Allowed List of Specific URLs

Allowed List of Specific URLs

This feature helps you to add specific URLs to allowed list on the controller or the AP so that those specific URLs are available for use, even when there is no connectivity to the internet. You can add URLs to allowed list for web authentication of captive portal and walled garden. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in allowed list, you are redirected to the Login page.

Adding URL to Allowed List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *<urlfilter-name>* **Example:** `Device(config)# urlfilter list url-allowedlist-nbn`	Configures the URL filter profile.
Step 3	**action** [**deny** | **permit**] **Example:** `Device(config-urlfilter-params)# action permit`	Configures the list as allowed list. The **permit** command configures the list as allowed list and the **deny** command configures the list as blocked list.

	Command or Action	Purpose
Step 4	{**redirect-server-ipv4** | **redirect-server-ipv6**} **Example:** `Device(config-urlfilter-params)# redirect-server-ipv4 X.X.X.X`	Configures the IP address of the redirect servers to which the user requests will be redirected in case of denied requests.
Step 5	**url** *url-to-be-allowed* **Example:** `Device(config-urlfilter-params)# url www.cisco.com`	Configures the URL to be allowed.

Note The controller uses two IP addresses and the mechanism only allows for one portal IP to be allowed. To allow pre-authentication access to more HTTP ressources, you need to use URL filters which will dynamically makes holes in the intercept (redirect) and security (preauth) ACLs for the IPs related to the website whose URL you enter in the URL filter. DNS requests will be dynamically snooped for the controller to learn the IP address of those URLs and add it to the ACLs dynamically.

Note **redirect-server-ipv4** and **redirect-server-ipv6** is applicable only in the local mode, specifically in post-authentication. For any further tracking or displaying any warning messages, the denied user request is redirected to the configured server.

But the **redirect-server-ipv4** and **redirect-server-ipv6** configurations do not apply to pre-authentication scenario as you will be redirected to the controller for the redirect login URL for any denied access.

You can associate the allowed URL with the ACL policy in flex profile.

Example

Associating the allowed URL with the ACL policy in flex profile:

```
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy user_v4_acl
Device(config-wireless-flex-profile-acl)# urlfilter list url_allowedlist_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"

Device(config)# urlfilter enhanced-list urllist_pre_cwa
Device(config-urlfilter-enhanced-params)# url url1.dns.com preference 1 action permit
Device(config-urlfilter-enhanced-params)# url url2.dns.com preference 2 action deny
Device(config-urlfilter-enhanced-params)# url url3.dns.com preference 3 action permit

Device(config)# wlan wlan5 5 wlan5
Device(config-wlan)#ip access-group web user_v4_acl
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa wpa2 ciphers aes
Device(config-wlan)#no security wpa akm dot1x
Device(config-wlan)#security web-auth
Device(config-wlan)#security web-auth authentication-list default
```

```
Device(config-wlan)#security web-auth parameter-map global
Device(config-wlan)#no shutdown
```

Verifying URLs on the Allowed List

Verify URLs on the Allowed List.

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                        ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------------
url-whitelist                   1    PRE-AUTH     PERMIT   1.1.1.1

Device#

Device# show wireless urlfilter details url-whitelist
List Name.................. : url-whitelist
Filter ID.............. : : 1
Filter Type................ : PRE-AUTH
Action..................... : PERMIT
Redirect server ipv4...... : 1.1.1.1
Redirect server ipv6...... :
Configured List of URLs
   URL..................... : www.cisco.com
```