlador do Wireless LAN.

A Web condicional reorienta

Se você permite uma Web condicional reoriente, o usuário está reorientado condicionalmente a um página da web particular depois que a autenticação do 802.1x terminou com sucesso. Você pode especificar a página e as condições de redirecionamento sob as quais o redirecionamento ocorre em seu servidor RADIUS. As circunstâncias podem incluir a senha de usuário quando alcança a data de expiração ou quando o usuário precisa de pagar uma conta pelo uso/acesso continuados. Se o servidor Radius retorna o par Cisco AV URL-**reoriente**, a seguir o usuário está reorientado ao URL especificado quando abrem um navegador. Se o server igualmente retorna o par Cisco AV URL-reorientar-**ACL**, a seguir o ACL especificado está instalado como uma PRE-autenticação ACL para este cliente. O cliente não é considerado autorizado inteiramente neste momento e pode somente passar o tráfego permitido pela PRE-autenticação ACL. Depois que o cliente termina uma operação particular no URL especificado (por exemplo, uma mudança da senha ou um pagamento da conta), a seguir o cliente deve autenticar novamente. Quando o servidor Radius não retorna uma URL-**reorientação**, o cliente está considerado autorizado inteiramente e permitido passar o tráfego.

Note: A Web condicional reorienta a característica está disponível somente para os WLAN que são configurados para o 802.1x ou WPA+WPA2 a Segurança da camada 2.

Depois que você configura o servidor Radius, você pode então configurar a Web condicional reorienta no controlador com o controlador GUI ou CLI. Refira estes guias passo a passo: Usando o GUI para configurar a Web reoriente e usando o CLI para configurar a Web reoriente.

A Web da página do respingo reorienta

Se você permite a Web da página do respingo reoriente, o usuário está reorientado a um página da web particular depois que a autenticação do 802.1x terminou com sucesso. Depois que a reorientação, o usuário tem o acesso direto à rede. Você pode especificar a página da reorientação em seu servidor Radius. Se o servidor Radius retorna o par Cisco AV URL-**reoriente**, a seguir o usuário está reorientado ao URL especificado quando abrem um navegador. Permitido

ao cliente é considerado autorizado inteiramente neste momento e passar o tráfego, mesmo se o servidor Radius não retorna uma URL-**reorientação**.

Note: A Web da página do respingo reorienta a característica está disponível somente para os WLAN que são configurados para o 802.1x ou WPA+WPA2 a Segurança da camada 2.

Depois que você configura o servidor Radius, você pode então configurar a Web da página do respingo reorienta no controlador com o controlador GUI ou CLI.

WebAuth na falha do filtro MAC

Isto exige-o configurar filtros MAC no menu Segurança da camada 2. Se os usuários são validados com sucesso com seus endereços MAC, a seguir vão diretamente ao estado de **corrida**. Se não são, a seguir vão ao estado **WEBAUTH_REQD** e a autenticação da Web normal ocorre.

Note: Isto não é apoiado com transmissão da Web. Para mais informação, siga a atividade na requisição de aprimoramento CSCtw73512 .

Autenticação da Web central

A autenticação da Web central refere uma encenação onde o WLC já não hospede todos os serviços. A diferença reside no fato de que o cliente está enviado diretamente ao portal da web ISE e não atravessa 192.0.2.1 no WLC. A página de login e o portal inteiro são exteriorizados.

A autenticação da Web central ocorre quando você tem o Network Admission Control (NAC) do RAIO permitido nos ajustes avançados dos filtros WLAN e MAC permitidos.

O conceito total é que o WLC envia uma autenticação RADIUS (geralmente para o filtro MAC) ao ISE, que responde com os pares do valor de atributo reorientar-**URL** (AV). O usuário está posto então no estado **POSTURE_REQD** até que o ISE dê a autorização com uma mudança do pedido da autorização (CoA). A mesma encenação acontece na postura ou na central WebAuth. WebAuth central não é compatível com WPA-Enterprise/802.1x porque o portal do convidado não pode retornar chaves de sessão para a criptografia como faz com Extensible Authentication Protocol (EAP).

Autenticação de usuário externo (RAIO)

Isto é somente válido para WebAuth local quando o WLC segura as credenciais, ou quando uma política da Web da camada 3 está permitida. Você pode então autenticar usuários localmente no WLC ou externamente através do RAIO.

Há uma ordem em que o WLC verifica para ver se há as credenciais do usuário.

1. Em todo caso, olha primeiramente em seu próprio base de dados.
2. Se não encontra os usuários lá, vai ao servidor Radius configurado no convidado WLAN (se há um configurado).
3. Verifica então dentro a lista global do servidor Radius contra os servidores Radius onde o **usuário de rede** é verificado.

Este terceiro ponto é muito importante e responde à pergunta de muitos que não configuram o

RAIO para esse WLAN, mas observa que ainda verifica contra o RAIO quando o usuário não é encontrado no controlador. Isto é porque o **usuário de rede** é verificado contra seus servidores Radius na lista global.

O WLC pode autenticar usuários ao servidor Radius com protocolo password authentication (PAP), protocolo de autenticação de cumprimento do desafio (RACHADURA) ou EAP-MD5 (mensagem Digest5). Este é um parâmetro global e é configurável do GUI ou do CLI:

Do GUI: navegue ao **controlador >** à **autenticação RADIUS da Web**

Do CLI: incorpore a costume-**Web RADIUSauth <pap|chap|md5chap> da configuração**

Note: O server do convidado NAC usa somente o PAP.

Como ajustar um convidado prendido WLAN

Éfácil configurar e muito próximo à configuração wireless do convidado. Você pode configurar-lo com um ou dois controladores (somente se um é auto-âncora).

Escolha um VLAN como o VLAN em que você coloca usuários convidado prendidos, por exemplo, em 50 pés VLAN. Quando um convidado prendido quer o acesso ao Internet, obstrua o portátil a uma porta em um interruptor configurado para 50 pés VLAN. Estes 50 pés VLAN devem estar reservados e atuais no trajeto através da porta de tronco WLC. Em um exemplo de dois WLC (umas âncora e uma estrangeiras), este convidado prendido VLAN deve conduzir ao WLC estrangeiro (WLC1 Nomeado) e não à âncora. WLC1 toma então de escavar um túnel o tráfego ao DMZ WLC (a âncora, WLC2 Nomeado), que libera o tráfego na rede roteada.

Estão aqui as cinco etapas para configurar o acesso prendido do convidado:

1. **Configurar uma interface dinâmica (VLAN) para o acesso de usuário convidado prendido.**

   Em WLC1, crie uma interface dinâmica VLAN50. Na página da **configuração da interface**, verifique a caixa do **convidado LAN**. Então, os campos tais como o **endereço IP de Um ou Mais Servidores Cisco ICM NT** e o **gateway** desaparecem. A única coisa que seu WLC precisa de saber sobre esta relação é que o tráfego está distribuído dos 50 pés VLAN. Estes clientes são convidados prendidos.

2. **Crie um LAN ligado com fio para o acesso de usuário convidado.**

   Em um controlador, uma relação é usada quando associada a um WLAN. O segundo passo é criar um WLAN em seus controladores do escritório principal. Navegue aos **WLAN** e clique **novo**. **No tipo WLAN**, escolha o **convidado LAN**.

   No nome de perfil e no **WLAN SSID**, dê entrada com um nome que identifique este WLAN. Estes nomes podem ser diferentes, mas não podem conter espaços. O termo WLAN é usado, mas este perfil da rede não é relacionado ao perfil da rede Wireless.

   O tab geral oferece duas listas de drop-down: **Ingresso** e **saída**. O ingresso é o VLAN de que os usuários vêm (50 pés VLAN); A saída é o VLAN a que você quer o enviar.

Para o **ingresso**, escolha **VLAN50**.

Para a **saída**, é diferente. Se você tem somente um controlador, você precisa de criar uma outra interface dinâmica, **padrão** esta vez (não um convidado LAN), e você envia seus usuários prendidos a esta relação. Neste caso, envie-os ao controlador DMZ. Consequentemente, para a **interface de saída**, escolha a **interface de gerenciamento**.

O modo de segurança para este convidado LAN "WLAN" é WebAuth, que é aceitável. **Aprovação do** clique a fim validar.

3. **Configurar o controlador estrangeiro (escritório principal).**

Da lista WLAN, clique a **âncora da mobilidade na** extremidade da linha do **convidado LAN**, e escolha seu controlador DMZ. Supõe-se aqui que ambos os controladores se conhecem. Se não se conhecem ainda, vá ao **grupo do Gerenciamento do controlador >** de **mobilidade >** da **mobilidade**, e adicionar **DMZWLC em** WLC1. Adicionar então **WLC1 no** DMZ. Ambos os controladores não devem estar no mesmo grupo da mobilidade. Se não, as regras de segurança básica são quebradas.

4. **Configurar o controlador da âncora (controlador DMZ).**

Seu controlador do escritório principal está pronto. Você precisa agora de preparar seu controlador DMZ. Abra uma sessão do navegador da Web a seu controlador DMZ e navegue aos **WLAN**. Crie um WLAN novo. **No tipo WLAN**, escolha o **convidado LAN**.

No nome de perfil e no **WLAN SSID**, dê entrada com um nome que identifique este WLAN. Use os mesmos valores como entrado no controlador do escritório principal.

A interface de ingresso aqui não é **nenhuma**. Realmente não importa, porque o tráfego é recebido com os Ethernet sobre o túnel IP (EoIP). Eis porque você não precisa de especificar nenhuma interface de ingresso.

A interface de saída é essa em que os clientes são supostos ser enviados. Por exemplo, o **DMZ VLAN** é VLAN 9. cria uma interface dinâmica padrão para VLAN 9 em seu DMZWLC, a seguir escolhe **VLAN 9** como a interface de saída.

Você precisa de configurar a extremidade do túnel da âncora da mobilidade. **Da lista WLAN**, escolha a **âncora da mobilidade para o convidado LAN**. Envie o tráfego ao controlador local, **DMZWLC**. O ambas as extremidades está agora pronto.

5. **Ajustar o convidado LAN.**

Você pode igualmente ajustar os ajustes WLAN no ambas as extremidades. Seja cuidadoso, os ajustes deve ser idêntico no ambas as extremidades. Por exemplo, se você escolhe clicar no **guia avançada WLAN**, **permita a ultrapassagem AAA em** WLC1, você precisam de verificar a mesma caixa em DMZWLC. Se há alguma diferença nas seleções no WLAN de cada lado, o túnel quebra. DMZWLC recusa o tráfego; você pode ver quando você **para ser executado debuga a mobilidade**.

Mantenha na mente que todos os valores estão obtidos realmente de DMZWLC: Endereços IP de Um ou Mais Servidores Cisco ICM NT, valores VLAN, e assim por diante. Configurar o lado WLC1 identicamente, de modo que retransmita o pedido ao WLCDMZ.

Certificados para a página de login

Esta seção fornece os processos que você precisa de seguir se você quer pôr seu próprio certificado sobre a página de WebAuth, ou se você quer esconder 192.0.2.1 WebAuth URL e indicar uma URL Nomeado.

Transfira arquivos pela rede um certificado para a autenticação da Web do controlador

Com o GUI (**WebAuth > certificado**) ou CLI (tipo **webauthcert de** transferência) você pode transferir arquivos pela rede um certificado no controlador. Se é um certificado que você criou com seu Certificate Authority (CA) ou um certificado oficial da terceira, deve estar no formato do .pem. Antes que você envie, você deve igualmente incorporar a chave do certificado.

Após a transferência de arquivo pela rede, uma repartição é exigida para que o certificado seja no lugar. Uma vez que recarregado, vá à página do certificado de WebAuth no GUI e mostra-lhe os detalhes do certificado que você transferiu arquivos pela rede (validez e assim por diante). O campo importante é o Common Name (CN), que é o nome emitido ao certificado. Este campo é discutido neste documento sob a seção “Certificate Authority e outros Certificados no controlador”.

Depois que você recarregou e verificou os detalhes do certificado, você é presentado com o certificado novo do controlador na página de login de WebAuth. Contudo, pode haver duas situações.

1. Se seu certificado foi emitido por um dos poucos a raiz principal CA que cada computador confia, a seguir é aprovado. Um exemplo é Verisign, mas você é assinado geralmente por Verisign secundário-CA e não a CA raiz. Você pode verificar dentro sua loja do certificado do navegador se você vê CA mencionado lá como confiado.

2. Se você obteve seu certificado de um company/CA menor, todos os computadores não o confiam. Você deve fornecer o certificado company/CA ao cliente também, e esperançosamente uma da raiz CA emitirá esse certificado. Eventualmente, você termina com uma corrente tal como o “certificado foi emitido acima por CA x > certificado de CA x foi emitido por CA y > certificado de CA y foi emitido por este root confiável CA”. O objetivo do fim é alcançar CA que o cliente confia.

Certificate Authority e outros Certificados no controlador

A fim para ser livrado do aviso que “este certificado não é confiado”, você deve igualmente entrar no certificado de CA que emitiu o certificado do controlador no controlador. Então o controlador apresenta ambos os Certificados (seu certificado de CA do controlador o certificado e). O certificado de CA deve ser CA confiado ou tem os recursos para verificar CA. Você pode realmente construir uma corrente dos certificados de CA que conduzem a CA confiado na parte

superior.

Você deve colocar a corrente inteira no mesmo arquivo. Isto significa que seu arquivo contém o índice tal 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 combine a URL

O WebAuth URL é ajustado a 192.0.2.1 a fim autenticar-se e o certificado é emitido (este é o campo do CN do certificado WLC). Se você quer mudar o WebAuth URL a “myWLC.com”, por exemplo, entre na **configuração do** virtualinterface **(a** relação de 192.0.2.1) e lá você pode entrar em um **hostname do** virtualDNS**, tal como** myWLC.com. Isto substitui 192.0.2.1 em sua barra URL. Este nome deve igualmente ser solucionável. O farejador de rastreamento mostra como todo trabalha, mas quando o WLC envia a página de login, o WLC mostra o endereço de myWLC.com, e o cliente resolve este nome com seu DNS. Este nome deve resolver como 192.0.2.1. Isto significa que se você igualmente usa um nome para o Gerenciamento do WLC, você deve usar um nome diferente para WebAuth. Ou seja se você usa myWLC.com traçado ao endereço IP de gerenciamento WLC, você deve usar um nome diferente para o WebAuth, tal como myWLCwebauth.com.

Pesquise defeitos edições do certificado

Esta seção explica como e que a verificar para pesquisar defeitos edições do certificado.

Como verificar

Você pode transferir o OpenSSL (para Windows, para procurar pelo OpenSSL Win32) e instalá-lo. Sem nenhuma configuração, você pode ir no diretório bin e no **OpenSSL da** tentativa **s_client – conecte** www.mywebauthpage.com:443, se esta URL é a URL onde sua página de WebAuth está ligada em seu DNS. Refira a “o que para verificar” a seção deste documento para ver se há um exemplo.

Se seus Certificados usam CA privado, você precisa de colocar o certificado CA raiz em um diretório em uma máquina local e de usar a opção do OpenSSL **- CApath**. Se você tem CA intermediário, você deve pô-lo no mesmo diretório também.

A fim obter a informação geral sobre o certificado e verificá-la, use:

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

Pôde ser igualmente útil converter Certificados com o uso do OpenSSL:

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

O que deve ser verificado?

Você pode ver que Certificados estão enviados ao cliente quando conecta. Leia o certificado do dispositivo — o CN deve ser a URL onde o página da web é alcançável. Leia “emitido” pela linha

do certificado do dispositivo. Isto deve combinar o CN do segundo certificado. Então este segundo certificado “emitido por” deve combinar o CN do certificado seguinte, e assim por diante. Se não, não faz uma corrente real. No OpenSSL output mostrado aqui, você pode ver que o **OpenSSL** não pode verificar o certificado do dispositivo porque o seu “emitido por” não combina o nome do certificado de CA fornecido.

Saída SSL

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

Um outro possível problema é o certificado não pode ser transferido arquivos pela rede ao controlador. Nesta situação não há nenhuma pergunta da validez, CA, e assim por diante. A fim verificá-lo isto, podem primeira verificação a Conectividade do Trivial File Transfer Protocol (TFTP) e tentá-los transferir um arquivo de configuração. Então, se você incorpora **transferência debugar todo o comando enable**, você vê que o problema é a instalação do certificado. Isto podia ser devido à chave errada usada com o certificado. Poder-se-ia igualmente ser que o certificado está em um formato errado ou está corrompido.

Cisco recomenda que você compara o índice do certificado a um sabido, certificado válido. Isto permite que você ver se um atributo de **LocalkeyID** mostra todo o 0s (já acontecido). Em caso afirmativo, então o certificado deve ser reciclado. Há dois comandos com OpenSSL que permitem que você retorne do .pem a .p12, e reedita então um .pem com a chave de sua escolha.

PRE-etapa: Se você recebeu um .pem que contém um certificado seguido por uma chave, copie/pasta a parte chave: **----COMECE A CHAVE ---- até ------- CHAVE DE FIM ------** do .pem em “key.pem”.

1. **pkcs12 do OpenSSL - exportação - em certificate.pem - inkey key.pem - para fora newcert.p12? Você** é alertado com uma chave; incorpore check123**.**

2. **o pkcs12 do OpenSSL - em newcert.p12 - para fora workingnewcert.pem - o passin pass:check123 - o passout pass:check123 isto** conduz a um .pem operacional com a senha check123**.**

Outras situações a pesquisar defeitos

Embora a **âncora da mobilidade** não esteja discutida neste documento, se você está em uma situação **ancorada do convidado**, certifique-se a troca da mobilidade ocorre corretamente e isso que você vê que o cliente chega na âncora. Toda a necessidade mais adicional dos problemas de WebAuth pesquisa defeitos na âncora.

Estão aqui alguns problemas comuns que você pode pesquisar defeitos:

- **Os usuários não podem associar ao convidado WLAN**.

  Isto não é relacionado a WebAuth. Verifique a configuração de cliente, as configurações de segurança no WLAN, se é permitido, e se os rádios são ativos e operativos, e assim por diante.

- **Os usuários não obtêm o endereço IP de Um ou Mais Servidores Cisco ICM NT**.

Em uma situação da âncora do convidado, isto é o mais frequentemente porque o estrangeiro e a âncora não foram configurados exatamente a mesma maneira. Se não, verifique a configuração de DHCP, Conectividade, e assim por diante. Confirme mesmo se outros WLAN podem usar o mesmo servidor DHCP sem um problema. Isto não é relacionado ainda a WebAuth.

- **O usuário não é reorientado à página de login**.

  Este é a maioria de sintoma comum, mas é mais preciso. Há dois cenários possíveis.

  O usuário não é reorientado (o usuário incorpora uma URL e nunca alcança a página de WebAuth). Para esta situação, verifique:

  que um server dos DN válidos esteve atribuído ao cliente através de DHCP (**ipconfig /all**),

  que o DNS é alcançável do cliente (**nslookup** www.website.com),

  que o usuário incorporou uma URL válida a fim ser reorientado,

  que o usuário foi em um URL DO HTTP na porta 80 (por exemplo, para alcançar um ACS com http://localhost:2002 não o reorienta desde que você enviou sobre a porta 2002 em vez de 80).

  O usuário é reorientado a 192.0.2.1 corretamente, mas a página própria não indica.

  Esta situação é mais provável um problema WLC (erro) ou um problema do lado do cliente. Poder-se-ia ser que o cliente tem algum Firewall ou software ou política da obstrução. Igualmente poder-se-ia ser que configuraram um proxy em seu navegador da Web.

  Recomendação: Tome um farejador de rastreamento no PC cliente. Não há nenhuma necessidade para o software wireless especial, simplesmente Wireshark, que é executado no adaptador Wireless e lhe mostra se o WLC responde e tenta reorientar. Você tem duas possibilidades: ou não há nenhuma resposta do WLC, ou algo é errado com a saudação de SSL para a página de WebAuth. Para a edição da saudação de SSL, você pode verificar se o navegador do usuário permita SSLv3 (alguns permitem somente SSLv2), e se é demasiado agressivo na verificação de certificado.

  Éuma etapa comum para entrar manualmente em http:// 192.0.2.1 a fim verificar se o página da web se publica sem DNS. Realmente, você pode datilografar http://6.6.6.6 e obter o mesmo efeito. O WLC reorienta todo o endereço IP de Um ou Mais Servidores Cisco ICM NT que você incorporar. Consequentemente, se você entra em http:// 192.0.2.1, não o faz trabalhar em torno da reorientação da Web. Se você entra em https:// 192.0.2.1(secure), este não trabalha porque o WLC não reorienta o tráfego HTTPS (à revelia, este é realmente possível na versão 8.0 e mais recente). A melhor maneira de carregar a página diretamente sem uma reorientação é entrar em https:// 192.0.2.1/login.html.

- **Os usuários não podem autenticar**.

Veja a seção deste documento que discute a autenticação. Verifique credenciais localmente no RAIO.

- **Os usuários podem com sucesso autenticar com WebAuth, mas não têm o acesso à internet mais tarde**.

  Você pode remover WebAuth da Segurança do WLAN, e então você deve ter um WLAN aberto. Você pode então tentar alcançar e assim por diante a Web, o DNS. Se você experimenta edições lá também, remova os ajustes de WebAuth completamente e verifique sua configuração das relações.

Para obter mais informações, consulte: Pesquisando defeitos a autenticação da Web em um controlador do Wireless LAN (WLC).

Servidor proxy HTTP e como trabalha

Você pode usar um servidor proxy HTTP. Se você precisa o cliente de adicionar uma exceção em seu navegador que 192.0.2.1 não é atravessar o servidor proxy, você pode fazer o WLC escutar o tráfego de HTTP na porta do servidor proxy (geralmente 8080).

A fim compreender esta encenação, você precisa de conhecer o que um proxy HTTP faz. É algo que você configura no lado do cliente (endereço IP de Um ou Mais Servidores Cisco ICM NT e porta) no navegador.

A encenação usual quando um usuário visita um Web site é resolvê-lo o nome ao IP com DNS, e então pede o página da web ao servidor de Web. O processo deve sempre enviar o pedido do HTTP para a página ao proxy. O proxy processa o DNS, se for necessário, e para a frente ao servidor de Web (se a página não é posta em esconderijo já no proxy). A discussão é cliente-à-proxy somente. Mesmo se o proxy obtém o página da web real é irrelevante ao cliente.

Está aqui o processo de autenticação da Web:

- O usuário datilografa dentro uma URL.
- O PC cliente envia ao servidor proxy.
- IP do servidor proxy das intercepções e das paródias WLC; responde ao PC com uma reorientação a 192.0.2.1

Nesta fase, se o PC não é configurado para ele, pede a página de 192.0.2.1 WebAuth ao proxy assim que não trabalha. O PC deve fazer uma exceção para 192.0.2.1; então envia um pedido do HTTP a 192.0.2.1 e continua com WebAuth. Quando autenticadas, todas as comunicações atravessam o proxy outra vez. Uma configuração da exceção está geralmente no navegador perto da configuração do servidor proxy. Você deve ver a mensagem: “Não use o proxy para aqueles endereços IP de Um ou Mais Servidores Cisco ICM NT”.

Com WLC libere 7.0 e mais atrasado, o **proxy do webauth da** característica **reorienta** pode ser permitido nas opções de configuração globais WLC. Quando permitido, o WLC verifica se os clientes são configurados para usar manualmente um proxy. Nesse caso, reorientam o cliente a uma página que lhes mostre como alterar seus ajustes do proxy para fazer tudo trabalhar. O proxy de WebAuth reorienta pode ser configurado para trabalhar em uma variedade de portas e é compatível com autenticação da Web central.

Para um exemplo na reorientação do proxy de WebAuth, refira o proxy da autenticação da Web em um exemplo da configuração de controle do Wireless LAN.

Autenticação da Web no HTTP em vez do HTTPS

Você pode entrar na autenticação da Web no HTTP em vez do HTTPS. Se você entra no HTTP, você não recebe alertas do certificado.

Para mais cedo do que o código da liberação 7.2 WLC, você deve desabilitar o gerenciamento HTTPS do WLC e deixar o Gerenciamento HTTP. Contudo, isto permite somente o gerenciamento de web do WLC sobre o HTTP.

Para o WLC libere 7.2 código, usam o **comando disable do secureweb do Web-AUTH da rede da configuração** desabilitar. Isto desabilita somente o HTTPS para a autenticação da Web e não o Gerenciamento. Note que isto exige uma repartição do controlador!

Na liberação 7.3 WLC e o código mais recente, você pode permitir/desabilitação HTTPS para WebAuth somente através do GUI e do CLI.

Informações Relacionadas

- Exemplo de configuração da autenticação da Web do controlador do Wireless LAN
- Software da transferência para pacotes wireless de WebAuth do controlador
- Criando uma página de login personalizada da autenticação da Web
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Exemplo de configuração da transmissão da Web do controlador do Wireless LAN
- Usando o GUI para configurar a Web reoriente
- Usando o CLI para configurar a Web reoriente
- Pesquisar defeitos a autenticação da Web em um controlador do Wireless LAN (WLC)
- Proxy da autenticação da Web em um exemplo da configuração de controle do Wireless LAN
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems