Pesquisar defeitos a autenticação da Web em um controlador do Wireless LAN (WLC)

Índice

Introdução

Este documento 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 protocolo de pouco peso do Access point (LWAPP) /Control e abastecimento dos pontos de acesso Wireless (CAPWAP)
- Conhecimento de configurar o Access point de pouco peso (REGAÇO) e o WLC para a operação básica.
- Conhecimento básico da autenticação da Web e da autenticação da Web configurar em WLC. Para obter informações sobre de 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 7.0.98.0.

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 documento pode igualmente ser usado com estes hardware:

- Controladores sem fio Cisco série 5500
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Controladores sem fio Cisco série 2500
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2000 Series Wireless LAN Controllers
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Cisco Wireless LAN Controller Module
- Módulo de Serviços sem fio do Cisco Catalyst 6500 Series (WiSM)
- Controladores sem fio Cisco Flex série 7500
- Cisco Wireless Services Module 2 (WiSM2)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

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 pacotes DNS-relacionados dos pacotes DHCP-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 o 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.

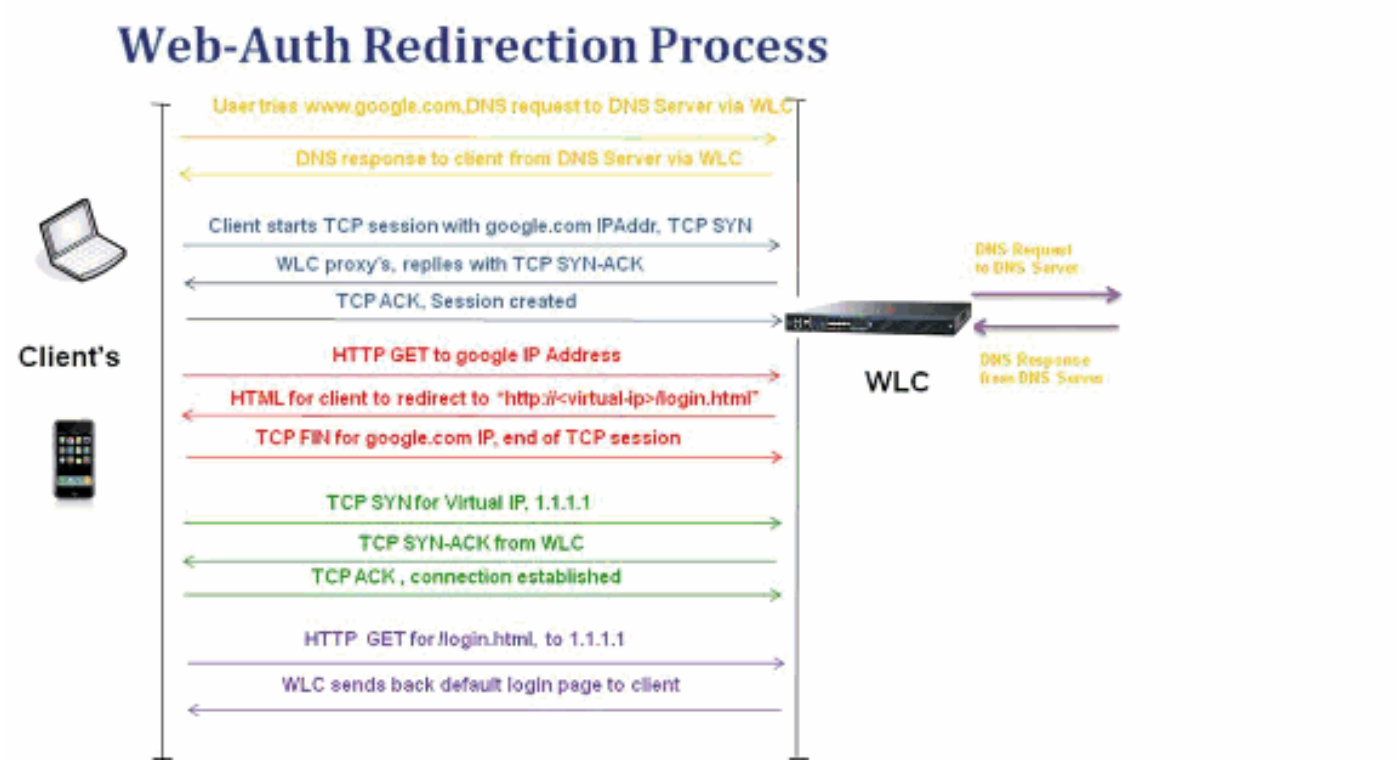
Quando a autenticação da Web é configurada no WLAN, o controlador obstrui todo o tráfego (até que o processo de autenticação esteja terminado) do cliente, à exceção do tráfego DHCP e DNS. Quando o cliente envia o primeiro HTTP GET à porta TCP 80, o controlador reorienta o cliente a https:1.1.1.1/login.html para processar. Este processo traz eventualmente acima o página da web

do início de uma sessão.

Nota: Quando você usa um servidor de Web externo para a autenticação da Web, algumas das Plataformas WLC precisam uma PRE-autenticação ACL para o servidor de Web externo, que inclui o controlador do Cisco 5500 Series, um Cisco 2100 Series controlador, o Cisco 2000 Series e o módulo de rede do controlador. Para as outras Plataformas WLC a PRE-autenticação ACL não é imperativa.

Nota: Mas, é uma boa prática configurar um ACL Pré-autenticação para o servidor de Web externo quando você usa uma autenticação do web externa.

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



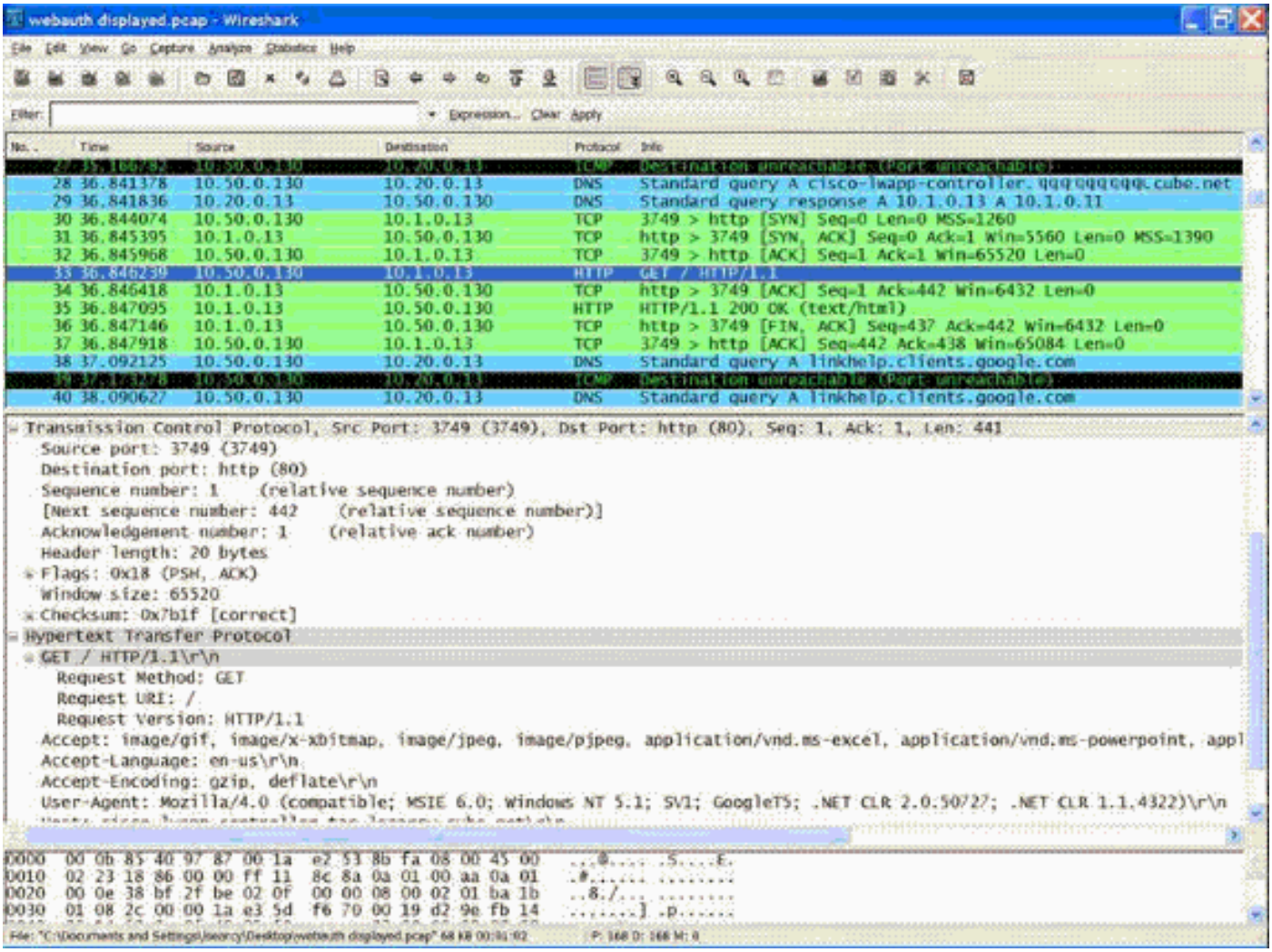
- Você abre o navegador da Web e datilografa dentro uma URL, por exemplo, `http://www.google.com`. O cliente manda um pedido DNS para que esta URL obtenha o IP para o destino. O WLC contorneia o pedido DNS ao servidor DNS e o servidor DNS responde para trás com uma resposta DNS, que contenha o endereço IP de Um ou Mais Servidores Cisco ICM NT do destino `www.google.com`, que é enviado por sua vez aos clientes Wireless
- O cliente tenta então abrir uma conexão de 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 de três maneiras e a conexão de TCP é estabelecida inteiramente.
- O cliente envia um pacote HTTP GET destinado a `www.google.com`. O WLC intercepta este pacote, envia-o para a manipulação da reorientação. O gateway de aplicativo HTTP prepara um corpo HTML e envia-o para trás como a resposta ao HTTP GET pedido pelo cliente. Este HTML faz o cliente para ir ao Web page URL do padrão 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://1.1.1.1/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 1.1.1.1 ao WLC.
- O WLC responde para trás com um TCP SYN-ACK e o cliente envia para trás um TCP ACK ao WLC a fim terminar o aperto de mão.
- O cliente envia um HTTP GET para /login.html destinou a 1.1.1.1 a fim pedir para 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 de navegador onde o usuário pode ir adiante e início de uma sessão.

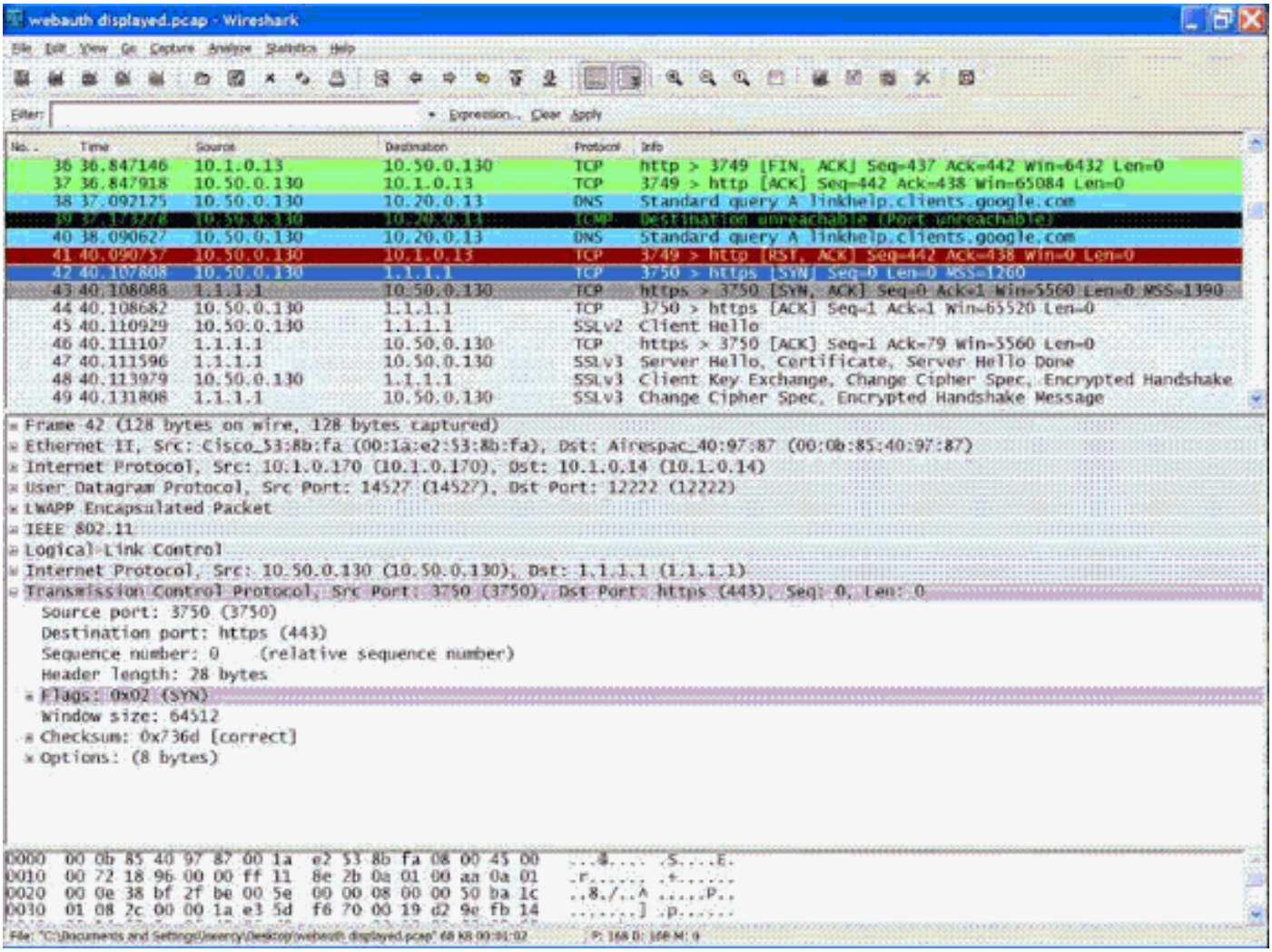
Exemplo: Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente é 10.50.0.130. O cliente resolveu a URL ao servidor de Web que alcançava 10.1.0.13. Como você pode ver, o cliente fez o reconhecimento de sentido três para pôr em andamento a conexão de TCP e enviou então um pacote HTTP GET que começa com pacote 30. O controlador está interceptando os pacotes e está respondendo com código 200. O pacote do código 200 tem uma reorientação URL nele:

```
<HTML><HEAD><TITLE>Cisco Systems Inc. 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://1.1.1.1/login.html?redirect=cisco-lwapp-controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

Fecha então a conexão de TCP através do reconhecimento de sentido três.



O cliente liga então a conexão de HTTPS à reorientação URL que a envia a 1.1.1.1, 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 42 começa as transações.



Você tem uma opção para configurar o Domain Name para o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do controlador do Wireless LAN. 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 e 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 IP 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 SSL.

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

- Autenticação da Web usando 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.
- Autenticação da Web usando 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.
- Autenticação da Web usando 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.

Nota: O pacote personalizado do AUTH 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.

Nota: Do WLC libere 7.0 avante, se a autenticação da Web está permitida no WLAN e você igualmente tem regras ACL CPU, as regras baseadas cliente 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.

Nota: 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 lá igualmente existe uma regra da NEGAÇÃO para a porta 443 ou 80 da precedência superior.

Nota: 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.

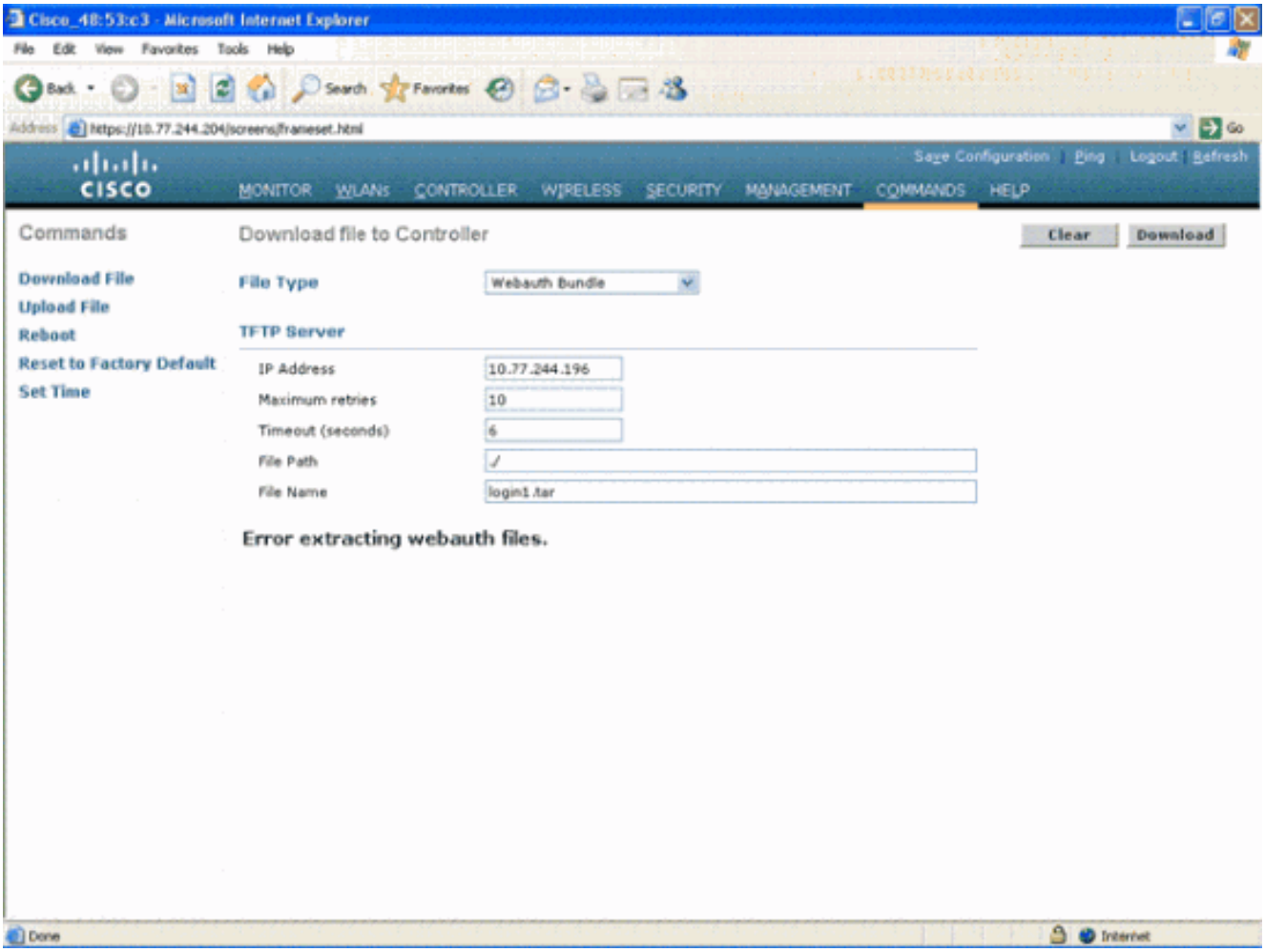
Pesquisando defeitos a autenticação da Web

Depois que você configura a autenticação da Web, se a característica não trabalha como esperado, termine estes passos de Troubleshooting:

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 exigido no** WLAN e dar ao cliente Wireless um endereço IP estático. Isto supõe a associação com o Access point. Refira a seção das *edições do endereçamento de IP de problemas de cliente do Troubleshooting na rede de Cisco Unified Wireless pesquisando defeitos problemas relacionados DHCP*.
2. Em versões WLC mais cedo do que 3.2.150.10, você deve manualmente entrar em **https://1.1.1.1/login.html** a fim navegar ao indicador da autenticação da Web.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 o HTTP obtém a sessão 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 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.Em 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 está obtendo 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 alcançar diretamente a página do webauth do controlador com https:// <Virtual_interface_IP_Address>/login.html. Tipicamente este é http://1.1.1.1/login.html.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 a utilização deles.

4. Para a autenticação da Web usando o 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 4400 controladores, escolha o **Produtos > o Sem fio > o controlador do Wireless LAN > os Controladores autônomos > o Controladores de LAN sem fio Cisco série 4400 > o controlador > o software do Wireless LAN de Cisco 4404 no chassi > na autenticação da Web Bundle-1.0.1 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 de transferir arquivos pela rede ao WLC. Assegure-se de que um dos arquivos incluídos no pacote do alcatrão 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.**Nota:** 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. O internet explorer 6.0 é SP1 ou mais tarde o navegador recomendado para o uso da autenticação da Web. Outros navegadores podem ou não podem trabalhar.
7. 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. Em IE 6.0, isto é desabilitado à revelia para efeitos de segurança.**Nota:** O PNF acima do construtor precisa de ser desabilitado no navegador se você configurou o algum estala acima mensagens para o usuário.**Nota:** Se você consulta a um local dos **https**, a reorientação não trabalha. Refira a identificação de bug Cisco CSCar04580 (clientes registrados somente) para mais informação.
8. 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.**Nota:** Navegue ao menu do **controlador > das relações do** WLC GUI a fim atribuir um **nome de host DNS à** interface virtual.
9. 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.
10. 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.

11. 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.
12. Desabilite os ajustes do proxy no navegador cliente até que a autenticação da Web esteja terminada.
13. O método de autenticação do web padrão é 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 ver debuga do servidor Radius.
14. Atualize o direcionador do hardware no computador ao código o mais atrasado do Web site do fabricante.
15. Verifique ajustes no suplicante (programa no portátil).
16. 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.
17. No cliente, gire sobre os logs EAPOL (WPA+WPA2) e RASTLS de uma janela de comando, Iniciar > Executar > 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.
18. 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`
19. Se a edição não é resolved depois que você termina estas etapas, recolha estes debuga e usam a ferramenta do pedido do serviço TAC (clientes registrados somente) 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 da autenticação da Web do controlador do Wireless LAN
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Suporte Técnico e Documentação - Cisco Systems