Revised: October 30, 2026

L3 and L7 Local Internet Breakout for Cisco 8000 Series Secure Routers using Cisco Meraki Dashboard

Feature history for L3 and L7 Local Internet Breakout

Table 1: Feature History of L3 and L7 Local Internet Breakout

Feature name	Release	Feature information
L3 and L7 Local Internet Breakout	Cisco IOS XE 26.2.1 Release	L3 and L7 Local Internet Breakout lets administrators send selected branch traffic directly to the Internet instead of backhauling it through a hub. Cisco 8000 Series Secure Routers can be configured for this feature using Cisco Meraki Dashboard.

L3 and L7 Local Internet Breakout

Layer 3 Direct Internet Access (L3 DIA) Breakout enables source- and destination-based routing decisions using IPv4 CIDR blocks. Selected traffic is routed locally to the Internet instead of being sent through VPN tunnels such as IPsec or AutoVPN.

Layer 7 Direct Internet Access (L7 DIA) Breakout enables application-aware routing decisions using NBAR application identification. Matching traffic uses the same local breakout action as L3 DIA.

For platform background, see the Cisco 8000 Series Secure Routers landing page

For configuration concepts related to policy-based routing, NBAR, NAT, and IP routing, see the Cisco IOS XE Secure 8200 Series Software Configuration Guide

L3 DIA matching

Policy-based L3 DIA matches traffic by supported source, destination, protocol, and port criteria. Destination CIDR and source CIDR criteria are used to select traffic for local Internet breakout.

L7 DIA matching

In Cisco IOS XE 26.2.1 Release, L7 DIA supports a limited NBAR match scope. Cisco Secure Routers support an unscoped NBAR application rule, an NBAR application rule scoped by source CIDR, and source protocol or source-port constraints only when the rule also contains a source CIDR and the protocol is TCP or UDP. Destination-CIDR scoping and source-VLAN scoping are not supported for L7 rules.

```
class-map match-any class-dia-traffic-L7
 match protocol youtube
!
ip access-list extended L7-DIA-APP-ACL-ABC123
 10 permit tcp 10.0.0.0 0.0.0.255 eq 8000 any
!
class-map match-all L7-DIA-APP-CLASS-ABC123
 match protocol facebook
 match access-group name L7-DIA-APP-ACL-ABC123
```

The suffix ABC123 is illustrative. Dashboard generates the actual suffix from the rule content.

Benefits of L3 and L7 Local Internet Breakout

- Reduces branch-to-Internet latency for selected Internet and SaaS traffic.
- Provides a cloud-managed policy surface in Cisco Meraki Dashboard while Cisco IOS XE performs local forwarding enforcement.
- Allows policy-based L3 and L7 breakout to coexist with AutoVPN or tunnel behavior.

Restrictions for L3 and L7 Local Internet Breakout

- L7 DIA follows the global uplink preference. It does not support a per-rule preferred uplink or performance/SLA-based routing action. Customers can switch global DIA forwarding behavior between load-balance enabled and load-balance disabled.
- User-configurable DNS-protocol and destination FQDN/URL VPN-exclusion rules are not supported. The DNS class shown in the generated IOS XE configuration is an internal helper used only for L7 first-packet classification.
- Hostname-based rules are not supported.

Table 2: L3 DIA support matrix

Field	Supported values
Protocol	Any, TCP, UDP, or ICMP
Source	Any, IPv4 CIDR, or VLAN
Source port	Any or one port where applicable
Destination	Any or IPv4 CIDR
Destination port	Any or one port where applicable

Table 3: L7 DIA support matrix

Rule form	Supported	Notes
NBAR application only	Yes	Generates an unscoped L7 application class.
NBAR application plus source CIDR	Yes	Generates a source ACL and a match-all class.
NBAR application plus source CIDR and TCP or UDP	Yes	Preserves the protocol in the source ACL.
NBAR application plus source CIDR, TCP or UDP, and source port	Yes	Source port requires source CIDR and TCP or UDP.
NBAR application plus destination CIDR	No	Not supported by the Cisco IOS XE 26.2.1 Release.
NBAR application plus source VLAN	No	Not supported by the Cisco IOS XE 26.2.1 Release.
Protocol or source port without source CIDR	No	Unsupported L7 scope.
Destination FQDN/URL, hostname-based, or user DNS-protocol rule	No	Not supported for cloud managed Cisco Secure Routers.

Configure L3 and L7 Local Internet Breakout

Choose one of the methods to configure L3 and L7 local internet breakout

- L3 and L7 local internet breakout configurations on Cisco Meraki Dashboard
- L3 and L7 local internet breakout configurations on Cisco Secure Routers

Configure L3 and L7 Local Internet Breakout on Cisco Meraki Dashboard

The Local Internet Breakout table is shown for Cisco Secure Router networks when the XE network participates in VPN and the device meets the supported Cisco IOS XE 26.2.1 Release firmware gate. For Dashboard configuration reference, see VPN Full-Tunnel Exclusion (Application and IP/URL Based Local Internet Breakout).

Step 1 In Cisco Meraki Dashboard, navigate to **Security & SD-WAN** > **SD-WAN & Traffic shaping**.

Step 2 Confirm that Local Internet Breakout or VPN exclusion rules is available.

The XE network must participate in VPN and the Cisco Secure Router must meet the supported firmware gate.

Step 3 In the Local Internet Breakout section, select **Add**.

Step 4 For an L3 rule, configure the supported source, destination, protocol, and port fields.

Step 5 For an L7 rule, select one or more supported NBAR applications.

Optionally configure a source CIDR. Source protocol or source-port constraints require a source CIDR and TCP or UDP.

Step 6 Save the rule.

Step 7 Confirm that the rule appears in the Dashboard Local Internet Breakout or VPN exclusion rules table.

L3 and L7 Local Internet Breakout configuration on Cisco Secure Routers

Router configuration is generated and pushed by Cisco Meraki cloud management; administrators do not manually enter the generated policy on the router.

Generated ePBR policy

The following example shows the single generated policy model used for Cisco IOS XE 26.2.1. The policy class order is L3, internal DNS helper, source-CIDR-scoped L7, and unscoped L7.

```
ip access-list extended L3-DIA-IP-ACL
 10 permit tcp any 10.1.19.0 0.0.0.255 eq 443
!
class-map match-any L3-DIA-IP-CLASS
 match access-group name L3-DIA-IP-ACL
!
ip access-list extended acl-dns-req-resp
 10 permit udp any any eq domain
 20 permit udp any eq domain any
 30 permit tcp any any eq domain
 40 permit tcp any eq domain any
!
class-map match-any class-dns-req-resp
 match access-group name acl-dns-req-resp
!
ip access-list extended L7-DIA-APP-ACL-ABC123
 10 permit tcp 10.0.0.0 0.0.0.255 eq 8000 any
```

```
!
class-map match-all L7-DIA-APP-CLASS-ABC123
 match protocol facebook
 match access-group name L7-DIA-APP-ACL-ABC123
!
class-map match-any class-dia-traffic-L7
 match protocol youtube
!
policy-map type epbr dia_policy-CLOUD_DEFAULT_VRF
 class L3-DIA-IP-CLASS
  set ipv4 global
 class class-dns-req-resp
 class L7-DIA-APP-CLASS-ABC123
  set ipv4 global
 class class-dia-traffic-L7
  set ipv4 global
!
interface <LAN-interface>
 ip nat inside
 service-policy type epbr input dia_policy-CLOUD_DEFAULT_VRF
```

The DNS helper class has no local-breakout action. It supports first-packet application classification and does not expose a user-configurable DNS or FQDN DIA rule.

NAT DIA configuration

The following route sets are mutually exclusive. Use AD 130 for normal local breakout. Use AD 210 instead of AD 130 for the applicable full-tunnel VRF. The global default route is required when the policy uses set ipv4 global.

Normal local breakout with a static gateway

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.1.17.13
ip route vrf <VRF_NAME> 0.0.0.0 0.0.0.0 GigabitEthernet1 10.1.17.13 130
```

Normal local breakout with a DHCP uplink

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet2 dhcp
ip route vrf <VRF_NAME> 0.0.0.0 0.0.0.0 GigabitEthernet2 dhcp 130
```

Applicable full-tunnel VRF with a static gateway

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.1.17.13
ip route vrf <VRF_NAME> 0.0.0.0 0.0.0.0 GigabitEthernet1 10.1.17.13 210
```

Applicable full-tunnel VRF with a DHCP uplink

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet2 dhcp
ip route vrf <VRF_NAME> 0.0.0.0 0.0.0.0 GigabitEthernet2 dhcp 210
```

For multiple active WAN uplinks, Dashboard generates the corresponding route for each eligible uplink. Do not install AD 130 and AD 210 route forms simultaneously for the same VRF and uplink.

LAN and WAN NAT attachment

```
interface GigabitEthernet3
 ip nat inside
 service-policy type epbr input dia_policy-CLOUD_DEFAULT_VRF
!
interface GigabitEthernet1
 ip nat outside
!
```

```
interface GigabitEthernet2
 ip nat outside
```

Verify L3 and L7 Local Internet Breakout

Verify policy objects and interface attachment with the following read-only commands:

Verify policy objects and interface attachment

```
show running-config | section policy-map type epbr
show running-config | section class-map
show running-config | section ip access-list extended
show running-config interface <LAN-interface>
show policy-map type epbr interface <LAN-interface>
```

Verify global and VRF default routes

Verify global and VRF default routes:

```
show ip route 0.0.0.0
show ip route vrf <VRF_NAME> 0.0.0.0
```

Verify NAT state

Verify NAT state without changing active sessions:

```
show ip nat translations
```

Verify DIA datapath counters

Verify DIA datapath counters:

```
show platform hardware qfp active feature cloud-mgmt datapath statistics
```

Clear dynamic NAT translations for lab troubleshooting

For lab troubleshooting only, the following command clears all dynamic NAT translations and can disrupt active sessions:

```
clear ip nat translation *
```