LISP and Zone-Based Firewalls Integration and Interoperability

The LISP and Zone-Based Firewalls Integration and Interoperability feature enables inner-packet inspection of all Locator ID Separation Protocol (LISP) data packets that pass through a device. To enable LISP inner packet inspection, you have to configure the **lisp inner-packet inspection** command. Without LISP inner packet inspection, endpoint identifier (EID) devices in a LISP network will not have any firewall protection.

This module describes how to configure this feature.

Feature Information for LISP and Zone-Based Firewall Integration and Interoperability

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 LISP and Zone-Based Firewall Integration and Interoperability

Feature Name	Releases	Feature Information
LISP and Zone-Based Firewall Integration and Interoperability	Cisco IOS XE Release 3.13S	The LISP and Zone-Based Firewalls Integration and Interoperability feature enables inner-packet inspection of all Locator ID Separation Protocol (LISP) data packets that pass through a device. To enable LISP inner packet inspection, you have to configure the lisp inner-packet inspection command. Without LISP inner inspection, endpoint identifier (EID) devices in a LISP network will not have any firewall protection. The following commands were introduced or modified by this feature: **lisp inner-packet-inspection**, **show parameter-map type inspect-global**, and **show parameter-map type inspect global**.
Intrachassis and Interchassis High Availability for Zone-Based Firewall and LISP Integration	Cisco IOS XE Release 3.14S	In Cisco IOS XE Release 3.14S, the LISP and Zone-Based Firewall Integration and Interoperability feature supports both intrachassis and interchassis high availability. No commands were introduced or modified by this feature.

Prerequisites for LISP and Zone-Based Firewall Integration and Interoperability

- The interchassis high availability configuration on active device and standby devices must be identical.

Restrictions for LISP and Zone-Based Firewall Integration and Interoperability

The following features are not supported:

- Locator ID Separator Protocol (LISP) mobility
- Zone-based firewall, LISP, and Web Cache Control Protocol (WCCP) interoperability
- Zone-based firewall and LISP subinterfaces with VRF interoperability

These features are not supported when LISP inner packet inspection is enabled:

- Asymmetric routing
- LISP control message inspection
- LISP inner packet fragmentation

- Network Address Translation (NAT) and NAT 64
- TCP reset
- Virtual routing and forwarding (VRF)
- Virtual TCP (vTCP)
- VRF-Aware Software Infrastructure (VASI)
- Web Cache Communication Protocol (WCCP)

Information About LISP and Zone-Based Firewalls Integration and Interoperability

LISP Overview

The Locator ID Separation Protocol (LISP) is a network architecture and protocol. LISP replaces a single IP address with two numbering spaces—Routing Locators (RLOCs), which are topologically assigned to network attachment points and used for routing and forwarding of packets through the network; and Endpoint Identifiers (EIDs), which are assigned independently from the network topology and used for numbering devices, and are aggregated along administrative boundaries.

LISP defines functions for mapping between the two numbering spaces and encapsulating traffic originated by devices using non-routable EIDs for transport across a network infrastructure that routes and forwards using RLOCs. LISP provides a set of functions for devices to exchange information that is used to map non-routable EIDs to routable RLOCs.

LISP requires LISP-specific configuration of one or more LISP-related devices, such as the LISP egress tunnel router (ETR), ingress tunnel router (ITR), proxy ETR (PETR), proxy ITR (PITR), map resolver (MR), map server (MS), and LISP alternative logical topology (ALT) device.

Zone-Based Firewall and LISP Interoperability Overview

The zone-based firewall can be deployed either on the southbound or northbound of the Locator ID Separator Protocol (LISP) xTR device, depending on where the edge router (routers such as Cisco ASR 1000 Aggregation Services Routers) is located in the network. The ingress tunnel router (ITR) and egress tunnel router (ETR) together are called the xTR device.

When the zone-based firewall is at the northbound of the xTR device; then the firewall can view LISP encapsulated packets, such as LISP tunneled packets, that pass through the network.

When the zone-based firewall is at the southbound of the xTR device, then the firewall can view the original packet. However; the firewall is not aware of any LISP xTR processing or do not see any LISP header. For egress packets, the xTR device does LISP encapsulation and adds the LISP header on top of the original packet after the firewall inspection. For ingress packets, the xTR device does LISP decapsulation (removal of the LISP header) before the firewall inspection and as a result, the firewall only inspects the original packet; and has no interaction with LISP at all.

This section describes the scenario when the zone-based firewall is deployed at the southbound of the LISP xTR device:

If an edge router is configured as a LISP xTR device to perform LISP encapsulation and decapsulation functions, you can configure the zone-based firewall between the LISP interface and the interfaces that face the LISP local endpoint identifier (EID) devices on the same edge router. LISP header decapsulation is performed before the header enters the zone-based firewall at the LISP interface. LISP header encapsulation is performed after the packet egresses from the firewall at the LISP interface. The firewall inspects only native traffic (what is native traffic here?) in the EID space.

This section describes the scenario when the zone-based firewall is deployed at the northbound of the LISP xTR devicce:

If more than one edge routers are deployed as load-sharing routers at the northbound of the xTR device, the firewall on the edge router is considered northbound of the xTR device. In this case, all packets that pass through the zone-based firewall are LISP encapsulated packets. When a packet arrives, the firewall inspects either the inner header or outer header of the LISP packets. By default, only the outer header is inspected. You can enable inner header inspection by using the **lisp inner-packet-inspection** command.

In Cisco IOS XE Release, if LISP inner packet inspection is enabled, the firewall only inspects the first fragmented inner packet, and all subsequent inner packets pass through the firewall without further inspection. If LISP inner packet inspection is enabled, the LISP instance ID is treated as virtual routing and forwarding (VRF) ID, and LISP packets that belong to different instance IDs are associated with different zone-based firewall sessions.

Feature Interoperability LISP

In Cisco IOS XE Release 3.13S, the LISP and Zone-Based Firewall Integration and Interoperability feature, works with the following features:

- IPv4 inner and outer headers
- IPv6 inner and outer headers
- LISP multitenancy
- Application layer gateways (ALGs)
- Application Inspection and Control (AIC)
- Mulitprotocol Label Switching (MPLS)
- In-Service Software Upgrade (ISSU)
- PxTR Case

Intrachassis and Interchassis High Availability for Zone-Based Firewall and LISP Integration

In Cisco IOS XE Release 3.14S, the LISP and Zone-Based Firewall Integration and Interoperability feature supports both intrachassis and interchassis high availability. When Location ID Separation Protocol (LISP) inner packet inspection is enabled, interchassis and intrachassis redundancy are supported at the xTR northbound device.

For LISP inner packet inspection at the northbound device, LISP instance ID is used as the virtual routing and forwarding (VRF) instance. The VRF configuration at northbound device is ignored if LISP inner packet inspection is enabled.

When two devices are located at the northbound of the xTR device and the xTR device is located inside the cloud, if LISP inner packet inspection is enabled on both devices, zone-based firewall sessions that are created for LISP inner packet flow is synced to the standby device.

A typical interchassis (box-to-box) high availability topology will have two devices in the routing locator (RLOC) space at the northbound of the xTR device. The xTR device sits in the inside network. If LISP inner packet inspection is enabled on both devices, zone-based firewall sessions that are created for LISP inner packets are synced to the standby device.

There are no configuration changes for intrachassis redundancy.

How to Configure LISP and Zone-Based Firewalls Integration and Interoperability

Enabling LISP Inner Packet Inspection

You can configure LISP inner packet inspection after configuring the **parameter-map type inspect global** command or the **parameter-map type inspect-global** command.

Note You cannot configure both these commands simultaneously.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **lisp inner-packet-inspection**
5. **end**
6. **show parameter-map type** {**inspect global** | **inspect-global**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect global** **Example:**	Configures a global inspect-type parameter map for connecting thresholds, timeouts, and other parameters

	Command or Action	Purpose
	`Device(config)# parameter-map type inspect global`	pertaining to the inspect action, and enters parameter-map type inspect configuration mode.
Step 4	**lisp inner-packet-inspection** **Example:** `Device(config-profile)# lisp inner-packet-inspection`	Enables LISP inner packet inspection.
Step 5	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.
Step 6	**show parameter-map type** {**inspect global** | **inspect-global**} **Example:** `Device# show parameter-map type inspect-global`	Displays global inspect-type parameter map information.

Example

The following sample output from the **show parameter-map type inspect-global** command displays that LISP inner-packet inspection is enabled:

```
Device# show parameter-map type inspect-global

parameter-map type inspect-global
  log dropped-packet off
  alert on
  aggressive aging disabled
  syn_flood_limit  unlimited
  tcp window scaling enforcement loose off
  max incomplete unlimited  aggressive aging disabled
  max_incomplete TCP unlimited
  max_incomplete UDP unlimited
  max_incomplete ICMP unlimited
  application-inspect all
  vrf default inspect vrf-default
  vrf vrf2 inspect vrf-default
  vrf vrf3 inspect vrf-default
  lisp inner-packet-inspection
```

Configuring Interchassis High Availability for LISP Inner Packet Inspection

Configuring the xTR Southbound Interface for Interchassis High Availability

Before you begin

Prerequisites

- Zones and zone-pairs must be configured.

- Redundancy and redundancy groups must be configured. See, the "Configuring Firewall Stateful Interchassis Redundancy" module in the *Zone-Based Policy Firewall Configuration Guide* for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **description** *string*
6. **ip address** *ip-address mask*
7. **exit**
8. **interface** *type number*
9. **description** *string*
10. **zone-member security** *zone-name*
11. **exit**
12. **interface** *type number*
13. **description** *string*
14. **ip address** *ip-address mask*
15. **zone-member security** *zone-name*
16. **cdp enable**
17. **end**

DETAILED STEPS

	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	**interface** *type number* **Example:** `Device(config)# interface TenGigabitEthernet 1/3/0`	Configures an interface and enters interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding lower`	Associates a VRF instance or a virtual network with an interface or subinterface.
Step 5	**description** *string* **Example:**	Adds a description to an interface configuration. • The zone-based firewall cannot be configured at this interface.

	Command or Action	Purpose
	`Device(config-if)# description facing RLOC and the LISP cloud; has a LISP header.`	
Step 6	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.0.1.27 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface LISP 0`	Configures an interface and enters interface configuration mode. • This is the LISP virtual interface.

Step 9	**description** *string*
	Example:
	`Device(config-if)# description LISP virtual interface.`
	`Adds LISP header after firewall inspection or removes LISP header before firewall inspection.`
		Adds a description to an interface configuration.

Step 10	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security ge0-0-3a`	Attaches an interface to a security zone.
Step 11	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 12	**interface** *type number* **Example:** `Device(config)# interface tengigabitethernet 0/3/0`	Configures an interface and enters interface configuration mode.
Step 13	**description** *string* **Example:** `Device(config-if)# description facing internal network, does not have a LISP header.`	Adds a description to an interface configuration.
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.0.2.5 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 15	**zone-member security** *zone-name* **Example:**	Attaches an interface to a security zone.

	Command or Action	Purpose
	`Device(config-if)# zone-member security ge0-0-0`	
Step 16	**cdp enable** **Example:** `Device(config-if)# cdp enable`	Enable Cisco Discovery Protocol (CDP) on an interface.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the xTR Northbound Interface for LISP Inner Packet Inspection

In this configuration, a Locator ID Separation Protocol (LISP) virtual interface is not needed because at northbound the LISP header is not inspected. However, you can configure the zone-based firewall to inspect either LISP inner packets or outer packets.

Before you begin

- Zones and zone-pairs must be configured.
- Redundancy and redundancy groups must be configured. See, the "Configuring Firewall Stateful Interchassis Redundancy" module in the *Zone-Based Policy Firewall Configuration Guide* for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **redundancy rii** *id*
9. **redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value*
10. **exit**
11. **interface** *type number*
12. **description** *string*
13. **ip address** *ip-address mask*
14. **zone-member security** *zone-name*
15. **negotiation auto**
16. **redundancy rii** *id*
17. **redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value*
18. **ip virtual-reassembly**
19. **end**

DETAILED STEPS

	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	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 1/2/1`	Configures an interface and enters interface configuration mode. • This interface can see the entire LISP packet.
Step 4	**description** *string* **Example:** `Device(config-if)# description RLOC-space/north LAN`	Adds a description to an interface configuration.
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 198.51.100.8 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 6	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security ge0-0-3`	Attaches an interface to a security zone.
Step 7	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface.
Step 8	**redundancy rii** *id* **Example:** `Device(config-subif)# redundancy rii 200`	Configures the redundancy interface identifier (RII) for redundancy group protected traffic interfaces
Step 9	**redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value* **Example:** `Device(config-if)# redundancy group 1 ip 198.51.100.12 exclusive decrement 50`	Enables the redundancy group (RG) traffic interface configuration.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 11	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/3`	Configures an interface and enters interface configuration mode. • This interface can see the entire LISP packet.
Step 12	**description** *string* **Example:** `Device(config-if)# description RLOC-space/south LAN`	Adds a description to an interface configuration.
Step 13	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 198.51.100.27 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 14	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security ge0-0-0`	Attaches an interface to a security zone.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface.
Step 16	**redundancy rii** *id* **Example:** `Device(config-subif)# redundancy rii 300`	Configures the redundancy interface identifier (RII) for redundancy group protected traffic interfaces
Step 17	**redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value* **Example:** `Device(config-if)# redundancy group 1 ip 194.88.4.1 exclusive decrement 50`	Enables the RG traffic interface configuration.
Step 18	**ip virtual-reassembly** **Example:** `Device(config-if)# ip virtual-reassembly`	Enables virtual fragment reassembly (VFR) on an interface.
Step 19	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for LISP and Zone-Based Firewalls Integration and Interoperability

Example: Enbaling LISP Inner Packet Inspection

```
Device# configure terminal
Device(config)# parameter-map type inspect-global
Device(config-profile)# lisp inner-packet-inspection
Device(config-profile)# end
```

The following example shows a zone-based firewall configuration with LISP inner-packet inspection enabled:

```
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

class-map type inspect match-any c-ftp-tcp
 match protocol ftp
 match protocol telnet
 match protocol http
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class type inspect c-ftp-tcp
  inspect
 class class-default
!
zone security ge0-0-0
!
zone security ge0-0-3
!
zone-pair security zp-ge000-ge003 source ge0-0-0 destination ge0-0-3
 service-policy type inspect p1
!
zone-pair security zp-ge003-ge000 source ge0-0-3 destination ge0-0-0
 service-policy type inspect p1
!
interface TenGigabitEthernet 1/3/0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:DB8:100::2/64
 zone-member security ge0-0-0
!
interface TenGigabitEthernet 0/3/0
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:DB8:200::2/64
 zone-member security ge0-0-3
!
parameter-map type inspect global
 lisp inner-packet-inspection
 log dropped-packet off
  alert on
```

!

Configuring Interchassis High Availability for LISP Inner Packet Inspection

Additional References for LISP and Zone-Based Firewalls Integration and Interoperability

Related Documents

Related Topic	Document Title
Cisco 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
LISP commands	Cisco IOS IP Routing: LISP Command Reference
LISP configuration guide	*IP Routing: LISP Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 6830	*The Locator/ID Separation Protocol (LISP)*

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/support