IP Addressing: Fragmentation and Reassembly Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Virtual Fragmentation Reassembly

Virtual fragmentation reassembly (VFR) enables the Cisco IOS Firewall to create the appropriate dynamic access control lists (ACLs) to protect the network from various fragmentation attacks.

Without VFR, the Cisco IOS Firewall--specifically Context-based Access Control (CBAC) and the Intrusion Detection System (IDS)--cannot identify the contents of the IP fragments nor can it gather port information from the fragment. These inabilities allow the fragments to pass through the network without being examined or without dynamic ACL creation.

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 at the end of this module.

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.

Restrictions for Virtual Fragmentation Reassembly

Performance Impact

VFR causes a performance impact on the basis of functions such as packet copying, fragment validation, and fragment reorder. This performance impact varies depending on the number of concurrent IP datagrams that are being reassembled.

VFR Configuration Restriction

VFR should not be enabled on a router that is placed on an asymmetric path. The reassembly process requires all of the fragments within an IP datagram. Routers placed in the asymmetric path may not receive all of the fragments, so the fragment reassembly will fail.

Information About Virtual Fragmentation Reassembly

VFR Detection of Fragment Attacks

VFR is responsible for detecting and preventing the following types of fragment attacks:

- Tiny fragment attack--In this type of attack, the attacker makes the fragment size small enough to force Layer 4 (TCP and UDP) header fields into the second fragment. Thus, the ACL rules that have been configured for those fields will not match.

VFR drops all tiny fragments, and an alert message such as “VFR-3-TINY_FRAGMENTS” is logged to the syslog server.

- Overlapping fragment attack--In this type of attack, the attacker can overwrite the fragment offset in the noninitial IP fragment packets. When the firewall reassembles the IP fragments, it might create wrong IP packets, causing the memory to overflow or the system to reload.

VFR drops all fragments within a fragment chain if an overlap fragment is detected.

- Buffer overflow attack--In this type of denial-of-service (DoS) attack, the attacker can continuously send a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

To avoid buffer overflow and control memory use, configure a maximum threshold for the number of IP datagrams that are being reassembled and the number of fragments per datagram. You can use the **ip virtual-reassembly** command or the **ip virtual-reassembly-out** command to specify these parameters.

When the maximum number of datagrams that can be reassembled at any given time is reached, all subsequent fragments are dropped, and the global statistics item “ReassDrop” is incremented by one.

When the maximum number of fragments per datagram is reached, subsequent fragments are dropped, and the global statistics item “ReassTooManyFrags” is incremented by one. .

In addition to the maximum threshold values being configured, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time, the timer expires and the IP datagram and all of its fragments are dropped.

VFR Enablement

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). By default, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, VFR will maintain a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled.

VFR on Outbound Interfaces

In Cisco IOS Release XE 3.2S and later releases, you can use the **ip virtual-reassembly-out**command to manually enable or disable VFR on outbound interface traffic.

How to Configure Virtual Fragmentation Reassembly

Configuring VFR

Perform this task to enable VFR on an interface, specify maximum threshold values to combat buffer overflow and control memory usage, and verify any VFR configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
5. **exit**
6. **exit**
7. show ip virtual-reassembly [interface type]

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/0/1`	Configures an interface type and enters interface configuration mode.
Step 4	ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments] **Example:** `Router(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5`	Enables VFR on the interface and specifies the maximum threshold values.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 7	show ip virtual-reassembly [interface type] **Example:** `Router# show ip virtual-reassembly GigabitEthernet0/0/1`	Displays the configuration and statistical information of the VFR. • If an interface is not specified, VFR information is shown for all configured interfaces.

Enabling VFR Manually on Outbound Interface Traffic

Perform this task to enable VFR manually on outbound interface traffic. You can use this procedure to reenable VFR on outbound interface traffic if it is disabled, for example, by the **no ip virtual-reassembly** command.

Note If VFR is enabled on both inbound and outbound interface traffic, you can use the **no ip virtual-reassembly-out**command to disable it on only the outbound interface traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/0/1`	Configures an interface type and enters interface configuration mode.
Step 4	ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments] **Example:** `Router(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5`	Enables VFR on the interface and specifies the maximum threshold values.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

• Troubleshooting Tips, page 6

Troubleshooting Tips

To display debugging messages related to the VFR subsystem, use the **debug ip virtual-reassembly** command.

Configuration Examples for Fragmentation Reassembly

Example Configuring VFR on Outbound Interface Traffic

The following example shows how to manually enable VFR on outbound traffic on interfaces GigabitEthernet0/0/1, GigabitEthernet0/0/0.773, and Serial 3/0:

```
interface Loopback 0
ip address 10.0.1.1 255.255.255.255
!
interface GigabitEthernet0/0/1
description LAN1
ip address 10.4.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface GigabitEthernet0/0/0.773
encapsulation dot1Q 773
description LAN2
ip address 10.15.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface Serial 3/0
description Internet
ip unnumbered Loopback0
encapsulation ppp
ip virtual-reassembly-out
serial restart-delay 0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
Dynamic IDS	Cisco IOS Intrusion Prevention System
CBAC	"Configuring Context-Based Access Control"

Standards

Standards	Title
None	--

MIBs

MIB	MIBs Link
None	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

RFCs

RFCs	Title
RFC 791	*Internet Protocol*
RFC 1858	*Security Considerations for IP Fragment Filtering*

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 Virtual Fragmentation Reassembly

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 Virtual Fragmentation Reassembly

Feature Name	Releases	Feature Information
Virtual Fragmenatation Reassembly	Cisco IOS XE Release 3.2S	VFR enables the Cisco IOS Firewall to create the appropriate dynamic ACLs to protect the network from various fragmentation attacks. In Cisco IOS Release XE 3.2S, functionality to manually configure VFR for outbound or inbound interface traffic was added. The following commands were introduced or modified: **ip virtual-reassembly-out, show ip virtual-reassembly**.

IPv6 Virtual Fragmentation Reassembly

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 at the end of this module.

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.

Information About IPv6 Virtual Fragmentation Reassembly

IPv6 Virtual Fragmentation Reassembly

Fragmentation is a process of breaking down an IP datagram into smaller packets to be transmitted over different types of network media. Non-initial fragments of a fragmented IPv6 packet is used to pass through IPsec and NAT64 without any examination due to the lack of the L4 header, which usually is only available on the initial fragment. The IPv6 Virtual Fragmentation Reassembly (VFR) feature provides the ability to collect the fragments and provide L4 info for all fragments for IPsec and NAT64 features.

How to Implement IPv6 Virtual Fragmentation Reassembly

Configuring IPv6 Virtual Fragmentation Reassembly

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. ipv6 virtual-reassembly [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**
5. **exit**
6. show ipv6 virtual-reassembly interface *interface-type*
7. show ipv6 virtual-reassembly features interface *interface-type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 3/1/1`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	ipv6 virtual-reassembly [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments** **Example:** `Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7`	Enables VFR on an interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and places the router in global configuration mode. • Enter this command twice to reach privileged EXEC mode.
Step 6	show ipv6 virtual-reassembly interface *interface-type* **Example:** `Router# show ipv6 virtual-reassembly interface e1/1/1`	Displays VRF configuration and statistical information on a specific interface.
Step 7	show ipv6 virtual-reassembly features interface *interface-type* **Example:** `Router# show ipv6 virtual-reassembly features`	Displays VFR information on all interfaces or on a specified interface.

Configuration Example for IPv6 Virtual Fragmentation Reassembly

- Example: Configuring IPv6 Virtual Fragmentation Reassembly, page 11

Example: Configuring IPv6 Virtual Fragmentation Reassembly

```
Router# show ipv6 virtual-reassembly interface gigabitethernet1/1/1
GigabitEthernet1/1/1:
IPv6 Virtual Fragment Reassembly (VFR) is ENABLED(in)
Concurrent reassemblies (max-reassemblies): 64
Fragments per reassembly (max-fragments): 16
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF
Current reassembly count: 0
Current fragment count: 0
Total reassembly count: 6950
Total reassembly timeout count: 9
GigabitEthernet1/1/1:
IPv6 Virtual Fragment Reassembly (VFR) is ENABLED(out)
Concurrent reassemblies (max-reassemblies): 64
Fragments per reassembly (max-fragments): 16
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF
Current reassembly count: 0
Current fragment count: 0
Total reassembly count: 0
Total reassembly timeout count: 0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Master Commands List, All Releases
IPv6 commands	IPv6 Command Reference
Cisco IOS IPv6 features	IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

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 Virtual Fragmentation Reassembly

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 2 Feature Information for IPv6 Virtual Fragmentation Reassembly

Feature Name	Releases	Feature Information
IPv6 Virtual Fragmentation Reassembly	Cisco IOS XE Release 3.4S	The IPv6 VFR feature provides the ability to collect the fragments and provide L4 info for all fragments for IPsec and NAT64 features.

GRE Fragment and Reassembly Performance Tuning

The GRE Fragment and Reassembly Performance Tuning feature enables you to customize reassembly resources. Reassembly resources are equally allocated to each interface to prevent fragment-related attack. However, in some generic routing encapsulation (GRE) tunnel deployments, fragments are reassembled in specific interfaces. This feature also allows you to adjust the reassembly timer to free up incomplete fragment sessions quickly and reserve the reassembly resources for high priority packets.

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 at the end of this module.

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.

Restrictions for GRE Fragment and Reassembly

- The IPv4 or IPv6 protocol must be enabled on an interface.
- This feature supports manually created tunnel interfaces or physical interfaces (virtual template is not officially supported).

Information About GRE Fragment and Reassembly

Fragmentation and Reassembly

In Cisco software, packets may be dropped due to nonavailability of reassembly resources of an interface when fragments arrive concurrently on an interface, though, other interfaces have the resources to reassemble fragments. In some cases, some interfaces need additional resources, such as generic routing encapsulation (GRE) tunnel deployment, and resources are freed only when fragments are reassembled. Therefore, if all fragments are not received, the reassembly resources are not freed.

The GRE Fragment and Reassembly Performance Tuning feature improves reassembly performance by reassembling high priority fragments first so that these fragments are not dropped when low priority fragments occupy the reassembly resources.

How to Use GRE Fragment and Reassembly

- Configuring GRE Fragment and Reassembly (GFR), page 16

Configuring GRE Fragment and Reassembly (GFR)

Perform this task to do the following:

- Enable generic routing encapsulation (GRE) Fragment and Reassembly (GFR) on an interface
- Specify maximum threshold values to combat buffer overflow and control memory usage
- Verify GFR configurations

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Enter one of the following:
   - **ip reassembly** [**max-reassemblies** *number*] [**timeout** *milliseconds*] [**percentage** *percent* {**dscp** *dscp-value* | **precedence** *precedence-value*}]
   - **ipv6 reassembly** [**max-reassemblies** *number*] [**timeout** *milliseconds*] [**percentage** *percent* {**dscp** *dscp-value* | **precedence** *precedence-value*}]
5. **end**
6. Enter one of the following:
   - **show ip reassembly interface** *type number*
   - **show ipv6 reassembly interface** *type number*

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 0/0/0`	Configures an interface type and enters interface configuration mode.

Step 4	Enter one of the following:
	• **ip reassembly** [**max-reassemblies** *number*] [**timeout** *milliseconds*] [**percentage** *percent* {**dscp** *dscp-value* | **precedence** *precedence-value*}]
	• **ipv6 reassembly** [**max-reassemblies** *number*] [**timeout** *milliseconds*] [**percentage** *percent* {**dscp** *dscp-value* | **precedence** *precedence-value*}]
	
	Example:
	`Device(config-if)# ip reassembly max-reassemblies 1024 timeout 1000 percentage 50 precedence critical routine`
	
	Example:
	`Device(config-if)# ipv6 reassembly max-reassemblies 1024 timeout 1000 percentage 50 precedence critical routine`
		Enables GFR on an IPv4 or IPv6 interface, as appropriate.

Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Command or Action	Purpose

Step 6 Enter one of the following:
• **show ip reassembly interface** *type number*
• **show ipv6 reassembly interface** *type number*
 	
Example:
`Device# show ip reassembly GigabitEthernet 0/0/0`
 	
Example:
`Device# show ipv6 reassembly GigabitEthernet 0/0/0`
	Displays statistical information of the GFR configured about the interface.

Configuration Examples for GRE Fragment and Reassembly

Example: Configuring GFR

The following example shows how to configure GFR on a Gigabit Ethernet interface and specify the maximum reassembly and timeout settings:

```
interface GigabitEthernet 0/0/0
 ip address 10.10.10.1 255.255.255.0
 ipv6 address 2001:DB8:1::1
 ip reassembly max-reassemblies 1024 timeout 1 percentage 50 dscp ef
 ipv6 reassembly max-reassemblies 1024 timeout 1 percentage 50 dscp ef
 ip virtual-reassembly max-reassemblies 1024 timeout 1 percentage 10 dscp af41
 ipv6 reassembly out max-reassemblies 1024 timeout 1 percentage 50 precedence cs1
```

Additional References for GRE Fragment and Reassembly

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*

Related Topic	Document Title
Security commands	• *Cisco IOS Security Command Reference Commands A to C* • *Cisco IOS Security Command Reference Commands D to L* • *Cisco IOS Security Command Reference Commands M to R* • *Cisco IOS Security Command Reference Commands S to Z*
Virtual Fragmentation and Reassembly	*Virtual Fragmentation and Reassembly*

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 GRE Fragment and Reassembly

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 3 Feature Information for GRE Fragment and Reassembly

Feature Name	Releases	Feature Information
GRE Fragment and Reassembly Performance Tuning	Cisco IOS XE Release 3.8S	The GRE Fragment and Reassembly Performance Tuning feature enables you to customize reassembly resources. Reassembly resources are equally allocated to each interface to prevent fragment-related attack. However, in some generic routing encapsulation (GRE) tunnel deployments, fragments are reassembled in specific interfaces. This feature also allows you to adjust the reassembly timer to free up incomplete fragment sessions quickly and reserve the reassembly resources for high priority packets. The following commands were introduced or modified: **ip reassembly**, **show ip reassembly**.