

Autenticação do web externa com o guia de distribuição do switching local de FlexConnect

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Visão geral do recurso](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento explica como usar um servidor web externo com switching local FlexConnect para políticas de web diferentes.

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico sobre a arquitetura de FlexConnect e os Access point (AP)
- Conhecimento em como estabelecer e configurar um servidor de Web externo
- Conhecimento em como estabelecer e configurar o DHCP e os servidores DNS

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- O controlador do Wireless LAN do Cisco 7500 (WLC) esse executa a versão de firmware 7.2.110.0
- Access point de pouco peso do Cisco 3500 Series (REGAÇO)
- Servidor de Web externo que hospeda a página de login da autenticação da Web
- DNS e servidores DHCP na site local para o address resolution e a alocação de endereço IP aos clientes Wireless

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Embora um 7500 Series WLC seja usado para este guia de distribuição, esta característica é apoiada em 2500, 5500, e WiSM-2 WLC. 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.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Visão geral do recurso

Esta característica estende a capacidade de executar a autenticação da Web a um servidor de Web externo do AP no modo de FlexConnect, para os WLAN com localmente o tráfego comutado (FlexConnect – switching local). Antes que a liberação 7.2.110.0 WLC, a autenticação da Web a um servidor interno estiver apoiada para AP no modo local ou no modo de FlexConnect para WLAN com centralmente tráfego comutado (FlexConnect – interruptor central).

Referido frequentemente como a autenticação do web externa, esta característica estende a capacidade para o switching local WLAN de FlexConnect de apoiar toda a Web da camada 3 reorienta os tipos da Segurança fornecidos atualmente pelo controlador:

- Autenticação da Web
- Web Passagem-atraves de
- A Web condicional reorienta
- A página do respingo condicional reorienta

Considerando que um WLAN configurado para a autenticação da Web e para o switching local, a lógica atrás desta característica é distribuir e aplicar o Access Control List de FlexConnect da PRE-autenticação (ACL) diretamente a nível AP em vez do nível WLC. Desta maneira, o AP comutará os pacotes que vêm do cliente Wireless que são permitidos pelo ACL, localmente. Os pacotes não permitidos são enviados ainda sobre o túnel CAPWAP ao WLC. Por outro lado, quando o AP receber o tráfego sobre a relação prendida, se permitido pelo ACL, o enviará ao cliente Wireless. Caso contrário, o pacote será perdido. Uma vez que o cliente é autenticado e autorizado, a PRE-autenticação FlexConnect ACL está removida, e todo o tráfego de dados do cliente é permitido e comutado localmente.

Nota: Esta característica trabalha sob a suposição que o cliente pode alcançar o servidor interno do VLAN localmente comutado.

Resumo:

- WLAN configurado para o switching local de FlexConnect e a Segurança L3
- FlexConnect ACL será usado como a PRE-autenticação ACL
- FlexConnect ACL configurado uma vez deve ser empurrado para o base de dados AP através do grupo do cabo flexível ou através do AP individual, ou pode ser aplicado no WLAN
- O AP permite todo o tráfego que combina a PRE-autenticação ACL a ser comutada localmente

Procedimento:

Termine estas etapas a fim configurar esta característica:

1. Configurar um WLAN para o switching local de FlexConnect.
2. A fim permitir a autenticação do web externa, você precisa de configurar a política da Web

como a política de segurança para o WLAN localmente comutado. Isto inclui uma destas quatro opções: Autenticação Passagem-através de A Web condicional reorienta A Web da página do respingo reorienta Este capturas de documento um exemplo para a autenticação da Web: Os primeiros dois métodos são similares e podem ser agrupados como métodos de autenticação da Web de um ponto de vista da configuração. Os segundos dois (condicional reorienta e página do respingo) são políticas da Web e podem ser agrupados como métodos da Web-política.

3. A PRE-autenticação FlexConnect ACL precisa de ser configurada permitindo que os clientes Wireless alcancem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor interno. O tráfego ARP, DHCP e DNS automaticamente é permitido e não precisa de ser especificado. Sob a Segurança > o Access Control List, escolha **FlexConnect ACL**. Então, o clique **adiciona** e define os nomes e as regras como um controlador normal ACL. **Nota:** FlexConnect ACL é diferente dos ACL regulares porque não há nenhuma necessidade de especificar a direção de tráfego. Cada regra contará para entrante e o tráfego de saída. Também, se você quer configurar a autenticação da Web para WLAN centralmente comutados (no modo local ou no cabo flexível) você ainda precisa de usar ACL regulares. Consequentemente, você precisa de especificar o sentido para o tráfego.
4. Uma vez que FlexConnect ACL é criado deve ser aplicado que pode ser feito a níveis diferentes: AP, grupo de FlexConnect e WLAN. Esta última opção (cabo flexível ACL no WLAN) é somente para a autenticação da Web e a Web Passagem-através para de outros dois métodos sob a política da Web, tal como condicional e o respingo reorienta. Os ACL podem somente ser aplicados no AP ou dobrar o grupo. Está aqui um exemplo de um ACL atribuído a nível AP. Vá ao **Sem fio > o AP seletor**, a seguir clica a aba de **FlexConnect**: Clique o link **externo de WebAuthentication ACL**. Então, escolha o ACL para a identificação particular WLAN: Similarmente, para a política ACL da Web (por exemplo, o condicionais reorientam ou a página do respingo reorienta), você receberá uma opção para selecionar o cabo flexível conecta o ACL sob WebPolicies depois que você clica o mesmo link externo de WebAuthentication ACL. Isto é mostrado aqui:
5. O ACL pode igualmente ser aplicado a nível do grupo de FlexConnect. A fim fazer isto, vá à aba do **mapeamento WLAN-ACL na** configuração de grupo de FlexConnect. Então, escolha a identificação WLAN e o ACL que você quer se aplicar. Clique em Add. Isto é útil quando você quer definir um ACL para um grupo de AP. Similarmente, porque a política ACL da Web (para a Web condicional e do respingo da página reorienta), você precisa de selecionar a aba de **WebPolicies**.
6. A autenticação da Web e a Web Passagem-através do cabo flexível ACL podem igualmente ser aplicadas no WLAN. A fim fazer isto, escolha o ACL da gota-para baixo de **WebAuth FlexACL** sob a aba da camada 3 no > segurança WLAN.
7. Para a autenticação do web externa, a reorientação URL precisa de ser definida. Isto pode ser feito a nível global ou a nível WLAN. Para o nível WLAN, clique o sinal do **config global da ultrapassagem** e introduza a URL. A nível global, vá ao **AUTH da Segurança > da Web > à página de login da Web**. **Limitações:** A autenticação da Web (interna ou a um servidor interno) exige o cabo flexível AP reagir do modo conectado. A autenticação da Web não é apoiada se o cabo flexível AP reage do modo independente. A autenticação da Web (interna ou a um servidor interno) é apoiada somente com autenticação central. Se um WLAN configurado para o switching local é configurado para a autenticação local, você não pode executar a autenticação da Web. Toda a reorientação da Web é executada no WLC e não a nível AP.

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)