GET VPN Support with Suite B

The GET VPN Support with Suite B feature adds support of the Suite B set of ciphers to Cisco Group Encrypted Transport (GET) VPN. Suite B is a set of cryptographic algorithms that includes Galois Counter Mode Advanced Encryption Standard (GCM-AES) as well as algorithms for hashing, digital signatures, and key exchange.

Suite B for IP security (IPsec) VPNs is a standard whose usage is defined in RFC 4869, Suite B Cryptographic Suites for IPsec . Suite B provides a comprehensive security enhancement for Cisco IPsec VPNs, and it allows additional security for large-scale deployments. Suite B is the recommended solution for organizations requiring advanced encryption security for the wide-area network (WAN) between remote sites.

Prerequisites for GET VPN Support with Suite B

All key servers (KSs) and group members (GMs) on which you want to enable this feature must be running GET VPN software version 1.0.4 or higher. You should use this feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature. This feature provides a command that you use on the KS (or primary KS) to check whether all devices in the network are running versions that support Suite B. For more information, see the "Ensuring That GMs Are Running Software Versions That Support Suite B" section.

Restrictions for GET VPN Support with Suite B

When they are using a GCM policy or a Galois Message Authentication Code (GMAC) traffic encryption key (TEK) policy, all cooperative KSs for a group must use an access control list (ACL) that has identical ACL entries (ACEs) in the identical order. If not, GMs that register to separate KSs cannot encrypt and decrypt correctly after downloading the policy. This is because with Suite B, an SPI (security parameter index ID that is associated with the TEK) is generated for *each* ACL entry and is unique to each ACL entry.

You cannot reorder entries in an existing ACL. So if you are using a GCM or GMAC TEK policy and must update the ACL on each KS so that it has identical entries in the identical order on each KS, you must remove the ACL from each secondary KS, then create a new ACL on the primary KS, then copy it to the secondary KSs, and then enter the **crypto gdoi ks rekey** command on the primary KS to trigger a rekey across the GET VPN network.

You remove an ACL by using the **no** form of the **ip access-list** command (or if you are using IPv6, the **no** form of the **ipv6 access-list** command).

Suite-B for G-IKEv2 does not work when crypto map is applied on multiple interfaces.

Cisco Catalyst 8000 Series Edge Platforms do not support Suite B in GET VPN. Suite B is supported only on the Cisco ASR 1000 Series Aggregation Services Routers and Cisco 4000 Series Integrated Services Routers.

Supported Platforms for GET VPN Support with Suite B

The following table details the platforms and their corresponding models, each supporting Suite B for GET VPN, organized by release:

Table 1: From Cisco IOS XE Release 16.9.1

Platforms	Models
Cisco ASR 1000 Series Aggregation Services Routers	• ASR1001-X • ASR1002-X • ASR1001-HX • ASR1002-HX • ESP100 • ESP200
Cisco 4000 Series Integrated Services Routers	• ISR 4461 • ISR4451-X • ISR4431

Information About GET VPN Support with Suite B

Suite B

Suite B is standardized by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). The GET VPN Support with Suite B feature allows these cryptographic algorithms to be used with GDOI and GET VPN in various ways, including the use of SHA-2/HMAC-SHA-2 and AEC-GCM/AES-GMAC.

Secure Hash Algorithm 2 (SHA-2) is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) designed by the NSA and published by the NIST as a U.S. Federal Information Processing Standard (FIPS). SHA-2 includes many changes from its predecessor, SHA-1. SHA-2 comprises a set of four hash functions with digests that are 224, 256, 384, or 512 bits.

HMAC is a mechanism for message authentication using iterative cryptographic hash functions. HMAC-SHA-2 is HMAC used in combination with the SHA-2 version (SHA-224, SHA-256, SHA-384, and SHA-512) iterative cryptographic hash functions in combination with a secret shared key in IPsec. These combinations are called HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512. These algorithms can be used as the basis for data origin authentication and integrity verification mechanisms for the authentication header (AH) (although not supported by GET VPN), encapsulating security payload (ESP), IKE, and IKEv2 protocols, and also as pseudo-random functions (PRFs) for IKE and IKEv2.

AES using GCM (AES-GCM) is an encryption algorithm for IPsec. AES using Galois Message Authentication Code (AES-GMAC) is a message integrity algorithm also used for IPsec.

SHA-2 and HMAC-SHA-2

The GET VPN Support with Suite B feature lets you use SHA-2 and HMAC-SHA-2 (HMAC-SHA-256, 384, and 512) as the hash and signature algorithms. SHA-2 and HMAC-SHA-2 with 256, 384, & 512-bit keys are used in

- GDOI registration using IKEv1 as the hash algorithm as described in Section 3.2 (authentication between KSs and GMs) of RFC 6407, The Group Domain of Interpretation .
- The key encryption key (KEK) rekey policy to hash the rekey message for authentication of the rekey message from the KS as well as authentication of the acknowledgment message from the GM.
- The TEK IPsec policy as HMAC-SHA-2 for IPsec SA integrity checking.

AES-GCM and AEC-GMAC

AES-GCM (AES-GCM-128, 192, and 256) and AES-GMAC (AES-GMAC-128, 192, and 256) cryptographic algorithms with 256, 384, and 512-bit keys are used in TEK IPsec policies as IPsec SA encryption and integrity algorithms. GCM is used for encryption and integrity, while GMAC is used for integrity only.

Sets of Cryptographic Algorithms that Comply with Suite B

RFC 4869 describes four sets of cryptographic algorithms for use with IKE and IPsec. When configured, any of these sets will comply with Suite B. Each set consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm:

- Suite-B-GCM-128: Provides ESP integrity protection and confidentiality using 128-bit AES-GCM (see RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)). Use this suite or Suite-B-GCM-256 when ESP integrity protection and encryption are both needed.
- Suite-B-GCM-256: Provides ESP integrity protection and confidentiality using 256-bit AES-GCM (see RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)). Use this suite or Suite-B-GCM-128 when ESP integrity protection and encryption are both needed.
- Suite-B-GMAC-128: Provides ESP integrity protection using 128-bit AES-GMAC (see RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH) but does not provide confidentiality. Use this suite or Suite-B-GMAC-256 only when there is no need for ESP encryption.

- Suite-B-GMAC-256: Provides ESP integrity protection using 256-bit AES-GMAC (see RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH) but does not provide confidentiality. Use this suite or Suite-B-GMAC-128 only when there is no need for ESP encryption.

Cisco software contains the ability to configure any of these algorithms. The GET VPN Support with Suite B feature allows GET VPN to use these algorithms.

SID Management

In GET VPN, a counter-based mode of operation (for example, ESP-GCM-AES) requires that an initialization vector (IV) is never reused with a group key. Therefore, this feature provides a method to allow a KS to allocate to each GM (for each interface) a unique sender identifier (SID) for IV construction.

In Suite B, TEK IPsec policies that are used as IPsec SA encryption and integrity algorithms require management of unique pools of SID values on KSs to distribute those unique SID values (GMSIDs) to GMs. Each cooperative KS must have a distinct pool of GMSIDs to allocate. Each KS configures unique KS SIDs (KSSIDs) to configure these SID pools.

A SID space is divided into two parts: a KSSID part and a GMSID part. Therefore, a SID is a concatenation of a KSSID and a GMSID, where the KSSID is the KS portion of a SID, and the GMSID is the GM portion of the SID. A SID is formed by the following bits:

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3  (bits)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    KSSID    |            GMSID                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

In this example, each KSSID (0 to 127) has 2^{17} (131,072) GMSIDs, which are dynamically assigned to each registering GM.

A GM uses GMSIDs to form a unique 64-bit IV for each packet sent with a given key when using AES-GCM or AES-GMAC. An IV is formed by the following bytes:

```
  0   1   2   3   4   5   6   7   (bytes)
+---+---+---+---+---+---+---+---+
|    SID    |       SSIV        |
+---+---+---+---+---+---+---+---+
```

The sender specific IV (SSIV) is a packet counter.

Group Size

The group size is the length of the SID space allocation for KSSIDs as well as GMSIDs that are reserved to a KS for distribution to GMs. Available group sizes are small (8, 12, or 16 bits), medium (24 bits, which is the default), and large (32 bits). Medium is sufficient for nearly all networks.

You should use a large group size only if you must strictly adhere to the requirement in section A.5, “Key/IV Pair Uniqueness Requirements from SP 800-38D” of the publication Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program in which GET VPN used in conjunction with Suite B must have at least 2^{32} unique possible “module names” (SIDs).This publication is issued and maintained by the NIST and the Communications Security Establishment Canada (CSEC).

For example, in a large group size with one KS, the SID is 32 bits, there are 512 KSSID values (in the range of 0 to 511), and each has 8,388,607 GMSIDs to distribute to registering GMs. With a large group size, use the following KSSID assignment guidelines to configure KSSID ranges:

Table 2: Recommended KSSID Ranges for Group Size Large

KS	1 KS (no cooperative KSs)	2 cooperative KSs	3 cooperative KSs	4 cooperative KSs
KS1	0 - 511	0 - 255	0 - 127	0 - 63
KS2	—	256 - 511	128 - 255	64 - 127
KS3	—	—	256 - 383	128 - 191
KS4	—	—	384 - 511	192 - 255
KS5	—	—	—	256 - 319
KS6	—	—	—	320 - 383
KS7	—	—	—	384 - 447
KS8	—	—	—	448 - 511

If you plan to expand the cooperative KS network to include more KSs, while you are initially configuring the original KS or KSs, use the column in the above table with the *anticipated* number of KSs in the network so that you can add the new KS or KSs later.

You should use a small (8-, 12-, or 16-bit) group size only in well-understood cases where strict interoperability with SID lengths of 8, 12, and 16 bits is required according to RFC 6054, Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic . If such interoperability is needed, you must be careful when designing the network, because the number of SIDs per group is severely limited (and therefore, the number of KSs and GMs in a group is severely limited). Following are the limitations for a small group size:

Table 3: Limitations for Group Size Small

SID length	KSSIDs (total KSs)	GMSIDs per KSSID	GMSIDs (total GMs)	Possible number of GM registrations for one KS (after assigning KSSIDs to all KSs evenly)			
—	—	—	—	1 KS	2 KSs	4 KSs	8 KSs
8 bits	2	128	255	320	96	—	—
12 bits	4	1,024	4,095	3,840	1,792	768	—
16 bits	16	4,096	65,535	64,512	31,744	15,360	7,168

KSSID Assignment with Cooperative Key Servers

You should plan ahead to assign a certain number of initial GDOI KS identifiers (KSSIDs) to each KS based on the configured group size, number of KSs, number of GMs, number of GMs per KS, and any future expansion of KSs or GMs (or both).

When there are multiple cooperative KSs in a GDOI group, each KS must have a unique set of KSSID values to ensure that a registering GM never receives the same SID as another registering GM in the group. Therefore, you should plan how you will assign KSSIDs across cooperative KSs in advance, while considering the number of cooperative KSs and if cooperative KSs will be added later. If none will be added, you can assign all

available KSSIDs across all KSs. If cooperative KSs will be added, you should reserve some KSSIDs to assign to those KSs when you add them to the network.

You can reassign KSSIDs; however, if KSSIDs that are already used by a KS to distribute GMSIDs are removed from the KS, the group will reinitialize (meaning that all GMs will be forced to re-register, and TEK IPsec SAs will be rekeyed to reset the used KSSIDs) without traffic loss. To avoid this group reinitialization, use the guidelines in the following table (which uses the default group size of medium):

Table 4: Recommended KSSID Assignment Ranges for Cooperative KSs (Group Size Medium)

	1 KS (no cooperative KSs)	2 cooperative KSs	3 cooperative KSs	4 cooperative KSs
KS1	0 - 127	0 - 63	0 - 31	0 - 15
KS2	—	64 - 127	32 - 63	16 - 31
KS3	—	—	64 - 95	32 - 47
KS4	—	—	96 - 127	48 - 64
KS5	—	—	—	65 - 80
KS6	—	—	—	81 - 95
KS7	—	—	—	96 - 112
KS8	—	—	—	113 - 127

If you plan to expand the cooperative KS network to include more KSs, when initially configuring the original KS (or KSs), use the column in the above table with the planned number of KSs in the *expanded* network so that the new KS or KSs can be added later.

Following are additional guidelines for assigning KSSIDs to KSs:

- Configure only contiguous blocks of KSSIDs across KSs (for example, KS1 = 0-9 + 40-49, KS2 = 10-19 + 50-59, KS3 = 20-29, KS4 = 30-39, and so on).
- Any one KS should have enough KSSID space to receive all GM registrations from the group (in case the other KSs fail all of their GM registrations).
- To avoid reinitialization of the group, only add new KSSID values or ranges; do not remove them unless necessary.
- During a network split (a connectivity loss among cooperative KSs), do not change the KSSID assignment; this prevents overlapping KSSIDs, which would cause reinitialization on a merge (when connectivity has been restored among cooperative KSs).
- If the group begins in an *n*-way split (meaning that secondary KSs are planned but not yet configured), configure all of the KSSIDs as if the group was not split.

The number of KSSIDs available depends on the group size configuration as in the following table:

Table 5: Ranges of Available KSSIDs Based on Group Size

Configured Group Size	Number of Available KSSIDs
Small (8-bit)	0 to 1
Small (12-bit)	0 to 3
Small (16-bit)	0 to 15
Medium	0 to 127
Large	0 to 511

Group Reinitialization

Group reinitialization is the process of retiring KSSIDs. Group reinitialization occurs across all KSs (primary and secondary). Any KS can trigger a group reinitialization, and it occurs whenever

- You change the TEK policy from non-GCM to GCM.
- You change the group size.
- You remove a previously used KSSID.
- A KS in the group runs out of both KSSIDs and GMSIDs.
- A KSSID overlap that was detected by a cooperative KS is resolved.

During reinitialization, all KSs move their used KSSIDs to old (used) KSSIDs (and they are thus retired). Then, reinitialization creates a new KEK and new TEKs, lowers the existing TEK lifetime, and deletes the existing TEKs to cause all GMs to re-register (within the window determined by the **clear crypto gdoi ks members** command). This window is five percent of the remaining lifetime, between 90 seconds and one hour. When the lifetime of the existing TEKs has expired, each KS resets its old (used) KSSIDs, then all KSSIDs are available for use once again.

Reinitialization does not cause traffic disruption on the GMs. All GMs receive new GMSIDs with new TEKs when re-registering.

Cisco GET VPN System Logging Messages for Suite B

The tables below explain the GET VPN system logging (also called syslog) messages that are related to Suite B.

Table 6: KS and Cooperative KS Messages

Message	Explanation
%GDOI-5-KS_REINIT_GROUP: *reason* for group *group-name* and will re-initialize the group.	The KS will reinitialize the group. The possible *reason* strings are as follows: • KS configured Suite-B transform requiring SIDs • KS configured Suite-B transform requiring SIDs during scheduled rekey • KS is running out of SIDs • KS changed Group Size • KS removed used KSSIDs • KS issued 'clear crypto gdoi ks members' • KS issued re-init test cmd • KSSID overlap was resolved • Pri KS peer changed used Group Size • Pri KS peer sent re-init request • Sec KS peer sent re-init request
%GDOI-5-KS_REINIT_FINISH: Re-initialization of group *group-name* completed.	Reinitialization for the group is complete. It is useful to know when a reinitialization has completed, because some operations are blocked during a reinitialization (such as when the group size is changed and used KSSIDs are removed). A reinitialization does not finish until the old (used) TEK is cleared, which might not occur until a reinitialization is checked again (for example while a **show** command is executing, while a group size or KSSIDs are being configured, or when a cooperative KS is being updated) or until the next GM registers.
%GDOI-3-KS_NO_SID_AVAILABLE: GMs for group *group-name* need SIDs but this KS has no KS SIDs configured or no more SIDs available.	(When using GCM and after a GM begins registration) GMs for the group need SIDs, but either the KS has no KSSIDs configured or has no more SIDs available.

Message	Explanation
%GDOI-3-COOP_KS_KSSID_OVERLAP: Overlapping KS Sender Identifier(s) (KSSID) {*KSSID*|*KSSID-Range*} with COOP-KS peer *ip-address* in group *group-name* blocking GM registration (MISCONFIG).	A KSSID or KSSID range that overlaps with a cooperative KS peer in another group is blocking GM registration. An overlapping KSSID configuration is blocked on cooperative KSs by the CLI, but it might occur in a GET VPN network split scenario (in which one or more cooperative KSs were temporarily unavailable but have come back online) or with saved configurations.
%GDOI-5-COOP_KS_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID) with COOP-KS peer allowing GM registrations once again.	A KSSID that overlaps with a cooperative KS peer was resolved (which allows GM registrations to resume).

Table 7: GM Messages

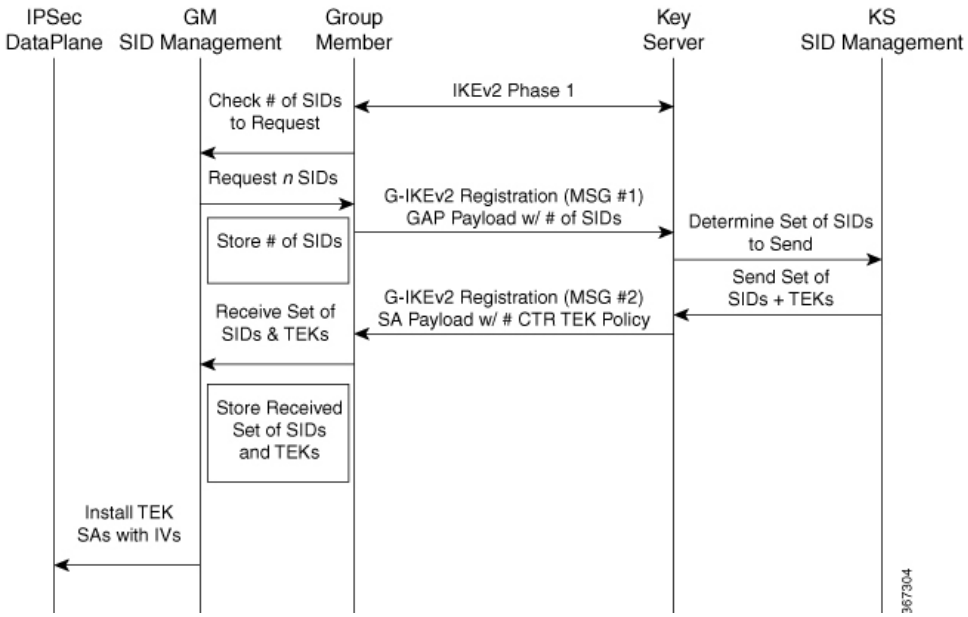
Message	Explanation
%GDOI-5-GM_IV_EXHAUSTED: GM for group *group-name* exhausted its IV space for interface *interface-name* and will re-register.	The GM for the group exhausted its IV space (meaning its set of unique IVs) for a particular SA and will re-register.
%GDOI-5-GM_REJECTING_SA_PAYLOAD: Registration: Policy in SA payload sent by KS *ip-address* rejected by GM in the group *group-name* reason: client rekey hash algorithm (*kek-policy*) is unacceptable by this GM.	The client rekey hash algorithm (the specified KEK policy) was not accepted by a GM in the specified group. At registration, the GM rejected the KEK policy.
%GDOI-5-GM_REJECTING_SA_PAYLOAD: Registration: Policy in SA payload sent by KS *ip-address* rejected by GM in the group *group-name* reason : client rekey transform-sets (*tek-policy*) for data-protection are unacceptable by this GM.	The client rekey transform sets (the specified TEK policy) for data protection was not accepted by the GM. At registration, the GM rejected the TEK policy.
%GDOI-5-GM_REKEY_TRANSFORMSET_CHECK_FAIL: The transform set (*transform-set*) for data protection in group *group-name* is unacceptable by this client.	The transform set for data protection in the group was not accepted by the client. The GM received a rekey and rejected the TEK policy.
%GDOI-3-KS_REKEY_AUTH_KEY_LENGTH_INSUFFICIENT: Rejected rekey sig-hash algorithm change: using sig-hash algorithm HMAC_AUTH_SHA*bits* requires an authentication key length of at least *number-of-bits* bits (*number-of-blocks* blocks in bytes) - current RSA key "360-bit" is only 45 blocks in bytes.	Configuration of the rekey signature hash algorithm was rejected, because the RSA key did not have a long enough modulus. HMAC-SHA-384 requires a modulus of at least 465 bits (59 blocks in bytes), and HMAC-SHA-512 requires a modulus of 593 bits (75 blocks in bytes).

Suite B and G-IKEv2

The Ability to use Suite B Algorithms with GIKEv2 with registration interface feature provides support for Suite B on GET VPN G-IKEv2 enabled networks.

The following figure explains the message exchanges between a group member and a key server on GET VPN network enabled with the Ability to use Suite B Algorithms with GIKEv2 with registration interface feature.

Figure 1: Message Exchanges between GM and KS



1. After an IKEv2 session is set up, GM determines the number of SIDs to be requested and sends a registration message to key server via Notify payload requesting the number of SIDs required by group member. At this point, the GM is not aware of the configured lifetime of the TEK SA when requesting SIDs. GM includes the SENDER_ID_REQUEST attribute in the message, irrespective of a CTR transform configuration.
2. KS accepts the Notify payload containing SENDER_ID_REQUEST attribute in the registration message and sends SA payload to GM.
3. If the **crypto ipsec transform-set** command is configured, key server sends KD payload containing the number of requested SIDs. If the **crypto ipsec transform-set** command is not configured, key server will not send SIDs, even though GM requests for SIDs.

Note If no SIDs are requested and if the **crypto ipsec transform-set** command is configured, the KS will send one SID, which is the default SID value.

Working of a Group Member with Suite B and G-IKEv2

GM must receive and install SIDs after a successful registration. To support Suite-B with G-IKEv2, a GM must do the following:

- Send Notify payload during GM registration requesting a number of SIDs.
- Determine the number of SIDs required based on the number of client registration interfaces to which crypto map is applied on GM.
- Receive KD payload from KS. KD payload contains SIDs sent from KS.
- Install TEK SAs with one or more SIDs. The number of SIDs + initial SSIV = IV.
- Reregister when SSIV exhausts, when no SIDs exist.

IPsec installs the SAs after receiving TEK SA with IV values in the KMI message from G-IKEv2 to IPsec.

Working of a Key Server with Suite B and G-IKEv2

To support Suite-B with G-IKEv2, KS must do the following:

- Receive and process Notify payload from GM during registration.
- If Notify payload is not received and the **crypto ipsec transform-set** command is configured, assign one unique SID to each GM.
- After receiving the SID request, the number of SIDs sent to GM is calculated based on the configured TEK SA lifetime.
- If SA lifetime is less than or equal to 1 day (86400 seconds), the number of SIDs that KS sends to GM will be calculated as follows:

  Number of SIDs KS sends = Number of SIDs GM requested
- If SA lifetime is more than 1 day, the number of SIDs that KS sends to GM will be calculated as follows. SIDs are specific to SA lifetime:

  Number of SIDs = Number of SIDs requested by GM * ceil (configured SA lifetime in KS/ 86400)
- SIDs are divided among the available crypto map interfaces and sent to GM via KD payload.

The following is a sample output of the **show gdoi gm identifier detail** command that displays the SID distribution if SA lifetime is greater than 1 day:

```
Device# show cry gdoi gm identifier detail

GM Sender ID (SID) Information for Group GKM-GROUP-KS_KDN:

  Group Member: 10.10.10.2       vrf: None
    Transform Mode                  : Counter (Suite-B)
    # of SIDs Last Requested        : 3

    CURRENT SIDs:
      Shared Across Interfaces?     : No
      SID Length (Group Size)       : 24 bits (MEDIUM)
      # of SIDs Downloaded          : 6
      First SID Downloaded          : 0x00000001
      Last SID Downloaded           : 0x00000006
```

```
  CM Interface       Packets / Sec   # Req # Rx   Installed SID Range
  ================== =============== ===== ====== ======================
  Ethernet0/0        16842           1     2      0x00000001 - 0x00000002
  Ethernet0/1        16842           1     2      0x00000003 - 0x00000004
  Ethernet0/2        16842           1     2      0x00000005 - 0x00000006

NEXT SID REQUEST:
  TEK Lifetime                  : 86453 sec
  SID Length (Group Size)       : 24 bits (MEDIUM)
```

How to Configure GET VPN Support with Suite B

Each feature in the GET VPN Support with Suite B feature set is independently configurable. But to be compliant with the Suite B standard, you must configure certain combinations of these features. For more information about these combinations, see RFC 4869, Suite B Cryptographic Suites for IPsec .

Ensuring that GMs Are Running Software Versions That Support Suite B

Because GET VPN is a technology that is based on groups, all devices in the same group (including the primary KS, cooperative KSs, and GMs) must support the Suite B feature before you can enable the feature. If you want to enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software.

To ensure that all devices in the GET VPN network support Suite B, perform the following steps on the KS (or primary KS).

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi feature suite-b**
3. **show crypto gdoi feature suite-b | include No**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi feature suite-b** **Example:** `Device# show crypto gdoi feature suite-b`	Displays the version of the GET VPN software running on each KS and GM in the network and displays whether that device supports Suite B.
Step 3	**show crypto gdoi feature suite-b | include No** **Example:**	(Optional) Finds only those devices that do not support Suite B.

	Command or Action	Purpose
	`Device# show crypto gdoi feature suite-b | include No`	

Configuring a Key Server for GET VPN Suite B

Configuring the Signature Hash Algorithm for the KEK

Perform this task to configure the signature hash algorithm for the KEK.

Before you begin

This task has the following prerequisites:

- Make sure that rekey authentication that is using an RSA key pair associated with the device is enabled. To do so, use the **rekey authentication** command with the **mypubkey rsa** *key-name* keywords and argument.
- Make sure that the RSA key pair has a modulus of sufficient length. HMAC-SHA-384 requires a modulus of at least 465 bits (59 blocks in bytes), and HMAC-SHA-512 requires a modulus of 593 bits (75 blocks in bytes). If the rekey signature hash algorithm is changed to SHA-384 or SHA-512 with a key pair of insufficient modulus length, a configuration rejection message appears on the console, and system logging messages are generated. Similarly, if the rekey signature hash algorithm is already SHA-384 or SHA-512 and the key pair is modified to one of insufficient modulus length, a similar message appears on the console, and the same system logging messages are generated.
- To use SHA-2/HMAC-SHA-2 for authentication of the *acknowledgment* from GMs to KSs after receiving a rekey message, you must enable unicast distribution of rekey messages to GMs. To do so, use the **rekey transport unicast** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. **server local**
5. **rekey sig-hash algorithm** *algorithm*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gdoi group mygroup`	Identifies a GDOI group and enters GDOI group configuration mode. • If you are using GET VPN over IPv6 in the data plane, you must use the **ipv6** keyword.
Step 4	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI KS and enters GDOI local server configuration mode.
Step 5	**rekey sig-hash algorithm** *algorithm* **Example:** `Device(gdoi-local-server)# rekey sig-hash algorithm sha512`	Configures the signature hash algorithm for the KEK. For Suite B, you must specify **sha256**, **sha384**, or **sha512**.
Step 6	**end** **Example:** `Device(gdoi-local-server)# end`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.

Configuring the Group Size

This task is optional. For nearly all deployments, the default group size (sender identifier length) of medium is recommended. Perform this task to configure the group size for Suite B.

When you change the group size in a group with cooperative KSs after Suite B (meaning ESP-GCM or ESP-GMAC) is configured and after the Suite B policy has been generated, you must change the group size on all secondary KSs before changing it on the primary KS.

Changing the group size causes the group to reinitialize (so that the new SID length can be used). Conflicting group size configurations across KSs will block GM registration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. **server local**
5. **group size** {**small** {**8** | **12** | **16**} | **medium** | **large**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gdoi group mygroup`	Identifies a GDOI group and enters GDOI group configuration mode. • If you are using GET VPN over IPv6 in the data plane, you must use the **ipv6** keyword.
Step 4	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI KS and enters GDOI local server configuration mode.
Step 5	**group size** {**small** {**8** | **12** | **16**} | **medium** | **large**} **Example:** `Device(gdoi-local-server)# group size small 16`	Configures the group size.
Step 6	**end** **Example:** `Device(gdoi-local-server)# end`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.

Configuring Key Server Identifiers

Suite B requires the assignment of unique GMSIDs to each GM, which means that a GM cannot reuse a previously used SID (either from itself or another GM) for the same key. Therefore, although GET VPN is designed to disallow overlapping SID values, you should correctly configure KSSID values among KSs so that each KS has a unique set. (KSSID overlap among KSs will cause a reinitialization.)

You must configure at least one unique KSSID to allot a pool of SIDs to the KS. You do so on the KS before configuring GCM or GMAC as the TEK IPsec policy.

Perform this task to assign a KSSID or a range of KSSIDs to a KS. Each KS must be assigned at least one KSSID when using GCM or GMAC. You can configure a single KSSID, a range of KSSIDs, or both. For the default group size of medium, there are 128 possible KSSID values in the range from 0 to 127.

KSSID values are not assigned to (and usable by) the KS until you exit GDOI local server ID configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. **server local**
5. **identifier**
6. **range** *lowest-kssid* **-** *highest-kssid*
7. **value** *kssid*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gdoi group mygroup`	Identifies a GDOI group and enters GDOI group configuration mode. • If you are using GET VPN over IPv6 in the data plane, you must use the **ipv6** keyword.
Step 4	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI KS and enters GDOI local server configuration mode.
Step 5	**identifier** **Example:** `Device(gdoi-local-server)# identifier`	Enters GDOI local server ID configuration mode.
Step 6	**range** *lowest-kssid* **-** *highest-kssid* **Example:** `Device(gdoi-local-server-id)# range 10 - 20`	Assigns a range of KSSIDs. • This range must be unique in the entire group.

	Command or Action	Purpose
Step 7	**value** *kssid* **Example:** `Device(gdoi-local-server-id)# value 0`	Assigns a KSSID. • This KSSID must be unique in the entire group. • The **value 0** command allots the pool of SIDs to the KS that begin with KSSID value 0 (meaning that it is allotted the pool of SID values beginning with 0x0 and ending with 0x1FFFF).
Step 8	**end** **Example:** `Device(gdoi-local-server-id)# end`	Exits GDOI local server ID configuration mode and returns to privileged EXEC mode.

If you try to configure one or more KSSIDs on a KS that are already assigned to another KS (and the cooperative KS network is not split), the configuration is denied, and the following message appears when you exit GDOI local server ID configuration mode:

```
% Key Server SID Configuration Denied:
%   The following Key Server SIDs being added overlap:
%   2, 200-250  (COOP-KS Peer: 10.0.9.1)
```

If the cooperative KS network *is* split, you should not configure overlapping KSSIDs. If overlapping KSSIDs are detected on a network merge, GM registration is blocked until the overlap is resolved. The following system logging message appears on both KSs:

```
%GDOI-3-COOP_KSSID_OVERLAP: Overlapping KS Sender Identifier(s) (KSSID) {2, 200-250} with
COOP-KS peer 10.0.9.1 in group diffint blocking GM registration (MISCONFIG)
```

When a KS unconfigures the overlapping KSSIDs, the group reinitializes (meaning that all GMs are forced to re-register, and TEK IPsec SAs are rekeyed to reset the used KSSIDs) without traffic loss. The following system logging messages appear on the KS:

```
%SYS-5-CONFIG_I: Configured from console by console
%GDOI-5-COOP_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID)
with COOP-KS peer allowing GM registrations once again
%GDOI-5-KS_REINIT_GROUP: KSSID overlap was resolved for group diffint and will re-initialize
 the group.
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group diffint from address 10.0.8.1
 with seq # 11
%GDOI-4-GM_DELETE: GM 10.0.3.1 deleted from group diffint.
%GDOI-4-GM_DELETE: GM 10.65.9.2 deleted from group diffint.
```

The %GDOI-5-KS_SEND_UNICAST_REKEY system logging message appears only if this is the primary KS. The peer KS that had overlapping KSSIDs also displays the %GDOI-5-COOP_KSSID_OVERLAP_RESOLVED system logging message.

Configuring the IPsec SA for Suite B

To configure the IPsec SA for Suite B, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**]
4. **crypto ipsec profile** *ipsec-profile-name*
5. **set transform-set** *transform-set-name*
6. **exit**
7. **crypto gdoi group** [**ipv6**] *group-name*
8. Enter one of the following commands:
   - **identity number** *number*
   - **identity address ipv4** *address*
9. **server local**
10. **sa ipsec** *sequence-number*
11. **profile** *ipsec-profile-name*
12. **match address** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*}
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec transform-set** *transform-set-name* {**esp-gcm**	**esp-gmac**} [**128**	**192**	**256**] **Example:** `Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	Defines a transform set—an acceptable combination of security protocols and algorithms—and enters crypto transform configuration mode. • For Suite B, you must specify a transform set using ESP-GCM or ESP-GMAC. (You can define multiple transform sets by entering the command again on separate command lines.) • You can optionally specify a key size of 128, 192, or 256. The default key size is 128.
Step 4	**crypto ipsec profile** *ipsec-profile-name* **Example:** `Device(config)# crypto ipsec profile profile1`	Defines the IPsec profile (the parameters to be used for IPsec encryption between two IPsec routers) and enters IPsec profile configuration mode.

	Command or Action	Purpose
Step 5	**set transform-set** *transform-set-name* **Example:** `Device(ipsec-profile)# set transform-set transformset1`	Specifies which transform sets can be used with the crypto map entry.
Step 6	**exit** **Example:** `Device(ipsec-profile)# exit`	Exits IPsec profile configuration mode.
Step 7	**crypto gdoi group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gdoi group gdoigroupname`	Identifies a GDOI group and enters GDOI group configuration mode. • If you are using GET VPN over IPv6 in the data plane, you must use the **ipv6** keyword.

Step 8	Enter one of the following commands:
	• **identity number** *number*
	• **identity address ipv4** *address*
	Example:
	`Device(config-gdoi-group)# identity number 3333`
	Example:
	`Device(config-gdoi-group)# identity address ipv4 209.165.200.225`
		Identifies a GDOI group number or address.
		• The **identity number** *number* command applies to IPv4 and IPv6 configurations.
		• The **identity address ipv4** *address* command applies only to IPv4 configurations.

Step 9	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI KS and enters GDOI local server configuration mode.
Step 10	**sa ipsec** *sequence-number* **Example:** `Device(gdoi-local-server)# sa ipsec 1`	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.
Step 11	**profile** *ipsec-profile-name* **Example:** `Device(gdoi-sa-ipsec)# profile gdoi-p`	Defines the IPsec SA policy for a GDOI group.
Step 12	**match address** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*} **Example:** `Device(gdoi-sa-ipsec)# match address ipv4 102`	Selects an IP extended access list (ACL) for a GDOI registration. • You must use the **ipv4** keyword for IPv4 groups and the **ipv6** keyword for IPv6 groups.

	Command or Action	Purpose

		• You must use a named (not numbered) access list for IPv6 configurations.
		
		Note Make sure that you select an ACL that has identical entries in the identical order among all the cooperative KSs for the group. If not, GMs that register to separate KSs cannot encrypt and decrypt correctly after downloading the policy.
		
		Note If you attempt to assign an IPv6 group with IPv4 policies, an error message appears indicating that the access list name is invalid, or the list already exists but is the wrong type:
		`Access-list type conflicts with prior definition`
		`% ERROR: access-list-name is either an invalid name or the list already exists but is the wrong type.`

Step 13	**end** **Example:** `Device(gdoi-sa-ipsec)# end`	Exits GDOI SA IPsec configuration mode and returns to privileged EXEC mode.

Configuring a Group Member for GET VPN Suite B

Configuring Acceptable Ciphers or Hash Algorithms for KEK for Suite B

To configure the Suite B ciphers and hash algorithms for KEK to be allowed by the GM, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. Enter one of the following commands:
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*
6. **client rekey encryption** *cipher* [... [*cipher*]]
7. **client rekey hash** *hash*

8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gdoi group gdoigroupone`	Identifies a GDOI group and enters GDOI group configuration mode. • If you are using GET VPN over IPv6 in the data plane, you must use the **ipv6** keyword.

Step 4	Enter one of the following commands:
	• **identity number** *number*
	• **identity address ipv4** *address*
	Example:
	`Device(config-gdoi-group)# identity number 3333`
	Example:
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		Identifies a GDOI group number or address.

Step 5	**server address ipv4** *address* **Example:** `Device(config-gdoi-group)# server address ipv4 10.0.5.2`	Specifies the address of the server that a GDOI group is trying to reach. • To disable the address, use the **no** form of the command.
Step 6	**client rekey encryption** *cipher* [... [*cipher*]] **Example:** `Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256`	Sets the client acceptable rekey ciphers for the KEK.
Step 7	**client rekey hash** *hash* **Example:** `Device(config-gdoi-group)# client rekey hash sha384`	Sets the client acceptable hash algorithm for KEK. • For Suite B, you must specify either **sha256**, **sha384**, or **sha512**.

	Command or Action	Purpose
Step 8	**end** **Example:** `Device(config-gdoi-group)# end`	Exits GDOI group configuration mode and returns to privileged EXEC mode.

Configuring Acceptable Transform Sets for TEKs for Suite B

To configure the transform sets used by TEKs for data encryption or authentication to be allowed by the GM, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**]
4. **exit**
5. **crypto gdoi group** [**ipv6**] *group-name*
6. **client transform-sets** *transform-set-name1* [... [*transform-set-name6*]]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**] **Example:** `Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	Defines a transform set—an acceptable combination of security protocols and algorithms—and enters crypto transform configuration mode. • For Suite B, you must specify a transform set using ESP-GCM or ESP-GMAC. • You can define multiple transform sets by entering the command again on separate command lines. • You can optionally specify a key size of 128, 192, or 256. The default key size is 128.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(cfg-crypto-trans)# exit`	Exits crypto transform configuration mode.
Step 5	**crypto gdoi group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gdoi group gdoigroupone`	Identifies a GDOI group and enters GDOI group configuration mode. • If you are using GET VPN over IPv6 in the data plane, you must use the **ipv6** keyword.
Step 6	**client transform-sets** *transform-set-name1* [... [*transform-set-name6*]] **Example:** `Device(config-gdoi-group)# client transform-sets g1`	Specifies the acceptable transform-set tags used by TEKs for data encryption and authentication. • You can specify up to six transform-set tags.
Step 7	**end** **Example:** `Device(config-gdoi-group)# end`	Exits GDOI group configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting GET VPN Support with Suite B

Verifying and Troubleshooting GET VPN Support with Suite B on a Key Server

To view the configuration that is running on a KS, use the **show running-config** command.

SUMMARY STEPS

1. **show crypto gdoi ks identifier** [**detail**]
2. **show crypto gdoi ks coop identifier** [**detail**]
3. **show crypto gdoi feature suite-b**
4. **show crypto gdoi ks policy**

DETAILED STEPS

Step 1 **show crypto gdoi ks identifier** [**detail**]

Example:

```
Device# show crypto gdoi ks identifier detail

KS Sender ID (KSSID) Information for Group diffint:

    Transform Mode           : Counter (Suite B)
    reinitializing          : No
```

```
SID Length (Group Size)  : 24 bits (medium)
Current KSSID In-Use     : 0
Last GMSID Used          : 1

KSSID (or SIDS)Assigned        : 0-15
KSSID (or SIDS)Used            : 0
KSSID (or SIDS) Used  (Old)      : none
Available KSSID (or SIDS): 1-15

REMAINING SIDs:
  KSSID to reinitialize at         : 15
  GMSID to reinitialize at         : 6291456
  # of SIDs Remaining for Cur KSSID : 8388606
  # of SIDs Remaining until Re-init : 132120575
```

This command displays the status of SID management for Suite B. The Transform Mode field can be either Non-Counter (Non-Suite B) or Counter (Suite B) to check if SID management and a Suite B policy is currently used in the group. If the group is currently reinitializing (meaning that all GMs will be forced to re-register, and TEK IPsec SAs will be rekeyed to reset the used KSSIDs), then the reinitializing field displays Yes. The SID Length (Group Size) field determines the group size currently used in the group, which defaults to 24 bits (medium).

The Current KSSID In-Use and Last GMSID Used fields correspond to the SID (or SIDS) to be distributed to the next registering GM. The KSSID (or SIDS) Assigned field corresponds to the locally configured KSSIDs that have been synced with cooperative KSs, and the Available KSSID (or SIDS) field corresponds to those KSSIDs that have not been used yet since the last reinitialization. Each time a new KSSID is used, it is added to the KSSID (or SIDS) Used field, and during a reinitialization, those used KSSIDs are transferred to the KSSID (or SIDS) Used (Old) field. At the end of a reinitialization period, the old used KSSIDs are cleared and put in the Available KSSIDs pool again.

Note When the value in the # of SIDs Remaining until Re-init field approaches 0, a reinitialization will occur soon if GMs are continuing to re-register. Although a reinitialization should not cause traffic disruption or network problems, it will cause all GMs to re-register.

Step 2 **show crypto gdoi ks coop identifier** [**detail**]

Example:

```
Device# show crypto gdoi ks coop identifier detail

COOP-KS Sender ID (SID) Information for Group diffint:

    Local KS Role: Primary   , Local KS Status: Alive
        Local Address                : 10.0.8.1
        Next SID Client Operation    : NOTIFY
        reinitializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (medium)
        SID Length (Group Size) Used : 24 bits (medium)
        Current KSSID In-Use         : 0
        KSSID (or SIDS)Assigned            : 0-15
        KSSID (or SIDS)Used                : 0
        Old KSSID (or SIDS)Used            : none

    Peer KS Role:  Secondary , Peer KS Status:  Alive
        Peer Address                 : 10.0.9.1
        Next SID Client Operation    : NOTIFY
        reinitializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (medium)
        SID Length (Group Size) Used : 24 bits (medium)
```

```
        Current KSSID In-Use         : 16
        KSSID (or SIDS)Assigned            : 16-31
        KSSID (or SIDS)Used                : 16
        Old KSSID (or SIDS)Used            : none
```

This command displays the status of SID information that is synchronized across cooperative KSs.

When the KSSID Overlap field displays Yes, GM registration is blocked until the overlap of KSSIDs (which could have happened during a network split) is resolved. You must unconfigure the overlapping KSSIDs from one cooperative KS or the other before GM registration can resume. When the overlapping KSSIDs are resolved, a reinitialization occurs.

When you change the group size (not recommended for most deployments), all secondary KSs must first configure the new group size. Then on the primary KS, the SID Length (Group Size) Cfg field displays the new group size on all cooperative KS peers. Only when the primary KS configures the new group size will all KSs start to use the new group size and update the SID Length (Group Size) Used field to display the new group size.

Step 3 **show crypto gdoi feature suite-b**

Example:

```
Device# show crypto gdoi feature suite-b

Group Name: diffint
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.4          Yes
        10.0.9.1         1.0.4          Yes

    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.4          Yes
        10.0.4.1         1.0.4          Yes
```

This command displays whether KSs and GMs can use the Suite B feature set (meaning AES-GCM, AES-GMAC, SHA-2, and HMAC-SHA2). The Version field must display 1.0.4 or higher, and the Feature Supported field must display Yes for all KSs in the cooperative KS group and for the registered GMs.

Step 4 **show crypto gdoi ks policy**

Example:

```
Device# show crypto gdoi ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

  # of teks : 4  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0x80474E999FE8F60364B7F51809E28C84
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec): 86400       remaining life(sec): 85586
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x9C666FA7
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.1.1 host 239.0.1.1
```

```
  transform          : esp-gcm
  alg key size       : 20            sig key size          : 0
  orig life(sec)     : 900           remaining life(sec)   : 87
  tek life(sec)      : 900           elapsed time(sec)     : 813
  override life (sec): 0             antireplay window size: 64


TEK POLICY (encaps : ENCAPS_TUNNEL)
  spi                : 0x54E8D5D3
  access-list        : gcm-acl
  Selector           : permit ip host 10.0.100.2 host 238.0.1.1
  transform          : esp-gcm
  alg key size       : 20            sig key size          : 0
  orig life(sec)     : 900           remaining life(sec)   : 87
  tek life(sec)      : 900           elapsed time(sec)     : 813
  override life (sec): 0             antireplay window size: 64


TEK POLICY (encaps : ENCAPS_TUNNEL)
  spi                : 0xC8B4DE6D
  access-list        : gcm-acl
  Selector           : permit ip host 10.0.1.1 host 10.0.100.2
  transform          : esp-gcm
  alg key size       : 20            sig key size          : 0
  orig life(sec)     : 900           remaining life(sec)   : 87
  tek life(sec)      : 900           elapsed time(sec)     : 813
  override life (sec): 0             antireplay window size: 64


TEK POLICY (encaps : ENCAPS_TUNNEL)
  spi                : 0x1C908AF3
  access-list        : gcm-acl
  Selector           : permit ip host 10.0.100.2 host 10.0.1.1
  transform          : esp-gcm
  alg key size       : 20            sig key size          : 0
  orig life(sec)     : 900           remaining life(sec)   : 87
  tek life(sec)      : 900           elapsed time(sec)     : 813
```

This command displays whether a TEK and IPsec SA were generated per ACE (displayed in the Selector field) from the ACL in the access-list field for the ESP-GCM or ESP-GMAC TEK policy. This command also displays whether the KEK policy is using SHA-2/HMAC-SHA-2 as the signature hash algorithm.

Verifying and Troubleshooting GET VPN Support with Suite B on a GM

To view the configuration that is running on a GM, use the **show running-config** command.

SUMMARY STEPS

1. **show crypto gdoi gm identifier** [**detail**]
2. **show crypto gdoi feature suite-b**
3. **show crypto gdoi**

DETAILED STEPS

Step 1 **show crypto gdoi gm identifier** [**detail**]

Example:

```
Device# show crypto gdoi gm identifier detail

GM Sender ID (SID) Information for Group diffint:

  Group Member: 10.65.9.2        vrf: None
    Transform Mode                  : Counter (Suite B)
    # of SIDs Last Requested        : 3

    CURRENT SIDs:
      Shared Across Interfaces?     : Yes
      SID Length (Group Size)       : 24 bits (medium)
      # of SIDs Downloaded          : 3
      First SID Downloaded          : 0x08000007
      Last SID Downloaded           : 0x08000009

      CM Interface   B/W (Kbps) MTU (B)  # Req # Rx  Installed SID Range
      ============== ========== ======== ===== ===== ======================
      Et2/0          10000      1500     1     3     0x08000007 - 0x08000009
      Et3/0          10000      1500     1     3     0x08000007 - 0x08000009
      Et4/0          10000      1500     1     3     0x08000007 - 0x08000009

    NEXT SID REQUEST:
      TEK Lifetime                  : 900 sec
      SID Length (Group Size)       : 32 bits (LARGE)
```

This command displays the status of received and installed SIDs on a GM when it is using GCM-AES or GMAC-AES as the TEK IPsec SA policy. The Transform Mode field can display Non-Counter (Non-Suite B) or Counter (Suite B) to check whether SIDs are being downloaded and installed and whether a Suite B policy is used in the group. The # of SIDs Last Requested field mainly depends on the number of interfaces to which the crypto map is applied for this registered GM (meaning using the local-address or client registration interface). The SIDs are Shared Across Interfaces field when using local-address and each CM Interface's Installed SID Range field will be the same. You use this command mainly to verify that each CM interface has SIDs installed.

Step 2 **show crypto gdoi feature suite-b**

Example:

```
Device# show crypto gdoi feature Suite B

       Version    Feature Supported
        1.0.4           Yes
```

This command displays whether this GM can use the Suite B feature set (meaning GCM-AES, GMAC-AES, SHA-2, and HMAC-SHA-2). The Version field must display 1.0.4 or higher, and the Feature Supported field must display Yes.

Step 3 **show crypto gdoi**

Example:

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : diffint
    Group Identity           : 1234
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 10.0.8.1

    Group member             : 10.0.3.1         vrf: None
       Version               : 1.0.4
       Registration status   : Registered
       Registered with       : 10.0.8.1
.
.
.
ACL Downloaded From KS 10.0.8.1:
   access-list   permit ip host 10.0.1.1 host 239.0.1.1
   access-list   permit ip host 10.0.100.2 host 238.0.1.1
   access-list   permit ip host 10.0.1.1 host 10.0.100.2
   access-list   permit ip host 10.0.100.2 host 10.0.1.1

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 85740
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA256
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet3/0:
    IPsec SA:
        spi: 0x318846DE(831014622)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xF367AEA0(4083658400)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xE583A3F5(3850609653)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xE9AC04C(245022796)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
```

The presence of multiple IPsec SAs shows that GCM or GMAC is configured (note that each IPsec SA has a unique SPI for each ACE that was downloaded). For each ACE listed in the TEK POLICY for the current KS-Policy ACEs Downloaded

section, this command displays whether a TEK policy and IPsec SA were downloaded (and installed) from the ACLs that are listed in the ACL Downloaded From KS section. This command also displays whether the KEK policy is using SHA-2/HMAC-SHA-2 for the signature hash algorithm (for example, HMAC_AUTH_SHA256).

Configuration Examples for GET VPN Support with Suite B

Example: Ensuring that GMs Are Running Software Versions That Support Suite B

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support Suite B cryptography:

```
Device# show crypto gdoi feature suite-b

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) find only those devices in the GET VPN network that do *not* support Suite B:

```
Device# show crypto gdoi feature suite-b | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

Example: Configuring a Key Server for GET VPN Suite B

Configuring the Signature Hash Algorithm for the KEK

The following example shows how to configure the signature hash algorithm for the KEK:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey sig-hash algorithm sha512
Device(gdoi-local-server)# end
```

Configuring the Group Size for Suite B

Configuring the group size for Suite B is optional, because the default group size of medium is sufficient for most deployments. The following example shows how to configure the group size for Suite B:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# group size small 16
Device(gdoi-local-server)# end
```

Configuring Key Server Identifiers

The following example shows how to assign a KSSID as well as a range of KSSIDs to a KS:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# identifier
Device(gdoi-local-server-id)# range 10 - 20
Device(gdoi-local-server-id)# value 0
Device(gdoi-local-server-id)# end
```

Configuring the IPsec SA for Suite B

The following example shows how to configure the IPsec SA for Suite B. This example uses an identity number instead of an identity address:

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec transform-set g1 esp-gcm 192
Device(config)# crypto ipsec profile profile1
Device(ipsec-profile)# set transform-set transformset1
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group gdoigroupname
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p
Device(gdoi-sa-ipsec)# match address ipv4 102
```

```
Device(gdoi-sa-ipsec)# end
```

Example: Configuring a Group Member for GET VPN Suite B

Configuring Ciphers or Hash Algorithms for the KEK for Suite B

The following example shows how to configure the Suite B ciphers and hash algorithms for the KEK to be allowed by the GM. This example uses an identity address (compatible only with IPv4 data plane configurations). You could instead use an identity number (which would be compatible with IPv4 and IPv6 data plane configurations).

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group gdoigroupone
Device(config-gdoi-group)# identity address ipv4 10.2.2.2
Device(config-gdoi-group)# server address ipv4 10.0.5.2
Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256
Device(config-gdoi-group)# client rekey hash sha384
Device(config-gdoi-group)# end
```

Configuring Acceptable Transform Sets for TEKs for Suite B

The following example shows how to configure the acceptable transform sets used by TEKs for data encryption or authentication.

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec transform-set g1 esp-gcm 192
Device(cfg-crypto-trans)# exit
Device(config)# crypto gdoi group gdoigroupone
Device(config-gdoi-group)# client transform-sets g1
Device(config-gdoi-group)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command References*
IKE and IKE policy configuration tasks IPsec transform configuration tasks	"Configuring Internet Key Exchange for IPsec VPNs" module in the Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2M&T

Related Topic	Document Title
Basic deployment guidelines for enabling GET VPN in an enterprise network	Cisco IOS GET VPN Solutions Deployment Guide

Standards and RFCs

Standard/RFC	Title
Federal Information Processing Standard (FIPS) Publication 140-2	Security Requirements for Cryptographic Modules
RFC 2401	Security Architecture for the Internet Protocol
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4543	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
RFC 4869	Suite B Cryptographic Suites for IPsec
RFC 6054	Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic
RFC 6407	The Group Domain of Interpretation

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 GET VPN Support with Suite B

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 8: Feature Information for GET VPN Support with Suite B

Feature Name	Releases	Feature Information
Ability to use Suite B Algorithms with GIKEv2 with registration interface	Cisco IOS XE Fuji 16.8.1	The Ability to use Suite B Algorithms with GIKEv2 with registration interface feature provides support for Suite B on GET VPN G-IKEv2 enabled networks. In Cisco IOS XE Fuji 16.8.1, this feature supported the following devices: • Cisco ASR 1000 Series Aggregation Services Routers • ISR4461, ISR4451-X, ISR4431 The following command was modified: **show crypto gdoi**.

Feature Name	Releases	Feature Information
GET VPN Support with Suite B	Cisco IOS XE Release 3.10S	The GET VPN Support with Suite B feature adds support of the Suite B set of ciphers to Cisco Group Encrypted Transport (GET) VPN. Suite B is a set of cryptographic algorithms that includes Galois Counter Mode Advanced Encryption Standard (GCM-AES) as well as algorithms for hashing, digital signatures, and key exchange. Suite B for IP security (IPsec) VPNs is a standard whose usage is defined in RFC 4869. Suite B provides a comprehensive security enhancement for Cisco IPsec VPNs, and it allows additional security for large-scale deployments. Suite B is the recommended solution for organizations requiring advanced encryption security for the wide-area network (WAN) between remote sites. The following commands were introduced or modified: **client rekey hash, crypto key export ec, crypto key generate ec keysize, crypto key import ec, group size, identifier, rekey sig-hash algorithm, show crypto gdoi.**