

show crypto

This chapter includes the **show crypto** command output tables.

- show crypto group summary, on page 1
- show crypto ikev2-ikesa security-associations summary, on page 2
- show crypto ikev2-ikesa security-associations summary spi, on page 2
- show crypto ipsec security-associations, on page 3
- show crypto ipsec security-associations statistics, on page 6
- show crypto ipsec security-associations summary, on page 9
- show crypto isakmp keys, on page 9
- show crypto isakmp security-associations, on page 10
- show crypto managers, on page 10
- show crypto managers instance, on page 11
- show crypto managers summary, on page 12
- show crypto map summary, on page 12
- show crypto statistics, on page 15
- show crypto statistics ikev2, on page 21
- show crypto template summary, on page 30

show crypto group summary

Table 1: show crypto group summary Command Output Descriptions

Field	Description
Crypto Group	Name of the crypto group
Primary Tunnel	Configuration information for the primary tunnel.
Secondary Tunnel	Configuration information for the secondary tunnel.

show crypto ikev2-ikesa security-associations summary

Table 2: show crypto ikev2-ikesa security-associations summary Command Output Descriptions

Field	Description
Mgr ID	SA Manager ID number
VPN	SA VPN number
Local IPsec GW	Local default gateway IP address
Port	UDP port number
Remote IPSec GW	Remote default gateway IP address
Port	UDP port number
Hostname	Name of the remote gateway
State	Authentication state • I = Initiator • R = Responder
Lifetime/Remaining	Originally configured lifetime for the SA in seconds/number of seconds left in this lifetime.

show crypto ikev2-ikesa security-associations summary spi

Table 3: show crypto ikev2-ikesa security-associations summary spi Command Output Descriptions

Field	Description
Local IPsec GW	Local default gateway IP address
Remote IPSec GW	Remote default gateway IP address
Initiator SPI	SPI (Security Parameter Index) of the Initiator
Responder SPI	SPI of the Responder
Lifetime	Originally configured lifetime for the SA in seconds/number of seconds left in this lifetime.

show crypto ipsec security-associations

Field	Description
Map Name	The name of the crypto map facilitating the security association.
Local Address	The IP address of the interface on the security gateway facilitating the security association.
Current Peer	The IP address of the interface on the peer gateway facilitating the security association.
Peer Hostname	The name of the peer.
Crypto Type	The type of crypto map facilitating the security association, which can be: • Dynamic Map • IKEv1 Map • IKEv2 Map • Manual Map
SA State	The state of the security association, which can be: • Established • Partially Established • No SAs
IPSec Manager	The identifying number of the IPsec manager facilitating the security association.
Rekeying	The state of rekeying for the security association, which can be: • Enabled • Disabled
Redundancy Status	The state of the security association, which can be: • Original Tunnel: No failure has occurred. • Recovered Session: A failure has occurred and a recovered session has been created.
Allocated Address	The IP address allocated to the Network Access Identifiers (NAIs) of the users.
Phase 1	The NAI used in Phase 1 authentication.
Phase 2	The NAI used in Phase 2 authentication.
Encoded	The number of packets and bytes of data that have been encoded for the security association.
Encoded Errors	The number of errors that occurred while the packets were being encoded.

Field	Description
Decoded	The number of packets and bytes of data that have been decoded for the security association.
Decoded Errors	The number of errors that occurred while the packets were being decoded.
Authentication Errors	The number of errors that occurred during authentication.
Replay Errors	The number of replay errors that occurred.
Too short Errors	The number of too short errors that occurred.
IPSec SA	
Diffie-Hellman Group	The number of the Diffie-Hellman group to which the security association belongs.
Outbound esp sas	
spi	The Security Parameter Index (SPI) of the outbound ESP security association.
transform	
hmac	The keyed-Hash Message Authentication Code used for the outbound ESP security association, which can be: • sha1-96 • md5-96
cipher	The cipher used for the outbound ESP security association, which can be: • null • des • 3des • aes-cbc-128 • aes-cbc-256
negotiated soft lifetime (kb/sec)	The soft lifetime in kilobits and/or seconds for the outbound ESP security association, created when a successful rekey has occurred. The soft lifetime is used to warn that the security association is about to expire, allowing the security gateway to create a new lifetime prior to the expiration of the hard lifetime.
remaining soft lifetime (kb/sec)	The remaining soft lifetime in kilobits and/or seconds.
negotiated hard lifetime (kb/sec)	The hard lifetime in kilobits and/or seconds for the outbound ESP security association. The hard lifetime is the number of kilobits and/or seconds used before the security association expires.
remaining hard lifetime (kb/sec)	The remaining hard lifetime in kilobits and/or seconds.
Encoded	The number of encoded packets and bytes of data for the outbound ESP security association.

Field	Description
Encoded Errors	The number of errors that occurred while the packets were being encoded.
Inbound esp sas	
spi	The Security Parameter Index (SPI) of the inbound ESP security association.
transform	
hmac	The keyed-Hash Message Authentication Code used for the inbound ESP security association, which can be: • sha1-96 • md5-96
cipher	The cipher used for the inbound ESP security association, which can be: • null • des • 3des • aes-cbc-128 • aes-cbc-256
negotiated soft lifetime (kb/sec)	The soft lifetime in kilobits and/or seconds for the inbound ESP security association, created when a successful rekey has occurred. The soft lifetime is used to warn that the security association is about to expire, allowing the security gateway to create a new lifetime prior to the expiration of the hard lifetime.
remaining soft lifetime (kb/sec)	The remaining soft lifetime in kilobits and/or seconds.
negotiated hard lifetime (kb/sec)	The hard lifetime in kilobits and/or seconds for the inbound ESP security association. The hard lifetime is the number of kilobits and/or seconds used before the security association expires.
remaining hard lifetime (kb/sec)	The remaining hard lifetime in kilobits and/or seconds.
Decoded	The number of packets and bytes of data that have been decoded for the inbound ESP security association.
Decoded Errors	The number of errors that occurred while the packets were being decoded.
Authentication Errors	The number of errors that occurred during authentication.
Replay Errors	The number of replay errors that occurred.
Too short Errors	The number of too short errors that occurred.

show crypto ipsec security-associations statistics

Table 4: show crypto ipsec security-associations statistics Command Output Descriptions

Field	Description
Map Name	The name of the crypto map for which statistics are being displayed.
Application Map Name	The application map name that concatenates the following: • **Application Supported:** MIP or L2TP • **Local Address:** The IP address of the interface on the system facilitating the security association (SA). • **Peer Address:** The IP address of the peer security gateway facilitating the SA. • **Traffic Type:** Control, GRE encapsulated data, or IPIP (IP-in-IP) encapsulated data **NOTE:** When a crypto map does not have any IPSec SAs established yet, i.e. No IKE negotiation has taken place OR the tunnel had been brought down after inactivity during the entire lifetime of the SAs, is marked as "Security Association is not established!"
local addr	The IP address of the interface on the system facilitating the security association (SA).
ACL	For ISAKMP or manual crypto maps, this is the name of the access control list (ACL) that is matched to the crypto map.
current peer	The IP address of the peer security gateway facilitating the SA.
Tunnel is keyed 1 times.	The number of times the tunnel was keyed. In this example, the tunnel was keyed once.
Encoded	The number of packets and bytes that have been encoded for the SA.
Encode Errors	The number of errors that have occurred while encoding packets.
Decoded	The number of packets and bytes that have been decoded for the SA.
Decode Errors	The number of errors that have occurred while decoding packets.
Authentication Errors	The number of errors that occurred during the system/security gateway authentication process.
Replay Errors	The number of replay errors that occurred for the SA.
outbound esp sas	
spi	The outbound (from the system to the security gateway) security parameter index (SPI) used for the Encapsulating Security Payload protocol.
transform	The protocols configured for the transform set used by the crypto map for outbound tunnels.

Field	Description
negotiated soft lifetime (kb/sec)	The soft lifetime negotiated by the system and the security gateway for outbound SAs. The lifetime is measured in terms kilobytes (kb) and/or seconds (sec). The soft lifetime is used to warn that the SA is about to expire allowing the systems to negotiate a new lifetime prior to the expiration of the hard lifetime.
remaining soft lifetime (kb/sec)	The amount of kilobytes and/or seconds remaining to the soft lifetime from what was initially negotiated.
negotiated hard lifetime (kb/sec)	The hard lifetime negotiated by the system and the security gateway for outbound SAs. The lifetime is measured in terms kilobytes (kb) and/or seconds (sec). The hard lifetime that dictates the maximum duration for the SA before its termination.
remaining hard lifetime (kb/sec)	The amount of kilobytes and/or seconds remaining to the hard lifetime from what was initially negotiated.
Encoded	The number of packets and bytes that have been encoded for the SA.
Encode Errors	The number of errors that have occurred while encoding packets.
inbound esp sas	
spi	The inbound (from the system to the security gateway) security parameter index (SPI) used for the Encapsulating Security Payload protocol.
transform	The protocols configured for the transform set used by the crypto map for inbound tunnels.
negotiated soft lifetime (kb/sec)	The soft lifetime negotiated by the system and the security gateway for inbound SAs. The lifetime is measured in terms kilobytes (kb) and/or seconds (sec). The soft lifetime is used to warn that the SA is about to expire allowing the systems to negotiate a new lifetime prior to the expiration of the hard lifetime.
remaining soft lifetime (kb/sec)	The amount of kilobytes and/or seconds remaining to the soft lifetime from what was initially negotiated.
negotiated hard lifetime (kb/sec)	The hard lifetime negotiated by the system and the security gateway for inbound SAs. The lifetime is measured in terms kilobytes (kb) and/or seconds (sec). The hard lifetime that dictates the maximum duration for the SA before its termination.
remaining hard lifetime (kb/sec)	The amount of kilobytes and/or seconds remaining to the hard lifetime from what was initially negotiated.
Decoded	The number of packets and bytes that have been decoded for the SA.
Decode Errors	The number of errors that have occurred while decoding packets.
Authentication Errors	The number of errors that occurred during the system/security gateway authentication process.
Replay Errors	The number of replay errors that occurred for the SA.

Field	Description
Too Short Errors	The number of too short errors that occurred for the SA.
ISAKMP sessions established for this tunnel	The total number of sessions successfully connected by this SA.
ISAKMP sessions failed for this tunnel	The total number of sessions that failed to be connected by this SA.
ISAKMP for this tunnel	**NOTE:** These items are displayed for the life of the ISAKMP SA.
Phase1 Completed as Responder	Indicates the state of the Phase 1 IPSec negotiation stage and role of the system (either responder or initiator).
Statistics	Displays statistics for the ISAKMP SA.
IN	The number of packets/bytes received.
OUT	The number of packets/bytes transmitted.
1 Phase2 negotiations	The number of negotiations that have taken place in Phase 2.
Negotiated Hard lifetime	The hard lifetime negotiated by the system and the security gateway for inbound SAs. The lifetime is measured in terms kilobytes (kb) and/or seconds (sec). The hard lifetime that dictates the maximum duration for the SA before its termination.

show crypto ipsec security-associations summary

Table 5: show crypto ipsec security-associations summary Command Output Descriptions

Field	Description
vvv	The first value (v) indicates the state of the security association (SA State), which can be: • **E**: Established • **P**: Partially Established • **N**: No SAs The second value (v) indicates the state of rekeying (Rekey/Keepalive), which can be: • **D**: Rekey Disabled • **E**: Rekey Enabled/No Keepalive • **K**: Rekey Enabled/Keepalive The third value (v) indicates the type of crypto map (Crypto Type) facilitating the security association, which can be: • **D**: Dynamic Map • **I**: IKEv1 Map • **J**: IKEv2 Map • **M**: Manual Map
Map Name	The name of the crypto map facilitating the security association.
Rekeys	The number of rekeys that occurred for the security association.
En Pkts	The number of packets that have been encrypted and transmitted over the security association.
De Pkts	The number of packets that have been received over the security association and decrypted.

show crypto isakmp keys

Table 6: show crypto isakmp keys Command Output Descriptions

Field	Description
Peer IP Address	The IP address of the security gateway(s).

Field	Description
Preshared Key	The pre-shared key(s) (in Hex) exchanged by the security gateway.

show crypto isakmp security-associations

Table 7: show crypto isakmp security-associations Command Output Descriptions

Field	Description
Local IPSec GW	The IP address of the local IPSec gateway.
Remote IPSec GW	The IP address of the remote IPSec gateway.
State	This displays the state of the SA. The two letters at the beginning of the state define the IKE mode as follows: • MM - Main Mode • QM - Quick Mode • AM - Aggressive Mode The letter in parentheses ( ) at the end of the state, describe where the state message was initiated as follows: • I - Initiator • R - Responder
Lifetime	The lifetime (time) the security association is active and amount of time remaining.

show crypto managers

Table 8: show crypto managers Command Output Descriptions

Field	Description
Total IKEv2 Invalid-MsgId Notify Sent	An invalid KE Payload was received and the receiver sent back a NOTIFY payload to indicate this. This is the number of times a NOTIFY payload was sent to indicate this error condition.
Total IKEv2 Invalid-MsgId Notify Received	A NOTFIY Payload was received indicating that the KE which had been previously sent to the peer was deemed invalid by the peer.
Total IKEv2 Invalid-KE Notify Sent	An IKE packet was received for which the message-id is invalid. A NOTIFY payload was sent to the peer to indicate that the received message-id was invalid. This maintains the count of the number of times that such a NOTIFY payload was sen.t

Field	Description
Total IKEv2 Invalid-KE Notify Received	A NOTIFY payload was received indicating that the message-id which had been previously sent to the peer was deemed invalid by the peer.
Total IKEv2 No-Prop-Chosen Notify Sent	The receiver could not accept the protocol proposal which was sent. A NOTIFY payload was sent back to indicate this. This maintains the count of the number of times such a NOTIFY payload was sent.
Total IKEv2 No-Prop-Chosen Notify Received	A NOTIFY payload was received indicating that the proposals which had been previously sent to the peer could not be accepted.

show crypto managers instance

Table 9: show crypto managers instance Command Output Descriptions

Field	Description
IKEv2 DoS Cookie-Challenge Status	Denial of Service status. • On • Off
Certificate Information	For non-expired certificates: • Serial number: <*string*> • Monitoring Timer: Running • Status: Not Expired • Next Timer <*datetime*> • Expiry: <*datetime*> For expired certificates • Serial number: <*string*> • Monitoring Timer: Stopped • Status: Expired • Next Timer: Not Scheduled • Expiry: <*datetime*>
IKEv2 Statistics	This displays the IKEv2 statistics for this manager instance
Current IKEv2 SAs	The total number of all IKEv2 SAs for this manager instance
Current half-open IKEv2 SAs	The number of IKEv2 SAs in half-open state for this manager instance

Field	Description
Current Connecting IKEv2 SAs	The number of IKEv2 SAs trying to connect for this manager instance
Current Established IKEv2 SAs	The number of established IKEv2 SAs for this manager instance
Internal Failure Sent	Indicates an internal failure in ipsecmgr or dcardmgr and a Notify message was sent to the peer.

show crypto managers summary

Table 10: show crypto managers summary Command Output Descriptions

Field	Description
demux-stats	Display sessions demux statistics on each IPsec Manager.
distribution	Display IPsec Manager distribution info.
handoff-stats	Display IKE request handoff Statistics on each IPsec Manager.
ike-stats	Display IKE statistics on each IPsec Manager.
ikev2-stats	Display IKEv2 statistics on each IPsec Manager.
ipsec-sa-stats	Display IPsec SA statistics on each IPsec Manager.

show crypto map summary

Table 11: show crypto map summary Command Output Descriptions

Field	Description
Total Crypto maps	The total number of crypto maps of all types.
Configured maps	The total number of configured crypto maps.
Service maps	The total number of service maps. There is one map per service.
Subscriber maps	The total number of subscriber maps.
Map Types	
ipsec-dynamic	The total number of dynamic IPsec tunnel crypto maps.
ipsec-l2tp	The total number of L2TP IPsec tunnel crypto maps.
ipsec-ikev1	The total number of IKEv1 IPsec tunnel crypto maps.
ipsec-manual	The total number of manual (static) IPsec tunnel crypto maps.

Field	Description
ipsec-ikev2-subscriber	The total number of IKEv2 subscriber tunnel crypto maps.
ipsec-mobile-ip	The total number of mobile IP IPsec tunnel crypto maps.
IKEv2 SA	
Cipher null	The total number of IKEv2 security associations using the block cipher NULL. All IKEv2 security association protected traffic is sent in the clear.
Cipher des	The total number of IKEv2 security associations using the block cipher Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher 3des	The total number of IKEv2 security associations using the block cipher Triple Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-128	The total number of IKEv2 security associations using the block cipher Advanced Encryption Standard with a 128-bit key in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-256	The total number of IKEv2 security associations using the block cipher Advanced Encryption Standard with a 256-bit key in Cypher Block Chaining (CBC) mode.
PRF sha1	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) with the cryptographic hash function Secure Hash Algorithm-1.
PRF md5	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) with the cryptographic hash function Message Digest 5.
HMAC sha1	The total number of IKEv2 security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Secure Hash Algorithm-1 truncated to 96 bits.
HMAC md5	The total number of IKEv2 security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Message Digest 5 truncated to 96 bits.
DH Group 1	The total number of IKEv2 security associations using Diffie-Hellman Group 1 security (the lowest security level). DH Group 1 provides 768 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 2	The total number of IKEv2 security associations using Diffie-Hellman Group 2 security. DH Group 2 (the default) provides 1024 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 5	The total number of IKEv2 security associations using Diffie-Hellman Group 5 security. DH Group 5 provides 1536 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.

Field	Description
DH Group 14	The total number of IKEv2 security associations using Diffie-Hellman Group 14 security (the highest security level). DH Group 14 provides 2048 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
IPSec SA	
Protocol esp	The total number of IPsec security associations using Encapsulating Security Payload (ESP) protocol.
Protocol ah	The total number of IPsec security associations using Authentication Header (AH) protocol.
Cipher null	The total number of IPsec security associations using the block cipher NULL. All IKEv2 IPsec security association derived traffic is sent in the clear.
Cipher des	The total number of IPsec security associations using the block cipher Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher 3des	The total number of IPsec security associations using the block cipher Triple Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-128	The total number of IPsec security associations using the block cipher Advanced Encryption Standard with a 128-bit key in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-256	The total number of IPsec security associations using the block cipher Advanced Encryption Standard with a 256-bit key in Cypher Block Chaining (CBC) mode.
HMAC sha1-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Secure Hash Algorithm-1 truncated to 96 bits (the default).
HMAC md5-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Message Digest 5 truncated to 96 bits.
DH Group 1	The total number of IPsec security associations using Diffie-Hellman Group 1 security (the lowest security level). DH Group 1 provides 768 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 2	The total number of IPsec security associations using Diffie-Hellman Group 2 security. DH Group 2 (the default) provides 1024 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 5	The total number of IPsec security associations using Diffie-Hellman Group 5 security. DH Group 5 provides 1536 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.

Field	Description
DH Group 14	The total number of IPsec security associations using Diffie-Hellman Group 14 security (the highest security level). DH Group 14 provides 2048 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.

show crypto statistics

Table 12: show crypto statistics Command Output Descriptions

Field	Description
Combined ipsec statistics for context <context-name>	The name of the system context for which statistics are displayed.
Transmit Statistics	
ESP Encode	The total number of packets and bytes that were transmitted having been encoded for the SA using the Encapsulating Security Payload (ESP) protocol.
AH Encode	The total number of packets and bytes that were transmitted having been encoded for the SA using the Authentication Header (AH) protocol.
Transmit Error Counters	
Encode Packets	The total number of packets which have errors while encoding.
Encode Bytes	The total number of bytes which have errors while encoding.
Receive Statistics	
ESP Decode	The total number of packets and bytes that were received having been encoded for the SA using the Encapsulating Security Payload (ESP) protocol.
AH Decode	The total number of packets and bytes that were received having been encoded for the SA using the Authentication Header (AH) protocol.
Receive Error Counters	
Decode Packets	The total number of packets which have errors while decoding.
Decode Bytes	The total number of bytes which have errors while encoding.
Replay Packets	The total number of packets which have been replayed.
Replay Bytes	The total number of bytes which have been replayed.
Combined Control Statistics for Context	The name of the system context for which statistics are displayed.
IKE Flow Counts	

Field	Description
IKE Gateway Flows	The number of UDP flows, incremented when UDP flows are allocated and decremented when UDP flows are freed.
IKE Session Flows	The number of cookie flows, incremented when cookie flows are allocated and decremented when cookie flows are freed.
Transmit Statistics	
IKE Packets	The total number of total IKE packets transmitted.
Receive Statistics	
IKE Packets Received	The total number of IKE packets received.
New IKE Req	The total number of IKE packets sent for new IKE requests.
Gateway Flow Packets	The total number of UDP flow packets received.
Session Flow Packets	The total number of cookie flow packets received.
Rekey Statistics	
IKE Rekeys	The total number of times the IKE SAs negotiated during phase 1 of the IPSec negotiation have been rekeyed. This field is for IKEv1 only and it will be 0 for IKEv2.
Dead Peer Detection (DPD) Statistics	
Req Sent	The total number of DPD R-U-THERE packets sent.
Rsp Rcvd	The total number of DPD R-U-THERE-ACK packets received.
Req Rcvd	The total number of DPD R-U-THERE packets received.
Rsp Sent	The total number of DPD R-U-THERE-ACK packets sent.
Disconnects	The total number of DPD disconnects that occurred between the peers.
Timeouts	The total number of ISAKMP DPD protocol messages that have exceeded their configured timeout period.
NAT-T Statistics	
Keepalives Sent	The total number of NATT keepalive packets sent.
Keepalives Rcvd	The total number of NATT keepalive packets received.
Detailed IKE Statistics	
Active IKE SAs	The total number of SAs: • Initiated • Responded.

Field	Description
Total IKE SAs	The total number of SAs (cumulative history): • Initiated • Responded.
Total Attempts	The total cumulative attempts made to establish SAs: • Initiated • Responded.
Total IKE SA Deletes	• Req Sent • Rsp Rcvd • Req Rcvd • Rsp Sent
Total Packets In	The total cumulative IKE packets received.
Total Packets Out	The total cumulative IKE packets sent.
Total Octets In	The total cumulative IKE octets received.
Total Octets Out	The total cumulative IKE octets sent.
Establishment Failure Statistics	
Initiation Neg Error	The total number of initiated negotiations that failed because of errors.
Initiation Neg Time Out	The total number of initiated negotiations that failed because of timeouts (no response).
Response Neg Error	The total number of responded negotiations that failed because of errors.
Congestion Reject	The total number of packets which were rejected due to congestion control.
Congestion Drop	The total number of packets which were dropped due to congestion control.
Total Cookie Error	Total errors in cookie challenge. Refer to the detailed counters in IKEv2 section.
Total Auth Failures	Total errors due to authentication failures during IKE_AUTH exchanges.
IKEv2 Statistics	
Current state:	• Current IKEv2 SAs • Current half-open IKEv2 SAs • Current connecting IKEv2 SAs • Current established IKEv2 SAs • Current child SAs

Field	Description
IKEv2 Timer Stats	• Total IKESA Retrans expirations • Total IKESA Setup expirations (no exchange) • Total IKESA Setup expirations • Total IKESA Lifetime (soft) expirations • Total IKESA Lifetime (hard) expirations • Total TSELSA Lifetime (soft) expirations • Total TSELSA Lifetime (hard) expirations
IKEv2 Exchanges dropped	• Total IKEv2 Resp Pkts Drop - No IKESA • Total invalid resp • Total non-init exch drop--no IKESA • Total invalid message ID • Total invalid major version • Total IKESA error • Total unknown critical payload
IKEv2 Cookie Statistics	• Total cookie notify packets sent • Total cookie notify packets received • Total cookie notify match • Total cookie notify not match
IKEv2 Rekey Statistics	• Total IKESA Rekey sent • Total IKESA Rekey received • Total IKESA Rekey ignored • Total ChildSA Rekey sent • Total ChildSA Rekey received • Total ChildSA Rekey ignored
IKEv2 MOBIKE Statistics	• Total MOBIKE notify sent • Total MOBIKE received • Total Mobike ignored
IKEv2 Misc Statistics	• Total SA create failure • Total SA flow operation failure • Total NAT Keepalive received • Total Invalid-KE notify sent • Total Invalid-KE notify received • Total Invalid-msgID notify received • Total No-Prop-Chosen notify sent • Total No-Prop-Chosen notify received

Field	Description
IKEv2 Exchange Decode failure statistics	• Total pkts failure • Total internal errors • Total invalid IP HDR • Total invalid UDR HDR • Total invalid IKE HDR • Total invalid IKE HDR payload • Total invalid IKE HDR MJ ver • Total invalid IKE HDR MN ver • Total invalid IKE HDR exchange type • Total invalid IKE HDR Rsvd flag • Total invalid IKE HDR length • Total invalid payload syntax • Total invalid payload len • Total unknown crit payload • Total too many payloads • Total invalid SA payload len • Total invalid SA proposal HDR • Total invalid SA proposal HDR Reserved • Total too many transforms • Total invalid SA proposal HDR len • Total too many proposals • Total invalid protocol ID • Total invalid first SA proposal num • Total invalid SA proposal num • Total invalid transform len • Total invalid transform HDR • Total invalid transform HDR Rsvd • Total invalid transform type • Total invalid transform ID

Field	Description
IKEv2 Exchange Decode failure statistics (continued)	• Total invalid KE payload len • Total invalid KE DH Group len • Total invalid ID payload type • Total invalid ID payload len • Total invalid KE DH group • Total invalid KE DH groups • Total invalid Transform ID • Total invalid auth payload len • Total invalid nonce payload len • Total invalid notify payload len • Total invalid notify payload SPI size • Total Invalid Notify payload Proto ID • Total invalid notify payload NATT • Total invalid notify payload Cookie • Total Invalid notify payload Rekey • Total invalid notify payload NATT • Total invalid notify payload Cookie • Total invalid notify payload Rekey • Total invalid EAP payload len • Total invalid CP payload len • Total invalid CP payload attr len • Total invalid payload unknown attr • Total invalid Encrypted Payload len • Total invalid TS payload len • Total invalid TS payload Rsvd • Total invalid TS payload TS-type • Total unsupported crit payload • Total unsupported cert payload • Total unsupported Auth method
IKEv2 Exchange Decode failure statistics (continued)	• Total unsupported SA payload Prot AH • Total unsupported Notify Prot AH • Total unsupported payload Crit VID • Total unsupported TS payload TS_Type • Total unsupported method • Total unknown error
IKEv2 Decrypt Failure statistics	• Total Pkts failure • Total HMAC mismatch • Total pad length error

Field	Description
IKEv2 Xchg statistics	• Total Bad Msg ID • Total bad response • Total stale message ID • Total unknown error • Total state lookup failure

show crypto statistics ikev2

Table 13: show crypto statistics IKEv2 Command Output Descriptions

Field	Description
Flow Counts	
Current UDP flows	The total number of UDP port based flows in the data path.
Current Cookie flows	The total number of cookie challenge based flows in the data path.
Transmit Statistics	
IKE Packets	The total number of total IKE packets transmitted.
Receive Statistics	
IKE Packets Received	The total number of IKE packets received.
New IKE Requests	The total number of IKE packets sent for new IKE requests.
UDP flow Packets	The total number of packets that matched the UDP flow.
Cookie flow Packets	The total number of packets that matched the cookie flow.
Rekey Statistics	
IKE Rekeys	The total number of successful IKE_SA rekeys.
Dead Peer Detection (DPD) Statistics	
Requests sent	The total number of DPD R-U-THERE packets sent.
Replies received	The total number of DPD R-U-THERE-ACK packets received.
Requests received	The total number of DPD R-U-THERE packets received.
Replies sent	The total number of DPD R-U-THERE-ACK packets sent.
Collisions	The total number of events that IKEv2 keepalive exchanges occur simultaneously from the PDIF and the MS.
Disconnects	The total number of DPD disconnects that occurred between the peers.

Field	Description
Timeouts	The total number of DPD protocol messages that have exceeded their configured timeout period.
NAT-T Statistics	
Keepalives sent	The total number of NAT-T keepalive packets sent.
Detailed IKE Statistics	
Active IKE SAs	The total number of IKE SAs.
Initiated	The total number of the active SAs initiated locally.
Responded	The total number of the active SAs responded.
Total IKE SAs so far	The total number of SAs (cumulative history).
Initiated	The total cumulative IKE SAs initiated locally.
Responded	The total cumulative IKE SAs responded to.
Total attempts so far	The total cumulative attempts made to establish SAs.
Initiated	The total number of SA establishment attempts initiated locally.
Responded	The total number of SA establishment attempts responded to.
Total deletes so far	The total cumulative deletes so far.
Requests received	The total number of requests received.
Requests sent	The total number of requests sent.
Replies received	The total number of replies received.
Replies sent	The total number of replies sent.
Total packets in	The total cumulative IKEv2 packets received.
Total packets out	The total cumulative IKEv2 packets sent.
Total octets in	The total cumulative IKEv2 octets received.
Total octets out	The total cumulative IKEv2 octets sent.
Failed initiated negotiations with errors	The total number of initiated negotiations that failed because of errors.
Failed initiated negotiations with time out:	The total number of initiated negotiations that failed because of timeouts (no response).
Failed responded negotiations with errors	The total number of responded negotiations that failed because of errors.
Total cookie errors	The total number of cookie errors encountered.

Field	Description
Congestion rejects	The total number of packets rejected due to congestion.
Congestion drops	The total number of packets dropped due to congestion.
Total Unknown Exchange SPI	The total number of unknown exchange SPIs.
IKEv2 Detail Statistics	
Current State	
Current IKEv2 SAs	The number of current IKEv2 SAs.
Current Half-Open IKEv2 SAs	The number of IKEv2 SAs in a half-open state.
Current Connecting IKEv2 SAs	The number of IKEv2 SAs currently connecting.
Current Established IKEv2 SAs	The number of established IKEv2 SAs.
Current Child SAs	The number of current child SAs.
Total IKEv2 Timer Statistics	
IKESA Retrans Expirations	The total number of retransmission expirations.
IKESA Setup Expirations (no Xchg)	The number of IKESA setups that expired with no exchange.
IKESA Setup Expirations	The total number of IKESA Session setups expired.
IKESA Lifetime (Soft) Expirations	The number of IKESA soft lifetime timer expirations.
IKESA Lifetime (Hard) Expirations	The number of IKESA hard lifetime timer expirations.
CHILD_SA Setup Expirations (no Xchg)	The number of Child SA setups that expired with no exchange.
CHILD_SA Lifetime (Soft) Expirations	The number of Child SA soft lifetime timer expirations.
CHILD_SA Lifetime (Hard) Expirations	The number of Child SA hard lifetime timer expirations.
Total IKEv2 Multiple Authentication Statistics	
Phase 1 Auth Successes	The number of multi-auth Phase 1 EAP authentication successes.
Phase 1 Auth Failures	The number of multi-auth Phase 1 EAP authentication failures.
Phase 1 Auth Req Sent	The number of multi-auth Phase 1 EAP authentication requests sent.
Phase 1 Auth Resp Rcvd	The number of multi-auth Phase 1 EAP authentication responses received.
Phase 2 Auth Successes	The number of multi-auth Phase 2 EAP authentication successes.
Phase 2 Auth Failures	The number of multi-auth Phase 2 EAP authentication failures.

Field	Description
Phase 2 Auth Req Sent	The number of multi-auth Phase 2 EAP authentication requests sent.
Phase 2 Auth Resp Rcvd	The number of multi-auth Phase 2 EAP authentication responses received.
Phase 2 Auth MD5 Successes	The number of multi-auth Phase 2 EAP authentication with MD5 successes.
Phase 2 Auth MD5 Failures	The number of multi-auth Phase 2 EAP authentication with MD5 failures.
Phase 2 Auth GTC Successes	The number of multi-auth Phase 2 EAP authentication with GTC mode successes.
Phase 2 Auth GTC Failures	The number of multi-auth Phase 2 EAP authentication with GTC mode failures.
Hash match failures	The number of hash match failures.
Signing failures	The number of signing failures.
MSK missing at phase 1 comp	The number of EAP Master Session Keys (MSK) not found.
Miss Another Auth Follows	The number of missed authentications that follow.
Total IKEv2 Exchanges Dropped	
Resp Pkts Drop - No IKESA	The number of IKEv2 response packets dropped without an IKEv2 SA being created.
Invalid Resp	The total number of invalid response messages.
Non-Init Exch Drop - No IKESA	The total number of IKEv2 exchanges dropped without an IKEv2 SA being created.
Invalid MSG ID	The total number of sessions dropped due to packets with invalid MSG ID.
Invalid Major Version	The total number of sessions dropped due to packets with invalid major version.
IKESA error	The total number of IKESA error messages.
Unknown Crit Payload	The total number of unknown critical payload messages.
Retransmitted request	IKEV2 Stack does not process the packets in the order they are received. New packets are queued if any packet is under processing. After completing the processing, stack consider processing the packets queue first instead of taking the latest packet received from network directly and leaving the packets in queue for later. And if any message is received with same message ID which is currently under processing, then that message will be discarded as retransmitted message received. The count for such request is 'Retransmitted Request'.
Total IKEv2 Notify Statistics	
Cookie Notify Sent	The total number of IKEv2 Denial of Service (DoS) cookie notify packets sent.
Cookie Notify Received	The total number of IKEv2 DoS cookie notify packets received.
Cookie Notify Match	The total number of IKEv2 DoS cookie notify messages that match.
Cookie Notify Not Match	The total number of IKEv2 DoS cookie notify messages that do not match.

Field	Description
Multi Auth Supported	The total number of multiple authentications supported.
Another Auth Follows	The total number of authentications that follow.
PDN Type IPv4 Sent	Displays the status of the IPv4 PDN type sent.
PDN Type IPv6 Sent	Displays the status of the IPv6 PDN type sent.
Total IKEv2 Rekey Statistics	
IKESA Rekey Sent	The total number of IKESA Rekey Request messages sent.
IKESA Rekey Rcvd	The total number of IKESA Rekey Request messages received.
IKESA Rekey Ignored	The total number of IKESA Rekey messages ignored.
ChildSA Rekey Req Sent	The total number of Child SA Rekey Request messages sent.
ChildSA Rekey Req Rcvd	The total number of Child SA Rekey Request messages received.
ChildSA Rekey Rsp Sent	The total number of Child SA Rekey Response messages sent.
ChildSA Rekey Rsp Rcvd	The total number of Child SA Rekey Response messages received.
ChildSA Rekey Ignored	The total number of Child SA Rekey messages ignored.
Total IKEv2 MOBIKE Statistics	
MOBIKE Notify Sent	The total number of MOBIKE notify messages sent. MOBIKE is not supported. All MOBIKE messages are treated as if they were never received.
MOBIKE Recvd	The total number of MOBIKE packets received.
MOBIKE Ignored	The total number of MOBIKE packets dropped.
Total IKEv2 Misc Statistics	
SA Create Failure	The total number of SA creations failed.
SA Flow Operation Failure	The total number of SA flow operations failed.
Total IKEv2 Notify Payload Sent Statistics	
Invalid KE Payload	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type Invalid KE Payload.
Invalid Major Version	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type Invalid Major Version.
Invalid Message ID	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type Invalid Message ID.
Invalid Syntax	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type Invalid Syntax.

Field	Description
No Additional SAs	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type No Additional SAs.
No Proposal Chosen	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type No Proposal Chosen.
TS Unacceptable	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type TS Unacceptable.
Unsupported Critical Payload	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type Unsupported Critical Payload.
Internal Failure Sent	The total number of IKEv2 NOTIFY payloads sent of the NOTIFY type Internal Failure Sent.
Total IKEv2 Notify Payload Received Statistics	
Invalid KE Payload	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type Invalid KE Payload.
Invalid Major Version	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type Invalid Major Version.
Invalid Message ID	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type Invalid Message ID.
Invalid Syntax	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type Invalid Syntax.
No Additional SAs	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type No Additional SAs.
No Proposal Chosen	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type No Proposal Chosen.
TS Unacceptable	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type TS Unacceptable.
Unsupported Critical Payload	The total number of IKEv2 NOTIFY payloads received of the NOTIFY type Unsupported Critical Payload.
IKEv2 Exchange Decode Failure Statistics	
Packet Failures	The number of IKEv2 packets that fail to decode.
Internal Errors	The total number of failures due to internal errors.
Invalid IP HDR	The total number of failures due to an invalid IP header.
Invalid UDP HDR	The total number of failures due to an invalid UDP header.
Invalid IKE HDR	The total number of failures due to an invalid IKE header.
Invalid IKE HDR Payload	The total number of failures due to an invalid IKE header payload.

Field	Description
Invalid IKE HDR Init SPI	The total number of failures due to an invalid IKE header initiator security parameter index.
Invalid IKE HDR Resp SPI	The total number of failures due to an invalid IKE header responder security parameter index.
Invalid IKE HDR Major Ver	The total number of failures due to an invalid IKE header major version.
Invalid IKE HDR Minor Ver	The total number of failures due to an invalid IKE header minor version.
Invalid IKE HDR Xchg Type	The total number of failures due to an invalid IKE header exchange type.
Invalid IKE HDR Rcvd Flag	The total number of failures due to an invalid IKE header received flags.
Invalid IKE HDR Len	The total number of failures due to an invalid IKE header length.
Invalid Syntax	The total number of failures due to an invalid syntax.
Invalid Payload Syntax	The total number of failures due to an invalid payload syntax.
Invalid Payload Len	The total number of failures due to an invalid payload length.
Unknown Crit Payload	The total number of failures due to an unknown critical payload.
Too many payloads	The total number of failures due to many payloads.
Invalid SA Payload Len	The total number of failures due to an invalid SA payload length.
Invalid SA Proposal HDR	The total number of failures due to an invalid SA proposal header.
Invalid SA Proposal HDR Rcvd	The total number of failures due to an invalid SA proposal header received.
Too many transforms	The total number of failures due to many transform-sets in the SA payload.
Invalid SA Proposal HDR Len	The total number of failures due to an invalid SA proposal header length.
Too many proposals	The total number of failures due to many proposals in SA payload.
Invalid first SA Proposal num	The total number of failures due to an invalid first SA proposal number.
Invalid SA Proposal ID	The total number of failures due to an invalid Protocol ID in SA payload.
Invalid SA Proposal num	The total number of failures due to an invalid SA proposal number.
Invalid Transform Len	The total number of failures due to an invalid transform-set length.
Invalid Transform HDR	The total number of failures due to an invalid transform-set header.
Invalid Transform HDR Rcvd	The total number of failures due to an invalid transform-set header received.
Invalid Transform Type	The total number of failures due to an invalid transform-set type.
Invalid Transform ID	The total number of failures due to an invalid transform-set ID.
Invalid KE Payload Len	The total number of failures due to an invalid key exchange payload length.

Field	Description
Invalid KE DH Group	The total number of failures due to an invalid key exchange Diffie-Hellman group number.
Invalid KE DH Group Len	The total number of failures due to an invalid ID payload length.
Invalid ID Pld Len	The total number of failures due to an invalid ID payload length.
Invalid ID Pld Type	The total number of failures due to an invalid ID payload type.
Invalid ID Pld Data	The total number of packets for which ID payload syntax validation has failed.
Invalid Auth Pld Len	The total number of failures due to an invalid authorization payload length.
Invalid Nonce Payload Len	The total number of failures due to an invalid nonce payload length.
Invalid Notify Payload Len	The total number of failures due to an invalid notify payload length.
Invalid Notify Payload SPI Len	The total number of failures due to an invalid notify payload security parameter index size.
Invalid Notify Payload NAT	The total number of failures due to an invalid notify payload Network Address Translation-Traversal.
Invalid Notify payload Proto Id	The total number of failures due to an invalid notify payload protocol ID.
Invalid EAP Payload len	The total number of failures due to an invalid Encapsulation Authentication Protocol payload length.
Invalid Notify Payload Rekey	The total number of failures due to an invalid notify payload rekey.
Invalid CP Payload len	The total number of failures due to an invalid CP payload length.
Invalid Notify Payload Cookie	The total number of failures due to an invalid notify payload cookie.
Invalid TS Payload len	The total number of failures due to an invalid transform-set payload length.
Invalid CP Payload Attr Len	The total number of failures due to an invalid CP payload unknown attribute length.
Invalid TS Payload Rcvd	The total number of failures due to an invalid transform-set payload received.
Invalid Encrypted Payload Len	The total number of failures due to an invalid encrypted payload length.
Invalid TS payload TS-Type	The total number of failures due to an invalid transform-set payload transform-set type.
Unsupported Crit Payload	The total number of failures due to an unsupported critical payload.
Unsupported Cert Payload	The total number of failures due to an unsupported certified payload.
Unsupported Notify Prot AH	The total number of failures due to an unsupported notify payload protocol Authentication Header.
Unsupported Auth method	The total number of failures due to an unsupported authentication method.
Unsupported Payload Crit VID	The total number of failures due to an unsupported payload critical V-LAN ID.

Field	Description
Unsupported method	The total number of failures due to an unsupported method.
Unknown Error	The total number of failures due to an unknown error.
Unsupported SA Payload Prot AH	The total number of failures due to an unsupported SA payload protocol Authentication Header.
Unsupported TS payload TS-Num	The total number of failures due to an unsupported transform-set payload number.
Unsupported TS Payload TS-Type	The total number of failures due to an unsupported transform-set payload transform-set-type.
Unsupported TS Payload TS-Prot	The total number of failures due to an unsupported transform-set payload protocol.
Unsupported CP Payload No IP Attr	The total number of failures due to an invalid CP because of no available IP attribute.
Invalid CP Payload UNK ATTR	The total number of failures due to an invalid CP because of an unknown attribute.
Total IKEv2 Decrypt Failure Statistics	
Packets Failure	The total number of session failures due to packets that failed to decrypt.
HMAC mismatch	The total number of session failures due to a HMAC mismatch.
Pad length error	The total number of failures due to a pad length error in the packet.
Total IKEv2 Xchg Statistics	
Bad Msg Id	The total number of session failures due to a bad message ID.
Bad Response	The total number of session failures due to a bad response.
Stale Msg ID	The total number of session failures due to a stale message ID.
Unknown error	The total number of session failures due to unknown errors.
Stale Lookup Failure	The total number of session failures due to a stale lookup failure.
Combined Crypto map Statistics	
Current Tunnels	The number of tunnels currently connected by the SA.
Current Tunnels Established	The number of tunnels successfully connected by the SA.
IKE Fails	The total number of tunnels that failed to be connected by the SA.
Total Tunnels	The total number of tunnels connected by the SA.
Total Tunnels Established	The total number of tunnels successfully connected by the SA.
Call Req Rejects	The total number of call request reject messages.
IKEv2 Authentication Failures Statistics	
No DEA message	The total number of non DEA messages.

Field	Description
Missing AVP in DEA	The total number of missing AVPs in the DEA message.
Invalid APN	The total number of invalid APNs.
Key mismatch	The total number of key mismatches in the authentication vectors.
Invalid result code or AVP in DEA	The total number of invalid result code or AVP in the DEA message.
Invalid NAI format	The total number of invalid NAI formats.
APN validation failed	The total number of failed APN validations.
Misc. auth failures	The total number of miscellaneous authentication failures.

show crypto template summary

Table 14: show crypto template summary Command Output Descriptions

Field	Description
Total Crypto maps	
Configured maps	The total number of crypto maps configured in this context.
Service maps	The total number of service maps. There is one map per service.
Subscriber maps	The total number of subscriber maps.
Map Types:	
ipsec-dynamic	The total number of dynamic IPsec tunnel crypto maps.
ipsec-ikev1	The total number of IKEv1 IPsec tunnel crypto maps.
ipsec-ikev1pst-subscr	The total number of IKEv1 PST subscriber tunnel maps.
ipsec-ikev2	The total number of IKEv2 subscriber tunnel crypto maps.
ipsec-ikev2-subscriber	The total number of IKEv2 subscriber tunnel crypto maps.
ipsec-l2tp	The total number of L2TP IPsec tunnel crypto maps.
ipsec-manual	The total number of manual (static) IPsec tunnel crypto maps.
ipsec-mobile-ip	The total number of mobile IP IPsec tunnel crypto maps.
IKEv2 SA:	
Cipher 3des	The total number of IKEv2 security associations using the block cipher Triple Data Encryption Standard in Cypher Block Chaining (CBC) mode.

Field	Description
Cipher aes-cbc-128	The total number of IKEv2 security associations using the block cipher Advanced Encryption Standard with a 128-bit key in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-256	The total number of IKEv2 security associations using the block cipher Advanced Encryption Standard with a 256-bit key in Cypher Block Chaining (CBC) mode.
Cipher des	The total number of IKEv2 security associations using the block cipher Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher null	The total number of IKEv2 security associations using the block cipher NULL. All IKEv2 security association protected traffic is sent in the clear.
DH Group 1	The total number of IKEv2 security associations using Diffie-Hellman Group 1 security (the lowest security level). DH Group 1 provides 768 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 2	The total number of IKEv2 security associations using Diffie-Hellman Group 2 security. DH Group 2 (the default) provides 1024 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 5	The total number of IKEv2 security associations using Diffie-Hellman Group 5 security. DH Group 5 provides 1536 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 14	The total number of IKEv2 security associations using Diffie-Hellman Group 14 security (the highest security level). DH Group 14 provides 2048 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
HMAC aes-xcbc-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) using the AES block cipher with a block size of 128 bits.
HMAC md5-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Message Digest 5 truncated to 96 bits.
HMAC sha2-256-128	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) in conjunction with the SHA-256 algorithm truncated to 128 bits.
HMAC sha2-384-192	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) in conjunction with the SHA-384 algorithm truncated to 192 bits.
HMAC sha2-512-256	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) in conjunction with the SHA-512 algorithm truncated to 256 bits.

Field	Description
PRF sha1	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) with the cryptographic hash function Secure Hash Algorithm-1.
PRF aes-xcbc-128	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) in conjunction with Advanced Encryption Standard (AES) with a key length restriction of 128 bits.
PRF md5	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) with the cryptographic hash function Message Digest 5.
PRF sha2-256	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) using the SHA-2 algorithm truncated to 256 bits.
PRF sha2-384	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) using the SHA-2 algorithm truncated to 384 bits.
PRF sha2-512	The total number of IKEv2 security associations using the IKE pseudo-random function (PRF) using the SHA-2 algorithm truncated to 512 bits.
IPSec SA	
Protocol esp	The total number of IPsec security associations using Encapsulating Security Payload (ESP) protocol.
Protocol ah	The total number of IPsec security associations using Authentication Header (AH) protocol.
Cipher 3des	The total number of IKEv2 security associations using the block cipher Triple Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-129	The total number of IKEv2 security associations using the block cipher Advanced Encryption Standard with a 129-bit key in Cypher Block Chaining (CBC) mode.
Cipher aes-cbc-256	The total number of IKEv2 security associations using the block cipher Advanced Encryption Standard with a 256-bit key in Cypher Block Chaining (CBC) mode.
Cipher des	The total number of IKEv2 security associations using the block cipher Data Encryption Standard in Cypher Block Chaining (CBC) mode.
Cipher null	The total number of IKEv2 security associations using the block cipher NULL. All IKEv2 security association protected traffic is sent in the clear.
DH Group 1	The total number of IKEv2 security associations using Diffie-Hellman Group 1 security (the lowest security level). DH Group 1 provides 768 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 2	The total number of IKEv2 security associations using Diffie-Hellman Group 2 security. DH Group 2 (the default) provides 1024 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.

Field	Description
DH Group 5	The total number of IKEv2 security associations using Diffie-Hellman Group 5 security. DH Group 5 provides 1536 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
DH Group 14	The total number of IKEv2 security associations using Diffie-Hellman Group 14 security (the highest security level). DH Group 14 provides 2048 bits of key exchange cryptographic strength. This is a modular exponential (MODP) DH group.
HMAC aes-xcbc-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) using the AES block cipher with a block size of 128 bits.
HMAC md5-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Message Digest 5 truncated to 96 bits.
HMAC sha1-96	The total number of IPsec security associations using a keyed-Hash Message Authentication Code (HMAC) with the cryptographic hash function Secure Hash Algorithm-1 truncated to 96 bits (the default).