Virtual Fragmentation Reassembly

Currently, 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 access control list (ACL) creation.

Virtual fragmentation reassembly (VFR) enables the Cisco IOS Firewall to create the appropriate dynamic ACLs, thereby, protecting the network from various fragmentation attacks.

Feature History for Virtual Fragmentation Reassembly

Release	Modification
12.3(8)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for Virtual Fragmentation Reassembly

Performance Impact

VFR will cause a performance impact on the basis of functions such as packet copying, fragment validation, and fragment reorder. This performance impact will vary depending on the number of concurrent IP datagram 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.

SIP and RTSP Limitation

The Session Initiation Protocol (SIP) and the Real-Time Streaming Protocol (RTSP) do not have the ability to parse port information across noncontiguous buffers. Thus, virtual fragmentation reassembly may fail. (If the application fails, the session will be blocked.)

Information About Virtual Fragmentation Reassembly

To use fragmentation support for Cisco IOS Firewall, you should understand the following concept:

- Detected Fragment Attacks, page 2
- Automatically Enabling or Disabling VFR, page 3

Detected 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 User Datagram Protocol (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 follows is logged to the syslog server: “VFR-3-TINY_FRAGMENTS.”

- 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 your system to crash.

  VFR drops all fragments within a fragment chain if an overlap fragment is detected, and an alert message such as follows is logged to the syslog server: “VFR-3-OVERLAP_FRAGMENT.”

- 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 usage, configure a maximum threshold for the number of IP datagrams that are being reassembled and the number of fragments per datagram. (Both of these parameters can be specified via the **ip virtual-reassembly** command.)

When the maximum number of datagrams that can be reassembled at any given time is reached, all subsequent fragments are dropped, and an alert message such as the following is logged to the syslog server: "VFR-4_FRAG_TABLE_OVERFLOW."

When the maximum number of fragments per datagram is reached, subsequent fragments will be dropped, and an alert message such as the following is logged to the syslog server: "VFR-4_TOO_MANY_FRAGMENTS."

In addition to configuring the maximum threshold values, 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 will expire and the IP datagram (and all of its fragments) will be dropped.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, 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.

How to Use Virtual Fragmentation Reassembly

This section contains the following procedures:

- Configuring VFR, page 3

Configuring VFR

Use 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** *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.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet1/1`	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 an interface.
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 ethernet1/1`	Displays the configuration and statistical information of the VFR. If an interface is not specified, VFR information is shown for all configured interfaces.

Troubleshooting Tips

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

Configuration Examples for Fragmentation Reassembly

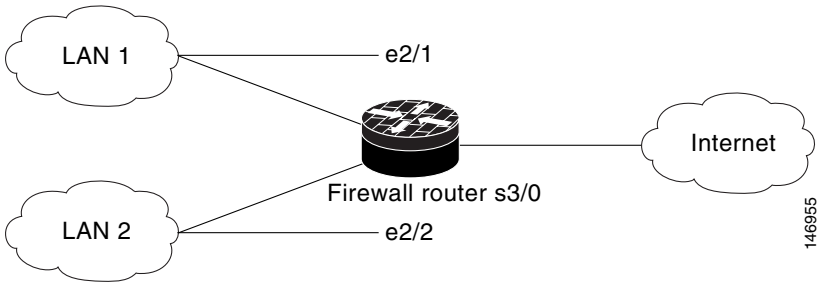
This section contains the following configuration example:

• Configuring VFR and a Cisco IOS Firewall: Example, page 5

Configuring VFR and a Cisco IOS Firewall: Example

The following example shows a typical scenario where the Virtual Fragment Reassembly module is enabled on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

Figure 1 VFR and Cisco IOS Firewall Sample Topology




```
!
ip inspect name INTERNET-FW ftp
ip inspect name INTERNET-FW http
ip inspect name INTERNET-FW smtp
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet2/0
 ip address 9.4.21.9 255.255.0.0
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 description LAN1
 ip address 14.0.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/2
 description LAN2
 ip address 15.0.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 description Internet
 ip unnumbered Loopback0
 encapsulation ppp
 ip access-group 102 in
 ip inspect INTERNET-FW out
 ip virtual-reassembly
```

```
 serial restart-delay 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 s3/0
!
!
! Access Control Rule that drops all internet originated traffic.
!
access-list 102 deny   ip any any
!
!
!
!
control-plane
!
no call rsvp-sync
!
!
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
!
end
```

Additional References

The following sections provide references related to virtual fragmentation reassembly.

Related Documents

Related Topic	Document Title
Dynamic IDS	*Cisco IOS Intrusion Prevention System*
CBAC	*Configuring Context-Based Access Control*

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS 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
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List*.

- **debug ip virtual-reassembly**
- **ip virtual-reassembly**
- **show ip virtual-reassembly**

Glossary

fragment—Part of an IP datagram that is fragmented into multiple pieces. Each piece is called a fragment or an IP fragment.

fragmentation—Process of breaking down an IP datagram into smaller packets (fragments) that are transmitted over different types of network media.

initial fragment— First fragment within a fragment set. This fragment should have a Layer 4 header and should have an offset of zero.

noninitial fragment—All fragments within a fragment set, except the initial fragment.