Virtual Fragmentation Reassembly

Virtual fragmentation reassembly (VFR) is automatically enabled by some features (such as NAT, Cisco IOS XE Firewall, IPSec) to get Layer 4 or Layer 7 information. VFR enables the Cisco IOS XE Firewall to create appropriate dynamic access control lists (ACLs) to protect the network from various fragmentation attacks.

Most non-initial fragments do not have the Layer 4 header because it usually travels with the initial fragments (except in the case of micro-fragmentation and tiny fragments). Due to this, some features (such as NAT, Cisco IOS XE Firewall, IPSec) are unable to gather port information from the packet. These features may need to inspect the Layer 7 payload, for which the fragments need to be reassembled, and then refragmented later.

• Finding Feature Information, page 1
• Restrictions for Virtual Fragmentation Reassembly, page 2
• Information About Virtual Fragmentation Reassembly, page 2
• How to Configure Virtual Fragmentation Reassembly, page 4
• Configuration Examples for Virtual Fragmentation Reassembly, page 7
• Additional References for Virtual Fragmentation Reassembly, page 8
• Feature Information for Virtual Fragmentation Reassembly, page 8

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

The reassembly process requires all fragments within an IP datagram. If fragments within an IP datagram are sent to different devices due to load balancing (per packet load balancing or include ports on Cisco Catalyst 6500 Series Switches or Cisco Nexus devices), VFR may fail and fragments may be dropped.

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 do 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 consume 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 XE Firewall, NAT, and IPSec). By default, NAT, Cisco IOS XE Firewall, Crypto-based IPSec, NAT64, and onePK enable and disable VFR internally; that is, when these features are 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 maintains 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.

If NAT is enabled on an interface (such as GigabitEthernet 0/0/0), VFR (input/output) is enabled on this interface.

Device(config-if)# do show ip virtual-reassembly features
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [in]
  Features to use if VFR is Enabled:NAT
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [out]
  Features to use if VFR is Enabled:NAT

If Cisco IOS XE Firewall is enabled on an interface (such as GigabitEthernet 0/0/0), VFR (out) is enabled on this interface.

Device(config-if)# do show ip virtual-reassembly features
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [out]
  Features to use if VFR is Enabled:FW

If IPSec is enabled on an interface (such as GigabitEthernet 0/0/0), VFR (out) is enabled on this interface.

Device(config-if)# do show ip virtual-reassembly features
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [out]
  Features to use if VFR is Enabled:IPSec

**Note**

If VFR is enabled by features such as NAT and Cisco IOS XE Firewall, the `ip virtual-reassembly [-out]` command is not displayed in the output of the `show running-config` command.

VFR can be manually enabled or disabled using the `[no] ip virtual-reassembly [-out]` command.

If VFR is manually enabled, regardless of whether it is enabled by features such as NAT and Cisco IOS XE Firewall, the `ip virtual-reassembly [-out]` command is displayed in the output of the `show running-config` command.

**VFR Disablement**

You can disable virtual fragmentation reassembly (VFR) using the following methods:
• If VFR is manually enabled, it can be manually disabled using the **no ip virtual-reassembly [-out]** command. This command is not displayed in the output of the **show running-config** command.

• If VFR is enabled by a feature (such as NAT or Cisco IOS Firewall), it can be manually disabled or it can be disabled by disabling the feature. If it is manually disabled, the **no ip virtual-reassembly [-out]** command is displayed in the output of the **show running-config** command.

• If VFR is both manually enabled and enabled by features, it can be manually disabled using the **no ip virtual-reassembly [-out]** command. This command is displayed in the output of the **show running-config** command.

---

**Note**

If VFR is not enabled, the **no ip virtual-reassembly [-out]** command is not displayed in the output of the **show running-config** command.

To enable VFR after it is disabled, that is, when the **no ip virtual-reassembly [-out]** command is displayed in the output of the **show running-config** command, manually enable VFR using the **ip virtual-reassembly [-out]** command or disable related features and then enable the features again.

In a crypto map-based IPSec deployment scenario (such as GETVPN), VFR is enabled by default in devices which are configured with IPSec. Fragments of the same packet may be sent to different devices (which are IPSec-enabled) by upper devices due to the packet load balance algorithm (per packet load balance or per destination on some Nexus devices). VFR may drop the fragments if it does not receive all fragment of the same IP packet. The recommended workaround of this issue is to change the load balance algorithm to ensure all fragments of the same packet go to the same path. If Layer 4 information (ports) is not a filter criterion in IPSec policy, another workaround is to manually disable VFR using **no ip virtual-reassembly [-out]** on interfaces where IPSec is configured.

---

**VFR on Outbound Interfaces**

In Cisco IOS XE Release 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 to specify maximum threshold values to combat buffer overflow and control memory usage, and to verify any VFR configurations.
SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-type interface-number</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface GigabitEthernet0/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]</td>
<td>Enables VFR on the interface and specifies the maximum threshold values.</td>
</tr>
<tr>
<td>Example: Device(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
### 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. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2.</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]</code></td>
<td></td>
</tr>
</tbody>
</table>
### Virtual Fragmentation Reassembly

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface type number</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Device(config)# interface GigabitEthernet0/0/1</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 4**        | **ip virtual-reassembly** |
|                   | [max-reassemblies number] |
|                   | [max-fragments number] |
|                   | [drop-fragments] |
| Example:          | Enables VFR on the interface and specifies the maximum threshold values. |
| Device(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5 |

| **Step 5**        | **end** |
| Example:          | Exits interface configuration mode. |
| Device(config-if)# end |

### Troubleshooting Tips

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

### Configuration Examples for Virtual 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:

```plaintext
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 for Virtual Fragmentation Reassembly**

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Dynamic IDS</td>
<td>Cisco IOS Intrusion Prevention System</td>
</tr>
<tr>
<td>CBAC</td>
<td>“Configuring Context-Based Access Control” chapter</td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 791</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>RFC 1858</td>
<td>Security Considerations for IP Fragment Filtering</td>
</tr>
</tbody>
</table>

### Technical Assistance

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

**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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Virtual Fragmentation 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`. |