DNS-Based Access Control Lists

Information About DNS-Based Access Control Lists

The DNS-based ACLs are used for wireless client devices. When using these devices, you can set pre-authentication ACLs on the embedded wireless controller to determine the data requests that are allowed or blocked.

To enable DNS-based ACLs on the embedded wireless controller, you need to configure the allowed URLs or denied URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs. The embedded wireless controller is configured with the ACL name that is returned by the AAA server. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

At the client authentication phase, the AAA server returns the pre-authentication ACL (url-redirect-acl, which is the attribute name given to the AAA server). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the embedded wireless controller, the CAPWAP payload is sent to the AP enabling DNS snooping for the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is sent to the embedded wireless controller as a CAPWAP payload. The embedded wireless controller adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

During pre-authentication or post-authentication, DNS ACL is applied to the client in the access point. If the client roams from one AP to another AP, the DNS learned IP addresses on the old AP is valid on the new AP as well.

Restrictions on DNS-Based Access Control Lists

The restriction for DNS-based ACLs is as follows:

- Pre-authentication and Post-authentication filters are supported in local modes. Only Pre-authentication filter is supported in Flex (Fabric) mode.
- ACL override pushed from ISE is not supported.
- FlexConnect Local Switching with External Web authentication using URL filtering is not supported until Cisco IOS XE Gibraltar 16.12.x.
- Fully qualified domain name (FQDN) or DNS based ACLs are not supported on Cisco Wave 1 Access Points.
- The URL filter considers only the first 20 URLs, though you can add more.
- The URL filter employs regular regex patterns and permits wildcard characters only at the beginning or at the end of an URL.
- The URL ACLs are defined and added to the FlexConnect policy profile in which they associate with a WLAN. The URL ACL creation follows a similar mechanism as that of local mode URL ACLs.
- In FlexConnect mode, the URL domain ACL works only if they are connected to a FlexConnect policy profile.
- The ACL can be attached to a WLAN by associating a policy profile with a WLAN or local policies. However, you can override it using "url-redirect-acl".
- For the Cisco AV pair received from ISE, the policy that needs to be applied for a particular client is pushed as part of ADD MOBILE

  message.
- When an AP joins or when an existing URL ACL is modified and applied on FlexConnect profile, the ACL definition along with mapped URL filter list is pushed to the AP.
- The AP stores the URL ACL definition with mapped ACL name and snoops the DNS packets for learning the first IP address for each URL in the ACL. When the AP learns the IP addresses, it updates the controller of the URL and IP bindings. The controller records this information in the client database for future use.
- When a client roams to another AP during the pre-authentication state, the learned IP addresses are pushed to a new AP. Otherwise, these learned IP addresses are purged when a client moves to a post-authentication state or when the TTL for the learned IP address expires.

Flex Mode

Defining URL Filter List

Before you begin

Ensure that you set up DNS for URL filtering to work as URL filtering uses DNS queries.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *list-name* **Example:** `Device(config)# urlfilter list urllist_flex_preauth`	Configures the URL filter list. Here, *list-name* refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters.
Step 3	**action permit** **Example:** `Device(config-urlfilter-params)# action permit`	Configures the action: permit (allowed list) or deny (blocked list).
Step 4	**redirect-server-ip4** *IPv4-address* **Example:** `Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8`	Configures the IPv4 redirect server for the URL list. Here, *IPv4-address* refers to the IPv4 address.
Step 5	**redirect-server-ip6** *IPv6-address* **Example:** `Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81`	Configures the IPv6 redirect server for the URL list. Here, *IPv6-address* refers to the IPv6 address.
Step 6	**url** *url* **Example:** `Device(config-urlfilter-params)# url url1.dns.com`	Configures an URL. Here, *url* refers to the name of the URL.
Step 7	**end** **Example:** `Device(config-urlfilter-params)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Applying URL Filter List to Flex Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *default-flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. The default flex profile name is *default-flex-profile*.
Step 3	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl_name`	Configures ACL policy.
Step 4	**urlfilter list** *name* **Example:** `Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth`	Applies the URL list to the Flex profile.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile-acl)# end`	Returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication (GUI)

Perform the following steps to configure ISE for Central Web Authentication.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Click **Policy** and then click **Policy Elements**.

Step 3 Click **Results**.

Step 4 Expand **Authorization** and click **Authorization Profiles**.

Step 5 Click **Add** to create a new authorization profile for URL filter.

Step 6 Enter a name for the profile in the **Name** field. For example, CentralWebauth.

Step 7 Choose **ACCESS_ACCEPT** option from the **Access Type** drop-down list.

Step 8 Alternatively, in the **Common Tasks** section, check **Web Redirection**..

Step 9 Choose the **Centralized Web Auth** option from the drop-down list.

Step 10 Specify the ACL and choose the ACL value from the drop-down list.

Step 11 In the **Advanced Attributes Setting** section, choose **Cisco:cisco-av-pair** from the drop-down list.

Note Multiple ACL can be applied on the controller based on priority. In L2 Auth + webauth multi-auth scenario, if the ISE returns ACL during L2 Auth then ISE ACL takes precedence over the default webauth redirect ACL. This leads to traffic running in webauth pending state, if ISE ACL has permit rule. To avoid this scenario, you need to set the precedence for L2 Auth ISE returned ACL. The default webauth redirect ACL priority is 100. To avoid traffic issue, you need to configure the redirect ACL priority above 100 for ACL returned by ISE.

Step 12 Enter the following one by one and click (+) icon after each of them:

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

  For example,

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?
sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpiry=value&action=cwa
```

Step 13 Verify contents in the **Attributes Details** section and click **Save**.

Viewing DNS-Based Access Control Lists

To view details of a specified wireless URL filter, use the following command:

```
Device# show wireless urlfilter details <urllist_flex_preauth>
```

To view the summary of all wireless URL filters, use the following command:

```
Device# show wireless urlfilter summary
```

To view the URL filter applied to the client in the resultant policy section, use the following command:

```
Device# show wireless client mac-address <MAC_addr> detail
```

Configuration Examples for DNS-Based Access Control Lists

Flex Mode

Example: Defining URL Filter List

This example shows how to define URL list in Flex mode:

```
Device# configure terminal
Device(config)# urlfilter list urllist_flex_pre
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8
```

```
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

Example: Applying URL Filter List to Flex Profile

This example shows how to apply an URL list to the Flex profile in Flex mode:

```
Device# configure terminal
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy acl_name
Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth
Device(config-wireless-flex-profile-acl)# end
```

Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL

IOS IPv6 ACLs is used to send webauth ACL to AP.

ACL definitions are pushed to AP in the following events:

- AP join.
- New ACL mapping in flex profile.
- When default External WebAuth (EWA) security ACL is pushed.
- Configuring IPv6 ACL definition in Flex profile.

Note All the custom ACLs must be mapped in Flex profile. Only the custom ACL definitions will be pushed to AP apart from the generated default ACLs.

Custom pre-authentication ACL is mapped under WLAN profile. Whereas, custom post-authentication ACL is mapped under default policy profile. All post-authentication ACL is configured under default Flex profile.

Default Local Web Authentication ACLs

The pre-defined default LWA IPv6 ACL is pushed to AP and plumbed to data plane.

Default External Web Authentication ACL

The default EWA ACLs are derived from the redirect portal address configured in the parameter map.

The following list covers the types of default EWA ACLs:

- Security ACL—Pushed to AP.
- Intercept ACL—Plumbed to data plane.

FQDN ACL

- FQDN ACL is encoded along with IPv6 ACL and sent to AP.

- FQDN ACL is always a custom ACL.
- AP does DNS snooping and sends the IPv4 and IPv6 addresses to the controller.
- Controller stores the snooped IPs from AP in a database and sends the message during AP-to-AP intra wncd roam.

The following applies to Flex and Local mode:

- If you are migrating from AireOS, you would explicitly need to execute the following commands:

```
redirect append ap-mac tag ap_mac
redirect append wlan-ssid tag wlan
redirect append client-mac tag client_mac
```

- If the login page has any resource that needs to be fetched from the server, you will need to include those resource URLs in URL filtering.
- If you are trying to access IPv6 URL and you have an IPv4 web server, the controller redirects the client to an internal page as domain redirection is not supported. It is recommended to have a dual-stack web server and configure virtual IPv6 address in the global parameter map.

Supported IPv6 Features in Flex Mode

Table 1: Supported IPv6 Features in Flex Mode

Flex Mode IPv6 Feature	Feature Parity Support
Flex client IPv6 learning	Yes
Pre auth IPv6 ACL	Yes
Post auth IPv6 ACL	Yes
Pre auth DNS ACL	Yes
Post auth DNS ACL	Yes

Enabling Pre-Authentication ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Uncheck the **WPAPolicy**, **AES** and **802.1x** check boxes.

Step 5 Choose **Security** > **Layer3** tab. Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and authentication list from the **Authentication List** drop-down list. Click **Show Advanced Settings** and under the **Preauthenticated ACL** settings, choose the IPv6 ACL from the **IPv6** drop-down list.

Step 6 Choose **Security** > **AAA** tab. Choose the authentication list from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Enabling Pre-Authentication ACL for LWA and EWA

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** If you have already configured WLAN, enter **wlan wlan-name** command.
Step 3	**ipv6 traffic-filter web** *acl_name-preauth* **Example:** `Device(config-wlan)# ipv6 traffic-filter web preauth_v6_acl`	Creates a pre-authentication ACL for web authentication.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables the WPA security.
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)#no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 6	**no security wpa akm dot1x** **Example:**	Disables security AKM for dot1x.

	Command or Action	Purpose
	`Device(config-wlan)#no security wpa akm dot1x`	
Step 7	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security.
Step 8	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list wcm_dot1x`	Enables authentication list for WLAN.
Step 9	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map param-custom-webconsent`	Maps the parameter map.
Step 10	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Shutdown the WLAN.

Enabling Post-Authentication ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**. The **Profile Name** is the profile name of the policy profile.

Step 4 Enter the **SSID** and the **WLAN ID**.

Step 5 Click **Apply to Device**.

Enabling Post-Authentication ACL for LWA and EWA

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**ipv6 acl** *acl_name* **Example:** `Device(config-wireless-policy)# ipv6 acl testacl`	Creates a named WLAN ACL.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling DNS ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**. The **Profile Name** is the profile name of the policy profile.

Step 4 Enter the **SSID** and the **WLAN ID**.

Step 5 Click **Apply to Device**.

Enabling DNS ACL for LWA and EWA

Note Post-authentication DNS ACL is not supported.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL

To verify the client state after L2 authentication, use the following command:

```
Device# show wireless client summary
Number of Local Clients: 1


MAC Address    AP Name                           WLAN  State             Protocol Method
  Role
-------------------------------------------------------------------------------------------------
1491.82b8.f8c1 AP4001.7A03.544C                  4      Webauth Pending   11n(5)   None
   Local

Number of Excluded Clients: 0
```

To verify the IP state, discovery, and MAC, use the following command:

```
Device# show wireless dev da ip
  IP                                        STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------------------
  15.30.0.4                                 Reachable   ARP         1491.82b8.f8c1
  2001:15:30:0:d1d7:ecf3:7940:af60          Reachable   IPv6 Packet 1491.82b8.f8c1
  fe80::595e:7c29:d7c:3c84                  Reachable   IPv6 Packet 1491.82b8.f8c1
```