Configurar o redirecionamento HTTPS pela autenticação da Web

Contents

Introduction

Este documento descreve a configuração sobre o redirecionamento de autenticação da Web sobre HTTPS. Este é um recurso apresentado na Cisco Unified Wireless Network (CUWN) versão 8.0.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Conhecimento básico da autenticação na Web do Wireless LAN Controller (WLC)
- Como configurar o WLC para autenticação da Web.

Componentes Utilizados

As informações neste documento são baseadas no Cisco 5500 Series WLC que executa o firmware CUWN versão 8.0.

> **Note**: A explicação de configuração e autenticação da Web fornecida neste documento é aplicável a todos os modelos de WLC e a qualquer imagem CUWN igual ou superior a 8.0.100.0.

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. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

A autenticação da Web é um recurso de segurança de Camada 3. Bloqueia todo o tráfego IP/de dados, exceto pacotes relacionados ao DHCP/pacotes relacionados ao DNS, de um cliente específico até que um cliente sem fio tenha fornecido um nome de usuário e uma senha válidos.A autenticação da Web é normalmente usada por clientes que desejam implantar uma rede de acesso de convidado.A autenticação da Web é iniciada quando o controlador intercepta o primeiro pacote HTTP TCP (porta 80) GET do cliente.

Para que o navegador da Web do cliente chegue tão longe, ele deve primeiro obter um endereço IP e fazer uma tradução do URL para o endereço IP (resolução DNS) para o navegador da Web. Isso permite que o navegador da Web saiba qual endereço IP enviar o HTTP GET. Quando o cliente envia o primeiro HTTP GET à porta TCP 80, o controlador redireciona o cliente para https:<virtual IP>/login.html para processamento. Esse processo eventualmente exibe a página da Web de login.

Antes das versões anteriores ao CUWN 8.0 (ou seja, até 7.6), se o cliente sem fio apresentar uma página HTTPS (TCP 443), a página não será redirecionada para o portal de autenticação da Web. À medida que cada vez mais sites começam a usar HTTPS, esse recurso é incluído nas versões CUWN 8.0 e posteriores. Com esse recurso em vigor, se um cliente sem fio tentar https://<site>, ele será redirecionado para a página de login do web-auth. Além disso, esse recurso é muito útil para os dispositivos que enviam solicitações https com um aplicativo (mas não com um navegador).

Erro de certificado

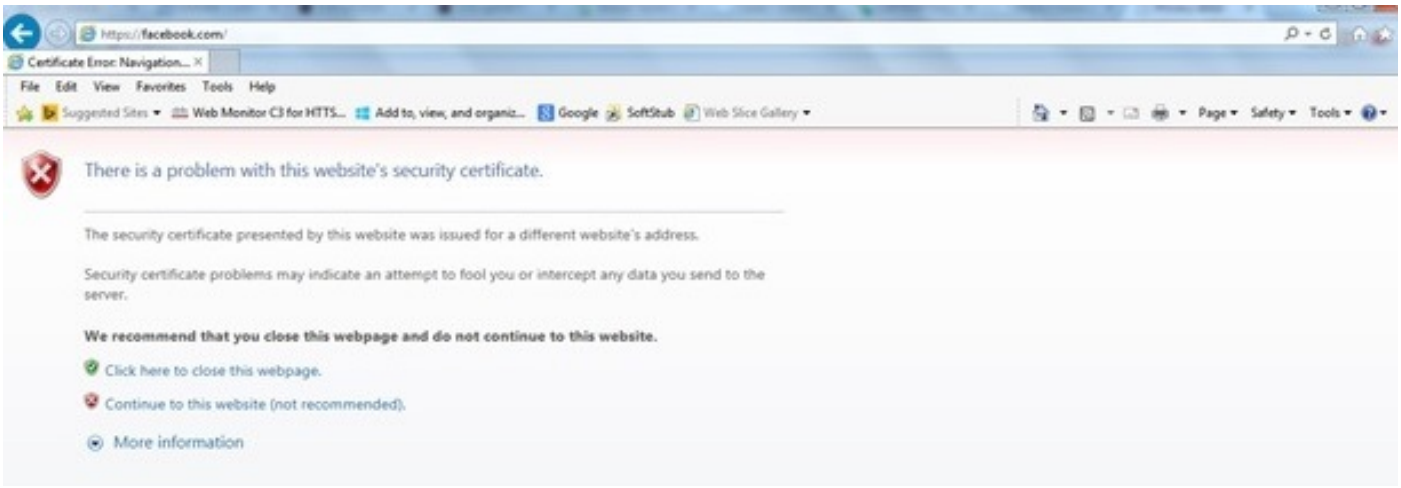
A mensagem de aviso "certificado não é emitido por uma autoridade de certificação confiável". aparece no navegador após você configurar o recurso https-redirect. Isso é visto mesmo se você tiver um certificado raiz ou encadeado válido no controlador, como mostrado na Figura 1 e na Figura 2. O motivo é que o certificado instalado no controlador é emitido para seu endereço IP virtual.

> **Note**: Se você tentar um redirecionamento HTTP e tiver esse certificado na WLC, não obterá este erro de aviso de certificado. No entanto, no caso do redirecionamento HTTPS, esse erro é exibido.

Quando o cliente tenta HTTPS://<web-site> , o navegador espera que o certificado emitido para o endereço IP do site seja resolvido pelo DNS. No entanto, o que eles recebem é o certificado emitido para o servidor web interno da WLC (endereço IP virtual) que faz com que o navegador emita o aviso. Isso é simplesmente por causa da maneira como o HTTPS funciona e sempre acontece se você tentar interceptar a sessão HTTPS para que o redirecionamento de autenticação da Web funcione.

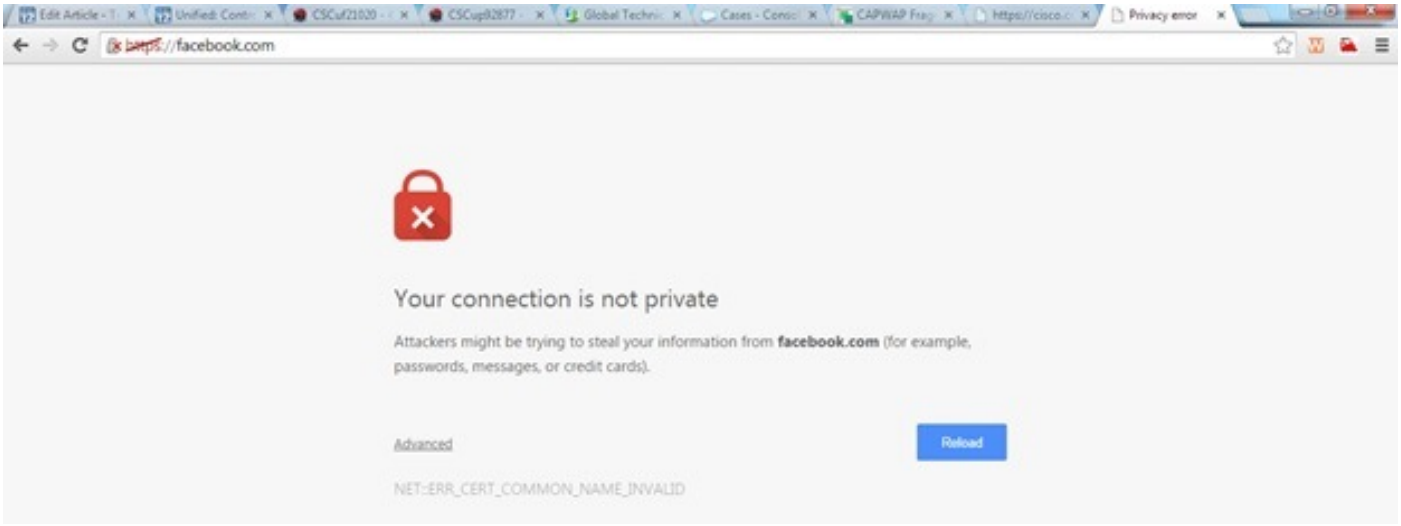
Você pode ver mensagens de erro de certificado diferentes em navegadores diferentes, mas todas estão relacionadas ao mesmo problema descrito anteriormente.

Figure 1



Este é um exemplo de como o erro pode aparecer no Chrome:

Figure 2



Configurar

Configurar a WLC para o redirecionamento HTTPS

Essa configuração pressupõe que a LAN sem fio (WLAN) já está configurada para a segurança de autenticação da Web da Camada 3. Para ativar ou desativar o redirecionamento HTTPS nesta WLAN com autenticação da Web:

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

Como mostra a configuração de exemplo, isso pode afetar o throughput de um redirecionamento HTTPS, mas não do redirecionamento HTTP

Para obter mais informações e uma configuração das WLANs de autenticação da Web, consulte

Autenticação da Web no controlador de WLAN.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

```
(WLC)>show network summary

Web Auth Secure Web ..................... Enable
Web Auth Secure Redirection ............. Enable
```

1. Ative estas depurações:
   ```
   (WLC) debug client
   ```

   ```
   (WLC)> debug web-auth redirect enable
   ```
2. Verifique as depurações:
   ```
   (WLC) >show debug

   MAC Addr 1.............................. 24:77:03:52:56:80

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Associe o cliente ao SSID habilitado para autenticação da Web.
4. Procure estas depurações:
   ```
   *webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received connection.
   client socket = 9
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204
   *webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled,
   checking for wispr in HTTP GET, client mac=24:77:3:52:56:80
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect
   URL according to configured Web-Auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName
   for virtual IP(wirelessguest.test.com)
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web
   config for WLAN ID:10
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is
   enabled, checking on web-auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,
   using URL:https://wirelessguest.test.com/fs/customwebauth/login.html
   ```

   Note: Certifique-se de que a Secure Web (config network secureweb enable/disable) ou a web-auth secure (config network web-auth secureweb enable/disable) estejam ativados para fazer o redirecionamento HTTPS funcionar. Observe também que pode haver uma ligeira redução na taxa de transferência quando o redirecionamento sobre HTTPS é usado.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.