IPv6 Zone-Based Firewall Support over VASI Interfaces

This feature supports VRF-Aware Service Infrastructure (VASI) interfaces over IPv6 firewalls. This feature allows you to apply services such as access control lists (ACLs), Network Address Translation (NAT), policing, and zone-based firewalls to traffic that flows across two different virtual routing and forwarding (VRF) instances. VASI interfaces support the redundancy of Route Processors (RPs) and Forwarding Processors (FPs). VASI interfaces support IPv4 and IPv6 unicast traffic.

This module provides information about VASI interfaces and describes how to configure VASI interfaces.

Restrictions for IPv6 Zone-Based Firewall Support over VASI Interfaces

- Multiprotocol Label Switching (MPLS) traffic over VRF-Aware Software Infrastructure (VASI) interfaces is not supported.
- IPv4 and IPv6 multicast traffic is not supported.
- VASI interfaces do not support the attachment of queue-based features. The following commands are not supported on modular QoS CLI (MQC) policies that are attached to VASI interfaces:
  - **bandwidth (policy-map class)**
  - **fair-queue**
  - **priority**
  - **queue-limit**
  - **random-detect**
  - **shape**

Information About IPv6 Zone-Based Firewall Support over VASI Interfaces

VASI Overview

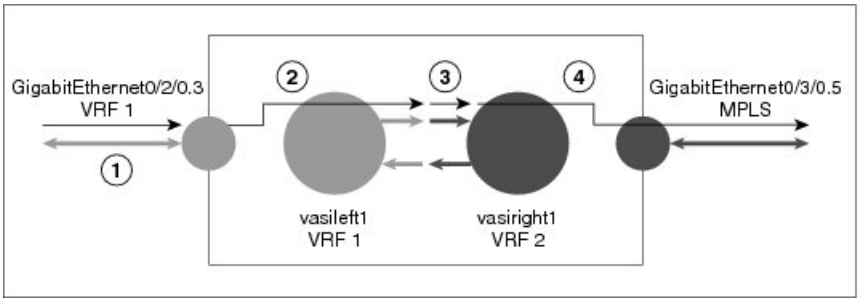
VRF-Aware Software Infrastructure (VASI) provides the ability to apply services such as, a firewall, GETVPN, IPsec, and Network Address Translation (NAT), to traffic that flows across different virtual routing and forwarding (VRF) instances. VASI is implemented by using virtual interface pairs, where each of the interfaces in the pair is associated with a different VRF instance. The VASI virtual interface is the next-hop interface for any packet that needs to be switched between these two VRF instances. VASI interfaces provide the framework to configure a firewall or NAT between VRF instances.

Each interface pair is associated with two different VRF instances. The pairing is done automatically based on the two interface indexes such that the vasileft interface is automatically paired to the vasiright interface. For example, in the figure below, vasileft1 and vasiright1 are automatically paired, and a packet entering vasileft1 is internally handed over to vasiright1.

On VASI interfaces, you can configure either static routing or dynamic routing with Internal Border Gateway Protocol (IBGP), Enhanced Interior Gateway Routing Protocol (EIGRP), or Open Shortest Path First (OSPF).

The following figure shows an inter-VRF VASI configuration on the same device.

Figure 1: Inter-VRF VASI Configuration



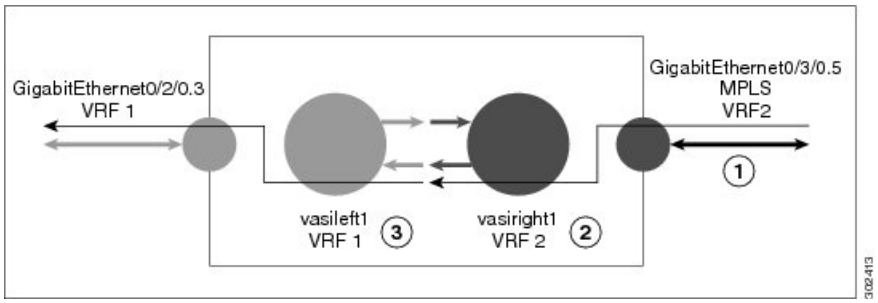
When an inter-VRF VASI is configured on the same device, the packet flow happens in the following order:

1. A packet enters the physical interface that belongs to VRF 1 (Gigabit Ethernet 0/2/0.3).
2. Before forwarding the packet, a forwarding lookup is done in the VRF 1 routing table. Vasileft1 is chosen as the next hop, and the Time to Live (TTL) value is decremented from the packet. Usually, the forwarding address is selected on the basis of the default route in the VRF. However, the forwarding address can also be a static route or a learned route. The packet is sent to the egress path of vasileft1 and then automatically sent to the vasiright1 ingress path.
3. When the packet enters vasiright1, a forwarding lookup is done in the VRF 2 routing table, and the TTL is decremented again (second time for this packet).
4. VRF 2 forwards the packet to the physical interface, Gigabit Ethernet 0/3/0.5.

The following figure shows how VASI works in a Multiprotocol Label Switching (MPLS) VPN configuration.

Note In the following figure, MPLS is enabled on the Gigabit Ethernet interface, but MPLS traffic is not supported across VASI pairs.

Figure 2: VASI with an MPLS VPN Configuration



When VASI is configured with a Multiprotocol Label Switching (MPLS) VPN, the packet flow happens in the following order:

1. A packet arrives on the MPLS interface with a VPN label.
2. The VPN label is stripped from the packet, a forwarding lookup is done within VRF 2, and the packet is forwarded to vasiright1. The TTL value is decremented from the packet.
3. The packet enters vasileft1 on the ingress path, and another forwarding lookup is done in VRF 1. The packet is sent to the egress physical interface in VRF1 (Gigabit Ethernet 0/2/0.3). The TTL is again decremented from the packet.

How to Configure IPv6 Zone-Based Firewall Support over VASI Interfaces

Configuring VRFs and Address Family Sessions

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition VRF1`	Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.
Step 4	**address-family ipv6** **Example:** `Device(config-vrf)# address-family ipv6`	Enters address family configuration mode and configures sessions that carry standard IPv6 address prefixes.
Step 5	**exit-address-family** **Example:** `Device(config-vrf-af)# exit-address-family`	Exits address family configuration mode and enters VRF configuration mode.
Step 6	**end** **Example:** `Device(config-vrf)# end`	Exits VRF configuration mode and enters privileged EXEC mode.

Configuring Class Maps and Policy Maps for VASI Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **class-map type inspect match-any** *class-map-name*
5. **match protocol** *name*
6. **match protocol** *name*
7. **exit**
8. **policy-map type inspect** *policy-map-name*
9. **class type inspect** *class-map-name*
10. **inspect**
11. **exit**

12. **class class-default**
13. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6-unicast routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**class-map type inspect match-any** *class-map-name* **Example:** `Device(config)# class-map type inspect match-any c-map`	Creates an inspect type class map and enters QoS class-map configuration mode.
Step 5	**match protocol** *name* **Example:** `Device(config-cmap)# match protocol icmp`	Configures a match criterion for a class map on the basis of a specified protocol.
Step 6	**match protocol** *name* **Example:** `Device(config-cmap)# match protocol tcp`	Configures a match criterion for a class map on the basis of a specified protocol.
Step 7	**exit** **Example:** `Device(config-cmap)# exit`	Exits QoS class-map configuration mode and enters global configuration mode.
Step 8	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect p-map`	Creates a protocol-specific inspect-type policy map and enters QoS policy-map configuration mode.
Step 9	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect c-map`	Specifies the traffic class on which an action is to be performed and enters QoS policy-map class configuration mode.

	Command or Action	Purpose
Step 10	**inspect** **Example:** `Device(config-pmap-c)# inspect`	Enables stateful packet inspection.
Step 11	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits QoS policy-map class configuration mode and enters QoS policy-map configuration mode.
Step 12	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Applies the policy map settings to the predefined default class and enters QoS policy-map class configuration mode. • If traffic does not match any of the match criteria in the configured class maps, it is directed to the predefined default class.
Step 13	**end** **Example:** `Device(config-pmap-c)# end`	Exits QoS policy-map class configuration mode and enters privileged EXEC mode.

Configuring Zones and Zone Pairs for VASI Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
6. **service-policy type inspect** *policy-map-name*
7. **exit**
8. **interface** *type number*
9. **vrf forwarding** *vrf-name*
10. **no ip address**
11. **zone member security** *zone-name*
12. **ipv6 address** *ipv6-address*/*prefix-length*
13. **ipv6 enable**
14. **negotiation auto**
15. **exit**
16. **interface** *type number*
17. **no ip address**
18. **ipv6 address** *ipv6-address*/*prefix-length*
19. **ipv6 enable**
20. **negotiation auto**
21. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**zone security** *zone-name* **Example:** `Device(config)# zone security in`	Creates a security zone and enters security zone configuration mode. • Your configuration must have two security zones to create a zone pair: a source and a destination zone. • In a zone pair, you can use the default zone as either the source or the destination zone.
Step 4	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.
Step 5	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* **Example:** `Device(config)# zone-pair security in-out source in destination out`	Creates a zone pair and enters security zone-pair configuration mode. • To apply a policy, you must configure a zone pair.
Step 6	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect p-map`	Attaches a policy map to a top-level policy map. • If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 7	**exit** **Example:** `Device(config-sec-zone-pair)# exit`	Exits security zone-pair configuration mode and enters global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 9	**vrf forwarding** *vrf-name* **Example:**	Associates a virtual routing and forwarding (VRF) instance or a virtual network with an interface or subinterface.

	Command or Action	Purpose
	`Device(config-if)# vrf forwarding VRF1`	
Step 10	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 11	**zone member security** *zone-name* **Example:** `Device(config-if)# zone member security in`	Attaches an interface to a security zone.
Step 12	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:2:1234/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 13	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 14	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface.
Step 15	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 16	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/1`	Configures an interface and enters interface configuration mode.
Step 17	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 18	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:3:1234/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 19	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 20	**negotiation auto** **Example:**	Enables advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface.

	Command or Action	Purpose
	`Device(config-if)# negotiation auto`	
Step 21	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Configuring VASI Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
6. **ipv6 address** *ipv6-address*/*prefix-length*
7. **ipv6 enable**
8. **no keepalive**
9. **zone member security** *zone-name*
10. **exit**
11. **interface** *type number*
12. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
13. **ipv6 address** *ipv6-address*/*prefix-length*
14. **ipv6 enable**
15. **no keepalive**
16. **exit**
17. **ipv6 route** *ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*
18. **ipv6 route vrf** *vrf-name ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*
19. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface vasileft 1`	Configures a VASI interface and enters interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding VRF1`	Associates a virtual routing and forwarding (VRF) instance or a virtual network with an interface or subinterface.
Step 5	**ipv6 address** *ipv6-address/prefix-length* **link-local** **Example:** `Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local`	Configures an IPv6 link-local address for an interface and enable IPv6 processing on the interface.
Step 6	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 7	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 8	**no keepalive** **Example:** `Device(config-if)# no keepalive`	Disables keepalive packets.
Step 9	**zone member security** *zone-name* **Example:** `Device(config-if)# zone member security out`	Attaches an interface to a security zone.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 11	**interface** *type number* **Example:** `Device(config)# interface vasiright 1`	Configures a VASI interface and enters interface configuration mode.
Step 12	**ipv6 address** *ipv6-address/prefix-length* **link-local** **Example:** `Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local`	Configures an IPv6 link-local address for an interface and enable IPv6 processing on the interface.
Step 13	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

	Command or Action	Purpose
Step 14	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 15	**no keepalive** **Example:** `Device(config-if)# no keepalive`	Disables keepalive packets.
Step 16	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 17	**ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number ipv6-address* **Example:** `Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64`	Establishes static IPv6 routes.
Step 18	**ipv6 route vrf** *vrf-name ipv6-prefix/prefix-length interface-type interface-number ipv6-address* **Example:** `Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64`	Specifies all VRF tables or a specific VRF table for an IPv6 address.
Step 19	**end** **Example:** `Device(config# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuration Examples for IPv6 Zone-Based Firewall Support over VASI Interfaces

Example: Configuring VRFs and Address Family Sessions

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# end
```

Example: Configuring Class Maps and Policy Maps for VASI Support

```
Device# configure terminal
Device(config)# ipv6-unicast routing
Device(config)# class-map type inspect match-any c-map
Device(config-cmap)# match protocol icmp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p-map
Device(config-pmap)# class type inspect c-map
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# end
```

Example: Configuring Zones and Zone Pairs for VASI Support

```
Device# configure terminal
Device(config)# zone security in
Device(config)# exit
Device(config)# zone security out
Device(config)# exit
Device(config)# zone-pair security in-out source in destination out
Device(config-sec-zone-pair)# service-policy type inspect p-map
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# vrf forwarding VRF1
Device(config-if)# no ip address
Device(config-if)# zone member security in
Device(config-if)# ipv6 address 2001:DB8:2:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8:3:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# end
```

Example: Configuring VASI Interfaces

```
Device# configure terminal
Device(config)# interface vasileft 1
Device(config-if)# vrf forwarding VRF1
Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# zone-member security out
Device(config-if)# exit
Device(config)# interface vasiright 1
Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
```

```
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# exit
Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64
Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64
Device(config)# end
```

Additional References for Firewall Stateful Interchassis Redundancy

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Zone-Based Firewall Support over VASI Interfaces

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 IPv6 Zone-Based Firewall Support VASI Interfaces

Feature Name	Releases	Feature Information
IPv6 Zone-Based Firewall Support over VASI Interfaces	Cisco IOS XE Release 3.7S	This feature supports VASI interfaces over IPv6 firewalls. This feature allows you to apply services such as access control lists (ACLs), Network Address Translation (NAT), policing, and zone-based firewalls to traffic that flows across two different virtual routing and forwarding (VRF) instances. VASI interfaces support the redundancy of Route Processors (RPs) and Forwarding Processors (FPs). VASI interfaces support IPv4 and IPv6 unicast traffic. No commands were introduced or modified for this feature.