Cisco OEAP Split Tunneling

• Cisco OEAP split tunneling, on page 1

Cisco OEAP split tunneling

Cisco OEAP split tunneling is a feature that

- provides secure communications from a controller to an AP at a remote location
- seamlessly extends the corporate WLAN over the internet to an employee's residence, and
- provides segmentation of home and corporate traffic using the split tunneling feature.

Routing all traffic through traditional VPNs increases volume, slows resource access, and negatively impacts remote user experience. Split tunneling allows for home device connectivity without security risks to corporate policy.

Feature history for Cisco OEAP split tunneling

Table 1: Feature history

Release	Feature	Feature information
Cisco IOS XE 17.8.1	IPv6 Support	IPv6 addressing is supported on the Cisco OEAP Split Tunneling feature.
Cisco IOS XE 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).

IPv6 address support for Cisco OEAP split tunneling

From Cisco IOS XE 17.8.1, IPv6 addressing is supported. You can disable IPv6 addressing only by disabling the feature.

The end-to-end network should support IPv6. Both the corporate network (controller, corporate gateway, and other related components) and the home network (wireless clients, home router, and others) should support IPv6.

Traffic to Software as a Service (SaaS) applications such as Cisco WebEx, Microsoft SharePoint, Microsoft Office365, Box, and Dropbox, which are required as part of the work routine, do not need to go through the corporate network when using the split tunneling feature.

Cisco OEAP split tunneling traffic management

A Cisco OEAP split tunnel is a network feature that

- classifies client traffic based on packet content using Access Control Lists (ACLs)
- switches matching packets locally from Cisco OEAP, and
- centrally switches other packets over Control and Provisioning of Wireless Access Points (CAPWAP).

Cisco OEAP provides seamless connectivity by broadcasting distinct Service Set Identifiers (SSIDs) for corporate use and personal use allowing for differentiated handling and prioritization of network traffic. Corporate SSID clients obtain their IP addresses from the central DHCP server within the corporate network. With split tunneling enabled, when a client connected to the corporate SSID attempts to access a device within a home network, the OEAP efficiently manages network traffic by performing Network Address Translation (NAT) or Port Address Translation (PAT) between the client's internal network and the home network.

These examples explains Cisco OEAP split tunneling manages and differentiates network traffic for various use cases:

- VPN Split Tunnel Example: Corporate data can be sent through the secure corporate VPN while allowing personal data to be routed directly to the internet for enhanced performance.
- Home Network Example (SSID): Devices connected to the home SSID receive IP addresses either from the local AP DHCP server or directly from home network equipment when the firewall feature is switched off.

By segmenting traffic, OEAP split tunneling ensures optimized use of WAN bandwidth, improved network performance, and increased security by distinguishing between corporate and personal data streams.

Prerequisites for Cisco OEAP split tunneling

Hardware Requirements

Cisco Wave 2 APs or Cisco Catalyst 9100AX Series APs

Configuration Requirements

URL filter list that matches the ACL name configured in split tunneling

Restrictions for Cisco OEAP split tunneling

These requirements outline the restrictions applicable to Cisco OEAP split tunneling:

- Cisco OfficeExtend Access Points (OEAPs) are not supported when Embedded Wireless Controller on Catalyst Access Points (EWC) is used as a controller.
- Mesh topology is not supported.

- Clients connected on a personal SSID or the home network (AP native VLAN) will not be able to discover devices.
- Split tunneling is not supported in standalone mode.
- URL split tunneling supports only up to 512 URLs.
- Specify actions, like deny or permit, only on the URL filter list, not for individual entries.
- If the URL-based ACL contains wildcard URLs, only ten URLs are supported.
- Use up to 128 IP address ACEs (rules) in the IP ACL for split tunneling.
- URL-based split tunnelling only works with IPv4 addresses.

DNS IP addresses restrictions

These requirements limit the amount of DNS IP addresses that can be snooped:

- 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 5 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.

IPv6 Addressing restrictions

These restrictions apply to IPv6 addressing for Cisco OEAP split tunneling:

- Multihoming, which involves multiple router advertisement prefixes, is not supported. If a home network receives multiple prefixes, the AP connected to the controller uses one prefix.
- The system does not support roaming.
- Filtering is not supported on the upstream traffic towards the wireless client.
- Split tunneling is disabled for clients with duplicate IPv6 addresses. Traffic for these clients is forwarded centrally to the controller.
- DHCPv6 prefix delegation is not supported for wireless clients.
- If the corporate prefix length is smaller than the home prefix length, split tunneling for a particular client is disabled.

Use cases for Cisco OEAP split tunneling

Before Cisco IOS XE 17.7.1, you could use IP ACLs for split tunneling. Cloud services, such as Cisco Webex, could be accessed directly. These services bypassed the corporate network. As a network administrator, you maintained the list of IP addresses that Cisco Webex used.

Starting with Cisco IOS XE 17.7.1, when you use the Cisco OEAP Split Tunneling feature, provide only the DNS names that Cisco Webex uses. The AP then routes traffic from these DNS names directly to the internet instead of through the corporate network.

How Cisco OEAP split tunneling works

Summary

This process involves configuring Cisco OEAP split tunneling by performing multiple steps that include creating ACLs, adding them to profiles, enabling split tunnelling, and verifying the configuration.

Workflow

The process involves these stages:

1. Defining ACLs: Create IP address ACL or URL ACL to specify allowed network paths.
2. Profile association: The administrator adds these ACLs to the FlexConnect Profile to prepare for policy enforcement.
3. Policy activation: Enable split tunneling on the policy profile to segment and direct data flows.
4. Configuration confirmation: The administrator verifies successful configuration to ensure policy compliance, and network functionality.

Result

You have configured Cisco OEAP Split Tunneling, allowing effective management of network traffic and enhanced security for remote devices.

Create an IP address ACL (CLI)

You can configure an IP address-based ACL on network devices to control and secure traffic flow.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Define an extended IPv4 access list using a name.

Example:

```
Device(config)# ip access-list extended vlan_oeap
```

Note
An IP ACL can define a default action if no matches exist in the URL ACL.

Step 3 Deny IP traffic from any host.

Example:

```
Device(config-ext-nacl)# 10 deny ip any 10.10.0.0 0.0.255.255
```

Step 4 Permit IP traffic from any destination host.

Example:

```
Device(config-ext-nacl)# 20 permit ip any any
```

Step 5 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-ext-nacl)# end
```

The IP address ACL effectively filters traffic according to the specified rules on the network device.

Create a URL ACL (CLI)

Create a URL Access Control List (ACL) on a network device using CLI, enabling control over which URLs can be accessed based on security policies.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the URL filter list.

Example:

```
Device(config)# urlfilter list vlan_oeap
```

Your list name must not exceed 32 alphanumeric characters.

Step 3 Configure the action: Permit (traffic is allowed directly on the home network) or Deny (traffic is directed to the corporate network).

Example:

```
Device(config-urlfilter-params)# action permit
```

Step 4 Configure the URL list as post authentication filter.

Example:

```
Device(config-urlfilter-params)# filter-type post-authentication
```

Step 5 Configure a URL.

Example:

```
Device(config-urlfilter-params)# url wiki.cisco.com
```

Step 6 (Optional) Configure a URL.

Example:

```
Device(config-urlfilter-params)# url example.com
```

Use this option when you want to add multiple URLs.

Step 7 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-urlfilter-params)# end
```

You have configured the URL ACL successfully, allowing specific URLs to be permitted or denied access through the network device according to the parameters set during configuration.

Add an ACL to a FlexConnect profile (GUI)

Associate an Access Control List (ACL) with a FlexConnect profile, applying filtering and control policies to FlexConnect APs.

Use this procedure to apply an ACL and URL filtering to a FlexConnect profile, enabling traffic control and optional OfficeExtend mode for remote APs.

Before you begin

Use these steps to add an ACL to a FlexConnect profile:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the target FlexConnect profile.

Example:

```
Device(config)# wireless profile flex default-flex-profile
```

Step 3 Define the ACL policy to associate with the profile.

Example:

```
Device(config-wireless-flex-profile)# acl-policy vlan_oeap
```

Step 4 Configure a URL filter list, if required.

Example:

```
Device(config-wireless-flex-profile-acl)# urlfilter list vlan_oeap
```

Step 5 Exit ACL configuration mode to return to the FlexConnect profile.

Example:

```
Device(config-wireless-flex-profile-acl)# exit
```

Step 6 Enable OfficeExtend mode for the FlexConnect AP, if applicable.

Example:

```
Device(config-wireless-flex-profile)# office-extend
```

Step 7 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-wireless-flex-profile)# end
```

The ACL and associated URL filter are applied to the selected FlexConnect profile, with OfficeExtend mode enabled if configured. The changes take effect for FlexConnect APs using this profile.

Enable split tunneling in a policy profile

Enable split tunneling in a policy profile to optimize network traffic and enhance performance by allowing specified traffic to bypass the central network and directly access the internet.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a FlexConnect profile.

Example:

```
Device(config)# wireless profile flex default-flex-profile
```

Step 3 Disable central association and enable local association for locally switched clients.

Example:

```
Device(config-wireless-flex-profile)# no central association
```

Step 4 Configure a split MAC ACL name.

Example:

```
Device(config-wireless-flex-profile)# flex split-mac-acl vlan_oeap
```

Note
Ensure that you use the same *acl-policy-name* in the FlexConnect profile.

Step 5 Exit configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-wireless-flex-profile)# end
```

Enable split tunneling in the policy profile so that traffic defined in the ACL can locally switch, which improves bandwidth use and network performance.

Verify the Cisco OEAP split tunnel configuration

To verify the split tunneling DNS ACLs per wireless client on the AP side, use this 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.   203.0.113.0
                                        203.0.113.1

2               base2.com       deny.   203.0.113.2

3               base3.com       deny.   203.0.113.5
```

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

```
Device# show split-tunnel mapping

VAP-Id       ACL Name
    0        SplitTunnelACL
```

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

```
Device# show flexconnect url-acl

ACL-NAME          ACTION      URL-LIST

SplitTunnelACL    deny        base.com
```