Configuring Layer 3 Security

Configuring Layer 3 Security Using Web Authentication

Prerequisites for Configuring Web Authentication on a WLAN

- To initiate HTTP/HTTPS web authentication redirection, use HTTP URL or HTTPS URL.
- If the CPU ACLs are configured to block HTTP / HTTPS traffic, after the successful web login authentication, there could be a failure in the redirection page.
- Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.
- When you enable web authentication for a WLAN, a message appears indicating that the controller forwards DNS traffic to and from wireless clients prior to authentication. We recommend that you have a firewall or intrusion detection system (IDS) behind your guest VLAN to regulate DNS traffic and to prevent and detect any DNS tunneling attacks.
- If the web authentication is enabled on the WLAN and you also have the CPU ACL rules, the client-based web authentication rules take higher precedence as long as the client is unauthenticated (in the webAuth_Reqd state). Once the client goes to the RUN state, the CPU ACL rules get applied. Therefore, if the CPU ACL rules are enabled in the controller, an allow rule for the virtual interface IP is required (in any direction) with the following conditions:
    - When the CPU ACL does not have an allow ACL rule for both directions.
    - When an allow ALL rule exists, but also a DENY rule for port 443 or 80 of higher precedence.
- The allow rule for the virtual IP should be for TCP protocol and port 80 (if secureweb is disabled) or port 443 (if secureweb is enabled). This process is required to allow client's access to the virtual interface IP address, post successful authentication when the CPU ACL rules are in place.

Restrictions for Configuring Web Authentication on a WLAN

- Web authentication is supported only with these Layer 2 security policies: open authentication, open authentication+WEP, and WPA-PSK. With the 7.4 release, web authentication is supported for use with 802.1X.
- Special charecters are not supported in the username field for web-authentication.
- When clients connect to a WebAuth SSID and a preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

  You can select the following identity stores to authenticate web-auth user, under **WLANs > Security > AAA servers > Authentication priority** order for web-auth user section:

  - Local
  - RADIUS
  - LDAP

  If multiple identity stores are selected, then the controller checks each identity store in the list, in the order specified, from top to bottom, until authentication for the user succeeds. The authentication fails, if the controller reaches the end of the list and user remains un-authenticated in any of the identity stores.

Information About Web Authentication

WLANs can use web authentication only if VPN passthrough is not enabled on the controller. Web authentication is simple to set up and use and can be used with SSL to improve the overall security of the WLAN.

Using Web Authentication with 802.1x

There are three types of timers that are active when your WLAN uses web authentication along with 802.1x. These timers are based on the timeout value received from the AAA server or the WLAN session timeout:

- Session timer—Client session timeout configured for a WLAN that requires reauthentication. This timer starts after a successful web authentication.
- Reauthentication timer—Timer that is used to trigger client reauthentication for WPA1.
- PMK cache timer—Cache lifetime timer that is used to trigger client reauthentication for WPA2.

This section describes the two scenarios that clients can encounter when a WLAN is configured to use web authentication along with 802.1x.

Client associated to a single controller—In this scenario, when the reauthentication or PMK cache timer expires, the client reauthenticates, updates the reauthentication/PMK cache timer and remains in the run state. When the client session timer (ST) expires, the client is deauthenticated even if the reauthentication/PMK cache timer is still valid.

Client roams from one controller to another controller—In this scenario, after the client roams the foreign controller triggers an L2 authentication and the anchor controller triggers an L3 authentication. The 802.1x reauthentication/PMK timer runs on the foreign controller and the client session timer runs on the anchor controller. When the reauthentication/PMK timer expires, 802.1x client reauthentication happens and the client is in the run state. Client is deauthenticated only when the client session timer expires.

The session timeout depends on the type of authentication, AAA or local, and the number of users:

- If we have AAA user with AAA override enabled, the session timeout is received from the RADIUS server.
- If we have AAA user with AAA override disabled, the session timeout is taken from the corresponding WLAN.
- If we use local authentication, 802.1x reauthentication/PMK cache timer is the WLAN ST value and web authentication local user remaining lifetime is configured as ST.

Note We can have same or different users for both 802.1x and web authentication.

Configuring Web Authentication

Configuring Web Authentication (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure web authentication. The **WLANs > Edit** page appears.

Step 3 Choose the **Security** and **Layer 3** tabs to open the **WLANs > Edit (Security > Layer 3)** page.

Step 4 Select the **Web Policy** check box.

Step 5 Make sure that the **Authentication** option is selected.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your settings.

Configuring Web Authentication (CLI)

Step 1 Enable or disable web authentication on a particular WLAN by entering this command:
config wlan security web-auth {**enable** | **disable**} *wlan_id*

Step 2 Release the guest user IP address when the web authentication policy timer expires and prevent the guest user from acquiring an IP address for 3 minutes by entering this command:
config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

The default value is disabled. This command is applicable when you configure the internal DHCP scope on the controller. By default, when the web authentication timer expires for a guest user, the user can immediately reassociate to the same

IP address before another guest user can acquire it. If there are many guest users or limited IP addresses in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy timer expires and the guest user is excluded from acquiring an IP address for 3 minutes. The IP address is available for another guest user to use. After 3 minutes, the excluded guest user can reassociate and acquire an IP address, if available.

Step 3 See the status of web authentication by entering this command:
show wlan *wlan_id*