Solução de problemas de autenticação da Web em controladores de LAN sem fio (WLC)

Índice

Introdução

Este original fornece pontas a fim pesquisar defeitos edições da autenticação da Web em um ambiente do controlador do Wireless LAN (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do controle e do abastecimento dos pontos de acesso Wireless (CAPWAP).
- Conhecimento de como configurar o Access point de pouco peso (REGAÇO) e o WLC para a operação básica.
- Conhecimento básico da autenticação da Web e como configurar a autenticação da Web em WLC. Para obter informações sobre de como configurar a autenticação da Web em WLC, refira o exemplo de configuração da autenticação da Web do controlador do Wireless LAN.

Componentes Utilizados

A informação neste documento é baseada em um WLC 5500 que execute a versão de firmware 8.3.121.

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.

Produtos Relacionados

Este original pode igualmente ser usado com este hardware:

- Controladores sem fio Cisco série 5500
- Controladores do Sem fio do Cisco 8500 Series
- Controladores sem fio Cisco série 2500
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Controladores sem fio Cisco Flex série 7500
- Cisco Wireless Services Module 2 (WiSM2)

Autenticação da Web em WLC

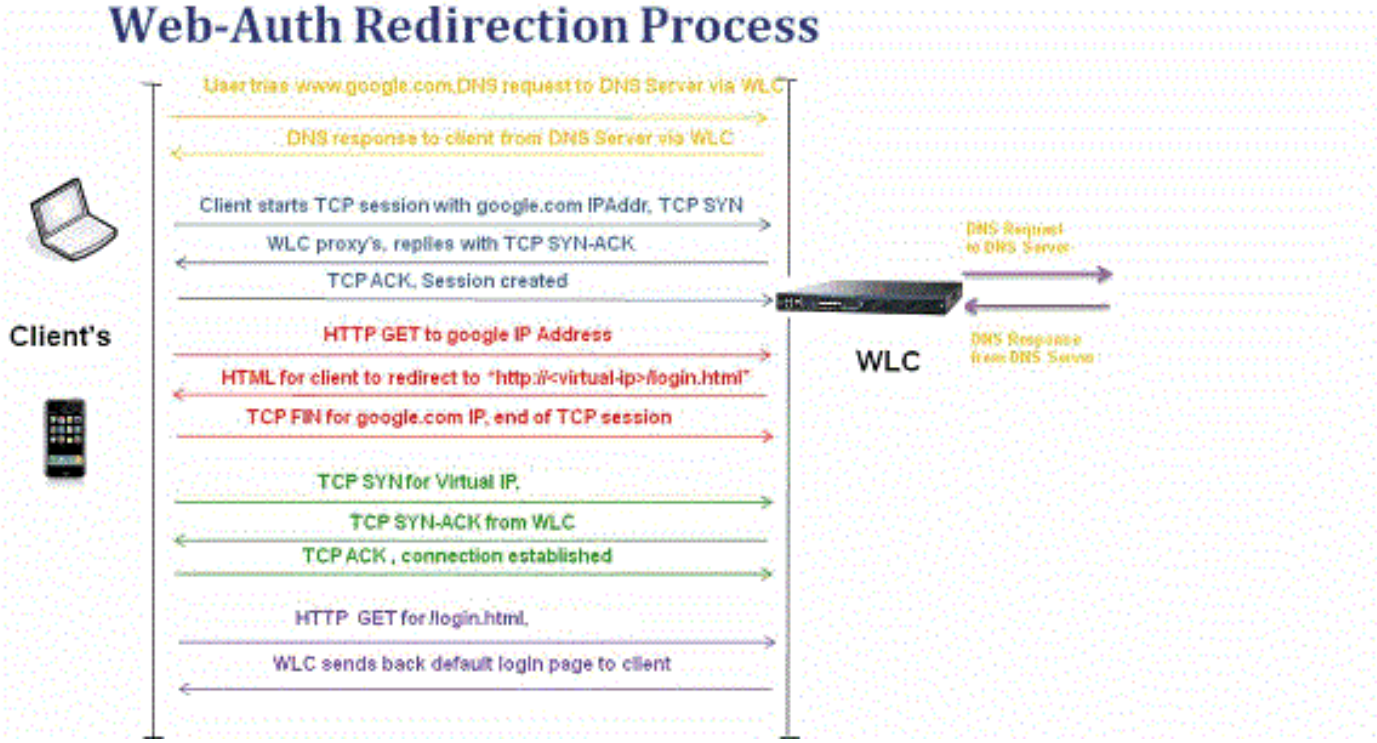
A autenticação da Web é uns recursos de segurança da camada 3 que façam com que o controlador não permita o tráfego IP, exceto Domain Name System (DNS) DHCP-relacionado dos pacotes - pacotes relacionados, de um cliente específico até que esse cliente forneça corretamente um nome de usuário válido e uma senha com uma exceção do tráfego permitida com um Access Control List do PRE-AUTH (ACL). A autenticação da Web é a única política de segurança que permite que o cliente obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT antes da autenticação. É um método de autenticação simples sem a necessidade para um suplicante ou um utilitário de cliente. 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 obtenha isto distante, o cliente deve primeiramente obter um endereço IP de Um ou Mais Servidores Cisco ICM NT, e faz uma tradução da URL ao endereço IP de Um ou Mais Servidores Cisco ICM NT (resolução de DNS) para o navegador da Web. Isto deixa o navegador da Web saber que endereço IP de Um ou Mais Servidores Cisco ICM NT para enviar o HTTP GET.

Quando a autenticação da Web é configurada no WLAN, o controlador obstrui todo o tráfego (até que o processo de autenticação esteja terminado) do cliente, à exceção do tráfego DHCP e DNS. Quando o cliente envia o primeiro HTTP GET à porta TCP 80, o controlador reorienta o cliente a https://192.0.2.1/login.html (se este é o IP virtual que está configurado) para processar. Este processo traz eventualmente acima o página da web do início de uma sessão.

> **Note**: Quando você usa um servidor de Web externo para a autenticação da Web, as Plataformas WLC precisam uma PRE-autenticação ACL para o servidor de Web externo.

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



- Você abre o navegador da Web e datilografa dentro uma URL, por exemplo, http://www.google.com. O cliente envia uma solicitação DNS para esse URL a fim de obter o IP de destino. O WLC passa o pedido DNS ao servidor DNS e o servidor DNS responde para trás com uma resposta DNS, que contenha o endereço IP de Um ou Mais Servidores Cisco ICM NT do destino www.google.com, que é enviado por sua vez aos clientes Wireless.
- Então, o cliente tenta então estabelecer uma conexão TCP com o endereço IP de destino. Manda um pacote SYN de TCP destinado ao endereço IP de Um ou Mais Servidores Cisco ICM NT de www.google.com.
- O WLC tem as regras configuradas para o cliente e daqui pode atuar como um proxy para www.google.com. Envia para trás um pacote TCP SYN-ACK ao cliente com fonte como o endereço IP de Um ou Mais Servidores Cisco ICM NT de www.google.com. O cliente envia para trás um pacote de ACK TCP a fim terminar o cumprimento de TCP tripartido e a conexão de TCP é estabelecida inteiramente.
- O cliente envia um pacote HTTP GET destinado a www.google.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 de TCP com o endereço IP de Um ou Mais Servidores Cisco ICM NT, por exemplo www.google.com.
- Agora o cliente quer ir a http:// <virtualip>/login.html e assim que tenta abrir uma conexão de TCP com o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do WLC. Envia um pacote SYN de TCP para 192.0.2.1 (que é nosso IP virtual aqui) ao 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 destinou a 192.0.2.1 a fim pedir a página de login.
- Este pedido é permitido até o servidor de Web do WLC e o server responde para trás com a página de login do padrão. O cliente recebe a página de login na janela do navegador, e é

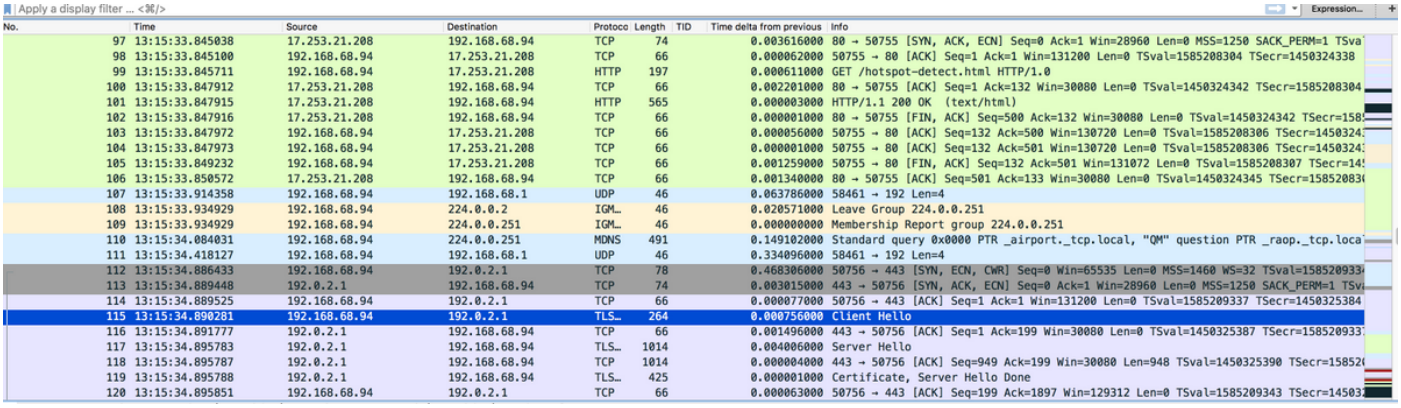
permitido ao usuário fazer o login.

Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente é 192.168.68.94. O cliente resolveu a URL ao servidor de Web que alcançava, 10.1.0.13. Como você pode ver, o cliente fez o cumprimento de três vias para pôr em andamento a conexão de TCP e enviou então um pacote HTTP GET que começa com pacote 96 (00 são o pacote de HTTP). Isto não esteve provocado pelo usuário, mas era a provocação portal automatizada sistema operacional da detecção (como nós podemos supor da URL pedida). O controlador intercepta os pacotes e as respostas com código 200. O pacote do código 200 tem uma reorientação URL nele:

```
<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>
```

Fecha então a conexão de TCP através do cumprimento de três vias.

O cliente liga então a conexão de HTTPS à reorientação URL que a envia a 192.0.2.1, que é o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do controlador. O cliente tem que validar o certificado de servidor ou ignorá-lo a fim trazer acima o túnel SSL. Neste caso, é um certificado auto-assinado assim que o cliente ignorou-o. O página da web do início de uma sessão é enviado através deste túnel SSL. O pacote 112 começa as transações.



No.	Time	Source	Destination	Protoco	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=145
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=158520836
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=158520933
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=158520
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=14503

Você tem a opção para configurar o Domain Name para o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do WLC. Se você configura o Domain Name para o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual, este Domain Name está retornado no pacote da APROVAÇÃO HTTP do controlador em resposta ao pacote HTTP GET do cliente. Você então tem que executar uma resolução de DNS para este Domain Name. Uma vez que obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT da resolução de DNS, tenta abrir uma sessão de TCP com esse endereço IP de Um ou Mais Servidores Cisco ICM NT, que é um endereço IP de Um ou Mais Servidores Cisco ICM NT configurado em uma interface virtual do controlador.

Eventualmente, o página da web é passado através do túnel ao cliente e o usuário envia para trás o username/senha através do túnel do secure sockets layer (SSL).

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

- Use um página da web interno (padrão). Refira a escolha da página da autentificação de login

do web padrão para obter mais informações sobre do uso do página da web do padrão.
- Use uma página de login personalizada. Refira a criação de uma página de login personalizada da autenticação da Web para obter mais informações sobre de como usar a página de login personalizada.
- Use uma página de login de um servidor de Web externo. Refira a utilização de uma página de login personalizada da autenticação da Web de um servidor de Web externo para obter mais informações sobre de como usar uma página de login de um servidor de Web externo.

Notas:
- O pacote personalizado da autenticação da Web tem um limite de até 30 caráteres para nomes de arquivo. Assegure-se de que nenhum nome de arquivo dentro do pacote esteja maior de 30 caráteres.

- Da liberação 7.0 WLC avante, se a autenticação da Web está permitida no WLAN e você igualmente tem regras ACL CPU, as regras cliente-baseadas da autenticação da Web tomam sempre a precedência superior enquanto o cliente é não-autenticado no estado de WebAuth_Reqd. Uma vez que o cliente vai ao estado de CORRIDA, as regras ACL CPU obtêm aplicadas.

- Consequentemente, se o CPU ACL é permitido no WLC, uma regra reservar para o IP da interface virtual é exigida (em ALGUM sentido) nestas circunstâncias:
 - Quando o CPU ACL não tiver reservar TODA A regra para ambos sentidos.
 - Quando existe reservar TODA A regra, mas igualmente existe uma regra da NEGAÇÃO para a porta 443 ou 80 da precedência superior.

- A regra reservar para o IP virtual deve ser para o protocolo de TCP e a porta 80 se o secureweb é desabilitado, ou a porta 443 se o secureweb é permitido. Isto está precisado a fim permitir o acesso do cliente à autenticação bem sucedida do cargo do endereço IP de Um ou Mais Servidores Cisco ICM NT da interface virtual quando o CPU ACL é no lugar.

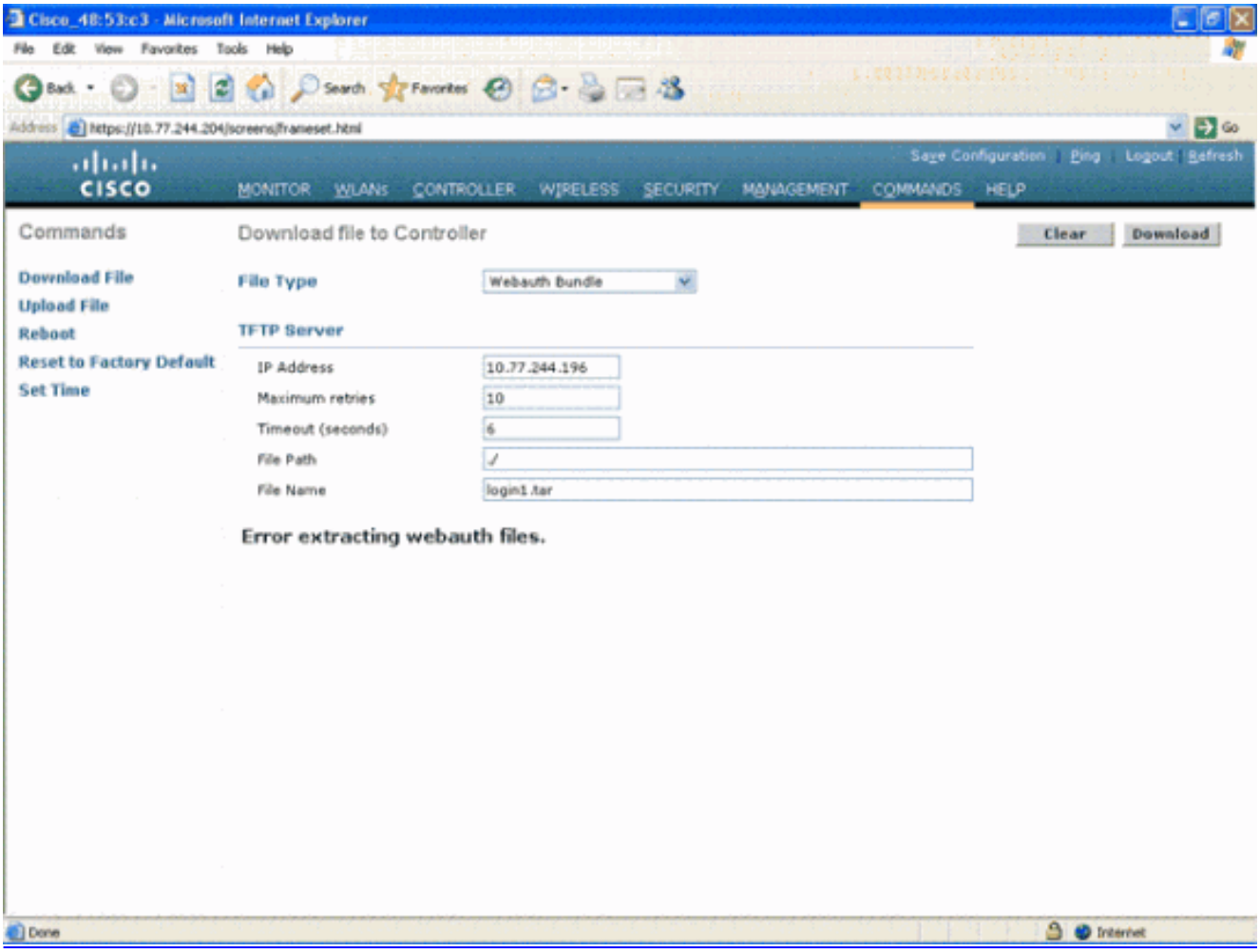
Solução de problemas de autenticação da Web

Depois que você configura a autenticação da Web e se a característica não trabalha como esperado, termine estas etapas:

1. Verifique se o cliente obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT. Se não, os usuários podem desmarcar o **DHCP exigiram a** caixa de verificação no WLAN e dão ao cliente Wireless um endereço IP estático. Isto supõe a associação com o Access point.
2. A próxima etapa no processo é resolução de DNS da URL no navegador da Web. Quando um cliente de WLAN conecta a um WLAN configurado para a autenticação da Web, o cliente obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP. O usuário abre um navegador da Web e incorpora um endereço de Web site. O cliente executa então a resolução de DNS para obter o endereço IP de Um ou Mais Servidores Cisco ICM NT do Web site. Agora, quando o cliente tenta alcançar o Web site, o WLC intercepta a sessão HTTP GET do cliente e reorienta o usuário à página de login da autenticação da Web.
3. , Assegure-se de consequentemente que o cliente possa executar a resolução de DNS para que a reorientação trabalhe. Em Microsoft Windows, escolha o **Iniciar > Executar**, entre no **CMD** a fim abrir uma janela de comando, e faça um “nslookup www.cisco.com” e veja se o

endereço IP de Um ou Mais Servidores Cisco ICM NT volta. Nos Mac/Linux, abra uma janela terminal e faça um “nslookup www.cisco.com” e veja se o endereço IP de Um ou Mais Servidores Cisco ICM NT volta.Se você acredita o cliente não obtém a resolução de DNS, você pode qualquer um:Incorpore ou o endereço IP de Um ou Mais Servidores Cisco ICM NT da URL (por exemplo, http://www.cisco.com é http://198.133.219.25).Tente datilografar todo o endereço IP de Um ou Mais Servidores Cisco ICM NT (mesmo não-existente) que dever resolver através do adaptador Wireless.Incorporando esta URL traz acima o página da web? Se sim, é mais provável um problema de DNS. Pôde igualmente ser um problema do certificado. O controlador, à revelia, usa um certificado auto-assinado e a maioria de navegadores da Web advertem contra seu uso.

4. Para a autenticação da Web com um página da web personalizado, assegure-se de que o código HTML para o página da web personalizado seja apropriado. Você pode transferir um script da autenticação da Web da amostra das transferências de software Cisco. Por exemplo, para os 5508 controladores, escolha o **Produtos > o Sem fio > o controlador do Wireless LAN > os controladores do Wireless LAN dos Controladores autônomos > do Cisco 5500 Series > o controlador > o software do Wireless LAN de Cisco 5508 no chassi > no pacote da autenticação da Web do controlador do Wireless LAN** e transfira o **arquivo webauth_bundle.zip**.Estes parâmetros estão adicionados à URL quando o navegador de Internet do usuário é reorientado à página de login personalizada:ap_mac - O MAC address do Access point a que o usuário Wireless é associado.switch_url - A URL do controlador a que as credenciais do usuário devem ser afixadas.reoriente - A URL a que o usuário é reorientado depois que a autenticação é bem sucedida.código de status - O código de status retornou do server da autenticação da Web do controlador.wlan - O WLAN SSID a que o usuário Wireless é associado.Estes são os códigos de status disponíveis:Código de status 1 - “você é entrado já. Nenhuma ação mais adicional é exigida em sua divisória”Código de status 2 - “você não é configurado para autenticar contra o portal da web. Nenhuma ação mais adicional é exigida em sua divisória”Código de status 3 - “o username especificado não pode ser usado neste tempo. Talvez o username é registrado já no sistema?”Código de status 4 - “você foi excluído.”Código de status 5 - “o nome de usuário e a combinação de senha que você incorporou são inválidos. Tente por favor outra vez.”
5. Todos os arquivos e imagens que precisam de aparecer no página da web personalizado devem ser empacotados em um arquivo de .tar antes que esteja transferido arquivos pela rede ao WLC. Assegure-se de que um dos arquivos incluídos no pacote de .tar seja login.html. Você recebe este Mensagem de Erro se você não inclui o arquivo de login.html:



Refira as diretrizes para a seção personalizada da autenticação da Web do exemplo de configuração da autenticação da Web do controlador do Wireless LAN para obter mais informações sobre de como criar um indicador personalizado da autenticação da Web.**Note**: Os arquivos que são grandes e os arquivos que têm nomes longos conduzirão a um erro da extração. Recomenda-se que as imagens estão no formato de .jpg.

6. Assegure-se de que a opção do **script** não esteja obstruída no navegador cliente porque o página da web personalizado no WLC é basicamente um script HTML.
7. Se você tem um **nome de host** configurado para a **interface virtual do** WLC, certifique-se de que a resolução de DNS está disponível para o nome de host da interface virtual. **Note**: Navegue ao menu do **controlador > das relações do** WLC GUI a fim atribuir um **nome de host DNS à** interface virtual.
8. Às vezes o Firewall instalado no computador de cliente obstrui a página de login da autenticação da Web. Desabilite o Firewall antes que você tente 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 server do Web-AUTH, que depende da rede. Quanto para a cada projeto de rede/solução executados, o utilizador final deve certificar-se que estas portas estão permitidas no firewall de rede.

10. Para que a autenticação da Web ocorra, o cliente deve primeiramente associar ao WLAN apropriado no WLC. Navegue ao menu do **monitor > dos clientes no** WLC GUI a fim ver se o cliente é associado ao WLC. Verifique se o cliente tem um endereço IP válido.
11. Desabilite os ajustes do proxy no navegador cliente até que a autenticação da Web esteja terminada.
12. O método de autenticação do web padrão é o protocolo password authentication (PAP).

Assegure-se de que a autenticação pap esteja permitida no servidor Radius para que esta trabalhe. A fim verificar o estado da authenticação do cliente, verifique debuga e mensagens de registro do servidor Radius. Você pode usar o **comando all aaa debugar no** WLC a fim ver debuga do servidor Radius.

13. Atualize o direcionador do hardware no computador ao código o mais atrasado do Web site do fabricante.
14. Verifique ajustes no suplicante (programa no portátil).
15. Quando você usar Windows zero suplicantes da configuração construído em Windows: Verifique que o usuário tem as correções de programa as mais atrasadas instaladas.Seja executado debuga no suplicante.
16. No cliente, gire sobre os logs EAPOL (WPA+WPA2) e RASTLS de uma janela de comando. Escolha o **Iniciar > Executar > o CMD**:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    A fim desabilitar os logs, execute o mesmo comando mas substitua-o permitem com desabilitação. Para o XP, todos os logs serão ficados situados em C:\Windows\tracing.
17. Se você ainda não tem nenhum página da web do início de uma sessão, recolha e analise esta 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 a edição não é resolved depois que você termina estas etapas, recolha estes debuga e o gerente do caso de suporte do uso a fim abrir um pedido do 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