External Web Authentication with FlexConnect Local Switching Deployment Guide

Contents

Introduction

This document explains how to use an External Web Server with FlexConnect Local Switching for different Web Policies.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge about FlexConnect Architecture and Access Points (APs)
- Knowledge on how to set up and configure an external web server
- Knowledge on how to set up and configure DHCP and DNS servers

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 7500 Wireless LAN Controller (WLC) that runs firmware release 7.2.110.0
- Cisco 3500 Series Lightweight Access Point (LAP)
- External web server that hosts the web authentication login page
- DNS and DHCP Servers on local site for address resolution and IP address allocation to wireless clients

The information in this document was created from the devices in a specific lab environment. Although a 7500 Series WLC is used for this deployment guide, this feature is supported on 2500, 5500, and WiSM-2 WLCs. 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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Feature Overview

This feature extends the capability of performing Web Authentication to an external web server from the AP in FlexConnect mode, for the WLANs with locally switched traffic (FlexConnect – Local Switching). Before WLC Release 7.2.110.0, the Web Authentication to an external server was supported for APs in Local mode or FlexConnect mode for WLANs with centrally switched traffic (FlexConnect – Central Switching).

Often referred to as External Web Authentication, this feature extends the capability for FlexConnect Local Switching WLAN to support all the Layer 3 Web Redirect Security types currently provided by the controller:

- Web Authentication
- Web Pass-through
- Web Conditional Redirect
- Splash Page Conditional Redirect

Considering a WLAN configured for Web Authentication and for local switching, the logic behind this feature is to distribute and apply the Pre-Authentication FlexConnect Access Control List (ACL) directly at the AP level instead of the WLC level. In this way, the AP will switch the packets coming from the wireless client that are allowed by the ACL, locally. The packets not allowed are still sent over the CAPWAP tunnel to the WLC. On the other hand, when the AP receives the traffic over the wired interface, if allowed by the ACL, will forward it to the wireless client. Otherwise, the packet is dropped. Once the client is authenticated and authorized, the Pre-Authentication FlexConnect ACL is removed, and all client data traffic is allowed and switched locally.

Note: This feature works under the assumption that the client can reach the external server from the locally switched VLAN.

Summary:

- WLAN configured for FlexConnect Local Switching and L3 Security
- FlexConnect ACLs will be used as Pre-Authentication ACLs
- FlexConnect ACLs once configured must be pushed to the AP database via Flex Group or via Individual AP, or can be applied on the WLAN
- AP allows all the traffic which matches Pre-Authentication ACL to be switched locally

Procedure:

Complete these steps in order to configure this feature:

1. Configure a WLAN for FlexConnect Local Switching.
2. In order to enable External Web Authentication, you need to configure Web Policy as the security policy for the locally switched WLAN. This includes one of these four options:AuthenticationPass-throughConditional Web RedirectSplash Page Web RedirectThis document captures an example for Web Authentication:The first two methods are similar and can be grouped as Web-Authentication methods from a configuration point of view. The

second two (Conditional Redirect and Splash Page) are Web Policies and can be grouped as Web-Policy methods.

3. The Pre-Authentication FlexConnect ACL needs to be configured allowing the wireless clients to reach the IP address of the external server. ARP, DHCP and DNS traffic are automatically allowed and do not need to be specified. Under Security > Access Control List, choose **FlexConnect ACLs**. Then, click **Add** and define the names and rules as a normal controller ACL.**Note:** You will need to create reverse rules for the traffic each time.
4. Once FlexConnect ACLs are created it should be applied which can be done at different levels: AP, FlexConnect Group and WLAN. This last option (Flex ACL at WLAN) is only for Web Authentication and Web Pass-through for other two methods under Web Policy, such as Conditional and Splash Redirect. ACLs can only be applied at the AP or Flex Group. Here is an example of an ACL assigned at the AP level. Go to **Wireless > select AP**, then click the **FlexConnect** tab:Click the **External WebAuthentication ACLs** link. Then, choose the ACL for the particular WLAN Id:Similarly, for the Web Policy ACL (for example, the Conditional Redirect or Splash Page Redirect), you will receive an option to select the Flex Connect ACL under WebPolicies after you click the same External WebAuthentication ACLs link. This is shown here:
5. The ACL can also be applied at the FlexConnect Group level. In order to do this, go to the **WLAN-ACL mapping** tab in the FlexConnect Group configuration. Then, choose the WLAN Id and the ACL you want to apply. Click **Add**. This is useful when you want to define an ACL for a group of APs.Similarly, for the Web Policy ACL (for Conditional and Splash Page Web Redirect), you need to select the **WebPolicies** tab.
6. Web Authentication and Web Pass-through Flex ACLs can also be applied on the WLAN. In order to do this, choose the ACL from the **WebAuth FlexACL** drop-down under the Layer 3 tab in WLAN > Security.
7. For External Web Authentication, the redirect URL needs to be defined. This can be done at a global level or at the WLAN level. For the WLAN level, click the **Over-ride Global Config** checkmark and insert the URL. At the global level, go to **Security > Web Auth > Web Login Page**:**Limitations:**Web Authentication (internal or to an external server) requires the Flex AP to be in Connected mode. Web Authentication is not supported if Flex AP is in Standalone mode.Web Authentication (internal or to an external server) is only supported with Central Authentication. If a WLAN configured for local switching is configured for Local Authentication, you cannot perform Web Authentication.All Web Redirection is performed at the WLC and not at the AP level.

Related Information

- **Technical Support & Documentation - Cisco Systems**