Flow-Based Redirect

The traffic from an IP session is redirected based on the destination address (for a simple IP session), and to a tunnel (for a mobile IP session). However, in some application scenarios, some of the traffic is routed to a specific system or a specific interface for additional service or processing. Through the Adult Content Filtering (ACF) capability, web traffic of some sessions can be routed to an ACF appliance that filters the traffic based on the URL or content. The Flow-Based Redirect (FBR) feature enables applications such as the ACF to route matching traffic to a specified next hop device.

The FBR feature is Virtual Routing and Forwarding (VRF)-aware. You can map an interface to a VRF or transfer a VRF as long as the session and the interface connecting the next hop device are within the same VRF network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Flow-Based Redirect for Adult Content Filtering

In a typical WiFi hotspot deployment, all subscriber traffic goes through Cisco ISG (Intelligent Service Gateway) after successful authentication. For unauthenticated traffic, L4R feature offers a logic to redirect traffic based on a pre-defined access-list (ACL). This L4R feature acts as a way to redirect some traffic to a web portal or opengarden environment using a translation logic. In order to implement a similar redirection logic after successful authentication without the need for translating the traffic, the flow based redirect has been implemented in ISG to allow traffic to be redirected/rerouted. A typical use case is Adult Content Filtering (ACF) where web traffic needs to be redirected to a Web Filtering Appliance.

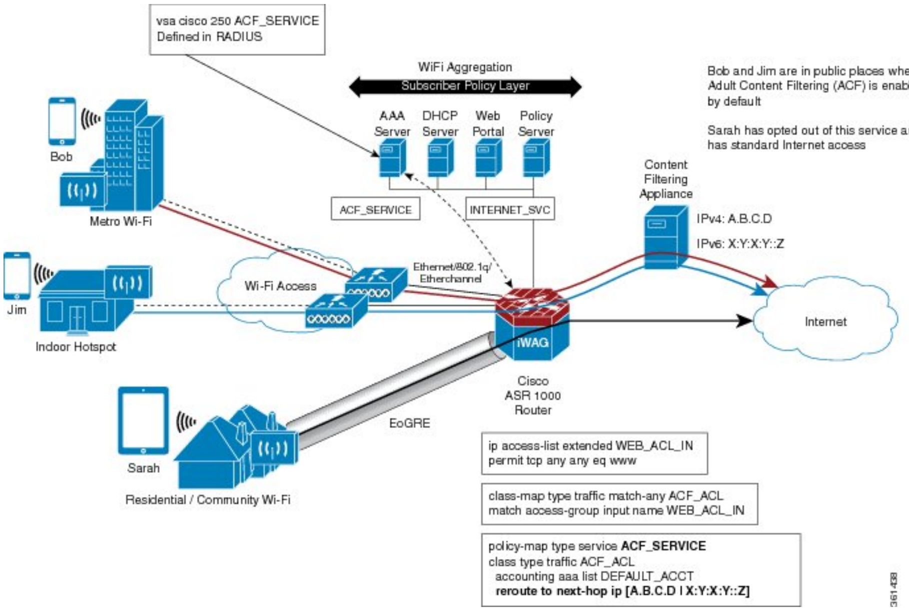
You can apply the ACF policy to subscriber traffic in the following ways:

- If the Wi-Fi hotspot provider allows individual subscribers to opt out of the ACF, the ACF policy is not applied on their personal profile. For those subscribers who do not opt out of the ACF, the ACF policy is applied on their personal profile through the RADIUS vendor-specific attribute (VSA) when they log in to their account. For more information about RADIUS VSA attributes, see Activating and Deactivating the Flow-Based Redirect Feature Through Vendor-Specific Attributes .

- If the Wi-Fi hotspot provider enforces ACF on all the subscribers accessing the internet from their site, the ACF policy is configured in the local policy of the Cisco ISG.

The following figure shows a typical scenario where ACF is applied on Wi-Fi hotspots.

Figure 1: Adult Content Filtering on Wi-Fi Hotspots



```
vsa cisco 250 ACF_SERVICE
Defined in RADIUS
```

Bob and Jim are in public places where Adult Content Filtering (ACF) is enabled by default

Sarah has opted out of this service and has standard Internet access

```
ip access-list extended WEB_ACL_IN
permit tcp any any eq www
```

```
class-map type traffic match-any ACF_ACL
match access-group input name WEB_ACL_IN
```

```
policy-map type service ACF_SERVICE
class type traffic ACF_ACL
 accounting aaa list DEFAULT_ACCT
 reroute to next-hop ip [A.B.C.D I X:Y:X:Y::Z]
```

Flow-Based Redirect for Selective IP Traffic Offload

Mobile IP sessions are provisioned with a traffic class service in the Cisco Intelligent Wireless Access Gateway (iWAG) for routing web traffic to a next hop device, depending on the local policies or the policies that are downloaded from the Cisco IOS authentication, authorization, and accounting (AAA) network security services.

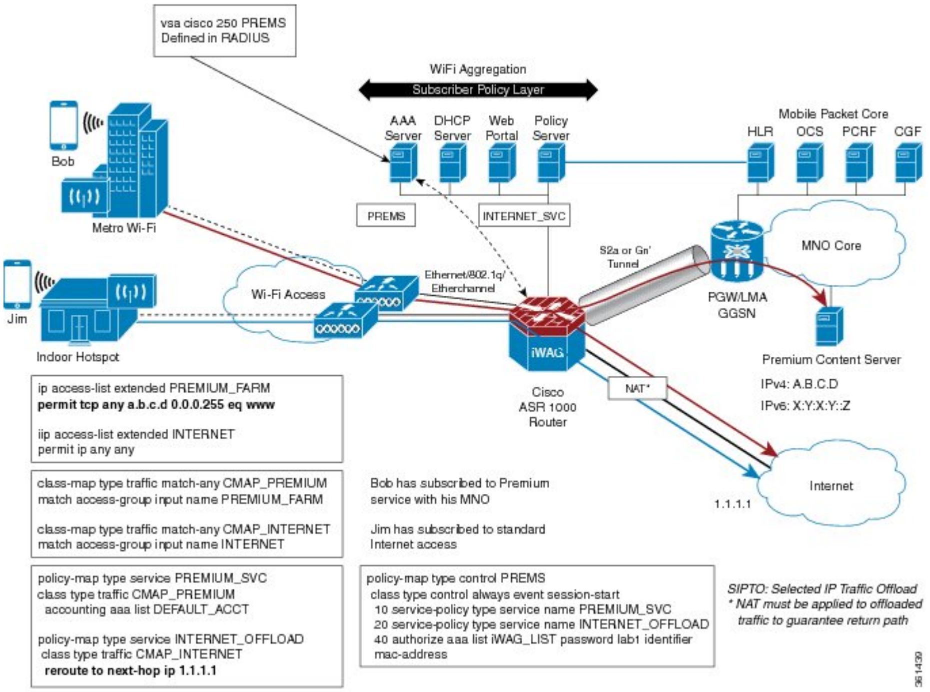
The traffic class service can be configured for routing traffic to the next hop along with the other supported features such as policing and Dynamic Rate Limit (DRL) accounting. You can configure multiple TC services with different next hop addresses with the Flow-Based Redirect feature. However, only 16 traffic class services can be applied to a session.

Network Address Translation (NAT) with Selective IP Traffic Offload (SIPTO) is required only for IPv4 and Dual Stack IPv4 traffic sessions. NAT is enabled at the outgoing interface level so NAT does not need to be IPoE session aware when used with Flow Based Redirect for Selective IP Traffic Offload.

Note In existing deployment, a NAT or Carrier Grade Network Address Translation (CGN) device may exist upstream of the Intelligent Wireless Access Gateway (iWAG) device. In such a scenario, it is possible to keep the architecture in place without enabling NAT on the Cisco ASR 1000 Series Aggregation Services Router acting as iWAG, if and only if, there is a simple way for the return traffic to go from the NAT or CGN device back to the iWAG. This needs to be verified prior to deployment to guarantee return paths.

The following figure shows a typical deployment scenario where internet traffic is offloaded from the access network, and is routed directly through the nearest IP gateway.

Figure 2: Flow-Based Redirect for Selective IP Traffic Offload



```
ip access-list extended PREMIUM_FARM
permit tcp any a.b.c.d 0.0.0.255 eq www

iip access-list extended INTERNET
permit ip any any
```

```
class-map type traffic match-any CMAP_PREMIUM
match access-group input name PREMIUM_FARM

class-map type traffic match-any CMAP_INTERNET
match access-group input name INTERNET
```

```
policy-map type service PREMIUM_SVC
class type traffic CMAP_PREMIUM
  accounting aaa list DEFAULT_ACCT

policy-map type service INTERNET_OFFLOAD
 class type traffic CMAP_INTERNET
  reroute to next-hop ip 1.1.1.1
```

Bob has subscribed to Premium service with his MNO

Jim has subscribed to standard Internet access

```
policy-map type control PREMS
 class type control always event session-start
  10 service-policy type service name PREMIUM_SVC
  20 service-policy type service name INTERNET_OFFLOAD
  40 authorize aaa list iWAG_LIST password lab1 identifier
  mac-address
```

SIPTO: Selected IP Traffic Offload
** NAT must be applied to offloaded traffic to guarantee return path*

Activating and Deactivating the Flow-Based Redirect Feature Through Vendor-Specific Attributes

You can provision or activate a traffic class service with the Flow-Based Redirect feature by adding the following vendor-specific attribute (VSA) in the user profile of the RADIUS server:

```
vsa cisco 250 ACF_SERVICE
```

You can activate a traffic class service with the Flow-Based Redirect feature for an established session through the RADIUS Change of Authorization (CoA) feature, using the following VSAs:

```
vsa cisco 250 S<sessionID>
vsa cisco generic 1 string "subscriber:command=activate-service"
vsa cisco generic 1 string "subscriber:service-name=ACF_SERVICE”
```

You can deactivate a traffic class service with the Flow-Based Redirect feature for an established session through the RADIUS CoA feature, using the following VSAs:

```
vsa cisco 250 S<sessionID>
vsa cisco generic 1 string "subscriber:command=deactivate-service"
vsa cisco generic 1 string "subscriber:service-name=ACF_SERVICE”
```

Configuring Flow-Based Redirect for a Traffic Class Service

The following steps show how to configure the Flow-Based Redirect feature for a traffic class service.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *traffic class*
4. **permit tcp** *source_IP destination_IP* **eq** *port*
5. **class-map type traffic match-any** *traffic class map*
6. **match access-group input name** *traffic class*
7. **policy-map type service** *policy-map name*
8. **class type traffic** *traffic class map*
9. **reroute to next-hop ip** *IP address*
10. **policy-map type control** *policy-map name*
11. **class type control always event account-logon**
12. **20 service-policy type service name** *service-policy name*
13. **class type control always event service-stop**
14. **1 service-policy type service unapply identifier service-name**
15. **class type control always event service-start**
16. **10 service-policy type service identifier service-name**
17. **class type control always event account-logoff**
18. **10 service disconnect delay 5**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list extended** *traffic class* **Example:** `Router (config)# ip access-list extended WEB_ACL_IN`	Defines the traffic class WEB_ACL_IN
Step 4	**permit tcp** *source_IP destination_IP* **eq** *port* **Example:** `Router (config-ext-nacl)# permit tcp any any eq www`	Permits TCP traffic with destination port values that match WWW (port 80).
Step 5	**class-map type traffic match-any** *traffic class map* **Example:** `Router (config)# class-map type traffic match-any ACF_ACL`	Creates the traffic class map ACF_ACL.
Step 6	**match access-group input name** *traffic class* **Example:** `Router (config-traffic-classmap)# match access-group input name WEB_ACL_IN`	Configures the match criteria for the ACF_ACL traffic class map on the basis of the specified host traffic class.
Step 7	**policy-map type service** *policy-map name* **Example:** `Router (config)# policy-map type service ACF_SERVICE`	Creates the ACF_SERVICE policy map, which is used to define an ISG service.

Step 8	**class type traffic** *traffic class map*
	Example:
	`Router (config-service-policymap)# class type traffic ACF_ACL`
		Associates the ACF_ACL traffic class map with the service policy map.

Step 9	**reroute to next-hop ip** *IP address* **Example:** `Router (config-service-policymap-class-traffic)# reroute to next-hop ip 44.0.0.22`	Redirects traffic to the specified IP address.
Step 10	**policy-map type control** *policy-map name* **Example:** `Router (config)# policy-map type control INTERNET_SERVICE_RULE`	Creates the INTERNET_SERVICE_RULE policy map, which is used to define a control policy.
Step 11	**class type control always event account-logon** **Example:**	Specifies a control class for an account-logon event.

	Command or Action	Purpose
	`Router (config-control-policymap)# class type control always event account-logon`	
Step 12	**20 service-policy type service name** *service-policy name* **Example:** `Router (config-control-policymap-class-control)# 20 service-policy type service name ACF_SERVICE`	Applies the ACF_SERVICE policy.
Step 13	**class type control always event service-stop** **Example:** `Router (config-control-policymap)# class type control always event service-stop`	Specifies a control class for a service-stop event.
Step 14	**1 service-policy type service unapply identifier service-name** **Example:** `Router (config-control-policymap-class-control)# 1 service-policy type service unapply identifier service-name`	Specifies the service name that is currently associated with the user.
Step 15	**class type control always event service-start** **Example:** `Router (config-control-policymap)# class type control always event service-start`	Specifies a control class for the service-start event.
Step 16	**10 service-policy type service identifier service-name** **Example:** `Router (config-control-policymap-class-control)# 10 service-policy type service identifier service-name`	Applies the defined service upon a service-start event.
Step 17	**class type control always event account-logoff** **Example:** `Router (config-control-policymap)# class type control always event account-logoff`	Specifies a control class for an account-logoff event.
Step 18	**10 service disconnect delay 5** **Example:** `Router (config-control-policymap-class-control)# 10 service disconnect delay 5`	Disconnects upon an account-logoff event, after a 5 second delay.

Examples

Configuring Flow-Based Redirect for a Traffic Class Service

The following sample output shows how a traffic class service with the Flow-Based Redirect feature is configured to redirect all HTTP traffic to a different next hop device upon logging in to the account:

```
Router# configure terminal
Router (config)# ip access-list extended WEB_ACL_IN
Router (config-ext-nacl)# permit tcp any any eq www
Router (config-ext-nacl)# permit tcp any any eq www
Router (config-ext-nacl)# class-map type traffic match-any ACF_ACL
Router (config-traffic-classmap)# match access-group input name WEB_ACL_IN
Router (config-traffic-classmap)# policy-map type service ACF_SERVICE
Router (config-service-policymap)# class type traffic ACF_ACL
Router (config-service-policymap-class-traffic)# reroute to next-hop ip 44.0.0.22
Router (config-control-policymap-class-control)# policy-map type control INTERNET_SERVICE_RULE
Router (config-control-policymap)# class type control always event account-logon
Router (config-control-policymap-class-control)# 20 service-policy type service name
ACF_SERVICE
Router (config-control-policymap-class-control)# class type control always event service-stop
Router (config-control-policymap-class-control)# 1 service-policy type service unapply
identifier service-name
Router (config-control-policymap)# class type control always event service-start
Router (config-control-policymap-class-control)# 10 service-policy type service identifier
 service-name
Router (config-control-policymap)# class type control always event account-logoff
Router (config-control-policymap-class-control)# 10 service disconnect delay 5
```

Viewing the FBR Policy that is Attached to a Session

To view the FBR policy that is attached to a session at session start, use the **show subscriber session uid** *uid* command:

```
Router# show subscriber session uid 249
Type: IPv4, UID: 249, State: authen, Identity: 33.0.0.4
IPv4 Address: 33.0.0.4
Session Up-time: 00:01:43, Last Changed: 00:01:43
Switch-ID: 16972

Policy information:
  Authentication status: authen
  Active services associated with session:
  name "ACF_SERVICE", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map INTERNET_SERVICE_RULE
      condition always event session-start
        80 authorize identifier source-ip-address
    subscriber rule-map default-internal-rule
      condition always event service-start
        1 service-policy type service identifier service-name


  Classifiers:
Class-id    Dir   Packets    Bytes                   Pri.  Definition
0           In    499        31936                   0    Match Any
1           Out   0          0                       0    Match Any
56          In    499        31936                   0    Match ACL WEB_ACL_IN
57          Out   0          0                       0    Match ACL WEB_ACL_OUT
```

```
Template Id : 1

Features:

Absolute Timeout:
Class-id   Timeout Value    Time Remaining       Source
0          3000             00:48:16             Peruser

Forced Flow Routing:
Class-id   FFR Tunnel Details Source
56
Next-hop IP: 44.0.0.2
 ACF_SERVICE

Configuration Sources:
Type  Active Time  AAA Service ID  Name
SVC   00:01:43     -               ACF_SERVICE
USR   00:01:43     -               Peruser
INT   00:01:43     -               GigabitEthernet0/0/4
```

Verifying the Packet Count Status

To verify whether the packet count on the interface that is connected to the next hop device is increasing, use the **show interface** *interface connected to the next hop device* command:

```
Router(config)# show interface GigabitEthernet0/0/5

GigabitEthernet0/0/5 is up, line protocol is up
  Hardware is SPA-8X1GE-V2, address is 0021.d81a.d305 (bia 0021.d81a.d305)
  Description: IXIA_Client_Facing
  Internet address is 44.0.0.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:05:03, output 00:05:03, output hang never
  Last clearing of "show interface" counters 00:06:48
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 12000 bits/sec, 20 packets/sec
     7 packets input, 690 bytes, 0 no buffer
     Received 2 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     4897 packets output, 382284 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Viewing Statistics of Dropped Packets

To display the statistics of all the dropped packets on the Embedded Services Processor (ESP), use the **show platform hardware qfp active statistics drop** command.

Note As per FBR behavior, the ISG drops packets if *next hop* is unreachable. The **show platform hardware qfp active statistics drop** command output shows counters for the dropped packets.

```
Router# Show platform hardware qfp active statistics drop
-------------------------------------------------------------------------
Global Drop Stats                         Packets                  Octets
-------------------------------------------------------------------------
Disabled                                       13                    1166
essipsubfsoldrop                               2327                  216495
UnconfiguredIpv6Fia                            90                    9492
```

Configuring NAT Access Interface for Ingress Traffic

```
interface GigabitEthernet0/0/4
 ip address 36.0.0.1 255.255.255.0
 ip nat inside
 negotiation auto
 ipv6 address FE80::200:5EFF:FE00:5213 link-local
 service-policy type control PREMS
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
!
```

Configuring NAT Network Interface for Egress Traffic

```
interface GigabitEthernet1/2/4
 description IXIA_port_for_offload
 ip address 44.0.0.1 255.255.255.0
 ip nat outside
 load-interval 30
 negotiation auto
 ipv6 address 44::1/60
!
```

Enabling Carrier Grade NAT

```
ip nat settings mode cgn
no ip nat settings support mapping outside
ip nat pool natpool 55.0.0.3 55.0.255.250 netmask 255.255.0.0
ip nat inside source list 100 pool natpool overload
```

Best Practices for Configuring the NAT on the Cisco ASR 1000 Series Routers

The following are the recommended best practices to configure the NAT on the Cisco ASR 1000 Series Aggregation Services Routers:

- Restriction on the total QFP DRAM usage

At 97 percent DRAM utilization, depletion messages are displayed in the syslog as a warning message to make the operator aware of low QFP DRAM availability. We recommend that you configure QFP DRAM CAC in the system to avoid any unexpected behavior. The Call Admission Control (CAC) functionality ensures that new subscriber sessions cannot be established when QFP DRAM utilization exceeds the configured threshold.

The configuration example below demonstrates configuration of a QFP DRAM threshold set to 95 percent:

platform subscriber cac mem qfp *95*.

- Set the maximum limit for total number of NAT translations:
  - ESP40: **ip nat translation max-entries** *1000000*
  - ESP100: **ip nat translation max-entries** *4000000*
- The **ip nat translation max-entries all-host** command can be used in scenarios where the Cisco ASR 1000 Series Router acting as ISG, performs NAT on all or most of the subscriber traffic. This helps the operator to prevent a single host from occupying the entire translation table, while allowing a reasonable upper limit to each host.
- The maximum number of translations per host can be configured using either of these ways:
  - Configuring the same number of maximum translation entries for all the subscribers using the following command:

    ip nat translation max-entries all-host *maximum number of NAT entries for each host*
  - Configuring the maximum translation entries for a given subscriber using the following command:

    ip nat translation max-entries host *ip-address* [*per-host NAT entry limit*]
- Ensure that you keep the translations timeout low, around 2 minutes for TCP, and 1 minute for UDP translations:
  - **ip nat translation timeout** *120*
  - **ip nat translation tcp-timeout** *120*
  - **ip nat translation udp-timeout** *60*

NAT Overloading and Port Parity

You can preserve the addresses in the global address pool by allowing a device to use one global address for many local addresses. This type of NAT configuration is called overloading.

When an Interface IP is overloaded for the translations and a single IP address is used for all the expected translations, a maximum of 60,000 translations can be achieved with this configuration depending on the traffic ports and the port parity involved. You can use the NAT Pool Overload configuration to achieve maximum translations.

There is a concept of port parity (even/odd) in NAT and NAT64. If a source port is in the port range of 0 to 1023, it is translated between ports 512 to 1023. If a source port range is more than 1023, it takes ports from 1024 onwards.

NAT Interface Overloading with VRF

The NAT Interface Overloading with VRF scenario assumes that the service provider is only interested in performing application-specific NAT, for example, the service provider perform NAT only on the DNS requests from clients and the rest of the traffic will proceed as it is. Therefore, we can use Interface Overloading instead of a pool. With this, we can have a maximum of 60000 translations per interface, which is deemed good for the application-specific NAT. Also, the IP sessions and NAT are in a VRF (named PROVIDER_WIFI_01, in the example below).

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
iWAG commands	Cisco IOS Intelligent Wireless Access Gateway Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Flow-Based Redirect

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Flow-Based Redirect

Feature Name	Releases	Feature Information
Flow-Based Redirect	Cisco IOS XE Release 3.11	Flow-Based Redirect (FBR) feature enables Adult Content Filtering (ACF) to route matching traffic to a specified next hop device.
Flow-Based Redirect for Selective IP Traffic Offload	Cisco IOS XE Release 3.12	Flow-Based Redirect (FBR) feature enables Selective IP Traffic Offload (SIPTO) to route matching traffic to a specified next hop device.