GETVPN G-IKEv2

Cisco Group Encrypted Transport VPN (GET VPN) includes a set of features that are necessary to secure IP multicast group traffic or unicast traffic over an enterprise private WAN that originates on or flows through a Cisco device. The GETVPN G-IKEv2 feature implements Internet Key Exchange version 2 (IKEv2) protocol on GETVPN thereby allowing GETVPN to derive the benefits of IKEv2.

- Restrictions for GETVPN G-IKEv2, on page 1
- Information About GETVPN G-IKEv2, on page 1
- How to Configure GETVPN G-IKEv2, on page 8
- Additional References for GETVPN G-IKEv2, on page 12
- Feature Information for GETVPN G-IKEv2, on page 13

Restrictions for GETVPN G-IKEv2

- You can configure either Group Key Management (GKM) or Group Domain of Interpretation (GDOI) for a group member (GM), whereas you can configure both GKM and GDOI for a key server (KS).
- IKEv2 for COOP is not supported. Use IKEv1 for COOP between the key servers in the G-IKEv2 setup.
- EAP is not currently supported with G-IKEv2.
- GETVPN G-IKEv2 does not support IP-D3P. IP-D3P with G-IKEv2 is yet to be supported on GETVPN Group Members (GMs).

Information About GETVPN G-IKEv2

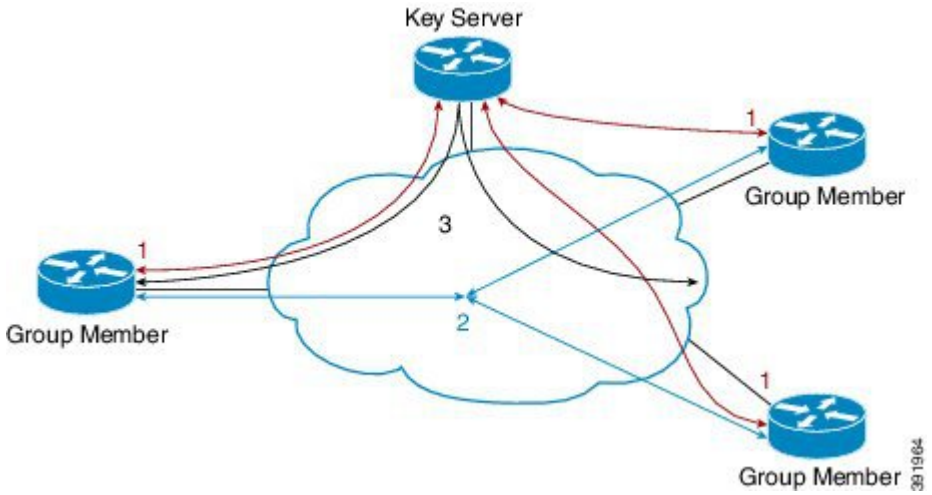
Overview of GETVPN G-IKEv2

Cisco Group Encrypted Transport Virtual Private Network (GETVPN) architecture is based on the Group Domain of Interpretation (GDOI) protocol. GETVPN uses Internet Security Exchange and Key Management Protocol (ISAKMP) to authenticate new group members, download cryptographic policy, and distribute traffic encryption key (TEK) and key encryption key (KEK) to group members. However, Internet Key Exchange Version 2 (IKEv2) has replaced. IKEv2 reduces network latency, reduces complexity in message exchanges, improves interoperability and reliability, and fixes cryptographic issue in HASH authentication. GET VPN combines IKEv2 protocol with IPsec to provide an efficient method to secure IP multicast traffic or unicast

traffic through the GETVPN G-IKEv2 feature. This feature provides a complete IKEv2 solution across all of Cisco's VPN technologies.

The G-IKEv2 protocol provides a mechanism for a group member (GM) to download policy and keys from a key server (KS). These policy and keys are used to secure communication among GMs in a group. G-IKEv2 is a new model to secure group communication between remote locations in an enterprise private WAN. The following figure depicts the basic system architecture of GETVPN using G-IKEv2 to register GM's with a KS and download keys and policy to GM's from a KS.

Figure 1: GETVPN Architecture through G-IKEv2 Protocol



Internet Key Exchange Version 2 (IKEv2)

Internet Key Exchange Version 2 (IKEv2), a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining security associations (SAs). For more information on IKEv2, see *FlexVPN and Internet Key Exchange Version 2 Configuration Guide*.

The following table compares the tunnel performance between IKE and IKEv2.

Protocol	Tunnels per Second	Maximum Simultaneous Tunnels
IKE	45	60
IKEv2	89	200

The benefits of IKEv2 are as follows:

Dead Peer Detection and Network Address Translation-Traversal

Internet Key Exchange Version 2 (IKEv2) provides built-in support for Dead Peer Detection (DPD) and Network Address Translation-Traversal (NAT-T).

Certificate URLs

Certificates can be referenced through a URL and hash, instead of being sent within IKEv2 packets, to avoid fragmentation.

Denial of Service Attack Resilience

IKEv2 does not process a request until it determines the requester, which addresses to some extent the Denial of Service (DoS) problems in IKEv1, which can be spoofed into performing substantial cryptographic (expensive) processing from false locations.

EAP Support

IKEv2 allows the use of Extensible Authentication Protocol (EAP) for authentication.

Multiple Crypto Engines

If your network has both IPv4 and IPv6 traffic and you have multiple crypto engines, choose one of the following configuration options:

- One engine handles IPv4 traffic and the other engine handles IPv6 traffic.
- One engine handles both IPv4 and IPv6 traffic.

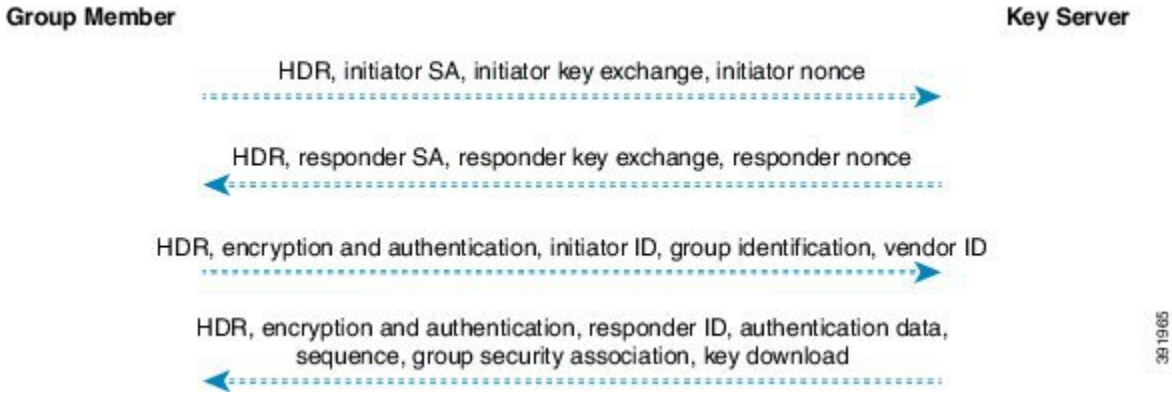
Reliability and State Management (Windowing)

IKEv2 uses sequence numbers and acknowledgments to provide reliability, and mandates some error-processing logistics and shared state management.

GETVPN G-IKEv2 Exchanges

The message exchanges between GM and KS conforms to the Internet Engineering Task Force (IETF) Group Key Management using IKEv2 Standards draft.

Figure 2: G-IKEv2 Message Exchanges



1. Group member initiates a registration request to key server by sending preferred cryptographic algorithms (in SAi payload), Diffie–Hellman public number, in initiator's key exchange (KE) phase 1 payload, and nonce, which is a random number for guaranteeing liveness in Initiator's nonce payload.
2. Key server responds with the negotiated cryptographic algorithm (in responder's SA phase 1 payload), Diffie–Hellman public number (in responder's KE payload), nonce (in responder's nonce payload). Optionally, if key server is configured to use Rivest, Shamir, and Adleman (RSA) digital signature as an authentication method, key server also sends a certificate request.

3. On receiving key server's response to the registration request, the group member uses the cryptographic algorithm in the SAr1 payload and Diffie–Hellman value to create keys and to encrypt the message sent to the key server. The encrypted message includes the initiator's ID and, optionally, certificate and certificate request, if RSA digital signature is used as authentication method. In case of Suite B implementations, a notify payload is sent for requesting sender IDs used with Galois/Counter Mode (GCM)–Advanced Encryption Standard (AES) or Galois Message Authentication Code (GMAC)–Advanced Encryption Standard (AES) transforms.

Note Group member requests a set of sender IDs applicable for interfaces for a lifetime of one day. After receiving the lifetime in a registration (for Long SA Lifetime) or a rekey (for Short SA Lifetime) message, group member stores the lifetime for calculating the number of sender IDs for future registrations.

4. After authenticating group manager, key server authorizes group member before registering group manager. After registration, key server sends the group's policy (in the GSA payload) and the group's keying material (in the KD payload) to group manager. The SEQ payload is optional and is sent when the key server wants to inform group manager of the current sequence number of the rekey message. These payloads are included in the GSA_AUTH response message.

Group Member Communication

Group members do not establish IPsec tunnels with one another, but use the IPsec policy and keys to secure communication between group members in a group.

Future Registrations

When a secure registration channel is established between group manager and key server, additional group member registrations for additional groups occurs through the established secure registration channel. In such scenario, group member uses the GSA_CLIENT_SERVER exchange that includes the group ID (IDg) to request either key encryption keys (KEK) or traffic encryption keys (TEKs) or both from key server.

Key Server Rekey

Key server distributes new group keys to group members using the G-IKEv2 group maintenance channel via unicast or multicast communication. Rekey is optional in G-IKEv2. When rekey is used, the KS sends a rekey message to group member. This message could be unicast or multicast depending on the key server configuration. Key server uses the KEK that is sent to the group member during registration to encrypt the rekey message. On receiving a rekey message, group member must ensure that the SEQ number in the rekey message is larger than the last received SEQ number. Group member could have received the SEQ number either via a registration message or a rekey message, whichever is later. If key server group is configured as both GDOI (IKEv1) and G-IKEv2 group, two rekey messages are sent—one over GDOI and another over G-IKEv2—for multicast rekey. In case of unicast rekey, key server only sends a GDOI or G-IKEv2 rekey depending on the group member's mode or type.

Note If the rekey is unicast, the group member must send an acknowledgment to key server.

Supported Features and GKM Version

The GETVPN G-IKEv2 feature supports the existing GETVPN features, which are as follows:

- Rekey and retransmission
- GM access control list (ACL)
- Fail-close mode
- Receive-only mode
- Anti-replay
- Authentication policy for group member registration
- GDOI MIBS
- VRF-Aware group member
- Group member removal and policy replacement
- Cooperative key server
- GETVPN IPv6 dataplane
- IPsec inline tagging support
- GETVPN resiliency phase 1 and phase 2
- Cooperative announcement message optimization

The GETVPN G-IKEv2 feature is supported in GKM version 1.0.12 and later releases. The supported GKM versions for a key server is 1.0.13 and a group member is 1.0.12. The difference between versions on a key server and a group member is because the IP D3P support on GETVPN Key Server and Internet-Draft ACK for Cisco GETVPN Key Server features are available on the key server from 1.0.13 only.

GDOI to G-IKEv2 Migration

Over a period of time, you may want to upgrade and migrate your key servers and group members to G-IKEv2. Migration from GDOI to G-IKEv2 for an entire GETVPN group requires careful planning. You cannot migrate all your group members at the same time. The migration entails allowing GDOI group members and G-IKEv2 group members to communicate using the same traffic encryption key (TEK) while using different control plane protocols—GDOI and G-IKEv2. A GDOI to G-IKEv2 migration sequence includes the following:

- Backward compatibility—The new Cisco IOS software image containing the GETVPN G-IKEv2 feature must support existing GDOI features and must be consistent with for earlier releases of GDOI features for Cisco IOS software.
- Service upgrade—The recommended sequence for changing the Cisco IOS software image is secondary key server, primary key server, and group member.
- Service downgrade—The recommended sequence for changing the Cisco IOS software image is group member, secondary key server, and primary key server.

Service Upgrade Procedure

1. Save the existing key server and group member GDOI configurations. For more information, see the "Configuration Replace and Configuration Rollback" feature module in the *Managing Configuration Files Configuration Guide*.
2. Configure a key encryption key (KEK) and a traffic encryption key (TEK) lifetime on all key servers to avoid network split and merge during the migration of the key servers. Use the crypto gdoi ks rekey command to configure the new lifetimes.
3. Upgrade key server to the new Cisco IOS software images. Follow the sequence mentioned above—start with the secondary key server followed by the primary key server. All existing configurations that use the keyword **gdoi** will be converted to the keyword **gkm**. For example, the global configuration command **crypto gdoi group** will be converted to **crypto gkm group** command. However, the groups continue to use GDOI for registration and rekey.
4. On key server, execute the **gikev2** command in the server local command for groups that support GDOI and G-IKEv2 group members.
5. Upgrade group members to the new Cisco IOS software image. All existing configurations that use the keyword "**gdoi**" will be converted to the keyword **gkm**. For example, the global configuration commands **crypto gdoi group** and **crypto map gdoi** will be converted to "**crypto gkm group**" and **crypto map gkm** respectively. These groups continue to use GDOI for registration and rekey and include the **client protocol gdoi** command.
6. Configure the **client protocol gikev2** command to use G-IKEv2 on group member.
7. Configure the **no gdoi** command in the server local command, to stop servicing GDOI group members.

For a group member to use GDOI after upgrading to G-IKEv2, configure the **client protocol gdoi** command in the group member group configuration. Group member registers again with key server using GDOI instead of G-IKEv2.

Note Before you convert group member, ensure that key server to which group member is registered is configured with the gdoi command in GDOI local server configuration mode.

Service Downgrade Procedure

Use the previously saved GDOI configurations (saved before upgrade procedure) and downgrade the Cisco IOS software for each group member. Next, downgrade the key server; beginning with the secondary key server followed by primary key server. For more information, see the "Configuration Replace and Configuration Rollback" feature module in the *Managing Configuration Files Configuration Guide*.

Migration Examples

This section provides examples on GDOI to G-IKEv2 migration. The following examples show how the GDOI group g1 is converted to a GKM group after upgrading to a G-IKEv2 Cisco IOS software image. The following is a sample key server configuration before Cisco IOS software upgrade.

```
crypto gdoi group g1
 identity 1111
 server local
  .
```

```
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

The following is a sample key server configuration after Cisco IOS software upgrade. In this example, the commands **gdoi**, **no gikev2**, and **gikev2** are automatically added. The **gikev2** command starts accepting G-IKEv2 registrations.

```
crypto gkm group g1
 identity 1111
 server local
  gdoi
  no gikev2
  gikev2 ikev2_profile1
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

The following is a sample group member configuration before Cisco IOS software upgrade.

```
crypto gdoi group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2

crypto map GETVPN_CM 10 gdoi
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

The following is a sample group member configuration after Cisco IOS software upgrade. In this example, the commands **client protocol gdoi** and **client protocol gikev2** are automatically added. The **client protocol gikev2** command starts using G-IKEv2.

```
crypto gkm group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2
 client protocol gdoi
 client protocol gikev2 ikev2_profile1 ] – Configure this to start using G-IKEv2

crypto map GETVPN_CM 10 gdoi
 set group g1
```

```
interface g0/0/0
 crypto map GETVPN_CM
```

GETVPN G-IKEv2 Configuration

All GETVPN commands—EXEC and global configuration commands—include the keyword **gdoi**. G-IKEv2 does not include the Domain of Interpretation, therefore, a generic abbreviation **gkm** referring to Group Key Management is used for a group that can use either GDOI or G-IKEv2 protocols for registration and rekey. As of now, both commands **crypto gdoi** and **crypto gkm** are available. However, the **GDOI** keyword will be deprecated and replaced by the **gkm** keyword in future. For example, to configure a key server group, the GDOI command is **crypto gdoi group** *group-name*, whereas the GKM command would be **crypto gkm group** *group-name*.

How to Configure GETVPN G-IKEv2

Configuring an IKEv2 Profile

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
5. **identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*}
6. **keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
7. **match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}
8. **pki trustpoint** *trustpoint-label* [**sign** | **verify**]
9. **end**

DETAILED STEPS

Procedure

	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 ikev2 profile** *profile-name* **Example:** `Device(config)# crypto ikev2 profile gkm-gikev2`	Defines an IKEv2 profile and enters IKEv2 profile configuration mode.
Step 4	**authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}} **Example:** `Device(config-ikev2-profile)# authentication local ecdsa-sig`	Specifies the local or remote authentication method. • **rsa-sig**—Specifies RSA-sig as the authentication method. • **pre-share**—Specifies the preshared key as the authentication method. • **ecdsa-sig**—Specifies ECDSA-sig as the authentication method. • **eap**—Specifies EAP as the remote authentication method. • **query-identity**—Queries the EAP identity from the peer. • **timeout** *seconds*—Specifies the duration, in seconds, to wait for the next IKE_AUTH request after sending the first IKE_AUTH response. **Note** You can specify only one local authentication method but multiple remote authentication methods.
Step 5	**identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*} **Example:** `Device(config-ikev2-profile)# identity local email abc@example.com`	This is an optional step. Specifies the local IKEv2 identity type. **Note** If the local authentication method is a preshared key, the default local identity is the IP address. If the local authentication method is a Rivest, Shamir, and Adleman (RSA) signature, the default local identity is a Distinguished Name.
Step 6	**keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] } **Example:** `Device(config-ikev2-profile)# keyring aaa keyring1 name-mangler mangler1`	Specifies the local or AAA-based key ring that must be used with the local and remote preshared key authentication method. **Note** You can specify only one key ring. Local AAA is not supported for AAA-based preshared keys. **Note**

	Command or Action	Purpose
		Depending on your release, the **local** keyword and the **name-mangler** *mangler-name* keyword-argument pair should be used. **Note** When using AAA, the default password for a Radius access request is "cisco". You can use the **password** keyword within the **keyring** command to change the password.
Step 7	**match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*} **Example:** `Device(config-ikev2-profile)# match address local interface Ethernet 2/0`	Uses match statements to select an IKEv2 profile for a peer.
Step 8	**pki trustpoint** *trustpoint-label* [**sign** | **verify**] **Example:** `Device(config-ikev2-profile)# pki trustpoint tsp1 sign`	Specifies Public Key Infrastructure (PKI) trustpoints for use with the RSA signature authentication method. **Note** If the **sign** or **verify** keyword is not specified, the trustpoint is used for signing and verification. **Note** In contrast to IKEv1, a trustpoint must be configured in an IKEv2 profile for certificate-based authentication to succeed. There is no fallback for globally configured trustpoints if this command is not present in the configuration. The trustpoint configuration applies to the IKEv2 initiator and responder.
Step 9	**end** **Example:** `Device(config-ikev2-profile)# end`	Exits the IKEv2 profile configuration mode and returns to the privileged EXEC mode.

Configuring GKM Policy on a Key Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gkm group** [**ipv6**] *group-name*
4. **server local**
5. **gikev2** *IKEv2-profile-name*
6. **end**

DETAILED STEPS

Procedure

	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 gkm group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gkm group gkm-grp1`	Configures a GKM policy and enters GKM group configuration mode.
Step 4	**server local** **Example:** `Device(config-gkm-group)# server local`	Designates a device as a GKM key server and enters GKM local server configuration mode.
Step 5	**gikev2** *IKEv2-profile-name* **Example:** `Device(gkm-local-server)# gikev2 gkm-gikev2`	Enables G-IKEv2 profile for registration and rekey on a key server.
Step 6	**end** **Example:** `Device(gkm-local-server)# end`	Exits GKM local server configuration mode and returns to privileged EXEC mode.

Configuring GKM Policy on Group Member

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gkm group** [**ipv6**] *group-name*
4. **client protocol gikev2** *gkm-gikev2*
5. **end**

DETAILED STEPS

Procedure

	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 gkm group** [**ipv6**] *group-name* **Example:** `Device(config)# crypto gkm group gkm-grp2`	Configures a GKM policy and enters GKM group configuration mode.
Step 4	**client protocol gikev2** *gkm-gikev2* **Example:** `Device(config-gkm-group)# client protocol gikev2 gkm-gikev2`	Enables G-IKEv2 profile for registration and rekey on a group member.
Step 5	**end** **Example:** `Device(config-gkm-group)# end`	Exits GKM group configuration mode and returns to privileged EXEC mode.

Additional References for GETVPN G-IKEv2

Related Documents

Related Topic	Document Title
Security Commands	• *Cisco IOS Security Command Reference Commands A to C* • *Cisco IOS Security Command Reference Commands D to L* • *Cisco IOS Security Command Reference Commands M to R* • *Cisco IOS Security Command Reference Commands S to Z*

Standards and RFCs

Standard/RFC	Title
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
Group Key Management using IKEv2	*draft-yeung-g-ikev2-07*

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 GETVPN G-IKEv2

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for GETVPN G-IKEv2

Feature Name	Releases	Feature Information
GETVPN G-IKEv2		The following commands were introduced or modified: **client protocol**, **crypto gkm group**, **gikev2**, **show crypto gkm**.