DF Bit Override Functionality with IPsec Tunnels

The DF Bit Override Functionality with IPsec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPsec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

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.

Prerequisites for DF Bit Override Functionality with IPsec Tunnels

IPsec must be enabled on your router.

Restrictions for DF Bit Override Functionality with IPsec Tunnels

Performance Impact

Because each packet is reassembled at the process level, a significant performance impact occurs at a high data rate. Two major caveats are as follows:

- The reassemble queue can fill up and force fragments to be dropped.
- The traffic is slower because of the process switching.

DF Bit Setting Requirement

If several interfaces share the same crypto map using the local address feature, these interfaces must share the same DF bit setting.

Feature Availability

This feature is available only for IPsec tunnel mode. (IPsec transport mode is not affected because it does not provide an encapsulating IP header.)

Information About DF Bit Override Functionality with IPsec Tunnels

The DF Bit Override Functionality with IPsec Tunnels feature allows customers to specify whether their router can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether a router is allowed to fragment a packet.

Some customer configurations have hosts that perform the following functions:

- Set the DF bit in packets they send
- Use firewalls that block Internet Control Message Protocol (ICMP) errors from outside the firewall, preventing hosts from learning about the maximum transmission unit (MTU) size outside the firewall
- Use IP Security (IPsec) to encapsulate packets, reducing the available MTU size

Customers whose configurations have hosts that prevent them from learning about their available MTU size can configure their router to clear the DF bit and fragment the packet.

Note In compliance with RFC 2401, this feature can be configured globally or per interface. If both levels are configured, the interface configuration will override the global configuration.

How to Configure DF Bit Override Functionality with IPsec Tunnels

Configuring the DF Bit for the Encapsulating Header in Tunnel Mode

The following task sets the DF bit for the encapsulating header in tunnel mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec df-bit** [**clear** | **set** | **copy**]
4. **interface** *type number*
5. **crypto ipsec df-bit** [**clear** | **set** | **copy**]
6. **exit**
7. **show running-config**

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	**crypto ipsec df-bit** [**clear** | **set** | **copy**] **Example:** `Router(config)# crypto ipsec df-bit set`	Sets the DF bit for the encapsulating header in tunnel mode for all interfaces. • The **clear** keyword clears the DF bit in the outer IP header, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.

	Command or Action	Purpose
		• The **set** keyword sets the DF bit in the outer IP header, however, the router may fragment the packet if the original packet had the DF bit cleared. • The **copy** keyword has the router look in the original packet for the outer DF bit setting. The copy keyword is the default setting.
Step 4	**interface** *type number* **Example:** `Router(config-if)# interface Ethernet0/0`	Specifies the interface on which the DF bit is configured and enters interface configuration mode.
Step 5	**crypto ipsec df-bit** [**clear** | **set** | **copy**] **Example:** `Router(config-if)# crypto ipsec df-bit clear`	(Optional) Sets the DF bit for a specified interface, **Note** DF bit interface configuration settings override all DF bit global configuration settings.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode and enters EXEC mode.
Step 7	**show running-config** **Example:** `Router# show running-config`	Verifies the current DF Bit settings on your router.

Configuration Example for DF Bit Override Functionality with IPsec Tunnels

DF Bit Setting Configuration Example

In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces except Ethernet0 will allow the router to send packets larger than the available MTU size; Ethernet0 will allow the router to fragment the packet.

```
crypto isakmp policy 1
  encryption aes
  hash sha
  authentication pre-share
  group 14
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
```

```
!
!
crypto ipsec transform-set BearMama ah-sha-hmac esp-aes
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102
!
!
interface Ethernet0
   ip address 192.168.10.38 255.255.255.0
   ip broadcast-address 0.0.0.0
   media-type 10BaseT
   crypto map armadillo
   crypto ipsec df-bit copy
!
interface Ethernet1
   ip address 192.168.11.75 255.255.255.0
   ip broadcast-address 0.0.0.0
   media-type 10BaseT
   crypto map basilisk
!
interface Serial0
   no ip address
   ip broadcast-address 0.0.0.0
   no ip route-cache
   no ip mroute-cache
```

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
Recommended cryptographic algorithms	Next Generation Encryption

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

RFC	Title
RFC 2401	Security Architecture for the Internet Protocol

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 DF Bit Override Functionality with IPsec Tunnels

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 DF Bit Override Functionality with IPsec Tunnels

Feature Name	Releases	Feature Information
DF Bit Override Functionality with IPSec Tunnels	12.2(11)T	The DF Bit Override Functionality with IPsec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPsec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting. This feature was introduced in Cisco IOS Release 12.2(11)T. The following commands were introduced or modified: **crypto ipsec df-bit (global configuration), crypto ipsec df-bit (interface configuration) .**