Cisco OEAP Split Tunneling

Feature History for Cisco OEAP Split Tunneling

This table provides release and related information for the feature explained in this module.

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 1: Feature History for Cisco OEAP Split Tunneling

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	Cisco OEAP Split Tunneling	The Split Tunneling feature in Cisco OfficeExtend Access Point (OEAP) provides a mechanism to classify client traffic, based on packet content, using access control lists (ACLs).

Information About Cisco OEAP Split Tunneling

The global pandemic has redefined the way people interact and work. The workplace has shifted from office cubicles to home desks, which requires applications that enable seamless collaboration among the workforce. For home-based workers, access to business services must be reliable, consistent, and secure. It should provide an experience that is similar to the office facility. Routing all of the traffic through the corporate network

using traditional VPNs increases the traffic volume, slows down access to resources, and negatively impacts the remote user experience.

Cisco OEAP provides secure communications from a controller to an access point (AP) at a remote location, seamlessly extending the corporate WLAN over the internet to an employee's residence. Cisco OEAP provides segmentation of home and corporate traffic using the Split Tunnelling feature, which allows for home device connectivity without security risks to corporate policy.

Split tunnelling classifies the traffic sent by a client, based on packet content, using ACLs. Matching packets are switched locally from Cisco OEAP, and other packets are centrally switched over CAPWAP. Clients on a corporate SSID can talk to devices on a local network (printers, wireless devices on a personal SSID, and so on) directly without consuming WAN bandwidth, by sending packets over CAPWAP.

Traffic to Software as a Service (Saas) applications such as Cisco WebEx, Microsoft SharePoint, Microsoft Office365, Box, Dropbox, and so on that is required as part of the work routine, need not go through the corporate network, by using the Split Tunnelling feature.

The Cisco OEAP advertises two SSIDs, one corporate and one personal. Corporate SSID clients obtain their IP address from the central DHCP server in the corporate network. If split tunneling is enabled and a client wants to access a device in the home network, the AP performs NAT (PAT) translation between the wireless client corporate network subnet and the home network where the AP is located.

The personal SSID is configurable by a Cisco OEAP user. Clients will either get their IP address from the home router (when the AP personal SSID firewall is disabled) or from the internal AP DHCP server (when the AP personal SSID firewall is enabled). In the latter scenario, if the clients want to reach the home network devices, the AP perform sNAT (PAT) translation between the wireless client's internal network and the home network where the AP is located.

Prerequisites for Cisco OEAP Split Tunneling

- Cisco Wave 2 APs or Cisco Catalyst 9100AX Series Access Points
- URL filter list that matches the ACL name configured in split tunneling

Restrictions for Cisco OEAP Split Tunneling

- Cisco OEAPs are not supported when Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) is used as a controller.
- Mesh topology is not supported.
- Clients connected on personal SSID or on home network (AP native VLAN) cannot discover devices on the corporate network.
- Split tunnelling is not supported in standalone mode.
- URL split tunnelling supports only up to 512 URLs.
- Action (deny or permit) can be specified only on the URL filter list, not for each individual entry.
- If URL-based ACL contains wild-card URLs, a maximum of 10 URLs are supported.
- The amount of snooped DNS IP addresses is limited as follows:

- An AP can snoop 4095 IP addresses per DNS response, if IP addresses are less than 150,000.
- An AP can snoop 10 IP addresses per DNS response, if IP addresses are between 150,000 and 200,000.
- An AP can snoop five IP addresses per DNS response, if IP addresses are between 200,000 and 250,000.
- An AP can snoop one IP address per DNS response, if IP addresses are greater than 250,000.

- A maximum of 128 IP address ACE (rules) can be used in the IP ACL for split tunnelling.
- URL-based split tunnelling only works with IPv4 addresses.

Use Cases for Cisco OEAP Split Tunneling

Before Release 17.7.1, split tunneling used IP ACLs. This meant that cloud services such as Cisco Webex were accessed directly without going through the corporate network. The network administrator maintained the list of IP addresses that Cisco Webex used, which was a daunting task. From Release 17.7.1, using the Cisco OEAP Split Tunneling feature, the network administrator needs to provide only the DNS names that Cisco Webex uses. The AP ensures that traffic from these DNS names is routed directly to the internet without using the corporate network.

Workflow to Configure Cisco OEAP Split Tunneling

1. Create an IP address ACL or URL ACL
2. Add ACL to FlexConnect Profile
3. Enable Split Tunnelling on Policy Profile
4. Verify the Configuration

Create an IP Address ACL (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:**	Defines an extended IPv4 access list using a name.

	Command or Action	Purpose
	`Device(config)# ip access-list extended vlan_oeap`	**Note** IP ACL can be used to define a default action if there is no match in the URL ACL.
Step 3	*seq-num* **deny ip any host** *hostname* **Example:** `Device(config-ext-nacl)# 10 deny ip any 10.10.0.0 0.0.255.255`	Denies IP traffic from any host.
Step 4	*seq-num* **permit ip any any** *hostname* **Example:** `Device(config-ext-nacl)# 20 permit ip any any`	Permits IP traffic from any source or destination host.
Step 5	**end** **Example:** `Device(config-ext-nacl)# end`	Exits configuration mode and returns to privileged EXEC mode.

Create a URL ACL (CLI)

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 vlan_oeap`	Configures the URL filter list. The list name must not exceed 32 alphanumeric characters.
Step 3	**action permit** **Example:** `Device(config-urlfilter-params)# action permit`	Configures the action: Permit (traffic is allowed directly on the home network) or Deny (traffic is directed to the corporate network).
Step 4	**filter-type post-authentication** **Example:** `Device(config-urlfilter-params)# filter-type post-authentication`	Configures the URL list as post authentication filter.
Step 5	**url** *url-name* **Example:**	Configures a URL.

	Command or Action	Purpose
	`Device(config-urlfilter-params)# url wiki.cisco.com`	
Step 6	**url** *url-name* **Example:** `Device(config-urlfilter-params)# url example.com`	(Optional) Configures a URL. Use this option when you want to add multiple URLs.
Step 7	**end** **Example:** `Device(config-urlfilter-params)# end`	Exits configuration mode and returns to privileged EXEC mode.

Add an ACL to a FlexConnect Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures a FlexConnext profile.
Step 3	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy vlan_oeap`	Configures an ACL policy.
Step 4	**urlfilter list** *url-filter* **Example:** `Device(config-wireless-flex-profile-acl)# urlfilter list vlan_oeap`	Configures a URL filter list.
Step 5	**exit** **Example:** `Device(config-wireless-flex-profile-acl)# exit`	Returns to FlexConnect profile configuration mode..
Step 6	**office-extend** **Example:** `Device(config-wireless-flex-profile)# office-extend`	Enables the OEAP mode for a FlexConnect AP.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Enable Split Tunnelling in a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures a FlexConnect profile.
Step 3	**no central association** **Example:** `Device(config-wireless-flex-profile)# no central association`	Disables central association and enables local association for locally switched clients.
Step 4	**flex split-mac-acl** *split-mac-acl-name* **Example:** `Device(config-wireless-flex-profile)# flex split-mac-acl vlan_oeap`	Configures a split MAC ACL name. **Note** Ensure that you use the same *acl-policy-name* in the FlexConnect profile.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying the Cisco OEAP Split Tunnel Configuration

To verify the split tunneling DNS ACLs per wireless client on the AP side, use the following command:

```
Device# show split-tunnel client 00:11:22:33:44:55 access-list

Split tunnel ACLs for Client: 00:11:22:33:44:55

IP ACL: SplitTunnelACL
```

```
Tunnel packets Tunnel bytes NAT packets NAT bytes
             1          242           3       768

URL ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             3          778           0         0

Resolved IPs for Client: 00:11:22:33:44:55 for Split tunnel

HIT-COUNT       URL             ACTION  IP-LIST

1               base1.com       deny.   20.0.1.1
                                        20.0.1.10

2               base2.com       deny.   20.0.1.2

3               base3.com       deny.   20.0.1.3
```

To verify the current binding between a WLAN and an ACL, use the following command:

```
Device# show split-tunnel mapping

VAP-Id       ACL Name
    0        SplitTunnelACL
```

To verify the content of the current URL ACL, use the following command:

```
Device# show flexconnect url-acl

ACL-NAME          ACTION      URL-LIST

SplitTunnelACL    deny        base.com
```