IPsec and IKE MIB Support forCisco VRF-Aware IPsec

The IPsec and IKE MIB Support for the Virtual Private Network routing and forwarding- (VRF-) aware IP security (IPsec) feature allows VRF-aware IPsec to be managed with MIBs, which provide the details of IPsec statistics and performance metrics on a per VRF basis.

Prerequisites for IPsec and IKE MIB Support forCisco VRF-Aware IPsec

- You should be familiar with configuring Simple Network Management Protocol (SNMP).

Information About IPsec and IKE MIB Support forCisco VRF-Aware IPsec

MIBs Supported by the IPsec and IKE MIB Support forCisco VRF-Aware IPsec Feature

- CISCO-IPSEC-FLOW-MONITOR-MIB supports IKE and IPSEC per-tunnel history and failure information. The length of this history and failure information can be configured and must be maintained on a per-VRF basis. The table sizes are controlled by using the **crypto mib ipsec flowmib history tunnel size number** and **crypto mib ipsec flowmib history failure size** commands in global configuration mode.

- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB is supported. However, because this MIB applies to the entire router rather than to a specific VPN VRF instance, it is not VRF aware; therefore, polling of the object identifiers (OIDs) that belong to this MIB is accomplished with respect to the global VRF context.

SNMP Traps Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

The following IKE and IPsec tunnel start and stop traps must go with their corresponding VRF:

- IPSEC_TUNNEL_STOP
- IKE_TUNNEL_STOP
- IPSEC_TUNNEL_START
- IKE_TUNNEL_START

The following traps are global traps that have been modified for the Cisco VRF-Aware IPsec feature:

- TOO_MANY_SAS_CREATED
- CRYPTOMAP_ADDED
- CRYPTOMAPSET_ATTACHED
- CRYPTOMAP_DELETED
- CRYPTOMAPSET_DELETED
- ISAKMP_POLICY_ADDED
- ISAKMP_POLICY_DELETED

How to Configure IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

No special configuration is needed for this feature. The SNMP framework can be used to manage VRF-aware IPsec using MIBs. See the Configuration Examples for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec section for more information.

The following section provides information about troubleshooting this feature:

How to Troubleshoot the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

The following **debug crypto mib** command and keywords may be used to display information about the IPsec and Internet Key Exchange (IKE) MIB as it relates to Cisco VRF-aware IPsec.

SUMMARY STEPS

1. **enable**
2. **debug crypto mib detail**
3. **debug crypto mib error**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto mib detail** **Example:** `Router# debug crypto mib detail`	Displays different events as they occur in the IPsec MIB subsystem. • Due consideration should be given to enabling **debug crypto mib detail**because the output for the **detail** keyword can be quite long.
Step 3	**debug crypto mib error** **Example:** `Router# debug crypto mib error`	Displays error events in the MIB agent.

Configuration Example for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

Configuration That Has Two VRFs Examples

The following output example is for a typical hub configuration that has two VRFs. The output is what you would see if you were to poll for the IPsec security association (SA). Router 3745b is the VRF-aware router.

Two VRFs Configured

The following output shows that two VRFs have been configured (vrf1 and vrf2).

```
Router3745b# show running-config
Building configuration...
Current configuration : 6567 bytes
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log uptime
```

```
no service password-encryption
!
hostname ipsecf-3745b
!
boot-start-marker
boot-end-marker
!
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
!
!
ip vrf vrf1
 rd 1:101
 context vrf-vrf1-context
 route-target export 1:101
 route-target import 1:101
!
ip vrf vrf2
 rd 2:101
 context vrf-vrf2-context
 route-target export 2:101
 route-target import 2:101
!
no ip domain lookup
!
!
crypto keyring vrf1-1 vrf vrf1
  pre-shared-key address 10.1.1.1 255.255.255.0 key vrf1-1
crypto keyring vrf2-1 vrf vrf2
  pre-shared-key address 10.1.2.1 255.255.255.0 key vrf2-1
!
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp policy 50
 authentication pre-share
crypto isakmp key global1-1 address 10.1.151.1
crypto isakmp key global2-1 address 10.1.152.1
crypto isakmp profile vrf1-1
   keyring vrf1-1
   match identity address 10.1.1.1 255.255.255.255 vrf1
crypto isakmp profile vrf2-1
   keyring vrf2-1
   match identity address 10.1.2.1 255.255.255.255 vrf2
!
crypto ipsec security-association lifetime kilobytes 99000
crypto ipsec security-association lifetime seconds 5000
!
crypto ipsec transform-set tset ah-sha-hmac esp-des esp-sha-hmac
!
crypto map global1-1 10 ipsec-isakmp
 set peer 10.1.151.1
 set transform-set tset
```

```
 match address 151
!
crypto map global2-1 10 ipsec-isakmp
 set peer 10.1.152.1
 set transform-set tset
 match address 152
!
crypto map vrf1-1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set tset
 set isakmp-profile vrf1-1
 match address 101
!
crypto map vrf2-1 10 ipsec-isakmp
 set peer 10.1.2.1
 set transform-set tset
 set isakmp-profile vrf2-1
 match address 102
!
!
interface FastEthernet0/0
 ip address 10.1.38.25 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 clock rate 128000
 no frame-relay inverse-arp
!
interface Serial1/0.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.3.1.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 21
!
interface Serial1/0.2 point-to-point
 ip vrf forwarding vrf2
 ip address 10.3.2.1 255.255.255.0
 no ip route-cache
```

```
 frame-relay interface-dlci 22
!
interface Serial1/0.151 point-to-point
 ip address 10.7.151.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 151
!
interface Serial1/0.152 point-to-point
 ip address 10.7.152.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 152
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 no frame-relay inverse-arp
!
interface Serial1/2.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.1.1.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 21
 crypto map vrf1-1
!
interface Serial1/2.2 point-to-point
 ip vrf forwarding vrf2
 ip address 10.1.2.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 22
 crypto map vrf2-1
!
interface Serial1/2.151 point-to-point
 ip address 10.5.151.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 151
 crypto map global1-1
!
interface Serial1/2.152 point-to-point
 ip address 10.5.152.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 152
 crypto map global2-1
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
ip default-gateway 10.1.38.1
ip classless
ip route 10.1.1.6 255.255.255.255 10.1.151.1
ip route 10.2.1.6 255.255.255.255 10.1.152.1
```

```
ip route 10.6.2.1 255.255.255.255 10.7.151.2
ip route 10.6.2.2 255.255.255.255 10.7.152.2
ip route 172.19.216.110 255.255.255.255 FastEthernet0/0
ip route vrf vrf1 10.20.1.1 255.255.255.255 10.1.1.1
ip route vrf vrf1 10.22.1.1 255.255.255.255 10.30.1.1
ip route vrf vrf2 10.20.2.1 255.255.255.255 10.1.2.1
ip route vrf vrf2 10.22.2.1 255.255.255.255 10.30.1.2
!
!
ip http server
no ip http secure-server
!
ip access-list standard vrf-vrf1-context
ip access-list standard vrf-vrf2-context
!
access-list 101 permit ip host 10.22.1.1 host 10.20.1.1
access-list 102 permit ip host 10.22.2.1 host 10.20.2.1
access-list 151 permit ip host 10.6.2.1 host 10.1.1.6
access-list 152 permit ip host 10.6.2.2 host 10.2.1.6
snmp-server group abc1 v2c context vrf-vrf1-context read view_vrf1 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf1-context
snmp-server group abc2 v2c context vrf-vrf2-context read view_vrf2 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf2-context
snmp-server view view_vrf1 iso included
snmp-server view view_vrf2 iso included
snmp-server community abc1 RW
snmp-server community global1 RW
snmp-server community abc2 RW
snmp-server community global2 RW
snmp-server enable traps tty
snmp-server enable traps config
snmp-server host 172.19.216.110 version 2c abc1
snmp-server host 172.19.216.110 vrf vrf1 version 2c abc1 udp-port 2001  ipsec isakmp
snmp-server host 172.19.216.110 version 2c abc2
snmp-server host 172.19.216.110 vrf vrf2 version 2c abc2 udp-port 2002  ipsec isakmp
snmp-server context vrf-vrf1-context
snmp-server context vrf-vrf2-context
!
!
snmp mib community-map  abc1 context vrf-vrf1-context
snmp mib community-map  abc2 context vrf-vrf2-context
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

Both VRFs Cleared

The following output, for abc1 and abc2, shows that both VRFs have been “cleared” to ensure that all the counters are initialized to a known value.

The following output shows that VRF abc1 has been cleared:

```
orcas:2> setenv SR_MGR_CONF /users/green1
orcas:3> setenv SR_UTIL_SNMP_VERSION v2c
orcas:5> setenv SR_UTIL_COMMUNITY abc1
orcas:6> setenv SR_MGR_CONF_DIR /users/green1
orcas:7> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
```

```
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
```

The following output shows that VRF abc2 has been cleared:

```
orcas:8> setenv SR_UTIL_COMMUNITY abc2
orcas:9> /auto/sw/packages/snmpr/14.2.0.0/solaris2bin/getmany -v2c 10.1.38.25 cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
```

```
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:10>
orcas:10>
orcas:10>
```

VRF abc1 Pinged

The following output shows that VRF abc1 has been pinged:

```
Router3745a# ping
Protocol [ip]:
Target IP address: 10.22.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.20.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.1.1
```

VRF abc1 Polled

Polling VRF abc1 results in the following output:

Note After the ping, the counters should show some nonzero values.

```
orcas:10>
orcas:12> setenv SR_UTIL_COMMUNITY abc1
orcas:13> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 1
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 336
cikeGlobalInPkts.0 = 2
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 1
cikeGlobalInP2Exchgs.0 = 2
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 344
cikeGlobalOutPkts.0 = 2
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 1
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cikePeerLocalAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 0a 01  01 02
cikePeerRemoteAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 0a 01  01 01
cikePeerActiveTime.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 13743
cikePeerActiveTunnelIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 1
cikeTunLocalType.1 = ipAddrPeer(1)
cikeTunLocalValue.1 = 010.001.001.002
cikeTunLocalAddr.1 = 0a 01  01 02
cikeTunLocalName.1 = ipsecf-3745b
cikeTunRemoteType.1 = ipAddrPeer(1)
cikeTunRemoteValue.1 = 010.001.001.001
cikeTunRemoteAddr.1 = 0a 01  01 01
cikeTunRemoteName.1 =
cikeTunNegoMode.1 = main(1)
cikeTunDiffHellmanGrp.1 = dhGroup1(2)
cikeTunEncryptAlgo.1 = des(2)
cikeTunHashAlgo.1 = sha(3)
cikeTunAuthMethod.1 = preSharedKey(2)
cikeTunLifeTime.1 = 86400
cikeTunActiveTime.1 = 13752
```

```
cikeTunSaRefreshThreshold.1 = 0
cikeTunTotalRefreshes.1 = 0
cikeTunInOctets.1 = 336
cikeTunInPkts.1 = 2
cikeTunInDropPkts.1 = 0
cikeTunInNotifys.1 = 1
cikeTunInP2Exchgs.1 = 2
cikeTunInP2ExchgInvalids.1 = 0
cikeTunInP2ExchgRejects.1 = 0
cikeTunInP2SaDelRequests.1 = 0
cikeTunOutOctets.1 = 344
cikeTunOutPkts.1 = 2
cikeTunOutDropPkts.1 = 0
cikeTunOutNotifys.1 = 0
cikeTunOutP2Exchgs.1 = 1
cikeTunOutP2ExchgInvalids.1 = 0
cikeTunOutP2ExchgRejects.1 = 0
cikeTunOutP2SaDelRequests.1 = 0
cikeTunStatus.1 = active(1)
cikePeerCorrIpSecTunIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1.1
 = 1
cipSecGlobalActiveTunnels.0 = 1
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 400
cipSecGlobalHcInOctets.0 = 0x0190
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 400
cipSecGlobalHcInDecompOctets.0 = 0x0190
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 4
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 4
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 4
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 704
cipSecGlobalHcOutOctets.0 = 0x02c0
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 704
cipSecGlobalHcOutUncompOctets.0 = 0x02c0
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 4
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 4
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 4
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecTunIkeTunnelIndex.1 = 1
cipSecTunIkeTunnelAlive.1 = true(1)
cipSecTunLocalAddr.1 = 0a 01  01 02
cipSecTunRemoteAddr.1 = 0a 01  01 01
cipSecTunKeyType.1 = ike(1)
cipSecTunEncapMode.1 = tunnel(1)
cipSecTunLifeSize.1 = 99000
cipSecTunLifeTime.1 = 5000
cipSecTunActiveTime.1 = 13749
cipSecTunSaLifeSizeThreshold.1 = 64
cipSecTunSaLifeTimeThreshold.1 = 10
cipSecTunTotalRefreshes.1 = 0
cipSecTunExpiredSaInstances.1 = 0
```

```
cipSecTunCurrentSaInstances.1 = 4
cipSecTunInSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunInSaEncryptAlgo.1 = des(2)
cipSecTunInSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunInSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunInSaDecompAlgo.1 = none(1)
cipSecTunOutSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunOutSaEncryptAlgo.1 = des(2)
cipSecTunOutSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaCompAlgo.1 = none(1)
cipSecTunInOctets.1 = 400
cipSecTunHcInOctets.1 = 0x0190
cipSecTunInOctWraps.1 = 0
cipSecTunInDecompOctets.1 = 400
cipSecTunHcInDecompOctets.1 = 0x0190
cipSecTunInDecompOctWraps.1 = 0
cipSecTunInPkts.1 = 4
cipSecTunInDropPkts.1 = 0
cipSecTunInReplayDropPkts.1 = 0
cipSecTunInAuths.1 = 4
cipSecTunInAuthFails.1 = 0
cipSecTunInDecrypts.1 = 4
cipSecTunInDecryptFails.1 = 0
cipSecTunOutOctets.1 = 704
cipSecTunHcOutOctets.1 = 0x02c0
cipSecTunOutOctWraps.1 = 0
cipSecTunOutUncompOctets.1 = 704
cipSecTunHcOutUncompOctets.1 = 0x02c0
cipSecTunOutUncompOctWraps.1 = 0
cipSecTunOutPkts.1 = 4
cipSecTunOutDropPkts.1 = 0
cipSecTunOutAuths.1 = 4
cipSecTunOutAuthFails.1 = 0
cipSecTunOutEncrypts.1 = 4
cipSecTunOutEncryptFails.1 = 0
cipSecTunStatus.1 = active(1)
cipSecEndPtLocalName.1.1 =
cipSecEndPtLocalType.1.1 = singleIpAddr(1)
cipSecEndPtLocalAddr1.1.1 = 16 01  01 01
cipSecEndPtLocalAddr2.1.1 = 16 01  01 01
cipSecEndPtLocalProtocol.1.1 = 0
cipSecEndPtLocalPort.1.1 = 0
cipSecEndPtRemoteName.1.1 =
cipSecEndPtRemoteType.1.1 = singleIpAddr(1)
cipSecEndPtRemoteAddr1.1.1 = 14 01  01 01
cipSecEndPtRemoteAddr2.1.1 = 14 01  01 01
cipSecEndPtRemoteProtocol.1.1 = 0
cipSecEndPtRemotePort.1.1 = 0
cipSecSpiDirection.1.1 = in(1)
cipSecSpiDirection.1.2 = out(2)
cipSecSpiDirection.1.3 = in(1)
cipSecSpiDirection.1.4 = out(2)
cipSecSpiValue.1.1 = 3891970674
cipSecSpiValue.1.2 = 1963217493
cipSecSpiValue.1.3 = 3691920464
cipSecSpiValue.1.4 = 3458912974
cipSecSpiProtocol.1.1 = ah(1)
cipSecSpiProtocol.1.2 = ah(1)
cipSecSpiProtocol.1.3 = esp(2)
cipSecSpiProtocol.1.4 = esp(2)
cipSecSpiStatus.1.1 = active(1)
cipSecSpiStatus.1.2 = active(1)
cipSecSpiStatus.1.3 = active(1)
```

```
cipSecSpiStatus.1.4 = active(1)
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:14>
orcas:14>
orcas:14>
```

VRF abc2 Polled

Polling VRF abc2 results in the following output:

Note The ping was completed for VRF abc1 only. Therefore, the counters of VRF abc2 should remain in the initialized state.

```
setenv SR_UTIL_COMMUNITY abc2
orcas:15>
orcas:15> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
```

```
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:16>
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands by technology	Cisco IOS Release Command References
Cisco IOS master commands list	Master Command List

Related Topic	Document Title
Configuring SNMP	The chapter "Configuring SNMP Support"in the *Cisco IOS Network Management Configuration Guide*.
Configuring VRF-Aware IPsec	VRF-Aware IPSec

Standards

Standard	Title
None.	--

MIBs

MIB	MIBs Link
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • The CISCO-IPSEC-POLICY-MAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None.	--

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/cisco/web/support/index.html

Feature Information for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

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 Feature Information for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

Feature Name	Releases	Feature Information
IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	IOS XE 3.1S	The IPsec and IKE MIB Support for the Virtual Private Network routing and forwarding- (VRF-) aware IP security (IPsec) feature allows VRF-aware IPsec to be managed with MIBs, which provide the details of IPsec statistics and performance metrics on a per VRF basis. This feature was introduced in Cisco IOS Release 12.4(4)T. This feature was integrated into Cisco IOS Release XE 3.1S. The following commands were introduced or modified: **debug crypto mib**.