Configurar o HTTPS reorientam sobre o Web-AUTH

Índice

Introdução

Este documento descreve a configuração sobre a reorientação da autenticação da Web sobre o HTTPS. Esta é uma característica introduzida na liberação 8.0 da rede de Cisco Unified Wireless (CUWN).

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

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

Componentes Utilizados

A informação neste documento é baseada no Cisco 5500 Series WLC que executa a versão de firmware 8.0 CUWN.

> Nota: A configuração e a explicação do Web-AUTH fornecida neste documento são aplicáveis a todos os modelos WLC e a toda a imagem CUWN iguais a ou mais tarde do que 8.0.100.0.

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.

Informações de Apoio

A autenticação da Web é uns recursos de segurança da camada 3. Obstrui todo o tráfego IP/data, exceto pacotes DNS-relacionados dos pacotes DHCP-relacionados, de um cliente específico até que um cliente Wireless forneça um nome de usuário válido e uma senha. 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 o cliente envia o primeiro HTTP GET à porta TCP 80, o controlador reorienta o cliente aos https: IP>/login.html <virtual para processar. Este processo traz eventualmente acima o página da web do início de uma sessão.

Antes das liberações mais cedo do que CUWN 8.0 (isto é até 7.6), se o cliente Wireless apresenta uma página HTTPS (TCP 443), a página não é reorientada ao portal da autenticação da Web. Enquanto cada vez mais os Web site começam a usar o HTTPS, esta característica está incluída nas liberações CUWN 8.0 e mais atrasado. Com esta característica no lugar, se um cliente Wireless tenta o <website> de https://, é reorientada à página de login do Web-AUTH. Igualmente esta característica é muito útil para os dispositivos que enviam pedidos dos https com um aplicativo (mas não com um navegador).

Erro do certificado

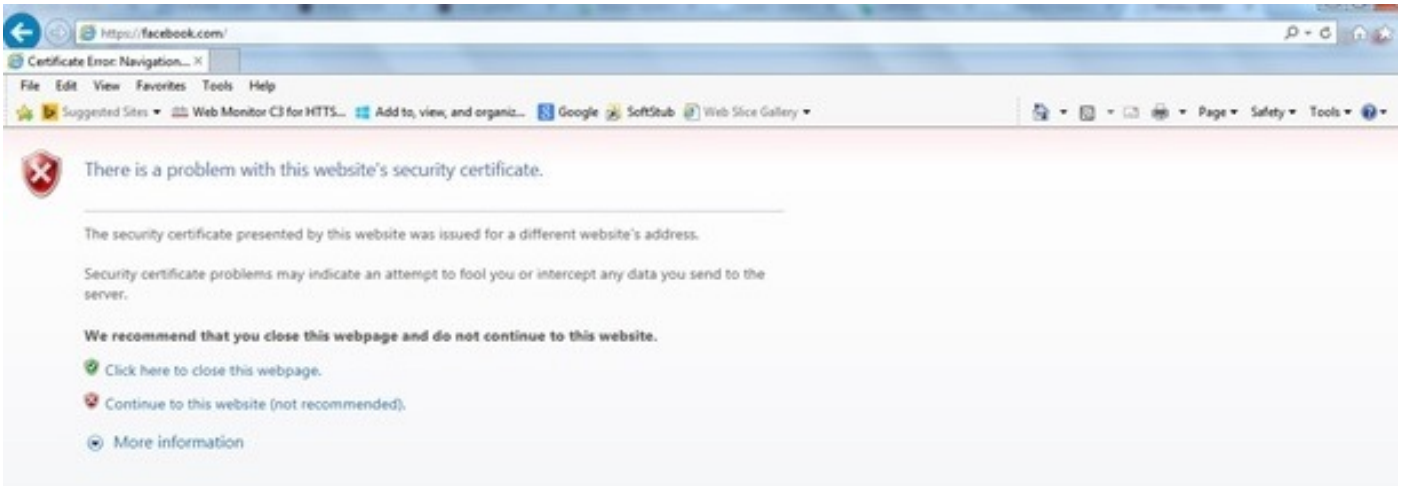
O mensagem de advertência “certificado não é emitido por um Certificate Authority confiado.” aparece no navegador depois que você configura a característica da https-reorientação. Isto é visto mesmo se você tem uma raiz válida ou um certificado acorrentado no controlador segundo as indicações de figura 1 e de figura 2. A razão é que o certficiate que você instalou no controlador está emitido a seu endereço IP de Um ou Mais Servidores Cisco ICM NT virtual.

> Nota: Se você tenta um redirecionamento de HTTP e tem este certifcate no WLC, você não obtém a este certificado erro de advertência. Porém no caso de HTTPS-reoriente, este erro aparece.

Quando o cliente tenta o <website> de HTTPS://, o navegador espera o certificado emitido ao endereço IP de Um ou Mais Servidores Cisco ICM NT do local resolvido pelo DNS. Contudo, o que recebem é o certificado que foi emitido ao servidor de Web interno do WLC (endereço IP de Um ou Mais Servidores Cisco ICM NT virtual) que faz com que o navegador emita o aviso. Isto é puramente devido à maneira que o HTTPS trabalha e acontece sempre se você tenta interceptar a sessão HTTPS para que a reorientação do Web-AUTH trabalhe.

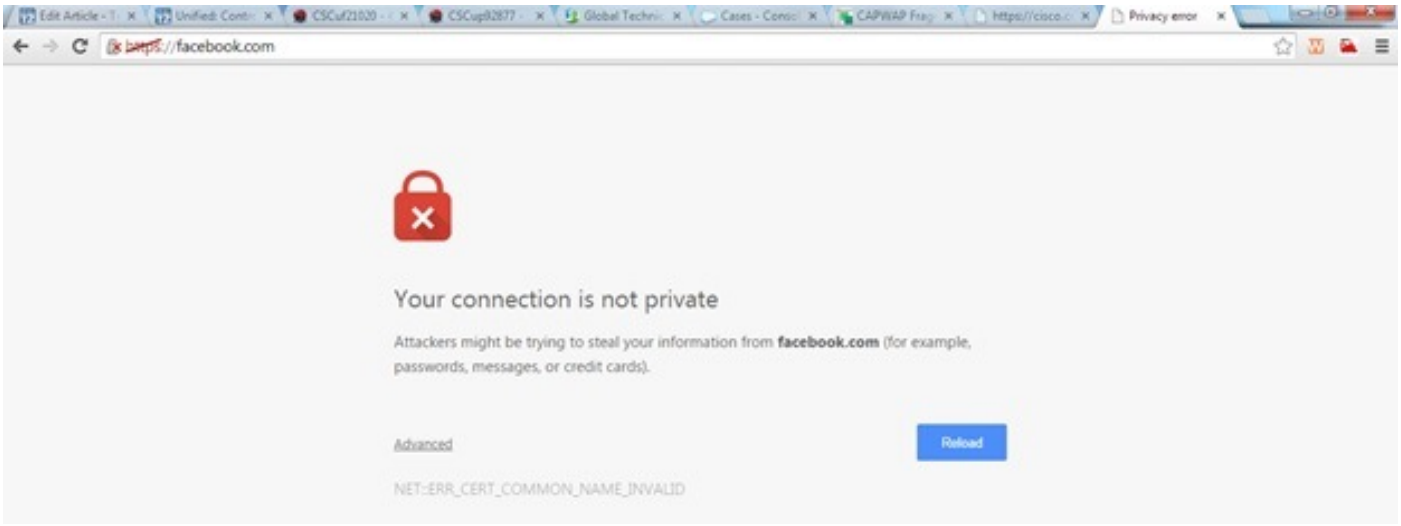
Você pôde ver Mensagens de Erro diferentes do certificado em navegadores diferentes mas em todos relacionar-se como descrito anteriormente ao mesmo problema.

Figura 1



Este é um exemplo de como o erro pode aparecer em Chrome:

Figura 2



Configurar

Configurar o WLC para o redirecionamento em https

Esta configuração supõe que o Wireless LAN (WLAN) está configurado já para a Segurança do authentciation da Web da camada 3. A fim permitir ou o desabilitação HTTPS reorienta neste Web-AUTH WLAN:

```
(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
```

Porque o exemplo de configuração mostra, este pôde impactar a taxa de transferência para um redirecionamento em https mas não o Redireção do HTTP

Para mais informação e uma configuração da autenticação da Web WLAN, veja a autenticação da Web no controlador de WLAN.

Verificar

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

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

```
(WLC)>show network summary

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

1. Permita estes debuga:`(WLC) debug client <MAC address>`

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

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

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Associe o cliente ao SSID permitido Web-AUTH.
4. Procure estes debuga:`*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`Nota: Assegure-se de que a Web segura (o secureweb da rede da configuração permite/desabilitação) ou o Web-AUTH seguro (o secureweb do Web-AUTH da rede da configuração permite/desabilitação) estejam permitidos a fim fazer o HTTPS reorientar o trabalho. Igualmente note que pôde haver uma leve redução na taxa de transferência quando a reorientação sobre o HTTPS é usada.

Troubleshooting

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